Microsoft 70-294 P4s Qs with Testking Answers [GMS]

Number: 070-294
Passing Score: 700
Time Limit: 240 min
File Version: 2.0

Microsoft 70-294
Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure

Q&A with explanations

Version 09.21.2006

**Original Design by Bruno, Redesigned by Jeil**

What's new:

-Just inserted the questions that appear in p4s (including the repeated ones, so there are the same question more than one time, for better memorizing, no more wrong answers, this is the perfect exam (as long as it could be checked).
-Just inserted the simulations that are present in the real exam (according to users experience they seem to be the same all the time now).

**Created on 5th May 2007**

**Organized into smaller Exam Sets by GrandMaster_S**

Exam A - 18 Questions
Exam B - 18 Questions
Exam C - 18 Questions
Exam D - 18 Questions
Exam E - 18 Questions
Exam F - 18 Question - Simulations

**Created on 18th September 2007**
Exam A

QUESTION 1
You are the network administrator for Blue Yonder Airlines. The company has offices in Toronto, New York, and Chicago. The network connections are shown in the exhibit. (Click the Exhibit button.)

The network consists of two Active Directory domains. User objects for users in the Toronto office and the New York office are stored in the blueyonderairlines.com domain. User objects for users in the Chicago office are stored in the production.blueyonderairlines.com domain. Active Directory is configured as shown in the following table.

<table>
<thead>
<tr>
<th>Location</th>
<th>Number of users</th>
<th>Number of domain controllers</th>
<th>Number of global catalog servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toronto</td>
<td>650</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>New York</td>
<td>15</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Chicago</td>
<td>500</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

Users in the New York office frequently report that they cannot log on to the network, or that logging on takes a very long time. You notice increased global catalog queries to servers in the Toronto office during peak logon times.

You need to improve logon performance for users in the New York office without increasing WAN traffic that is due to replication.

What should you do?

Exhibit:

A. Configure the domain controller in the New York office as a global catalog server.
B. Configure Active Directory to cache universal group memberships for the Toronto office.
C. Install an additional domain controller in the New York office.
D. Configure Active Directory to cache universal group memberships for the New York office.

Answer: D  
Section: (none)

Explanation/Reference:  
Explanation:  
Logons for NewYork must contact a global catalog server across the WAN to check the universal group membership from the global catalog in Toronto. Configuring universal group membership caching at the NewYork site would speedup logons and would not generate additional WAN traffic.

Incorrect Answers:  
A: This would only make sense if there were applications that need a Global Catalog.  
B: caching is not required in that office. Furthermore, the Toronto office does have two Global Catalog servers.  
C: The number of Domain Controllers is sufficient for the number of users in NY.

Reference:  

QUESTION 2  
HOTSPOT  
You are a network administrator for TestKing.com. The relevant portion of your network configuration is shown in the work area.

TestKing has offices in Toronto and New York. The Toronto office has 500 employees, and the New York office has 150 employees. Employees in both offices use an application that frequently reads configuration data in the global catalog.

You need to plan the placement of global catalog servers for TestKing.com. You need to ensure that the application performs well during times of peak activity. You need to ensure that the application continues to function in the event of multiple global catalog failures.

Where should you place the global catalog server or servers?

To answer, select the appropriate computer or computers in the work area.

Leading the way in IT testing and certification tools, www.testking.com

Answer:
**Question 3**

You are a network administrator for a company that has a main office and five branch offices. The network consists of six Active Directory domains. All servers run Windows Server 2003. Each office is configured as a single domain. Each office is also configured as an Active Directory site.

Your company uses an application server that queries user information from the global catalog. You install application servers in the main office and in three branch offices. The network is configured as shown in the exhibit. (Click the **Exhibit** button.)

You monitor the WAN connections between the main office and each branch office and discover that the utilization increased from 70 percent to 90 percent. Users report slow response times when accessing information on the application server.
You need to place global catalog servers in offices where they will improve the response times for the application servers. You need to achieve this goal with a minimum amount of increase in WAN traffic.

In which office or offices should you place a new global catalog server or servers? (Choose all that apply.)

Exhibit:

A. Bonn  
B. Rome  
C. New York  
D. San Francisco  
E. Chicago

Answer: BCD
Section: (none)

Explanation/Reference:
Explanation:
Because the application server queries Global catalog attributes, we need to place them in Rome, New York and San Francisco.

Incorrect Answers:
A: Bonn does not host an application server and therefore does not require a Global Catalog Server.  
E: Chicago does not host an application server and therefore does not require a Global Catalog Server.
QUESTION 4
You are a network administrator for TestKing.com. The network consists of a single Active Directory forest that contains one root domain and multiple child domains. The functional level of all child domains is Windows Server 2003. The functional level of the root domain is Windows 2000 native.

You configure a Windows Server 2003 computer named Testking1 to be a domain controller for an existing child domain. Testking1 is located at a new branch office and you connect Testking1 to a central data center by a persistent VPN connection over a DSL line. Testking1 has a single replication connection with a bridgehead domain controller in the central data center.

You configure DNS on Testking1 and create secondary forward lookup zones for each domain in the forest.

You need to minimize the amount of traffic over the VPN connection caused by logon activities.

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

A. Configure the DNS zones to be Active Directory-integrated zones.
B. Configure Testking1 to be the PDC emulator for the domain.
C. Configure Testking1 to be a global catalog server.
D. Configure universal group membership caching on Testking1.

Answer: CD
Section: (none)

Explanation/Reference:
Explanation:
Logon traffic over the VPN is caused by the local domain controller retrieving universal group information from a global catalog server. We can reduce this traffic by either configuring TestKing1 to be a global catalog server, or by enabling universal group membership caching on TestKing1.

A global catalog server stores information about all objects in the forest, but not their attributes, so that applications can search Active Directory without referring to specific domain controllers that store the requested data. Universal group membership caching, on the other hand allows the domain controller to cache universal group membership information for users. This eliminates the need for a global catalog server at every site in a domain, which minimizes network bandwidth usage because a domain controller does not need to replicate all of the objects located in the forest. It also reduces logon times because the authenticating domain controllers do not always need to access a global catalog to obtain universal group membership information.

Incorrect Answers:
A: In Active Directory-integrated zones the DNS Zone is replicated as part of Active
Directory. This will increase replication traffic. Logon traffic over the VPN is caused by the local domain controller retrieving universal group information from a global catalog server. It is not caused by DNS replication.

B: A PDC Emulator is required for authentication purposes for Windows NT 4.0 clients. Thus the PDC emulator is not used in the logon process (except for down-level clients).

Reference:

QUESTION 5
DRAG DROP
You are the network administrator for TestKing.com. The network consists of a single Active Directory forest that contains multiple domains. The functional level of the forest is Windows Server 2003.

The forest includes two Active Directory sites named TestKingSite1 and TestKingSite2. TestKingSite1 contains two domain controllers that are global catalog servers named TestKingA and TestKingB. TestKingSite2 contains two domain controllers that are not global catalog servers named TestKingC and TestKingD. The two sites are connected by a WAN connection. Users in TestKingSite2 report that logon times are unacceptably long.

You need to improve logon times for the users in TestKingSite2 while minimizing replication traffic on the WAN connection.

How should you configure the network?

To answer, drag the appropriate configuration option or options to the correct location or locations in the work area.
We need to improve logon times for the users in TestKingSite2 while minimizing replication traffic on the WAN connection. Logon times in TestKingSite2 are slow because the domain controllers need to contact a global catalog server in TestKingSite1 for universal group information. We can prevent this by enabling Universal group membership caching in TestKingSite2. Enabling Universal group membership caching at the site level will ensure that all the domain controllers in TestKingSite2 will be able to cache the information. We could improve logon times by placing a global catalog server enabling Universal group membership caching is a better solution.

Universal group membership caching allows the domain controller to cache universal group membership information for users. You can enable domain controllers that are running Windows Server 2003 to cache universal group memberships by using the Active Directory Sites and Services snap-in. Enabling universal group membership caching eliminates the need for a global catalog server at every site in a domain, which minimizes network bandwidth usage because a domain controller does not need to replicate all of the objects located in the forest. It also reduces logon times because the authenticating domain controllers do not always need to access a global catalog to obtain universal group membership information.

Reference:
QUESTION 6
You are the network administrator for TestKing.com. The network consists of a single Active Directory forest that contains a forest root domain named testking.com and a child domain named child2.testking.com. The functionality of the forest is Windows Server 2003.

The company uses universal groups to prevent temporary employees from accessing confidential information on computers in the forest.

The child1.testking.com domain contains a Windows 2000 Server computer named TestKing1. TestKing1 runs an application that makes frequent LDAP queries to the global catalog. TestKing1 is located on a subnet associated with an Active Directory site named Site2 that has no global catalog servers. Site2 is connected to another site by a WAN connection.

You need to enable the application on TestKing1 to run at high performance levels and to continue operating if a WAN connection fails. You also need to minimize traffic over the WAN connection.

What should you do?

A. Enable universal group membership caching in Site2.
B. Configure at least one global catalog server in Site2.
C. Add the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGC Failures key to the registry on all domain controllers in Site2.
D. Remove Server1 from the child1.testking.com domain and add it to a workgroup.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
The application needs to read data from the global catalog. This information is stored on the global catalog servers in the other site. This means that the application needs to contact the global catalog servers over a WAN link. We can improve performance by configuring a global catalog server in Site2. This will enable the application to contact a global catalog server over fast LAN connections. It will also enable the application to run if the WAN link fails.

Incorrect Answers:
A: Universal group caching likely has no effect on the application. Universal group information is just a small part of the information stored in the global catalog. The application would still need to contact a global catalog server.
C: This setting allows users to log on to a domain if the domain controller is unable to contact a global catalog server. It will have no effect on the application.
D: The application won't be able to query the global catalog if the computer isn't a member of the domain.

Reference:

QUESTION 7
You are the network administrator for Alpine Ski House. The network consists of a single Active Directory forest that contains five domains. The functional level of the forest is Windows 2000. You have not configured any universal groups in the forest.

One domain is a child domain named child1.alpineskihouse.com that contains two domain controllers and 50 client computers. The functional level of the domain is Windows Server 2003.

The network includes an Active Directory site named Site1 that contains two domain controllers. Site1 represents a remote clinic, and the location changes every few months. All of the computers in child1.alpineskihouse.com are located in the remote clinic. The single WAN connection that connects the remote clinic to the main network is often saturated or unavailable. Site1 does not include any global catalog servers.

You create several new user accounts on the domain controllers located in Site1. You need to ensure that users in the remote clinic can always quickly and successfully log on to the domain.

What should you do?

A. Enable universal group membership caching in Site1.
B. Add the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key to the registry on both domain controllers in Site1.
C. Add the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key to the registry on all global catalog servers in the forest.
D. Raise the functional level of the forest to Windows Server 2003.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
When all domain controllers are at least Windows 2000 domain controllers and the domain is switched to Windows 2000 native mode, the usage of universal groups. When processing a logon request for a user in a native-modedomain, a domain controller sends a query to a global catalog server to determine the user's universal group memberships. Since you can explicitly deny a group access to a resource, complete knowledge of a user's group memberships is necessary to enforce access control correctly. If a domain controller of a native-mode domain cannot contact a global catalog server to determine universal group membership when a user wants to log on, the domain
controller refuses the logon request.

The following registry key can be set so that the domain controller ignores the global catalog server failure when expanding universal groups:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures

The domain controller still tries to connect to the global catalog server, however, and the timeout for that query must expire.

Incorrect Answers:
A: Universal group membership caching allows the domain controller to cache universal group membership information for users. This eliminates the need for a global catalog server at every site in a domain, which minimizes network bandwidth usage because a domain controller does not need to replicate all of the objects located in the forest. It also reduces logon times because the authenticating domain controllers do not always need to access a global catalog to obtain universal group membership information. However, new user accounts would not be located on the global catalog until Active Directory replication occurs.
C: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key must be added to the registry both domain controllers in Site1, not the global catalog servers.
D: Raising the functional level of the forest to Windows Server 2003 won’t solve the problem as Windows 2000 native mode is sufficient.

Reference:

QUESTION 8
You are the network administrator for Contoso Pharmaceuticals. Your network consists of a single Active Directory forest that contains three domains. The forest root domain is named contoso.com. The domain contains two child domains named usa.contoso.com and europe.contoso.com. The functional level of the forest is Windows Server 2003.

Each domain contains two Windows Server 2003 domain controllers named DC1 and DC2. DC1 in the contoso.com domain performs the following two operations master roles: schema master and domain naming master. DC1 in each child domain performs the following three operations master roles: PDC emulator master, relative ID (RID) master, and infrastructure master. DC1 in each domain is also a global catalog server.

The user account for Nancy Buchanan in the europe.contoso.com domain is a member of the Medicine Students security group. Because of a name change, the domain administrator of europe.contoso.com changes the Last name field of Nancy’s user account from Buchanan to Anderson.

The domain administrator of usa.contoso.com discovers that the user account for Nancy is still listed as Nancy Buchanan.
You need to ensure that the user account for Nancy Anderson is correctly listed in the Medicine Students group.

What should you do?

A. Transfer the PDC emulator master role from DC1 to DC2 in each domain.
B. Transfer the infrastructure master role from DC1 to DC2 in each domain.
C. Transfer the RID master role from DC1 to DC2 in each domain.
D. Transfer the schema master role from DC1 to DC2 in the contoso.com domain.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
Problems like this can occur when the Infrastructure master role is on the same domain controller as the Global Catalog. The infrastructure master updates the group-to-user reference whenever group memberships change and replicates these changes across the domain. The infrastructure master compares its data with that of a global catalog. Global catalogs receive regular updates for objects in all domains through replication, so the global catalog data will always be up to date. If the infrastructure master finds that its data is out of date, it requests the updated data from a global catalog. The infrastructure master then replicates that updated data to the other domain controllers in the domain.

Unless there is only one domain controller in the domain, the infrastructure master role should not be assigned to the domain controller that is hosting the global catalog. If the infrastructure master and global catalog are on the same domain controller, the infrastructure master will not function. The infrastructure master will never find data that is out of date, so it will never replicate any changes to the other domain controllers in the domain. Transferring the Infrastructure master role to a different computer would resolve this problem. There is no reason to transfer any other master roles.

Incorrect Answers:
A: The PDC Emulator is responds to Windows NT 4 BDCs. It also receives all new password and lockout information changes immediately for the entire domain. Neither of these functions will ensure that the user account changes are updated in the domain.
C: The RID Master keeps track of the allocation RIDs to domain controllers to ensure that two domain controllers do not hand out the same SID.
D: The Schema Master controls what is allowed in the Active Directory directory.

Reference:

QUESTION 9
You are the network administrator for your company. The network consists of a single Active Directory forest that contains one domain.
The functional level of the forest is Windows 2000, and the functional level of the domain is Windows 2000 mixed.

The domain contains four domain controllers named DC1, DC2, DC3, and DC4. There are two sites in the forest. DC1 and DC2 are in one site. DC3 and DC4 are in the other site.

DC1 fails. You need to wait until the following week to restore DC1. While connected to DC3, you perform a bulk import of user accounts and receive an error message stating that a number of the user accounts could not be created.

You need to ensure that the user accounts can be created. What should you do?

A. Seize the PDC emulator role to DC3.
B. Seize the relative ID (RID) master role to DC3.
C. Create a replication object to connect DC3 to DC2.
D. Raise the functional level of the domain and the functional level of the forest to Windows Server 2003.

Answer: B
Section: (none)

Explanation/Reference:
Extracted from p4s, no explanations available.

QUESTION 10
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 three Active Directory sites named Site1, Site2, and Site3. The sites are connected by site links as shown in the work area.

SiteLink1 and SiteLink2 include redundant, high-speed WAN connections.

Each site has one subnet associated with it. The number of computers in each site and the operating system that the computers are running are indicated in the following table.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Site1</th>
<th>Site2</th>
<th>Site3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 98</td>
<td>50</td>
<td>30</td>
<td>550</td>
</tr>
<tr>
<td>Windows NT Workstation 4.0</td>
<td>50</td>
<td>20</td>
<td>550</td>
</tr>
<tr>
<td>Windows 2000 Professional</td>
<td>0</td>
<td>500</td>
<td>100</td>
</tr>
<tr>
<td>Windows XP Professional</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>10</td>
<td>20</td>
<td>15</td>
</tr>
</tbody>
</table>

Site1 contains a Windows Server 2003 domain controller named Server1 that is the relative ID (RID) master for the domain. Site2 contains two Windows Server 2003 domain controllers named Server2 and Server3. Server2 is the infrastructure master for the domain. Site3 contains a Windows Server 2003 domain controller named Server4.
You need to decide where to place the PDC emulator role holder. You want to optimize the overall response time for users in all sites.

Where should you place the PDC emulator role?

To answer, select the appropriate domain controller or domain controllers in the work area.

**Answer:**

**Section:** (none)

**Explanation/Reference:**

Explanation:
Place the PDC emulator on Site3. This site has the most Windows 98 and NT 4.0 workstations which need a PDC emulator to contact to logon while XP and Windows 2000 can logon at any DC.
Leading the way in IT testing and certification tools, www.testking.com

Reference:

QUESTION 11
You are the network administrator for TestKing.com. The network consists of a single Active Directory forest, as shown in the exhibit.


TestKing is engaged in a joint venture with Litware, Inc. The network of Litware, Inc., consists of a single Active Directory forest named litwareinc.com that contains one domain. The functional level of the litwareinc.com forest is Windows Server 2003.

You need to ensure that the users of TestKing can log on to the litwareinc.com forest. You upgrade dc1.corp.testking.com to Windows Server 2003.

Which two additional courses of action should you take? (Each correct answer presents part of the solution. Choose two)

Exhibit:


C. Create a one-way forest trust relationship in which the testking.com forest trusts the litwareinc.com forest.

D. Create a one-way forest trust relationship in which the litwareinc.com forest trusts the testking.com forest.

Answer: AD
Section: (none)

Explanation/Reference:
Explanation:
relationship. The minimum forest functional level for a forest trust relationship is Windows Server 2003. This must be the forest functional level of the root domain in the two forests. To raise the forest functional level to Windows Server 2003, all domain must be at least Windows 2000 native.

Incorrect Answers:
B: We cannot raise a child domain to a functional level higher than that of the parent domain. The east.corp.testking.com domain is a child domain of the corp.testking.com domain.

C: The litwareinc.com forest trusts the testking.com forest because TestKing users must be able to log on to the litwareinc.com forest.

Reference:

**QUESTION 12**
You are the network administrator for Acme Inc. Your network consists of a single Active Directory forest that contains one domain named acme.com. The functional level of the forest is Windows Server 2003.


A business decision by Proseware requires that asia.proseware.com domain to be removed.

You need to move all user accounts from the asia.proseware.com domain to the acme.com domain by using the Active Directory Migration Tool. You need to accomplish this task without changing the logon rights and permissions for all other users. You need to ensure that users in asia.proseware.com can log on to acme.com by using their current user names and passwords.

What should you do ?

A. Create a two-way Windows Server 2003 external trust relationship between the acme.com domain and the proseware.com domain.
B. Create a one-way Windows Server 2003 external trust relationship in which the acme.com domain trusts the proseware.com domain.
C. Create a temporary two-way external trust relationship between the acme.com domain and the asia.proseware.com domain.
D. Create a temporary one-way external trust relationship in which the asia.proseware.com domain trusts the acme.com domain.

**Answer:** C

**Explanation/Reference:**
Explanation:
To use ADMT, we need a two way trust between the acme.com domain and the asia.proseware.com domain.

To run ADMT asia.proseware.com must trust acme.com. To satisfy "You need to ensure that users in asia.proseware.com can log on to acme.com by using their current user names and passwords." acme.com must then also trust asia.proseware.com.
Incorrect Answers:
A: This would enable users in proseware.com to log in to acme.com and users in acme.com to log in to proseware.com.
B: This would enable users in proseware.com to log in to acme.com.
D: The trust must be a two-way trust.

Reference:

QUESTION 13
HOTSPOT
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. The functional level of the domain is Windows Server 2003.

You configure two Active Directory sites named Testking1 and Testking2. Testking1 contains all of the operations masters and two global catalog servers. Testking2 contains a domain controller named Server1. You create a site link named SiteLink1 that includes Testking1 and Testking2.

You need to provide global catalog services locally in Testking2.

Which Active Directory component should you configure?

To answer, select the appropriate component in the work area.
Select "NTDS Settings" under SERVER1.
The global catalog service is added or removed in the NTDS Settings Properties dialog box of the Active Directory Sites and Services console.

Reference:

QUESTION 14
You are a network administrator for your company. The network consists of a single Active Directory forest that contains one domain. The company has its main office and one branch office in San Francisco. The company has additional branch offices in Chicago, New York, and Toronto.

Administrators at the main office are responsible for managing all objects in the domain. Administrators at each branch office are responsible for managing user and computer objects for employees who work in the same branch office as the administrator. Administrators for the San Francisco branch office are also responsible for managing user and computer objects for employees who work in the main office. These users are managed as a single unit. You want administrators to be authorized to make changes only to the objects for which they are responsible.

You need to plan an organizational unit (OU) structure that allows the delegation of required permissions. You want to achieve this goal by using the minimum amount of administrative effort.

Which OU structure should you use?

exb-A (exhibit):
Testking.com

Branch Offices

Main Office

exb-D (exhibit):
A.

Testking.com

Chicago

Toronto

New York

Domain

Chicago

New York

Toronto

San Francisco

Domain
Answer: A
Section: (none)
Explanation/Reference:

Explanation:
Administrators at each branch office are responsible for managing user and computer objects for employees who work in the same branch office as the administrator. A separate OU for each office will achieve this.

Administrators for the San Francisco branch office are also responsible for managing user and computer objects for employees who work in the main office. We can put the main office user and computer accounts in the San Francisco OU.

Administrators at the main office are responsible for managing all objects in the domain. The Main office administrators can be set permissions at the domain level. The permissions will apply to all OUs.

Incorrect Answers:
B: Administrators at the main office are responsible for managing all objects in the domain. The Main office administrators can be set permissions at the domain level, not the OU level.
C: Administrators at each branch office are responsible for managing user and computer objects for employees who work in the same branch office as the administrator. Therefore, we need a separate OU for each office.
D: Administrators at each branch office are responsible for managing user and computer objects for employees who work in the same branch office as the administrator. A separate OU for each office will achieve this. However, there are four branch offices: San Francisco, Chicago, Toronto and New York.

Reference:

**QUESTION 15**
You are the network administrator for your company. The network consists of a single Active Directory domain. The relevant portion of the organizational unit (OU) structure is shown in the exhibit. (Click the Exhibit button.)

The company's sales division consists of an inside sales department, a mobile sales department, and a telemarketing department. User objects for users in these departments are stored in the Inside, Mobile, and Telemarket OUs respectively. User objects for all junior managers and senior managers are stored in the Managers OU.

The company decides to train junior managers to perform basic administrative tasks. Junior managers are responsible for enabling and disabling accounts for all sales users except junior managers and senior managers.

You need to enable junior managers to perform the assigned administrative tasks. You must not affect any existing permissions.

