

# The best learning assistants

**Exam** : **Microsoft 70-293**  
**Title** : Planning and Maintaining a  
Microsoft Windows Server  
2003 Network Infrastructure  
**Update** : Demo



1. You are the network administrator for your company. The network consists of a single Active Directory domain. The 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 settings for each of the application servers differently based on their knowledge and skills. 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 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 modified 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, the Setup security.inf template next, and then the Hisecws.inf template.
- D. Apply the Setup security.inf template and then the Application.inf template.

Answer: A

2. You are a network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. The Active Directory domain contains three organizational units (OUs): Payroll Users, Payroll Servers, and Finance Servers. The Windows XP Professional computers used by the users in the payroll department are in the Payroll Users OU. The Windows Server 2003 computers used by the payroll department are in the Payroll Servers OU. The Windows Server 2003 computers used by the finance department are in the Finance Servers OU. You are planning the baseline security configuration for the payroll department. The company's written security policy requires that all network communications with servers in the Payroll Servers OU must be secured by using IPsec. The written security policy states that IPsec must not be used on any other servers in the company. You need to ensure that the baseline security configuration for the payroll department complies with the written security policy. You also need to ensure that members of the Payroll Users OU can access resources in the Payroll Servers OU and in the Finance Servers OU. What should you do?

- A. Create a Group Policy object (GPO) and assign the Secure Server (Require Security) IPsec policy setting. Link the GPO to only the Payroll Servers OU. Create a second GPO and assign the Client (Respond Only) IPsec policy setting. Link the second GPO to the Payroll Users OU.
- B. Create a Group Policy object (GPO) and assign the Secure Server (Require Security) IPsec policy setting. Link the GPO to the Payroll Servers OU and to the Finance Servers OU. Create a second GPO and assign the Client (Respond Only) IPsec policy setting. Link the second GPO to the Payroll Users OU.
- C. Create a Group Policy object (GPO) and assign the Server (Request Security) IPsec policy setting. Link the GPO to only the Payroll Servers OU. Create a second GPO and assign the Client (Respond Only)

IPSec policy setting. Link the second GPO to the Payroll Users OU.

D. Create a Group Policy object (GPO) and assign the Server (Request Security) IPSec policy setting. Link the GPO to the Payroll Servers OU and to the Finance Servers OU. Create a second GPO and assign the Client (Respond Only) IPSec policy setting. Link the second GPO to the Payroll Users OU.

Answer: A

3. You are a network administrator for your company. The network consists of a single Active Directory domain. 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. Your company 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 service enabled: .SMTP .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

4. You are the network administrator for your company. The network consists of a single Active Directory domain. The functional level of the domain is Windows Server 2003. The domain contains an organizational unit (OU) named Servers that contains all of the company's Windows Server 2003 resource servers. The domain also contains an OU named Workstations that contains all of the company'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 secdit 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 secdit command. Import the Workstation.inf template into the Default Domain Policy Group Policy object (GPO).

Answer: C

5. You are the network administrator for your company. The network consists of a single Active Directory domain. 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. (Click the Exhibit button.) You want to make only the changes that are required to meet the requirements. Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)

Policy	Database Setting	Computer Setting
Maximum application log size	16384 kilobytes	30016 kilobytes
Maximum security log size	29952 kilobytes	16384 kilobytes
Maximum system log size	16384 kilobytes	16384 kilobytes
Prevent local guests group from a...	Enabled	Enabled
Prevent local guests group from a...	Enabled	Enabled
Prevent local guests group from a...	Enabled	Enabled
Retention method for application log	As needed	As needed
Retention method for security log	Manually	As needed
Retention method for system log	Not Defined	As needed

- 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 security log setting on the file server.
- F. Correct the Retention method for system log setting for the file server.

Answer: B AND E

6. You are the network administrator for your company. The network consists of a single Active Directory domain. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional. The company 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

7. You are the network administrator for your company. The network consists of a single Active Directory domain. 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. The company'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 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 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

8. You are the network administrator for your company. The network consists of a single Active Directory domain. 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

9. You are the network administrator for your company. All servers run Windows Server 2003. You configure a baseline security template named Baseline.inf. Several operations groups are responsible for creating templates containing settings that satisfy operational requirements. You receive the templates shown in the following table.

Operations group	Template name	Applies to
File and Print	File.inf	File servers
Database	Db.inf	Database servers
Security	Sec.inf	All resource servers

The operations groups agree that in the case of conflicting settings, the priority order listed in the following table establishes the resultant setting.

Template	Priority
Sec.inf	1
Baseline.inf 2	2
Specific server role template	3

You need to create one or more Group Policy objects (GPOs) to implement the security settings. You want to minimize the amount of administrative effort required when changes are requested by the various operations groups. What should you do?

