QUESTION 1
You are a network administrator for Certkiller . The network consists of a single Active Directory forest that contains three domains. The functional level of the forest and of all three domains is Windows Server 2003. Certkiller has a main office and 30 branch offices. Each branch office is connected to the main office by a 56Kbps
WAN connection.
You configure the main office and each branch office as a separate Active Directory site. You deploy a Windows Server 2003 domain controller at the main office and at each branch office. Each domain controller is configured as a DNS server.
You can log on to the network from client computers in the branch offices at any time. However, users in the branch offices report that they cannot log on to the network during peak hours.
You need to allow users to log on to the network from branch office computers. You do not want to affect the performance of the branch office domain controllers. You need to minimize Active Directory replication traffic across the WAN connections.
What should you do?

A.Use Active Directory Sites and Services to enable universal group membership caching for each branch office site.
B.Use the DNS console to configure the branch office DNS servers to forward requests to a DNS server in the main
office.
C.Use Active Directory Sites and Services to configure each branch office domain controller as a global catalog server.
D.Use the DNS console to configure the branch office DNS servers to use an Active Directoryintegrated zone.

Answer: A

Explanation: When a user logs on to the network, the global catalog provides universal group membership information
for the account to the domain controller processing the user logon information. If a global catalog is not available when a
user initiates a network logon process, the user is able to log on only to the local computer unless the site has been
specifically configured to cache universal group membership lookups when processing user logon attempts. In this
scenario the domain controller must contact the global catalog server across a WAN link that is saturated. Enabling
universal group membership caching will overcome this problem.
Incorrect
Answers:
B:When users log on, the requests are sent to the global catalog not the DNS server.
C:Configure each branch office domain controller as a global catalog server would result in increased replication traffic.
We want to avoid this.

D:An Active Directoryintegrated
zone is a DNS zone that is part of Active Directory and is part of Active Directory
replication. Making the DNS zone a part of Active Directory will not overcome logon latency and will lead to an
increase in replication traffic.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-43.

QUESTION 2
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The functional level of the domain is Windows Server 2003.
You configure two Active Directory sites named Certkiller 1 and Certkiller 2. Certkiller 1 contains all of the
operations masters and two global catalog servers. Certkiller 2 contains a domain controller named Server1.
You create a site link named SiteLink1 that includes Certkiller 1 and Certkiller 2.
You need to provide global catalog services locally in Certkiller 2.
Which Active Directory component should you configure?
To answer, select the appropriate component in the work area.

Answer:

Explanation: 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 5-41 to 5-45,5-48 to 5-50
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
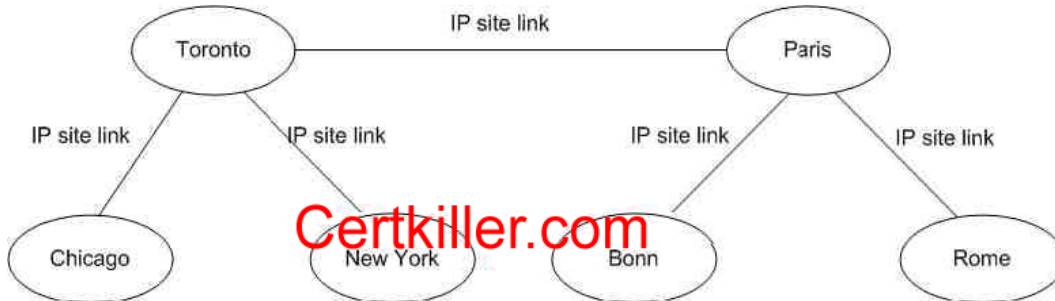Shinder, MCSE: Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543,
547,
550-552.

QUESTION 3

You are a network administrator for Certkiller . The network consists of two Active Directory domains. All servers run Windows Server 2003. Certkiller has offices in several cities as shown in the exhibit.

```
            IP site link
Toronto ————————————————— Paris

IP site link   IP site link       IP site link   IP site link

Chicago      New York           Bonn              Rome
```

Certkiller.com

Each office is configured as an Active Directory site. There are global catalog servers in the Toronto and Paris sites. You enable universal group membership caching for all other sites.
Users in your company use an application that is integrated with Active Directory. The application reads data from the global catalog. Users report that during periods of peak activity, the application responds slowly.
You need to improve the response time of the application.
What should you do?

A.Disable universal group membership caching in the Chicago, New York, Bonn, and Rome sites.
B.Decrease the replication interval on the site links that connect the Chicago and New York sites to the Toronto sites,
and on the site links that connect the Bonn and Rome sites to the Paris site.
C.Configure global catalog servers in the Chicago, New York, Bonn, and Rome sites.
D.Perform an offline defragmentation of the Active Directory database on the domain controllers in the Toronto and
Paris sites.

Answer: C

Explanation: The application reads data from the global catalog, however, there are Global Catalog servers only in
Toronto and Paris. Therefore, global catalog information must be accessed across the WAN links, which is where the
problem occurs. We need to add Global Catalog serversin the Chicago, New York, Bonn, and Rome sites.
Incorrect Answers:
A:Universalgroup membership caching is used for logon purposes. It is thus irrelevant to this scenario.
B:Decreasing the replication interval will not improve response times. The Chicago, New York, Bonn, and Rome sites
must still access the global catalog information across the WAN links.
D: Chicago, New York,
Bonn, and Rome sites must still access the global catalog information across the WAN links.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50.

Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active
Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 547, 550-552.

QUESTION 4

You are the network administrator for Certkiller .com. Certkiller has offices in Chicago, New York and
Toronto. Each office employs 500 people.

The network consists of a single Active Directory forest with one domain in each office. Each domain
contains two domain controllers named Certkiller 1 and Certkiller 2. All domain controllers run Windows
Server

2003. Each office is configured as an Active Directory site. The domain structure is shown in the exhibit.
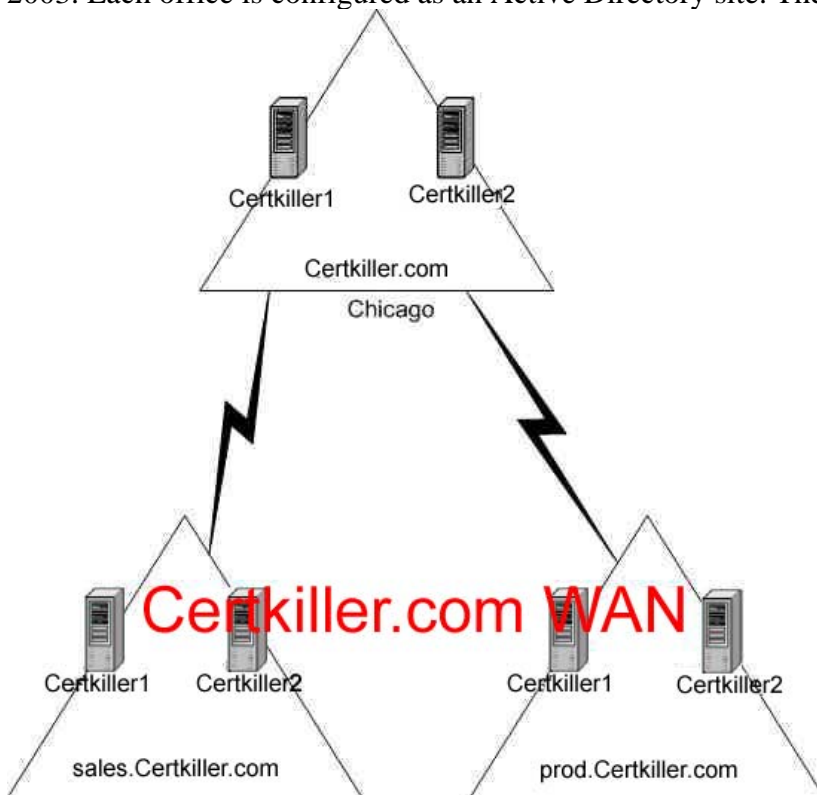
New YorkToronto

The Windows Server 2003 computer named Certkiller 1. Certkiller .com holds all operations master roles for its
domain, and it holds both forestlevel

operations master roles. The Windows Server 2003 computer named

Certkiller 1.sales. Certkiller .com and Certkiller 1.prod. Certkiller .com hold all operations master roles for their
respective domains. WAN connectivity between the offices is unreliable.

You need to plan the placement of global catalog servers for the network. You need to ensure that each user
can log on in the event of the failure of a single domain controller and WAN connection. You need to ensure
that the consistency of universal group membership information remains intact.

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

A.Configure both domain controllers in Certkiller .com as global catalog servers.
B.Configure only Certkiller 1 in each domain as a global catalog server.
C.Configure only Certkiller 2 in each domain as a global catalog server.
D.Enable universal group membership caching for each site.
E.Enable universal group membership caching for the Chicago office.
F.Enable universal group membership caching for the Toronto office and the New York office.

Answer: A, F

Explanation: We could have global catalog server s in each site. This would ensure that users can log on in the event of
a WAN connection failure. However, we also need to ensure the consistency ofuniversal group membership
information. Therefore, placing global catalog servers in the remote sites are not an option. Instead, we need to enable
universal group membership caching for both remote sites. For redundancy purposes, the main site must have more than
one global catalog.
Incorrect Answers:
B, C:For redundancy purposes, the main site must have more than one global catalog.
E:We need to enable universal group membership caching for both remote sites.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543, 547,
550-552.

QUESTION 5
You are a network administrator for Certkiller .com. The network consists of two Active Directory domains.
All servers run Windows Server 2003. Certkiller has offices in New York and Rome. The two offices are connected by a 128Kbps
WAN connection. Each office is configured as a single domain. Each office is also
configured as an Active Directory site.
Certkiller stores printer location information in Active Directory. Users frequently perform searches of
Active Directory to find information on printers by selecting the Entire Directory option. Users in the New
York Office report that response time is unacceptably slow when searching for printers.
You need to improve the response time for users in the New York office.
What should you do?

A.Place a domain controller for the Rome domain in the New York office.

B.Place a domain controller for the New York domain in the Rome office.
C.Enable universal group membership caching in the New York office.
D.Configure a global catalog server in the New York office.

Answer: D

Explanation: 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.
Incorrect Answers:
A:This would work but it is unnecessary.Replicating the entire Active Directory from the Rome office to the New York
office over the slow WAN link is a waste of resources.A global catalog server in the New York office would suffice.
B:This won't solve the problem at all.
C:Universal Group caching (as its name implies) caches information about universal groups.This scenario involves
searching for printers which is nothing to do with universal groups.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,
pp.31, 543, 547, 550-552.

QUESTION 6
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
forest that contains a forest root domain named Certkiller .com and a child domain named child2. Certkiller
.com
The functional level 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. Certkiller .com domain contains a Windows 2000 Server computer named Certkiller 1. Certkiller 1
runs an application that makes frequent LDAP queries to the global catalog. Certkiller 1 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 Certkiller 1 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 theHKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailureskey to the
registry on all domain controllers in Site2.
D.Remove Server1 from the child1. Certkiller .com domain and add it to a workgroup.

Answer: B

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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,54-85 to 5-0.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543, 547,
550-552.

QUESTION 7
You are a network administrator for Certkiller .com. The relevant portion of your network configuration is shown in the work area.
Certkiller 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 install Windows Server 2003 on all domain controllers. You create a single Windows Server 2003 Active Directory domain. The functional level of the forest is Windows Server 2003. You configure servers as shown in the following table.

Server name	Configuration
Certkiller 1	Domain controller, domain naming master, schema master
Certkiller 2	Domain controller, PDC emulator master, relative ID (RID)
Certkiller 3	Member server, file and print server
Certkiller 4	Member server, Web server
Certkiller 5	Domain controller
Certkiller 6	Member server, file and print server

You need to plan the placement of global catalog servers for Certkiller .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.
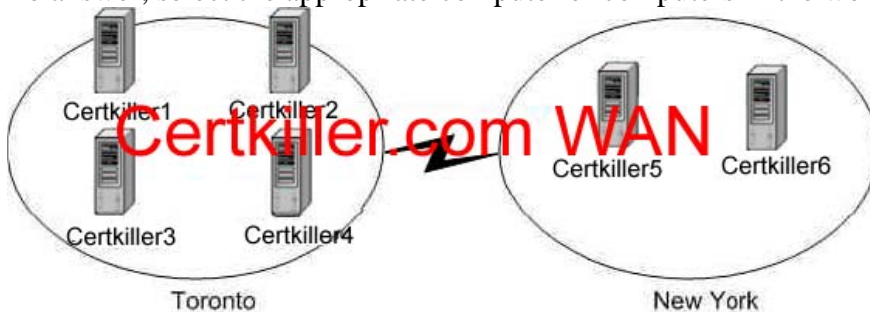
Answer:

Explanation: Select Certkiller 1, Certkiller 2 and Certkiller 5.
Only domain controllers can function as Global Catalog servers. In this case, only Certkiller 1, Certkiller 2 and Certkiller 5
are domain controllers. We need to use all domain controllersto ensure that the application continues to function in the
event of multiple global catalog failures.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 11-7 to 11-8,5-41 to 5-45,5-48 to 5-50.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543, 547,
550-552.

QUESTION 8
You are a network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains 30 domains. Certkiller has 400 offices. The network contains 150,000 user objects. All servers run Windows Server 2003.
You are responsible for administering the marketing department, which has offices in North America and Europe, as shown in the work area. Offices in Toronto, Chicago, and New York are part of the america. Certkiller .com domain. Offices in Paris, Bonn, and Rome are part of the europe. Certkiller .com domain.
The number of users in each office is shown in the following table.

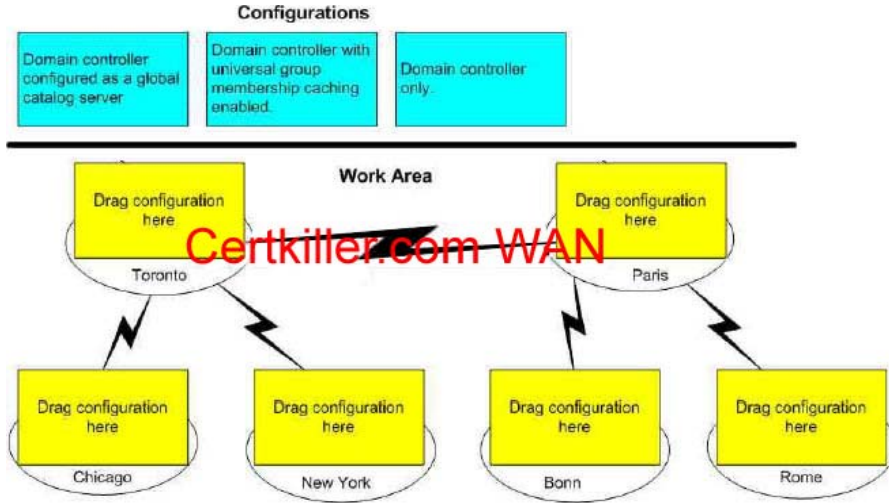| Office	Number of users
Toronto	750
Chicago	20
New York	650
Paris	650
Bonn	10
Rome	15

Users in the Bonn, New York, and Toronto offices require access to a directoryenabled application that
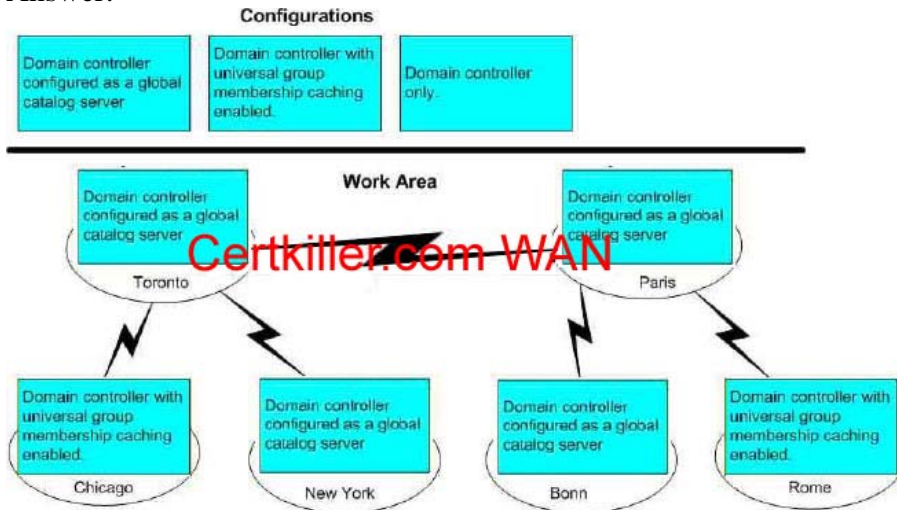stores configuration information in the global catalog.
You need to plan the placement of domain controllers for the network. You need to ensure that each user can log on without using cached credentials and that users have access to the application if a WAN connection fails. You need to achieve this goal while minimizing the increase in WAN traffic.

What should you do?

To answer, drag the appropriate domain controller configuration or configurations to the correct location or locations in the work area.

Configurations

Domain controller configured as a global catalog server	Domain controller with universal group membership caching enabled.	Domain controller only.

Work Area

Drag configuration here — Toronto

Drag configuration here — Paris

Certkiller.com WAN

Drag configuration here — Chicago

Drag configuration here — New York

Drag configuration here — Bonn

Drag configuration here — Rome

Answer:

Configurations

Domain controller configured as a global catalog server	Domain controller with universal group membership caching enabled.	Domain controller only.

Work Area

Domain controller configured as a global catalog server — Toronto

Domain controller configured as a global catalog server — Paris

Certkiller.com WAN

Domain controller with universal group membership caching enabled. — Chicago

Domain controller configured as a global catalog server — New York

Domain controller configured as a global catalog server — Bonn

Domain controller with universal group membership caching enabled. — Rome

Explanation:

Because the applicationstores configuration informationin the Global catalog, we need to put one Global Catalog server

in each site that host users who require access to the application; in this case Bonn, New York, and Toronto.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 505509,

543,547, 550-552.

Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50.

QUESTION 9
You are a network administrator for Certkiller 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.
Certkiller 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.
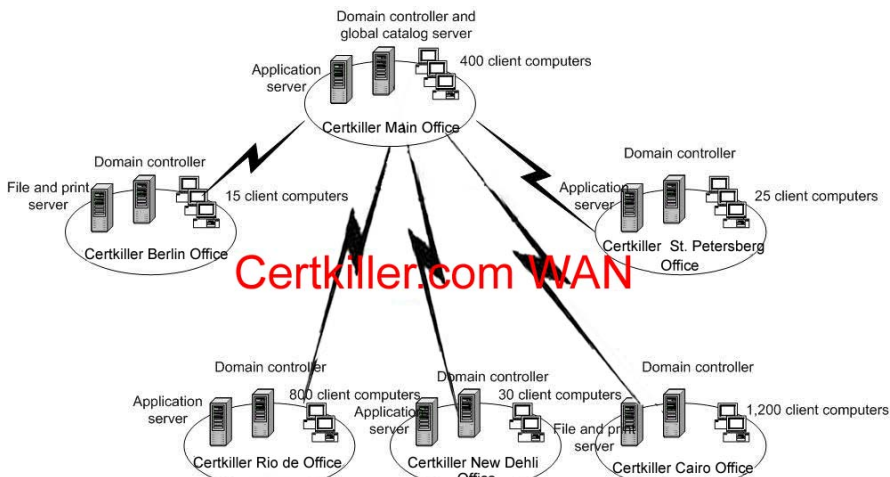
You monitor the WAN connections between the main office and each branch office and discover that the utilization increased from 70 percent to 90 percent. Users report slow response times when accessing information on the application server.
You need to place global catalog servers in offices where they 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)
A.Berlin
B.Rio de Janeiro
C.New Delhi
D.St Petersburg
E.Cairo

Answer: B, C, D

Explanation: Because the application server queries Global catalog attributes, we need to put one Global Catalog
Incorrect Answers:
A:Berlin does not host an application server and therefore does not require a Global Catalog Server.
Reference:
Michael Cross, Jeffery
A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31,
505509.

QUESTION 10
You are the administrator of the Certkiller company network. Certkiller has a main office and a small branch
office.Each office is configured as an Active Directory site in the Certkiller .com domain.All servers run
Windows Server 2003 and all client computers run Windows XP Professional.The branch office is connected
to the main office by a 128Kbps WAN link.Two domain controllers are located in each office.The main office
domain controllers are named MainDC1 and MainDC2.The branch office domain controllers are named
BranchDC1 and BranchDC2.MainDC1 is an Active Directoryintegrated
DNS server and a global catalog
server.
Users in the branch office report that it takes a long time to log on to the network. You need to reduce the
logon time for users in the branch office.
What should you do?
A.Install another domain controller in the branch office.
B.In Active Directory Sites and Services, enable universal group membership caching for BranchDC1.
C.In Active Directory Sites and Services, move MainDC2 to the branch office site.
D.Decrease the value of the replication interval at the site link between main office and the branch office.

Answer: B

Explanation: It takes a long time to log on in the branch office because the branch office domain controller
needs to
contact the global catalog server (MainDC1) over a slow WAN link. A global catalog server is a domain
controller that
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.
We can improve the logon times for the branch office users by enabling universal group membership caching
on a
branch office domain controller. 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.
Incorrect Answers:
A, C:Adding another domain controller in the branch office won't improve logon times.
D:Reducing the replication interval will not overcome the problem of thebranch office domain controller needs

to
contact the global catalog server (MainDC1) over a slow WAN link
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active
Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543,
547,
550-552.

QUESTION 11
You are a network administrator for Certkiller .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 Certkiller 1 to be a domain controller for an existing
child domain. Certkiller 1 is located at a new branch office and you connect Certkiller 1 to a central data center
by a persistent VPN connection over a DSL line. Certkiller 1 has a single replication connection with a
bridgehead domain controller in the central data center.
You configure DNS on Certkiller 1 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 Directoryintegrated
zones.
B.Configure Certkiller 1 to be the PDC emulator for the domain.
C.Configure Certkiller 1 to be a global catalog server.
D.Configure universal group membership caching on Certkiller 1.

Answer: C, D

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 Certkiller 1 to be a global catalog
server, or
by enabling universal group membership caching on Certkiller 1.
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:InActive Directoryintegrated
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 downlevel
clients).
Reference:
David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70294): Que
Publishing, Indianapolis, 2004, Chapter 5
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 117 to 118,541 to 545,548 to 550.
J. C. Mackin, Ian McLean, MCSA/MCSE selfpaced
training kit (exam 70291):
Implementing, Managing, and
Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond,
Washington,
2004,pp. 430.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543,
547,
550-552.

QUESTION 12
You are the network administrator for Certkiller .com. Certkiller has offices in Toronto, New York, and
Chicago. The network connections are shown in the exhibit.
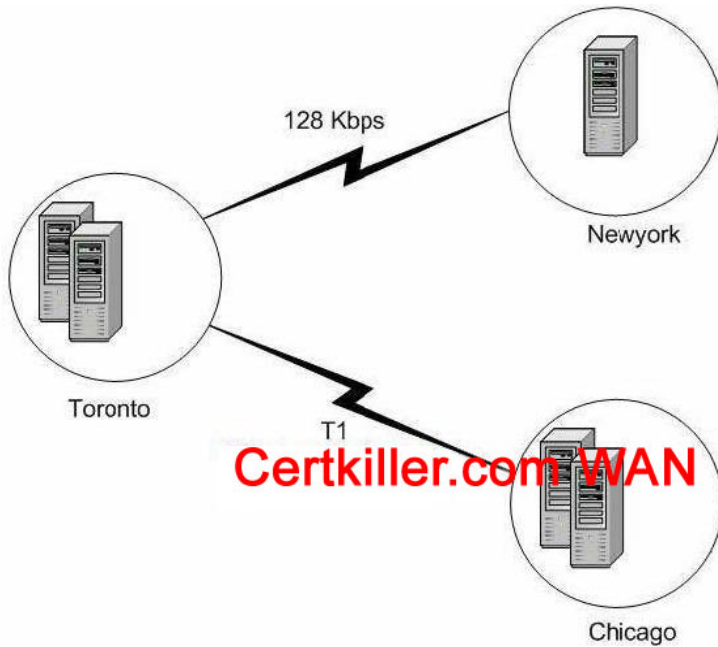
The network consists of two Active Directory domains. User objects for users in the Toronto office and the New York office are stored in the Certkiller .com domain. User objects for users in the Chicago office are stored in the production. Certkiller .com. Active Directory is configured as shown in the following table.

Location	Numbers of Users	Number of Domain Controllers	Number of global Catalog servers
Toronto	650	4	2
New York	15	1	0
Chicago	500	3	2

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?
A.Configure the domain controller in the New York office as a global catalog server.
B.Configure Active Directory to cache universal group membership 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

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 speed up 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:

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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50.

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543, 547,

550-552.

QUESTION 13 HOTSPOT

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains multiple domains. The functional level of the forest is Windows Server 2003.
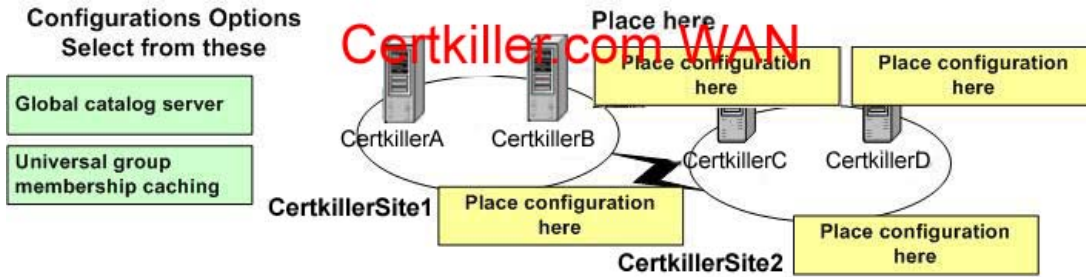
The forest contains several Active Directory sites that represent branch offices and a site named MainOffice that represent the central data center. A site named Branch1 contains one domain controller named Server1 that is not a global catalog server. The MainOffice site contains one domain controller named Server2 that is a global catalog server.

You need to use universal group membership caching in the Branch1 site.