What should you do?
Exhibit:

A. On the Managers OU, block the inheritance of permissions.
   Copy all existing permissions.
   On the Sales OU, grant junior managers the permission to enable and disable accounts.

B. On the Inside, Mobile, and Telemarket OUs, block the inheritance of permissions.
   Copy all existing permissions.
   On the Sales OU, grant junior managers the permission to enable and disable accounts.

C. On the Managers OU, block the inheritance of permissions.
   Remove all existing permissions.
   On the Sales OU, grant junior managers the permission to enable and disable accounts.

D. On the Sales OU, block the inheritance of permissions.
   Copy all existing permissions.
   On the Sales OU, grant junior managers the permission to enable and disable accounts.

Answer: A
Section: (none)

Explanation/Reference:
Explanation:
You want to set the policy on a higher OU (parent) than the three target child OUs where you want administration. For junior managers to be able to perform administrative tasks on only the three target OUs and not the managers OU we have to Block the inheritance of the Policy at the Managers OU. You also want to preserve permissions that were inherited before setting the block so copying all permissions would satisfy that requirement.

Incorrect Answers:
B: Junior managers must be able to perform administrative tasks on only the Inside, Mobile, and Telemarket OUs and not the Managers OU. Therefore we have to Block the inheritance of the Policy on the Managers OU, not on the Inside, Mobile, and Telemarket OUs.
C: You want to preserve permissions that were inherited before you blocked inheritance to the Managers OU. Therefore you need to copy the permissions to the Managers OU.
D: You need to block inheritance at the child OU, not the parent OU.
QUESTION 16
You are the network administrator for a company that has six offices. The network consists of a single Active Directory domain.

Each office has users who work in the sales, marketing, and production departments. All Active Directory administration is performed by the IT group. The IT group provides a help desk, a level-two support group, and an MIS group. Each office has one employee who works for the help desk group. Administrative responsibilities are listed in the following table.

<table>
<thead>
<tr>
<th>Group</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help desk</td>
<td>User account maintenance for all employees who are not management</td>
</tr>
<tr>
<td>Level-two</td>
<td>User account maintenance for all employees, the help desk users, and all management users</td>
</tr>
<tr>
<td>support group</td>
<td></td>
</tr>
<tr>
<td>MIS group</td>
<td>Service account maintenance, maintenance of domain administrator accounts, and built-in accounts in Active Directory</td>
</tr>
</tbody>
</table>

You need to plan an organizational unit (OU) structure that allows delegation of administration. Your plan must ensure that permissions can be maintained by using the minimum amount of administrative effort.

Which OU structure should you use?

exb-A (exhibit):
exb-B (exhibit):
exb-C (exhibit):
exb-D (exhibit):
We need to delegate the management of different groups of users. We have the non-management employees, who should be managed by the Help Desk staff. We have the employees (including management and help desk staff), who should be managed by the level 2 staff. The MIS group needs to manage every other account.

To solve this question is to delegate the management of user accounts at domain level for the MIS group. Delegate the management of user accounts to the Employees OU to the help desk staff. Delegate the management of user accounts to the Corp OU to the second-level support staff.

Incorrect Answers:
A, B: Level 2 staff should manage HelpDesk, Employees and Managers.
D: We need to delegate administrative control based on user groups, not on office location.

Reference:

QUESTION 17
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com.
The company has its main office in Chicago and branch offices in Toronto and New York. The main office contains a sales department and a marketing department. The company's MIS department is responsible for administration of the entire domain. Each office has an IT group that is responsible for the administration of user accounts. In addition, the main office MIS group has one administrator to manage the sales department and one administrator to manage the marketing department.

You need to plan the organizational unit (OU) structure for TestKing.com. You want administrators to be delegated control to only objects for which they are responsible. Your plan must ensure that permissions can be maintained by using the minimum amount of administrative effort.

Which OU structure should you use?

exb-A (exhibit):

```
PLAN A

Testking.com

Toronto  Chicago  New York

Sales  Marketing
```

exb-B (exhibit):

```
PLAN B

Testking.com

Toronto  Chicago  New York
```
**Answer:** A  
**Section:** (none)

**Explanation/Reference:**

Explanation:
The Company's MIS department is responsible for administration of the entire domain. They can be set permissions at the domain level. These permissions would apply to all OUs in the domain.

Each office has an IT group that is responsible for the administration of user accounts. A separate OU for each office would allow the necessary delegation of control.

The main office MIS group has one administrator to manage the sales department and one administrator to manage the marketing department. OUs in the main office OU (Chicago) would allow the necessary delegation of control.

**Incorrect Answers:**
B: The main office MIS group has one administrator to manage the sales department and one administrator to manage the marketing department. We need OUs in the main office OU (Chicago) to allow for the necessary delegation of control.
C: The Company's MIS department is responsible for administration of the entire domain but there is a second level of administration: The main office MIS group has one administrator to manage the sales department and one administrator to manage the marketing department.
D: The Company's MIS department is responsible for administration of the entire domain. They can be set permissions at the domain level. These permissions would apply to all OUs in the domain.

**Reference:**
QUESTION 18
You are the network administrator for your company. The network consists of a single Active
Directory domain. User and group objects for the sales department are located in an organizational
unit (OU) named Sales.

Peter and Mary are administrators for your company. Peter is responsible for managing Sales user
objects. Mary is responsible for managing Sales group objects.

You need to delegate Peter and Mary control over only the objects for which they are responsible.

What should you do?

A. In the Sales OU, create two new OUs.
   Name one OU SalesUsers and place all user objects for the sales department in this OU.
   Name the other OU SalesGroups and place all group objects for the sales department in this OU.
   Grant Peter and Mary full control over the Sales OU.
B. On the Sales OU, grant Peter the right to manage user objects.
   On the Sales OU, grant Mary the right to manage group objects.
C. In the Sales OU, create a new OU. Name this OU SalesGroups.
   Place all Sales groups in the SalesGroups OU.
   Grant Peter the right to manage all objects in the Sales OU.
   Grant Mary the right to manage all objects in the SalesGroups OU.
D. On the Sales OU, deny Peter the right to manage group objects.
   On the Sales OU, deny Mary the right to manage user objects.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
We can assign users the right to manage certain objects in an OU. This would be the easiest
solution.

Incorrect Answers:
A: Granting Peter and Mary full control over the Sales OU would allow them control over all objects
in the Sales OU.
C: Through Inheritance, Peter will be able to control all objects in the Sales OU and in its child OU.
D: The right to manage objects in an OU must be assigned explicitly.

Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003
to 9-26
Exam B

QUESTION 1
You are a network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. The functional level of the domain is Windows Server 2003. The organizational unit (OU) structure is shown in the exhibit. (Click the Exhibit button.)

Your company uses an X.500 directory service enabled product to support a sales and marketing application. The application is used only by users in the sales department and the marketing department. The application uses InetOrgPerson objects as user accounts. InetOrgPerson objects have been created in Active Directory for all Sales and Marketing users. These users are instructed to log on by using their InetOrgPerson object as their user account.

Microsoft Identity Integration Server is configured to copy changes to InetOrgPerson objects from Active Directory to the X.500 directory service enabled product. All InetOrgPerson objects for marketing employees are located in the Marketing OU. All InetOrgPerson objects for sales employees are located in the Sales OU.

Mikhail is another administrator in your company. Mikhail is responsible for managing the objects for users who require access to the X.500 directory service enabled product.

You need to configure Active Directory to allow Mikhail to perform his responsibilities.

Which action or actions should you take? (Choose all that apply.)

Exhibit:

A. On the domain, grant Mikhail the permission to manage user objects.
B. On the domain, grant Mikhail the permission to manage InetOrgPerson objects.
C. On the Sales OU, block the inheritance of permissions.
D. On the Marketing OU, block the inheritance of permissions.
E. On the Dev OU, block the inheritance of permissions

Answer: BE
The administrator needs to manage the InetorgPerson objects. We could delegate this task to the
administrator or we can use permissions at the domain level to accomplish this. However, the
permissions shouldn't apply to the Dev OU, so we'll have to block the inheritance of the permissions
for the Dev OU.

Incorrect Answers:
A: Mikhail needs to manage the InetorgPerson objects, not he user objects.
C, D: User accounts are located in the Sales OU and the Marketing OU. Blocking inheritance to
these OUs would mean that the permissions will not apply to these OUs.

Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003
to 9-26

QUESTION 2
You are the network administrator for TestKing.com. You plan to create an Active Directory domain
named testking.com that will have a functional level of Windows Server 2003.

TestKing has one main office and four branch offices, which are all located in one country. A central
security department in the main office is responsible for creating and administering all user
accounts in all offices. Each office has a local help desk department that is responsible for resetting
passwords within the individual department's office only.

All user accounts are located in the default Users container.

You need to create an organizational unit (OU) structure to support the delegation of authority
requirements. You want to minimize the amount of administrative effort required to maintain the
environment.

What should you do?

A. Create a top-level OU named Testking_Users under the testking.com domain. Create a
   separate child OU for each office under Testking_Users. Move the user accounts of all
   employees in each office to the child OU for that office.

B. Create a top-level OU named Main_Office under the testking.com domain. Move the user
   accounts of all users in the main office to the Main_Office OU. Create a separate child OU for
   each branch office under the Main_Office OU. Move the user accounts of all users in each
   branch office to the child OU for that office.

C. Create a top-level OU named Testking_Users under the testking.com domain. Create a child OU
   named Central_Security under TestKing_Users. Move the user accounts of the central security
   department users to the Central_SecurityOU. Create a child OU named Help_Desk under
   TestKing_Users. Move the user accounts of the help desk users to the Help_Desk OU.

D. Create a top-level OU named TestKing_Users under the testking.com domain. Create a child OU
   named Central_Security under TestKing_Users. Move the user accounts of the central security
   department users to the Central_SecurityOU.
**Answer:** A  
**Section:** (none)

**Explanation/Reference:**

**Explanation:**
Two OU levels will fit the requirement. You can delegate control for central security on the OU "Testking_Users" and each office can be administered by the local help desk team.

**Incorrect Answers:**
B: All user accounts are located in the default Users container in the domain. Therefore it is not necessary to move them to the top level OU  
C, D: There is not need for a Central_security OU as administrators at each branch office are responsible for administrating user accounts in their respective branch.

**Reference:**


**QUESTION 3**

Each domain contains Windows Server 2003 file and print servers. All of the file and print server computer accounts are located in the default Computers container in each domain. There is a central operations department that is responsible for administering the file server computer accounts in all domains. There is a separate operations department for each domain that is responsible for administering the print server computer accounts in that domain.

You need to delegate authority to create an environment to support your file and print server administration requirements. You need to create an organizational unit (OU) structure to support the delegation of authority requirements.

**What should you do?**

A. Create a top-level OU for file server computer accounts under the testking.com domain.  
B. Create a top-level OU for file server computer accounts under the testking.com domain.  
C. Create a top-level OU for file server computer accounts under each domain.  
D. Create a top-level OU for file server computer accounts under each domain.

**Answer:** C
Explanation/Reference:
The central operations department is responsible for administering the file server computer accounts in all domains and there is a separate operations department for each domain that is responsible for administering the print server computer accounts in that domain. Thus, we need two top-level OUs.

Incorrect Answers:
A, B: OUs cannot transcend domains therefore the OU structure needs to be implemented at the child domain level, not at the testking.com domain.
D: There is no need for child OUs as the central operations department is not responsible for the print server accounts.

Reference:

QUESTION 4
You are the network administrator for the Baldwin Museum of Science. The network consists of a single Active Directory forest that contains one domain named baldwinmuseumofscience.com.

You need to deploy a new domain named NA.baldwinmuseumofscience.com as a child domain of baldwinmuseumofscience.com.

You install a new stand-alone Windows Server 2003 computer named DC1. You plan to make DC1 the first domain controller in the NA.baldwinmuseumofscience.com domain. You configure DC1 with a static IP configuration.

You run the Active Directory Installation Wizard on DC1. The wizard prompts you for the network credentials to use to join the NA.baldwinmuseumofscience.com domain to the forest. You enter the appropriate credentials for an account in the baldwinmuseumofscience.com domain.

You receive an error message stating that a domain controller in the baldwinmuseumofscience.com domain cannot be located.

You need to be able to promote DC1 to a domain controller as the first domain controller of the child domain in the existing forest.

What should you do?
A. Configure the client WINS settings on DC1 to use a WINS server that contains entries for the baldwinmuseumofscience.com domain controllers.
B. Configure the client DNS settings on DC1 to use a DNS server that is authoritative for the baldwinmuseumofscience.com domain.
C. Configure the DNS Server service on DC1 to have a zone for NA.baldwinmuseumofscience.com.
D. Configure DC1 to be a member server in the baldwinmuseumofscience.com domain.
**Answer:** B  
**Section:** (none)

**Explanation/Reference:**

**Explanation:**
This is typically the effect of a DNS problem because the client (in this case a member server) can't locate the SRV records of a domain. The process needs to contact the DNS server that is authoritative for the parent domain that you want to make a child domain in. First, in the Active Directory installation wizard, you specify the DNS name of the Active Directory domain for which you are promoting the server to become a domain controller. Later in the installation process, the wizard tests for the following:

Based on its TCP/IP client configuration, it checks to see whether a preferred DNS server is configured. If a preferred DNS server is available, it queries to find the primary authoritative server for the DNS domain you specified earlier in the wizard.

It then tests to see whether the authoritative primary server can support and accept dynamic updates as described in the DNS dynamic update protocol.

If, at this point in the process, a supporting DNS server cannot be located to accept updates for the specified DNS domain name you are using with Active Directory, you are provided with the option to install the DNS Server service.

**Incorrect Answers:**
A: WINS is used for name resolution for down level clients. TK1 is a Windows Server 2003 computer.
C: NA.testking.com does not yet exist.
D: We want to install TK1 as a domain controller for the na.testking.com domain. Making TK1 a member server would mean demoting the server and then promoting it again at a later point. This does not make sense.

**Reference:**
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 4-6 to 4-9, 4-17

**QUESTION 5**

You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory forest that contains a single domain named contoso.com. You have a user account named CONTOSO\admin that is a member of the Domain Admins global group.

You need to create a new child domain named NA.contoso.com in the forest. You install a stand-alone Windows Server 2003 computer named DC3.

You use the Active Directory Installation Wizard to promote DC3 to a domain controller in the new domain. You choose to create a domain controller for a new child domain in an existing domain tree. You enter the user name and password for CONTOSO\admin. You choose contoso.com as the parent domain, and you type NA as the name of the child domain.

You receive the error message shown in the exhibit. (Click the Exhibit button.)
You need to be able to create the new child domain.

What should you do?

**Exhibit:**

![New Credentials dialog box](image)

The operation failed because: Managing the network session with \DC3.Contoso.com failed
"Logon failure: unknown user name or bad password."

Type the user name and password of an account with sufficient privileges to create a child domain of the Contoso.com domain.

- **User name:** admin
- **Password:** ********
- **Domain:** Contoso.com

**Options:**

A. of the local Administrative group.
B. Add DC3 to the contoso.com domain and then run the Active Directory Installation Wizard.
C. Enter the network credentials for a member of the Enterprise Admins group for the contoso.com forest.
D. Enter the network credentials for a member of the Schema Admins group for the contoso.com forest.

**Answer:** C

**Section:** (none)

**Explanation/Reference:**

We don't have the exhibit, but from the answers, we can guess that the problem is a permissions problem. To add a domain in a forest, you need to be a member of the Enterprise Admins group. Therefore, to add the domain, you need to enter the network credentials for a member of the Enterprise Admins group for the testking.com forest.

**Incorrect Answers:**

A: To add a domain in a forest, you need to be a member of the Enterprise Admins group. You do need administrative rights on the local computer, but that alone isn't enough.
B: This is not necessary.
D: To add a domain in a forest, you need to be a member of the Enterprise Admins group, not the Schema Admins group.

Reference:

QUESTION 6
You are the network administrator for your company. The company consists of two subsidiaries named Contoso, Ltd., and Fabrikam, Inc. The network consists of two Active Directory forests. The WAN connections that connect some domain controllers are unreliable. The domain and trust configuration is shown in the Network Diagram exhibit. (Click the Exhibit button.)

You create shared folders on Windows Server 2003 member servers in both forests. Some of the shared folders are accessible to users from both forests. For each of the shared folders, you create a domain local group. You add global groups from domains in either forest to the domain local group.

The Fabrikam, Inc., division is sold to a different company. You delete the trust relationship between the two forests.

You notice that after the trust relationship is deleted, the membership lists for some of the domain local groups are no longer accurate. When you view a membership list, it contains entries without user-friendly names. A sample is shown in the Membership List exhibit. (Click the Exhibit button.)

You need to delete all the unknown groups from the membership list for the domain local groups. You want to achieve this goal by using the minimum amount of administrative effort, and without modifying the access to resources for users in the contoso.com forest.

What should you do?

qb2_Membership_List (exhibit):
qb2_Network_Diagram (exhibit):

Two-way forest trust relationship

contoso.com
asial.contoso.com
na.contoso.com

fabrikam.com
A. Create new domain local groups. Add the required global groups from the testking.com forest to the domain local groups. Grant appropriate permissions to the domain local groups. Delete the original domain local groups.

B. Re-create the trust relationship between testking.com forest and the fabrikam.com forest. Delete all fabrikam.com global accounts from the domain local group membership lists. Delete the trust relationship between the two forests.

C. Verify all remaining trust relationships. Then delete the unknown accounts from the domain local groups.

D. Delete all the affected domain local groups. Re-create the groups. Add the appropriate global groups from the testking.com forest to the groups. Grant appropriate permissions to the domain local groups.

Answer: C
Section: (none)

Explanation/Reference:
Explanation:
A method of seek and destroy will represent the least administrative effort.
To keep administrative effort to the minimum and deleting all the unknown groups from the membership list without modifying access to resources for the testking.com forest users, then you should verify all remaining trust relationships and then delete the unknown accounts from the domain local groups.

Incorrect answers:
A: Creating new domain local groups and adding only the required testking.com forest global group to the domain local group will not reveal where unknown accounts are located. It could well be that amongst the required global testking.com forest group there are unknown accounts.
B: This option suggests too much administrative effort to complete the task. And it will also result in modifying access to resources for the testking.com forest users.
D: How would you know which are all the affected groups without verifying the trust relationships first.

Reference:

QUESTION 7
You are the network administrator for Litware, Inc., which is located in New York. Litware, Inc., owns a company named Lucerne Publishing, which is located in London. The Litware, Inc., network consists of a single Active Directory forest that contains two domains.

Litware, Inc., opens a new office in Cairo. The structure of the Active Directory network after the addition of the Cairo office is shown in the exhibit. (Click the Exhibit button.)

Both site links are configured to be transitive. The site links are configured as shown in the following table.
Users in all three sites report that response times are unacceptably slow when crossing WAN connections to access information in other offices. You discover that replication between servers in NYSite and CairoSite is happening throughout the day.

You need to ensure that users’ access to remote offices is not slowed as a result of replication traffic.

What should you do?

**Exhibit:**

<table>
<thead>
<tr>
<th></th>
<th>NYLondon</th>
<th>LondonCairo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>Interval</td>
<td>30 minutes</td>
<td>45 minutes</td>
</tr>
<tr>
<td>Schedule</td>
<td>11:00 P.M. - 1:00 A.M. UTC</td>
<td>7:00 P.M. - 9:00 P.M. UTC</td>
</tr>
</tbody>
</table>

A. Replace the current site links with SMTP-based site links.
B. Create a site link bridge and include both site links.
C. Configure the cost on both site links to be 500.
D. Configure the schedule times to overlap.

**Answer:** D

**Section:** (none)

**Explanation/Reference:**
Explaination:
Replication is occurring throughout the day. We need to reconfigure the replication schedule to prevent this.

Incorrect Answers:
A: Replacing the links with SMTP-based links won't reduce the replication traffic.
B: A site link bridge won't reduce the replication traffic.
C: Site link costs are used when there are alternative paths between sites. However, there are only
QUESTION 8
You are the network administrator for your company. The network consists of a single Active Directory domain. The company has an office in San Diego, which is configured as a single Active Directory site. The company has 500 users.

The company opens a new office in Los Angeles, which employs 50 users. A T1 line connects both offices. You configure the Los Angeles office as a single site. You create a subnet object for the Los Angeles office. In the Los Angeles office, you install and configure a server named DC1 as a domain controller and global catalog server. You configure the Los Angeles site to use DC1 and the Los Angeles subnet object. You configure a site link that connects the site in San Diego and the site in Los Angeles.

You need to ensure that changes to the domain are replicated as soon as possible. What should you do?

A. Configure the interval for the site link to its minimum value
B. Remove the Los Angeles site and move DC1 and the Los Angeles subnet object to the San Diego site.
C. Create an RPC-based connection object at each of the two sites.
D. Create a site link bridge between the two sites.

Answer: A
Section: (none)

Explanation/Reference:
No explanation since it was extracted directly from p4s and was not found on any TK

QUESTION 9
You are the network administrator for a company that has three offices. The offices are in Boston, Chicago, and New York. All three offices are connected by leased lines as shown in the exhibit. (Click the Exhibit button.)

Your company is deploying a Windows Server 2003 forest. You create a single Active Directory domain. You configure each office as a single site.
You configure three domain controllers in NYSite. You create a domain controller in each of the other sites. You create site links based on the network topology. Each leased line is represented by a site link. Each site link connects only two sites. The cost and the schedule for all site links is the same. The sites and site links are named as shown in the following table.
Users report that network requests between BosSite and ChiSite are taking much longer than they used to take. You discover that replication traffic is using an unacceptably large percentage of the bandwidth between BosSite and ChiSite.

You need to reduce replication traffic over the ChiBoston site link.

What should you do?

**Exhibit:**

<table>
<thead>
<tr>
<th>Site link name</th>
<th>Linked site</th>
<th>Linked site</th>
</tr>
</thead>
<tbody>
<tr>
<td>NYBoston</td>
<td>NYSite</td>
<td>BosSite</td>
</tr>
<tr>
<td>NYChi</td>
<td>NYSite</td>
<td>ChiSite</td>
</tr>
<tr>
<td>ChiBoston</td>
<td>ChiSite</td>
<td>BosSite</td>
</tr>
</tbody>
</table>

A. Create an SMTP-based connection object from a domain controller in NYSite to a domain controller in BosSite.
B. Increase the cost for the ChiBoston site link.
C. Create a site link bridge that includes the NYBoston and NYChi site links.
D. Increase the replication interval for the NYBoston site link.

**Answer:** B

**Section:** (none)

**Explanation/Reference:**

Explanation:
To reduce the replication traffic over the ChiBoston site link, we need to increase the site link cost of that site link. The ChiBoston site link cost should be higher than that of the other two site links. Replication traffic will then pass over the site link with the lowest cost.

Incorrect Answers:
A: You can use either IP or SMTP as the protocol for replication traffic. However, SMTP replication requires an Enterprise Certification Authority (ECA) because Public Key encryption and certificates are used to verify identity of domain controllers and provide digital signatures. It would be easier to increase the site link costs for the ChiBoston site.

C: By default, all site links are bridged together, making the site links transitive. We need to disable the transitive property of the ChiBoston site link rather than create another sitelink bridge.

