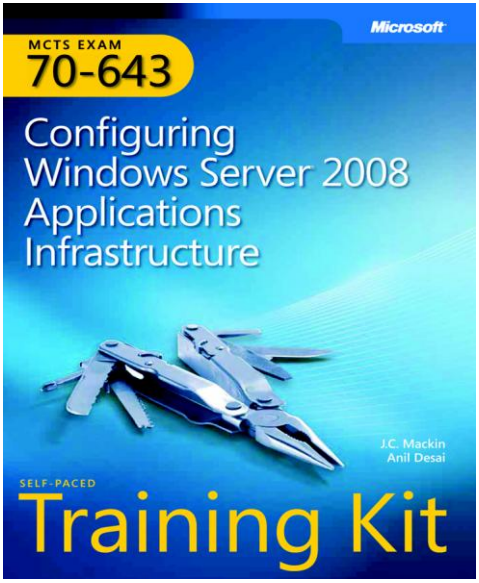

MCTS Self-Paced Training Kit (Exam 70-643): Configuring Windows Server® 2008 Applications Infrastructure

J.C. Mackin and Anil Desai

To learn more about this book, visit Microsoft Learning at http://www.microsoft.com/MSPress/books/11756.aspx.

9780735625112

Microsoft® Press

Table of Contents

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Chapter 3

Installing and Configuring Terminal Services

If you think of an application infrastructure as a set of technologies that helps deliver applications to remote users, then Terminal Services has to be considered one of its very central components. Terminal Services is, in fact, a technology that enables remote users to establish interactive sessions—both desktop sessions and application sessions—on a computer running Windows Server 2008.

The central role of Terminal Services is reflected on the 70-643 exam. With the many features, tools, and functions associated with Terminal Services, there's a fair amount to learn about this topic both for real-world administration and for the test. For this reason, the content is divided into two chapters. This chapter covers the deployment and configuration of the core Terminal Services role. In the next chapter, we will discuss the many complementary components that make up a Terminal Services infrastructure.

Exam objectives in this chapter:

- Configuring Terminal Services
  - Configure Terminal Services server options.
  - Configure Terminal Services licensing.
  - Configure Terminal Services load balancing.

Lessons in this chapter:

Before You Begin

To complete the lessons in this chapter, you must have:

- A computer running Windows Server 2008 named Server1 that is a domain controller in a domain named Contoso.com.
- A computer running Windows Server 2008 named Server2 that is a member server in the Contoso.com domain.
- A Server Core installation of Windows Server 2008 named Core1 that is a member server in the Contoso.com domain.

Real World

JC Mackin

The most important thing to know about Terminal Services in Windows Server 2008 is that it includes some radically new and important features beyond those offered in Remote Desktop or in any previous version of Windows Server. The RemoteApp feature, to begin with, enables you to run a remote program on another computer as if that program were installed locally. Another feature, Terminal Services Web Access (TS Web Access), provides a Web page from which you can launch these same remote applications, and Terminal Services Gateway (TS Gateway), for its part, gives your organization an attractive alternative to virtual private networks (VPNs) by allowing authorized users to connect from the Internet to any desired desktop on your internal network.

In the past, such functionality was available only through third-party applications. Now that these powerful features are built into Windows Server 2008, more organizations will start to take advantage of them. As a Windows support technician, you might have dismissed Terminal Services in the past as a feature that you didn't really have to understand too well, but the role of Terminal Services is now certain to grow.

Terminal Services is moving closer to the core of essential, real-world support technologies that you absolutely must know and understand. Given this, it's time to start looking very closely at this feature if you haven't already.

Lesson 1: Deploying a Terminal Server

The decision to deploy Terminal Services is complicated by the fact that Windows Server 2008 already includes a technology—Remote Desktop—that essentially performs the same function as Terminal Services. For this reason, before you deploy Terminal Services, it is important to understand the features this server role offers beyond those of Remote Desktop.

This lesson describes the features unique to the Terminal Services role and then describes the steps necessary to install and deploy a terminal server.

After this lesson, you will be able to:

- Understand the basic features and function of Terminal Services.
- Compare and contrast Terminal Services with the built-in Remote Desktop feature of Windows.
- Install the Terminal Services role on a full installation and a server core installation of Windows Server 2008.
- Describe client licensing options for a terminal server.
- Prepare a terminal server for deployment.

Estimated lesson time: 40 minutes

Understanding Terminal Services

Terminal Services enables remote users to establish interactive desktops or application sessions on a computer running Windows Server 2008. During a Terminal Services session, Terminal Services clients offload virtually the entire processing load for that session to the terminal server. This functionality offered by Terminal Services thus enables an organization to distribute the resources of a central server among many users or clients. For example, Terminal Services is often used to offer a single installation of an application to many users throughout an organization. This option can be especially useful for companies deploying line-of-business (LOB) applications and other programs responsible for tracking inventory.

Figure 3-1 illustrates how a terminal server can make a central application available to remote clients.

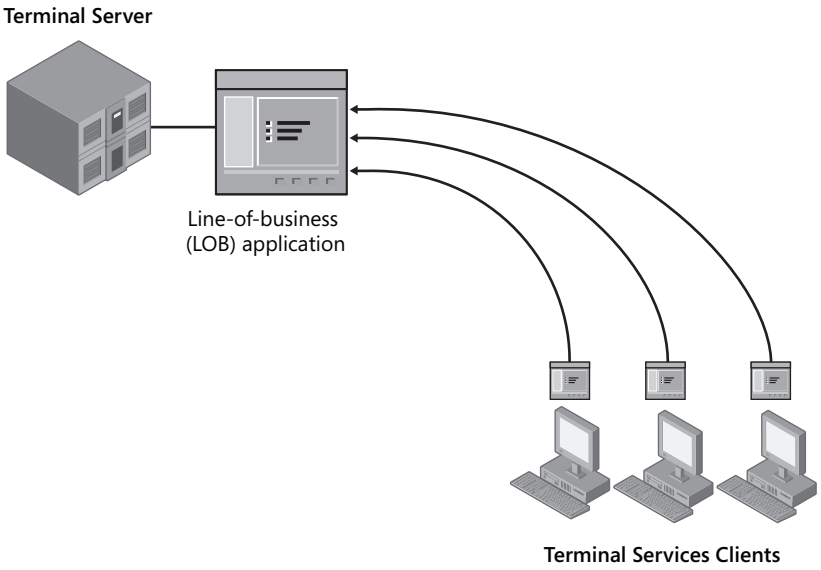

Figure 3-1 Using terminal servers to deploy an application

Comparing Terminal Services and Remote Desktop

Microsoft Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 all include a feature called Remote Desktop, which, like Terminal Services, enables users to establish an interactive desktop session on a remote computer. Remote Desktop and Terminal Services are in fact closely related. First, both technologies use the same client software, named Remote Desktop Connection (also called Terminal Services Client or Mstsc.exe). This client software is built into all versions of Windows since Windows XP can be installed on virtually any Windows-based or non-Windows–based computer. From the remote user's perspective, then, the procedure of connecting to a terminal server is identical to connecting to a remote desktop. Second, the server component of both features is also essentially the same. Both Terminal Services and Remote Desktop rely on the same service, called the Terminal Services service. Finally, both Remote Desktop and Terminal Services establish sessions by means of the same protocol, called Remote Desktop Protocol (RDP), and through the same TCP port, 3389.

Despite these similarities, the differences between Remote Desktop and Terminal Services are significant in that Terminal Services offers much greater scalability and a number of important additional features. For example, on a computer running Windows Server 2008 on which Remote Desktop is enabled, only two users can be connected concurrently to an active desktop session (including any active local user console session). However, no such limitation exists for a server on which Terminal Services has been installed and configured.

NOTE Connections vs. sessions

Strictly speaking, what is the difference between a Terminal Services connection and session? A Terminal Services connection is merely an open Remote Desktop Connection window displaying a desktop on a remote computer. A Terminal Services session, however, is a continuous period during which a user is logged on to a remote computer. If you closed a Remote Desktop Connection window without logging off from a remote computer, the connection would end, but (provided that the server settings allow it) the session would continue. If you then reconnected to the remote server, you would find the same session in progress with the open programs and files exactly as you had left them. The *console session*, as you might guess from its name, is not a Terminal Services session at all. It is instead the particular desktop session that is active at the physical computer.

Terminal Services in Windows Server 2008 also includes the following additional features beyond those available in Remote Desktop:

- **Multiuser capability** Terminal Services includes two modes: Execute mode (for the normal running of applications) and Install mode (for installing programs). When you install an application on a terminal server in Install mode, settings are written to the Registry or to .ini files in a way that supports multiple users. Unlike Terminal Services, the Remote Desktop feature in Windows does not include an Install mode or provide multiuser support for applications.
- **RemoteApp** In Windows Server 2008, the RemoteApp component of Terminal Services enables you to deploy an application remotely to users as if the application were running on the end user's local computer. Instead of providing the entire desktop of the remote terminal server within a resizable window, RemoteApp enables a remote application to be integrated with the user's own desktop. The application deployed through Terminal Services thus runs in its own resizable window with its own entry in the taskbar.
- **TS Web Access** TS Web Access enables you to make applications hosted on a remote terminal server available to users through a Web browser. When TS Web Access is configured, users visit a Web site (either from the Internet or from the organization's intranet) and view a list of all the applications available through RemoteApp. To start one of the listed applications, users simply click the program icon on the Web page.
- **TS Session Broker** By using Network Load Balancing (NLB) or DNS round-robin distribution, you can deploy a number of terminal servers in a farm that, from the perspective of remote users, emulates a single server. A terminal server farm is the best way to support many users, and to enhance the functionality of such a farm, you can use the Terminal Services Session Broker (TS Session Broker) role service. The TS Session Broker component ensures that clients connecting to a terminal server farm can reconnect to disconnected sessions.
- **TS Gateway** TS Gateway enables authorized users on the Internet to connect to remote desktops and terminal servers located on a private corporate network. TS Gateway

provides security for these connections by tunneling each RDP session inside an encrypted Hypertext Transfer Protocol Secure (HTTPS) session. By providing authorized users broad access to internal computers over an encrypted connection, TS Gateway can eliminate the need for a VPN in many cases.

Advantages of Remote Desktop

The main advantage of Remote Desktop, compared to Terminal Services, is that its functionality is built into Windows Server 2008 and does not require the purchase of any Terminal Services client access licenses (TS CALs). If you don't purchase any TS CALs for Terminal Services, the feature will stop working after 120 days. After this period, Terminal Services functionality will revert to that of Remote Desktop.

Another advantage of Remote Desktop, compared to Terminal Services, is that the feature is very easy to implement. Whereas enabling Terminal Services requires installing and configuring a new server role, enabling Remote Desktop requires you to select only a single option in the System Properties dialog box.

NOTE Remote Desktop vs. Remote Desktop for Administration

In Windows Server 2003 and Windows Server 2008, the built-in Remote Desktop feature is often referred to as Remote Desktop for Administration (RDA). The difference between RDA and the Remote Desktop feature in Windows XP and Windows Vista is that RDA in Windows Server 2008 enables two active desktop sessions to the RDA-enabled server: either two remote sessions, or one remote session and one console session. Windows XP and Windows Vista, however, do not allow concurrent desktop sessions. Only one Remote Desktop user can connect at a time and, when a remote user does connect, any locally logged-on user must first be logged off.

