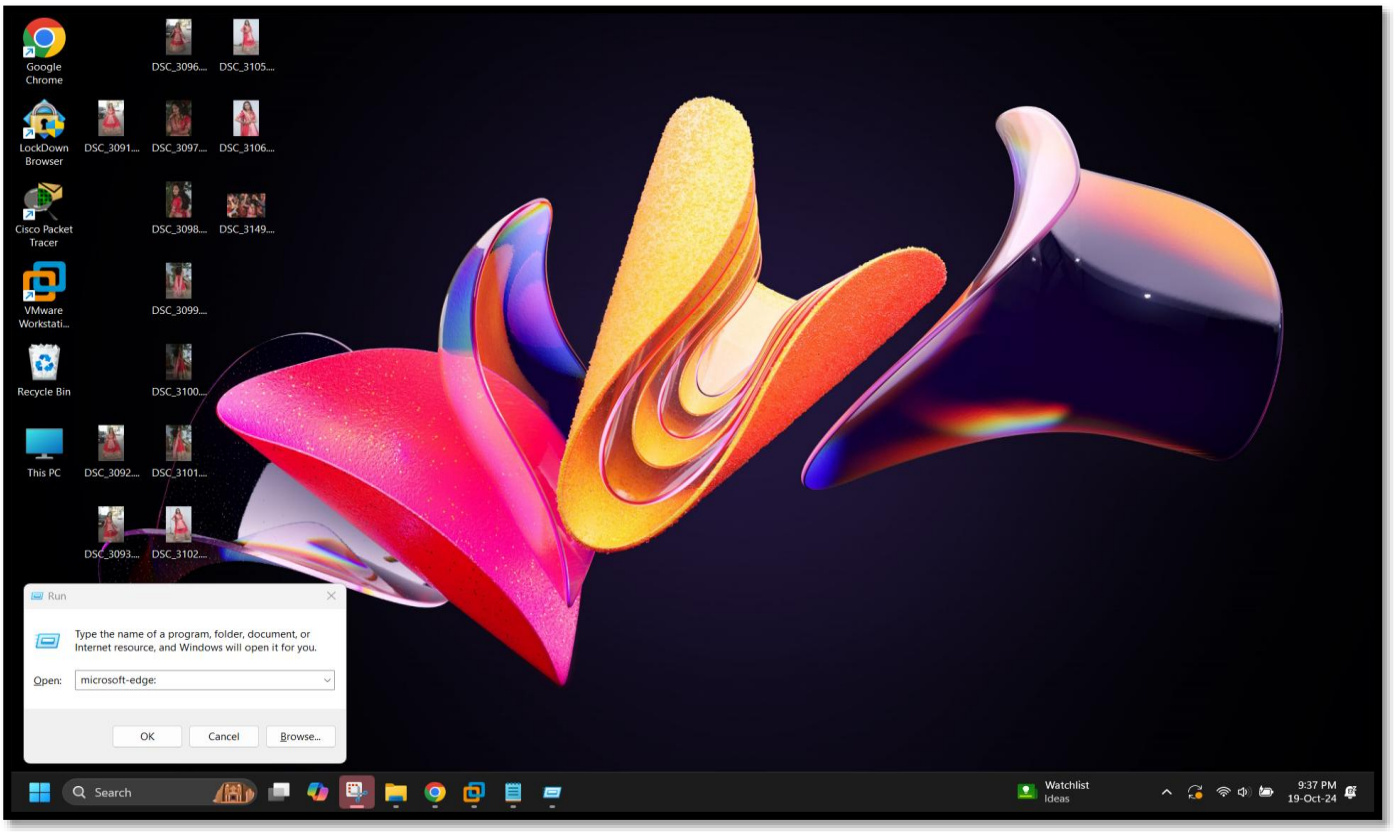
Name: Shivani Shaileshkumar Varu Student ID: 101481565

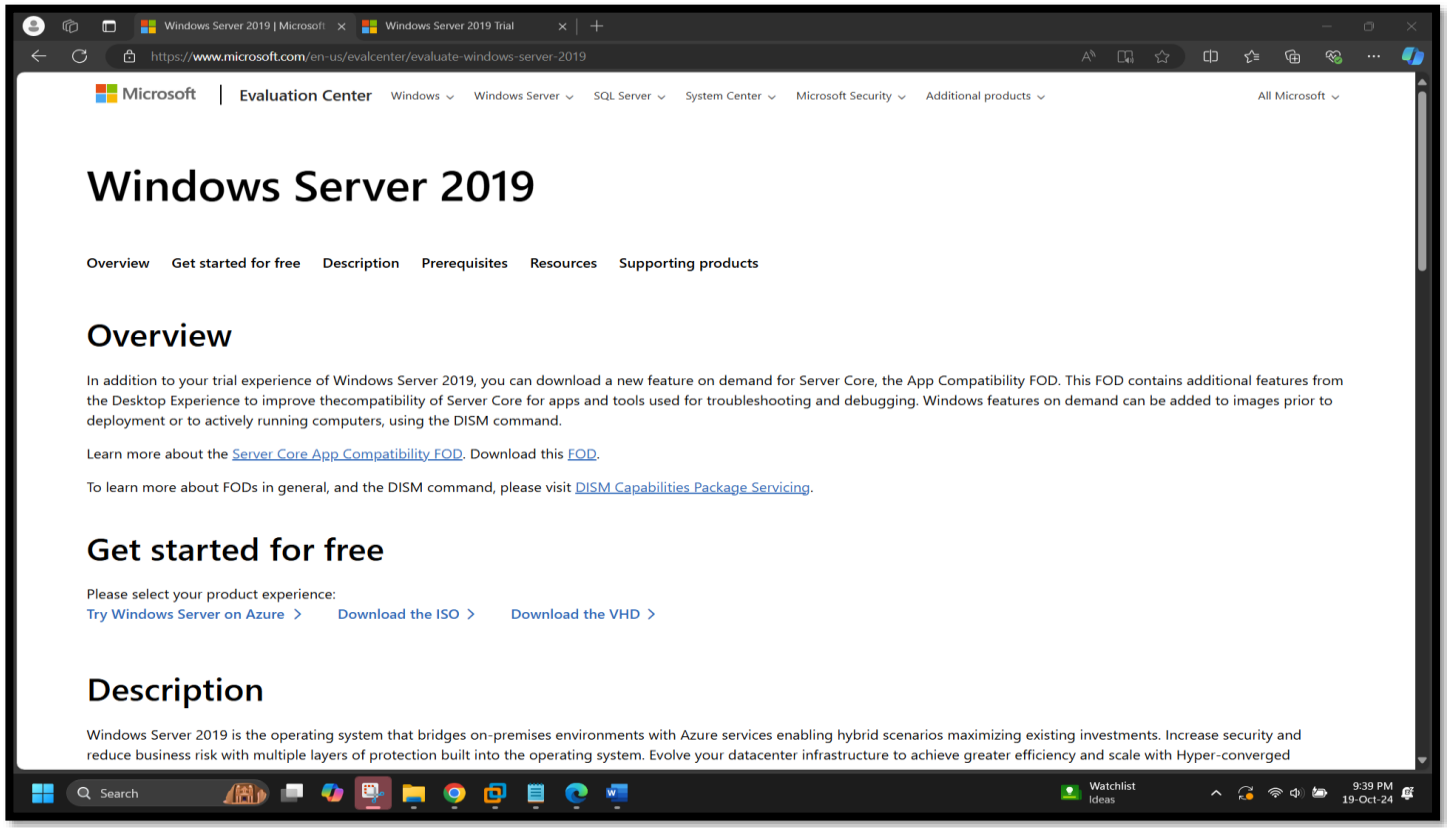
Exercise – 1 Downloading Windows Server 2019, Download Windows Admin Center, Use the VMware to install the server on a VM machine

[Screenshot 1 : Opening Microsoft Edge via Run Command]

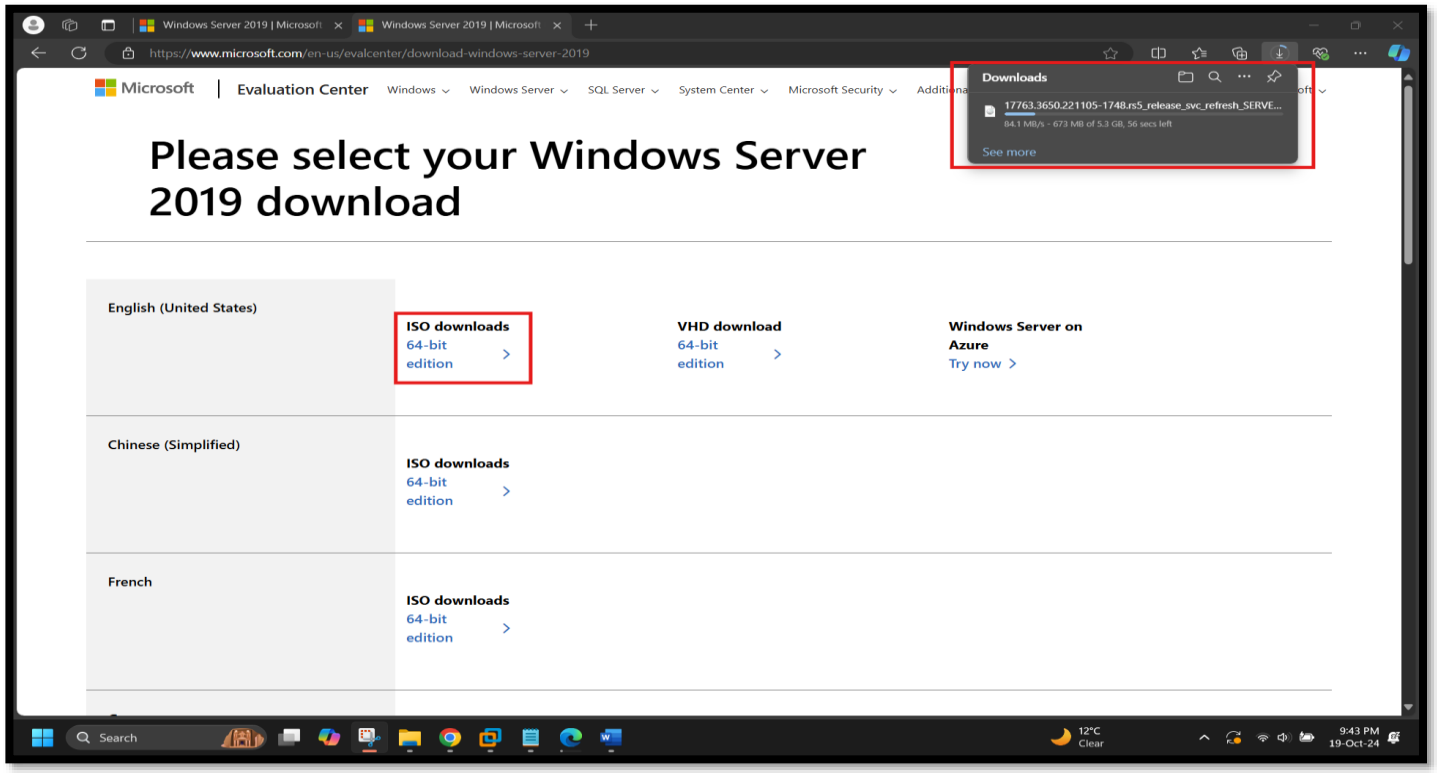


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 2: Opened Windows Server 2019 on Microsoft page]

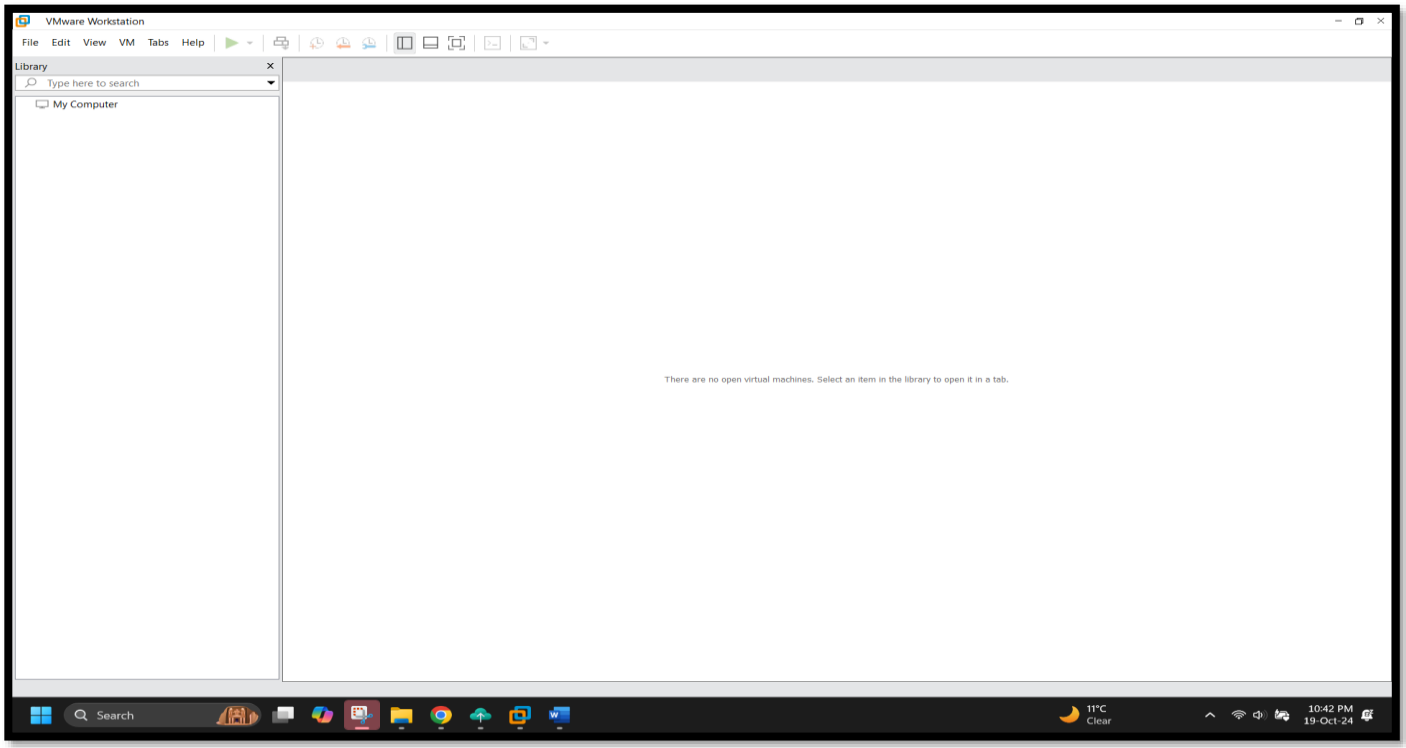


[Screenshot 3: Downloading ISO file of Windows Server 2019 from Microsoft Windows Server 2019]

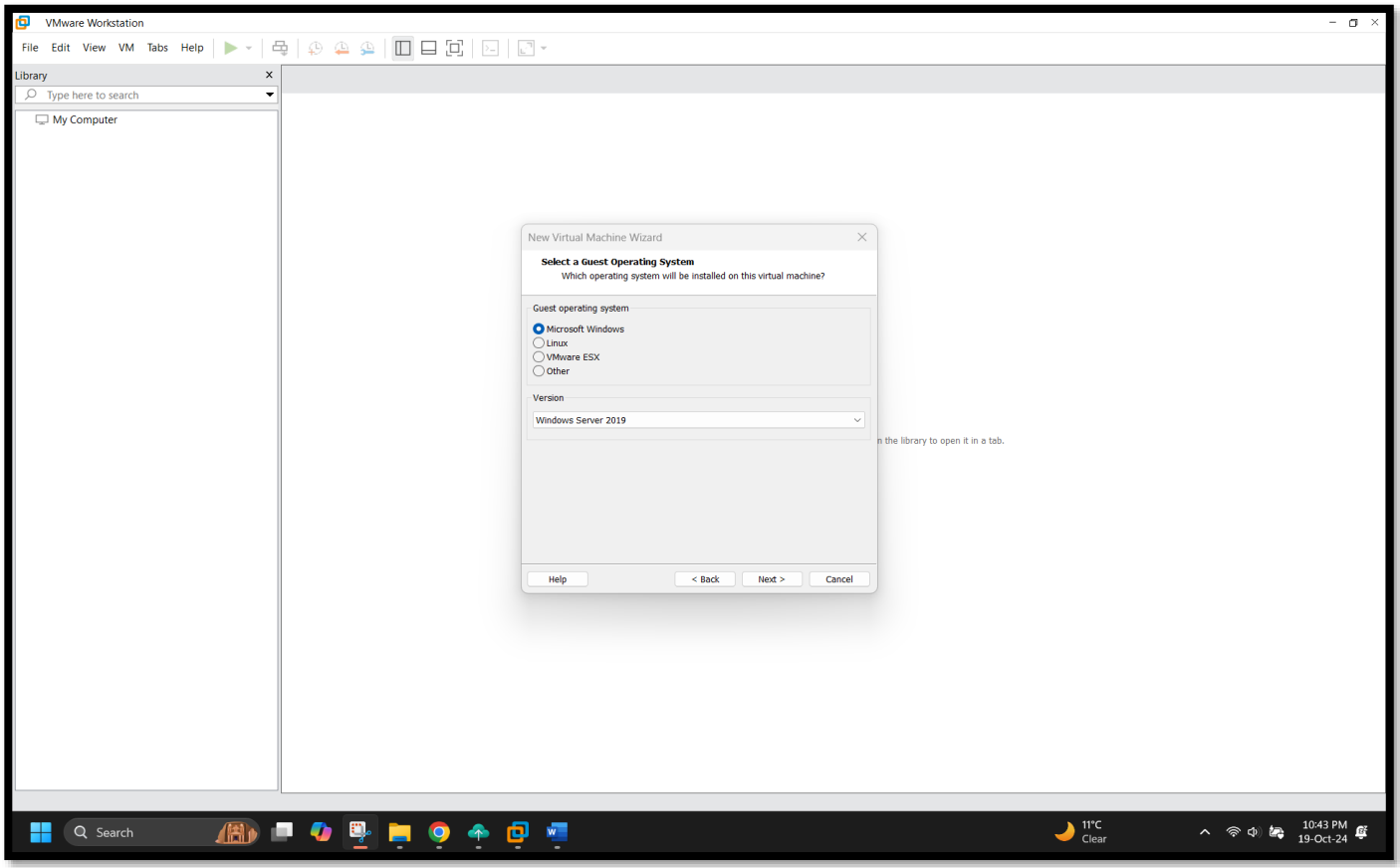


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 4: Installed and Download VM ware Workstation Pro]

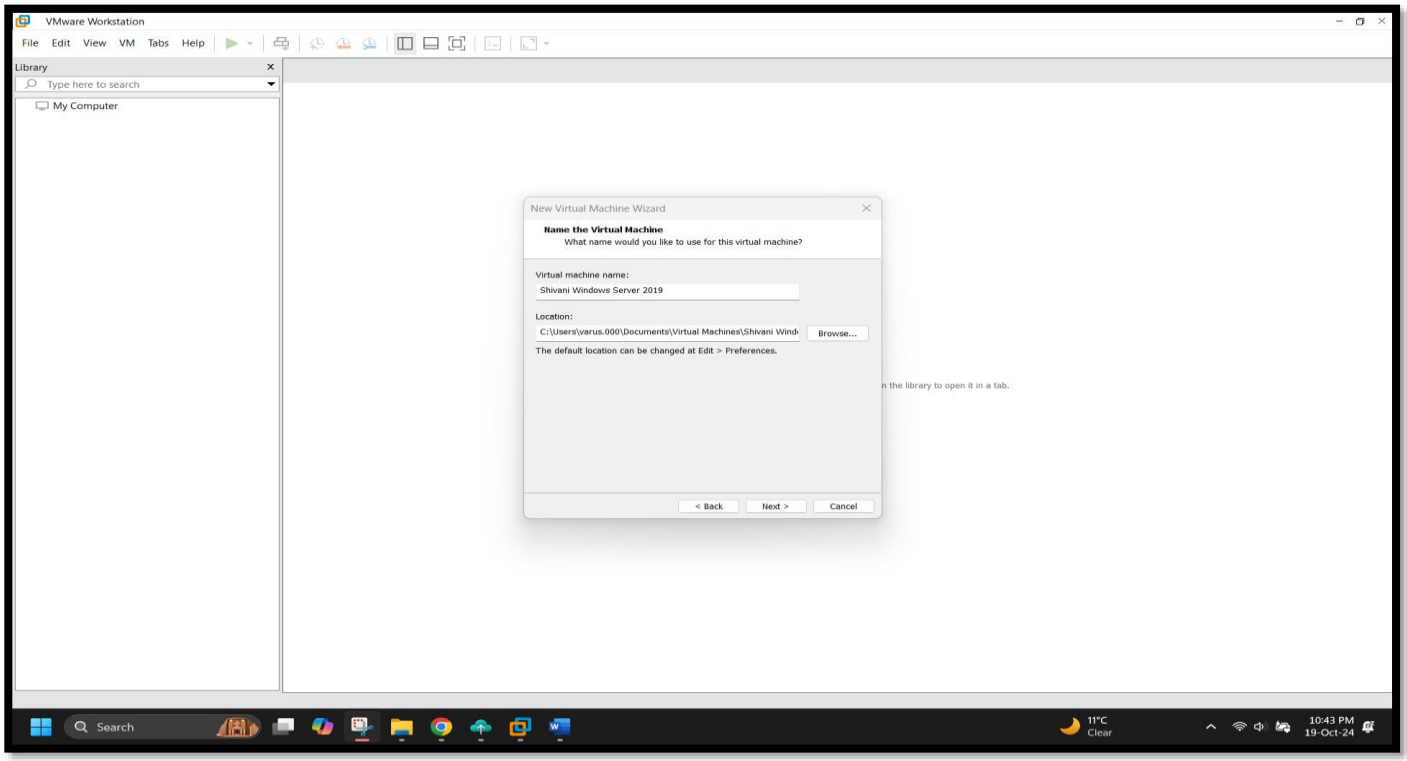


[Screenshot 5: Added Microsoft Windows as Guest Operating System on VM]

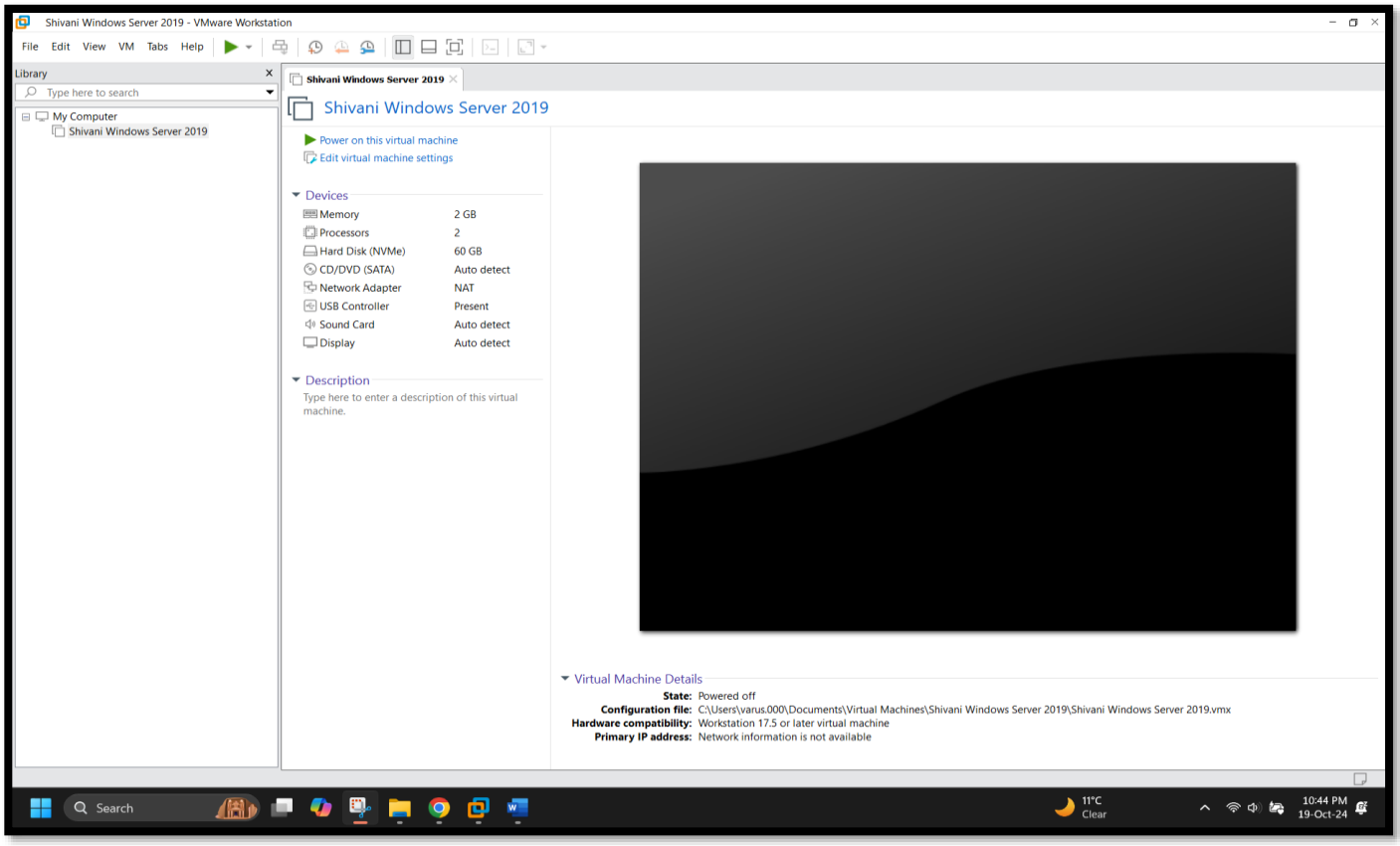


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 6 : Naming the windows server 2019 on VM]

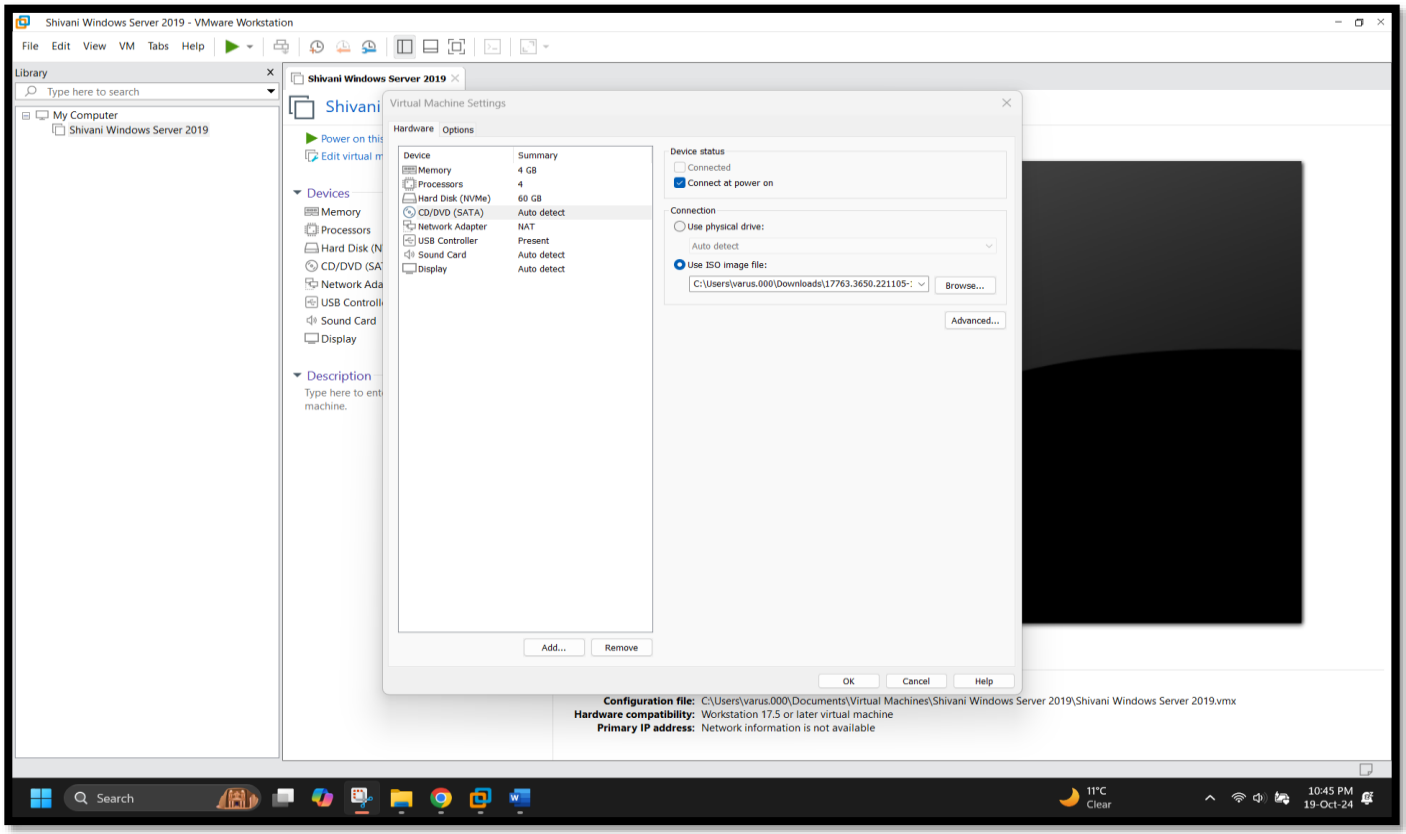


[Screenshot 7 : Windows Server 2019 Added on VM]

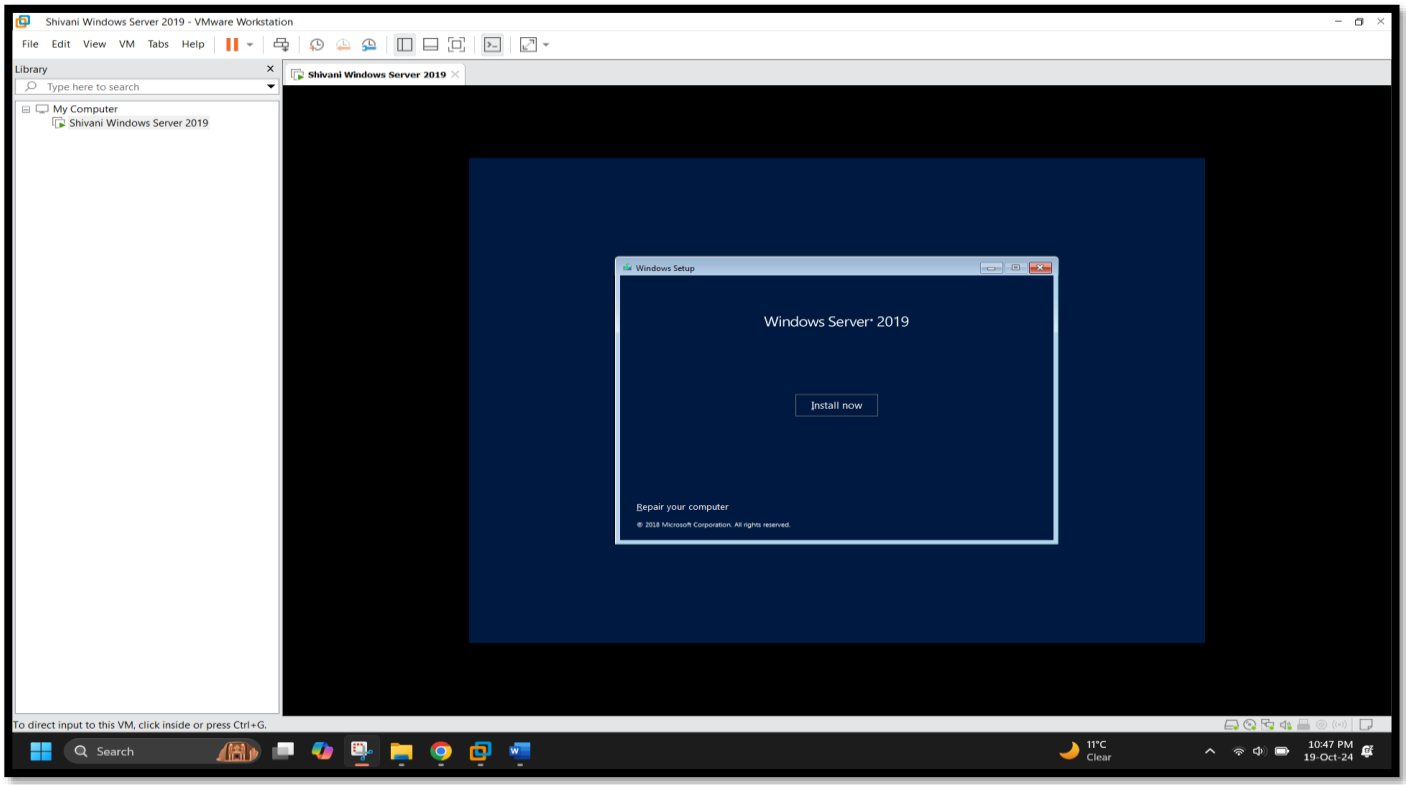


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 6 : Added ISO file of Windows Server 2019 inside Vm]

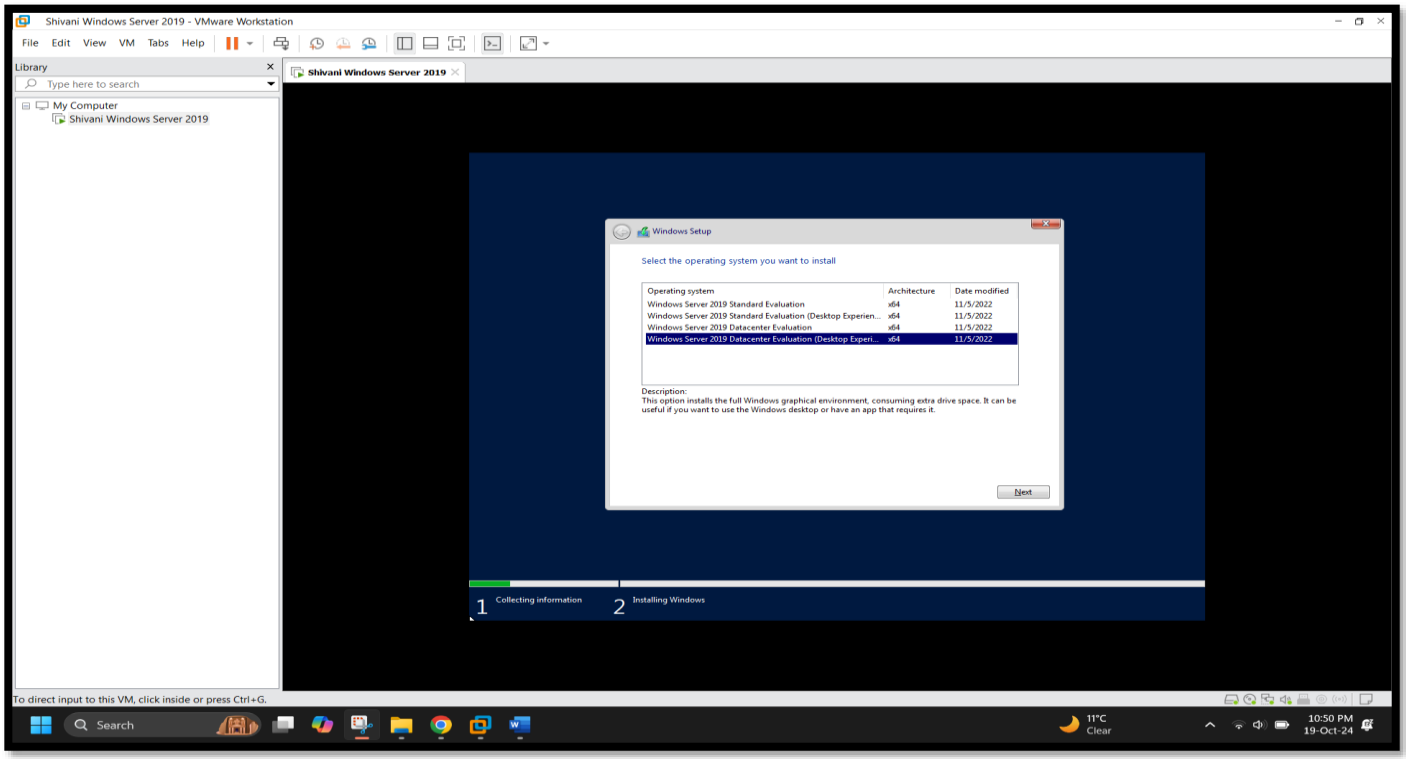


[Screenshot 7 : Installing Windows Server 2019 on VM]

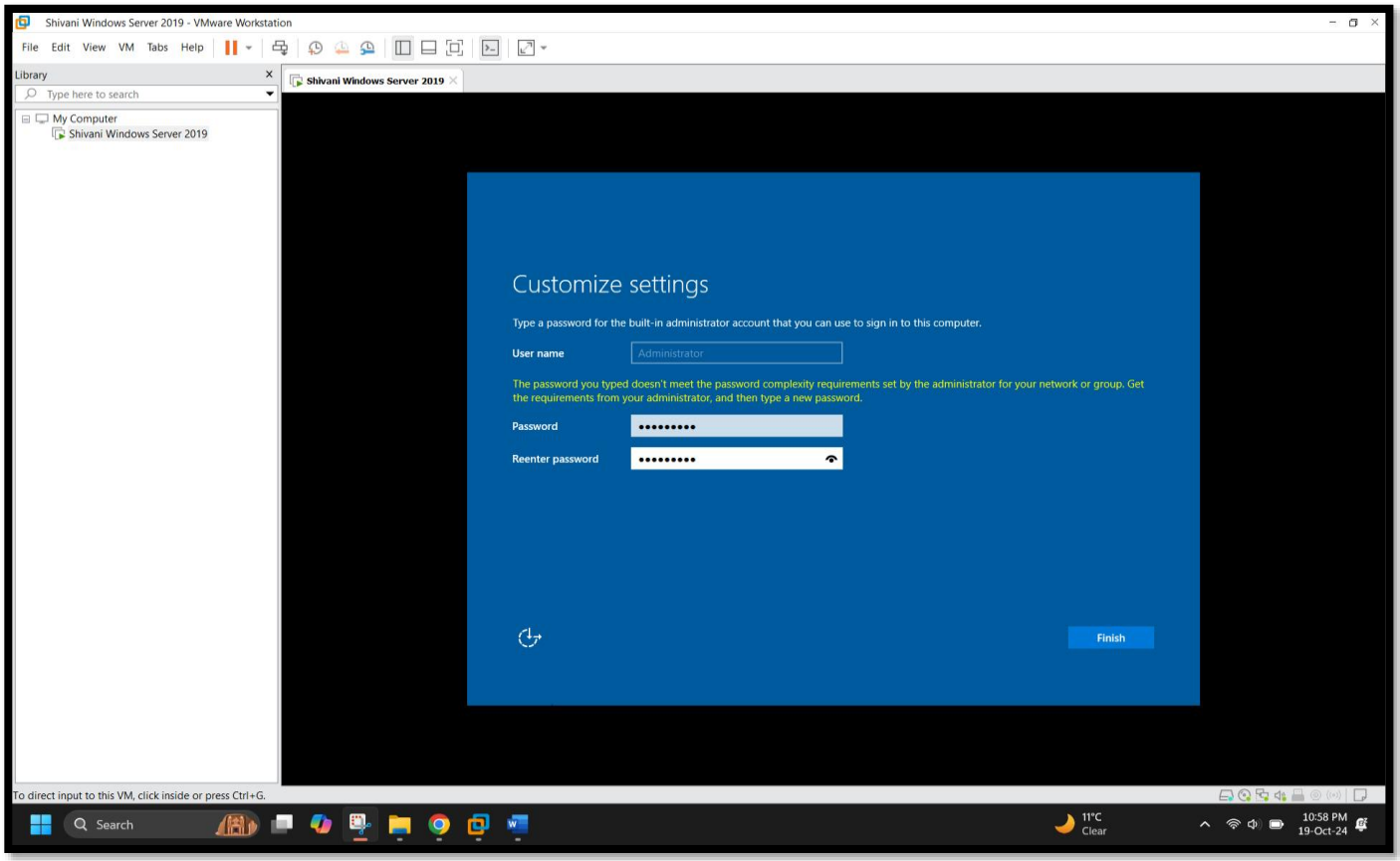


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 8 : Selecting Windows Server 2019 Datacenter Evaluation (Desktop Experience)]

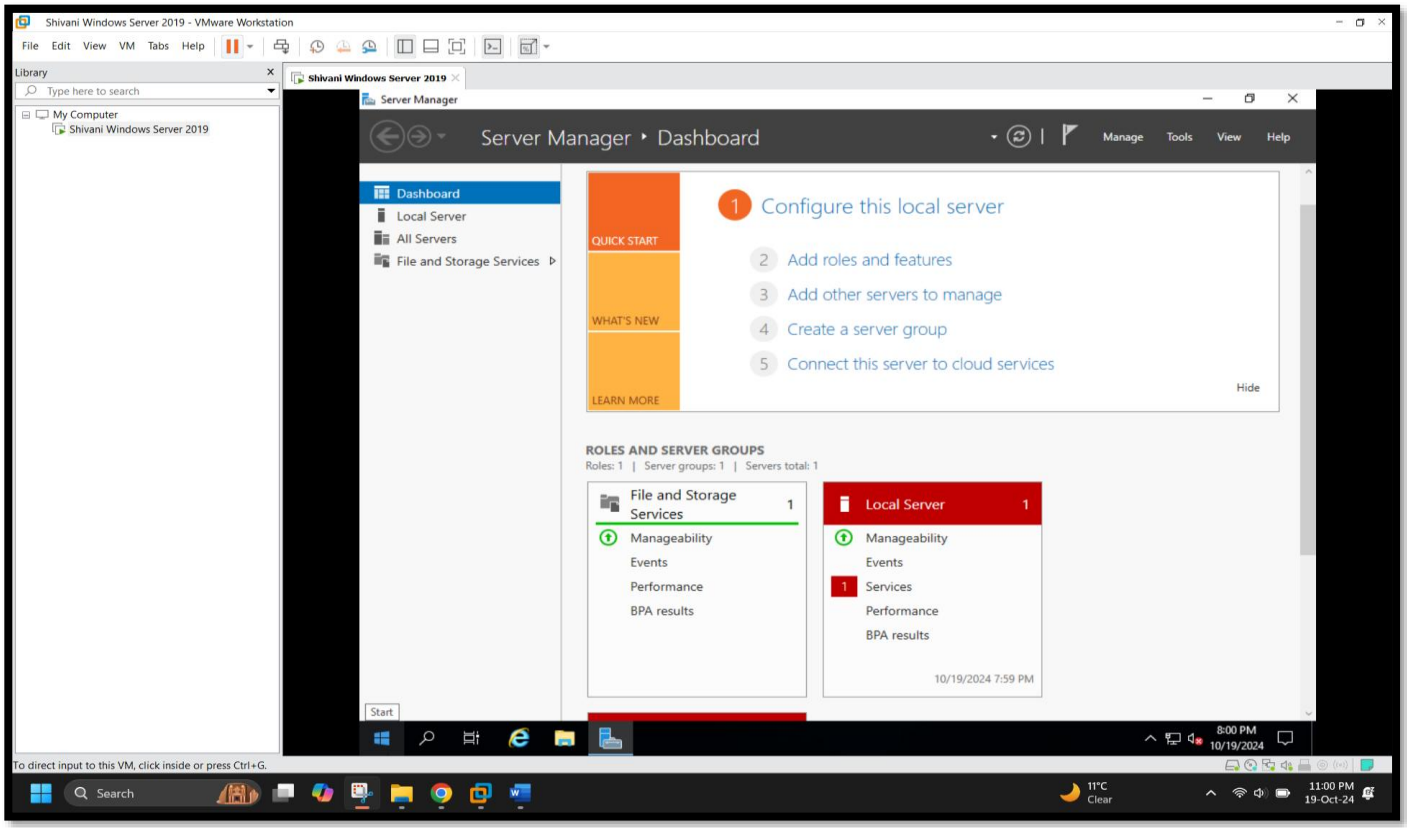


[Screenshot 9: added Administration ID and Password]

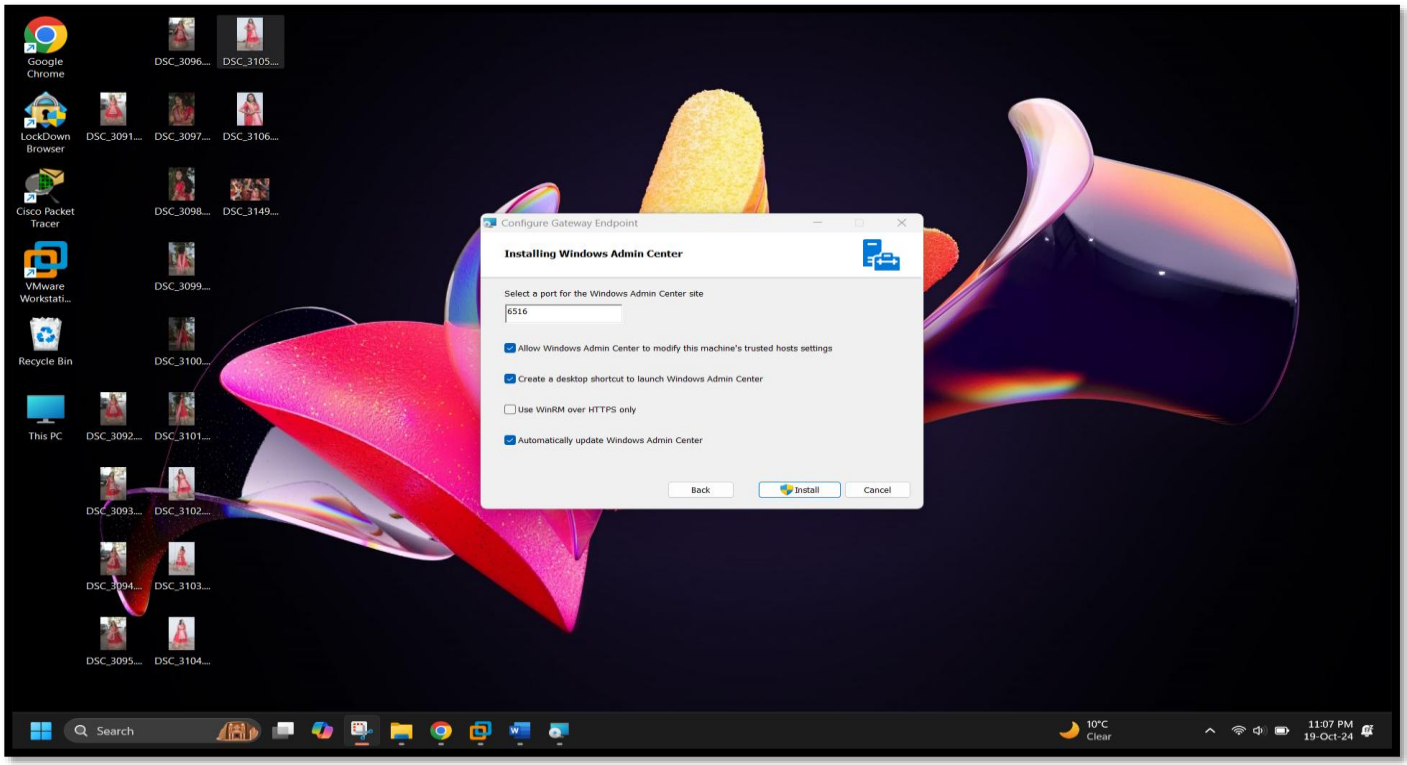


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 10 : Successfully Install Windows Server 2019 on VM]

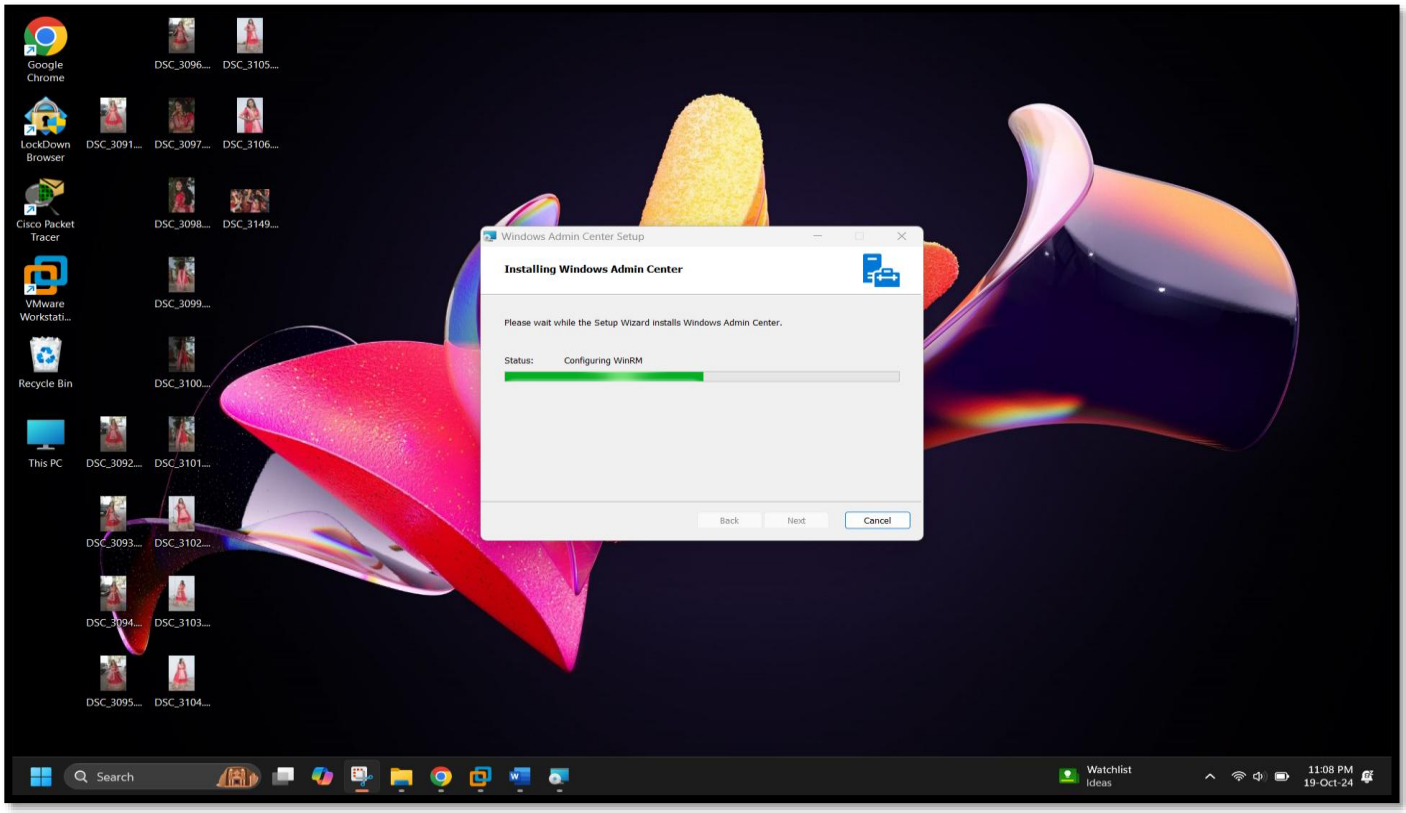


[Screenshot 11: Installing **Windows Admin Center** on Host machine]

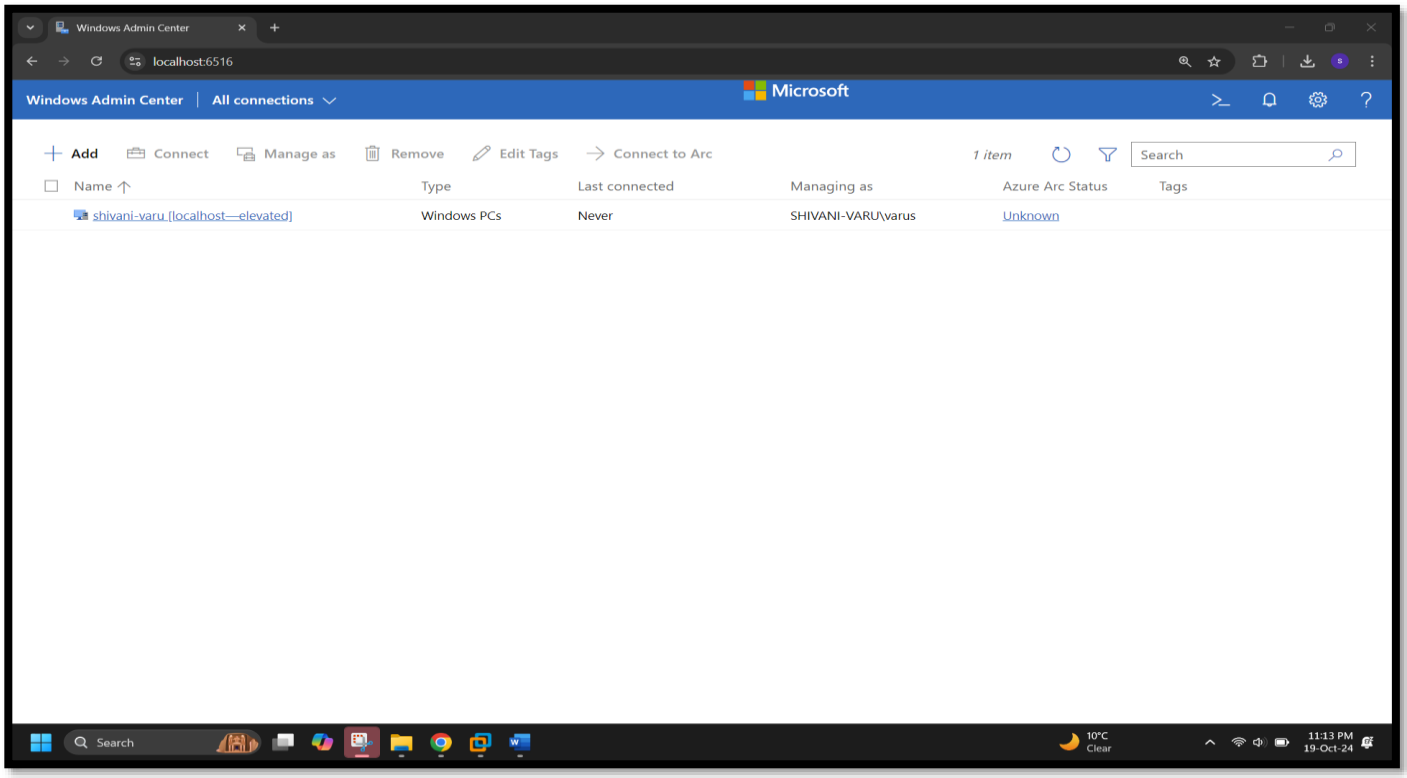


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 12 : Installing WAC on Host machine]