D: Increasing the replication interval for the NYBoston site link will result in even more replication traffic passing over the NYChi and ChiBoston site links.

Reference:

MS Windows server 2003 Deployment Kit: Designing and Deploying Directory and Security Services: - Setting Site Link Properties

QUESTION 10
DRAG DROPYou are the network administrator for TestKing.com. The network consists of a single Active Directory domain with four sites. The sites are connected by site links, as shown in the work area.

<table>
<thead>
<tr>
<th>WAN connection</th>
<th>Type of connection</th>
<th>Available bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site TK1 - Site TK2</td>
<td>56 Kbps</td>
<td>30 percent</td>
</tr>
<tr>
<td>Site TK2 - Site TK3</td>
<td>T3</td>
<td>70 percent</td>
</tr>
<tr>
<td>Site TK3 - Site TK4</td>
<td>T1</td>
<td>40 percent</td>
</tr>
<tr>
<td>Site TK4 - Site TK1</td>
<td>T3</td>
<td>70 percent</td>
</tr>
</tbody>
</table>

You need to ensure that the Knowledge Consistency Checker (KCC) uses the faster connection links when possible.

What should you do?

To answer, drag the appropriate site link cost or costs to the correct location or locations in the work area.
Site link costs determine which links are first used for replication. The link with the lowest cost is used first. If that link is down, the link with the next lowest cost is used.

We must therefore assign the lowest cost to the site links with the highest available bandwidth, i.e., Site TK1 - Site TK4 and Site TK2 - Site TK3. We must then assign the site link with the next highest
available bandwidth (Site TK3 - Site TK4) the next lowest cost. The site link with the lowest available bandwidth (Site TK1 - Site TK2) must have the highest cost.

Reference:

QUESTION 11
You are a network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. TestKing has offices in 25 cities. Each office is configured a single site. You are responsible for one site that is configured as shown in the exhibit.

An IP site link connects your site and the site at TestKing’s main office. TestKing replaces your router with a firewall device. The firewall is configured to allow HTTP, SMTP, FTP, NTTP, global catalog queries, and VPN packets to pass. You discover that replication with other sites is not occurring.

You need to ensure that you can replicate with other sites. You need to achieve this goal without removing or reconfiguring the firewall.

What should you do?

Exhibit:

A. Create a new SMTP site link between your site and each of the other sites.
B. Configure one domain controller in your site as a global catalog server.
C. Configure both domain controllers in your site to use a fixed port when replicating.
D. Create a VPN between your site and the site at the main office.

Answer: D
We need to enable replication through an Internet connection. The best solution would be to use a virtual private network (VPN) connection between our site and the corporate network.

Incorrect Answers:
A: You can use either IP or SMTP as the protocol for replication traffic. However, SMTP replication requires an Enterprise Certification Authority (ECA) because Public Key encryption and certificates are used to verify identity of domain controllers and provide digital signatures.
B: The global catalog is the central repository of information about Active Directory objects in a tree or forest. The domain controller that holds a copy of the global catalog is called a global catalog server. The global catalog enables a user to log on to a network by providing universal group membership information to a domain controller when a logon process is initiated, and enables finding directory information regardless of which domain in the forest actually contains the data. It does not control replication.
C: We need to create a connection via the Internet. Configuring ports for replication on its own will not accomplish this.

Reference:

QUESTION 12
You are the network administrator for Northwind Traders. The network consists of a single Active Directory forest that contains one root domain and one child domain. The forest also contains three separate sites, as shown in the Network Diagram exhibit. (Click the Exhibit button.)

The network is not fully routed and there is no direct physical connection between Site1 and Site3. Site links are not bridged.

You discover that the domain controllers for namerica.northwindtraders.com located in Site1 have additional accounts that are not on the domain controllers for namerica.northwindtraders.com located in Site3. You examine the directory service log in Event Viewer on a domain controller for namerica.northwindtraders.com. You discover the error message shown in the Error Message exhibit. (Click the Exhibit button.)

You need to resolve the condition that is causing this error.

What should you do?

qa59_Network_Diagram (exhibit):
A. Add a domain controller for the namerica.northwindtraders.com domain to Site2.
B. Configure a site link bridge between the site links for Site1 and Site3.
C. Configure at least one domain controller in each site to be a global catalog server.
D. Create a site link between Site1 and Site3.

**Answer:** B

**Section:** (none)

**Explanation/Reference:**

Explanation:

B is correct.
Solution
Use the following procedures for troubleshooting event ID 1311:
Identify the scope of the problem.
Check site link bridging.
Determine whether the network is fully routed.
Verify that all sites are connected.
Check preferred bridgehead servers.

Determine Whether the Network Is Fully Routed
Determine whether a fully routed network connection exists between two sites.
If the network is not fully routed and site link bridging is enabled, either make the network fully routed, or disable site link bridging and then create the necessary site links and site link bridges.

If the network is not fully routed, be sure that you have created site links to connect all sites.

QUESTION 13
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 is shown in the exhibit. (Click the Exhibit button.)

Replication is scheduled to take place once per day. Each server is fully backed up daily.

You connect to Server1 and create seven logon scripts in the Default Domain Policy Group Policy object (GPO).

Three days later, an administrator in Tel Aviv inadvertently corrupts the scripts on Server3. Ten minutes later, you successfully make changes to one of the logon scripts on Server1.

You need to make the latest version of the logon scripts available to users in Tel Aviv as soon as possible.

What should you do?

To answer, drag the action that you should perform first to the First Action box. Continue dragging actions to the corresponding numbered boxes until you list all required actions in the correct order. You might not need to use all numbered boxes.
### Possible Actions

- Restart Server1 normally.
- Restart Server3 normally.
- Restart Server1 in Directory Services Restore Mode.
- Restart Server3 in Directory Services Restore Mode.
- Use Backup to restore the SYSVOL folder.
- Use the Ntdsutil utility to mark restored objects as authoritative.

### Required Actions in Order

<table>
<thead>
<tr>
<th>Action</th>
<th>Drag action here</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Action</td>
<td></td>
</tr>
<tr>
<td>Second Action</td>
<td></td>
</tr>
<tr>
<td>Third Action</td>
<td></td>
</tr>
<tr>
<td>Fourth Action</td>
<td></td>
</tr>
<tr>
<td>Fifth Action</td>
<td></td>
</tr>
<tr>
<td>Sixth Action</td>
<td></td>
</tr>
</tbody>
</table>

**Answer:**
**Possible Actions**

- Restart Server1 normally.
- Restart Server3 normally.
- Restart Server1 in Directory Services Restore Mode.
- Restart Server3 in Directory Services Restore Mode.
- Use Backup to restore the SYSVOL folder.
- Use the Ntdsutil utility to mark restored objects as authoritative.

**Required Actions in Order**

1. **First Action**
   - Restart Server3 in Directory Services Restore Mode.
2. **Second Action**
   - Use Backup to restore the SYSVOL folder.
3. **Third Action**
   - Restart Server3 normally.

**Section:** (none)

**Explanation/Reference:**

**Explanation:**
You want to get TestKing3 back up to the most current script versions that are stored in active Directory. Restoring the SySVol restores the scripts to the good versions that were backed up in the previous backup. After rebooting, changes in Active Directory since the last backup will be replicated to this server's Active Directory.

**Reference:**

**QUESTION 14**
You are a network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. The functional level of the domain is Windows Server 2003. All domain controllers run Windows Server 2003. All domain controllers are fully backed up every Friday evening at 5:00 P.M.
The Directory Services object is configured to have the properties shown in the following table.

<table>
<thead>
<tr>
<th>Directory Services object property</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>garbageCollPeriod</td>
<td>15 hours</td>
</tr>
<tr>
<td>tombstoneLifetime</td>
<td>5 days</td>
</tr>
</tbody>
</table>

On Monday morning, a network administrator deletes several domain user accounts. On Wednesday evening at 5:00 P.M., one of the domain controllers fails.

You plan to restore the directory database domain controller from backup. You need to ensure that Active Directory is not corrupted by the restoration process.

What should you do?

A. Increase the garbageCollPeriod setting by 5.
B. Decrease the garbageCollPeriod setting by 5.
C. Increase the tombstoneLifetime setting by 5.
D. Decrease the tombstoneLifetime setting by 5.

**Answer:** C  
**Section:** (none)

**Explanation/Reference:**

Explanation:
The "tombstoneLifetime" attribute is the time a deleted object will remain in Active Directory before it is permanently deleted. We can use one of the Active Directory editing tools, such as Adsiedit.msc, Ldp.exe, and ADSI Scripts, to change the "tombstoneLifetime" attribute. We should set the "tombstoneLifetime" attribute to be older than the backup used to restore the Active Directory.

Incorrect Answers:
A, B: The garbageCollPeriod is the interval by which deleted objects whose tombstonelifetime has expired are removed from Active Directory. This does not affect the restoration process.
D: We should set the "tombstoneLifetime" attribute to be older than the backup used to restore the Active Directory.

Reference:

**QUESTION 15**

You are a network administrator for your company. The company consists of two subsidiaries named Litware, Inc., and Contoso, Ltd. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest contains a forest root domain.
named litwareinc.com and an additional domain tree named contoso.com, which contains two child domains. All domain controllers run Windows Server 2003.

The Directory Services object is configured with the default property settings. The forest contains 250,000 objects that are changed frequently.

You need to be able to restore objects in one of the child domains in the contoso.com domain tree from a three-month-old backup. You need to make a change to a Directory Services property on a domain controller in one of the domains in order to achieve this goal.

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

A. Run the `netdom` command on a domain controller in contoso.com.
B. Use the `Ntdsutil` utility on a domain controller in litwareinc.com.
C. Use the `ADSIEdit` utility on a domain controller in contoso.com.
D. Run the `ldp` command on a domain controller in litwareinc.com.

**Answer:** CD  

**Explanation/Reference:**

Explanation:

We need to edit a property of Active Directory. We can use a low level editor, such as `AdsiEdit` and `Ldp`, to do this. `AdsiEdit` is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for the Active Directory service. It provides a means to add, delete, and move objects within the Directory Services. The attributes of each object can be viewed, changed, and deleted. The `Ldp` is a graphical tool that allows users to perform Lightweight Directory Access Protocol (LDAP) operations, such as connect, bind, search, modify, add, and delete, against any LDAP-compatible directory, such as Active Directory. LDAP is an Internet-standard wire protocol used by Active Directory.

**Incorrect Answers:**

A: Netdom.exe is a command line to manage Windows Server 2003 domains and trust relationships.  
B: The `Ntdsutil` command-line utility performs database maintenance and clean up. However, it does not allow you to add, move, or delete objects.

**Reference:**


**QUESTION 16**

You are a network administrator for Litware, Inc. The network consists of a single Active Directory domain named sales.litwareinc.com.

The Active Directory database is contained on a Windows Server 2003 domain controller named
DC1. The hard disk that contains the Active Directory database fails.

You restart DC1 in Directory Services Restore Mode. When prompted to log on, you type administrator@sales.litwareinc.com as your user name and enter your domain password. Your logon attempt fails.

You need to log on to DC1 to complete the restore operation.

What should you do?

A. Type sales\administrator as your user name and enter your domain password.
B. Type administrator as your user name and enter the password that was associated with the local administrator account.
C. Type administrator as your user name and enter your domain password.
D. Type administrator as your user name and enter the password that you supplied during the installation of Active Directory.

Answer: D

Explanation/Reference:
Explanation:
Because you must always log on to a Windows Server 2003 computer before you can use the operating system, a small version of a local directory service database (called a SAM database) remains on the computer after it has been promoted to a DC. This database has a single account, the local administrator account. Thus you need to use administrator as the user name and enter the password that was supplied during the Active Directory installation to be able to complete the restoration.

Incorrect answers:
A: This is not the local administrator account and furthermore, the question already mentioned that the domain password does not allow you to log on when restarting in the Directory Services Restore Mode.
B: You should make use of the password that was supplied during the Active Directory installation and not the password of before the installation.
C: Entering the domain password will not allow you to complete the restoration process. The question does mention that the domain password does not allow you to log on when restarting in the Directory Services Restore Mode.

Reference:

QUESTION 17
You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory forest that contains a single domain named contoso.com. The network contains four Windows Server 2003 domain controllers. The DNS Server service is running on two Windows Server 2003 member servers in the domain.

You decide to create a new child domain named dev.contoso.com in the forest. You install Windows Server 2003 on a new server. You join the server to the contoso.com domain.
The first domain controller installed in the contoso.com domain fails because of a hardware failure. You find out that it will take several days to repair the domain controller. You decide to continue creating the new child domain. You attempt to promote the member server to a domain controller in the dev.contoso.com domain.

The promotion of the domain controller fails. You receive the following error message.

![Active Directory Installation Wizard](image)

The operation failed because:

Active Directory could not contact the domain naming master DC1.Contoso.com.

"The specified server cannot perform the requested operation."

This server has been disjoined from domain CONTOSO.

You need to resolve the error to create the new domain.

What should you do?

A. Configure the DNS client settings on the new server to use the DNS server that is authoritative for the contoso.com domain.
B. Configure the DNS server for the Contoso.com zone to have a zone named dev.contoso.com. Configure the zone for dynamic updates.
C. Configure one of the other contoso.com domain controllers to hold all of the operations master roles.
D. Configure one of the existing domain controllers as a global catalog server.

**Answer:** C  
**Section:** (none)

**Explanation/Reference:**

Explanation:
The first domain controller installed in the forest will by default, have the domain naming master operations master role. The question states that the first domain controller installed fails due to a hardware failure. This means that the forest has no domain naming master. A domain naming master is required to create additional domains in the forest. To add another domain, we need to configure one of the other testking.com domain controllers to hold at least the domain naming master role (or as the answer states, all of the operations master roles).

Incorrect Answers:
A: This is not a DNS problem.
B: This is not a DNS problem.
D: We need a domain naming master, not a global catalog server.

Reference:
Michael Cross, Jeffery A. Martin, Todd A. Walls, Martin Grasdal, Debra Littlejohn
QUESTION 18
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain with three sites named Testking1, Testking2, and Testking3. The sites and site links are configured to use Testking2 to connect Testking1 and Testking3. Each site contains three Windows Server 2003 domain controllers. A domain controller in each site is configured as a preferred bridgehead server. All user and group accounts are created in Testking1.

Several new users start work in Testking2. When they attempt to log on to the network, the logon fails. You confirm that the user accounts are created and are visible in Testking1 and Testking2. You discover that the preferred IP bridgehead server in Testking2 failed. You repair the server and confirm that replication is successful to Testking2.

You need to ensure that the failure of a single domain controller in any site will not interfere with Active Directory replication between sites.

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

A. Configure an IP site link between Testking1 and Testking3.
B. Configure two domain controllers in each site as preferred IP bridgehead servers.
C. Configure two domain controllers in each site as preferred SMTP bridgehead servers.
D. Configure each site to have no preferred bridgehead servers.
E. Configure an SMTP site link between each of the sites. Assign a cost of 200 to the SMTP site link.

Answer: BD
Section: (none)

Explanation/Reference:
Explanation:
Directory information is replicated both within and among sites. Active Directory replicates information within a site more frequently than across sites. This balances the need for up-to-date directory information with the limitations imposed by available network bandwidth.

You customize how Active Directory replicates information by using site links to specify how your sites are connected. Active Directory uses the information about how sites are connected to generate Connection objects that provide efficient replication and fault tolerance. Active Directory uses this information to determine which site link will be used to replicate information. Customizing replication schedules so replication occurs during specific times, such as when network traffic is low, will make replication more efficient.

You can further control replication behavior by specifying a bridgehead server for inter-site replicated information. The bridgehead server is a specific server you want to dedicate for inter-site replication, rather than using any server available. You can also establish a bridgehead server when your deployment uses proxy servers, such as for sending and receiving information through a firewall.

Incorrect Answers:
A: Site1 is linked to Site3 through Site2. Adding a direct site link between Site1 and Site3 will create an alternative path for replication between Site1 and Site3. This however does not address redundancy for Site2.

C, E: You can use either IP or SMTP as the protocol for replication traffic. However, SMTP replication requires an Enterprise Certification Authority (ECA) because Public Key encryption and certificates are used to verify identity of domain controllers and provide digital signatures.

Reference:
Exam C

QUESTION 1
You are the network administrator for TestKing. The network consists of a single Active Directory domain with two sites named Testking1 and Testking2. Testking1 contains two domain controllers. Testking2 contains one domain controller. Each site contains two member servers. All domain controllers are backed up every night.

Each of the domain controllers is installed with a similar hardware configuration, which includes a single processor and a single hard disk.

You create several user accounts on the domain controller in Testking2. The hard disk on that domain controller fails. You install a new hard disk on the domain controller and restore the domain controller from the most recent backup tape. You notice that the new user accounts you created on the domain controller do not appear. The only way that you can restore the user accounts is to re-create them.

You need to configure the domain controllers so that the loss of data in Active Directory is minimized during a similar hard disk failure.

What should you do?

A. Configure an existing member server as an additional domain controller in Testking2.
B. Install an additional hard disk in each domain controller. Move the Active Directory log files to the new hard disk.
C. Install an additional hard disk in each domain. Move the Active Directory database file to the new hard disk.
D. Configure a new site link between Testking1 and Testking2.

Answer: A
Section: (none)

Explanation/Reference:
Explanation:
To ensure redundancy in the Testking2 site in the event of a failure to the domain controller, we should add another domain controller to the site. We could do this by promoting one of the member servers in the Testking2 site to a domain controller.

Incorrect Answers:
B, C: The placement of the Active Directory log files or database will not ensure that the Active Directory information is available should the new hard drives fail.
D: Creating a new site link will not ensure redundancy in the Testking2 site.

Reference:

QUESTION 2
You are the network administrator for Contoso Pharmaceuticals. The network consists of a single Active Directory domain named contoso.com.
The domain contains three Windows Server 2003 domain controllers.

A domain controller named DC2.contoso.com fails because of a hardware failure. You decide not to rebuild the domain controller. However, because several applications refer to DC2.contoso.com by its NetBIOS name, you need to provide a new domain controller that has the same name.

You install a new Windows Server 2003 computer and name it DC2. You attempt to promote the server to a domain controller in the contoso.com domain. The promotion fails and you receive the following error message.

You need to install a new domain controller named DC2 in the contoso.com domain.

What should you do?

A. Use the WINS administrative console to remove all WINS records for DC2.contoso.com.
B. Use the Ntdsutil utility to remove the metadata associated with the DC2.contoso.com domain controller object from Active Directory.
C. Use Active Directory Users and Computers to remove the DC2.contoso.com domain controller computer account from the contoso.com domain.
D. Use the DNS administrative console to remove all DNS records that refer to DC2.contoso.com.

Answer: B

Explanation/Reference:
Explanation:
When DC2 failed metadata associated with the DC2 remained in Active Directory. This metadata is indicating that DC2 already exists. We must remove this metadata by using the Ntdsutil tool with the cleanup command. It removes the defunct domain controller's identification and information from the directory.

Incorrect Answers:
A, D: This is not a name resolution problem. When DC2 failed metadata associated with the DC2 remained in Active Directory.
C: Objects deleted from Active Directory remain there until the to mbstone lifetime attribute has expired. This is 60 days by default.

Reference:
QUESTION 3
You are the network administrator for TestKing.com. Your network consists of a single Active Directory domain named testking.com. All the user accounts, groups, and application servers of the human resources (HR) department are located in an organizational unit (OU) named HR.

The managers in the HR department need access to the application servers to perform administrative tasks. A local group named HRManagers exists on each application server. The HRManagers local groups supply the permissions that the HR managers require. For security reasons, the company wants user accounts for managers in the HR department to be the only members of the HRManagers groups.

You need to ensure that membership of the HRManagers group in each application server is as secure as possible.

What should you do?

A. Create a Group Policy object (GPO) that configures restricted groups for each HRManagers group. Link the GPO to the HR OU.

B. Create a new OU for application servers under the HR OU, and move the servers to the new OU. Block permissions inheritance at the new OU.

C. Create a universal group named HRManagers and make the user accounts for HR managers members of that group. Make the HRManagers universal group a member of the HRManagers local group on each application server.

D. Create a script that adds the user accounts for managers in the HR department to the HRManagers local groups. Configure the script to act as the startup and shutdown script for the application servers.

Answer: A

Section: (none)

Explanation/Reference:
Explanation:
Given the organization structure of the company and the security concerns, the way to ensure that membership of the HRManagers group in each application server is as secure as possible, you need to place restrictions on the group membership by creating a GPO that configures restricted groups for each HRManagers group and linking this GPO to the HR OU.

Incorrect answers:
B: There is no need to create a new organizational unit and applying the block permissions inheritance at the new OU when all that is necessary is to create a GPO that configures restricted groups for each HRManagers group and linking this GPO to the HR OU.
C: Universal security groups are most often used to assign permissions to related resources in multiple domains. A universal security group has the following characteristics:
   (i) Open membership - You can add members from any domain in the forest.
   (ii) Access to resources in any domain - You can use a universal group to assign permissions to gain access to resources that are located in any domain in the forest. (iii) Available only in domains with a domain functional level set to Windows 2000 native or Windows Server 2003 Universal security groups are not available in domains with the domain functional level set to Windows 2000 mixed. This is not secure enough for the purposes of this question.
D: The Membership rules for local groups include the following:
Local groups can contain local user accounts from the computer where you create the local group. Local groups cannot be members of any other group. This option is thus not a viable option in the light of the security concerns and the nature of the HRManagers group.

Reference:

**QUESTION 4**

You add eight servers for a new application. You create an organizational unit (OU) named Application to hold the servers and other resources for the application.

Users and groups in the domain will need varied permissions on the application servers. The members of a global group named Server Access Team need to be able to grant access to the servers. The Server Access Team group does not need to be able to perform any other tasks on the servers.

You need to allow the Server Access Team group to grant permissions for the application servers without granting the Server Access Team group unnecessary permissions.

What should you do?

A. Create a Group Policy object (GPO) for restricted groups. Configure the GPO to make the Server Access Team group a member of the Power Users group on each application server. Link the GPO to the Application OU.

B. Grant the Server Access Team group permissions to modify computer objects in the Application OU.

C. Move the Server Access Team group object into the Application OU.

D. Create domain local groups that grant access to the application servers. Grant the Server Access Team group permissions to modify the membership of the domain local groups.

**Answer:** D

**Section:** (none)

**Explanation/Reference:**
Explanation:
The simplest way to do this is to create domain local groups with various permissions to the application servers. For example, one group has read access, another group has read and write access and so on. We can then use the Delegation of Control Wizard to grant the right to add or remove members of the groups.

Incorrect Answers:
A: The Power Users group can perform many administrative tasks on the servers. This is more permission than necessary.
B: They don't need to modify the computer objects. This is more permission than necessary.
C: This won't give them the required permissions.
Reference:

QUESTION 5
DRAG DROP
You are the network administrator for TestKing.com. Your network consists of a single Active Directory domain named testking.com.

You are responsible for configuring Active Directory security for the domain. All groups for the domain are in an organizational unit (OU) named Groups. Resource groups will be used to provide permissions to users in accounts groups.

The human resources department needs to be able to manage the membership of only the accounts groups. The server support department needs to be able to manage the membership of only the resource groups. The Domain Admins group needs to be able to manage all groups.