Exam Tip In Windows Server 2008, the Remote Desktop feature typically is used for remote administration, and Terminal Services is used to host applications. However, the main difference between these two features is scale, and the purposes of their implementations do overlap. You can use the Remote Desktop feature to connect to a seldom-used application just as you can administer a server remotely on which Terminal Services has been installed. Remember also that the core client and server components of these technologies are shared, so do not be surprised if you hear the terms used interchangeably.

Enabling Remote Desktop

By default, Windows Server 2008 does not accept connections from any Remote Desktop clients. To enable the Remote Desktop feature in Windows Server 2008, use the Remote tab of the System Properties dialog box. To access this tab, you can open System located in Control

Panel and then click the Remote Settings link, or you can type **control sysdm.cpl** in the Run box and then, after the System Properties dialog box opens, click the Remote tab.

On the Remote tab, if you want to require a high standard of security from RDP connections, select the option to require Network Level Authentication (NLA), as shown in Figure 3-2. This selection will enable connections only from Remote Desktop Connection clients running Windows Vista or later. Alternatively, you can select the option to allow connections from computers running any version of Remote Desktop.

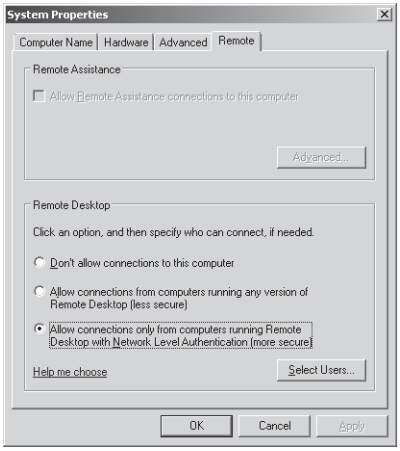

Figure 3-2 Enabling the Remote Desktop feature on Windows Server 2008

In Windows Server 2008, when you use the System Properties dialog box to allow Remote Desktop connections, a Windows Firewall exception for RDP traffic is created automatically. Therefore, you do not have to create the exception manually to allow connections from Remote Desktop clients.

NOTE What is Network Level Authentication?

NLA is a feature of Remote Desktop Protocol 6.0 that ensures that user authentication occurs before a Remote Desktop connection is fully established between two computers. With earlier versions of RDP, a user could enter a username and password for authentication only after a Log On To Windows screen from the remote computer appeared in the Remote Desktop session. Because every attempt to authenticate a session demanded relatively significant resources from the server, this behavior in earlier versions of RDP made Remote Desktop–enabled and Terminal Services–enabled computers susceptible to denial-of-service attacks.

Also important to know is that, by default, Remote Desktop Connection 6.0 (also known as Terminal Services Client 6.0 or mstsc.exe) does not support NLA on computers running Windows XP. However, this version of the Remote Desktop client can be made to support NLA on Windows XP SP2 if you download and install the Terminal Services Client 6.0 update for Windows XP (KB925876), available on the Microsoft Web site.

Enabling Remote Desktop on a Server Core Installation

A Server Core installation of Windows Server 2008 does not support the full Terminal Services role. However, you can enable the Remote Desktop feature on a Server Core installation by using the Server Core Registry Editor script, Scregedit.wsf. Scregedit.wsf provides a simplified way of configuring the most commonly used features in a Server Core installation of Windows Server 2008.

IMPORTANT Where can you find Scregedit.wsf?

Scregedit.wsf is located in the *%SystemRoot%*\System32 folder of every Server Core installation.

To use the Scregedit.wsf script to enable Remote Desktop, use Cscript.exe to invoke the script, and then pass the /AR switch a value of 0, which allows Remote Desktop connections. (By default, the /AR value is set to 1, which disables Remote Desktop connections.) The full command to enable Remote Desktop is shown here:

```
Cscript.exe C:\Windows\System32\Scregedit.wsf /AR 0
```

By default, enabling Remote Desktop on the Server Core installation in this way configures the server to accept Remote Desktop connections only from clients running Windows Vista or later. To enable the server to accept Remote Desktop connections from earlier versions of RDP, you need to relax the security requirements of the server by using the Scregedit.wsf script with the /CS switch and a value of 0, as shown:

```
Cscript.exe C:\Windows\System32\Scregedit.wsf /CS 0
```

NOTE Connecting to a Server Core through Remote Desktop

When you connect to a Server Core installation by means of Remote Desktop, you receive the same interface that you would receive as if you were seated locally at the server. A Remote Desktop connection to a computer running Windows Server 2008 Server Core, in other words, does not provide you with access to any additional graphical tools to manage the server.

Exam Tip For the 70-643 exam, you need to know how to enable Remote Desktop on a Server Core installation of Windows Server 2008 and how to allow connections from RDP clients earlier than RDP 6.0. Also, do not be surprised if the exam refers to this process as "enabling Terminal Services" or "enabling Terminal Services for remote administration."

Installing Terminal Services

Unlike Remote Desktop, the full implementation of Terminal Services requires you to add the Terminal Services server role. As with any server role, the simplest way to install Terminal Services on a full installation of Windows Server 2008 is to click Add Roles in Server Manager.

Clicking Add Roles launches the Add Roles Wizard. On the Select Server Roles page, select the Terminal Services check box, as shown in Figure 3-3.

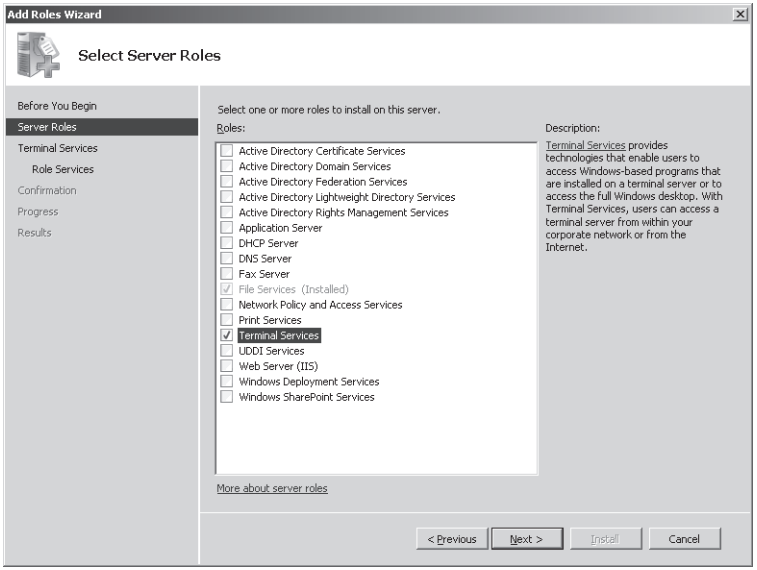

Figure 3-3 Adding the Terminal Services role

Click Next on the Add Roles Wizard page to open the Terminal Services page. This page provides a brief explanation of the Terminal Services role. Then, click Next on the Terminal Services page to open the Select Role Services page.

Selecting Role Services

On the Select Role Services page of the Add Roles Wizard, you can select any of the following five role services associated with the Terminal Services role:

- **Terminal Server** This role service provides the basic functionality of Terminal Services, including the RemoteApp feature.
- **TS Licensing** You need to install this role service only if you have purchased Terminal Services client access licenses (TS CALs) and can activate a license server. Terminal Services has a 120-day grace period: if you have not purchased any TS CALs and installed them on a Terminal Services license server, Terminal Services will stop functioning after this many days. (For information about how to install and configure Terminal Services Licensing (TS Licensing) Terminal Services, see Lesson 2, "Configuring Terminal Services," of this chapter.)
- **TS Session Broker** Install and configure this role service when you plan to implement Terminal Services in a server farm. As mentioned in the "Comparing Terminal Services and Remote Desktop" section earlier in this lesson, this role service enhances the functionality of the server farm by ensuring that clients are able to reconnect to disconnected sessions.
- **TS Gateway** Install this role service if you want to make a number of terminal servers accessible to authorized external clients beyond a firewall or Network Address Translation (NAT) device.
- **TS Web Access** Install this role service if you want to make applications deployed through Terminal Services available to clients through a Web page.

The Select Role Services page is shown in Figure 3-4.

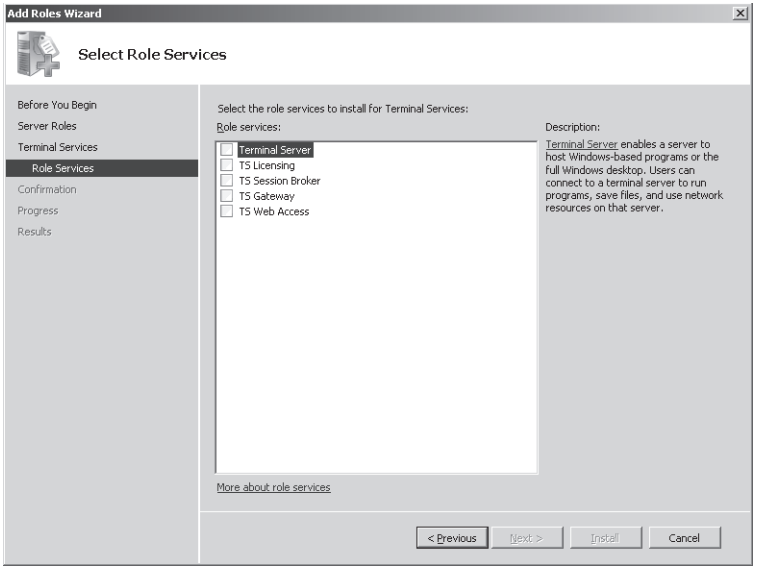

Figure 3-4 Adding the Terminal Services role services

The following sections describe the process of installing the Terminal Services role services.

Uninstalling Applications

After you select the Terminal Services role service, the Add Roles Wizard reminds you that any applications that you want to deploy to users through Terminal Services should be installed after you add the Terminal Services role. If you have already installed any applications you want to deploy, you should uninstall and reinstall them later (in Terminal Services Install mode) if you want them to be available to multiple users. This reminder is shown in Figure 3-5.

