**Lab 9 - Securing Windows Server 2016**

**Lab Assessment 3 Requirements:**

You are given time **until Friday 11:30pm** to complete Lab 09 on **a provided platform independently** without assistance from other people including your Lab Tutor and classmates:

1. Rename this word document as **Lab\_Assessment\_3\_YourName\_YourID.docx** where YourName is your real name and YourID is your VU Student ID with s.
2. In this lab assessment, you are required to **capture 13 screens (with figure captions) and answer 7 questions**. **All screen shots must show date and time from task bar**. Each is worth 5 points and make up a total of 100 points.
3. Capture the required screenshots and insert them underneath their step instructions. Then save to your file. Marks will be subject to quality of screenshots and figure captions.
4. Upon completion, upload the following **two files** via dropbox on VU Collaborate:
   1. **CoES Assignment Cover Sheet** and
   2. **Lab\_Assessment\_3\_YourName\_YourID.doc**

**Late Submission Penalty**

* 1-2 days – 10 points each day
* 3-6 days – 20 points each day
* After 6 days – **0** (**zero**) mark

**Deduction**

* Missing Cover Sheet – 5 points
* Wrong file name – 5 points
* Combined cover sheet file with Lab Assessment file – 5 points
* Missing figure numbers (step numbers) – 5 points
* Missing figure captions – 5 points
* Captured screens without task bar – up to 50 points

**Task 3 – Activity**

**Activity 10-1: Using the Group Policy Management Tool**

**Objective**: Learn how to use the Group Policy Management tool.

**Description**: Group Policy can be configured using the Group Policy Management tool and the Group Policy Management Editor. In this activity, you practice accessing features in the Group Policy Management tool and the Group Policy Management Editor. Also, for this activity, Internet Explorer Enhanced Security Configuration should be turned off (which is the default) to avoid viewing Internet Explorer security warnings. If you need to turn it back on after you finish the activities in this chapter, repeat Steps 1–3, but set it to On rather than Off.

**Requirements**: Take screenshots on **Steps 1.0, 1.12, 1.15, 1.20, and 1.25**, and answer questions in **Steps 1.10, 1.21, 1.31, and 1.42**.

**1.0** Open PowerShell prompt, type: **date; ipconfig /all** (two commands in one line) as below. Press **Enter**.

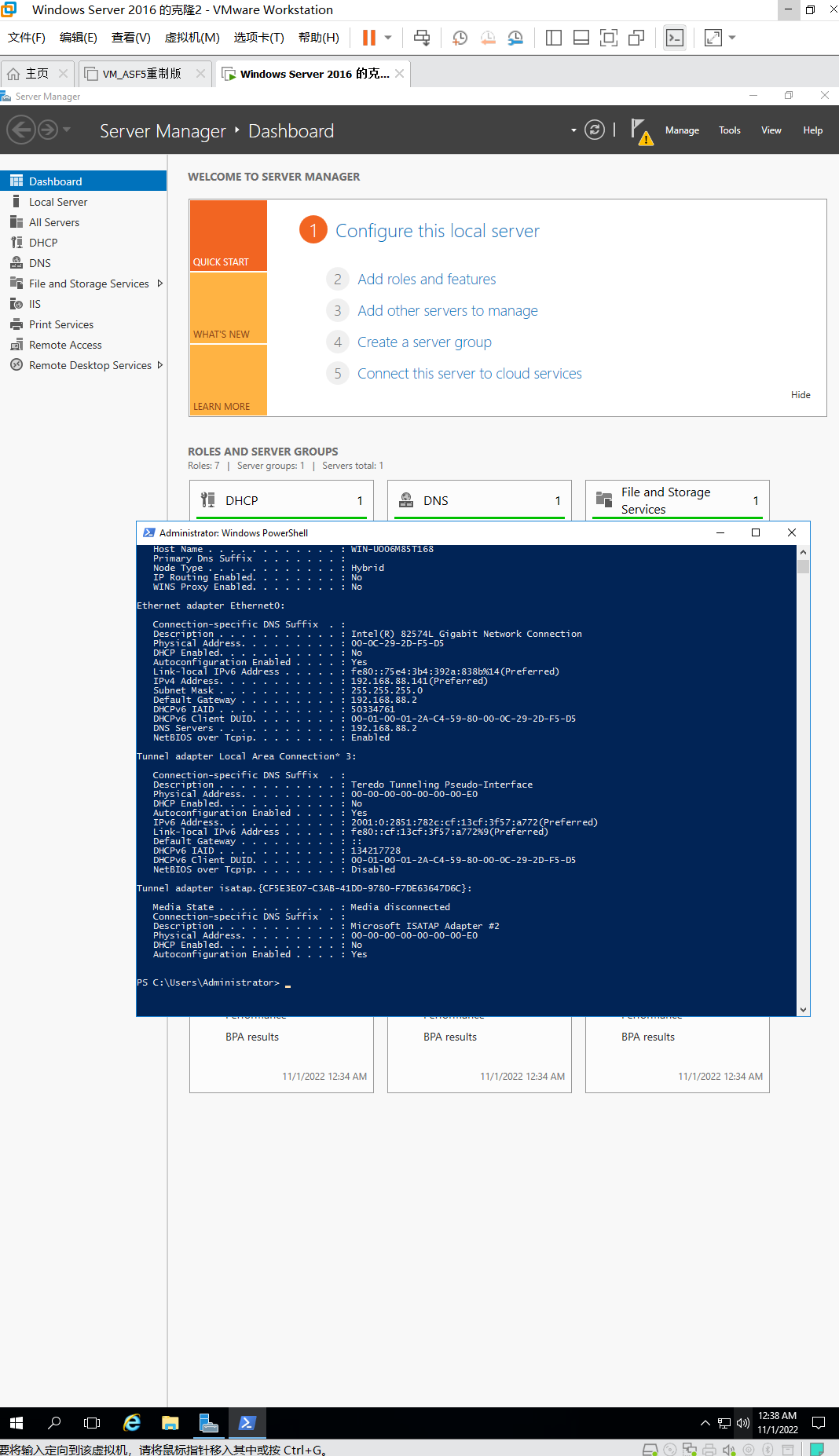


Figure 1.0 Windows Server 2016 Info 1 **Capture your screen, replace the above and save to your file.**

1.1 Open Server Manager, if it is not open.

1.2 Click Local Server in the left pane.

1.3 In the right pane, find IE Enhanced Security Configuration. If it is set to On, click On and in the Internet Explorer Enhanced Security Configuration dialog box, click Off for both Administrators and for Users. Click OK.

1.4 In Server Manager, click Tools and click Group Policy Management.

1.5 Click the right-pointing arrows to expand to see the items under Domains and then under the domain name, such as **YourID.com**.

1.6 Click Default Domain Policy and then click OK in the Group Policy Management Console box.

1.7 In the right pane, click the Settings tab.

1.8 In the right pane, click show for Windows Settings (under Computer Configuration => Policies), if necessary (do not click if it says hide, you can go between hide and show).

1.9 Click show for Security Settings under Windows Settings if the settings are not displayed.

**1.10** Click show for Account Policies/Password Policy.

• What is the minimum required length for a password? What is the maximum time a password can be used before the account holder needs to change the password?