You need to configure the OU structure to allow the appropriate permissions to be granted. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do?

To answer, drag the appropriate OU or OUs to the correct location or locations in the work area.
Answer:
Section: (none)

Explanation/Reference:
Explanations:
We need to create two top level OUs to delegate control of the appropriate departments to the appropriate groups. By having the OUs at the same level means that neither department will have control over the other OU.

The human resources department needs to be able to manage the membership of only the accounts groups. An OU for the accounts groups will enable us to delegate the necessary permissions to the Human Resources department.

The server support department needs to be able to manage the membership of only there source groups. An OU for the resource groups will enable us to delegate the necessary permissions to the Server Support department.

The Domain Admins group needs to be able to manage all groups. The domain admins group has permission to manage all groups in the domain.

Reference:
QUESTION 6
You are the network administrator for your company. The network consists of a single Active
Directory forest. The forest consists of 19 Active Directory domains. Fifteen of the domains contain
Windows Server 2003 domain controllers. The functional level of all the domains is Windows 2000
native. The network also consists of a single Microsoft Exchange 2000 Server organization.

You need to create groups that can be used only to send e-mail messages to user accounts
throughout the company. You want to achieve this goal by using the minimum amount of replication
traffic and minimizing the size of the Active Directory database.

You need to create a plan for creating e-mail groups for your company.

What should you do?

A. · Create global distribution groups in each domain.
   · Make the appropriate users from each domain members of the global distribution group
     in the same domain.
   · Create universal distribution groups.
   · Make the global distribution groups in each domain members of the universal distribution
     groups.

B. · Create global security groups in each domain.
   · Make the appropriate users from each domain members of the security group in the same
     domain.
   · Create universal security groups.
   · Make the global security groups in each domain members of the universal security groups.

C. · Create universal distribution groups.
   · Make the appropriate users from each domain members of a universal distribution group.

D. · Create universal security groups.
   · Make the appropriate users from each domain members of a universal security group.

Answer: A
Section: (none)

Explanation/Reference:
Explanation:
We can minimize replication traffic by placing the users into Global groups, and then place the
Global groups into Universal groups. In Active Directory, a Universal group lists all its members. If
the Universal group contained user accounts, and a user account was added or removed, then the
Universal group information would be replicated throughout the forest. This is why placing user
accounts directly into Universal groups are not recommended. In addition, we need to use
Distribution groups for email groups.

Incorrect Answers:
B: We to use Distribution groups for email groups, not security groups.
C: We should not place user accounts directly into Universal groups as we want to reduce replication
traffic.
D: We should not place user accounts directly into Universal groups as we want to reduce replication
traffic. Furthermore, we to use Distribution groups for email groups, not security groups.

Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003
QUESTION 7
You are the network administrator for TestKing.com. The network structure is shown in the exhibit.

The functional level of both forests is Windows Server 2003. All three domains are Active Directory domains.

Domain3 contains a computer named Server1. A shared folder on Server1 is named Share1. Users in an organizational unit (OU) named Accounts in Domain2 need access to Share1. However, whenever the users in the Accounts OU attempt to connect to Share1, they receive an error message stating that access was denied.

You need to ensure that users in the Accounts OU can connect to Share1.

What should you do?

Exhibit:

A. Create a universal distribution group in Domain2 that includes all users in the Accounts OU. Create a domain local security group in Domain3. Grant access to \Server1\Share1 to the domain local security group. Make the universal distribution group a member of the domain local security group.
B. Create a global security group in Domain2 that includes all users in the Accounts OU. Create a domain local security group in Domain3. Grant access to \Server1\Share1 to the domain local security group. Make the global security group a member of the domain local security group.
C. Create a shared folder in the Accounts OU for \Server1\Share1.
D. Create a one-way external trust relationship in which Domain2 trusts Domain3.
**Answer:** B

**Section:** (none)

**Explanation/Reference:**
Explanations: In this scenario, there is a forest trust between the two forests. The users in the Accounts OU get an access denied error when trying to connect to share1 on the server named server1. This is a simple permissions problem. All we need to do is to assign the appropriate permissions to the accounts users to access share1. The recommended way of assigning permissions is to create a domain local security group and assign the group permissions to the resource, \server1\share1 in this case. Then we need to group together the accounts users by adding the user accounts to a domain global security group. We then grant the permissions by adding the domain global group to the domain local group.

Incorrect Answers:
A: This would work, but a universal group isn't recommended. We can use a global group in this case, so a universal group isn't necessary.
C: The shared folder is in another domain, so this solution wouldn't work.
D: There is a forest trust between the two forests, so there is no need to create another trust relationship.

Reference:

**QUESTION 8**
You are the network administrator for Consolidated Messenger. The network consists of a single Active Directory forest that contains three domains named consolidatedmessenger.com, child1.consolidatedmessenger.com, and child2.consolidatedmessenger.com. The functional level of the forest is Windows Server 2003.

Both the child1.consolidatedmessenger.com domain and the child2.consolidatedmessenger.com domain contain user accounts of users in the accounting department. All accounting users need to access resources in both child domains.

You need to ensure that all accounting users can access the appropriate resources. You want to restrict administrators in the child domains to managing the access requirements for user accounts in their domain. You also want to minimize global catalog replication.

What should you do?

A. · Create a global group named All_Accounting in each child domain.
   · Add all user accounts for accounting users in a domain to the All_Accounting group for that domain.
   · Create a universal group in the consolidatedmessenger.com domain.
   · Add both All_Accounting groups to the universal group.

B. · Create a global group named All_Accounting in each child domain.
   · Add all user accounts for accounting users in a domain to the All_Accounting group for that domain.
Create a domain local group in the consolidatedmessenger.com domain.
Add both All_Accounting groups to the domain local group.

C. Create a universal group in the consolidatedmessenger.com domain.
Add all user accounts for accounting users in both child domains to the universal group.

D. Create a domain local group in the consolidatedmessenger.com domain.
Add the user accounts for accounting users in both child domains to the domain local group.

Answer: A

Section: (none)

Explanation/Reference:
Explanation:
The recommended practice for group membership is to use domain local groups to control access to resources and use global groups to organize similar groups of users. The global groups can then be applied to the domain local groups as members, allowing those users permissions to those resources. Global groups can be added to universal groups which limits the effect that replication has on a network environment.

Incorrect Answers:
B, D: A domain local group can have members from any domain in the forest but can only be assigned permissions to resources that are local to that domain.
C: You should not place users into universal groups as this doesn't reduce the amount of replication of objects to the Global Catalog. Instead, universal groups should be used to hold global groups with common requirements.

Reference:
Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 4-21 to 4-23, 4-26 to 4-30

QUESTION 9

TestKing is adding 15 new servers to run a new application. TestKing is also adding an organizational unit (OU) named Application to hold the servers and other resources for the application.

The server access team needs to be able to grant various types of access to the servers. The server access team does not need to be able to perform any other tasks on the servers.

You need to allow the server access team to grant permissions for application servers without granting the team unnecessary permissions.
What should you do?

A. Create a Restricted Groups Group Policy object (GPO) to make the server access team a member of the Power Users group on each application server. Link the GPO to the Application OU.
B. Grant the server access team permission to modify computer objects in the Application OU.
C. Make the server access team a member of the Server Operators group.
D. Create Domain Local security groups that grant the appropriate access to the servers.
   Grant the server access team permission to modify the membership of the Domain Local security groups.

Answer: D

Explanation/Reference:
Explanation:
The server access team needs to grant various types of access to the servers therefore we need to place them in a security group. This would need to be a domain local group.

Incorrect Answers:
A, C: This would provide them with too much administrative control.
B: The server access team needs to grant access to the servers, they do not need to modify the computer objects for the Application OU.

Reference:

QUESTION 10

The Graphic Design Institute network consists of a single Active Directory forest that contains a single domain named graphicdesigninstitute.com.

Users in the litwareinc.com domain require access to file and print resources stored on a computer named server1.graphicdesigninstitute.com.

Users in the graphicdesigninstitute.com domain require access to all computers in the litwareinc.com forest.

You must provide administrators with the ability to grant users access to the required resources.

What should you do?
A. Create a two-way forest trust relationship between the litwareinc.com domain and the graphicdesigninstitute.com domain.
   In the litwareinc.com domain, enable forest-wide authentication for the graphicdesigninstitute.com domain.
   In the graphicdesigninstitute.com domain, enable selective authentication for the litwareinc.com domain.

B. Create a two-way external trust relationship between the litwareinc.com domain and the graphicdesigninstitute.com domain.

C. Create a one-way forest trust relationship in which the graphicdesigninstitute.com domain trusts the litwareinc.com domain.
   In the litwareinc.com domain, enable forest-wide authentication for the graphicdesigninstitute.com domain.

D. Create a one-way external trust relationship in which the litwareinc.com domain trusts the graphicdesigninstitute.com domain.
   Create a second incoming external trust relationship on the graphicdesigninstitute.com domain.
   Specify that the trust relationship is between the dev.litwareinc.com domain and the graphicdesigninstitute.com domain.

Answer: A
Section: (none)

Explanation/Reference:
Explanation:
When all domains in two forests trust each other and need to authenticate users, establish a forest trust between the forests. When only some of the domains in two Windows Server 2003 forests trust each other, establish one-way or two-way external trusts between the domains that require interforest authentication.

Using Active Directory Domains and Trusts, you can determine the scope of authentication between two forests that are joined by a forest trust.

You can set selective authentication differently for outgoing and incoming forest trusts. With selective trusts, administrators can make flexible forest-wide access control decisions.

If you use forest-wide authentication on an incoming forest trust, users from the outside forest have the same level of access to resources in the local forest as users who belong to the local forest.

Incorrect Answers:
B, D: We have two separate forests here. We would require a forest trust relationship between them.
C: Users in the testking.com domain require access to the graphicdesigninstitute.com domain. We will thus need the graphicdesigninstitute.com domain to trust the testking.com domain.

Reference:
QUESTION 11
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 company's written security policy requires the following account policies:

- User accounts must be automatically locked out in the event of three consecutive failed logon attempts within a 30-minute period.
- Manual administrative action must be required to unlock a user account.

You need to configure the account policies for the domain to comply with the security requirements.

What should you do?

To answer, drag the appropriate account policy setting or settings to the correct location or locations in the work area.

Answer:
**Explanation/Reference:**

**Explanation:**
The Account lockout duration security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

The Account lockout threshold security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

The Reset account lockout counter after security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes.

**Reference:**

**QUESTION 12**
You are the network administrator for TestKing.com. Your network consists of a single Active Directory domain named testking.com. You work in the corporate IT department.

TestKing consists of 12 business divisions. Each business division has its own top-level organizational unit (OU) in the domain. Each business division is responsible for managing its own OU structure. The OU of each division includes an administrative group for that division.

Members of each administrative group have the Allow - Read permission for their division's OU object and the Allow - Full Control permission for all child objects of the OU structure of only their own division. The administrators of each division must be approved by the members of the Domain Admins group.

You need to prevent administrators of individual divisions from adding additional administrators in their administrative group. You need to ensure that members of the Domain Admins group are able to manage those groups.

**What should you do?**

A. Create a new OU under the OU of each division. Move the appropriate administrative groups into the new OUs. Block the inheritance of permissions. When prompted, remove permissions applied from the parent.
B. Assign the Domain Admins group the Allow - Full Control permission for the administrative groups in the OU of each division.
C. Create a new OU at the same level in the OU structure as the OUs of the individual divisions.
Move all the administrative groups of the divisions into the new OU.
D. Create a Restricted Groups Group Policy object (GPO) and link the GPO to the OU of each division.

Answer: C
Section: (none)

Explanation/Reference:
Explanation:
We need to ensure that members of the Domain Admins group are able to manage the business divisions OUs and we need to prevent administrators of individual divisions from adding additional administrators in their administrative group. We can accomplish this by placing the administrative groups of the divisions into a top-level OU that is managed by the Domain Admins group.

Incorrect Answers:
A: Creating an OU under each division will make the new OU a child OU of the business division. This will allow the administrators of the division to manage the new OU.
B: Assigning the Domain Admins group the Allow - Full Control permission for the administrative groups in the OU of each division won't prevent the division administrators from also managing the OU.
D: Creating a Restricted Groups Group Policy object (GPO) and link the GPO to the OU of each division will prevent the administrators from adding more administrators to their administrative groups but this won't allow the Domains Admins group from managing the administrative groups.

Reference:

QUESTION 13
You are the network administrator for your company. The network consists of a single Active Directory domain. The company contains several departments. One of these departments is sales. A group named Sales Admins is responsible for administering the sales department. In addition, the sales department has two teams that are responsible for daily support. One of these teams supports the sales department's user accounts. The other team supports the sales department's computers.

Each department in the company has a specific set of Group Policy objects (GPOs). The sales department has two additional sets of GPOs. One set of GPOs is for user accounts. The other set of GPOs is for computers.

You need to configure the organizational unit (OU) structure to support the implementation of GPOs and delegation of security for the sales department. You want to accomplish this task by using the minimum amount of administrative effort.

How should you configure the OU structure?

To answer, drag the appropriate OU or OUs to the correct location or locations in the work area.
Answer:

Section: (none)

Explanation/Reference:
Explanation:
The Sales OU has two additional GPOs: one for User accounts and one for computer. Therefore we need a two level OU structure with the Sales OU as the parent OU and the Accounts OU and Computers OU being child OUs.

Reference:

QUESTION 14
You are the network administrator for Consolidated Messenger. The network consists of a single Active Directory forest that contains three domains named consolidatedmessenger.com, child1.consolidatedmessenger.com, and child2.consolidatedmessenger.com. The functional level of the forest is Windows Server 2003.

Both child1.consolidatedmessenger.com and child2.consolidatedmessenger.com contain employee user accounts, client computer accounts, and resource server computer accounts. The domain named consolidatedmessenger.com contains only administrative user accounts and computer accounts for two domain controllers. Each resource server computer provides a single service of file server, print server, Web server, or database server.

Your company plans to use Group Policy objects (GPOs) to centrally apply security settings to resource server computers. Some security settings need to apply to all resource servers and must not be overridden. Other security settings need to apply to specific server roles only.

You need to create an organizational unit (OU) structure to support the GPO requirements. You want to create as few GPOs and links as possible.

What should you do?

A. · Create a top-level OU for each server role under the consolidatedmessenger.com domain.
   · Create a top-level OU named Servers under the child1.consolidatedmessenger.com domain.
   · Create a top-level OU named Servers under the child2.consolidatedmessenger.com domain.

B. · Create a top-level OU named Servers under the child1.consolidatedmessenger.com domain.
   · Create a child OU for each server role under the Servers OU.
   · Create a top-level OU named Servers under the child2.consolidatedmessenger.com domain.
   · Create a child OU for each server role under the Servers OU.

C. · Create a top-level OU named Servers under the consolidatedmessenger.com domain.
   · Create a child OU for each server role under the Servers OU.

D. · Create a top-level OU for each server role under the child1.consolidatedmessenger.com domain.
   · Create a top-level OU for each server role under the child2.consolidatedmessenger.com domain.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
With a top-level OU named Servers, we can apply group policies to all the resource servers. With child OUs for each server role, we can apply group policies to individual server roles. Two domains have resource servers, child1.consolidatedmessenger.com domain and child2.consolidatedmessenger.com domain. We need to create the OU structure in each of these
two domains.

Incorrect Answers:
A: We need an OU for each server role in child1.consolidatedmessenger.com domain and child2.consolidatedmessenger.com domain, because the resource servers are in those domains.
C: We need a top level OU for all the resource servers in child1.consolidatedmessenger.com domain and child2.consolidatedmessenger.com domain, so we can apply group policies to all the servers.
D: We need a top level OU for all the resource servers in child1.consolidatedmessenger.com domain and child2.consolidatedmessenger.com domain, so we can apply group policies to all the servers.

Reference:

**QUESTION 15**
You are the network administrator for your company. The network consists of a single Active Directory domain.

The following table shows the types and quantities of Windows Server 2003 Web and database servers in the domain.

<table>
<thead>
<tr>
<th>Server type</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonproduction test Web server</td>
<td>2</td>
</tr>
<tr>
<td>Nonproduction test database server</td>
<td>2</td>
</tr>
<tr>
<td>Production Web server</td>
<td>10</td>
</tr>
<tr>
<td>Production database server</td>
<td>10</td>
</tr>
</tbody>
</table>

The computer accounts for the Web and database servers are located in the default Computers container. The domain also includes many organizational units (OU) that contain other computer accounts.

Your company plans to use Group Policy objects (GPOs) to centrally apply security settings to the Web and database server computers. The settings need to be applied as follows:

- Some security settings need to apply to all Web and database servers.
- Some security settings need to apply to the nonproduction servers only.
- Some security settings need to apply to the production servers only and must not be overridden.
- Other security settings need to apply to specific server types only.

You need to create an organizational unit (OU) structure to support the GPO requirements. You want to create as few GPOs and links as possible while using only the default security permissions for GPO links. You also want to limit the number of GPO links to one link per GPO.
What should you do?

A. · Create two top-level OUs named Web and Database under the domain.
   · Create two child OUs named Nonproduction and Production under both the Web OU
     and the Database OU.
B. · Create two top-level OUs named Nonproduction and Production under the domain.
   · Create two child OUs named Web and Database under both the Nonproduction OU
     and the Production OU.
C. · Create a top-level OU named Servers under the domain.
   · Create two child OUs named Web and Database under the Servers OU.
   · Create two child OUs named Nonproduction and Production under both the Web OU
     and the Database OU.
D. · Create a top-level OU named Servers under the domain.
   · Create two child OUs named Nonproduction and Production under the Servers OU.
   · Create two child OUs named Web and Database under both the Nonproduction OU
     and the Production OU.

**Answer:** D

**Section:** (none)

**Explanation/Reference:**

Explanation:

We need some setting to apply to all web servers and database servers, and then we need some
settings that apply only to the non-production servers and some settings that apply only to the
production servers - settings that are applied to the production servers must not be overwritten. In
addition, we have other settings that apply to different server types. The other settings thus apply
only to the server types. Thus, we need three levels - a top level that contains all servers; a middle
level that contains production servers and non-production servers, and a bottom level that contains
server types (one for web servers and one for database servers).

Incorrect Answers:

A, B: The top-level OU should contain all servers.
C: The server types OU must be at the lowest level because the other settings would apply only to
them and should not be inherited. Inheritance is from parent to child.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003
Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 6-3 to 6-9, 6-16 to
6-23

**QUESTION 16**

You are the network administrator for a company that has two locations, New York and Singapore.
The company is installing an Active Directory forest that consists of a single domain.

The company's departments are divided into two main divisions named Operations and Support.
The local IT staff at each location is responsible for user support at their location, regardless of the
user's division. The research and development (R&D) department has its own IT support staff. The
R&D department maintains its own IT support staff regardless of location.

You need to plan a top-level organizational unit (OU) structure that facilitates delegation of
administrative control.

Which top-level OU or OUs should you create?

To answer, drag the appropriate top-level OU or OUs to the correct location or locations in the work area.

Answer:
Explanation/Reference:
Explanation:
The local IT staff at each location is responsible for user support at their location, regardless of the user's division. An OU for each location will enable the local IT staff to manage resources in that location (except for R&D resources).

The research and development (R&D) department has its own IT support staff. The R&D department maintains its own IT support staff regardless of location. An OU for R&D resources will enable the R&D support staff to manage the R&D resources.

Reference:

QUESTION 17
You are the network administrator for your company. The network consists of a single Active Directory domain.

The company's written domain administration policy requires that help desk employees must have the ability to reset passwords. The help desk employees must be able to reset passwords for all user accounts except for members of the Domain Admins global group and members of the
Executives global group. The help desk employees must not have any other administrative rights in the domain.

All help desk employees are members of the Help Desk global group.

All members of the Domain Admins group are located in an organizational unit (OU) named AdminsOU. All members of the Executives group are located in an OU named ExecutiveOU. All other user accounts are located in an OU named EmployeesOU. The relevant portion of the OU design for the domain is shown in the exhibit. (Click the Exhibit button.)

You need to configure the permissions for the help desk employees as defined by the written domain administration policy.

What should you do?

Exhibit:

A. Assign the Help Desk global group the right to reset passwords in the OU named EmployeesOU.
B. Assign the Help Desk global group the right to manage user accounts in the OU named AllUsersOU. Block the inheritance of permissions at the OU named AdminsOU and the OU named ExecutiveOU.
C. Assign the Help Desk global group the right to reset passwords in the OU named AllUsersOU.
D. Assign the Help Desk global group the right to manage user accounts at the domain level. Deny the help desk employees the right to reset passwords in the OU named AdminsOU and the OU named ExecutiveOU.

Answer: A
Section: (none)
Explanation/Reference:

Explanation:
The user accounts that the Help Desk group need to reset passwords for are located in an OU named EmployeesOU. We can simply delegate the "Reset Passwords" permission on the EmployeesOU.

Incorrect Answers:
B: The right to manage user accounts will enable the Help Desk group to do more than just reset the passwords.
C: The All UsersOU contains all user accounts. This would enable the Help Desk group to reset passwords on all user accounts including the domain admins and executives.
D: The right to manage user accounts will enable the Help Desk group to do more than just reset the passwords.

Reference:

QUESTION 18
You are a network administrator for your company. The company has one main office and 11 branch offices. The network consists of a single Active Directory domain. The domain contains an organizational unit (OU) named BranchOffices. The BranchOffices OU contains an OU for each of the 11 branch offices.

The network administrators who administer the branch offices are members of the BranchOffice Admins global group. You delegate full control of all child objects in the BranchOffices OU to the BranchOffice Admins group.

The company's written security policy states the following requirements:

· Members of the BranchOffice Admins group must have the right to modify the assignment of Group Policy objects (GPOs) for the individual branch office OUs.
· Members of the BranchOffice Admins group must not be able to block the inheritance of GPOs at the individual branch office OUs.
· Members of the BranchOffice Admins group must not be able to modify any GPO settings at the BranchOffices OU level.

You need to configure the delegation of the administration of GPOs as defined by the written security policy. You must also ensure that you do not remove more permissions than is necessary from the BranchOffice Admins group.

What should you do?

A. · Modify the permissions granted to the BranchOffice Admins group so that the group is denied permission to write the gPOptions attribute at the BranchOffices OU level.
   · Configure the permission to apply to the BranchOffices OU and all child objects.
B. · Modify the permissions granted to the BranchOffice Admins group so that the group is granted permission to read and write the gPOptions attribute at the BranchOffices OU level.
· Configure the permission to apply to child objects of the BranchOffices OU only.
C. · In the Group Policy Management Console (GPMC), remove the BranchOffice Admins group from the **Permissions** tab for the BranchOffices OU.
   · Add the BranchOffice Admins group to the LinkGPOs permission in the **Delegation** tab for the BranchOffices OU.
   · Configure the permissions to apply to the BranchOffice Admins container only.
D. · In the Group Policy Management Console (GPMC), remove the BranchOffice Admins group from the **Permissions** tab for the BranchOffices OU.
   · Add the BranchOffice Admins group to the LinkGPOs permission in the **Delegation** tab for the BranchOffices OU.
   · Configure the permissions to apply to the BranchOffice Admins container and all child containers.