- A. Create a GPO and import the following templates in the following order: Baseline.inf, Sec.inf. Create a GPO for each server role and import only the specific template for that role into each respective GPO.
- B. Create a GPO and import the following templates in the following order: Sec.inf, Baseline.inf. Create a GPO for each server role and import only the specific template for that role into each respective GPO.
- C. Create a GPO for each server role and import the following templates in the following order: Baseline.inf, specific server role template, Sec.inf.
- D. Create a GPO and import the following templates in the following order: Sec.inf, Db.inf, File.inf, Baseline.inf.

Answer: A

10. You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. The network contains servers that have Terminal Server enabled. The terminal servers host legacy applications that currently require users to be members of the Power Users group. A new requirement in the company's written security policy states that the Power Users group must be empty on all resource servers. You need to maintain the ability to run the legacy applications on the terminal servers when the new security requirement is implemented. 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 template into the Default Domain Controllers Policy Group Policy object (GPO).

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

11. You are the network administrator for your company. The network consists of a single Active Directory domain. The company 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 secdit command with Baseline1.inf every day.

D. Create a startup script in the Default Domain Policy Group Policy object (GPO) that runs the secdit command with Baseline1.inf.

Answer: C

12. You are a network administrator for your company. All domain controllers run Windows Server 2003. The network contains 50 Windows 98 client computers, 300 Windows 2000 Professional computers, and 150 Windows XP Professional computers. According to the network design specification, the Kerberos version 5 authentication protocol must be used for all client computers on the internal network. You need to ensure that Kerberos version 5 authentication is used for all client computers on the internal network. What should you do?

A. On each domain controller, disable Server Message Block (SMB) signing and encryption of the secure channel traffic.

B. Replace all Windows 98 computers with new Windows XP Professional computers.

C. Install the Active Directory Client Extensions software on the Windows 98 computers.

D. Upgrade all Windows 98 computers to Windows NT Workstation 4.0.

Answer: B

13. You are a network administrator for your company. The network consists of an intranet and a perimeter network, as shown in the work area. The perimeter network contains:

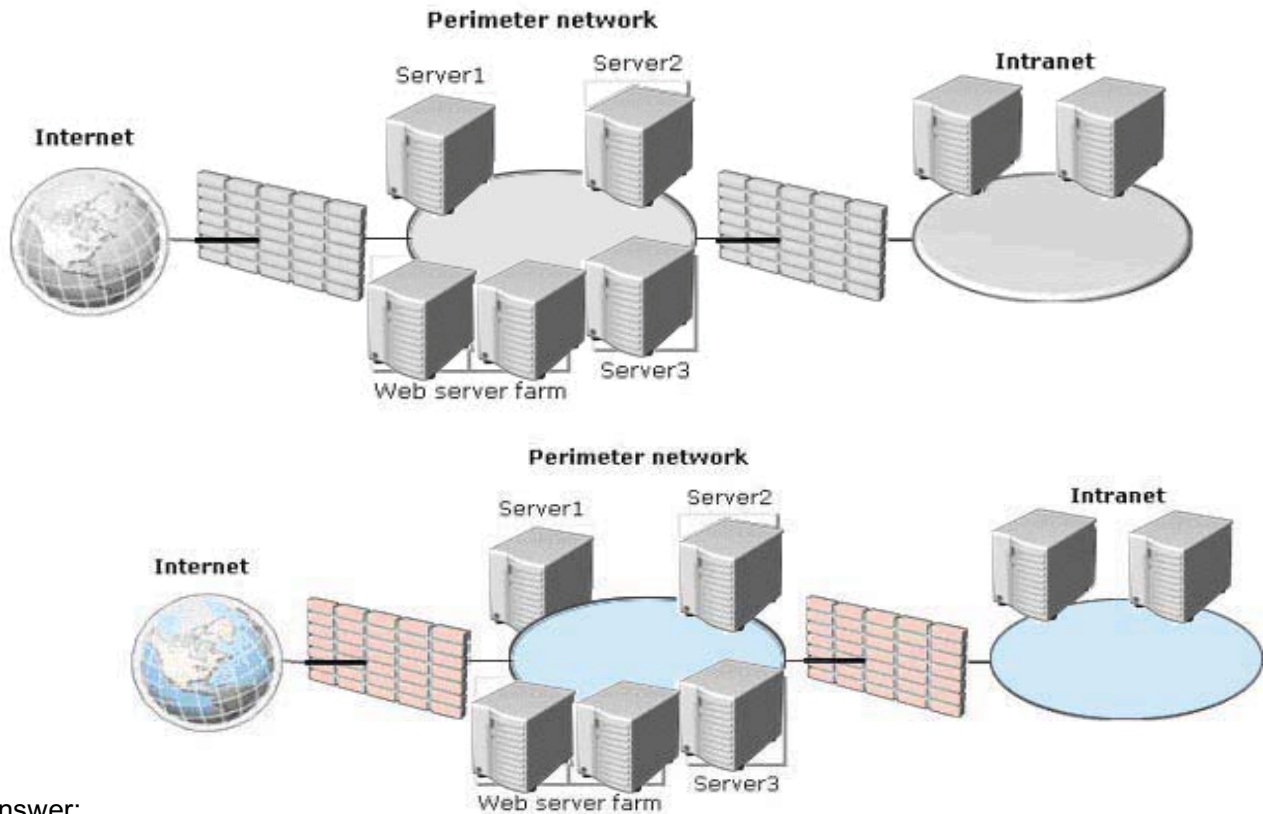
.One Windows Server 2003, Web Edition computer named Server1.

.One Windows Server 2003, Standard Edition computer named Server2.

.One Windows Server 2003, Enterprise Edition computer named Server3.

One Web server farm that consists of two Windows Server 2003, Web Edition computers. All servers on the perimeter network are members of the same workgroup. The design team plans to create a new

Active Directory domain that uses the existing servers on the perimeter network. The new domain will support Web applications on the perimeter network. The design team states that the perimeter network domain must be fault tolerant. You need to select which server or servers on the perimeter network need to be configured as domain controllers. Which server or servers should you promote? To answer, select the appropriate server or servers in the work area.



Answer:

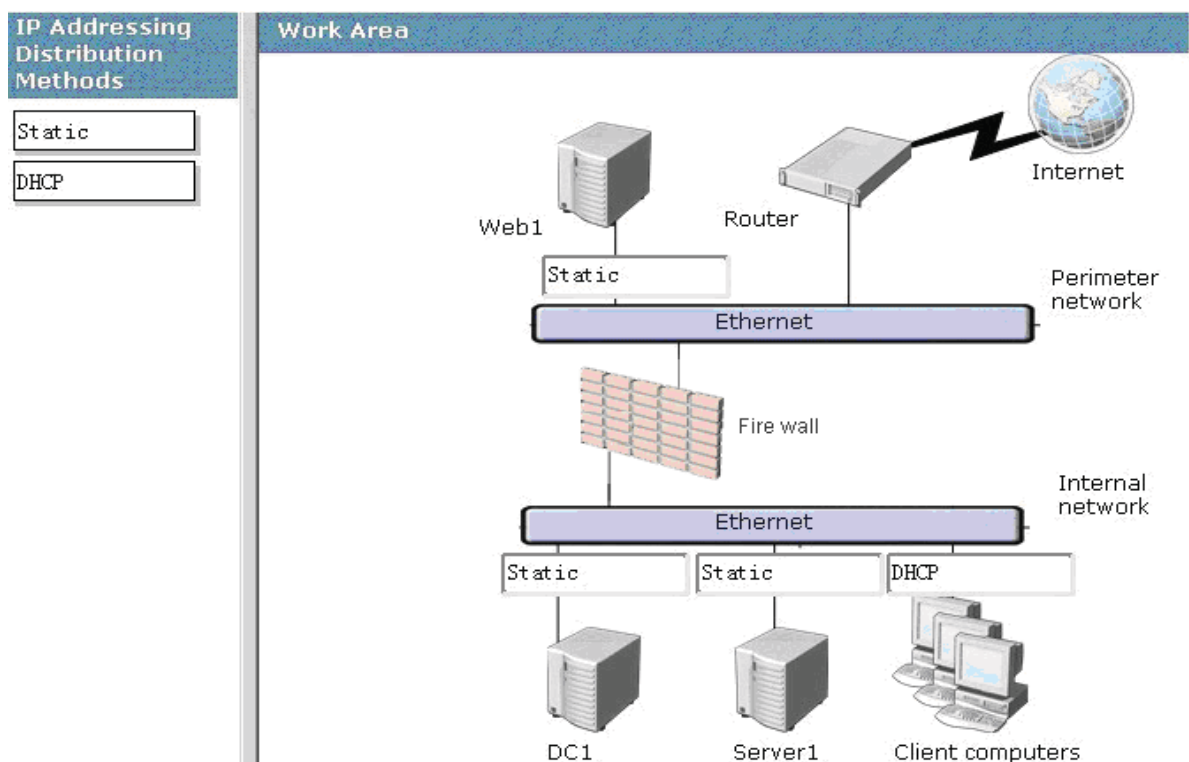
14. You are a network administrator for your company. You need to test a new application. The application requires two processors and 2 GB of RAM. The application also requires shared folders on the application server and requires the installation of software on the client computers. You create the test plan. You assemble a server in the test lab. You install Windows Server2003, Web Edition on the server. You install the application on the server. You install the client software components for the application on 20 client computers in the test lab. You test the application. You discover that only some of the client computers can run the application. You turn off the client computers that ran the application successfully, and you test again. The client computers that failed in the first test now run the application successfully. You need to identify the cause of the failure and update your test plan. What should you do?