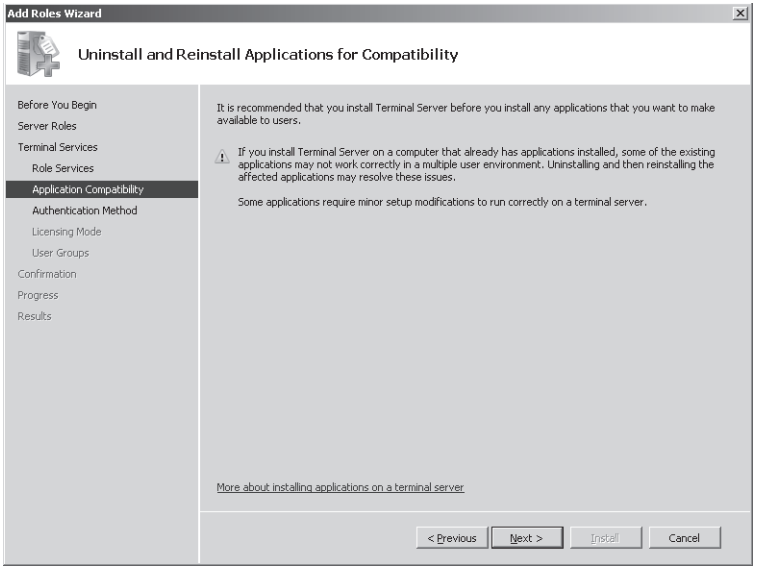

Figure 3-5 Reminder to reinstall TS applications

Specifying NLA Settings

Next, you have to specify whether the terminal server will accept connections only from clients that can perform NLA. When you select this requirement, shown in Figure 3-6, Remote Desktop connections will be blocked from computers with operating systems earlier than Windows Vista.

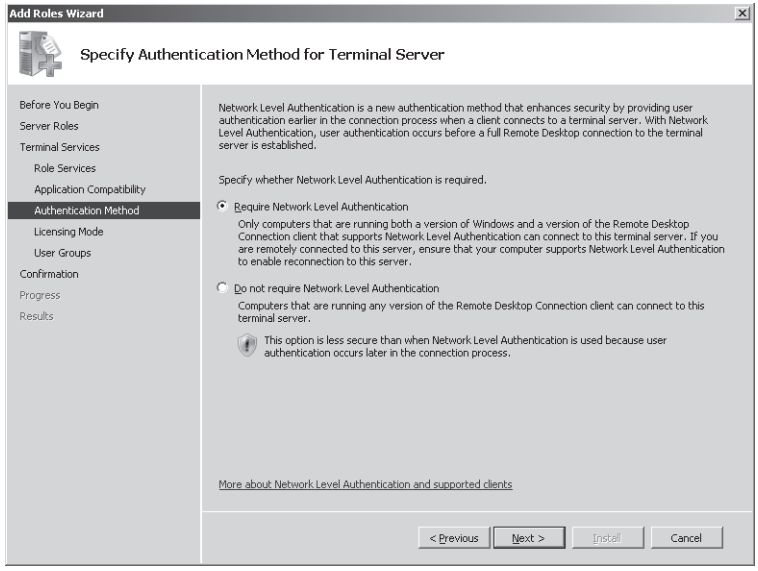

Figure 3-6 Setting NLA/client version requirements

Specifying Client Access License Types

The Add Roles Wizard then gives you the option to specify the TS CAL types you have purchased. Two types of CALs for Terminal Services are available:

- **TS Per Device CALs** TS Per Device CALs are permanent CALs assigned to any computer or device that connects to Terminal Services more than once. When the Per Device licensing mode is used and a client computer or device connects to a terminal server for the first time, the client computer or device is issued a temporary license by default. When a client computer or device connects to a terminal server for the second time, if the license server is activated and if enough TS Per Device CALs are available, the license server issues the client computer or device a permanent TS Per Device CAL.
- **TS Per User CALs** TS Per User CALs give users the right to access Terminal Services from any number of devices. TS Per User CALs are not assigned to specific users. If you opt for per user licensing, you simply need to make sure that you have purchased enough licenses for all the users in your organization.

Exam Tip Windows Server 2008 includes automatic per-device and per-user license tracking to help you determine how many TS licenses are currently in use. Windows Server 2003 only included per-device license tracking.

In deciding which of these two CALs to purchase for your organization, consider several factors. First, consider the number of devices and users in your organization. In general, it's financially preferable to choose per device CALs if you anticipate having fewer devices than users over the life of the terminal server and to choose per user licensing if you anticipate fewer users than devices. Another factor to consider is how often your users travel and connect from different computers. Per user licensing is often preferable when a small number of users tend to connect from many different sites, such as from customer networks.

If you have not yet decided which TS CALs to purchase, you can select the Configure Later option, as shown in Figure 3-7. You then have 120 days to purchase TS CALs and to install these licenses on a locally activated license server. After this grace period, Terminal Services stops functioning.

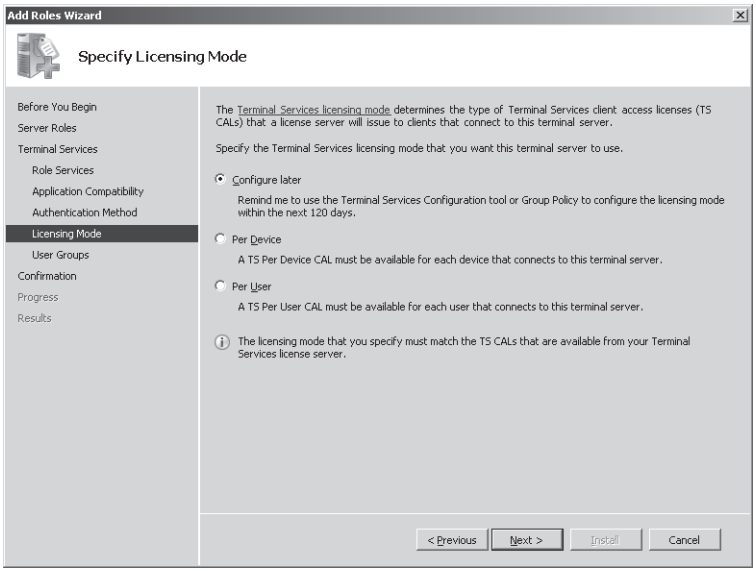

Figure 3-7 Specifying a licensing mode

Exam Tip For the 70-643 exam, you definitely need to know the difference between the client access license modes.

Authorizing Users

The last configuration step is to choose the users and groups you want to allow access through Terminal Services. The Remote Desktop Users built-in local group automatically is granted the user right to connect to the local computer through Terminal Services, and the Add Roles Wizard here simply provides a fast way of adding accounts to this Remote Desktop Users group. By default, local administrators are already members of the Remote Desktop Users group, as shown in Figure 3-8.

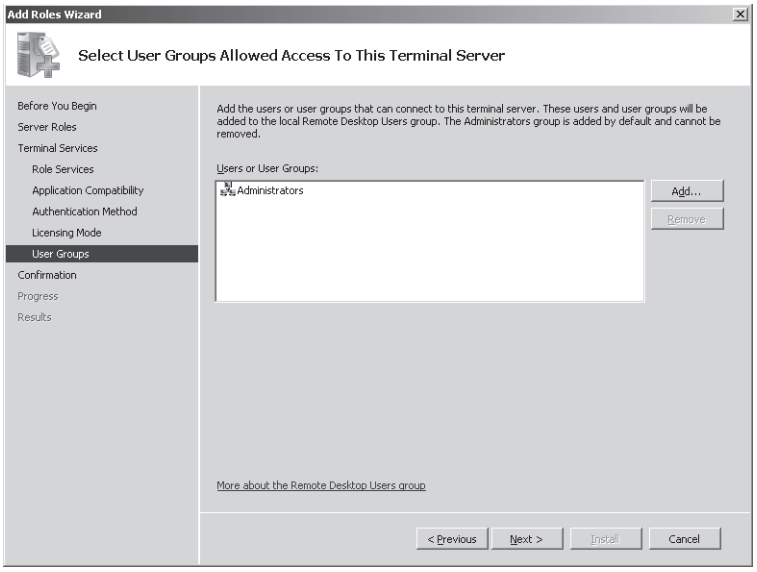

Figure 3-8 Authorizing users for Terminal Services

After this last step, you simply need to confirm your selections and begin the Terminal Services installation, as shown in Figure 3-9.

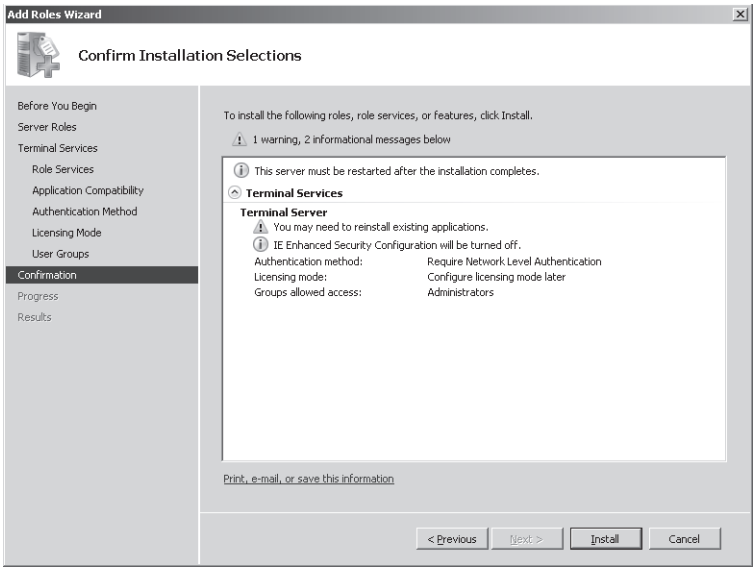

Figure 3-9 Confirming Terminal Services installation options

Staging the Terminal Server

Staging a server refers to the process of preparing it in advance of deployment. In the case of a terminal server, staging a computer involves installing and configuring all the components on the server that you want to make available to Terminal Services clients. At a minimum, this process includes installing appropriate server features and applications.

Installing Windows Server 2008 Built-in Features

Server Manager enables you not only to add server roles but also to install any of 36 Windows Server 2008 features. Features are smaller Windows components that enable specific functionality in the operating system. To prepare a terminal server for deployment, you need to know which of these Windows Server 2008 features you want to make available to clients connecting to the terminal server.

Because the only features available to remote users are those that you install on the terminal server, you need to review client needs and the functionality offered by each feature. For example, if you want Windows Media Player or Windows Aero to be made available to clients connecting to Terminal Services, you have to install the Desktop Experience feature on the computer running Terminal Services.

To install a feature, click Add Features in Server Manager to launch the Add Features Wizard. Figure 3-10 shows a partial list of the features made available by the Add Features Wizard.

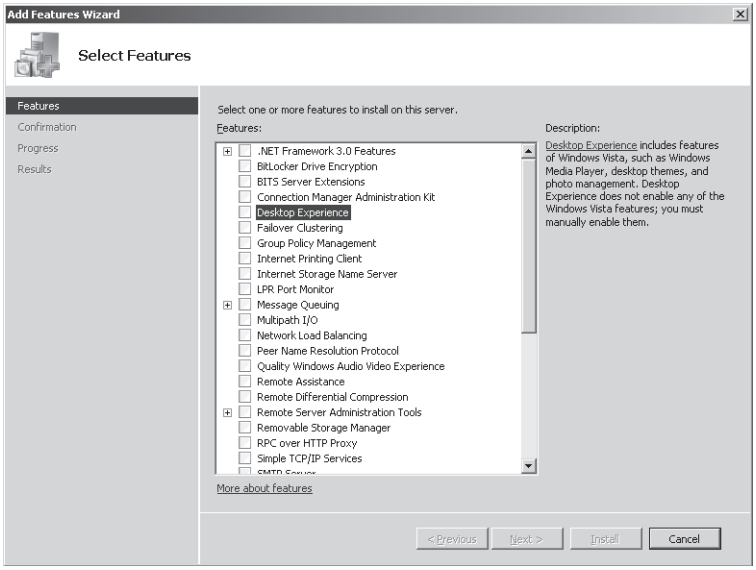

Figure 3-10 The Add Features Wizard

A list follows of some example Windows Server 2008 features that you might need to make available to Terminal Services clients. Successful deployment of Terminal Services requires you to understand these features and to review them during the server staging process.