**Answer:** A

**Section:** (none)

**Explanation/Reference:**

**Explanation:**
We need to restrict the administrative abilities of the BranchOffice Admins group at the Branch level. The gPOptions attribute indicates whether the Block Policy Inheritance option of a domain or OU is enabled. Denying the BranchOffice Admins group permissions to this attribute will prevent them from being able to block the inheritance of GPOs at the individual branch office OUs.

**Incorrect Answers:**
B: We must deny the BranchOffice Admins group permissions to the gPOptions attribute.
C, D: The BranchOffice Admins group must be able to administrate at the branch level. We should not remove them from the Delegation tab for the BranchOffices OU.

**Reference:**
Exam D

QUESTION 1

The help desk department is responsible for resetting passwords for all user accounts in the forest except for accounts that have administrative privileges. There is an organizational unit (OU) named Corp_Users in each domain that contains the user accounts in that domain. All of the user accounts that have administrative privileges are in the default Users container in each domain.

There is a universal group named HD_Users in the adatum.com domain. All user accounts for the help desk department users are members of the HD_Users group. You need to delegate the required authority for resetting passwords to the users in the help desk department.

For which Active Directory component or components should you delegate control?

To answer, select the appropriate component or components in the work area.

Answer:
We need to delegate the required authority for resetting passwords for the Corp_UsersOU to the HD_Users universal group. The Corp_Users OU in each domain contains the users that the help desk staff need to reset passwords for. The HD_Users universal group contains the help desk staff and is visible to all domains in the forest.

Reference:

QUESTION 2
You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory domain. All servers run Windows Server 2003. The organizational unit (OU) structure is shown in the exhibit. (Click the Exhibit button.)

The File Servers OU subtree contains 20 file and print servers. All of the company's user accounts are in the User Accounts OU subtree. The company uses Group Policy objects (GPOs) linked to OUs within the User Accounts OU subtree to configure the users' environment. These GPOs are
configured to install desktop utilities for all user accounts. The desktop utilities are for use on only client computers.

You are responsible for planning and implementing the Group Policy infrastructure for the company. The company wants to apply a new GPO named ServerSecurity to the 20 file and print servers. The ServerSecurity GPO includes computer configuration settings and user configuration settings. These settings will be used to secure the file and print servers.

You plan to apply the ServerSecurity GPO to the File Servers OU. You need to ensure that the desktop utilities are not installed on the servers when users log on to the network.

What should you do?

Exhibit:

A. Grant the file and print servers permissions to link GPOs at the File Servers OU.
B. Configure the ServerSecurity GPO to enable the Loopback policy.
C. Configure a shutdown script that refreshes the computer configuration settings for the file and print servers.
D. Apply the ServerSecurity GPO at the site level rather than at the OU level.

Answer: B

Section: (none)

Explanation/Reference:

Explanation:
You don't want the user's settings applying the Desktop utilities so you must also configure the Replace Mode. You do not want the users settings applied at all in this case. If user settings were allowed to apply, then the Desktop utilities would get installed. In some cases, this processing order may not be appropriate (for example, when you do not want applications that have been assigned or published to the users in their OU to be installed while they are logged on to the computers in some specific OU).

Incorrect Answers:
A: This is not possible.
C: Shutdown scripts are applied when the computer shuts down. This won't prevent the user settings from being applied when a user logs on to the computer.
D: This won't prevent the user settings from being applied when a user logs on.

Reference:

QUESTION 3
You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory domain named contoso.com. All servers run Windows Server 2003. You are planning the implementation of new Group Policy objects (GPOs).

The accounting department and the research department each has its own organizational unit (OU). The accounting department includes the accounts payable (AP) department and the accounts receivable (AR) department. The Accounting OU contains an AP OU and an AR OU. User accounts are in the Accounting, AP, AR, and Research OUs.

The accounting department has an accounting application that must be installed on the computers that are used by users in the accounting department. You want to avoid installing the accounting application on the computers of any other users. You plan to create a GPO named Software to install the accounting application.

The research department's user accounts must have passwords that are at least eight characters in length and must be changed every 30 days. There are no specific password requirements for any other users in the contoso.com domain. You plan to create a GPO named Password to configure the minimum password length and password age.

You need to decide the correct locations for placing the Password GPO and the Software GPO, while minimizing the time it takes for any user to log on to the domain.

Where should you link the Password GPO and the Software GPO?

To answer, drag the appropriate GPO or GPOs to the correct location or locations in the work area. If both policies need to be linked to the same location, use the source labeled Both GPOs.
### GPOs

<table>
<thead>
<tr>
<th></th>
<th>Software GPO</th>
<th>Password GPO</th>
<th>Both GPOs</th>
</tr>
</thead>
</table>

### Active Directory

![Active Directory Diagram]

---

**Section:** (none)

**Explanation/Reference:**

**Explanation:**
The accounting department has an accounting application that must be installed on the computers that are used by users in the accounting department. You want to avoid installing the accounting application on the computers of any other users. You plan to create a GPO named Software to install the accounting application. The software GPO can be applied to the Accounting OU. This GPO will also apply to the AP and AR OUs (which also contain accounts users).

The research department user accounts must have passwords that are at least eight characters in length and must be changed every 30 days. There are no specific password requirements for any other users in the testking.com domain. You plan to create a GPO named Password to configure the minimum password length and password age. Password policies for domain user accounts must be applied at the domain level. The policies will have no effect on domain user accounts if they are applied at any other level.
QUESTION 4
You are the network administrator for a bank that has a main office and many small branch offices. The bank's network consists of a single Active Directory domain. All servers run Windows Server 2003. The domain has an organizational unit (OU) for each branch office. Group Policy objects (GPOs) linked to these OUs are used to configure bank resources.

Under each branch office's OU, there is an OU named UserAccounts that contains user accounts and an OU named Workstations that contains client computer accounts. A single administrative user at each branch office provides desktop support and administration for the branch office.

The number of support calls for the branch office administrators recently increased because users are making configuration changes to their computers.

You need to restrict desktop features and administrative tools for all users except the administrative user in each branch office. You create a GPO that applies the desktop restrictions.

What else should you do?

A. Link the GPO to each branch office's Workstations OU.
   Create an OU underneath each branch office's Workstations OU and move the administrative user's computer account into the new OU.
   Block GPOs from applying to the new OU.
B. Link the GPO to each branch office's UserAccounts OU.
   Create an OU underneath each branch office's UserAccounts OU and move the administrative user's account into the new OU.
   Block GPOs from applying to the new OU.
C. Link the GPO to each branch office's Workstations OU.
   Filter the GPO on the administrative user's computer for each branch office, so that the computer does not apply the new GPO.
D. Link the GPO to each branch office's UserAccounts OU.
   Filter the GPO on the administrative user's account for each branch office, so that the user account does not apply the new GPO.

Answer: D
Section: (none)

Explanation/Reference:
Explanation:
We need to restrict desktop features and administrative tools for all users other than the administrative user in each branch office. We have already created a GPO that applies the desktop restrictions. We now need to link the GPO to each branch office's UserAccounts OU which contains all user accounts for the branch. We can ensure that this GPO doesn't apply to the administrator by assigning the Deny -Apply Group policy to the administrator account in each branch.

Incorrect Answers:
A, C: The GPO must be linked to the users not the computers.
B: Simply assigning the Deny -Apply Group policy to the administrator account will ensure that the administrator can't have the GPO settings.

Reference:

QUESTION 5
You are the network administrator for Humongous Insurance. The network consists of a single Active Directory domain named humongousinsurance.com. All servers run Windows Server 2003. All servers that are not domain controllers are located in an organizational unit (OU) named Servers. All user accounts are located in an OU named Accounts.

The health insurance department has servers that store the medical records of customers. These records servers contain information that must be closely monitored. A non-Microsoft auditing tool is installed on the records servers to monitor that information. Access to the auditing information is available only to a small number of local user accounts on each record server. For legal reasons, the health insurance department needs to change its account lockout and password settings for the local user accounts on records servers.

You need to ensure that the records servers adhere to the security requirements. You want to accomplish this task by using the minimum amount of administrative effort.

What should you do?

A. · Create a new domain under the humongousinsurance.com domain. Make the records servers members of the new domain.
   · Create a Group Policy object (GPO) that contains the account lockout and password settings.
   · Link the GPO to the new domain.
B. · Create a new domain under the humongousinsurance.com domain. Make the health insurance user accounts members of the new domain.
   · Create a Group Policy object (GPO) that contains the account lockout and password settings.
   · Link the GPO to the new domain.
C. · Create a new OU under the Servers OU. Make the records servers members of the new OU.
   · Create a Group Policy object (GPO) that contains the account lockout and password settings.
   · Link the GPO to the new OU.
D. · Create a new OU under the Accounts OU. Make the health insurance user accounts members of the new OU.
   · Create a Group Policy object (GPO) that contains the account lockout and password settings.
   · Link the GPO to the new OU.

Answer: C
Section: (none)

Explanation/Reference:
Explanation:
We need to move the records servers to a new OU to that we can easily apply settings to them by using a GPO. Account lockout and password settings for domain user accounts must be applied at domain level. However, for this question, we need to configure the account lockout and password
settings for the local user accounts. We can do this by linking a GPO to an OU containing the records servers.

Incorrect Answers:
A: It is not necessary to create a new domain because we need to configure settings for local user accounts, not domain user accounts.
B: It is not necessary to create a new domain because we need to configure settings for local user accounts, not domain user accounts.
D: We need to configure the account lockout and password settings for the local user accounts. The local user accounts are not objects in Active Directory and so cannot be moved to an OU.

Reference:

QUESTION 6
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain with two sites. The two sites are named Testking1 and Testking2. TestKing has two offices, and each office is configured as one of the sites. All servers run Windows Server 2003.

The two offices are connected by a 256-Kbps leased line. In addition, Testking1 and Testking2 are connected by a site link. Testking1 has 1,000 users and Testking2 has 15 users. There are no domain controllers in Testking2.

You create a Group Policy object (GPO) to redirect the My Documents folder. You link the GPO to the domain. Users in Testking1 have their folders redirected successfully, but users in Testking2 do not.

You need to ensure that users in Testking2 have their folders redirected.

What should you do?
A. Combine Testking1 and Testking2 into a single site.
B. Enable loopback processing in Merge mode in the GPO.
C. Remove the link for the GPO from the domain. Link the GPO to Testking1 and to Testking2.
D. Create a new GPO that disables Group Policy slow link detection. Link the new GPO to Testking2.

Answer: D
Section: (none)

Explanation/Reference:
Explanation:
The users in TestKing2 receive their GPOs from domain controllers in TestKing1.
The bandwidth of the link between the two sites is less than 500Kbps which is the 'slow link' threshold. Therefore, if slow link detection is enabled, the policy won't apply. To apply the policy to users in TestKing2, we need to disable slow link detection.

Incorrect Answers:
A: Combining the two sites will make administration more complex.
B: Merge mode merges the user's normal policy settings and the loopback settings. This is not
relevant to this scenario.
C: Linking the GPO at the OU level won't accomplish anything because the GPO is applied to the domain already.

Reference:

QUESTION 7
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain with two sites. The two sites are named Testking1 and Testking2. All servers run Windows Server 2003.

TestKing has two offices, and each office is configured as one of the sites. A 256-Kbps leased line connects the two offices. In addition, a site link connects the two sites. The site link is configured to replicate during off-peak hours.

There are domain controllers in both sites. Testking1 contains all of the operations master role holders.

You plan to create Group Policy objects (GPO) for each site. Some GPOs will be used to resolve potential support issues for a specific site, and you need to minimize any delay in the propagation of GPOs.

You need to ensure that GPOs are applied to users in the appropriate site with minimal delay.

What should you do?

A. Configure the Group Policy Object Editor and Active Directory Users and Computers snap-ins to connect to the infrastructure master.
B. Configure the Group Policy and Active Directory snap-ins to connect to a domain controller in the site where the GPO must be applied.
C. Create a remote procedure call (RPC) connection object between the two sites.
D. Create a GPO that disabled Group Policy slow link detection. Link the GPO to both sites.

Answer: B

Section: (none)

Explanation/Reference:
Explanation:
Creating the GPO on a domain controller in a particular site will apply the GPO much quicker than if the GPO were created on a domain controller in a different site across a site link. This is because no replication will need to occur for the settings to take effect.

Incorrect Answers:
A: We need to apply the GPOs to the domain controllers in the site where the GPO is required, not the infrastructure master.
C, D: We need apply the GPO with minimal delay. The quickest way to apply the GPO is to apply it to the domain controller in the site where the GPO is required. This can be done by configuring the Group Policy and Active Directory snap-in to connect to a domain controller in the site where the
GPO must be applied.

Reference:

QUESTION 8
You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003.

The user accounts for support staff users are located in an organizational unit (OU) named Support. All other user accounts are located in an OU named UserAccounts. As the company expands, user accounts for users other than support staff might be created in OUs other than the UserAccounts OU.

A written company policy states that all users, including support staff, must comply with the following rules:

· Users are not allowed to use offline files.
· Only support staff employees are allowed to edit the registry.

The written policy also states that any changes to these rules must be applied to the entire company as quickly as possible.

You need to enforce the written company policy by using the minimum amount of administrative effort.

Which action or actions should you take, and where should you take the action or actions?

To answer, drag the appropriate action or actions to the correct location or locations in the work area.
Possible Actions

- Link a GPO that disables the **Disable registry editing tools** setting.
- Link a GPO that enables the **Prevent use of offline files folder** setting.
- Link a GPO that enables the **Disable registry editing tools** setting.
- Block policy inheritance.

Targets

**Domain**

- Drag action here
- Drag action here

**Support OU**

- Drag action here
- Drag action here

**User Accounts OU**

- Drag action here
- Drag action here
**Possible Actions**

- Link a GPO that disables the **Disable registry editing tools** setting.
- Link a GPO that enables the **Prevent use of offline files folder** setting.
- Link a GPO that enables the **Disable registry editing tools** setting.
- Block policy inheritance.

**Targets**

**Domain**

- Link a GPO that enables the **Disable registry editing tools** setting.
- Link a GPO that enables the **Prevent use of offline files folder** setting.

**Support OU**

- Link a GPO that disables the **Disable registry editing tools** setting.

**User Accounts OU**

- Drag action here
- Drag action here
**Section**: (none)

**Explanation/Reference**:  
**Explanation:**
All users, including support staff, are not allowed to use offline files and only support staff employees are allowed to edit the registry. This means we need an OU at the domain level that disables the registry editing tools, and one that prevents the use of offline tools. These GPOs will ensure that all users, including support staff, are not allowed to use offline files. It will also disable the use of registry editing tools for all users. Therefore, we need another GPO that allows the use of the registry editing tools for the Support OU. GPOs are applied at the domain level before the OU level so the GPO applied at the OU level will override the GPO applied at the domain level.

**Reference:**

**QUESTION 9**
You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. Each department in the company has an organizational unit (OU) for all its resources and accounts.

The company has a desktop support team that provides support to all departments. A separate team creates Group Policy objects (GPOs) for the desktop support staff to use. The GPO creation team is not allowed to link the GPO to any departmental OUs. The desktop support staff is allowed to use the GPOs created by the GPO creation team with departmental OUs. If members of the desktop support staff need a GPO that does not exist, they can request it, but they are not allowed to create any GPOs.

You need to ensure that the appropriate teams are granted the appropriate permissions.

What should you do?

To answer, drag the appropriate action or actions to the correct location or locations in the work area.
Possible Actions

Make users members of Group Policy Creator Owners.

Assign the **Allow - Read** and the **Allow - Write** permissions to the `gPLink` property of the departmental OUs.

Assign the **Allow - Read** and the **Allow - Write** permissions to the `gPOptions` property of the departmental OUs.

Work Area

**GPO creation team**

- Drag action here

**Support staff**

- Drag action here

- Drag action here

Answer:

Possible Actions

Make users members of Group Policy Creator Owners.

Assign the **Allow - Read** and the **Allow - Write** permissions to the `gPLink` property of the departmental OUs.

Assign the **Allow - Read** and the **Allow - Write** permissions to the `gPOptions` property of the departmental OUs.

Work Area

**GPO creation team**

- Make users members of Group Policy Creator Owners.

- Assign the **Allow - Read** and the **Allow - Write** permissions to the `gPLink` property of the departmental OUs.

- Drag action here

**Support staff**

- Assign the **Allow - Read** and the **Allow - Write** permissions to the `gPOptions` property of the departmental OUs.
QUESTION 10
You are the network administrator for your company. The network consists of a single Active Directory domain with three sites. There is a domain controller at each site. All servers run Windows Server 2003. Each client computer runs either Windows 2000 Professional or Windows XP Professional.

The IT staff is organized into four groups. The IT staff works at the three different sites. The computers for the IT staff must be configured by using scripts. The script or scripts must run differently based on which site the IT staff user is logging on to and which of the four groups the IT staff user is a member of.

You need to ensure that the correct logon script is applied to the IT staff users based on group membership and site location.

What should you do?

A. Create four Group Policy objects (GPOs). Create a script in each GPO that corresponds to one of the four groups. Link the four new GPOs to all three sites. Grant each group permissions to apply only the GPO that was created for the group
B. Create a single script that performs the appropriate configuration based on the user's group membership. Place the script in the Netlogon shared folders on the domain controllers.
C. Configure a Group Policy object (GPO) with a startup script that configures computers based on IT staff group. Link the GPO to the three sites.
D. Create a script that configures the computers based on IT staff group membership and site. Create and link a GPO to the Domain Controllers OU to run the script.

Answer: A

Explanation/Reference:
Explanation:
The easiest way to filter which users or computers a GPO should apply to is to set permissions on the GPO. A user or computer needs the Allow -Read and Apply Group Policy permissions in order to apply the GPO. In this question, we have four groups, each with different requirements. By creating four different GPOs and linking them to each of the three sites, we can manage who
receives the GPO by configuring the permissions on the GPOs.

Incorrect Answers:
B: The script needs to be linked to an Active Directory container.
C: It’s easier to use GPO permissions to determine which users or computers should receive a GPO.
D: It’s easier to use GPO permissions to determine which users or computers should receive a GPO. Furthermore, the GPO is linked to the wrong container in this answer.

Reference:

QUESTION 11
You are the network administrator for your company. The network consists of two Active Directory forests. Each forest contains a single domain. All servers run Windows Server 2003. One forest is used for testing and the other forest is used for production. The test forest contains a single domain controller. The test forest is used to test Group Policy objects (GPOs).

You are testing 60 GPOs in the test environment that will be deployed in the production environment. You assign the Testuser account in the test forest the Deny - Apply Group Policy permission. Logging on to the test forest takes longer than would be acceptable in the production forest.

You must reduce logon times in the test forest.

What should you do?

A. Assign the Testuser account the Deny - Read permission for unused GPOs.
B. Assign the Testuser account the Deny - Write gpoLink permission for the domain.
C. Create a GPO to enable the Negative DC Discovery Cache Setting, specify the setting to be 60 seconds, and apply it to the client computers.
D. Create a GPO to enable the Group Policy refresh interval for computers setting, specify the update rate to be 120 minutes, and apply it to the client computers.

Answer: A

Explanation/Reference:
Explanation:
Group Policy is still processed but not applied when the Deny - Apply Group Policy permission is assigned. The Deny - Read permission will ensure that the GPO is not processed. This will improve logon times.

Incorrect Answers:
B: There is not Write gpoLink permission.
C: The Negative DC Discovery Cache Setting specifies the amount of time the DC locator retains that a domain controller could not be found in a domain. When a subsequent attempt to locate the
domain controller occurs within the time set in this setting, DC Discovery immediately fails, without attempting to find the domain controller.

D: Setting the group policy refresh interval won’t prevent the GPO from being processed at logon.

Reference:

QUESTION 12
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run Windows XP Professional and are members of the domain. Only designated IT support staff have administrative rights on client computers.

TestKing requires all client computers to run antivirus software. TestKing licenses an antivirus application that is installed on a file server named Testking1. An unattended installation can be performed on each client computer by running the setup command from a shared folder on Testking1.

Several users report that when they attempt to install the antivirus application, they receive the following error message: “You do not have sufficient privileges on this computer to perform this action.” You verify that the antivirus application is not installed on any client computers.

You need to ensure that all client computers have the antivirus application installed. You want to accomplish this task by using the minimum amount of administrative effort.

What should you do?

A. Create a Group Policy object (GPO) linked to the domain. Use the GPO to launch a login script that runs the setup command to install the antivirus application if it is not currently installed. Instruct all users to restart their client computers.
B. Create a Group Policy object (GPO) linked to the domain. Use the GPO to launch a startup script that runs the setup command to install the antivirus application if it is not currently installed. Instruct all users to restart their client computers.
C. Create a batch file that runs the setup command. Send this batch file in an e-mail message to all users. Instruct all users to run this batch file.
D. Use Remote Assistance to run the setup command on each client computer.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
Group Policy is the component within Active Directory that enables directory-based change and configuration management of user and computer settings, including security and user data. Use Group Policy to define configurations for groups of users and computers. With Group Policy, you can specify policy settings for registry-based policies, security, software installation, scripts, folder redirection, remote installation services, and Microsoft Internet Explorer Maintenance. See also Group Policy Object; Group Policy Object Editor. On the other hand, Group Policy Object (GPO) is
a collection of Group Policy settings. GPOs are essentially the documents created by the Group Policy Object Editor. GPOs are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units (OUs). In addition, each computer has exactly one group of settings stored locally, called the local Group Policy Object. Making use of a GPO that is linked to the domain to launch a startup script that runs the setup command to install the antivirus application and instructing all users to restart their computers, will represent the least administrative effort to ensure that all client computers have the application installed.

Incorrect answers:
A: This option describes the correct procedure that is needed, but it says to launch a login script, this is not what is required. You need to launch a startup script to run the setup command to install the application.
C: The creation of batch file and e-mailing it to all users telling them to install the batch file is not what is required in this case.
D: There is no need to make use of Remote Assistance since this option will also accomplish the task, but with much more administrative effort than is necessary.

Reference:

QUESTION 13
You are the 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.

All servers that are not domain controllers have computer accounts in an organizational unit (OU) named ApplicationServers. Client computers have computer accounts in 15 OUs organized by department. All users have user accounts in an OU named CompanyUsers.

Your company wants all users to have Microsoft Word available on their client computers. Your company does not want to install Word on domain controllers or other servers.

You need to configure the network to install the application as required, without affecting any existing policies or settings.

What should you do?

A. · Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the computer settings.
   · Link this GPO to the domain.
   · Configure the Domain Controllers OU and the ApplicationServers OU to block policy inheritance.
B. · Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the computer settings.
   · Link this GPO to the domain.
   · Configure permissions on the GPO so that all server and domain controller accounts are
denied the permissions to read and apply the GPO.

C. · Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the user settings.
   · Link this GPO to the domain.
   · Configure the Domain Controllers OU and the ApplicationServers OU to block policy inheritance.

D. · Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the user settings.
   · Link this GPO to the domain.
   · Configure permissions on the GPO so that all server and domain controller accounts are denied the permissions to read and apply the GPO.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
The software can be installed on all the client computers, but not the domain controllers or application servers. Because the client computers are in 15 OUs, it would be easier to link the GPO at the domain level. The OUs containing the client computers would then inherit the GPO settings. To prevent the GPO applying to the domain controllers and servers, we can simply deny the read and apply GPO permission for the domain controller and server computer accounts.

Incorrect Answers:
A: It is likely that some domain level policies should apply to the domain controllers and the servers. Therefore, blocking policy inheritance isn't recommended.
C: It is likely that some domain level policies should apply to the domain controllers and the servers. Therefore, blocking policy inheritance isn't recommended.
D: This won't stop the software being installed on the servers, because the software installation would be defined in the user section of the group policy.

Reference:

QUESTION 14
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run Windows XP Professional with the most recent service pack. All client computers have computer accounts in an organizational unit (OU) named TestKingComputers.

TestKing requires all computers to be kept up-to-date with service packs and hotfixes from Microsoft. Administrators will manually update servers as required.

You need to configure the network so that client computers are automatically updated as new critical updates are issued.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Create a Group Policy object (GPO) linked to the domain. Configure the GPO so that client computers automatically download and install updates from Microsoft update servers from the Internet.

B. Create a Group Policy object (GPO) linked to the TestkingComputers OU. Configure the GPO so that client computers automatically download and install updates from Microsoft update servers from the Internet.

C. Create a Group Policy object (GPO) linked to the domain. Configure the GPO so that client computers automatically download and install updates from an internal server on which you install and configure Software Update Services.

D. Create a Group Policy object (GPO) linked to the TestkingComputers OU. Configure the GPO so that client computers automatically download and install updates from an internal server on which you install and configure Software Update Services.

Answer: BD
Section: (none)

Explanation/Reference:
Explanation:
To ensure that computers download and install the updates, we must configure a GPO to download and apply the updates either from the Microsoft updates server, or from the internal server on which you install and configure Software Update Services. The GPO must apply to only client computers as administrators will manually update server computers as required. All client computers are in the TestkingComputers OU therefore we should link the GPO to the OU.

Incorrect Answers:
A, C: The GPO must apply only to client computers as the administrators will manually update server computers as required. Therefore the GPO should be linked to the Testking Computers OU and not the domain.

Reference:

QUESTION 15
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Except for IT staff, users are not local administrators on client computers.

TestKing obtains a new application for order processing. This application must be installed on each client computer. The application is contained in an .msi file. You copy the .msi file to a shared folder on a file server. You assign the Authenticated Users group the Allow - Read permissions for the shared folder.
To deploy the application, you instruct users to double-click the .msi file in the shared folder. When users attempt to install the application, they receive an error message, and setup fails.

You need to configure the network so that the application can be installed successfully.

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

A. Modify the Default Domain Policy Group Policy object (GPO) and assign the new application to all client computers.
B. Grant the users the permissions required to create temporary files in the shared folder that contains the .msi file.
C. Modify the Default Domain Policy Group Policy object (GPO) and disable the Prohibit User Installs setting in the Windows Installer section of the computer settings.
D. Modify the Default Domain Policy Group Policy object (GPO) and enable the Always install with elevated privileges setting in the Windows Installer section of the computer settings.

Answer: AD  
Section: (none)

Explanation/Reference:
Explanation:
The software installation fails because the users don't have the necessary permissions to install the software. We can solve this problem by either assigning the application to the users in a group policy, or by using a group policy to enable the Always install with elevated privileges setting in the Windows Installer section of the computer settings.

Incorrect Answers:
B: Users don't have the necessary permissions to install the software. Granting users permissions to create temporary files in the shared folder won't overcome this problem.
C: We need to enable the Always install with elevated privileges setting rather than disable the Prohibit User Installs setting.

Reference:

QUESTION 16
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. The domain includes an organizational unit (OU) named Processing. There are 100 computer accounts in the Processing OU.

You create a Group Policy object (GPO) named NetworkSecurity and link it to the domain. You configure NetworkSecurity to enable security settings through the Computer Configuration section of the Group Policy settings.
You need to ensure that NetworkSecurity will apply only to the computers in the Processing OU. You need to minimize the number of GPO links.

What should you do?

A. Link NetworkSecurity to the Processing OU. Disable the User Configuration section of Network Security.
B. Link NetworkSecurity to the Processing OU. Remove the link from Network Security to the domain.
C. Modify the discretionary control list (DACL) for NetworkSecurity to assign all computer accounts on the Processing OU the Allow - Read and the Allow - Supply Group Policy permissions.
D. Modify the discretionary access control list (DACL) for Network Security to assign the Authenticated Users group the Deny - Apply Group Policy permission and to assign all of the computer accounts in the Processing OU the Allow - Read and the Allow - Apply Group Policy permissions.

Answer: B

Explanation/Reference:
Explanation:
We need to ensure that the Network Security GPO is applied to the domain. We should link the Network Security GPO to the Processing OU, not the domain.

Incorrect Answers:
A: Linking the NetworkSecurity GPO to the Processing OU won't work if the Network Security GPO is still linked to the domain. We need to also remove the link to the domain.
C, D: The Network Security GPO is linked to the domain and is thus applied to all computers. Assigning all computer accounts on the Processing OU the Allow - Read and the Allow - Supply Group Policy permissions won't stop the GPO from applying to all computers in the domain.

Reference:

QUESTION 17
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. All client computers run Windows XP Professional.

All user accounts for the sales department users are located in an organizational unit (OU) named Sales. The client computers are located in the default Computers container.

All users in the sales department require a sales application to be installed on their client computers. You create a new Group Policy object (GPO). You create a software installation package and use the GPO to assign the package to computers. You link the GPO to the Sales OU.

Users in the sales department report that the application is not installed on any client computers.

You need to install the application on all client computers in the sales department. You need to ensure that the application is installed only on the client computers used by users in the sales
department.

What should you do?

A. Modify the GPO to specify that Windows Installer packages will be installed by using elevated permissions.
B. Modify the GPO so that the application is assigned to user accounts.
C. Enable loopback processing for the GPO.
D. Link the GPO to the Computers container.

Answer: B

Section: (none)

Explanation/Reference:
Explanation:
Applications should either be published or assigned.

Incorrect Answers:
A: We need to assign or publish the application. Specifying the packages to be installed by using elevated permissions will not work.
C: Loop back processing is not required.
D: We need to assign or publish the application. Simply linking the GPO won't work.

Reference:

QUESTION 18
You are the network administrator for your company. The network consists of a single Active Directory domain.

All user accounts for users in the engineering department are located in an organizational unit (OU) named Engineering. These users' client computers are all located in an OU named EngineeringWorkstations, which is a child OU of the Engineering OU. All users in the engineering department are members of a global group named Engineers.

You create a Group Policy object (GPO) that assigns a software installation package to users in the Engineering OU. To comply with the licensing requirements for the application, the application must be uninstalled from a user's computer when that user is moved out of the Engineering OU.

A user named Francesca is transferred out of the engineering department. The user account for Francesca is moved into an OU named Research. Francesca reports that the application is still installed on her computer.

You must ensure that the application is automatically uninstalled from Francesca's computer. The application must remain on the computers of all users who are still in the Engineering OU.

What should you do?
A. Move Francesca's user account back into the Engineering OU. Configure the software installation package so that the software is uninstalled when Francesca's user account falls out of the scope of management. Ensure that Francesca logs on to the network. Move Francesca's user account back into the Research OU.

B. Move Francesca's user account back into the Engineering OU. Modify the GPO so that the software installation package is removed. Ensure that Francesca logs on to the network. Move Francesca's user account back to the Research OU.

C. Move the client computer object for Francesca's computer out of the EngineeringWorkstations OU.

D. Remove Francesca from the Engineers global group.

Answer: A

Section: (none)

Explanation/Reference:
Explanation:
The Uninstall The Applications When They Fall Out Of The Scope Of Management option can be used to remove the application if it no longer applies to users or computers. However, the application must first apply to the user or computer. Therefore we should move Francesca's user account back into the Engineering OU so that the application applies to her again and Francesca must log on to the network for the GPO to apply. Then we can move Francesca's user account back into the Research OU. The application will no longer apply to Francesca and will be uninstalled.

Incorrect Answers:
B: Modifying the GPO so that the software installation package is removed will result in the application being removed for all users in the Engineering OU.
C:computer is irrelevant.
D: The GPO is applied at the OU. The Engineers global group is not in the Engineering OU.

Reference:
Exam E

QUESTION 1
You are a network administrator for TailSpin Toys. The company has a main office and one branch office. All client computers run Windows XP Professional.

The network consists of a single Active Directory forest that contains a single domain named Tailsptoy.com. The forest has two sites named MainOffice and BranchOffice.

The organization unit (OU) structure is shown in the exhibit.

A written company policy requires different Group Policy objects (GPOs) to be linked to the various OUs. All of the users in the BranchOffice site require a specific application. You create a new GPO named and configure it to assign the required application to all users in the BranchUsers OU.

A special project suddenly requires two users who normally work in the MainOffice site to take their portable computers to work in the BranchOffice site. When the users log on to the network at the branch office, the required application is not automatically installed on the two portable computers. The application must not be installed on any of the other computers in the main office. You must also ensure that settings that are currently applied to the two users remain in effect.

What should you do?

A. Move the two user accounts from the MainOfficeUsers OU to the BranchUsers OU
B. Move computer accounts for the two users from the MainOfficeClients OU to the BranchClients OU
C. Link the BranchApps GPO to the MainOffice site
D. Link the BranchApps GPO to the BranchOffice site

Answer: D
Section: (none)

Explanation/Reference:
D is correct.

Incorrect answers:
Incorrect answers:
A - The question says "You must also ensure that settings that are currently applied to the two users remain in effect", therefore we can't move the two users account from the MainOfficeUsers OU to the BranchUsers OU without affecting their settings that applied at MainOfficeUsers OU.
B - In question says that "You create a new GPO named and configure it to assign the required application to all users in the BranchUsers OU." So if we moved two computer accounts in to the BranchUsers OU, the application is not be installed.
C - We need use application in the BranchUsers OU. So this answer is absolutely wrong.

QUESTION 2
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain. The domain includes an organizational unit (OU) named TerminalServers and a global group named Accounting. TheTerminalServers OU contains all of the Windows Server 2003 computer accounts running Terminal Services. Members of the Accounting group connect to terminal servers to access their software applications.

You create a Group Policy object (GPO) and link it to the TerminalServers OU.You configure the GPO to publish a software installation package that installs the most recent tax application.

Users in the Accounting group report that the new tax application is not installed on any of the terminal servers. You log on to one of the servers running Terminal Services and attempt to use Add or Remove Programs in Control Panel. When you select Add New Program, you receive the following message: "Applications are not available to install from the network in this mode."

You need to ensure that the new tax application is installed on the computers running Terminal Services.

What should you do?

A. Modify the GPO and configure the software installation package to be assigned under the Computer Configuration section of the GPO under Software Settings.
B. Modify the GPO and configure the software installation package to be assigned under the User Configuration section of the GPO under Software Settings.
C. Modify the discretionary access control list (DACL) settings of the GPO to assign the Authenticated Users group the Deny - Read and the Allow - Apply Group Policy permissions.
D. Modify the discretionary access control list (DACL) settings of the GPO to assign the computer accounts in the TerminalServers OU the Allow - Read and the Allow -Apply Group Policy permissions.

Answer: A

Explanation/Reference:
Explanation:
In order for the Software application to be available through a Terminal Session, the software application must be installed on the server itself. If the GPO assigns the software installation package under user configuration the software will not get installed onto the Terminal Server.
Incorrect Answers:
B: We need the application applied to the computer not the user.
C, D: This doesn't make sense.

Reference:

QUESTION 3
You are the network administrator for your company. Your network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. Employees use client computers and also use Remote Desktop to connect to a terminal server named TS1.

All users in your company have user accounts in an organizational unit (OU) named Company Users. All users receive applications that are assigned to their user accounts by Group Policy objects (GPOs) linked to the Company Users OU. The GPOs use security filtering to control which security groups receive which applications.

Users report that when using TS1, their assigned applications are not available.

You need to configure your network so that the applications are available to users when they connect to TS1. You need to ensure that users cannot run any application that is not currently assigned to them.

What should you do?

A. Reconfigure the GPOs containing software installation packages so that the software installation packages are published to users.
B. Reconfigure the GPOs containing software installation packages so that assigned software installation packages are automatically installed at logon.
C. Install all required software on TS1. Use NTFS permissions to control which security groups can access which applications.
D. Link the GPOs containing software installation packages to the domain, not to an OU.

Answer: C
Section: (none)

Explanation/Reference:
Explanation:
When an application is assigned to a user, it is not available if the user connects to a Terminal Server using a Remote Desktop Connection. The only way to make the applications available on a Terminal Server is to manually install the applications on the server. We can use NTFS permissions to ensure that only the appropriate users are able to use the application.

Incorrect Answers:
A: It doesn't matter if the applications are published or assigned. They will not be available on a Terminal Server.
B: The software will be installed on the users' client computers, but not the Terminal
The applications are assigned to users, not computers. The users receive the GPOs, so linking the GPO to the domain won't make any difference.

Reference:

QUESTION 4
You are the network administrator for your company. Your network consists of a single Active Directory domain. All servers run Windows Server 2003. All user accounts in your domain are located in an organizational unit (OU) named User Accounts.

User accounts are separated into two types: accounts for users who use portable computers and accounts for users who use desktop computers.
The accounts for the users who use portable computers are in an OU named Portable, and the accounts for the users who use desktop computers are in an OU named Desktop. The OU structure is shown in the work area.

Users who use portable computers often travel with them, but they do not connect to the network when they are out of the office.

You need to install an application on all client computers. Users must be able to run the application even if the client computer is not connected to the network. You need to perform the installation in a way that reduces network load on the installation source. All software installed by using a Group Policy object (GPO) must require as little support as possible.

You need to configure Group Policy to install the application. You also need to link any GPO to the appropriate OU.

What should you do?

To answer, drag the appropriate action or actions for a GPO to perform to the correct OU or OUs in the work area.
Answer:

<table>
<thead>
<tr>
<th>Possible Actions</th>
<th>Work Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish</td>
<td>User Accounts</td>
</tr>
<tr>
<td></td>
<td>Portable</td>
</tr>
<tr>
<td></td>
<td>Desktop</td>
</tr>
<tr>
<td>Assign On Demand</td>
<td>Drag action here</td>
</tr>
<tr>
<td>Assign Install at Logon</td>
<td>Drag action here</td>
</tr>
</tbody>
</table>

Section: (none)
Explanation/Reference:

Explanation:
The application must be installed on all client computers. However, some computers are portable computers. We therefore should not apply the GPO at the domain level but at the OU level because we can only have the application installed on the portable computers when users log on to the network from the portable computers. Once installed, this application must be available even when users aren't connected to the network, therefore we need to assign and not publish the application.

Because we apply the GPO at the OU level, desktop users can be treated differently. To reduce network load on the installation source we can configure the GPO for the Desktop OU to install the application on demand rather than at log on.

Reference:

QUESTION 5
You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional.

You use a Group Policy object (GPO) to distribute an application to users. The application is contained in an .msi file that is stored in a shared folder.

Users report that they do not have the application installed. You verify that the GPO successfully installed the application on your computer. On the client computers, you see the error message shown in the exhibit. (Click the Exhibit button.)

You need to ensure that users can install the application.

What should you do?

Exhibit:
A. Configure the default package location in the GPO to be the network path to the application.
B. Configure the Windows Installer service on each client computer to start as a member of the Domain Admins group.
C. Create a GPO to enable the Always install with elevated privileges setting.
D. Assign the users the Allow - Read permission for the .msi file.

Answer: D
Section: (none)

Explanation/Reference:
Explanation:
To assign the application to users, the users need at least Allow - Read permission to the msi file.

Incorrect Answers:
A, B: Configuring the package location or the Windows Installer service won't help if the users don't have Allow - Read permissions.
C: Users need the Allow - Read permission to the msi file.

Reference:
QUESTION 6
You are the network administrator for your company. Your network consists of a single Active Directory domain. All servers run Windows Server 2003. You use Group Policy objects (GPOs) to distribute software.

Your company uses two different applications to view graphics. Users are allowed to choose which program they will use based on the features and formats they require. Only the users are allowed to decide which of these two applications will be installed.

You need to configure the GPOs to install either graphics application based on the user's choice.

What should you do?

A. Publish both applications with file extension activation.
B. Publish both applications without file extension activation.
C. Assign both applications to install on demand.
D. Assign both applications to complete a full installation.

Answer: B

Explanation/Reference:
Explaination:
You can publish applications to users, making the application available for users to install. To install a published application, users can use Add or Remove Programs in Control Panel, which includes a list of all published applications that are available for them to install.

Incorrect Answers:
A: Only one application will install when a file is opened. The users won't have the choice.
C: The applications should be published, not assigned.
D: This doesn't make sense.

Reference:

QUESTION 7

Users report some instabilities in the application that cause data loss. The software vendor releases a patch that fixes the problem. The patch is released as an .msp file.
You need to ensure that users do not lose data when running the application.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Copy the .msp file to the folder where the application source files exist.
B. Create a .zap file for the patch and deploy the .zap file.
C. Rename the .msp file to an .mst file.
D. Apply the patch to the application source files.
E. Redeploy the GPO that installs the application.

Answer: DE
Section: (none)

Explanation/Reference:
Explanation:
Patches in the .msp format must be allied to the source files which are then applied to the appropriate container by redeploying the GPO that installs the application.

Incorrect Answers:
A: The patch file must be applied to the source files, merely copying it to the source folder won't work.
B, C: The patch is released as an .msp file. There is no need to repackage it as a .zap file, which is not as flexible as an .msp file, or an .mst file.

Reference:

QUESTION 8
You are the network administrator for your company. The network consists of a single Active Directory domain that contains four domain controllers. All servers run Windows Server 2003. All user accounts are located in an organizational unit (OU) named CompanyUsers.

A written company policy requires all users to use strong passwords. User passwords must contain a mixture of letters, numbers, or special characters. Passwords must be at least 10 characters long. Passwords must be changed at least every 60 days, and the new password cannot be the same as the old one.

To enforce this requirement, you create a Group Policy object (GPO) named Password Policies and link the GPO to the CompanyUsers OU. The settings in the Password Policy section of the Password Policies GPO are shown in the exhibit. (Click the Exhibit button.)

You discover that users are creating simple passwords that do not meet the complexity requirements.

You need to ensure that the company password requirements are enforced.

What should you do?
Exhibit:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce password history</td>
<td>1 passwords remembered</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>60 days</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>0 days</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>10 characters</td>
</tr>
<tr>
<td>Password must meet complexity requirements</td>
<td>Enabled</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

A. Link the Password Policies GPO to the Domain Controllers OU. Make it the first GPO in the list.
B. Configure the properties of the Password Policies GPO so that it cannot be overridden.
C. Delete the Password Policies GPO. Edit the Default Domain Policy GPO to include the settings from the Password Policy section of the Password Policies GPO.
D. Delete the Password Policies GPO. Edit the Default Domain Controllers Policy GPO to include the settings from the Password Policy section of the Password Policies GPO.

Answer: C
Section: (none)

Explanation/Reference:
Explanation:
Changes in Security Policies such as a password policy can only affect the user if applied at the Domain Level using the Default Domain Policy. Security Policies that affect computers can be applied at the OU level as well as at the Domain Level.

Incorrect Answers:
A: This GPO is applied to the Domain Controllers OU and would thus affect the policies set on a Domain Controller.
B: The password polices are set on a Users OU and not a computers OU.
C: This answer is nearly the same as A except that you delete and recreate the GPO.

Reference:

QUESTION 9
You are a network administrator for Fabrikam, Inc. The network consists of a single Active Directory domain named fabrikam.com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

The company restricts all users so that they can use only authorized applications. All domain users are authorized to use the Microsoft Office suite of applications. Members of a security group named CRM Users are also authorized to use a customer relationship management (CRM) application.

You configure Group Policy objects (GPOs) as shown in the exhibit. (Click the Exhibit button.)
The Office Applications GPO has only the Microsoft Office applications listed as allowed applications. The CRM Application GPO has only the CRM application listed as an allowed application. The CRM Application GPO has security settings so that it applies only to members of the CRM Users security group.

Users who are members of the CRM Users security group report that they cannot run the CRM application.

You need to reconfigure the domain to meet the following requirements:

· All users must be able to run the Microsoft Office applications.
· Members of the CRM Users security group must be able to run the CRM application.
· All users must be prevented from running unauthorized software.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)

Exhibit:

A. Configure the Default Domain Policy GPO so that the CRM application is published to the members of the CRM Users security group.
B. Disable the No Override setting for the CRM Application GPO. Leave the CRM Application
C. Reorder the GPOs so that the CRM Application GPO is higher in the list than the Office Applications GPO.

D. Create a new OU. Move the user accounts for all members of the CRM Users security group into this OU. Link the CRM Application GPO to this OU. Enable the Block Policy inheritance setting for this OU. Unlink the CRM Application GPO from the domain.

E. Add the Microsoft Office applications to the list of allowed applications in the CRM Application GPO.

Answer: CE

Explanation/Reference:
Explanation:
The Office Application GPO is set to no override. This is preventing the CRM Application GPO from being applied. We should make the CRM Application apply before the Office Application and make the Microsoft applications an allowable application on the CRM Application list. Now the CRM Application will be applied but only to members of the CRM Users security group. These users will also get the Office applications because that is now in the CRM Applications GPO. The users that are not members of the CRM Users security group won't get any of the settings of the CRM Applications GPO, therefore it's no override setting is irrelevant to them. The Office Applications will be applied for these users.

Note: We added the Microsoft Office applications to the CRM Applications GPO because the CRM Applications are set to no override. Therefore the Office Applications will not apply to the CRM Users security group. But the Office applications are now in the CRM Applications GPO so it no longer matters that the Office Applications GPO is not applied for the CRM Users security group.

Incorrect Answers:
A: The Office Application GPO is set to no override. This is preventing the CRM Application GPO from being applied.
B: The Office Application GPO is set to no override. This is preventing the CRM Application GPO from being applied. Therefore, disabling the No Override setting for the CRM Application GPO won't accomplish anything.
D: Simply moving the CRM Application before the Office Application and making the Microsoft applications an allowable application on the CRM Application list would require less administrative effort.

Reference:

QUESTION 10
You are the network administrator for Southridge Video. The network consists of a single Active Directory domain named southridgevideo.com. The domain contains one domain controller. All servers run Windows Server 2003. All client computers run Windows XP Professional. The company uses Group Policy objects (GPOs) to configure user and computer settings.

The Active Directory database and the SYSVOL shared folder are stored on separate hard disks.
The hard disk containing the SYSVOL folder fails.
Some Group Policy settings are still applied, but new users do not receive the Group Policy settings.

You replace the failed disk. You discover that there are no valid backups of the SYSVOL folder. You have a list of GUIDs and friendly names for each GPO. On the new disk, you create a new shared folder named SYSVOL in the same location as the previous SYSVOL folder.

You need to configure the network so that the user and computer settings will be applied to all users.

Which three courses of action should you take? (Each correct answer presents part of the solution. Choose three.)

