

Managing and Maintaining a Microsoft Windows Server 2003

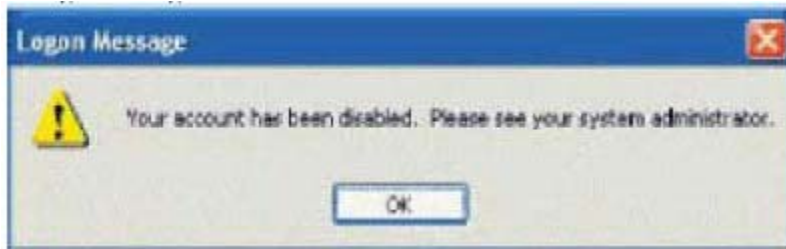
70-290

**Demo Version
From
ITCertKeys.com
To
CertsBraindumps.com**

This study guide demo consists of 18 numbers of questions and answers with explanation. You can buy the full version of this study guide from the sponsored website.

Question 1.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain. All domain controllers run Windows Server 2003, and all client computers run Windows XP Professional. A user named ITCert reports that she cannot log on to the domain from his computer. ITCert receives the logon message shown in the exhibit.



You need to enable ITCert to log on. What should you do?

- A. Run the net user command with the appropriate switches.
- B. Run the net accounts command with the appropriate switches.
- C. Run the dsmod user command with the appropriate switches.
- D. Add ITCert to the Users group.
- E. Remove ITCert from the Guests group.

Answer: C

Explanation:

DSmod is a command line tool that can be used to modify the user and group relevant tasks through command prompt.

The syntax of this command is shown below.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Admin.SERVER>dsmod
Description: This dsmod command modifies existing objects in the directory.
The dsmod commands include:

dsmod computer - modifies an existing computer in the directory.
dsmod contact - modifies an existing contact in the directory.
dsmod group - modifies an existing group in the directory.
dsmod ou - modifies an existing organizational unit in the directory.
dsmod server - modifies an existing domain controller in the directory.
dsmod user - modifies an existing user in the directory.
dsmod quota - modifies an existing quota specification in the directory.
dsmod partition - modifies an existing quota specification in the directory.

For help on a specific command, type "dsmod <ObjectType> /?" where
<ObjectType> is one of the supported object types shown above.
For example, dsmod ou /?.

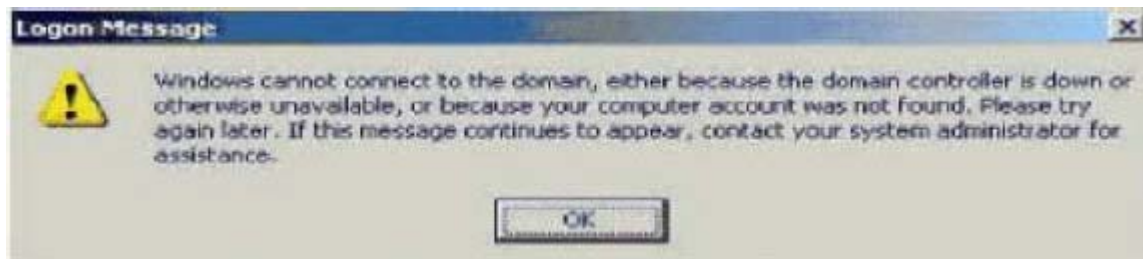
Remarks:
The dsmod commands support piping of input to allow you to pipe results from
the dsquery commands as input to the dsmod commands and modify the objects
found by the dsquery commands.

Commas that are not used as separators in distinguished names must be
escaped with the backslash "\" character
(for example, "CN=Company\, Inc.,CN=Users,DC=microsoft,DC=com").
Backslashes used in distinguished names must be escaped with a backslash
(for example,
"CN=Sales\\ Latin America,OU=Distribution Lists,DC=microsoft,DC=com").

