Lab 8 Configuring Remote Access Services

**Task 3 – Activity**

**(Save your work because your answers may be required to provide in the Mid-Semester and Final Examination.)**

# Activity 8-1: Installing Network Policy and Access Services and Remote Access

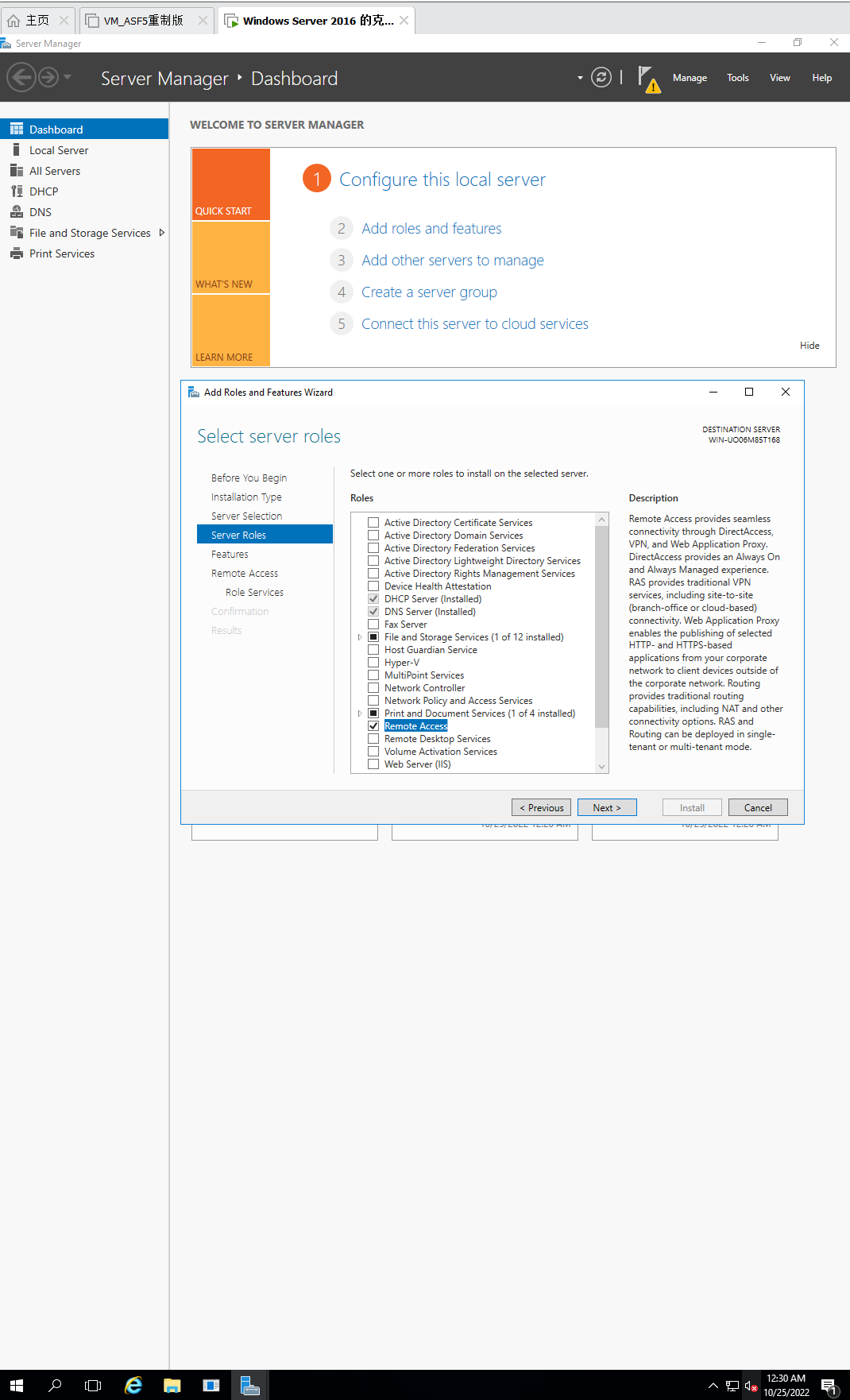
**Time Required**: Approximately 25 minutes

**Objective**: Learn how to install the Network Policy and Access Services and Remote Access roles.

**Description**: VPN servers enable remote users to access a Windows Server 2016 server through using secure tunneling protocols. In this activity, you install the Network Policy and Access Services role along with the Remote Access role as a first step in implementing a VPN server.

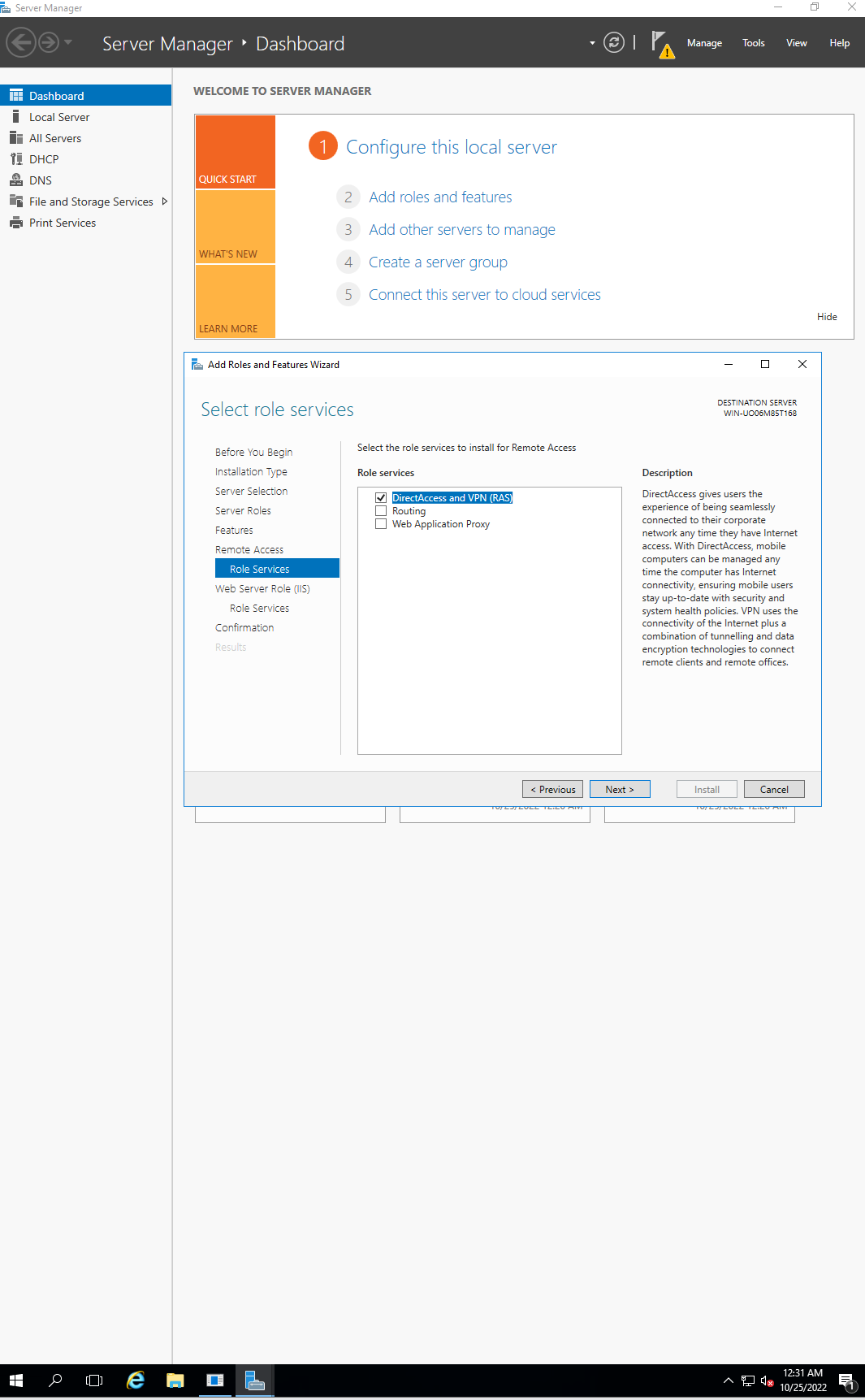
**Requirements**: Take Screenshots on Step 8, 14, 24 and 31.

1. Open Server Manager, if it is not open.
2. Click Manage and click Add Roles and Features.
3. If you see the Before you begin window, click Next.
4. In the Select installation type window, ensure Role-based or feature-based installation is selected. Click Next.
5. Your server should be selected in the Select destination server window. Click Next.
6. Click the check box for **Network Policy and Access Services**.
7. Click Add Features to install the Network Policy and Access Services Tools in the Add Roles and Features Wizard dialog box.
8. Click the check box for **Remote Access** in the Select server roles window. The Network Policy and Access Services and Remote Access roles should now be selected. Click Next.



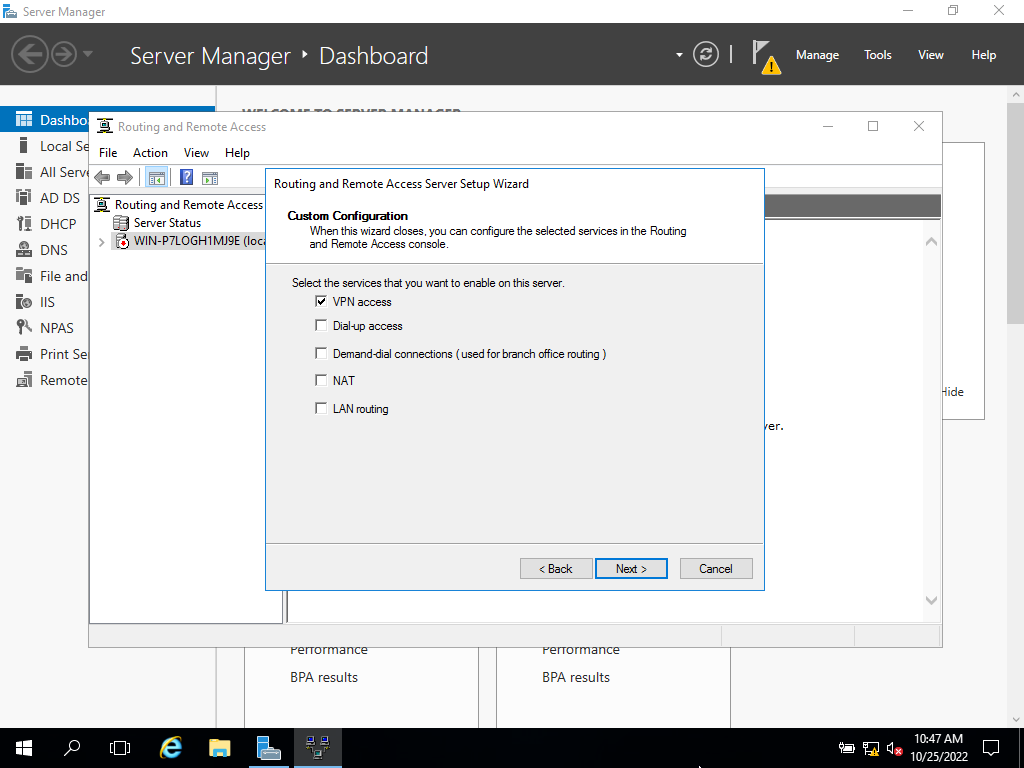
**Figure 1.0 Add Remote Access and Network Policy and Access Services**

1. Click Next in the Select features window.
2. Read the introductory information in the Network Policy and Access Services window. Click Next.
3. Read the introductory information in the Remote Access window. Click Next.
4. Click the box for **DirectAccess and VPN (RAS)** in the Select role services window.
5. Click Add Features in the Add Roles and Features Wizard dialog box.
6. Click Next in the Select role services window.



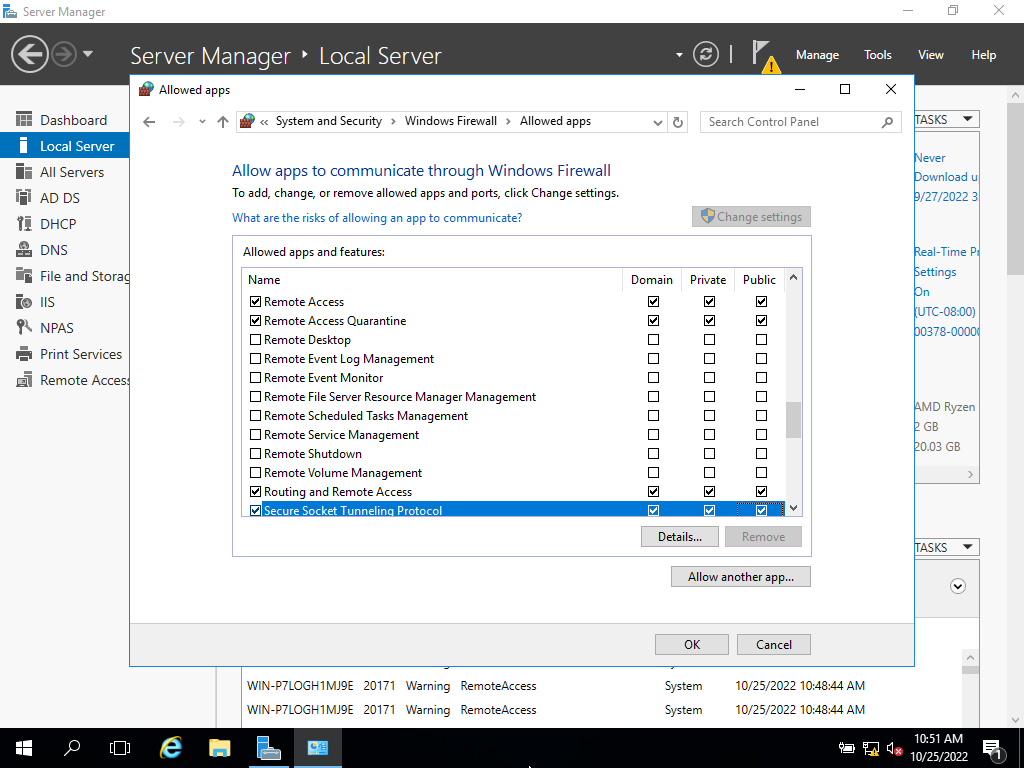
**Figure 1.1 Add DirectAccess and VPN (RAS)**

1. Click Install.
2. Make sure the installation succeeded in the Installation progress window and then click Close.
3. Open Server Manager, if it is not open.
4. Click the exclamation point near Manage in the top part of the window.
5. Click Open the Getting Started Wizard.
6. In the Configure Remote Access window, select **Deploy VPN only**.
7. In the **Routing and Remote Access window**, right-click the server and click Configure and Enable Routing and Remote Access.
8. Click Next.
9. You can select from five options. Click Custom configuration. Click Next.
10. Click VPN access.



**Figure 1.2 Add VPN access**

1. Click Next.
2. Click Finish.
3. If you see the Routing and Remote Access box, click OK.
4. Click Start service to start the Routing and Remote Access service. (Wait for a while to start the service, and then go to next step, maybe around 30s)
5. Click Local Server from Server Manager in the left pane and in the right pane within the **PROPERTIES** box, click the **Windows Firewall** parameter, such as Domain: On.
6. In the Windows Firewall window, click Allow an app or feature through Windows Firewall.
7. In the Allowed apps window scroll to find **Remote Access** and ensure there is a check in its box and in the boxes for Domain, Private, and Public. Check the boxes for **Routing and Remote Access** and for **Secure Socket Tunneling Protocol**, if they are not checked. Make sure that Domain, Private, and Public are checked for these as well. Click OK.



**Figure 1.3 Check for Three Apps and Features**

1. Close the Windows Firewall window.

# Activity 8-2: Configuring a DHCP Relay Agent

**Time Required**: Approximately 25 minutes

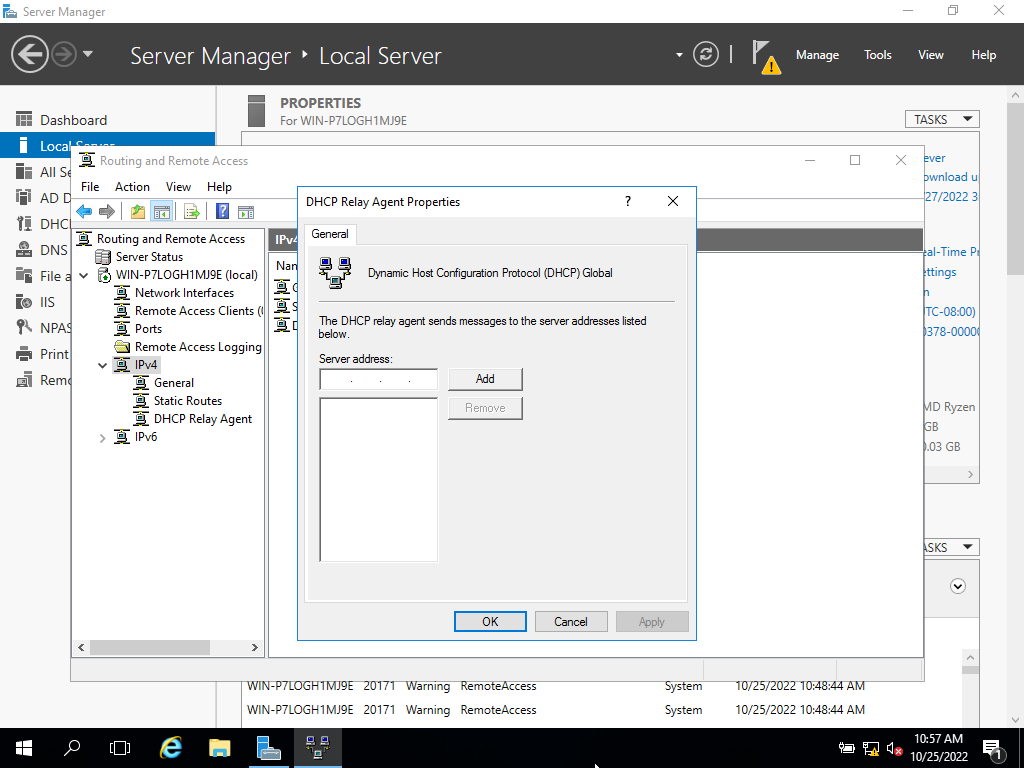
**Objective**: Set up a DHCP relay agent.

**Description**: In this activity, you configure the VPN server you set up to be a DHCP relay agent. Because you have already set up your server as a DHCP server in Activity 7, you can use the IP address of your server. Or ask your instructor what address to use for the DHCP server. (If you don’t know the address of your server, click Start and click the Windows Power- Shell tile, enter the command ipconfig, and record the IPv4 address.)

**Requirements**: Take screenshots on Step 4, 5, 13, 18, 20, 25, and answer question on

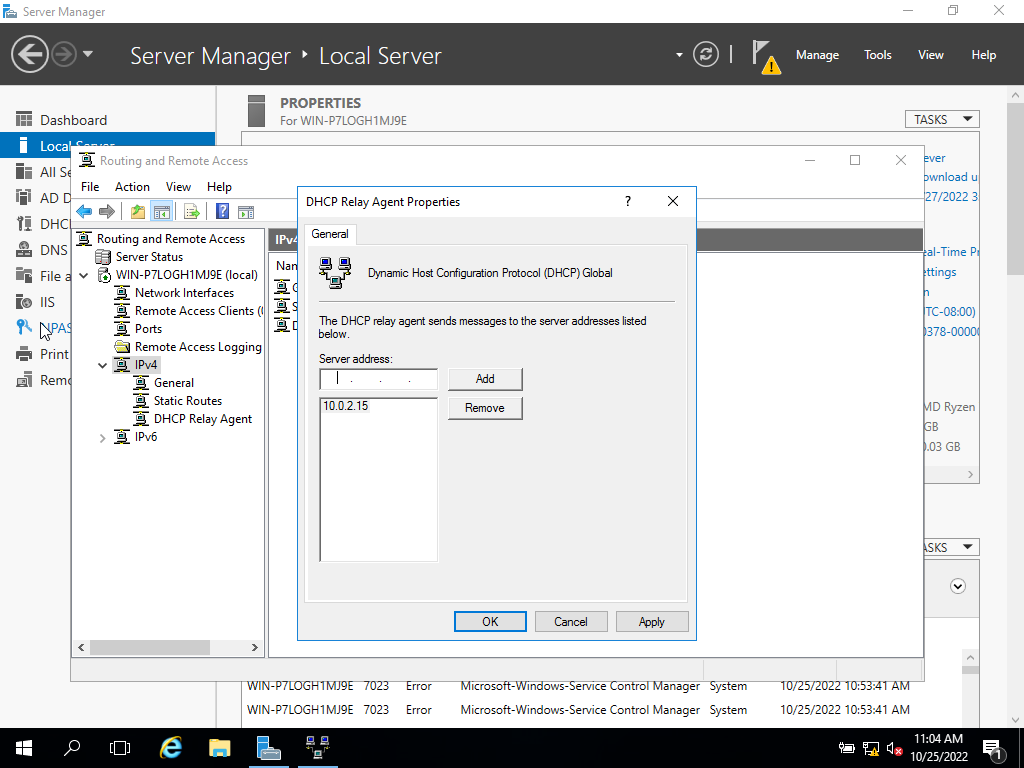
Step 22.

1. Access the Routing and Remote Access window, or if it is closed, access Server Manager, click Tools, and click **Routing and Remote Access**.
2. Double-click the name of the server in the tree in the left pane, if the items under the name are not displayed.
3. Double-click IPv4 in the tree.
4. In the left pane, right-click **DHCP Relay Agent**, and click Properties.



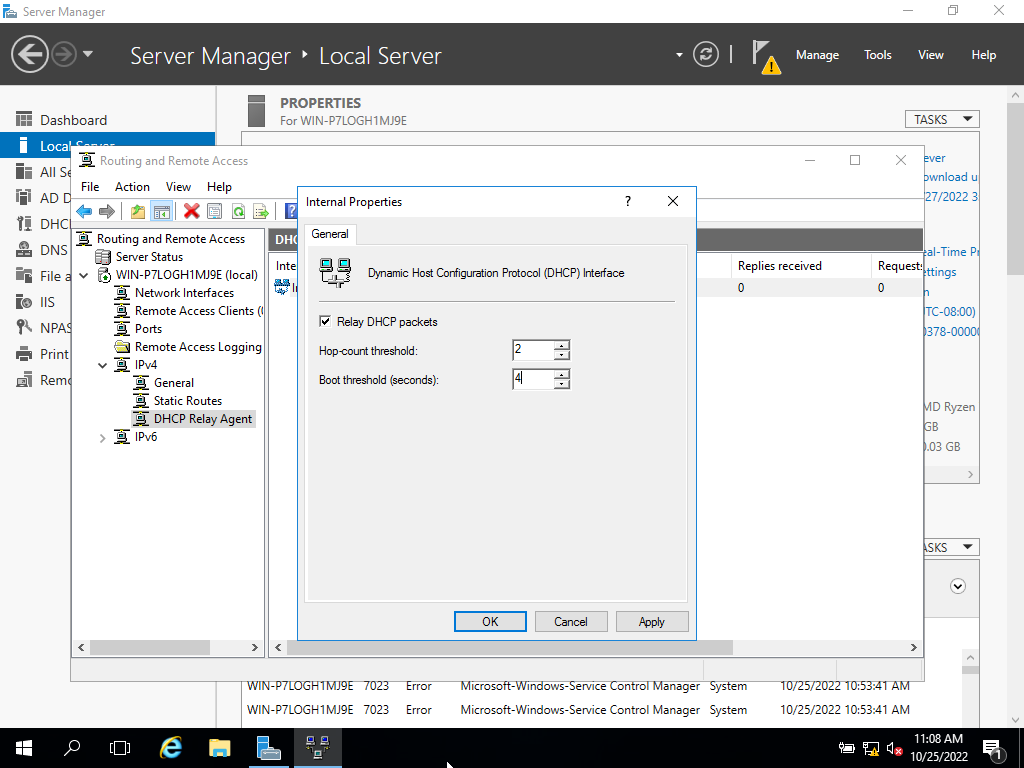
**Figure 2.0 the Detail of DHCP Relay Agent Properties**

1. In the Server address box within the DHCP Relay Agent Properties window, enter the IP address of the DHCP server and click Add. (If the DHCP server’s address has already been added automatically, you don’t need to put it in; otherwise add your current server’s private IP address)