**Answer**：The minimum required length for a password is 7 characters.

42 days is the maximum password age.

1.11 Right-click Default Domain Policy in the left pane and click Edit to open the Group Policy Management Editor.

**1.12** In the right pane, expand the tree under Computer Configuration to see Policies > Windows Settings>Security Settings > Account Policies.

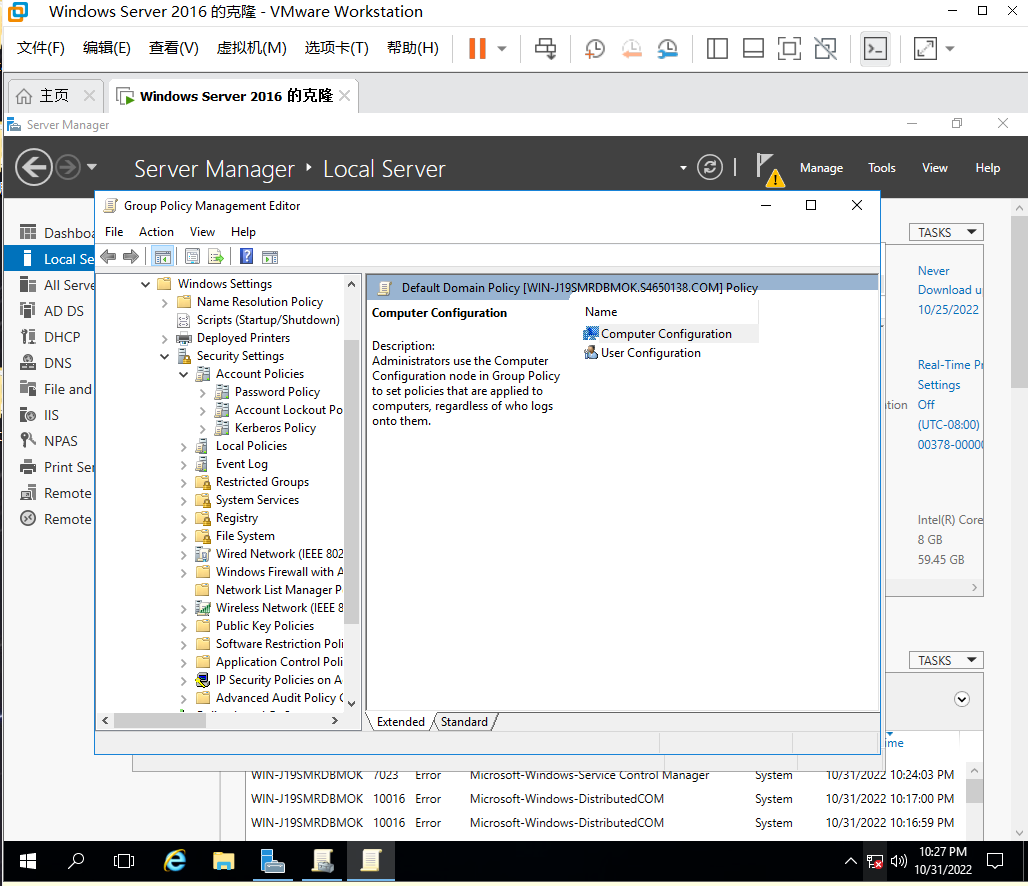


Figure 1.1 Expand Window settings

1.13 Click the down arrow for Account Polices in the left pane, to display the items under Account Policies. Click Password Policy.

1.14 Double-click Enforce password history in the middle pane. Ensure that Define this policy setting is checked. The default setting is 24 passwords remembered, which is the maximum. Assume you work for a company that has a policy to set this number at

**1.15** Enter 15 in the box. Click OK.

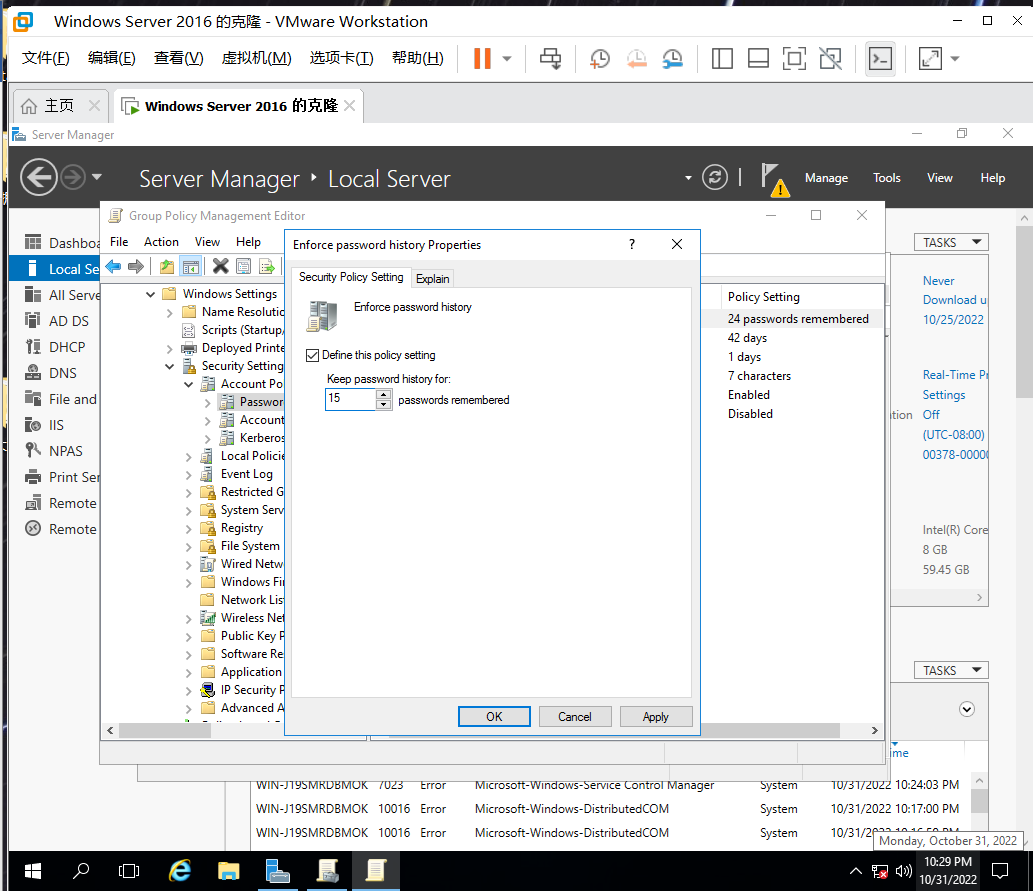


Figure 1.2 Change Enforce password history

1.16 Double-click Maximum password age and ensure that Define this policy setting is checked. Change the days text box to 60 and click OK.

1.17 Double-click Minimum password length. Be sure that Define this policy setting is checked and set the characters text box to 8. Click OK. The Default Domain Security Settings window should now look similar to the one.

1.18 Click Account Lockout Policy in the tree under Computer Configuration, Policies, Windows Settings, Security Settings, and Account Policies.