A. In the SYSVOL folder, create a folder named southridgevideo.com. In the southridgevideo.com folder, create a folder named Policies.
B. In the SYSVOL folder, create a folder named System State. In the System State folder, create a folder named Policies.
C. In the Policies folder, create a folder for each GPO. Name the folders by using the friendly name of each GPO. In the folder for each GPO, create a folder named MACHINE and a folder named USER.
D. In the Policies folder, create a folder for each GPO. Name the folders by using the GUID of each GPO. In the folder for each GPO, create a folder named MACHINE and a folder named USER.
E. Use Active Directory Users and Computers to open each GPO. Close each GPO without changing any settings.
F. Use Active Directory Users and Computers to open each GPO. Change at least one setting in each GPO before closing it.

Answer: ADF
Section: (none)

Explanation/Reference:
Explanation:
A globally unique identifier (GUID) is a 128-bit hexadecimal number that is guaranteed to be unique within the enterprise. GUIDs are assigned to objects when the objects are created. The GUID never changes, even if you move or rename the object. A GUID is unique across all domains, meaning that you can move objects from domain to domain and they will still have a unique identifier.

Ensure the integrity of the computer’s Group Policy by performing one of the following:
(i) If you authoritatively restored the entire Active Directory database, copy the Sysvol directory on the alternate location over the existing one after the Sysvol share is published.
(ii) If you authoritatively restored specific Active Directory objects, copy only the policy folders (identified by the GUID) corresponding to the restored policy objects from the alternate location after the Sysvol share is published. Then, copy them over the existing ones. When authoritatively restoring either the entire Active Directory database or selected objects, it is important that you copy the Sysvol and policy data from the alternate location after the Sysvol share is published. If the computer is in a replicated domain, it may take several minutes before the Sysvol share is published because it needs to synchronize with its replication partners. If all computers in the domain are authoritatively restored and restarted at the same time, then each will be waiting (indefinitely) to synchronize with each other. In this case, restore one of the domain
nonauthoritatively. Thus options A, D and F will ensure that all settings will be applied to all users in the given circumstances.

Incorrect answers:
B: The folder that should be created should be testking.com and not system state folder
C: Making use of the friendly name of each GPO will not have the desired effect.
E: You need to change at least one setting in each GPO before closing it.

Reference:

QUESTION 11
You are the network administrator for TestKing.com. The network consists of a single Active Directory forest. The forest functional level is Windows 2000. The forest consists of a forest root domain named testking.com and two child domains named child1.testking.com and child2.testking.com. The functional level of all three domains is Windows 2000 native. All domain controllers in the forest run Windows 2000 Server.

Your user account has administrative privileges is in the child1.testking.com domain and is a member of the following groups: Schema Admins, Domain Admins, and Domain Users.

You need to successfully run the adprep.exe /forestprep command.

What should you do?

A. Run the adprep.exe /forestprep command on the PDC emulator for the testking.com domain.
B. Restart the schema master in Directory Services Restore Mode and run the adprep.exe /forestprep command.
C. Add your user account that has administrative privileges to the Enterprise Admins group. Run the adprep.exe /forestprep command on the schema master.
D. Run the adprep.exe /domain prep command on the PDC emulator for the testking.com domain. Then run the adprep.exe /forestprep command on the schema master.
E. Run the adprep.exe /domainprep command on the infrastructure master in each domain. Then run the adprep.exe /forestprep command on the schema master.

Answer: C
Section: (none)

Explanation/Reference:
Explanation:
Because ForestPrep updates the schema and configuration partitions in Active Directory, the account used to run ForestPrep must be a member of the Schema Admins and Enterprise Admins security groups.

Incorrect Answers:
A, B, D: To run adprep.exe /forestprep, you must be a member of the Schema Admins security group, as well as the Enterprise Admins security group.

Reference:
QUESTION 12
You are the network administrator for Northwind Traders. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest consists of a forest root domain named northwindtraders.com and a child domain named child1.northwindtraders.com. The child1.northwindtraders.com domain contains all of the user accounts for the network.

Your company acquires a company named Contoso, Ltd. The Contoso, Ltd., network consists of a single Active Directory forest that contains a forest root domain named contoso.com and a child domain named child1.contoso.com. All domain controllers run Windows 2000 Server. Both domains contain user accounts and resource servers.

The domains and existing trust relationships are shown in the exhibit. (Click the Exhibit button.)

You need to create the minimum number of trust relationships required for the users in the child1.northwindtraders.com domain to access resources in both domains in the contoso.com forest.

What should you do?

Exhibit:

A. Create a one-way trust relationship in which the northwindtraders.com domain trusts the contoso.com domain.
B. Create a one-way trust relationship in which the contoso.com domain trusts the northwindtraders.com domain.
C. Create a one-way trust relationship in which the child1.northwindtraders.com domain trusts the contoso.com domain.
   Create a one-way trust relationship in which the child1.northwindtraders.com domain trusts the child1.contoso.com domain.
D. Create a one-way trust relationship in which the contoso.com domain trusts the child1.northwindtraders.com domain.
   Create a one-way trust relationship in which the child1.contoso.com domain trusts the child1.northwindtraders.com domain.

Answer: D

Section: (none)

Explanation/Reference:
Explanation:
Users in child1.testking.com need to access resources in contoso.com and child1.contoso.com. Therefore, the contoso.com and child1.contoso.com domains need to trust the child1.testking.com domain. We can achieve this by configuring two one-way trust relationships: one in which the contoso.com domain trusts the child1.testking.com domain and one in which the child1.contoso.com domain trusts the child1.testking.com domain.

Incorrect Answers:
A: The TestKing user accounts are in the child1.testking.com domain, not the testking.com domain. Therefore, the contoso.com and child1.contoso.com domains need to trust the child1.testking.com domain.
B: The TestKing user accounts are in the child1.testking.com domain, not the testking.com domain. Therefore, the contoso.com and child1.contoso.com domains need to trust the child1.testking.com domain.
C: The contoso.com and child1.contoso.com domains need to trust the child1.testking.com domain.

Reference:

QUESTION 13
You are the network administrator for Wingtip Toys. The network consists of a single Active Directory domain named wingtiptoys.com. The network also consists of two sites named Site1 and Site2. Each site contains domain controllers. An organizational unit (OU) named Accounting contains two child OUs named Accounts Payable and Accounts Receivable. All user accounts for users in the accounting department are located in these three OUs.

User accounts in the Accounting OU need to have password lengths of at least eight characters. You need to ensure that users in the Accounting OU, the Accounts Receivable OU, and the Accounts Payable OU cannot modify their screen savers. In addition, you need to ensure that users in the Accounts Payable OU cannot change their desktop wallpaper.

Another administrator creates the four Group Policy objects (GPOs) listed in the following table.
You need to decide where to link the appropriate GPOs to each OU.

Where should you link the GPOs?

To answer, drag each appropriate GPO to the correct location or locations in the work area.

<table>
<thead>
<tr>
<th>Name</th>
<th>GPO section</th>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPO1</td>
<td>User Configuration</td>
<td>Prevent changing wallpaper</td>
<td>Disabled</td>
</tr>
<tr>
<td>GPO2</td>
<td>Computer Configuration</td>
<td>Minimum password length equals 6 characters</td>
<td>Enabled</td>
</tr>
<tr>
<td>GPO3</td>
<td>User Configuration</td>
<td>Screen Saver</td>
<td>Disabled</td>
</tr>
<tr>
<td>GPO4</td>
<td>User Configuration</td>
<td>Prevent changing wallpaper</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
We need to ensure that user accounts in the Accounting OU have password lengths of at least eight characters. We can accomplish this by applying GPO2 at the domain level.

Next we need to ensure that users in the Accounting OU, the Accounts Receivable OU, and the
Accounts Payable OU cannot modify their screen savers. We can accomplish this by applying GPO3 at the Accounting OU because the Accounts Receivable OU and the Accounts Payable OU is child OUs of the Accounting OU.

Finally, we must ensure that users in the Accounts Payable OU cannot change their desktop wallpaper. We can accomplish this by applying GPO4 at the Accounts Payable OU. We would use GPO4 rather than GPO1 because the setting is Prevent changing wallpaper. This must be enabled.

Reference:

**QUESTION 14**
You are the network administrator for your company. Your network consists of a single Active Directory domain. Three security groups named Accountants, Processors, and Management are located in an organizational unit (OU) named Accounting. All of the user accounts that belong to these three groups are also in the Accounting OU.

You create a Group Policy object (GPO) and link it to the Accounting OU. You configure the GPO to disable the display options under the User Configuration section of the GPO.

You need to achieve the following goals:

- You need to ensure that the GPO applies to all user accounts that are members of the Processors group.
- You need to prevent the GPO from applying to any user account that is a member of the Accountants group.
- You need to prevent the GPO from applying to any user account that is a member of the Management group, unless the user account is also a member of the Processors group.

What should you do?

A. Modify the discretionary access control list (DACL) settings of the GPO to assign the Accountants and Management security groups the **Deny - Read** and the **Deny - Apply Group Policy** permissions.
   - Modify the DACL of the GPO to assign the users who are in both the Accountants and Management security groups the **Allow - Read** and the **Allow - Apply Group Policy** permissions.
B. Modify the discretionary access control list (DACL) settings of the GPO to assign the Accountants and Management security groups the **Deny - Read** and the **Deny - Apply Group Policy** permissions.
   - Create a new security group named Mixed that contains all the user accounts from the Processors group and the specific user accounts from the Management group to which you want the GPO to apply.
   - Modify the DACL of the GPO to assign the Mixed security group the **Allow - Read** and the **Allow - Apply Group Policy** permissions.
C. Modify the discretionary access control list (DACL) settings of the GPO to assign the Accountants security group the **Deny – Read** and the **Deny - Apply Group Policy** permissions.
   - Modify the DACL settings of the GPO to remove the Authenticated Users special group.
   - Modify the DACL settings of the GPO to add the Processors group and assign the **Allow - Read** and the **Allow - Apply Group Policy** permissions.
D. · Modify the discretionary access control list (DACL) settings of the GPO to assign the Accountants security group the Deny – Read and the Allow - Apply Group Policy permissions. 
   · Modify the DACL settings of the GPO to assign the Management security group the Deny - Read and the Deny - Apply Group Policy permissions.

Answer: C
Section: (none)

Explanation/Reference:
Explanation:
You need to prevent the GPO from applying to any user account that is a member of the Accountants group. We can achieve this by modifying the discretionary access control list (DACL) settings of the GPO to assign the Accountants security group the Deny - Read and the Deny - Apply Group Policy permissions. We need to remove the authenticated users group so that the policy doesn't apply to anyone that isn't a member of any of the three groups.

You need to ensure that the GPO applies to all user accounts that are members of the Processors group. We can achieve this by modifying the DACL settings of the GPO to add the Processors group and assign the Allow - Read and the Allow - Apply Group Policy permissions. You need to prevent the GPO from applying to any user account that is a member of the Management group, unless the user account is also a member of the Processors group. The Management group isn't listed in the DACL. Therefore, no user in the Management group will receive the GPO. Management users will only receive the GPO if they are also a member of the Processors group, because the Processors group have the Allow - Read and the Allow - Apply Group Policy permissions.

Incorrect Answers:
A, B, D: Assigning the Management security groups the Deny - Read and the Deny - Apply Group Policy permissions will prevent the members that are members of both the Management and Processors group from receiving the GPO.

Reference:

QUESTION 15
You are the network administrator for TestKing.com. The network consists of a single Active Directory forest that contains an empty root domain named testking.com and a child domain named research.testking.com.

You need to implement secure password protection for the accounts located in the research.testking.com domain.

What should you do?

A. Configure the Default Domain Policy Group Policy object (GPO) of the research.testking.com domain to enable the Password must meet complexity requirements policy.
B. Configure the Default Domain Controllers Policy Group Policy object (GPO) of the research.testking.com domain to enable the Password must meet complexity requirements policy.
C. Configure the Default Domain Policy Group Policy object (GPO) of the testking.com domain to enable the Password must meet complexity requirements policy. Enable the No Override setting on the GPO.

D. Configure the Default Domain Controllers Policy Group Policy object (GPO) of the testking.com domain to enable the Password must meet complexity requirements policy. Enable the No Override setting on the GPO.

Answer: A

Explanation/Reference:
Explanation: GPOs are applied at the level at which they are linked. The password policy must be configured at the domain level if it is to be applied to the domain. Therefore, we must link the GPO at the domain level.

Incorrect Answers:
B: The password policy must be configured at the domain level, i.e., testking.com and not research.testking.com.
C: We don’t need the No Override setting if the GPO is applied at the domain level.
D: The GPO must be configured at the domain not the domain controller.

Reference:

QUESTION 16
You are the network administrator for your company. The network consists of a single Active Directory domain. The domain contains an organizational unit (OU) named Sales. You create three Group Policy objects (GPOs) that have four configuration settings, as shown in the following table.

<table>
<thead>
<tr>
<th>Location</th>
<th>GPO name</th>
<th>GPO configuration</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>ScreenSaver</td>
<td>Hide Screen Saver tab</td>
<td>Disabled</td>
</tr>
<tr>
<td>Sales OU</td>
<td>Display and Wallpaper</td>
<td>Hide Screen Saver tab</td>
<td>Enabled</td>
</tr>
<tr>
<td>Sales OU</td>
<td>Display and Wallpaper</td>
<td>Set Active Desktop Wallpaper to c:\WINNT\wallpaper\bliss.jpg</td>
<td>Enabled</td>
</tr>
<tr>
<td>Sales OU</td>
<td>Wallpaper</td>
<td>Set Active Desktop Wallpaper to c:\WINNT\wallpaper\autumn.jpg</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

The ScreenSaver GPO has the No Override setting enabled. The Sales OU has the Block Policy inheritance setting enabled. The priority for GPOs linked to the Sales OU specifies first priority for the Display and Wallpaper GPO and second priority for the Wallpaper GPO.

For user accounts in the Sales OU, you want the Screen Saver tab to be hidden and the desktop wallpaper to be Autumn.jpg. You log on to a test computer by using a user account from the Sales OU, but you do not receive the settings you wanted.

You need to configure the settings to hide the Screen Saver tab and set the desktop wallpaper to Autumn.jpg for the user accounts in the Sales OU. You want to avoid affecting user accounts in
other OUs.

What should you do?

A. Enable the No Override setting for the Display and Wallpaper GPO.
B. Disable the No Override setting on the ScreenSaver GPO. Reorder the Wallpaper GPO to be first in the list.
C. Create a GPO and link it to the Default-First-Site-Name. Configure the GPO to set the Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg
D. Disable the Block Policy inheritance setting on the Sales OU. Change the Display and Wallpaper GPO to set the Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
The No Override setting on the ScreenSaver GPO is causing all computers in the domain to display the ScreenSaver tab. We want to hide the screen saver tab for the Sales OU, so we'll have to remove the No Override settings from the ScreenSaver GPO. This will enable the ScreenSaver GPO settings to be overwritten by GPOs applied further down the order.

By configuring the Wallpaper GPO to be first in the list, we are giving it a higher priority than the Display and Wallpaper GPO. This means that the Wallpaper GPO settings will overwrite the Display and Wallpaper GPO settings, thus setting the wallpaper to Autumn.jpg.

Incorrect Answers:
A: The Screen saver settings in the Display and Wallpaper GPO is in effect because the ScreenSaver setting, which doesn't hide the ScreenSaver tab, is set to No Override. Thus subsequent GPOs cannot override this setting. Enabling the No Override setting for the Display and Wallpaper GPO won't result in it being applied.
C: A GPO linked to the Site is applied first and will be overwritten by subsequent GPOs applied at the lower levels.
D: Group policies set to Block Policy inheritance setting on the Sales OU does not affect the ScreenSaver GPO. This is part of the problem.

Reference:

QUESTION 17
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run either Windows XP Professional or Windows 2000 Professional. All client computer accounts are located in an organizational unit (OU) named Workstation.

A written company policy states that the Windows 2000 Professional computers must not use offline folders. You create a Group Policy object (GPO) to enforce this requirement. The settings in the GPO exist for both Windows 2000 Professional computers and Windows XP Professional
You need to configure the GPO to apply only to Windows 2000 Professional computers.

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

A. Create a WMI filter that will apply the GPO to computers that are running Windows 2000 Professional.
B. Create a WMI filter that will apply the GPO to computers that are not running Windows XP Professional.
C. Create two OUs under the Workstation OU. Place the computer accounts for the Windows XP Professional computers in one OU, and place the computer accounts for the Windows 2000 Professional computers in the other OU. Link the GPO to the Workstation OU.
D. Create a group that includes the Windows XP Professional computers. Assign the group the Deny - General Resultant Set of Policy (Logging) permission.
E. Create a group that includes the Windows 2000 Professional computers. Assign the group the Deny - Apply Group Policy permission.

Answer: AB

Section: (none)

Explanation/Reference:

Explanation:
WMI filters are ignored by Windows 2000 clients but not by Windows XP clients. Thus, the Windows XP clients will evaluate the filter to see if the GPO should apply to them or not, while the Windows 2000 clients will just apply the GPO without evaluating the WMI filter.

Incorrect Answers:
C: This looks like a good idea. However, applying the GPO to the Workstation OU will (by inheritance) apply the GPO to the two child OUs.
D: This won't prevent the application of the GPO.
E: This answer is close, but incorrect. This will prevent the GPO applying to the Windows 2000 clients. If the group contained the Windows XP clients, then it would work.

Reference:

QUESTION 18

You are the network administrator for your company. The network consists of a single Active Directory domain that contains two domain controllers. Both domain controllers run Windows Server 2003. All client computers run Windows XP Professional. The only account in the Domain Admins security group is the Administrator account in the domain. Each night, a full backup is made of the hard disks in each domain controller.

You disable the local Administrator account in the Default Domain Policy Group Policy object (GPO).
You discover that you are no longer able to log on to either domain controller as the Administrator from the domain.

You need to ensure that you can log on to both domain controllers as the Administrator from the domain.

What should you do?

A. Restart one domain controller in Safe Mode. Log on as Administrator.
   Create an account for a second administrator.
   Restart the domain controller and use the new account to remove the restrictions on the local Administrator accounts.

B. Restore the entire hard disk on one domain controller by using the last nightly backup before the change was made. Restart the domain controller.
   Allow time for Active Directory replication to complete.

C. Restart one domain controller and use a Windows Server 2003 CD to run the Recovery Console.
   Stop the GPC service.
   Restart the domain controller.

D. Restart one domain controller in Directory Services Restore Mode.
   Perform an authoritative restore operation of the Domain Controllers OU in Active Directory from the last nightly backup before the change was made.
   Restart the domain controller.

Answer: A
Section: (none)

Explanation/Reference:
Explanation:
The default domain group policy object is disabling the Administrator accounts. When you restart a domain controller in safe mode, the group policy isn't applied, so the administrator account isn't disabled. You need to start the computer in Safe Mode with Networking. This will enable you to access Active Directory Users and Computers. You can't modify existing objects, but you can create a new administrative account. Then you can reboot in normal mode and log in using the new administrative account and the new account to remove the restrictions on the local Administrator accounts.

Incorrect Answers:
B: It is not necessary to restore the entire hard disk. Furthermore, this won't work, because the GPO would plicate to the restored server and you'd be back to square one.
C: This will prevent all GPOs in the Group Policy Container (GPC) for being applied and would constitute a serious security risk.
D: The default domain group policy would still apply to the restored domain controller objects, so the administrator account will be disabled.

Reference:
Exam F

QUESTION 1
SIMULATION
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named TestKing.com.

The company has a main office and two branch offices. Due to a recent reorganization within the company, your Active Directory Site topology no longer reflects the current network infrastructure as shown in the following exhibit.

Exhibit

You need to modify the Active Directory site and subnets topology to reflect the current network infrastructure.

What should you do?

A. Simulation

Answer: A
Section: (none)

Explanation/Reference:
You are the network administrator for your company. The network consists of a single Active Directory domain. The company has a main office and two branch offices.

Due to a recent reorganization within the company, your Active Directory Site topology no longer reflects the current network infrastructure as shown in the following exhibit. (Click the Exhibit button.)

You need to modify the Active Directory site and subnets topology to reflect the current network infrastructure.

What should you do?

To answer, perform the appropriate actions in the simulation. (When you are finished, click the Done button.)

Answer:

STEP 1.
STEP 2.

You are the network administrator for your company. The network consists of a single Active Directory domain. The company has a main office and two branch offices.

Due to a recent reorganization within the company, your Active Directory Site topology no longer reflects the current network infrastructure as shown in the following exhibit. (Click the Exhibit button.)

You need to modify the Active Directory site and subnets topology to reflect the current network infrastructure.

What should you do?
To answer, perform the appropriate actions in the simulation. (When you are finished, click the Done button.)
You are the network administrator for your company. The network consists of a single Active Directory domain. The company has a main office and two branch offices.

Due to a recent reorganization within the company, your Active Directory site topology no longer reflects the current network infrastructure as shown in the following exhibit. (Click the Exhibit button.)

You need to modify the Active Directory site and subnets topology to reflect the current network infrastructure.

What should you do?

To answer, perform the appropriate actions in the simulation. (When you are finished, click the Done button.)

STEP 3.
STEP 4.
STEP 5.
STEP 6.
STEP 7.
STEP 8.
STEP 9.
You are the network administrator for your company. The network consists of a single Active Directory domain. The company has a main office and two branch offices.

Due to a recent reorganization within the company, your Active Directory Site topology no longer reflects the current network infrastructure as shown in the following exhibit. (Click the Exhibit button.)

You need to modify the Active Directory site and subnets topology to reflect the current network infrastructure.

What should you do?

To answer, perform the appropriate actions in the simulation. (When you are finished, click the Done button.)

This window can be resized.

STEP 10.
QUESTION 2
!!! Same simulation as Question Exam F #15 with different printscreens !!!

SIMULATION
You are the network administrator for Fabrikam.com. The network consists of a single Active Directory domain.

All client computer accounts for the sales department reside in the organizational unit (OU) named Sales Computers. All user accounts for sales department employees reside in the OU named Sales Employees. These Group Policy objects (GPOs) are already linked to some of the OUs.

You need to lock down the desktops for only the users in the sales department. The desktop security settings that you need to enable must meet the following requirements:

1. Do not allow users to access Control Panel
2. Do not allow users to access Network Connections from the Start menu
3. Ensure that the My Computer icon does not appear on the desktop
4. Ensure that any changes made to the desktop do not remain when users log off

You must configure the desktop security settings without creating additional GPOs or GPO links. You want to minimize the number of GPO settings you configure.
What should you do?

A. Simulation

Answer: A
Section: (none)

Explanation/Reference:

We need to modify the GPO that applies to the Sales Employees OU.

STEP 1.
In Group Policy Management, right click the Sales Employees OU GPO and select "Edit" to open Group Policy Editor.
STEP 2.
The first requirement of the question is: Do not allow users to access Control Panel. Expand User Configuration > Administrative Templates and click the Control Panel Folder.
STEP 3.
Double click "Prohibit access to the Control Panel", select Enabled and click OK.
STEP 4.
The second requirement of the question states: Do not allow users to access Network Connections from the Start menu.