Examples:
```

Question 2.

You are the network administrator for ITCertKeys.com. All network servers run Windows server 2003, and all client computers run Windows XP Professional. A user named ITCert manages an application server named Server25. One morning, ITCert tries to log on to ITCert notifies you of the problem.



You open Active Directory Users and Computers and see the display



You need to enable ITCert to log on to Server 25. Your solution must require the minimum amount of administrative effort. What should you do?

- A. Enable the computer account for Server 25
- B. Reset the computer account for Server 25.
- C. Remove Server 25 from the domain, and then rejoin Server25 to the domain.
- D. Delete the computer account for Server25, and then create a new account with the same name.

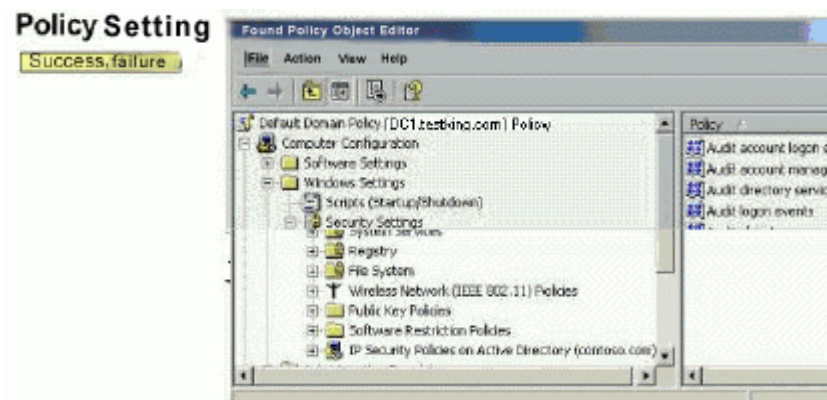
Answer: A

Explanation:

The red mark against Server25 indicates that the computer account for Server25 is disabled. You should enable this account.

Question 3.

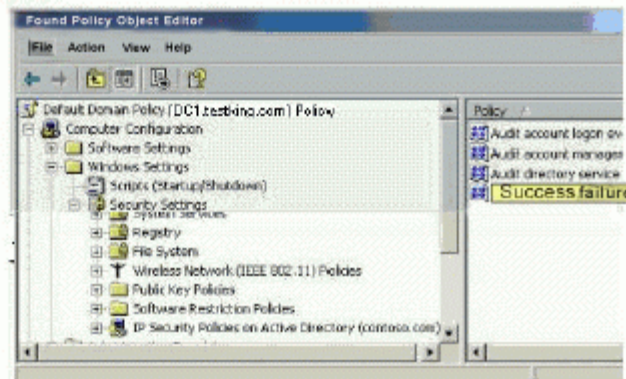
You are the network administrator for Contoso, Ltd. Your network consists of a single Active Directory domain ITCertKeys.com. All network servers run Windows Server 2003. You need to audit all logon attempts by domain users. You must ensure that the minimum amount of necessary information is audited. To achieve this goal, you will edit the Default Domain Controller Group Policy object (GPO). What should you do?



Answer:

Policy Setting

Success, failure



Explanation:

This setting will audit all logon events that use domain user accounts.

The Audit Logon Events policy is for auditing log on attempts using local user accounts.

Question 4

You are the network administrator for ITCertKeys. All network servers run Windows Server 2003. You install Software Update Services (SUS) on one server. You configure the following settings:

- Do not use a proxy server for Internet access.
- Synchronize directly from the Microsoft Windows Update servers.
- Automatically approve new versions of previously approved updates.
- Save updates in a local folder.

You perform a manual synchronization. Now you need to back up the critical information that is related to your installation of SUS. What should you do?

- A. First, use the Backup utility to back up the System State data.
Then, use the IIS administration tool to back up the default Web site.
- B. First, use the IIS administration tool to back up the default Web site.
Then, use the Backup utility to back up the System State data.
- C. First, use the IIS administration tool to back up the IIS metabase. Then, use the Backup utility to back up the IIS metabase file, the default Web site, and the content storage location.
- D. First, use the Backup utility to back up the IIS metabase file, the default Web site, and the content storage location. Then, use the IIS administration tool to back up the IIS metabase.

Answer: C

Explanation:

In order to have a fully functional server running SUS after a failure, you need to backup the Web site directory that the administration site was created in, the SUS directory that contains the content, and the IIS metabase.

1. You should take these steps to backup the SUS.
2. Start by creating a backup of the IIS metabase using the IIS MMC Snap-in. After creating the IIS metabase backup, run NTBackup to backup and verifies that the C:\inetpub\wwwroot (Default Web Site) and the C:\inetpub\msus directories (Content Storage Location) and %windir%\system32\inetpub\metaback (IIS metabase) are selected for backup. All of this data is required for proper operation of SUS and IIS after the data has been restored.

Question 5.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain ITCertKeys.com. All network servers run Windows Server 2003. Server with two logical disks, P:\ and U:\. Each disk has a capacity of 20 GB. For each department in the branch office, P:\ hosts one folder in which departmental users save shared documents. For all users in the branch office, U:\ hosts home folders.