Which component pr components should you configure?

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

Answer:

Explanation: Select the "NTDS Site Settings" for the Branch1 office in the right hand pane.
Universal group membership caching, is enabled or disabled in the NTDS Settings Properties dialog box of the Active
Directory Sites and Services console. This must be performed in the site where you want to enable universal group
membership caching, i.e., in the Branch1 site.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-41 to 5-45,5-48 to 5-50.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543, 547,
550-552.

QUESTION 14
You are the network administrator for Certkiller .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 Certkiller Site1 and Certkiller Site2. Certkiller Site1 contains two domain controllers that are global catalog servers named Certkiller A and Certkiller B.
Certkiller Site2 contains two domain controllers that are not global catalog servers named Certkiller C and Certkiller D. The two sites are connected by a WAN connection. Users in Certkiller Site2 report that logon times are unacceptably long.
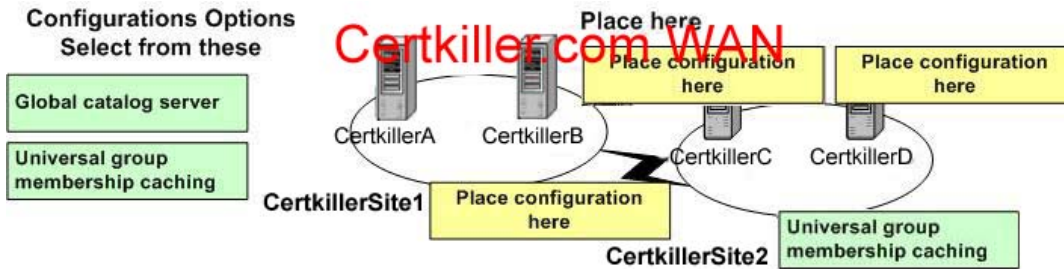You need to improve logon times for the users in Certkiller Site2 while minimizing replication traffic on the WAN connection.
How should you configure the network?
To answer, drag the appropriate configuration option or options to the correct location or locations in the work area.

Configurations Options
Select from these

Certkiller.com WAN

Place here
Place configuration here

Place configuration here

Global catalog server

Universal group membership caching

CertkillerA   CertkillerB   CertkillerC   CertkillerD

CertkillerSite1

Place configuration here

Place configuration here

CertkillerSite2

Answer:

Configurations Options
Select from these

Certkiller.com WAN

Place here
Place configuration here

Place configuration here

Global catalog server

Universal group membership caching

CertkillerA   CertkillerB   CertkillerC   CertkillerD

CertkillerSite1

Place configuration here

Universal group membership caching

CertkillerSite2

Explanation:
We need to improve logon times for the users in Certkiller Site2 while minimizing replication traffic on the WAN
connection.Logon times in Certkiller Site2 are slow because the domain controllers need to contact a global catalog
server in Certkiller Site1 for universal group information.We can prevent this by enabling Universal group membership
caching in Certkiller Site2.Enabling Universal group membership caching at the site level will ensure that all the domain
controllers in Certkiller Site2 will be able to cache the information.We could improve logon times by placing a global
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 Server2003 to cache universal group memberships
by using the Active Directory Sites and Services snapin.
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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-46.
Michael Cross, Jeffery

A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active
Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543,
547,
550-552.

QUESTION 15
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory that
contains two domains named Certkiller .com and chicago. Certkiller .com. The functional level of the forest is
Windows Server 2003. The network contains two sites named New York and Chicago. A 128Kbps
site link
connects the New York and Chicago sites.
The Certkiller .com domain contains a domain controller named CK1 in the New York site. The Chicago
Certkiller .com domain contains a domain controller named CK2 in the Chicago site. CK1 is an Active
Directoryintegrated
DNS server and a global catalog server. There are 1,500 users in the New York site
and 80 users in the Chicago site.
Users in the Chicago site report that it takes a long time to log on to the network. You need to ensure that
the users in the Chicago site can log on faster.
What should you do?
A.Decrease the value of theMaximum lifetime for user ticketKerberos policy in the Default Domain Policy
Group
Policy object (GPO) of the chicago. Certkiller .com domain.
B.Enable universal group membership caching for CK2 in Active Directory Sites and Services.
C.Enable theInteractive Logon: Number of previous logons to cache security policy in the Default Domain
Policy
Group Policy object (GPO) of the chicago. Certkiller .com domain.
D.Decrease the value of the replication interval at the site link between the Chicago and New York sites.

Answer: B

Explanation: The reason why it takes a long time to log on to DC2 is because DC2 needs to contact DC1 over a
WAN link to obtain universal group information whenever someone logs on. The global catalog server is the
domain
controller that 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. Like all domain
controllers, a global catalog server stores full, writable replicas of the schema and configuration directory
partitions and
a full, writable replica of the domain directory partition for the domain that it is hosting.
We can prevent WAN traffic by sing Universal group membership caching. 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 snapin.

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.

Incorrect Answers:

A:Windows Server 2003 uses Kerberos for authentication purposes. It does not affect logon times.

C:TheInteractive Logon: Number of previous logons to cache security policydetermines the number of times a user

can log on to a Windows domain using cached account information. All previous users' logon information is cached

locally so that, in the event that a domain controller is unavailable during subsequent logon attempts, they are able to log

on. This is enabled by default is set to 10.

D:The problem in this scenario is not a replication problem.DC2 needs to contact DC1 over a WAN link to obtain

universal group information whenever a user logs on. Reducing the replication interval will not resolve this problem.

Reference:

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50.

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543, 547,

550-552.

Server Help: Interactive Logon

QUESTION 16

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains a single domain named Certkiller .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. Certkiller .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 message:
The operation failed because:
Active Directory could not contact the domain naming master DC1. Certkiller .com.
"The specified server cannot perform the requested operation".
The server has been disjoined from domain Certkiller .
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
Certkiller .com
domain.
B.Configure the DNS server for the Certkiller .com zone to have a zone named dev. Certkiller .com. Configure
the zone for
dynamic updates.
C.Configure one of the other Certkiller .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: 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 configureone of the other Certkiller .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 Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 501-508.

QUESTION 17
You are the network administrator for Certkiller .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 Certkiller 1. Domain2 has domain controllers in all three
sites. The domain controllers in Certkiller 1 and Certkiller 2 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 Certkiller 1, 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.

	Certkiller 1	Certkiller 2	Certkiller 3
Users Domain1	5	0	0
Users Domain2	5	100	25,000

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.

Number of Roles per Site

Work area

Certkiller1   Certkiller2   Certkiller3

1 role in site
2 role in site
3 role in site
4 role in site
5 role in site

Drag number of roles here   Drag number of roles here   Drag number of roles here

Answer:

Number of Roles per Site

Work area

Certkiller1   Certkiller2   Certkiller3

1 role in site
2 role in site
3 role in site
4 role in site
5 role in site

5 role in site   1 role in site   2 role in site

Explanation:
Domain1 had one domain controller only in the Certkiller 1 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 Certkiller 3. The two forestwide 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 4-29 to 4-30.
Windows Server 2003 Active Directory and Network Infrastructure, Microsoft Press, Redmond, Washington, 2004,
pp. 5-13 to 5-14.
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 300312, 505-508.

QUESTION 18

You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. All domain controllers run Windows Server 2003. The domain controllers are configured as shown in the following table.

Server name	Server role
CertkillerSrvA	Global catalog server, schema master, domain naming master
CertkillerSrvB	Domain controller, infrastructure master, PDC emulator
CertkillerSrvC	Domain controller
CertkillerSrvD	Global catalog server, relative ID (RID) master

You plan to take Certkiller SrvD offline for maintenance. Another network administrator plans to add 1,250 new user accounts while Certkiller SrvD is offline.
You need to ensure that the network administrator can add the user accounts while Certkiller SrvD is offline.
You also need to ensure that there is no disruption of user account creation after Certkiller SrvD is brought back online.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A.Use the Ntdsutil utility to connect to Certkiller SrvA.
B.Use the Ntdsutil utility to connect to Certkiller SrvD.
C.Remove the global catalog server role from Certkiller SrvD.
D.Add the global catalog server role to Certkiller SrvD.
E.Transfer the RID master role.

Answer: A, E

Explanation:
The RID master is assigned to allocate unique sequences of relative IDs to each domain controller in its domain.

As the
domain controllers use the IDs allocated, they contact the RID master and are allocated additional sequences as
needed. At any time, the RID master role can be assigned to only one domain controller in each domain.The
Relative ID
is part of a security ID (SID) that uniquely identifies an account or group within a domain.We will be creating
1250 new
user accounts so the domain controller will need to contact the RID master to obtain more RIDs.
We can transfer the RID master role using the ntdsutil utility.
Incorrect Answers:
B:We need to connect to the computer we will be transferring the role to, not from.
C:Removing the Global Catalog on Certkiller SrvD won't accomplish anything.
D: Certkiller SrvD is already a global catalog server.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, Chapter 1, p. 30
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs
/entserver/sag_adTransRIDMaster.

QUESTION 19
You are a network administrator for Certkiller . Certkiller has 25 offices in major cities throughout the world.
The network consists of a single Active Directory forest that contains five domains. All domain controllers
run Windows 2000 Server. Each domain contains user objects for five offices.
The offices in Paris and Toronto provide help desk services to 20,000 users in all domains. The help desk
frequently processes group membership changes requested by department managers.
Help desk administrators report that changes made to group memberships are often lost and have to be
recreated.
You discover that this problem is caused by replication conflicts that occur when a large number
of help desk requests are being processed in a short period of time.
You upgrade all domain controllers to Windows Server 2003. Help desk administrators continue to report
that work is often lost during times of peak activity.
You need to reduce the amount of work lost by help desk administrators. You want accomplish this task by
using the minimum amount of administrative effort.
What should you do?
A.Ensure that all help desk administrators are connecting to the PDC emulator in their domain when they
perform
updates to group memberships.
B.Raise the functional level of the domain and of the forest to Windows Server 2003.
C.Enable universal group membership caching on domain controllers used by the help desk administrators.
D.Disable site link bridging for all site links in the forest.

Answer: A

Explanation: The PDC emulator master is responsible for authentication requests for accounts with recently
changed
passwords, if the change has not been replicated yet to the entire domain. In additions, the PDC emulator
receives

preferential replication of password changes performed by other domain controllers in the domain. If a password was
recently changed, that change takes time to replicate to every domain controller in the domain.
Incorrect Answers:
B:The functional level of the forestwill not reduce the amount of replication that occurs at any one time.
C:Universal group membership caching enables users to log on to the domain when the WAN link is down. The helpdesk
staff is already logged on.
D:Site link bridging won't reduce the amount of replication that occurs at any one time.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,p. 426.

QUESTION 20
You are the network administrator for Certkiller .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
Certkiller .com and two child domains named child1. Certkiller .com and child2. Certkiller .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. Certkiller .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 theadprep.exe /forestprepcommand on the PDC emulator for the Certkiller .com domain.
B.Restart the schema master in Directory Services Restore Mode and run theadprep.exe /forestprepcommand.
C.Add your user account that has administrative privileges to the Enterprise Admins group.
Run theadprep.exe /forestprepcommand on the schema master.
A.Run theadprep.exe /domain prepcommand on the PDC emulator for the Certkiller .com domain.
Then run theadprep.exe /forestprepcommand on the schema master.
A.Run theadprep.exe /domainprepcommand on the infrastructure master in each domain.
Then run theadprep.exe /forestprepcommand on the schema master.

Answer: C

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,p. 3-5.2003, 2004, p 2-12 to 2-15

QUESTION 21

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory forest that contains a forest root domain named Certkiller .com and one child domain named miami. Certkiller .com. All domain controllers run Windows 2000 Server. The miami. Certkiller .com domain contains one Windows Server 2003 member server named Certkiller 2.

You attempt to promote Certkiller 2 to be an additional domain controller of the miami. Certkiller .com domain. The promotion fails and you receive the error message shown in the exhibit.

You need to resolve the error in order to promote Certkiller 2 to be an additional domain controller of the miami. Certkiller .com domain.

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

A.Force replication between the schema master and the PDC emulator of only the Certkiller .com domain.

B.Force replication between the schema master and the PDC emulator of the Certkiller .com and the miami. Certkiller .com
domain.

C.Run theadprep /forestprepcommand on the schema master of the Certkiller .com domain.

D.Run theadprep /domainprepcommand on the infrastructure master of only the Certkiller .com domain.

E.Run theadprep /domainprepcommand on the infrastructure masters of the Certkiller .com domain and the miami. Certkiller .com domain.

Answer: C, E

Explanation: To promote a Windows Server 2003 member server to a domain controller in a Windows 2000 domain,

You must run the adprep /forestprep command on the existing Windows 2000 Server domain controller holding the

schema operations master role. You must also run the adprep /domainprep command on the Windows 2000 Server

domain controller holding Infrastructure Operations Master rolefor the domain that you are going to upgrade.

Incorrect Answers:

A, B:The PDC Emulator is used for authentication purposes for Windows NT 4.0 machines.

D:You must run the adprep /domainprep command on the Windows 2000 Server domain controller holding Infrastructure Operations Master rolefor the domain that you are going to upgrade, i.e., miami. Certkiller .com.

41

Reference:

Mark Minasi, Christa Anderson, Michele Beveridge, C.

A. Callahan & Lisa Justice, Mastering Windows Server 2003,

Sybex Inc. Alameda, 2003, p.pp. 614615.

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 35.

QUESTION 22
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. The domain contains three Active Directory sites named Certkiller 1, Certkiller 2, and Certkiller 3. The sites are connected by site links as shown in the work area.
SiteLink1 and SiteLink2 include redundant, highspeed
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.

Operating system	Certkiller 1	Certkiller 2	Certkiller 3
Windows 98	50	30	550
Windows NT Workstation 4.0	50	20	550
Windows 2000 Professional	0	500	100
Windows XP Professional	100	0	0
Windows Server 2003	10	20	15

Certkiller 1 contains a Windows Server 2003 domain controller named Server1 that is the relative ID (RID) master for the domain. Certkiller 2 contains two Windows Server 2003 domain controllers named Server2 and Server3. Server2 is the infrastructure master for the domain. Certkiller 3 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.
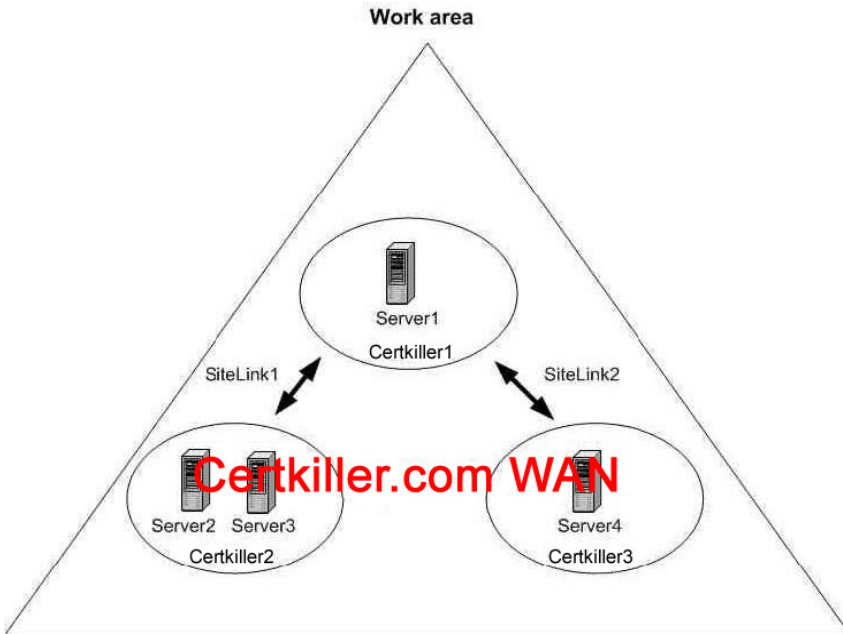
Answer: <m x1="474" x2="557" y1="384" y2="509"></m>

Explanation:
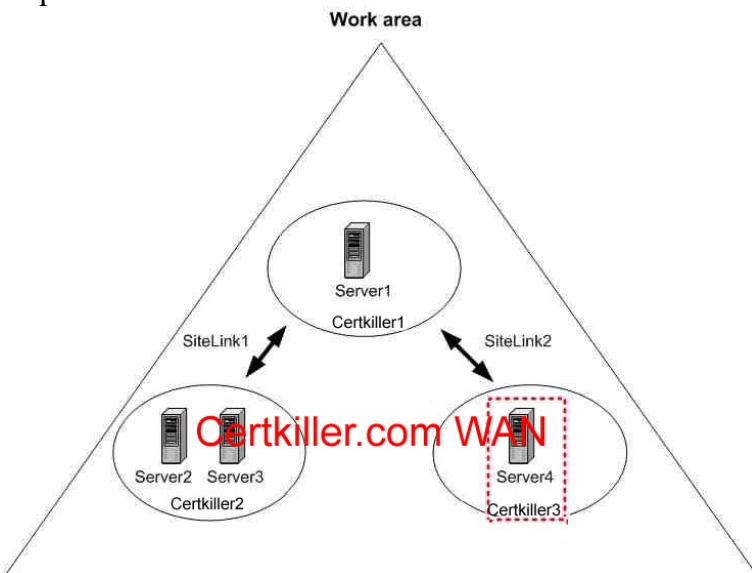
Place
the PDC emulator on Certkiller 3.This site has the most Windows 98 and NT 4.0 workstations which need a PDC
emulator to contact to logon while XP & Windows 2000 can logon at any DC.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows Server 2003,
Sybex Inc. Alameda, 2003, pp. 565567.
Michael Cross, Jeffery
A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active
Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,p.505.

QUESTION 23

You are the network administrator for Certkiller . The Certkiller network consists of a single Active Directory
forest that contains three domains: a forest root domain, named Certkiller .com, and two child domains named
asia. Certkiller .com and africa. Certkiller .com. The functional level of the forest is Windows Server 2003.
Each of the domains contains two Windows Server 2003 domain controllers named DC1 and DC2.
DC1. Certkiller .com is the schema master as well as the domain naming master. DC1 in each of the child
domains is the PDC emulator master, the relative ID (RID) master, and the infrastructure master. DC1 in
each of the three domains is also a global catalog server.
A user named Jack King is a member of the Medicine Students security group. Her user account resides in
the africa. Certkiller .com domain. Jack King marries and become Jack Edwards. Because of the name change,
the domain administrator of africa. Certkiller .com changes the Last name field of Jack user account from King
to Edwards.
However, the administrator of the asia. Certkiller .com domain discovers that the user account for Jack is still
listed as Jack King.
You need to ensure that the user account for Jack Edwards 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 on each domain.
D.Transfer the schema master role from DC1 to DC2 in the Certkiller .com domain.

Answer: B

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 grouptouser
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 domaincontroller 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:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 505-509.

QUESTION 24

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

You need to create a new child domain named NA. Certkiller .com in the forest. You install a standalone Windows Server 2003 computer named CK3 .

You use the Active Directory Installation Wizard to promote CK3 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 Certkiller \admin. You choose Certkiller .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.

MISSING

You need to be able to create the new child domain.

What should you do?

A.Enter the network credentials for a member of the local Administrative group.

B.Add CK3 to the Certkiller .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 Certkiller .com forest.

D.Enter the network credentials for a member of the Schema Admins group for the Certkiller .com forest.

Answer: C

Explanation: 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 enterthe network credentials for a member of the Enterprise Admins group for the Certkiller .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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 4-6 to 4-8

QUESTION 25
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com 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.
A.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.
A.Restart one domain controller and use a Windows Server 2003 CD to run the Recovery Console.
Stop the GPC service.
Restart the domain controller.
A.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

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-4 to 10-12,11-6

QUESTION 26
You are the network administrator for Certkiller , The network consists of a single Active Directory domain with two sites named Certkiller 1 and Certkiller 2. Certkiller 1 contains two domain controllers. Certkiller 2 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 Certkiller 2. 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 recreate
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 Certkiller 2.
B.Install an additional hard disk in each domain controller.
Move the Active Directory log files to the new hard disk.
A.Install an additional hard disk in each domain.
Move the Active Directory database file to the new hard disk.

A.Configure a new site link between Certkiller 1 and Certkiller 2.

Answer: A

Explanation: To ensure redundancy in the Certkiller 2 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 Certkiller 2
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 Certkiller 2 site
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 2-19 to 2-26

QUESTION 27
You are the administrator of Certkiller 's Windows 2003 network. The network contains two Active Directory
sites: Munich and Singapore. The network also consists of two domains: fabrikam.com and
asia.fabrikam.com. The network is configured as shown in the exhibit.

Users from the Singapore office often travel to the Munich office with their portable computers. When these
users log on to the network from Munich, their computers display the text "Applying your personal settings"
for a long time.
You want to ensure that users from Singapore do not experience these delays when they log on to the
network from Munich.
What should you do?
A.Associate the Munich subnet with the Singapore site.
B.Create a trust relationship so that fabrikam.com trusts asia.fabrikam.com.
C.Install a domain controller for asia.fabrikam.com in the Munich subnet.
D.Use the Active Directory Sites and Services snapin
to move DC3 to the Munich site.

Answer: C

Explanation: The asia.fabrikam.com domain is in the Singapore site.When a user from Singapore logs on in
Munich the
client computer connects to a domain controller in Singapore to authenticate the user and download any policy

settings.
This traffic over the WAN link is what is causing the delay.We can prevent this by installing a domain controller for the
asia.fabrikam.com domain in Munich.This way, the logon process for Singapore users in Munich can occur locally.
Incorrect Answers:
A:The Munich subnet should be associated with the Munich site.Associating the Munich subnet with the Singapore site
would cause all authentication traffic from clients in Munich to go over the WAN link to Singapore.
B:A twoway
transitive trust already exists between the domains.
D:DC3 is physically in Singapore.The logon traffic would still travel over the WAN link to DC3.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-3 to 5-6

QUESTION 28
You are the administrator of Certkiller Inc. The network consists of a single domain. The company's main office is located in South Africa and branch offices are located in Asia and Europe. The offices are connected by dedicated 256Kbps
lines. To minimize logon authentication traffic across the slow links, you create an
Active Directory site for each company office and configure site links between the sites.
Users in branch offices report that it takes a long time to log on to the domain. You monitor the network and discover that all authentication traffic is still being sent to the domain controllers in South Africa.
You need to improve network performance. What should you do?
A.Schedule replication to occur more frequently between the sites.
B.Schedule replication to occur less frequently between the sites.
C.Create a subnet for each physical location, associate the subnets with the South Africa site, and move the domain
controller objects to the South Africa site.
D.Create a subnet for each physical location, associate each subnet with its site, and move each domain controller
object to its site.

Answer: D.

Explanation: You have created the sites and configured site links, but you haven't configured the sites.To configure the
site you need to create a subnet object for each physical location and associate each subnet with its site.Then move
each domain controller object to its site.This will configure active directory so that authentication requests get sent to the
'local' domain controller rather than going across the WAN links.
Incorrect Answers:
A:No replication will occur between the sites, because all domain controllers in the same (default) site.The domain

controller objects need to be moved to their respective sites.
B:No replication will occur between the sites, because all domain controllers in the same (default) site.The domain
controller objects need to be moved to their respective sites.
C:We don't want all the subnets to be in one site.They should be in their respective sites.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-3 to 5-6

QUESTION 29
You are the network administrator for Certkiller . The network consists of a single Active Directory domain that contains only one domain controller. The domain controller is named Certkiller Srv
A. The domain
contains only one site named Valencia.
You are adding a new site named Barcelona. You need to promote an existing Windows Server 2003 member server named Certkiller SrvB to be an additional domain controller of the domain. A 56Kbps WAN connection connects the Valencia and Barcelona sites.
You need to install Certkiller SrvB as a new domain controller on the Barcelona site. You need to minimize the use of the WAN connection during this process.
What should you do?
A.Set the site link cost between the Valencia and Barcelona sites to 50.
Promote Certkiller SrvB to be an additional domain controller in the Barcelona site.
A.Restore the backup files from the system state data on Certkiller SrvA to a folder on Certkiller SrvB and install Active
Directory by running thedcpromo /advcommand.
B.Promote Certkiller SrvB to be an additional domain controller by running thedcpromocommand over the network.
C.Promote Certkiller SrvB to be an additional domain controller by using an unattended installation file.

Answer: B

Explanation: We want to minimize the use of the WAN link. We can use the newdcpromo /advcommand to promote
the DC from a backup of the system state data of an existing domain controller.
Installing from media drastically reduces the time required to install directory information by reducing the amount of data
that is replicated over the network. Installing from media is most beneficial in large domains or for installing new domain
controllers that are connected by a slow network link. To use the install from media feature, you first create a backup of
System State from the existing domain controller, then restore it to the new domain controller by using the Restore to:
Alternate location option.
In this scenario, we can restore the system state data to a member server, then use that restored system state data to
promote a member server to a domain controller.

Incorrect Answers:
A:Site link costs are a mechanism for controlling replication traffic. In this scenario we need to install Active Directory,
not control Active Directory replication.
C:Running thedcpromocommand over the network will result in large amounts of traffic across the WAN link. We want
to reduce this.
D:We could promote Certkiller SrvB to a domain controller by using unattended installation, however, Active Directory
would need to be synchronized with the Active Directory on Certkiller Srv
A. This synchronization would result in WAN
traffic that could be reduced by installing Active Directory from a backup.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 226
to 228
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 294-6, 298-300

QUESTION 30
You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains one forest root domain named Certkiller .com and two child domains named
europe. Certkiller .com and usa. Certkiller .com. The functional level of the forest is Windows 2000 native.
The Certkiller .com domain contains a Windows 2000 Server domain controller named Certkiller 3 that is running Service Pack 4 or later. You take Certkiller 3 offline. You also remove all references to Certkiller 3 from the Configuration container in Active Directory.
Five days later, you upgrade all remaining domain controllers to Windows Server 2003.You then raise the functional level of the forest to Windows Server 2003.
You need to integrate Certkiller 3 into the new Active Directory infrastructure.You want Certkiller 3 to be an additional domain controller of the europe. Certkiller .com domain.
What should you do?
A.Upgrade Certkiller 3 to Windows Server 2003.Add the computer account for Certkiller 3 into the Computers container of the europe. Certkiller .com domain.
B.Demote Certkiller 3 to a Windows 2000 member server by running thedcpromo
/forceremovalcommand.Upgrade
Certkiller 3 to a Windows Server 2003 member server. Run thedcpromocommand to promote Certkiller 3 to be an
additional domain controller of the europe. Certkiller .com domain.
C.Demote Certkiller 3 to a Windows 2000 member server by running thedcpromo /forceremovalcommand.Add the

computer account for Certkiller 3 into the Domain Controllers organizational unit (OU) of the europe. Certkiller .com
domain.
D.Upgrade Certkiller 3 to Windows Server 2003.Add the computer account for Certkiller 3 into the Domain Controllers
organizational unit (OU) of the europe. Certkiller .com domain.