1.19 Double-click Account lockout duration in the right pane.

**1.20** Check the box for Define this policy setting, if it is not already checked. Enter 40 in the minutes text box, and click OK.

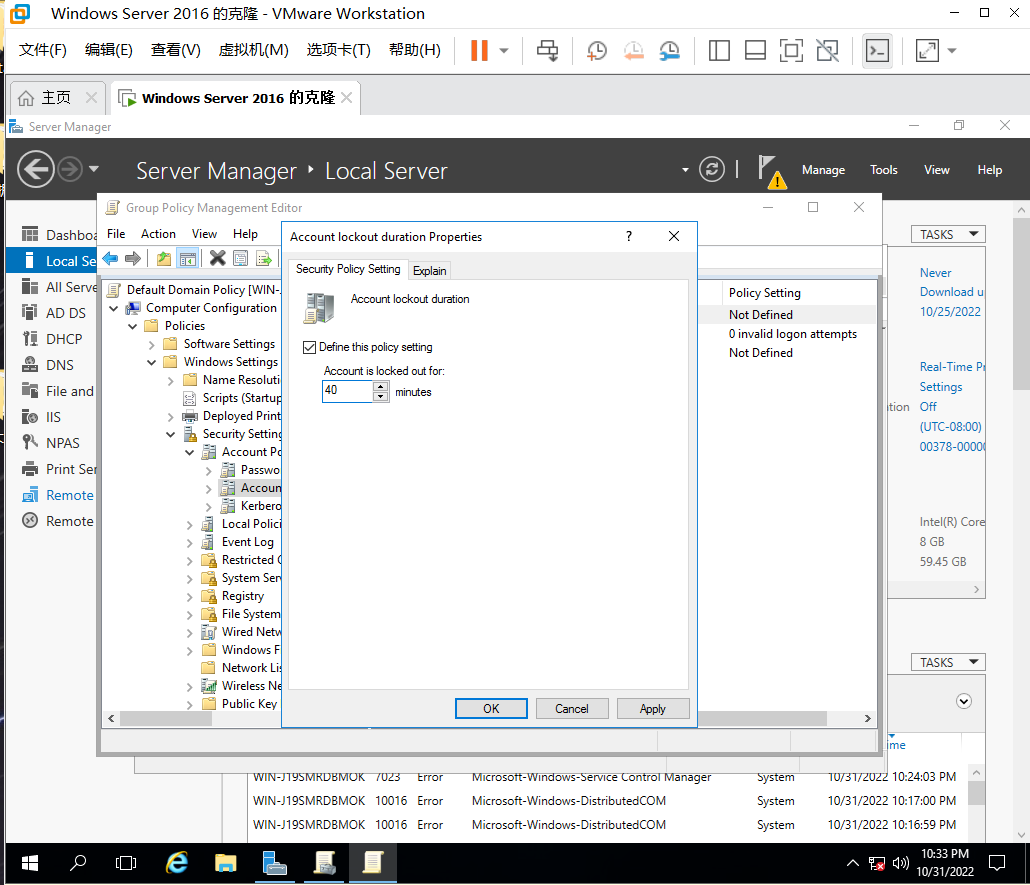


Figure 1.3 Define this policy setting

**1.21** You should see the Suggested Value Changes box.

• What changes are suggested?

**Answer: Account lockout threshold is suggested to change 0 invalid logon attempts to 5 invalid logon attempts. Reset account lockout counter after is suggested to 30 minutes**

1.22 Click OK in the Suggested Value Changes box. In the middle pane, notice that your change plus the suggested changes have been implemented.

1.23 Click Kerberos Policy in the tree under Computer Configuration, Policies, Windows Settings, Security Settings, and Account Policies.

1.24 Double-click Maximum lifetime for service ticket in the right pane. Ensure the box for Define this policy setting is checked. Enter 720 in the minutes text box. Click OK.

**1.25** Click OK in the Suggested Value Changes dialog box to also set Maximum lifetime for user ticket to 12 hours.

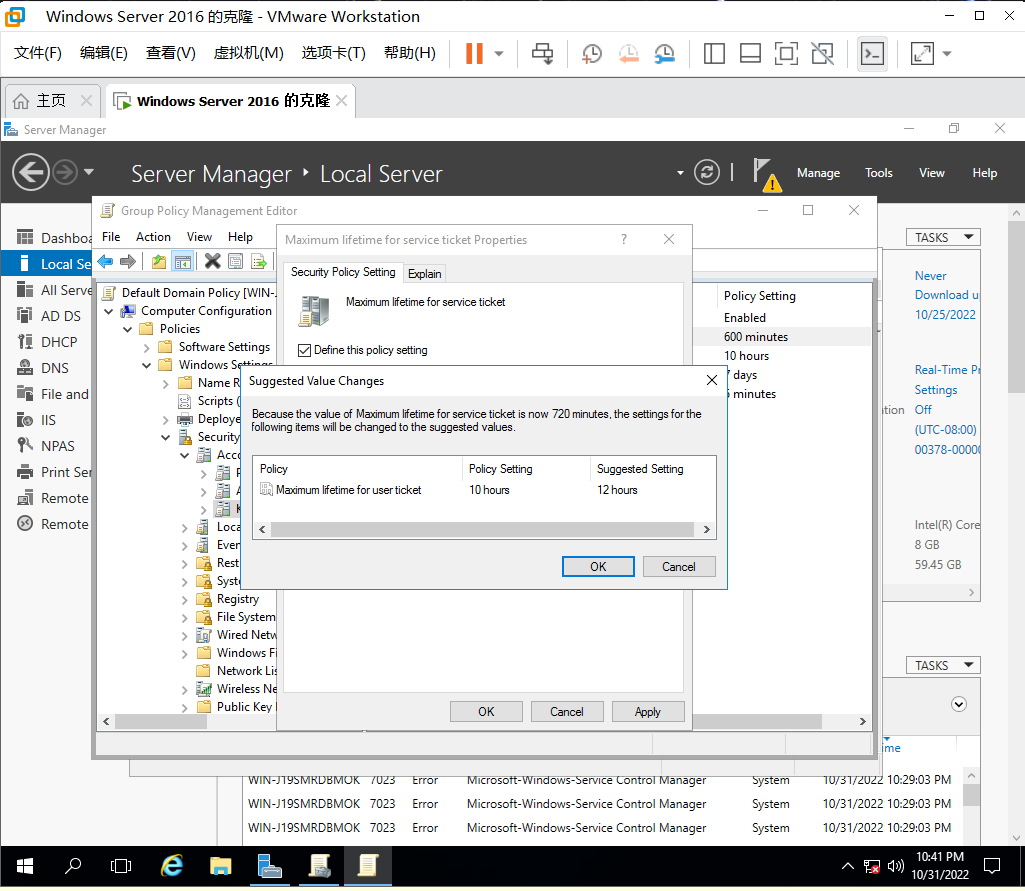


Figure 1.4 Maximum lifetime for user ticket Properties

1.26 Click the right-pointing arrow in front of Local Policies in the tree under Computer Configuration, Policies, Windows Settings, and Security Settings to display the items under Local Polices.