The main office includes a network operations center that monitors servers and network status. However, branch office users frequently report that their servers have no more disk space. In such cases, local support technicians log on to the servers and delete unnecessary files.

You need to create a proactive monitoring strategy for the network operations center. Monitoring must alert the network operations center before the branch office servers run out of disk space. Monitoring must also report which disks on the servers are approaching capacity. The monitoring strategy must require the minimum amount of administrative effort. What should you do?

- A. Configure a server in the main office to report performance alters on the branch office servers. Use the logicaldisk(_total)\ &Free Space counter to indicate when free space is less than 5 percent. Use the logicaldisk(_total)\Free megabytes counter to indicate when free space is less than 100 MB.
- B. On each branch office server, create a performance alert. Use the logicaldisk(_total)\ %Free Space counter to indicate when free space is less than 5 percent. Use the logicaldisk(_total)\Free megabytes counter to indicate when free space is less than 1000 MB.
- C. Configure a server in the main office to report performance alerts on the branch office servers. Use the logicaldisk(P)\ %Free Space counter and the logicaldisk(U)\ %Free Space counter to indicate when free space is less than 5 percent.
- D. On each branch office server, create a performance alert. Use the logicaldisk(P)\ %Free Space counter and the logicaldisk(U)\ %Free Space counter to indicate when free space is less than 5 percent.

Answer: B

Explanation:

According to the given situation "Monitoring must alert the network operations center before the branch office servers run out of disk space. Monitoring must also report which disks on the servers are approaching capacity" choice B is correct.

% Free Space is the percentage of total usable space on the selected logical disk drive that was free.

Free Megabytes displays the unallocated space, in megabytes, on the disk drive in megabytes. One megabyte is equal to 1,048,576 bytes.

Question 6.

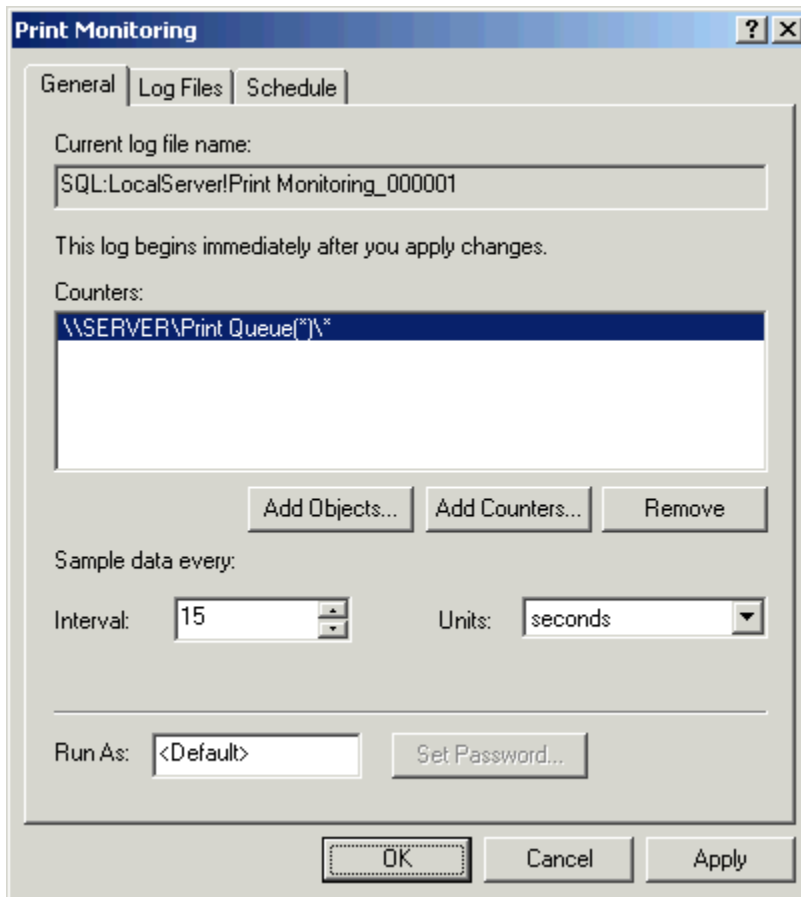
You are the network administrator for ITCertKeys. The network is distributed across five countries in Europe, namely Spain, Italy, Hungary, Austria, and Germany. All network servers run Window Server 2003. Each location has three print servers. You need to monitor usage of print queues on all print servers on the network. You plan to enable monitoring for each print server in the same way. Monitoring data must be stored in a central location and archived for five years to enable data comparison. What should you do?

- A. Create a counter log on specify SQL Database as the log file type.
- B. Create a trace log and specify Circular Trace File as the log file type.
- C. Create a counter log and specify Binary Circular File as the log file type.
- D. Create a trace log and specify Sequential Trace File as the log file type.

Answer: A

Explanation:

For this purpose, you should create a counter log for the print queue and specify a SQL database for five years archived data comparison.

**Question 7.**

You are the network administrator for ITCertKeys. All network servers run Windows Server 2003. A member server named ITCertKeys1 hosts several hundred folders, which reside in various locations on the server. ITCertKeys1 is configured to run a normal backup of the folder every Saturday at 1:00 A. M. You discover that users edit the contents of the folders on Saturday and Sunday. You need to use the Backup utility to reschedule the backup job so that it runs every Monday at 1:00 A. M. instead of every Saturday at 1:00 A. M. You must achieve this goal by using the minimum amount of administrative effort. What should you do?

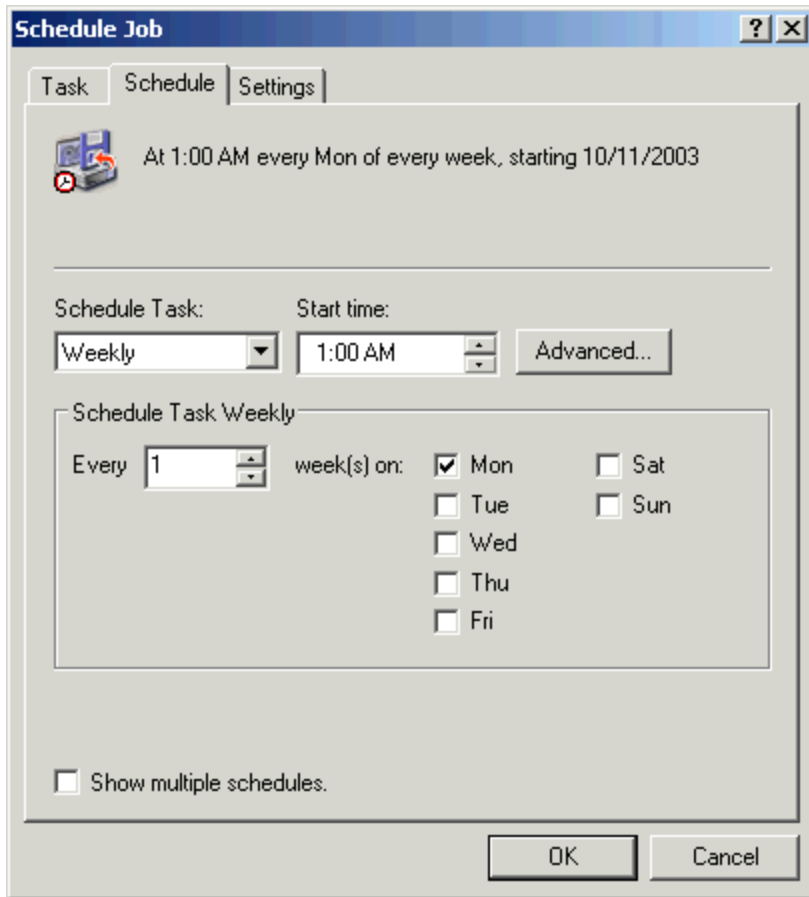
- A. Specify Monday as the start date of the job.
- B. Reconfigure the job schedule to run the backup every Monday at 1:00 A. M.
- C. Add an additional schedule to the job. Configure the additional schedule to run the backup on Monday at 1:00 A. M.
- D. Use the Repeat Task option to configure the existing job to repeat every 48 hours until an interval of 336 hours passes.

Answer: B

Explanation:

You should run the ntbackup utility and under Scheduled jobs tab reconfigure your backup job to run the backup on Monday at 1:00 A. M.





Question 8.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain ITCertKeys.com. All network servers run Windows Server 2003. A member server named ITCertKeysSrvA has a locally attached tape device. You need to back up all data on ITCertKeysSrvA at least once every week. Every day, you need to back up only the data that was changed after the last backup. You need to minimize the amount of data that must be backed up every day. Which backup types should you use? To answer, drag the appropriate backup type to the corresponding backup schedule.

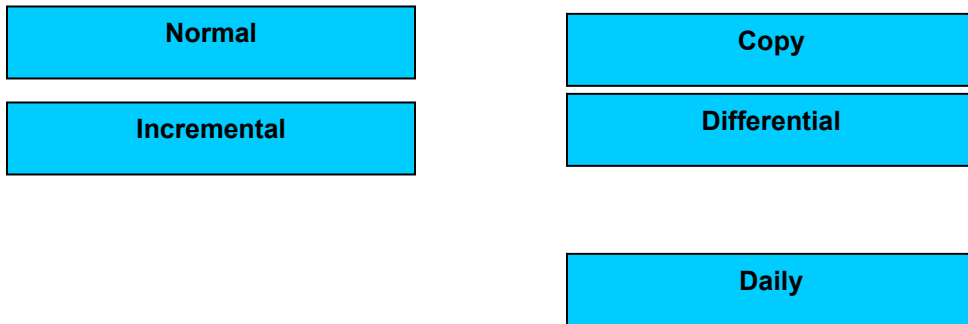
Backup Schedule Place here

Every Week
Every Day

Backup Types

Normal
Copy
Differential
Incremental
Daily

Answer:



Explanation:

Backing up your data using a combination of normal backups and incremental backups requires the least amount of storage space and is the quickest backup method. However, recovering files can be time-consuming and difficult because the backup set might be stored on several disks or tapes.

Backing up your data using a combination of normal backups and differential backups is more time-consuming, especially if your data changes frequently, but it is easier to restore the data because the backup set is usually stored on only a few disks or tapes.

Question 9.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain ITCertKeys.com. All servers run Windows Server 2003, and all client computers run Windows XP Professional. You install Terminal Server on a member server named ITCertKeys4. Several days later, users report that server performance is unacceptably slow. On Server1, you discover 75 disconnected session and 25 sessions that have been idle for at least three hours. You need to configure ITCertKeys4 to fulfill the following requirements:

- . • Disconnected sessions remain on the server for a maximum of 1 minute.
- . • Idle sessions remain on the server for a maximum of 30 minutes.
- . • Session idle for more than 30 minutes are automatically reset.
- Active sessions are not affected. What should you do? To answer, configure the appropriate option or options in the dialog box.

RDP-Tcp Properties [?] [X]

Remote Control | Client Settings | Network Adapter | Permissions
General | Logon Settings | Sessions | Environment

Use this tab to set Terminal Services timeout and reconnection settings.

☐ Override user settings

End a disconnected session: [1 minute]

Active session limit: [Never]

Idle session limit: [Never]

☐ Override user settings

When session limit is reached or connection is broken:

☒ Disconnect from session

☐ End session

☐ Override user settings

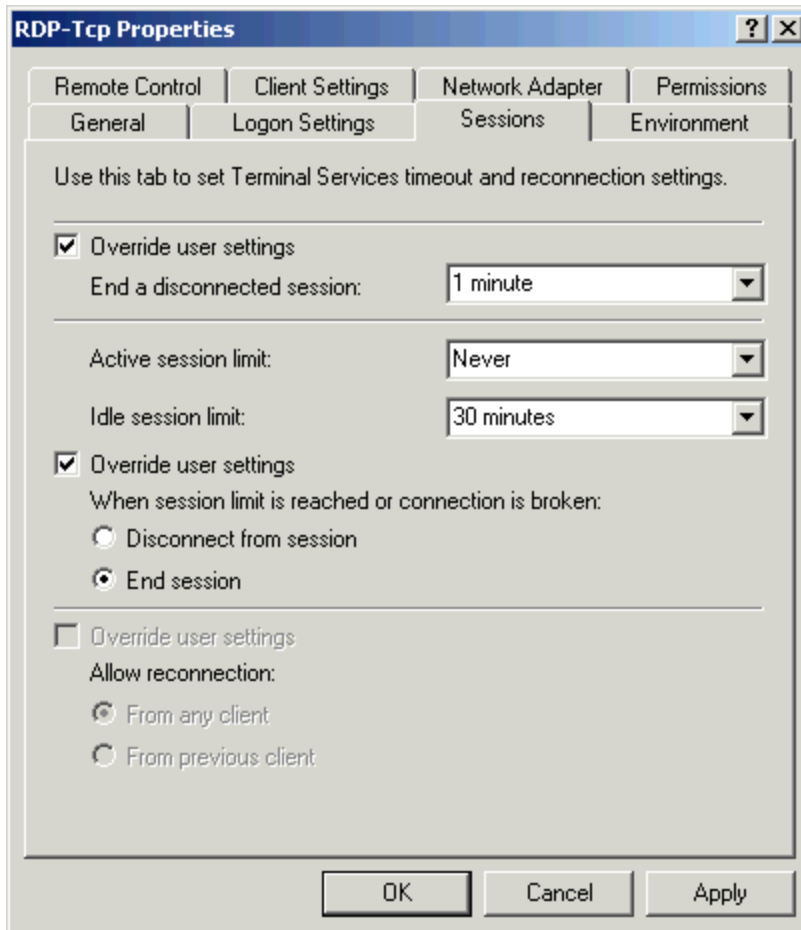
Allow reconnection:

☒ From any client

☐ From previous client

[OK] [Cancel] [Apply]

Answer:



Explanation:

The above exhibit fully explains the configuration of the terminal service.

Question 10.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain named ITCertKeys.com. All network servers run Windows Server 2003, and all client computers run Windows XP Professional. You install a new server named Server22 with default settings.

During installation, you set the IP configuration shown in the exhibit.