In Group Policy Editor, click the "Start Menu and Taskbar" folder.
STEP 5.
Double click "Remove Network Connections from Start Menu", select Enabled and click OK.
STEP 6.
The third requirement of the question states: Ensure that the My Computer icon does not appear on the desktop.

In Group Policy Editor, click the "Desktop" folder.
STEP 7.
Double click "Remove My Computer icon on the desktop", select Enabled and click OK.
STEP 8.
The fourth requirement of the question states: Ensure that any changes made to the desktop do not remain when users log off.
The option we need to configure is also under the "Desktop" folder.
STEP 9.
Double click "Don't save settings at exit", select Enabled and click OK.
QUESTION 3
SIMULATION
You are the domain administrator for your company's Active Directory domain. You create a custom console to manage schema objects.

You install a new version of a custom application. The old version of the custom application created a custom Active Directory schema class named entity, which is not used by the new version. The new version creates a custom schema named dataObject.

You need to ensure that no new directory objects can be created by using the entity class, and that objects created by the dataObject class will be visible in Active Directory. You also need to ensure that a user named Bruno will be able to administer Active Directory schema.
What should you do?

A. Simulation

**Answer:** A

**Section:** (none)

**Explanation/Reference:**

In this question, we need edit the properties of two schema classes in the "Active Directory Schema.msc" - dataObject and entity.

dataObject: we need to enable "Show objects of this class while browsing" and "Class is active"

entity: we need disable both those options.

**STEP 1.**

**STEP 2.**
Press Start button > Programs > Administrative tools > Active Directory Schema.msc
Note:
If Schema.msc does not appear in a list, we need to first register the schmmgmt.dll library
by pressing Start > RUN and typing: **regsvr32 schmmgmt.dll**.
Press OK. We should receive a success confirmation.

STEP 3.
Go to dataObject schema class > right click > Properties
STEP 4.
In General tab, ensure that "Show objects of this class while browsing" and "Class is active" are enabled.
STEP 5.
Go to entity schema class and uncheck the both "Show objects of this class while browsing" and "Class is active"
STEP 6.

You are the domain administrator for your company's Active Directory domain. You create a custom console to manage schema objects. You install a new version of a custom application. The old version of the custom application created a custom Active Directory schema class named `entity`, which is not used by the new version. The new version creates a custom schema class named `dataObject`.

You need to ensure that no new directory objects can be created by using the `entity` class, and that objects created by using the `dataObject` class will be visible in Active Directory. You also need to ensure that a user named Bruno will be able to administer the Active Directory schema.

What should you do?
To answer, perform the appropriate actions in the simulation. (When you are finished, click the **Done** button.)
STEP 7.
We need add Bruno's account to Schema Admins group by using Active Directory
Users
and Computers
STEP 9.
We know that only Enterprise Admins group and Schema Admins group have permission to make changes in Active Directory Schema, so we need ensure that Bruno is member of Schema Admin group. Making Bruno member of Enterprise Admins group will grant him too much unnecessary permissions.
You are the domain administrator for your company's Active Directory domain. You create a custom console to manage schema objects. You install a new version of a custom application. The old version of the custom application created a custom Active Directory schema class named `entity`, which is not used by the new version. The new version creates a custom schema class named `dataObject`.

You need to ensure that no new directory objects can be created by using the `entity` class, and that objects created by using the `dataObject` class will be visible in Active Directory. You also need to ensure that a user named Bruno will be able to administer the Active Directory schema.

What should you do?

To answer, perform the appropriate actions in the simulation. (When you are finished, click the `Done` button.)
STEP 11.

You are the domain administrator for your company's Active Directory domain. You create a custom console to manage schema objects. You install a new version of a custom application. The old version of the custom application created a custom Active Directory schema class named `entity`, which is not used by the new version. The new version creates a custom schema class named `dataObject`.

You need to ensure that no new directory objects can be created by using the `entity` class, and that objects created by using the `dataObject` class will be visible in Active Directory. You also need to ensure that a user named Bruno will be able to administer the Active Directory schema.

What should you do?

To answer, perform the appropriate actions in the simulation. (When you are finished, click the Done button.)
STEP 12.
QUESTION 4
You are a network administrator for a company that operates a call center. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers are members of the domain.

Computers in the call center are configured by a Group Policy object (GPO) to have a common, restricted desktop. All computers in the call center have accounts in an organizational unit (OU) named Call Center Computers.

Nonmanagement users have user accounts in an OU named CallCenterStaff. Managers have user accounts in an OU named ManagementUsers.

You link a GPO to the Call Center Computers OU. The current settings of the GPO are shown in the work area.

Any user logging on to these computers receives the restricted desktop. Currently, a manager who logs on to a computer in the call center is presented with the restricted desktop. The restricted desktops prevent managers from performing management tasks.

You need to ensure that any manager logging on to a computer in the call center receives a normal, unrestricted desktop.
Which GPO setting should you change?

To answer, select the appropriate setting in the work area.

<table>
<thead>
<tr>
<th>Setting</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn off background refresh of Group Policy</td>
<td>Disabled</td>
</tr>
<tr>
<td>Group Policy refresh interval for computers</td>
<td>Enabled</td>
</tr>
<tr>
<td>Group Policy refresh interval for domain controllers</td>
<td>Enabled</td>
</tr>
<tr>
<td>User Group Policy loopback processing mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Allow Cross-Forest: User Policy and Roaming User Profiles</td>
<td>Disabled</td>
</tr>
<tr>
<td>Group Policy slow link detection</td>
<td>Enabled</td>
</tr>
<tr>
<td>Turn off Resultant Set of Policy logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remove users ability to invoke machine policy refresh</td>
<td>Enabled</td>
</tr>
<tr>
<td>Disallow Interactive Users from generating Resultant Set of Policy...</td>
<td>Enabled</td>
</tr>
<tr>
<td>Registry policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Internet Explorer Maintenance policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Software Installation policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Folder Redirection policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Scripts policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Security policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>IP Security policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Wireless policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>EFS recovery policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Disk Quote policy processing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Always use local ADM files for Group Policy Object Editor</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Answer:
QUESTION 5
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 company’s written security policy requires the following account policies:

- User accounts must be automatically locked out in the event of three consecutive failed logon attempts within a 30-minute period.
- Manual administrative action must be required to unlock a user account.

You need to configure the account policies for the domain to comply with the security requirements.

What should you do?

To answer, drag the appropriate account policy setting or settings to the correct location or locations in the work area.
Explanation/Reference:
Explanation:
The Account lockout duration security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

The Account lockout threshold security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

The Reset account lockout counter after security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad
logon attempts. The available range is 1 minute to 99,999 minutes.

Reference:

QUESTION 6
DRAG DROP

TestKing has a main office and four branch offices. Each branch office is connected to the main office by a WAN connection. You configure an Active Directory site for each office. The sites and WAN connections are shown in the exhibit.

You need to create site links to minimize replication traffic over WAN connections.

Which site link or site links should you create?

To answer, drag the appropriate site link or site links to the correct location or locations in the work area.

Answer:
Explanation/Reference:
Explanation:
Each branch office is only connected to the main office. Therefore, site links should be between the main office and the branch offices, no between two branch offices.

Reference:

QUESTION 7
You are the network administrator for Tailspin Toys. The network consists of a single Active Directory forest. The functional level of the forest is Windows 2000. The forest consists of a root domain named tailspintoys.com and two child domains named child1.tailspintoys.com and child2.tailspintoys.com.


You need to be able to rename all domain controllers in tailspintoys.com. You want to minimize impact to the network.

What should you do?

To answer, drag the appropriate action or actions to the correct location or locations in the work area.
Possible Domain Action

Raise functional level of domain

Possible Forest Action

Raise functional level of forest

Work Area

Drag forest action here

Drag domain action here

tailspintoy.com

child1.tailspintoy.com

child2.tailspintoy.com

Answer:
To rename domain controllers, the domain has to be in Windows 2003 functional level.

Reference:
QUESTION 8
You are a network administrator for A. Datum Corporation. The network consists of a single Active Directory forest that contains two domains. All servers run Windows Server 2003. The domains and organizational units (OUs) are structured as shown in the work area.

Users in the research department have user accounts in the research.adatum.com domain. All other user accounts and resources are in the adatum.com domain. All domain controllers are in the Domain Controllers OU of their respective domain. No other computer or user accounts are in the Domain Controllers OUs.

A written company policy requires that all users working in the research department must use complex passwords of at least nine characters in length. The written policy states that no other users are to have password restrictions. All affected users have user accounts in an OU named Research Users in the research.adatum.com domain.

You create a Group Policy object (GPO) that contains the required settings.

You need to ensure that these settings affect the users in the research department, and that the settings do not affect any other domain users or local accounts.

Where should you link the GPO?
To answer, select the appropriate location or locations in the work area.
Select the research.adatum.com domain.

Password restrictions for domain user accounts must always be set at domain level. Password policies applied at OU level will only apply to local user accounts. In this scenario, research.testking.com contains only research users so applying the policy at the domain level will not affect any other others.

Reference:

**QUESTION 9**
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 company’s written security policy requires the following account policies:

- User accounts must be automatically locked out in the event of three consecutive failed logon attempts within a 30-minute period.
- Manual administrative action must be required to unlock a user account.
You need to configure the account policies for the domain to comply with the security requirements.

What should you do?

To answer, drag the appropriate account policy setting or settings to the correct location or locations in the work area.

Answer:

Section: (none)

Explanation/Reference:
Explanation:
The Account lockout duration security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.
The Account lockout threshold security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

The Reset account lockout counter after security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes.

Reference:

QUESTION 10
You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory forest that contains a single domain named contoso.com. The network contains four Windows Server 2003 domain controllers. The DNS Server service is running on two Windows Server 2003 member servers in the domain.

You decide to create a new child domain named dev.contoso.com in the forest. You install Windows Server 2003 on a new server. You join the server to the contoso.com domain.

The first domain controller installed in the contoso.com domain fails because of a hardware failure. You find out that it will take several days to repair the domain controller. You decide to continue creating the new child domain. You attempt to promote the member server to a domain controller in the dev.contoso.com domain.

The promotion of the domain controller fails. You receive the following error message.

You need to resolve the error to create the new domain.

What should you do ?

A. Configure the DNS client settings on the new server to use the DNS server that is authoritative
for the contoso.com domain.
B. Configure the DNS server for the Contoso.com zone to have a zone named dev.contoso.com. Configure the zone for dynamic updates.
C. Configure one of the other contoso.com domain controllers to hold all of the operations master roles.
D. Configure one of the existing domain controllers as a global catalog server.

Answer: C
Explanation/Reference:
Explanation:
The first domain controller installed in the forest will by default, have the domain naming master operations master role. The question states that the first domain controller installed fails due to a hardware failure. This means that the forest has no domain naming master. A domain naming master is required to create additional domains in the forest. To add another domain, we need to configure one of the other testking.com domain controllers to hold at least the domain naming master role (or as the answer states, all of the operations master roles).

Incorrect Answers:
A: This is not a DNS problem.
B: This is not a DNS problem.
D: We need a domain naming master, not a global catalog server.

Reference:

QUESTION 11
HOTSPOT
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. The domain contains an organizational unit named Accounting.

The Accounting OU contains both user accounts and computer accounts. You create a Group Policy object (GPO) named Custom ADM Template and link it to the Accounting OU.

You need to apply specific security-related registry entries to all of the computer accounts in the Accounting OU. You create an ADM template named Custom Security Settings that includes the security-related registry entries.

You need to import the Custom Security Settings template into the Custom ADM Template GPO so that you can enable the new policy settings in the Custom Security Settings template.

Where should you import the Custom Security Settings template?

To answer, select the appropriate section of the GPO in the dialog box.
Select "Administrative templates" under Computer Configuration. You would import a security INF file into the SECURITY node.

But if you create an ADM file, you must add it into the ADMINISTRATIVE TEMPLATES node.

CODE
http://support.microsoft.com/kb/323639

QUESTION 12
HOTSPOT
You are the network administrator for TestKing.com. The company consists of two subsidiaries named TestKing and TestKing.com. The network consists of two Active Directory domains with two sites. The sites are named Site1 and Site2. The domains are named testking.com and fabrikam.com.

The network includes one Active Directory application partition named AppPartition1. This application partition is replicated to domain controllers in Site1 and Site2.

The network contains six domain controllers. The domain controller locations and the roles of the domain controllers are identified in the work area below.

You need to configure preferred bridgehead servers in each site. You need to configure the minimum number of domain controllers as preferred bridgehead servers such that no bridgehead servers will be automatically selected.

Which domain controller or domain controllers should you configure as preferred bridgehead servers?

To answer, select the appropriate domain controller or domain controllers in the work area.

<table>
<thead>
<tr>
<th>Domain Controller Name</th>
<th>Location</th>
<th>Role(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC1.testking.com</td>
<td>Site1</td>
<td>Domain controller</td>
</tr>
<tr>
<td>DC2.testking.com</td>
<td>Site1</td>
<td>Domain controller AppPartition1 application partition Global catalog server</td>
</tr>
<tr>
<td>DC3.fabrikam.com</td>
<td>Site1</td>
<td>Domain controller</td>
</tr>
<tr>
<td>DC4.testking.com</td>
<td>Site2</td>
<td>Domain controller</td>
</tr>
<tr>
<td>DC5.testking.com</td>
<td>Site2</td>
<td>Domain controller Global catalog server</td>
</tr>
<tr>
<td>DC6.fabrikam.com</td>
<td>Site2</td>
<td>Domain controller AppPartition1 application partition</td>
</tr>
</tbody>
</table>

Answer:
You are the network administrator for Northwind Traders. The network consists of a single Active Directory domain named northwindtraders.com. Windows Server 2003 domain controllers are located in two sites named Site1 and Site2. The domain contains an organizational unit (OU) named Accounting. The user accounts for users in the accounting department are located in the Accounting OU. Users in the accounting department can log on to any client computer.

You need to deploy an antivirus application to all computers on the network without user intervention. You also need to deploy a special accounting application to user accounts in the Accounting OU without user intervention. The accounting application must be available to users in the accounting department regardless of which computer they are using. You need to minimize the number of GPO links.

You create the Group Policy objects (GPOs) listed in the following table.
Where should you link the GPOs?

To answer, drag the appropriate GPO or GPOs to the correct domain component or components in the work area.

<table>
<thead>
<tr>
<th>Name</th>
<th>GPO section</th>
<th>Policy setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>GP01</td>
<td>Computer Configuration</td>
<td>Assign the antivirus application</td>
</tr>
<tr>
<td>GP02</td>
<td>User Configuration</td>
<td>Assign the antivirus application</td>
</tr>
<tr>
<td>GP03</td>
<td>Computer Configuration</td>
<td>Assign the accounting application</td>
</tr>
<tr>
<td>GP04</td>
<td>User Configuration</td>
<td>Assign the accounting application</td>
</tr>
<tr>
<td>GP05</td>
<td>User Configuration</td>
<td>Publish the antivirus application</td>
</tr>
<tr>
<td>GP06</td>
<td>User Configuration</td>
<td>Publish the accounting application</td>
</tr>
</tbody>
</table>

GPOs

GP01  GP02  GP03
GP04  GP05  GP06

Work Area

Site1  Site2

Drag GPO here

Drag GPO here

Drag GPO here

northwindtraders.com

Accounting OU

Drag GPO here
**Answer:**

<table>
<thead>
<tr>
<th>GPOs</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GP01</td>
<td>GP02</td>
<td>GP03</td>
</tr>
<tr>
<td>GP04</td>
<td>GP05</td>
<td>GP06</td>
</tr>
</tbody>
</table>

**Work Area**

![Diagram showing network structure and GPO placement](image)

**Section:** (none)

**Explanation/Reference:**

**Explanation:**

We need to apply the antivirus application to all computers on the network. This means we should configure Computer Configuration section of the GPO to assign the antivirus application and link the GPO at the Domain level. Applications can only be assigned to computers they cannot be published to computers. The only GPO that meets this is GPO1.

We also need to apply an accounting application to user accounts in the Accounting OU without user intervention. The accounting application must be available to users in the accounting department regardless of which computer they are using. This means the applications must become part of the users desktop or start menu. So we should configure User Configuration section of the GPO to assign the accounting application and link the GPO at the OU level. The only GPO that meets this is GPO4.
Reference:

QUESTION 14
You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003.

The user accounts for support staff users are located in an organizational unit (OU) named Support. All other user accounts are located in an OU named UserAccounts. As the company expands, user accounts for users other than support staff might be created in OUs other than the UserAccounts OU.

A written company policy states that all users, including support staff, must comply with the following rules:

· Users are not allowed to use offline files.
· Only support staff employees are allowed to edit the registry.

The written policy also states that any changes to these rules must be applied to the entire company as quickly as possible.

You need to enforce the written company policy by using the minimum amount of administrative effort.

Which action or actions should you take, and where should you take the action or actions?

To answer, drag the appropriate action or actions to the correct location or locations in the work area.
Possible Actions

- Link a GPO that disables the Disable registry editing tools setting.

- Link a GPO that enables the Prevent use of offline files folder setting.

- Link a GPO that enables the Disable registry editing tools setting.

- Block policy inheritance.

Targets

Domain

![Domain Targets]

Support OU

![Support OU Targets]

User Accounts OU

![User Accounts OU Targets]

Answer:
Possible Actions

- Link a GPO that disables the **Disable registry editing tools** setting.
- Link a GPO that enables the **Prevent use of offline files folder** setting.
- Link a GPO that enables the **Disable registry editing tools** setting.
- Block policy inheritance.

Targets

Domain

- Link a GPO that enables the **Disable registry editing tools** setting.
- Link a GPO that enables the **Prevent use of offline files folder** setting.

Support OU

- Link a GPO that disables the **Disable registry editing tools** setting.

User Accounts OU

- Drag action here
- Drag action here

Section: (none)
**Explanation/Reference:**

**Explanation:**
All users, including support staff, are not allowed to use offline files and only support staff employees are allowed to edit the registry. This means we need an OU at the domain level that disables the registry editing tools, and one that prevents the use of offline tools. These GPOs will ensure that all users, including support staff, are not allowed to use offline files. It will also disable the use of registry editing tools for all users. Therefore, we need another GPO that allows the use of the registry editing tools for the Support OU. GPOs are applied at the domain level before the OU level so the GPO applied at the OU level will override the GPO applied at the domain level.

**Reference:**

**QUESTION 15**
**DRAG DROP**
You are the network administrator for TestKing.com. The network consists of a single Active Directory forest that contains two domains with three sites. Domain1 is used as an empty root domain for security purposes. Domain1 has a domain controller only in Testking1. Domain2 has domain controllers in all three sites.
The domain controllers in Testking1 and Testking2 are global catalog servers. Each client computer on the network runs Windows NT Workstation 4.0, Windows 2000 Professional, or Windows XP Professional.
You and your administration staff are located at Testking1, where you perform administrative tasks. You want to minimize network traffic as much as possible. The number of user accounts per site for each domain is shown in the following table.

<table>
<thead>
<tr>
<th></th>
<th>Testking1</th>
<th>Testking2</th>
<th>Testking3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users - Domain1</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Users - Domain2</td>
<td>5</td>
<td>100</td>
<td>25,000</td>
</tr>
</tbody>
</table>

You are planning the placement of the operations master role holders. You need to place your operations master roles in the appropriate sites.

How many operations master roles should you place in each site?
To answer, drag the appropriate number of roles to the correct locations in the work area.
Domain1 had one domain controller only in the Testking1 site. Therefore, the domain controller in Domain1 will need all five FSMO roles: the Schema role, the Domain Naming Master role, the Primary Domain Controller (PDC) Emulator Role, the Relative Identifier (RID) Master Role, and the Infrastructure Master Role.

Domain2 has domain controllers in all three sites but most users are in site Testking3. The two forest-wide roles - the Schema role and the Domain Naming Master role - cannot be assigned again. This leaves us with three roles. The Primary Domain Controller (PDC) Emulator Role and the Relative Identifier (RID) Master Role should be in the site with the most users, and the Infrastructure Master Role can be placed in the remaining site.

Reference:
QUESTION 16
HOTSPOT You are a network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. The domain consists of four sites as shown in the work area.

Pedro is another administrator for TestKing.com. Pedro is responsible for managing the frequency of Active Directory replication among the four sites.

You need to allow Pedro to manage the frequency of intersite replication. You must ensure that Pedro cannot modify any other objects.

Where should you grant Pedro the permission that he needs?

To answer, select the appropriate node in the dialog box.

Answer:
**Section:** (none)

**Explanation/Reference:**
Explanation:
Select "Inter-Site Transports". Pedro needs to manage intersite replication. This is managed through the Inter-Site Transports node in Active Directory Sites and Services.

Reference:

**QUESTION 17**
MULTIPLE HOTSPOT
You are the network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. All client computers run Windows XP Professional.

A written TestKing policy requires all documents created by the legal department to be saved to a shared folder named MyDocs on a file server named FileS1. The written policy also states that each user in the legal department must have a unique folder in which to store the user's documents.

The user accounts for all users in the legal department are in an organizational unit (OU) named Legal. The users belong to various Active Directory groups.

You create a new Group Policy object (GPO) and link it to the Legal OU. In the GPO, you open the properties of the Folder Redirection setting for My Documents folder. The dialog box is shown in the work area.

You need to configure folder redirection by using the minimum amount of administrative effort.

How should you configure the folder redirection settings?

To answer, configure the appropriate option or options in the dialog box.
Section: (none)

Explanation/Reference:
Explanation:
Select "Basic - Redirect everyone's folder to the same location"
Select "Create a folder for each user under the root path"

Reference:
Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003
QUESTION 18
You are a network administrator for TestKing.com. The network consists of a single Active Directory domain named testking.com. The domain contains three sites named MainOffice, EastCoast, and WestCoast. Each site contains four domain controllers and 100 client computers. One server in the EastCoast site is named TestKing1. All DNS servers contain Active Directory-integrated zones.

Other administrators report that they cannot connect to TestKing1 when attempting to perform Active Directory administration. They report they can perform these tasks locally at TestKing1. You verify that Server1 is operational and that file and print resources are accessible by using the host name.

You need to ensure that administrators can perform Active Directory administration on TestKing1 without requiring physical access to the server.

What should you do?

A. On Server1, force registration of DNS hosts (A) resource records.
B. On Server1, restart the Net Logon service.
C. Install DNS on TestKing1.
D. Configure TestKing as a local bridgehead server for the EastCoast site.

Answer: B
Section: (none)

Explanation/Reference:
Explanation:
TestKing1 is a domain controller. We know this because administrators are trying to perform Active Directory administration on TestKing1. File and print resources on TestKing1 are accessible by using the host name. This means that the A records are present in DNS. The problem in this question is that the SRV records are missing. We need to restore the SRV in DNS.

The Net Logon service on a domain controller registers the DNS resource records required for the domain controller to be located in the network every 24 hours. To initiate the registration performed by Net Logon service manually, you can restart the Net Logon service.

Incorrect Answers:
A: File and print resources on TestKing1 are accessible by using the host name. This means that the A records are present in DNS.
C: It is not necessary to install DNS on TestKing1.
D: TestKing1 does not need to be a bridgehead server to enable the administrators to access it.

Reference: