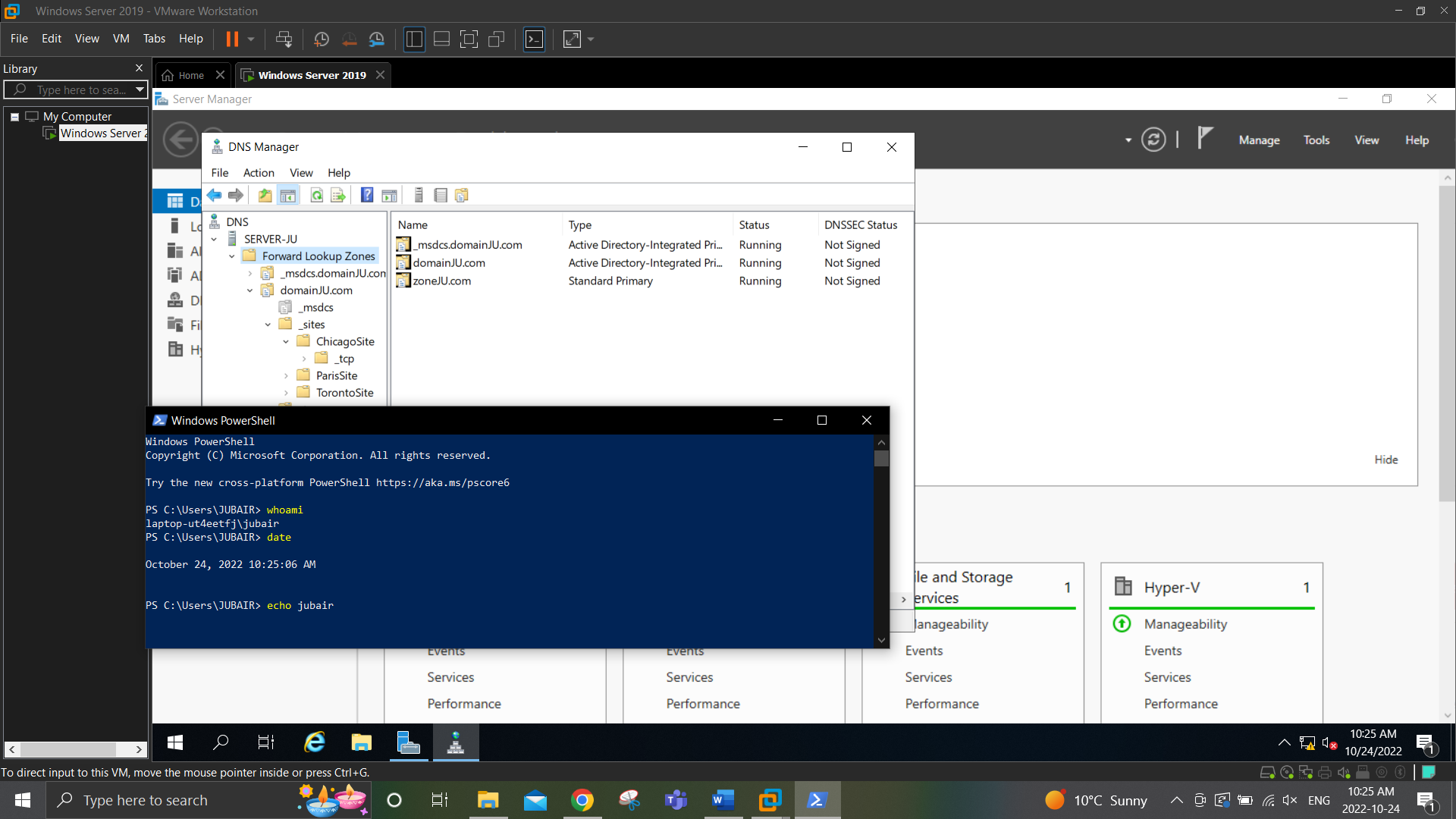
**Project 1: Configuring DNS Zones**

*In this Hands-On Project, you explore the properties of your DNS server and the Active Directory-integrated primary zone used by Active Directory on your Windows Server 2019 host. Next, you create a primary forward lookup zone as well as a reverse lookup zone that is Active Directory-integrated. Finally, you attempt to create a stub zone for your partner’s Active Directory domain that has a conditional forwarder previously configured from Hands-On Project 4.*

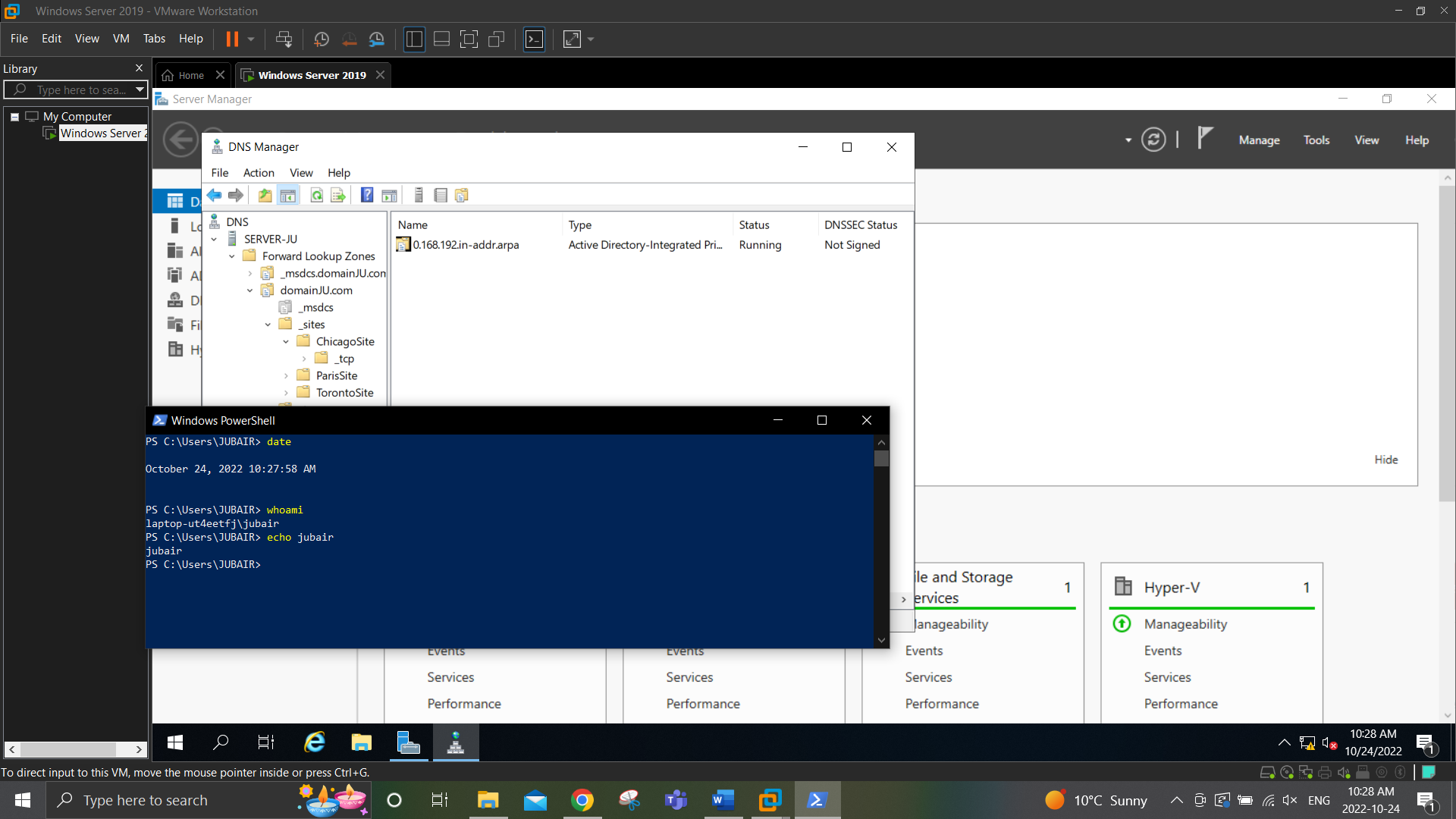
1. Boot your Windows Server 2019 host and log into domainX.com as Administrator using the password **Secret555**. Next, click **Start** and then click **Server Manager**.
2. In Server Manager, click the **Tools** menu and then click **DNS.**
3. In the DNS Manager window, right-click the **SERVERX** object in the navigation pane and click **Properties**.
4. On the Interfaces tab of the SERVERX Properties window, note that your DNS server will respond to DNS lookups that are received on all network interfaces by default.
5. Highlight the **Forwarders** tab. Note that your DNS server is configured as a default forwarder to the IP addresses that you use in your classroom environment (8.8.8.8) and that root hints are used if no forwarders are available.
6. Highlight the **Advanced** tab and note that round robin and netmask ordering are enabled by default. Select **Enable automatic scavenging of stale records** and note the default value of 7 days.
7. Highlight the **Root Hints** tab and note the entries that identify the top-level DNS servers and click **OK**.
8. In the navigation pane, expand **Forward Lookup Zones** and highlight **domainX.com**. Note the default A resource records for the computers in your domain. Also note that the SOA, NS, and A resource records for serverX list static under the Timestamp column, whereas the A resource records for other computers in your domain list the date and time that they were dynamically updated.
9. In the navigation pane, expand **domainX.com** and highlight **\_tcp**. Note the SRV resource records that identify the FQDN of the domain controllers in your domain that host the global catalog (\_gc), Kerberos (\_kerberos), Kerberos password (\_kpasswd), and LDAP (\_ldap) services using the TCP/IP protocol.
10. In the navigation pane under domainX.com, expand **sites, ChicagoSite** and highlight **\_tcp.** Note the SRV resource records for the domain controllers that are part of the ChicagoSite site. Collapse **domainX.com** in the navigation pane when finished.
11. Right-click **domainX.com** in the navigation pane and click **Properties**. Note that the zone type is Active Directory-integrated and that records are replicating to other domain controllers that host DNS in the domain. Also note that the zone accepts secure dynamic updates.
12. Click **Aging**. At the Zone Aging/Scavenging Properties window, select **Scavenge stale resource records**, note the default values for the No-refresh and Refresh intervals, and click **OK.** Click **OK** to close the domainX.com Properties window.
13. Right-click **Forward Lookup Zones** in the navigation pane and click **New Zone**.
14. At the New Zone Wizard, click **Next**.
15. At the Zone Type page, note the default selection of Primary zone. Deselect **Store the zone in Active Directory** and click **Next**.
16. At the Zone Name page, type **zoneX.com** and click **Next**.
17. At the Zone File page, note that a zone file called zoneX.com.dns will be created in the C:\Windows\system32\dns folder to store resource records and click **Next**.
18. At the Dynamic Update page, note the default option that does not allow dynamic updates and click **Next.**
19. Click **Finish** to create zoneX.com.

**(Take Screenshot)**



1. Right-click **Reverse Lookup Zones** in the navigation pane and click **New Zone**.
2. At the New Zone Wizard, click **Next**.
3. At the Zone Type page, note that an Active Directory-integrated primary zone will be created by default and click **Next**.
4. At the Active Directory Zone Replication Scope page, note the default option that replicates the zone to domain controllers in domainX.com and click **Next**.
5. At the Reverse Lookup Zone Name page, note the default selection of IPv4 Reverse Lookup Zone and click **Next**.
6. At the Reverse Lookup Zone Name page, type **192.168.0** in the Network ID text box and click **Next**.
7. At the Dynamic Update page, note the default option that allows only secure dynamic updates and click **Next**.
8. Click **Finish** to create the 0.168.192.in-addr.arpa reverse lookup zone.

**(Take Screenshot)**

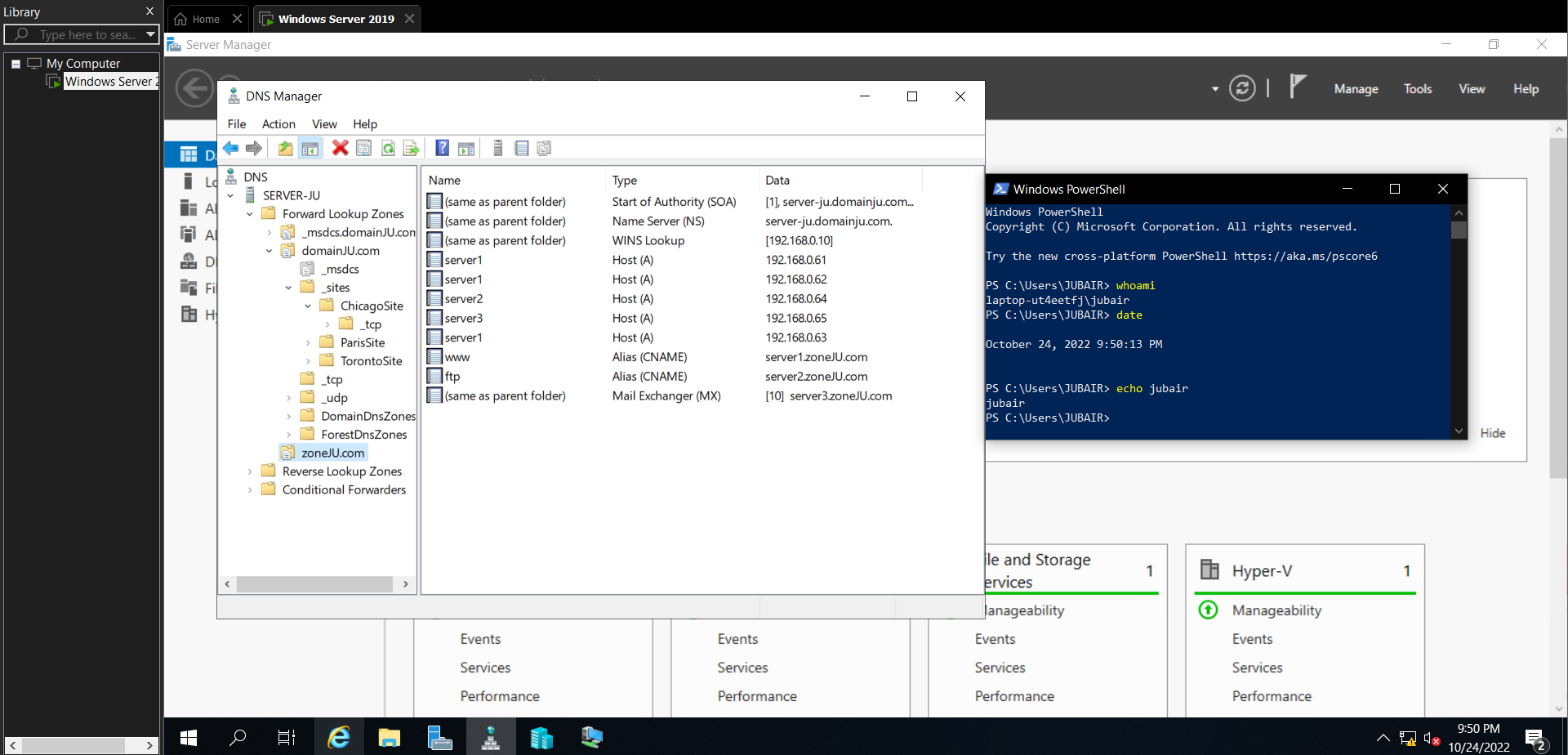


**Project 2: DNS Zone Properties and Resource Records**

*In this Hands-On Project, you explore and configure resource records in the zoneX.com forward lookup zone and 0.168.192.in-addr.arpa reverse lookup zone. Following this, you test name resolution using these resource records.*

1. In the navigation pane of DNS Manager on your Windows Server 2019 host, highlight **zoneX.com** and note the default SOA and NS records that were created.
2. Right-click **zoneX.com** in the navigation pane and click **Properties**. Note that the zone type is Primary and that dynamic updates are not enabled.
3. Highlight the **Start of Authority (SOA)** tab and note the default zone transfer intervals and default TTL values in the SOA record.
4. Highlight the **Name Servers** tab and note that serverX.domainX.com is listed as an authoritative DNS server for the zone.
5. Highlight the **WINS** tab and select **Use WINS forward lookup**. Enter the IPv4 address of your Windows Server 2019 host (192.168.0.10) in the IP address text box and click **Add**. We will install and configure WINS on your Windows Server 2019 host in Hands-On Project 4.
6. Highlight the **Zone Transfers** tab.
7. Select **Only to the following servers** and click **Edit**.
8. In the Allow Zone Transfers window, type the IP address of your WindowsServer2019VM2 virtual machine and click OK.
9. Click **Notify**. Select **The following servers**, type the IP address of your WindowsServer2019VM2 virtual machine and click **OK**.
10. Click **OK** to close the zoneX Properties window.
11. Right-click **zoneX.com** in the navigation pane and click **New Host (A or AAAA).**
12. At the New Host window, type server1 in the Name text box, type **192.168.0.61** in the IP address text box, and select **Create associated pointer (PTR) record**. Click **Add Host** and then click **OK**.
13. At the New Host window, type **server1** in the Name text box and type **192.168.0.62** in the IP address text box. Click **Add Host** and then click **OK**.
14. At the New Host window, type **server1** in the Name text box and type **192.168.0.63** in the IP address text box. Click **Add Host** and then click **OK.**
15. At the New Host window, type **server2** in the Name text box and type **192.168.0.64** in the IP address text box. Click **Add Host** and then click **OK**.
16. At the New Host window, type **server3** in the Name text box and type **192.168.0.65** in the IP address text box. Click **Add Host** and then click **OK.**
17. Click **Cancel** to close the New Host window.
18. Right-click **zoneX.com** in the navigation pane and click **New Alias (CNAME).** At the New Resource Record window, type **www** in the Alias name text box, type **server1.zoneX.com** in the Fully qualified domain name (FQDN) for target host text box and click **OK**.
19. Right-click **zoneX.com** in the navigation pane and click **New Alias (CNAME).** At the New Resource Record window, type ftp in the Alias name text box, type **server2.zoneX.com** in the Fully qualified domain name (FQDN) for target host text box and click **OK**.
20. Right-click **zoneX.com** in the navigation pane and click **New Mail Exchanger (MX).** At the New Resource Record window, type **server3.zoneX.com** in the Fully qualified domain name (FQDN) of mail server text box and click **OK.**
21. Highlight **zoneX.com** in the navigation pane. Note the WINS Lookup, A, CNAME, and MX records that were created.