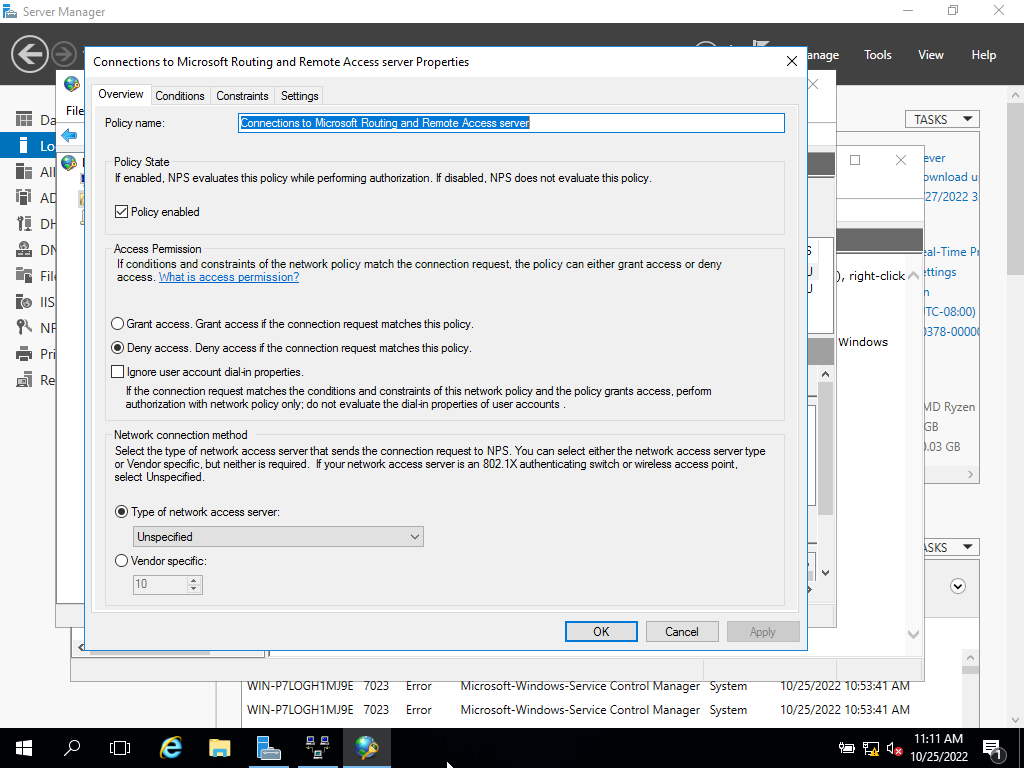
**Figure 2.1 Add IP Address**

1. Click OK.
2. Make sure the Routing and Remote Access window is open and that you see DHCP Relay Agent in the tree under IPv4.
3. Click DHCP Relay Agent in the tree.
4. In the right pane, right-click the interface, such as Internal and click Properties. (If no interface is shown, right-click DHCP Relay Agent, click New Interface, click an interface such as Internal, click OK, click OK, right-click the interface in the right pane, and click Properties.)
5. Be certain that the Relay DHCP packets box is checked.
6. In the Hop-count threshold text box, enter 2 for this activity. Note that the maximum number you can enter is 16.
7. If necessary, set the Boot threshold (seconds) value at 4 (the default). This parameter is used to give the DHCP server on the local network time to respond (in this case, four seconds) before a DHCP server on a remote network is contacted.
8. Click OK.



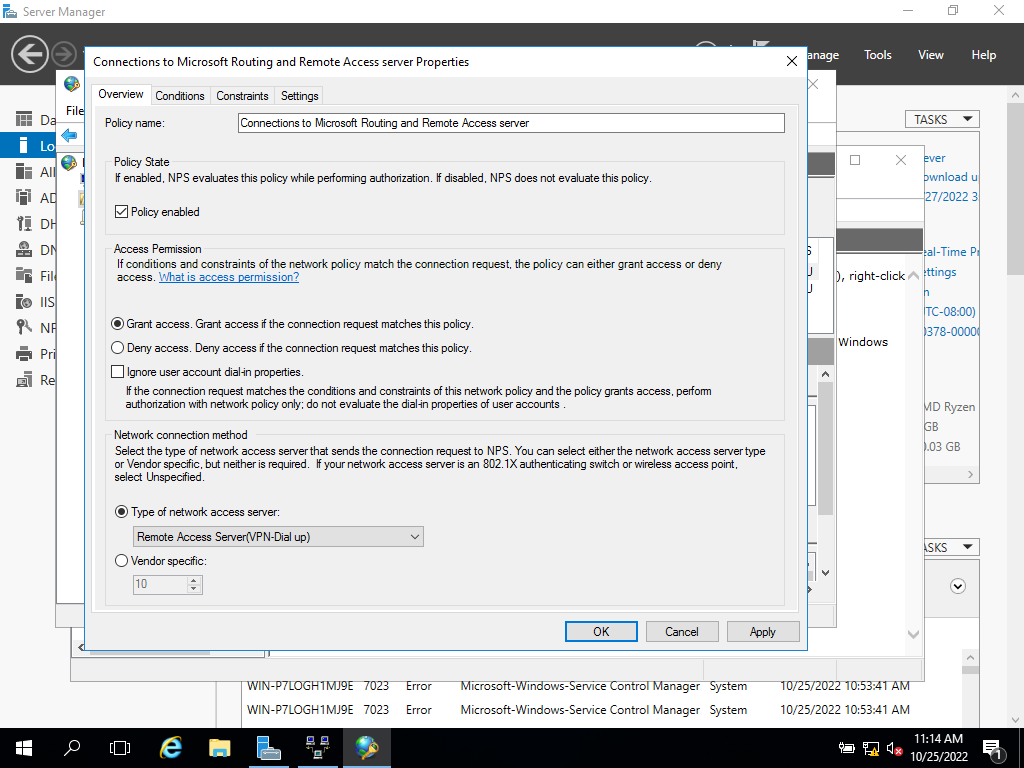
**Figure 2.2 Modify the Data**

1. Go to left panel of Routing and Remote Access window, click your server.
2. Make sure that the tree is expanded to show the elements under the server.
3. First click (to activate, if necessary) and then right-click the folder for **Remote Access Logging & Policies** and click Launch NPS.
4. Be sure that the **Network Policies** folder in the left pane is highlighted, or click it if it is not.
5. In the right pane, right-click **Connections to Microsoft Routing and Remote Access** server and click Properties.



**Figure 2.3 the Detail of Properties**

1. The Overview tab is displayed. In the Access Permission section, notice that access to the VPN server is denied by default. Click Grant access. Grant access if the connection request matches this policy.
2. Under the Network connection method section, make sure that Type of network access server is selected. Click the down arrow for the box associated with this option and click Remote Access Server (VPN-Dial up).



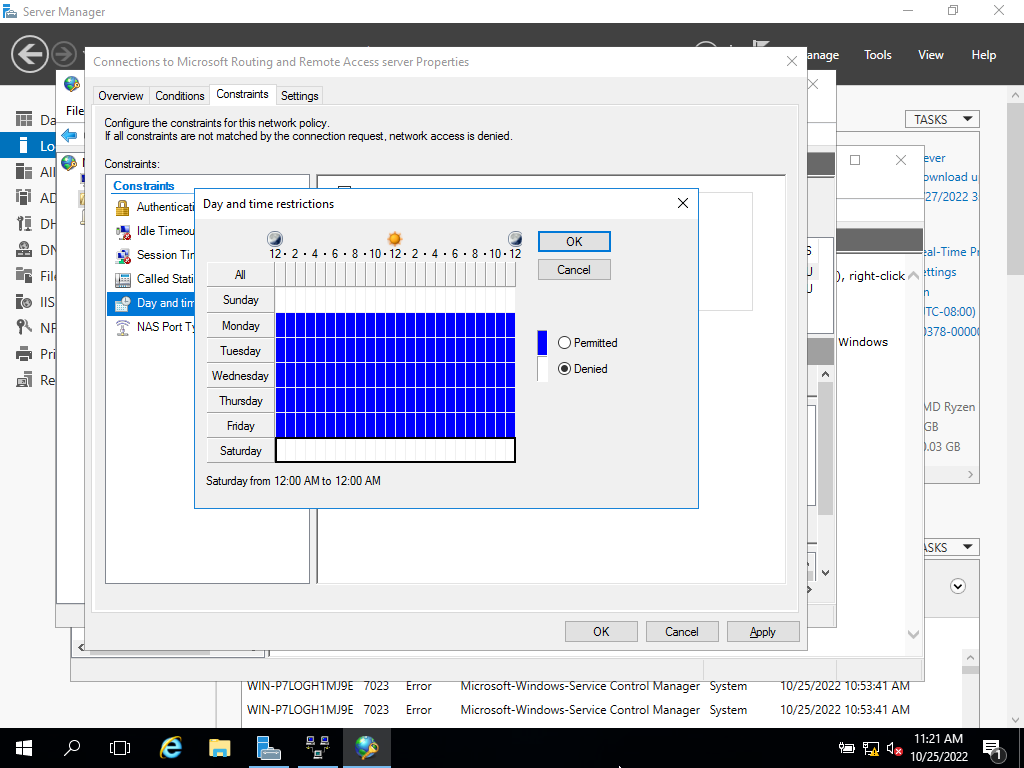
**Figure 2.4 Modify the Type of Overview Tab**

1. Click the Constraints tab.
2. In the left pane under Constraints, if necessary click Authentication Methods. Under EAP Types, notice that the two default selections are Microsoft: Secured password (EAP- MSCHAP v2) and Microsoft: Smart Card or other certificate.