1.27 Click Audit Policy in the left pane.

1.28 Double-click Audit account logon events in the right pane.

1.29 Click the box for Define these policy settings.

1.30 Ensure that both the Success and Failure boxes are checked.

**1.31** Click Apply to have these take effect immediately and then click OK.

• If you were concerned about tracking changes to Group Policy, what would you audit?

**Answer: I will audit account logon events and directory service access and object access.**

1.32 Click User Rights Assignment in the left pane.

1.33 Scroll through the middle pane to view the rights that can be configured.

1.34 Double-click Allow log on locally.

1.35 Check the box for Define these policy settings.

1.36 Click Add User or Group.

1.37 Click the Browse button in the Add User or Group box.

1.38 Click the Advanced button in the Select Users, Computers, Service Accounts, or Groups dialog box.

1.39 Click the Find Now button in the Select Users, Computers, Service Accounts, or Groups dialog box.

1.40 Hold down the Ctrl key and click Student, Administrators, and Server Operators (you can release the Ctrl key temporarily to scroll to Server Operators). Ensure that Account Operators is not selected at the top of the listing. If it is selected, continue holding down the Ctrl key and click Access Control Assistance Operators to deselect it. Click OK.

1.41 Click OK in the Select Users, Computers, Service Accounts, or Groups dialog box.

**1.42** Click OK in the Add User or Group box.

• What now appears in the text box on the Allow log on locally Properties dialog box?

**Answer: They are Administrators and S4650138\Administrator and Server Operators.**

1.43 Click OK in the Allow log on locally Properties dialog box.

1.44 Double-click Shut down the system. Place a check in the box for Define these policy settings.

1.45 Click Add User or Group.

1.46 Click the Browse button in the Add User or Group box.

1.47 Click the Advanced button in the Select Users, Computers, Service Accounts, or Groups dialog box.

1.48 Click Find Now in the Select Users, Computers, Service Accounts, or Groups dialog box.

1.49 Double-click Administrators.

1.50 Click OK in the Select Users, Computers, Service Accounts, or Groups dialog box. 51. Click OK in the Add User or Group box.

1.52 Click OK in the Shut down the system Properties dialog box.

1.53 Close the Group Policy Management Editor window.

1.54 Close the Group Policy Management window, if it is still open.

**Activity 10-2: Using the Security Templates Snap-In**

**Objective**: Learn to use the Security Templates snap-in.

**Description**: In this activity, you learn how to use the Security Templates snap-in.

**Requirements**: Take screenshots on **Steps 2.0, 2.6, 2.22, 2.25, and 2.27**, and answer questions in **Step 2.9**.

**2.0** Open PowerShell prompt, type: **date; ipconfig** **/all** (two commands in one line) as below. Press **Enter**.

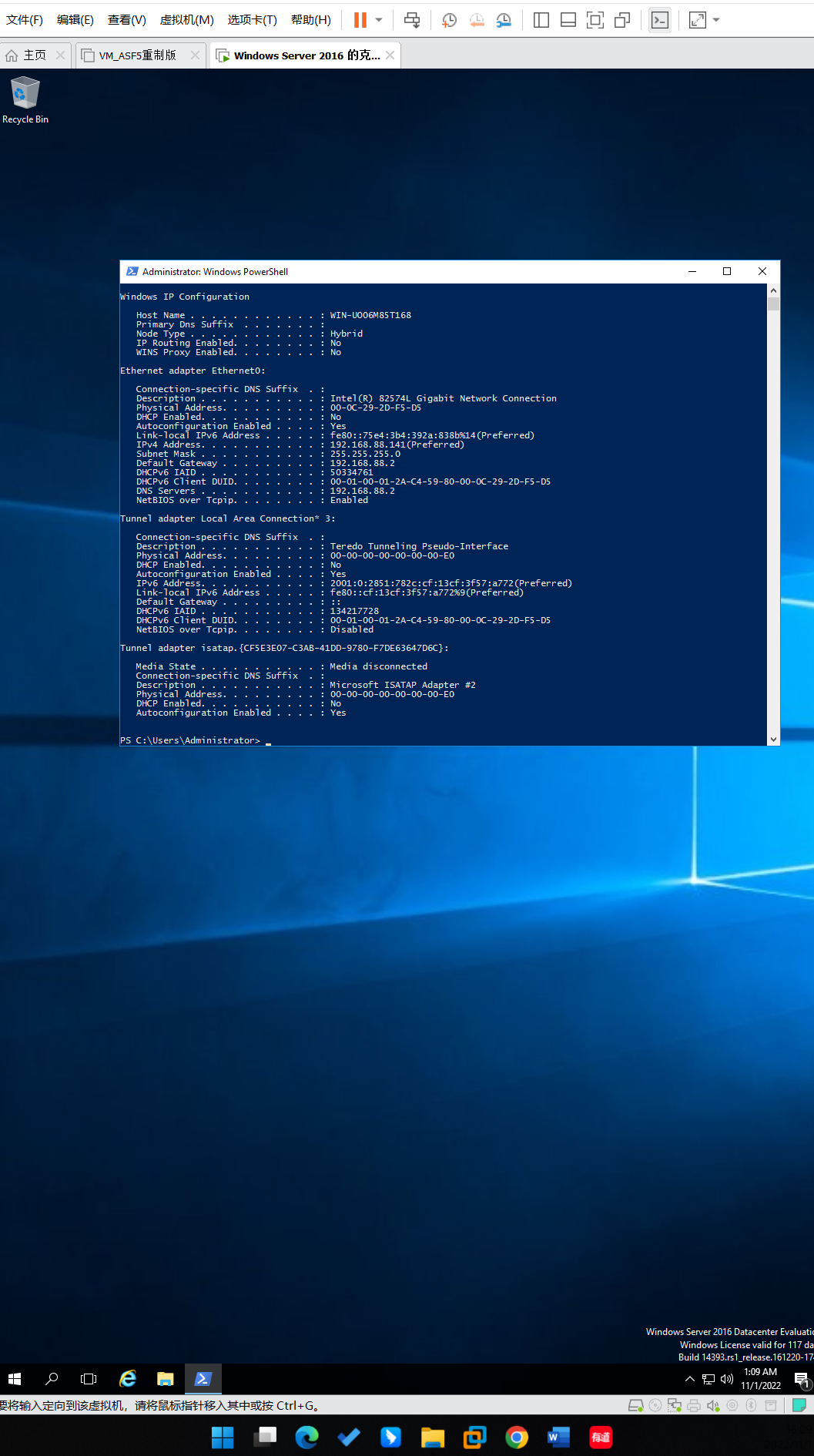


Figure 2.0 Windows Server 2016 Info 2 **Capture your screen, replace the above and save to your file.**

2.1 Right-click Start, click Run, type mmc in the Open text box and click OK.

2.2 Click File and click Add/Remove Snap-in.

2.3 In the Add or Remove Snap-ins dialog box, click Security Templates and click the Add button. Now click Security Configuration and Analysis and click the Add button.

2.4 Click OK.

2.5 Click Security Templates in the tree.

**2.6** In the middle pane, right-click the path to the Templates folder, such as C:\Users\Administrator\Documents\Security\Templates and click New Template.

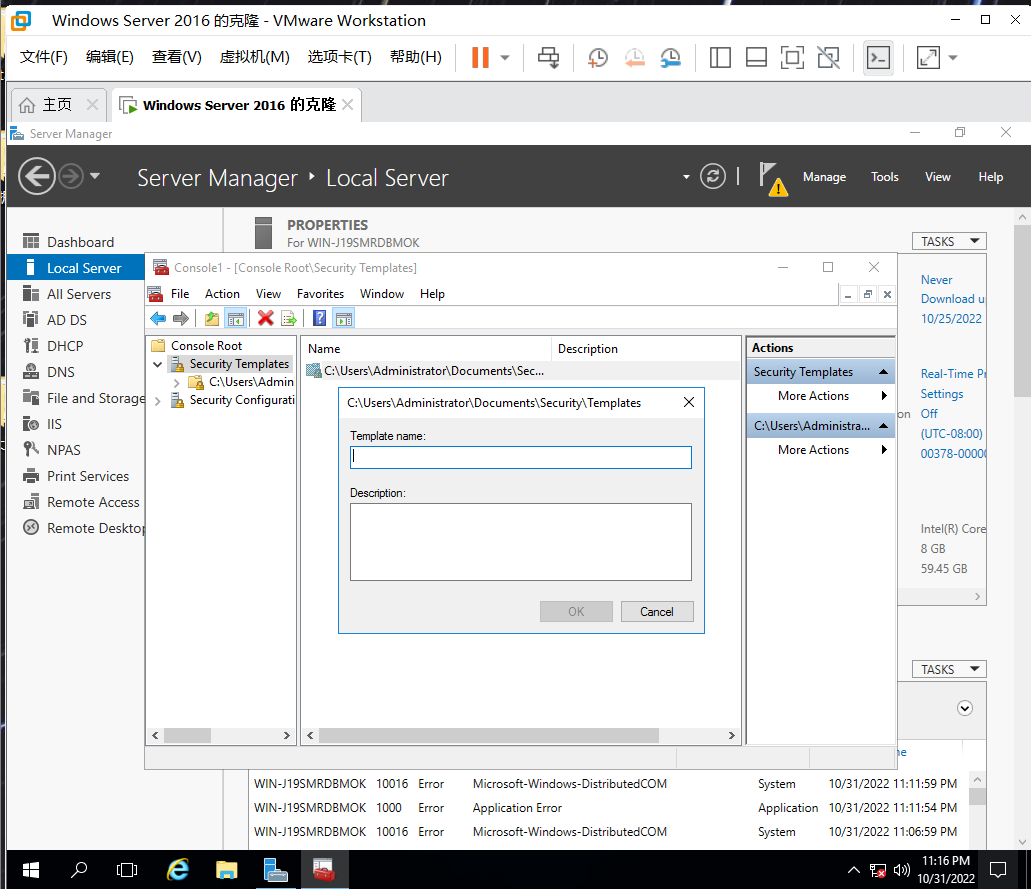


Figure 2.1 Right-click the path

2.7 In the Template name box, enter the word Template plus your first name, i.e. **TempYourFirstName**. In the Description box, enter Practice template. Click OK.

2.8 In the left pane under Console Root, Security Templates, click the path to the template in the tree, such as C:\Users\Administrator\Documents\ Security\Templates, to ensure the new template is displayed in the middle pane.

**2.9** Double-click the template name in the middle pane, such as **TempYourFirstName**.

• What Group Policy elements are displayed in the middle pane that you can now configure?

**Answer: There are Account Policies, Local Policies, Event Log.**

2.10 Double-click Account Policies in the middle pane.

2.11 Double-click Password Policy in the middle pane.

2.12 Configure Enforce password history to 20 passwords remembered and click OK in the Enforce password history Properties dialog box. Next, configure Maximum password age to 45 days. If you see the Suggested Value Changes box to set the Minimum password age to 30 days, click OK (or manually configure Minimum password age to 30 days). Further, configure Minimum password length to eight characters. If necessary you can position the cursor over the line in the box separating the middle pane from the right pane and drag the line to the right to view the settings for the parameters in the middle pane or maximize the window.

2.13 Click Account Lockout Policy in the tree.

2.14 Configure Account lockout duration to 40 minutes and after you click OK in the Account lockout duration Properties dialog box, click OK in the Suggested Value Changes dialog box to use the suggested values for Account lockout threshold (five invalid logon attempts) and Reset account lockout counter after (30 minutes), refer to Activity 9-1.

2.15 Click the template in the tree, such as **TempYourFirstName**. Configure any other policies as desired in the middle pane.

2.16 Close the console window and click Yes in the Microsoft Management Console window, click Desktop in the left pane of the Save As window, use the file name Security Tools plus your initials, such as Security Tools JR and click Save.

2.17 If you see the Save Security Templates box, click Yes.

2.18 From the desktop, open the Security Tools console you created.

2.19 Click Security Configuration and Analysis in the tree in the left pane.

2.20 Right-click Security Configuration and Analysis in the left pane and click Open Database.

2.21 In the File name text box, enter a database name consisting of Domain plus your first name, such as **DomainYourFirstName**, and then click Open.

**2.22** In the Import Template dialog box, notice that the template you created is listed. Click the template, such as **TempYourFirstName**, and click Open.

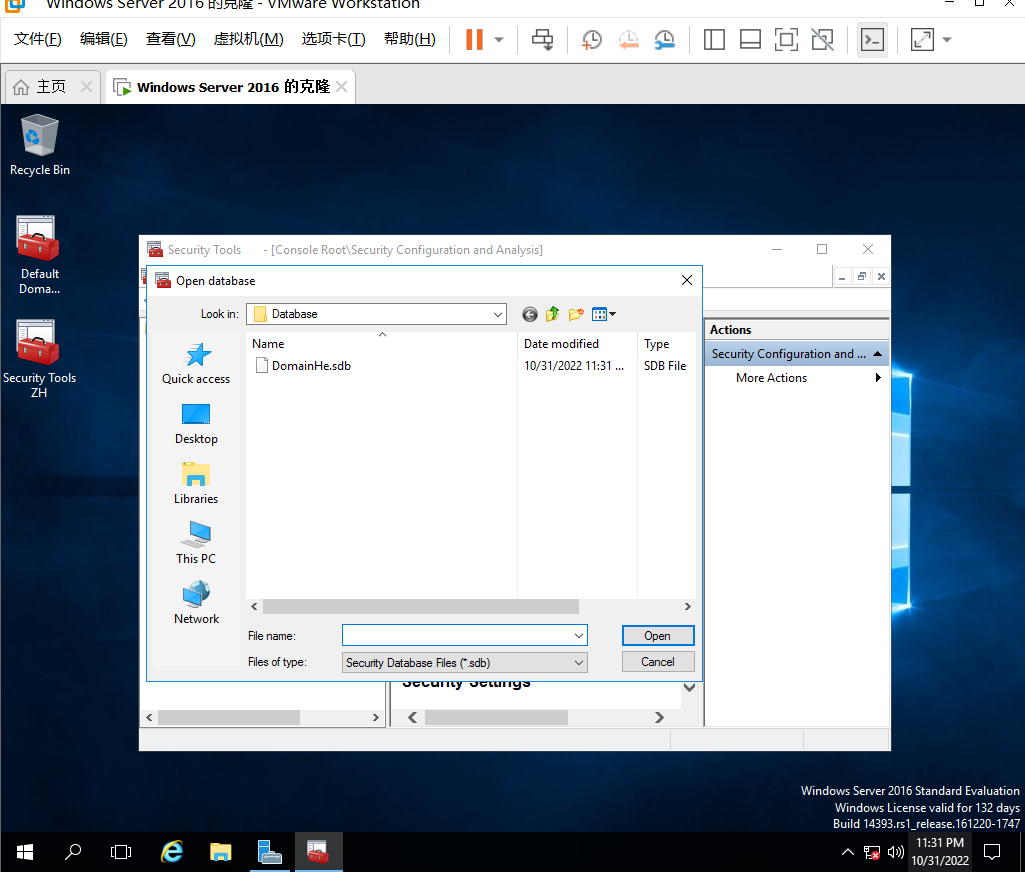


Figure 2.2 Open Database Files

2.23 Right-click Security Configuration and Analysis in the left pane of the console window and click Analyze Computer Now.

2.24 In the Perform Analysis box, notice that the error log is created in the path \Users\Administrator\Documents\Security\Logs and the log file name uses the name of your database, such as **DomainYourFirstName**.log. Click OK.

**2.25** Right-click Security Configuration and Analysis in the left pane of the console window and click View Log File. You see the log file contents to review security analysis information. Use the scroll bar to view the contents. (Because you generated a sample database for demonstration purposes, your results don’t necessarily reflect actual errors on your system.)

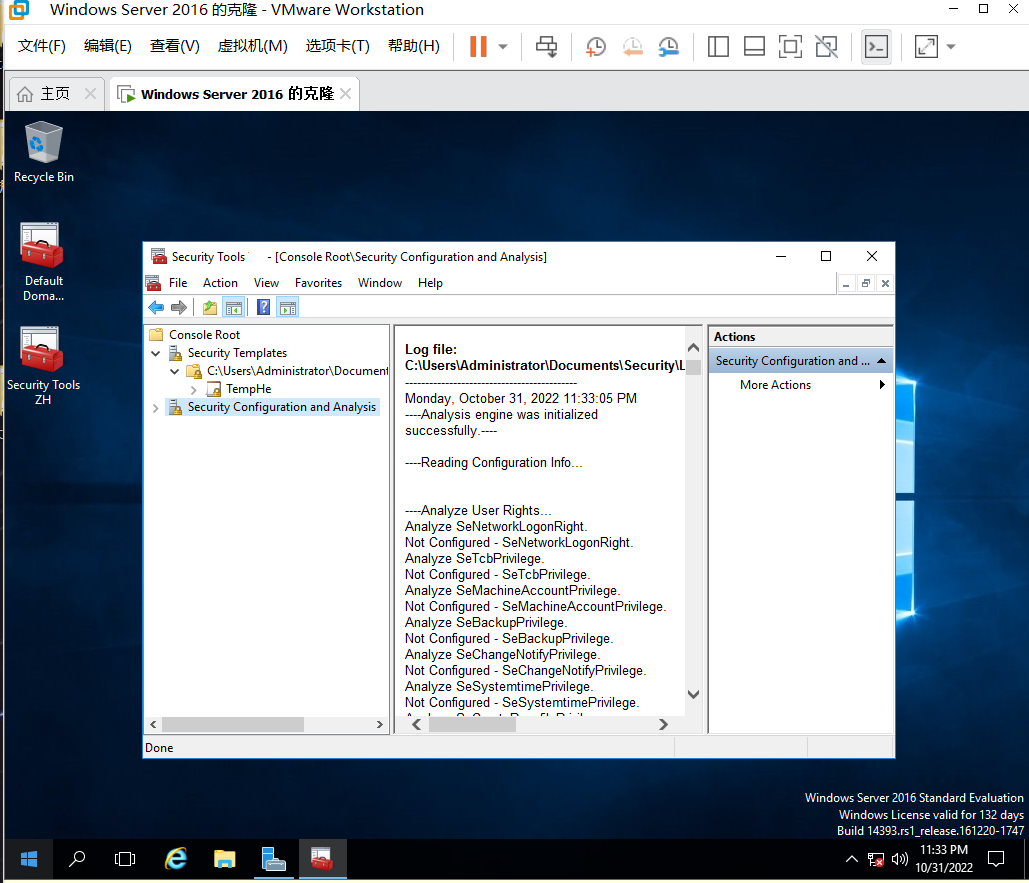


Figure 2.3 View Security Configuration and Analysis

2.26 To configure your system using the imported template, right-click Security Configuration and Analysis and click Configure Computer Now, then click OK in the Configure System dialog box.

**2.27** Notice that the log contents in the middle pane are now changed to show the successful configuration of security policies.

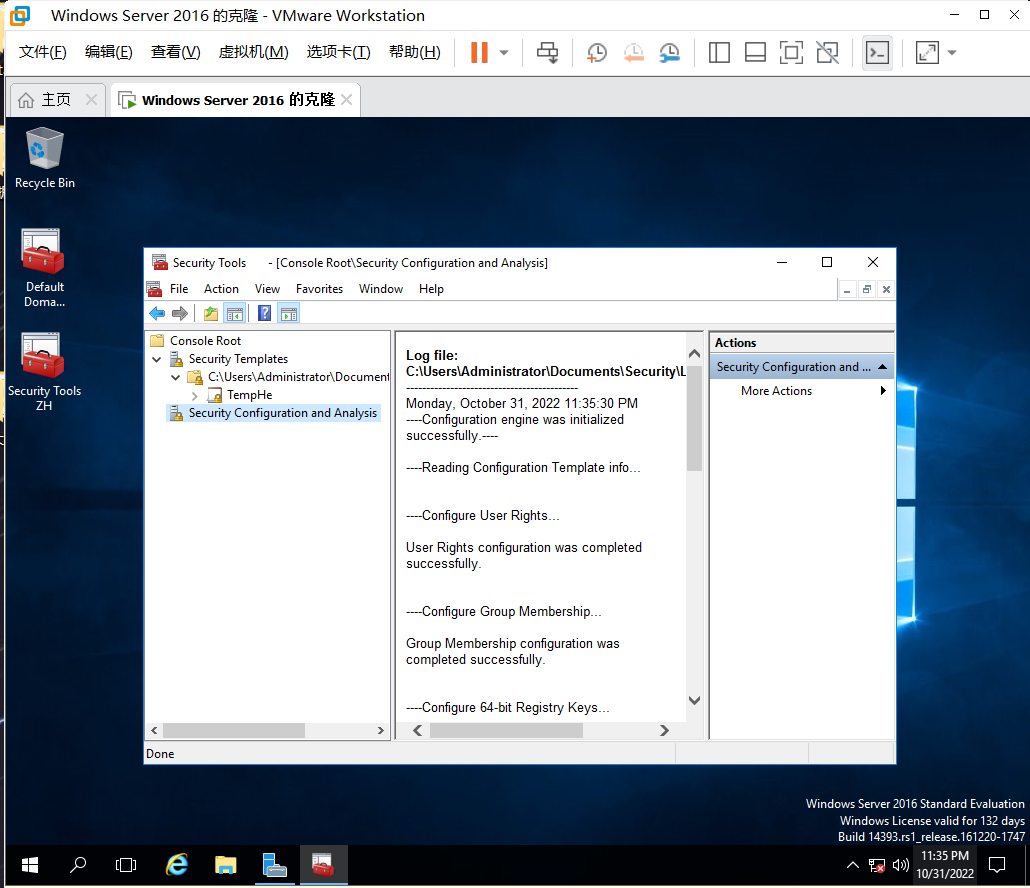


Figure 2.4 Show the successful configuration

2.28 Close the console window and click Yes.

**Activity 10-3: Configuring Policies to Apply to Clients**

**Objective**: Learn how to configure a Group Policy to apply to Windows Server 2016 clients.

**Description**: This activity gives you experience configuring policies to apply to clients. For this activity, you set up File Explorer so that a confirmation dialog box is displayed when a user deletes a file. Also, as a result of users configuring their own computers, the user support group has had to work overtime on unnecessary problems, and some security breaches have occurred. In response, the organization’s management has decided to prohibit access to Control Panel on every client computer.

**Requirements**: Take screenshots on **Steps 3.0, 3.16, and 3.19**, and answer questions on **Steps 3.11 and 3.12**.

**3.0** Open PowerShell prompt, type: **date; ipconfig /all** (two commands in one line) as below. Press **Enter**.

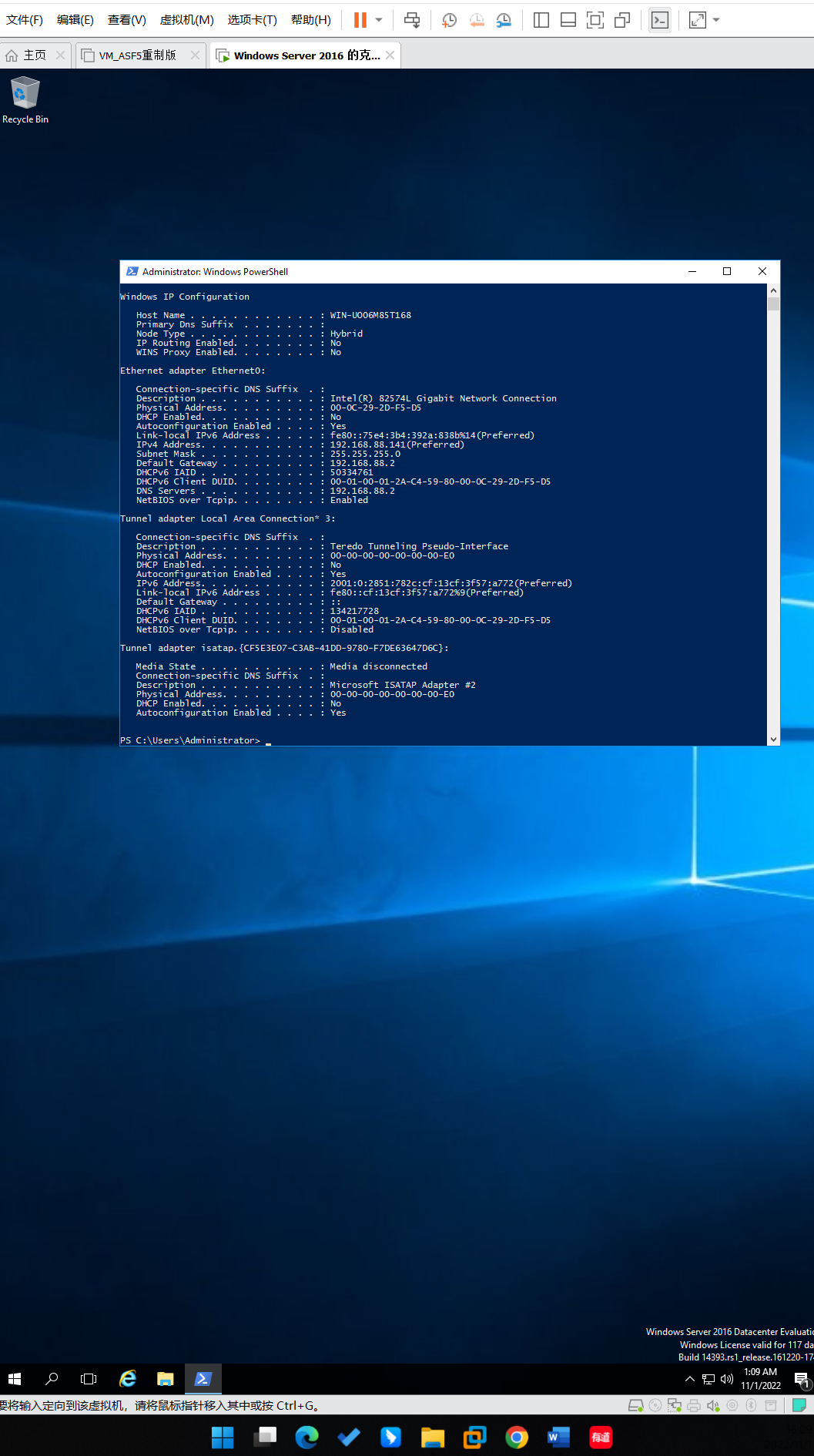


Figure 3.0 Windows Server 2016 Info 3 **Capture your screen, replace the above and save to your file.**

3.1 Open Server Manager, if it is not open.

3.2 Click Tools and click Group Policy Management.

3.3 Expand the tree in the left pane to view Default Domain Policy under Domains and the domain name.

3.4 Right-click Default Domain Policy and click Edit to open the Group Policy Management Editor window.

3.5 If necessary, click the right-pointing arrow in front of User Configuration in the tree to display the elements under it.

3.6 Click the right-pointing arrow in front of Policies under User Configuration.

3.7 Double-click Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer in the tree to display its contents.

3.8 Double-click Windows Components in the tree. Notice the range of folders that appear in the left and right panes.

3.9 Double-click File Explorer in the left pane to view the settings you can configure.

3.10 In the right-pane, click Display confirmation dialog when deleting files. View the information in the right pane that describes what this setting does. Double-click Display confirmation dialog when deleting files. Click the option for Enabled in the Display confirmation dialog when deleting files window. Click OK.

**3.11** In the left pane under User Configuration\Policies\Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer\Windows Components, click Network Sharing.

• How would you keep users from sharing files within their profile?

**3.12** In the left pane under User Configuration\Policies\Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer, click Control Panel. Click Prohibit access to Control Panel and PC settings. View the explanation to see what this option does.

• How would you enable this policy?

**Answer: You can click Edit policy settings in the Control Panel and change Not Configured to Enabled.**

3.13 In the left pane, click each of the main folders under User Configuration\Policies\Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer that you have not yet opened to view their contents (Desktop, Network, Shared Folders, Start Menu and Taskbar, System, and All Settings).