- **Desktop Experience** This feature installs Windows Media Player 11, desktop themes, and the photo gallery. It also makes the Windows Aero graphical features available, although these features must be enabled manually by each user.
- **Quality Windows Audio Video Experience** This feature enables high-quality performance for streaming media over IP networks.
- **Network Load Balancing** The NLB feature enables you to join a server to an NLB cluster or NLB server farm.
- **Windows Server Backup Features** You can install the Windows Server Backup Features to enable administrators to perform backups as part of remote maintenance of the computer running the terminal server.
- **Windows PowerShell** Windows PowerShell is a command-line environment and administrative scripting language built into Windows Server 2008. You can install the Windows PowerShell feature to enable remote administration of the computer running Terminal Services by using Windows PowerShell.

- **Group Policy Management** Group Policy Management is a console that facilitates administration of Group Policy. You can install this feature if you anticipate that administrators will use the server to manage Group Policy remotely.
- **Windows System Resource Manager** Windows System Resource Manager (WSRM) enables you to manage the resources of a server so that the workload is spread equitably among roles.

Exam Tip Be sure to review server features for the 70-643 exam. Although it's a good idea to review all features, pay special attention to those just listed.

Installing Terminal Services Applications

Terminal Services is often used to deploy a single installation of an application to many users. Deploying an application in this way is frequently the best option for data-entry programs designed to run on a single server or for those tied to a locally installed database. However, you might also want to deploy an application through Terminal Services to reduce associated licensing fees, to offload processing from client computers, or simply to facilitate user productivity within a Terminal Services session.

After you have decided which applications to make available to remote users through Terminal Services, you need to install these applications in a way that makes them available to multiple users. To do this, you must install the applications while Terminal Services is in Install mode. You can install programs in Install mode by using an MSI installer program, by using the Install Application on Terminal Server program in Control Panel, or by using the *Change user/install* or *Chgusr/install* command. For more information about using Install mode, see Chapter 4, "Configuring and Managing a Terminal Services Infrastructure."

Quick Check

1. Which server feature should you install on a terminal server if you want users to be able to play audio and video in Terminal Services sessions?
2. On a computer running Windows Server 2008 that has the Remote Desktop feature enabled, what is the maximum number of concurrent active user sessions (including remote and console sessions) that can be hosted?

Quick Check Answers

1. Desktop Experience
2. Two

PRACTICE Installing a Terminal Server

In this practice, you will install Terminal Services on a full installation of Windows Server 2008 and then enable the Remote Desktop feature on a server core installation.

▶ Exercise 1 Install the Terminal Services Role

In this exercise, you will install the Terminal Services server role on Server2.

1. As a domain administrator, log on to Contoso.com from Server2.
2. In Server Manager, select the Roles node in the console tree, and then click Add Roles in the details pane.

   If the Before You Begin page is displayed, click Next.
3. On the Select Server Roles page of the Add Roles Wizard, select the Terminal Services check box, and then click Next.
4. On the Terminal Services page, read all the text on the page, and then 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, read all the text on the page, and then click Next.
7. On the Specify Authentication Method For Terminal Services page, read all the text on the page, select Require Network Level Authentication, and then click Next.
8. On the Specify Licensing Mode page, read all the text on the page, leave the default selection of Configure Later, and then click Next.
9. On the Select User Groups Allowed Access To This Terminal Server page, read all the text on the page, and then click Next.
10. On the Confirm Installation Selections page, read all the text on the page, and then click Install.
11. After the installation is complete, read all the text on the Installation Results page, and then click Close.
12. In the Add Roles Wizard dialog box, click Yes to restart the server.
13. After the server reboots, log back on to Contoso.com from Server2 by using the same domain administrator account.

IMPORTANT Always log back on with the same account

In Windows Server 2008, whenever you add or remove a server role, you are prompted to restart the server. You must immediately log back on with the same user account to complete the procedure.

After several moments, the Resume Configuration Wizard appears.

When the Installation Results page appears, click Close.

14. In Control Panel, open Windows Firewall.
15. Click the Allow A Program Through Windows Firewall option.
16. On the Exceptions tab of the Windows Firewall Settings dialog box, verify that the Remote Desktop and Terminal Services check boxes are checked, and then click OK.
17. Close all open windows, and then proceed to Exercise 2.

▶ Exercise 2 Test the Terminal Services Connection

In this exercise, you will test the Terminal Services configuration on Server2 by connecting to it from a Remote Desktop Connection on Server1.

1. Log on to Contoso.com from Server1 as a domain administrator.
2. From the Start menu, select Run.
3. In the Run box, type **mstsc**, and then press Enter.

Exam Tip You need to know the function of the *Mstsc* command for the 70-643 exam.

The Remote Desktop Connection window opens.

4. In the Computer text box of the Remote Desktop Connection window, type **server2.contoso.com**, and then press Enter.

   The Windows Security window opens.

5. In the Windows Security window, enter the credentials of a domain administrator. Be sure to enter the username in the form **contoso*username***.

   After several moments, a Remote Desktop connection is established to Server2. Within the desktop of Server1, the remote Server2 desktop is designated with a yellowish banner labeled "server2.contoso.com."

6. Using the Start button within the Remote Desktop session to Server2, log off the Remote Desktop connection.

   The Remote Desktop window closes.

▶ Exercise 3 Enable Remote Desktop on a Server Core Installation of Windows Server 2008

In this exercise, you will enable Remote Desktop on the Core1 computer and then test the configuration.

NOTE Server1 and Server2

Although Server1 is needed for this exercise, Server2 is not. If you are using virtual machines and do not have enough RAM to support all three computers, you can shut down Server2 before beginning this exercise.

---

1. Log on to Contoso.com from Core1 as a domain administrator.
2. At the command prompt, type the following command: **cd C:\Windows\System32**.
3. At the command prompt, type the following command: **cscript scregedit.wsf /AR /v**.

   This command shows the current status of the fDenyTSConnections registry setting. When set to 1, the local computer is configured to deny incoming Remote Desktop connections.
4. Type the following command: **cscript scregedit.wsf /AR 0**.
5. To verify the setting change, type the following command: **cscript scregedit.wsf /AR /v**.

   The output from the command reveals that the fDenyTSConnections registry setting is now set to 0.
6. To ensure that the server will accept connections from RDP clients earlier than 6.0, or from clients native to Windows XP and earlier, type the following command: **cscript scregedit.wsf /CS 0**.
7. To verify the setting, type the following command: **cscript scregedit.wsf /CS /v**.
8. The output from the command reveals that the RDP-Tcp UserAuthentication setting is now set to 0. This setting enables connections from earlier versions of Remote Desktop.

   Type the following command: **netsh firewall show service**.

   This command displays the firewall exceptions that have been created for various services on Core1. In this case, the output verifies that a firewall exception has been created (enabled) for the Remote Desktop service in the Domain profile.
9. Log on as a domain administrator to Contoso.com from Server1.
10. In the Run box, type **mstsc**, and then press Enter.

    The Remote Desktop Connection window opens.
11. In the Computer text box, type **core1.contoso.com**, and then click Connect.
12. In the Windows Security window, enter the username and password of a domain administrator. Be sure to enter the name in this format: contoso*username*.

13. In the Windows Security window, click OK.

    After a few moments, a Remote Desktop connection to Core1 is established. The Remote Desktop connection shows the same Server Core desktop that you can see when you log on to Core1 locally.

14. On Server1, within the Remote Desktop session to Core1, type **logoff** at the command prompt.

    On Server1, the Remote Desktop session closes.

15. On Core1, type **shutdown /p** at the command prompt to shut down the computer.

Lesson Summary

- Terminal Services enables users to establish and interact with a desktop or application session on a remote computer running Terminal Services.
- Terminal Services shares its core functionality with that of Remote Desktop. In terms of its core functionality, the biggest difference between these two features is that when Remote Desktop is enabled, Windows Server 2008 allows only two concurrent desktop sessions (including any local console session). Terminal Services has no such limits.
- In Windows Server 2008, Terminal Services includes many new and important features such as TS Gateway, RemoteApp, and TS Web Access. (These topics are covered in detail in Chapter 4.)
- To install Terminal Services on a computer running Windows Server 2008, add the Terminal Services server role.
- Terminal Services requires client access licenses (CALs) either for all connecting users or for all connecting devices. If you do not purchase and install Terminal Services CALs, Terminal Services will stop working after 120 days.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

---

1. You want to enable Remote Desktop on a Server Core installation of Windows Server 2008 and then enable the server to accept connections from clients configured with RDP versions prior to 6.0. Which commands should you use? (Choose two.)
   - **A.** cscript scregedit.wsf /AR 0
   - **B.** cscript scregedit.wsf /AR 1
   - **C.** cscript scregedit.wsf /CS 0
   - **D.** cscript scregedit.wsf /CS 1
2. You are 1 of 75 consultants employed by an IT services company named Contoso.com. As part of your job, you and other team members provide network support for over 150 businesses in your city. Your company is about to implement a business process in which consultants must connect to an application server on the Contoso.com network while working at customer premises. When connected to the application server, consultants provide critical information about each assignment in the field. To connect to the Contoso.com application server, consultants are expected to use Remote Desktop Connection on customer computers running Windows XP or Windows Vista. You have been asked to determine whether your company needs to purchase client access licenses (CALs) for Terminal Services. Which of the following options best suits the needs of your organization?
   - **A.** Use Remote Desktop for Administration on the application server, and purchase per user CALs.
   - **B.** Use Remote Desktop for Administration on the application server, but do not purchase any CALs.
   - **C.** Install Terminal Services on the application server, and purchase per device CALs.
   - **D.** Install Terminal Services on the application server, and purchase per user CALs.

Lesson 2: Configuring Terminal Services

The Terminal Services Configuration console is the main tool used to configure the Terminal Services role. The server options available in this tool primarily affect the user's environment when connecting to the local terminal server. Other options available in this tool, however, relate to server licensing and load balancing features. After describing all the options and features configurable in the Terminal Services Configuration console, this lesson describes supplementary configuration options available in Group Policy for one feature in particular: printer redirection.

After this lesson, you will be able to:

- Configure terminal server options.
- Configure Terminal Services load balancing.
- Install and configure a Terminal Services license server.

Estimated lesson time: 50 minutes

Introducing the Terminal Services Configuration Console

The Terminal Services Configuration (TSC) console is designed to control settings that affect all users connecting to the terminal server or all users connecting through certain connection types. For instance, you can use the TSC console to set the encryption level of all Terminal Services sessions, to configure the graphical resolution of sessions, or to restrict all users to one session. The TSC console is shown in Figure 3-11.

The TSC console provides two general areas for configuration: the connection (RDP-Tcp) properties dialog box and the Edit Terminal Server Settings area. The following sections describe the options available through each of these configuration areas.

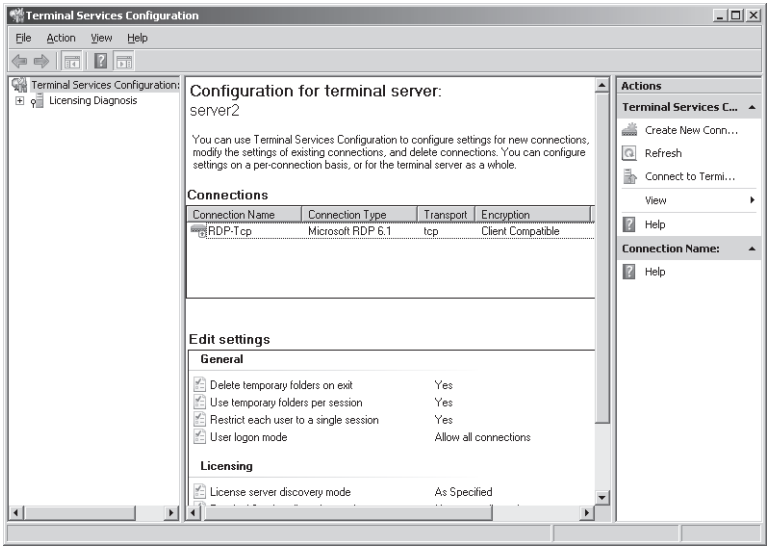

Figure 3-11 The Terminal Services Configuration console

Configuring Connection (RDP-Tcp) Properties

Connection properties are used to customize the behavior of all Terminal Services sessions initiated through certain specific transport protocols (such as RDP over TCP) or through specific network adapters on the terminal server. By default, only one connection (named RDP-Tcp) is available for configuration; the properties configured for this connection apply to RDP sessions through all local network adapters. Beyond this default connection, you can also create new connections that apply to third-party transport protocols or to particular adapters.

For environments using only the built-in functionality offered by Windows Server 2008, the RDP-Tcp connection normally will serve as the only connection, and the RDP-Tcp Properties dialog box provides key configuration options for the entire server.

To open the properties of the RDP-Tcp connection, in the TSC console Connections area, right-click RDP-Tcp, and then click Properties. This procedure opens the RDP-Tcp Properties dialog box, as shown in Figure 3-12.

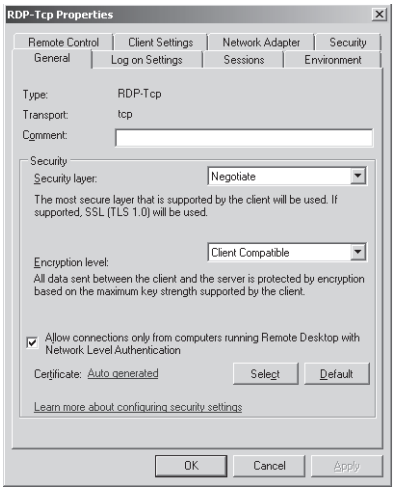

Figure 3-12 RDP-Tcp Properties General tab

The following section explains the configurable options available through each of the eight tabs.

Exam Tip Learn all the settings on the eight RDP-Tcp Properties tabs.

General Tab

The General tab enables you to modify settings in three security areas: security layer, encryption level, and NLA. These three areas are described in the following section.

Security Layer All RDP connections are encrypted automatically. Security layer settings determine the type of encryption used for these Terminal Services connections. Three options for the security level are available: RDP Security Layer, SSL (TLS 1.0), and Negotiate.

- The RDP Security Layer option limits encryption to the native encryption built into Remote Desktop protocol. The advantages of this option are that it requires no additional configuration and that it offers a high standard of performance. Its disadvantage is that it does not provide terminal server authentication for all client types. Although RDP 6.0 can provide server authentication for clients running Windows Vista and later, Terminal Services clients running Windows XP and earlier do not support server authentication. If you want to enable RDP clients running Windows XP to authenticate the terminal server before establishing a connection, you have to configure SSL encryption.

- The SSL (TSL 1.0) option offers two advantages over RDP encryption. First, it offers stronger encryption. Second, it offers the possibility of server authentication for RDP client versions earlier than 6.0. SSL is, therefore, a good option if you need to support terminal server authentication for Windows XP clients. However, this option does have some drawbacks. To begin with, SSL requires a computer certificate for both encryption and authentication. By default, only a self-signed certificate is used, which is equivalent to no authentication. To improve security, you must obtain a valid computer certificate from a trusted certification authority (CA), and you must store this certificate in the computer account certificate store on the terminal server. Another disadvantage of SSL is that its high encryption results in slower performance compared to that of other RDP connections.
- When you choose the Negotiate option, the terminal server will use SSL security only when supported by both the client and the server. Otherwise, native RDP encryption is used. Negotiate is also the default selection.

Encryption Level The Encryption Level setting on the General tab enables you to define the strength of the encryption algorithm used in RDP connections. The default selection is Client Compatible, which chooses the maximum key strength supported by the client computer. The other available options are FIPS Compliant (highest), High, and Low.

Network Level Authentication When the Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication setting is enabled, only clients that support NLA will be allowed to connect to the terminal server.

To determine whether a computer is running a version of the Remote Desktop Connection (RDC) client that supports NLA, start the RDC client, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. Look for the phrase "Network Level Authentication Supported" in the About Remote Desktop Connection dialog box, shown in Figure 3-13.

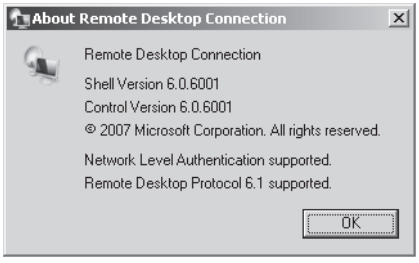

Figure 3-13 Verifying NLA support

Logon Settings Tab

The Logon Settings tab, shown in Figure 3-14, enables you to configure all Terminal Services clients to use a single predefined username and password. Sharing credentials in this way enables users to connect to the terminal server without having to supply any credentials. Choosing this option might be suitable for testing environments or for public terminals.

When you select the Always Prompt For Password option, the user must always supply at least a password (if not the username) before connecting.

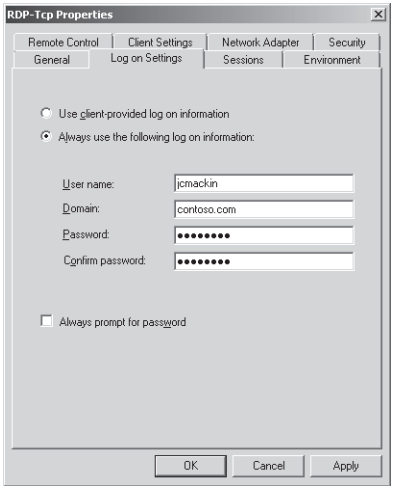

Figure 3-14 Configuring Terminal Services logon settings

Sessions Tab

You can use the Sessions tab to control session timeout settings for the terminal server. Specifically, this tab enables you to choose timeout settings for disconnected sessions, set time limits for active and idle sessions, and define the behavior for disconnections and session limits.

By default, these settings are defined not in this RDP-Tcp Properties dialog box but in each user's domain account properties. To override these user-defined settings, you can click the Override User Settings check box, as shown in Figure 3-15, and then choose options for the following policies:

- **End A Disconnected Session** This setting determines when (if ever) a user is automatically logged off from a disconnected session.
- **Active Session Limit** This setting determines how long a user can stay active within a Terminal Services session before automatically being disconnected.

- **Idle Session Limit** This setting determines how long a user can leave an inactive connection open to a Terminal Services session before automatically being disconnected.
- **When Session Limit Is Reached Or Connection Is Broken** This setting determines whether a user is logged off automatically when a connection is broken (manually or automatically).

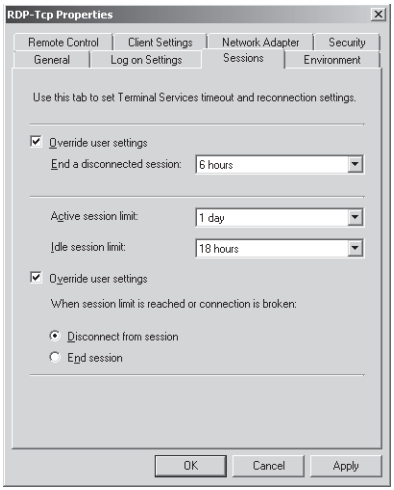

Figure 3-15 Terminal Service timeout and reconnection settings

Environment Tab

This tab enables you to control whether initial programs defined in a user's profile should be allowed to run automatically at the start of a Terminal Services session. It also enables you to specify a program to start for all users connecting to the local terminal server through RDP.

The Environment tab is shown in Figure 3-16.

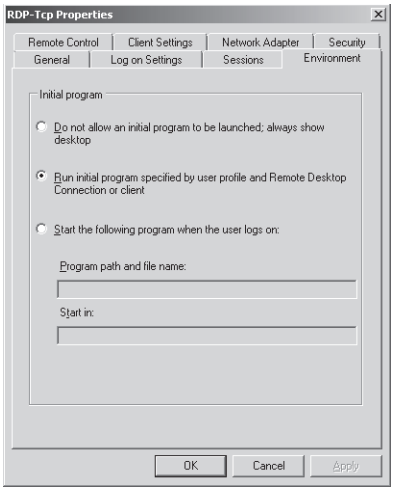

Figure 3-16 Initial program settings

Remote Control Tab

The remote control feature of Terminal Services enables an administrator to see or interact with another user's Terminal Services session. By default, the properties that define the behavior of this feature are set on a per-user basis in each user account's properties dialog box. (These properties define how an administrator can view or control that user's Terminal Services sessions.) The Remote Control tab enables you to control the settings of this feature on a per-server basis instead.

The default settings of a user account enable an administrator to interact with another user's Terminal Services session only if the user provides consent. However, you can use the Environment tab of the RDP-Tcp Properties dialog box to enable administrators to interact with (or merely to view) all user sessions with or without consent. You can also prevent administrators from viewing or interacting with other users' sessions completely.

IMPORTANT Remote Control works only from remote session

You can use the Remote Control feature only from within an RDP session. If an administrator is logged on to a terminal server locally, the feature is disabled.

The Remote Control tab is shown in Figure 3-17.

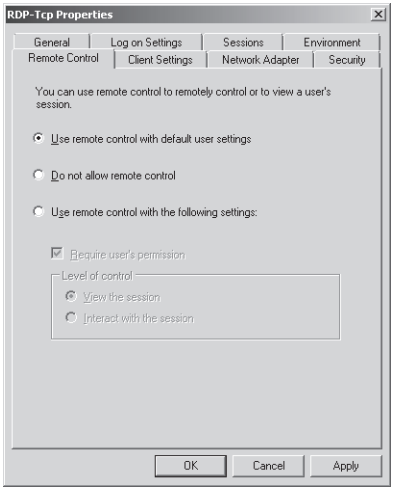

Figure 3-17 Remote control settings

Client Settings Tab

The Client Settings tab, shown in Figure 3-18, enables you to configure redirection of certain user interface features.