Answer: B

Explanation: Once the forest functional level is raised to Windows Server 2003, you cannot add a Windows 2000
domain controller to the forest. We would need to upgrade the Windows 2000 domain controller to Windows Server
2003. However, we must first demote the Windows 2000 domain controller and then upgrade it to Windows Server
2003. Add it to the network and then promote it.
Incorrect Answers:
A, D:If we upgrade the Windows 2000 domain controller to Windows Server 2003 while it is disconnected from the
network, the upgraded computer will assume that it is the first domain controller for the domain. It will then old the RID,
Global Catalog and Schema Master roles. This will cause a conflict when we eventually add the domain controller to the
network.
C:Once the forest functional level is raised to Windows Server 2003, you cannot add a Windows 2000 server to the
forest.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
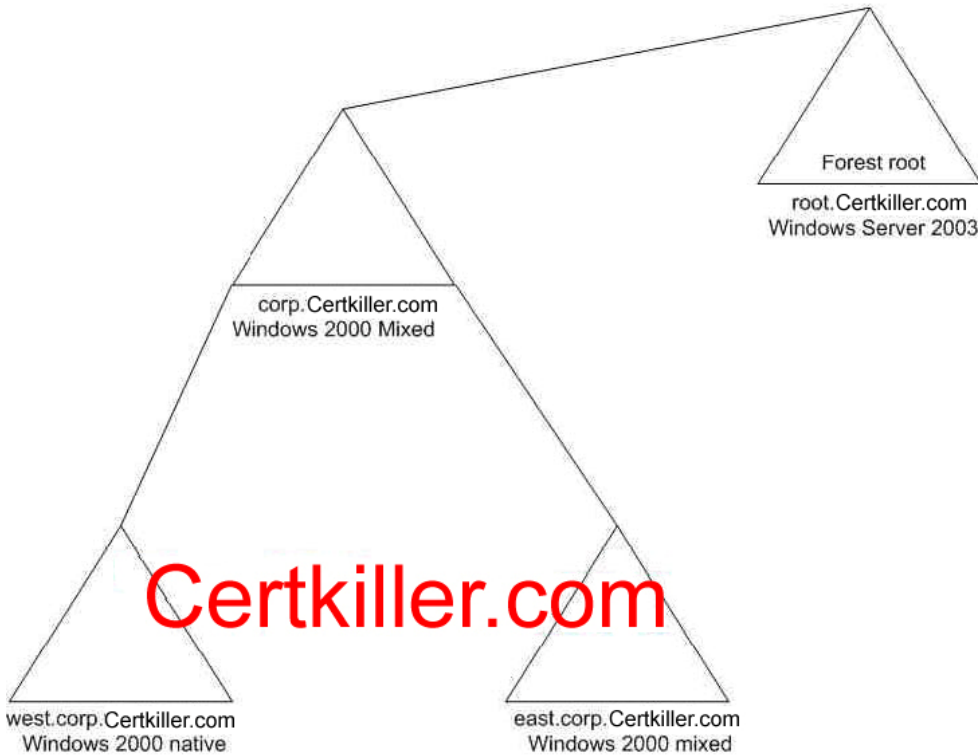and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 4-24 to 4-37

QUESTION 31
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
forest that contains three domains. The functional level of all three domains is Windows 2000 native.
Certkiller is merging with a company named Acme. The Acme network consists of a single Active Directory
forest that contains one domain named acme.com. The functional level of the domain is Windows 2000
native. The forests of both companies are shown in the exhibit.
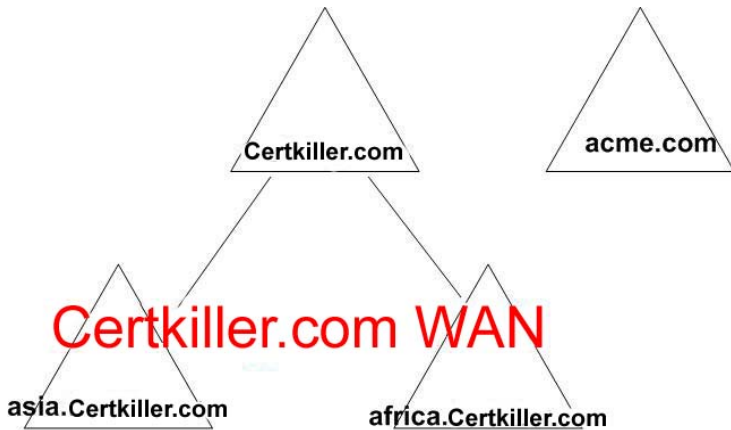
You need to allow users in each forest to fully access resources in the domains of the other forest. In addition, users must be able to log on between domains by using Kerberos authentication. You need to ensure that users can continue to access all resources by using their existing user accounts.
What should you do?
A.Demote the Windows 2000 domain controllers in the acme.com domain to become member servers.
Promote these servers into the Certkiller .com domain.
A.Demote the Windows 2000 domain controllers in the acme.com domain to become member servers.
Upgrade these servers to Windows Server 2003.
Promote the upgraded computers to become domain controllers for a new domain tree in the Certkiller forest.
A.Upgrade the Windows 2000 domain controllers in the acme.com domain to Windows Server 2003.
Create external trust relationships between the root domains of each forest.
A.Upgrade all domain controllers in both forests to Windows Server 2003.
Raise the functional level of both forests to Windows Server 2003.
Create a forest trust relationship between the root domains of each forest.

Answer: D

Explanation: To enable users in each forest to fully access resources in the domains of the other forest and log on to
either domain with Kerberos authentication, we need to create a forest trust between the two forests.To create a forest
trust, the forests must be in Windows 2003 domain functional level.This requires that all domain controllers in each
domain are running Windows server 2003.
Incorrect Answers:
A:This will decommission the acme.com domain/forest.This isn't a requirement.
B:This will decommission the acme.com forest.This isn't a requirement.
C:We need a forest trust to enable Kerberos authentication across the trust link.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,p. 4-43

QUESTION 32
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
forest, as shown in the exhibit.

Certkiller forest functional level: Windows 2000 mixed

Forest root

root.Certkiller.com
Windows Server 2003

corp.Certkiller.com
Windows 2000 Mixed

Certkiller.com

west.corp.Certkiller.com
Windows 2000 native

east.corp.Certkiller.com
Windows 2000 mixed

A domain controller named dc1.corp. Certkiller .com runs Windows 2000 Server. All other domain controllers
run Windows Server 2003.

Certkiller 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 Certkiller can log on to the litwareinc.com forest. You upgrade
dc1.corp. Certkiller .com to Windows Server 2003.

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

A.Raise the functional level of corp. Certkiller .com domain and the east.corp. Certkiller .com domain to
Windows 2000

native.

Raise the functional level of the Certkiller .com forest to Windows Server 2003.

A.Raise the functional level of the corp. Certkiller .com domain to Windows 2000 native.

Raise the functional level of the east.corp. Certkiller .com domain to Windows Server 2003.

Raise the functional level of the west. Certkiller .com domain to Windows Server 2003.

A.Create a oneway

forest trust relationship in which the Certkiller .com forest trusts the litwareinc.com forest.

B.Create a oneway

forest trust relationship in which the litwareinc.com forest trusts the Certkiller .com forest.

Answer: A, D

Explanation:
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. Certkiller .com
domain is a child domain of the corp. Certkiller .com domain.
C:The litwareinc.com forest trusts the Certkiller .com forest because Certkiller users must be able to log on to the
litwareinc.com forest.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,p. 4-43

QUESTION 33
You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest. The functional level of the forest is Windows 2000. The forest consists of a forest root domain named Certkiller .com and two child domains named asia. Certkiller .com and europe. Certkiller .com.
The functional level of all the domains is Windows 2000 mixed. Each domain contains one domain controller running Windows Server 2003. All of the other domain controllers in the forest run Windows 2000 Server.
Certkiller recently acquired another company named Acme that has an Active Directory forest named acme.com. The functional level of the forest is Windows Server 2003.
You need to be able to establish a forest trust relationship between Certkiller .com and acme.com.
What should you do?
To answer, drag the appropriate action or actions to the correct location or locations in the work area.
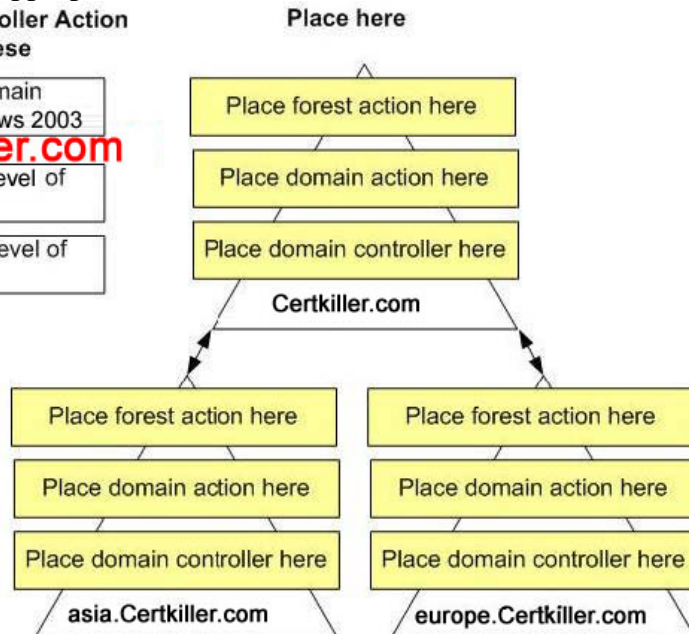
Answer:
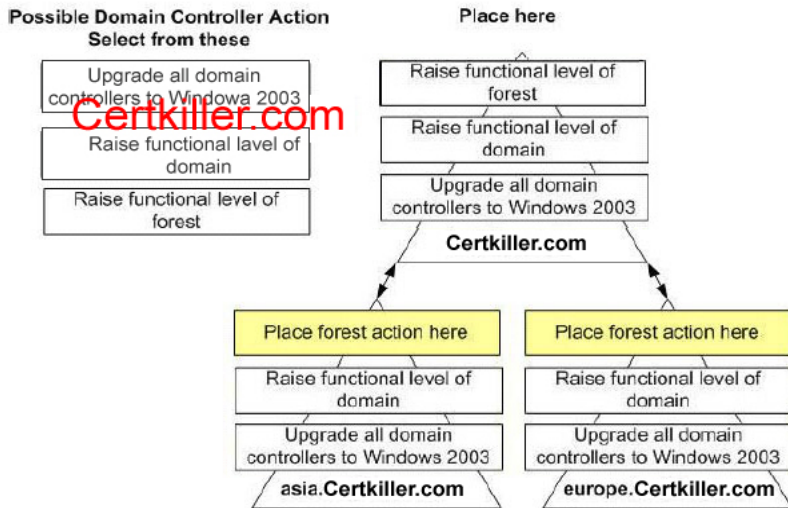
Explanation:
The question explicitly asks for a "Forest Trust Relationship", rather than just an external trust.To create a forest trust
relationship, both forests must be in Windows 2003 functional level.For this functional level, all domains must be in
Windows 2003 functional level which requires that all domain controllers are running Windows 2003 Server.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 4-46

QUESTION 34
You are the network administrator for Certkiller .com. You are implementing a new Windows Server 2003
network environment. You install one Active Directory forest root domain named cpandl.com. You install the
first domain controller named DC1. You configure DC1 as a DHCP server and as an Active
Directoryintegrated
DNS server with dynamic updates enabled. Later you install an additional domain
controller named DC2.
You cannot raise the functional level of the domain to Windows Server 2003. You discover that the service
locator (SRV) resource records of DC1 are not created in the cpandl.com zone on the DNS server. You run
the Dcdiag tool on DC1 and receive the output shown in the exhibit.

You need to make it possible to raise the functional level of the domain to Windows Server 2003.
What should you do?
A.Upgrade DC2 to a global catalog server.
B.Use the DHCP server locator utility to find out which DHCP servers are available in the cpandl.com zone.
C.Start the Net Logon service on DC1.
D.Restart the DNS Server service on DC1 to enable DNS clients to resolve host names by answering queries and
update requests.

Answer: C

Explanation: SRV records are required for clients to locate hosts that provide required services. The Netlogon service
registers a set of default SRV resource records on the DNS server. However, the exhibit indicates that the NetLogon
service is stopped on DC1.We should restart this service.
Incorrect Answers:
A: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 affect the forest level.
B:DHCP is used to assign IP configurations to DHCP clients. However, the SVR records are missing. We will thus not
be able to locate the DHCP server.
D:The DNS server does not have the SRV records. Restarting the DNS service will not generate these records.

We
should start the NetLogon service.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 4, p.
276
Server Help-NetLogon

QUESTION 35
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
forest that contains five domains and 30 remote sites located in cities throughout the world. There are a total
of 40,000 users in the five domains. All remote sites are connected to the company network by unreliable
56Kbps WAN connections.
Each site contains at least one domain controller and one global catalog server. All domain controllers in the
forest run Windows Server 2003. The functional level of all the domains in the forest is Windows 2000
native.
You plan to deploy several Active Directoryenabled
applications over the next six months. Each of these
applications will add attributes to the global catalog or modify existing attributes in the global catalog.
You need to make modifications to the Active Directory infrastructure in order to prepare for these
deployments. You plan to accomplish this task during offpeak
hours. You need to ensure that you can
minimize any potential network disruption that would be caused by the deployment of these applications in
the future. You also need to ensure that the modifications do not disrupt user access to resources.
What should you do?
A.Decrease the tombstone lifetime attribute in the Active Directory Schema NIDSService
object class.
B.Remove the global catalog role from the global catalog servers in each remote site.
C.Raise the functional level of the forest to Windows Server 2003.
D.Configure universal group membership caching in each remote site.

Answer: C

Explanation: To prepare for the new application the best option is to raise the forest functional level.This will
enable us
to deactivate any wrong schema class, and create DNS and Active Directory partitions for the new applications
Domain controllers running Windows Server 2003 do not permit the deletion of classes or attributes, but they
can be
deactivated if they are no longer needed or if there was an error in the original definition. A deactivated class or
attribute
is considereddefunct
If your forest has been raised to the Windows Server 2003 functional level, you can reuse the object identifier

(governsId and attributeId values), the ldapDisplayName, and the schemaIdGUID that were associated with the defunct
class or attribute. This allows you to change the object identifier associated with a particular class or attribute.
If your forest has been raised to the Windows Server 2003 functional level, you can deactivate a class or attribute and
then redefine it.
Incorrect Answers:
A:The tombstone lifetime is the number of days that a deleted object will remain in the Active Directory before it's
deleted. The garbage collector runs every 12 hours on each server to delete objects whose tombstone lifetimes have
expired. However, we are not deleting Active Directory objects in this scenario.
B:The sites are linked to the company network through unreliable WAN connections. Removing the Global Catolog
from these sites will result in log on problems for users as well as the application's access to Active Directory.
D:Universal group membership caching can be used to improve logon times for users. It will not affect the application's
access to Active Directory.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows Server 2003,
Sybex Inc. Alameda, 2003, p. 1539

QUESTION 36
You are the network administrator for Certkiller .com. 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
Certkiller .com and two child domains named europe. Certkiller .com and australia. Certkiller .com.
The functional level of all domains is Windows 2000 native. All domain controllers in the Certkiller .com
domain run Windows Server 2003. All domain controllers in the europe. Certkiller .com and
australia. Certkiller .com domains run Windows 2000 Server.
You need to able to rename all domain controllers in Certkiller .com. You want to minimize impact to the
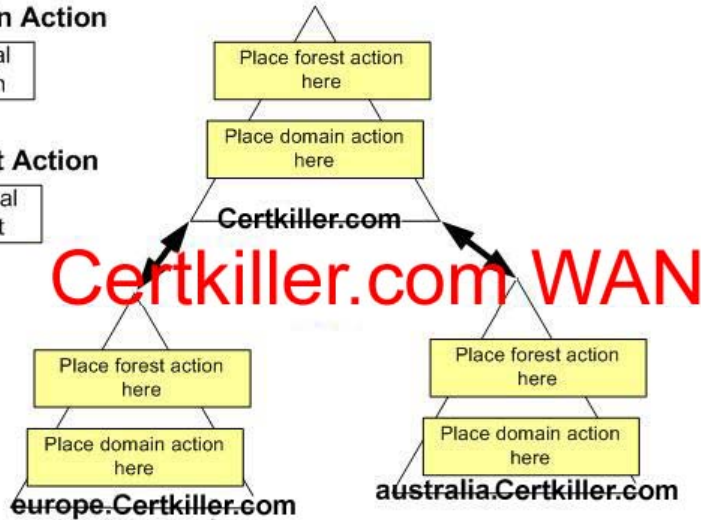network.
What should you do?
To answer, drag the appropriate action or actions to the correct location or locations in the work area.
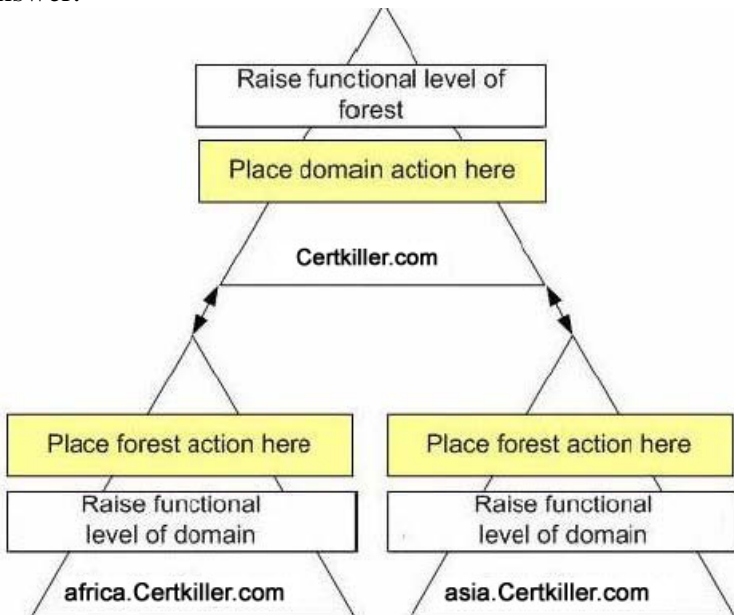
Possible Domain Action

Raise functional level of domain

Possible Forest Action

Raise functional level of forest

Place forest action here

Place domain action here

Certkiller.com

Certkiller.com WAN

Place forest action here

Place domain action here

europe.Certkiller.com

Place forest action here

Place domain action here

australia.Certkiller.com

Answer:

Raise functional level of forest

Place domain action here

Certkiller.com

Place forest action here

Raise functional level of domain

africa.Certkiller.com

Place forest action here

Raise functional level of domain

asia.Certkiller.com

Explanation:
To rename domain controllers, the domains have to be in Windows 2003 functional level. We don't have the option to
raise the domain functional levels, but upgrading the forest functional level will automatically upgrade the domain
functional levels if the domains are in Windows 2000 native functional level.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 4, p.

320
MS white paper:StepbyStep
Guide to Implementing Domain Rename
MS Knowledge base article:Q814589 HOW TO: Rename a Windows 2003 Domain Controller
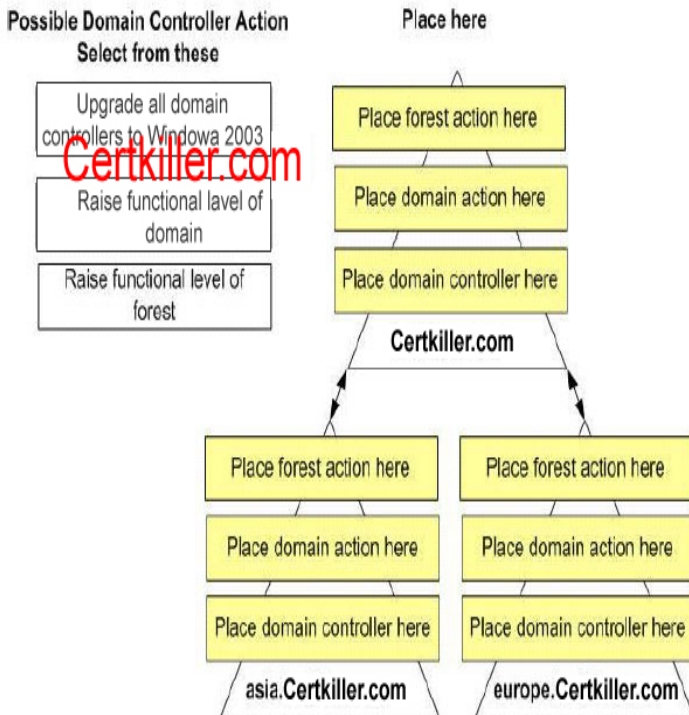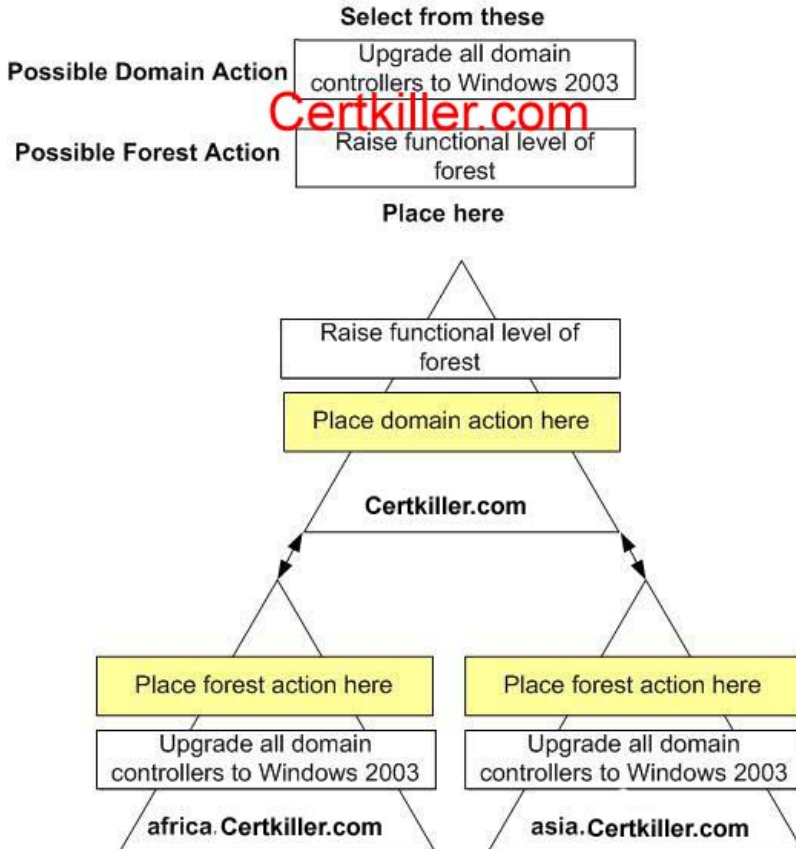
QUESTION 37

You are the network administrator for Certkiller . The network consists of a single Active Directory forest
Certkiller .com. The functional level of the forest is Windows 2000. The forest consists of a root domain named
Certkiller .com and two child domains named africa. Certkiller .com and asia. Certkiller .com.
The functional level of the domains is Windows 2000 native. All domain controllers in the Certkiller .com
domain run Windows Server 2003. All domain controllers in the africa. Certkiller .com and asia. Certkiller .com
domains run Windows 2000 Server.
You need to be able to rename all domain controllers in Certkiller .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.