- A. Increase the Maximum number of worker processes to 20 for the default application pool.
- B. Use Add or Remove Programs to add the Application Server Windows component.
- C. Change the Application pool identity to Local Service for the default application pool.
- D. Change the test server operating system to Windows Server 2003, Standard Edition or Windows Server 2003,Enterprise Edition.

Answer: D

15. You are the network administrator for your company. The company has an internal network and a

perimeter network, as shown in the work area. The internal network consists of a single Active Directory domain. The internal network contains a Windows Server 2003 domain controller named DC1, which runs the DNS Server service. The internal network also contains a Windows Server 2003 file server named Server1, which runs the DHCP Server service. The network contains 500 Windows XP Professional computers. The perimeter network contains a public Web server named Web1. The internal network is connected to the perimeter network by a firewall. The perimeter network is connected to the Internet. You need to plan an IP address strategy. The IP address strategy must provide TCP/IP connectivity from the internal network to Web1. The company wants to reduce administrative overhead by automatically assigning IP addresses whenever possible. You need to choose the appropriate IP addressing distribution method for the computers on the networks. What should you do? To answer, drag the appropriate IP addressing distribution method or methods to the correct computer or computers in the work area.



Answer:

16. You are the network administrator for Woodgrove Bank. The company has 20,000 users in 20 physical locations worldwide. The company is expecting to grow by 50 percent in the next five years. The company recently became a subsidiary of Humongous Insurance. Humongous Insurance has five other subsidiaries. Humongous Insurance has 100,000 users in 100 physical locations worldwide. Humongous Insurance uses the 10.0.0.0/8 network and requires that all subsidiaries integrate into this network. The network design team at Woodgrove Bank provides you with a network design for integrating into the Humongous Insurance network. The design specifies that Woodgrove Bank will use a single block of IP network numbers to assign IP addresses to its network. You need to plan the IP address space to meet the design specification. You need to request a block of IP addresses from Humongous Insurance that will accommodate all Woodgrove Bank users. To reduce the difficulty of obtaining the addresses and to conserve the Humongous Insurance address space, you want to request the smallest block of IP addresses that meets the design specification. What should you do?

- A. Request a 10.0.0.0 block of IP addresses with an 8-bit subnet mask from Humongous Insurance.
- B. Request a 10.0.0.0 block of IP addresses with a 16-bit subnet mask from Humongous Insurance.
- C. Request a 10.0.0.0 block of IP addresses with a 24-bit subnet mask from Humongous Insurance.
- D. Request a 10.0.0.0 block of IP addresses with a 32-bit subnet mask from Humongous Insurance.

Answer: B

17. You are the network administrator for Tailspin Toys. The company has a main office and two branch offices. The network in the main office contains 10 servers and 100 client computers. Each branch office contains 5 servers and 50 client computers. Each branch office is connected to the main office by a direct T1 line. The network design requires that company IP addresses must be assigned from a single classful private IP address range. The network is assigned a class C private IP address range to allocate IP addresses for servers and client computers. Tailspin Toys acquires a company named Wingtip Toys. The acquisition will increase the number of servers to 20 and the number of client computers to 200 in the main office. The acquisition is expected to increase the number of servers to 20 and the number of client computers to 200 in the branch offices. The acquisition will also add 10 more branch offices. After the acquisition, all branch offices will be the same size. Each branch office will be connected to the main office by a direct T1 line. The new company will follow the Tailspin Toys network design requirements. You need to plan the IP addressing for the new company. You need to comply with the network design requirement. What should you do?

- A. Assign the main office and each branch office a new class A private IP address range.
- B. Assign the main office and each branch office a new class B private IP address range.
- C. Assign the main office and each branch office a subnet from a new class B private IP address range.
- D. Assign the main office and each branch office a subnet from the current class C private IP address range.

Answer: C

ExamSavior.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially [Adobe](#), [Apple](#), [Citrix](#), [Comptia](#), [EMC](#), [HP](#), [HuaWei](#), [LPI](#), [Nortel](#), [Oracle](#), [SUN](#), [Vmware](#) and so on. And help you pass any IT Certification exams at the first try.

You can reach us at any of the email addresses listed below.

English Customer:

Sales : [sales@examsavior.com](mailto:sales@examsavior.com)

Support: [support@examsavior.com](mailto:support@examsavior.com)

Website: [www.examavior.com](http://www.examavior.com)