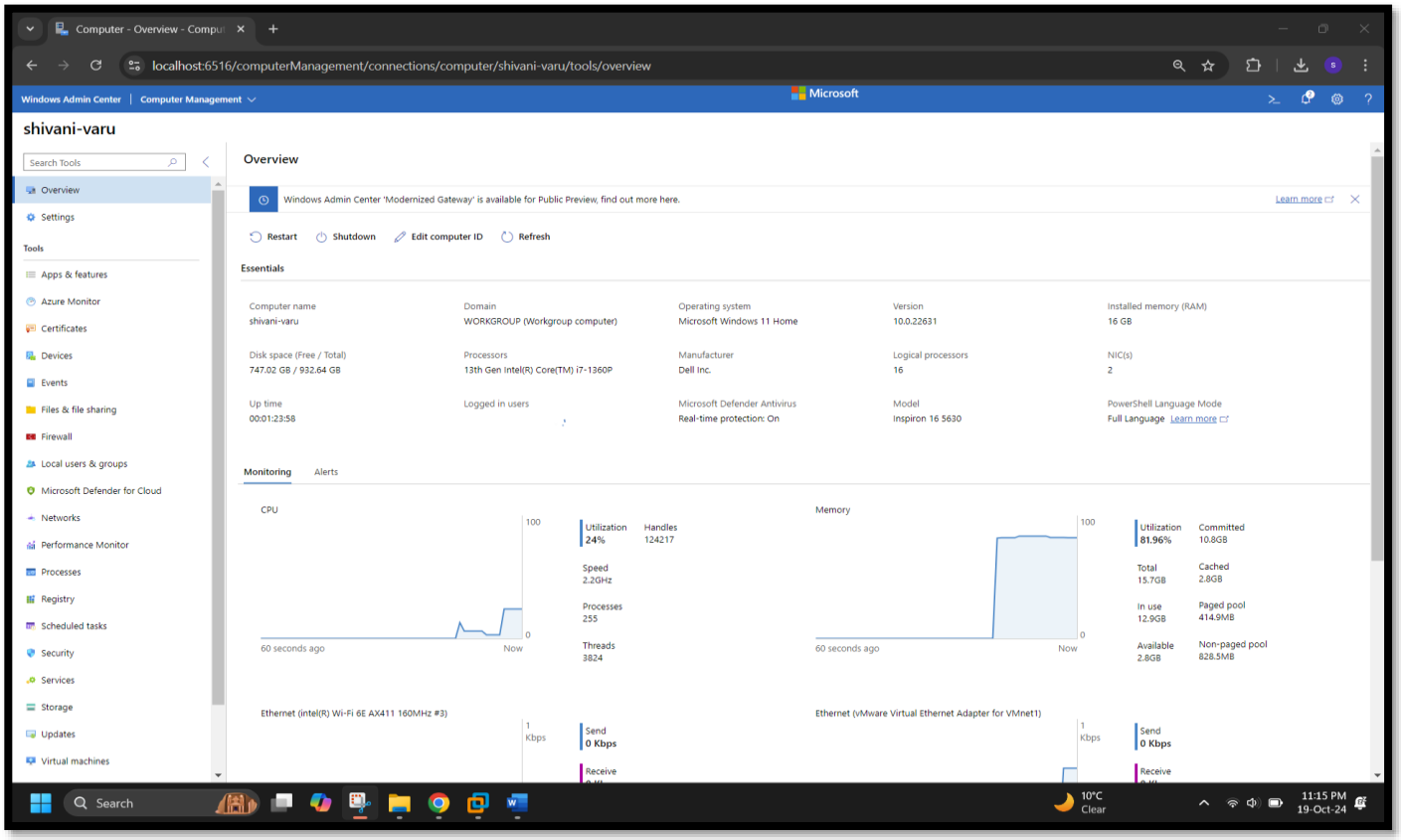


[Screenshot 13 : Successfully Installed **Windows Admin Center** on Host machine to manage]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

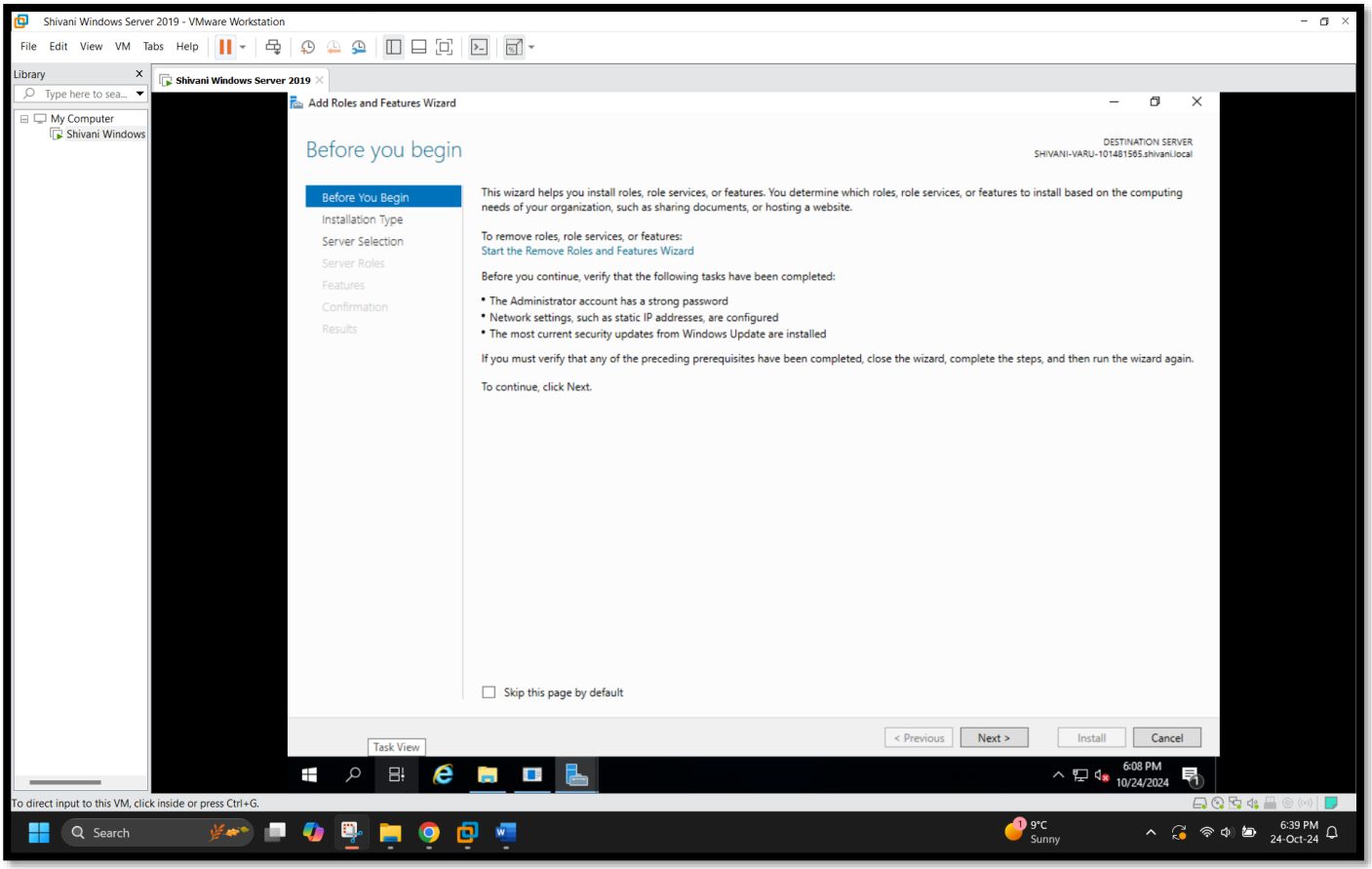
[Screenshot 14 : Viewing Overview Of Windows Admin Center]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

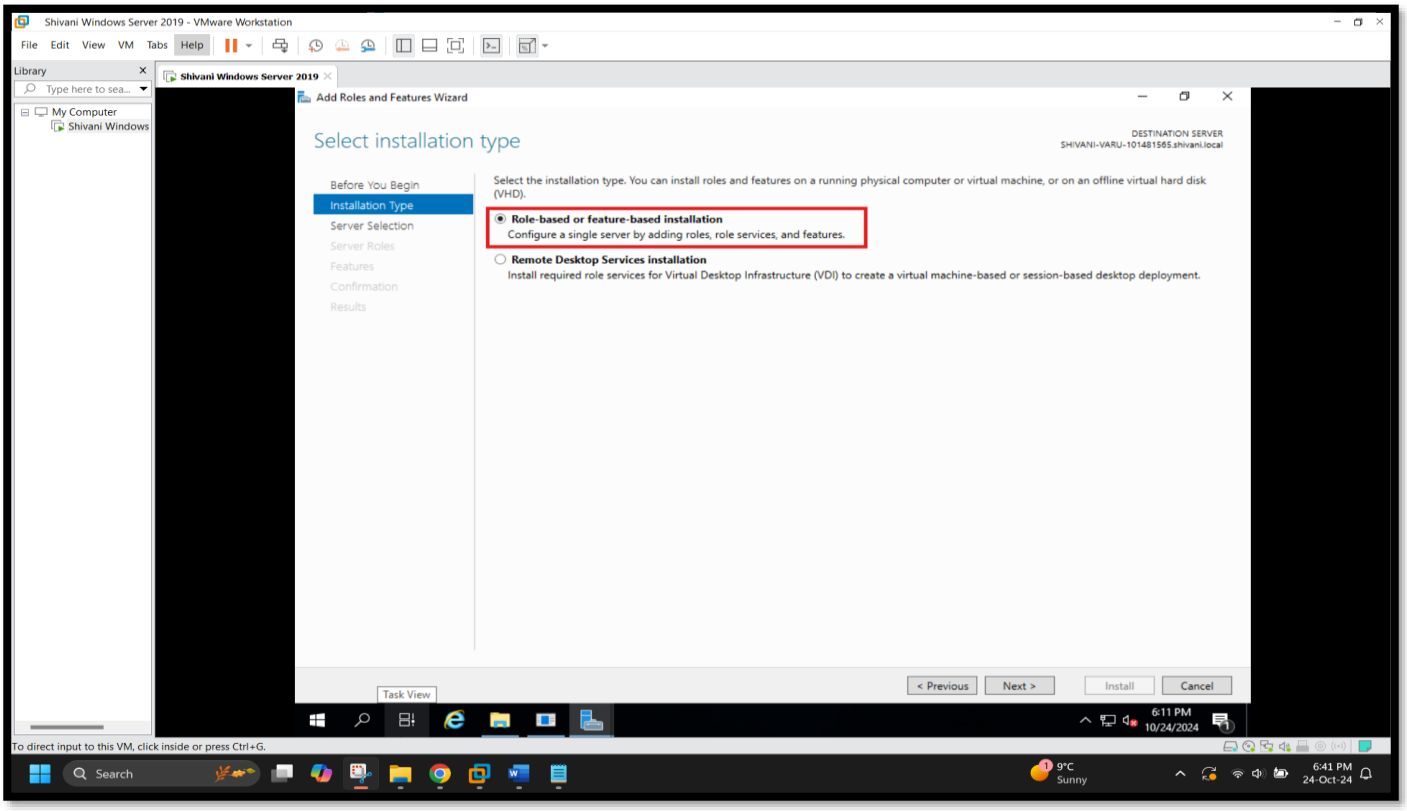
Exercise – 2 Installing and Setting up Windows Deployment Services, WDS

[Screenshot 1 : Starting the Add Roles and Features Wizard on Windows Server 2019 in VMware Workstation]

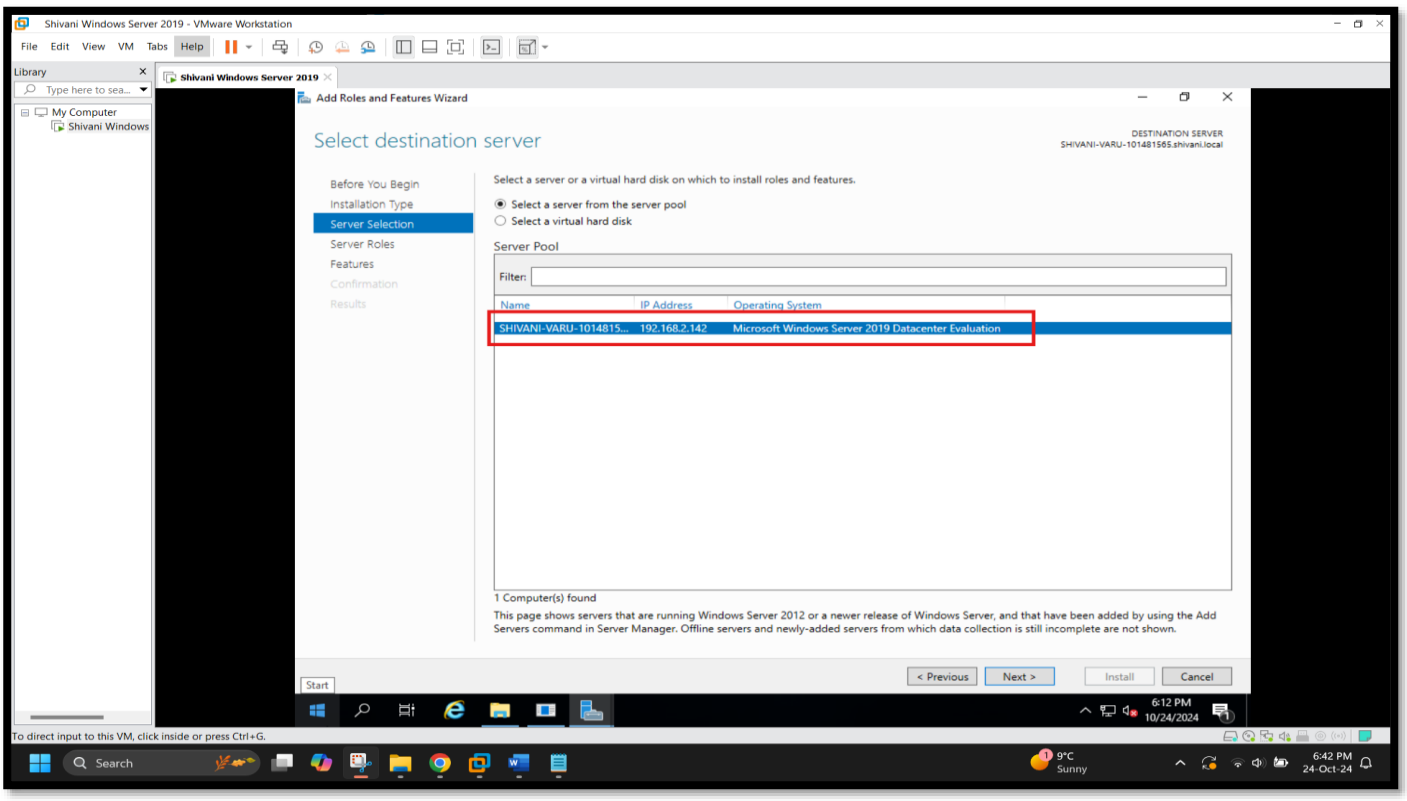


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 2 : Selecting Installation Type in the Add Roles and Features]

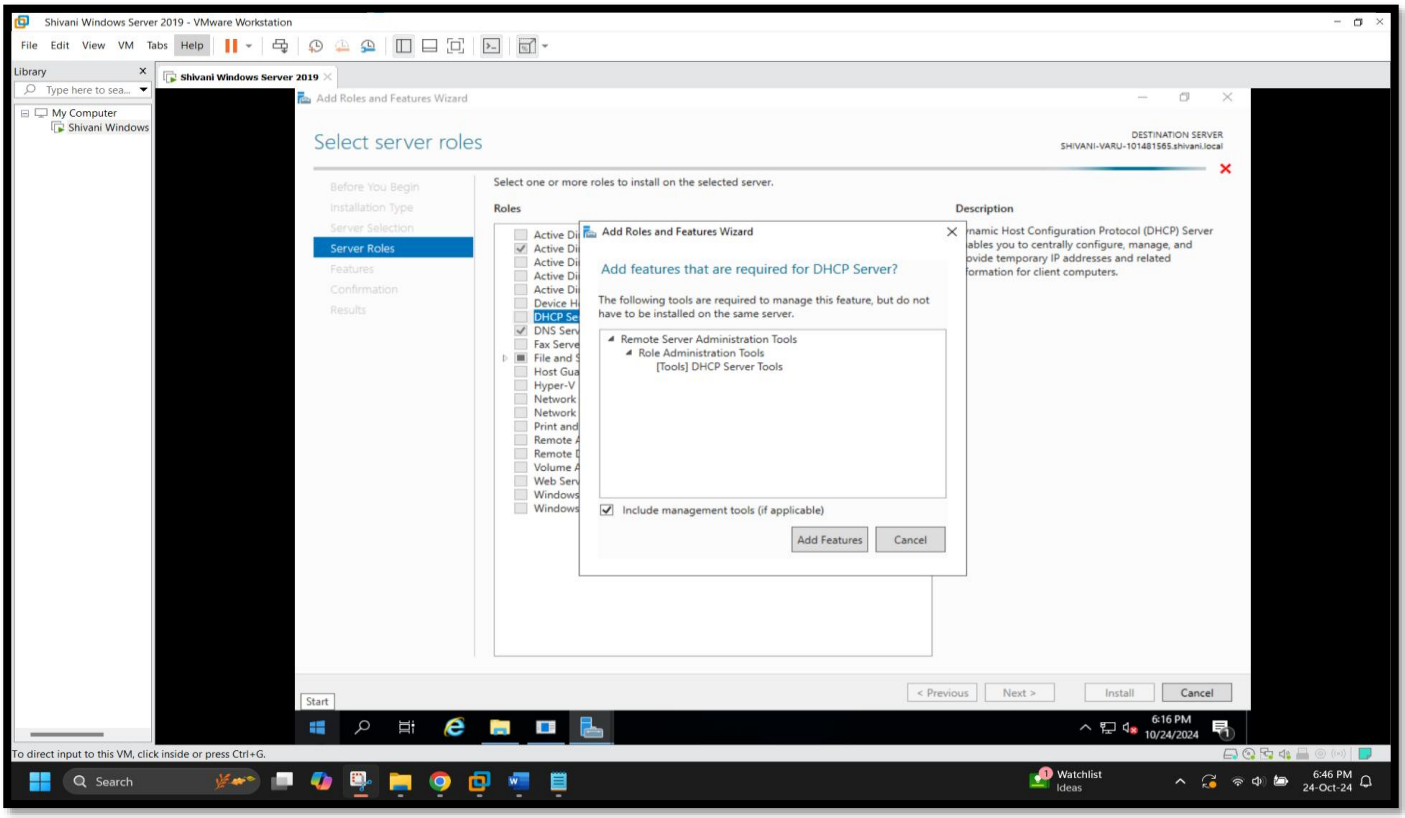


[Screenshot 3 : Selecting the Destination Server in the Add Roles and Features]

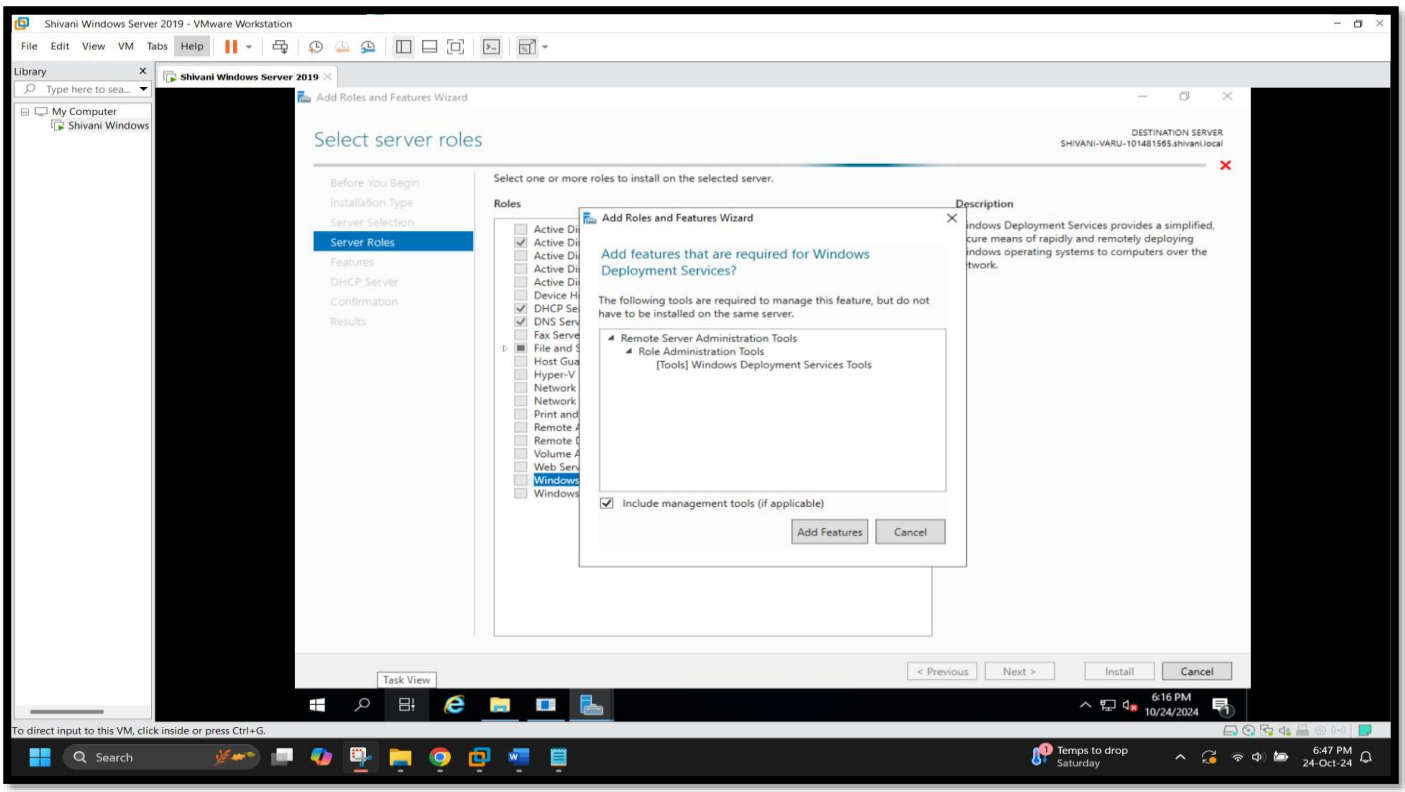


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 4: Selecting DHCP Server Role in the Add Roles and Features]

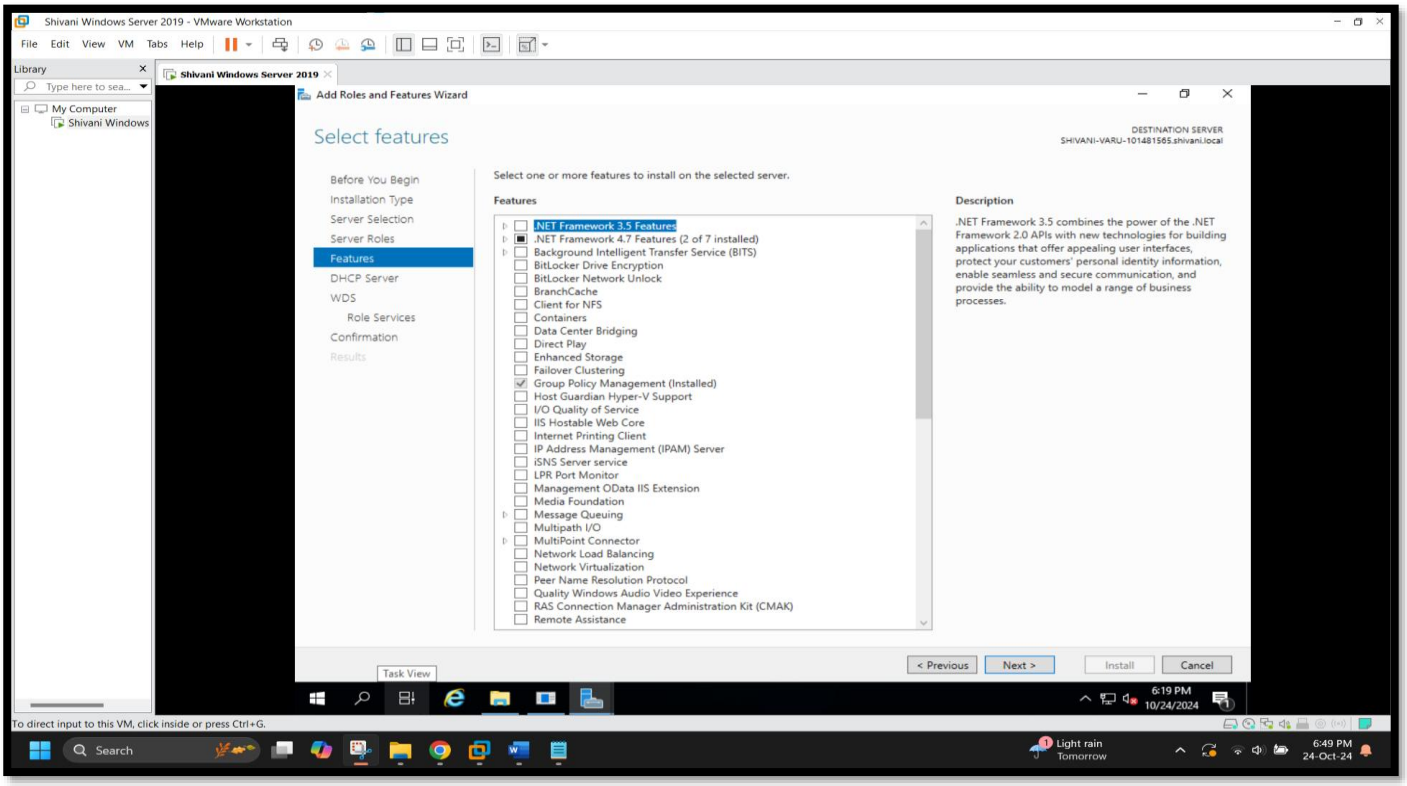


[Screenshot 5: Selecting Windows Deployment Services Role in the Add Roles and Features]

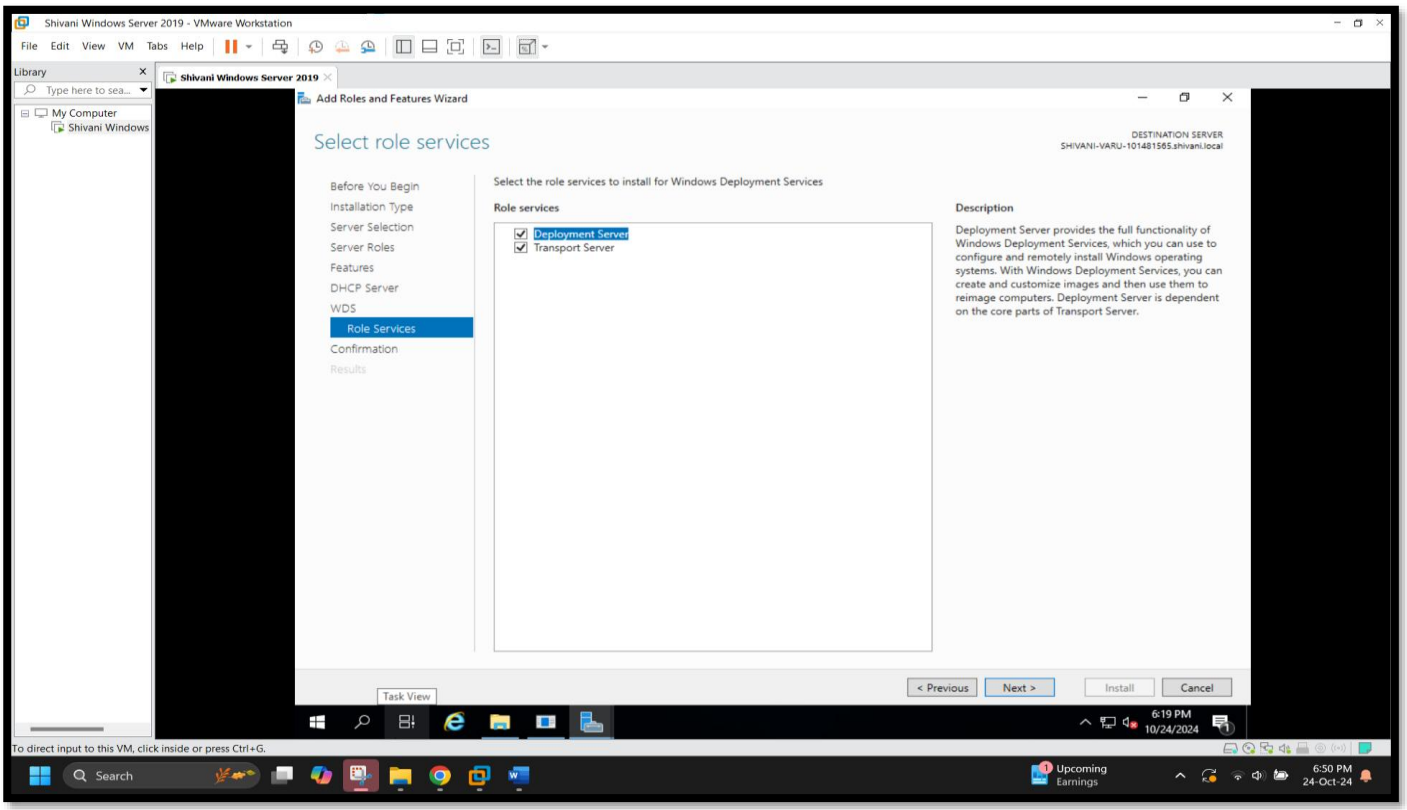


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 6: Selecting Additional Features in the Add Roles and Features]

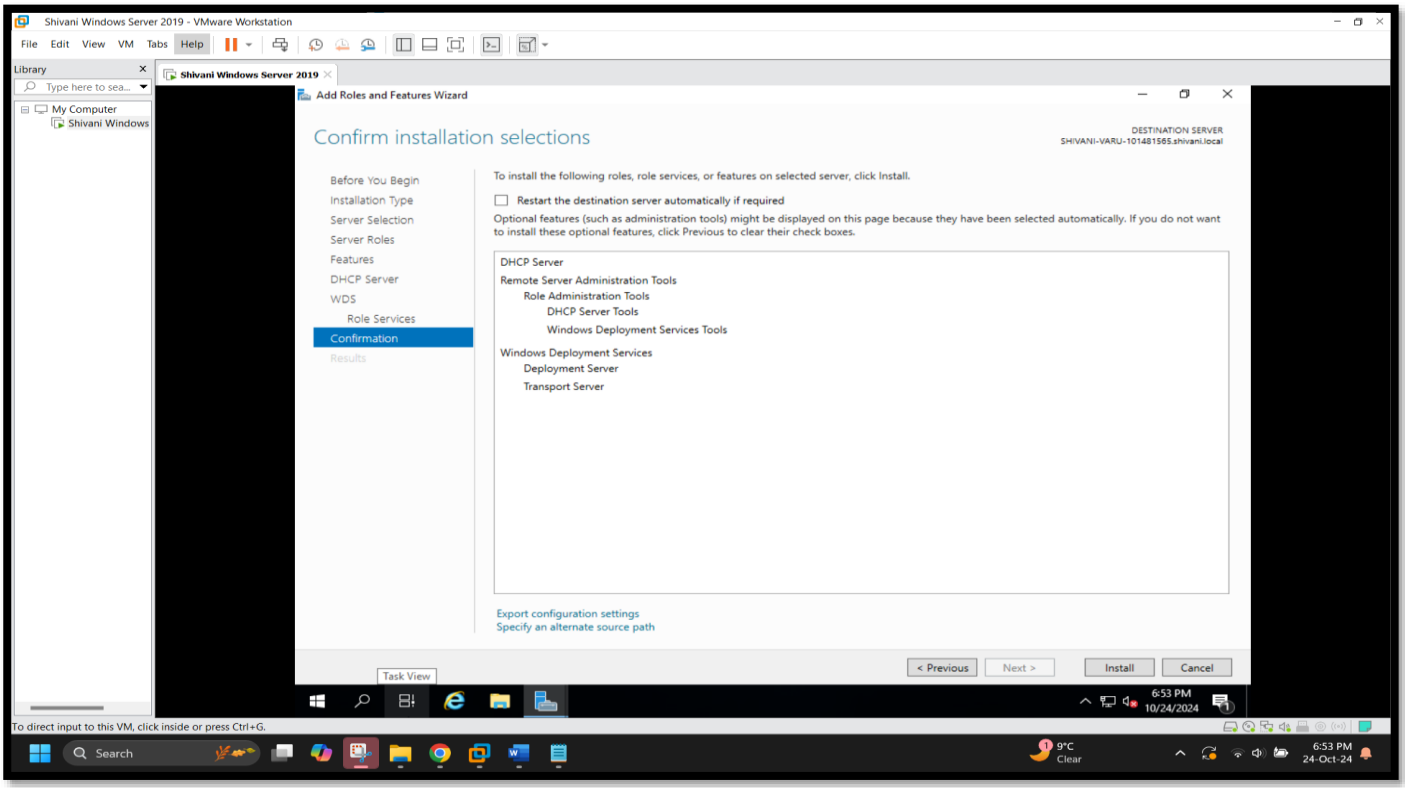


[Screenshot 7: Selecting Role Services for Windows Deployment Services]

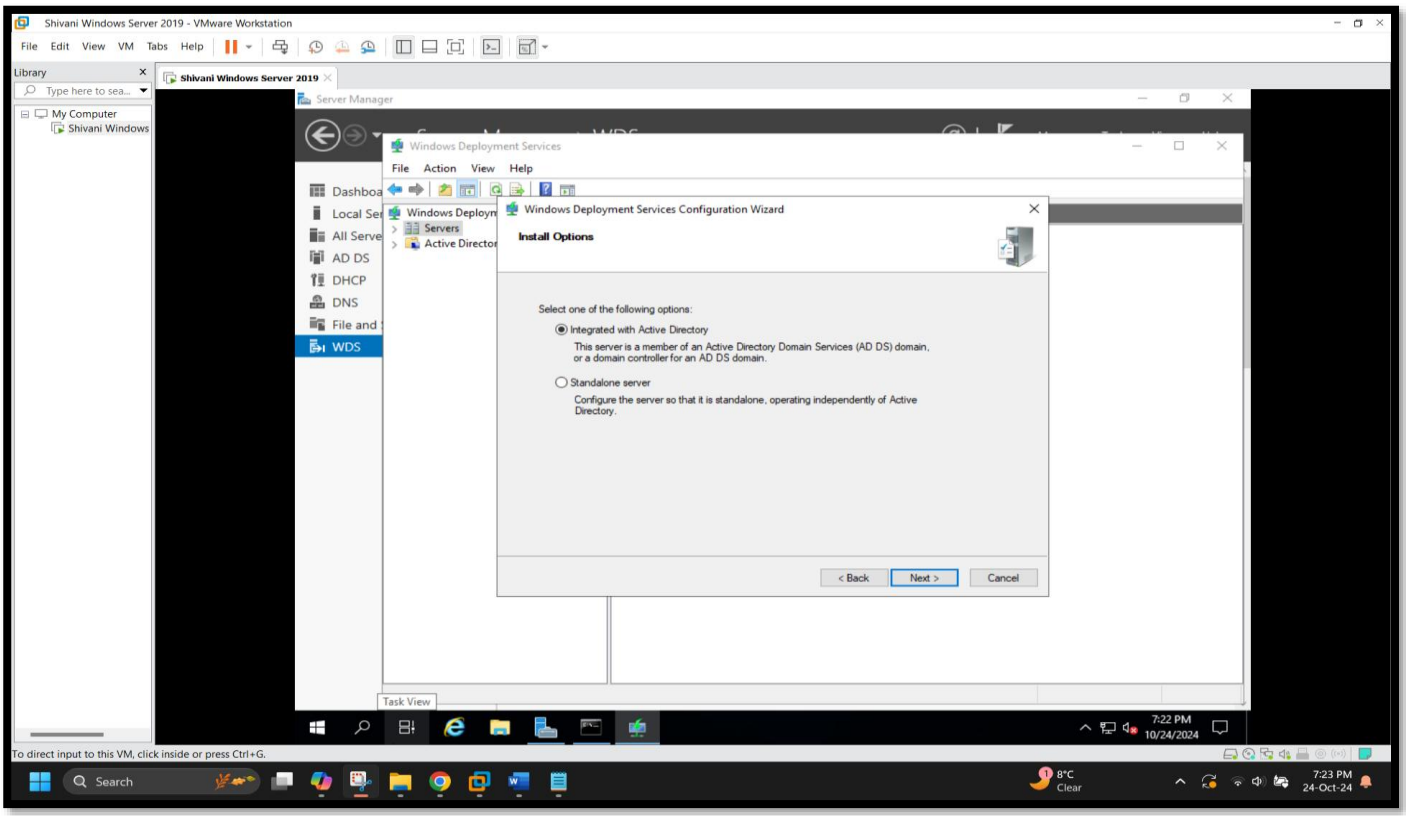


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 8: Confirm installation selections for DHCP Server and WDS roles]

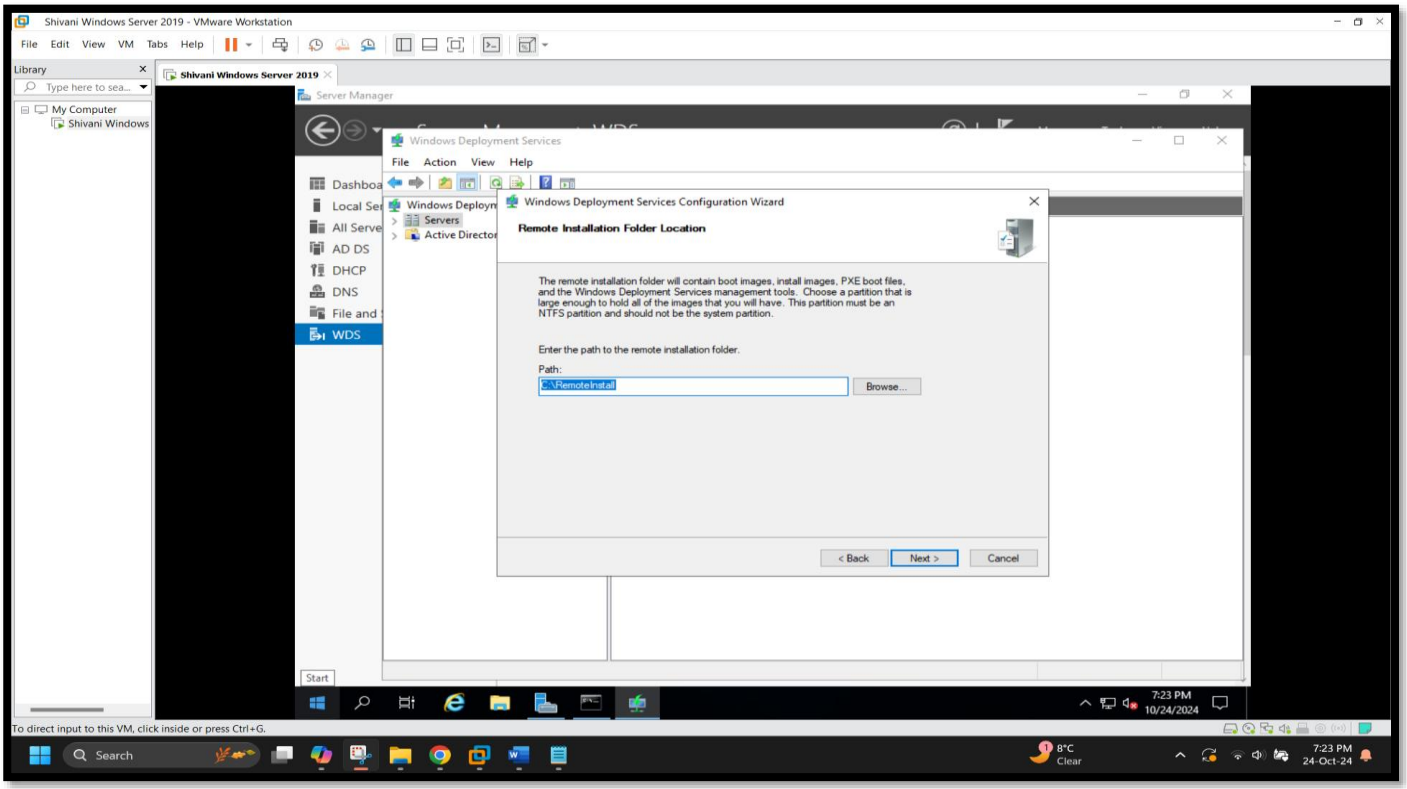


[Screenshot 9: Selecting installation option as Integrated with Active Directory]

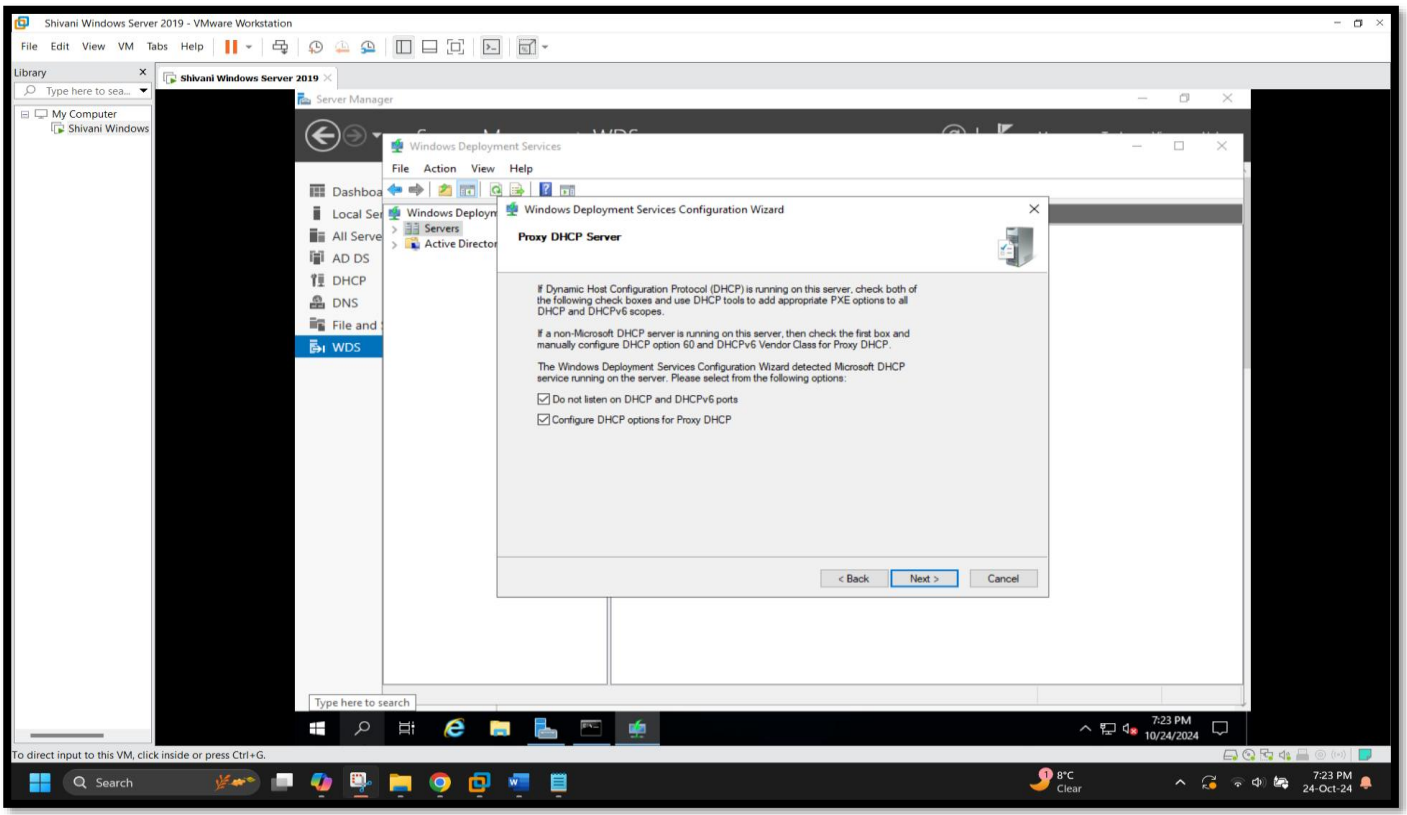


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 10: Specify the remote installation folder location for Windows Deployment Services]

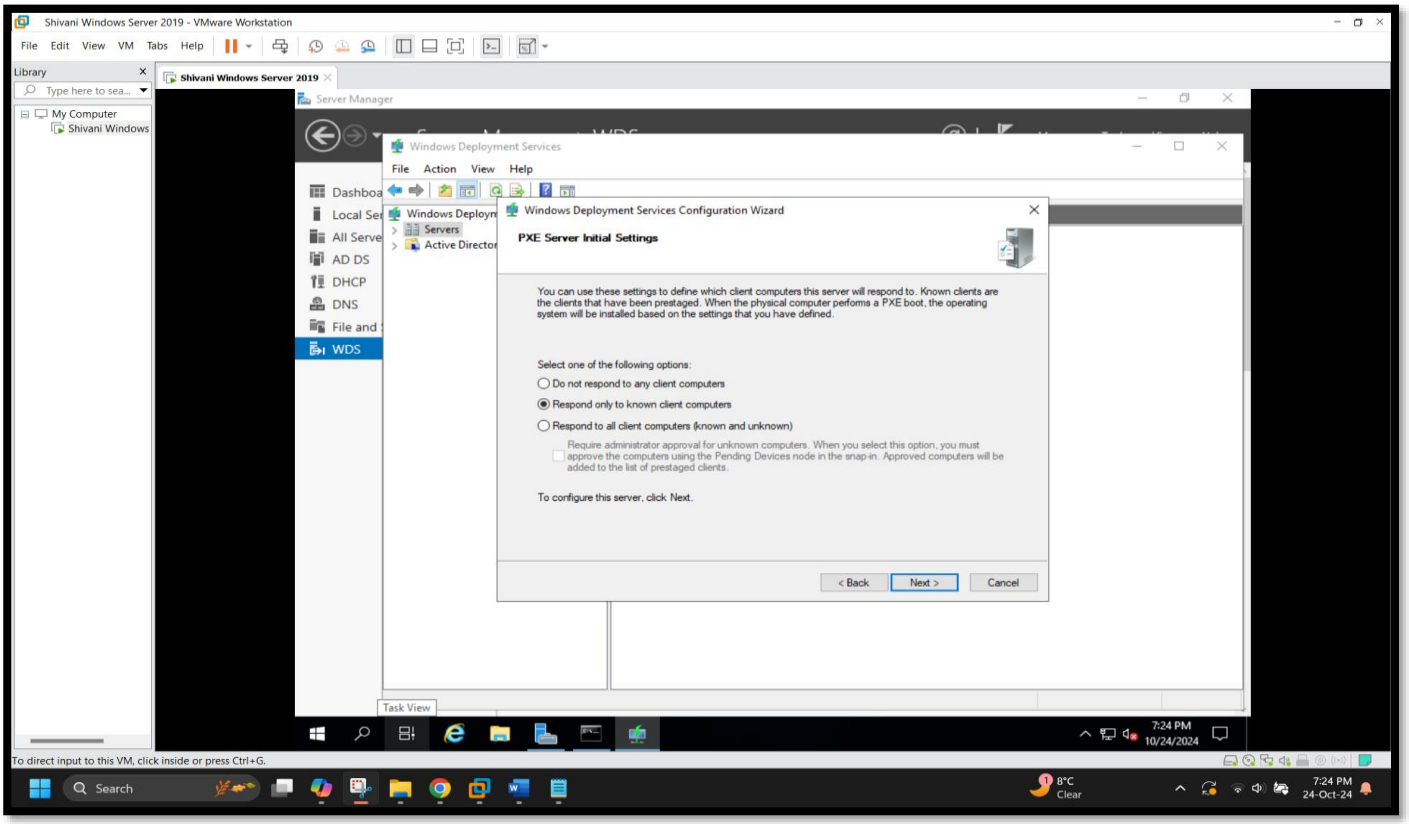


[Screenshot 11: Configure Proxy DHCP Server in WDS]

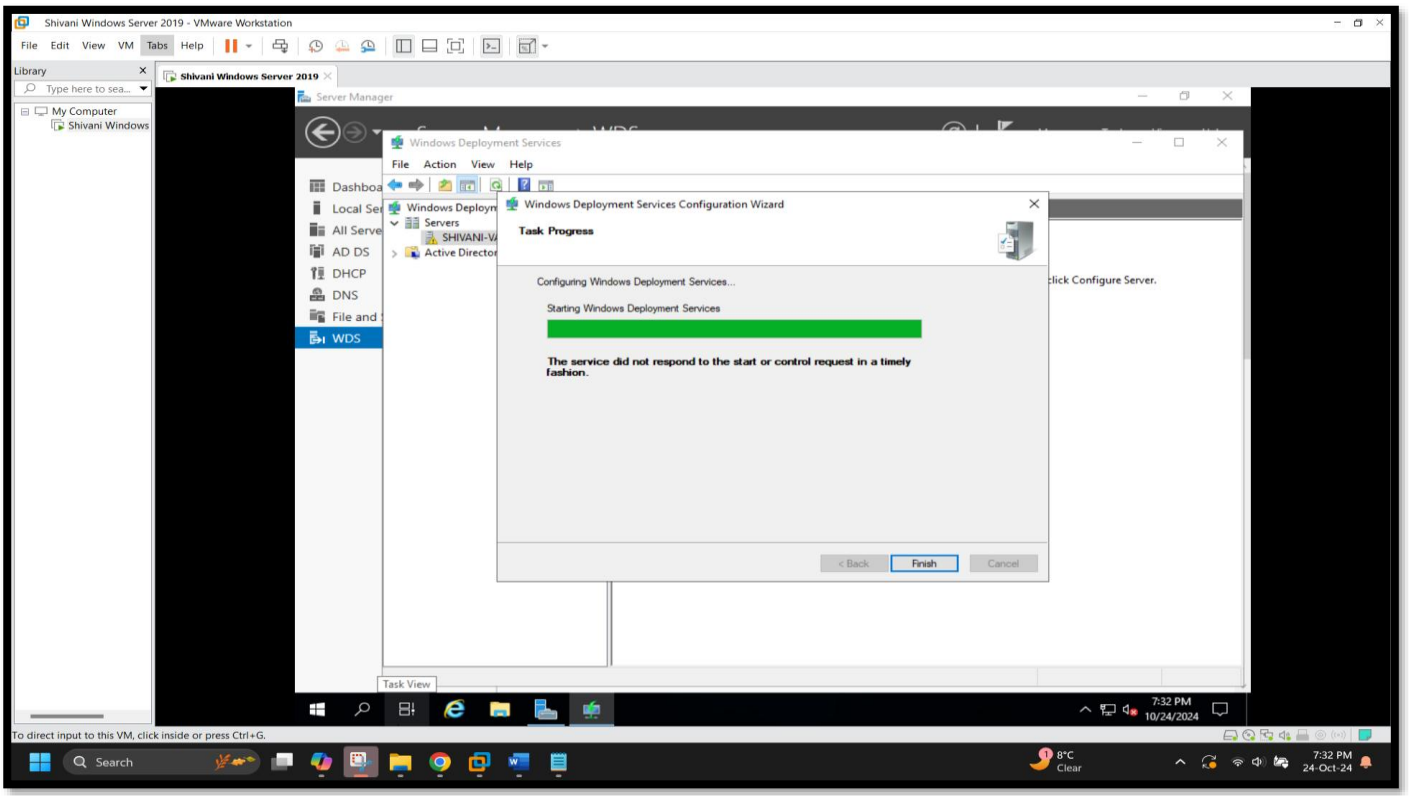


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 12: PXE Server Initial Settings]

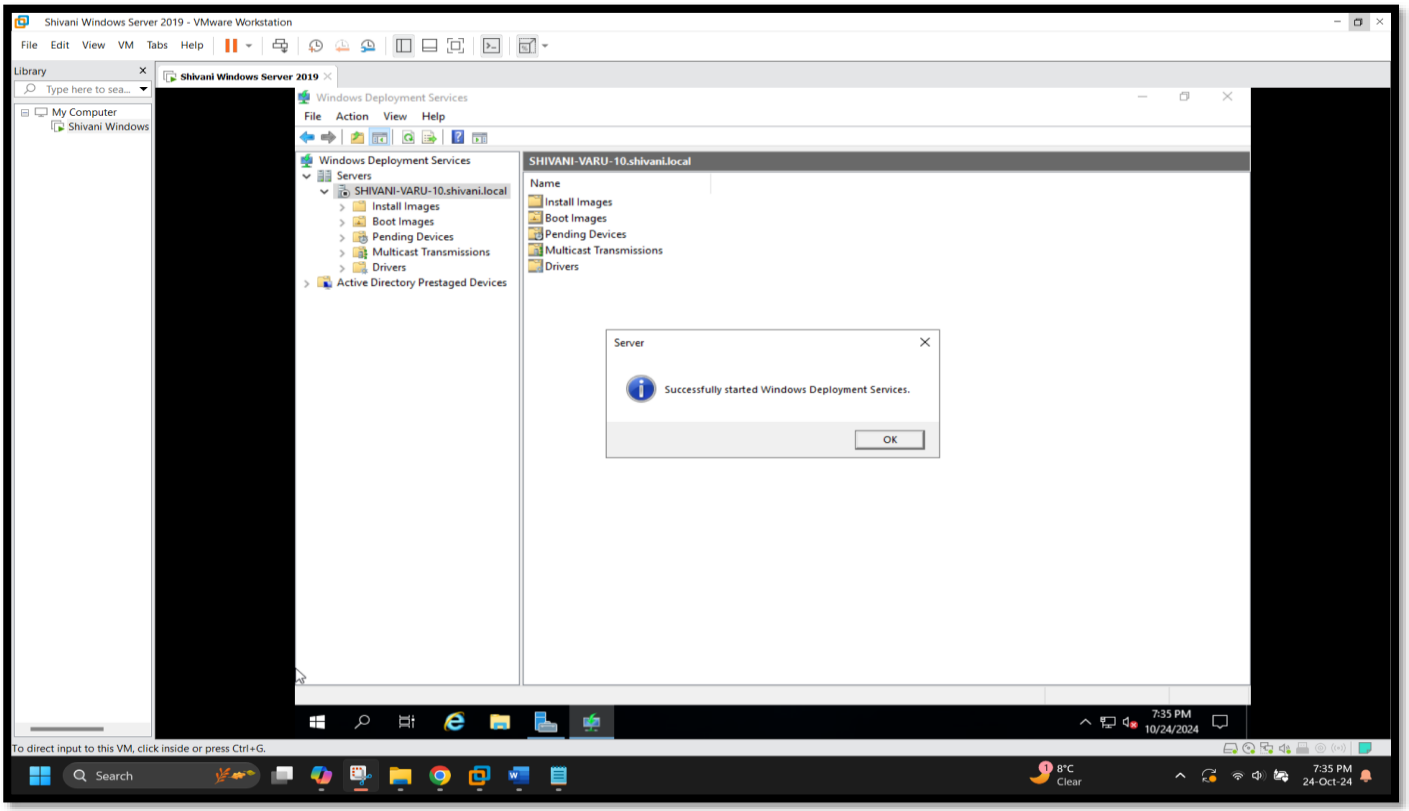


[Screenshot 13: WDS Service Start Issue]

