Exam Code: 070-296
Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Environment for a W2K MCSE

Demo Version

To Access Full Version, Please go to
www.itexamworld.com

QUESTION 1:

You are the network administrator for Itexamworld .com. The network consists of a single Active Directory domain Itexamworld .com. The network contains two Windows Server 2003 domain controllers, two Windows
2000 Server domain controllers, and two Windows NT Server 4.0 domain controllers.
All file servers for the finance department are located in an organizational unit (OU) named Finance Servers. All file servers for the payroll department are located in an OU named Payroll Servers. The Payroll Servers OU is a child OU of the Finance Servers OU.
Itexamworld 's written security policy for the finance department states that departmental servers must have security settings that are enhanced from the default settings. The written security policy for the payroll department states that departmental servers must have enhanced security settings from the default settings, and auditing must be enabled for file or folder deletion.
You need to plan the security policy settings for the finance and payroll departments.
What should you do?

A. Create a Group Policy object (GPO) to apply to the Compatws.inf security template to computer objects, and link it to the Finance Servers OU.
Create a second GPO to enable the Audit object access audit policy on computer objects, and link it to the Payroll Servers OU.
B. Create a Group Policy object (GPO) to apply the Securews.inf security template to computer objects, and link it to the Finance Servers OU.
Create a second GPO to enable the Audit object access audit policy on computer objects, and link it to the Payroll Servers OU.
C. Create a Group Policy object (GPO) to apply to the Compatws.inf security template to computer objects, and link it to the Finance Servers OU.
Create a second GPO to apply the Hisecws.inf security template to computer objects, and link it to the Payroll Servers OU.
D. Create a Group Policy object (GPO) to apply the Securews.inf security template to computer objects, and link it to the Finance Servers and to the Payroll Servers OUs.
Create a second GPO to enable the
Audit object access audit policy on computer objects, and link it to the Payroll Servers OU.

Answer: B

Explanation: The Securews.inf template contains policy settings that increase the security on a workstation or member server to a level that remains compatible with most functions and applications. The template includes many of the same account and local policy settings as Securedc.inf, and implements digitally signed communications and greater anonymous user restrictions.
Audit Object Access
A user accesses an operating system element such as a file, folder, or registry key. To audit elements like these, you must enable this policy and you must enable auditing on the resource that you want to monitor. For example, to audit user accesses of a particular file or folder, you display its Properties dialog box with the Security tab active, navigate to the Auditing tab in the Advanced Security Settings dialog box for that file or folder, and then add the users or groups whose access to that file or folder you want to audit.
Incorrect Answers:

A, C: The Compatws.inf security template is designed for Windows NT compatible applications that require lower security settings in order to run. These settings are lower than the default settings.
D: The Payroll Servers OU is a child OU of the Finance Servers OU. GPO settings applied to parent OUs are inherited by child OUs; therefore we do not need to link the GPO to both the finance Server OU and the Payroll Servers OU.
Reference:
Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington, Chapter 9 and 10.

QUESTION 2:

You are the network admin for Itexamworld . Your network contains 50 application servers that run Windows Server 2003.
The security configuration of the application servers is not uniform. The application servers were deployed by local administrators who configured the setting for each of the application servers differently based on their knowledge and skill. The application servers are configured with different authentication methods, audit settings and account policy settings.
The security team recently completed a new network security design. The design includes a baseline configuration for security settings on all servers. The baseline security settings use the hisecws.inf predefined security template. The design also requires modified settings for servers in an application server role. These settings include system service startup requirements, renaming the administrator account, and more stringent account lockout policies. The security team created a security template named application.inf that contains the required settings.
You need to plan the deployment of the new security design. You need to ensure that all security settings for the application servers are standardized, and that after the deployment, the security settings on all application servers meet the design requirements. What should you do?

A. Apply the setup security.inf template first, the hisecws.inf template next, and then the application.inf template
B. Apply the Application.inf template and then the Hisecws.inf template.
C. Apply the Application.inf template first, then setup.inf template next, and then the hisecws.inf template
D. Apply the Setup.inf template and then the application.inf template

Answer: A.

Explanation: The servers currently have different security settings. Before applying our modified settings, we should reconfigure the servers with their default settings. This is what the security.inf template does. Now that our servers have the default settings, we can apply our baseline settings specified in the hisecws.inf template. Now we can apply our custom settings using the application.inf template.
Incorrect Answers:
B: The hisecws.inf template would overwrite the custom application.inf template.

C: Same as answer
A. Also, the setup.inf security template does not exist. To return a system to its default security settings, we use the security.inf template.
D: The setup.inf security template doesn't exist. To return a system to its default security settings, we use the security.inf template.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); planning, implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 13:62
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70-294): Que Publishing, Indianapolis, 2004, Chapter 8

QUESTION 3:

Your network contains Terminal servers that host legacy applications that require users to be members of the Power Users group in order to run them.
A new company policy states that the Power Users Group must be empty on all servers. You need to maintain the ability to run legacy applications on your servers when the new security requirement is enabled.
What should you do?

A. Add the domain users global group to the Remote Desktop Users built-in group in the domain
B. Add the domain users global group to the Remote Desktop Users local group on each terminal server
C. Modify the compatws.inf security template settings to allow members of the local users group to run the applications. Import the security settings into the default Domain Controllers Group Policy Object.
D. Modify the compatws.inf security template settings to allow members of the local users group to run the applications. Apply the modified template to each terminal server

Answer: D

Explanation: The default Windows 2000 security configuration gives members of the local Users group strict security settings, while members of the local Power Users group have security settings that are compatible with Windows NT 4.0 user assignments. This default configuration enables certified Windows 2000 applications to run in the standard Windows environment for Users, while still allowing applications that are not certified for Windows 2000 to run successfully under the less secure Power Users configuration. However, if Windows 2000 users are members of the Power Users group in order to run applications not certified for Windows 2000, this may be too insecure for some environments. Some organizations may find it preferable to assign users, by default, only as members of the Users group and then decrease the security privileges for the Users group to the level where applications not certified for Windows 2000 run successfully. The compatible template (compatws.inf) is designed for such organizations. By lowering the security levels on specific files, folders, and registry keys that are commonly accessed by applications, the compatible template allows most applications to run successfully under a User context. In addition, since it is assumed that the administrator applying the compatible template does not want users to be Power Users, all members of the Power Users group are removed.
Incorrect Answers:
A, B: Global group is a group that is available domain-wide in any domain functional level, so why would you

add to another group.
C: The Compatws.inf template is not intended for domain controllers, so you should not link it to a site, to the domain, or to the Domain Controllers OU
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 8:5
Dan Holme, and Orin Thomas, MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Chapter 9.

QUESTION 4:

You are the network administrator for Itexamworld .com. The network consists of a single Active Directory domain named Itexamworld .com. The functional level of the domain is Windows Server 2003. The domain contains an organizational unit (OU) named Servers that contains all of Itexamworld 's Windows Server
2003 resource servers. The domain also contains an OU named Workstations that contains all of Itexamworld 's Windows XP Professional client computers.
You configure a baseline security template for resource servers named Server.inf and a baseline security template for client computers named Workstation.inf. The Server.inf template contains hundreds of settings, including file and registry permission settings that have inheritance propagation enabled. The Workstation.inf template contains 20 security settings, none of which contain file or registry permissions settings.
The resource servers operate at near capacity during business hours.
You need to apply the baseline security templates so that the settings will be periodically enforced. You need to accomplish this task by using the minimum amount of administrative effort and while minimizing the performance impact on the resource servers.
What should you do?

A. Create a Group Policy object (GPO) and link it to the domain.
Import both the Server.inf and the Workstation.inf templates into the GPO.
B. Import both the Server.inf and the Workstation.inf templates into the Default Domain Policy Group Policy object (GPO).
C. On each resource server, create a weekly scheduled task to apply the Server.inf settings during off-peak hours by using the secedit command.
Create a Group Policy object (GPO) and link it to the Workstations OU.
Import the Workstation.inf template into the GPO.
D. On each resource server, create a weekly scheduled task to apply the Server.inf settings during off-peak hours by using the secedit command.
Import the Workstation.inf template into the Default Domain Policy Group Policy object (GPO).

Answer: C

Explanation: The question states that you need to apply the baseline security templates so that the settings will be periodically enforced. To accomplish this you must create a scheduled task so that the performance impact on resource servers is minimized. Furthermore the question also states that

Workstation.inf is a baseline security template for client computers. Therefore, the GPO has to be linked to the OU that contains the client computers, and the Workstation.inf template must be imported to the said GPO so that it can be applied.
Secedit.exe is a command line tool that performs the same functions as the Security Configuration And Analysis snap-in, and can also apply specific parts of templates to the computer. You can use Secedit.exe in scripts and batch files to automate security template deployments.
You can create a baseline security configuration in a GPO directly, or import a security template into a GPO. Link the baseline security GPO to OUs in which member servers' computer objects exist.
Incorrect Answers:
A: GPOs process security templates from the bottom up; therefore, by import both the Server.inf and the Workstation.inf templates into a single GPO, we would ensure that the settings in the security template imported last are applied in cases where there are conflicting settings. If we apply this to the domain, then all computers would have the same settings.
B, D: The Default Domain Policy Group Policy object (GPO) is applied only to the Domain Controllers group.
Reference:
Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington, Chapter 10.
Dan Holme, and Orin Thomas, MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Microsoft Press, Redmond, Washington, Chapter 9