```
c:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : server22
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : AMD PCNET Family PCI Ethernet Adapter
Physical Address. . . . . : 00-50-56-59-01-F8
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.10.100.71
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.10.10.3
DNS Servers . . . . . : 10.10.100.71

c:\>
```

You make Server22 a member of a workgroup. Then you restart Server22 and use the local Administrator account to log on locally. You join Server22 to the domain. You restart Server22 and use the Domain Administrator account to log on. However, you are unsuccessful. You need to ensure that Server22 is a member of the domain. What should you do?

- A. Open the Active Directory Users and Computers and reset Server22.
- B. From a command prompt on another member server or domain controller, type: `dsmod computer Server22.ITCertKeys.com-reset`
- C. Log on locally. In the TCP/IP properties, change the DNS server of Server22.
- D. Log on locally. In the TCP/IP properties, change the subnet mask of Server22.
- E. From a command prompt on another member server or domain controller, type: `nltest /server:Server22.ITCertKeys.com /trusted_domains`

Answer: C

Explanation:

The exhibit shows that server22 is configured with its own IP address as a DNS server. When a computer joins a domain, it requires the address of DNS server that host the domain controller information. This DNS server is normally the domain controller itself.

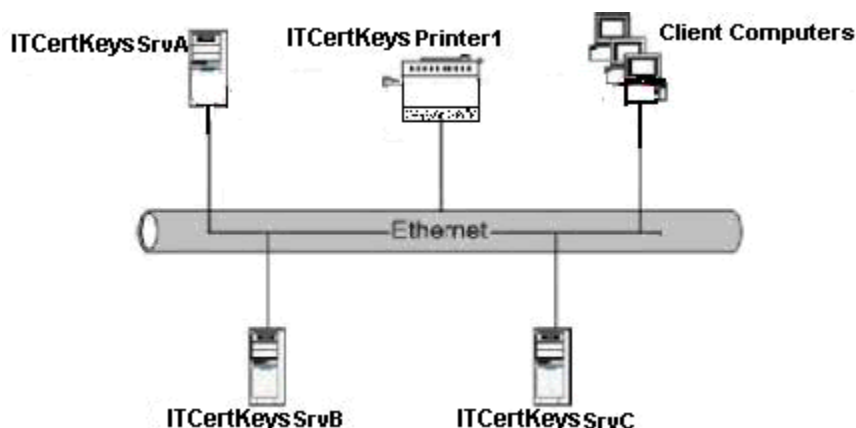
Therefore, you should change the IP address of the DNS server on the server22.

Question 11.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain named contoso.com. The network contains 100 Windows 2000 Professional computers and three Windows Server 2003 computers. Information about the three servers is shown in the following table.

Name	Operating System	Roles
ITCertkeysSrvA	Windows Server 2003	Domain controller, primary DNS server
ITCertkeysSrvB	Windows Server 2003	Domain Controller, WINS server
ITCertkeysSrvC	Windows Server 2003	Member server, DHCP server

You add a network interface print device named ITCertKeys Printer1 to the network. You manually configure the IP address for ITCertKeys Printer1. ITCertKeys Printer1 is not currently registered on the DNS server. The relevant portion of the network is shown in the exhibit.



You need to ensure that client computers can connect to ITCertKeys Printer1 by using its name. What should you do?

- A. On ITCertKeys SrvA, add an alias (CNAME) record that references ITCertKeys Printer1.
- B. In the Hosts file on ITCertKeys SrvC, add a line that references ITCertKeys Printer1.
- C. On ITCertKeys SrvA, add a service locator (SRV) record that reference ITCertKeys Printer1.
- D. On ITCertKeys SrvA, add a host (A) record that references ITCertKeys Printer1.
- E. In the Hosts file on ITCertKeys SrvB, add a line that references ITCertKeys Printer1.

Answer: D

Explanation:

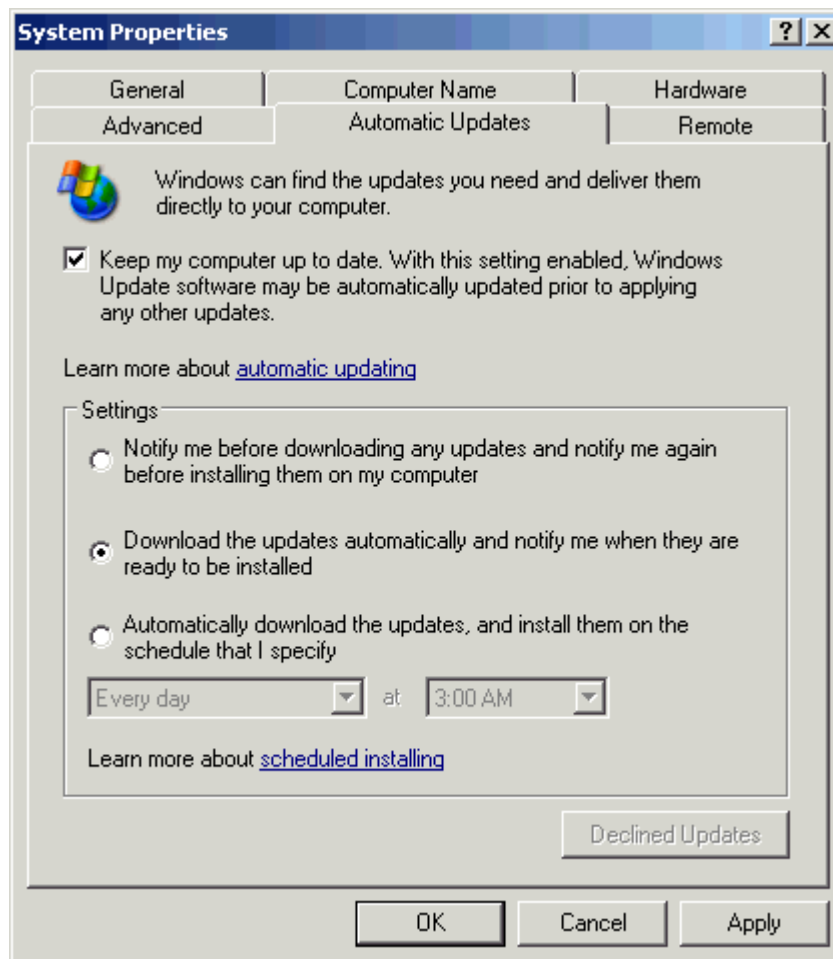
You should add a host (A) record to map the IP address of the printer with its name. In this the client computers will be able to connect to the printer1 with its name.

Question 12.

You are the network administrator for ITCertKeys. The network contains Windows Server 2003 computers and Windows XP Professional computers. You are configuring Automatic Update on the servers. The written company network security policy states that all updates must be reviewed and approved before they are installed. All updates are received from the Microsoft Windows Update servers. You want to automate the updates as much as possible.

What should you do?

To answer, configure the appropriate option or options in the dialog box.



Answer: Check the “Keep my computer up to date” checkbox. Select the “Download the updates automatically and notify me when they are ready to be installed” radio button.

Explanation:

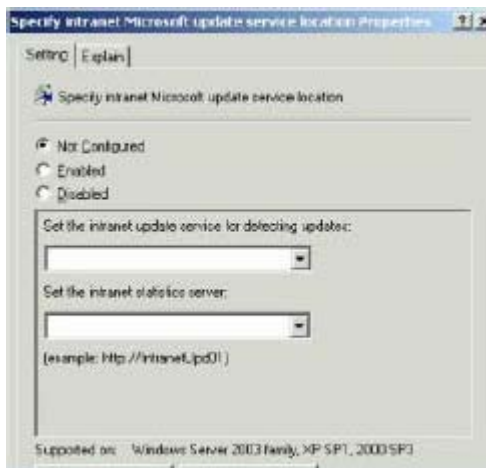
The updates will be automatically downloaded, but you will be able to review the updates before they are installed.

Question 13.

You are the network administrator for ITCertKeys. The network contains Windows Server 2003 computers and Windows XP Professional computers.

You install Software Update Services on a server named ITCertKeys A. You create a new Group Policy object (GPO) at the domain level. You need to properly configure the GPO so that all computers receive their updates from ITCertKeys A. How should you configure the GPO?

To answer, configure the appropriate option or options in the dialog box.

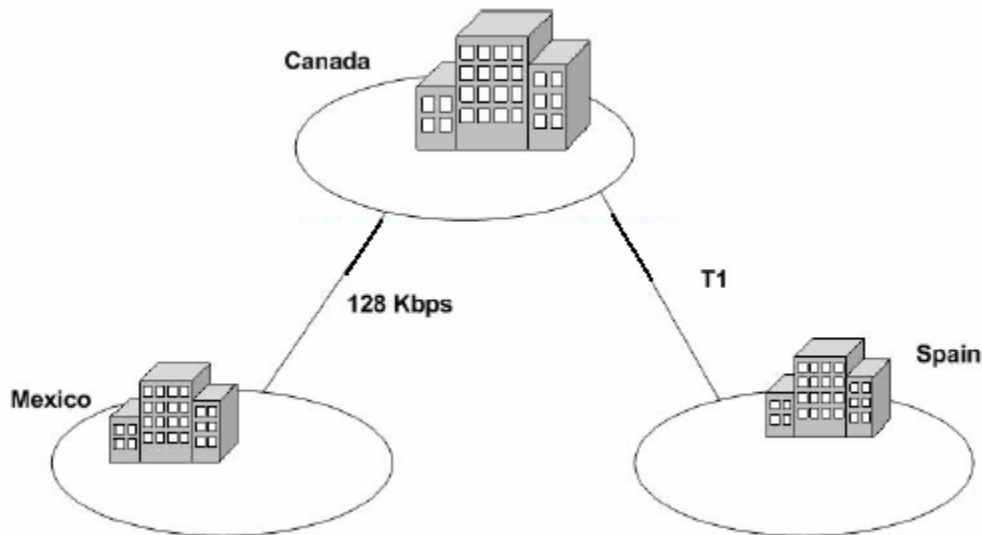


Answer:

Select the “Enabled” radio button. In the “Set the intranet update service for detecting updates” box, enter the name of the server; in this case you would enter http://ITCertKeys A. You should also enter http://ITCertKeys A as the address of the intranet statistics server.

Question 14.

You are the network administrator for ITCertKeys. ITCertKeys has offices in three countries. The network contains Windows Server 2003 computers and Windows XP Professional computers. The network is configured as shown in the exhibit.



Software Update Services (SUS) is installed on one server in each office. Each SUS server is configured to synchronize by using the default settings.

Because bandwidth at each office is limited, you want to ensure that updates require the minimum amount of time.

What should you do?

- A. Synchronize the updates with an SUS server at another office.
- B. Select only the locales that are needed.
- C. Configure Background Intelligent Transfer Service (BITS) to limit file transfer size to 9 MB.
- D. Configure Background Intelligent Transfer Service (BITS) to delete incomplete jobs after 20 minutes.

Answer: B

Explanation:

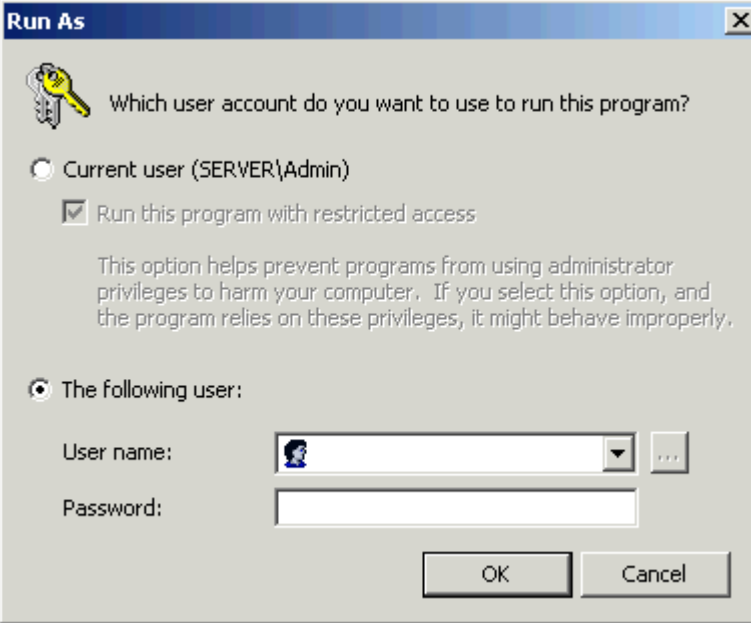
You should select the locales that are needed.

Question 15.

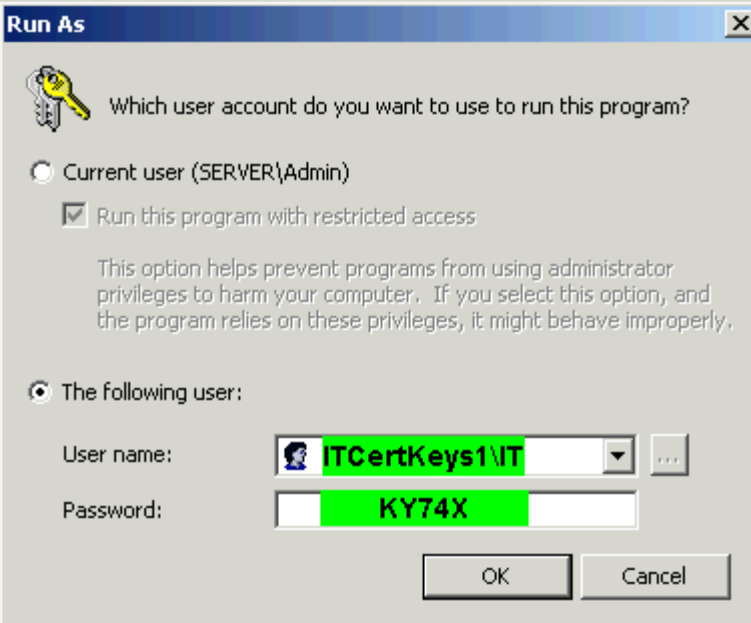
You are the file server administrator for ITCertKeys. The company network consists of a single Active Directory domain named ITCertKeys.com. The domain contains 12 Windows Server 2003 computers and 1,500 Windows XP Professional computers. You manage three servers named Server, ITCertKeys 2, and ITCertKeys 3. You need to update the driver for the network adapter that is installed in Server. You log on to Server 1 by using a non administrative domain user account named ITCert. You open the Computer Management console. When you select Device Manager, you receive the following error message: "You do not have sufficient security privileges to uninstall devices or to change device properties or device drivers". You need to be able to run the Computer Management console by using the local administrator account. The local administrator account on Server, ITCertKeys 2, and ITCertKeys 3 has been renamed IT. IT's password is kY74X.

In Control Panel, you open Administrative Tools. You right-click the Computer Management shortcut and click Run as on the shortcut menu.

What should you do next?

<div style="background-color: yellow; border: 1px solid black; padding: 2px; margin-bottom: 5px;">ITCertKeys1\IT</div> <div style="background-color: yellow; border: 1px solid black; padding: 2px; margin-bottom: 5px;">ITCertKeys\IT</div> <div style="background-color: yellow; border: 1px solid black; padding: 2px; margin-bottom: 5px;">ITCertKeys\Administrator</div> <div style="background-color: yellow; border: 1px solid black; padding: 2px;">KY74X</div>	 <p>The 'Run As' dialog box is shown. It asks 'Which user account do you want to use to run this program?'. There are two main options: 'Current user (SERVER\Admin)' and 'The following user:'. The 'Current user' option is selected. Below it, there is a checkbox for 'Run this program with restricted access' which is checked. A text box explains that this option helps prevent programs from using administrator privileges. At the bottom, there are fields for 'User name' and 'Password', and 'OK' and 'Cancel' buttons.</p>
---	---

Answer:

<div style="background-color: yellow; border: 1px solid black; padding: 2px; margin-bottom: 5px;">ITCertKeys\IT</div> <div style="background-color: yellow; border: 1px solid black; padding: 2px;">ITCertKeys\Administrator</div>	 <p>The 'Run As' dialog box is shown. It asks 'Which user account do you want to use to run this program?'. There are two main options: 'Current user (SERVER\Admin)' and 'The following user:'. The 'The following user:' option is selected. Below it, there is a checkbox for 'Run this program with restricted access' which is checked. A text box explains that this option helps prevent programs from using administrator privileges. At the bottom, the 'User name' field is filled with 'ITCertKeys1\IT' and the 'Password' field is filled with 'KY74X'. 'OK' and 'Cancel' buttons are at the bottom right.</p>
--	--

Explanation:

Choose "The following User", Enter "ITCertKeys1\IT" in the User Name field, enter KY74X" in the password field.

Question 16.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain named ITCertKeys.com. The domain contains Windows Server 2003 computers

and Windows XP Professional computers. All confidential company files are stored on a file server named ITCertKeys 1. The written company security states that all confidential data must be stored and transmitted in a secure manner. To comply with the security policy, you enable Encrypting File System (EFS) on the confidential files. You also add EFS certificates to the data decryption field (DDF) of the confidential files for the users who need to access them. While performing network monitoring, you notice that the confidential files that are stored on ITCertKeys 1 are being transmitted over the network without encryption. You must ensure that encryption is always used when the confidential files on ITCertKeys 1 are stored and transmitted over the network.

What are two possible ways to accomplish this goal? (Each correct answer presents a complete solution. Choose two)

- A. Enable offline files for the confidential files that are stored on ITCertKeys 1, and select the Encrypt offline files to secure data check box on the client computers of the users who need to access the files.
- B. Use IPsec encryption between ITCertKeys 1 and the client computers of the users who need to access the confidential files.
- C. Use Server Message Block (SMB) signing between ITCertKeys 1 and the client computers of the users who need to access the confidential files.
- D. Disable all LM and NTLM authentication methods on ITCertKeys 1.
- E. Use IIS to publish the confidential files.
Enable SSL on the IIS server.
Open the files as a Web folder.

Answer: B, E

Explanation:

You should implement the IPsec policies for the secure and encrypted communication between ITCertKeys1 computer and client computers. Similarly, you can use IIS to publish these files.

Question 17.

You are the network administrator in the New York office of ITCertKeys. The company network consists of a single Active Directory domain ITCertKeys.com. The New York office currently contains one Windows Server 2003 file server named ITCertKeys A.

All file servers in the New York office are in an organizational unit (OU) named New York Servers. You have been assigned the Allow – Change permission for a Group Policy object (GPO) named NYServersGPO, which is linked to the New York Servers OU.

The written company security policy states that all new servers must be configured with specified predefined security settings when the servers join the domain. These settings differ slightly for the various company offices.

You plan to install Windows Sever 2003, on 15 new computers, which all functions as file servers. You will need to configure the specified security settings on the new file servers. ITCertKeys A currently has the specified security settings configured in its local security policy. You need to ensure that the security configuration of the new file servers is identical to that of ITCertKeys A. You export a copy of ITCertKeys A's local security policy settings to a template file.

You need to configure the security settings of the new servers, and you want to use the minimum amount of administrative effort.

What should you do?

- A. Use the Security Configuration and Analysis tool on one of the new servers to import the template file.
- B. Use the default Domain Security Policy console on one of the new servers to import the template file.
- C. Use the Group Policy Editor console to open NYServersGPO and import the template file.
- D. Use the default Local Security Policy console on one of the new servers to import the template file.

Answer: C

Explanation:

The easiest way to accomplish this task is to use the group policy editor console to open NYServersGPO and then import the template file.

Question 18.

You are the network administrator for ITCertKeys. The network consists of a single Active Directory domain named ITCertKeys.com. The domain contains Windows Server 2003 computers and Windows XP Professional computers.

The Default Domain Policy has been modified by importing a security template file, which contain several security settings. A server named ITCertKeys1 cannot run a program that is functioning on other similarly configured servers. You need to find out whether additional security settings have been added to the local security policy on ITCertKeys1. To troubleshoot, you want to use a tool to compare the current security settings on ITCertKeys1 against the security template file in order to automatically identify any settings that might have been added to the local security policy.

Which tool should you run on ITCertKeys1?

- A. Microsoft Baseline Security Analyzer (MBSA)
- B. Security Configuration and Analysis console
- C. gpresult.exe
- D. Resultant Set of Policy console in planning mode

Answer: B

Explanation:

Security Configuration and Analysis is an MMC snap-in that provides security configuration and analysis for Windows computers using security template files. You can use this tool to compare the two security template files.