3.14 Under User Configuration\Policies in the left pane, click Software Settings.

3.15 In the right pane, right-click Software installation, and then click Properties.

**3.16** Make sure that the General tab is displayed in the Software installation Properties dialog box. Notice that you can use the Default package location box to specify the location of the software that users will install, which can be on this server such as C:\Windows\Installer (hidden folder) or on a different server in the network. Also, among the New packages parameters, there are options to Publish or Assign software.

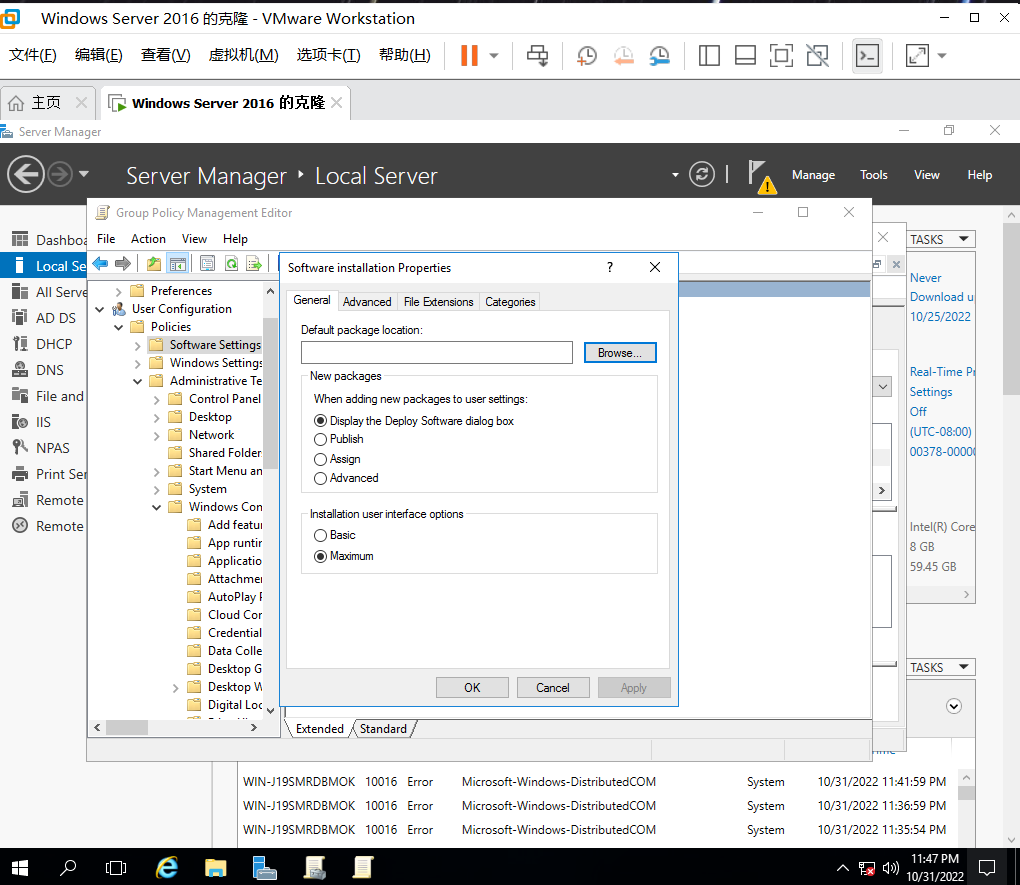


Figure 3.1 View Software installation Properties

3.17 Click each of the Advanced, File Extensions, and Categories tabs to view the properties that can be configured on these tabs.

3.18 Click Cancel.

**3.19** To view from where to set up published or assigned software, in the right pane right-click Software installation, point to New, and notice the Package option. If you were publishing or assigning software, from this point you would click Package, use the Open window to locate an installer package from C:\Windows\Installer for a software, click Open, select Publish or Assigned, click OK, and complete the setup steps.

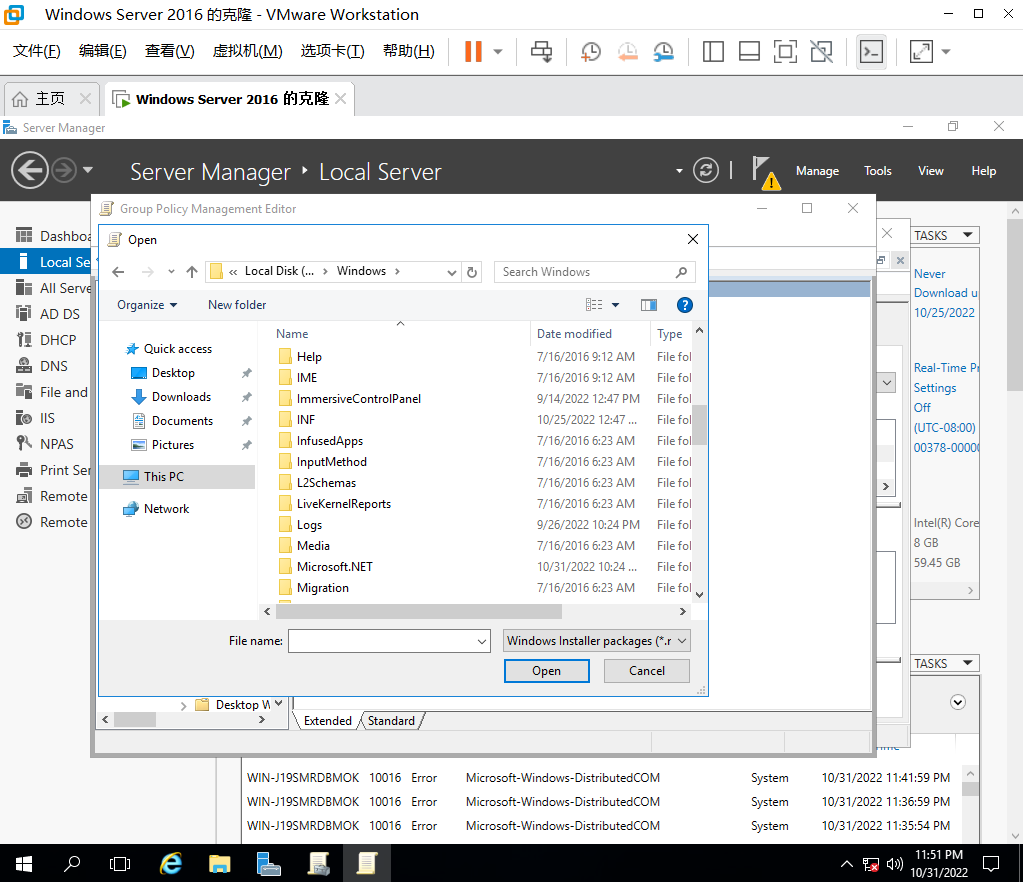


Figure 3.2 View Published Software

3.20 Click in an open location on your desktop to close the menus.

3.21 Close the Group Policy Management Editor window.

**Congratulations! You reach the end of Lab Assessment 3**.

Logon VU Collaborate and upload two separated files:

1. **CoES Assignment Cover Sheet**
2. **Lab\_Assessment\_3\_YourName\_YourID.docx**

via dropbox.

**Turn off your virtual machine on a provided platform.**