Answer:

Select from these

Possible Domain Action	Upgrade all domain controllers to Windows 2003

Certkiller.com

Possible Forest Action	Raise functional level of forest

Place here

Raise functional level of forest

Place domain action here

Certkiller.com

Place forest action here

Place forest action here

Upgrade all domain controllers to Windows 2003

Upgrade all domain controllers to Windows 2003

africa.Certkiller.com

asia.Certkiller.com

Explanation:
To rename domain controllers, the domains have to be in Windows 2003 functional level.
We don't have the option to raise the domain functional levels, but upgrading the forest functional level will automatically
upgrade the domain functional levels if the domains are in Windows 2000 native functional level.
To rename a Windows Server 2003 domain controller,
You must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory.
Domain functional level is set to Windows Server 2003
NOTE: YOU do not need to raise the forest level, just domain level.
Note:Before you rename a domain controller in a domain with multiple domain controllers, make sure that the computer
that you want to rename is not the global catalog server and that it does not hold other Flexible Single Master Operations (FSMO) roles.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 4, p. 320
MS white paper: StepbyStep

Guide to Implementing Domain Rename
MS Knowledge base articleQ814589: HOW TO: Rename a Windows 2003 Domain Controller

---

QUESTION 38
You are the network administrator for Acme. Acme consists of two subsidiaries namely Mimex and Certkiller
Ltd. The network contains two Active Directory forests. The functional level of each domain is Windows
2000 native. All domain controllers run Windows 2000 Server. External relationships exist between domains,
as shown in the exhibit.
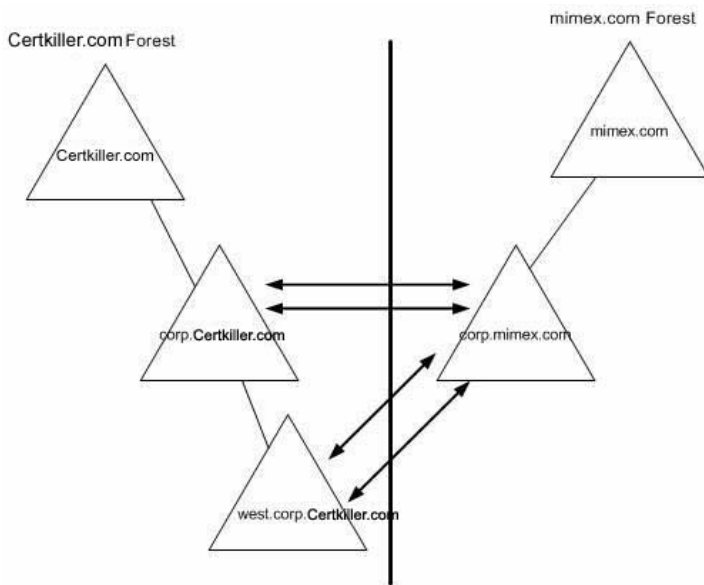
User accounts and resources are located in the child domains. All user principal names (UPNs) in each forest
comply with a standard company email
address.
Each domain controller functions as a DNS server. All DNS zones are Active Directoryintegrated
zones.
The Certkiller .com and mimex.com DNS zones have no root (".") zone. DNS servers in each forest root DNS
zone are configured with root hints to Internet root servers.
You upgrade each domain controller in both forests to Windows Server 2003. You raise the functional level
for each domain to Windows Server 2003. You plan to implement a smartcard
authentication strategy for
the entire company.
You need to ensure that users are able to access resources in all domains in each forest and on the Internet.
You want to accomplish this task by using the minimum amount of administrative effort. You also need to
ensure that access to resources is not disrupted.
Which two courses of action should you take? (Each correct answer presents part of the solution. Choose
two)
A.Create a twoway
external trust relationship between the two forest root domains.Raise the functional level of the
forest to Windows Server 2003.
B.Raise the functional level of the forest to Windows Server 2003.Replace existing trust relationships with a
twoway
forest trust relationship between the two forest root domains.
C.Create root hints between DNS servers in each child domain and DNS servers in the root domain for the

opposite
forest.
D.Create conditional DNS forwarders between domain controllers in each root domain.

Answer: B, D

Explanation: Raising the forest functional level to Windows Server2003 enables you to take advantage of all Windows
Server2003 forestlevel
features. If any domains in the forest are still operating at the Windows Server2003 interim
functional level, you will be unable to raise the forest functional level to Windows Server2003. Ensure that all domains
are operating at the Windows Server2003 functional level before you raise the forest functional level. To have a
complete trust between all the Certkiller domains and all the mimex domains, we need to create aforest trust relationship
between the two forest root domains.This can only be done after the functional level of the forests has been raised to
Windows Server 2003.
If your internal network does not have a private root and your users need access to other namespaces, such as a
network belonging to a partner company, use conditional forwarding to enable servers to query for names in other name
spaces. Conditional forwarding in Windows Server2003DNS eliminates the need for secondary zones by configuring
DNS servers to forward queries to different servers based on the domain name.
In order to avoid traffic and get the resources from any of the forest we need to configure conditional forwarding in each
zone. With option D we will create in Certkiller .com a conditional forwarder to mimex.com, and in mimex.com a
conditional forwarder to Certkiller .com.
Incorrect answers:
A:In order to create a twoway
external trust relationship between the two forest root domains, you first need to raise
the functional level of the forest to Windows Server 2003
C:There is no need to root hints between DNS servers in each child domain when all that is necessary is to create
conditional forwarding between the two domain controllers in each root domain.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, pp. 4: 42-44

QUESTION 39
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.
Acme, Inc. acquires a company named Certkiller . The Certkiller network consists of a single Active
Directory forest that contains a root domain named Certkiller .com and a child domain named

asia. Certkiller .com. The functional level of the forest is Windows 2000. The functional level of the
asia. Certkiller .com domain is Windows 2000 native.
A business decision by Certkiller requires that asia. Certkiller .com domain to be removed.
You need to move all user accounts from the asia. Certkiller .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. Certkiller .com can log on to acme.com
by using their current user names and passwords.
What should you do?
A.Create a twoway
Windows Server 2003 external trust relationship between the acme.com domain and the
Certkiller .com domain.
B.Create a oneway
Windows Server 2003 external trust relationship in which the acme.com domain trusts the
Certkiller .com domain.
C.Create a temporary twoway
external trust relationship between the acme.com domain and the asia. Certkiller .com
domain.
D.Create a temporary oneway
external trust relationship in which the asia. Certkiller .com domain trusts the acme.com
domain.

Answer: C

Explanation:
To use ADMT, we need a two way trust between the acme.com domain and the asia. Certkiller .com domain.
Incorrect Answers:
A:This would enable users in Certkiller .com to log in to acme.com and users in acme.com to log in to
Certkiller .com.
B:This would enable users in Certkiller .com to log in to acme.com.
D:The trust must be a twoway
trust.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 618,
619621,
629-641

QUESTION 40
You are the network administrator of a company that consists of two subsidiaries named Certkiller and
Contoso, Ltd. The network consists of a single Active Directory forest that contains two domain trees, as
shown in the exhibit.
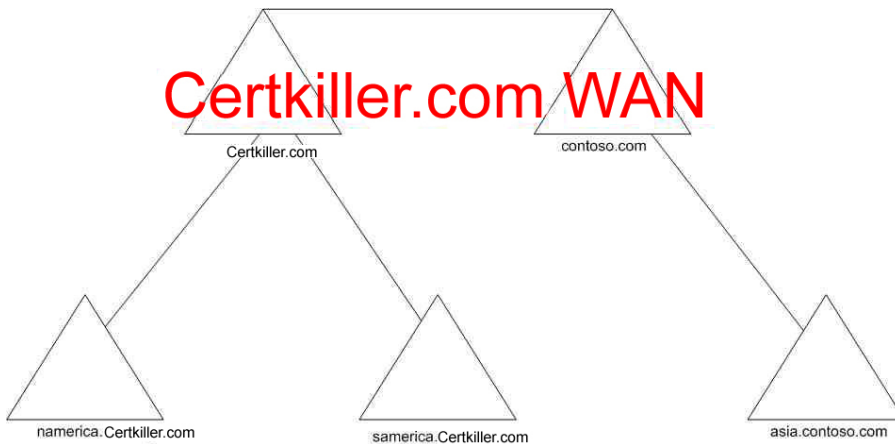
Some users are temporarily relocated from Hong King to New York. Their user accounts remain in the asia.contoso.com domain, and they use their principal names (UPNs) to log on from the namerica. Certkiller .com domain. The relocated users report that their authentication time is extremely slow. You need to improve their authentication time.

What should you do?

A.Create a universal security group in the asia.contoso.com domain and add the relocated users into the group.
Add the universal group to the domain local groups in the asia.contoso.com domain that have permission for the object
to which the users need access.

A.Create a universal security group in the namerica. Certkiller .com domain and add the relocated users into the group.
Add the universal group to the domain local groups in the asia.contoso.com domain that have permission for the objects
to which the users need access.

A.Create a shortcut trust relationship in which the asia.contoso.com domain trusts the namerica. Certkiller .com domain.

B.Create a shortcut trust relationship in which the namerica. Certkiller .com domain trusts the asia.contoso.com domain.

Answer: D

Explanation: Logon times can be slow when two domains are logically distant from each other in a forest or tree hierarchy. A shortcut trust must be explicitly created between the two domains to improve logon times. The direction
needs to be fromasia.contoso.com because the user accounts are located there. Thus, the namerica. Certkiller .com
domain must trust the asia.contoso.com domain.
Incorrect Answers:
A, B:Universal security groups are most often used to assign permissions to related resources in multiple domains.
However, the problem here is not access permissions but slow authentication times. A permissions problem would
produce an error message.
C:The direction is wrong. The User accounts are in theasia.contoso.com domain thus users are authenticated in the

asia.contoso.com now those authentications must be trusted by the namerica. Certkiller .com domain.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 1-25
to 1-27,8-6

QUESTION 41
You are the network administrator for
A. Datum Corporation. The company has a subsidiary named
Certkiller . The
A. Datum Corporation network consists of a single Active Directory forest. The forest
contains one domain named adatum.com. The functional level of the domain is Windows Server 2003. The
Certkiller network consists of a single Windows NT 4.0 domain named Certkiller .
A file server named Server1 is a member of the adatum.com domain. All users in both domains need to save
files on Server1 every day.
You need to allow users in the Certkiller domain to access files on Server1. You need to ensure that the
domain administrators of the Certkiller domain cannot grant users in the adatum.com domain permissions on
servers in the Certkiller domain.
What should you do?
A.Upgrade the Certkiller domain to Windows Server 2003 and make this domain the root domain of a second
tree in
the existing forest.
B.Upgrade the Certkiller domain to Windows Server 2003 and make this domain the root domain of a new
forest.
Create a twoway
forest trust relationship.
C.Create a oneway
external trust relationship in which the adatum.com domain trusts the Certkiller domain.
D.Create a oneway
external trust relationship in which the Certkiller domain trusts the adatum.com domain.

Answer: C

Explanation: Users in the Certkiller domain need to access resources on Server1 in the adatum domain.Users in
the
adatum domain do not need access to resources in the Certkiller domain.Therefore, we need aoneway
external trust
relationship in which the adatum.com domain trusts the Certkiller domain.
Incorrect Answers:
A:It is not necessary to upgrade the Certkiller domain.Furthermore, this solution would enable usersin the
adatum
domain to access resources in the Certkiller domain (Certkiller administrators could grant permissions to the

adatum

users to access resources).

B:It is not necessary to upgrade the Certkiller domain.Furthermore, this solution would enable usersin the

adatum

domain to access resources in the Certkiller domain (Certkiller administrators could grant permissions to the

adatum

users to access resources).

D:This solution would enable usersin the adatum domain to access resources in the Certkiller domain (

Certkiller

administrators could grant permissions to the adatum users to access resources), but users in the Certkiller

domain

would not be able to access resources on Server1 (in the adatum domain).

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,

Washington, 2004,pp. 4-41 to 4-48

QUESTION 42

You are the network administrator for a company named Certkiller Holdings. The company consists of two

subsidiaries named Contoso, Ltd, and City Power & Light.The network contains two Active Directory

forests named contoso.com and cpand1.com.The functional level of each forest is Windows Server 2003.

A twoway

forest trust relationship exists between the forests.

You need to achieve the following goals:

1.Users in the contoso.com forest must be able to access all resources in the cpand1.com forest.

2.Users in the cpand1.com forest must be able to access only resources on a server named

HRApps.contoso.com.

You need to configure the forest trust relationship and the resources on HRApps.contoso.com to achieve the

goals.

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

A.On a domain controller in the contoso.com forest, configure the properties of the incoming forest trust

relationship to

use selective authentication.

B.On a domain controller in the contoso.com forest, configure the properties of the incoming forest trust

relationship to

use forestwide

authentication.

C.On a domain controller in the cpand1.com forest, configure the properties of the incoming forest trust

relationship to

use selective authentication.

D.On a domain controller in the cpand1.com forest, configure the properties of the incoming forest trust

relationship to

use forestwide

authentication.

E.Modify the discretionary access control list (DACLs) on HRApps.contoso.com to allow access to the Other

Organization security group.

F.Modify the discretionary access control lists (DACLs) on HRApps.contoso.com to deny access to This Organization
security group.

Answer: A, D, E

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
oneway
or twoway
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 forestwide
access control decisions.
If you use forestwide
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:If you use forestwide
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. However, users in the cpand1.com forest
must be able to access only resources on a server named HRApps.contoso.com. We should therefore use selective
authentication for the cpandl.com forest to access the contoso.com.
C:Users in the contoso.com forest must be able to access all resources in the cpand1.com forest, in other words, they
need forest-wide access.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 448
to 449
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,p. 254

QUESTION 43
You are the network administrator for Certkiller .com. The company consists of two subsidiaries named Certkiller ., and Fabrikam, Inc. The network consists of two Active Directory forests. All servers run Windows Server 2003. The domain configuration is shown in the exhibit.
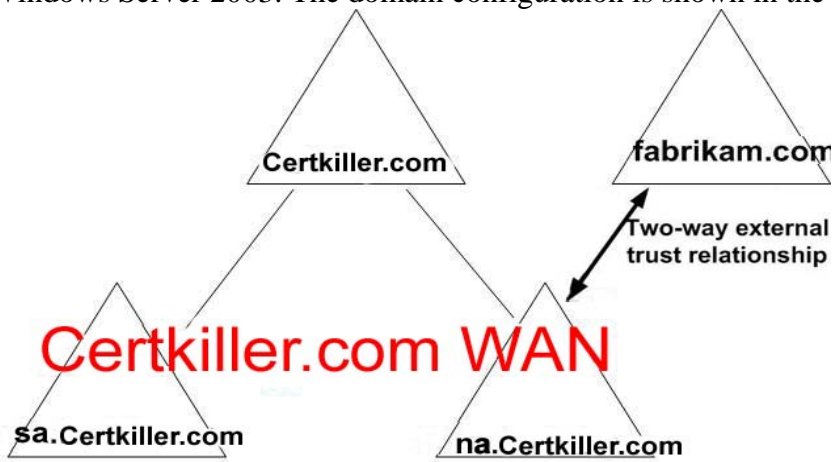
The North American department in the company is renamed to Northwind Traders. You rename the NA. Certkiller .com domain to northwindtraders.com. You change the NetBIOS name for the domain to northwindtraders. The northwindtraders.com domain is a second tree in the Certkiller .com forest.
After the domain is renamed, users in the northwindtraders.com domain report that they cannot access any shared resourced in the fabrikam.com domain. In addition, users in the fabrikam.com domain report that they cannot access shared resources in the norhwindtraders.com domain.
You need to reenable
the sharing of resources between the northwindtraders.com domain and the
fabrikam.com domain.
What should you do?
A.Change the NetBIOS name for the northwindtraders.com domain to NA.
B.Delete and recreate
the two oneway
trust relationships between the northwindtraders.com domain and the
fabrikam.com domain.
C.Configure conditional forwarding on the DNS server in the fabrikam.com domain to forward requests for the northwindtraders.com domain to the DNS servers in the Certkiller .com domain.
D.Reset the computer account passwords on all of the domain controllers in the northwindtraders.com domain.

Answer: B

Explanation: After renaming the domain, the external trust relationships will need to be recreated.
Incorrect Answers:
A:Changing the NetBIOS name will not affect the trust relationship.
C:A conditional forwarder is a DNS server on a network that is used to forward DNS queries according to the DNS
domain name in the query. It does not affect trust relationships.
D:The computer account passwords will not affect the trust relationship.
Reference:
Michael Cross, Jeffery

A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 1, pp.
3640
MS White paper StepbyStep
Guide to Implementing Domain Rename

QUESTION 44
You are the network administrator at Acme Inc. The network consists of a single Active Directory forest
that contains a single domain named acme.com. The functional level of the forest is Windows Server 2003.
Acme purchase a company named Certkiller . The Certkiller network consists of one Windows NT 4.0 account
domain and two Windows NT 4.0 resource domains, as shown in the exhibit.
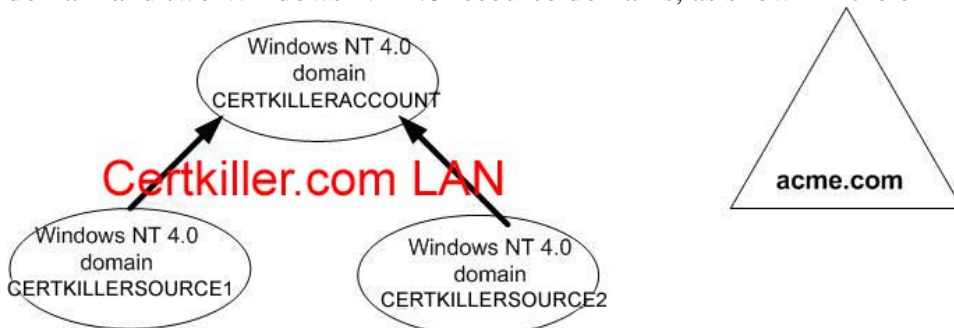
All file resources are stored on file servers in the acme.com domain and in the Certkiller SOURCE1
domain.
You need to accomplish the following goals:
1.You need to minimize the number of trust relationships that must be maintained in the network
environment.
2.Users in each company must be able to access the file resources on the file servers in the other company's
domain.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A.Create a oneway
external trust relationship in which the Certkiller SOURCE1 domain trusts the acme.com
domain.
B.Create a oneway
external trust relationship in which the acme.com domain trusts the Certkiller SOURCE1
domain.
C.
Create a one-way external trust relationship in which the acme.com domain trusts the Certkiller ACCOUNT
domain.
D.Create a oneway
external trust relationship in which the Certkiller ACCOUNT domain trusts the acme.com
domain.

Answer: A, C

Explanation: The file resources in the Certkiller network are located in the Certkiller SOURCE1 domain. In the

Acme network, the file resources are in the acme.com domain.

Users in the Certkiller network are located in the Certkiller ACCOUNTS domain while users in the Acme network

are located in the acme.com domain.

For users in the acme.com domain to access file resources in the Certkiller network, we would need the Certkiller SOURCE1 domain to trust the acme.com domain.

For users in the Certkiller network to access file resources in the acme.com domain, we need the acme.com domain to

trust the Certkiller ACCOUNT domain.

Incorrect Answers:

B:In oneway

trust relationships, the direction of access is always in the opposite direction. Thus, ifthe acme.com domain trusts the Certkiller SOURCE1 domain, then the Certkiller SOURCE1 domain can access the acme.com domain. Therefore, the oneway

trust is in the wrong direction.

D:In oneway

trust relationships, the direction of access is always in the opposite direction. Thus, ifthe Certkiller ACCOUNT domain trusts the acme.com domain, then the acme.com domain can access the Certkiller ACCOUNT domain. However, the file resources in the Certkiller network are in the Certkiller SOURCE1 domain.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 43, 315317,

396

QUESTION 45

You are the network administrator for your company. The company consists of three subsidiaries named Certkiller Ltd, Fabricam Inc and Adatum Corporation. The network consists of three Active Directory forests that include external trust relationships, as shown in the exhibit.
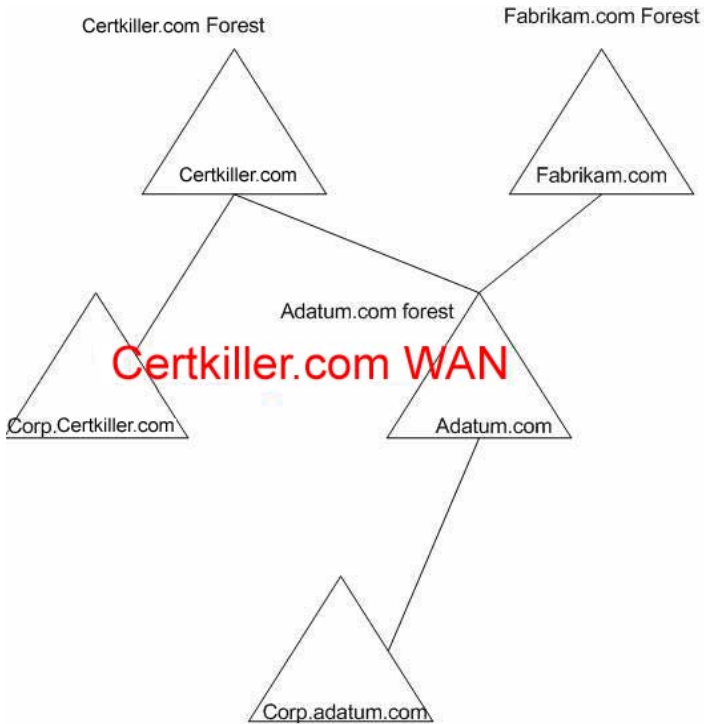
The functional level of each forest is Windows 2000. The functional level of each domain is Windows 2000 native.

Certkiller requires users in each domain to be able to access resources in all domains across all forests by using the minimum number of trust relationships.

You need to ensure that users don't have accounts in one of the other two forests. You need to accomplish this goal by using the minimum amount of administrative effort. You upgrade every domain controller to Windows Server 2003.

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

A.Raise the functional level of each forest to Windows Server 2003

B.Create shortcut relationship between each child domain.

C.Replace existing external trust relationship with twoway

forest trust relationships.

D.Create a twoway

forest trust relationship between Certkiller .com and fabricam.com.

Answer: A, C, D

Explanation: We have Windows 2000 forests which mean we can only create oneway

trusts between the forests.If

we raise the functional level of each forest to Windows Server 2003, we can use twoway

forest trust relationships

which will reduce the number of required trust relationships.

Forest trust relationships are not transitive.This means that although Certkiller .com trusts adatum.com and adatum.com

trusts fabrikam.com, Certkiller .com does not trust fabrikam.com.Therefore, we need to configure a twoway

forest trust

relationship between Certkiller .com and fabricam.com.

Incorrect Answers:
B:Creating shortcut trust relationships between each child domain is not necessary and will add to the number of trust
relationships.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 4: 4145
Part 4: Implement an Active Directory site topology.

QUESTION 46
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain with six sites. These sites are located in six different cities. The site configuration is shown in the exhibit.
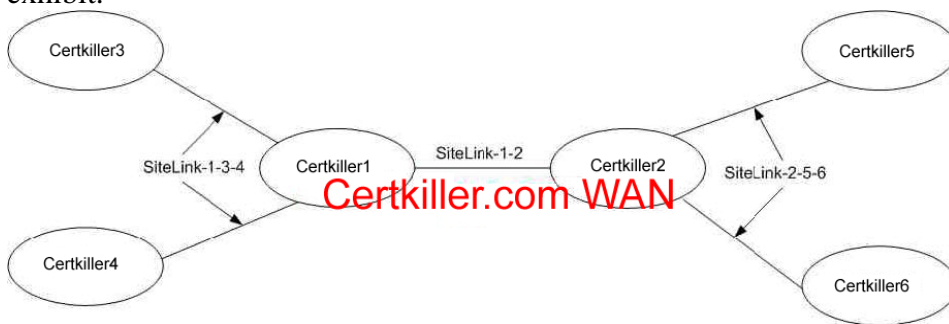
The site links are configured as shown in the following table.

Site link name	Replication schedule	Replication frequency
SiteLink12	24 hours per day	1 hour
SiteLink134	6:00 P.M. to 6:00 A.M.	1 hour
SiteLink256	10:00 P.M. to 6:00 A.M.	2 hours

All user accounts for the entire company are created by network administrators in Certkiller 1. The number of employees in the office at Certkiller 3 is growing rapidly. Several accounts for new employees are created for users in Certkiller 3 every day. The new employees report that they cannot log on to the domain on the same day that their accounts are created. They can log on to the domain successfully the next day.
You need to ensure that the employees can log on to the domain on the same day that their accounts are created. You also need to ensure that the replication traffic between the Certkiller 1 and Certkiller 3 is compressed.
What should you do?
A.Move the Active Directory domain controller objects from Certkiller 3 to Certkiller 1.
B.Add the Active Directory subnet object for Certkiller 3 to Certkiller 1.
C.Reconfigure SiteLink12
to include Certkiller 1, Certkiller 2, and Certkiller 3.
Remove Certkiller 3 from SiteLink1-3-4.
A.Remove Certkiller 1 from SiteLink1-3-4.

Answer: C

Explanation: The changes to Active Directory in Certkiller 1 are replicated to Certkiller 2 and hour later and to the other
sites only after 6 P.M. in the case of Certkiller 3 and Certkiller 4, and after 10 P.M to Certkiller 5 and Certkiller 6.
Incorrect Answers:
A:Moving the Active Directory domain controller objects from Certkiller 3 to Certkiller 1 will not change the replication
schedule.
B:AddingActive Directory subnet object for Certkiller 3 to Certkiller 1 will not change the replication schedule.
D:Removing Certkiller 1 fromSiteLink134
would mean that changes made in Certkiller 1 are never replicated to
Certkiller 3 and Certkiller 4. Instead, replication will occur only between Certkiller 3 and Certkiller 4.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 446448,
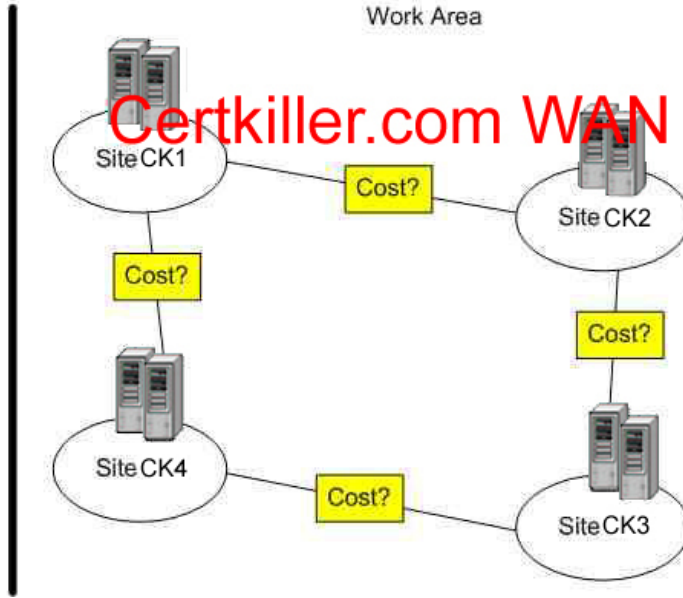452-454,457-460

QUESTION 47
You are the network administrator for Certkiller .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.

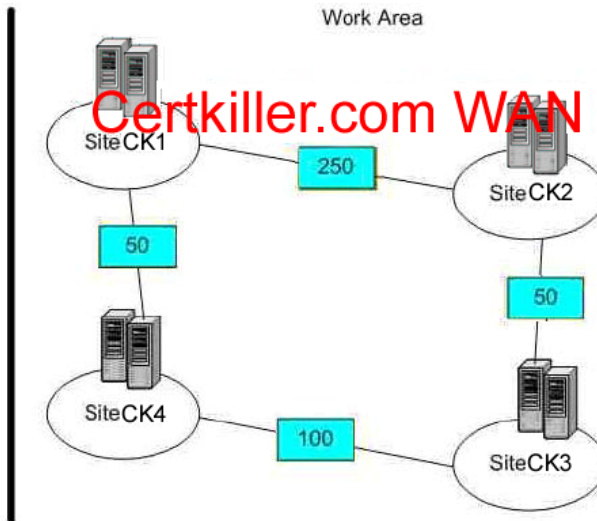| WAN connection	Type of connection	Available bandwidth
Site CK1 Site CK2	56 Kbps	30 percent
Site CK2 Site CK3	T3	70 percent
Site CK3 Site CK4	T1	40 percent
Site CK4 Site CK1	T3	70 percent

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

50   100   250

Work Area

Certkiller.com WAN

Site CK1 — Cost? — Site CK2

Cost?

Cost?

Site CK4 — Cost? — Site CK3

Answer:

Site Link Costs

50   100   250

Work Area

Certkiller.com WAN

SiteCK1 — 250 — SiteCK2

50

50

SiteCK4 — 100 — SiteCK3

Explanation:
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 CK1 Site
CK4 and Site CK2 Site
CK3 . We must then assign the site link with
the next highest available bandwidth (Site CK3 Site
CK4) the next lowest cost. The site link with the lowest available
bandwidth (Site CK1 Site
CK2) must have the highest cost.
Reference:

QUESTION 48
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
named Certkiller .com. The functional level of the domain is Windows Server 2003.
Certkiller 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
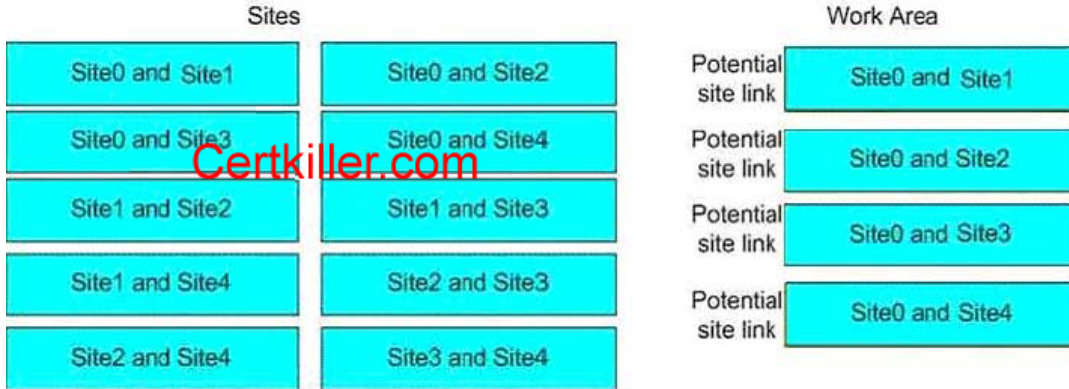are shown in the exhibit.

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:
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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-7 to 5-8

QUESTION 49
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com with five sites.
You configure the five Active Directory sites in accordance with the requirements of the company's site configuration design. The network and site configuration is shown in the exhibit.

The site configuration design also requires you to configure site link bridges. The design requires the site links connecting Certkiller 1, Certkiller 2, and Certkiller 3 to be transitive and all other site links to be nontransitive.
You need to configure site link bridges to comply with the site configuration design.
Which action or actions should you take? (Choose all that apply)
A.Disable automatic site link bridging in the IP object properties.
B.Create new site links between each of the Active Directory sites.
C.Remove each of the sites from the default site link.
D.Create a new site link bridge.
Add the site links connecting Certkiller 1, Certkiller 2, and Certkiller 3 to the site link bridge.
A.Create a new link bridge.
Add the site links connecting Certkiller 3, Certkiller 4, and Certkiller 5 to the site link bridge.

Answer: A, C, D.

Explanation:

A:We must disable automatic site link bridging in the IP object properties, to prevent all site links being transitive.

C:

been manually added.But, we should do this just to be sure.

D:The design requires the site links connecting Site1, Site2, and Site3 to be transitive.Therefore, we should create a

new site link bridge and add the site links connecting Site1, Site2, and Site3 to the site link bridge.

Incorrect Answers:

B:This would mean that every site is connected to each of the other sites.

E:This would make the site links connecting Site3, Site4, and Site5 transitive.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 449-452, 458,458-459

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

---

QUESTION 50

You are the network administrator for Certkiller , 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.
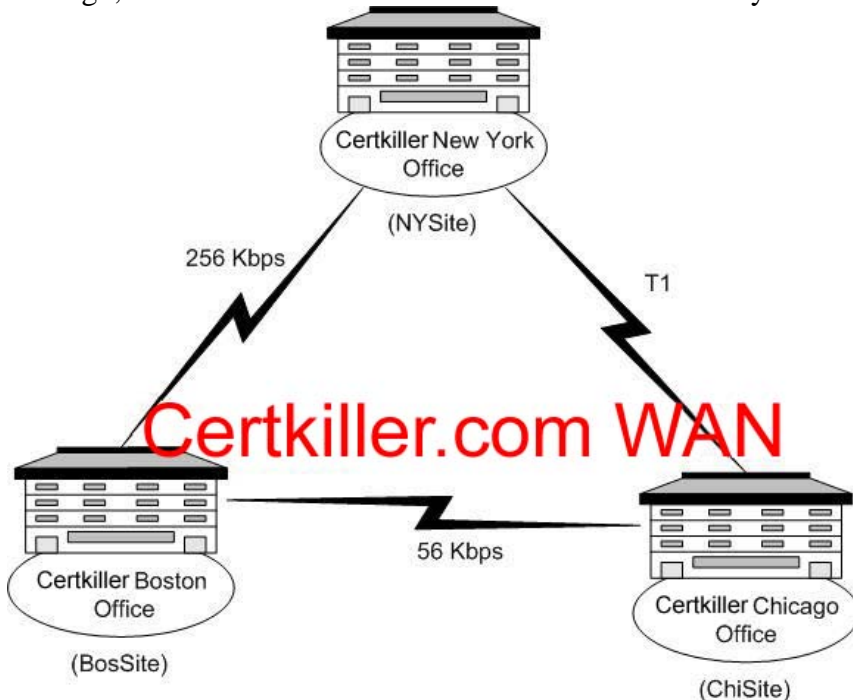
Certkiller is deploying a Windows Server 2003 forest. You create a single Active Directory domain named

Certkiller .com. 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.

Site link name	Linked site	Linked site
NYBoston	NYSite	BosSite
NYChi	NYSite	ChiSite
ChiBoston	ChiSite	BosSite

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?
A.Create an SMTPbased
connection object from a domain controller in NYSite to a domain controller in BosSite.
B.Increase the cost of 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

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 cops for the ChiBoston site
link; theref
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 site link 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:

QUESTION 51

You are the network administrator for Certkiller .com. Certkiller has three offices. The network consists of a
single Active Directory domain named Certkiller .com with three sites. Each office is configured as a separate
site.

Certkiller opens a new branch office in Montreal that has 10 users. This office does not contain a domain
controller.

The Montreal Office has WAN connections to two of the existing offices. A router is installed at each of the
four offices to route network traffic across the WAN connections. The network after the addition of the
Montreal Office is shown in the exhibit.

Certkiller Site1

256 Kbps   256 Kbps

Certkiller Site2   Certkiller Site3

Certkiller.com WAN

256 Kbps   56 Kbps

Certkiller Montreal Office
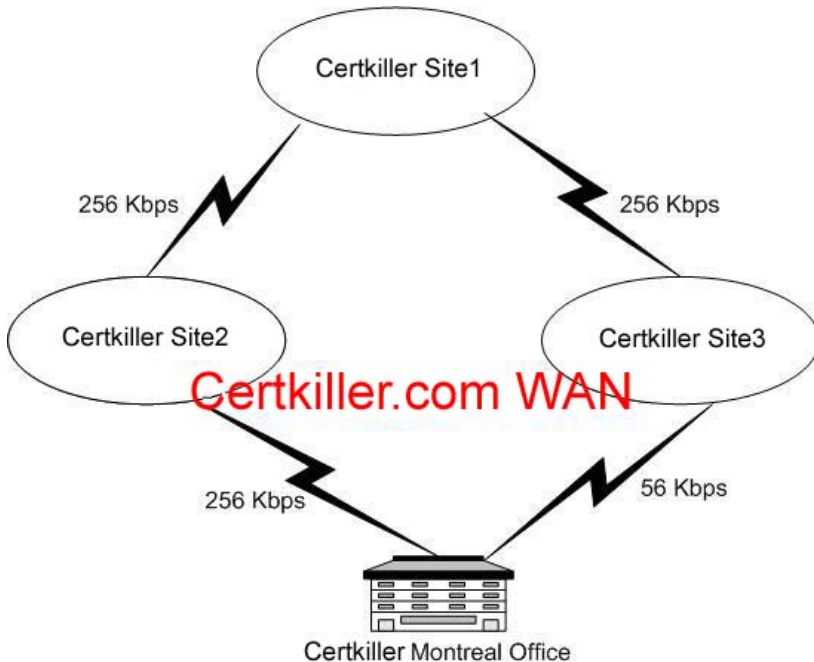
You need to ensure that when the users in the Montreal office log on the domain during normal operations,
they will be authenticated by a domain controller in Certkiller Site2.

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

A.Create a new IP subnet object that includes the subnet used in the Montreal Office.
Link the new subnet object to the Certkiller Site2 site object.

A.Create a new IP subnet object that includes the subnet used in the Montreal Office.
Link the new subnet object to the Certkiller Site3 site object.

A.Create an additional site for the Montreal Office.
Configure a site link to Certkiller Site3 with a cost of 300.
Configure a site link to Certkiller Site2 with a cost of 200.
A.Create an additional site for the Montreal Office.
Configure a site link to Certkiller Site2 with a cost of 300.
Configure a site link to Certkiller Site3 with a cost of 200.
A.Assign IP addresses to the client computers in the Montreal Office that are on the same IP subnet as the network at
Site2.

Answer: A, C

Explanation:
A:If we create a new subnet for the Montreal site that contains a Domain Controller for the Montreal site, all the computers that are in that subnet will logon via the Domain Controller on the Montreal subnet.
C:If we create a new site, andconfigure a site link to Certkiller Site3 with a cost of 300 and a site link to Certkiller Site2
with a cost of 200, user logons will go over the site link with the lowest cost first and will use the other site link as a fail
over mechanism.
Incorrect Answers:
B:Users in the Montreal office should be authenticated by a domain controller in Certkiller Site2. Therefore weshould
link the new subnet object to the Certkiller Site2 site object, and not the Certkiller Site3 site object.
D:Users in the Montreal office should be authenticated by a domain controller in Certkiller Site2. Therefore, the Certkiller Site 2 site link should have a lower cost.
E:We could assign IP addresses to the client computers in the Montreal Office that are on the same IP subnet as the
network at Site2. However, the network will be easier to administrate if the offices are on separate sites. This is therefore not the best option.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 6, p. 434
MS Windows server 2003 Deployment Kit:Designing and Deploying Directory and Security Services: Setting Site
Link Properties

QUESTION 52
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com with two sites. Each site contains two domain controllers. One domain controller in each site is a global catalog server.

You add a domain controller to each site. Each new domain controller has a faster processor than the existing domain controllers.

Certkiller requires Active Directory replication to flow through the servers that have the most powerful CPUs in each site.

You need to configure the intersite replication to comply with Certkiller 's requirement for Active Directory replication.

What should you do?

A.Configure the new domain controllers as global catalog servers.

B.Configure the new domain controller in each site as a preferred bridgehead server for the IP transport.

C.Configure the new domain controller in each site as a preferred bridgehead server for the SMTP transport.

D.Configure an additional IP site link between the two sites.

Assign a lower site link cost to this site link than the site link cost for the original site link.

Answer: B

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 uptodate

directory information with the limitations

imposed by available network bandwidth.

You can customize how Active Directory replicates information 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.

should be used. 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.

Ordinarily, all domain controllers are used to exchange information between sites, but you can further control replication

behavior by specifying a bridgehead server for intersite

replicated information.A bridgehead server is dedicated for

intersite

replication. 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: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: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.
D:We can control the flow of replication traffic by creating a new site link with a lower cost. Replication will then occur
across the site link with the lower cost. However, this option does not specify that the new site link must be between
MainDC3 and BranchDC3.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 6, pp. 453-455
MS Windows Server 2003 Deployment KitDesigning
and Deploying Directory and Security Services Active
Directory Replication Concepts

QUESTION 53

You are the network administrator for your company. The company consists of two subsidiaries named Certkiller and Fabrikam, Inc. The network consists of two Active Directory domains with two sites. The sites are named Site1 and Site2. The domains are named Certkiller .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.

Domain Controller Name	Location	Role(s)
DC1.Certkiller.com	Site1	Domain controller
DC2.Certkiller.com	Site1	Domain controller
		AppPartition1 application partition
		Global catalog server
DC3.fabrikam.com	Site1	Domain controller
DC4.Certkiller.com	Site2	Domain controller
DC5.Certkiller.com	Site2	Domain controller
		Global catalog server
DC6.fabrikam.com	Site2	Domain controller
		AppPartition1 application partition

Answer:

Explanation: Select DC2. Certkiller .com and DC5. Certkiller .com
If you specify preferred bridgehead servers, you must assign one bridgehead
server for each domain and writable
directory partition combination in your forest.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 5-8,5-31 to 5-32

QUESTION 54
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain with three sites named Certkiller 1, Certkiller 2, and Certkiller 3. The sites and site links are configured
to use Certkiller 2 to connect Certkiller 1 and Certkiller 3. 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 Certkiller 1.
Several new users start work in Certkiller 2. When they attempt to log on to the network, the logon fails. You
confirm that the user accounts are created and are visible in Certkiller 1 and Certkiller 2. You discover that the
preferred IP bridgehead server in Certkiller 2 failed. You repair the server and confirm that replication is
successful to Certkiller 2.
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 Certkiller 1 and Certkiller 3.
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: B, D

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 uptodate
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 intersite
replicated information. The
bridgehead server is a specific server you want to dedicate for intersite
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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-21 to 1-24,5-3 to 5-8,5-25 to 5-37

QUESTION 55
You are the administrator of the Certkiller company network. Certkiller has a main office and a branch office.
Each office is configured as an Active Directory site in the Certkiller .com domain.All servers run Windows
Server 2003 and all client computers run Windows XP Professional.The branch office is connected to the
main office by a 256Kbps WAN link.
The main office has two domain controllers named MainDC1 and MainDC2.The branch office has two
domain controllers named BranchDC1 and BranchDC2.
You purchase two new servers.MainDC3 will be a domain controller in the main office.BranchDC3 will be a
domain controller in the branch office.
To improve network performance, you want toconfigure the intersite replication to flow through the new
servers.
What should you do?
A.Configure MainDC3 and BranchDC3 as global catalog servers.
B.Configure MainDC3 and BranchDC3 as a preferred bridgehead server for the IP transport.
C.Configure MainDC3 and BranchDC3 as a preferred bridgehead server for the SMTP transport.
D.In Active Directory Sites and Services, configure an additional IP site link between the two sites.
Assign a lower site link cost to this site link than the site link cost for the original site link.

Answer: B

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 uptodate

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 intersite
replicated information. The
bridgehead server is a specific server you want to dedicate for intersite
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: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: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.
D:We can control the flow of replication traffic by creating a new site link with a lower cost. Replication will then occur
across the site link with the lower cost. However, this option does not specify that the new site link must be between
MainDC3 and BranchDC3.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 6, pp. 453-455
MS Windows Server 2003 Deployment Kit Designing

and Deploying Directory and Security Services Active
Directory Replication Concepts

QUESTION 56

You are a network administrator for Certkiller .com. The company has offices in Paris and New York. The network consists of a single Active Directory domain named Certkiller .com that contains six domain controllers, as shown in the exhibit.

The Paris and New York offices are connected by an IP site link. The six domain controllers are configured as shown in the following table.

Server name	Function
Certkiller 1	File and print server
Certkiller 2	Application server
Certkiller 3	Routing and Remote Access server
Certkiller 4	Routing and Remote Access server
Certkiller 5	File and print server
Certkiller 6	Application server

You notice that at regular intervals the CPU utilization on some of the file and print servers increases to 100 percent for a period of time. During this time, the servers become unresponsive to user requests. You discover that this problem occurs during Active Directory replication.

You need to ensure that the file and print servers are responsible to use requests during Active Directory replication.

What should you do?

A.Increase the replication interval of the site link connecting the two offices.

B.Decrease the replication interval of the site link connecting the two offices.

C.Configure Certkiller 1 and Certkiller 5 as preferred bridgehead servers.

D.Configure Certkiller 3 and Certkiller 4 as preferred bridgehead servers.

Answer: D

Explanation: The poor performance of the File and Print servers is due to Active Directory replication.The replication is
occurring between the File and Print servers.This is because they are configured aspreferred bridgehead servers.We can
improve their performance by configuring the replication to occur between different servers (in this case, the RRAS
servers, Certkiller 3 and Certkiller 4).We do this by configuring Certkiller 3 and Certkiller 4 as preferred bridgehead
servers.
Incorrect Answers:
A:The problems occur during replication.This solution will decrease the frequency of the problems, but it won't eliminate
the problems.
B:The problems occur during replication.This solution will increase the frequency of the problems.
C: Certkiller 1 and Certkiller 5 are already preferred bridgehead servers.This is the cause of the problem.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 5-25 to 5-34
Walter Glenn, and Michael T. Simpson; MCSE Self
Windows Server 2003 Active Directory and Network Infrastructure, Microsoft Press, Redmond, Washington, 2004,
pp. 5-24 to 5-28

QUESTION 57
You are the network administrator for Certkiller .com. Certkiller consists of two subsidiaries named Contoso, Ltd., and Fabrikam, Inc. The network consists of two Active Directory domains in a single forest with four sites. The network configuration is shown in the exhibit.
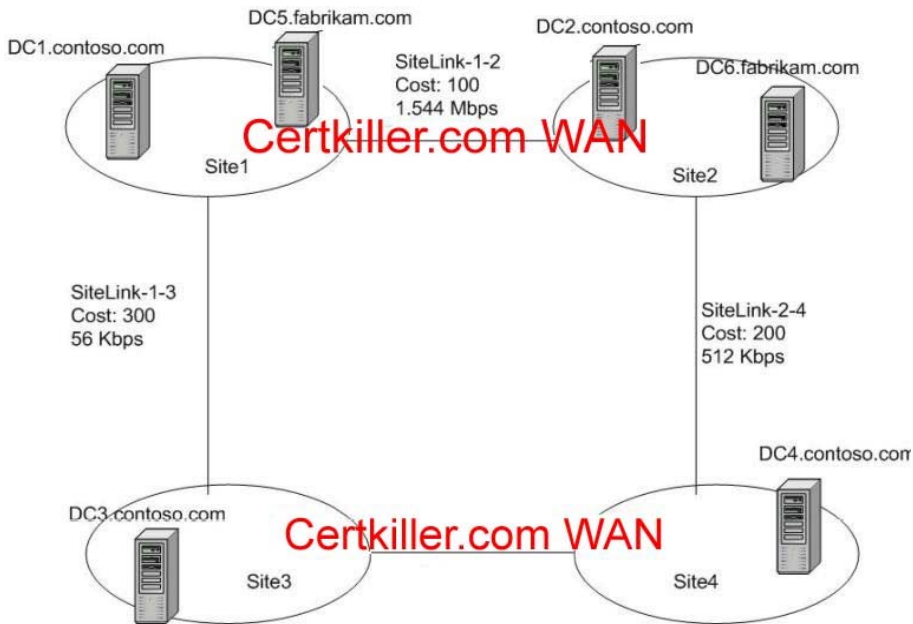
All client computers run Windows XP Professional.

Users who have accounts in the fabrikam.com domain frequently travel to Site3. When these users log on to the network in Site3, the logon process can take up to 10 minutes.

You discover that when these users log on to the network in Site3, they are authenticated by DC5.Fabrikam.com in Site1.

You need to ensure that Fabrikam, Inc., users can log on more quickly from Site3.

What should you do?

A.Increase the site link cost for SiteLink13
to 500.

B.Configure a site link bridge that will bridge SiteLink34
and SiteLink24.

C.Modify the subnet object linked to Site3 so that is linked to Site1.

D.Move the DC5.Fabrikam.com domain controller object from Site1 to Site3.

Answer: B

Explanation: SiteLink13 is across a slow WAN link. By crating a site link that bridgesSiteLink34
and SiteLink24,we would create an alternative path to DC6.fabrikam.com.

Incorrect Answers:

A:Increasing the Site Link costfor SiteLink13
will not improve log on time.

C:Site 3 is already linked to Site1 viaSiteLink13

D:Movingthe DC5.fabrikam.com domain controller to Site3 would resolve the problem but might cause problems when
Fabrikam users log on from Site1. This is thus not the best option.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-7 to 5-8

QUESTION 58
You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com com with two sites. All servers run Windows Server 2003. The network is configured as shown in the Network Diagram exhibit.
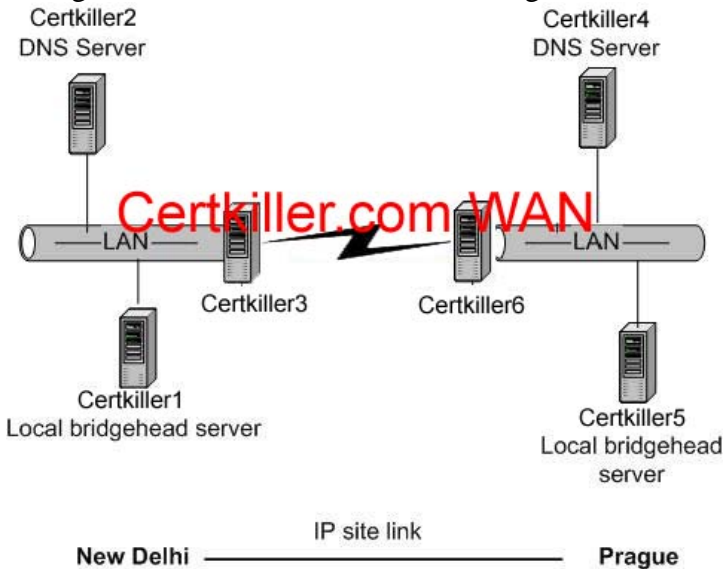
You use Replication Monitor to monitor Active Directory replication. You discover that replication connections are being established as shown in the Replication Monitor exhibit.
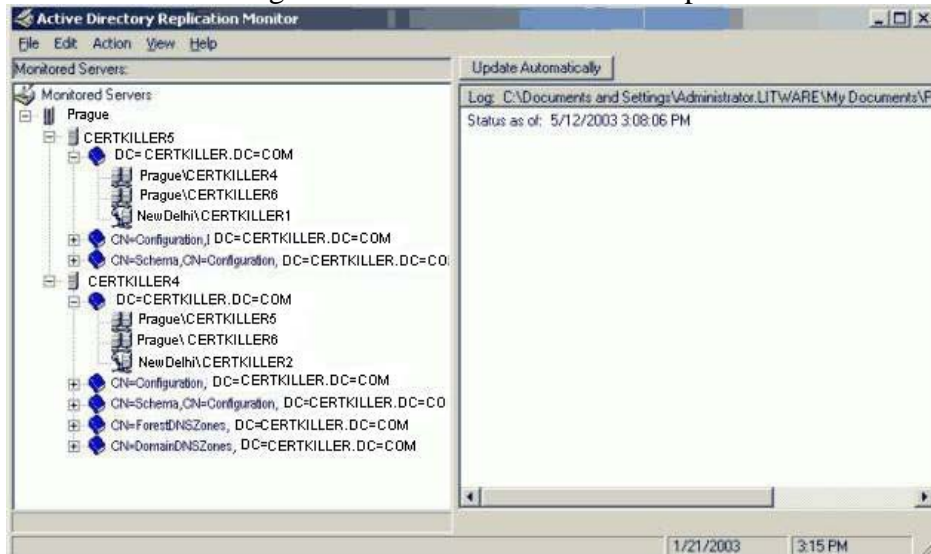
You need to ensure that replication takes place only between defined preferred bridgehead servers. You need to accomplish this task without incurring any additional replication traffic.
What should you do?
A.Configure Certkiller 1 and Certkiller 5 as additional DNS servers.
B.Configure Certkiller 3 and Certkiller 6 as additional DNS servers.
C.Configure only Certkiller 2 and Certkiller 4 as preferred bridgehead servers.
D.Configure only Certkiller 3 and Certkiller 4 as preferred bridgehead servers.

Answer: C

Explanation: We have replication between the bridgehead servers and between the DNS servers. If we configure the

DNS servers as bridgehead servers, all the replication will occur between only those two machines.

When two sites are connected by a site link, the replication system automatically creates connections between specific

domain controllers in each site calledbridgehead servers. In Microsoft Windows 2000, intersite replication of the

directory partitions between domain controllers in different sites is performed by the domain controllers (one per

directory partition) in those sites designated by the KCC as the bridgehead server. In Windows Server 2003, the KCC

may designate more than one domain controller per site hosting the same directory partition as a candidate bridgehead

server. The replication connections created by the KCC are randomly distributed between all candidate bridgehead

servers in a site to share the replication workload. By default, the randomized selection process takes place only when

new connection objects are added to the site.

However, you can run a new Windows Resource Kit tool called Active Directory Load Balancing (ADLB) to rebalance the load each time a change occurs in the site topology or in the number of domain controllers the site. In

addition, ADLB can stagger schedules so that the outbound replication load for each domain controller is spread out

evenly across time.

Incorrect Answers:

A, B, D:We have replication between the bridgehead servers and between the DNS servers. If we configure the DNS

servers as bridgehead servers, all the replication will occur between only those two machines. Only Certkiller 2 and

Certkiller 4 are DNS servers, therefore those two servers should be made the bridgehead servers, not Certkiller 1,

Certkiller 3, Certkiller 5, or Certkiller 6.

Reference:

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-8 to 5-9

Michael Cross, Jeffery

A. Martin, Todd

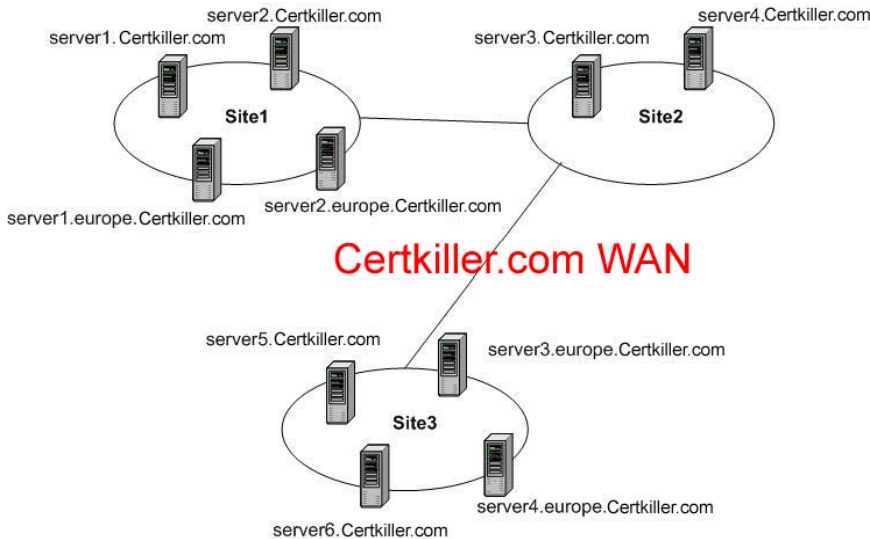A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,p. 459

QUESTION 59

You are the network administrator for Certkiller .com. 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.

server2.Certkiller.com server4.Certkiller.com
server1.Certkiller.com server3.Certkiller.com

Site1 Site2

server1.europe.Certkiller.com server2.europe.Certkiller.com

Certkiller.com WAN

server5.Certkiller.com server3.europe.Certkiller.com

Site3

server6.Certkiller.com server4.europe.Certkiller.com

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 europe. Certkiller .com located in Site1 have additional accounts that are not on the domain controllers for europe. Certkiller .com located in Site3. You examine the directory service log in Event Viewer on a domain controller for europe. Certkiller .comYou
discover the error message shown in the Error Message exhibit.

```
Event ID: 1311
    Source: NTDS KCC
    Category: Knowledge Consistency Checker
    Event Type: Error
    User: NT AUTHORITY\ANONYMOUS LOGON
    COMPUTER: Server1

Description: The Directory Service consistency checker has determined that
there is not enough physical connectivity published via the Active
Directory Sites and Services Manager to create a spanning tree connecting
all the sites connecting the Naming Context
DC=Europe,DC= Certkiller,DC=com
```

You need to resolve the condition that is causing this error.
What should you do?
A.Add a domain controller for the europe. Certkiller .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

Explanation: There is no physical connectivity between Site1 and Site3. We have a site link between Site1 and Site2
and between Site2 and Site3. We should therefore create asite link bridge between the site links for Site1 and Site3.
Any replication between Site1 and Site3 will then travel over the two existing site links.
One computer in any given site owns the role of creating inbound replication connection objects between bridgehead
servers from other sites. This domain controller is known as the InterSite

Topology Generator. While analyzing the Site

Link and Site Link Bridge structure to determine the most costeffective

route to synchronize a naming context between

two points, it may determine that a site does not have membership in any Site Link and therefore has no means to create

a replication object to a bridgehead server in that site.

Incorrect Answers:

A:This will cause excessive replication traffic between site2 and site3.This defeats the object of using sites to control

replication traffic.

C:Global Catalog placement is not the cause of the error in this question.

D:We have no physical connectivity between site1 and site3.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 6, p. 427

Troubleshooting Event ID 1311: Knowledge Consistency Checker KB article 214745
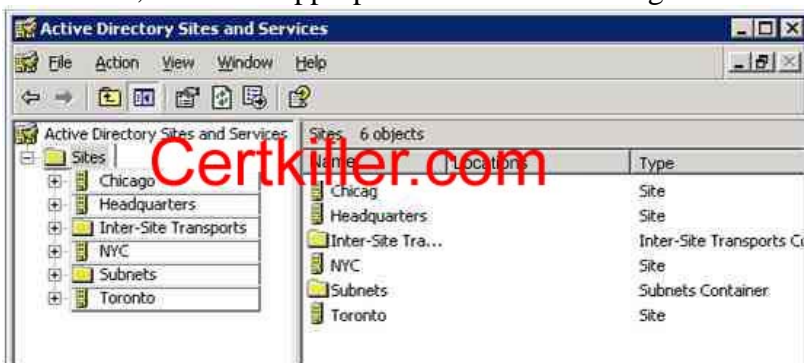

QUESTION 60

You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain consists of four sites as shown in the work area.

Pedro is another administrator for Certkiller .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:

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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-26 to 5-30

QUESTION 61

You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. Certkiller 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.
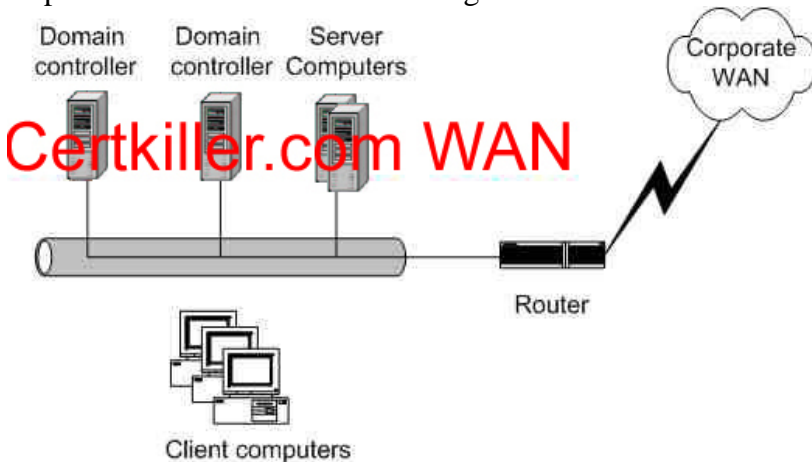
An IP site link connects your site and the site at Certkiller 's main office. Certkiller replaces your router with a firewall device. The firewall is configured to allow HTTP, SMTP, FTP, NTTP, global catalog queries, and VPN packets to pass. You discover that replication with other sites is not occurring.

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?

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

Explanation: 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:

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-17 to 1-18,541 to 5-45,5-48 to 5-50

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543, 547,

550-552

QUESTION 62

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com with six sites. The Active Directory site configuration is shown in the exhibit.
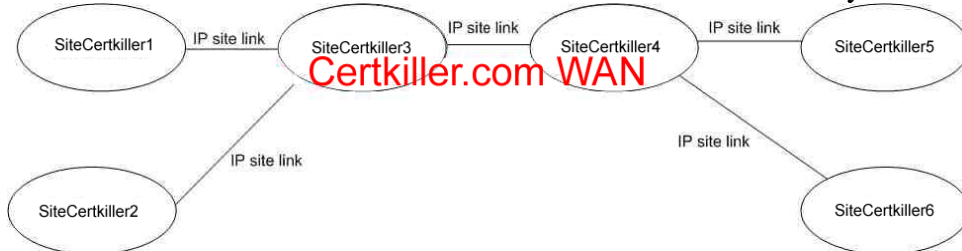
The network connection connecting Site Certkiller 3 and Site Certkiller 4 has more than 80 percent utilization during Certkiller 's business hours. The network bandwidth is required for a critical business application, and so you must ensure that Active Directory replication does not interfere with the application. The other network connections have adequate bandwidth to support Active Directory replication.

You must ensure that Active Directory replication traffic does not cross the network connection connecting Site Certkiller 3 and Site Certkiller 4 during Certkiller 's business hours. Replication connecting all other Active Directory sites must occur at least every three hours throughout the day.

What should you do?

A.Configure the replication schedule for the site link connecting Site Certkiller 3 and Site Certkiller 4 to replicate only during

nonbusiness hours.

B.Disable automatic site link bridging.

Create one site link bridge that bridges the site links connecting Site Certkiller 1, Site Certkiller 2, and Site Certkiller 3.

Create another site link bridge that bridges the site links connecting Site Certkiller 4, Site Certkiller 5, and Site Certkiller 6.

A.Configure one domain controller in Site Certkiller 3 and one domain controller in Site Certkiller 4 as preferred bridgehead

servers.
B.Configure the site link cost between Site Certkiller 3 and Site Certkiller 4 to be 1,000.
Configure the other site link costs to be 100.

Answer: A

Explanation: In Active Directory, the replication process ensures that changes made to a replica on one domain
controller are synchronized to replicas on all other domain controllers within the domain. Creating, modifying,
moving, or
deleting an object triggers replication between domain controllers. Active Directory replicates information in
two ways:
intrasite (within a site) and intersite (between sites). This means that if you configure replication schedule
between Site
Certkiller 3 and Site TEsttking4 to be during nonbusiness
hours, then you will ensure that replication traffic does not
cross the network connection between business hours.
Incorrect Answers:
B:Replication needs to occur betweenSite Certkiller 3 and Site Certkiller 4. Disabling automatic sitelink
bridging will not
prevent this.
C:This will limit replication to occur only between these two servers. However, we must prevent replications
from
occurring during business hours.
D:When we have redundant links, we can use site link costs to determine which links are used for replication
traffic.
However, there is no alternative route betweenSite Certkiller 3 and Site Certkiller 4.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 449-452,
458,458-459.
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, pp. 5: 4, 10

QUESTION 63
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com with three sites named Site1, Site2, and Site3.
Site links are configured between the sites so that Site1 and Site3 are connected by using Site2. The site
links are configured as shown in the following table.

Site link	Replication schedule	Replication interval	Cost

Site1 Site2 site link	1:00 A.M. 6:00 A.M.	60 minutes	200
Site2 Site3 site link	8:00 P.M. 1:00 A.M.	30 minutes	500

All user and group accounts are managed by network administrators at Site1. Users at Site3 report that it takes more than a day for changes made to Active Directory at Site1 to be visible in the domain at Site3. You must ensure that the changes made by Active Directory at Site1 between 8:00 A.M. and 6:00 P.M. are visible at Site3 when the business opens at 8:00 A.M. the next day.
What should you do?
A.Modify the replication interval for the site link between Site1 and Site2 to 30 minutes.
B.Modify the replication schedule for the site link between Site2 and Site3 to replicate between 6:00 P.M. and 1:00
A.M.
C.Modify the site link cost between Site2 and Site3 to be 200.
D.Modify the replication schedule for the site link between Site1 and Site2 to replicate between 9:00 P.M. and 2:30
A.M.

Answer: D

Explanation: In this scenario, when an administrator in Site1 makes a change to Active Directory, this information is
replicated to Site2 between1:00 A.M. and 6:00 A.M the next morning.
This information is then replicated to Site3 between8:00 P.M. and 1:00 A.M that evening.Users in Site3 will thus see the
changes when they start work the following morning.
We should change the replication schedule for the site link between Site1 and Site2 to occur earlier. Then, when an
administrator in Site1 makes a change to Active Directory, this information is replicated to Site2 between9:00 P.M. and
2:30 A.M that evening.This information is then replicated to Site3 between8:00 P.M. and 1:00 A.M.Users in Site3 will
then see the changes when they start work the next morning.
Incorrect Answers:
A:Replication is configured to occur on a schedule. Reducing the replication interval will thus not resolve this problem.
B:When an administrator in Site1 makes a change to Active Directory, this information is replicated to Site2 between
1:00 A.M. and 6:00 A.M the next morning.If this information is then replicated to Site3 between6:00 P.M. and 1:00
A.M that evening, users in Site3 will still see the changes only when they start work the following morning.
C:Site link costs will influence the path along which replication occurs when we have redundant links. In this case, Site1
is connected to Site3 through Site2. There is thus no alternative or redundant links.
Reference:

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-7 to 5-8

QUESTION 64

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains three domains named Certkiller .com, child1. Certkiller .com and child2. Certkiller .com. The

functional level of the forest is Windows Server 2003.

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 toplevel
OU for file server computer accounts under the Certkiller .com domain.
Create a toplevel
OU for print server computer accounts under the Certkiller .com domain.

A.Create a toplevel
OU for file server computer accounts under the Certkiller .com domain.
Create a toplevel
OU for print server computer accounts under each domain.

A.Create a toplevel
OU for file server computer accounts under each domain.
Create a toplevel
OU for print server computer accounts under each domain.

A.Create a toplevel
OU for file server computer accounts under each domain.
Create a child OU for print server computer accounts under each file server OU.

Answer: C

Explanation: Thecentral 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 toplevel
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 Certkiller .com domain.

D:There is no need for child OUs as thecentral operations departmentis not responsible for the print server accounts.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 65
You are the network administrator for Certkiller .com. The network consists of an Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003.
Certkiller has a main office and four branch offices, which are located in one country. Each office has a data center that contains domain controllers and servers with a corresponding Active Directory site. There is a central operations department in the main office that is responsible for administering all resource servers and domain controllers in all locations. Each office has a local operations department that is responsible for administering all client computers within the individual department's office only. The local operations departments are also responsible for running backups on the servers in their data centers.
The computer accounts for all domain controllers are located in the default Domain Controllers organizational unit (OU). The computer accounts for all other computers are located in the default Computers container.
You decide to use delegation of authority to meet the requirements for administration of computer accounts. You need to create an OU structure for computer accounts 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 toplevel
OU under the Certkiller .com domain for each office.
Move the computer accounts of all computers in each office to the appropriate OU for that office.
A.Create a toplevel
OU named Corp_Computers under the Certkiller .com domain.
Create a separate child OU for each office and place the child OUs under Corp_Computers.
Move all of the client and resource server computer accounts located in each office to the appropriate child OU for that
office.
A.Create a toplevel
OU named Servers under the Certkiller .com domain.
Move the computer accounts of resource servers and domain controllers in all offices to the Servers OU.
Create an OU named Desktops under the Certkiller .com domain.
Move the computer accounts of the client computers in all offices to the Desktops OU.
A.Create a toplevel
OU named Servers under the Certkiller .com domain.
Create a separate child OU for each office under Servers.
Move the computer accounts of all resource servers in each office to the appropriate child OU for that office.
Create an OU named Desktops under the Certkiller .com domain.
Create a separate child OU for each office under Desktops.
Move the computer accounts of all client computers in each office to the appropriate child OU for that office.
A.Create a toplevel
OU named Servers under the Certkiller .com domain.

Create a separate child OU for each office under Servers.
Move the computer accounts of all resource servers and domain controllers in each office to the appropriate child OU
for that office.
Create a toplevel
OU named Desktops under the Certkiller .com domain.
Create a separate child OU for each office under Desktops.
Move the computer accounts of all client computers in each office to the appropriate child OU for that office.

Answer: E

Explanation: We have a central operations department that is responsible for administering all resource servers and
domain controllers in all locations. The new have a local operations department in each office that is responsible for
administering all client computers within the individual department's office only, as well asrunning backups on the servers
in their data centers.
Therefore, we need atoplevel
OU under the Certkiller .com domain so that the central operations department can
administer all resource servers and domain controllers in all locations.
Incorrect Answers:
A, C:All computer accounts are located in the default computers container in the domain. Therefore it is not necessary
to move them to the top level OU. Also, we need to allow thelocal operations department in each office to administer all
client computers within the individual department's office, as well asrunning backups on the servers in their data
centers.
B:Thelocal operations department in each office is responsible for administering all client computers within the individual
department's office only, and is responsible forrunning backups only on the servers in their data centers. Placing the
client computers as well as the resource computers in the same OU will allow the local operations department to
administer the resource servers as well.
D:Thelocal operations department in each office is responsible forrunning backups on all the servers in their data
centers, not just the resource servers. Therefore, thechild OU for each office under the Servers OU must contain the
computer accounts of all resource servers and domain controllers in each office to the appropriate child OU for that
office.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 66
You are the network administrator for Certkiller .com. You plan to create an Active Directory domain named Certkiller .com that will have a functional level of Windows Server 2003.
Certkiller 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 toplevel
OU named Certkiller _Users under the Certkiller .com domain.
Create a separate child OU for each office under Certkiller _Users.
Move the user accounts of all employees in each office to the child OU for that office.
A.Create a toplevel
OU named Main_Office under the Certkiller .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.
A.Create a toplevel
OU named Certkiller _Users under the Certkiller .com domain.
Create a child OU named Central_Security under Certkiller _Users.
Move the user accounts of the central security department users to the Central_Security OU.
Create a child OU named Help_Desk under Certkiller _Users.
Move the user accounts of the help desk users to the Help_Desk OU.
A.Create a toplevel
OU named Certkiller _Users under the Certkiller .com domain.
Create a child OU named Central_Security under Certkiller _Users.
Move the user accounts of the central security department users to the Central_Security OU.

Answer: A

Explanation: Two OU levels will fit the requirement. You can delegate control for central security on the OU
" Certkiller _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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 63 to 69,616 to 623
Windows Server 2003 Active Directory and Network Infrastructure, Microsoft Press, Redmond, Washington,
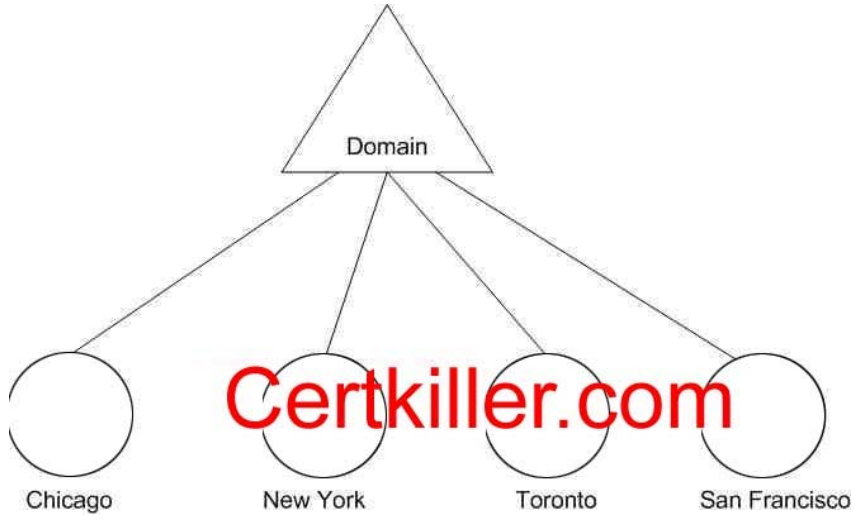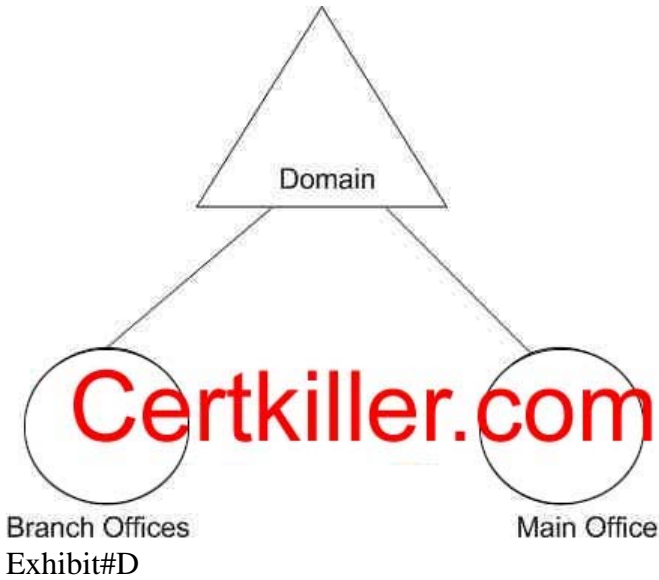
2004,
p. 4-11

QUESTION 67
Exhibit #A

Chicago   New York   Toronto   San Francisco

Exhibit #B

Chicago   New York   Main Office   Toronto   San Francisco

Exhibit#C

Domain

Certkiller.com

Branch Offices   Main Office

Exhibit#D

Domain

Certkiller.com

Chicago   Toronto   New York

You are a network administrator for Certkiller .com. 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 organization 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?

A. Exhibit A
B.Exhibit B
C. Exhibit C

D. Exhibit D

Answer: A

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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
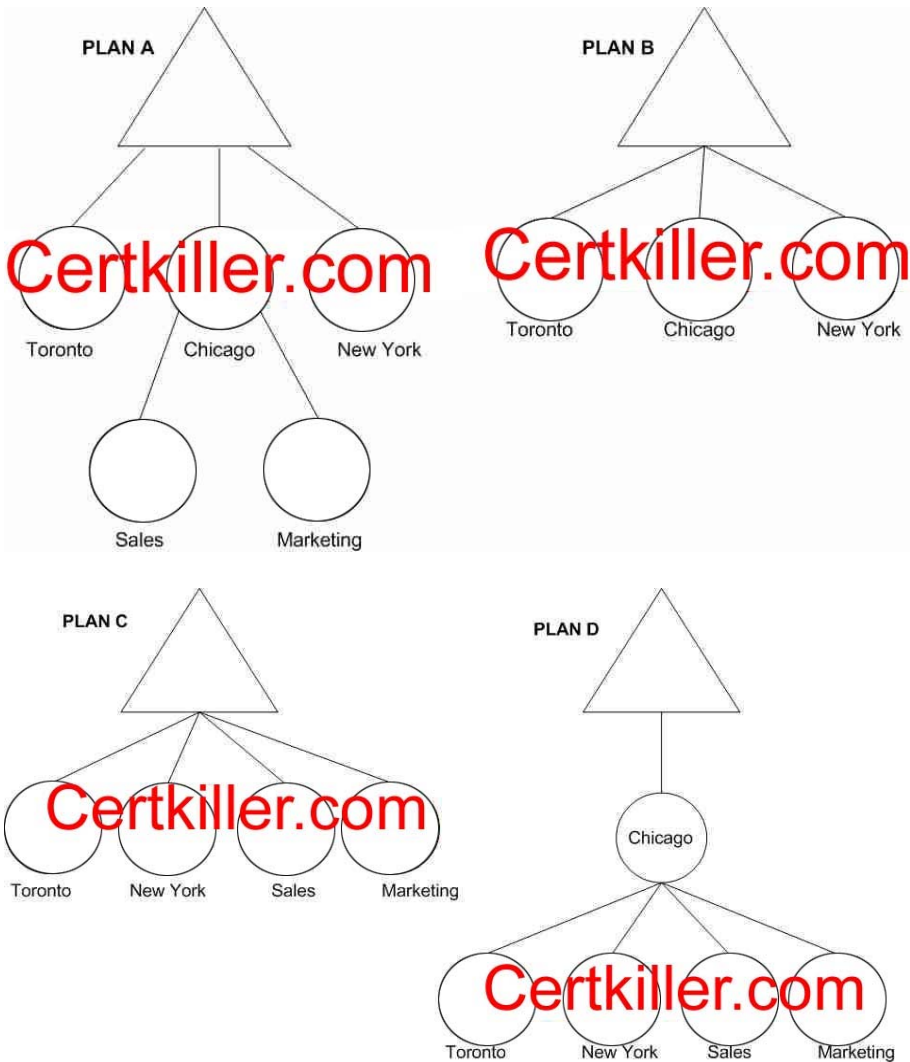Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 68
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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 Certkiller .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?

PLAN A
Toronto Chicago New York
Sales Marketing

PLAN B
Toronto Chicago New York

PLAN C
Toronto New York Sales Marketing

PLAN D
Chicago
Toronto New York Sales Marketing

A.Plan A
B.Plan B
C.Plan C
D.Plan D

Answer: A

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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 69
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory
domain named Certkiller .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.
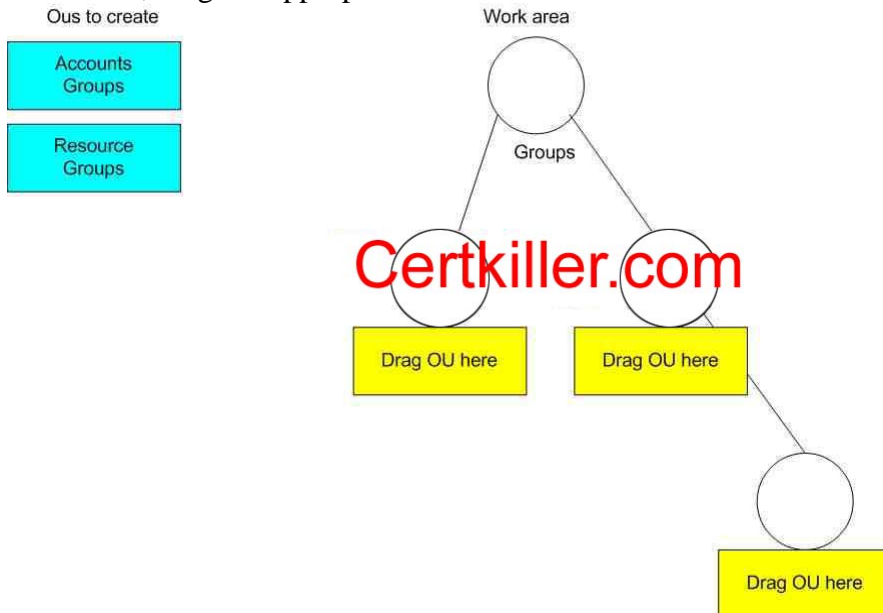The human resources department needs to be able to manage the membership of only the accounts groups.
The server support department needs to be able to manage the membership of only the resource groups.
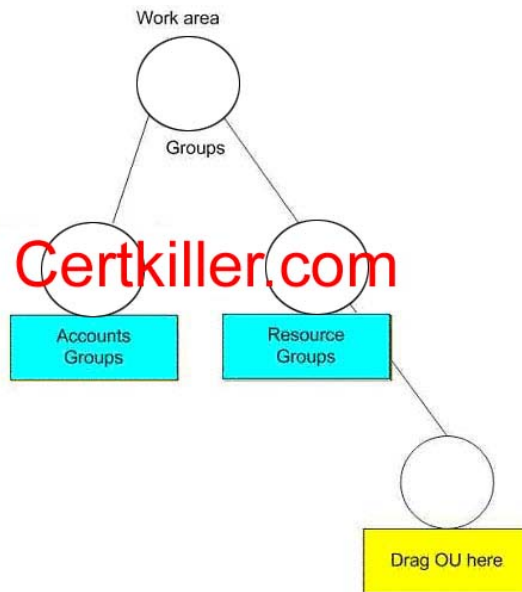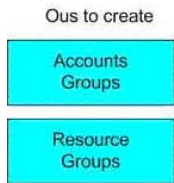The Domain Admins group needs to be able to manage all groups.
You need to configure the OU structure to allow the appropriate permissions to be granted. You want to
achieve this goal by using the minimum amount of administrative effort.
What should you do?
To answer, drag the appropriate OU or OUs to the correct location or locations in the work area.