* What options are selected by default under Less secure authentication methods?
* Answer:

‘User can change password after it has expired’ which is under ‘Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)’ and ‘Microsoft Encrypted Authentication (MS-CHAP)’.

1. In the left pane, click Idle Timeout. In the right pane, click Disconnect after the maximum idle time. Enter 30 in the box to configure this for 30 minutes. This action disconnects users who have been idle and helps reduce the connection load on the server.
2. Click Day and time restrictions in the left pane. In the right pane, click Allow access only on these days and at these times.
3. Click the Edit button in the right pane. Notice that all of the times are blocked out as Permitted. Click the left most block under 12 for the Sunday row of times and drag your pointing device to block all of Sunday. Click Denied. Next, click the left most block for the Saturday row of times and drag the cursor to highlight the entire row. Click Denied. This action secures the VPN server so that it cannot be accessed on the weekends. Click OK.



**Figure 2.5 Deny the Time in Sunday and Saturday**

1. Click NAS Port Type in the left pane. Under Common dial-up and VPN tunnel types, click Virtual (VPN). Also, under Common 802.1X connection tunnel types, make the selection appropriate to your type of network, such as Ethernet.
2. Click the Conditions and then the Settings tabs to see what they offer.
3. Click OK in the Connections to Microsoft Routing and Remote Access server Properties window to save your changes.
4. Close the Network Policy Server window.
5. Close the Routing and Remote Access window.

**Activity 8-3: Installing and Configuring Remote Desktop Services**

**Time Required**: Approximately 40 minutes

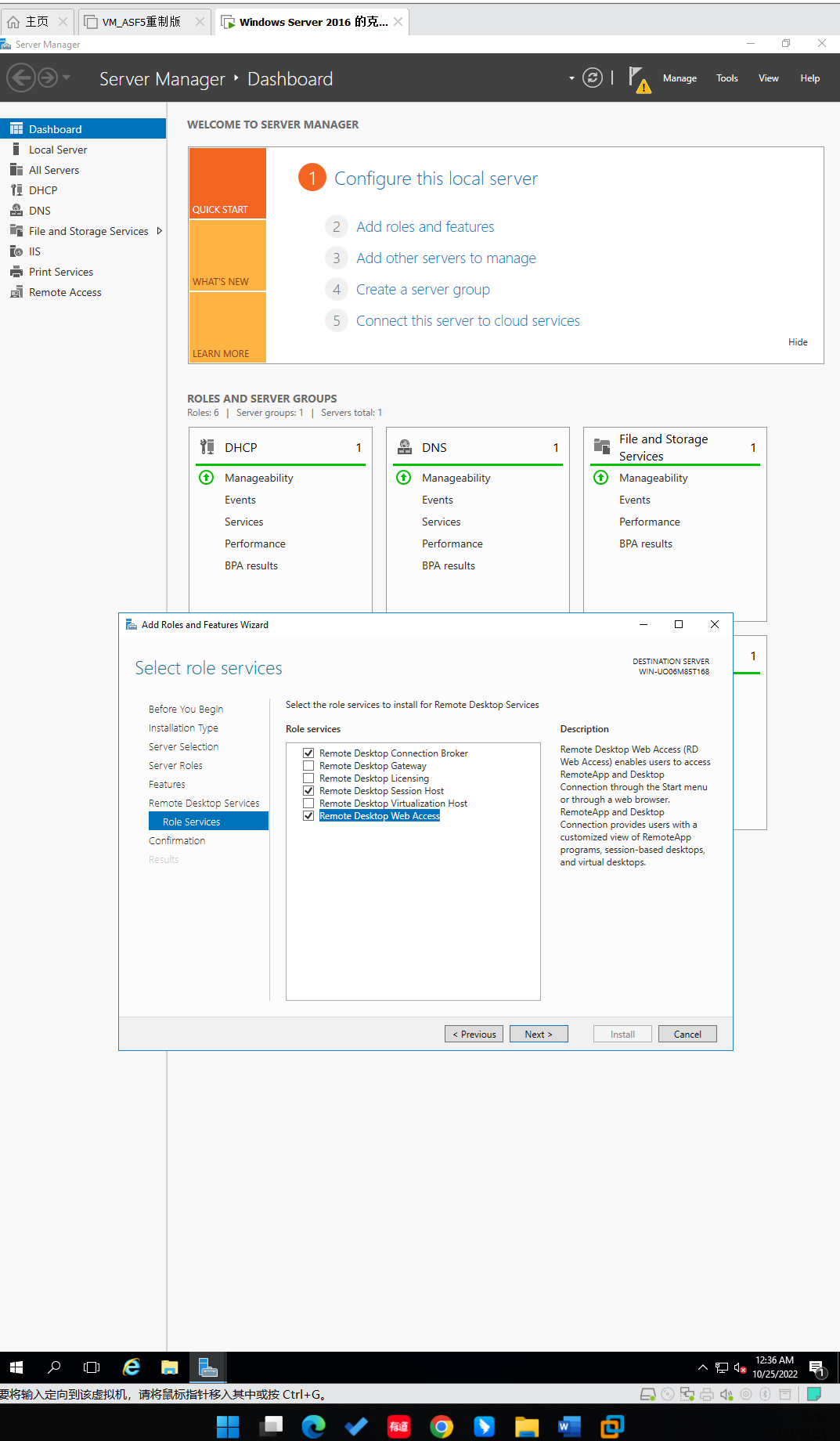
**Objective**: Learn how to install the Remote Desktop Services role.

**Description**: Using Remote Desktop Services can save a company money on client computer hardware, and it can be used for secure remote communications as an alternative to a VPN/ DirectAccess server. Further, it offers a sound way to manage which applications users can access and how they use the applications. In this activity,

you install the Remote Desktop Services role. You’ll need to restart the server after you install the role.

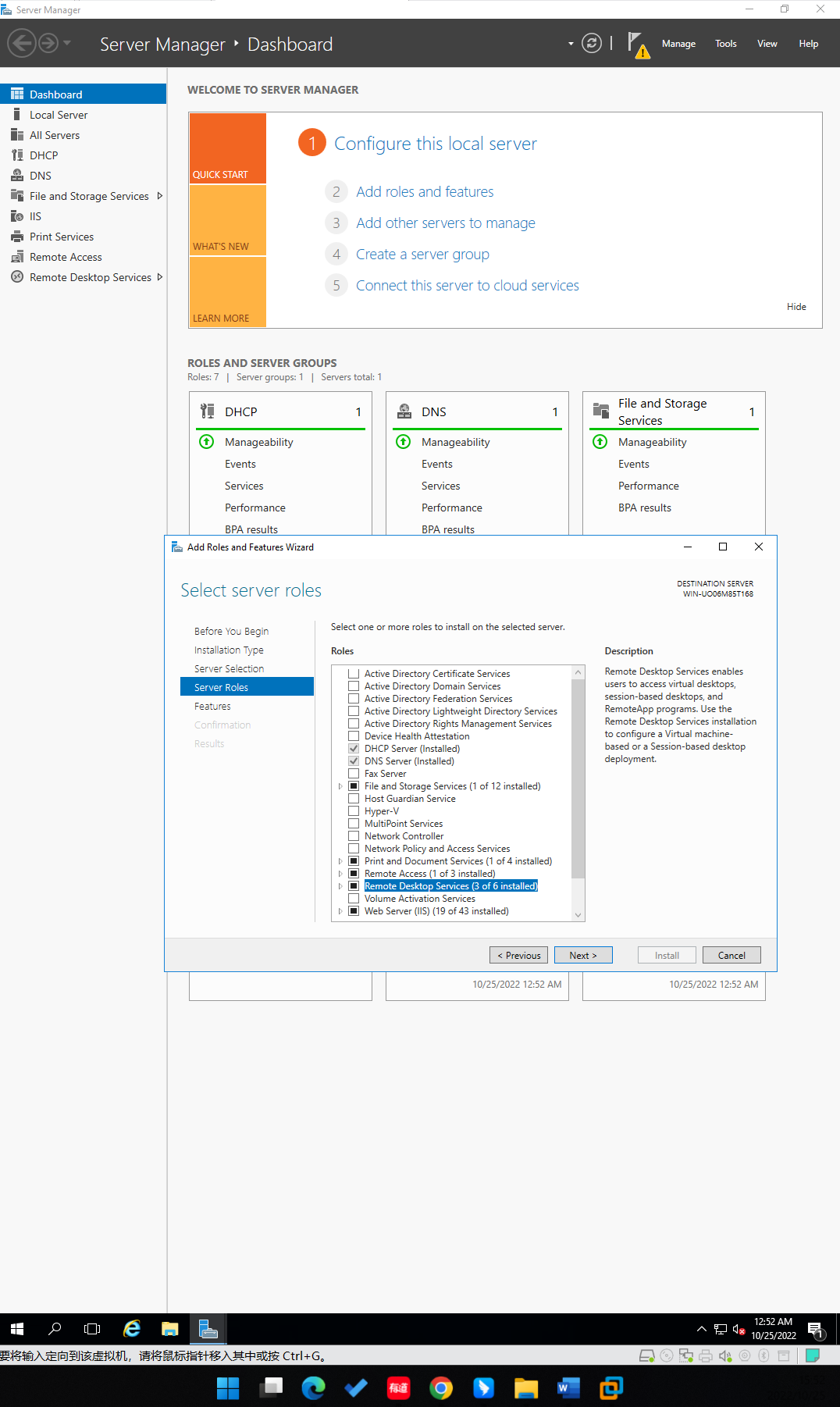
**Requirements**: Take screenshots on Step 14, 23, 24, 27, 30, 32, 36, 45 and 53, and answer question in Step 37.