**(Take Screenshot)**



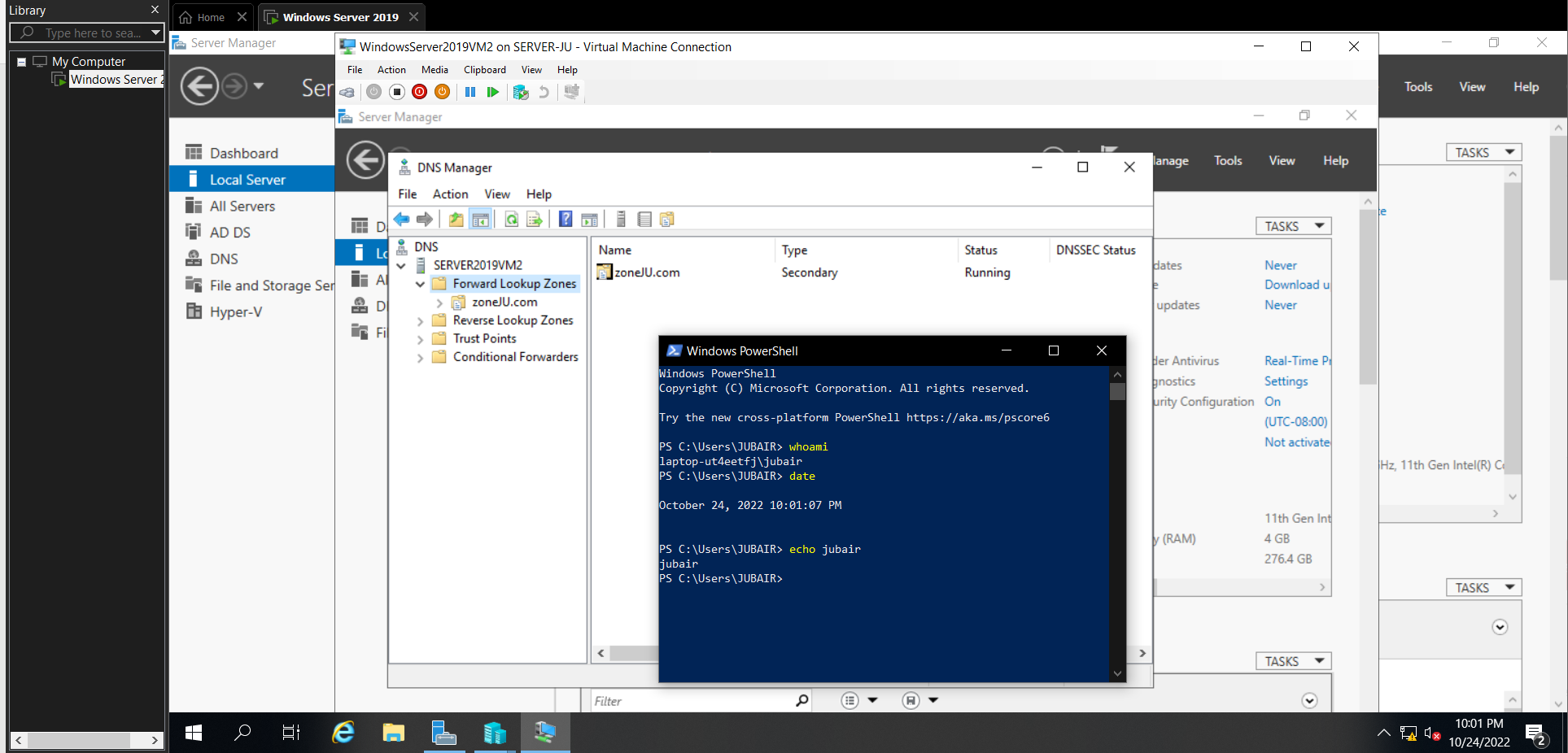
1. Expand **Reverse Lookup Zones** in the navigation pane and highlight **0.168.192.in-addr.arpa**. Note the PTR resource records that were created in Step 3.
2. Right-click **SERVERX** in the navigation pane and click **Launch nslookup**.
3. At the interactive > prompt in nslookup, type **www.zoneX.com** and press **Enter**. Note that www.zoneX.com is an alias to server1.zoneX.com. Also note that server1.zoneX.com returns three IP addresses (192.168.0.61, 192.168.0.62, and 192.168.0.63).
4. Type **www.zoneX.com** again and press **Enter**. Note that the order of the three IP addresses (192.168.0.62, 192.168.0.63, and 192.168.0.61) has been rotated using round robin.
5. Type **ftp.zoneX.com** and press **Enter**. Note that ftp.zoneX.com is an alias to server2 .zoneX.com, which has an IP address of 192.168.0.64.
6. Type **192.168.0.64** and press **Enter**. Note that 192.168.0.64 is associated with the FQDN of server2.zoneX.com.
7. Type **set type=mx** and press **Enter**. Next, type **zonex.com** and press **Enter**. Note that the mail server for zonex.com is server3.zoneX.com, which has an IP address of 192.168.0.65.
8. Type **exit** and press **Enter** to quit the nslookup utility.
9. Type **exit** again and press **Enter** to close the Command Prompt window.
10. Close DNS Manager.

**Project 3: Configurng DNS Secondary Zones**

*In this Hands-On Project, you install the DNS Server role on your WindowsServer2019VM2 virtual machine, configure a secondary zone for zoneX.com, and perform a zone transfer.*

1. In Server Manager on your Windows Server 2019 host, select the **Tools** menu and then click **Hyper-V Manager**.
2. Highlight **WindowsServer2019VM2** in the virtual machines pane of Hyper-V Manager and click **Connect** in the Actions pane. In the Virtual Machine Connection window, click **Start** to boot your virtual machine.
3. At the login screen, click the **Ctrl+Alt+Delete** button in the Virtual Machine Connection window, supply the password **Secret555** for Administrator and press **Enter** to log into the system.
4. On your WindowsServer2019VM2 virtual machine, click **Start** and then click **Server Manager**. Next, click the **Manage** menu and then click **Add Roles and Features**.
5. At the Select installation type page, click **Next**.
6. At the Select destination server page, click **Next**.
7. At the Select server roles page, select **DNS Server** and click **Add Features** when prompted. Click **Next**.
8. At the Select features page, click **Next**.ser
9. At the DNS Server page, click **Next**.
10. At the Confirm installation selections page, click **Install**.
11. At the Installation progress page, click **Close**.
12. In Server Manager, click the **Tools** menu and then click **DNS**.
13. In the navigation pane of the DNS Manager window, expand your server object, and expand **Forward Lookup Zones**. Next, right-click **Forward Lookup Zones** and click **New Zone**.
14. At the New Zone Wizard, click **Next**.
15. At the Zone Type page, note that the option to store the zone in Active Directory is unavailable because WindowsServer2019VM2 is not a domain controller. Select **Secondary zone** and click **Next**.
16. At the Zone Name page, type **zoneX.com** and click **Next**.
17. At the Master DNS Servers page, type the IP address of your Windows Server 2019 host and press **Enter**. Note that SERVERX is shown next to the IP address and click **Next**.
18. Click **Finish** to create zoneX.com.