Answer:

Explanation:
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 the resource 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 70
The company's departments are divided into two main divisions named Operations and Support. The local IT staff at each location are 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.
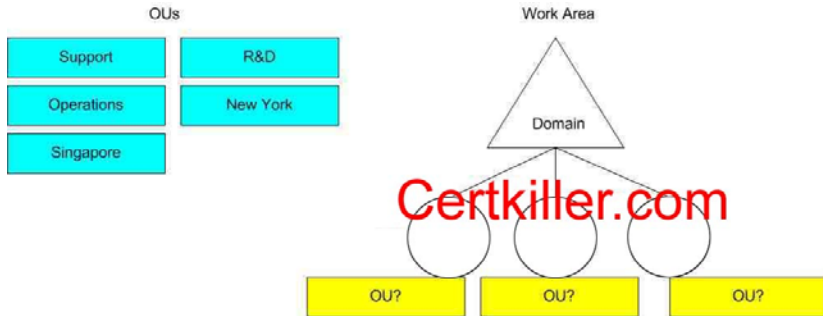You need to plan a toplevel
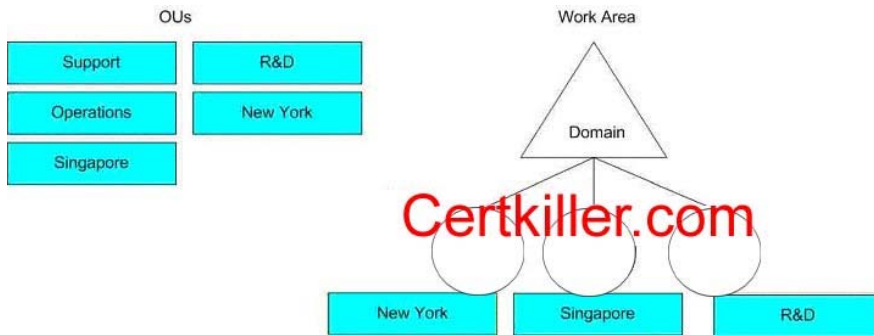organizational unit (OU) structure that facilitates delegation of administrative
control.
Which toplevel
OU or OUs should you create?

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

Answer:

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 71
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. 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.
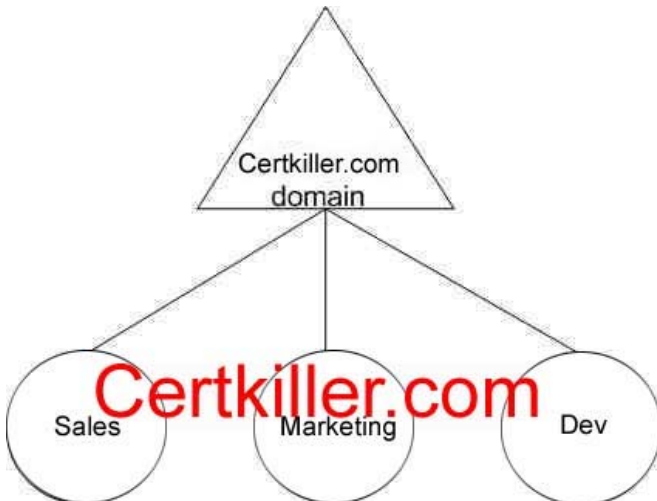
Certkiller uses an X.500 directory service enabled product to support a sales and marketing application. The application is used only by users in the sales department and the marketing department. The application uses InetOrgPerson objects as user accounts. InetOrgPerson objects have been created in 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.

King is another administrator in Certkiller . King 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 King to perform his responsibilities.

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

A.On the domain, grant King the permission to manage user objects.
B.On the domain, grant King 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: B, E

Explanation: 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:King needs to manage theInetorgPerson 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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 9-18 to 9-20,9-23 to 9-26

QUESTION 72

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. You work in the corporate IT department.

Certkiller consists of 12 business divisions. Each business division has its own toplevel 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.

A.Assign the Domain Admins group theAllow Full

Controlpermission for the administrative groups in the OU of each

division.

B.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.

A.Create a Restricted Groups Group Policy object (GPO) and link the GPO to the OU of each division.

Answer: C

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 theadministrative groups of the divisions into a toplevel

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 theAllow Full

Controlpermission 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 73
Exhibit A

Exhibit B
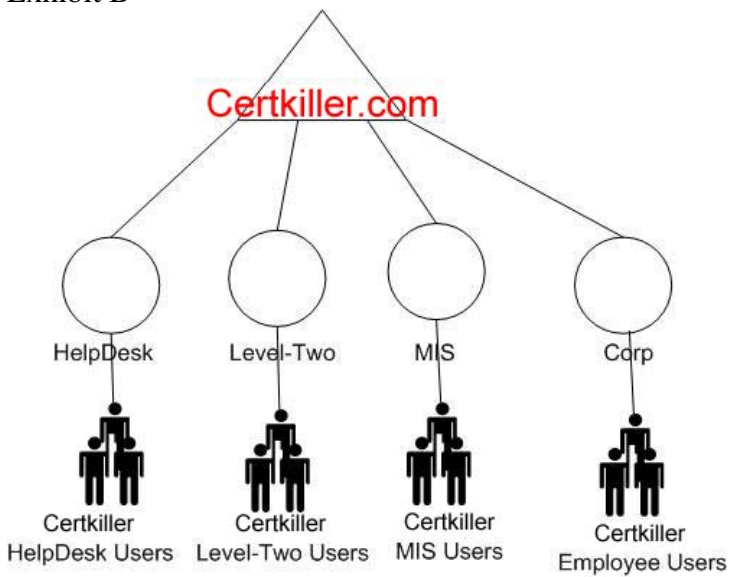
Exhibit C
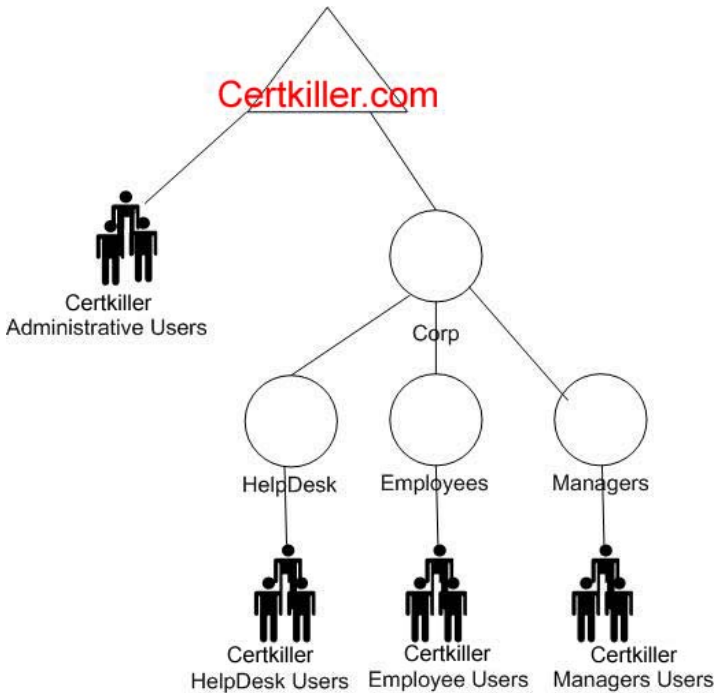
Exhibit D
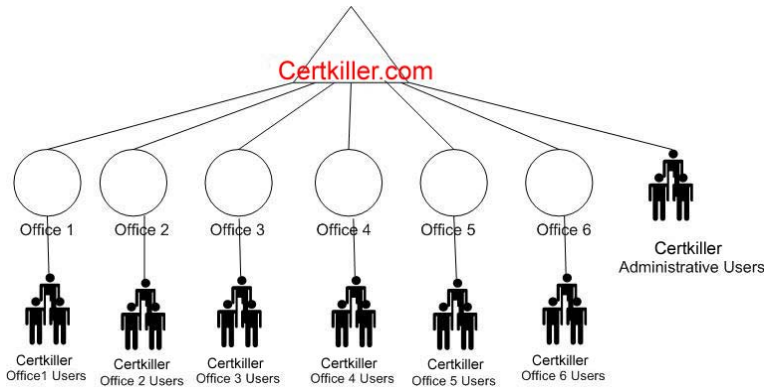
You are the network administrator for Certkiller , a company with six offices. The network consists of a single Active Directory domain named Certkiller .com.

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 leveltwo 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.

Group	Role
Help desk	User account maintenance for all employees who are not management
Leveltwo support	User account maintenance for all employees, the help desk users, and all management users

MIS group	Service account maintenance, maintenance of domain administrator accounts, and builtin accounts in Active Directory

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?

A. Exhibit A
B. Exhibit A
C. Exhibit C
D. Exhibit D

Answer: C

Explanation: We need to delegate the management of different groups of users.We have the nonmanagement 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 need to manage every other account.
To solution to 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 secondlevel
support staff.
Incorrect Answers:
A, B:Level 2 staff should manage HeldDesk, Employees and Managers.
D:We need to delegate administrative control based on user groups, not on office location.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 408411
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 74
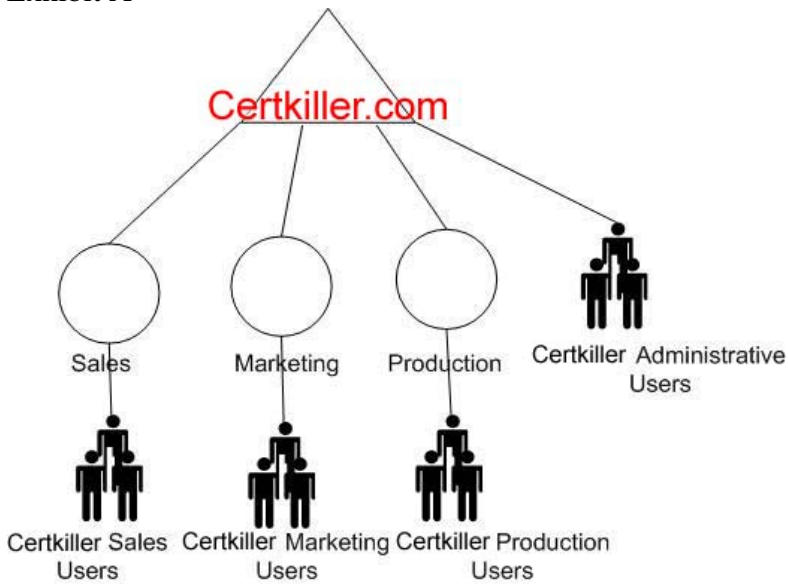You are a network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains two domains named Certkiller .com and dev. Certkiller .com. All domain controllers run Windows Server 2003. The functional level of the forest is Windows Server 2003. Certkiller acquires a company named Graphic Design Institute.
The Graphic Design Institute network consist of a single Active Directory forest that contains a single domain named graphicdesigninstitute.com. All domain controllers run Windows Server 2003. The functional level of the forest is Windows Server 2003.
Users in the Certkiller .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 Certkiller .com forest.
You must provide administrators with the ability to grant users access to the required resources.
What should you do?
A.Create a twoway
forest trust relationship between the Certkiller .com domain and the graphicdesigninstitute.com
domain.
In the Certkiller .com domain, enable forestwide
authentication for the graphicdesigninstitute.com domain.
In the graphicdesigninstitute.com domain, enable selective authentication for the Certkiller .com domain.
A.Create a twoway
external trust relationship between the Certkiller .com domain and the graphicdesigninstitute.com
domain.
B.Create a oneway
forest trust relationship in which the graphicdesigninstitute.com domain trusts the Certkiller .com
domain.
In the Certkiller .com domain, enable forestwide
authentication for the graphicdesigninstitute.com domain.
A.Create a oneway
external trust relationship in which the Certkiller .com domain trusts the graphicdesigninstitute.com
domain.
Create a second incoming external trust relationship on the graphicdesigninstitute.com domain.
Specify that the trust relationship in between the dev. Certkiller .com domain and the
graphicdesigninstitute.com domain.

Answer: A

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 forestwide
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 Certkiller .com domain require access to the graphicdesigninstitute.com domain. We will thus need the
graphicdesigninstitute.com domain to trust the Certkiller .com domain.

Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 4-48 to 4-49
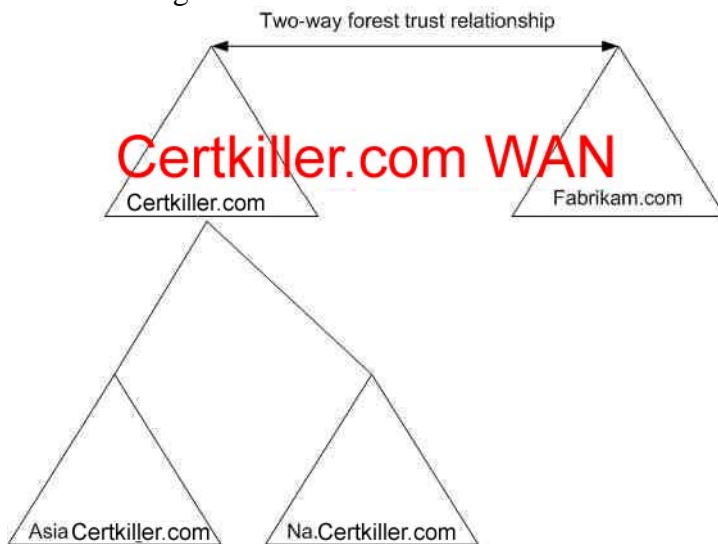Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,p. 254

QUESTION 75
Network Diagram

You notice that after the forest 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 userfriendly
names. A sample is shown in the Membership List exhibit.
MISSING
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 Certkiller .com forest.
What should you do?
A.Create new domain local groups.
Add the required global groups from the Certkiller .com forest to the domain local groups.
Grant appropriate permissions to the domain local groups.
Delete the original domain local groups.
A.Recreate
the trust relationship between Certkiller .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.
A.Verify all remaining trust relationships.
Then delete the unknown accounts from the domain local groups.

A.Delete all the affected domain local groups.
Recreate
the groups.
Add the appropriate global groups from the Certkiller .com forest to the groups.
Grant appropriate permissions to the domain local groups.

Answer: C

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 Certkiller .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 Certkiller .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
Certkiller .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 Certkiller .com forest users.
D:How would you know which are all the affected groups without verifying the trust relationships first.
Reference:
Craig Zacker, MCSE SelfPaced
Training Kit (Exam 70293):
Planning and Maintaining a Microsoft Windows Server
2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 4: 70

QUESTION 76
You work as a network administrator at Certkiller . You administer the Windows 2003 domain Certkiller .com
and a child domain named child1. Certkiller .com. The child1. Certkiller .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.
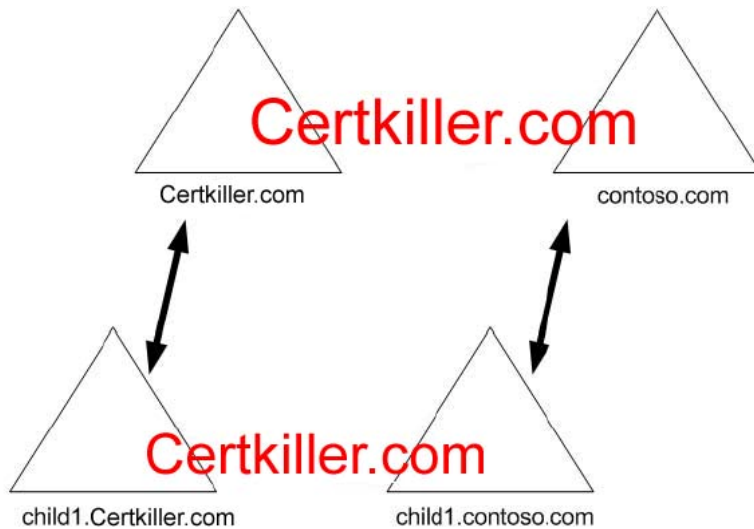
You need to create the minimum number of trust relationships required for the users in the
child1. Certkiller .com domain to access resources in both domains in the contoso.com forest.
What should you do?
A.Create a oneway
trust relationship in which the Certkiller .com domain trusts the contoso.com domain.
B.Create a oneway
trust relationship in which the contoso.com domain trusts the Certkiller .com domain.
C.Create a one-way trust relationship in which the child1. Certkiller .com domain trusts the contoso.com
domain. Create
a one-way relationship in which the child1. Certkiller .com domain trusts the child1.contoso.com domain.
D.Create a oneway
trust relationship in which the contoso.com domain trusts the child1. Certkiller .com domain. Create
a oneway
trust relationship in which the child1.contoso.com domain trusts the child1. Certkiller .com domain.

Answer: D

Explanation: Users in child1. Certkiller .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. Certkiller .com domain.We can
achieve this by
configuring two oneway
trust relationships: one in which the contoso.com domain trusts the child1. Certkiller .com
domain and one in which the child1.contoso.com domain trusts the child1. Certkiller .com domain.
Incorrect Answers:
A:The Certkiller user accounts are in the child1. Certkiller .com domain, not the Certkiller .com
domain.Therefore, the
contoso.com and child1.contoso.com domains need to trust the child1. Certkiller .com domain.
B:The Certkiller user accounts are in the child1. Certkiller .com domain, not the Certkiller .com
domain.Therefore, the
contoso.com and child1.contoso.com domains need to trust the child1. Certkiller .com domain.
C:The contoso.com and child1.contoso.com domains need to trust the child1. Certkiller .com domain.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 4-41 to 4-48

QUESTION 77
You are the network administrator for Certkiller . Your user account is a member of the Schema Admins
group. The network consists of a single Active Directory forest that contains three domains. The functional
level of the forest is Windows Server 2003. A Windows Server 2003 domain controller named Certkiller A
holds the schema master role.
An application named Application1 creates additional schema classes. You notice that this application
created some classes that have incorrect class names.
You need to correct the class names as quickly as possible.
What should you do?
A.Deactivate the Application1 classes that have the incorrect class names.
Set the default security permission for the Everyone group for those schema classes toDeny.
A.Deactivate the Application1 classes that have the incorrect class names.
Create the Application1 classes with the correct class names.
A.Rename the description of the Application1 classes to the correct class name.
Instruct the developers of Application1 to change the code of the application so that the renamed schema classes
can be
used.
A.Instruct the developers of Application1 to change the code of the application so that the application creates
the new
schema classes with the correct class names.
Reinstall Application1 and selectReload the schemain the Active Directory Schema console.

Answer: B

Explanation: We need to deactivatethe Application1 classes that have the incorrect class names. This is because
you
cannot delete or rename a class. We can only deactivate the incorrect classes and recreate the classes with the
correct
class names.
Extending the schema When
the set of classes and attributes in the base Active Directory schema do not meet your
needs, you can extend the schema by modifying or adding classes and attributes. You should only extend the
schema
when absolutely necessary. The easiest way to extend the schema is through the Schema Microsoft
Management
Console (MMC) snapin.
You should always develop and test your schema extensions in a test lab before moving them
to your production network.
Schema extensions are not reversible. Attributes or classes cannot be removed after creation. At best, they can
be
modified or deactivated.

Domain controllers running Windows Server2003 do not permit the deletion of classes or attributes, but they can be
deactivated if they are no longer needed or if there was an error in the original definition. A deactivated class or attribute
is considereddefunct
If your forest has been raised to the Windows Server2003 functional level, you can reuse the object identifier
(governsId and attributeId values), the ldapDisplayName, and the schemaIdGUID that were associated with the defunct
class or attribute. This allows you to change the object identifier associated with a particular class or attribute. The only
exception to this is that an attribute used as a rdnAttId of a class continues to own its attributeId, ldapDisplayName, and
schemaIdGuid values even after being deactivated (for example, those values cannot be reused).
If your forest has been raised to the Windows Server2003 functional level, you can deactivate a class or attribute and
then redefine it.
Incorrect Answers:
A:It is not necessary to deny access to the classes after deactivating them. We need to recreate the classes with the
correct names.
C:Changing the description of a class doesn't rename the class. It is not possible to rename a class.
D:We need to deactivate the classes that have the incorrect class names.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 7, p. 506

QUESTION 78
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. The domain contains a secure site and a main office site, as shown in the exhibit.

All domain controllers are configured as shown in the following table.

Drive	Contents

C	Boot partition, system partition, Active Directory database log files
D	Active Directory database
E	Files and folders

The motherboard on Certkiller 2 fails and Certkiller 2 is taken offline. One week later, an administrator connects to Certkiller 3 and seizes the schema master role.
You need to access files on drive E on Certkiller 2. You replace the motherboard on Certkiller 2 and bring Certkiller 2 online on an isolated subnet.
You need to be able to bring Certkiller 2 back into the secure site as quickly as possible in order to access the files.
What should you do?
A.Perform a full format of drive D on Certkiller 2.
Transfer the schema master role to a domain controller in the MainOffice site.
Remove references to Certkiller 2 from Active Directory by using the Ntdsutil utility and the ADSIEdit utility on
Certkiller 1.
A.Perform a full format of drive C on Certkiller 2.
Reinstall the operating system on Certkiller 2.
Remove references to Certkiller 2 from Active Directory by using the Ntdsutil utility and the ADSIEdit utility on
Certkiller 1.
A.Perform a full format of drive E on Certkiller 2.
Run thedcpromocommand on Certkiller 2.
Transfer the schema master role to a domain controller in the MainOffice site.
Join Certkiller 2 to the domain.
A.Perform a full format of drive C on Certkiller 2.
Transfer the schema master role to a domain controller in the MainOffice site.
Remove references to Certkiller 2 from Active Directory by using the Ntdsutil utility and the ADSIEdut utility on
Certkiller 1.

Answer: B

Explanation: We have seized the schema master role from Certkiller 2 on Certkiller 3.Therefore, we don't want to bring
Certkiller 2 back online with its old schema master role.Having two schema masters will cause problems in the forest.To
bring Certkiller 2 back online, we should format the C drive and reinstall the operating system.We should also 'clean' the
Active Directory database by removing references to Certkiller 2 from Active Directory by using the Ntdsutil utility

and the ADSIEdit utility on another domain controller.
Incorrect Answers:
A:We need to reinstall the operating system, so we should format drive C, not drive D.
C:Formatting drive E will erase the data we want to access.
D:The schema master role has already been transferred.We need to reinstall the operating system after formatting drive
C.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 7, p. 506

QUESTION 79

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com
Certkiller merges with a company named Acme. You need to create new user accounts for all of the Acme employees.
The email
address format for all users at Acme isalias@acme.com. The users need to continue to use their email
addresses after the merger. To decrease confusion, these users also need to be able to use their email
addresses as their user logon names when logging on to the company network.
You need to ensure that new users can log on by using their email
addresses as their logon names. You want
to achieve this goal by incurring the minimum cost and by using the minimum amount of administrative effort.
What should you do?
A.Create a new domain tree named acme.com in the Certkiller .com forest.
Create user accounts for all of the users in the acme.com domain.
A.Create a new forest named acme.com.
Create user accounts for all of the users in the acme.com domain.
Configure a forest trust relationship between the two forests.
A.Create user accounts for all of the new users in the Certkiller .com domain.
Configure the email
addresses for all of the Acme users asalias@acme.com.
A.Configure acme.com as an additional user principal name (UPN) suffix for the Certkiller .com forest.
Configure each user account to use the acme.com UPN suffix.

Answer: D

Explanation:
You can simplify the logon process for users by enabling UPN logon. When UPN logon is enabled, all users use the
same UPN suffix to log on to their domains. UPN names are comprised of the user's logon name and the DNS name of
the domain. When you enable UPN logon, users' logon names remain the same even when their domains change.
You might choose to enable UPN logon if:
1.Domain names in your enterprise are complex and difficult to remember.
2.Users in your organization might change domains as a result of domain consolidation or other organizational changes.
3.All domains in the forest are in native mode.
4.User logon names are unique within the forest.
5.A global catalog server is available to match the UPN to the correct domain account.
You can use one UPN suffix for all users in the forest.
Incorrect Answers:
A, B:Creating a new domain tree or forest and recreating the user accounts for all of the users in the acme.com domain
would require excessive administrative effort.
C:Creating new user accounts for all of the users in the acme.com domain would require excessive administrative effort.
Using the UPN logon feature would require less administrative effort.
Reference:
MS White Paper, Designing an Authentication Strategy
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 956

QUESTION 80
You are the network administrator for Certkiller Ltd. The network consists of a single Windows 2003 Active Directory domain named Certkiller .internal. The network includes 20 servers running Windows 2003 Server and 700 client computers running Windows 2000 Professional.
All servers belong to the default computer container. All client computers belong to an organization unit (OU) named Clients. All domain controllers belong to the default domain controller OU. Name resolution and IP addressing are controlled by DNS, WINS, and DHCP.
You need to ensure that the DNS suffix in the system properties of each client computer is set to Certkiller .com.
What should you do?
A.Create a new Group Policy object and link it to Clients.
Set the configuration of the primary DNS suffix to Certkiller .com.
A.Modify the default domain policy.
Set the configuration of the primary DNS suffix to Certkiller .com.
A.In the DHCP scope options, define the DNS domain name as Certkiller .internal.

B.In the DHCP scope options, define the NIS domain name as Certkiller .internal.