1. Open Server Manager, if it is not open.
2. Click Manage and click Add Roles and Features.
3. If you see the Before you begin window, click Next.
4. Use Role-based or feature-based installation in the Select installation type window and click Next.
5. Make sure your server is highlighted in the Select destination server window and click Next.
6. In the Select server roles window, click the check box for Remote Desktop Services and click Next.
7. In the Select features window click Next.
8. Review the information about Remote Desktop Services and click Next.
9. In the Select role services window, click the check box for Remote Desktop Connection Broker.
10. Click the check box for Remote Desktop Web Access.
11. In the Add Roles and Features Wizard dialog box, click Add Features.
12. Click the check box for Remote Desktop Session Host.
13. In the Add Roles and Features Wizard dialog box, click Add Features.
14. Review your choices in the Select role services window and click Next.



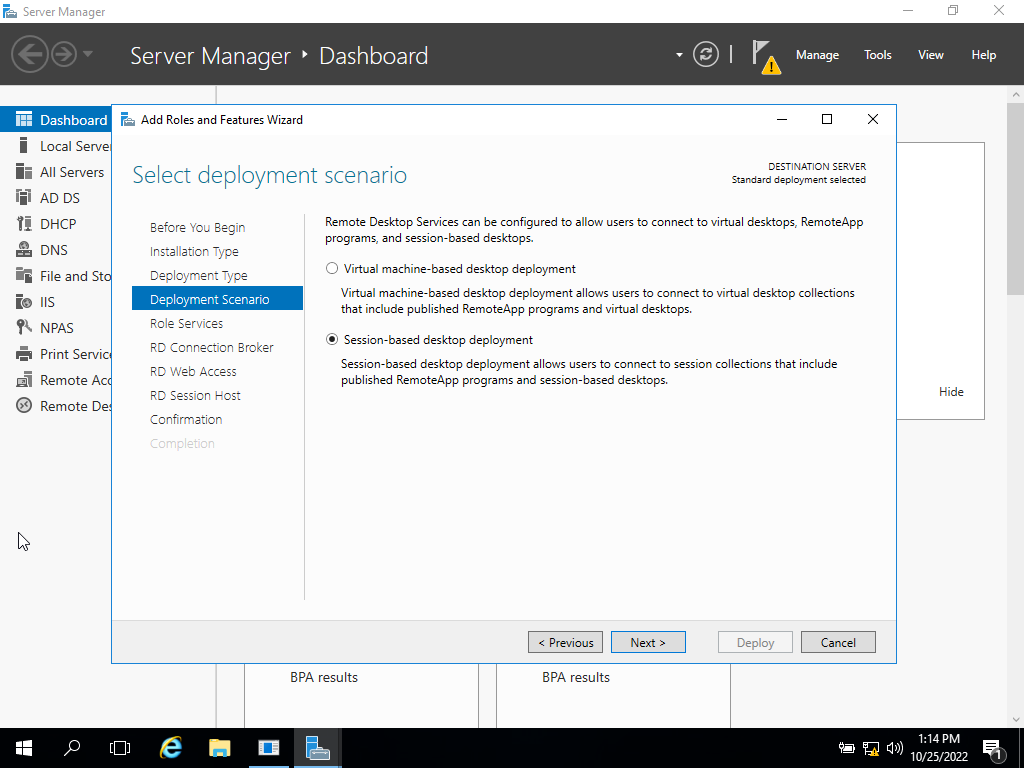
**Figure 3.0 Check the Three Services**

1. In the Confirm installation selections window, click Install.
2. Click Close when you see the message that you need to restart the server (under the blue bar).
3. Right-click the Start button, point to Shut down or sign out, and click Restart.
4. Specify the reason for the restart and click Continue. Wait for the server to restart and sign back in.
5. Open Server Manager, if necessary.
6. Click Manage and click Add Roles and Features.
7. If you see the Before you begin window, click Next.
8. Click Remote Desktop Services installation and click Next.
9. Ensure Standard deployment is selected in the Select deployment type window. Click Next.

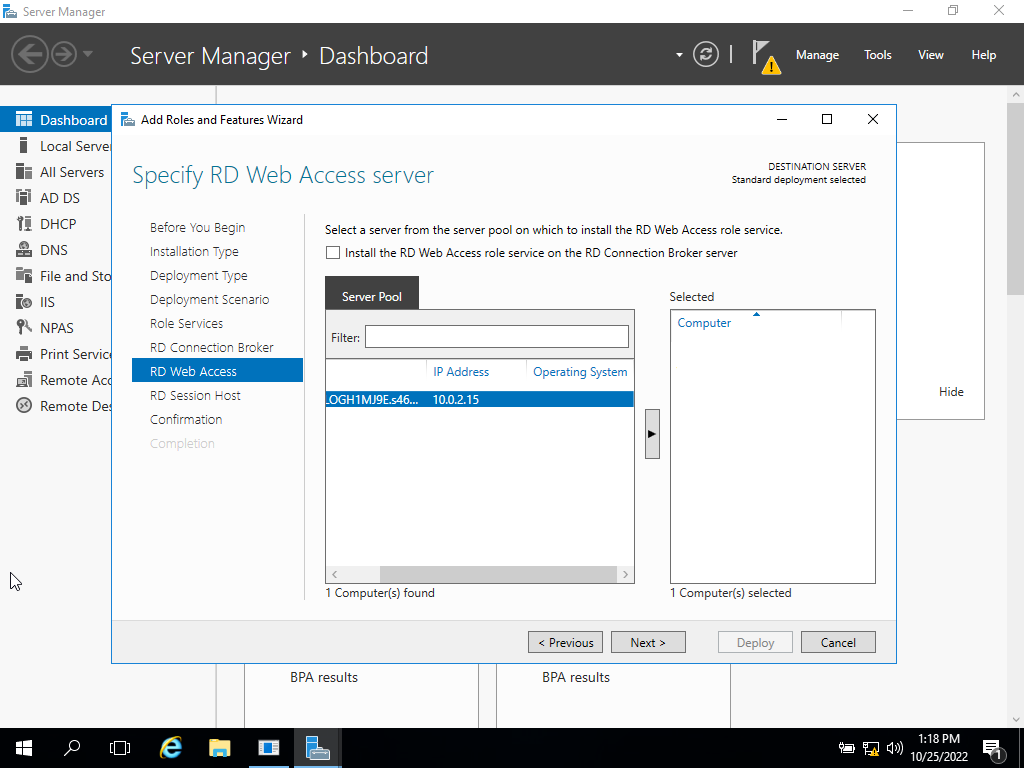


**Figure 3.1 Select Standard Deployment**

1. Click Session-based desktop deployment in the Select deployment scenario window and click Next.

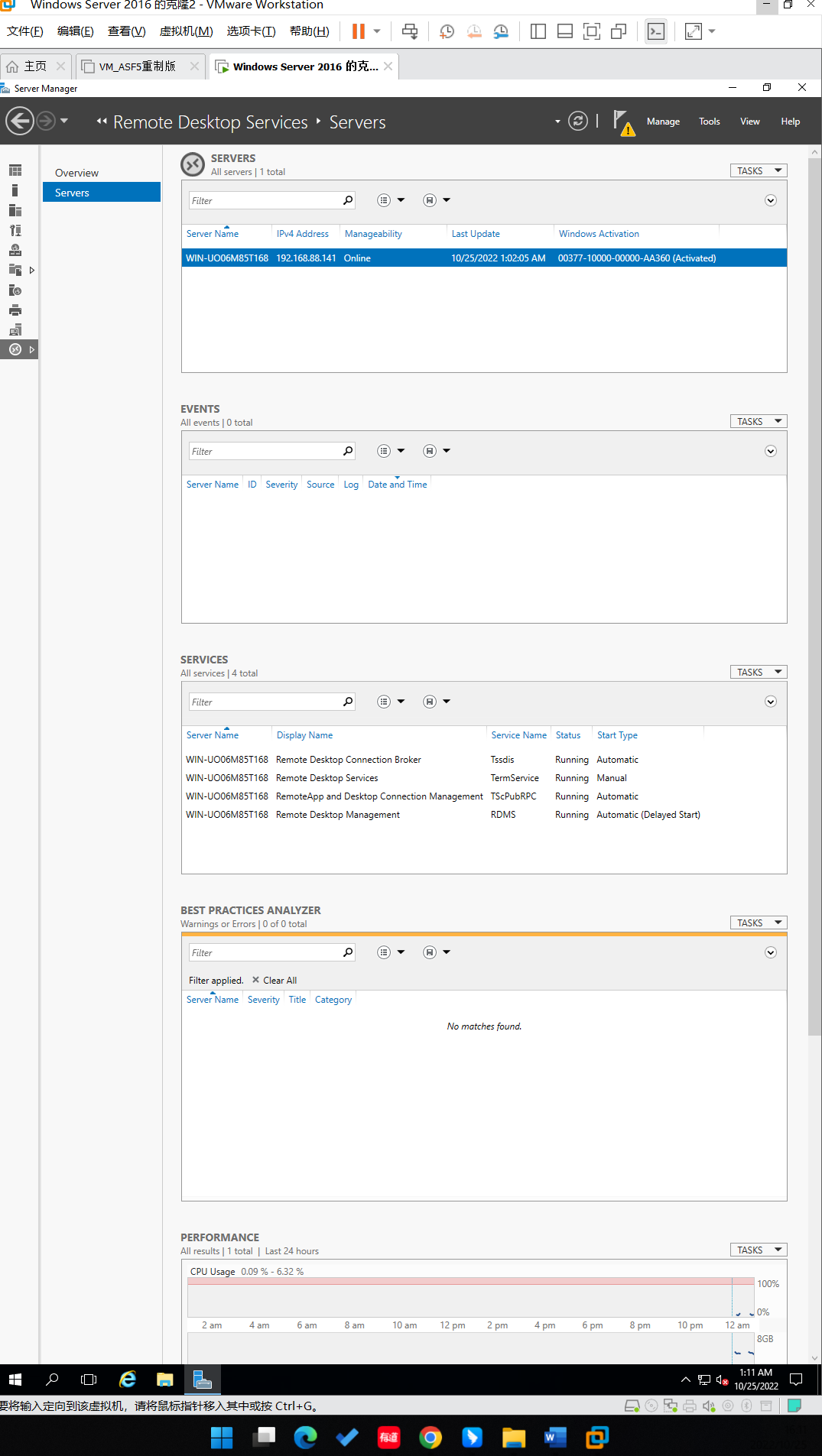
 **Figure 3.2 Select Session-Based Desktop Deployment**

1. In the Review role services window, notice that the role services listed are those you selected earlier: Remote Desktop Connection Broker, Remote Desktop Web Access, and Remote Desktop Session Host. Click Next.
2. Use your server as the selected broker server in the Server Pool box within the Specify RD Connection Broker server window; and, if necessary, click the right- pointing arrow between the boxes to add your server to the Selected box. Click Next.
3. Ensure your server is selected in the Specify RD Web Access server window in the Server Pool box. Click the right-pointing arrow between the boxes to add your server to the Selected box. Click Next.



**Figure 3.3 Select the Computer**

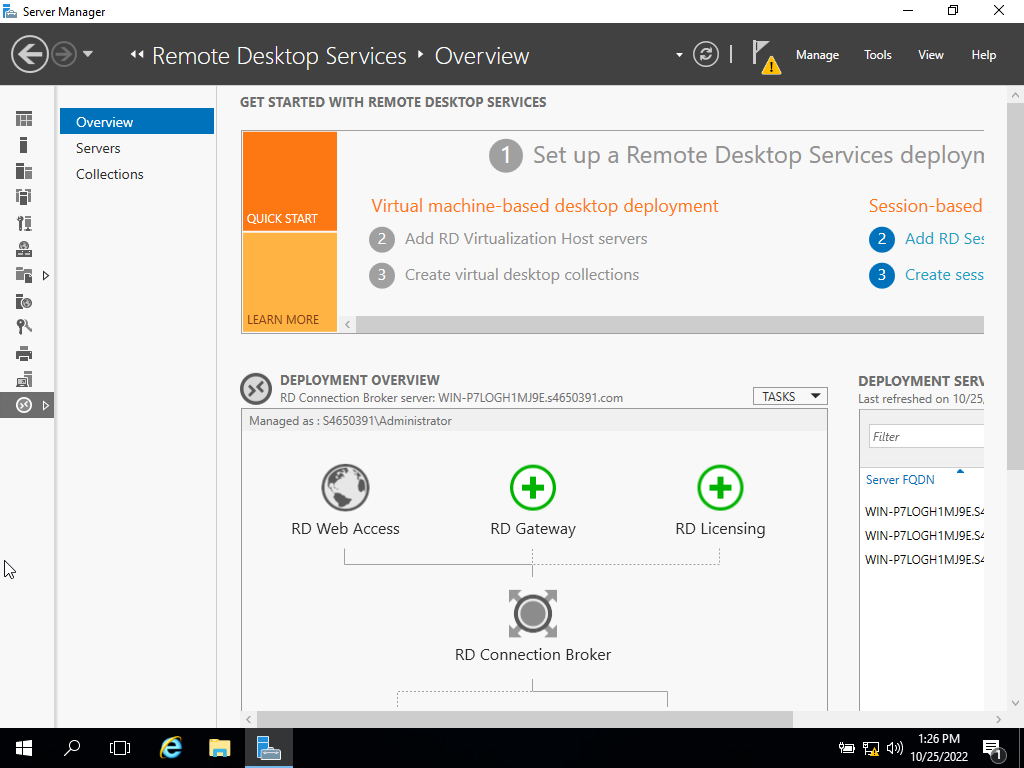
1. Be sure your server is selected in the Specify RD Session Host servers window in the Server Pool box. Click the right-pointing arrow between the boxes to add your server to the Selected box. Click Next.
2. In the Confirm selections window, click the check box for Restart the destination server automatically, if required. Click Deploy.
3. In the View progress window, wait for the three role services to finish installing. Click Close.



**Figure 3.3 Install the Three Services**

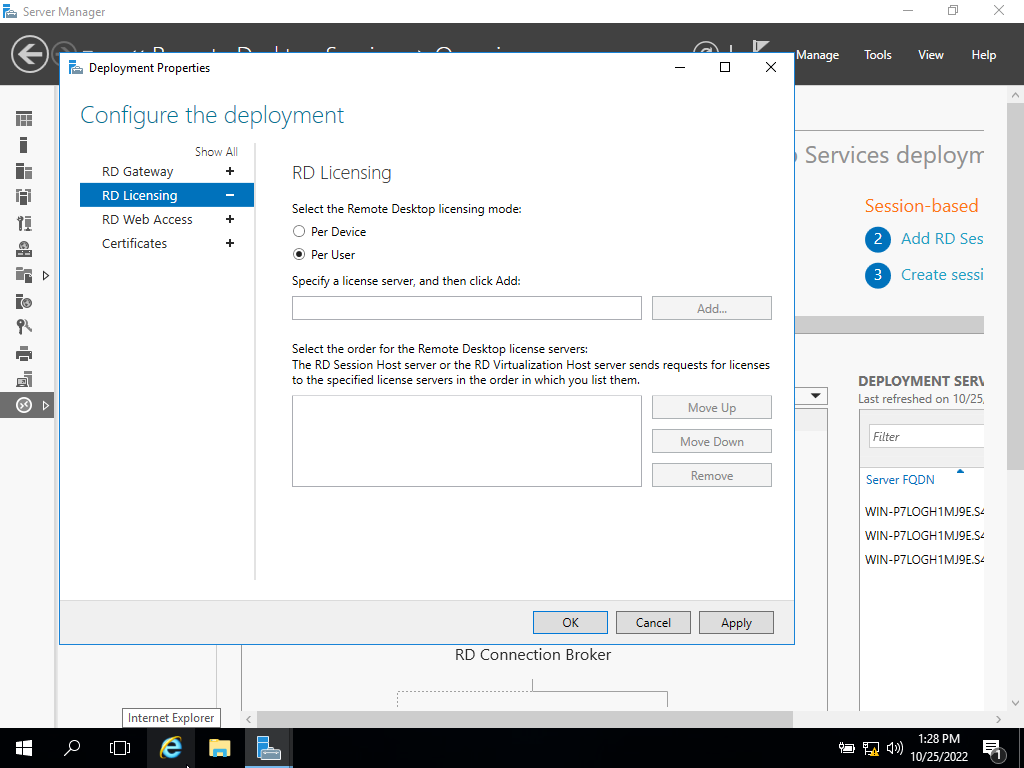
1. Restart the server. Right-click the Start button, point to Shut down or sign out, and click Restart. Specify the reason for the restart and click Continue.
2. Open Server Manager, if it is not open. In the left pane, click Remote Desktop Services to see the Overview window.