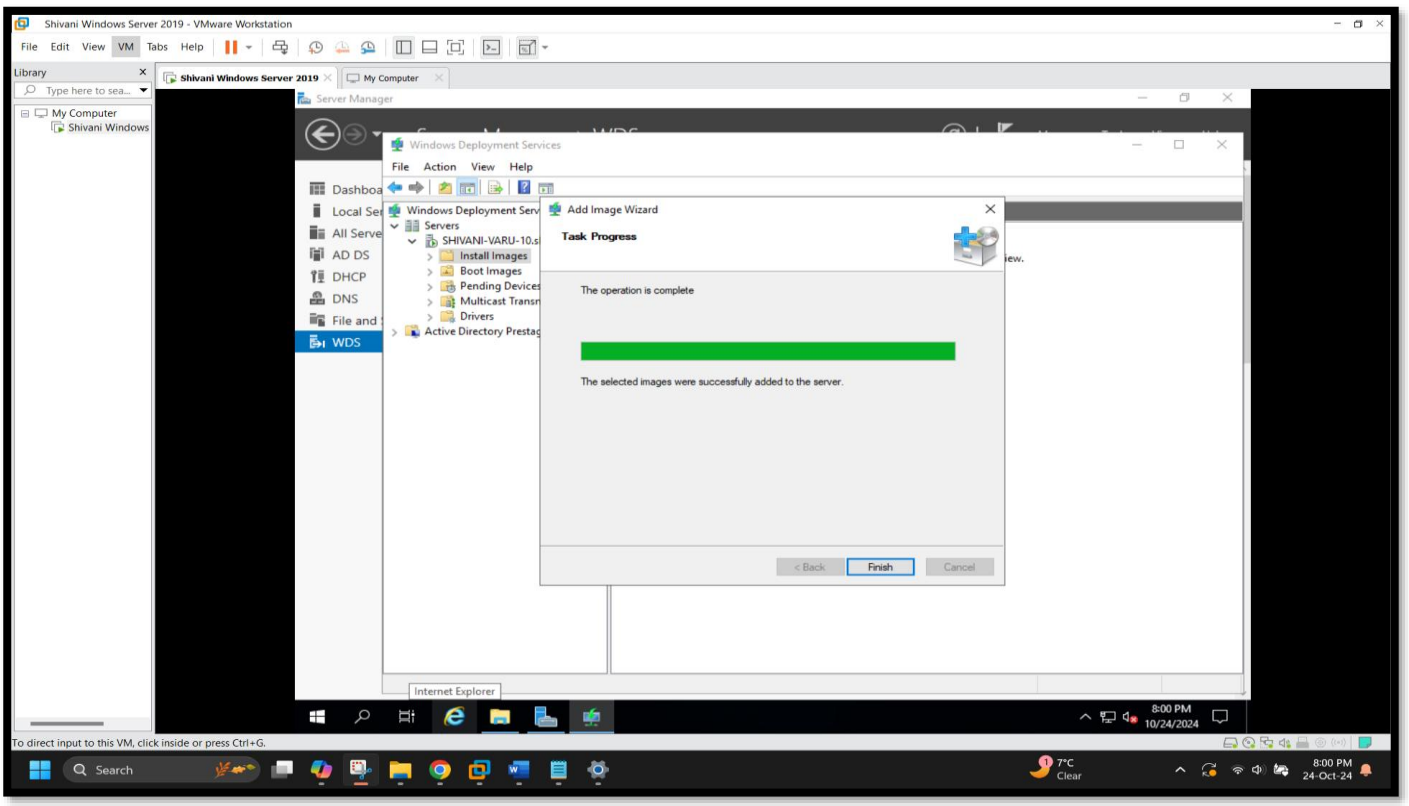


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 14: Successfully Configured and Started WDS]

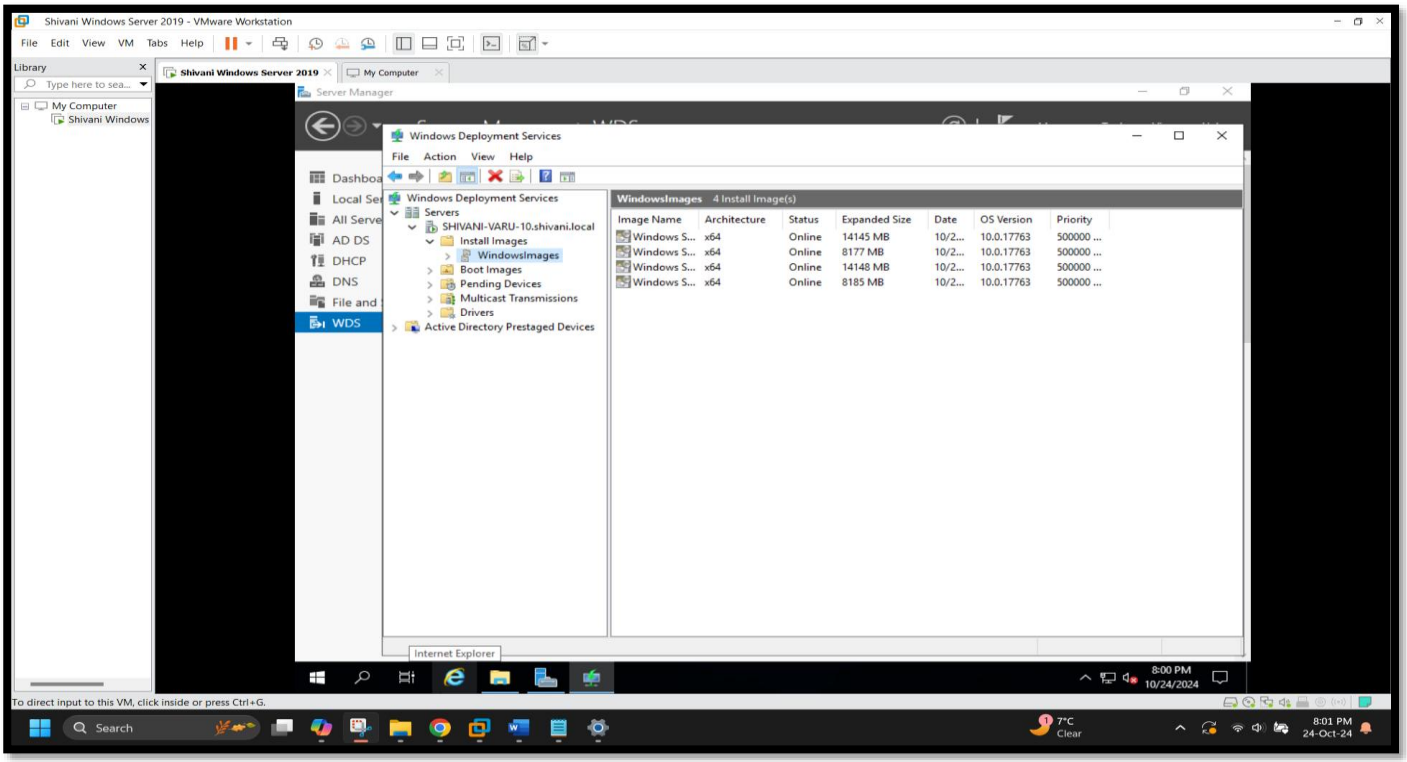


[Screenshot 15: Install Images Successfully Added]

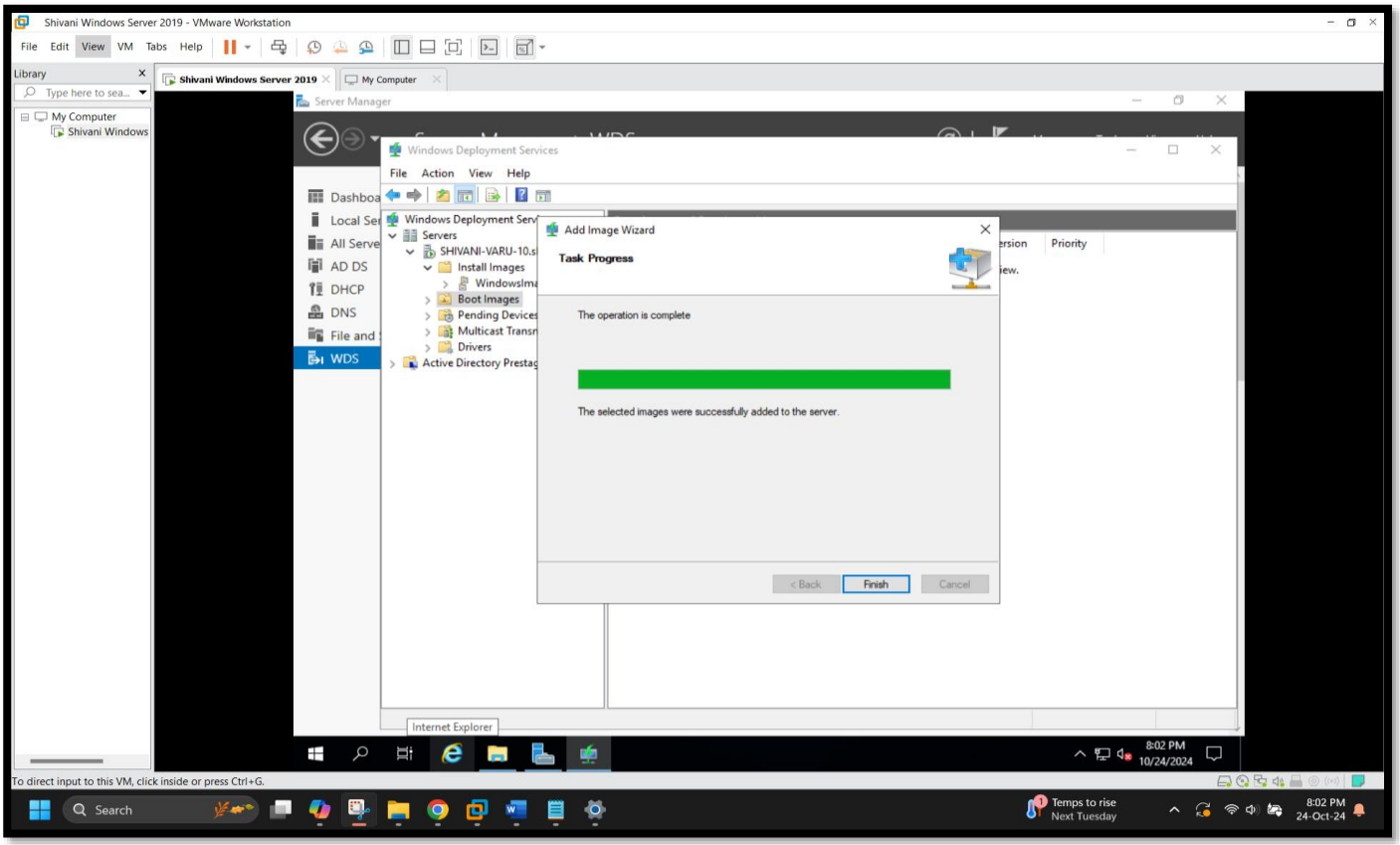


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 16: Install Images List in WDS]

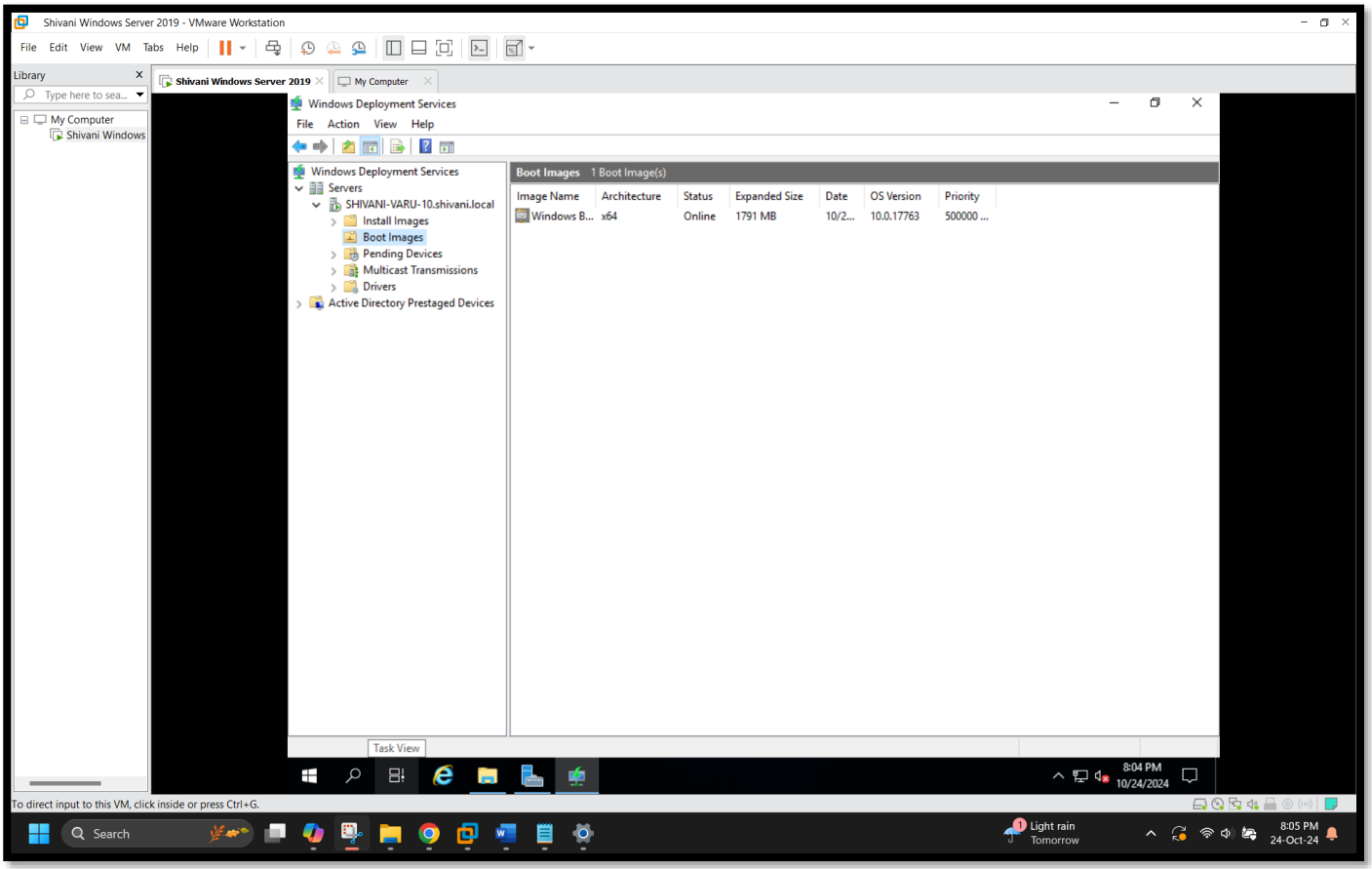


[Screenshot 17: Boot Images Successfully Added]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 18: WDS console showing added boot image on SHIVANI-VARU-10 server]

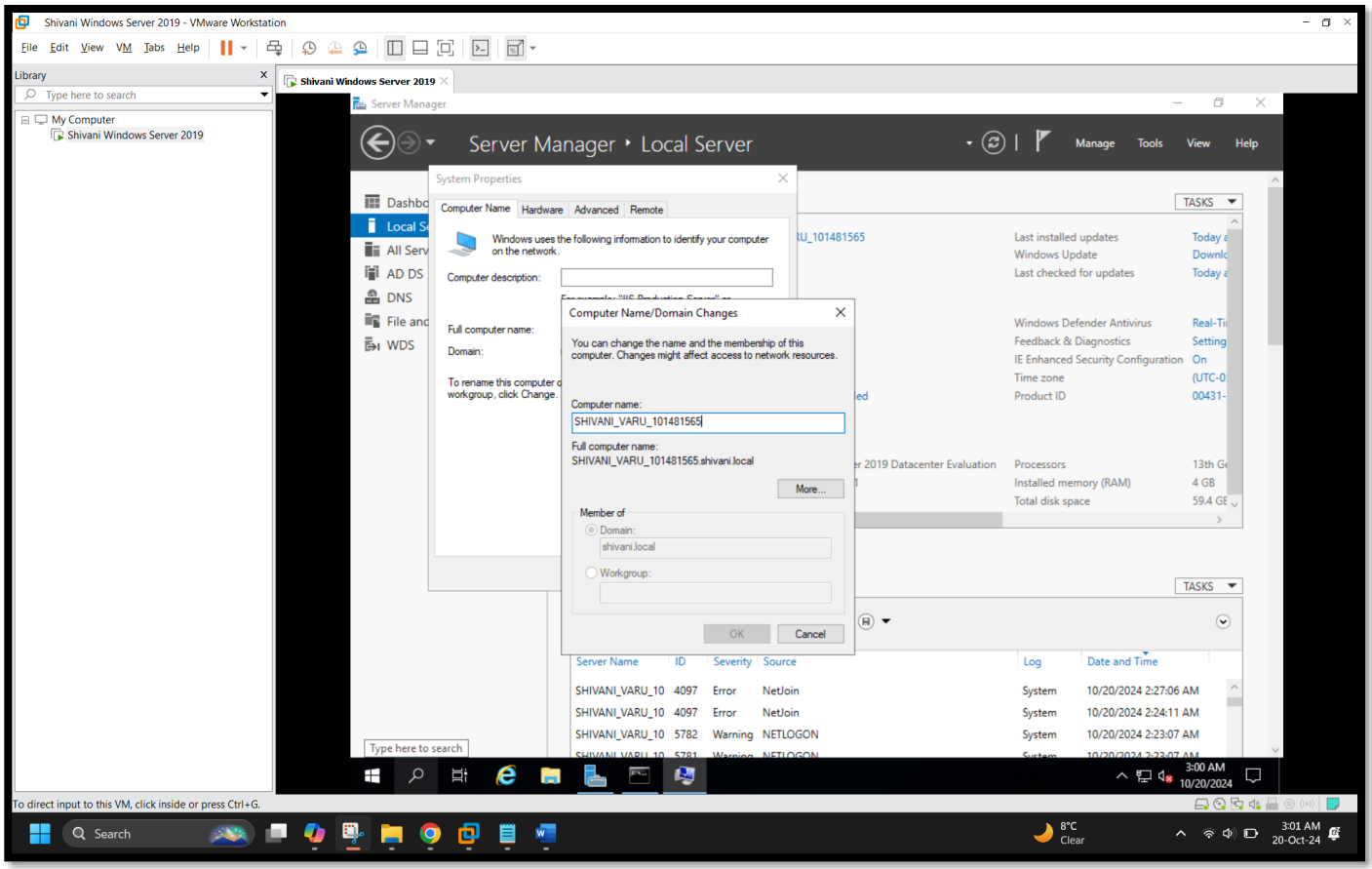


Name: Shivani Shaileshkumar Varu Student ID: 101481565

Exercise 3 - Performing an Initial Windows Server Configuration using Server Manager and Server Configuration.

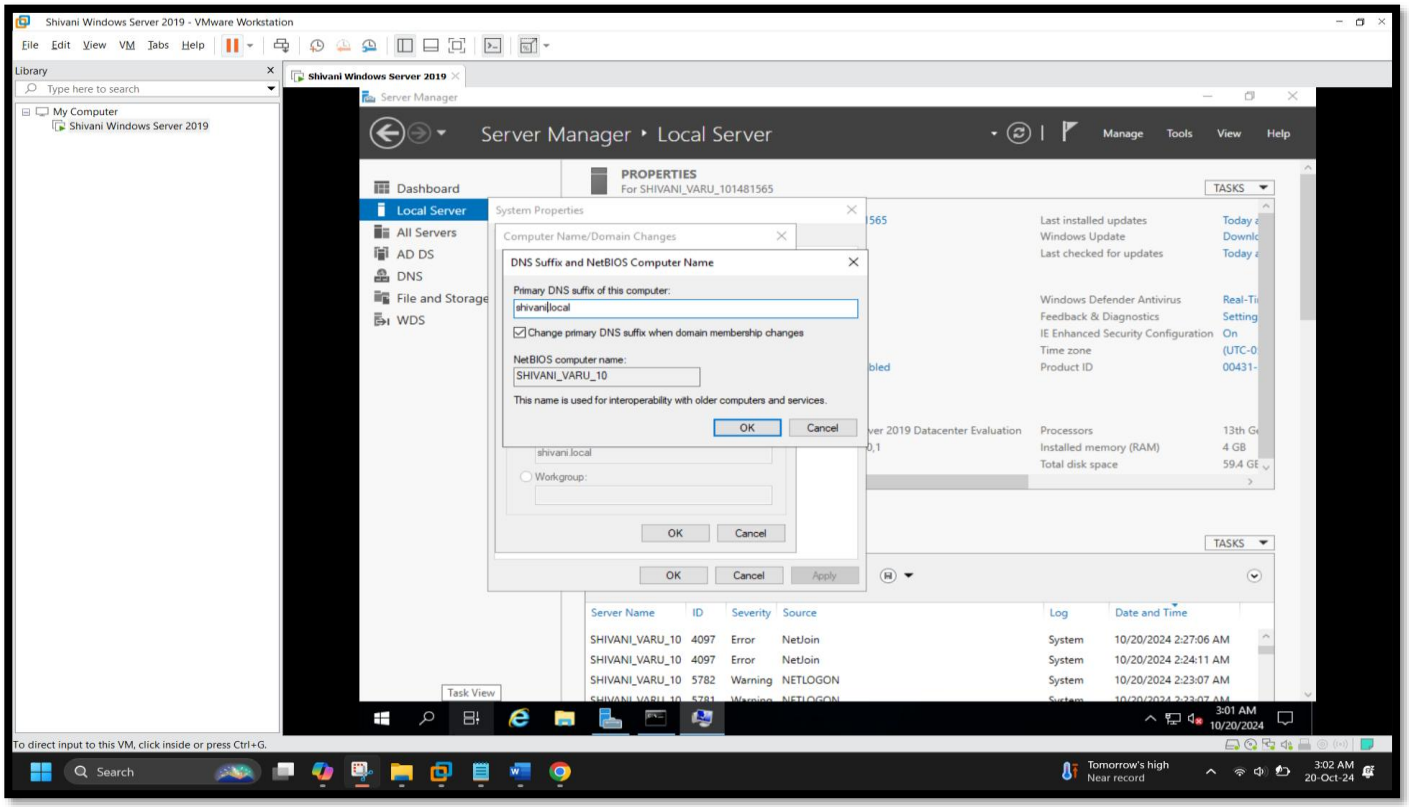
1) Performing an Initial Windows Server Configuration using Server Manager

[Screenshot 1: Change Computer Name]

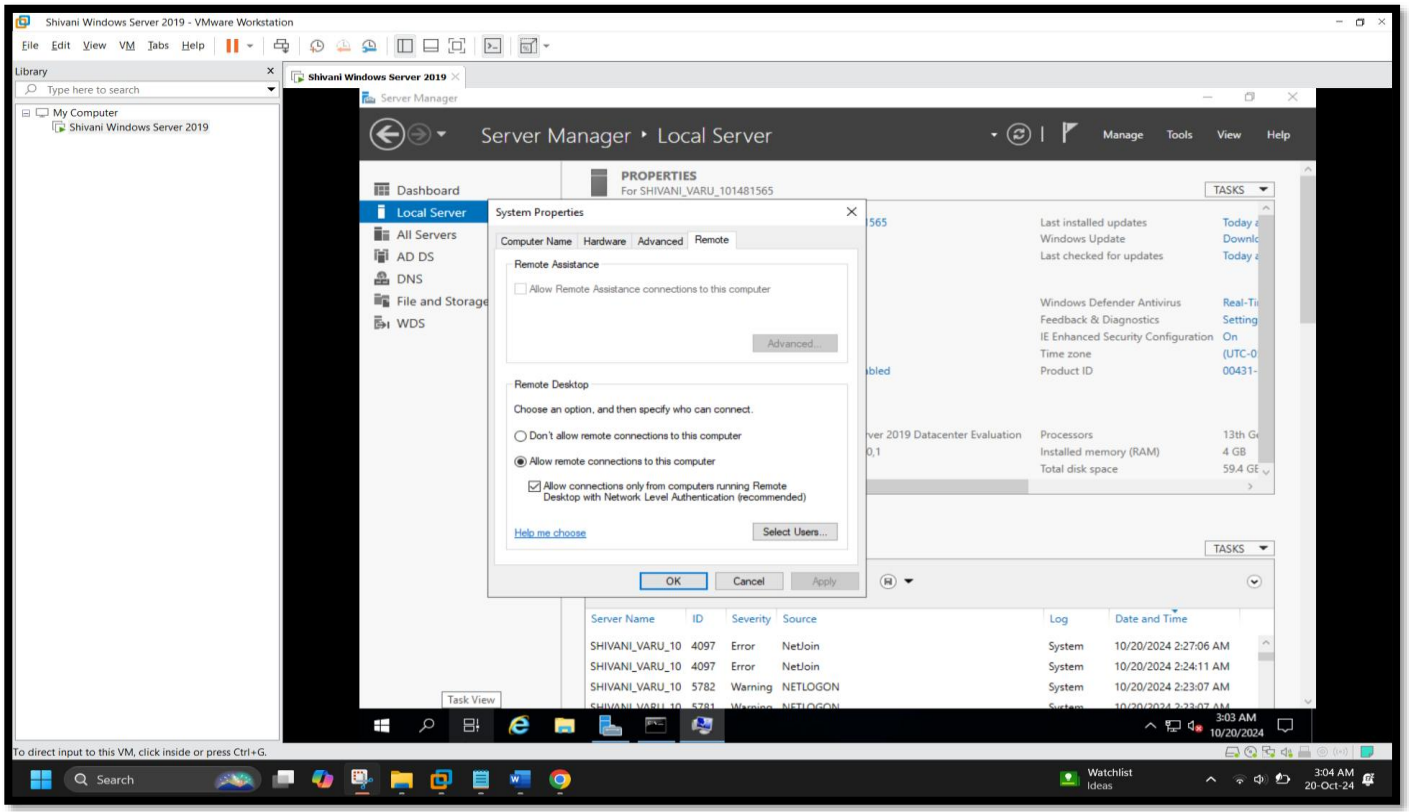


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 2: Joining Domain Name]

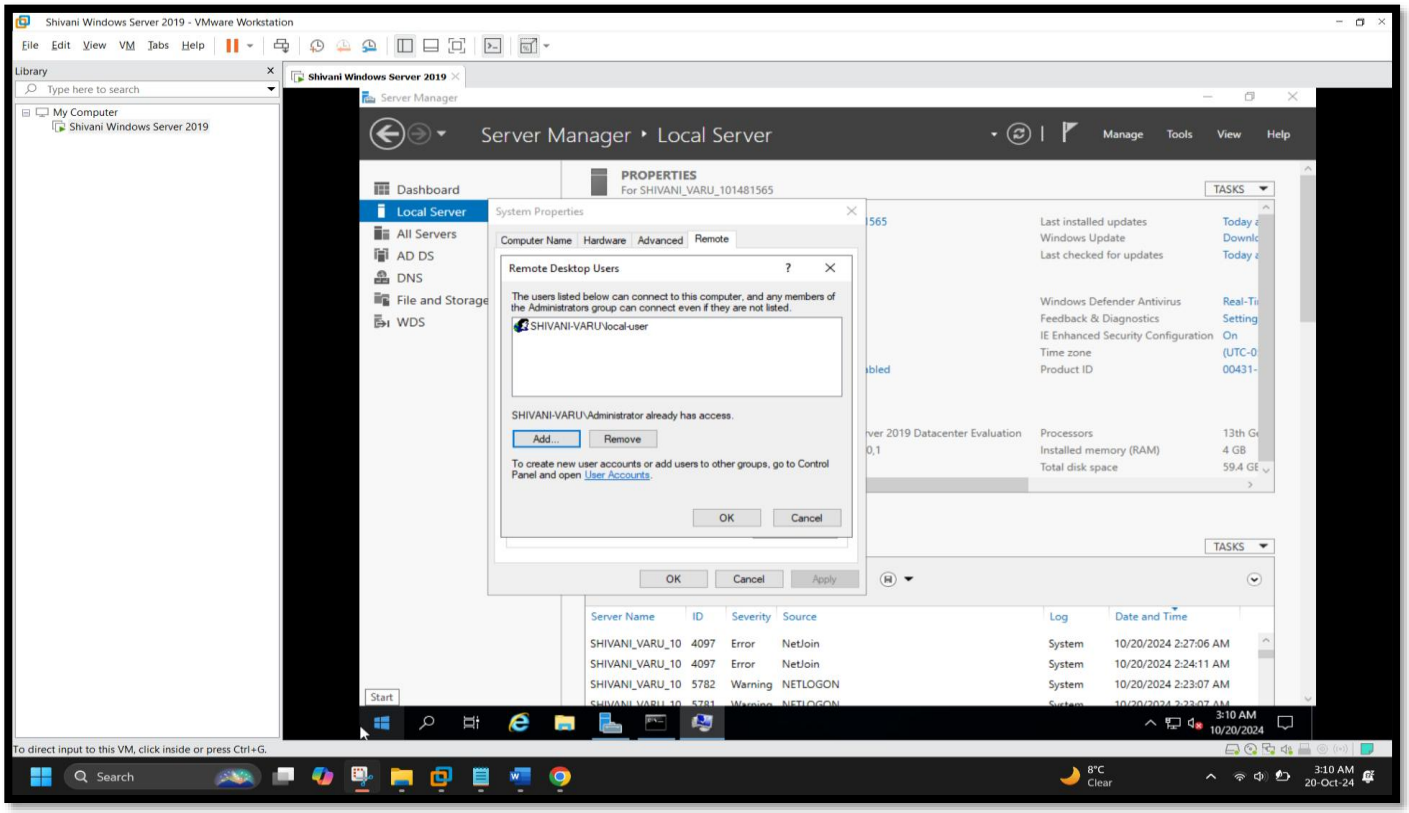


[Screenshot 3: Enabling Remote Desktop]

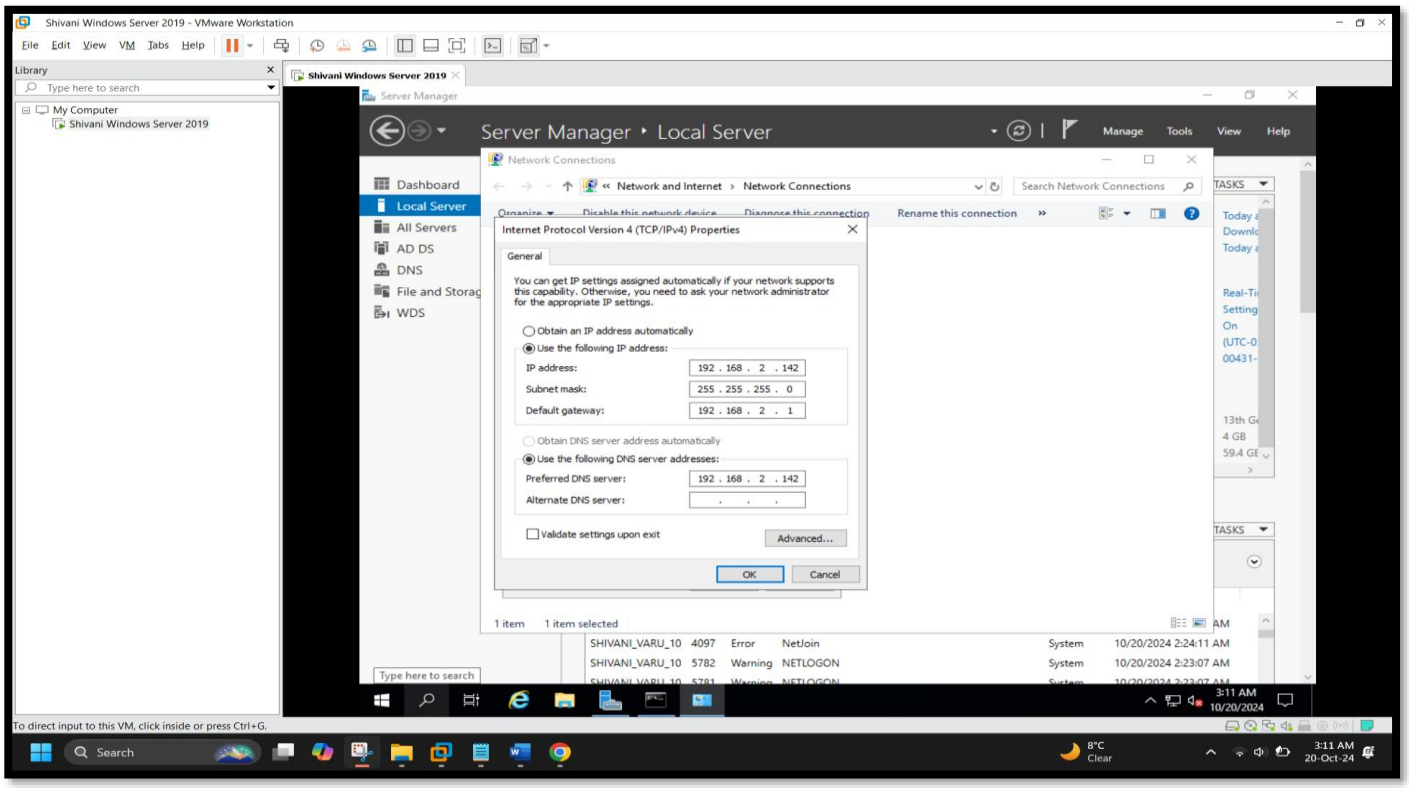


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 3: Adding User Account for Enabling Remote Desktop]

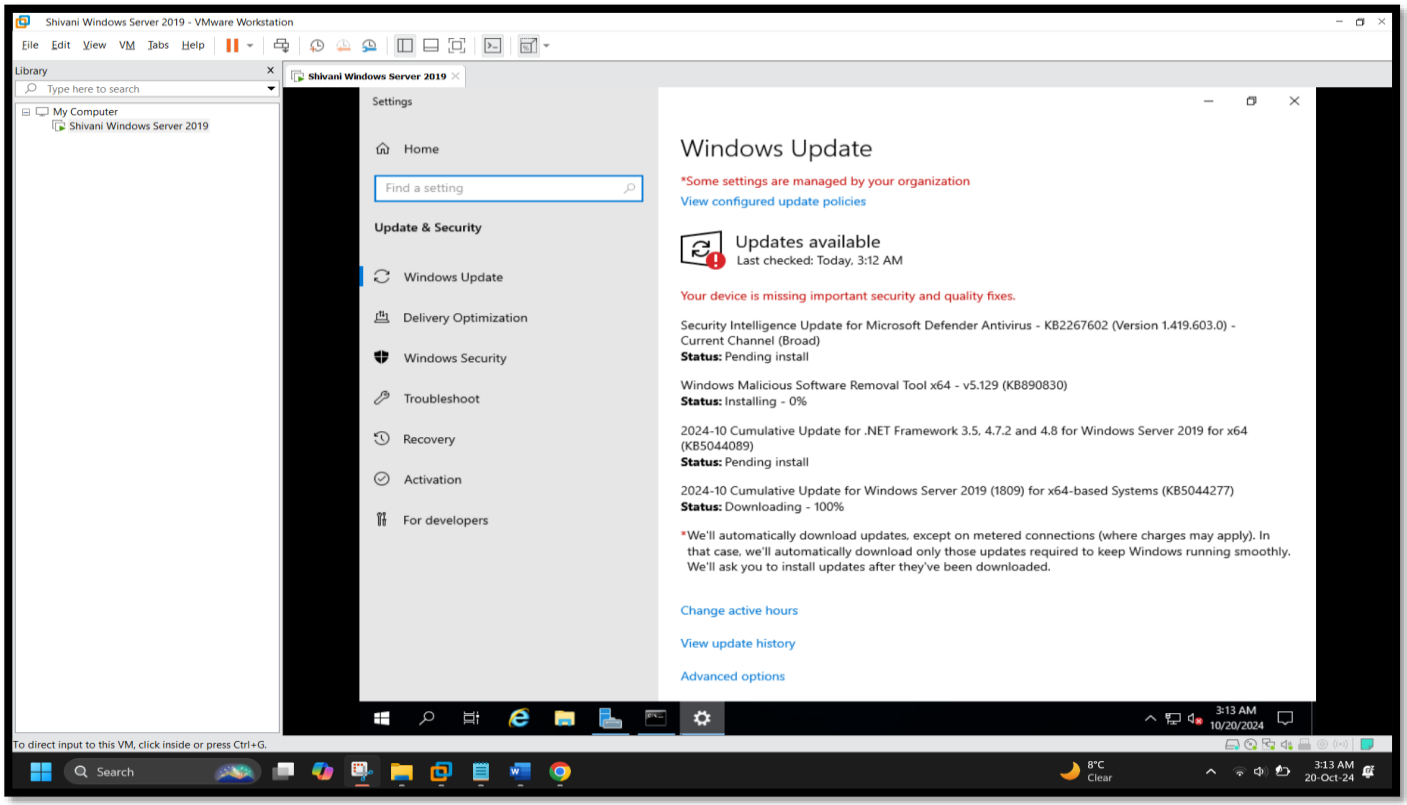


[Screenshot 4: Setting up IP address]

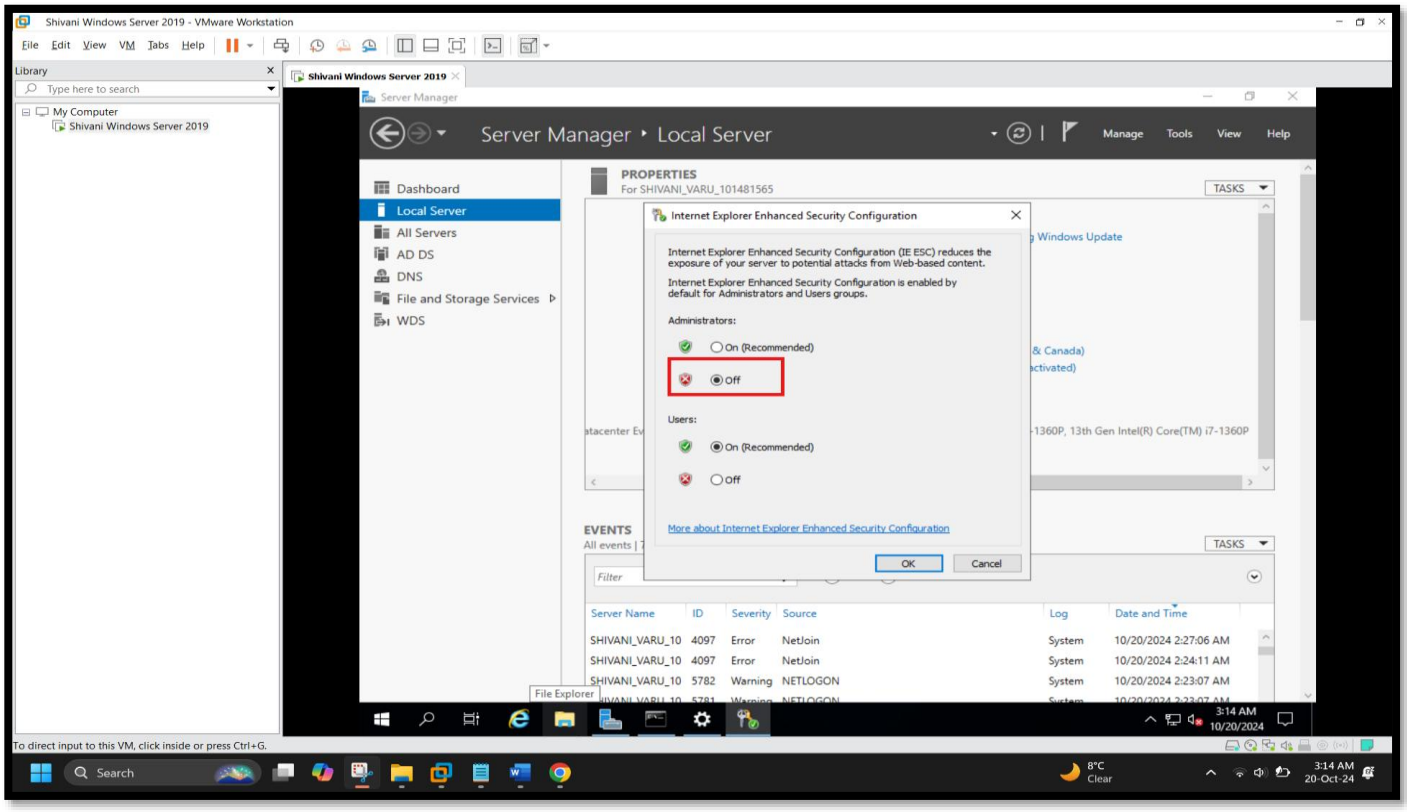


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 5: Checking Windows Update]

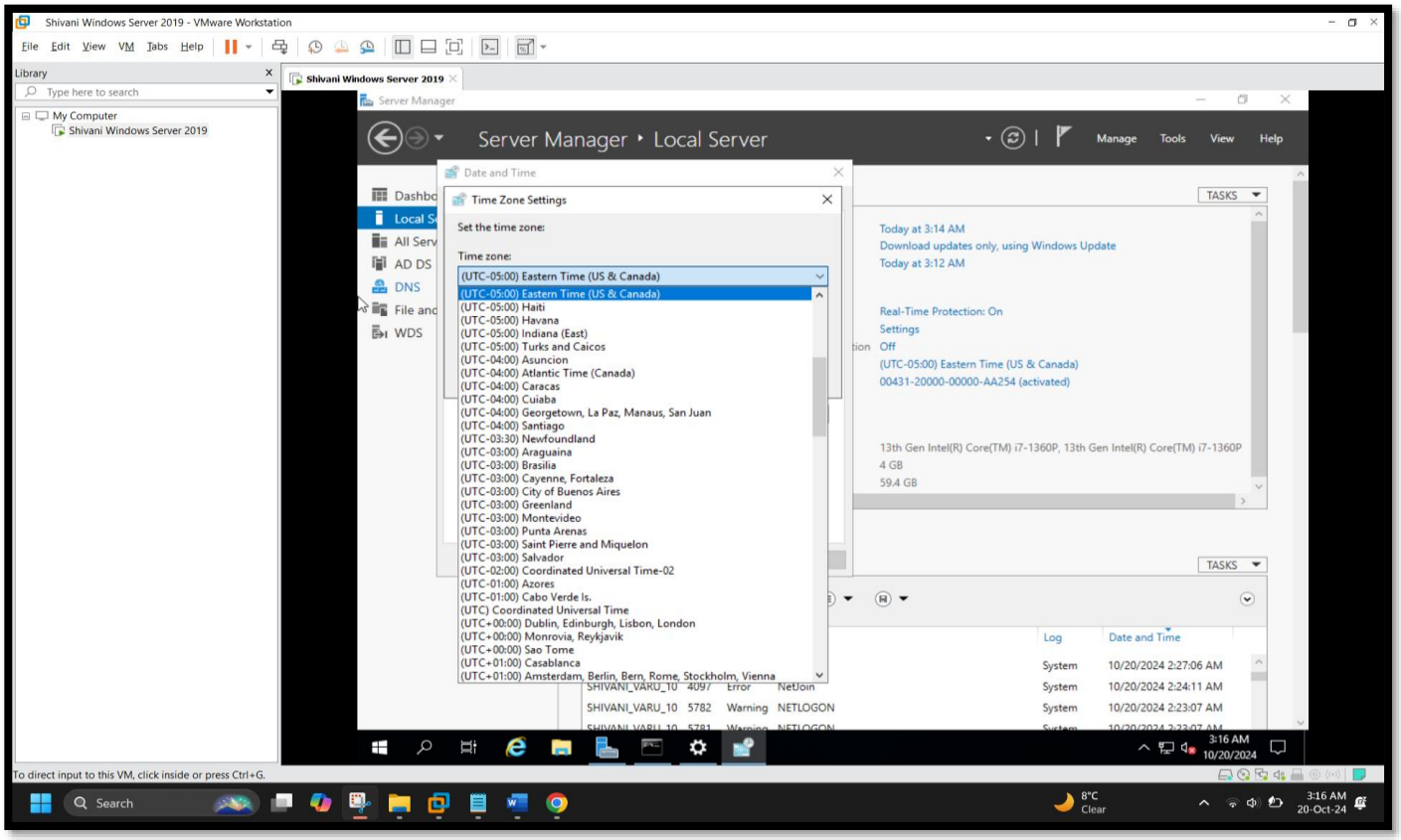


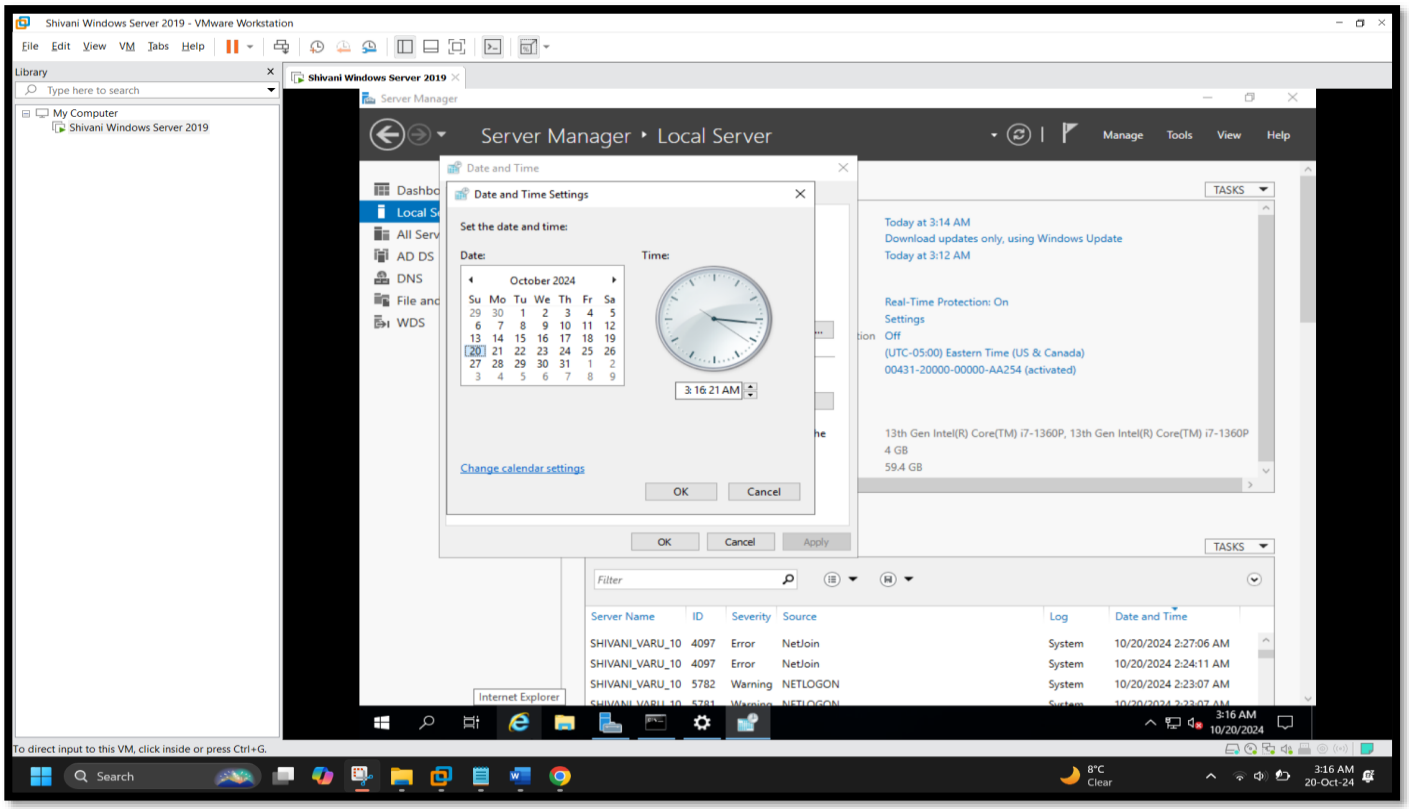
[Screenshot 6: Turning Off IE Enhanced Security]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

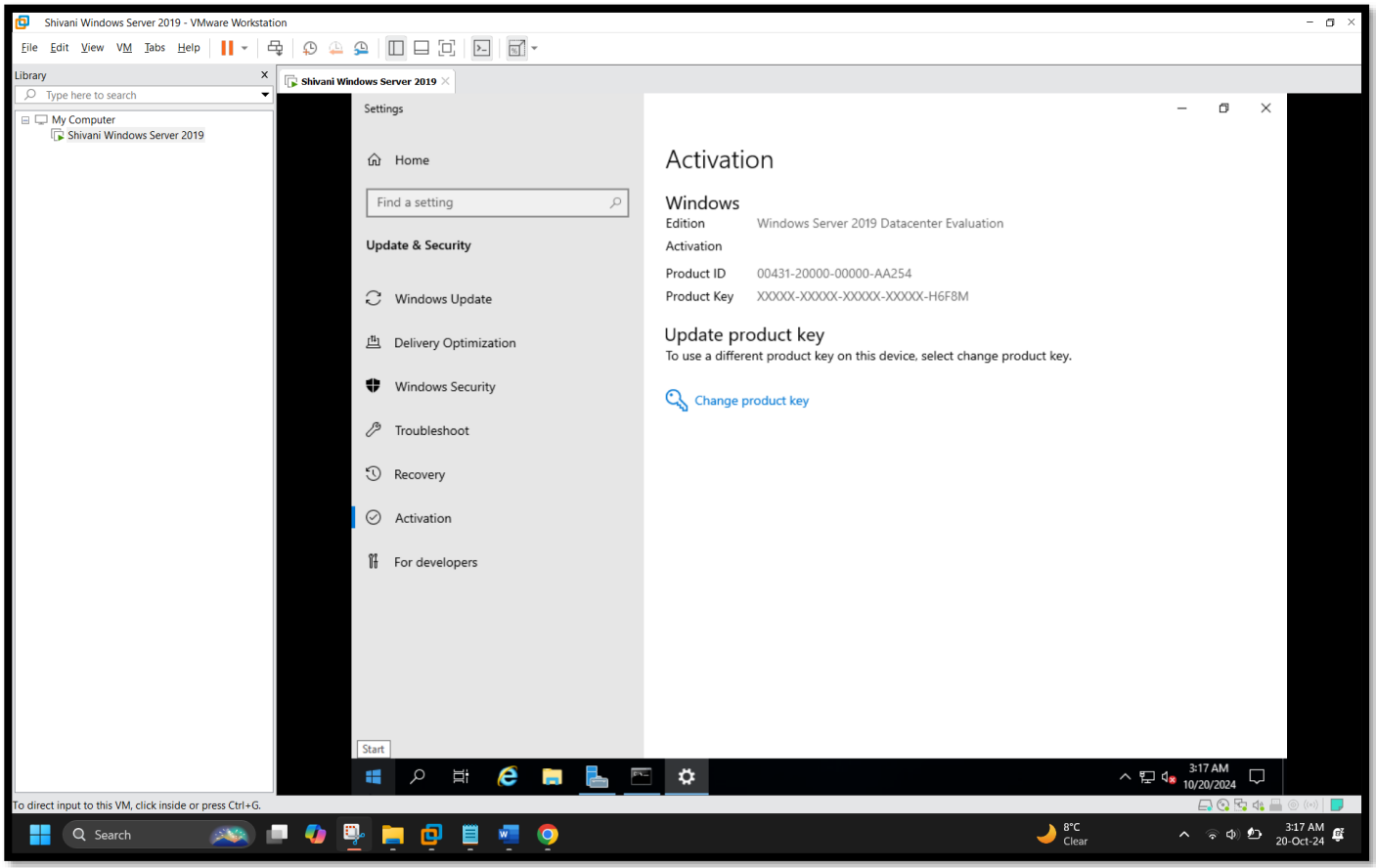
[Screenshot 7: Changing the Time Zone]





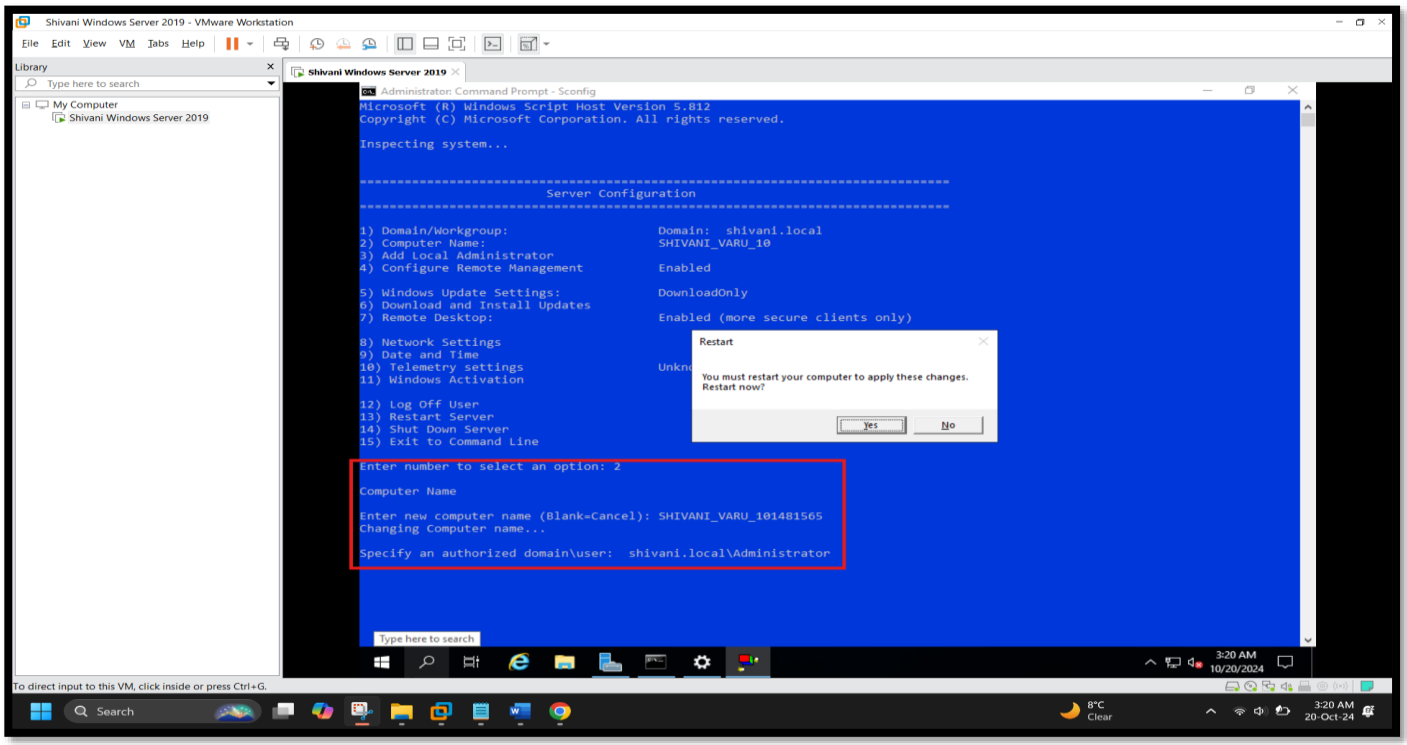
Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 8: Activating Windows Server]

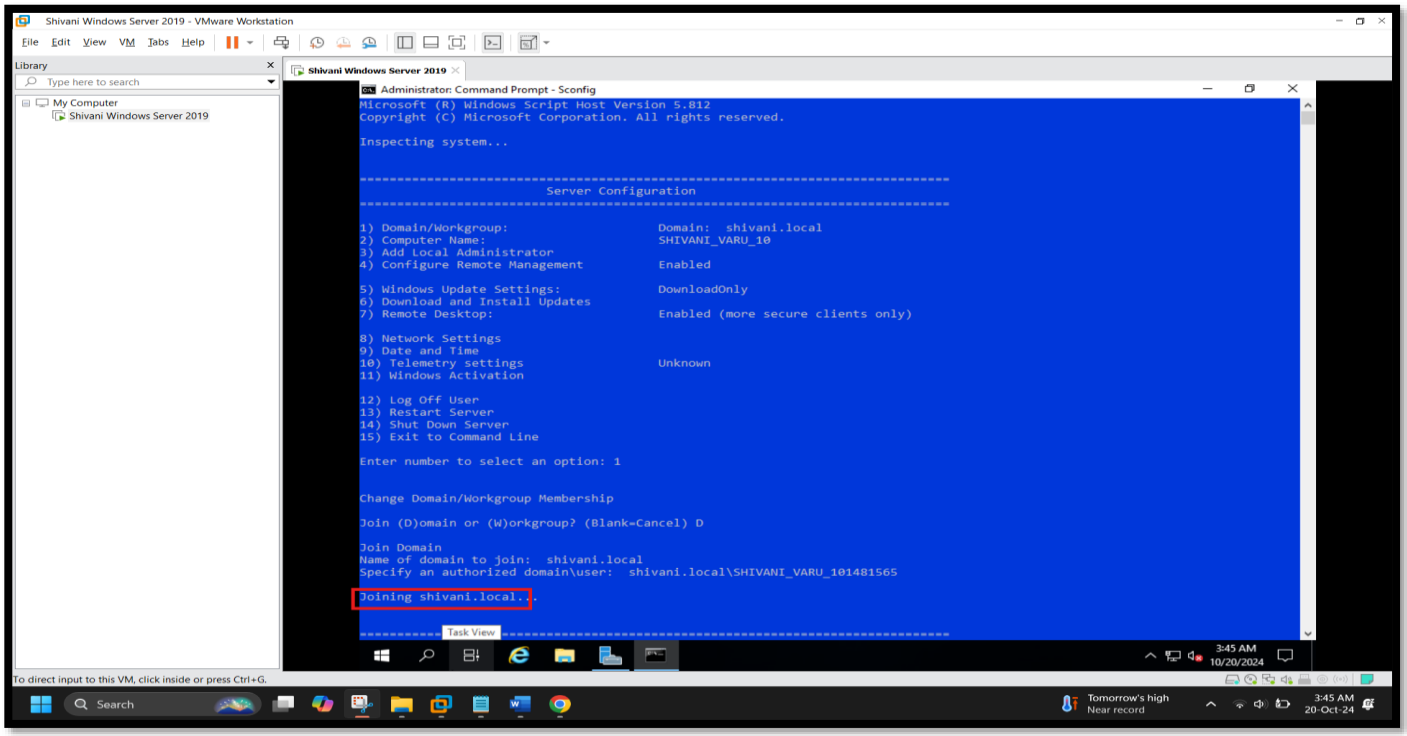


2) Performing Windows Server initial configuration using Server Configuration

[Screenshot 9: Changing Server Name using SConfig in Command Line]

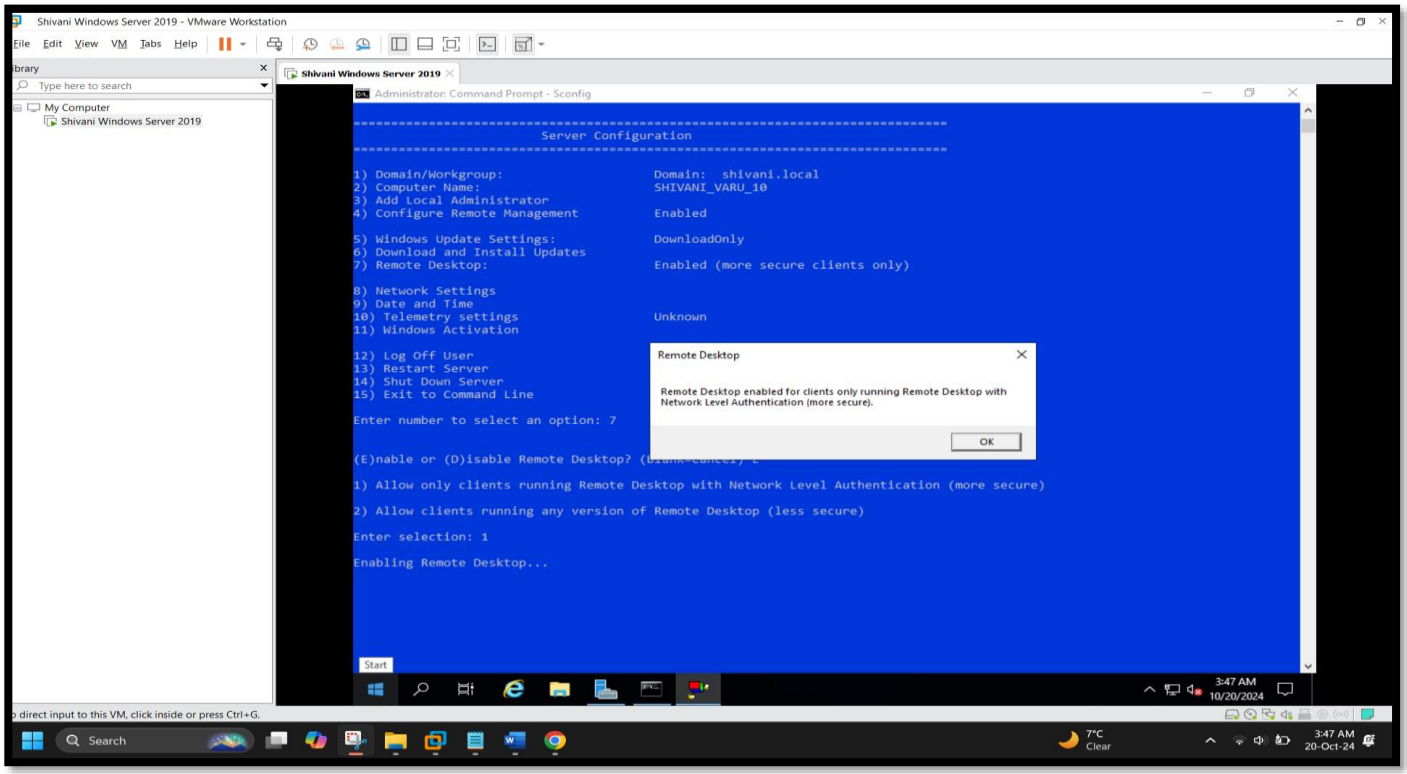


[Screenshot 10: [Screenshot 9: Joining the server]

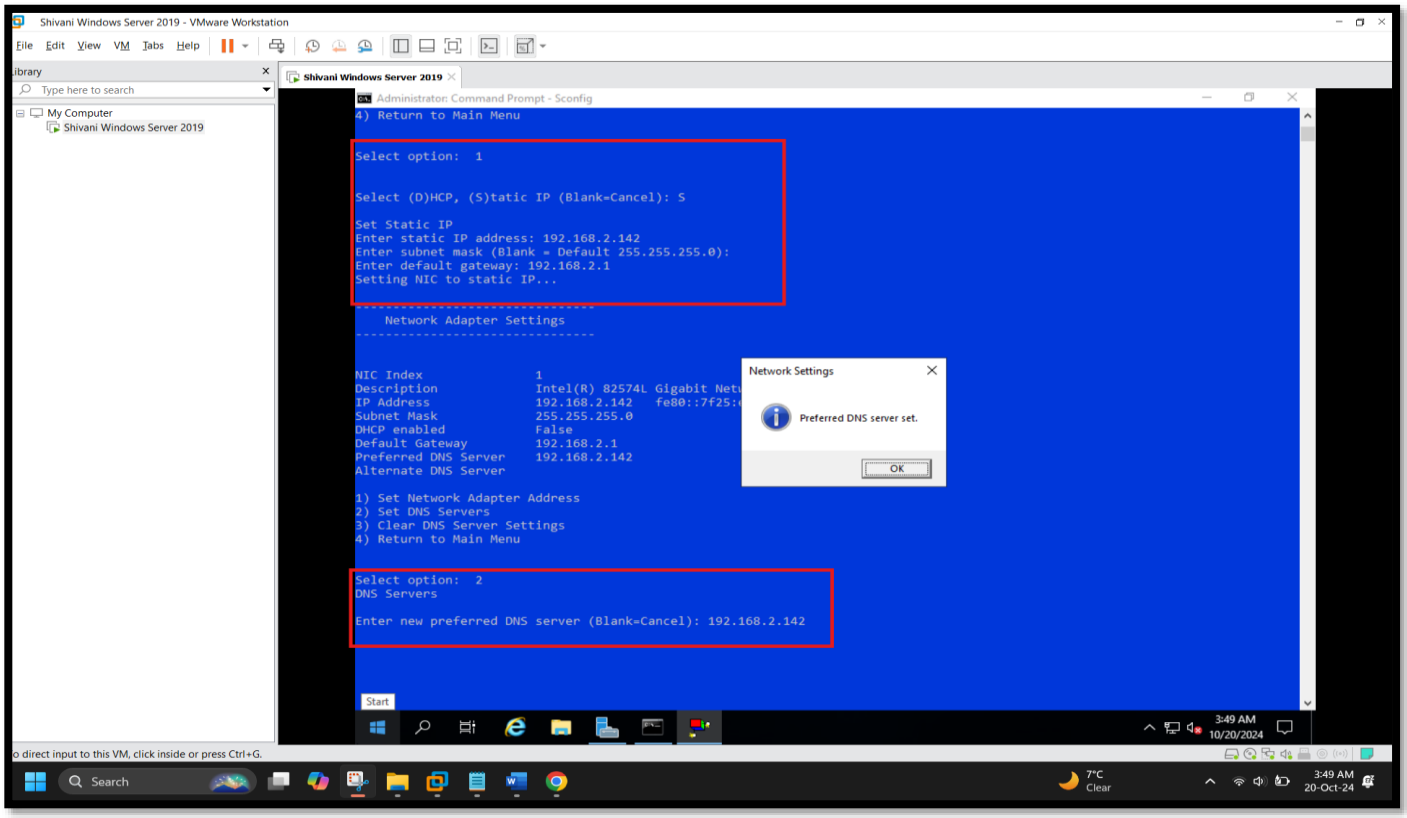


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 11: Enabling Remote Desktop using SConfig]

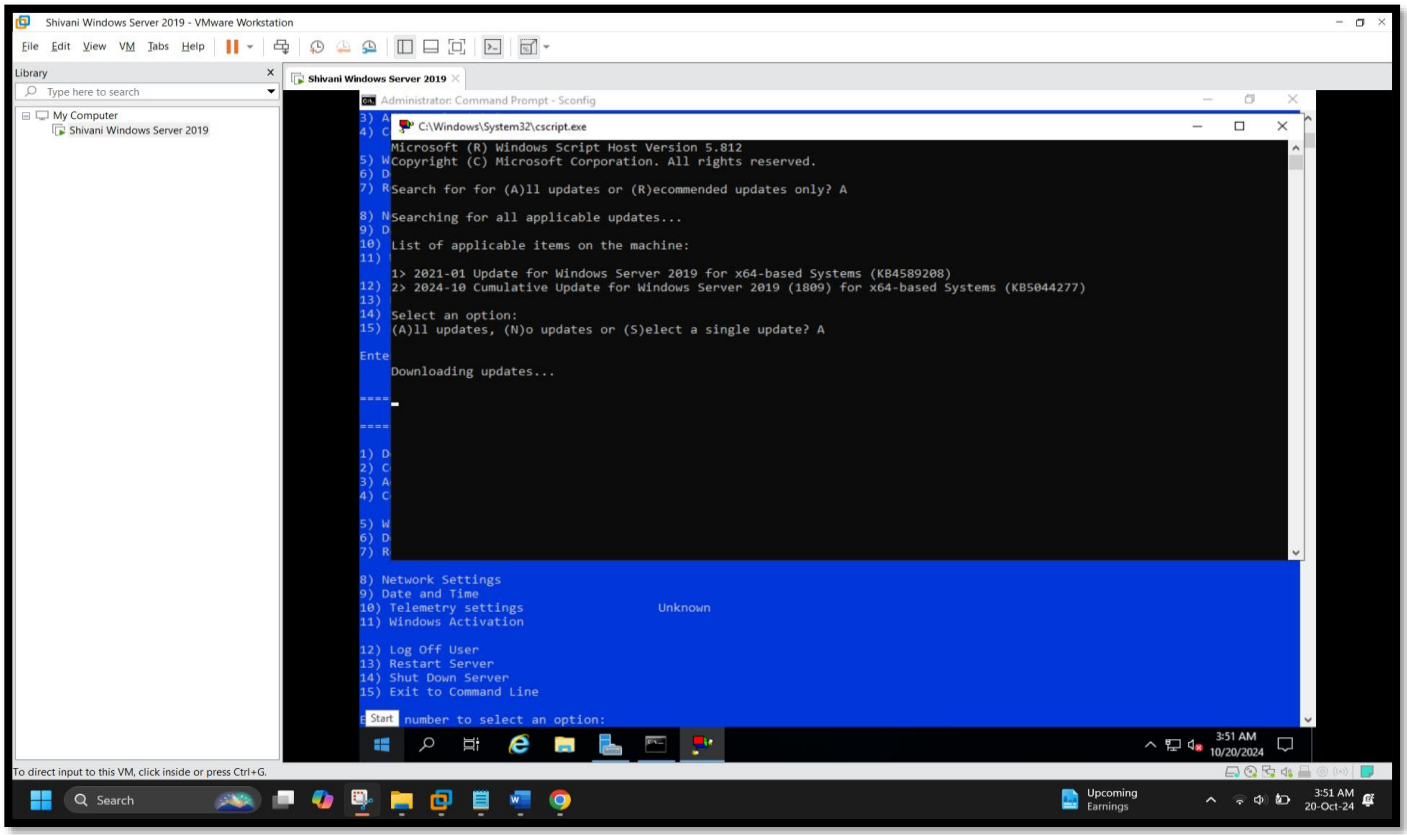


[Screenshot 12: Changing Static IP, Default Mask, Default gateway]

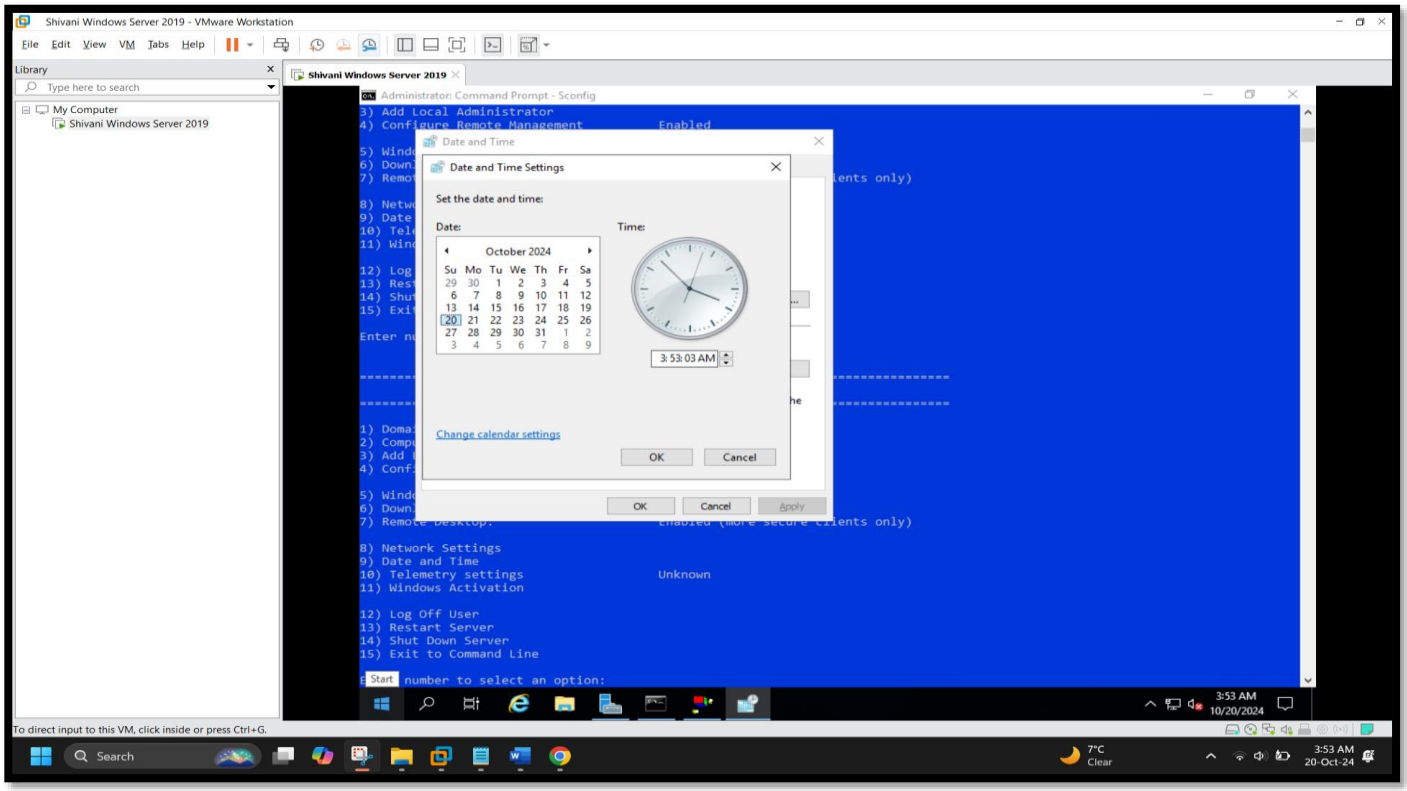


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 13: Windows Update using SConfig in command line]

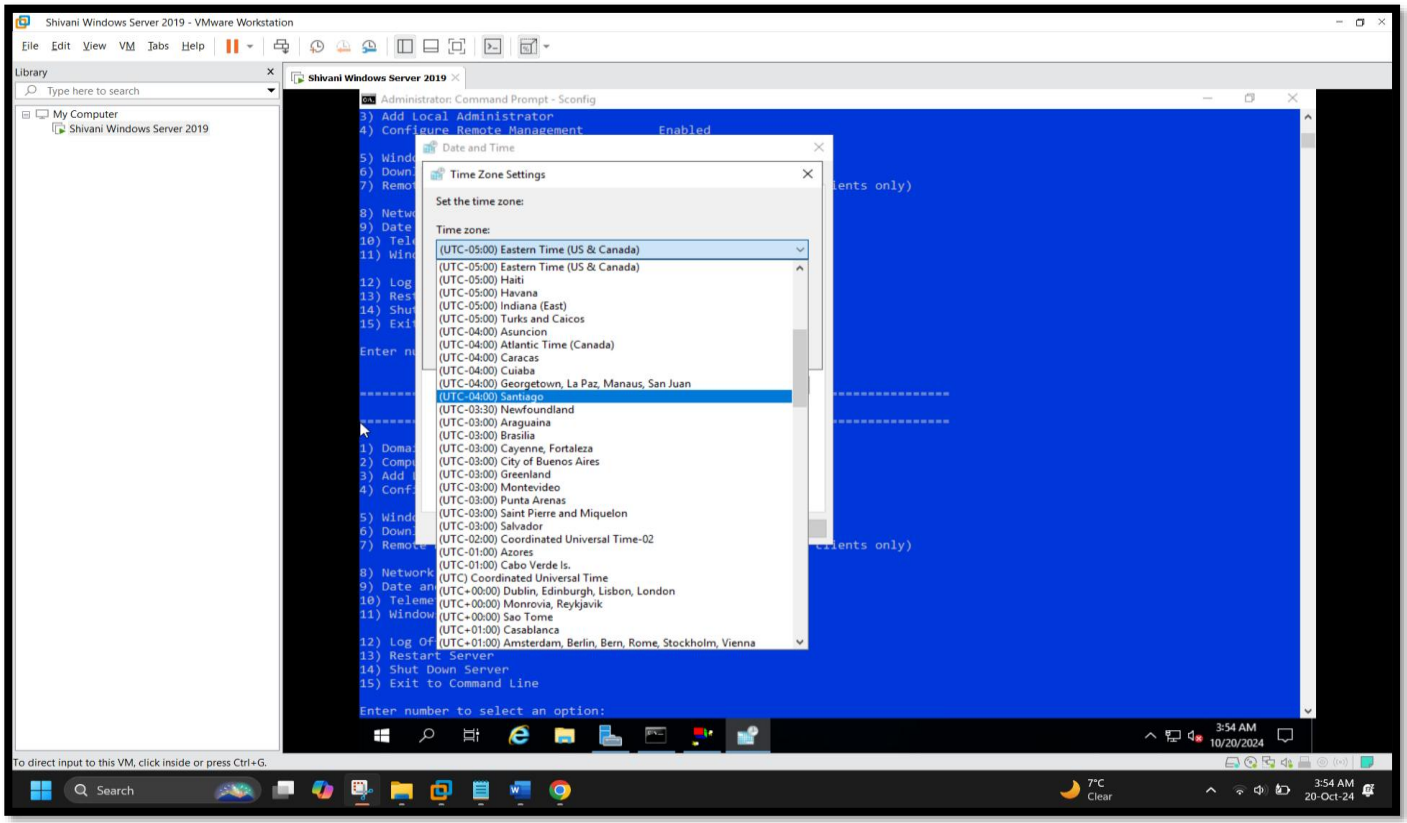


[Screenshot 14: Changing the Time Zone using SConfig in command line]

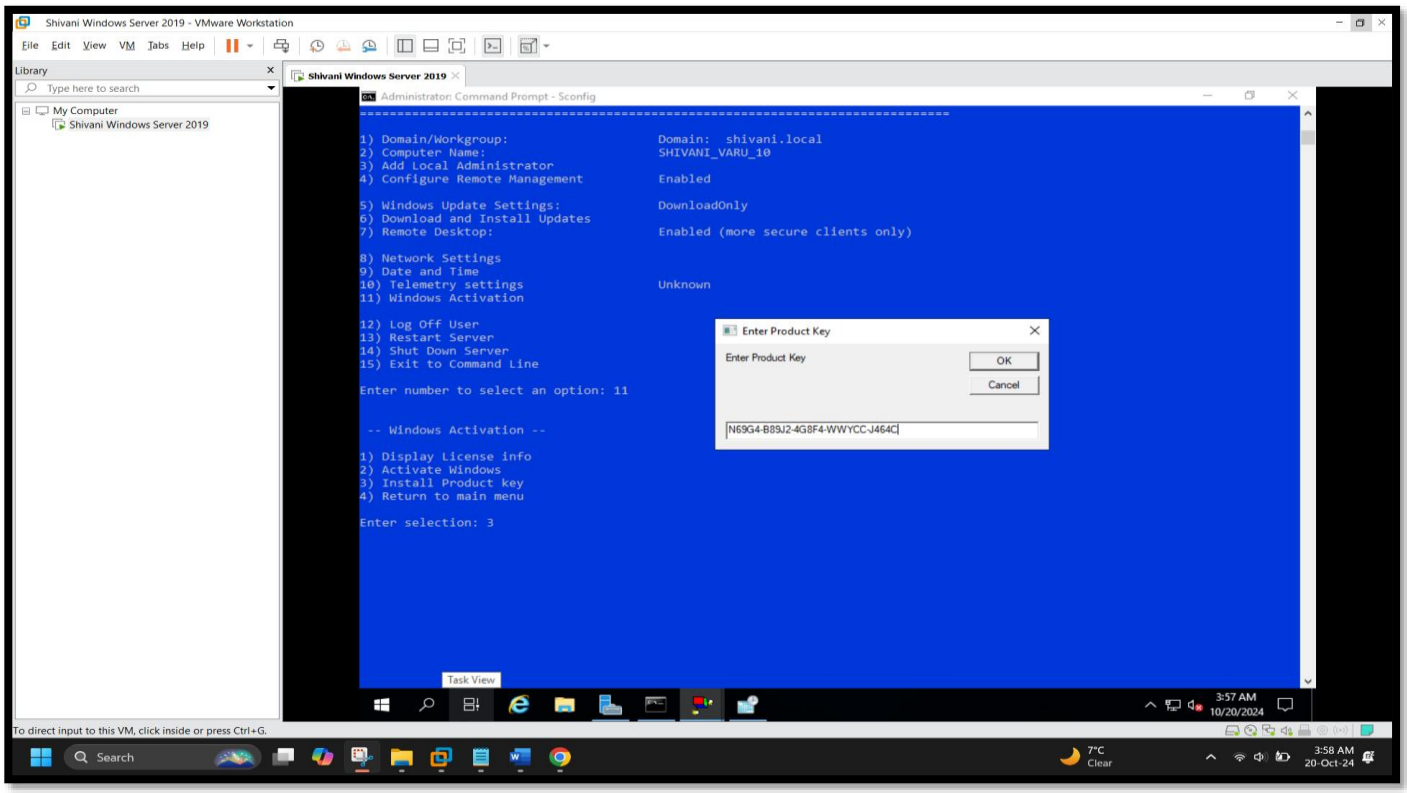


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 15: Changing the Time Zone using SConfig in command line]



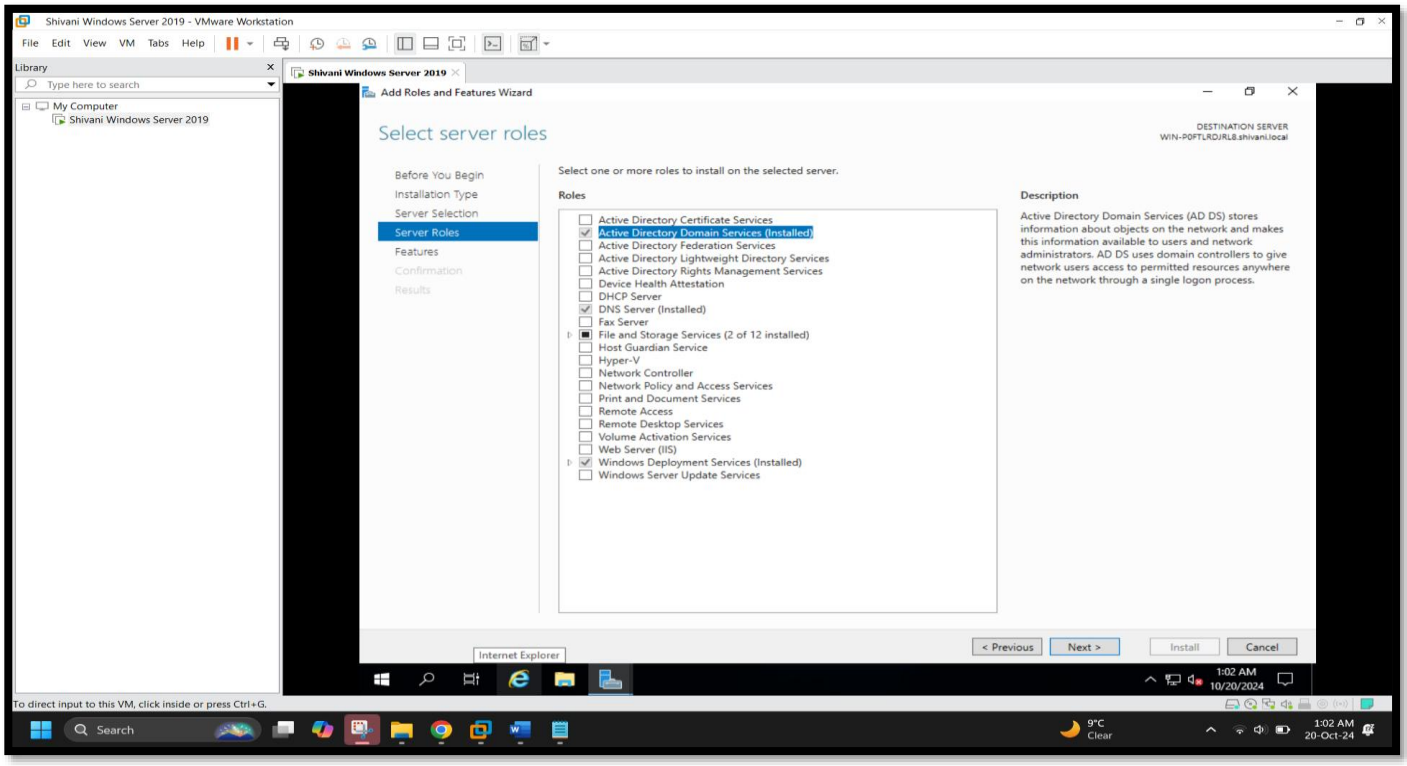
[Screenshot 16: Activating Windows Server using SConfig in command line]

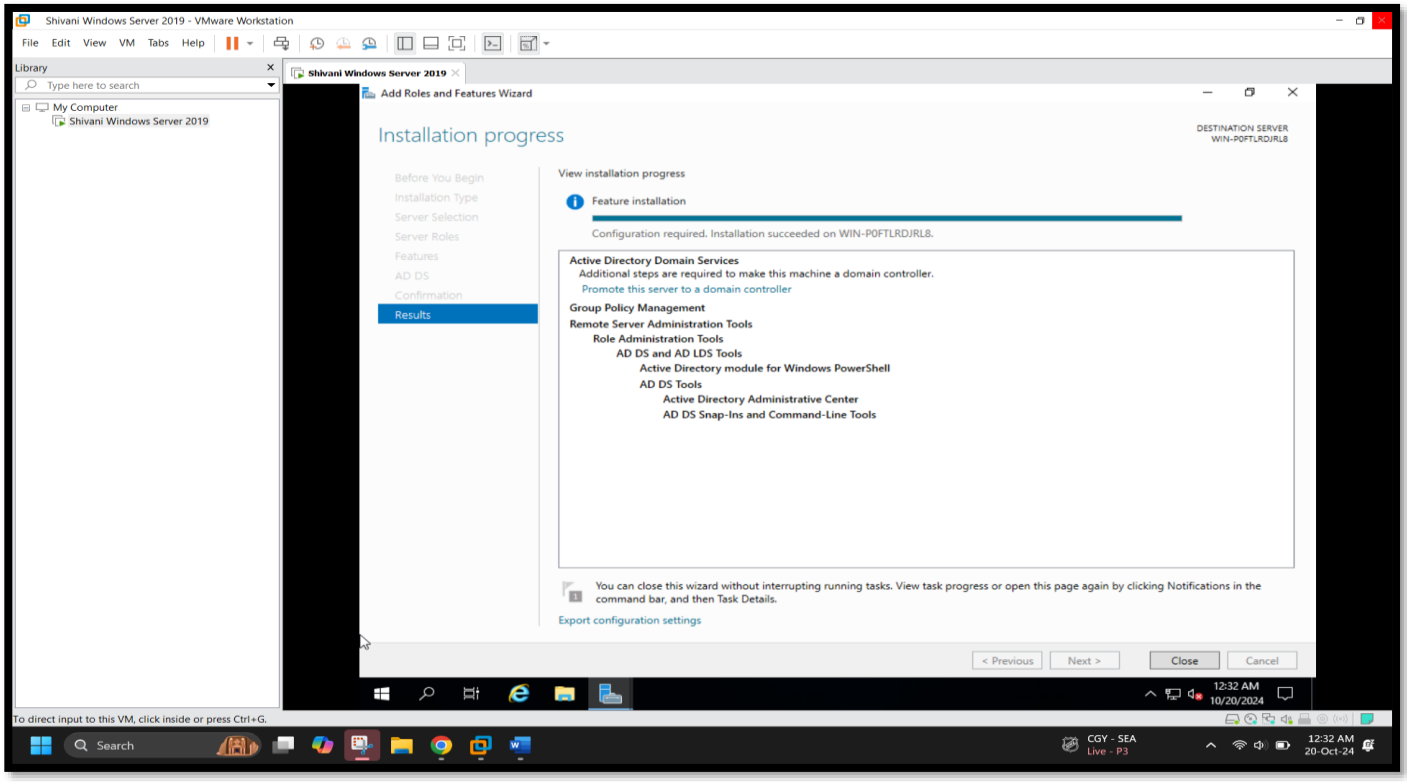


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Exercise – 4 Installing the AD DS and DNS roles, and promoting the server to a DC

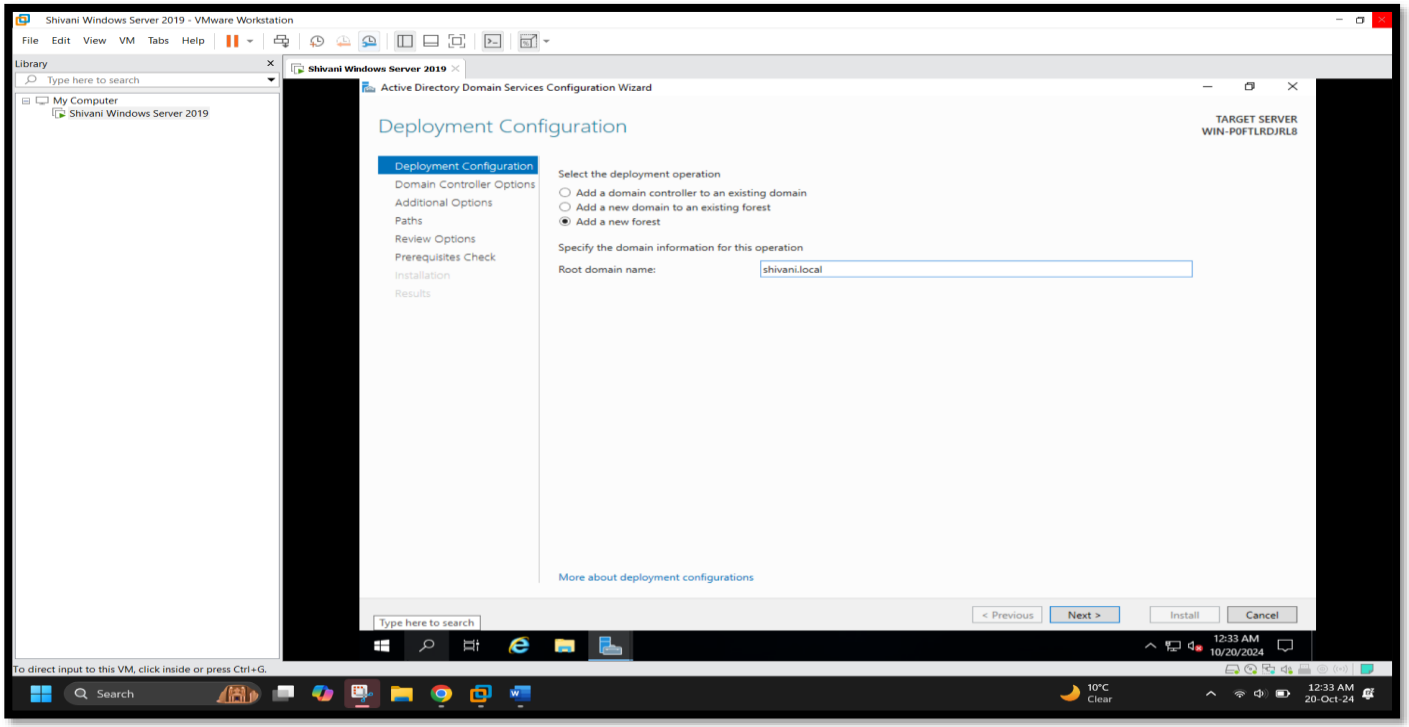
[Screenshot 1: Successful Installation of AD DS and DNS Roles]



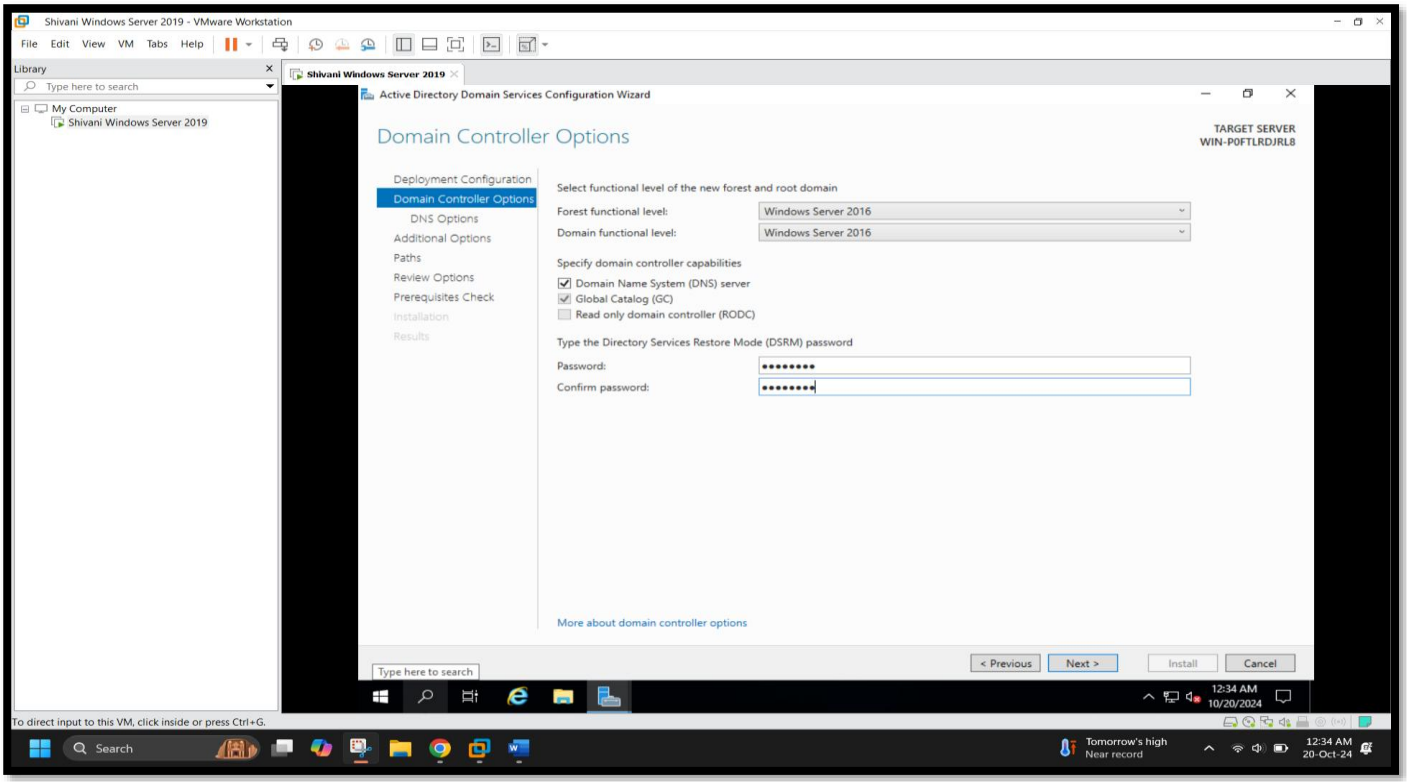


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 2: Deployment Configuration for New Forest Setup - the configuration to add a new forest with the domain name shivani.local]

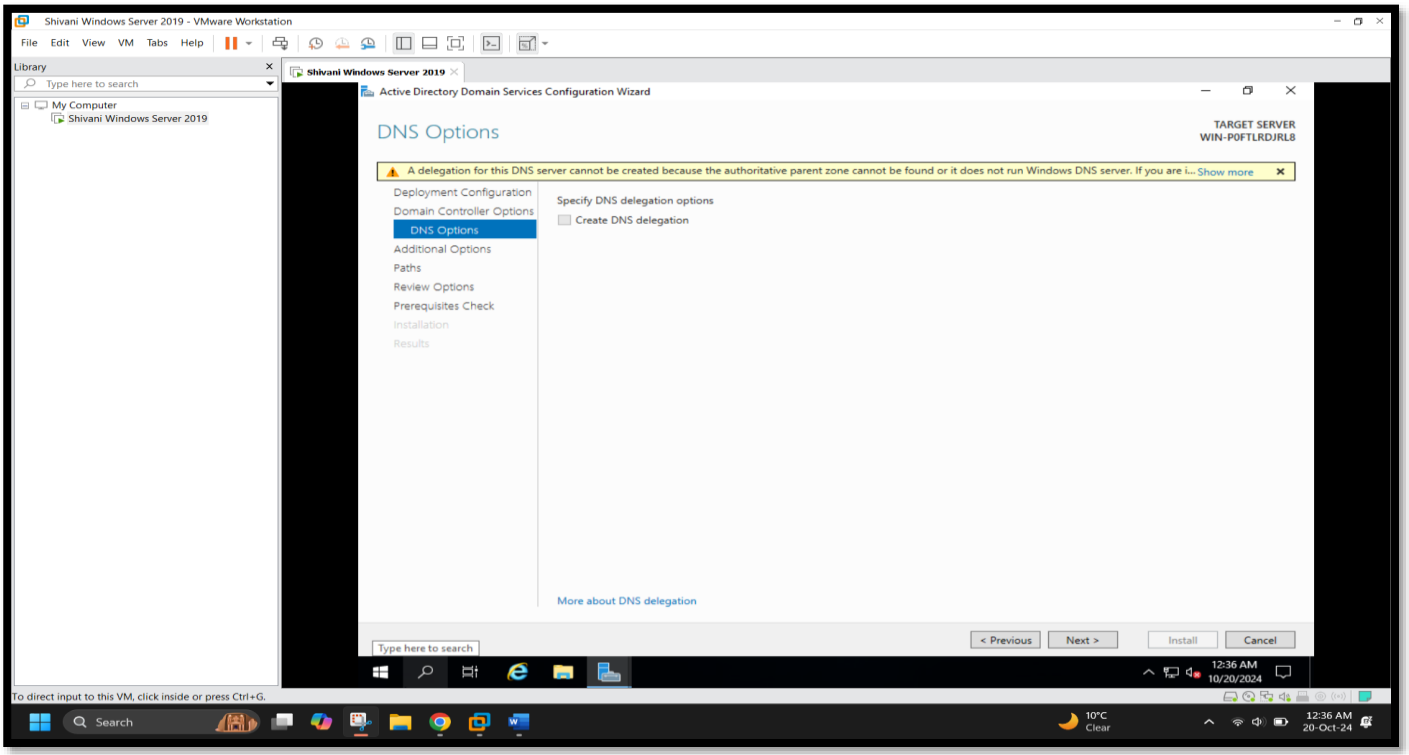


[Screenshot 3: the domain controller options where the functional levels are set, DNS is selected, and the DSRM password is configured]

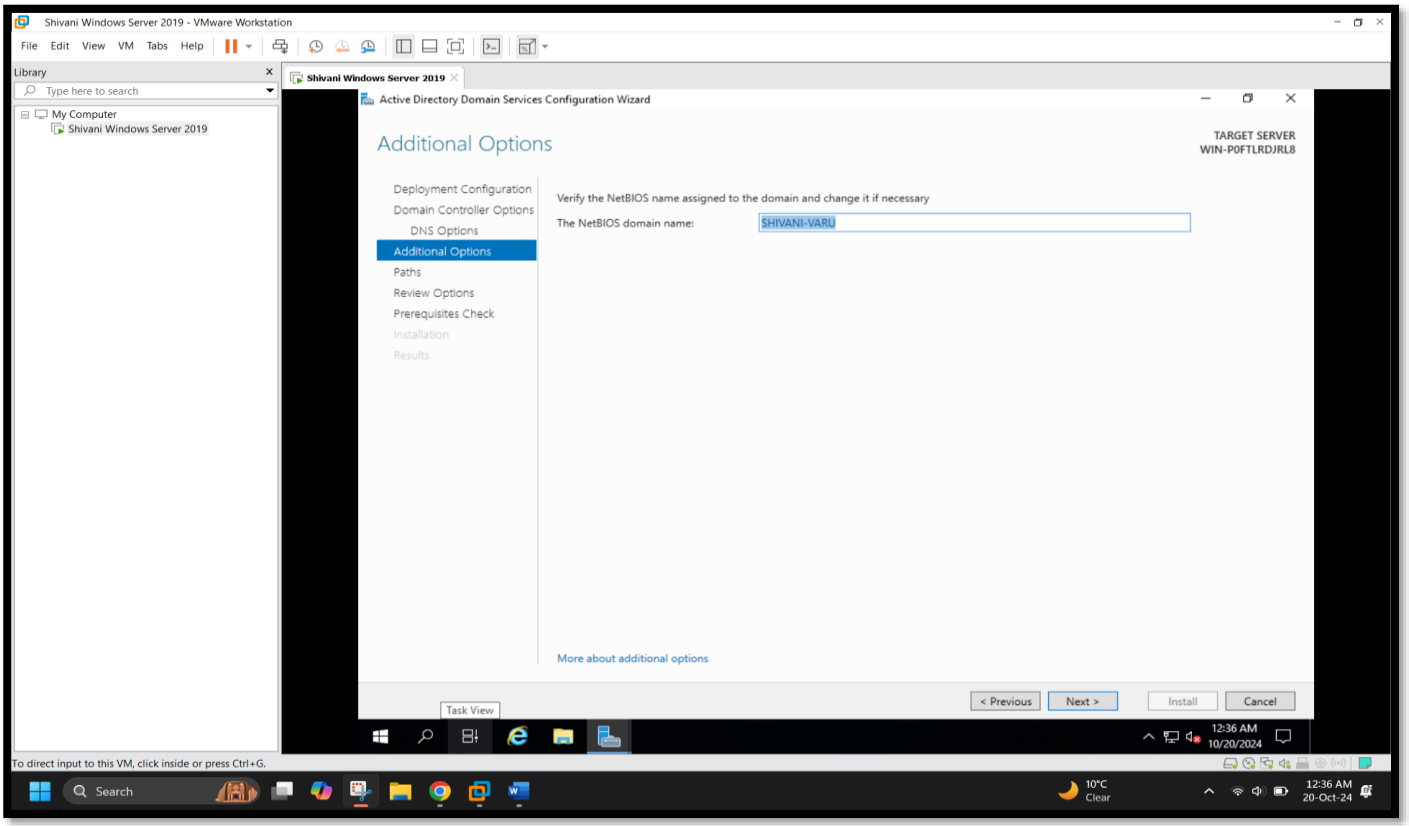


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 4: DNS Delegation Warning Message]

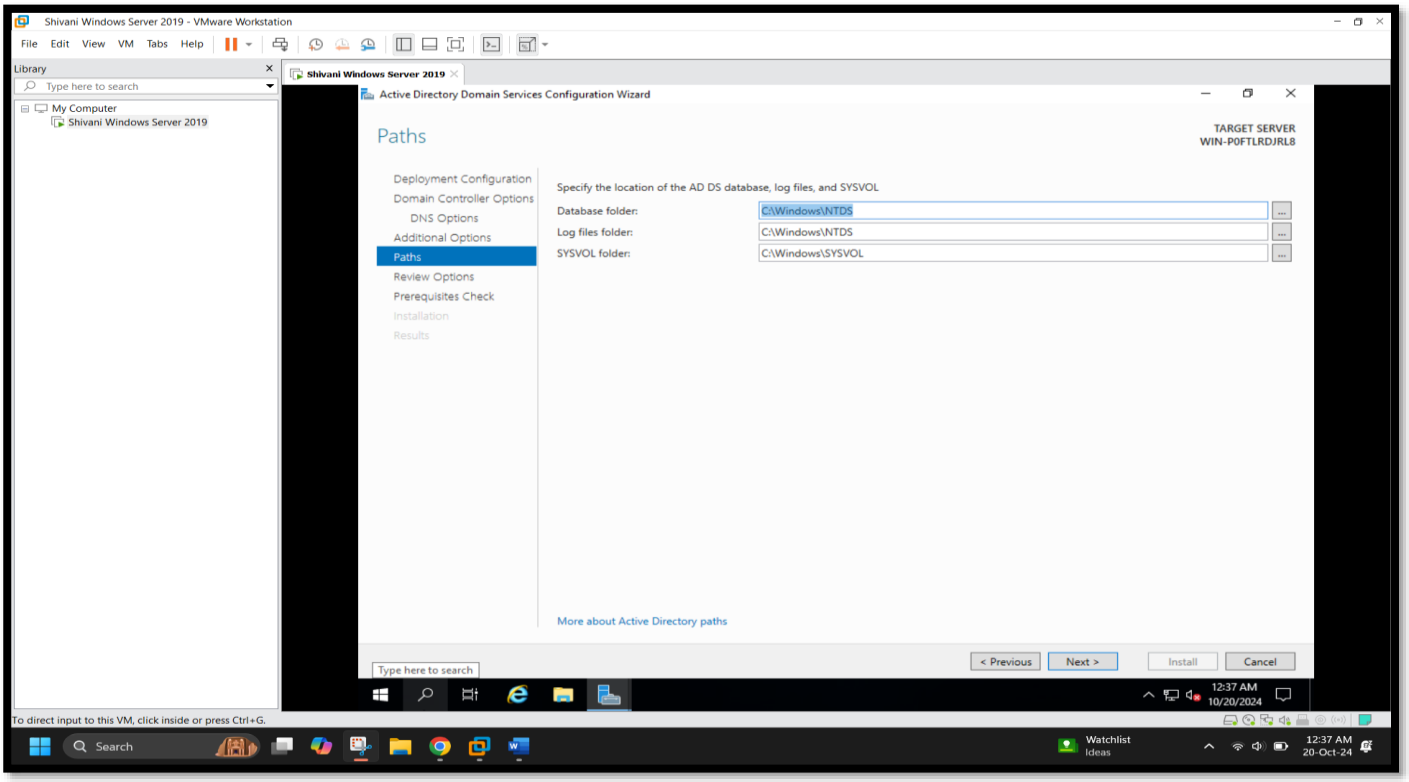


[Screenshot 5: the NetBIOS name assigned to the domain (SHIVANI-VARU)]

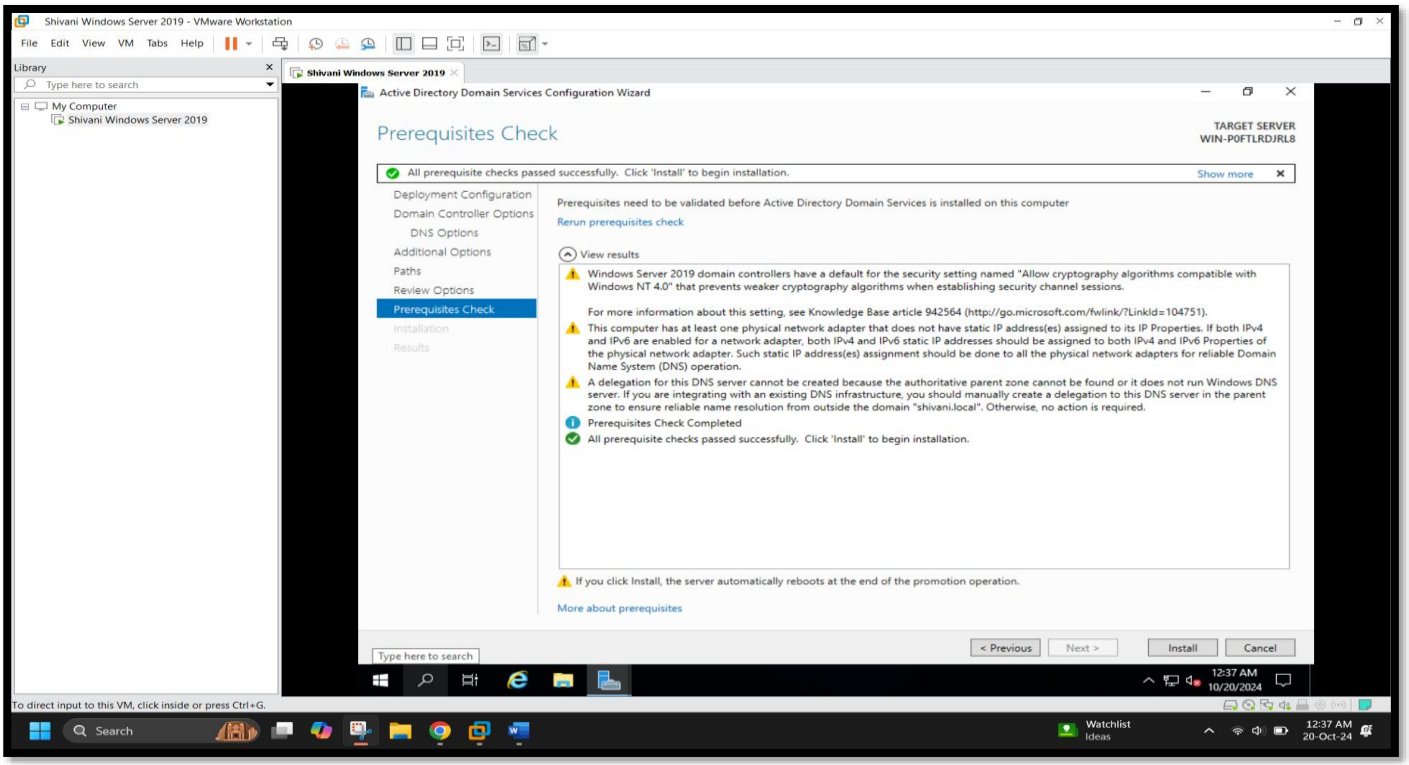


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 6: Paths Configuration for AD DS Database, Logs, and SYSVOL]

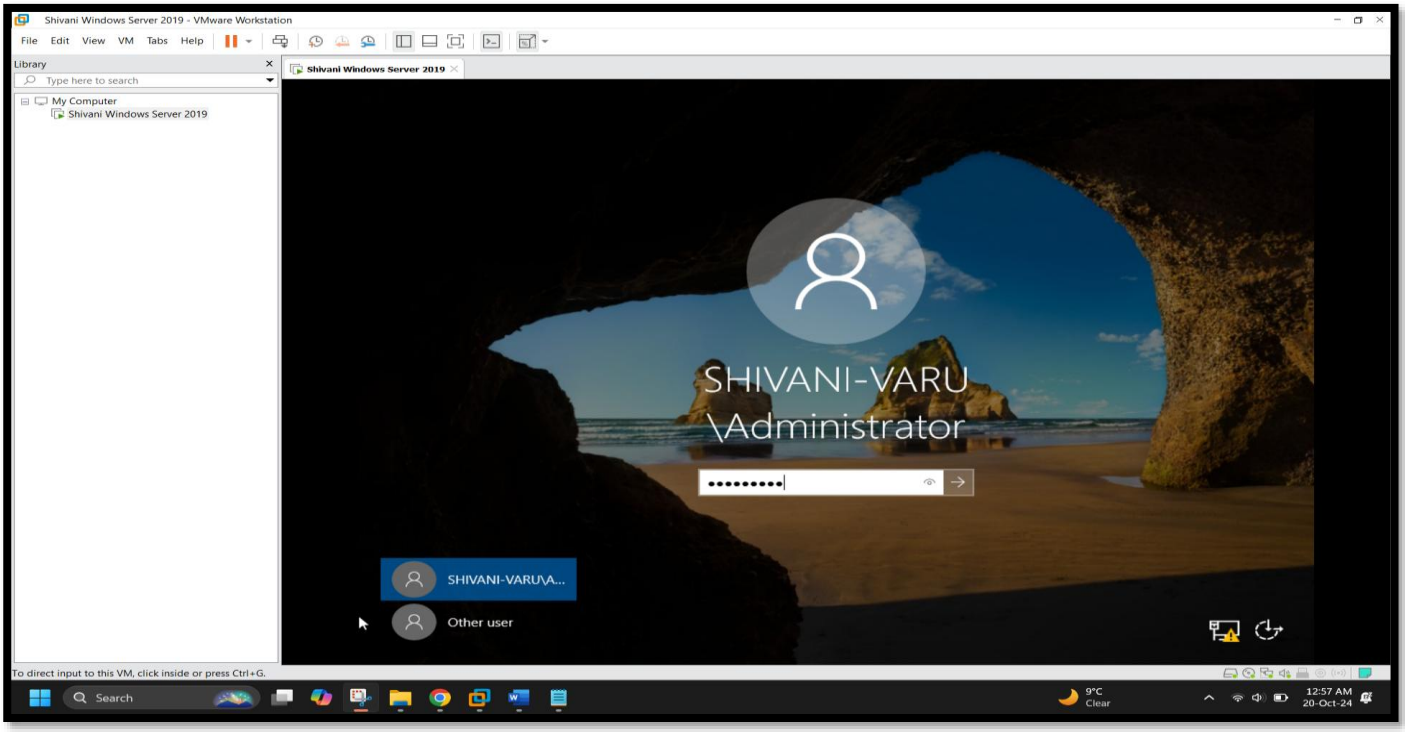


[Screenshot 7: the completed prerequisites check before promoting the server to a domain controller, indicating that all checks passed.]

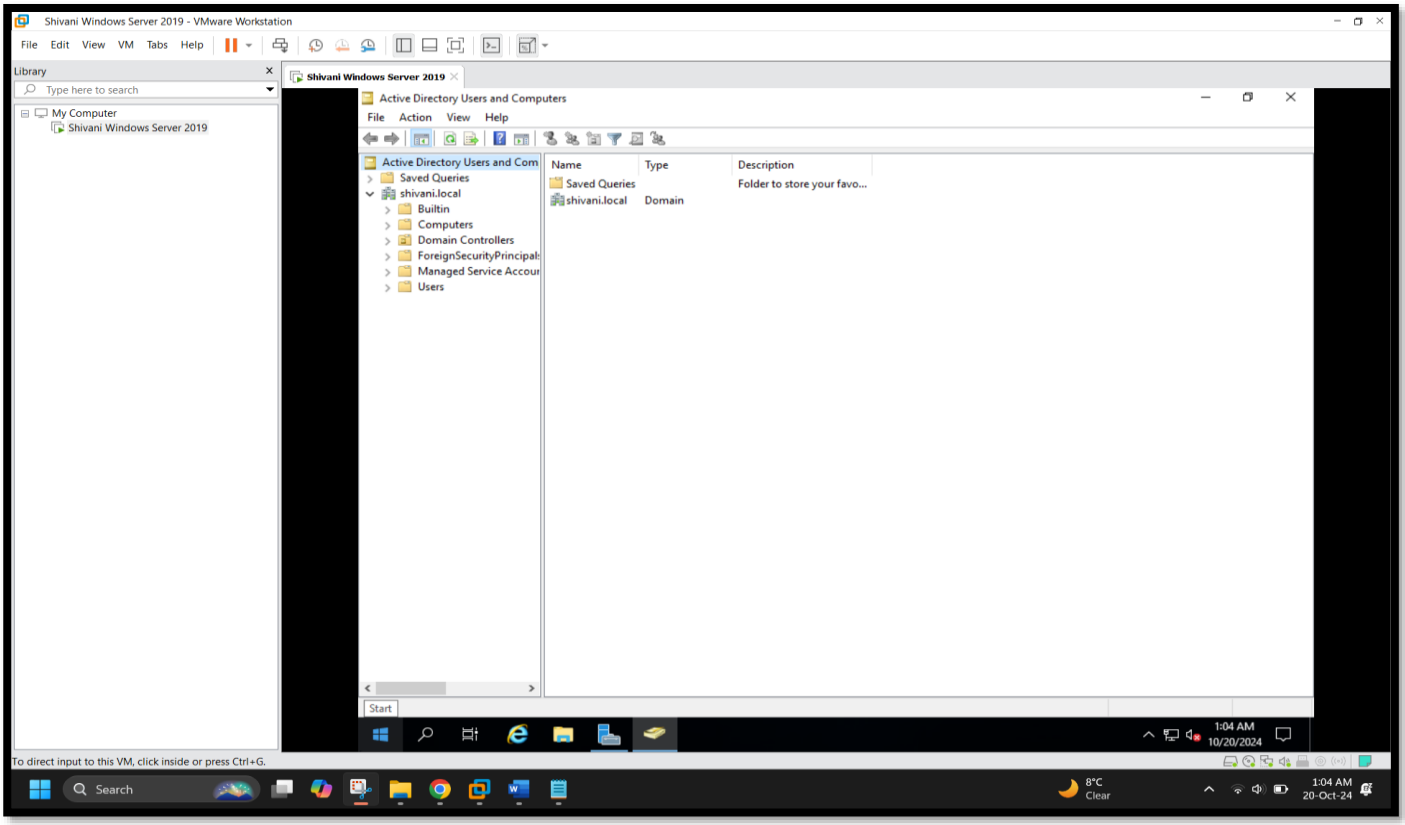


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 8: the login screen for the Administrator account on the domain controller (SHIVANI-VARU), which indicates that the domain promotion and server setup are complete.]



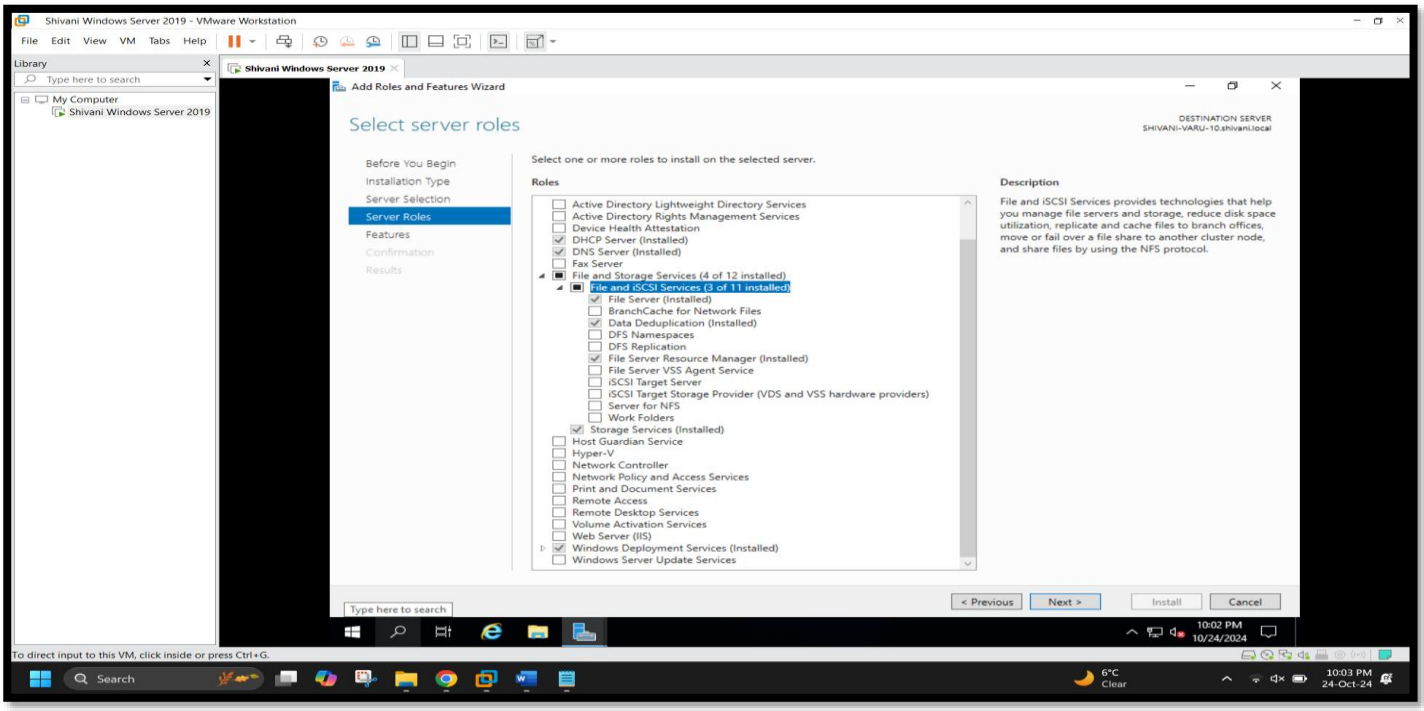
[Screenshot: Active Directory Users and Computers - Domain shivani.local]



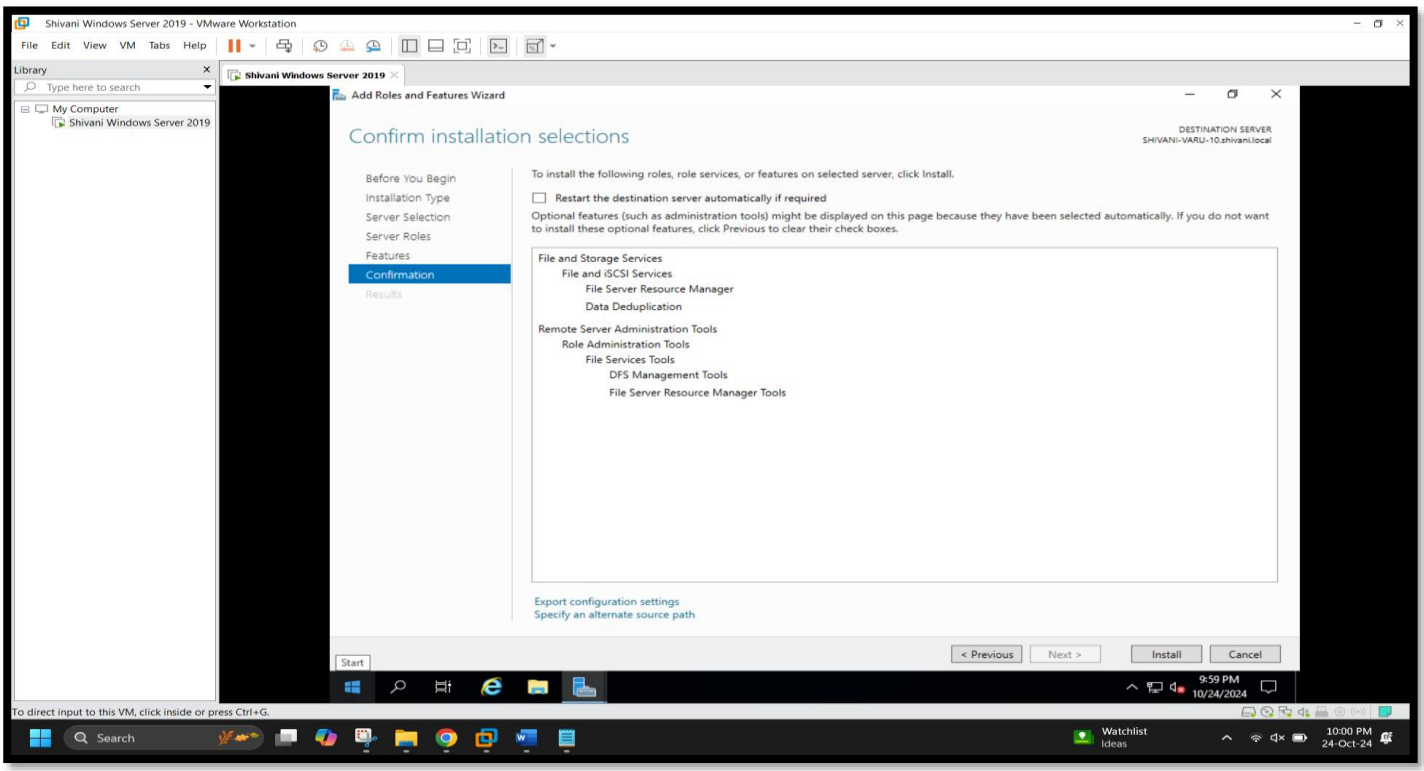
Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Exercise – 5 Enabling dedup (deduplication) on Windows Server 2019

[Screenshot 1 : Selecting Server Roles]

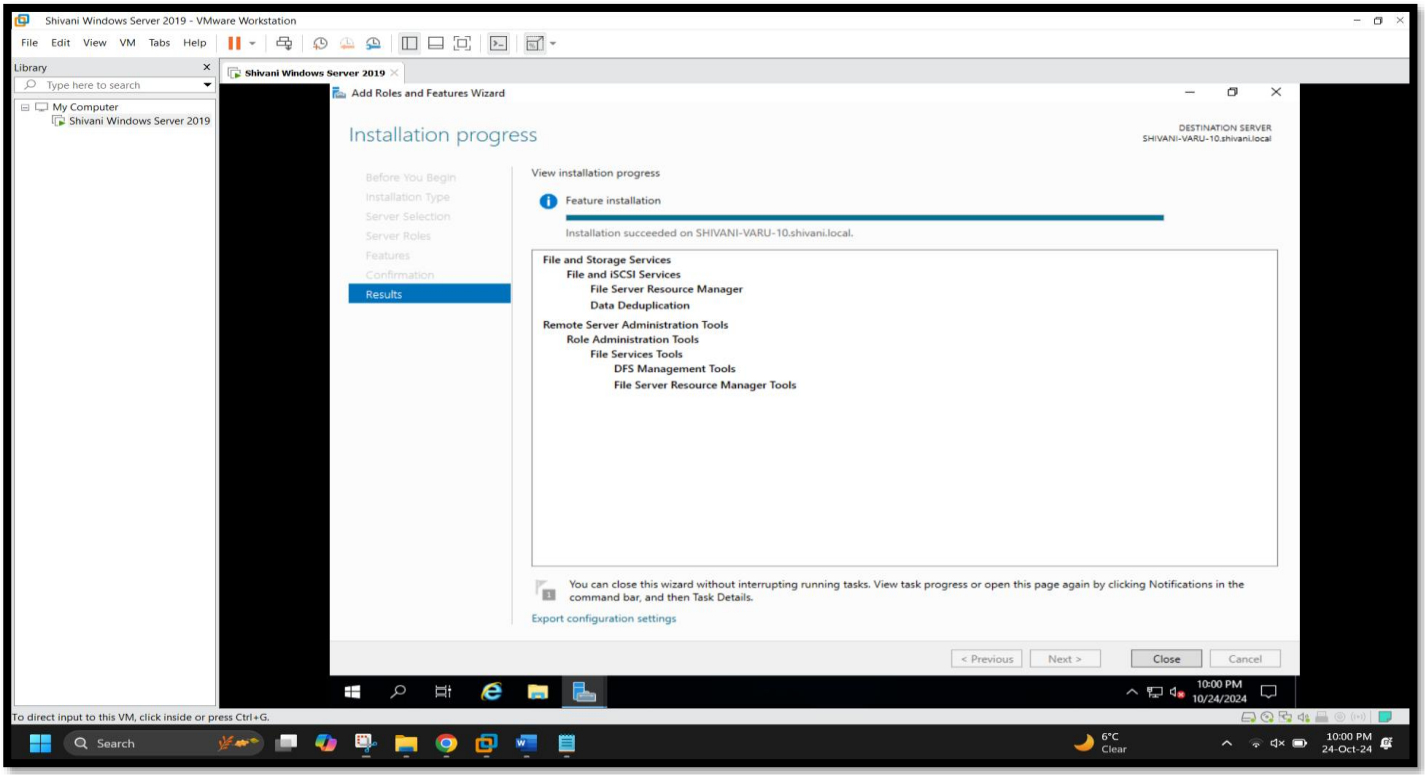


[Screenshot 2 : Confirmation of Installation]

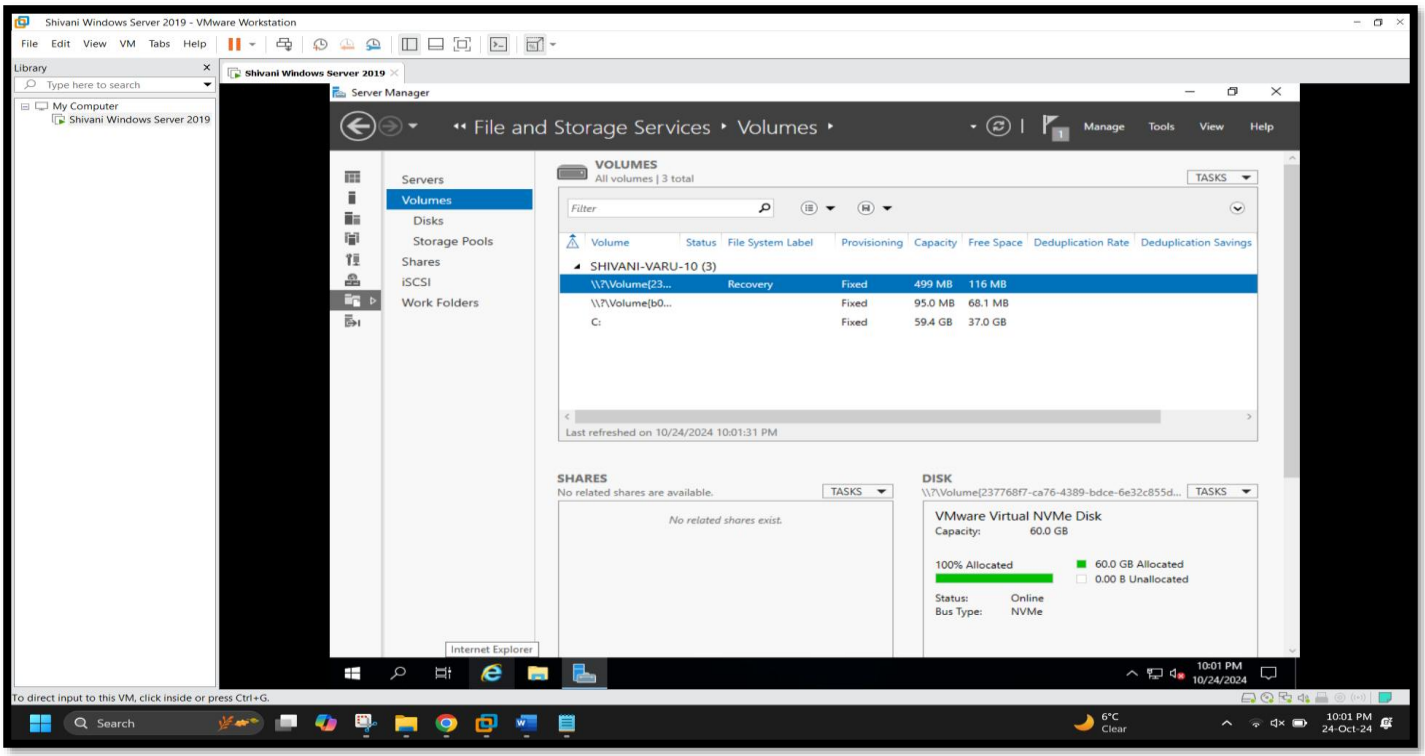


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 3 : Data Deduplication and other file services installed successfully on the destination server.]



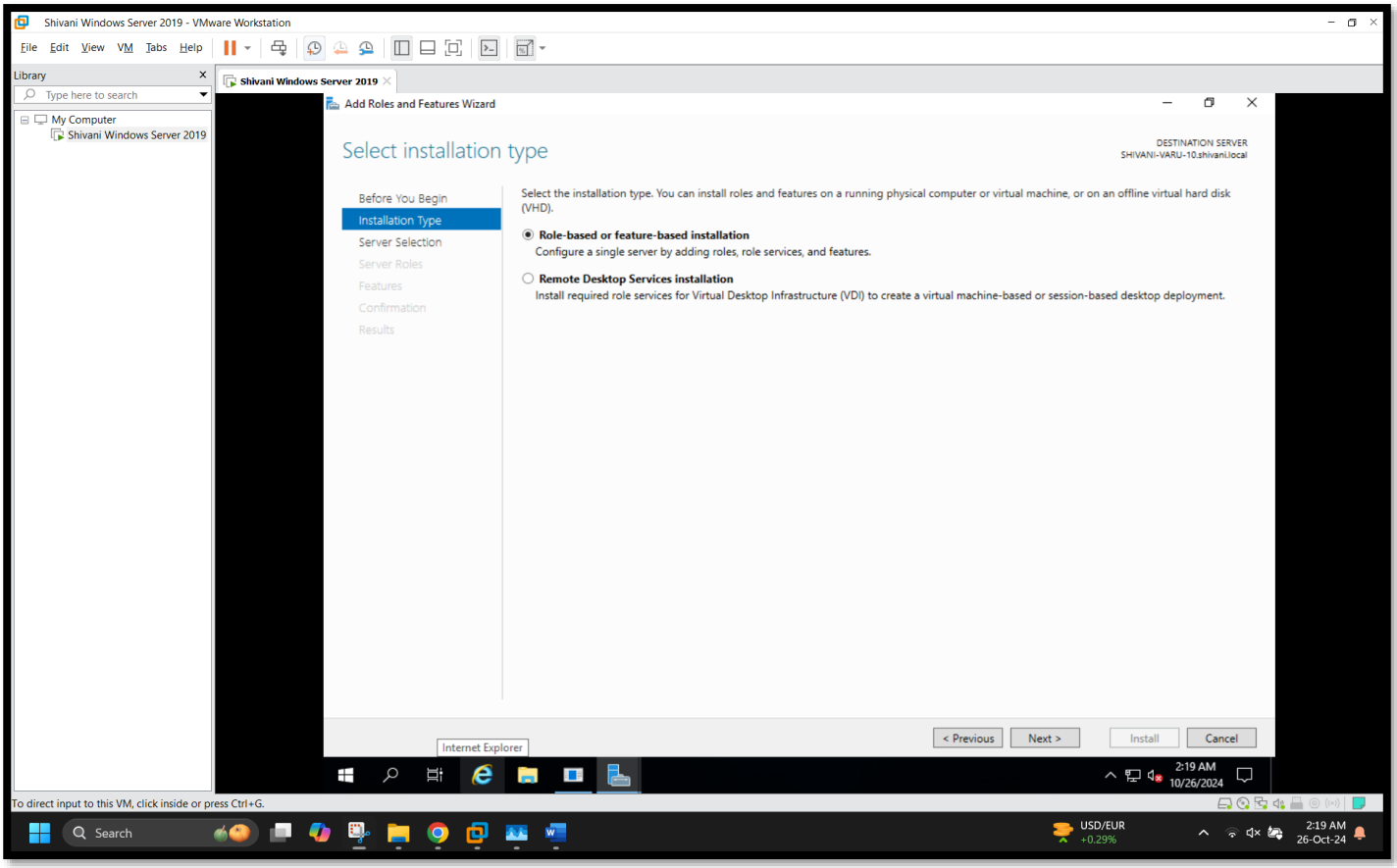
[Screenshot 4 : Viewing available volumes and deduplication settings within File and Storage Services on the server.]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

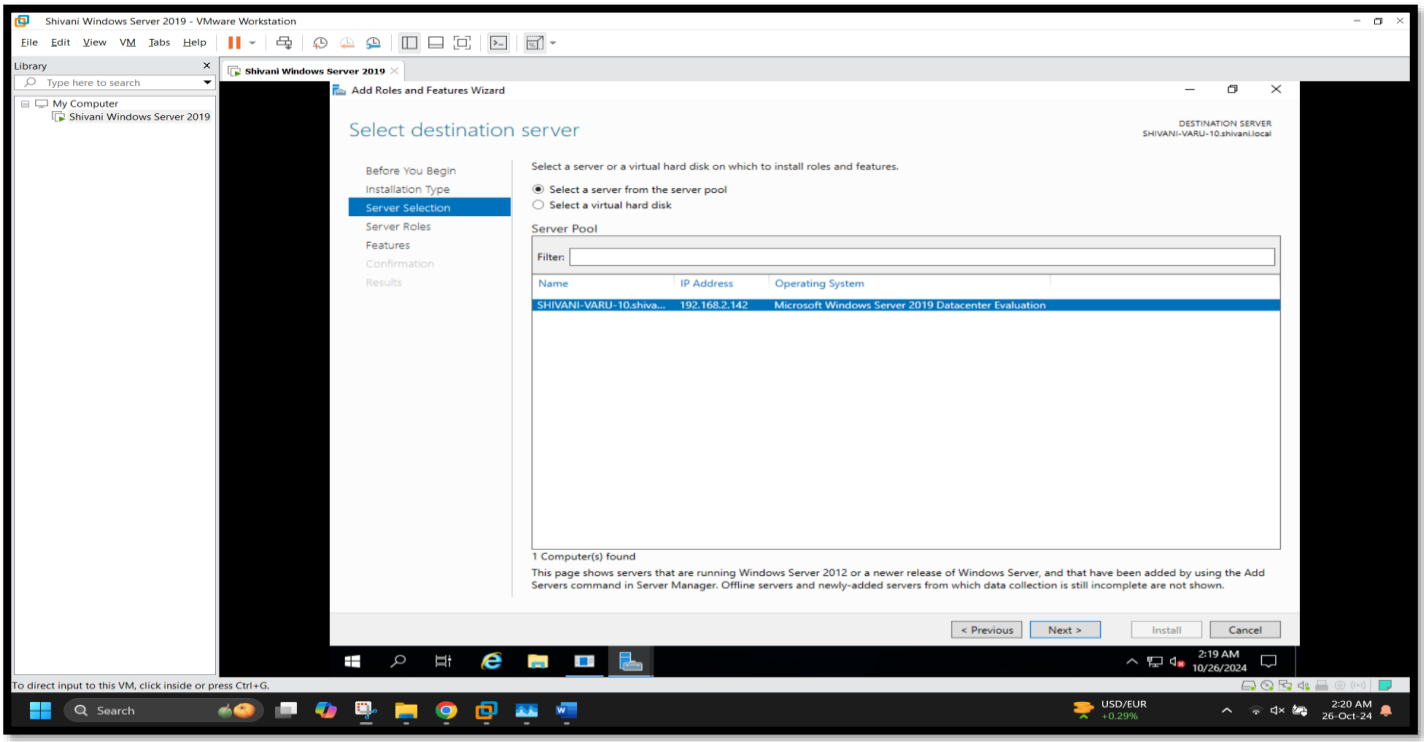
Exercise – 6 Installing Hyper-V on Windows Server 2019

[Screenshot 1 : Choosing the installation type for the Hyper-V role, with "Role-based or feature-based installation" selected]

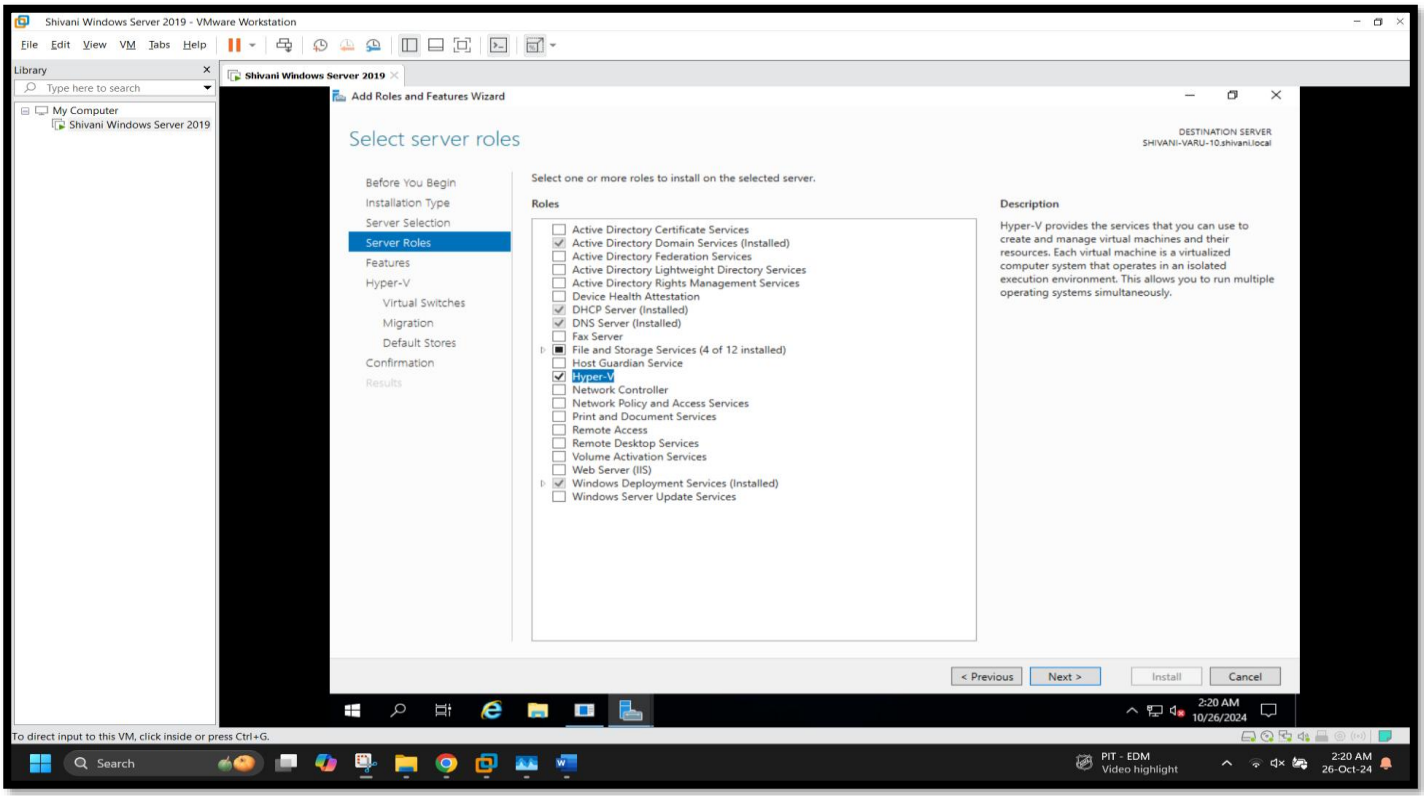


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 2 : Selecting the server from the server pool to install the Hyper-V role]

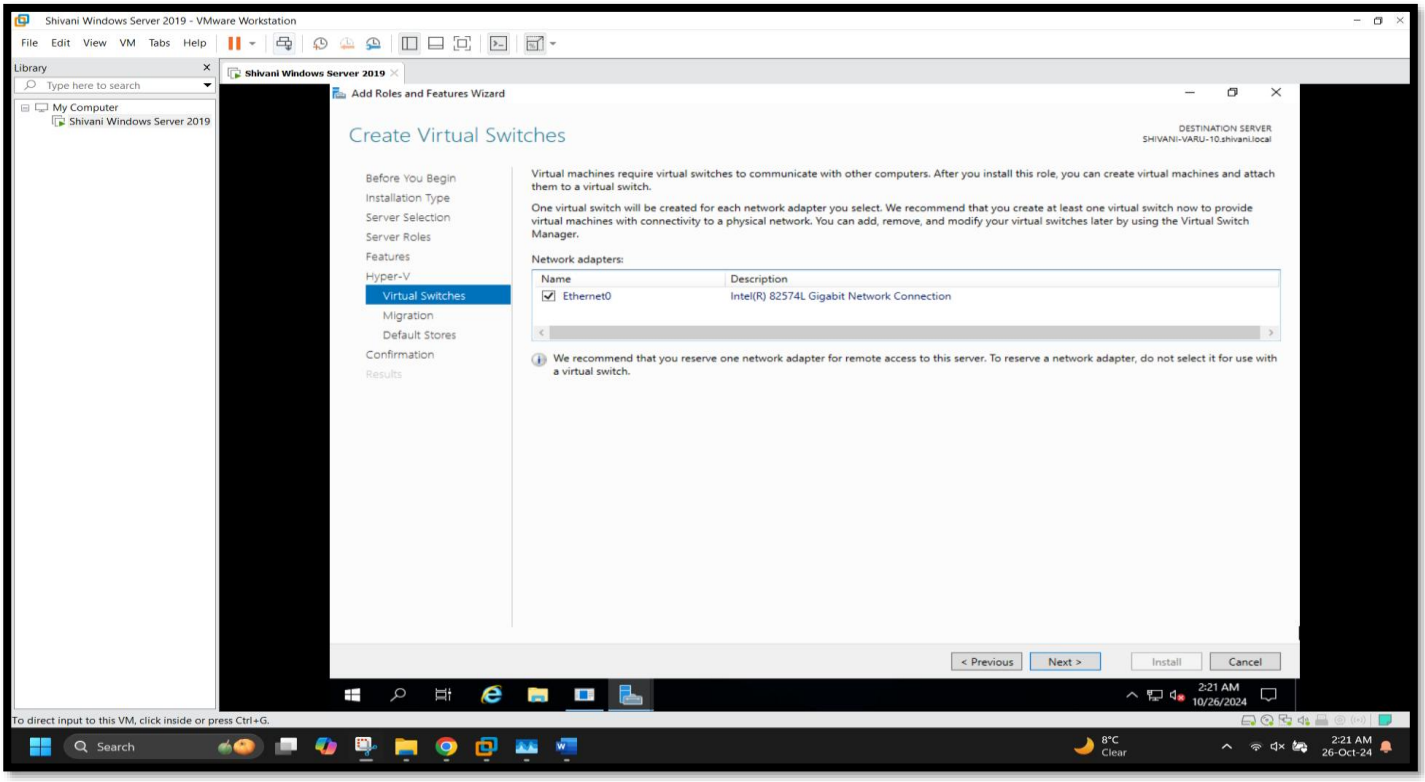


[Screenshot 3 : Selecting "Hyper-V" from the list of available server roles to install]

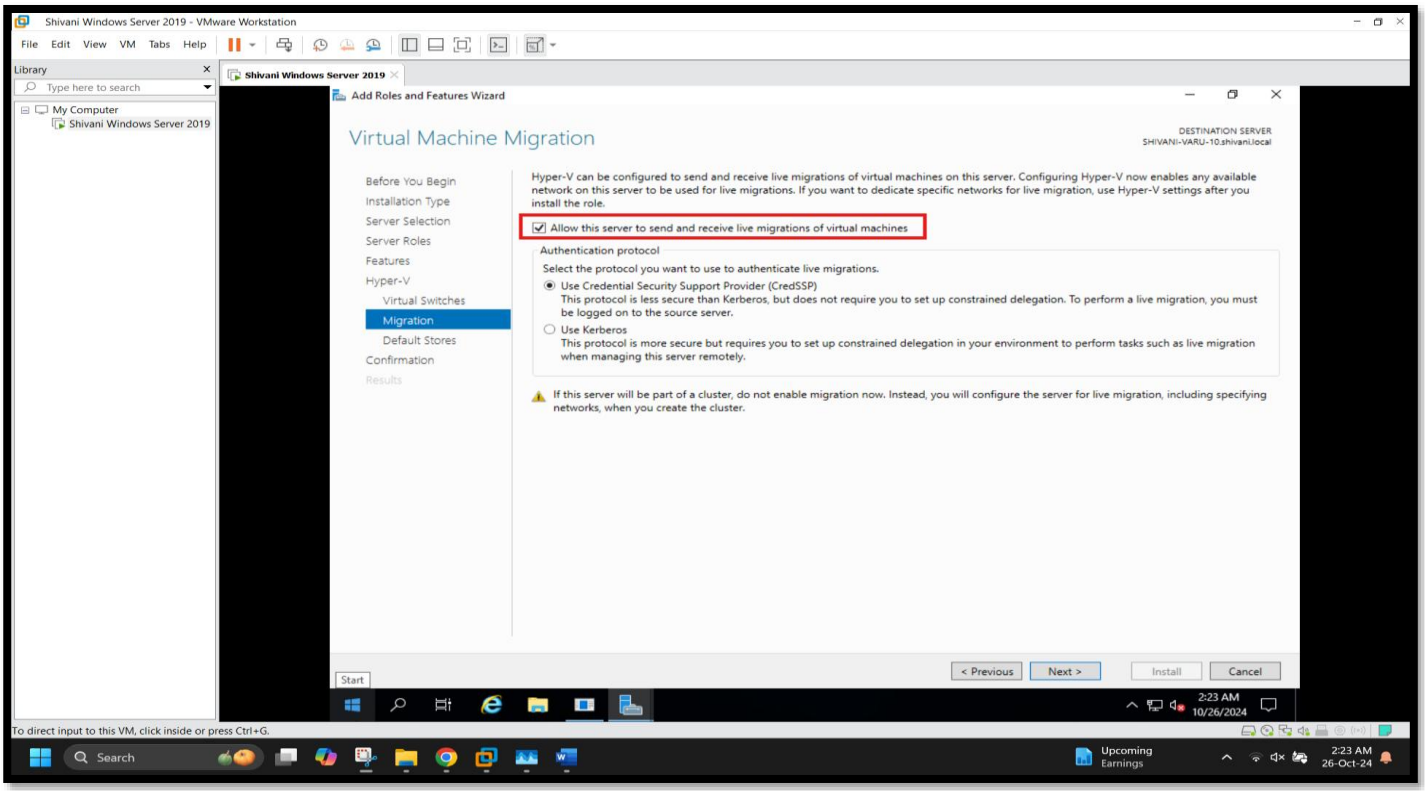


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 4 : Configuring the network adapter as a virtual switch for communication with other computers.]

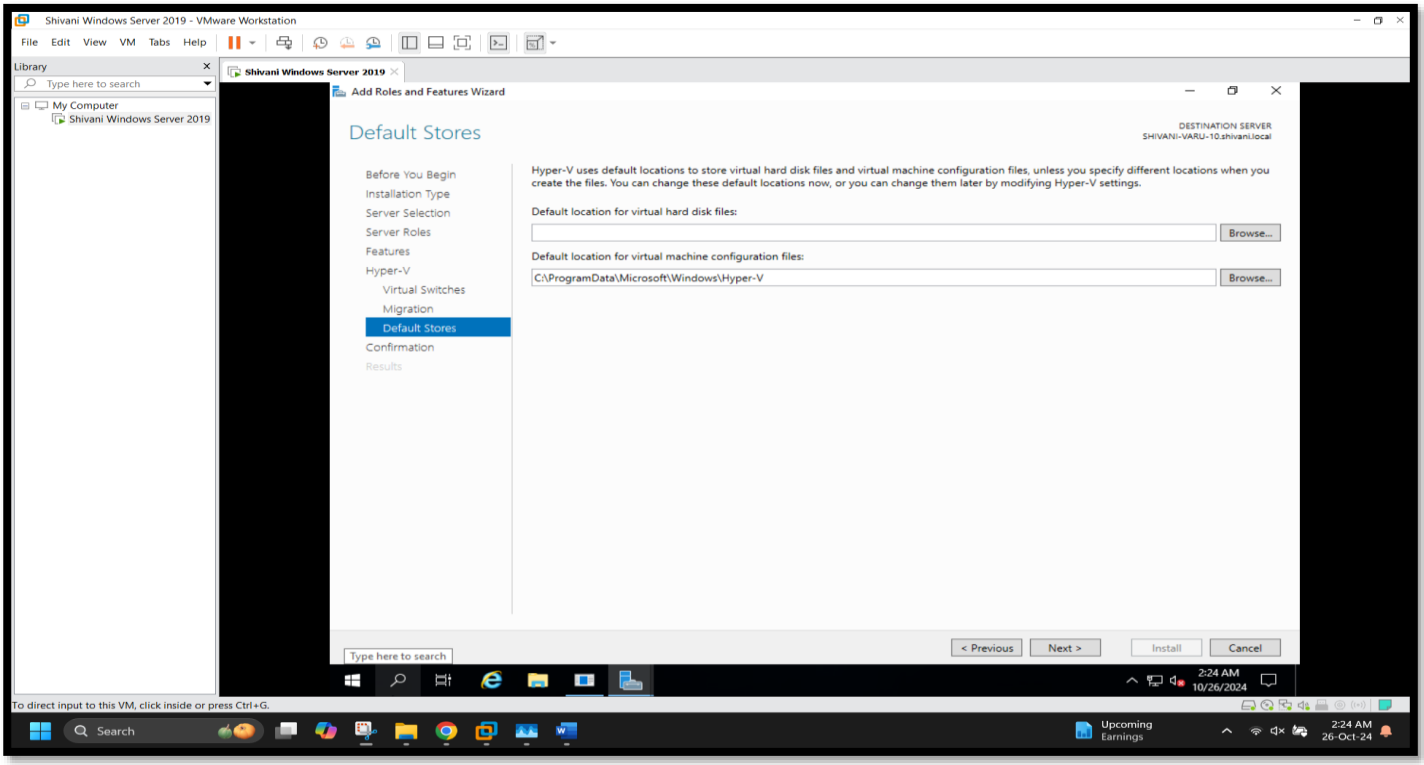


[Screenshot 5 : Enabling live migration for virtual machines and selecting the authentication protocol.]

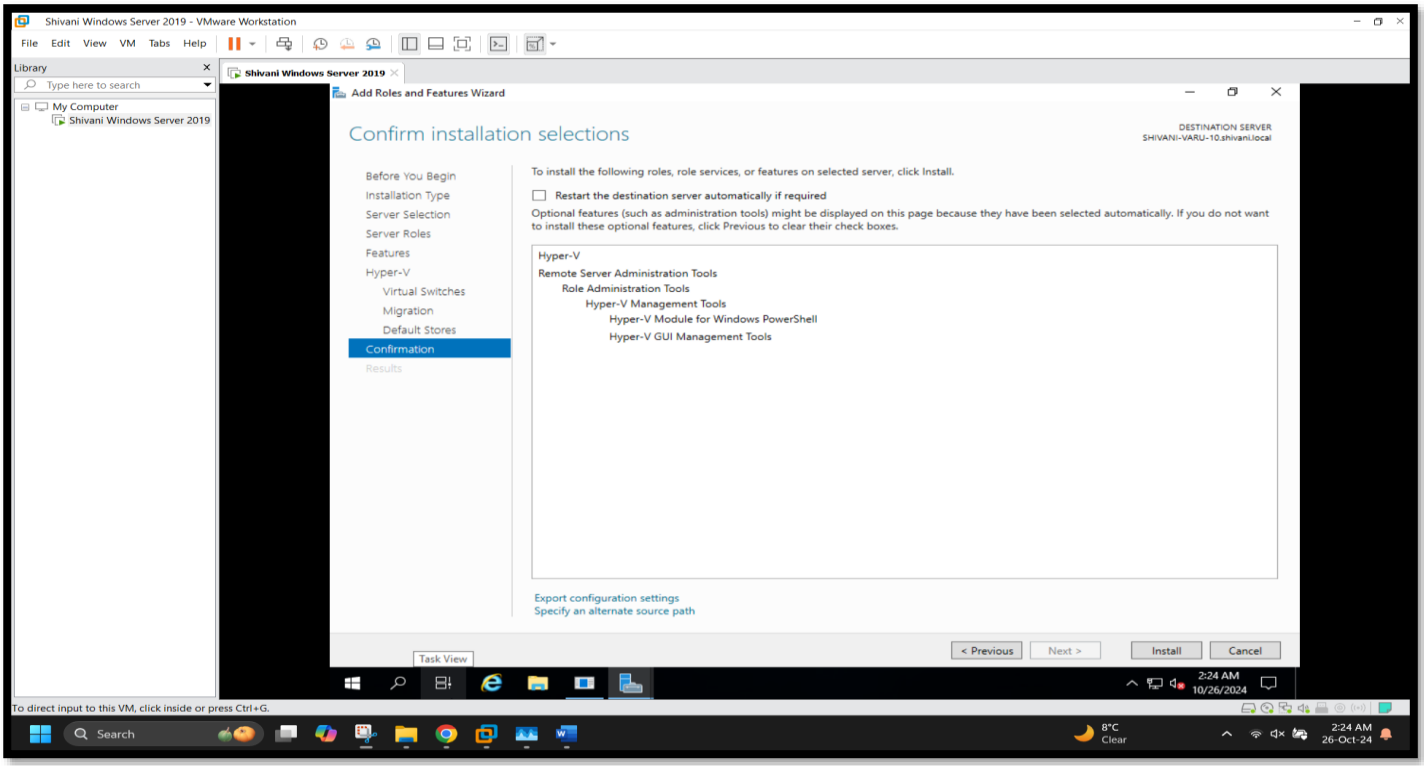


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 6 : Setting the default storage locations for virtual hard disk files and virtual machine configuration files.]

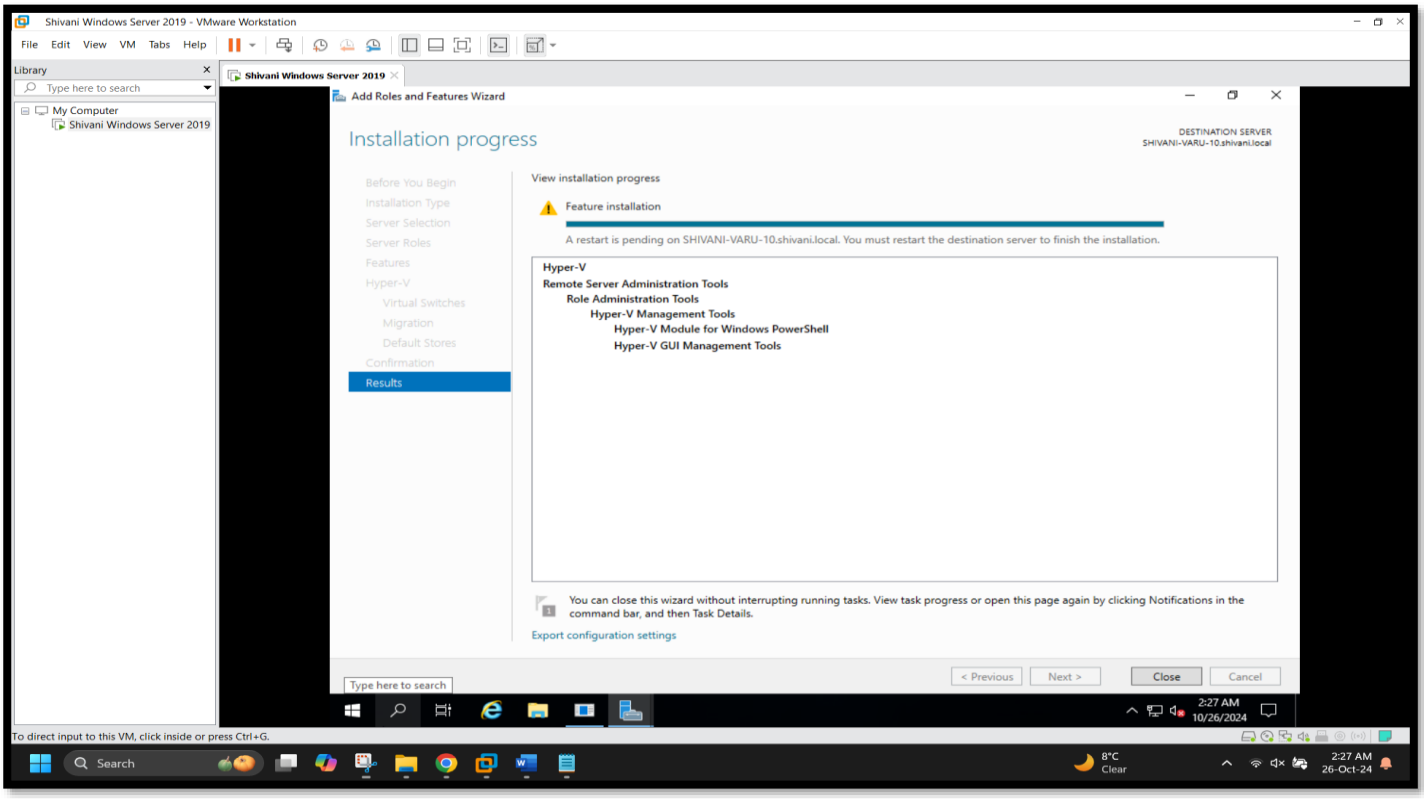


[Screenshot 7 : Reviewing the selected options for the Hyper-V installation before starting the installation process.]

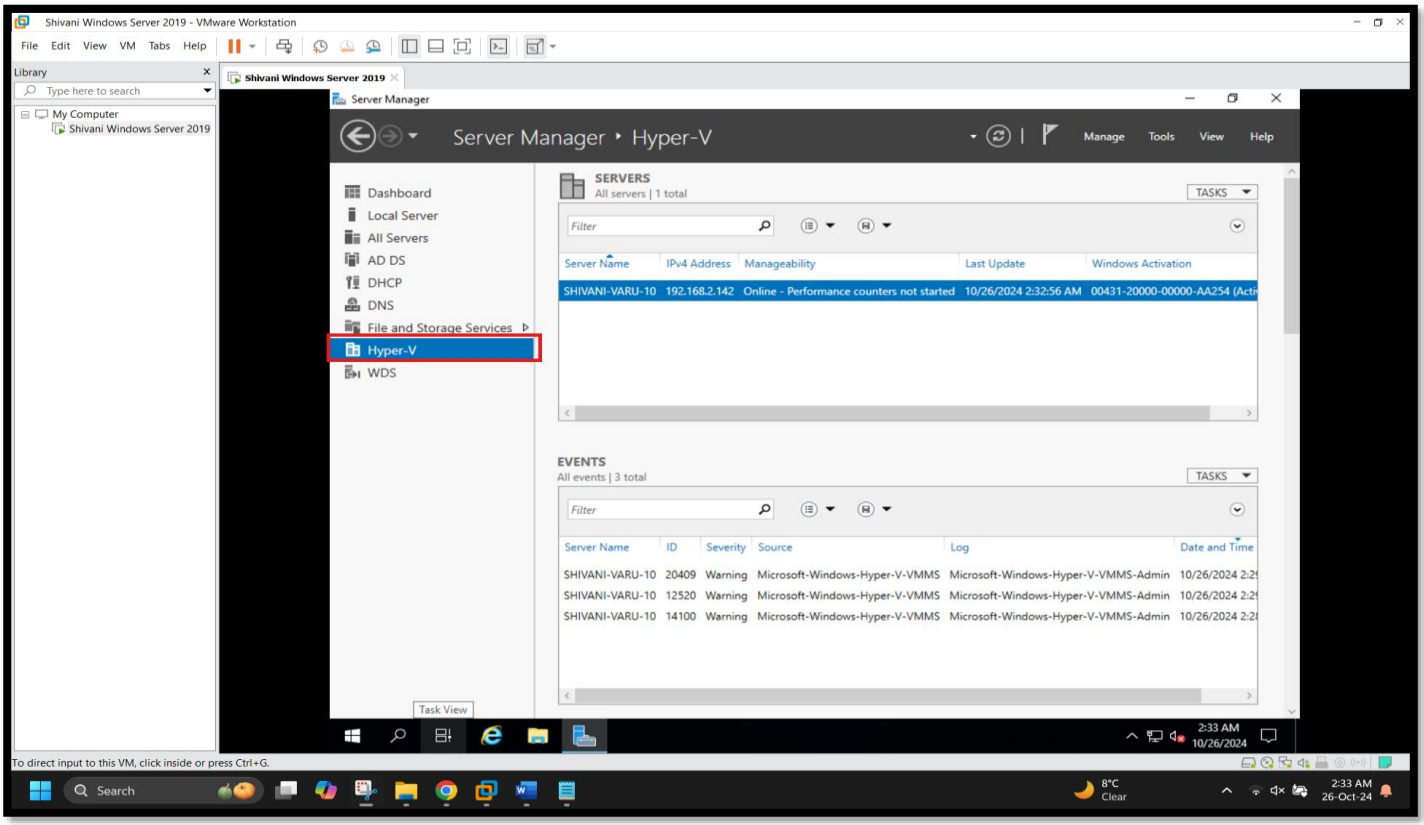


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 8 : Displaying the progress of the Hyper-V installation on the server.]



[Screenshot 9 : Hyper-V role has been successfully installed and added to Server Manager



Name: Shivani Shaileshkumar Varu Student ID: 101481565

Creating and Configuring Failover Clusters

Scenario

As the business of Contoso Ltd. grows, it's becoming increasingly important that many of the applications and services on its network are always available. Contoso has many services and applications that must be available to internal and external users who work in different time zones around the world. Many of these applications can't be made highly available by using Network Load Balancing (NLB). Therefore, you should use a different technology to make these applications highly available.

As one of the senior network administrators at Contoso, you're responsible for implementing failover clustering on the servers that are running Windows Server 2019 to provide high availability for network services and applications. You're also responsible for planning the failover cluster configuration and deploying applications and services on the failover cluster.

Objectives

After completing this Exercise, you'll be able to:

- Configure a failover cluster.
- Deploy and configure a highly available file server on the failover cluster.
- Validate the deployment of the highly available file server.

.....