QUESTION 5:

You are a network administrator for Itexamworld . The network consists of a single Active Directory domain named Itexamworld .com. The network contains 80 Web servers that run Windows 2000 Server. The IIS Lockdown Wizard is run on all Web servers as they are deployed.
Itexamworld is planning to upgrade its Web servers to Windows Server 2003. You move all Web servers into an organizational unit (OU) named Web Servers.
You are planning a baseline security configuration for the Web servers. The company's written security policy states that all unnecessary services must be disabled on servers. Testing shows that the server upgrade process leaves the following unnecessary services enabled:
1. SMTP
2. Telnet
Your plan for the baseline security configuration for Web servers must comply with the written security policy.
You need to ensure that unnecessary services are always disabled on the Web servers.
What should you do?

A. Create a Group Policy object (GPO) to apply a logon script that disables the unnecessary services. Link the GPO to the Web Servers OU.
B. Create a Group Policy object (GPO) and import the Hisecws.inf security template. Link the GPO to the Web Servers OU.
C. Create a Group Policy object (GPO) to set the startup type of the unnecessary services to Disabled. Link the GPO to the Web Servers OU.
D. Create a Group Policy object (GPO) to apply a startup script to stop the unnecessary services. Link the GPO to the Web Servers OU.

Answer: C

Explanation:
Windows Server 2003 installs a great many services with the operating system, and configures quite a few with the Automatic startup type, so that these services load automatically when the system starts. Many of these services are not needed in a typical member server configuration, and it is a good idea to disable the ones that the computer does not need. Services are programs that run continuously in the background, waiting for another application to call on them. Instead of controlling the services manually, using the Services console, you can configure service parameters as part of a GPO. Applying the GPO to a container object causes the services on all the computers in that container to be reconfigured. To configure service parameters in the Group Policy Object Editor console, you browse to the Computer Configuration\Windows Settings\Security Settings\System Services container and select the policies corresponding to the services you want to control. The servers have been moved to an OU. This makes it easy for us to configure the servers using a group policy. We can simply assign a group policy to the Servers OU to disable the services.
Incorrect Answers:
A: The logon script would only run when someone logs on to the web servers. It's likely that the web servers will be running with no one logged in.
B: The Hisecws.inf security template is designed for workstations, not servers.
D: The startup script would only run when the servers are restarted. A group policy would be refreshed at regular intervals.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 13: 85-86

QUESTION 6:

You are the network admin for Itexamworld . All servers run Windows Server 2003.
Every week, you run the mbsacli.exe /hf command to ensure that all servers have the latest critical updates installed. You run the mbsaclie.exe /hf command from a server named server1.
When you scan a server named Itexamworld B you receive the following error message stating Error 200, System not found, Scan failed.
When you ping Itexamworld B you receive a reply.
You need to ensure that you can scan Itexamworld B by using the mbsacli.exe /hf. What should you do?

A. Copy the latest version of the Mssecure.xml to the program files\microsoft baseline security analyzer folder on server1
B. Ensure that the Server service is running on Itexamworld B
C. Install IIS common files on Server1
D. Install the latest version of IE on Itexamworld B

Answer: B

Explanation: From Microsoft: Error: 200 - System not found. Scan not performed. This error message indicates that mbsacli /hf did not locate the specified computer and did not scan it. To resolve this error, verify that this computer is on the network and that the host name and IP address are correct. We know that the computer is on the network because we can successfully ping it. Therefore, the cause of the problem must be that the Server service isn't running.
Incorrect Answers:
A: We can successfully scan other computers from Server1. Therefore, the problem is unlikely to be with Server1.
C: We can successfully scan other computers from Server1. Therefore, the problem is unlikely to be with Server1.
D: The version of IE that comes with Windows Server 2003 is sufficient, and therefore does not need to be upgraded.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q303/2/15.asp&NoW
Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 13:5

QUESTION 7:

You are the network administrator for Itexamworld . The network consists of a single Active Directory domain named Itexamworld .com. The network contains 10 application servers that run Windows Server
2003.
The application servers are accessed from the Itexamworld network and from the Internet. The network design requires that the application servers must have specifically configured security settings, including the password policy, audit policies, and security options settings. You create a security template named App.inf that contains the security settings required by the network design.
You are concerned that an unauthorized user will modify the configuration and gain access to the application servers. You want to capture any changes made to the security settings of the application servers.
You need to generate a report that compares the current settings of each application server with the required settings every 24 hours.
What should you do?

A. Use a Group Policy startup script to run the secedit command in analysis mode with the App.inf template, and set the Group Policy refresh interval for computers to 24 hours.
B. Import the App.inf template into Group Policy, and set the Group Policy refresh interval for computers to 24 hours.
C. Use Task Scheduler to run the gpresult command in verbose mode every 24 hours.
D. Use a custom script in Task Scheduler to run the secedit command in analysis mode with the App.inf template every 24 hours.

Answer: D

Explanation: Secedit.exe is a command line version of the Security Configuration and Analysis tool. In

'analysis' mode, this tool can be used to compare the current system settings with the required settings.
We can use the Task Scheduler to run a script that runs secedit.exe to analyse the current settings.
Incorrect Answers:
A: A Group Policy startup script will only run when the computer starts up. It does not run every time the group policy is refreshed.
B: This will reapply the required settings every 24 hours, but the question states that you want to capture any changes by comparing the current settings to the required settings.
C: The gpresult utility is a command line version of the RSoP utility. In verbose mode, it will list the effective policies on a computer. However, it won't list the differences between the current settings and the required settings.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 10:44

QUESTION 8:

You are the network administrator for Itexamworld 's Active Directory domain. Itexamworld 's written security policy was updated and now requires a minimum of NTLM v2 for LAN manager authentication.
You need to identify which Operating Systems on your network do not meet the new requirement
Which OS would require an upgrade to the OS or software to meet the requirement?

A. Windows 2000 Professional
B. Windows Server 2003
C. Windows XP Professional
D. Windows NT Workstation with service pack 5
E. Windows 95

Answer: E.

Explanation: Windows 95 does not natively support NTLM v2 authentication. To enable it, you would need to install the Directory Services Client software.
Incorrect Answers:
A, B, C, D: Windows 2000 Professional, Server 2003, XP Professional, and NT Workstation with service pack 5 natively supports NTLM v2 authentication.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 1:24-26

QUESTION 9:

You are a consultant for several different companies. You design the security policies for the computers running Windows 2003 Server and Windows 2000 Professional in your customers' networks.
You use these security policies to configure a server named Server1. You want to deploy the security configuration on Server1 to computers in your customer's networks by using the least amount of administrative effort.
What should you do first?

A. Create a Group Policy Object (GPO) that configures the security settings for all computers to match the settings on Server1, and then link the GPO to the domain.
Export the console list to a file.
B. In the Security Configuration and Analysis snap-in, analyze Server1 and export the security template in a file.
C. In the System Information snap-in, save the system summary as a system information file.
D. In the Security Templates snap-in, export the console list to a file.

Answer: B

Explanation: We can use the Security Configuration and Analysis snap-in to export all the security settings from a computer to a template file. This will enable us to apply the same security settings to other computers. We can apply the template to other computers either by using the Security Configuration and Analysis snap-in (for single computers) or by importing the template into a group policy object (for multiple computers).
Incorrect Answers:
A: You have already manually configured the settings on Server1. It would be quicker to export them to a template file, rather than manually enter the settings into a GPO.
C: The system summary does not contain the security settings.
D: The console list does not contain the security settings.
Reference:
Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 13-57 to 13-65, 13-70-13-80
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 13-57 to 13-65, 13-70-13-80

security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings. Additionally, the Secure templates limit the use of LANManager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LANManager responses. In order to apply Securews.inf to a member computer, all of the domain controllers that contain the accounts of all users that log on to the client must run WindowsNT4.0 Service Pack4 or higher.
The system key utility (SYSKEY) is a security measure used to restrict logon names to user accounts and access to computer systems and resources.
By running the syskey utility with the Password startup option, the account information in the directory services is encrypted and a password needs to be entered during system start. The start of the Domain Controllers is therefore restricted to everybody with this password.
Incorrect Answers:
A: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
B: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
D: We need to apply the policy to the domain controllers container, not the entire domain.
F: The System Key Utility (syskey) is used to encrypt the account password information that is stored in the SAM database or in the directory services. By selecting "Store Key locally" the computer stores an encrypted version of the key on the local computer. This doesn't help in controlling the start of the Domain Controllers.
Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); planning, implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 1:24-26
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam
Cram 2 (Exam 70-294): Que Publishing, Indianapolis, 2004, Chapter 8

QUESTION 10:

You are a network administrator for Itexamworld . The network consists of a single Active Directory forest. All domain controllers run Windows Server 2003.
The bank decides to provide access to its mortgage application services from a real estate agency that has offices throughout the country. You install a Itexamworld domain controller in each real estate agency office. You need to further protect the domain controllers' user account databases from unauthorized access.
You want to achieve this goal by using the minimum amount of administrative effort.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Use the system key utility (syskey) with the most secure security level on the domain controllers.
B. Create a Group Policy object (GPO), import the Securedc.inf security template, and apply the GPO to the

domain controllers.
C. Create a Group Policy object (GPO), configure the Network security: LAN Manager authentication level security option to the Send NTLMv2 response only\refuse LM setting, and apply the GPO to the domain controllers.
D. Create a Group Policy object (GPO), import the DC security.inf security template, and apply the GPO to the domain controllers.

Answer: A, B

Explanation: On domain controllers, password information is stored in directory services. It is not unusual for password - cracking software to target the Security Accounts Manager (SAM) database or directory services to access passwords for user accounts. The System Key utility (Syskey) provides an extra line of defence against offline password - cracking software. Syskey uses strong encryption techniques to secure account password information that is stored in directory services. Mode 3 is the most secure Syskey utility, because it uses a computer-generated random key and stores the key on a floppy disk. This disk is required for the system to start, and it must be inserted at a prompt during the startup sequence. The system key is not stored anywhere on the computer.
Secure (Secure*.inf) Template define enhanced security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings. Additionally, the Secure templates limit the use of LANManager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LANManager responses.
Incorrect Answers:
C: You should be importing the Securedc.inf security template instead of configuring the Network security: LAN
Manager authentication level security option to the Send NTLMv2 response only\refuse LM setting.
D: DC Security.inf templates contain a large number of settings, and in particular a long list of file-system permission assignments. For this reason, you should not apply these templates to a computer by using group policies.
Reference:
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70-294): Que Publishing, Indianapolis, 2004, Chapter 8

QUESTION 11:

You are the network administrator for Itexamworld . The network consists of a single Active Directory domain Itexamworld .com. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional.
Itexamworld has legacy applications that run on UNIX servers. The legacy applications use the LDAP protocol to query Active Directory for employee information.
The domain controllers are currently configured with the default security settings. You need to configure enhanced security for the domain controllers. In particular, you want to configure stronger password settings, audit settings, and lockout settings. You want to minimize interference with the proper functioning of the legacy applications.
You decide to use the predefined security templates. You need to choose the appropriate predefined security template to apply to the domain controllers.
What should you do?

A. Apply the Setup security.inf template to the domain controllers.
B. Apply the DC security.inf template to the domain controllers.
C. Apply the Securedc.inf template to the domain controllers.
D. Apply the Rootsec.inf template to the domain controllers.

Answer: C

Explanation: Securedc.inf contains policy settings that increase the security on a domain controller to a level that remains compatible with most functions and applications. The template includes more stringent account policies, enhanced auditing policies and security options, and increased restrictions for anonymous users and LanManager systems.
Incorrect Answers:
A: This template allows you to reapply the default security settings.
B: The DC security.inf template is available to undo security template policy settings.
D: Rootsec.inf contains only the default file system permissions for the system drive on a computer running Windows Server 2003. You can use this template to restore the default permissions to a system drive that you have changed, or to apply the system drive permissions to the computer's other drives.
Reference:
Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington 98052-6399, Chapter 10.
Dan Holme, and Orin Thomas, MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Chapter 9

QUESTION 12:

You are the administrator of the Itexamworld company network. The network consists of a single active directory domain named Itexamworld .com. The network includes 20 servers running Windows Server 2003 and 200 client computers running Windows XP Professional.
The company purchases 10 new servers to function as file servers for the domain.
You install Windows Server 2003 on the new servers. The computer accounts for the file servers are located on an OU named File Servers. A security expert configures one of the servers named CKFile1 with various security settings. You need to apply and maintain the same security settings on the remaining 9 servers. You need to do this by using the minimum amount of administrative effort.
What should you do? (Choose two)

A. Use disk imaging software to take an image of CKFile1. Apply the disk image to the remaining 9 servers.
B. Use gpedit.msc to create a new Group Policy object (GPO). Manually configure the GPO with the same security settings as CKFile1. Link the GPO to the File Servers OU.
C. Use gpedit.msc to create a new Group Policy object (GPO). Import the security template into the Security Settings of the Computer Configuration section of the GPO. Link the GPO to the File Servers OU.
D. On the PDC Emulator, use Security Configuration and Analysis to export the security settings to a security template.
E. On CKFile1, use Security Configuration and Analysis to export the security settings to a security template.

Answer: C, E

Explanation:
The easiest way to configure multiple computers with multiple security settings is to use a GPO. In this question, we have a computer configured with the required settings. We can use the Security Configuration and Analysis to export the security settings to a security template. We can then import the template into a Group Policy Object and apply the settings to the File Servers OU.
Incorrect Answers:
A: This could work (if we changed the computer names and SIDS), but there is a catch in the question. The question states that you need to apply and maintain the security settings contained in the security template to the new file servers. Using a GPO, the settings will be periodically refreshed, ensuring that the security settings are maintained.
B: This is a long way of doing it and definitely not the least amount of administrative effort that will also accomplish the task. Exporting the settings to a security template would be easier and less effort.
D: This would have no effect on the file servers.
Reference:
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70-294): Que Publishing, Indianapolis, 2004, Chapter 8

QUESTION 13:

You are the administrator of the Itexamworld company network. The network consists of a single Active Directory domain Itexamworld .com. The network includes 30 servers running Windows Server 2003 and 2000 client computers running Windows XP Professional.
20 member servers are located in an organisational unit (OU) named Servers. 10 domain controllers are in the default Domain Controllers container. All 2000 client computers are located in an organisational unit (OU) named Clients.
The member servers are configured with the following security settings:
1. Logon events must be audited.
2. System events must be audited.
3. Passwords for local user accounts must meet complexity requirements.
4. Passwords must be changed every 30 days.
5. Password history must be enforced.
6. Connections to the servers must be encrypted.
The written security policy states that you need to be able to verify the custom security settings during audits. You need to deploy and refresh the custom security settings on a routine basis.
What should you do?

A. Create a custom security template and apply it by using a Group Policy linked to the Servers OU.
B. Create a custom security template and apply it by using a Group Policy linked to the domain.
C. Create and apply a custom Administrative Template.
D. Create a custom application server image and deploy it by using RIS.

Answer: A

Explanation: The easiest way to deploy multiple security settings to a group of Windows 2003 computer

is to create a security template with all the required settings and import the settings into a GPO. In this case, the security settings apply to local accounts on the servers. This means that we can apply the settings with a GPO assigned to an Organisation Unit containing the servers.
Incorrect Answers:
B: The security settings need to apply to the member servers only. Applying the GPO to the domain would affect all computers in the domain.
C: We need a security template, not an administrative template.
D: We cannot use imaging in this way.
Reference:
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70-294): Que Publishing, Indianapolis, 2004, Chapter 8

QUESTION 14:

Itexamworld has a single active directory domain named Itexamworld .com.
The company's written security policy requires that computers in a file server role must have a minimum file size for event log settings. In the past, logged events were lost because the size of the event log files was too small. You want to ensure that the event log files are large enough to hold history. You also want the security event log to be cleared manually to ensure that no security information is lost. The application log must clear events as needed.
You create a security template named fileserver.inf to meet the requirements. You need to test each file server and take the appropriate corrective action if needed. You audit a file server by using fileserver.inf and receive the results shown in the exhibit.
MISSING
You want to make only the changes that are required to meet the requirements. Which two actions should you take?

A. Correct the maximum application log size setting on the file server
B. Correct the maximum security log size setting on the file server
C. Correct the maximum system log size setting on the file server
D. Correct the retention method for application log setting on the file server
E. Correct the retention method for the security log setting on the file server
F. Correct the retention method for the system log setting for the file server

Answer: B, E.

Explanation: The Event Log security area defines attributes related to the application, security, and system logs in the Event Viewer console for computers in a site, domain, or OU. The attributes are: maximum log size, access rights for each log, and retention settings and methods. Event log size and log wrapping should be defined to match your business and security requirements. In this particular case you should be correcting the maximum security log size setting and the retention method for the security log setting on the file server so as to comply with the stated requirements.
Incorrect answers:
A, C, D, F: The question states that the company's written security policy requires that computers in a file server role must have a minimum file size for event log settings. And given the past experiences of the company regarding the size of security events and its retention, you should be correct the maximum log size and retention

methods of the security logs and not the application log or the system log.
Reference:
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70-294): Que Publishing, Indianapolis, 2004, Chapter 10
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 13:6

QUESTION 15:

You are the network administrator for Itexamworld . The network consists of a single Active Directory domain named Itexamworld .com. Itexamworld 's perimeter
network contains 50 Web servers that host the company's public Internet site. The Web servers are not members of the domain.
The network design team completed a new design specification for the security of servers in specific roles. The network design requires that security settings must be applied to Web servers. These settings include password restrictions, audit settings, and automatic update settings.
You need to comply with the design requirements for securing the Web servers. You also want to be able to verify the security settings and generate a report during routine maintenance. You want to achieve these goals by using the minimum amount of administrative effort.
What should you do?

A. Create a custom security template named Web.inf that contains the required security settings.
Create a new organizational unit (OU) named WebServers and move the Web servers into the new OU.
Apply Web.inf to the WebServers OU.
B. Create a custom security template named Web.inf that contains the required security settings, and deploy Web.inf to each Web server by using Security Configuration and Analysis.
C. Create an image of a Web server that has the required security settings, and replicate the image to each Web server.
D. Manually configure the required security settings on each Web server.