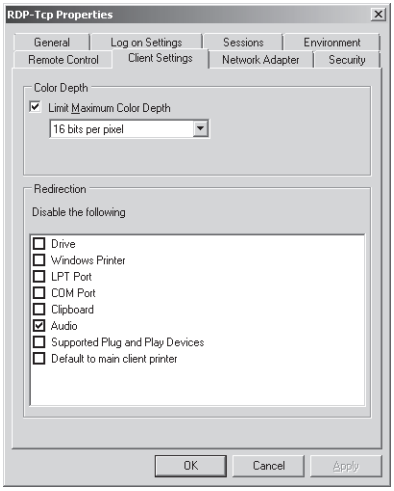

Figure 3-18 The Client Settings tab

In the Color Depth area of the tab, you can define the amount of color detail sent from the Terminal Server to the client. The default setting is 16 bits per pixel, but you can adjust this higher

or lower. In general, when you require more bit depth for RDP connections, appearance is improved at the expense of performance.

In the Redirection – Disable The Following area of the tab, you can determine which features should not be redirected to the client. The advantage of disabling redirection is improved performance, but this improvement comes at the expense of the advantages offered by each particular feature that you choose to disable.

- **Drive** When you select this option, the drives local to the client cannot be included in the Terminal Services connection. (To include the drives, this check box must be cleared, and the Drives option must be selected on the Local Resources tab of the Remote Desktop Connection client.)
- **Windows Printer** When you select this option, printers local to the client cannot be accessed in the Terminal Services connection. However, a user can still connect to the client printer at the command prompt by using LPT port mapping or COM port mapping.
- **LPT Port** Selecting this option prevents users from mapping a connection to an LPT printer.
- **COM Port** Selecting this option blocks a connection from the Terminal Services session to COM devices on the client computer.
- **Clipboard** This option, when selected, prevents users from cutting or copying data from a Remote Desktop (Terminal Services) session and then pasting that data into the local session on the client computer. Over slow connections, disabling clipboard redirection can prevent screen freezes.
- **Audio** When enabled, this option prevents the transmission of audio data from the remote desktop to the local client computer. This is the only option that is selected by default.
- **Supported Plug and Play Devices** This option, when selected, prevents Plug and Play devices local to the client from being redirected to a Terminal Services session.
- **Default to Main Client Printer** When you select this option, the default printer assigned to the Terminal Services client is prevented from serving as the default printer for the Terminal Services session.

Network Adapter Tab

This tab enables you to restrict the default RDP-Tcp connection to listen for RDP connection attempts on only one particular network adapter. The tab also enables you to set a limit on the number of connections allowed by the terminal server. By default, no limit is set, as shown in Figure 3-19.

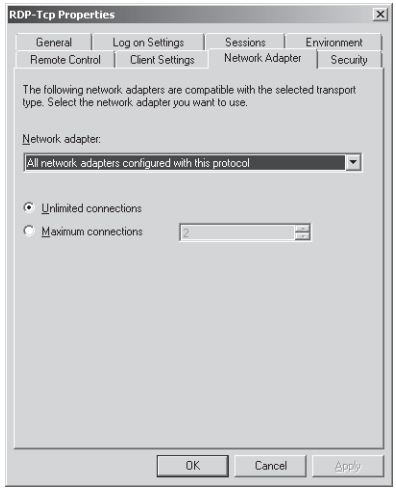

Figure 3-19 The Network Adapter tab

Security Tab

This tab enables you to set user permissions for all RDP connections to the terminal server. It is recommended that you do not use this tab to configure user access to Terminal Services; for that, use the Remote Desktop Users group instead. You should use this tab to determine which users should have administrative control (Full Control) of Terminal Services.

The Security tab is shown in Figure 3-20.

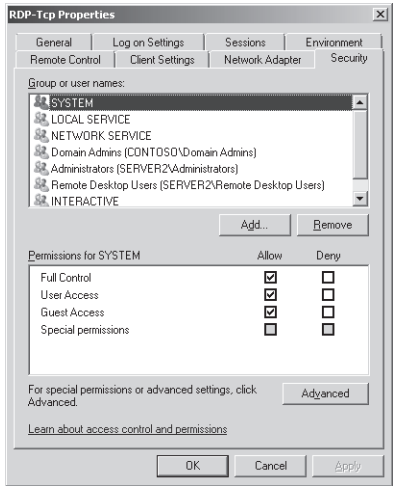

Figure 3-20 The RDP-Tcp Properties Security tab

Configuring Terminal Services Server Properties

Besides the RDP-Tcp Properties tabs, the TSC console offers a second important set of Terminal Services configuration options, available through the Edit Settings area. These settings apply to the entire terminal server only; unlike RDP-Tcp or other connection settings, they cannot be configured to apply merely to one transport protocol or to one particular network adapter.

The Edit Settings area provides a summary of seven terminal server options organized under three categories: General, Licensing, and TS Session Broker. To change these server options, double-click any one of them. This procedure opens a Properties dialog box whose three tabs are also named General, Licensing, and TS Session Broker.

The options available in these three tabs are explained in the following section.

General Tab

The General tab enables you to configure the following features related to user logon sessions:

- **Delete Temporary Folders On Exit** When this option is enabled, as it is by default, all temporary data is deleted when a user logs off from a Terminal Services session. Deleting temporary data in this way decreases performance but improves privacy because it prevents users from potentially accessing another user's data.

  This setting functions only when the next option, Use Temporary Folders Per Session, is also enabled.
- **Use Temporary Folders Per Session** Enabled by default, this option ensures that a new folder to store temporary data is created for each user session. When this option is disabled, temporary data is shared among all active sessions. Sharing temporary data among users can improve performance at the expense of user privacy.
- **Restrict Each User To a Single Session** This option is enabled by default. When enabled, it allows only one logon session to the terminal server per user. For instance, if you are logged on to a server locally with the built-in Administrator account, you cannot log on to the same computer through a Remote Desktop connection by using the same Administrator account until you first log off the server locally.

  By ensuring that you log off one session before beginning another, this default setting prevents possible data loss in the user profile. It also prevents stranded user sessions and, therefore, conserves server resources.
- **User Logon Mode** The settings in the User Logon Mode area enable you to prevent new users from logging on to the terminal server, for instance, in advance of a maintenance shutdown. The Allow All Connections option is the default setting. To prevent users from connecting to the terminal server indefinitely, you can select the Allow Reconnections, But Prevent New Logons option. To prevent users from connecting to the

server only until you reboot the server, you can select the Allow Reconnections, But Prevent New Logons Until The Server Is Restarted option. Note that none of these options forces a session termination. If you need to reboot a server, you might need to end these sessions manually, as described in Chapter 4.

The General tab is shown in Figure 3-21.

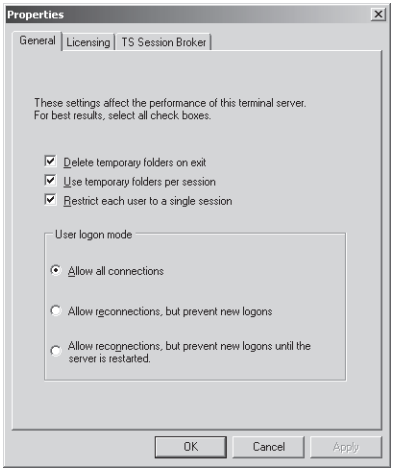

Figure 3-21 User Logon Mode settings

Exam Tip The three settings available in the User Logon Mode area are new to Windows Server 2008. For this reason, you should expect to see at least one question about these options on the 70-643 exam. Also note that the feature to prevent new logons is sometimes called "Drain Mode."

Licensing Tab

The Licensing tab, shown in Figure 3-22, enables you to configure two features related to terminal server licensing: the licensing mode and the license server discovery mode.

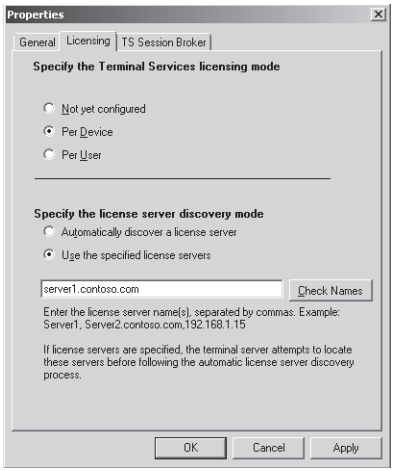

Figure 3-22 Server Options Licensing tab

- **Terminal Services licensing mode** During the installation of the Terminal Services server role, you can specify the licensing mode of the terminal server or select the option to configure the licensing mode later. To set or reset the licensing mode after installation, select the Server Properties Licensing tab, and then choose the Per Device or Per User option in the Specify The Terminal Services Licensing Mode area.
- **License server discovery mode** The license server discovery mode is the method by which a terminal server contacts a license server to obtain TS CALs. By default, the discovery mode is set to Automatically Discover A License Server. In the automatic license server discovery process, a terminal server attempts to contact any license servers published in Active Directory services or installed on domain controllers in the local domain. As an alternative to the automatic discovery mode, you can specify the license server manually by selecting the Use The Specified License Servers option and by then typing a license server name or address in the associated text box.

Exam Tip In Active Directory Users and Computers, you can see a domain local security group called Terminal Server Computers. You can edit the membership of this group to restrict the terminal servers allowed to communicate with license servers in the domain.

TS Session Broker Settings Tab

The TS Session Broker Settings tab, shown in Figure 3-23, is used to configure settings for a member server in a TS Session Broker farm. TS Session Broker can be used to balance the session load among servers in a farm by directing new user sessions to the server in the farm with

the fewest sessions. TS Session Broker is also used to ensure that users can reconnect automatically to disconnected sessions on the appropriate farm member server.

NOTE TS Session Broker and Active Directory

The server on which you install TS Session Broker must be a member of a domain.

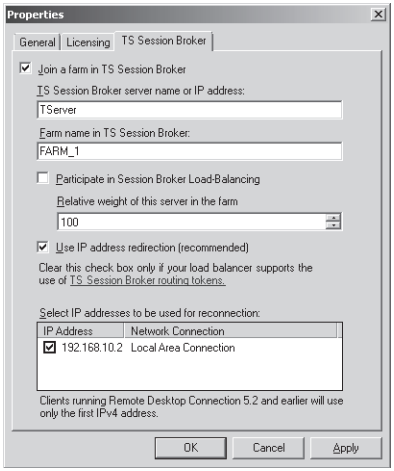

Figure 3-23 Configuring Terminal Services load balancing

To configure a terminal server farm, the first step is to install the TS Session Broker role service on a server that you want to use to track user sessions for the entire farm. This server becomes the TS Session Broker server. Then, you need to add the terminal servers in the farm to the Session Directory Computers local group on the TS Session Broker server. Finally, you have to configure the terminal servers to join the farm by configuring the following desired options on this tab:

- **Join A Farm In TS Session Broker** Select this check box to add the local server to a farm and to make the remaining options available for configuration.
- **TS Session Broker Server Name Or IP Address** In this text box, type the name or IP address of the server on which you have installed the TS Session Broker role service.
- **Farm Name In TS Session Broker** In this text box, you must type the name of the farm that will be shared by all farm members. This name also represents the Domain Name System (DNS) name that clients will use to connect to the terminal server farm. (For this reason, in the appropriate DNS server, be sure to add multiple DNS records that correspond to this farm name and that specify the IP address of each farm member.)

- **Participate In Session Broker Load-Balancing** Select this check box to configure the local server to participate in the load balancing feature enabled by TS Session Broker.
- **Relative Weight Of This Server In The Farm** You can use this setting to give powerful servers a larger proportion of user sessions than less powerful servers. For example, if you assign a powerful server a weight of 200 and a less powerful server a weight of 100, the first server will receive twice the number of sessions as the second server.
- **Use IP Address Redirection (Recommended)** Session Broker can use two methods to redirect a client to a disconnected session: IP address redirection and routing token redirection. IP address redirection is enabled by default and is suitable in most scenarios. This redirection method works when the clients can connect to each terminal server in the farm directly. Clear this check box only if your terminal services clients cannot connect to all terminal servers in the farm and when your network load balancing solution supports TS Session Broker routing tokens.
- **Select IP addresses to be used for reconnection** Use this section to select the IP address that you want to enable for use in the terminal server farm.

Exam Tip Remember to disable IP address redirection in TS Session Broker when your network includes a load balancer (usually a hardware load balancer) that supports routing tokens.

Exam Tip For both the 70-643 exam and the real world, remember that you need to add each farm member to the Session Directory Computers local group on the TS Session Broker server.

IMPORTANT TS Session Broker and load balancing initial connections

To distribute the initial connections to the server farm, TS Session Broker load balancing must rely on a load balancing solution such as DNS round-robin, Network Load Balancing, or a hardware load balancer.

Configuring Terminal Services Printer Redirection

Printer redirection is a feature that enables the client's printers to be used as printers for a Terminal Services session. Although you can easily modify basic options regarding printer redirection in the Client Settings tab of the RDP-Tcp Properties dialog box, Group Policy contains important additional options concerning this feature.

You can disable or customize the behavior of printer redirection by using Group Policy and the Group Policy Management console. To find printer redirection configuration options in Group Policy, open a Group Policy object (GPO), and navigate to Computer Configuration\Policies

\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Printer Redirection. Within the Printer Redirection folder, you can configure the following five policy settings:

- **Do Not Set Default Client Printer To Be Default Printer In A Session** By default, Terminal Services automatically designates the client default printer as the default printer in a Terminal Services session. You can use this policy setting to override this behavior. If you enable this policy setting, the default printer in the Terminal Services session will be designated as the printer specified on the remote computer.
- **Do Not Allow Client Printer Redirection** This policy setting essentially disables printer redirection completely. If you enable this policy setting, users cannot redirect print jobs from the remote computer to a local client printer in Terminal Services sessions.
- **Specify Terminal Server Fallback Printer Driver Behavior** This policy setting determines the behavior that occurs when the terminal server does not have a printer driver that matches the client's printer. By default, when this occurs, no printer is made available within the Terminal Services session. However, you can use this policy setting to fall back to a Printer Control Language (PCL) printer driver, to a PostScript (PS) printer driver, or to both printer drivers.
- **Use Terminal Services Easy Printer Driver First** The Terminal Services Easy Printer driver enables users to print reliably from a terminal server session to the correct printer on their client computer. It also enables users to have a more consistent printing experience between local and remote sessions. By default, the terminal server first tries to use the Terminal Services Easy Printer driver to install all client printers. However, you can use this policy setting to disable the use of the Terminal Services Easy Printer driver.
- **Redirect Only The Default Client Printer** By default, all client printers are redirected to Terminal Services sessions. However, if you enable this policy setting, only the default client printer is redirected in Terminal Services sessions.

Exam Tip Be sure to understand these Group Policy settings for the 70-643 exam.

Quick Check

1. You want to prepare to take a server in a server farm offline. You do not want to force any users off. What should you do?
2. You want to enable audio in Terminal Services connections to a server named TS1. What should you do?

Quick Check Answers

1. In the Terminal Services Configuration console, configure the terminal server properties to allow reconnections but prevent new logons.
2. Clear the Audio check box on the Client Settings tab in RDP-Tcp properties on TS1.

PRACTICE Installing and Configuring a License Server

After you have purchased TS CALs from Microsoft or a third-party reseller, you need to install and activate the license server. In this exercise, you will install a Terminal Services license server on Server1. Server1 will thus act as a license server for Server2, on which Terminal Services is already installed.

After installing the license server, you will then open the TS Licensing Manager console to review the procedures for activating a license server and installing TS CALs.

▶ Exercise 1 Install the TS Licensing Server Role

In this exercise, you will use the Add Roles Wizard to install a Terminal Services license server on the Contoso.com domain controller.

1. Log on to Contoso.com from Server1 as a domain administrator.
2. Open Server Manager.
3. In the Server Manager console tree, select the Roles node, and then click Add Roles in the details pane.

   The Add Roles Wizard opens.
4. On the Before You Begin page, click Next.
5. On the Select Server Roles page, select the Terminal Services check box, and then click Next.
6. On the Terminal Services page, click Next.
7. On the Select Role Services page, select the TS Licensing check box, and then click Next.
8. On the Configure Discovery Scope For TS Licensing page, read all the text on the page.

   Note that you can configure the license server for the local Active Directory domain or for the entire forest in a multidomain environment. The current Active Directory environment is composed of a single-domain forest.

Exam Tip Be sure to read this page carefully. For the exam, you need to understand the concepts of discovery scopes for TS licensing.

---

9. On the Configure Discovery Scope For TS Licensing page, leave the default selection of This Domain, and then click Next.
10. On the Confirm Installation Selections page, read all the text on the page, and then click Install.

    When the installation completes, the Installation Results page appears.
11. On the Installation Results page, click Close.

▶ Exercise 2 Activate a Terminal Services Licensing Server

In this exercise, you will activate the license server and review the process for installing TS CALs. This process requires Server1 to be connected to the Internet.

1. While you are logged on to Server1 as a domain administrator, open the TS Licensing Manager console by clicking Start, pointing to Administrative Tools, pointing to Terminal Services, and then clicking TS Licensing Manager.

   TS Licensing Manager opens.

   Although TS Licensing Manager is installed automatically on any server on which you have installed the TS Licensing role service, you do not need to manage the licensing server from the server itself. You can also install TS Licensing Manager on any server and connect to the license server remotely.
2. In the TS Licensing Manager console tree, expand the All Servers node, and then select the SERVER1 node. (The node should be marked by a red X at this point because it has not been activated.)
3. Right-click the SERVER1 node, and then click Activate Server.

   The Activate Server Wizard appears.
4. On the Welcome To The Activate Server Wizard page, read all the text on the page, and then click Next.
5. On the Connection Method page, read all the text on the page, and then answer the following question: By default, which is the default Connection Method assigned to the license server?

   Answer: Automatic Connection (Recommended)
6. On the Connection Method page, in the Connection Method drop-down list, select Web Browser.
7. Read the new associated Description and Requirements sections that have been refreshed on the page. The Web Browser connection method is useful when the licensing server does not connect to the Internet. With this option, you need merely to be able to connect from another server to both the licensing server and the Internet.
8. On the Connection Method page, in the Connection Method drop-down list, select Telephone.

9. Read the new associated Description and Requirements sections that have been refreshed on the page. The Telephone connection method is useful when your network is not connected to the Internet.
10. On the Connection Method page, in the Connection Method drop-down list, select Automatic Connection, and then click Next.

    The Activate Server Wizard dialog briefly appears while Server1 contacts the activation server at the Microsoft Clearinghouse. After a moment, the Company Information page appears.
11. On the Company Information page, enter appropriate information in the First Name, Last Name, and Company text boxes. Then, choose your country from the Country Or Region drop-down list.
12. Click Next.
13. Another Company Information page appears. Optionally, you may provide the requested information. Click Next.

    The Activate Server Wizard dialog box appears briefly, and then the Completing The Activate Server Wizard page appears. Note that the Start Install Licenses Wizard Now check box is selected.
14. On the Completing The Activate Server Wizard page, read all the text, and then click Next.

    The Welcome To The Install Licenses Wizard page appears.
15. Leave all windows open and proceed to Exercise 3.

▶ Exercise 3 Review the Process to Install TS CALs

Installing client licenses is the last stage of deploying a license server. Even if you do not have any TS CALs to install at this point, it is a good idea to review the pages of the Install Licenses Wizard to gain a better understanding of this deployment process in its entirety.

In this exercise, you will review the process of installing TS CALs in your newly activated server.

1. On the Welcome To The Install Licenses Wizard page, shown in Figure 3-24, read all the text on the page, and then click Next.

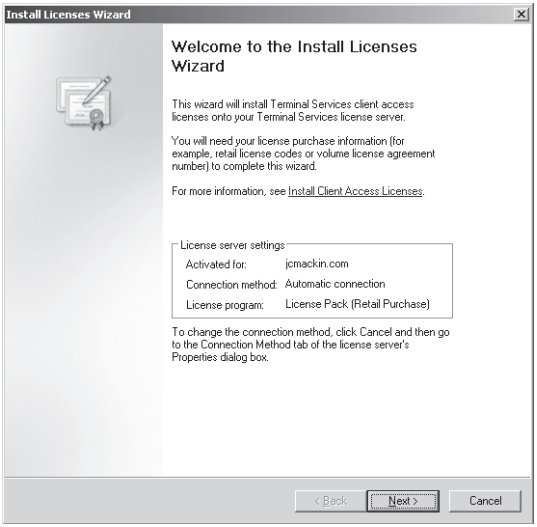

Figure 3-24 The Welcome page of the Install Licenses Wizard

The Install Licenses page briefly appears, and then the License Program page appears. The License Program page is shown in Figure 3-25.

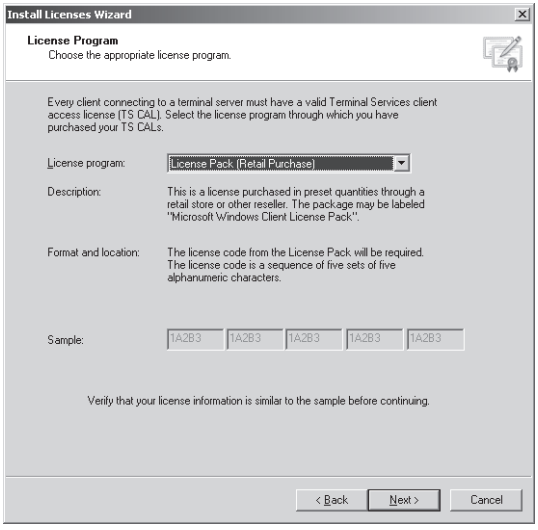

Figure 3-25 The License Program page of the Install Licenses Wizard

2. Read all the text on the License Program page.
3. Review the options from the License Program drop-down list.
4. Take a few moments to explore the various license program options by selecting each option and reading the entire associated text on the page.
5. In the License Program drop-down list, ensure that the default option of License Pack (Retail Purchase) is selected, and then click Next.