(You may need to click Remote Desktop Services again after it connects.)



**Figure 3.4 the Overview of Remote Desktop Services**

1. Notice that in the QUICK START section you have already completed the first step, which is to set up the RDS deployment. Also, you can decide to add RD session host servers or virtualization host servers (additional servers) in the second step, and you can create session collections or virtual desktop collections in the third step, which consists of pointing to disks that contain user profiles to be used. In this activity, we omit these last two steps because you can still have a basic setup without them.
2. Click the down-arrow for TASKS for the DEPLOYMENT OVERVIEW box, and click Edit Deployment Properties.
3. In the Configure the deployment box, leave Do not use an RD Gateway server selected as the default.
4. In the left pane, click RD Licensing. For this activity, select Per User.



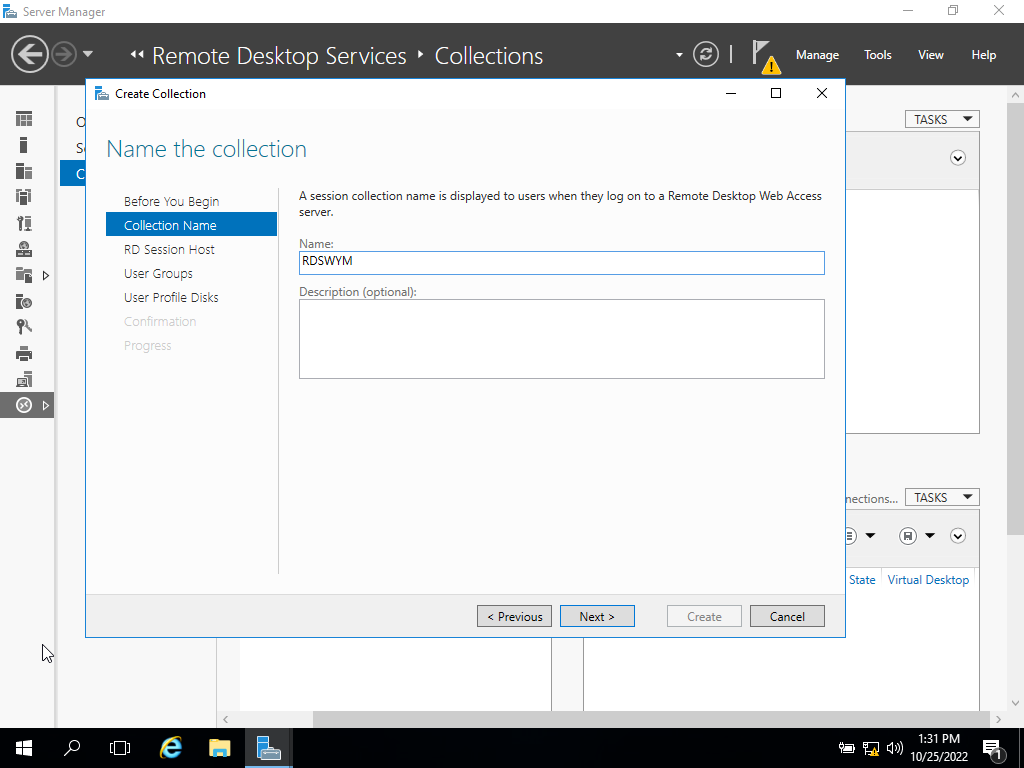
**Figure 3.5 Select Per User**

1. Click RD Web Access in the left pane.

* What server is the default selection for web access?
* Answer:

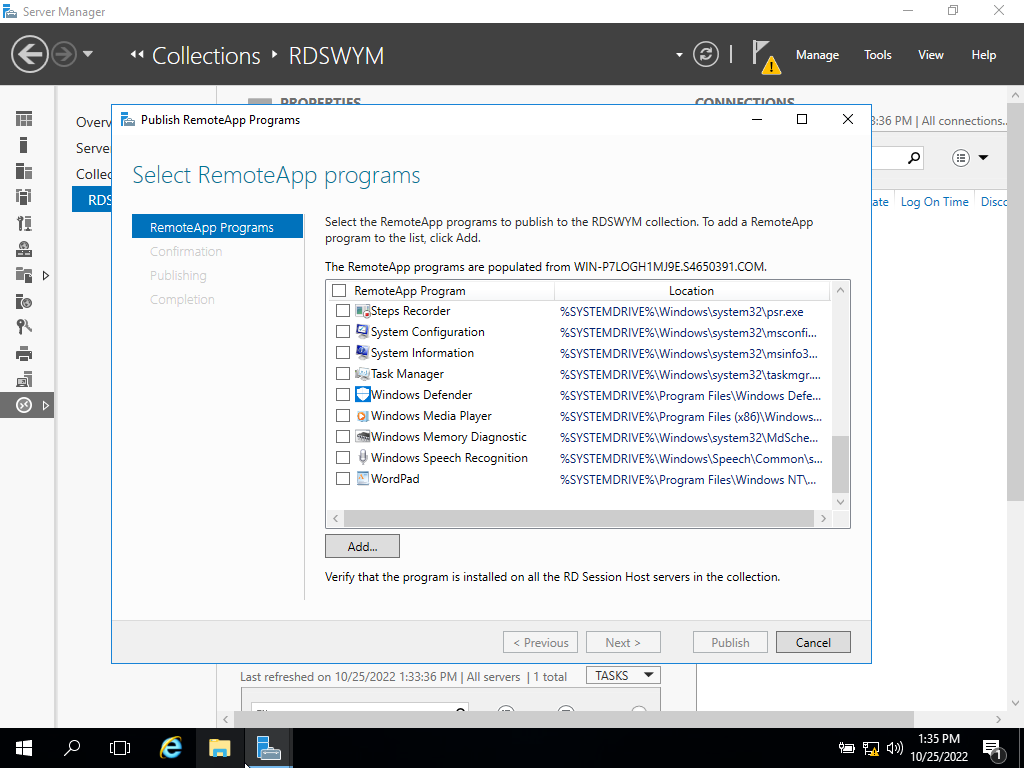
WIN-P7LOGH1MJ9E.S4650391.COM

1. In the left pane, click Certificates. The Manage certificates window enables you to configure a certificate for security and to specify the certificate level.
2. Click OK in the Deployment Properties window.
3. In the DEPLOYMENT OVERVIEW box, notice that you can further configure RD Gateway (with a green plus sign) to add an RD gateway to the deployment. Also, you can further con- figure RD Licensing to add additional licensing servers.
4. In the left pane of Server Manager, click Remote Desktop Services.
5. Click Collections on the left side of the window.
6. At the top of the window, click the down arrow for TASKS in the COLLECTIONS section and click Create Session Collection.
7. In the Before you begin window, click Next.
8. In the Name the collection window, enter a name for the collection, such as RDS plus your initials, such as RDSJR. Click Next.



**Figure 3.6 Add a Name**

1. In the Specify RD Session Host servers window, click the right-pointing arrow between the boxes to add your server to the Selected box. Click Next.
2. In the Specify user groups window, use the default Domain Users security group and click Next.
3. In the Specify user profile disks window, remove the check from the box for Enable user profile disks. Click Next.
4. In the Confirm selections window, click Create.
5. In the View Progress window, wait for the progress bars to complete and then click Close.
6. Now in Server Manager, the collection you created appears under Collections in the left side of the window. Click the collection, such as RDSJR.
7. At the top of the REMOTEAPP PROGRAMS box, click the down-arrow for TASKS and click Publish RemoteApp Programs.
8. Wait for a moment as the system finds programs that can be published and then scroll through the programs.



**Figure 3.7 Select RemoteApp programs**

1. Click the check box for Paint in the Select RemoteApp programs window. Click Next.
2. In the Confirmation window, click Publish.
3. In the Completion window, click Close.
4. Notice that the Paint program appears in the REMOTEAPP PROGRAMS box in Server Manager.
5. Close Server Manager.