Answer: B

Explanation: The easiest way to deploy multiple security settings to a Windows 2003 computer is to create a security template with all the required settings and import the settings using the Security Configuration and Analysis tool.
Incorrect Answers:
A: The web servers are not domain members. Therefore they cannot be moved to an OU in Active Directory.
C: We cannot use imaging in this way.
D: This is a long way of doing it. A security template would simplify the task

considerably.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); planning, implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 13:57

QUESTION 16:

You are the network administrator for Itexamworld . The network consists of a single Active Directory domain named Itexamworld .com.
The company plans to deploy 120 Windows Server 2003 member servers as file servers in the domain.
The new file servers will be located in a single organizational unit (OU) named File Servers.
The security department provides you with a security template that must be applied to the new file servers.
You need to apply and maintain the security settings contained in the security template to the new file servers. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. On a reference computer, use the Local Security Settings console to import the security template.
Use imaging technology to install and configure the new file servers based on the configuration of the reference computer.
B. On a reference computer, run the secedit command to apply the security template.
Make use of imaging technology to install and configure the new file serves based on the configuration of the reference computer.
C. Create a new Group Policy object (GPO).
Import the security template into the Security Settings of the Computer Configuration section of the GPO.
Link the GPO to the File Servers OU.
D. On the PDC emulator master in the domain, run the secedit command to apply the security template.

Answer: C

Explanation: We have a security template with the required security settings. We can simply import the template into a Group Policy Object and apply the settings to the File Servers OU.
Incorrect Answers:
A: This would work, but there is a catch in the question. The question states that you need to apply and maintain the security settings contained in the security template to the new file servers. Using a GPO, the settings will be periodically refreshed, ensuring that the security settings 'maintained'.
B: This would work, but there is a catch in the question. The question states that you need to apply and maintain the security settings contained in the security template to the new file servers. Using a GPO, the settings will be periodically refreshed, ensuring that the security settings 'maintained'.
D: This would have no effect on the file servers.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 13:73

QUESTION 17:

You are the network administrator for Itexamworld . Itexamworld is deploying a public Web server farm on Windows Server 2003 computers. This Web server farm will allow the public to view company information. The Web servers in the Web server farm will be placed in Itexamworld 's perimeter network, which uses a public
Internet address space.
Itexamworld wants to reduce the probability of external unauthorized users breaking into the public Web servers.
You need to make the Web servers less vulnerable to attack. You also want to ensure that the public will be able to view information that is placed in Itexamworld 's perimeter network.
What should you do?

A. Configure each Web server's IP address to a private reserved Internet address.
B. Configure the Web servers to allow only IPSec communications.
C. Disable any unneeded services on the Web servers.
D. Disable TCP/IP filtering on all adapters in the Web servers.

Answer: C

Explanation: We should disable any unneeded services on the Web servers. This includes unneeded web services and unneeded server services. This will also ensure that no unnecessary ports are open on the servers.
Reducing the Attack Surface of the Web Server - Immediately after installing Windows Server2003 and IIS6.0 with the default settings, the Web server is configured to serve only static content. If your Web sites consist of static content and you do not need any of the other IIS components, then the default configuration of IIS minimizes the attack surface of the server. When your Web sites and applications contain dynamic content, or you require one or more of the additional IIS components, you will need to enable additional features. However, you still want to ensure that you minimize the attack surface of the Web server. The attack surface of the Web server is the extent to which the server is exposed to a potential attacker.
However, if you reduce the attack surface of the Web server too much, you can eliminate functionality that is required by the Web sites and applications that the server hosts. You need to ensure that only the functionality that is necessary to support your Web sites and applications is enabled on the server. This ensures that the Web sites and applications will run properly on your Web server, but that the attack surface is minimized.
Incorrect Answers:
A: The public web servers need public IP addresses.
B: You can not use IPSec on public web servers. No one would be able to access the web pages.
D: TCP/IP filtering should be enabled, not disabled.
Reference
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70-294): Que Publishing, Indianapolis, 2004, Chapter 1

MS Windows Server 2003 Deployment Kit
Deploying Internet Information Services (IIS) 6.0
Reducing the Attack Surface of the Web Server
B: Create custom security templates based on server roles.

QUESTION 18:

You are the network administrator for Itexamworld . The network consists of a single Active Directory domain named Itexamworld .com. The network contains 10 domain controllers and 50 servers in application server roles. All servers run Windows Server 2003.
The application servers are configured with custom security settings that are specific to their roles as application servers. Application servers are required to audit account logon events, object access events, and system events. Application servers are required to have passwords that meet complexity requirements, to enforce password history, and to enforce password aging. Application servers must also be protected against man-in-the-middle attacks during authentication.
You need to deploy and refresh the custom security settings on a routine basis. You also need to be able to verify the custom security settings during audits.
What should you do?

A. Create a custom security template and apply it by using Group Policy.
B. Create a custom IPSec policy and assign it by using Group Policy.
C. Create and apply a custom Administrative Template.
D. Create a custom application server image and deploy it by using RIS.

Answer: A

Explanation: The easiest way to deploy multiple security settings to a Windows 2003 computer is to create a security template with all the required settings and import the settings into a group policy. We can also use secedit to analyze the current security settings to verify that the required security settings are in place.
Incorrect Answers:
B: An IPSec policy will not configure the required auditing policy.
C: We need a security template, not an administrative template.
D: This will create multiple identical machines. We cannot use RIS images in this scenario.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-paced Trainning Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 13:57

QUESTION 19:

Itexamworld is a network administrator for Itexamworld . The network consists of a single Active Directory domain Itexamworld .com. The network contains 12 domain controllers and 50 servers in the application server roles. All servers run Windows Server 2003.
The application servers are configured with custom security settings that are specific to their roles as application servers. Applications servers are required to audit account logon events, object access events,

and system events. Application servers required to have passwords that meet complexity requirements, to enforce password history, and to enforce password aging. Application servers must also be protected against man-in-the-middle attacks during authentication.
Jack needs to deploy and refresh the custom security settings on a routine basis. She also needs to be able to verify the customer security settings during audits.
What actions should Itexamworld take?

A. She should create a custom security template and apply it by using Group Policy.
B. She should create a customer IPSec policy and assign it by using Group Policy.
C. She should create and apply a custom Administrative Template.
D. She should create a custom application server image and deploy it by using RIS.

Answer: A

Explanation: A security template is a physical file representation of a security configuration that can be applied to a local computer or imported to a Group Policy Object (GPO) in Active Directory. When you import a security template to a GPO, Group Policy processes the template and makes the corresponding changes to the members of that GPO, which can be users or computers.
A Group Policy Object (GPO) is a collection of configuration parameters that you can use to create a secure baseline installation for a computer running Windows Server 2003. To deploy a GPO, you associate it with an Active Directory container, and all the objects in the container inherit the GPO configuration settings. Audit and Event Log policies enable you to specify what information a computer logs, how much information the computer retains in logs, and how the computer behaves when logs are full. Windows Server 2003 loads many services by default that a member server usually doesn't need. You can use a GPO to specify the startup type for each service on a computer. GPOs include a great many security options that you can use to configure specific behaviours of a computer running Windows Server 2003.
Incorrect Answers:
B: IPSec is required to secure network traffic, not application servers.
C: Administrative templates are used to provide settings required to allow for the performance of administrative tasks. Security templates are used to provide security settings, such as minimum password lengths.
D: Custom application server images deployed through RIS are used to install automate the installation of operating systems with applications pre-installed. It is not used to apply security settings.
Reference:
J. C. Mackin, and Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft Press, Redmond, Washington, Glossary.
Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2003, Chapter 9.

QUESTION 20:

You are the network administrator for Itexamworld . The network consists of a single Active Directory domain Itexamworld .com. Itexamworld has an internal network and a perimeter network. The internal network is protected by a firewall. Application servers on the perimeter network are accessible from the Internet. You are deploying 10 Windows Server 2003 computers in application server roles. The servers will be located in the perimeter network and will not be members of the domain. The servers will host only

publicly available Web pages.
The network design requires that custom security settings must be applied to the application servers.
These custom security settings must be automatically refreshed every day to ensure compliance with the design.
You create a custom security template named Baseline1.inf for the application servers. You need to comply with the design requirements.
What should you do?

A. Import Baseline1.inf into the Default Domain Policy Group Policy object (GPO).
B. Create a task on each application server that runs Security and Configuration Analysis with Baseline1.inf every day.
C. Create a task on each application server that runs the secedit command with Baseline1.inf every day.
D. Create a startup script in the Default Domain Policy Group Policy object (GPO) that runs the secedit command with Baseline1.inf.

Answer: C

Explanation: Secedit.exe is a command line tool that performs the same functions as the Security Configuration And Analysis snap-in, and can also apply specific parts of templates to the computer. You can use Secedit.exe in scripts and batch files to automate security template deployments.
Incorrect Answers:
A, D: The Default Domain Policy Group Policy object (GPO) is applied to the domain controllers. We need to configure the application servers, not the domain controllers.
B: Security and Configuration Analysis analyzes the security settings. It doesn't apply it.
Reference:
Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2003, Chapter 10.