Theoretical Background and Procedure:

Creating and configuring failover clusters overview

Failover clusters that you create in Windows Server have specific, recommended hardware and software configurations that allow Microsoft to support the cluster. The intent of failover clusters is to provide a higher level of service than standalone servers. Therefore, cluster hardware requirements are often stricter than the requirements for standalone servers.
This Exercise describes how to prepare for cluster implementation. It also discusses the hardware, network, storage, infrastructure, and software requirements for Windows Server 2019 failover clusters. Finally, this exercise outlines the steps for using the **Validate a Configuration Wizard** to help ensure the correct cluster configuration.

The Validate a Configuration Wizard and cluster support policy requirements

The Validate a Configuration Wizard

Whether you're configuring a brand new Windows failover cluster or are maintaining an existing one, the **Validate a Configuration Wizard** is a tool for verifying a storage configuration. Use the **Validate a Configuration Wizard** to perform a variety of tests to help ensure that cluster components are accurately configured and supported in a clustered environment.
The wizard includes various tests, such as listing the system configuration or performing storage and network tests. These tests can run on a new, proposed member of a cluster, or you can run

them to establish a baseline for an existing cluster. The wizard can also troubleshoot a broken cluster by isolating the network, storage, or system component that's failing a particular test.

Support policy requirements
Before you create a new failover cluster, Microsoft strongly recommends that you validate the configuration to make sure that the hardware and hardware settings are compatible with failover clustering. Run the failover cluster validation tests on a fully configured failover cluster before you install the Failover Clustering feature.

Cluster validation is intended to:
- Find hardware or configuration issues before a failover cluster goes into production.
- Help ensure that the clustering solution that you deploy is dependable.
- Provide a way to validate changes to the hardware of an existing cluster.
- Perform diagnostic tests on an existing cluster.

Note: Microsoft supports a cluster solution only if the complete configuration passes all validation tests and if all hardware is certified for the version of Windows Server that the cluster nodes are running.

Indicators and their meanings
The possible indicators that the wizard will present include:
- A green check mark (passed). This indicates that the failover cluster is valid.
- A yellow yield sign (warning). The yellow yield sign indicates that the aspect of the proposed failover
cluster that's being tested isn't in alignment with Microsoft best practices. Investigate this aspect to make sure that the configuration of the cluster is acceptable for the cluster's environment, the requirements of the cluster, and the roles that the cluster hosts.
- A red circle with a single bar (canceled). If a failover cluster receives a red “X” (fail) in one of the tests, you can't use the part of the failover cluster that failed in a Windows Server failover cluster. Addition- ally, if a test fails, all other tests don't run, and you must resolve the issue before you install the
failover cluster.

Validate after changes
Run validation tests when a major component of the cluster is changed or updated. For example, run validation tests when you make any of the following configuration changes to a failover cluster:

- Add a node to the cluster.
- Upgrade or replace the storage hardware.
- Upgrade the firmware or the driver for host bus adapters.
- Update the multipathing software or the version of the device-specific module.

● Change or update a network adapter.

Microsoft Support might also ask you to run validation tests against a production cluster. When you do this, failover cluster validation tests perform a hardware and software inventory, test the network, validate the system configuration, and perform other relevant tests. In some scenarios, you can run only a subset of the tests. For example, when troubleshooting a problem with networking, Microsoft Support might ask you to run only the hardware and software inventory and the networking test against the production cluster.
When an underlying storage configuration change or problem causes a cluster storage failure, Microsoft Support might also ask that you run validation tests on production clusters. The relevant disk resources and the resources on which the disks depend are taken offline during the test. Therefore, run validation tests when the production environment isn't in use.

Create a failover cluster
Before creating a failover cluster, verify the following prerequisites:
● Make sure that all the servers that will function as nodes are running the same version of Windows Server.
● Ensure that you meet all hardware and software requirements.
● To add clustered storage during the creation process, make sure that all servers can access the storage.

Adding a failover cluster by using the Create Cluster Wizard

Follow the instructions in the **Create Cluster Wizard** to specify:
● The servers to include in the cluster.
● The name of the cluster.
● Any IP address information that your Dynamic Host Configuration Protocol (DHCP) settings don't automatically supply.

After the wizard runs, a **Summary** page appears. Select the **View Report** option to access a report on the tasks that the wizard performed. After you close the wizard, you can find the report at <*SystemRoot*>\ Cluster\Reports, where *SystemRoot* is the location of the operating system; for example, C:\Windows.

Note: If you're using Windows Server 2019, you can use a distributed network name for the cluster. A distributed network name uses the IP addresses of the member servers instead of requiring a dedicated IP address for the cluster. By default, Windows uses a distributed network name if it detects that you’re creating a cluster in Microsoft Azure, which means that you don't have to create an internal load balancer for the cluster. Windows will use a normal static or IP address if you're running on-premises.

Adding a failover cluster in Windows Admin Center

Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Windows Admin Center is a browser-based management tool that allows you to manage Windows Server computers with no Azure or cloud dependencies. You can manage failover cluster nodes as individual servers by adding them as server connections in Windows Admin Center. You can also add them as failover clusters to a view and manage cluster resources, storage, network, nodes, roles, virtual machines, and virtual switches.

Windows Admin Center provides one user interface (UI) in which you can:

- Examine cluster performance history to assess how clusters and nodes are performing.
- Examine the system insights feature of Windows Server, which uses machine learning and predictive analytics.
- Utilize persistent memory.

When you use **Failover Cluster Manager** in Windows Server 2019, you'll receive a prompt to try managing your clusters with Windows Admin Center. To add a failover cluster to Windows Admin Center, add a failover connection through the UI. Additionally, you can manage hyper-converged clusters by adding a cluster as a hyper-converged cluster connection.

To create a failover cluster by using Windows Admin Center, follow these steps:

1. Under **All Connections**, select **Add**.
2. Select **Failover Connection**.
3. Enter the name of the cluster, and if prompted, enter the credentials to use.
4. Add the cluster nodes as individual server connections.
5. Select **Submit** to finish.

After creating a cluster, you can use the **Failover Cluster Management** console to monitor its status and manage the available options.

Additional reading: For more information about failover clustering requirements and storage, refer to **Failover clustering hardware requirements and storage options**

Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Exercise #7: Create a failover cluster

In this Exercise, you will learn how to:

- Validate a cluster configuration.
- Create a failover cluster.

Exercise steps:

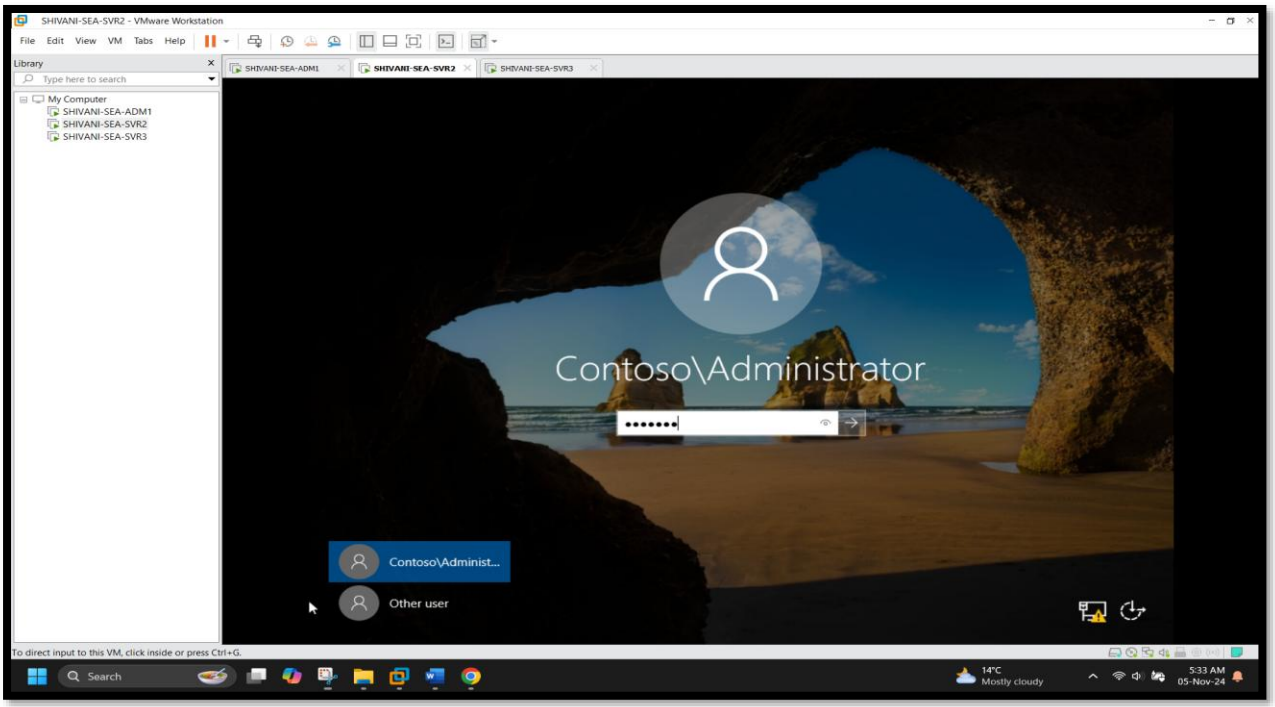
Validate and create a failover cluster

1. On **SEA-SVR2 (use your server's name)**, sign in as **Contoso\Administrator** with password **Pa55w.rd**.
2. Select **Start**, and then select **Windows PowerShell**.
3. Use the **Test-Cluster SEA-SVR2, SEA-SVR3** cmdlet to start cluster validation.
4. Review the validation report. You can expect a few warning messages to display, but there should be no errors.
5. Use the **New-Cluster -Name WFC2019 -Node sea-svr2 -StaticAddress 172.16.10.125** cmdlet to create a new cluster.
6. Use the **Add-ClusterNode -Name SEA-SVR3** cmdlet to add **SEA-SVR3** as a cluster node.

~~~~~~

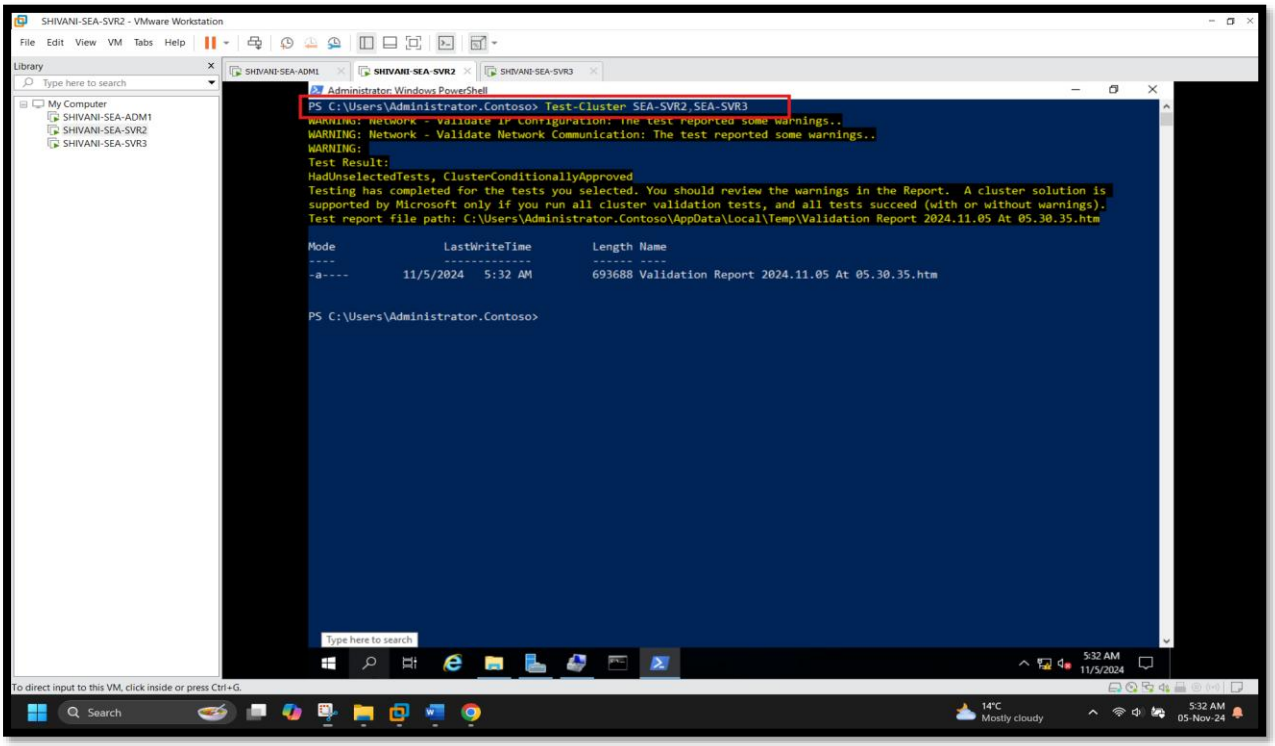
Paste your screenshots here

[Screenshot 1 : Logged into SEA-SVR2 as Contoso\Administrator]

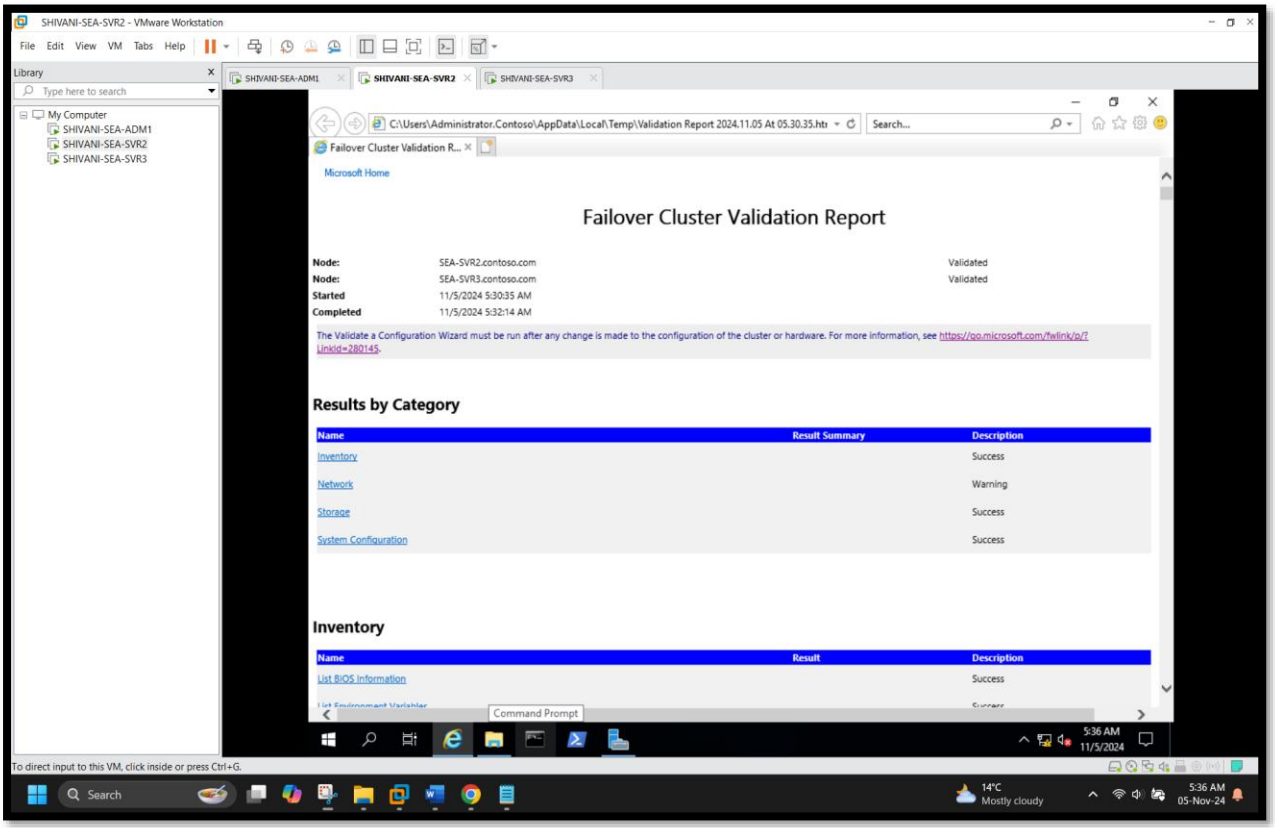

~~~~~~

Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 2: Executing the Test-Cluster command on SEA-SVR2 and SEA-SVR3]

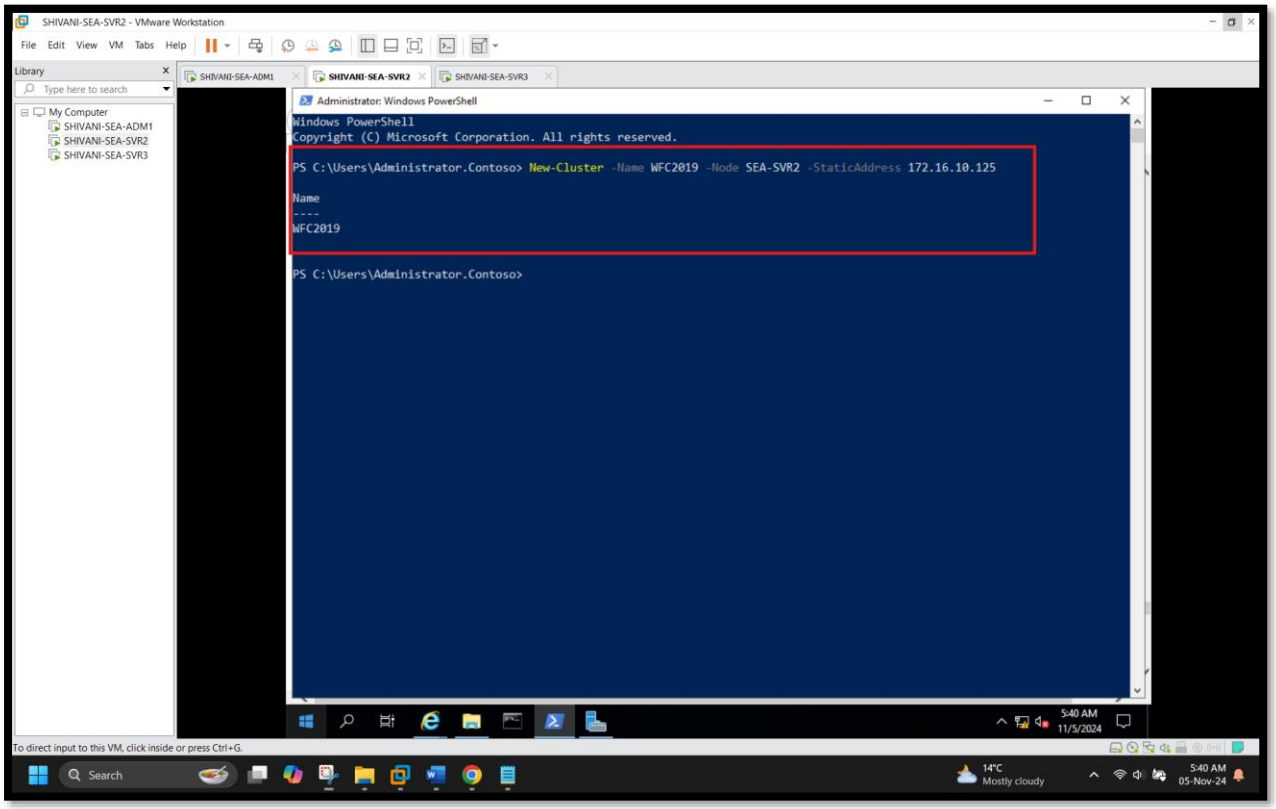


[Screenshot 3 : Validation report summary showing test results for both server node]

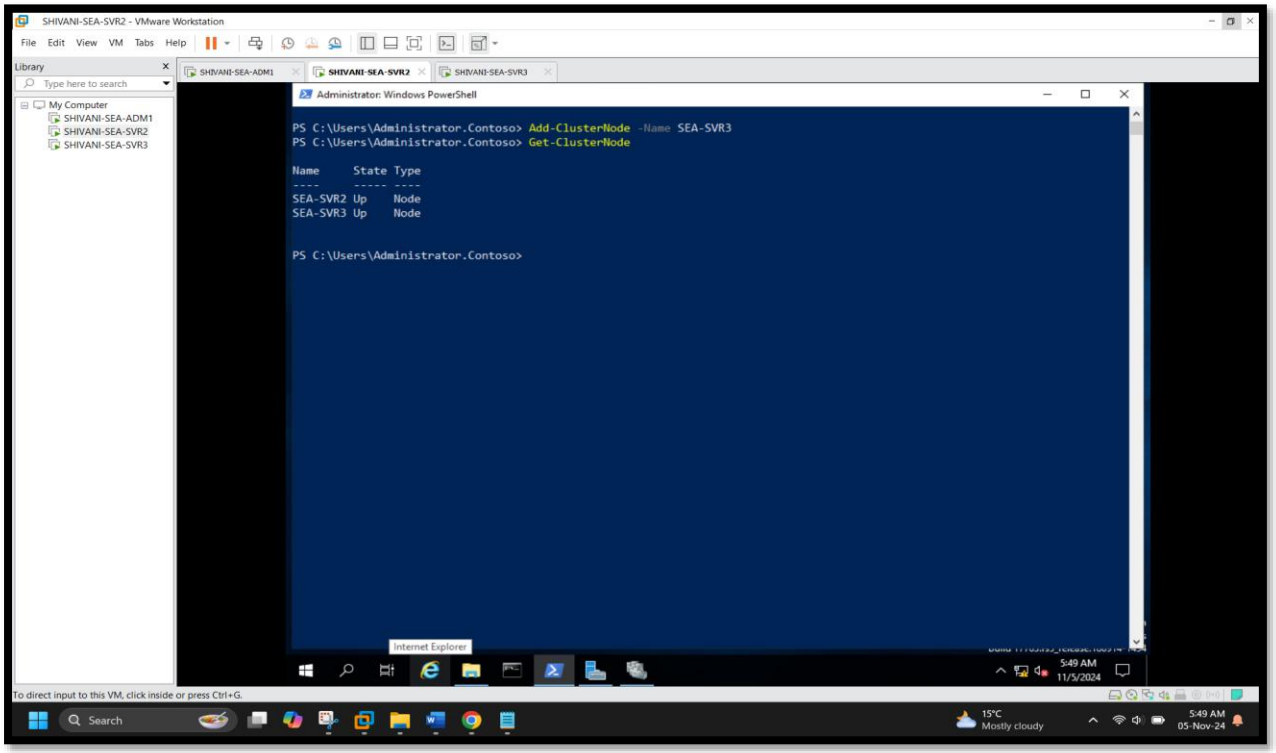


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 4: Creating the failover cluster using New-Cluster on SEA-SVR2]

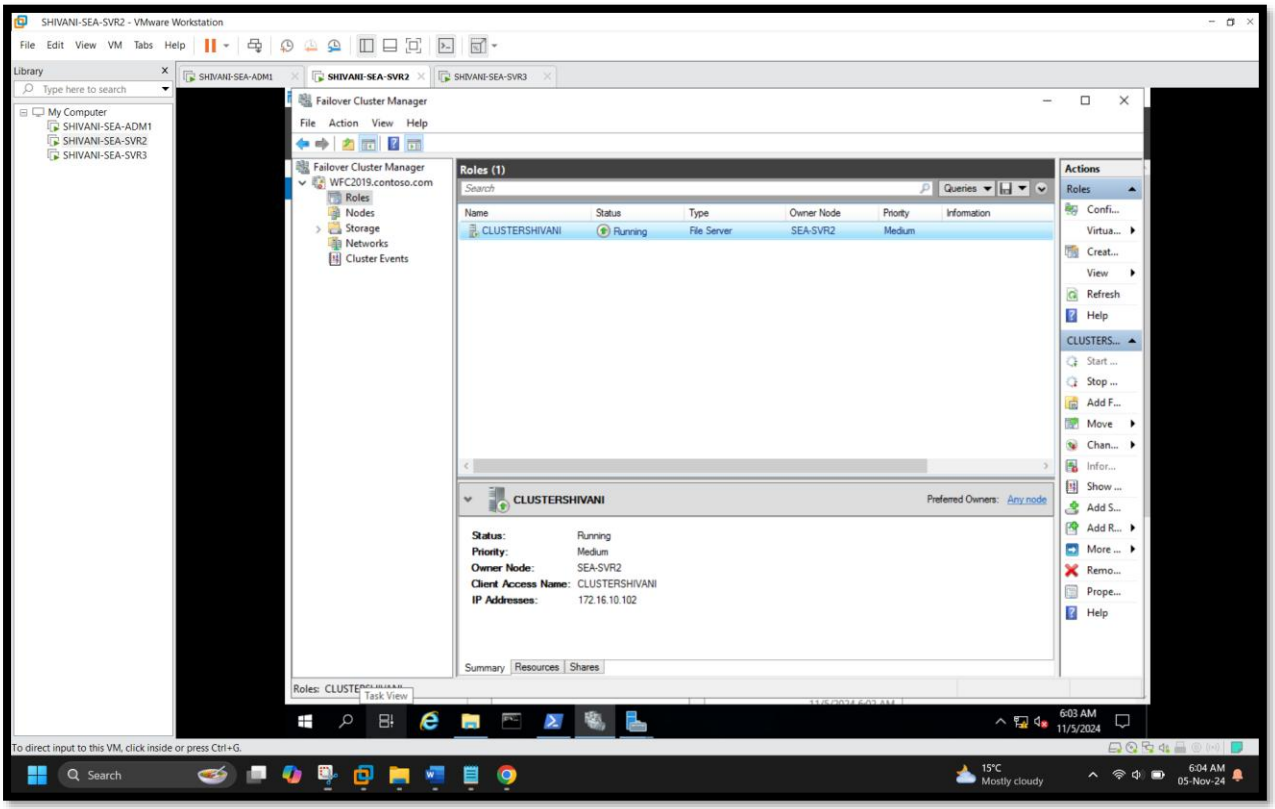


[Screenshot 5: Adding SEA-SVR3 to the cluster using the Add-ClusterNode command]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 6: Configured highly available file server role in Failover Cluster Manager]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Implementing Hyper-V Replica and Windows Server Backup

Scenario

You're working as an administrator at Contoso, Ltd. Contoso wants to assess and configure new disaster recovery and backup features and technologies. As the system administrator, you have been tasked with performing that assessment and implementation. You decided to evaluate **Hyper-V Replica** and Windows Server Backup.

Objective

- Configure and implement **Hyper-V Replica**.

.....

Theoretical Background

Overview of Hyper-V Replica

Hyper-V failover clusters are used to make virtual machines (VMs) highly available, but they're often limited to a single location. Multisite clusters usually depend on specialized hardware and are expensive to implement, even with Windows Server Storage Replica. In case of a natural disaster such as an earthquake or a flood, all server infrastructure at the affected location can be lost.
Hyper-V Replica can protect against data loss from natural disasters, and it can be used to implement an affordable business continuity and disaster recovery (BCDR) solution for a virtual environment. Use **Hyper-V Replica** to replicate VMs to a Hyper-V host in a secondary location across a wide area network (WAN) link and even to a third location. If you have a single location, you can still use **Hyper-V Replica** to replicate VMs to a partner organization in another location, to a hosting provider, or to Microsoft Azure.

Hyper-V hosts that participate in replication don't have to be in the same Active Directory Forest or have the same configuration. You can also encrypt network traffic between them.

Hyper-V Replica can have two instances of a single VM residing on different Hyper-V hosts. One of the instances will be the primary, running VM, and the other instance will be a replica—an offline copy. If necessary, you can even extend replication of the offline copy to a third location. Hyper-V syncs these instances, and you can perform manual failover at any time. If a failure occurs at a primary site, you can use **Hyper-V Replica** to perform a failover of the VMs to Replica servers at a secondary location with minimal downtime.

Prerequisites for Hyper-V Replica implementation

Before implementing **Hyper-V Replica**, ensure that the virtualization infrastructure has the following prerequisites:

● Windows Server 2012 or a newer version of Windows Server with the Hyper-V role installed at both locations. Server hardware should have enough capacity to run all VMs: the local VMs and the replicated VMs. Replicated VMs are in a turned-off state and start only if you perform a failover.
● Sufficient storage on both the primary and replica Hyper-V hosts to store both local and replicated VM data.
● Network connectivity between the locations that are hosting the primary and the replica Hyper-V hosts. Connectivity can be through a WAN or a local area network link.
● Firewall rules to allow replication between the primary and replica sites. When you install the Hyper-V role, Hyper-V Replica HTTP Listener (TCP-In) and Hyper-V Replica HTTPS Listener (TCP-In) rules are added to Windows Defender Firewall. Before you can use **Hyper-V Replica**, you must enable one or both rules on the replica Hyper-V host.

● An X.509v3 certificate from a trusted certification authority to support mutual authentication at both Hyper-V hosts if you plan to use certificate-based authentication. When you use certificate-based authentication, Hyper-V hosts can be in different Active Directory forests.
● Both Hyper-V hosts joined to the same Active Directory Forest if you intend to use Kerberos authentication.

Hyper-V Replica high-level architecture

When you configure a VM for replication, it performs an initial replication and creates a copy of the VM on the second Hyper-V host at the recovery site. The replicated VM stays turned off until you initiate a failover, while the primary VM keeps running. Changes in the primary VM are written in a log file that's periodically replicated and applied to the replica. **Hyper-V Replica** has several components:

● Replication engine. This component manages the initial replication, replication configuration details, replication of delta changes, and failover and test failover operations. It also tracks VM, and storage mobility events and takes appropriate actions when necessary. For example, it pauses replication and **Hyper-V Replica** configurations when the source or the replica Hyper-V hosts are part of a Hyper-V failover cluster.

● Change tracking module. This component tracks changes that occur to the VM on a source Hyper-V host. The change tracking module tracks write operations to the virtual hard disks (VHDs) regardless of where the VHDs are stored locally—on a storage area network, on a Server Message Block version 3 or newer share, or on a Cluster Shared Volume.

● Network module. This component provides a secure and efficient way to transfer VM data between Hyper-V hosts. By default, the network module minimizes traffic by compressing data. It can also encrypt data when HTTPS and certification-based authentication are used.

● **Hyper-V Replica Broker**. This component is used only when a Hyper-V host is a node in a failover cluster. **Hyper-V Replica Broker** enables you to use **Hyper-V Replica** with highly available VMs that can move between cluster nodes. The **Hyper-V Replica Broker** role queries the cluster database. It then redirects all requests to the cluster node where the VM is currently running.

● Management tools. With tools such as Hyper-V Manager and Windows PowerShell, you can configure and manage **Hyper-V Replica**. Use **Failover Cluster Manager** for all VM management and **Hyper-V Replica** configurations when the source or the replica Hyper-V hosts are part of a Hyper-V failover cluster.

Hyper-V Replica security considerations

You can set up **Hyper-V Replica** with a Hyper-V host regardless of its location and domain membership if you have network connectivity with it. Hyper-V hosts don't have to be part of the same Active Directory domain. You can implement **Hyper-V Replica** when Hyper-V hosts are members of untrusted domains by configuring certificate-based authentication. **Hyper-V Replica** implements security at the following levels:

● On each server, Hyper-V creates a local security group named **Hyper-V Administrators**. Members of this group, in addition to local administrators, can configure and manage **Hyper-V Replica**.

● You can configure a Replica server to allow replication from any authenticated server or to limit replication to specific servers. In the first case, you must specify a fully qualified domain name for the primary server (for example, lon-svr1.adatum.com), or use a wildcard character with a domain suffix (for example, *.adatum.com). Using IP addresses isn't allowed. If the Replica server is in a failover cluster, replication is allowed at the cluster level. When you limit replication to specific servers, you also must specify a trust group, which is used to identify the servers within which a VM can move. For example, if you provide disaster recovery services to partner organizations, the trust group prevents one organization from gaining access to another organization's replica machines.

● The replica Hyper-V host can authenticate a primary Hyper-V host by using Kerberos authentication or certificate-based authentication. Kerberos authentication requires both Hyper-V hosts to be in the same Active Directory Forest, while you can use certificate-based authentication in any environment. Kerberos authentication is used with HTTP traffic, which isn't encrypted, while certificate-based authentication is used with HTTPS traffic, which is encrypted.

● You can establish **Hyper-V Replica** only if network connectivity exists between the Hyper-V hosts. Configure Windows Defender Firewall to allow HTTP or HTTPS **Hyper-V Replica** traffic as needed.

Plan for Hyper-V Replica

When planning for **Hyper-V Replica** deployment, you must define several parameters used in replica configuration. Careful planning is important before setting up replication between Hyper-V hosts.

Hyper-V Replica configurations

You can set up **Hyper-V Replica** between Hyper-V hosts irrespective of whether they're nodes in a failover cluster. You can also set up **Hyper-V Replica** irrespective of whether the Hyper-V hosts are members of the same Active Directory Forest or are in different Active Directory forests without any trust between them. You can use **Hyper-V Replica** in four different configurations:

● Both Hyper-V hosts are standalone servers. This configuration isn't recommended, because it includes only disaster recovery and not high availability.

● The Hyper-V host at the primary location is a node in a failover cluster, and the Hyper-V host at the secondary location is on a standalone server. Many environments use this type of implementation. A failover cluster provides high availability for running virtual machines (VMs) at the primary location. If a disaster occurs at the primary location, a replica of the VMs is still available at the secondary location.

● Each Hyper-V host is a node in a different failover cluster. This enables you to perform a manual failover and continue operations from a secondary location if a disaster occurs at the primary location.

● The Hyper-V host at the primary location is a standalone server, and the Hyper-V host at the secondary location is a node in a failover cluster. Although technically possible, this configuration is rare. You typically want VMs at the primary location to be highly available, while their replicas at the secondary location are turned off and aren't used until a disaster occurs at the primary location.

Note: You can configure **Hyper-V Replica** regardless of whether the Hyper-V host is a node in a failover cluster.

Replication settings

Because you must configure replication for each VM individually, you also must plan resources for each VM on replication hosts. Besides resources, you also must plan on how to configure the following replication settings:

● **Replica Server**. Specify the computer name or the fully qualified domain name (FQDN) of the Replica server—an IP address isn't allowed. If the Hyper-V host that you specify isn't yet configured to allow replication traffic, you can configure it here. If the Replica server is a node in a failover cluster, you should enter the name or FQDN of the connection point for the **Hyper-V Replica Broker**.

● **Connection Parameters**. If the Replica server is accessible, the **Enable Replication Wizard** populates the authentication type and replication port fields automatically with appropriate values. If the Replica server is inaccessible, you can configure these fields manually. However, you should be aware that you won't be able to enable replication if you can't create a connection to the Replica server. On the **Connection Parameters** page, you can also configure Hyper-V to compress replication data before transmitting it over a network.

● **Replication virtual hard disks**. By default, all virtual hard disks (VHDs) are replicated. If some of the VHDs aren't required at the replica Hyper-V host, exclude them from replication; for example, a VHD that's dedicated to storing page files. Excluding VHDs that include operating systems or applications can result in that particular VM being unusable at the Replica server.

● **Replication Frequency**. You can set replication frequency to 30 seconds, 5 minutes, or 15 minutes based on the network link to the Replica server and the acceptable state delay between primary and replica VMs. Replication frequency controls how often data replicates to the Hyper-V host at the recovery site. If a disaster occurs at the primary site, a shorter replication frequency means less loss as fewer changes aren't replicated to the recovery site.

● **Additional recovery points**. You can configure the number and types of recovery points to send to a Replica server. By default, the option to maintain only the latest point for recovery is selected, which means that only the parent VHD replicates. All changes merge into that VHD. However, you can choose to create more hourly recovery points and then set the number of additional recovery points (up to 24). You can configure the Volume Shadow Copy Service snapshot frequency to save application consistent replicas for the VM and not just the changes in the primary VM.

● **Initial replication method and schedule**. VMs have large virtual disks, and initial replication can take a long time and cause a lot of network traffic. While the default option is to immediately send the initial copy over the network, if you don't want immediate replication, you can schedule it to start at a specific time. If you want an initial replication but want to avoid network traffic, you can opt to send the initial copy to external media or use an existing VM on the Replica server. Use the last option if you restored a copy of the VM at the Replica server and you want to use it as the initial copy.

● **Extended replication**. With Windows Server 2012 R2 and later Windows Server operating systems, you can replicate a single VM to a third server. Thus, you can replicate a running VM to two independent servers. However, the replication doesn't happen from one server to the two other servers. The server that's running an active copy of the VM replicates to the Replica server, and the Replica server then replicates to the extended Replica server. You create a second replica by running the **Extend Replication Wizard** on a passive copy. In this wizard, you can set the same options that you chose when you configured the first replica.

Note: Hyper-V Replica now allows administrators to use a Microsoft Azure instance as a replica repository. This enables administrators to take advantage of Azure rather than having to build out a disaster recovery site or manage backup tapes offsite. To use Azure for this purpose, you must have a valid subscription. Note that this service might not be available in all world regions.

Configure and implement Hyper-V Replica

Hyper-V Replica implements as part of the Hyper-V role. You can use it on standalone Hyper-V servers or on servers that are part of a failover cluster, in which case you should configure **Hyper-V Replica Broker**. Unlike failover clustering, the Hyper-V role doesn't depend on Active Directory. You can use the Hyper-V role with standalone Hyper-V servers or servers that are members of different Active Directory domains, except when servers that participate in **Hyper-V Replica** are part of the same failover cluster. To enable **Hyper-V Replica** technology, complete following steps:

● In the **Replication Configuration** group of options, enable the Hyper-V server as a Replica server.

● Configure Hyper-V server settings. Select the authentication and port options, and then configure the authorization options. You can choose to enable replication from any server that successfully authenticates. This is convenient in scenarios where all servers are part of the same domain, or you can enter the fully qualified domain names (FQDNs) of servers that you accept as Replica servers. Additionally, you must configure the location for replica files. You should configure these settings on each server that serves as a Replica server.

● Specify both the Replica server name and the connection options.

● Select the virtual hard disks (VHDs) to replicate in cases where a virtual machine (VM) has more than

one VHD. You can also configure the recovery history and the initial replication method. Configure the replication interval for 30 seconds, 5 minutes (the default value), or 15 minutes.

● After configuring these options, you can start replication. After you make the first replica, you can also make an extended replica to a third physical or cloud-based instance that's running Hyper-V. The extended replica site is built from the first replica site, not from the primary VM. It's possible to configure different replication intervals for the replica and extended replica instances of a VM.

After you establish the replication relationship, the **Status** column in Hyper-V Manager displays the replication progress as a percentage of the total replication for the configured VM. The VM replica is in a turned-off state and will start only when you perform a failover.

After the initial replication is done, the replica updates regularly with changes from the primary VM. One of the configuration steps is configuring the replication frequency setting. This setting controls the longest time interval until changes from the primary VM are applied to the replica. In a real-world environment, however, there can be many reasons why changes from a primary VM aren't applied to the replica for extended periods; for example, because network connectivity is lost or because you pause the replication. This will be reflected in replication health, but when replication is established again, all changes will be applied to the replica.

When you enable replication, VM network adapters receive more settings that were previously unavailable. These new settings pages are **Failover TCP/IP** and **Test Failover**. Failover TCP/IP is available only for network adapters and not for legacy network adapters. The settings on this page are useful when a VM has a static IP address assigned and the replica site is using IP settings different from the primary site. You can configure the TCP/IP settings that a network adapter will use after a failover is performed. If you use static IP addresses to configure VMs, you should configure failover TCP/IP settings on the primary and replica VMs. VMs must also have integration services installed to be able to apply failover TCP/IP settings.

Replication health monitoring

When you enable replication for a VM, changes in the primary VM write to a log file, which periodically transfers to the replica Hyper-V host and is then applied to a VHD of a replica VM. Replication health monitors the replication process and displays important events in addition to the replication and sync state of the Hyper-V host.

Replication health includes the following data:
● **Replication State**. This indicates whether replication is enabled for a VM.
● **Replication Type**. This indicates whether you're monitoring replication health on a primary VM or replica VM.
● **Primary and Replica server names**. This indicates which Hyper-V host the primary VM is running on and which Hyper-V host is the replica.
● **Replication Health**. This indicates replication status. Replication health can have one of three values: Normal, Warning, or Critical.
● **Replication statistics**. This displays replication statistics since the time that the VM replication started or since you reset the statistics. Statistics include data such as maximum and average sizes of a replication, average replication latency, number of errors encountered, and the number of successful replication cycles.
● **Pending replication**. This displays information about the size of data that still needs to replicate and when the replica was last synced with the primary VM.

Failover options

Three types of failovers are possible with **Hyper-V Replica**: test failover, planned failover, and failover:

● **Test failover**. A test failover is a nondisruptive task that enables you to test a VM on a Replica server while the primary VM is running without interrupting the replication. You can perform it after you configure **Hyper-V Replica** and after the VMs start replicating. Initiating a test failover on a replicated VM creates a new checkpoint, and you can use this checkpoint to select a recovery point from which to create a new test VM. The test VM has the same name as

the replica, but with "- Test" appended to the end. The test VM stays disconnected by default to avoid potential conflicts with the running primary VM. After you finish testing, to stop the test VM and delete it from the replica Hyper-V host, stop the test failover. This option is available only if a test failover is running. If you run a test failover on a failover cluster, you'll have to manually remove the Test-Failover role from the failover cluster.

● **Planned failover**. You can start a planned failover to move the primary VM to a replica site, for example, before site maintenance or before an expected disaster. Because this is a planned event, no
data loss will occur, but the VM will be unavailable for some time during its startup. A planned failover confirms that the primary VM is turned off before the failover runs. During the failover, the primary VM sends all the data that it hasn't yet replicated to the Replica server. The planned failover process then fails over the VM to the Replica server and starts the VM on the Replica server. After the planned failover, the VM will run on the Replica server, and it doesn't replicate its changes. If you want to set up replication again, you should reverse the replication. You'll have to configure settings similar to when you enabled replication, and it will use the existing VM as an initial copy.

● **Failover**. If a disruption occurs at the primary site, you can perform a failover. You start a failover at the replicated VM only if the primary VM is either unavailable or is turned off. A failover is an unplanned event that can result in data loss because changes at the primary VM might not have replicated before the disaster happened. The replication frequency setting controls how often changes replicate. During a failover, the VM runs on a Replica server. If you start the failover from a different recovery point and discard all the changes, you can cancel the failover. After you recover the primary site, you can reverse the replication direction to reestablish replication. This also removes the option to cancel failover.

Configuration options for replication

Besides performing various types of failovers, you can configure several other options for replication. Other Hyper-V replication–related actions include:

● **Pause Replication**. This action pauses replication for the selected VM.

● **Resume Replication**. This action resumes replication for the selected VM. It's available only if replication for the VM is paused.

● **View Replication Health**. This action provides data about the replication events for a VM.
● **Extend Replication**. This action is available on the replica VMs, and it extends VM replication from a Replica server to a third server (the extended Replica server).

● **Remove Recovery Points**. This action is available only during a failover. If you select it, all recovery points (checkpoints) for a replica VM are deleted, and their differing VHDs are merged.

● **Remove Replication**. This action stops replication for the VM.

Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Exercise #8: Implement Hyper-V Replica

In this exercise, you'll learn how to implement the **Hyper-V Replica** feature on a Windows Server computer that's running Server Core.

Exercise steps

1. On **SEA-ADM1 (your VM server)**, open Windows PowerShell as an administrator.

2. In PowerShell, create a new remote PowerShell session to sea-svr1.contoso.com. Use **Contoso\Administrator** credentials to connect to the remote PowerShell on **SEA-SVR1**.

3. In the remote PowerShell session on sea-svr1.contoso.com, use the **Enable-Netfirewallrule** cmdlet to enable the firewall rule named Hyper-V Replica HTTP Listener (TCP-In).

4. Use the **Get-Netfirewallrule** cmdlet to verify that the Hyper-V Replica HTTP Listener (TCP-In) rule is enabled.

5. Use the following command to configure **SEA-SVR1** for **Hyper-V Replica**: powershellSet-VMReplicationServer -ReplicationEnabled $true -AllowedAuthenticationType Kerberos -ReplicationAllowedFromAnyServer $true -DefaultStorageLocation c:\ReplicaStorage

6. Use the **Get-VM** cmdlet to verify that the **SEA-CORE1** virtual machine (VM) is present on **SEA-SVR1**.

7. Open a new remote PowerShell session for sea-svr2.contoso.com in a new PowerShell window. Repeat steps 2 through 5 to configure **SEA-SVR2** for **Hyper-V Replica**.

8. Switch to the PowerShell window where you have the remote PowerShell session opened for sea-svr1.contoso.com, enter the following command, and then select Enter: powershellEnable-VMReplication SEA-CORE1 -ReplicaServerName SEA-SVR2.contoso.com -Replica- ServerPort 80 -AuthenticationType Kerberos -computername SEA-SVR1.contoso.com

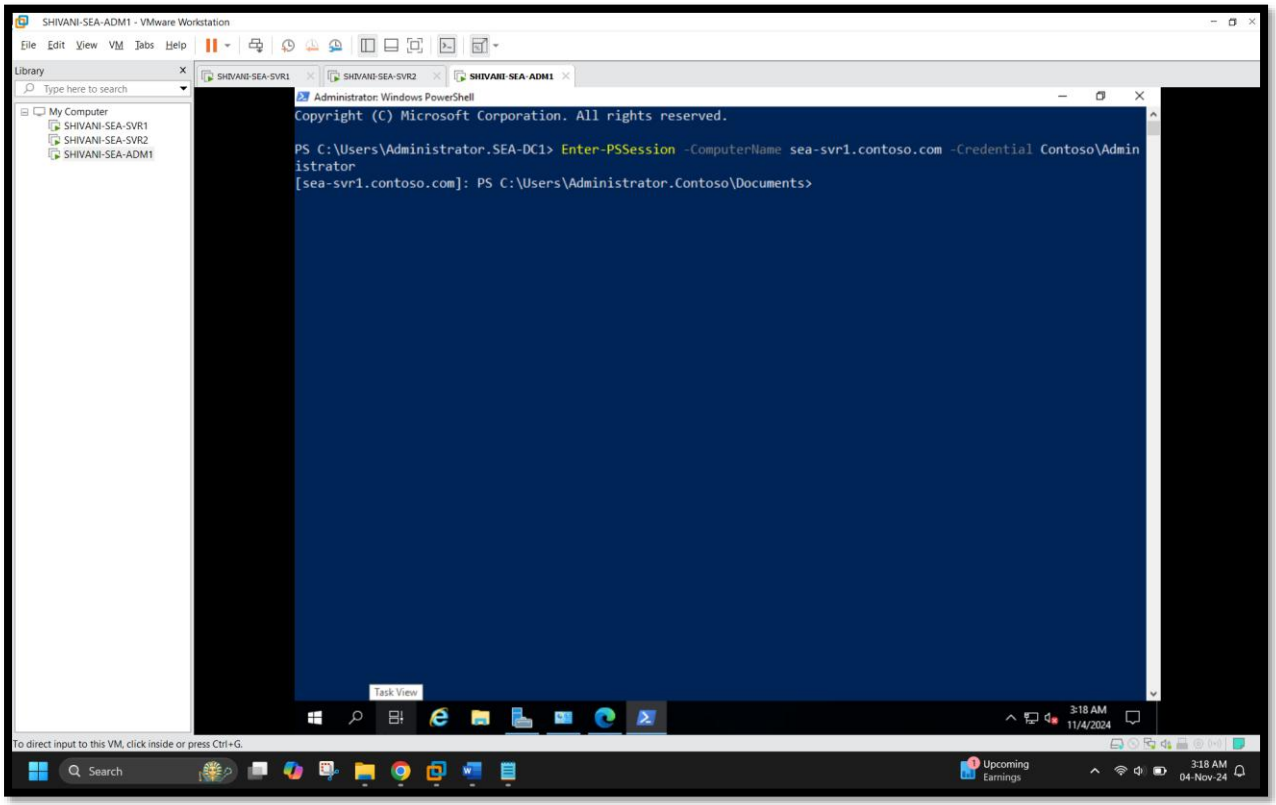
9. Start replication with the following command: powershellStart-VMInitialReplication SEA-CORE1

~~~~~~

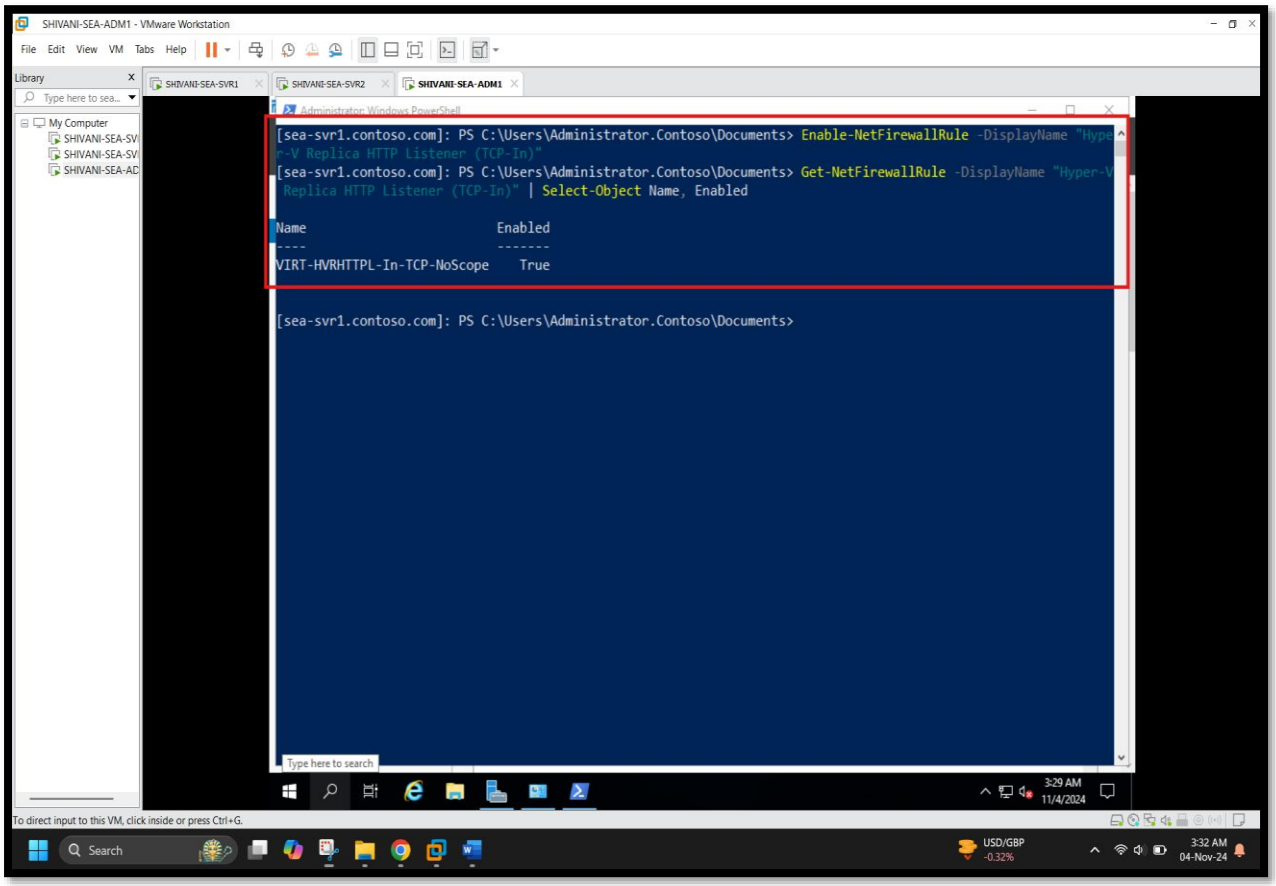
Paste your screenshots here
~~~~~~

Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 1: Remote PowerShell session to SEA-SVR1]

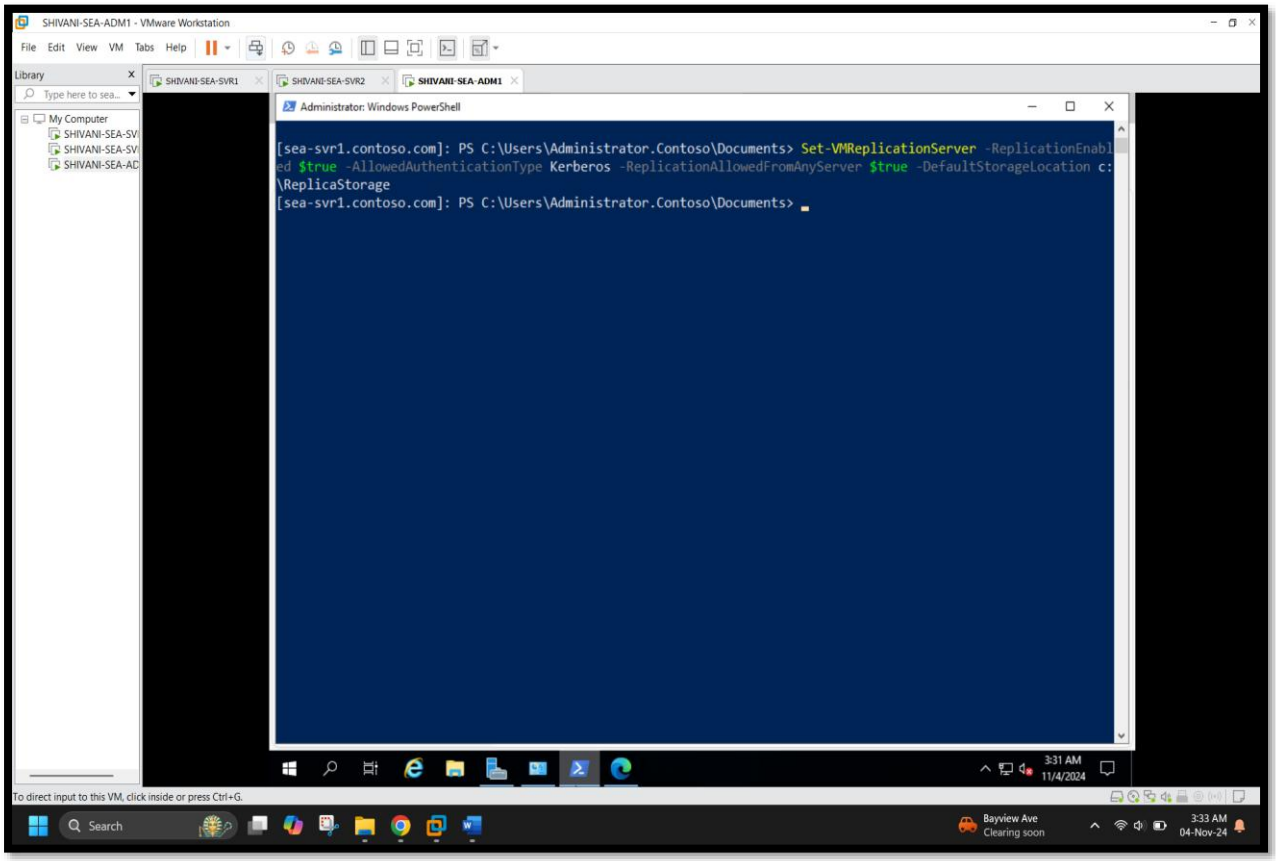


[Screenshot 2: Firewall rule enabled on SEA-SVR1]

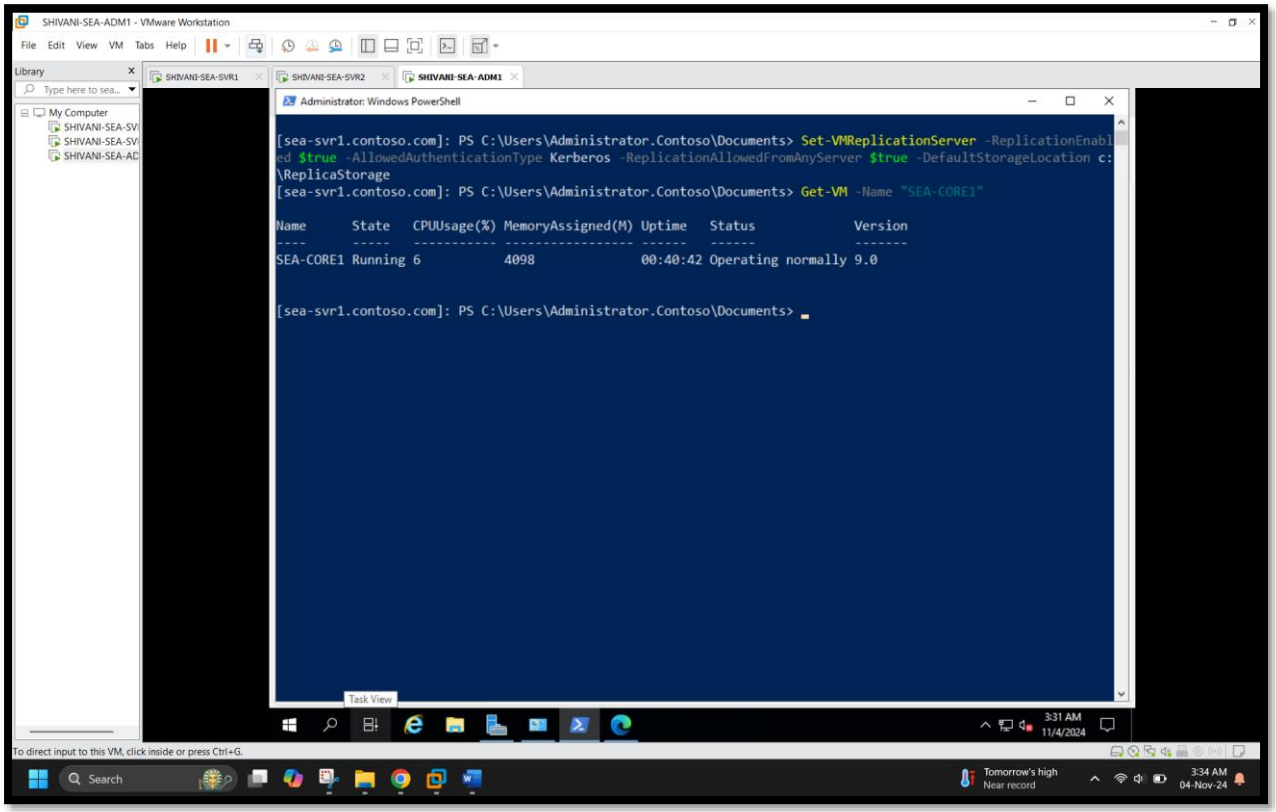


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 3: Configure SEA-SVR1 as a Hyper-V Replica server]

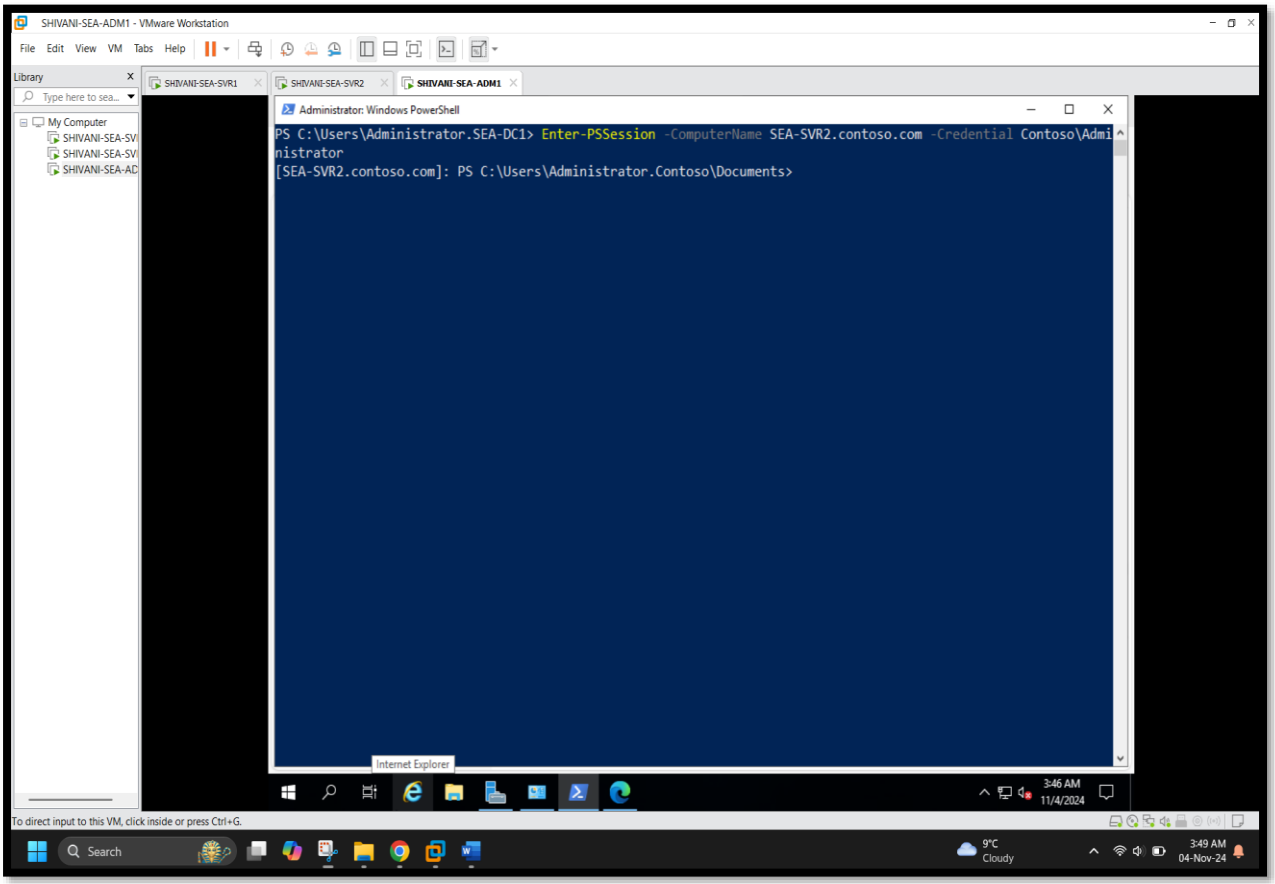


[Screenshot 4 :SEA-CORE1 presence verified on SEA-SVR1]

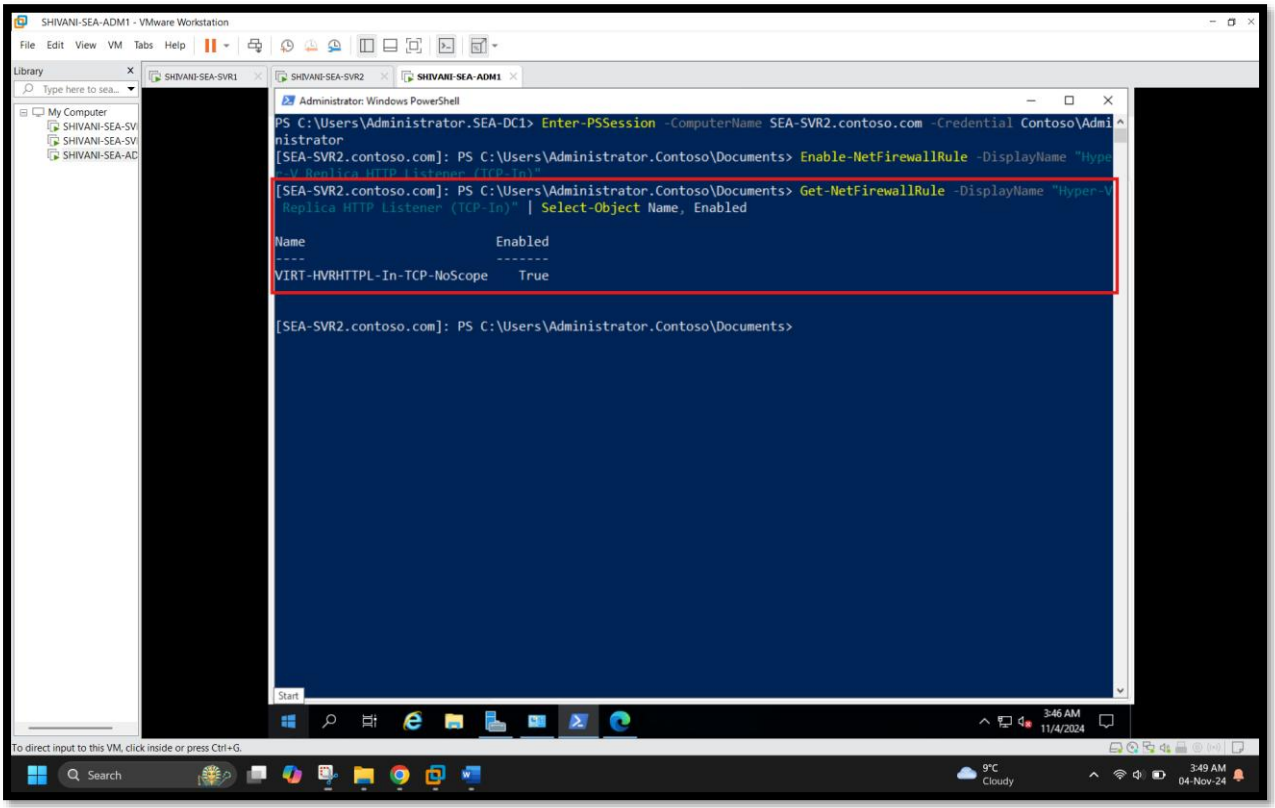


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 5 : Remote PowerShell session to SEA-SVR2.]

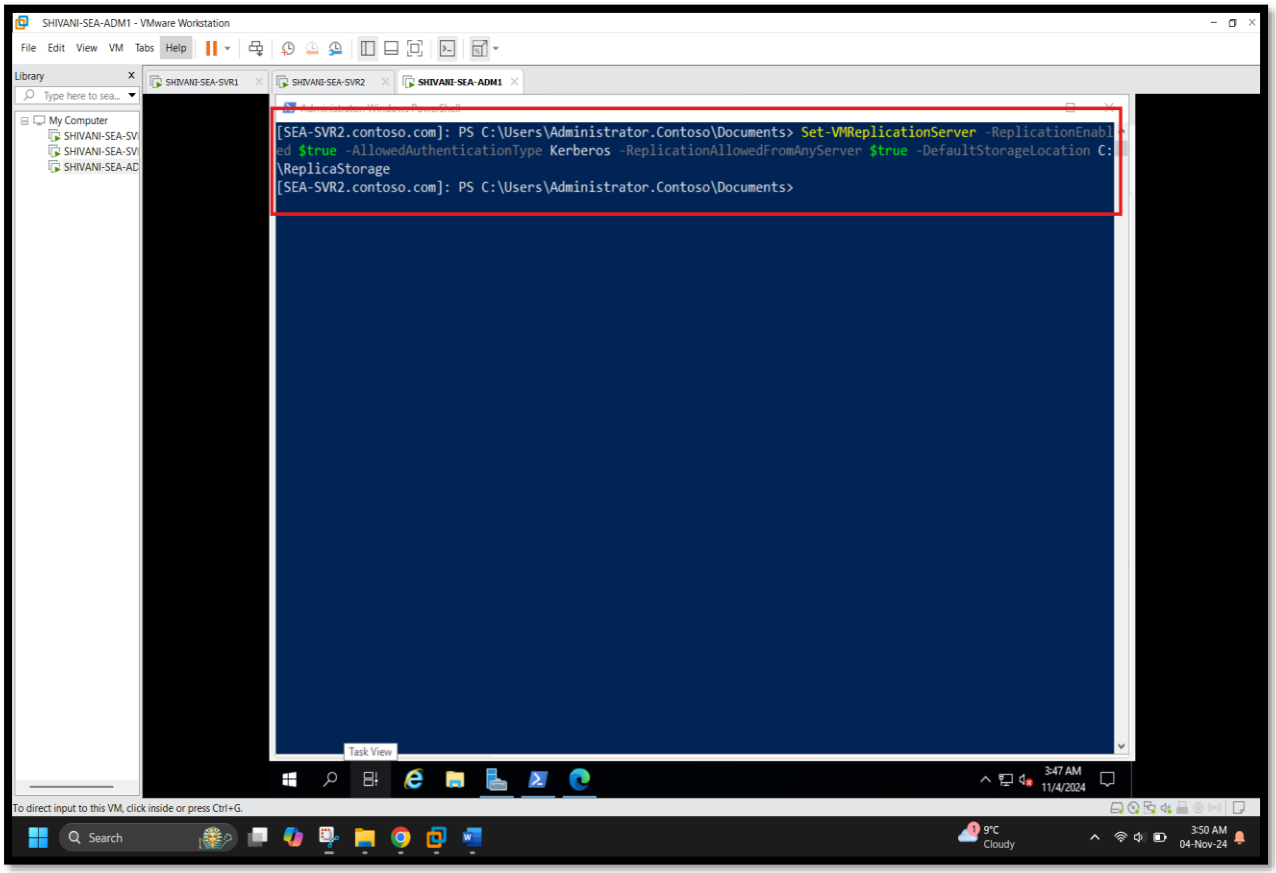


[Screenshot 6 : Firewall rule enabled on SEA-SVR2]

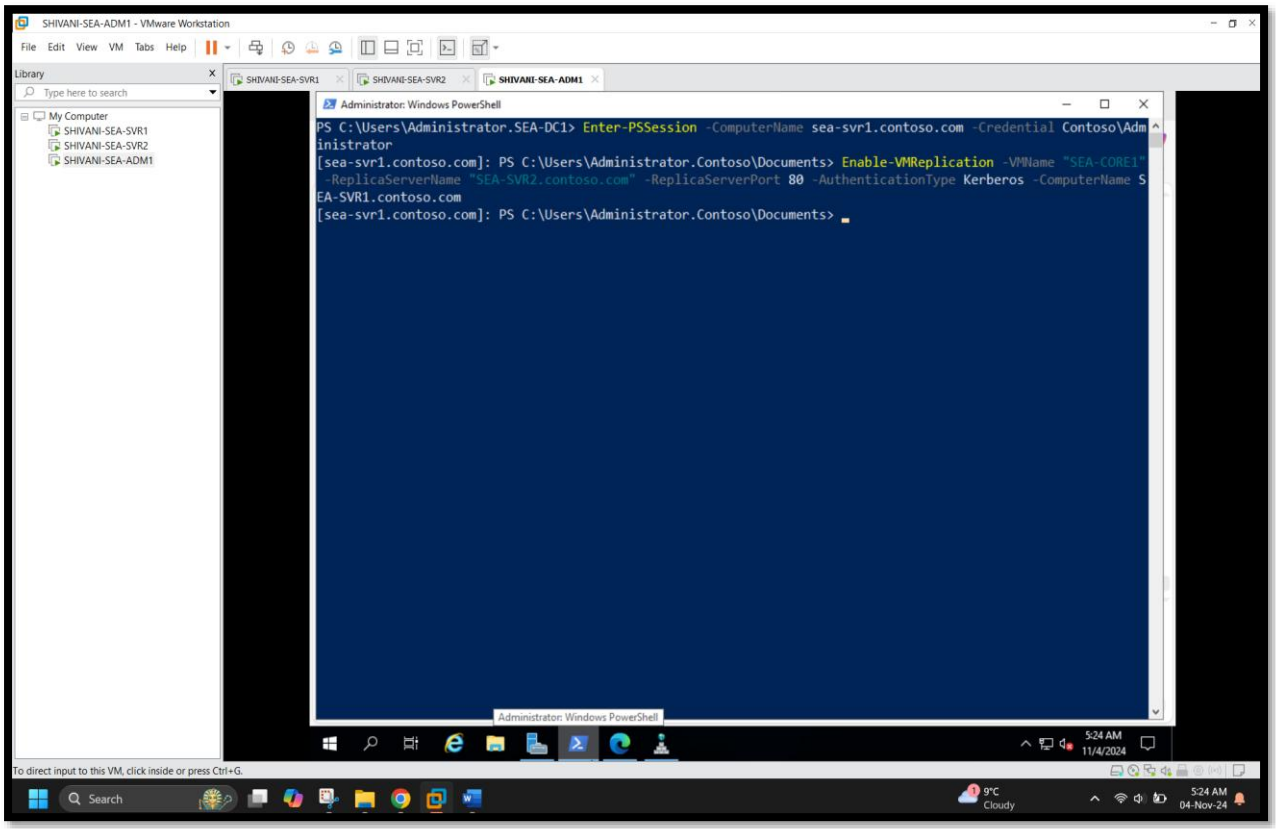


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

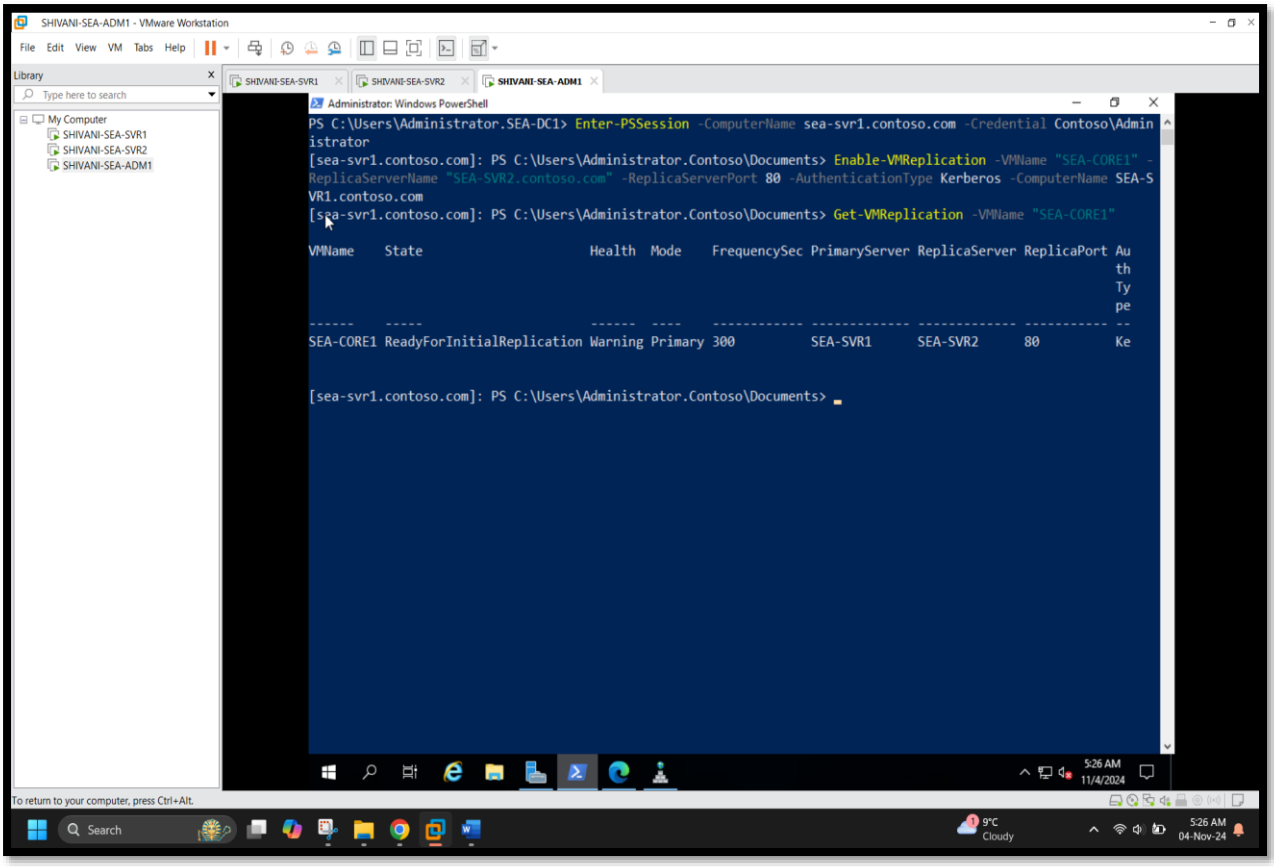
[Screenshot 7: Configure SEA-SVR2 as a Hyper-V Replica server]



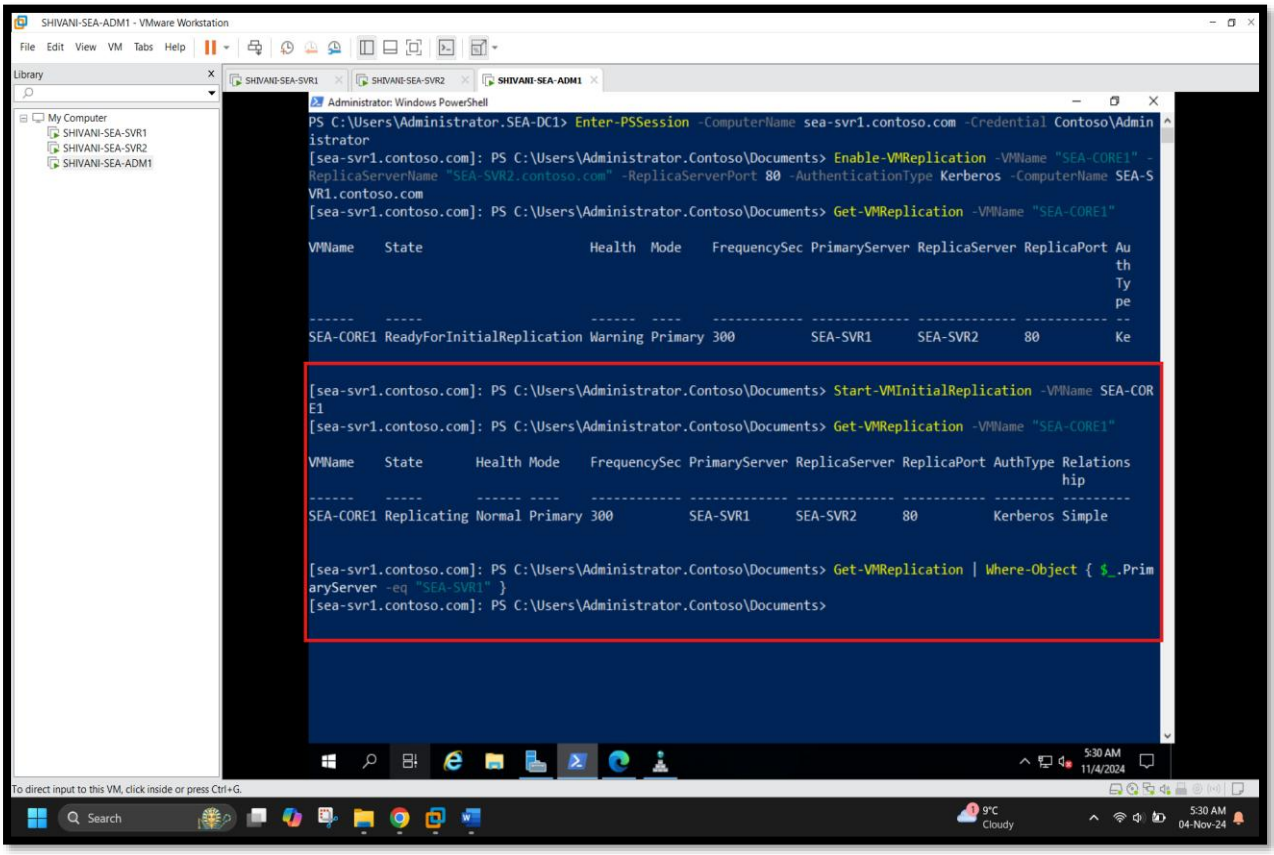
[Screenshot 8 : Enable replication from SEA-SVR1 to SEA-SVR2 for SEA-CORE1]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

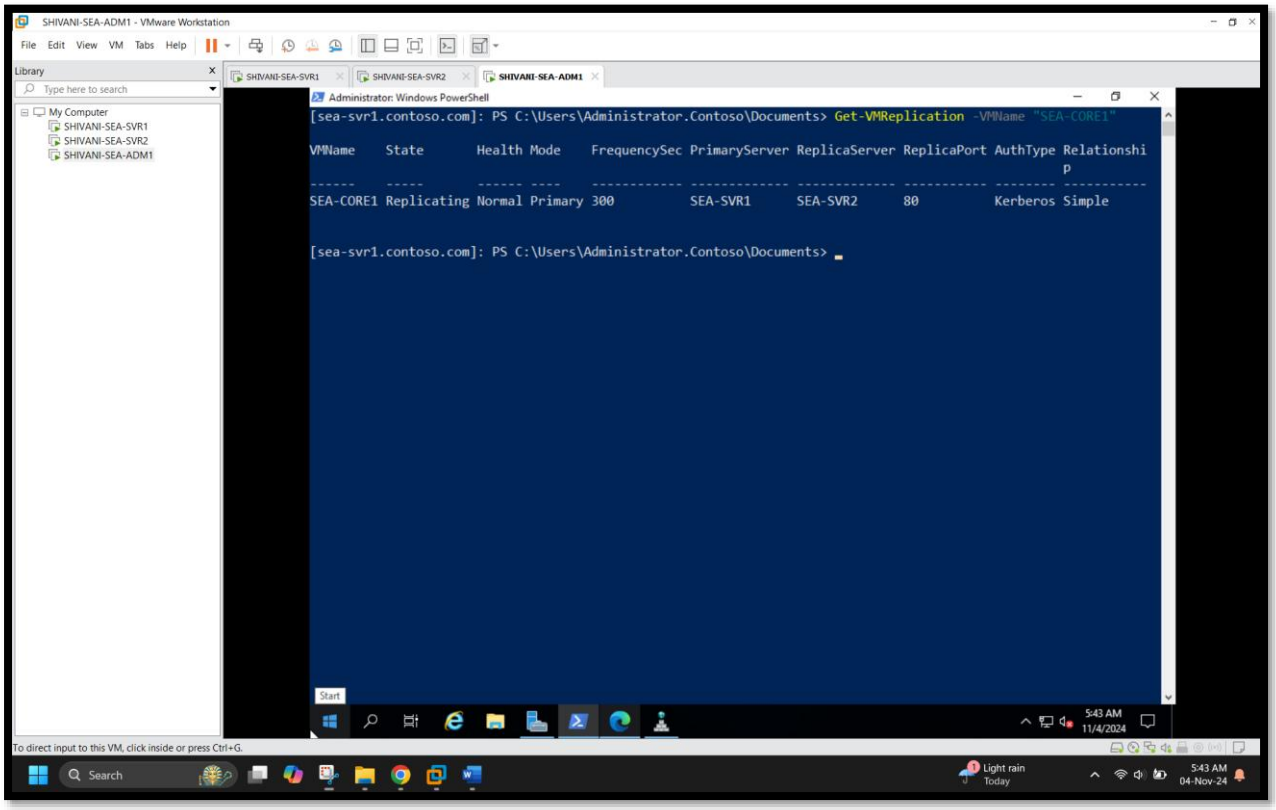


[Screenshot 9: Start initial replication for SEA-CORE1]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

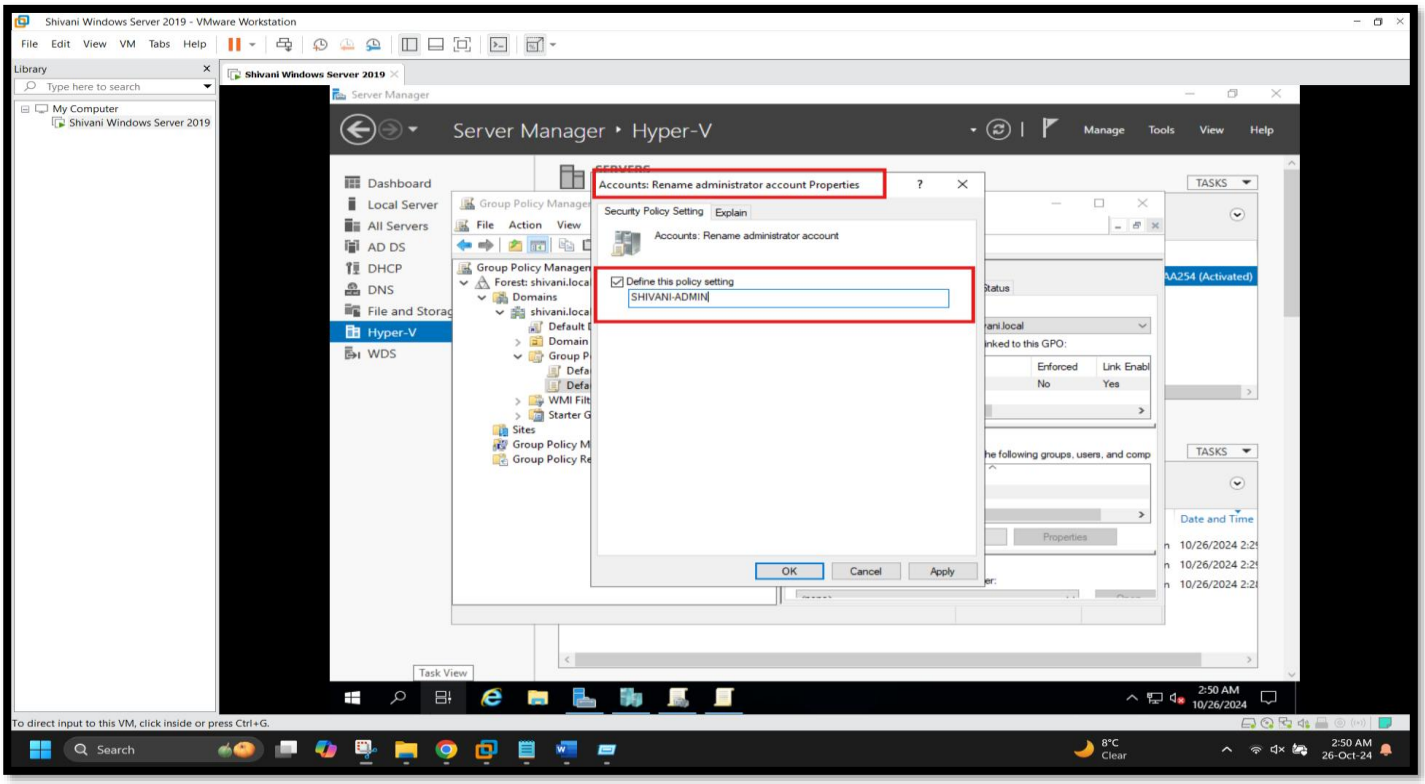
[Screenshot 10 : Replication progress and replication health verification]



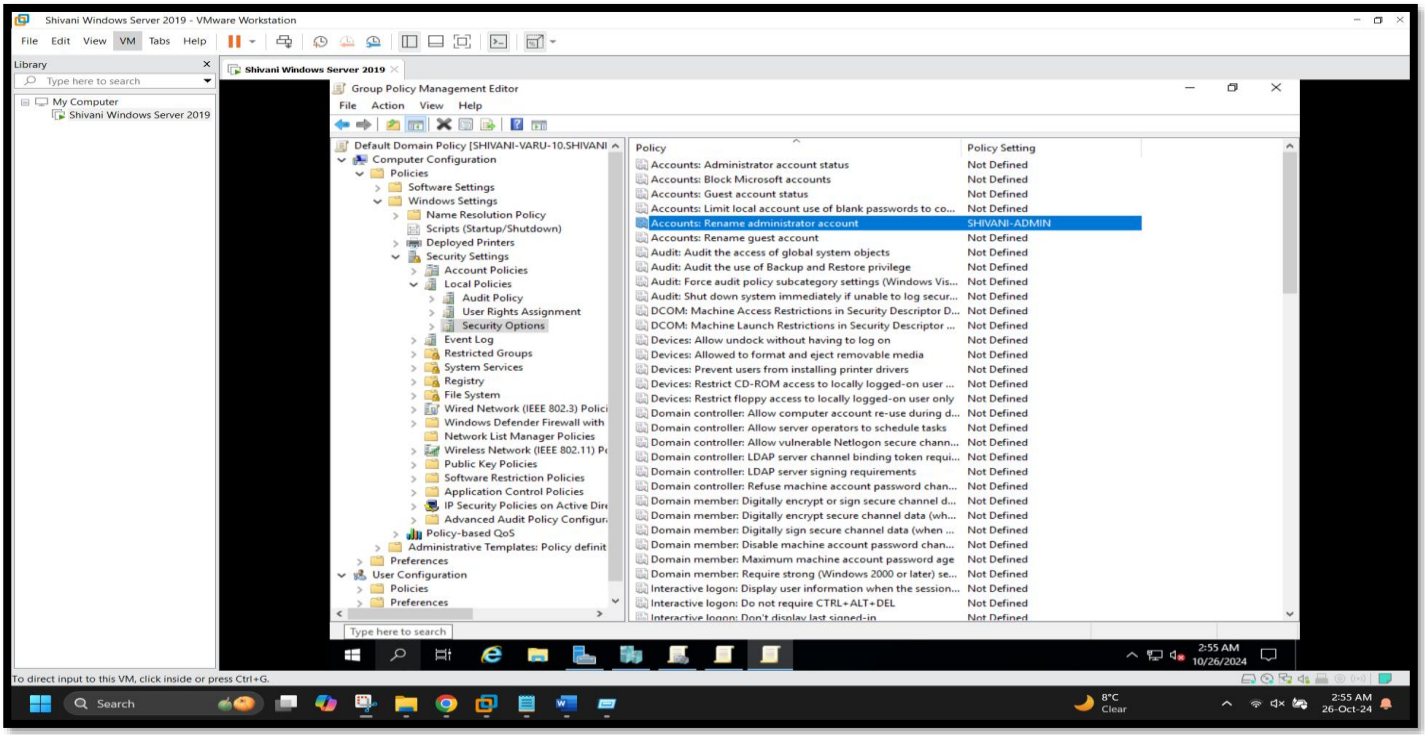
Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Exercise – 9 Examples of GPOs for System Admin

[Screenshot 1: Renaming the Administrator Account]

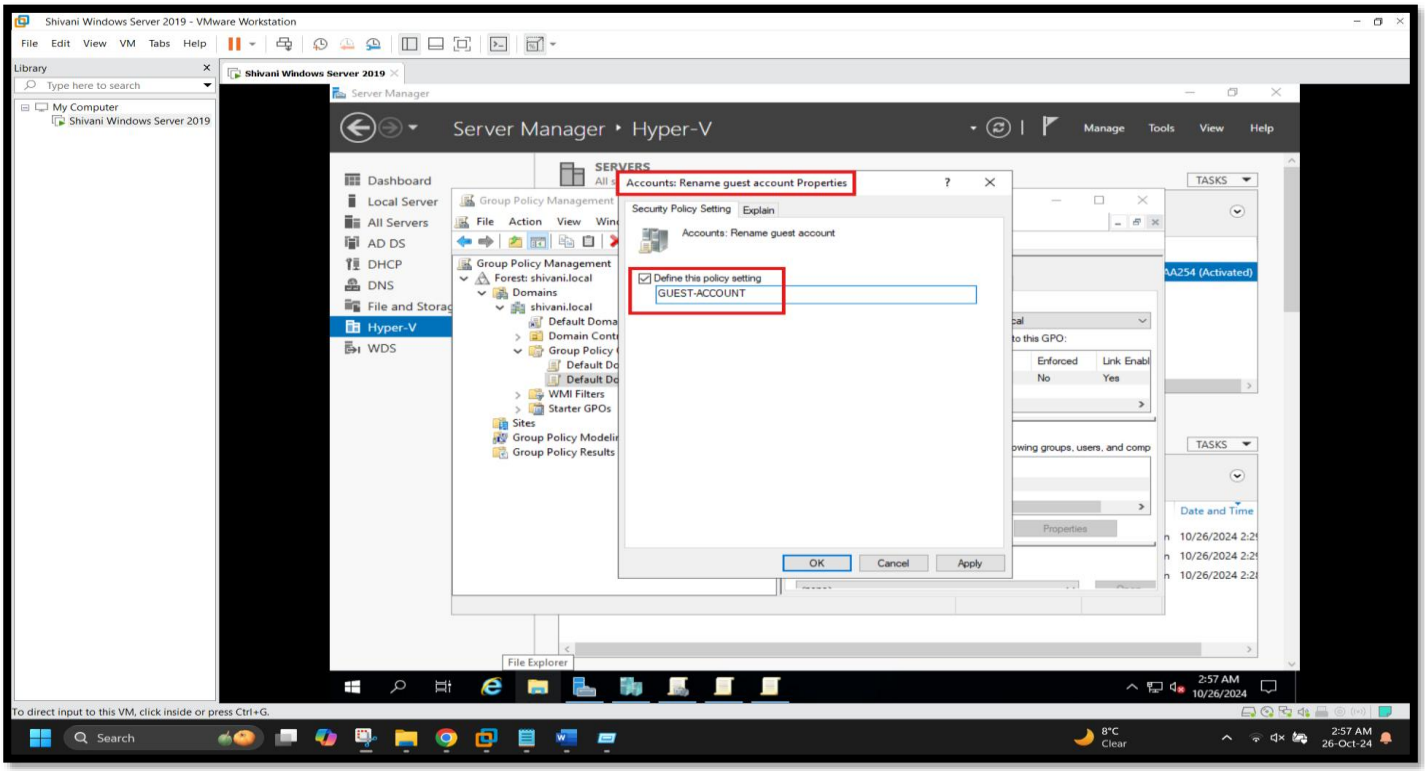


[Screenshot 2 : Administrator Account's name has been changed]

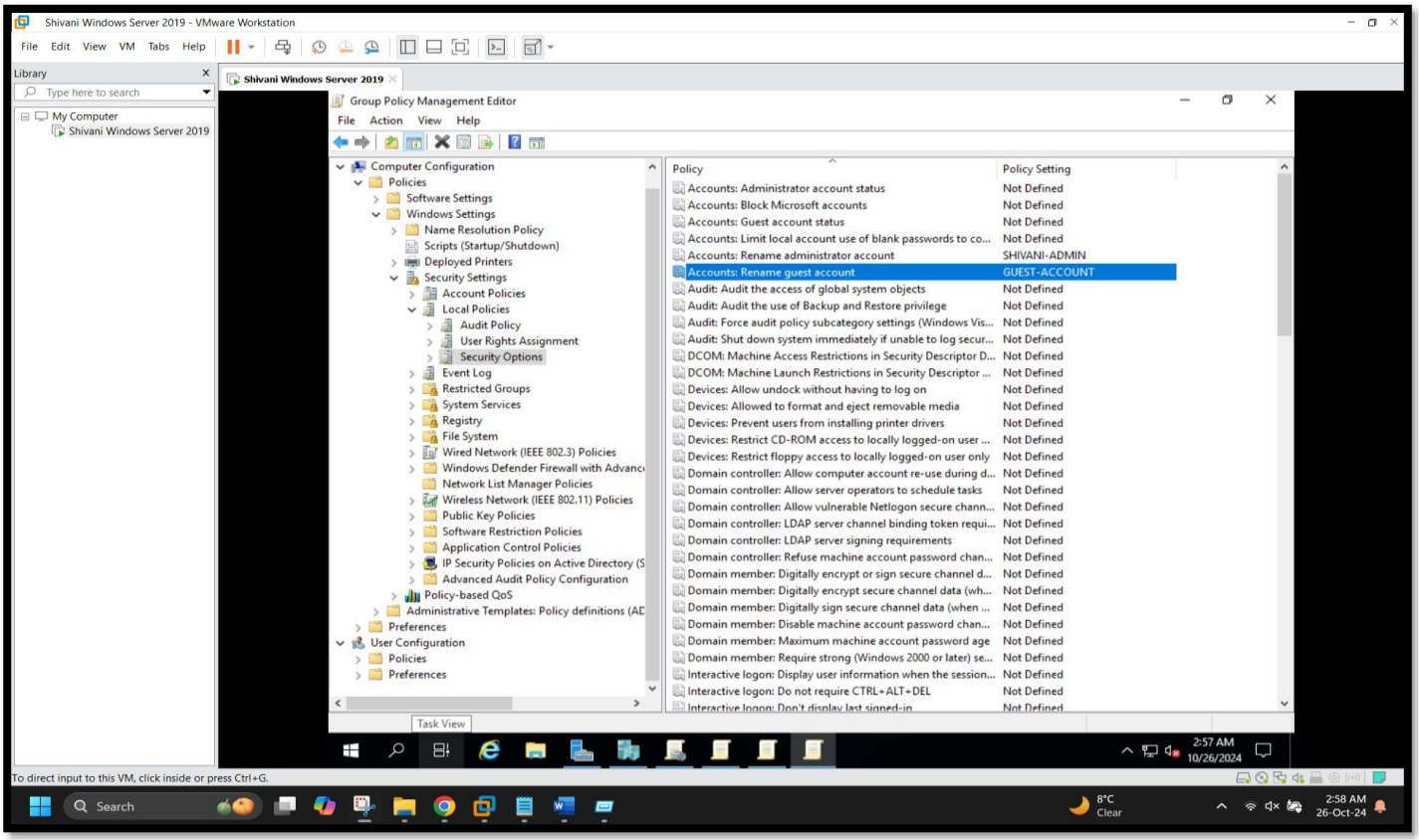


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 3: Renaming the Guest Account]

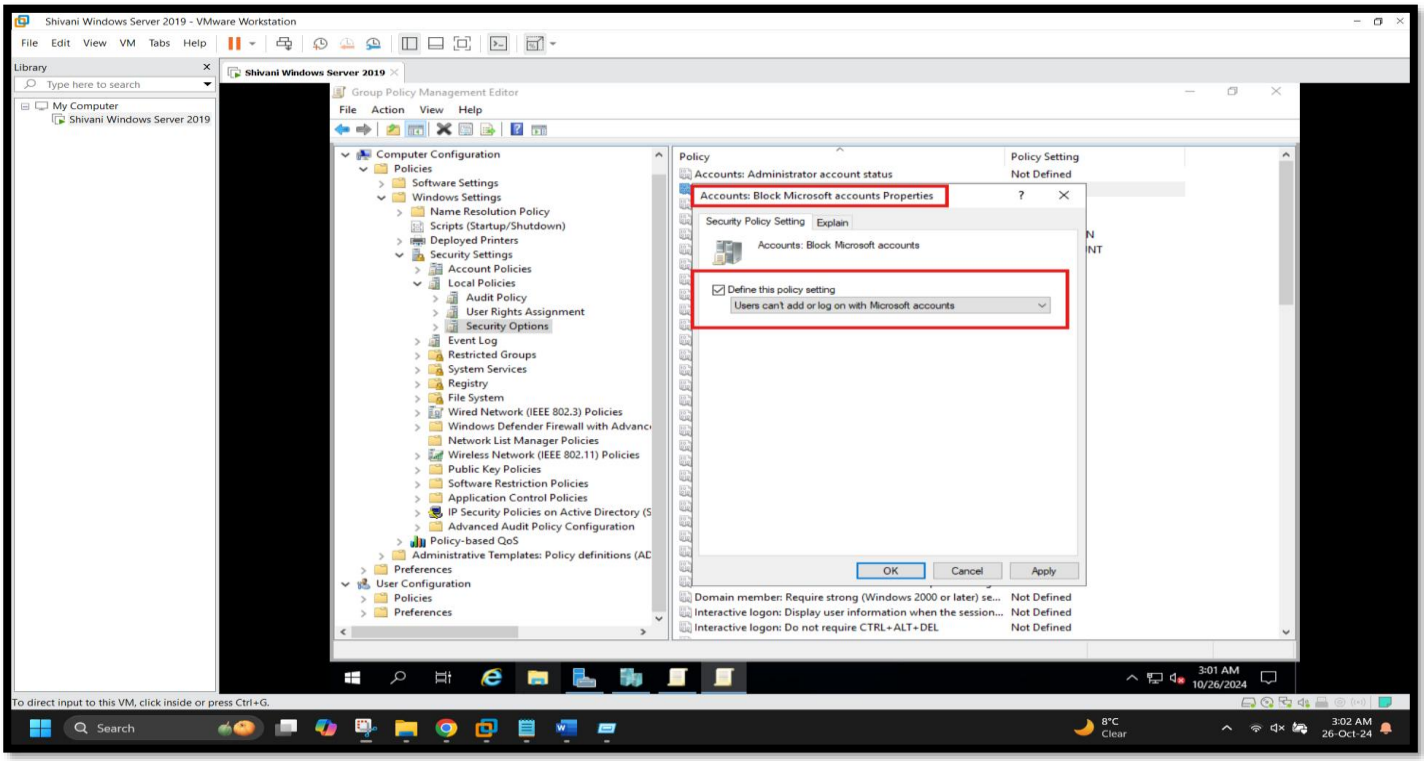


[Screenshot 4 : Guest Account's name has been changed]

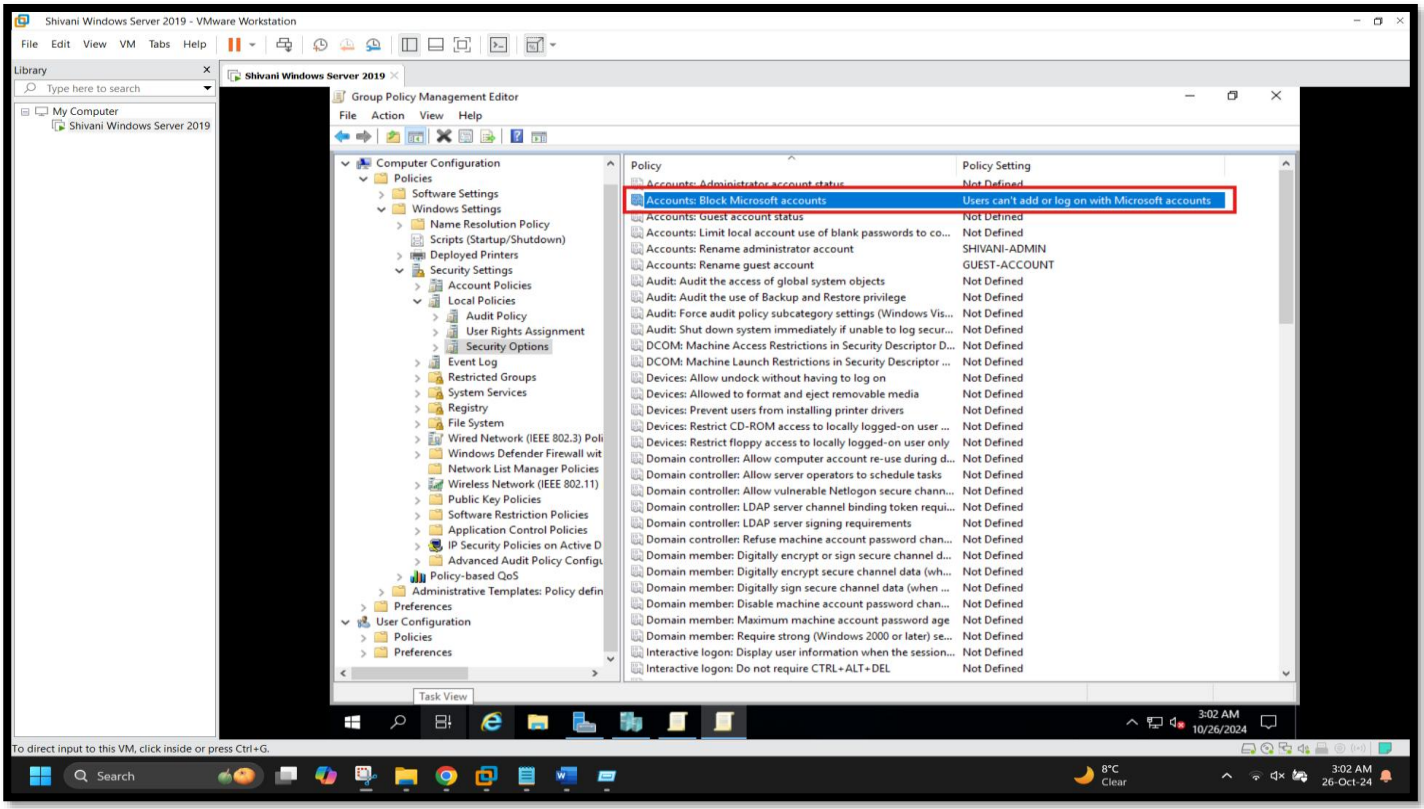


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 5 : Blocking Microsoft Accounts]

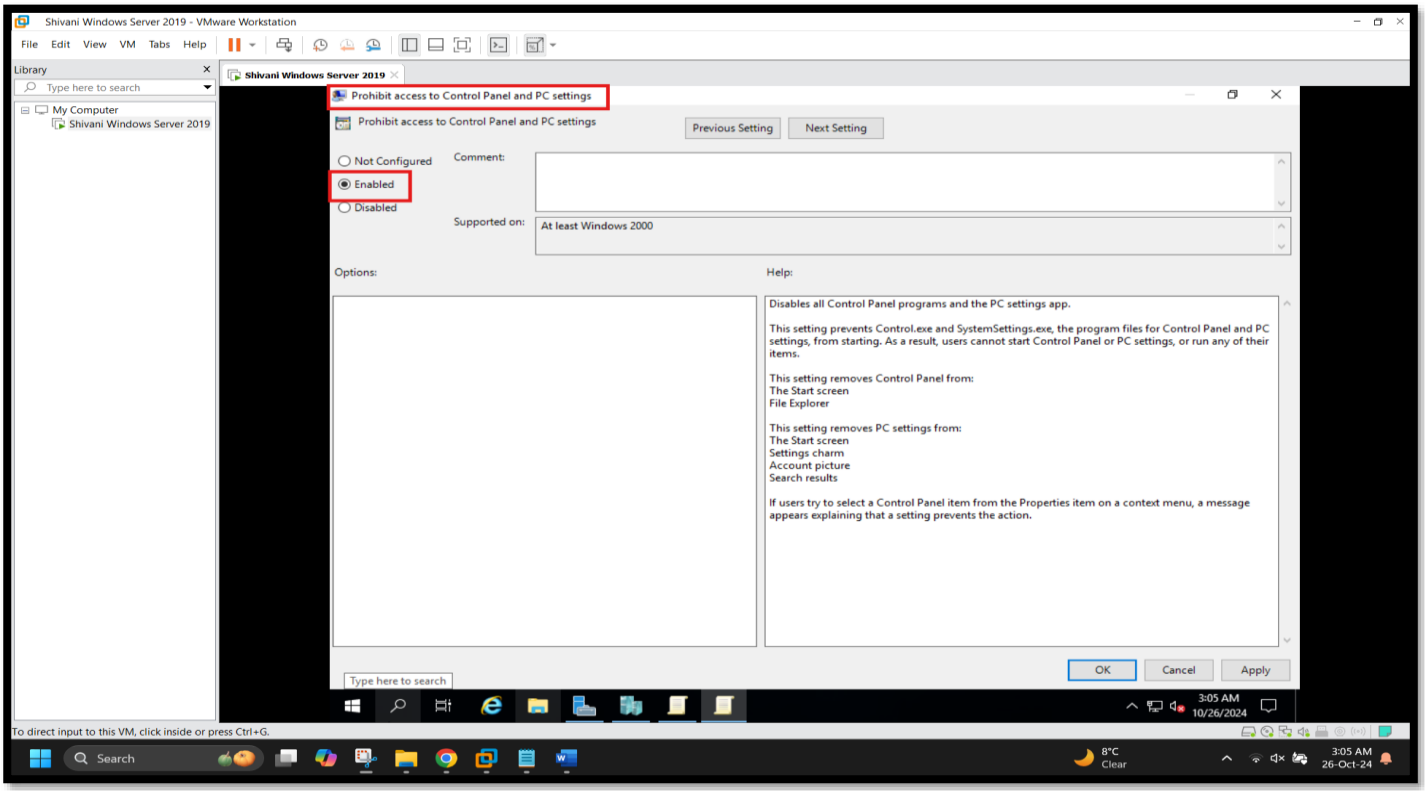


[Screenshot 6 : Enabled Blocking Microsoft Accounts – User can't add or login with Microsoft Account]

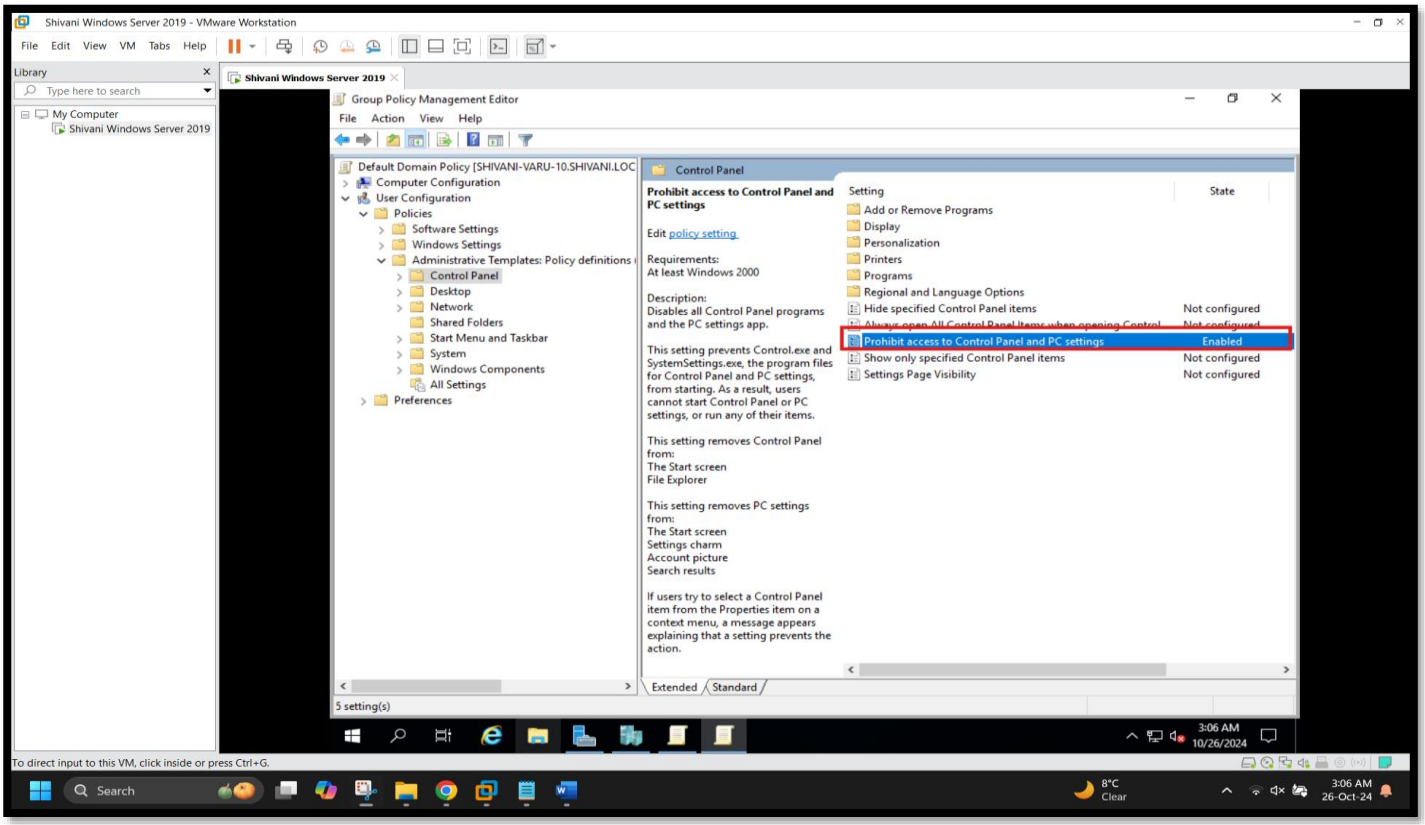


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 7: Prohibiting access to the Control Panel and PC settings]

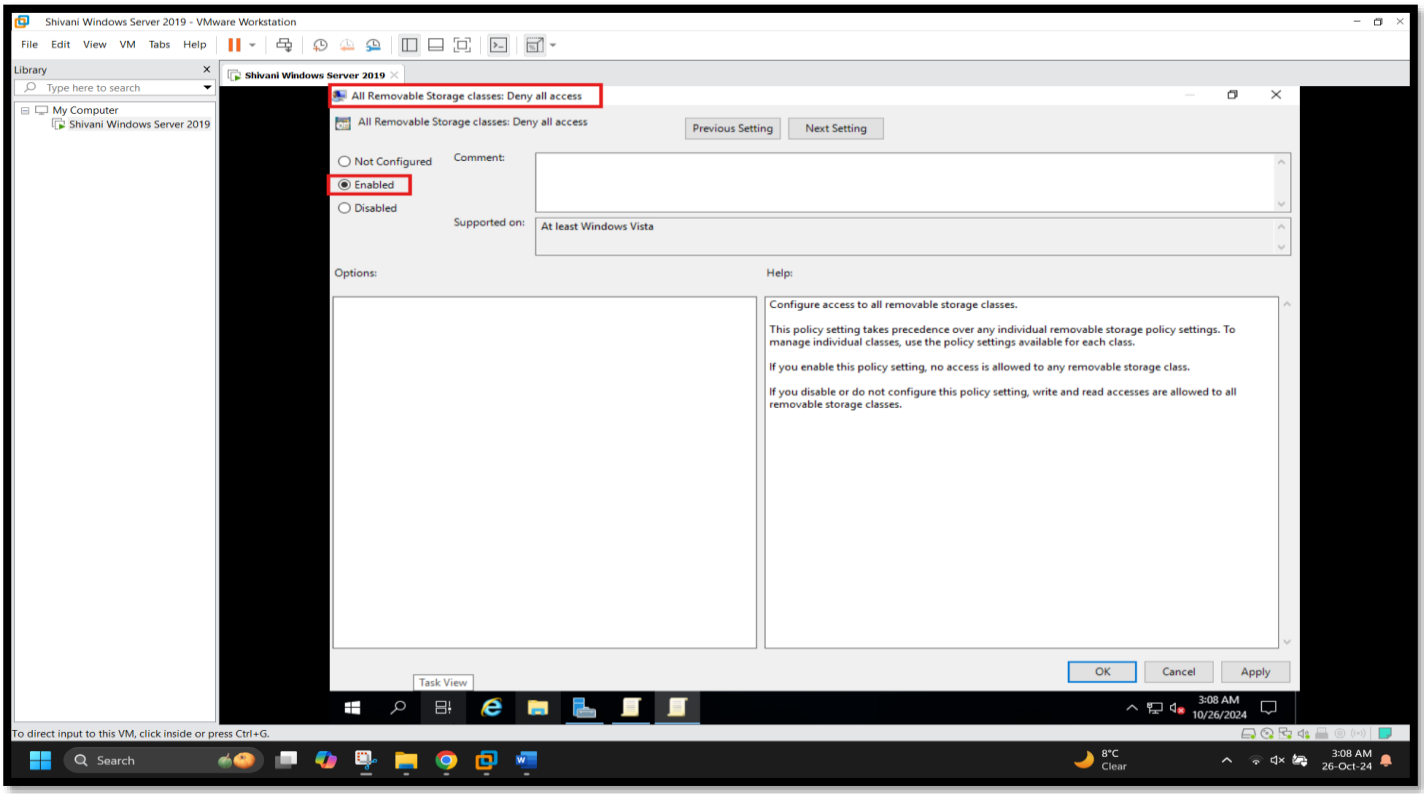


[Screenshot 8: Enabled Prohibiting access to the Control Panel and PC settings]

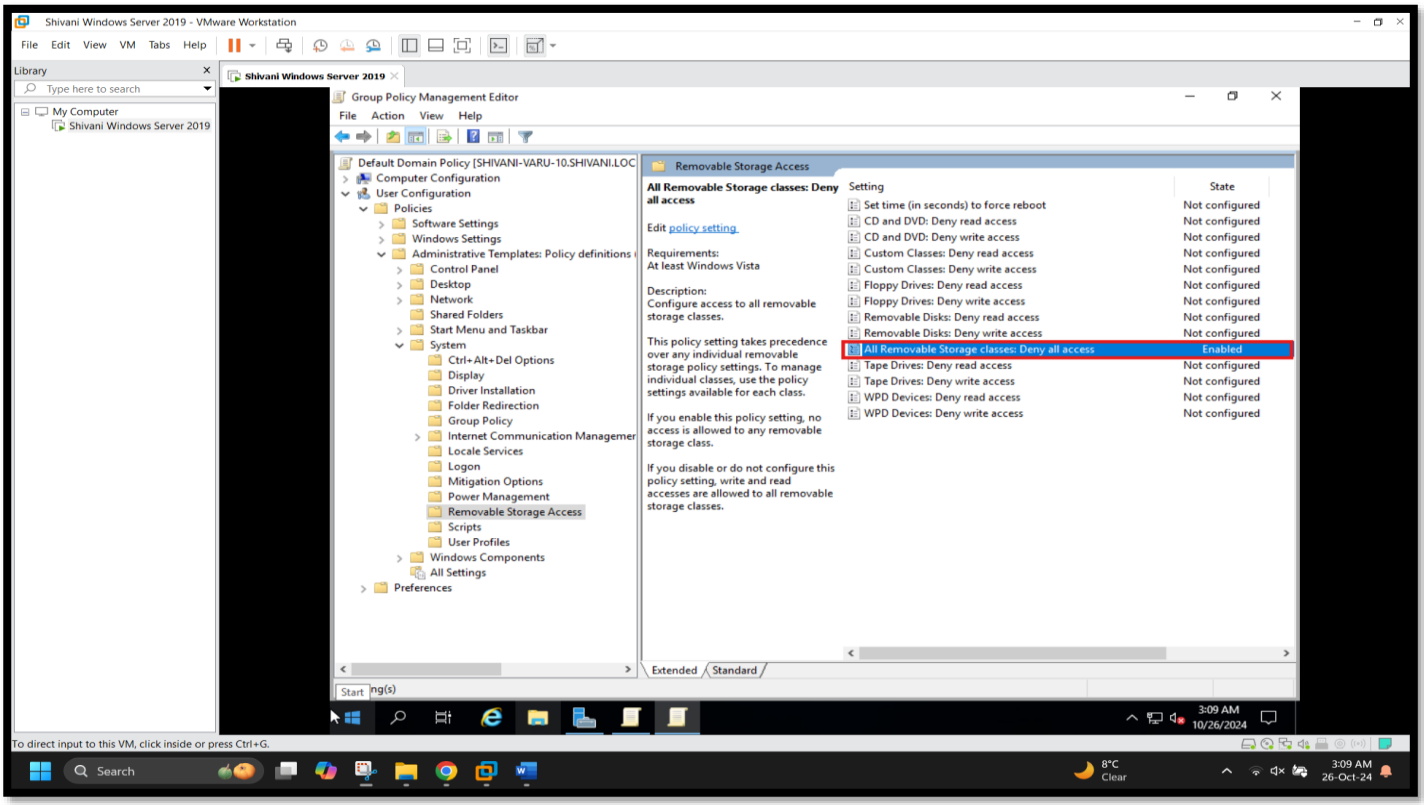


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 9: Denying access to all removable storage classes]



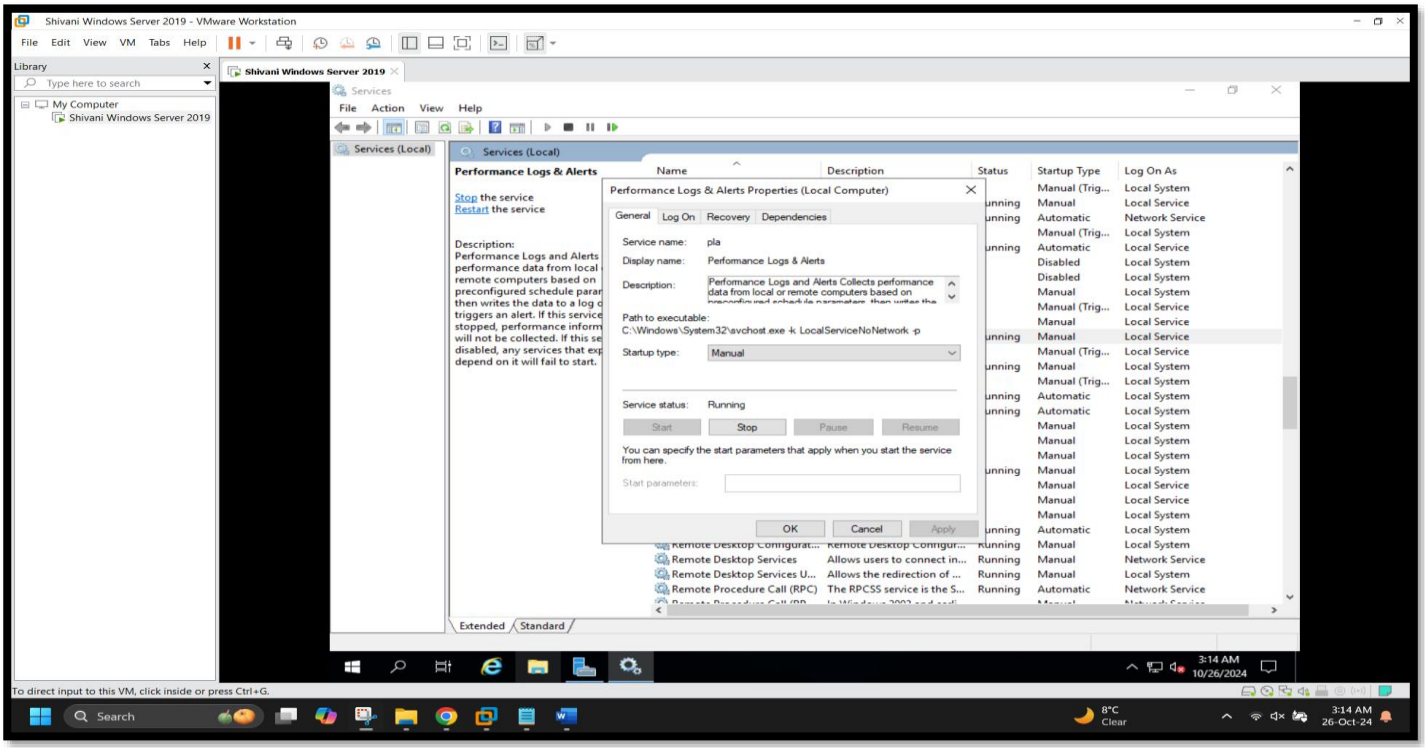
[Screenshot 10: Enabled Denying access to all removable storage classes]



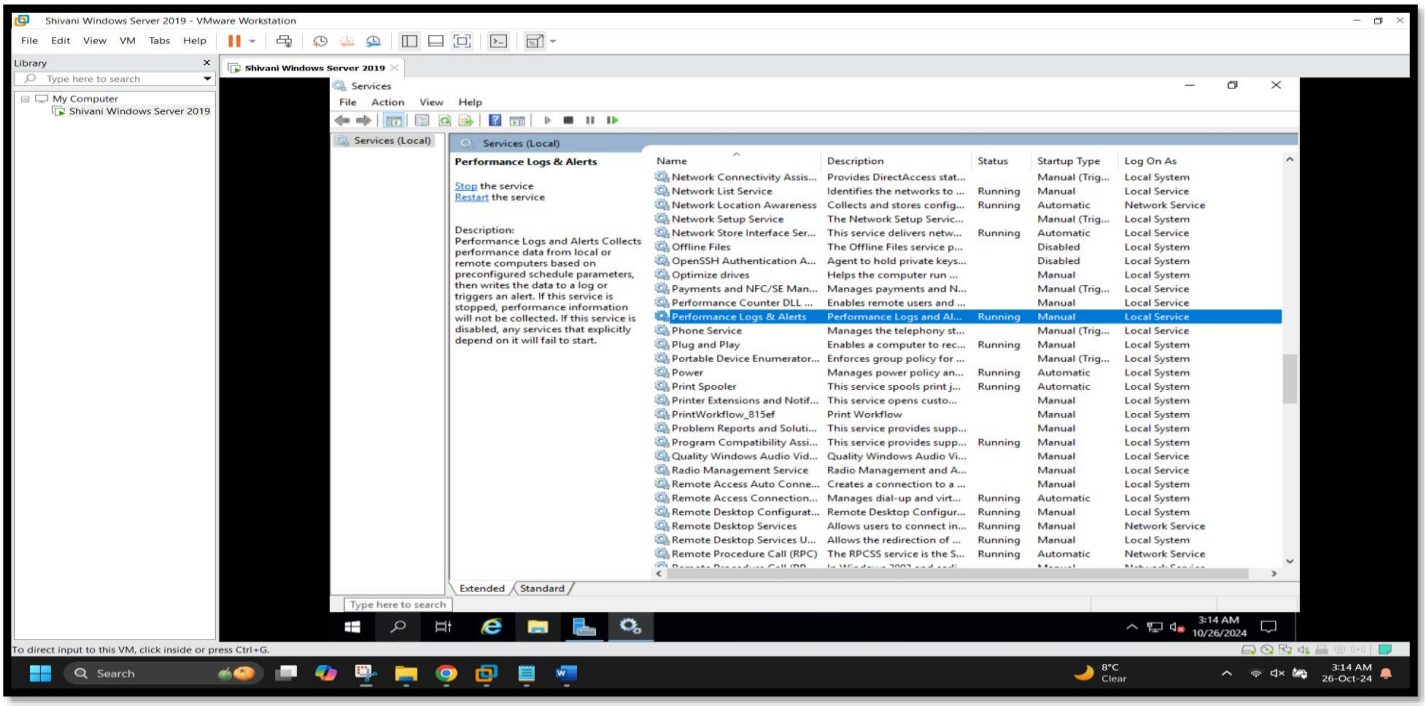
Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

Exercise – 10 The Performance Logs and Alerts Services

[Screenshot 1: Starting the Performance Logs and Alerts Service]

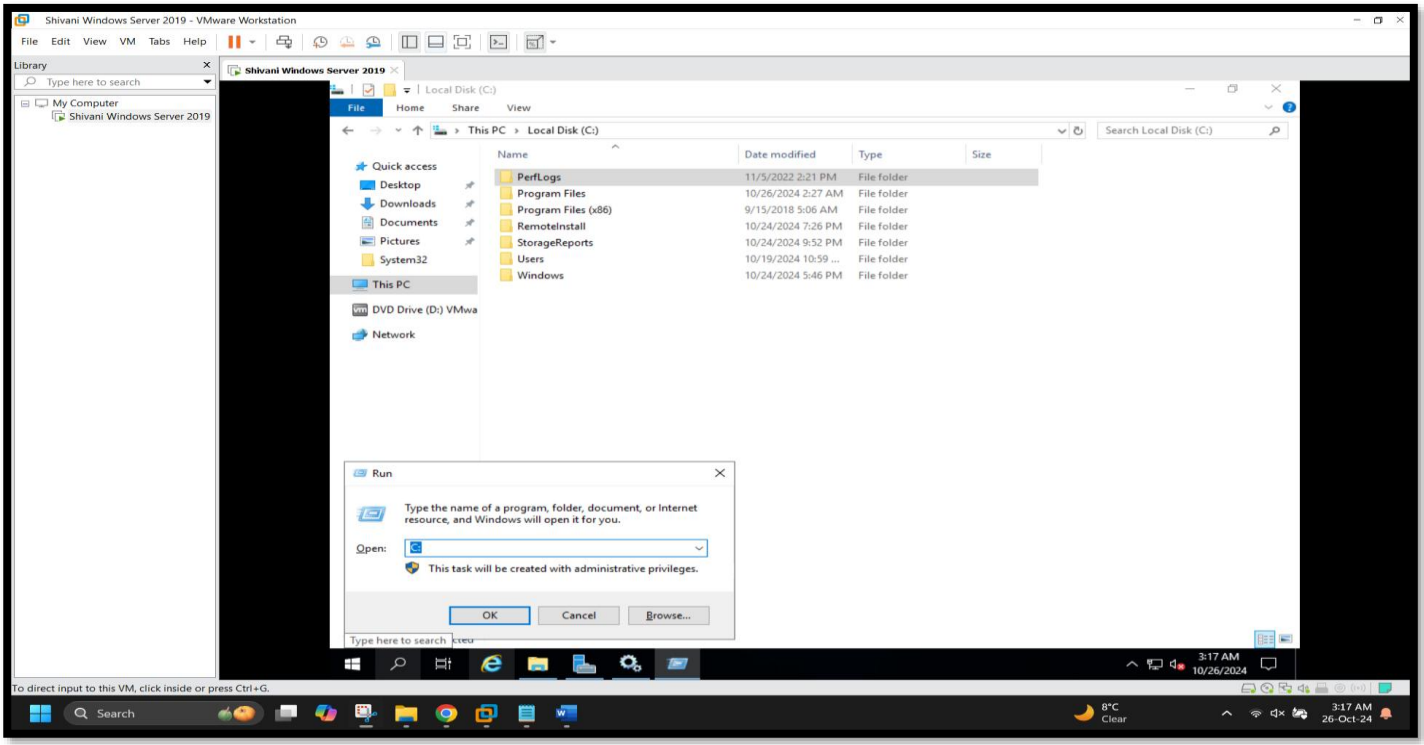


[Screenshot 2: Starting the Performance Logs and Alerts Service]

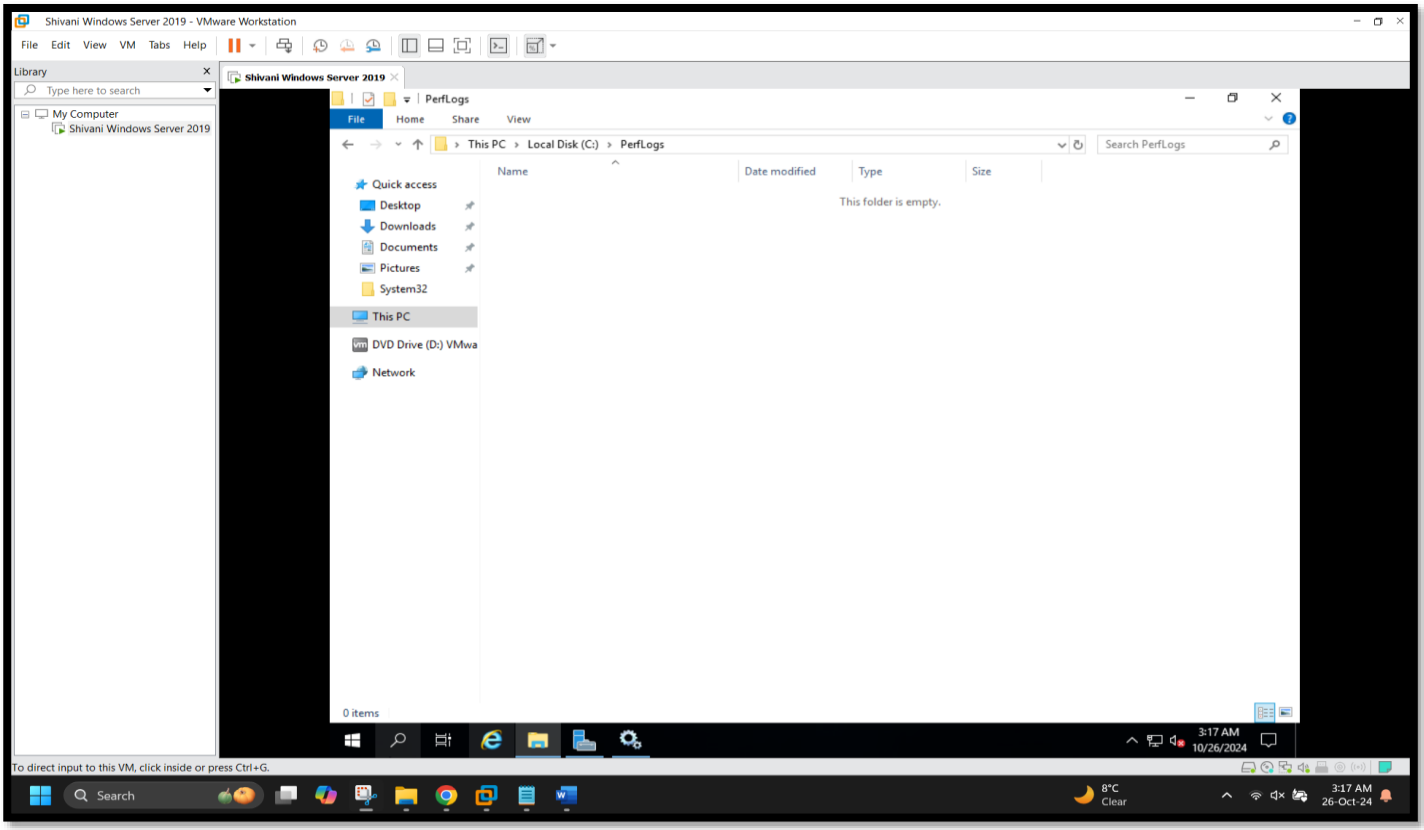


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 3: PerfLogs folder in the C: drive, accessible for storing performance logs collected by the Performance Monitor]

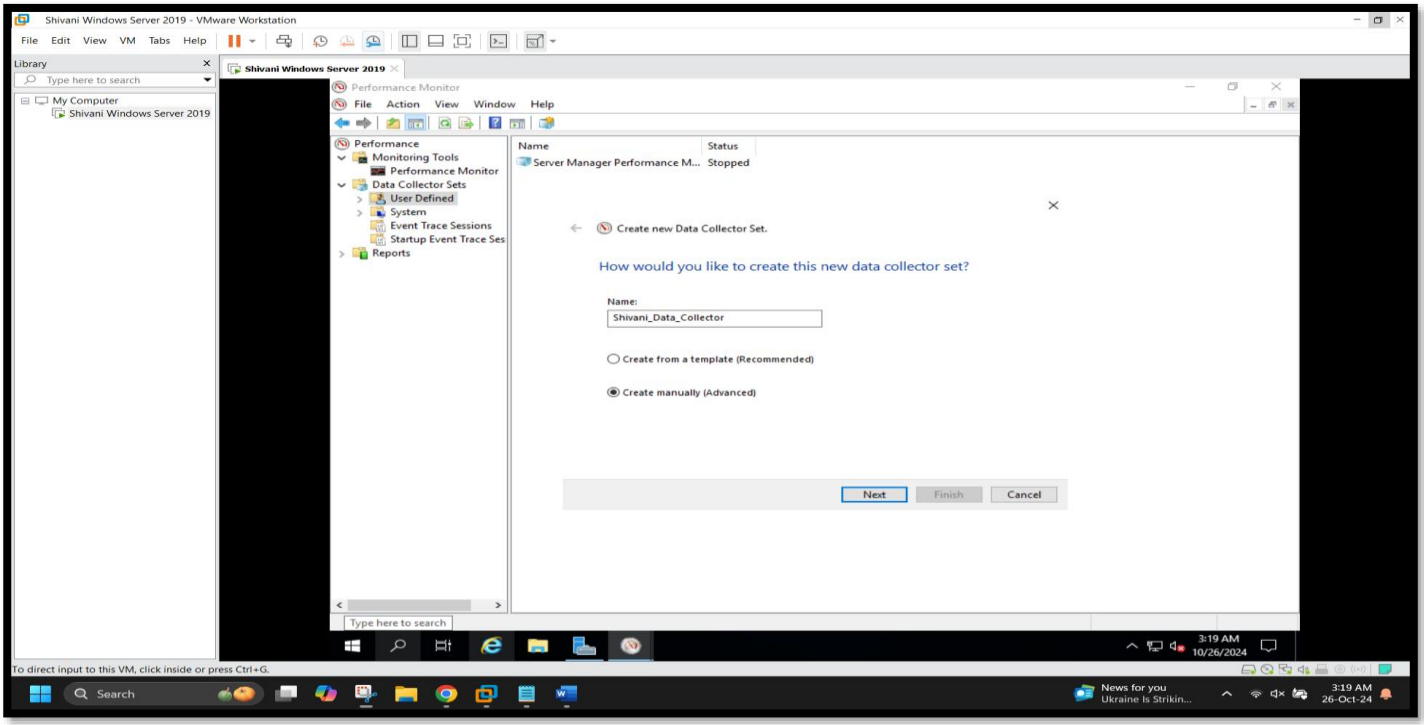


[Screenshot 4: Accessing the PerfLogs Folder]

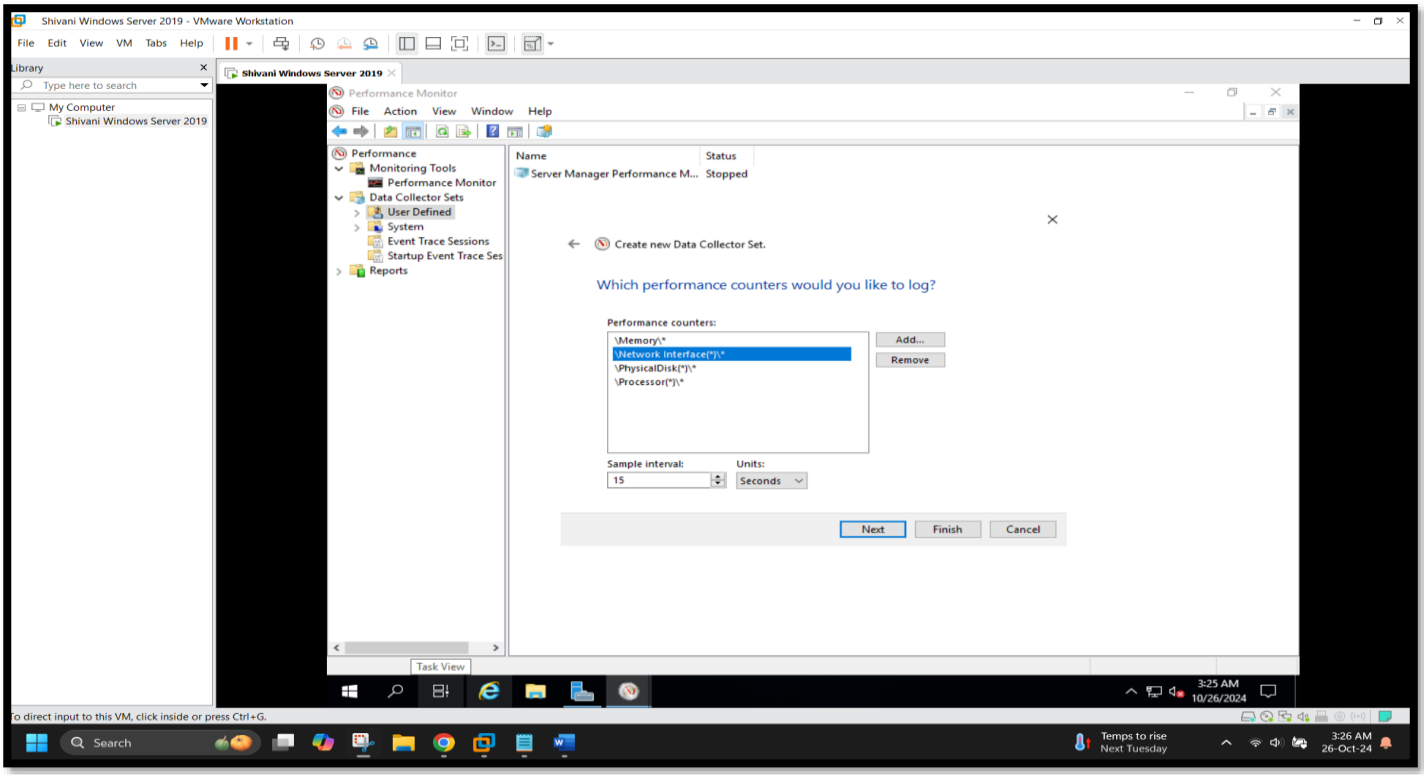


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 5: Setting up a new Data Collector Set in Performance Monitor and naming it 'Shivani_Data_Collector']

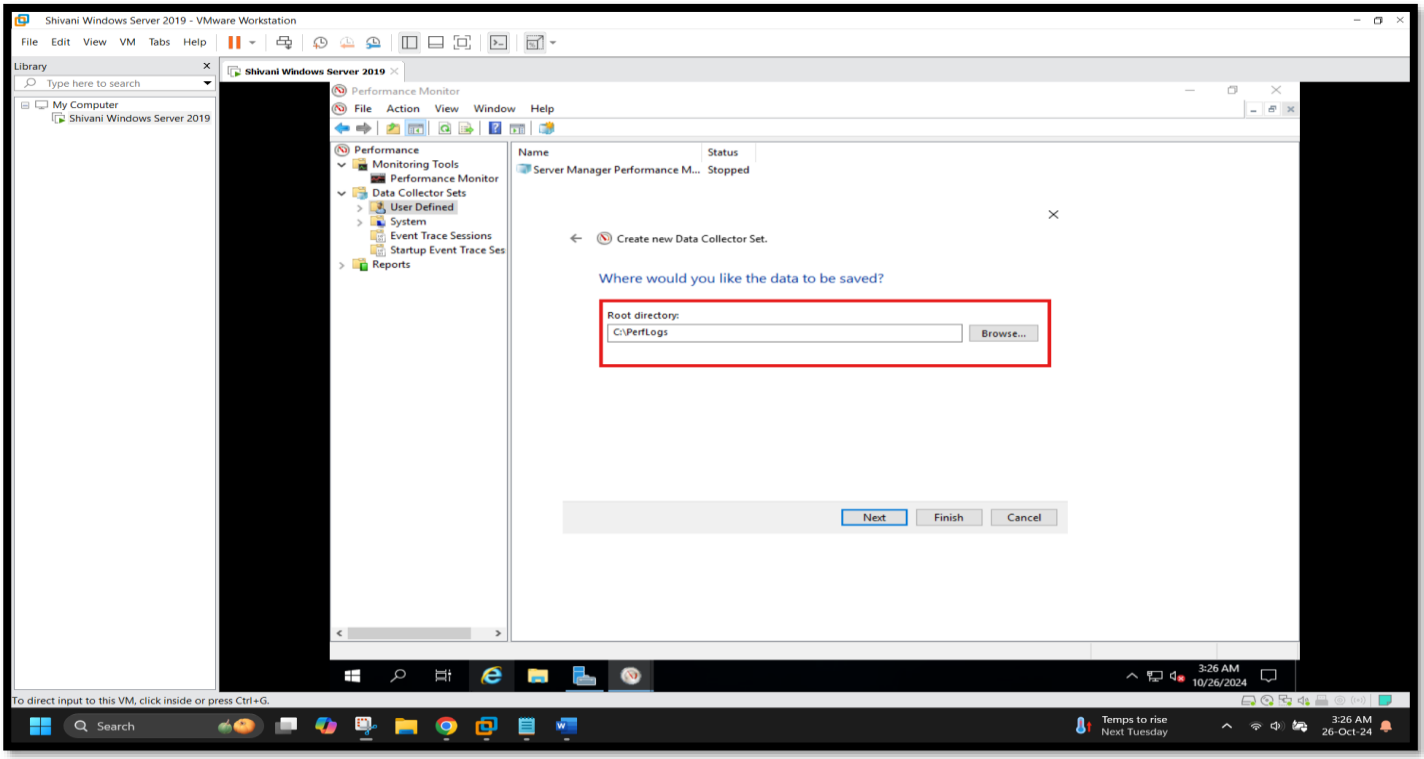


[Screenshot 6: Choosing the 'Performance counter' option for data logging in the new Data Collector Set.]

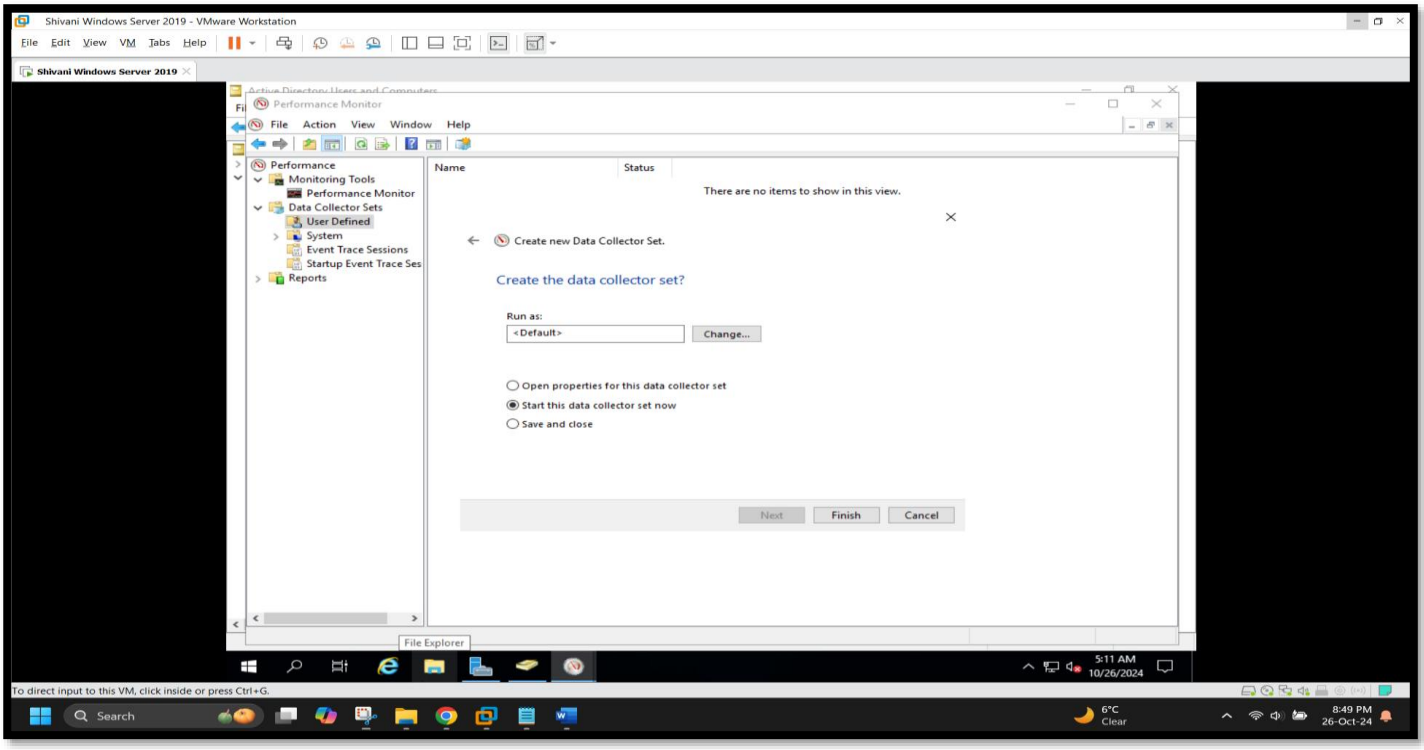


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 7: Specifying the data storage location as the PerfLogs folder in the C: drive for the new Data Collector Set]

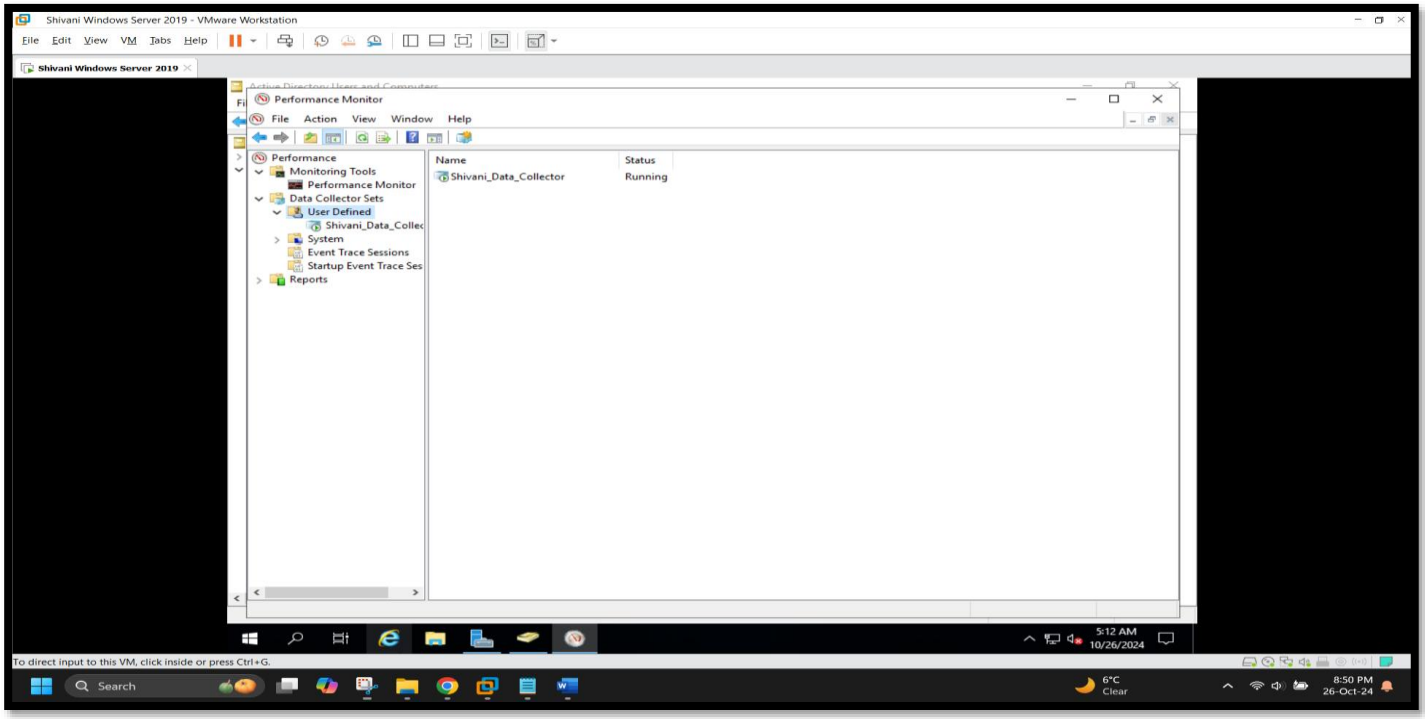


[Screenshot 8: Setting the user account for running the Data Collector Set and starting the collection immediately upon completion]

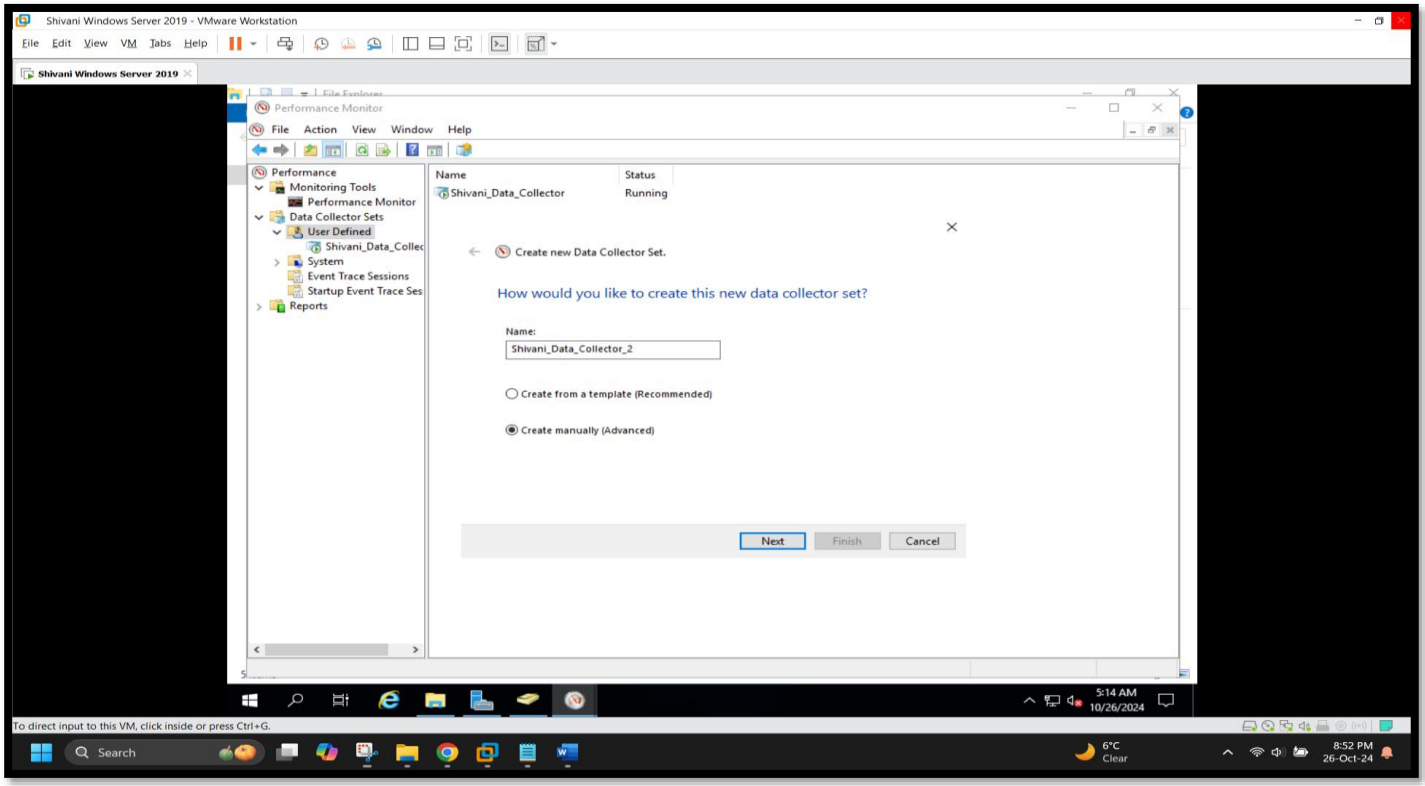


Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

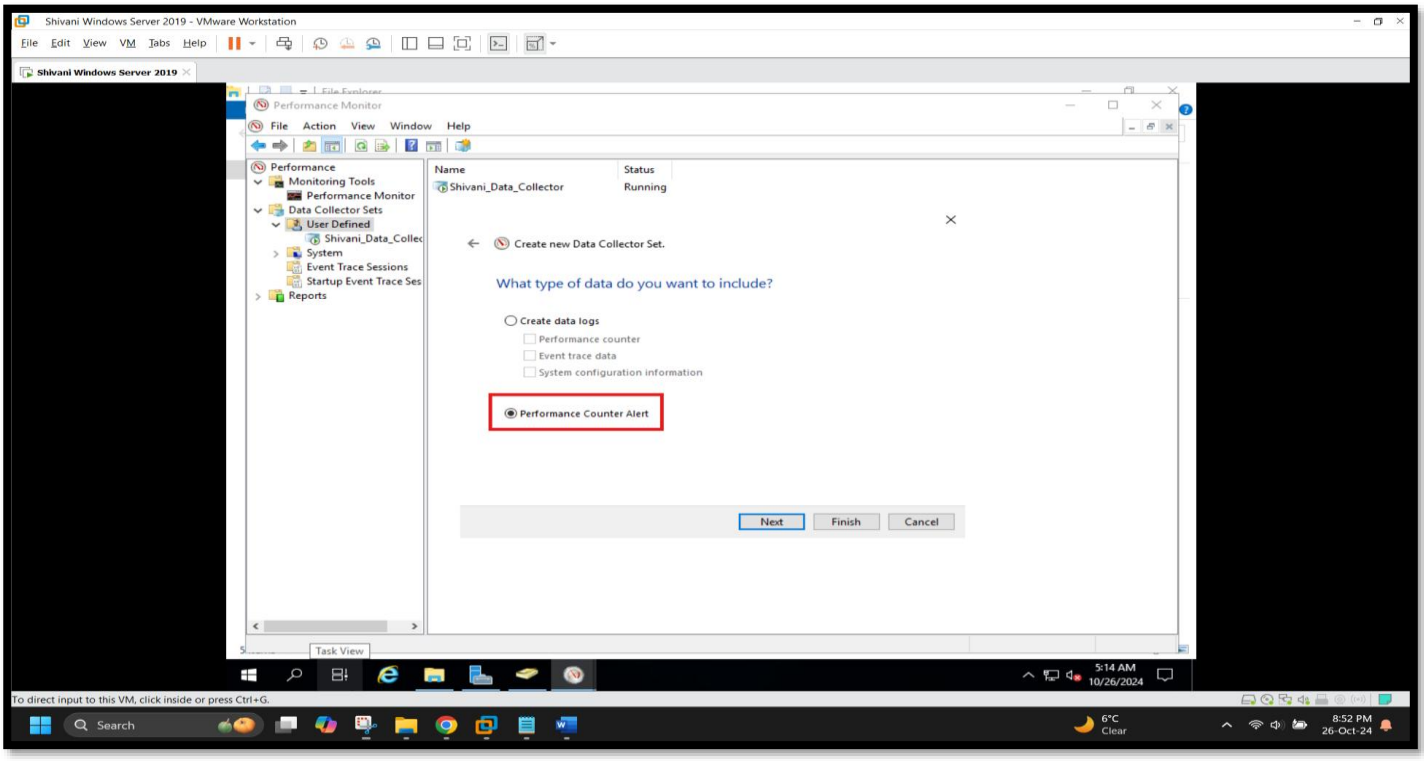
[Screenshot 9: The 'Shivani_Data_Collector' is now actively running and collecting performance data under User Defined in Performance Monitor]



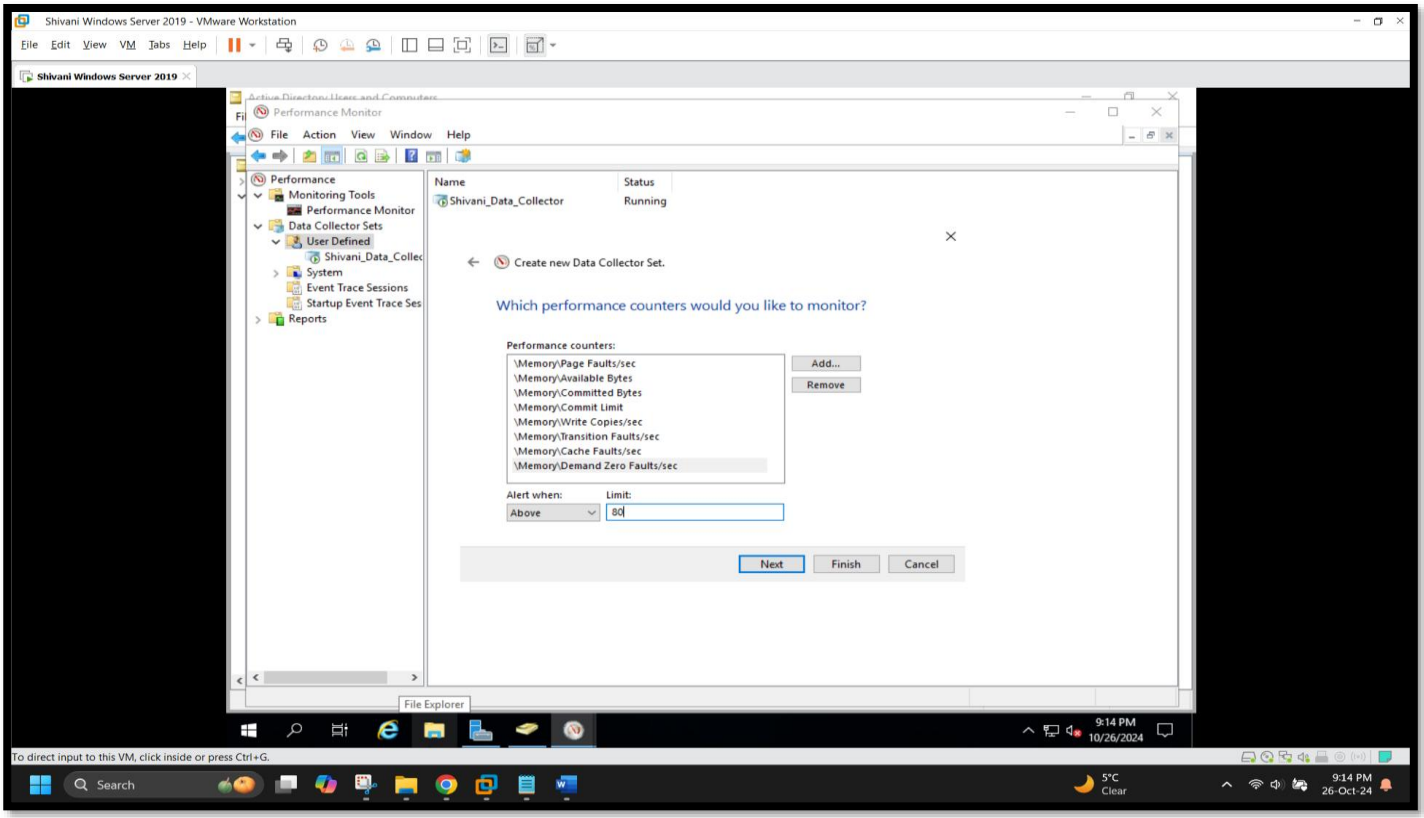
[Screenshot 10: Setting up an additional Data Collector Set named 'Shivani_Data_Collector_2' with custom configurations]



[Screenshot 11: Selecting Performance Counter Alert]

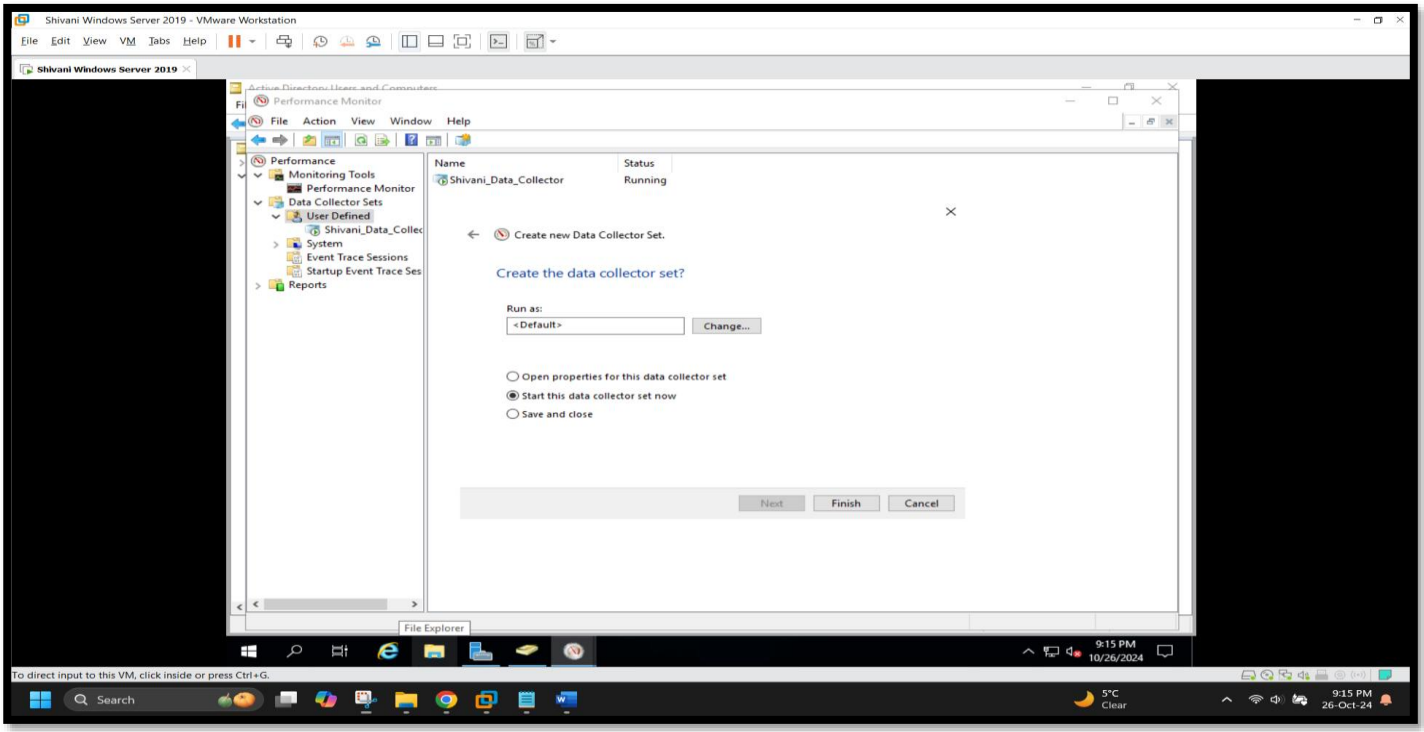


[Screenshot 12: Adding specific performance counters and setting an alert threshold, such as triggering an alert when memory usage goes above 80%]



Name: Shivani Shaileshkumar Varu **Student ID: 101481565**

[Screenshot 13: Setting up the 'Run As' user for the Data Collector Set and choosing to start the data collection immediately]



[Screenshot 14: Both 'Shivani_Data_Collector' and 'Shivani_Data_Collector_2' Data Collector Sets are actively running, collecting data as configure]