   The License Code page appears. The License Code page is shown in Figure 3-26.

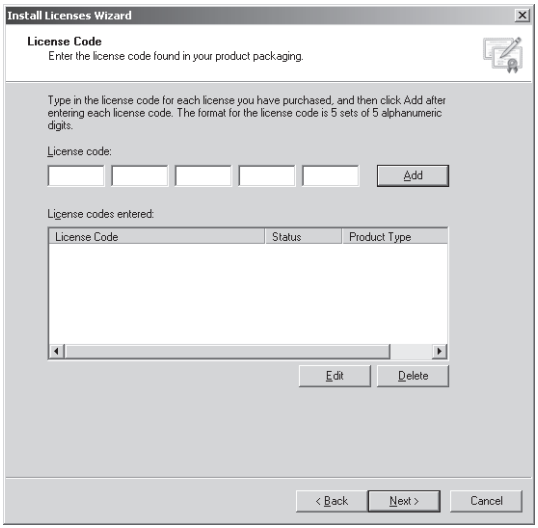

Figure 3-26 The License Code page of the Install Licenses Wizard

6. Read all the text on the page.

   If you have obtained a valid license code, you can perform the remaining steps of the practice. Otherwise, you can click Cancel to close the wizard and then simply read the remaining steps of the practice.
7. In the License Code text boxes, type a valid license code, and then click the Add button.
8. On the License Code page, click Next.

   The Install Licenses Wizard dialog box briefly appears, and then the Completing The Install Licenses Wizard page appears. This page is shown in Figure 3-27.

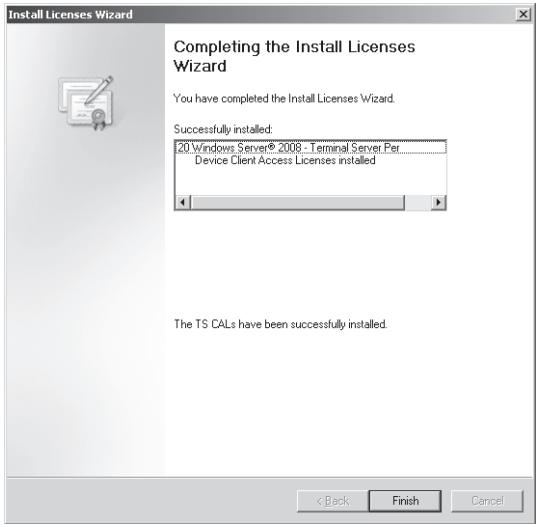

Figure 3-27 The Completing page of the Install Licenses Wizard

9. On the Completing The Install Licenses Wizard page, click Finish.
10. In the TS Licensing Manager console tree, the Server1 node is now designated with a green check mark, as shown in Figure 3-28. The licensing server is now configured.

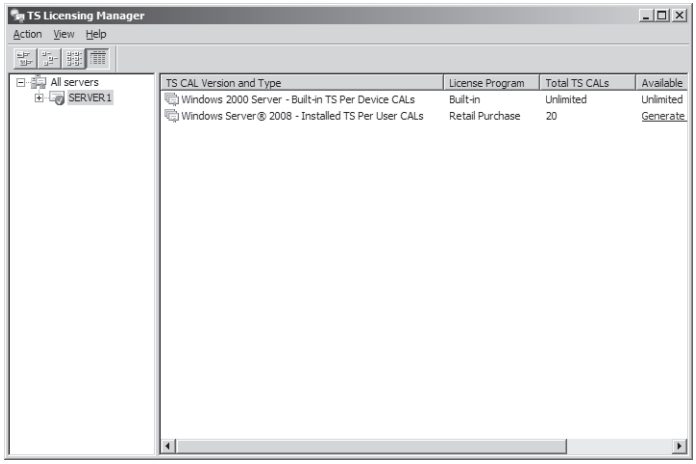

Figure 3-28 Successful deployment of a licensing server

11. Log on to Contoso.com from Server2 as a domain administrator, and then open the Terminal Services Configuration console.

12. In the Edit Settings – Licensing area, double click the Terminal Services Licensing Mode option.
13. On the Licensing tab of the Properties dialog box, select either the Per Device or the Per User option, corresponding to the type of TS CALs you have installed on Server1.
14. In the Specify The License Server Discovery Mode area, select the Use The Specified License Servers option, and then type **Server1.contoso.com** in the associated text box.
15. Click Check Names to verify the connection to the server.
16. When you receive a message indicating that the server specified is a valid terminal server license server, click OK.
17. In the Properties dialog box on Server2, click OK.

    In the Terminal Services Configuration console, the Terminal Services Licensing Mode option is now specified as Per Device or Per User.
18. Close all open windows, and then log off both Server1 and Server2.

Lesson Summary

- The main tool used for configuring Terminal Services is the Terminal Services Configuration console.
- You can edit RDP-Tcp properties in the Terminal Services Configuration console to configure Terminal Services session features such as encryption strength, timeout settings, and printer availability.
- The Terminal Services server properties available in the Terminal Services Configuration console enable you to configure settings related to load balancing, license server discovery, temporary folders, and new logon prevention.
- Group Policy offers additional control for Terminal Services printer redirection, notably for the option to fall back to a generic printer driver and to redirect only the default client printer.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

---

1. Your company network has implemented a terminal server farm named TSFARM1. The farm consists of five computers running Windows Server 2008, including a server named TSLB1 on which the TS Session Broker role service is installed. You want to add a sixth computer running Windows Server 2008, named TSLB6, to the farm. After configuring the server with the same hardware and software options as those of the other farm members, you join TSLB6 to the farm by specifying TSLB1 as the TS Session Broker Server and TSFARM1 as the farm name in the TS Session Broker properties on TSLB6. You verify that some users who attempt to connect to the virtual server name TSFARM1 are able to establish Terminal Services sessions on TSLB6, but these users are not able to reconnect to disconnected sessions. You want users connecting to TSLB6 through TSFARM1 to be able to reconnect to disconnected RDP sessions. What should you do?
   - **A.** Add TSLB6 to the Session Directory Computers local group on TSLB6.
   - **B.** Add TSLB6 to the Session Directory Computers local group on TSLB1.
   - **C.** In the DNS server, add a Host (A) record named TSFARM1 that maps to the IP address of TSLB6.
   - **D.** In the DNS server, add a Host (A) record named TSLB6 that maps to the IP address of TSLB6.
2. Your company network consists of a single Active Directory domain named Contoso.com. In the company network, you have deployed Terminal Services on a computer named TS1 that is running Windows Server 2008. Some users who connect to TS1 through RDP complain that they cannot print successfully to their local printers. You want to ensure that TS1 uses a generic PostScript printer driver whenever Terminal Services cannot find an adequate driver for Terminal Services client printers. What should you do?
   - **A.** On the Client Session tab of RDP-Tcp properties on TS1, select the Windows Printer option.
   - **B.** On the Client Session tab of RDP-Tcp properties on TS1, select the Default To Main Client Printer option.
   - **C.** In a Group Policy object (GPO), configure the User Terminal Services Easy Printer Driver First policy setting, and then apply the GPO so that TS1 falls within the scope of the policy.
   - **D.** In a Group Policy object (GPO), configure the Specify Terminal Server Fallback Printer Driver policy setting with the PS option, and then apply the GPO so that TS1 falls within the scope of the policy.

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenario. This scenario sets up a real-world situation involving the topics of this chapter and asks you to create solutions.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- Terminal Services enables users to establish a desktop or application session on a remote computer. In Windows Server 2008, Terminal Services includes many new and important features such as TS Gateway, RemoteApp, and TS Web Access.
- Terminal Services requires client access licenses (CALs) either for all connecting users or for all connecting devices. If you do not purchase and install Terminal Services CALs, the feature will stop working after 120 days.
- To install Terminal Services on a computer running Windows Server 2008, add the Terminal Services server role.
- The main tool used for configuring Terminal Services is the Terminal Services Configuration (TSC) console. In the TSC console, you can edit RDP-Tcp properties to configure Terminal Services user session features such as encryption strength, timeout settings, and printer availability. You can also edit server properties to configure settings related to load balancing, license server discovery, and new logon prevention.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- Network Level Authentication (NLA)
- Printer Redirection
- Remote Desktop for Administration (RDA)
- Remote Desktop Protocol (RDP)
- Terminal Services connection
- Terminal Services session

- Terminal Services client access license (TS CAL)
- TS Session Broker

Case Scenarios

In the following case scenario, you will apply what you've learned in this chapter. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Choosing a TS Licensing Strategy

You work as a network administrator in a large company. Your department has recently implemented two terminal servers, named TS1 and TS2, and you have been tasked with making licensing recommendations for each server.

TS1 is an application server. Although the application is not considered mission critical, as many as five users tend to be connected to it simultaneously. Overall, 20 users need to connect to TS1 at some point during the day. They can connect from any of 50 different computers.

TS2 is a DNS server that occasionally requires remote maintenance and administration. Only administrators connect to TS2.

1. Do you need to install Terminal Services on TS1? Which type of client access licenses would you purchase, if any?
2. Do you need to install Terminal Services on TS2? Which type of client access licenses would you purchase, if any?

Case Scenario 2: Troubleshooting a Terminal Services Installation

You work in IT support for a large company whose network consists of a single Active Directory domain. One of your responsibilities is supporting terminal servers in the Advertising department. Over the course of a week, you encounter the following two problems:

1. You deploy Terminal Services on a new computer running Windows Server 2008 named App3, but you discover that no users running Windows XP can connect to it. What should you do?
2. Users that connect to a terminal server named App1 complain that they cannot always reconnect to a disconnected session. What should you do?

Suggested Practices

To help you successfully master the exam objectives presented in this chapter, complete the following tasks.

Deploy a Terminal Server Farm

In this practice, you create a load balanced terminal server farm.

- **Practice** Using either virtual or physical computers, join two identical installations of Windows Server 2008 to a domain. Install the Terminal Server role service on both computers but the TS Session Broker role service on just one. Add both computer names to the Session Directory Computers local group on the Session Broker computer. Use the TS Session Broker tab in the Terminal Services Configuration console on both computers to configure the Terminal Services farm. Create Host (A) records for the farm name in DNS, one record for each server IP address. Then, connect to the server farm through from a remote RDP client.

Watch a Webcast

In this practice, you watch a Webcast about Terminal Services in Windows Server 2008.

- **Practice** Watch the "A Technical Overview of Windows Server 2008 Terminal Services" Webcast by Blain Barton, available on the companion CD in the Webcasts folder. This Webcast is also available online at *http://msevents.microsoft.com*; search for event ID 1032345660.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-643 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO Practice tests

For details about all the practice test options available, see the "How to Use the Practice Tests" section in this book's introduction.