**(Take Screenshot)**



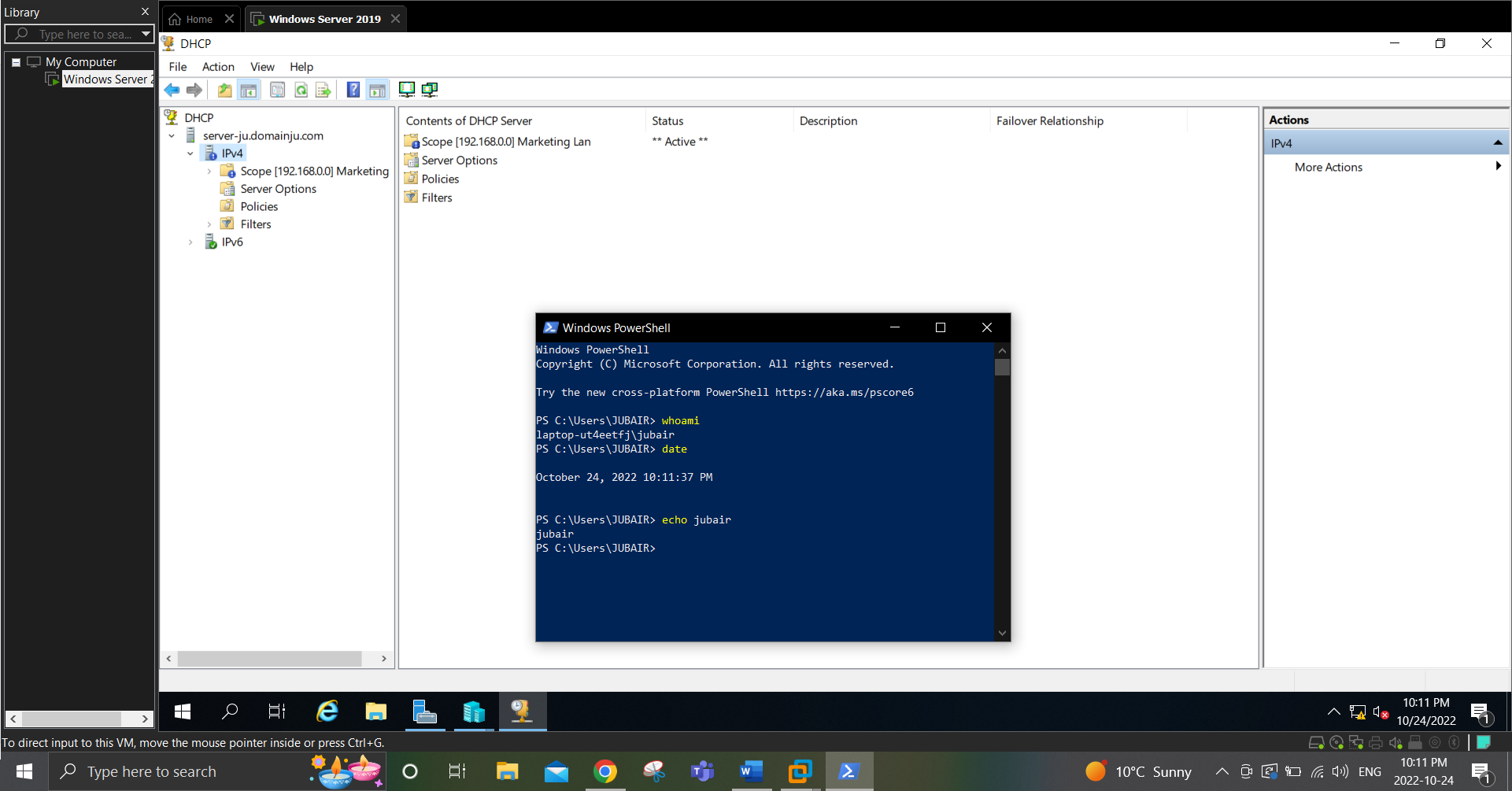
1. Highlight **zoneX.com** in the navigation pane and note the error indicating that the zone has not been loaded by the DNS server.
2. Right-click **zoneX.com** in the navigation pane and click **Transfer from Master** to perform the initial zone transfer. Next, right-click **zoneX.com** in the navigation pane and click **Refresh**. Note that the records you configured in zoneX.com on your Windows Server 2019 host are present.
3. Right-click **zoneX.com** in the navigation pane and note that there are no options available to create resource records. Click **Properties** and highlight the **Start of Authority (SOA)** tab. Note that you are unable to modify the configuration of the secondary zone parameters and click **OK**.
4. Close DNS Manager.

**Project 4: Installing and Configuring DHCP**

*In this Hands-On Project, you install the DHCP Server role on your Windows Server 2019 host as well as configure a new DHCP scope, reservation, and policy.*

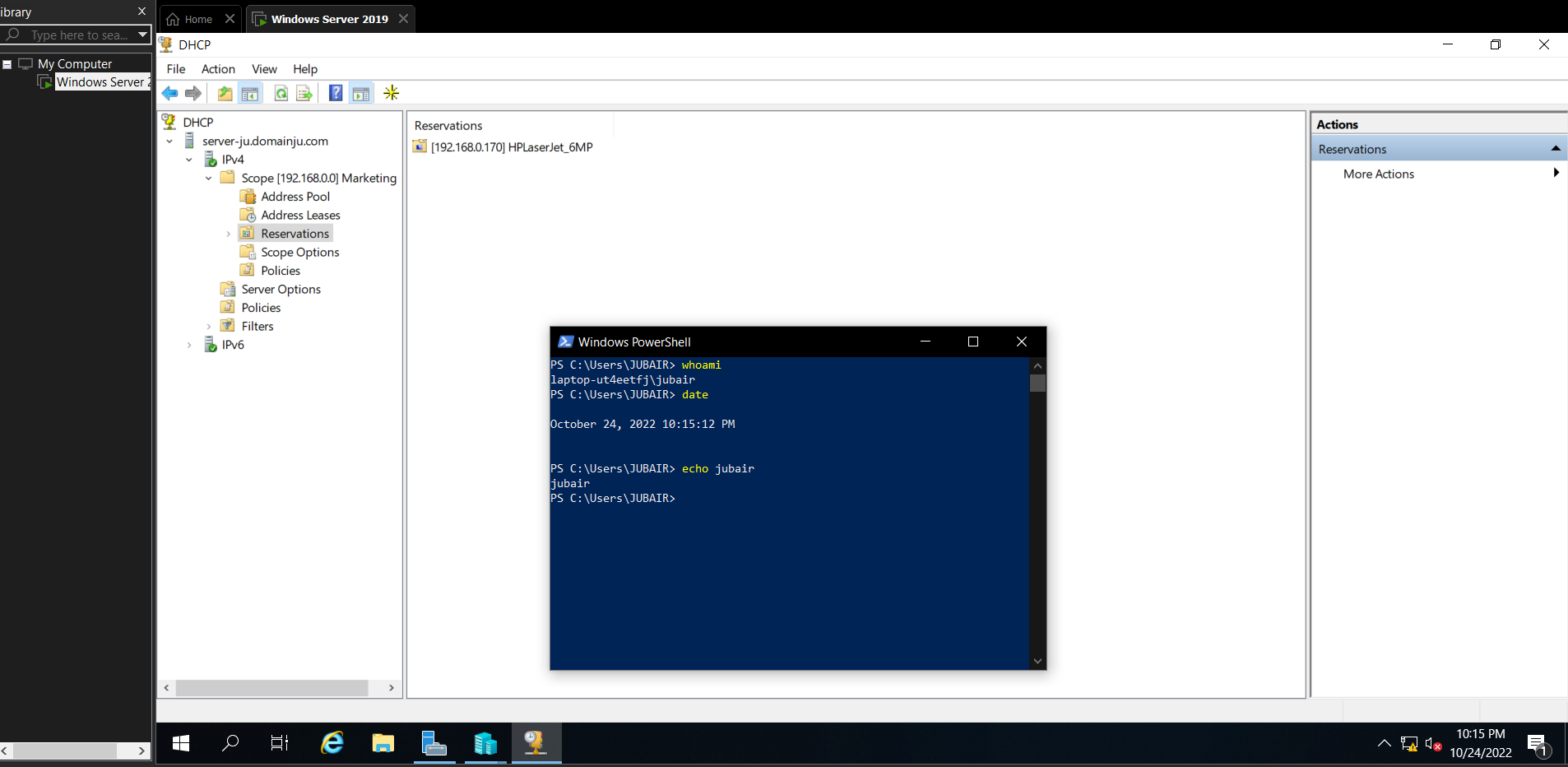
1. In Server Manager on your Windows Server 2019 host, click the **Manage** menu and then click **Add Roles and Features**.
2. At the Select installation type page, click **Next**.
3. At the Select destination server page, click **Next**.
4. At the Select server roles page, select **DHCP Server**, and click **Add Features** when prompted. Click **Next**.
5. At the Select features page, click **Next.**
6. At the DHCP Server page, read the information regarding best practices and click **Next**.
7. Click **Install.**
8. After the installation has completed, click **Complete DHCP configuration**, click **Next**, click **Commit**, and then click **Close**.
9. Click **Close** to close the Add Roles and Features Wizard.
10. In Server Manager, select the Tools menu and then click **DHCP**.
11. In the DHCP tool, expand your server in the navigation pane and then expand IPv4. Note that the Scope [192.168.0.0] Internal Network scope you configured in Hands-On Project 3 is available. This is because DHCP configuration is not removed when you remove the DHCP Server role.
12. Expand **Scope [192.168.0.0] Internal Network** and highlight **Address Pool**. Note the address range of 192.168.0.50 to 192.168.0.100. (Note: You might need to go to scope properties and change the address range as above).
13. Highlight **Scope Options**. Note that the only option configured is 060 PXEClient, used for WDS deployment.
14. Highlight **Scope [192.168.0.0] Internal Network** in the navigation pane and click **More Actions, Delete** in the Actions pane. Click **Yes**, and then click **Yes** again to remove your scope.
15. Highlight **Server Options** in the navigation pane and click **More Actions, Configure Options** in the Actions pane.
16. In the Server Options window, check **004 Time Server**.
17. Type **time.windows.com** in the Server name text box and click **Resolve**.
18. Click **Add**.
19. Click **OK** to close the Server Options window. Note that both the 004 Time Server and 060 PXEClient server options are displayed.
20. Highlight **IPv4** in the navigation pane and click **More Actions, New Scope** in the Actions pane.
21. In the Welcome page of the New Scope Wizard, click **Next**.
22. At the Scope Name page, type **Marketing LAN** in the Name text box and click **Next.**
23. At the IP Address Range page, supply a Start IP address of **192.168.0.100**. Next, supply an End IP address of **192.168.0.200** and click **Next**.
24. At the Add Exclusions and Delay page, type **192.168.0.150** in the Start IP address text box, click **Add**, and click **Next**.
25. At the Lease Duration page, note the default value of 8 days and click **Next**.
26. At the Configure DHCP Options page, click **Next**.
27. At the Router (Default Gateway) page, type **192.168.0.2** in the IP address text box, click **Add**, and click **Next.**
28. At the Domain Name and DNS Servers page, note that the DHCP server is configured to provide the domainX.com domain name suffix and DNS server of 192.168.0.1 to DHCP clients and click **Next.**
29. At the WINS Servers page, type **192.168.0.1** in the IP address text box, click **Add**, and click **Next**.
30. At the Activate Scope page, note that the scope will be activated following creation and click **Next**.
31. Click **Finish** to complete the New Scope Wizard.

**(Take Screenshot)**



1. Expand **Scope [192.168.0.0]** **Marketing LAN** and highlight **Address Pool**. Note that the address range and exclusion you configured are present.
2. Highlight **Scope Options**. Note the options that were configured during the New Scope Wizard as well as the two options that were inherited from the server.
3. Highlight **Reservations** and click **More Actions, New Reservation** in the Actions pane.
4. At the New Reservation window, type **HPLaserJet\_6MP** in the Reservation name text box.
5. Type **192.168.0.170** in the IP address text box.
6. Type **f20000ada4d5** in the MAC address text box and click **Add**.
7. Click Close.

**(Take Screenshot)**



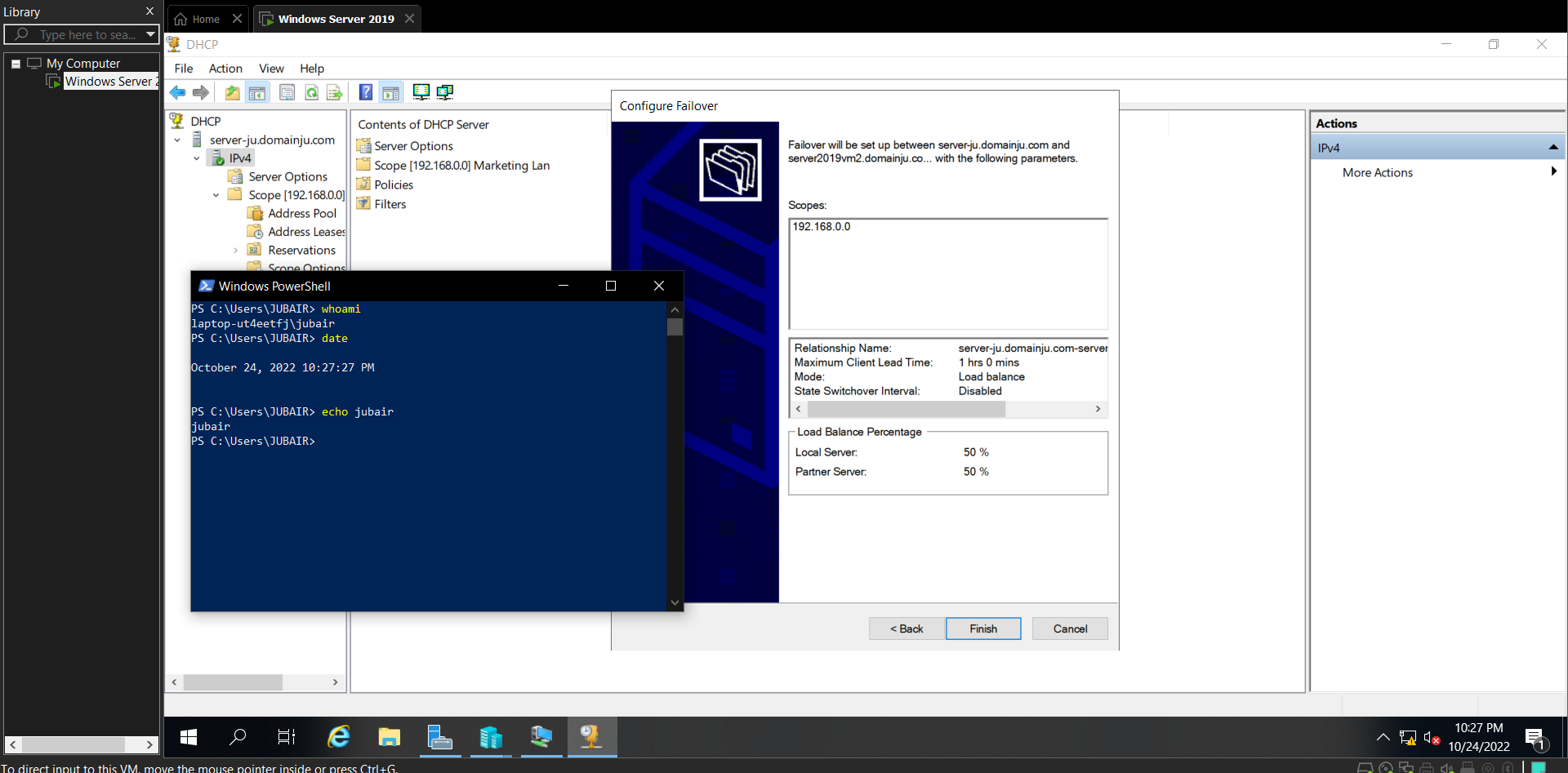
1. Expand **Reservations** and highlight **[192.168.0.170] HPLaserJet\_6MP**. Note the options inherited from both the scope and server.
2. Highlight **Policies** under Scope [192.168.0.0] Marketing LAN. In the Actions pane, click **More Actions, New Policy**.
3. At the DHCP Policy Configuration Wizard, type **Polycom VoIP phones** in the Policy Name dialog box and click **Next**.
4. At the Configure Conditions for the policy page, click **Add**. Select **Client Identifier** from the Criteria drop-down box, type **4E00D5** in the Value text box, click **Add**, and then click **OK**. Click **Next** when finished.
5. At the Configure settings for the policy page, select **No** and click **Next**.
6. At the next Configure settings for the policy page, check **003 Router**, type **192.168.0.254** in the IP address text box, and click **Add.** Click **Next**.
7. Click **Finish** to create a policy for the scope that provides a different default gateway for Polycom VoIP phones.
8. Highlight **Scope [192.168.0.0] Marketing LAN** and click **More Actions, Properties** in the Actions pane.
9. On the General tab of Scope [192.168.0.0] Marketing LAN Properties, note that you can modify all scope parameters except for the subnet mask as well as set an unlimited lease duration.
10. Highlight the **DNS** tab and note the default values. Select **Always dynamically update DNS records** and check **Dynamically update DNS records for DHCP clients that do not request updates**.
11. Click **Configure**, check **Enable Name Protection**, and click **OK**.
12. Click **OK** to close the Scope [192.168.0.0] Marketing LAN Properties window.

**Project 5: DHCP Testing and Fault Tolerance**

*In this Hands-On Project, you install a second network interface on your WindowsServer2019VM2 virtual machine to test the scope you created in Hands-On Project 4. Next, you install the DHCP Server role on your WindowsServer2019VM2 virtual machine and configure fault tolerance for the scope.*

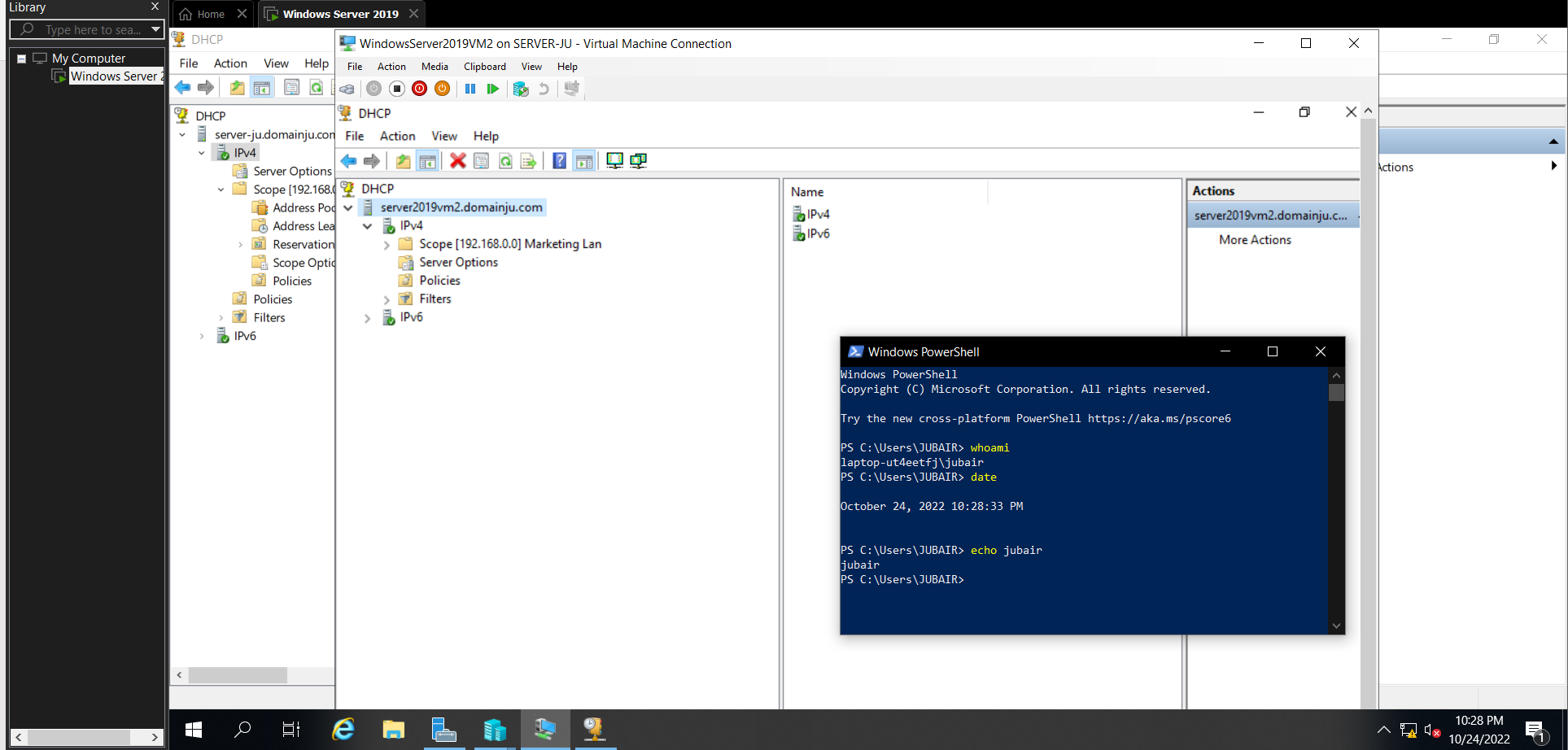
1. Highlight **WindowsServer2019VM2** in the virtual machines pane of Hyper-V Manager and click **Connect** in the Actions pane.
2. In the Virtual Machine Connection window, click **Start** to boot your virtual machine.
3. At the login screen, click the **Ctrl+Alt+Delete** button in the Virtual Machine Connection window, supply the password **Secret555** for Administrator, and press **Enter** to log into the system
4. On your WindowsServer2019VM2 virtual machine, click **Start** and then click **Server Manager**. Navigate to **Local Server**. In the Properties section, click the hyperlink next to your Ethernet network interface.
5. In the Network Connections window, right-click your Ethernet network interface and click **Status**.
6. In the Ethernet Status window, click **Details**. Note down network interface IP address (192.168.0.\_\_\_).
7. Click **Close** to close the Network Connection Details window.
8. Click **Close** to close the Ethernet Status window, and then close the Network Connections window.
9. In Server Manager on your WindowsServer2019VM2 virtual machine, click the **Manage** menu and then click **Add Roles and Features**.
10. At the Select installation type page, click **Next**.
11. At the Select destination server page, click **Next**.
12. At the Select server roles page, select **DHCP Server**, and click **Add Features** when prompted. Click **Next**.
13. At the Select features page, click **Next**.
14. At the DHCP Server page, read the information regarding best practices and click **Next**.
15. Click **Install**.
16. After the installation has completed, click **Complete DHCP configuration**, click **Next**, click **Commit,** and then click **Close**.
17. Click Close to close the Add Roles and Features Wizard.
18. In the DHCP tool on your Windows Server 2019 host, highlight **Address Leases** under Scope [192.168.0.0] Marketing LAN. All IP addresses that have been already assigned will show up here. Also note that the reservation for HPLaserJet\_6MP is displayed.
19. Highlight **Scope [192.168.0.0] Marketing LAN** and **click More Actions, Display Statistics** in the Actions pane. It shows the IP addresses that are in use from your scope. Click **Close** when finished.
20. Highlight **IPv4** and click **More Actions, Configure Failover** in the Actions pane.
21. At the Configure Failover wizard, note that all available scopes are selected and click **Next**.
22. At the Specify the partner server to use for failover page, type **192.168.0.\_\_\_\_** (IP address of WindowsServer2019VM2) in the Partner Server text box and click **Next**.
23. At the Create a new failover relationship page, note the default options, type **Secret555** in the Shared Secret text box, and click **Next**.

**(Take Screenshot)**



1. Click **Finish** to complete the failover configuration.
2. Click **Close** to close the Configure Failover window.
3. Close the DHCP tool.
4. In Server Manager on your WindowsServer2019VM2 virtual machine, click the **Tools** menu and then click **DHCP**.
5. In the DHCP tool, expand your server, and then expand **IPv4.** Note that Scope [192.168.0.0] Marketing LAN has automatically been copied from your Windows Server 2019 host.

**(Take Screenshot)**



1. Expand **Scope [192.168.0.0] Marketing LAN** and highlight **Address Leases**. Note that the address lease for your WindowsServer2019VM2 virtual machine is present to ensure that your DHCP server does not lease the 192.168.0.100 address to DHCP clients. Also note that the reservation for HPLaserJet\_6MP is displayed to ensure that your DHCP server will provide the correct IP address if a DHCPDISCOVER packet it received from HPLaserJet\_6MP printer.
2. Close the DHCP tool.