Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

6428A

Configuring and Troubleshooting Windows Server® 2008 Terminal Services

Companion Content

Product Number: 6428A

Released: 06/2008

MICROSOFT LICENSE TERMS

OFFICIAL MICROSOFT LEARNING PRODUCTS COURSEWARE – STUDENT EDITION – Pre-Release and Final Versions

These license terms are an agreement between Microsoft Corporation and you. Please read them. They apply to the licensed content named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this licensed content, unless other terms accompany those items. If so, those terms apply.

By using the licensed content, you accept these terms. If you do not accept them, do not use the licensed content.

If you comply with these license terms, you have the rights below.

1. **OVERVIEW.**

   Licensed Content. The licensed content includes software, printed materials, academic materials (online and electronic), and associated media.

   License Model. The licensed content is licensed on a per copy per device basis.

2. **INSTALLATION AND USE RIGHTS.**

   a. **Licensed Device.** The licensed device is the device on which you use the licensed content. You may install and use one copy of the licensed content on the licensed device.

   b. **Portable Device.** You may install another copy on a portable device for use by the single primary user of the licensed device.

   c. **Separation of Components.** The components of the licensed content are licensed as a single unit. You may not separate the components and install them on different devices.

   d. **Third Party Programs.** The licensed content may contain third party programs. These license terms will apply to your use of those third party programs, unless other terms accompany those programs.

3. **PRE-RELEASE VERSIONS.** If the licensed content is a pre-release ("beta") version, in addition to the other provisions in this agreement, then these terms also apply:

   a. **Pre-Release Licensed Content.** This licensed content is a pre-release version. It may not contain the same information and/or work the way a final version of the licensed content will. We may change it for the final, commercial version. We also may not release a commercial version. You will clearly and conspicuously inform any Students who participate in an Authorized Training Session and any Trainers who provide training in such Authorized Training Sessions of the foregoing; and, that you or Microsoft are under no obligation to provide them with any further content, including but not limited to the final released version of the Licensed Content for the Course.

   b. **Feedback.** If you agree to give feedback about the licensed content to Microsoft, you give to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software, licensed content, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your feedback in them. These rights survive this agreement.

   c. **Confidential Information.** The licensed content, including any viewer, user interface, features and documentation that may be included with the licensed content, is confidential and proprietary to Microsoft and its suppliers.

      i. **Use.** For five years after installation of the licensed content or its commercial release, whichever is first, you may not disclose confidential information to third parties. You may disclose confidential information only to your employees and consultants who need to know the information. You must have written agreements with them that protect the confidential information at least as much as this agreement.

      ii. **Survival.** Your duty to protect confidential information survives this agreement.

iii. **Exclusions**. You may disclose confidential information in response to a judicial or governmental order. You must first give written notice to Microsoft to allow it to seek a protective order or otherwise protect the information. Confidential information does not include information that

- becomes publicly known through no wrongful act;
- you received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
- you developed independently.

d. **Term**. The term of this agreement for pre-release versions is (i) the date which Microsoft informs you is the end date for using the beta version, or (ii) the commercial release of the final release version of the licensed content, whichever is first ("beta term").

e. **Use**. You will cease using all copies of the beta version upon expiration or termination of the beta term, and will destroy all copies of same in the possession or under your control.

f. **Copies**. Microsoft will inform Authorized Learning Centers if they may make copies of the beta version (in either print and/or CD version) and distribute such copies to Students and/or Trainers. If Microsoft allows to such distribution, you will follow any additional terms that Microsoft provides to you for such copies and distribution.

4. **ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.**

a. Media Elements and Templates. You may use images, clip art, animations, sounds, music, shapes, video clips and templates provided with the licensed content solely for your personal training use. If you wish to use these media elements or templates for any other purpose, go to www.microsoft.com/permission to learn whether that use is allowed.

b. Academic Materials. If the licensed content contains academic materials (such as white papers, labs, tests, datasheets and FAQs), you may copy and use the academic materials. You may not make any modifications to the academic materials and you may not print any book (either electronic or print version) in its entirety. If you reproduce any academic materials, you agree that:

- The use of the academic materials will be only for your personal reference or training use
- You will not republish or post the academic materials on any network computer or broadcast in any media;
- You will include the academic material's original copyright notice, or a copyright notice to Microsoft's benefit in the format provided below:

Form of Notice:

c. Distributable Code. The licensed content may contain code that you are permitted to distribute in programs you develop if you comply with the terms below.

i. Right to Use and Distribute. The code and text files listed below are "Distributable Code."

- REDIST.TXT Files. You may copy and distribute the object code form of code listed in REDIST.TXT files.
- Sample Code. You may modify, copy, and distribute the source and object code form of code marked as "sample."
- Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.

ii. Distribution Requirements. For any Distributable Code you distribute, you must

- add significant primary functionality to it in your programs;
- require distributors and external end users to agree to terms that protect it at least as much as this agreement;
- display your valid copyright notice on your programs; and
- indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs.

iii. **Distribution Restrictions.** You may not

- alter any copyright, trademark or patent notice in the Distributable Code;
- use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
- distribute Distributable Code to run on a platform other than the Windows platform;
- include Distributable Code in malicious, deceptive or unlawful programs; or
- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
  - the code be disclosed or distributed in source code form; or
  - others have the right to modify it.

5. **INTERNET-BASED SERVICES.** Microsoft may provide Internet-based services with the licensed content. It may change or cancel them at any time. You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.
6. **SCOPE OF LICENSE.** The licensed content is licensed, not sold. This agreement only gives you some rights to use the licensed content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the licensed content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the licensed content that only allow you to use it in certain ways. You may not
   - disclose the results of any benchmark tests of the licensed content to any third party without Microsoft's prior written approval;
   - work around any technical limitations in the licensed content;
   - reverse engineer, decompile or disassemble the licensed content, except and only to the extent that applicable law expressly permits, despite this limitation;
   - make more copies of the licensed content than specified in this agreement or allowed by applicable law, despite this limitation;
   - publish the licensed content for others to copy;
   - transfer the licensed content marked as 'beta' or 'pre-release' to any third party;
   - allow others to access or use the licensed content;
   - rent, lease or lend the licensed content; or
   - use the licensed content for commercial licensed content hosting services.
   - Rights to access the server software that may be included with the Licensed Content, including the Virtual Hard Disks does not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that may access the server.
7. **BACKUP COPY.** You may make one backup copy of the licensed content. You may use it only to reinstall the licensed content.
8. **TRANSFER TO ANOTHER DEVICE.** You may uninstall the licensed content and install it on another device for your personal training use. You may not do so to share this license between devices.
9. **TRANSFER TO A THIRD PARTY.** You may not transfer those versions marked as 'beta' or 'pre-release' to a third party. For final versions, these terms apply: The first user of the licensed content may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the licensed content. The first user must uninstall the licensed content before transferring it separately from the device. The first user may not retain any copies.
10. **EXPORT RESTRICTIONS.** The licensed content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the licensed content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
11. **NOT FOR RESALE SOFTWARE/LICENSED CONTENT.** You may not sell software or licensed content marked as "NFR" or "Not for Resale."

12. **ACADEMIC EDITION.** You must be a "Qualified Educational User" to use licensed content marked as "Academic Edition" or "AE." If you do not know whether you are a Qualified Educational User, visit www.microsoft.com/education or contact the Microsoft affiliate serving your country.

13. **ENTIRE AGREEMENT.** This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the licensed content and support services.

14. **APPLICABLE LAW.**

    a. **United States.** If you acquired the licensed content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

    b. **Outside the United States.** If you acquired the licensed content in any other country, the laws of that country apply.

15. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the licensed content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

16. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**

17. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. $5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

    This limitation applies to

    - anything related to the licensed content, software, services, content (including code) on third party Internet sites, or third party programs; and
    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this licensed content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence , aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Module 1

Configuring Terminal Services Core Functionality

Contents:

Lab Answer Keys

Lab: Configuring TS Core Functionality

Exercise 1: Installing and Configuring the TS Server Role Service

Exercise 2: Configuring the TS Settings

Logon Information:

- Virtual Machine1: **6428A-NYC-DC1-01**
- Virtual Machine 2: **6428A-NYC-TS-01**
- User Name: **Administrator/Baris**
- Password: **Pa$$w0rd**

Estimated time: 65 minutes

Exercise 1: Installing and Configuring the TS Server Role Service

Exercise Overview

In this exercise, you will install and configure the TS core functionality at the New York head office.

The main tasks for this exercise are as follows:

1. Start the 6428A-NYC-DC1-01 and 6428A-NYC-TS-01 virtual machines and log on to these machines as **Administrator**.
2. Install the TS server role service.
3. Configure authentication on the terminal server.
4. Configure the default credentials to be used on the terminal server.
5. Create a .rdp file and configure custom display.
6. Enable ClearType and Font smoothing.
7. Enable support for PnP redirection.
8. Install and configure WSRM.
9. Install the Desktop Experience.
10. Remotely connect to TS by using RDC.

► Task1: Start the 6428A-NYC-DC1-01 and 6428A-NYC-TS-01 virtual machines and log on to these machines as Administrator

1. Start 6428A-NYC-DC1-01 using the Lab Launcher tool.

   Wait for the virtual machine to start. The Recent Events section will display the messages of the events.

2. Log on with the default login ID **WOODGROVEBANK\Administrator** and the password **Pa$$w0rd**, and then click **Go**. The **Server Manager** snap-in is displayed.

Note: Wait for the domain controller, 6428A-NYC-DC1-01, logon screen to appear before starting 6428A-NYC-TS-01 virtual machine. If the virtual machine is not properly shut down, the

Shutdown Event Tracker dialog box will be displayed. Select the **Security issue** option from the drop-down list and click **OK**.

3. Start 6428A-NYC-TS-01 using the Lab Launcher tool.
4. Log on with the ID **WOODGROVEBANK\administrator** and password **Pa$$w0rd**.The Server Manager snap-in is displayed.
5. On 6428A-NYC-DC1-01, click **Start**, point to **Administrative Tools**, click **Active Directory Users and Computers**.
6. In the left pane, click the **WoodgroveBank.com** node, click **Computers**, and verify that **NYC-TS** is displayed in the right pane.

► Task 2: Install the TS server role service

1. On 6428A-NYC-TS-01, in **Server Manager**, in the left pane, right-click **Roles**, and then click **Add Roles**.
2. In the **Add Roles Wizard**, on the **Before You Begin** page, click **Next**.
3. On the **Select Server Roles** page, under **Roles** list, select the **Terminal Services** check box, and then click **Next**.
4. On the **Terminal Services** page, click **Next**.
5. On the **Select Role Services** page, select the **Terminal Server** check box, and then click **Next**.
6. On the **Uninstall and Reinstall Applications for Compatibility** page, click **Next**.
7. On the **Specify Authentication Method for Terminal Server** page, select **Require Network Level Authentication** option, and then click **Next**.
8. On the **Specify Licensing Mode**, select **Per User**, and then click **Next**.
9. On the **Select User Groups Allowed Access To This Terminal Server** page, click **Add**.
10. In the **Select Users, Computers, or Groups** dialog box, verify that **From this location** box has **WoddgroveBank.com**.
11. In the **Enter the object names to select{examples}** box, type **NYC_MarketingGG**, click **Check Names**, click **OK**, and then click **Next**.
12. On the **Confirm Installation Selections** page, click **Install**.
13. On the **Installation Progress** page, note the installation progress. On completion of the installation, the Installation Results page is displayed.
14. On the **Installation Results** page, you are prompted to restart the server to finish the installation process. Click **Close**.
15. On the **Add Roles Wizard** message box, click **Yes** to restart the server.
16. After the server restarts and you log on to the computer as **WOODGROVEBANK\Administrator** and password **Pa$$w0rd**, the **Resume Configuration Wizard** is displayed. On the **Installation Progress** page, note the installation progress. On completion of the installation, the Installation Results page is displayed.
17. Observe that the installation of the **Terminal Services** has succeeded. Click **Close**.

18. On the **Server Manager** link, scroll down to the **Roles Summary** section, click the **Terminal Services** link.
19. On the **Terminal Services** page, scroll down to **System Services** section, and confirm that the **Status** for TS is **Running**.
20. In the **Role Services** section, confirm that the **Status** for TS is **Installed**.
21. Close the **Server Manager**.

► Task 3: Configure authentication on the terminal server

1. Start the **Terminal Services Configuration** snap-in on 6428A-NYC-TS-01. Click **Start**, click **Run**, in the **Open** box type **tsconfig.msc**, and then click **OK**.
2. On the **Terminal Services Configuration** page, in the middle pane, in the **Connections** section, under **Connection Name**, right-click **RDP-Tcp**, and then click **Properties**.
3. In the **RDP-Tcp Properties** dialog box, on the **General** tab, in the **Security Layer** box, select **SSL (TLS 1.0)** from the drop-down list box, and then click **OK**.

► Task 4: Configure the default credentials to be used on the terminal server

1. Start the **Local Group Policy Editor** on 6428A-NYC-TS-01. Click **Start**, in the **Start Search** box, type **gpedit.msc**, and then press ENTER.
2. In the left pane, under the **Computer Configuration** node, open the **Administrative Templates** folder, then open the **Systems** folder, and then open the **Credentials Delegation** folder.
3. In the right pane, under **Setting**, double-click **Allow Delegating Default Credentials**.
4. In the **Allow Delegating Default Credentials Properties** dialog box, on the **Setting** tab, click **Enabled**, and then click **Show**.
5. In the **Show Contents** dialog box, click **Add** to add servers to the list.
6. In the **Add Item** dialog box, in the Enter the item to be added box, type **6428A-NYC-TS-01**, and then click **OK**.
7. Click **OK** to close the **Show Contents** dialog box.
8. In the **Allow Delegating Default Credentials Properties** dialog box, click **OK**.
9. Close the Local Group Policy Editor.

► Task 5: Create .a rdp file and configure custom display

1. To create .rdp file, click **Start**, click **Administrative tools**, click **Terminal Services**, and then click **TS RemoteApp Manager**.
2. On the **TS RemoteApp Manager** page, in the Actions pane, click **Add RemoteApp Programs**, and then click **Next**.
3. In the **RemoteApp Wizard** page, select **Remote Desktop Connection** check box, and click **Next**.
4. In the **Review settings** page, click **Finish**.
5. In **TS RemoteApp Manager**, scroll down to **RemoteApp Programs**, click **Remote Desktop Connection**, and then right-click **Create .rdp** file to display the **RemoteApp Wizard** page.
6. In the **RemoteApp Wizard** page, click **Next**.

7. Under the **Specify Package Settings**, verify the location of package is **C:\Program Files\Packaged Programs**, click **Next**.
8. In the **Review Settings** page, click **Finish**.
9. To configure the custom display, click **Start**, click **Computer**, and browse to **C:\Program files\Packaged Programs\Mstsc.rdp**.
10. Right-click the **mstsc.rdp** file, click **Open With**, double-click **Other Programs**, and then select **Notepad**. Click **OK**.
11. At the bottom of the **mstsc.rdp** file, type **desktopwidth:i:1680**. Press ENTER.
12. Then type **desktopheight:i:1050**. Press ENTER.
13. Then type **Span:i:1**.
14. Click **File**, and then click **Save**. Close the mstsc.rdp file.
15. Close Packaged Programs.

► Task 6: Enable ClearType and Font smoothing

1. Click **Start**, click **Control Panel**, and then in the left panel, click **Control Panel Home**.
2. In **Control Panel**, click the **Appearance and Personalization** link.
3. Under **Personalization**, click **Change the color scheme**.
4. On the **Appearance Settings** page, on the **Appearance** tab, click **Effects**, and then select the **Use the following method to smooth edges of screen fonts** check box.
5. Verify that **ClearType** is selected by default, and then click **OK** twice.
6. Close the Control Panel\Appearance and Personalization screen.
7. Click **Start**, point to **All Programs**, click **Accessories**, and then click **Remote Desktop Connection**.
8. In the **Remote Desktop Connection** dialog box, click **Options**.
9. In the **Remote Desktop Connection** dialog box, click the **Experience** tab, in the **Performance** section, select the **Font smoothing** check box.

► Task 7: Enable support for PnP redirection

1. In the **Remote Desktop Connection** dialog box, on the **Local Resources** tab, under **Local devices and resources** section, click **More**.
2. Under **Local devices and resources**, expand the **Supported Plug and Play devices** node.
3. Select the **Devices that I plug in later** check box, and then click **OK**.
4. Close the **Remote Desktop Connection** dialog box.

► Task 8: Install and configure WSRM

1. To start the **Server Manager** snap-in on 6428A-NYC-TS-01, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. In the **Server Manager**, scroll down to the **Features Summary** section, click the **Add Features** link. The Add Features Wizard page is displayed.
3. In the wizard, on the **Select Features** page, scroll down and select the **Windows System Resource Manager** check box. The Add Features Wizard message box is displayed informing you that Windows

Internal Database also needs to be installed for Windows System Resource Manager (WSRM) to work properly.

4. Click **Add Required Features**, and then click **Next**.
5. On the **Confirm Installation Selections** page, click **Install**.
6. On the **Installation Progress** page, note the installation progress. On completion of the installation, the Installation Results page is displayed.
7. On the **Installation Results** page, confirm that the installation of Windows Internal Database and WSRM succeeded, and then click **Close**.
8. To start the **WSRM** snap-in, click **Start**, point to **Administrative Tools**, and then click **Windows System Resource Manager**. The WSRM snap-in is displayed.
9. In the **Connect to computer** dialog box, under **Administer**, verify that **This Computer** is selected, and then click **Connect**. This will enable the WRSM to administer the local computer."
10. Close WSRM [Windows System Resource Manager (local)].

► Task 9: Install the Desktop Experience

1. To start the **Server Manager** snap-in on 6428A-NYC-TS-01, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. In the **Server Manager**, scroll down to the **Features Summary** section, click the **Add Features** link. The Add Features Wizard page is displayed.
3. In the wizard, on the **Select Features** page, select the **Desktop Experience** check box, and then click **Next**.
4. On the **Confirm Installation Selections** page, observe the message that the server must be restarted after the installation of the Desktop Experience completes, and then click **Install**.
5. On the **Installation Progress** page, note the installation progress. On completion of the installation, the Installation Results page is displayed.
6. On the **Installation Results** page, you are prompted to restart the server to finish the installation process. Click **Close**.
7. On the **Add Features Wizard** message box, click **Yes** to restart the server.
8. After the server restarts and you log on to the computer as **WOODGROVEBANK\Administrator** with password **Pa$$w0rd**, the **Resume Configuration Wizard** is displayed. On the **Installation Progress** page, note the installation progress. On completion of the installation, the Installation Results page is displayed.
9. Observe that the installation of the **Desktop Experience** has succeeded.
10. Click **Close**.
11. Close the Server Manager.

► Task 10: Remotely connect to TS by using RDC

1. On 6428A-NYC-DC1-01, open the **Remote Desktop Connection**. Click **Start**, and then type **mstsc** in the **Start Search** box, and then press ENTER.
2. In the **Remote Desktop Connection** dialog box, in the **Computer** box, verify that **NYC-TS** is displayed by default, and then click **Connect**. The Windows Security dialog box is displayed.

3. In the **Windows Security** dialog box, click **Use another account**.
4. In the **User name** box, type **WOODGROVEBANK\Baris**.
5. In the **Password** box, type **Pa$$w0rd**, and then click **OK**. The Remote Control screen is displayed.
6. Close the remote connection. The Disconnect Terminal Services Session confirmation message box is displayed. Click **OK**.

Result: After this exercise, you should have installed and configured the TS server role service.

Exercise 2: Configuring the TS Settings

In this exercise, you will configure TS settings and the session broker settings.

Exercise Overview

The main tasks for this exercise are as follows:

1. Specify the program to start when user logs on to a remote session.
2. Configure the TS settings by using the Terminal Services Configuration snapin.
3. Modify the default permissions for built-in accounts.
4. Configure the Session Broker settings.
5. Shut down the virtual machines.

► Task 1: Specify the program to start when user logs on to a remote session

1. Log on to 6428A-NYC-TS-01. Start **Terminal Services Configuration** on 6428A-NYC-TS-01. Click **Start**, point to **Administrative tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. In the **Terminal Services Configuration** snap-in, in the middle pane, in the **Connections** section, under **Connection Name**, right-click **RDP-Tcp**, and then click **Properties**.
3. In the **RDP-Tcp Properties** dialog box, click the **Environment** tab, under **Initial program** area, click **Start the following program when the user logs on** option.
4. In **Program path and file name** box, type **C:\Program Files\Packaged Programs\wordpad**, and then click **OK**.

► Task 2: Configure the TS settings by using the Terminal Services Configuration snap-in

1. In **Terminal Services Configuration NYC-TS**, in the middle panel, under the **Edit Settings** area, under the **General** section, double-click the **Delete Temporary folders on exit** option. The **Properties** dialog box is displayed.
2. On the **General** tab, verify that the following check boxes are selected:
   - **Restrict each user to a single session**
   - **Delete Temporary folders on exit**
   - **Use Temporary folders per session**

   Then click **OK**.
3. Close Terminal Services Configuration.

► Task 3: Modify the default permissions for built-in accounts

1. Start **WMI Console**. Click **Start**, click **Run** and type **wmimgmt.msc**, and press ENTER.
2. In the **Root** tree, right-click **WMI Control(Local)**, and then click **Properties**.
3. In the **WMI Control (Local) Properties** dialog box, click the **Security** tab, click **Security**.
4. In the **Security for Root** dialog box, click **Add**.
5. In the **Select Users, Computers, or Groups** dialog box, in the **Enter the object names to select (Examples)** box, type **Baris**, and then click **Check Names**. Click **OK**.
6. Under **Permissions for Baris Centinok**, select the **Allow** check box for the **Read Security** permission, and then click **OK**.
7. Click **OK** to close WMI Control.

► Task 4: Configure the Session Broker Settings

1. Click **Start**, point to **Administrative tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. In the middle pane, in the **Edit settings** area, scroll down to the **TS Session Broker** section, double-click **Member of farm in TS Session Broker**.
3. In the **Properties** page, on the **TS Session Broker** tab, select the **Join a farm in TS Session Broker** check box.
4. In the **TS Session Broker server name or IP address** box, type **NYC-TS**.
5. In the **Farm name in TS Session Broker** box, type **WoodgroveBank**.
6. Select the **Participate in Session Broker Load-Balancing** check box.
7. Verify that the **Use IP address redirection (recommended)** check box is enabled.
8. Select the IP address **10.10.0.23** check box, and then click **OK**.
9. The **Terminal Services Configuration** dialog box is displayed. Click **Yes**. Close Terminal Services Configuration.

► Task 5: Shut down the virtual machines

1. Exit the Lab Launcher tool by clicking the close button.
2. In the **Close** window, click **Turn off machine and discard changes**.
3. Click **OK**.

Module 3

Configuring and Troubleshooting Terminal Services Connections

Contents:

Lab Answer Keys

Lab: Configuring and Troubleshooting TS Connections

Exercise 1: Configuring the TS Connection Properties

Exercise 2: Configuring the TS Connection Properties by Using Server Group Policy

Exercise 3: Configuring SSO by Using Client Group Policy

Exercise 4: Troubleshooting Connectivity Issues

Logon Information:

- Virtual Machine1: **6428A-NYC-DC1-01**
- Virtual Machine 2: **6428A-NYC-TS-03**
- User Name: **Administrator/Bernard/Baris/Anton/Monika/Dan**a
- Password: **Pa$$w0rd**
- Password 2: **Pass@word1**

Estimated time: 70 minutes

Exercise 1: Configuring the TS Connection Properties

Exercise Overview

In this exercise, you will configure the TS connection properties by using the Terminal Services Configuration snap-in.

The main tasks for this exercise are as follows:

1. Start the 6428A-NYC-DC1-01 and 6428A-NYC-TS- 03 virtual machines and log on to these machines as Administrator.
2. Configure the TS connection properties by using the Terminal Services Configuration snap-in.

► Task1: Start the 6428A-NYC-DC1-01 and 6428A-NYC-TS- 03 virtual machines and log on to these machines as Administrator

1. Start 6428A-NYC-DC1-01 using the Lab Launcher tool.
2. The login ID is displayed as **WOODGROVEBANK\Administrator**. Log on by using the password **Pa$$w0rd**, and then press ENTER.

Note: Wait for the domain controller 6428A-NYC-DC1-01 logon screen to appear before starting the 6428A-NYC-TS-03 virtual machine.

3. Start 6428A-NYC-TS-03 using the Lab Launcher tool.
4. Log on as **WoodgroveBank\Administrator** using the password **Pa$$w0rd**, and then press ENTER. The Server Manager page is displayed by default.
5. On 6428A-NYC-TS-03, verify that TS is installed on this virtual machine by performing the following steps:

- In the **Server Manager**, scroll down to the **Roles Summary** section, click the **Terminal Services** link.
- On the **Terminal Services** page, under **System Services** section, verify that the **Status** of **Terminal Services** is shown as **Running**.
- Under the **Role Services** section, verify that the **Status** of **Terminal Server** is shown as **Installed**.
- Close the **Server Manager** console.

► Task 2: Configure the TS connection properties by using the Terminal Services Configuration snap-in

1. To start the **Terminal Services Configuration** snap-in on 6428A-NYC-TS-03, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
2. Verify the remote control setting as follows:
   a. In the middle pane, in the **Connections** section, under **Connection Name**, right-click **RDP-Tcp**, and then click **Properties**.
   b. In the **RDP-Tcp Properties** dialog box, click the **Remote Control** tab and verify that the **Use remote control with default user settings** option is selected.
3. To configure connection permissions:
   a. In the **RDP-Tcp Properties** dialog box, click the **Security** tab.
   b. The **Terminal Services Configuration** message box is displayed. Click **OK**.
   c. Click the **Advanced** button below the **Permissions for SYSTEM** section. The **Advanced Security Settings for RDP-Tcp** dialog box is displayed.
   d. On the **Permissions** tab, in the **Permission entries** list, select the record for **Baris Cetinok**, and then click the **Edit** button. The **Permission Entry for RDP-Tcp** dialog box is displayed.
   e. On the **Object** tab, in the **Permissions** list, select the **Deny** check box for the **Disconnect** permission, and then click **OK**.
   f. In the **Advanced Security Settings for RDP-Tcp** dialog box, on the **Permissions** tab, in the **Permission entries** list, select the record for **Bernard Duerr**, and then click **Edit**. The **Permission Entry for RDP-Tcp** dialog box is displayed.
   g. On the **Object** tab, in the **Permissions** list, verify that the **Allow** check boxes for all permissions are selected, and then click **OK**.
   h. In the **Advanced Security Settings for RDP-Tcp** dialog box, on the **Permissions** tab, in the **Permissions entries** list, select the record for **Anton Kirilov**, and then click **Edit**.
   i. On the **Object** tab, in the **Permissions** list, select the **Allow** check box for the **Disconnect** permission and **Deny** check box for login permission. A Windows Security Warning dialog box appears. Click **Yes**.
   j. Click **Yes** to close the **RDP-Tcp Properties** dialog box.
4. Close the Terminal Services Configuration snap-in.

Results: After this exercise, you should have configured the connection properties.

Exercise 2: Configuring the TS Connection Properties by Using Server Group Policy

Exercise Overview

In this exercise, you will configure the TS connection properties by using Group Policy.

The main tasks for this exercise are as follows:

1. Configure the TS connection properties.
2. Verify that a maximum of two clients can connect to the terminal server.

► Task 1: Configure the TS connection properties

1. To open the **Group Policy Management** snap-in on 6428-NYC-DC1-01, click **Start**, click **Run** and in the **Open** box type **gpmc.msc**, and then click **OK**.
2. In the **Group Policy Management** snap-in, expand **Forest: WoodgroveBank.com**, expand **Domains**, **WoodgroveBank.com**, **NYC** nodes, then right-click **Marketing**, and then click **Create a GPO in this domain, and Link it here**.
3. In the **New GPO** dialog box that is displayed, type the name of the policy as **GPO for TS Connection**, and then click **OK**.
4. On the **Marketing** node, right-click the **GPO for TS Connection** link, and then click **Edit**.
5. In the **Group Policy Management Editor** page, under the **Computer Configuration** node, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, click **Terminal Services**, and under the **Terminal Server** node, click **Connections**.
6. In the right pane, under **Setting**, double-click **Limit number of connections**.
7. In the **Limit number of connections properties** dialog box, on the **Setting** tab, select **Enabled**, in the **TS Maximum Connections allowed** box, select **2**, and then click **OK**.
8. In the right pane of the **Group Policy Management Editor** snap-in, under **Setting**, double-click **Automatic reconnection**.
9. In the **Automatic reconnection Properties** dialog box, select **Enabled**, and then click **OK**.
10. In the left pane of the **Group Policy Management Editor** snap-in, under **Terminal Services** node, expand the **Terminal Server** node, and then click **Security**.
11. In the right pane of the **Group Policy Management Editor** snap-in, under **Setting**, double-click **Set client connection encryption level**.
12. In the **Set client connection encryption level Properties** dialog box, select **Enabled**.
13. From the **Encryption level** drop-down list, verify that **Client Compatible** is selected, and then click **OK**.
14. In the left pane, under **Terminal Services** node, click **Terminal Server**, and then click **Session Time Limits**.
15. In the right pane, double-click **Set time limit for disconnected sessions**.
16. In the **Set time limit for disconnected sessions Properties** dialog box, select **Enabled**.
17. In the **End a disconnected session** box, select **5 minutes** from the drop-down list, and then click **OK**.
18. Close the **Group Policy Management Editor** page.

19. Close the **Group Policy Management** snap-in.

► Task 2: Verify that a maximum of two clients can connect to the terminal server

1. On 6428A-NYC-DC1-01, click **Start**, click **Run**, in the **Open** box type **mstsc**, and then click **OK**.
2. In the **Remote Desktop Connection** dialog box, verify that the **Computer** box displays **Nyc-ts**, and then click **Connect**.

Note: If the Remote Desktop Connection is disconnected perform the following steps to create the remote connection:

   a. Open **Control Panel**.
   b. Click the **Network and Sharing Center** icon. Verify whether NYC-DC is connected to Unidentified network.
   c. Check the status of the **Local Area Connection**.
   d. In the **Network and Sharing Center** window, under **Tasks**, click **Manage network connections**.
   e. In the **Network Connections** window, right-click **Local Area Connection**, and then click **Disable**.
   f. Then right-click **Local area Connection**, and click **Enable**.
   g. Close the **Network Connections** window. In the **Network and Sharing Center** window, check whether NYC-DC is connected to WoodgroveBank.com.

3. In the **Windows Security** dialog box, click **Use another account**. Log on with the login ID **WOODGROVEBANK\Baris** using the password **Pa$$w0rd**, and then press ENTER.
4. Minimize the **Nyc-ts Remote Desktop** connection.
5. To log on as the second user, click **Start**, click **Run**, in the **Open** box type **mstsc**, and then click **OK**.
6. In the **Remote Desktop Connection** dialog box, verify that the **Computer** is **Nyc-ts**, and then click **Connect**.
7. In the **Windows Security** dialog box, click **Use another account**.
8. Log on as **WOODGROVEBANK\Bernard** with the password as **Pa$$w0rd** and then press ENTER.
9. Minimize the **Nyc-ts Remote Desktop** connection.
10. To log on as the third user, click **Start**, click **Run**, in the **Open** box type **mstsc**, and then click **OK**.
11. In the **Remote Desktop Connection** dialog box, verify that the **Computer** is **Nyc-ts**, and then click **Connect**.
12. In the **Windows Security** dialog box, click **Use another account**, log on with the login ID **WOODGROVEBANK\Anton** using the password **Pa$$w0rd**, and then click **OK**.
13. Observe that a message displaying "The requested session access is denied" appears on the screen. Click **OK**.
14. Close all the remote connections.
15. The **Disconnect Terminal Services Session** dialog box is displayed. Click **OK**.

Results: After this exercise, you should have configured the TS connection properties by using Server Group Policy.

Exercise 3: Configuring SSO by Using Client Group Policy

Exercise Overview

The main task for this exercise is to configure SSO by using client Group Policy.

► Task 1: Configure the SSO setting by using client Group Policy

1. To open the **Terminal Services Configuration** snap-in on 6428A-NYC-DC1- 01, click **Start**, click **Run**, in the **Open** box type **tsconfig.msc**, and then click **OK**.
2. In the middle pane, under **Connections** section, under **Connection Name**, right-click **RDP-Tcp**, and then click **Properties**.
3. In the **RDP-Tcp Properties** dialog box, on the **General** tab, in the **Security layer** box, select **SSL (TLS 1.0)** from the drop-down list, and then click **OK**.
4. Close the Terminal Services Configuration snap-in.
5. To open the **Local Group Policy Editor**, click **Start** and in the **Start Search** box, type **gpedit.msc**, and then press ENTER.
6. In the left pane, under the **Computer Configuration** node, expand the **Administrative Templates** node, expand **System** node, and then click **Credentials Delegation**.
7. In the right pane, under **Setting**, double-click **Allow Delegating Default Credentials**.
8. In the **Allow Delegating Default Credentials Properties** dialog box, on the **Setting** tab, click **Enabled**, and then click **Show** to add servers to the list.
9. In the **Show Contents** dialog box, click **Add** to add servers to the list.
10. In the **Add Item** dialog box, in the **Enter the item to be added** box, type **6428A-NYC-TS- 03**, and then click **OK**.
11. Click **OK** to close the **Show Contents** dialog box.
12. In the **Allow Delegating Default Credentials Properties** dialog box, click **OK**.
13. Close the **Local Group Policy Editor**.

Results: After this exercise, you should have configured SSO by using client Group Policy.

Exercise 4: Troubleshooting Connectivity Issues

Exercise Overview

In this exercise, you will troubleshoot connectivity issues.

The main tasks for this exercise are as follows:

1. Verify the RDP settings, and check the event logs.
2. Verify the user and group permissions and policy settings.
3. Verify that the users are able to log on with the updated settings.
4. Shut down the virtual machines.

► Task 1: Verify the RDP settings and check the event Logs

1. On 6428A-NYC-TS-03, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS RemoteApp Manager**.
2. In the **TS RemoteApp Manager** page, under the **Overview** section for **RDP Settings**, click the **Change** link.
3. In the **RemoteApp Deployment Settings** dialog box, click the **Terminal Server** tab.
4. On the **Terminal Server** tab, ensure that the **Server name** box has **NYCTS. WoodgroveBank.Com**.
5. Ensure that the port number in **RDP Port** is **3389**, and then click **OK** to close the **RemoteApp Deployment Settings** dialog box.
6. Close the **TS RemoteApp Manager**.
7. To display the **Event Viewer** dialog box, click **Start**, click **Run**, in the **Open** box type **eventvwr**, press ENTER.
8. In the **Event Viewer** dialog box, expand the **Windows Logs** node.
9. Click **Application**, and check the details of any error in the events.
10. Close Event Viewer.

► Task 2: Verify the user and group permissions and policy settings

1. On 6428A-NYC-DC1-01, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the left pane, under the **WoodgroveBank.com** node, expand the **NYC** node, and then click **Marketing**.
3. In the right pane, right-click **Monika Buschmann** and then click **Reset Password**.
4. In the **Reset Password** dialog box, in the **New password** box type **Pass@word1**.
5. In the **Confirm password** box type **Pass@word1**, and then click **OK**.
6. In the **Active Directory Domain Services** confirmation box, click **OK**.
7. Close Active Directory Users and Computers snap-in.
8. To start the **Terminal Services Configuration** snap-in on 6428A NYC-TS-03, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Configuration**.
9. In the **Connections** section, under **Connection Name**, right-click **RDP-Tcp**, and then click **Properties**.
10. In **the RDP-Tcp Properties** dialog box, click the **Security** tab. The Terminal Services Configuration message box is displayed. Click **OK** to close the message box.
11. On the **Security** tab, under **Group or user names** section, select **Dana Birkby**.
12. Click **Advanced**, select the record for Dana Birkby, click **Edit** and verify that the check box under **Deny** for **Remote Control** is not selected. If selected, clear the check box, and then click **OK** twice.
13. In the **RDP-Tcp Properties** dialog box, click the **General** tab.
14. In the **Encryption level** box, verify that the value is **Client Compatible**, and then click **OK**.
15. Close the Terminal Services Configuration snap-in.

► Task 3: Verify that the users are able to log on with the updated settings

1. On 6428A-NYC-DC1-01, click **Start**, click **Run**, in the **Open** box type **mstsc**, and then click **OK**.
2. In the **Remote Desktop Connection** dialog box, verify that the computer is **Nyc-ts**, and then click **Connect**.

Note: If the Remote Desktop Connection is disconnected, perform the following steps to create the remote connection:

   a. Open **Control Panel**.
   b. Click the **Network and Sharing Center** icon. Verify that NYC-DC is connected to Unidentified network.
   c. Check the status of the **Local Area Connection**.
   d. In the Network and Sharing Center window, under Tasks, **click Manage network connections**.
   e. In the Network Connections window, right-click **Local Area Connection**, and then click **Disable**.
   f. Then, right-click **Local area Connection** and click **Enable**.
   g. Close the Network Connections window. In the Network and Sharing Center window, verify that **NYC-DC** is connected to **WoodgroveBank.com**.

3. In the **Windows Security** dialog box, click **Use another account**, log on as **WOODGROVEBANK\Monika** with the password as **Pass@word1** and then click **OK**.
4. To log off **Monika**, click **Start**, point to the arrow key next to the lock computer button, and then click **Log off**.
5. To log on as the second user, click **Start**, click **Run**, type **mstsc**, and then click **OK**.
6. In the **Remote Desktop Connection** dialog box, click **Connect**.
7. In the **Windows Security** dialog box, click **Use another account**.
8. Log on as **WOODGROVEBANK\Dana** with the password as **Pa$$w0rd** and then click **OK**.
9. Close the remote connection.
10. The **Disconnect Terminal Services Session** dialog box is displayed. Click **OK**.

► Task4: Shut down the virtual machines

1. Exit the Lab Launcher tool by clicking the close button.
2. In the **Close** window, click **Turn off machine and discard changes**.
3. Click **OK**.

Results: After this exercise, you should have used troubleshooting techniques to resolve connectivity issues.

Module 4

Configuring Terminal Services RemoteApp and Easy Print

Contents:

Lab Answer Keys

Lab: Configuring TS RemoteApp and Easy Print

Exercise 1: Configuring and Deploying TS RemoteApp Programs

Exercise 2: Configuring TS Easy Print

Logon Information:

- Virtual Machine1: **6428A-NYC-DC1-01**
- Virtual Machine 2: **6428A-NYC-TS-03**
- User Name: **Administrator/Baris**
- Password: **Pa$$w0rd**

Estimated time: 45 minutes

Exercise 1: Configuring and Deploying TS RemoteApp Programs

Exercise Overview

In this exercise, you will install TS Web Access and create a link to Microsoft® PowerPoint Viewer for the Marketing group.

The main tasks for this exercise are as follows:

1. Start the 6428A-NYC-DC1-01 and 6428A-NYC-TS-03 virtual machines and log on to these machines as Administrator.
2. Install the TS Web Access role service.
3. Add the computer account of the TS Web Access server to the security group.
4. Specify the data source.
5. Install PowerPoint Viewer.
6. Add the PowerPoint Viewer program in the RemoteApp Programs list.
7. Configure an RDP file from the PowerPoint Viewer RemoteApp program.
8. Determine if the RemoteApp program is enabled for TS Web Access.
9. Configure the TS Web Access server to allow access from the Internet.

► Task1: Start the 6428A-NYC-DC1-01 and 6428A-NYC-TS-03 virtual machines and log on to these machines as Administrator

1. Start 6428A-NYC-DC1-01 using the Lab Launcher tool.
2. Log on using the default ID as **WOODGROVEBANK\Administrator and** password **Pa$$w0rd**. The **Server Manager** page is displayed by default.

Note: Wait for the domain controller 6428A-NYC-DC1-01 logon screen to appear before starting the 6428A-NYC-TS-03 virtual machine.

3. Start 6428A-NYC-TS-03 using the Lab Launcher tool.

4. Log on as **WoodgroveBank\Administrator** using the password **Pa$$w0rd**. The Server Manager page is displayed by default.

► Task 2: Install the TS Web Access role service

1. On 6428A-NYC-TS-03, in **Server Manager**, scroll down to the **Roles Summary** section, click the **Terminal Services** link. On **Terminal Services**, scroll down to **Roles Services**.
2. In the **Role Services** section, click the **Add Role Services** link.
3. On the **Select Role Services** page, select the **TS Web Access** check box. The Add Role Services dialog box is displayed.
4. Review the information about the required role services for Web Server (IIS) and click **Add Required Role Services**, and then click **Next**.
5. Review the **Web Server (IIS)** page, and then click **Next**.
6. On the **Select Role Services** page, you are prompted to select the role services that you want to install for IIS. Then, click **Next**.
7. On the **Confirm Installation Selections** page, click **Install**.
8. On the **Installation progress** page, note the installation progress. On completion of the installation, the Installation Results page is displayed.
9. On the **Installation Results** page, confirm that the installation of TS Web Access succeeded, and then click **Close**.
10. On the **Server Manager** page under **Roles Services**, confirm that **TS Web Access** is **Installed**.
11. Close the **Server Manager**.

► Task 3: Add the computer account of the TS Web Access server to the security group

1. On 6428A-NYC-TS-03, click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
2. In the left pane, click the **Local Users and Groups** node, and then click the **Groups** node.
3. In the middle pane, double-click the group name **TS Web Access Computers**.
4. In the **TS Web Access Computers Properties** dialog box, to add members in the group, click the **Add** button.
5. In the **Select Users, Computers, or Groups** dialog box, click **Object Types**.
6. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
7. In the **Enter the object names to select {examples}** box, type **NYC-TS** as the computer account of the TS Web Access server, click **Check Names**, and then click **OK**.
8. Click **OK** to close the **TS Web Access Computers Properties** dialog box.

► Task 4: Specify the data source

1. To start **Internet Explorer**, click **Start**, click **All Programs**, and then click **Internet Explorer**.
2. To connect to the TS Web Access Web site, in the URL box, type **http://NYCTS/ts**. Click the **go** button.
3. In the **Connect to nyc-ts** dialog box, log on to the site as **WoodgroveBank\Administrator** with the password **Pa$$w0rd**.

4. A message box regarding the blocked content is displayed. To add the site as a trusted site, click the **Add** button.
5. The **Trusted sites** message box is displayed. Click **Add**.
6. Close the Trusted sites message box.

Note: If you are already logged on to the computer, you are not prompted for the credentials. You need to add the Web site as a trusted Web site only the first time you access the site.

7. On the title bar, click the **Configuration** tab.
8. On the right side of the page, in the **Editor Zone** area, in the **TS Web Access Properties** section, in the **Terminal server name** box, type **NYC-TS**.
9. Click **Apply** to apply the changes.

► Task 5: Install PowerPoint Viewer

1. Click **Start**, and then click **Command Prompt**.
2. At the command prompt, type **change user /install**, press ENTER, and then close the window.
3. Click **Start**, click **Control Panel**, and then double-click the **Install Application on Terminal Server** icon.
4. In the **Install Program From Floppy Disk or CD-ROM** wizard, click **Next**.
5. Click **Browse**. In the left pane, click **Computer**, and then browse to **E:\Tools**.
6. At the bottom of the page, in the **Setup programs** box, select **All Files** from the drop-down list.
7. Double-click **PowerPointViewer.exe**.
8. In the **Run Installation Program** page, click **Next**.
9. In the **Microsoft Office PowerPoint Viewer 2007** license agreement page, select the check box to accept the license terms, and click **Continue**.
10. The **Microsoft Office PowerPoint Viewer 2007** message box informing about the completion of the installation is displayed. Click **OK**.
11. On the **Finish Admin Install** page, click **Finish**.

► Task 6: Add the PowerPoint Viewer program in the RemoteApp Programs list

1. Start **TS RemoteApp Manager** on 6428A-NYC-TS-03. Click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS RemoteApp Manager**.
2. In the **Actions** pane on the right, click **Add RemoteApp Programs**.
3. On the **Welcome to the RemoteApp Wizard** page, click **Next**.
4. On the **Choose programs to add to the RemoteApp Programs list** page, select the check box next to Microsoft Office PowerPoint Viewer 2007 program.
5. Click **Microsoft Office PowerPoint Viewer 2007 program**, and then click **Properties**.
6. In the **RemoteApp Properties** dialog box, verify that the **RemoteApp program is available through TS Web Access** check box is selected, click **OK**, and then click **Next**.

7. On the **Review Settings** page, review the settings and then click **Finish**.

► Task 7: Configure an RDP file from the PowerPoint Viewer RemoteApp program

1. Scroll down to the **RemoteApp Programs** list and click **Microsoft Office PowerPoint Viewer 2007**.
2. On the **Actions** pane under **Microsoft PowerPoint Viewer 2007**, click **Create .rdp File**.
3. On the **Welcome to the Remote App Wizard** page, click **Next**.
4. On the **Specify Package Settings page**:
   - Keep the default location to save the program as **C:\Program Files\Packaged Programs**.
   - Verify that the terminal server setting is **NYC-TS.WoodgroveBank.com**.
   - Verify that the required server authentication is set to **Yes**.
   - Verify that the port is **3389**.
5. Click **Next**.
6. On the **Review Settings** page, click **Finish**.

► Task 8: Determine if the RemoteApp program is enabled for TS Web Access

1. On 6428A-NYC-TS-03, in the **RemoteApp Programs** list, verify that a **Yes** value appears for **TS Web Access** next to **Microsoft Office PowerPoint Viewer 2007** that you want to make available through TS Web Access.
2. Click **Start**, click **All Programs**, and then click **Internet Explorer**.
3. In **URL** box type **http:// NYC-TS/TS**.
4. In the **Connect to nyc-ts** dialog box, provide user credentials from the Marketing Group. In **User name** type **WoodGroveBank\Baris** and provide password **Pa$$w0rd**, and then click **OK**.

► Task 9: Configure the TS Web Access Server to allow access from the Internet

1. On 6428A-NYC-TS-03, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the left pane of **Internet Information Services (IIS) Manager**, click the **NYC-TS(WOODGROVEBANK\Administrator)** node, click the **Sites** node, click the **Default Web Site** node, and then click **TS**.
3. In the middle pane, scroll down to **IIS**, double-click the **Authentication** icon.
4. Verify **Windows Authentication** is set to **Enabled**. If it is not, right-click **Windows Authentication**, and then click **Enable**.

Results: After this exercise, you should have installed the PowerPoint program and created a link to C:\Program Files\Packaged Programs.

Exercise 2: Configuring TS Easy Print

Exercise Overview

The main tasks for this exercise are as follows:

1. Configure the printer redirection settings.
2. Shut down the virtual machines.

► Task 1: Configure the printer redirection settings

1. On 6428A-NYC-DC1-01, start the **Group Policy Management** snap-in. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. In the left panel, under **Group Policy Management**, click **Forest:**

   WoodgroveBank.com, followed by **Domains**, **WoodgroveBank.com**, **NYC** nodes, and right click the **Marketing** node.
3. Click **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** dialog box, under the **Name** box, type **GPO for RDP Link**, and then click **OK**.
5. In the left panel, click the **Marketing** node, right click **GPO for RDP link**, and then click **Edit**.
6. In the left panel on the **Group Policy Management Editor** page, under **Computer Configuration**, click **Policies** and **Administrative Templates** nodes, and then click the **Windows Components** node.
7. Under **Windows Component**, click the **Terminal Services** node, and then click the **Terminal Server** node.
8. In the left panel, double-click **Printer Redirection**.
9. In the right panel, double-click **Use Terminal Services Easy Print printer driver first**.
10. In the **Use Terminal Services Easy Print printer driver first Properties** dialog box, on the **Setting** tab, select **Enabled**, and then click **OK**.
11. In the right panel, double-click **Redirect only the default client printer**.
12. In the **Redirect only the default client printer Properties** dialog box, on the **Setting** tab, select **Enabled**, and then click **OK**.

► Task 2: Shut down the virtual machines

1. Exit the Lab Launcher tool by clicking the close button.
2. In the **Close** window, click **Turn off machine and discard changes**.
3. Click **OK**.

Results: After this exercise, you should have configured TS Easy Print and the client print driver should have been redirected to TS.

Module 5

Configuring Terminal Services Web Access and Session Broker

Contents:

Lab Answer Keys

Lab: Configuring TS Web Access and Session Broker

Exercise 1: Configuring TS RemoteApp Programs for TS Web Access.

Exercise 2: Customizing TS Web Access by Using WSS.

Exercise 3: Configuring TS Session Broker.

Logon Information:

- Virtual Machine1: **6428A-NYC-DC1-01**
- Virtual Machine 2: **6428A-NYC-TS-05**
- Virtual Machine 2: **6428A-NYC-WEB-05**
- User Name: **Administrator/Bernard**
- Password: **Pa$$w0rd**

Estimated time: 60 minutes

Exercise 1: Configuring TS RemoteApp Programs for TS Web Access

Exercise Overview

In this exercise, you will install and configure the TS Web Access role service on the terminal server and create a .msi file for Microsoft® Office PowerPoint Viewer. A link for this .msi file needs to be created so that the Marketing group can access it through a Web browser.

The main tasks for this exercise are as follows:

1. Start the 6428A-NYC-DC1-01, 6428A-NYC-TS-05, and 6428A-NYC-WEB-05 virtual machines and log on to these machines as Administrator.
2. Install the TS Web Access role service.
3. Determine if the RemoteApp program is enabled for TS Web Access.
4. Create an MSI file.
5. Create a link to the TS RemoteApp program on the terminal server.
6. Verify that the link is functional and available through the Web browser.

► Task1: Start the 6428A-NYC-DC1-01, 6428A-NYC-TS-05, and 6428ANYC-WEB-05 virtual machines and log on to these machines as Administrator

1. Start 6428A-NYC-DC1-01using the Lab Launcher tool.
2. Log on using the default **WOODGROVEBANK\Administrator** user ID and password **Pa$$w0rd**.
3. Start 6428A-NYC-TS-05 using the Lab Launcher tool.
4. Log on as **WoodgroveBank\Administrator** by using the password **Pa$$w0rd**.
5. Start 6428A-NYC-WEB-05 using the Lab Launcher tool.
6. Log on as **WOODGROVEBANK\Administrator** by using the password **Pa$$w0rd**.

► Task 2: Install the TS Web Access role service

1. Start the **Server Manager** snap-in on 6428A-NYC-TS-05. In the snap-in, scroll down to **Roles Summary**, and click the **Terminal Services** link.
2. Scroll down to **Role Services**, and click the **Add Role Services** link.
3. On the **Select Role Services** page, select the **TS Web Access** check box.
4. In the **Add Role Services** message box, click **Add Required Role Services**.
5. On the **Select Role Services** page, click **Next**.
6. On the **Web Server (IIS)** page, click **Next**.
7. On the **Select Role Services** page, click **Next**.
8. On the **Confirm Installation Selections** page, click **Install**.
9. The **Installation Progress** page is displayed. Observe the progress indicator.
10. On the **Installation Results** page, observe that the installation of TS Web Access succeeded, and then click **Close**.
11. On the **Server Manager** page, under **Role Services**, verify that TS Web Access is installed.
12. Close the Server Manager.
13. On 6428A-NYC-TS-05, click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
14. In the left pane of the **Computer Management** window, click the **Local Users and Groups** node, and then click **Groups**.
15. In the right pane, double-click **TS Web Access Computers**.
16. In the **TS Web Access Computers Properties** dialog box, click **Add** to add members in the group.
17. In the **Select Users, Computers, or Groups** dialog box, click **Object Types**.
18. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
19. In the **Enter the object names to select (examples)** box, type **NYC-TS** as the computer account of the TS Web Access server. Click **Check Names**, and then click **OK**.
20. Click **OK** to close the **TS Web Access Computers Properties** dialog box.
21. Click **Start**, click **All Programs**, and then click **Internet Explorer**.
22. In the **URL** box, type **http://NYC-TS/ts**, and then press ENTER.
23. In the **Connect to nyc-ts** dialog box, log on to the site by using **WoodgroveBank\Administrator** as the login ID and **Pa$$w0rd** as the password, and then click **OK**.
24. A message box regarding blocked content is displayed. To add the site as a trusted site, click the **Add** button.
25. The **Trusted sites** message box is displayed. Click Add.
26. Close the **Trusted sites** message box.

Note: If you are already logged on to the computer, you are not prompted for the credentials. You need to add the Web site as a trusted Web site only the first time you access the site.

27. On the title bar, click the **Configuration** tab.
28. On the right side of the page, in the **Editor Zone** section, in the **TS Web Access Properties** section, in the **Terminal Server name** box, type **NYC-TS**.
29. Click **Apply** to apply the changes.

► Task 3: Determine if the RemoteApp program is enabled for TS Web Access

1. On 6428A-NYC-TS-05, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS RemoteApp Manager**.
2. Scroll down to the **RemoteApp Programs** list and verify that a **Yes** value appears for **TS Web Access** next to **Microsoft Office PowerPoint Viewer 2007**.
3. Click **Microsoft Office Power Point Viewer 2007**.
4. To enable a RemoteApp program for TS Web Access, on the **Actions** pane for **Microsoft Office PowerPoint Viewer 2007**, click **Show in TS Web Access**.
5. Close the **TS RemoteApp Manager**.

► Task 4: Create an MSI file

1. On 6428A-NYC-TS-05, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS RemoteApp Manager**.
2. Scroll down to the **RemoteApp Programs** list, and click **Microsoft Office PowerPoint Viewer 2007**.
3. In the **Actions** pane for **Microsoft Office PowerPoint Viewer 2007**, click **Create Windows Installer package**.
4. On the **Welcome to the RemoteApp Wizard** page, click **Next**.
5. On the **Specify Package Settings** page, click **Next**.
6. On the **Configure Distribution Package** page, click **Next**.
7. On the **Review Settings** page, click **Finish**.
8. Close the **Packaged Programs** folder.

► Task 5: Create a link to the TS RemoteApp program on the terminal server

1. On the **TS RemoteApp Manager** page, in the **RemoteApp Programs** list, verify that a **Yes** value is displayed for **TS Web Access** next to **Microsoft Office PowerPoint Viewer 2007**.
2. Click **Start**, click **All Programs**, and then click **Internet Explorer**.
3. In the **URL** box, **type http:// NYC-TS/ts**, and then click **Go**.
4. In the **Connect to nyc-ts** dialog box, provide a user credential from the Marketing Group. In **User name**, type **WoodGroveBank\Bernard** and type the password as **Pa$$w0rd**, and then click **OK**.
5. A message box regarding blocked content is displayed. To add the site as a trusted site, click the **Add** button, and then click **Close**.
6. Configure the TS Web Access server to allow access from the Internet. On 6428A-NYC-TS-05, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
7. In the left pane of Internet Information Services (IIS) Manager, expand the **NYC-TS (WOODGROVEBANK\Administrator)** node, expand the **Sites** node, expand the **Default Web Site** node, and then click **TS**.

8. In the middle pane, scroll down to **IIS**, and double-click the **Authentication** icon.
9. Select **Status** from the **Group by** drop-down list. Select **Enabled** for **Windows Authentication**.

► Task 6: Verify that the link is functional and available through the Web browser

1. On 6428A-NYC-WEB-05, verify that you are logged on as **Woodgrovebank\Administrator** with the password **Pa$$w0rd**.
2. Click **Start**, click **All Programs**, and then click **Internet Explorer**. In the **URL** box, type **http://NYC-TS/ts**, and then click **Go**.
3. In the **Connect to nyc-ts** dialog box, type the user name as **WoodgroveBank\Bernard** and the password as **Pa$$w0rd**. Then click **OK**.
4. The Trusted Sites message box is displayed. Click **Add**. Close the Trusted Sites message box.
5. Observe that **Microsoft Office PowerPoint** is listed in the remote application program list.

Results: After this exercise, you should have installed TS Web Access on the terminal server, created an MSI file for the remote program, created a link to the remote program, and verified that the link is functional through Internet Explorer.

Exercise 2: Customizing TS Web Access by Using WSS

Exercise Overview

In this exercise, you will create a customized Web part and export it to a WSS Web site.

The main task for this exercise is as follows:

- Add a Web part to a WSS site.

► Task 1: Add a Web part to a WSS site

1. On 6428A-NYC-WEB-05, click **Start**, point to **Administrative Tools**, and then click **SharePoint 3.0 Central Administration**.
2. To connect to the WSS site **http://nyc-web:44341/,** in the authentication dialog box, type the user name as **WoodgroveBank\Administrator** and password as **Pa$$w0rd**. Then click **OK**.
3. On the **Home** page of the **Central Administration** site, click **Site Actions**, and then select **Edit Page** from the drop-down list.
4. On the **Edit Page**, in the center panel, click **Add a Web Part**.
5. On the **Add Web Parts – Webpage Dialog** page, in the **Add Web Parts to Left** section, under the **List and Libraries** section, select the **Resources** check box, and then click **Add**.
6. On the **Central Administration** page, under the **Resources** section, click the **Add new link link**.
7. On the **Resources: New Item** page, in the **URL** box, type **http:// NYC-TS/ts**.
8. In the **Description** box, type **Link for TS Web Access Web Part**, and then click **OK**.
9. Connect to **NYC-ts** and click **Link for TS Web Access Web Part**. The Connect to nyc-ts dialog box is displayed.
10. Log on to the site as **WOODGROVEBANK\Administrator** with the password **Pa$$w0rd**. Then click **OK**.

    The TS Web Access Web site with the remote applications list will be displayed.

Results: After this exercise, you should have added a customized Web part by using TS Web Access, and exported it to a WSS site.

Exercise 3: Configuring TS Session Broker

Exercise Overview

In this exercise, you will install the Session Broker role service and configure the TS Session Broker settings for servers in a TS farm.

The main tasks for this exercise are as follows:

1. Install the TS Session Broker role service.
2. Add each server in the farm to the Session Directory Computers local group.
3. Configure the TS Session Broker settings by using Group Policy.
4. Shut down the virtual machines.

► Task 1: Install the TS Session Broker role service

1. On 6428A-NYC-TS-05, start **Server Manager**. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. Scroll down to the **Roles Summary** section, click the **Terminal Services** link.
3. On the **Terminal Services** page, scroll down to **Role Services**, and then click the **Add Role Services** link.
4. On the **Select Role Services** page, select the **TS Session Broker** check box, and then click **Next**.
5. On the **Confirm Installation Selections** page, click **Install**.
6. The Installation Progress page is displayed. Observe the progress indicator.
7. On the **Installation Results** page, confirm that the installation succeeded, and then click **Close**.

► Task 2: Add each server in the farm to the Session Directory Computers local group

1. Click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
2. In the left pane, click the **Local Users and Groups** node, and then click **Groups**.
3. In the middle pane, right-click the **Session Directory Computers** group, and then click **Properties**.
4. In the **Session Directory Computer Properties** dialog box, click **Add**.
5. In the **Select Users, Computers or Groups** dialog box, click **Object Types**.
6. In the **Object Type** dialog box, select the **Computers** check box, and then click **OK**.
7. In the **Enter the object names to select {examples}** box, type **NYC-WEB; NYC–TS**, and then click **Check Names**. Click **OK** twice.
8. Close Computer Management.

► Task 3: Configure the TS Session Broker settings by using Group Policy

1. On 6428A-NYC-DC1-01, click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.

2. In the Group Policy Management snap-in, in the left pane, expand the **Forest: WoodgroveBank.com** node, followed by **Domains** and **WoodgroveBank.com**. Then, right-click the **NYC** node, and click **Create a GPO in this domain, and Link it here**.
3. In the **New GPO** dialog box, in the **Name** box, type **GPO for TS Web Access**, and then click **OK**.
4. In the left pane, expand the **Group Policy Objects** node, and expand **GPO for TS Web Access**.
5. In the right pane, click the **Settings** tab.
6. Right-click **Computer Configuration**, and then click **Edit**.
7. In the left pane, expand the **Computer Configuration** node, expand the **Policies** node, expand **Administrative Templates** followed by the **Windows Components**, **Terminal Services**, **Terminal Server** nodes, and then click **TS Session Broker**.
8. In the right pane, double-click the **Join TS Session Broker** policy setting.
9. In the **Join TS Session Broker Properties** dialog box, click **Enabled**, and then click **OK**.
10. Double-click the **Configure TS Session Broker farm name** policy setting.
11. In the **Configure TS Session Broker farm name Properties** dialog box, click **Enabled**.
12. In the **TS Session Broker farm name** box, type **NYC-TS**, and then click **OK**.
13. Double-click the **Use TS Session Broker load balancing** policy setting.
14. In the **Use TS Session Broker load balancing Properties** dialog box, click **Enabled**, and then click **OK**.
15. Close the **Group Policy Management editor**.

► Task 4: Shut down the virtual machines

1. Exit the Lab Launcher tool by clicking the close button.
2. In the **Close** window, click **Turn off machine and discard changes**.
3. Click **OK**.

Results: After this exercise, you should have configured TS Session Broker load balancing for a farm.

Module 6

Configuring and Troubleshooting Terminal Services Gateway

Contents:

Lab Answer Keys

Lab: Configuring and Troubleshooting TS Gateway

Exercise 1: Configuring and Monitoring TS Gateway

Exercise 2: Troubleshooting the TS Gateway Connections

Logon Information:

- Virtual Machine1: **6428A-NYC-DC1-06**
- Virtual Machine 2: **6428A-NYC-TS-05**
- User Name: **Administrator**
- Password: **Pa$$w0rd**

Estimated time: 60 minutes

Exercise 1: Configuring and Monitoring TS Gateway

Exercise Overview

In this exercise, you will install and configure the TS Gateway server role on the terminal server and create a CAP and a RAP for the HR group.

The main tasks for this exercise are as follows:

1. Start the 6428A-NYC-DC1-06 and 6428A-NYC-TS-05 virtual machines and log on to these machines as Administrator.
2. Install the TS Gateway role.
3. Install the certificate.
4. Create a CAP for the HR group.
5. Select the pre-configured Active Directory Security group HR.
6. Create a RAP for the HR group.

► Task1: Start the 6428A-NYC-DC1-06 and 6428A-NYC-TS-05 virtual machines and log on to these machines as Administrator

1. Start 6428A-NYC-DC1-06 using the Lab Launcher tool.
2. Log on as **WOODGROVEBANK\Administrator** by using the password **Pa$$w0rd**. The Server Manager snap-in is displayed.
3. Start 6428A-NYC-TS-05 using the Lab Launcher tool.
4. Log on as **Administrator** by using the password **Pa$$w0rd**. The Server Manager snap-in is displayed.

► Task 2: Install the TS Gateway role

1. On 6428A-NYC-TS-05, in the **Server Manager** snap-in, scroll down to **Roles Summary**, click the **Terminal Services** link.
2. Scroll down to **Role Services**, click **Add Role Services**.
3. On the **Select Role Services** page, select the **TS Gateway** check box.

4. On the **Select Role Services** page, click **Next**.
5. On the **Choose a Server Authentication Certificate for SSL Encryption** page, select **Choose a certificate for SSL encryption later**, and then click **Next**.
6. On the **Create Authorization Policies for TS Gateway** page, select **Later**, and then click **Next**.
7. On the **Confirm Installation Selections** page, click **Install**. The Installation Progress page is displayed.
8. On the **Installation Results** page, observe that the installation for TS Gateway roles, role services, and features is successful, and then click **Close**.
9. Close the Server Manager snap-in.

► Task 3: Install the certificate

1. Click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS Gateway Manager**.
2. In the **TS Gateway Manager** console tree, right-click **NYC-TS (Local)**, and then click **Properties**.
3. On the **NYC-TS Properties** page, click the **SSL Certificate** tab, verify that the **Create a self-signed certificate for SSL encryption** option is selected, and then click **Create Certificate**.
4. In the **Create Self-Signed Certificate** dialog box, under **Certificate name** verify that **NYC-TS.WoodgroveBank.com** appears by default.
5. Under **Certificate location**, delete the default location, type **c:\certificate\NYC-TS.cer**, and then click **OK**.
6. A message box stating that TS Gateway has successfully created a self-signed certificate is displayed. Click **OK** twice.
7. Close the TS Gateway Manager.
8. To open the **Certificates snap-in**, click **Start**, click **Run**, type **MMC**, and then click **OK**. The Console1-[Console Root] window is displayed.
9. On the **File** menu, click **Add/Remove Snap-in**.
10. In the **Add or Remove Snap-ins** dialog box, under the **Available snap-ins** list, click **Certificates**, and then click **Add**.
11. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
12. In the **Select Computer** dialog box, verify that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**.
13. In the **Add or Remove snap-ins** dialog box, click **OK**.
14. In the console dialog box, in the console tree, double-click the **Certificates (Local Computer)** node.
15. Right-click the **Trusted Root Certification Authorities** folder, point to **All Tasks**, and then click **Import**.
16. On the **Certificate Import Wizard** page, click **Next**.
17. On the **File to Import** page, in the **File name** box type **c:\certificate\NYCTS.cer**, and then click **Next**.
18. On the **Certificate Store** page, click **Next**.

19. On the **Completing the Certificate Import Wizard** page, click **Finish**.
20. A message stating that the import was successful is displayed. Click **OK**.
21. In the **Console1-[Console Root]** window, click **File**, and then click **Exit**.
22. A message prompting you to save the console settings to Console1 is displayed. Click **No**.
23. To open the **TS Gateway Manager**, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS Gateway Manager**.
24. In the **TS Gateway Manager** console tree, right-click **NYC-TS(Local)**, and then click **Properties**.
25. In the **NYC-TS Properties** dialog box, click the **SSL Certificate** tab, verify **Select an existing certificate for SSL encryption (recommended)** is selected, and then click **Browse Certificates**.
26. In the **Install Certificate** dialog box, click **NYC-TS.WoodgroveBank.com**, click **Install**, and then click **OK**.

► Task 4: Create a CAP for the HR group

1. In the **TS Gateway Manager** console tree, expand the **NYC-TS(Local)** node, and then expand the **Policies** node.
2. Under **Policies**, right-click the **Connection Authorization Policies** folder, point to **Create New Policy**, and then click **Custom**.
3. In the **New TS CAP** dialog box, on the **General** tab, in **Policy name**, type **TS CAP**.
4. Click the **Requirements** tab, under **Supported Windows authentication methods**, verify that **Password** is selected.
5. Under **User group membership (required)**, click **Add Group**.
6. In the **Select Groups** dialog box, click **Advanced**, and then click **Find Now**.
7. Under the **Search Results** section, scroll down and select the group name **HR**, click **OK** twice.
8. In the **New TS CAP** dialog box, click the **Device Redirection** tab, verify that **Enable device redirection for all client devices** is selected, and then click **OK**.
9. Close the **TS Gateway Manager**.

► Task 5: Select the pre-configured Active Directory Security group HR

1. On 6428A-NYC-DC1-06, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** console tree, under the **WoodgroveBank.com** node, click **Users**.
3. In the right pane, click **HR Security Group**.
4. Right-click **HR Security Group**, click **Properties**.
5. In the **HR Properties** dialog box, click the **Members** tab, and then click **Add**.
6. In the **Select Users, Contacts, Computers or Groups** dialog box, click **Object Types**.
7. Select the **Computers** check box, and then click **OK**.
8. Click **Advanced**, and then click **Find Now**.

9. Under the **Search Results** section, scroll down to select the computer name as **NYC-TS**, click **OK**. Then click **OK** twice.
10. Close Active Directory Users and Computers.

► Task 6: Create a RAP for the HR group

1. Start the **TS Gateway Manager** on 6428A-NYC-TS-05. Click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS Gateway Manager**.
2. In the console tree, open the **NYC-TS (Local)** folder.
3. Open the **Policies** folder, and then right-click the **Resource Authorization Policies** folder, point to **Create New Policy**, and then click **Custom**.
4. In the **New TS RAP** dialog box, on the **General** tab, in **Policy name**, type **TS RAP**.
5. On the **User Groups** tab, click **Add**.
6. In the **Select Groups** dialog box, click **Advanced**, click **Find Now**.
7. Under the **Search Results** section, scroll down to select the group name **HR**, and then click **OK** twice.
8. Click the **Computer Group** tab, verify **Select an existing Active Directory security group** is selected, and then click **Browse**.
9. In the **Select Groups** dialog box, click **Advanced**, and then click **Find Now**.
10. Under the **Search Results** section, scroll down to select group **HR**, and then click **OK** twice.
11. Click **Allowed Ports** tab, verify **Allow connections only through TCP port 3389** is selected, and then click **OK**.

Results: After this exercise, you should have installed the TS Gateway Server role service and created a TS CAP and TS RAP for the HR group.

Exercise 2: Troubleshooting the TS Gateway Connections

Exercise Overview

In this exercise, you need to verify that the TS Gateway server certificate has not expired. You also need to check the TS CAP and RAP for the HR group. In addition, you need to verify the existence of the user Baris in the HR group and add a new user Bernard to the HR group.

The main tasks for this exercise are as follows:

1. Verify that the TS Gateway Server certificate has not expired.
2. Verify that the TS CAP is accurate.
3. Verify that the TS RAP is accurate.
4. Verify that the user Baris exists in the HR group.
5. Add Bernard to the HR group.
6. Verify that the TS RAP is functional.
7. Shut down the virtual machines.

► Task 1: Verify that the TS Gateway Server certificate has not expired

1. In the **TS Gateway Manager**, in the console tree, right-click **NYC-TS (Local)**, and then click **Properties**.

2. In the **NYC-TS Properties** dialog box, click the **SSL Certificate** tab, verify **Select an existing certificate for SSL encryption (recommended)** is selected, and then click **Browse Certificates**.
3. In the **Install Certificate** dialog box, click **NYC-TS.WoodgroveBank.com**.
4. Click **View Certificate** and verify that the validity of certificate has not expired in the valid from field.
5. Click **OK**, click **Cancel**, and then click **OK**.

► Task 2: Verify that the TS CAP is accurate

1. In the console tree, under the **NYC-TS (Local)** node, under the **Policies** node, click **Connection Authorization Policies**.
2. In the right pane, right-click **TS CAP** policy, and then click **Properties**.
3. In the **TS CAP Properties** dialog box, on the **General** tab, verify that **Enable this policy** is selected.
4. Click the **Requirements** tab. Under **Supported Windows authentication methods**, verify that **Password** is selected.
5. Under **User group membership (required)**, verify that **WOODGROVEBANK\HR** group exists.
6. Click **Device Redirection** tab, verify **Enable device redirection for all client devices** is selected, and then click **OK**.

► Task 3: Verify that the TS RAP is accurate

1. In **TS Gateway Manager**, under the **Policies** node, click **Resource Authorization Policies**.
2. In the right-pane, right-click **TS RAP policy**, and then click **Properties**.
3. In the **TS RAP Properties** dialog box, on the **General** tab, verify **Enable this policy** is selected.
4. Click the **User Groups** tab and verify that the **WOODGROVEBANK\HR** group exists.
5. Click the **Computer Group** tab, under **Select an existing Active Directory security group**, verify that **WOODGROVEBANK\HR** exists.
6. Click **Allowed Ports** tab, verify A**llow connections only through TCP port 3389** is selected, and then click **OK**.
7. Close the TS Gateway Manager.

► Task 4: Verify that the user Baris exists in the HR group

1. On 6428A-NYC-DC1-06, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** console tree, under **WoodgroveBank.com**, click **Users**.
3. In the right pane, click **HR Security Group**.
4. Right-click **HR Security Group**, click **Properties**.
5. In the **HR Properties** dialog box, click the **Members** tab, verify user **Baris Cetinok** exists, and then click **OK**.

► Task 5: Add Bernard to the HR group

1. In **Active Directory Users and Computers**, under **WoodgroveBank.com**, click **Users**.
2. In the right pane, right-click **HR** Security group, and then click **Properties**.

3. In the **HR Properties** dialog box, click the **Members** tab, and then click **Add**.
4. In the **Select Users, Contacts, Computers or Groups** dialog box, click **Advanced**, and then click **Find Now**.
5. Scroll down to select user name **Bernard Duerr**, click **OK**,
6. In the **Active Directory Domain Services** dialog box, click **OK** twice.
7. Close Active Directory Users and Computers.

► Task 6: Verify that the TS RAP is functional

1. On 6428A-NYC-TS-05, click **Start**, click **Run**, type **\\NYC-TS\certificate**, and then click **OK**.
2. In the **Certificate (\\NYC-TS) Explorer**, select **NYC-TS.cer**.
3. Right-click **NYC-TS.cer**, click **Install Certificate**.
4. The **Open file – Security Warning** dialog box is displayed, click **Open**.
5. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
6. On the **Certificate Store** page, select **Place all certificates in the following store**, and then click **Browse**.
7. In the **Select Certificate Store** dialog box, select **Trusted Root Certification Authorities**, click **OK**, and then click **Next**.
8. On the **Completing the Certificate Import Wizard** page, click **Finish**.
9. A message box that the import was successful is displayed, click **OK**.
10. Close **Certificate Explorer**.
11. On 6428A-NYC-DC1-06, click **Start**, click **Run**, type **mstsc**, and then click **OK**.
12. In the **Remote Desktop Connection** dialog box, click **Options**, click the **Advanced** tab, and then click **Settings**.
13. On the **TS Gateway Server Settings** page, select **Use these TS Gateway Server settings**.
14. In the **Server name** box, type **NYC-TS.woodgrovebank.com**, in the **Logon method** box select **Ask for password (NTLM)** from the drop-down list, and then click **OK**.
15. Click the **General** tab, in the **Computer** box, type **NYC-TS**, and then click **Connect**.
16. . In the **Windows Security** dialog box, type user name as **Woodgrovebank\Baris** and password as **Pa$$w0rd**, and then click **OK**.
17. Close **Remote Desktop Connection**.

► Task 7: Shut down the virtual machines

1. Exit the Lab Launcher tool by clicking the close button.
2. In the **Close** window, click **Turn off machine and discard changes**.
3. Click **OK**.

Results: After this exercise, you should have verified that the configuration of TS Gateway is correct and the user Baris exists in the HR group. In addition, you should have added a new user Bernard to the HR group.

Module 7

Managing and Monitoring Terminal Services

Contents:

Lab Answer Keys

Lab: Managing and Monitoring TS

Exercise 1: Managing the TS Connections

Exercise 2: Monitoring the TS Connections

Exercise 3: Configuring WSRM for TS

Logon Information:

- Virtual Machine1: **6428A-NYC-DC1-06**
- Virtual Machine 2: **6428A-NYC-TS-07**
- Virtual Machine 2: **6428A-NYC-WEB-05**
- User Name: **Administrator/Susan**
- Password: **Pa$$w0rd**

Estimated time: 60 minutes

Exercise 1: Managing the TS Connections

Exercise Overview

In this exercise, you will configure the TS Gateway settings on the client computer. You will then disconnect the NOC technician's computer and reset the connection.

The main tasks for this exercise are as follows:

1. Start the 6428A-NYC-DC1-06 and 6428A-NYC-TS -07 virtual machines and logon to these machines as Administrator.
2. Start the 6428A-NYC-WEB-05 virtual machine and log on as Susan.
3. Configure the TS Gateway settings on the client.
4. Manage the TS connections on the terminal server.

► Task1: Start the 6428A-NYC-DC1-06 and 6428A-NYC-TS-07 virtual machines and log on to these machines as Administrator

1. Start 6428A-NYC-DC1-06 using the Lab Launcher tool.
2. The default login ID **WOODGROVEBANK\Administrator** is displayed. Logon with the password **Pa$$w0rd**.

Note: Wait for the domain controller, 6428A-NYC-DC1-06, logon screen to appear before starting 6428A-NYC-TS-07 virtual machine.

3. Start 6428A-NYC-TS-07 using the Lab Launcher tool.
4. Log on as **WoodgroveBank\Administrator** with the password **Pa$$w0rd**.
5. On 6428A-NYC-DC1-06, to verify the membership of the **NYC-TS,** click **Start,** point to **Administrative Tools**, and then click **Active Directory users and Computers**.

6. In the left pane, click **Computers** node.
7. In the right pane, verify that the computer name **NYC-TS** exists.

► Task 2: Start the 6428A-NYC-WEB-05 virtual machine and log on as Susan

1. Start 6428A-NYC-WEB-05 using the Lab Launcher tool.
2. Log on as **WoodgroveBank\Susan** who belongs to the NOC Department by using the password **Pa$$w0rd**.

► Task 3: Configure the TS Gateway settings on the client

1. To configure TS Gateway on 6428A-NYC-WEB-05, click **Start**, click **All Programs**, click **Accessories**, and then click **Remote Desktop Connection**.
2. In the **Remote Desktop Connection** dialog box, click **Options**, and then click the **Advanced** tab.
3. On the **Advanced** tab, under **Connect from anywhere** area, click **Settings**.
4. Under **Connection settings**, select **Use these TS Gateway server settings**.
5. In the **Server name** box, verify that the FQDN of TS Gateway Server is **NYCTS.Woodgrovebank.com**.
6. Under **Logon method**, verify that **Ask for password (NTLM)** from the dropdown list is selected
7. Verify that the **Bypass TS Gateway server for local address** check box is not selected. If selected, then clear the check box and then click **OK**.
8. Click the **General** tab. Under **Logon settings**, in the **Computer** box, type **NYC-TS**.
9. Click **Save**, and then click **Connect**.
10. In the **Windows Security** dialog box, enter the login ID as **Woodgrovebank\Susan**. Log on with the password **Pa$$w0rd**, and then click **OK**.

Note: If the Remote Desktop Connection is disconnected, perform the following steps tocreate the remote connection:

a. Log off **WoodgroveBank\Susan** on 6428A-NYC-WEB-05.
b. Log on to 6428A-NYC-WEB-05 as **Administrator** with the password **Pa$$w0rd**.
c. Open **Control Panel**.
d. Click the **Network and Sharing Center** icon. Verify that NYC-WEB is connected to Unidentified network.
e. Check the status of the **Local Area Connection**.
f. In the **Network and Sharing Center** window, under **Tasks**, click **Managenet work connections**.
g. In the Network Connections window, right-click Local Area Connection, and then click Disable.
h. Then, right-click Local area Connection and click Enable.
i. Close the Network Connections window. In the Network and Sharing Center window, check whether NYC-WEB is connected toWoodgroveBank.com.

11. Log off as administrator and log on as **WoodgroveBank\Susan** using the password **Pa$$w0rd**.

► Task 4: Manage the TS connections on the terminal server

1. To log off all TS Gateway connections on 6428A-NYC-TS-07, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **Terminal Services Manager**.
   a. In **Terminal Services Manager**, the **Terminal Services Manager** dialog box is displayed, click **OK**. In the left panel, select **NYC-TS**.
   b. In the middle panel, on the **Users** tab, observe that the **RDP-Tcp#0Session** for **Susan** has the state as **Active**.
   c. In the middle panel, select the user **Susan**. In the right panel, under **Actions,** click **Logoff**.
   d. The **Terminal Services Manager** message box about the selected user getting logged off is displayed. Click **OK**.
   e. The RDC connection in 6428A-NYC-WEB-05 will also get disconnected. Perform steps 2 to 9 in Task 3 of this exercise to set up the RDC connection before moving on to the next steps.
2. Disconnect all TS Gateway connections.
   a. In the middle panel, select the user **Susan**. In the right panel, under **Actions**, click **Disconnect**.
   b. The **Terminal Services Manager** message box about the selected user getting disconnected is displayed. Click **OK**.
   c. The RDC connection in 6428A-NYC-WEB-05 will also get disconnected. Perform steps 2 to 9 in Task 3 of this exercise to set up the RDC connection before moving on to the next steps.
3. Reset all TS Gateway Connections.
   a. In the middle panel, select the user **Susan**. In the right panel, under **Actions**, click **Reset**.
   b. The **Terminal Services Manager** message box about the selected user getting reset is displayed. Click **OK**.
   c. The RDC connection in 6428A-NYC-WEB-05 will also get disconnected. Log off from 6428A-NYC-WEB-05 and then log on again using WOODGROVEBANK\Administrator with the password Pa$$w0rd.
4. Close the Terminal Services Manager.

Results: After this exercise, you should have configured the TS Gateway settings on the client and managed TS connections remotely.

Exercise 2: Monitoring the TS Connections

Exercise Overview

In this exercise, you need to monitor the TS connections by using the TS Gateway Manager and specify the TS Gateway events to be logged.

The main tasks for this exercise are:

1. Connect to the remote computer.
2. Monitor TS Gateway.
3. Specify the TS Gateway events to be logged.

► Task 1: Connect to the remote computer

1. To connect using TS Gateway on 6428A-NYC-WEB-05, click **Start**, click **All Programs**, click **Accessories**, and then click **Remote Desktop Connection**.
2. In the **Remote Desktop Connection** dialog box, click **Connect**.
3. In the **Windows Security** dialog box, the login ID is displayed as**Woodgrovebank\Susan**. Log on with the password **Pa$$w0rd**, and then click **OK**.

► Task 2: Monitor TS Gateway

1. On 6428A-NYC-TS-07, click **Start**, point to **Administrative tools**, point to **Terminal Services**, and then click **TS Gateway Manager**.
2. In **TS Gateway Manager**, expand the **NYC-TS** node, and then expand **Monitoring**.
3. Select Susan's session in the middle panel.
4. In the **Actions** panel, under **Monitoring**, click **Edit Connection**. The **NYC-TS Properties** dialog box is displayed.
5. Click **Limit maximum allowed simultaneous connections to** and select **2** in the spin box, and then click **OK**.
6. In the **Actions** panel, under **Monitoring**, click **Set Automatic Refresh Options**.
7. In the **Set Automatic Refresh Options** dialog box, verify **Refresh automatically** is selected, in the spin box verify **0:30:0** seconds is selected, and then click **OK**.
8. In the middle panel, right-click **Susan**, click **Disconnect This Connection**. The TS Gateway message box about disconnecting from Susan Burk to the computer NYC-TS is displayed. Click **Yes**.
9. The RDC connection in 6428A-NYC-WEB-05 will also get disconnected. Perform steps 2 to 9 in Task 3 of Exercise 1 to set up the RDC connection before moving on to the next steps.

► Task 3: Specify the TS Gateway events to be logged

1. In the **TS Gateway Manager**, right click **NYC-TS (Local)**, and then click **Properties**.
2. In the **NYC-TS Properties** dialog box, on the **Auditing** tab, select all the checkboxes that you want to monitor for TS Gateway, and then click **OK**.
3. Close the TS Gateway Manager.
4. To check the event log, click **Start**, click **Administrative Tools**, and click **Event Viewer**.
5. On the **Event Viewer** page, in the middle panel, check the **Overview and Summary** page.
6. Under **Summary of Administrative Events**, scroll down and click the **Audit Success** node.
7. In the **Actions** panel, under **Audit Success**, click **View All Instances of This Event**.
8. In the middle panel, under **Summary** page events, view the event logs.
9. Close the Event Viewer.

Results: After this exercise, you should have monitored TS Gateway and specified the events to be logged for TS Gateway.

Exercise 3: Configuring WSRM for TS

Exercise Overview

The main tasks for this exercise are as follows:

1. Install WSRM on TS.
2. Configure the TS resource allocation policy for per session.
3. Monitor TS performance by using Resource Monitor.
4. Configure the TS resource allocation policy for per user.
5. Shut down the virtual machines.

► Task 1: Install WSRM on TS

1. To start the **Server Manager** snap-in on 6428A-NYC-TS-07, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. In the **Server Manager**, scroll down to the **Features Summary** section, click the **Add Features** link. The Add Features Wizard page is displayed.
3. In the **Add Features Wizard**, on the **Select Features** page, scroll down to select the Windows System Resource Manager check box. If the **Add Features Wizard** message box displays, informing you that Windows Internal Database also needs to be installed for WSRM to work properly click **Add Required Features**, and then click Next.
4. On the **Confirm Installation Selections** page, click **Install**.
5. On the **Installation Progress** page, note the installation progress. On completion of the installation, the Installation Results page is displayed.
6. On the **Installation Results** page, confirm that the installation of Windows Internal Database and WSRM succeeded, and then click **Close**.
7. Close the Server Manager.
8. To start the **WSRM** snap-in, click **Start**, point to **Administrative Tools**, and then click **Windows System Resource Manager**.
9. In the **Connect to computer** dialog box, under **Administer**, verify **This computer** is selected, and then click **Connect** to enable the WSRM to administer the local computer.

► Task 2: Configure the TS resource allocation policy for per session

1. To implement the Equal_Per_Session resource-allocation policy, on the **Windows System Resource Manager** snap-in, in the left pane, click the **Resource Allocation Policies** node.
2. Right-click **Equal_Per_Session** and then click **Set as Managing Policy**.
3. If the **End Snap-In** dialog box appears stating that snap-in is not responding, click **Cancel**.
4. If a **Warning** dialog box is displayed informing you that the calendar will be disabled, click **OK**.

► Task 3: Monitor TS performance by using Resource Monitor

1. On the **Windows System Resource Manager** snap-in, in the navigation tree, click **Resource Monitor**.
2. Review the performance data.

3. In the middle pane, on the toolbar, click **Properties**.
4. In the **Properties** dialog box, click the **Graph** tab.
5. On the **Graph** tab, in the **View** box, select **Report** from the drop-down list, and then click **OK**.
6. Observe the report for **Equal_Per_Session**.
7. To configure the notification options, in the left pane, right-click **Windows System Resource Manager (Local)**, and then click **Properties**. The Windows System Resource Manager Properties dialog box is displayed.
8. Click the **Notification** tab, select **Enable e-mail notification**.
9. In **Notify these e-mail aliases**, type **administrator@woodgrovebank.com**.
10. In **Use this SMTP server**, type **NYC-TS.woodgrovebank.com**.
11. In **Select the event log messages**, select two or more events. To view the list of events for each category, click the **Error** node, followed by the **Warning** and **Information** nodes.
12. Click each category, and then select two or more events in each category.
13. When you have finished selecting the events, click **OK**.

► Task 4: Configure the TS resource allocation policy for per user

1. To implement the Equal_Per_User resource-allocation policy, in the **Windows System Resource Manager** snap-in, in the console tree, click the **Resource Allocation Policies** node.
2. Right-click **Equal_Per_User**and then click **Set as Managing Policy**.
3. If a dialog box appears informing you that the calendar will be disabled, click **OK**.

► Task 5: Shut down the virtual machines

1. Exit the Lab Launcher tool by clicking the close button.
2. In the **Close** window, click **Turn off machine and discard changes**.
3. Click **OK**.

Results: After this exercise, you should have configured WSRM, configured resource allocation policies, and monitored the TS performance by using the Resource Monitor.

Send Us Your Feedback

You can search the Microsoft Knowledge Base for known issues at Microsoft Help and Support before submitting feedback. Search using either the course number and revision, or the course title.

Note Not all training products will have a Knowledge Base article – if that is the case, please ask your instructor whether or not there are existing error log entries.

Courseware Feedback

Send all courseware feedback to support@mscourseware.com. We truly appreciate your time and effort. We review every e-mail received and forward the information on to the appropriate team. Unfortunately, because of volume, we are unable to provide a response but we may use your feedback to improve your future experience with Microsoft Learning products.

Reporting Errors

When providing feedback, include the training product name and number in the subject line of your e-mail. When you provide comments or report bugs, please include the following:

- Document or CD part number
- Page number or location
- Complete description of the error or suggested change

Please provide any details that are necessary to help us verify the issue.

Important All errors and suggestions are evaluated, but only those that are validated are added to the product Knowledge Base article.