Answer: A

Explanation: We need to ensure that the DNS suffix in the system properties of each client computer is set to Certkiller .com.The client computers are located in an organization unit (OU) named Clients.The easiest way to achieve
this is to configure a GPO to set the configuration of the primary DNS suffix to Certkiller .com and link the GPO to the
Clients OU.
Incorrect Answers:
B:The setting should apply to the clients only.Linking the GPO to the domain will apply the settings to all computers in
the domain (including servers and domain controllers).
C:The question doesn't say that the servers have static IP addresses.If they are configured to use DHCP, then we can't
use DHCP to apply the DNS suffix setting because it will apply the settings to all computers in the domain (including
servers and domain controllers).
D:An NIS domain is a Unix/Linux domain.We have a Windows domain.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-4 to 10-7

QUESTION 81
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Certkiller has one office in Hong Kong and another office in Beijing. Each office is configured as an Active Directory site. Each site contains two domain controllers.
The network is configured to display a legal notice on the computer screens of all users before they log on to their client computers. At the request of the legal department, you make changes to the wording of the notice by changing the settings in a Group Policy object (GPO). The GPO is linked to the domain.
The legal department reports that not all users are receiving the new notice. You discover that users in the Beijing office receive the new notice, but users in the Hong Kong office receive the old notice. The problem continues for several days.
You need to ensure that the new notice appears correctly on all computers in the network.
What should you do?
A.Create a new security group that contains the computer accounts for all computers in the Hong Kong site. Grant permissions to this security group to read and apply the GPO.
A.Temporarily assign one of the domain controllers in the Hong Kong site to the Beijing site.
Wait 24 hours, and then reassign the domain controller to the Hong Kong site.
A.Force replication of Active Directory between the two sites.
B.Log on to one of the domain controllers in the Hong Kong site, and seize the infrastructure master role.

Answer: C

Explanation: It looks like the GPO settings have not been replicated to the Hong Kong office as they are still receiving
the old notice. We can manually force replication between the two sites to ensure that the Hong Kong office receives
the new GPO settings.
Incorrect Answers:
A:The Hong Kong users still receive the old legal notice.Therefore, this is not a permissions problem on the group
policy object.
B:This is unnecessary an impractical.
D:This has nothing to do with the replication of the GPO.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-21 to 1-24,5-3 to 5-9,5-25 to 5-37

QUESTION 82
You are a network administrator for Certkiller . The network consists of single Active Directory forest that
contains two domains and four sites. All servers run Windows Server 2003. You are responsible for
administering domain controllers in one site. Your site contains four domain controllers. The hard disk that
contains the Active Directory database fails on a domain controller named Certkiller 2.
You replace the failed disk.
You need to recover Certkiller 2. You need to achieve this goal without affecting existing Active Directory
data.
What should you do?
A.Perform a nonauthoritative restoration of the Active Directory database.
B.Perform an authoritative restoration of the Active Directory database.
C.Use the Ntdsutil utility to run thesemantic database analysiscommand.
D.Use the Ntdsutil utility to run therestore subtreecommand.

Answer: A

Explanation: The nonauthoritative restore is also called the normal restore method. This method should be
selected
when you have more than one domain controller on the network and you do not need to roll back changes that
have
been made to Active Directory. In this method, when replication takes place between the restored domain
controller
and other domain controllers on the network, the restored domain controller receives updates from its
replication
partners. You have four domain controllers in your site. You can simply perform a nonauthoritative
restore of theActive
Directory database. Any changes to the Active Directory database since the data was backed up will be
replicated from

another domain controller.
Incorrect Answers:
B:This is not necessary. This will overwrite theActive Directory database on the other domain controllers.The other
domain controllers will have the most recent copies of theActive Directory database. These changes can be replicated
to the failed machine.
C:You can use this process to generate reports on the number of records present in theActive Directory database,
including deleted and phantom records. It is not used to restore theActive Directory database.
D:We need to restore the entireActive Directory database, not just a subtree of it.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, p. 16: 28

QUESTION 83

You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. Password resets are performed on user accounts on all servers regularly
throughout each day. The Windows Server 2003 computers named Certkiller A, Certkiller B, and Certkiller C
are configured as shown in the following table.

Server name	Site	Server role	Backup schedule
CertkillerA	Toronto	Global catalog server	Daily
CertkillerB	San Francisco	Domain controller, forest-wide and domain-wide operations master roles	Daily
CertkillerC	Boston	Global catalog server	Weekly on Fridays

One Wednesday morning, another network administrator in Boston connects to Certkiller C and deletes an
organizational unit (OU) named BostonUsers. The change replicates to all sites in the forest.
Users in Boston report that they can no longer log on to the network.
You need to provide the users in Boston with the ability to log on to the network as soon as possible. You
must also ensure that there is minimal disruption to the users in Toronto and San Francisco.
What should you do?
A.Restore the BostonUsers OU on Certkiller A from backup.
Use the Ntdsutil utility to mark the BostonUsers OU as authoritative.
Allow replication to take place.
A.Restore the BostonUsers OU on Certkiller B from backup.
Allow replication to take place.
A.Restore the Ntdsutil utility to connect to Certkiller A.
Use themetadata cleanupcommand to remove Certkiller C from Active Directory.
Force replication.
A.Use the Ntdsutil utility on Certkiller C to mark the domain context as authoritative.
Force replication.

Answer: A

Explanation: We need to restore the BostonUsers OU.We should restore it on Certkiller A because that domain
controller has a more recent backup.We need to mark the BostonUsers OU as authoritative so that it gets

replicated to
the other domain controllers.If we didn't mark the BostonUsers OU as authoritative, it would get deleted again at the
next AD replication.
Incorrect Answers:
B:We need to mark the BostonUsers OU as authoritative so that it gets replicated to the other domain controllers.If we
didn't mark the BostonUsers OU as authoritative, it would get deleted again at the next AD replication.
C:We need to restore the BostonUsers OU.This won't restore the OU.
D:We need to restore the BostonUsers OU.This won't restore the OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 2-49 to 2-51

QUESTION 84
You are a network administrator for Certkiller .com. The network consist of a single Active Directory domain named Certkiller .com. The domain name is Certkiller .com. The network contains three Windows Server 2003 domain controllers.
You are creating the recovery plan for the company. According to the existing backup plan, domain controllers are backed up by using normal backups each night. The normal backups of the domain controllers include the system state of each domain controller.
Your recovery plan must incorporate the following organization requirements:
1.Active Directory objects that are accidentally or maliciously deleted must be recoverable.
2.Active Directory must be restored to its most recent state of quickly as possible.
3.Active Directory database replication must be minimized.
You need to create a plan to restore a deleted organizational unit (OU).
Which two actions should you include in your plan? (Each correct answer presents part of the solution. Choose two)
A.Restart a domain controller in Directory Services Restore Mode.
B.Restart a domain controller in Safe Mode.
C.Use the Ntdsutil to perform an authorative restore operation of the Active Directory database.
D.Restore the system state by using theAlways replace the file on my computeroption.
E.Use the Ntdsutil utility to perform an authoritative restore operation of the appropriate subtree.

Answer: A, E

Explanation: If an OU gets deleted from the Active Directory, we can restore it from a backup of the system state
data.Directory Services Restore Mode is a sort of safe mode in which we can boot a domain controller without loading
the Active Directory.This will enable us to restore all or part of the Active Directory database.
To ensure that the deleted OU isn't deleted again by replication from another domain controller, we must use the Ntdsutil utility to mark the restored subtree as authoritative.
Incorrect Answers:
B:To restore part of the Active Directory, we must start a domain controller in Directory Services Restore

Mode, not
safe mode.
C: We don't need to restore the entire Active Directory database; we can just restore part of
D:This will overwrite the existing Active Directory database.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 2-49 to 2-53

QUESTION 85
You are a network administrator for Certkiller . The network consists of a single Active Directory domain
Certkiller .com. The network contains three Windows Server 2003 domain controllers.
You are creating the recovery plan for Certkiller . According to the existing backup plan, domain controllers
are backed up by using normal backups each night. The normal backups of the domain controllers include
the system state of each domain controller.
Your recovery plan must incorporate the following organizational requirements:
1.Active Directory objects that are accidentally or maliciously deleted must be recoverable.
2.Active Directory must be restored to its most recent state as quickly as possible.
3.Active Directory database replication must be minimized.
You need to create a plan to restore a deleted organizational unit (OU).
Which two actions should you include in your plan? (Each correct answer presents part of the solution.
Choose two)
A.Restart a domain controller in Directory Services Restore Mode.
B.Restart a domain controller in Safe Mode.
C.Use the Ntdsutil utility in Safe Mode.
D.Restore the system state by using theAlways replace the file on my computeroption.
E.Use the Ntdsutil to perform an authoritative restore operation of the appropriate subtree.

Answer: A, E

Explanation: If an OU gets deleted from the Active Directory, we can restore it from a backup of the system
state
data. Directory Services Restore Mode is a sort of safe mode in which we can boot a domain controller without
loading
the Active Directory. This will enable us to restore all or part of the Active Directory database.
To ensure that the deleted OU isn't deleted again by replication from another domain controller, we must use the
Ntdsutil utility to mark the restored subtree as authoritative.
Incorrect Answers:
B:To restore part of the Active Directory, we must start a domain controller in Directory Services Restore
Mode, not
safe mode.
C: We don't need to restore the entire Active Directory database; we can just restore part of
D:This will overwrite the existing Active Directory database.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 2-49 to 2-53

QUESTION 86
You are a network administrator for Certkiller . Your network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
A help desk user reports that a user object was accidentally deleted and the user can no longer log on to the domain and access resources. You confirm that the user object was included in the most recent backup.
You need to enable the user to log on to the domain. You must ensure that the user retains access to resources.
What should you do?
A.Install a new domain controller.
Install Active Directory from media by using the most recent backup.
Manually initiate replication.
A.Decrease the garbage collection interval.
Perform a nonauthorative restoration of Active Directory by using the most recent backup.
A.Perform a nonauthorative restoration of Active Directory by using the most recent backup.
Authoritatively restore the user object that was deleted.
A.Recreate
a user object that has the same user principal name (UPN) as the user object that was deleted.
Authoritatively restore this user object.

Answer: C

Explanation: If you inadvertently delete or modify objects stored in the Active Directory directory service, and those
objects are replicated or distributed to other servers, you will need to authoritatively restore those objects so they are
replicated or distributed to the other servers. If you do not authoritatively restore the objects, they will never get
replicated or distributed to your other servers because they will appear to be older than the objects currently on your
other servers. Using the Ntdsutil utility to mark objects for authoritative restore ensures that the data you want to restore
gets replicated or distributed throughout your organization. On the other hand, if your system disk has failed or the
Active Directory database is corrupted, then you can simply restore the data nonauthoritatively without using the
Ntdsutil utility.
Active Directory gives network users access to permitted resources anywhere on the network using a single logon
process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of
administration for all network objects. Active directory service data can be restored using one of three restore methods:
1.Primary restore
2.Normal (nonauthoritative) restore
3.Authoritative restore
In Backup, a type of restore operation performed on an Active Directory domain controller in which the objects

in the
restored directory are treated as authoritative, replacing (through replication) all existing copies of those objects.
We need to restore the Active Directory database nonauthoritatively,
and then from the restored copy of the database,
we need to authoritatively restore the user object.
Incorrect Answers:
A:It isn't necessary to install a new domain controller.
B:We need to authoritatively restore the user object, otherwise AD replication will delete the user object again.
D:Creating a new user account won't work because the new user account will have a different SID from the deleted
account.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, p. 16: 28

QUESTION 87
You are a network administrator for Certkiller . The network consists of a single Active Directory domain
named Certkiller .com. All servers run Windows Server 2003. Eric works in the sales department. User objects
for sales users are stored in an organizational unit (OU) named Sales. When Eric is transferred to another
department, you delete Eric's user account. Several weeks later, Eric is transferred back to the sales
department. You create a new user accounts in the Sales OU and grant the account access to sales
resources. When Eric attempts to open any of the 1,000 files that he created before he was transferred, he
receives the following error message. "Access Denied". He reports that he receives this error message for
all 1,000 files in 150 different locations.
You need to provide Eric with access to files that he created both before his first transfer and after his return
to the sales department, you must accomplish this task without affecting other users on the network.
What should you do?
A.Move Eric's existing account to a new OU. Nonauthoritatively restore the OU that contained Eric's previous
account.
B.Nonauthoritatively restore Eric's old account. Force Active Directory replication to occur.
C.Authoritatively restore Eric's old account. Force Active Directory replication to occur.
D.Rename Eric's existing account. Authoritatively restore Eric's old account.

Answer: D

Explanation: Although we have created another account named Eric, Eric will not be able to access any of his
files.This
is because the new 'Eric' account has a different Security Identifier (SID) to the previous account.It is therefore
considered to be a different account.We could set permissions on the new account, but this would take a long
time.It
would be easier to restore a copy of Eric's old account from backup.To avoid have two accounts with the same
name,
we should rename the existing account, before restoring the previous account.
Incorrect Answers:
A:We don't need to restore an entire OU.We can restore just Eric's previous account.

B:We need an authoritative restore.Otherwise, the restored account would be deleted again at the next Active Directory replication.

C:To avoid have two accounts with the same name, we should rename the existing account, before restoring the previous account.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 16: 2829

QUESTION 88

You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The Active Directory database contains 500 MB of information.

Certkiller has its main office in Moscow and a branch office in Minsk. The two offices are connected by a 56Kbps

WAN connection that is used only for Active Directory replication. The Moscow office has 450

users, and the Minsk office has 15 users.

The Minsk office has a single Windows Server 2003 domain controller and two Windows Server 2003 file and print servers. The hard disk containing the operating system on the domain controller in Minsk fails and cannot be recovered.

You need to reestablish

a domain controller that contains a current copy of Active Directory in the Minsk

office. You need to achieve this goal as quickly as possible.

What should you do?

A.Replace the hard disk on the domain controller.

Install Windows Server 2003 on the domain controller.

Install Active Directory from restored backup files.

A.Install Active Directory on a file and print server.

Force replication.

A.Install Active Directory on a file and print server from restored backup files.

B.Replace the hard disk on the domain controller.

Install Windows Server 2003 on the domain controller.

Force replication.

Answer: C

Explanation: We need to re-establish a domain controller in the Minsk office as quickly as possible. Therefore, we

should install Active Directory fromrestored backup files. Answer A is the recommended answer, but answer C is

quicker.We can use the new dcpromo /adv command to promote the DC from a backup of the system state data of an

existing domain controller.

The /adv switchis only necessary when you want to create a domain controller from restored backup files. It is not

required when creating an additional domain controller over the network.

For additional domain controllers in an existing domain, you have the option of using the install from media

feature,
which is new in Windows Server2003. Install from media allows you to prepopulate
Active Directory with System
State data backed up from an existing domain controller. This backup can be present on local CD, DVD, or hard disk
partition.
Installing from media drastically reduces the time required to install directory information by reducing the amount of data that is replicated over the network.Installing from media is most beneficial in large domains or for
installing new domain controllers that are connected by a slow network link.
Incorrect Answers:
A:This would work but answer C is quicker.
B:We don't want to replicate a 500MB Active Directory database over a 56Kbps WAN link.
D:We don't want to replicate a 500MB Active Directory database over a 56Kbps WAN link.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 2: 27

QUESTION 89
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com with two sites. The Active Directory database is backed up every evening.
A network administrator in Site1 deletes an empty organizational unit (OU) named Projects. At about the
same time, a network administrator in Site2 moves 20 existing user accounts into the Projects OU. Later, the
administrator in Site2 discovers that the Projects OU was deleted from Active Directory. He cannot see the
user accounts that he moved into the OU.
You need to provide an OU named Projects and add the 20 user accounts to the Projects OU. The users'
access to network resources must not be affected by this process.
What should you do?
A.Perform an authoritative restore operation of the Projects OU and the user accounts on a domain controller in
Site2.
B.Perform a nonauthoritative restore operation of the Projects OU and the user accounts on a domain controller
in
Site2.
C.Create a new OU named Projects.
Create 20 new user accounts that have the same user principal name (UPN) prefix.
Move the user accounts into the new Projects OU.
A.Create a new OU named Projects.
Move the 20 user accounts from the LostAndFound container to the new Projects OU.

Answer: D

Explanation: You moved the users to an OU that had just been deleted.When you move objects to an object that is no
longer there, the objects get moved to the LostAndFound container.This means that we haven't lost the user accounts,

so we can just recreate
the Projects OU and move the users from the LostAndFound container to the new OU.
Incorrect Answers:
A:The user accounts haven't been deleted, so we don't need to restore them.
B:The user accounts haven't been deleted, so we don't need to restore them.
C:The user accounts haven't been deleted, so we don't need to recreate them.Furthermore, recreating the user accounts
in this way will not work to restore the original accounts.The new accounts will be different accounts with different SIDs
(Security Identifiers).
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 38-39, 99-101

QUESTION 90
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains three Windows Server 2003 domain controllers.
A domain controller named DC2. Certkiller .com fails because of a hardware failure. You decide not to rebuild the domain controller. However, because several applications refer to DC2. Certkiller .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 Certkiller .com domain. The promotion fails and you receive the following error message.

You need to install a new domain controller named DC2 in the Certkiller .com domain.
What should you do?
A.Use the WINS administrative console to remove all WINS record for DC2. Certkiller .com
B.Use the Ntdsutil utility to remove the metadata associated with the DC2. Certkiller .com domain controller object from
Active Directory.
C.Use Active Directory Users and Computers to remove the DC2. Certkiller .com domain controller computer account
for the Certkiller .com domain.
D.Use the DNS administrative console to remove all DNS record that refer to DC2. Certkiller .com

Answer: B

Explanation:
When DC2 failed metadataassociated with the DC2remained in Active Directory.This metadata is indicating that DC2
already exists. We must remove this metadata by using theNtdsutil 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 metadataassociated with the DC2remained in Active
Directory.
C:Objects deleted from Active Directory remain there until the tombstonelifetime attribute has expired. This is 60 days
by default.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 2-49 to 2-51

QUESTION 91
You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
Certkiller 's written security policy requires that all administrative passwords be changed every 30 days. You configure the domain security policy to enforce the written security policy. A security audit reveals that the password used to log on to domain controllers in Directory Services Restore mode is 10 months old.
You need to ensure that all passwords are changed in accordance with the written security policy. You must accomplish this task without causing disruption to user access.
What should you do?
A.Restart each domain controller in Directory Services Restore More.
Use Computer Management to reset the password for the Administrator account.
A.Use the Ntdsutil utility to reset the password on each domain controller for Directory Services Restore Mode.
B.Configure the Domain Controller Security Policy to enforce the written security policy.
C.Reset the Administrator password by using Active Directory Users and Computers.

Answer: B

Explanation: In Windows Server 2003, you can use the Ntdsutil utility to modify the Directory Service Restore Mode
Administrator password.
Incorrect Answers:
A:Restarting the domain controllers will cause a disruption in user access.
C:The Domain Controller Security Policy is enforced when the domain controller is booted and can be refreshed at set
intervals. However, the Directory Service Restore Mode Administrator password is a user account setting, not a computer account setting and should be enforced when t he user logs on.
D:Directory Service Restore Mode Administrator password cannot be set in Active Directory Users and Computers.

References:
MS Knowledgebase Article 322672: How to reset theDirectory Service Restore Mode Administrator Account
Password in Windows Server 2003.
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 2-49 to 2-53

QUESTION 92
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .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.

Directory Services object property	Setting
garbageCollPeriod	15 hours
tombstoneLifetime	5 days

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

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 tombstone lifetime 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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 14: 3940

http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q216/9/93. ASP&NoWebContent=

QUESTION 93

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. The domain is shown in the exhibit.

Replication is scheduled to take place once per day. Each server is fully backed up daily.
You connect to Certkiller 1 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 Certkiller 3. Ten minutes later, you successfully make changes to one of the logon scripts on Certkiller 1.
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 Certkiller1 normally.

Restart Certkiller3 normally.

Restart Certkiller1 in Directory Services Restore Mode.

Restart Certkiller3 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

Drag 1st action here

Drag 2nd action here

Drag 3rd action here

Drag 4th action here

Drag 5th action here

Drag 6th action here

Answer:

Possible Actions

Restart Certkiller1 normally.

Restart Certkiller3 normally.

Restart Certkiller1 in Directory Services Restore Mode.

Restart Certkiller3 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

Restart Certkiller3 in Directory Services Restore Mode.

Use Backup to restore the SYSVOL folder.

Restart Certkiller3 normally.

Drag 4th action here

Drag 5th action here

Drag 6th action here

Explanation:
You want to get Certkiller 3 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 2-40 to 2-41

QUESTION 94
You are the network administrator for Certkiller . The network consists of a single Active Directory domain
named Certkiller .com that contains two Windows Server 2003 domain controllers named Certkiller 1 and
Certkiller 2. Certkiller 1 runs DNS for the domain. Backups of the system state are performed each night on
each domain controller.
A power surge damages both domain controllers. You replace the domain controllers with two new computers
and retrieve the latest backup tapes.
You need to restore the Active Directory domain by using the backup tapes. You want to restore name
resolution services first.

What should you do?
To answer, drag the action that should perform first to the First Action box for each server. Continue dragging actions to the corresponding numbered boxes until you list all three required actions to restore Certkiller 1 and all three required actions to restore Certkiller 2.

Actions	Required Actions	
Perform an authoritative restore operation of the system state.	First Action	Drag action here
Install Windows Server 2003 and then restart the server.	Second Action	Drag action here
Restart the server in Directory Services Restore Mode.	Certkiller1 Third Action	Drag action here
Restart the server to the Recovery Console.		
Perform a nonauthoritative restore operation of the system state.	First Action	Drag action here
Perform a primary restore operation of the system state.	Second Action	Drag action here
Promote the server to become a domain controller.	Certkiller2 Third Action	Drag action here

Answer:

Actions	Required Actions	
Perform an authoritative restore operation of the system state.	First Action	Install Windows Server 2003 and then restart the server.
Install Windows Server 2003 and then restart the server.	Second Action	Restart the server in Directory Services Restore Mode.
Restart the server in Directory Services Restore Mode.	Certkiller1 Third Action	Perform a primary restore operation of the system state.
Restart the server to the Recovery Console.		
Perform a nonauthoritative restore operation of the system state.	First Action	Install Windows Server 2003 and then restart the server.
Perform a primary restore operation of the system state.	Second Action	Restart the server in Directory Services Restore Mode.
Promote the server to become a domain controller.	Certkiller2 Third Action	Perform a nonauthoritative restore operation of the system state.

Explanation:
Both domain controllers need to be restored.The first thing to do on each new server is to install Windows Server 2003.
To restore the System State data on a domain controller, you must first start your computer in a special startup option
called Directory Services Restore Mode. This will allow you to restore the SYSVOL directory and Active Directory
service database. To access Directory Services Restore Mode, press F8 during startup and select it from the list of
startup options.On the first domain controller, we can do a primary restore of the System State data as this will be the
first domain controller on the network.On the second domain controller, we can do a nonauthoritative restore of the
system state data.This way, any changes to the Active Directory on the first server will be replicated to the second
server.

QUESTION 95
You are the network administrator for Certkiller .com. Certkiller consists of a single Active Directory domain
named Certkiller .com Certkiller has a main office and a branch office. The domain contains four domain
controllers. Two domain controllers are located in the main office, and two domain controllers are located in
the branch office.
You create a Group Policy object (GPO) named WPSoft and link it to the domain. You configure WPSoft to
assign a word processing application to the User Configuration section of the GPO. Users in the branch
office report that the application is not available to use. Users in the main office report that they can use the
application.
You need to ensure that the users at the branch office receive the Word processing application.
What should you do?
A.Synchronize the Netlogon shared folder on both domain controllers in the branch office.
B.Force replication between the domain controllers in the main office and the branch office.
C.Run thegpresultcommand on the client computers in the branch office.
D.Run thegpotoolcommand on a client computer in the branch office.

Answer: B

Explanation: We have created a GPO and linked it to the domain.The domain controllers will receive the new
group
policy at the next replication interval.Alternatively, we can force replication between the domain controllers in
the main
office and the branch office by running thegpupdate /forcecommand.
Incorrect Answers:
A:We need to initiate AD replication between the main office and the branch office.
C:The Gpresult commandline
tool allows you to create and display an RSoP query, which can be used to analyze the
cumulative effects of GPOs, through the command line. It also provides general information about the operating
system,
user, and computer.This will have no effect as the domain controllers in the branch office haven't received the
new GPO
yet.
D:This will have no effect as the domain controllers in the branch office haven't received the new GPO yet.
Reference:
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/
refrgp.mspx
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-44 to 10-21,11-4,11-6,11-19 to 11-22,19-3

QUESTION 96
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain with two sates. The two sites are named Certkiller 1 and Certkiller 2. All servers run Windows Server
2003.
Certkiller has two offices, and each office is configured as one of the sites. A 256Kbps
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. Certkiller 1 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 snapins
to connect to the
infrastructure master.
B.Configure the Group Policy and Active Directory snapins
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

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 he
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
snapin
to connect to a domain controller in the site where the GPO must be applied.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-31 to 10-48

QUESTION 97
You are the administrator of the Certkiller company network. Certkiller has a main office and two branch offices.The branch offices are named Branch1 and Branch2.Each office is configured as an Active Directory site in the Certkiller .com domain.All servers run Windows Server 2003 and all client computers run Windows XP Professional.The two branch offices are connected to the main office by 256Kbps WAN links.
AGroup Policy object (GPO) linked to the domain is configured to display a message when users log on their computers.You change the wording of the message to comply with new company guidelines.Users in the main office and Branch1 receive the new logon message.However, users in Branch2 still receive the old logon message.
You need to ensure that the new logon message appears correctly on all computers in the network.
What should you do?
A.In Active Directory Users and Computers, create a new global security group that contains the computer accounts
for all computers in Branch2.
Grant permissions to this security group to read and apply the GPO.
A.Create a new Group Policy Object (GPO) linked to the Branch2 site to display the new logon message.
B.Force replication of Active Directory between the main office and Branch2.
C.Log on to one of the client computers in Branch2 and run thegpupdatecommand.

Answer: C

Explanation: It appears that the GPO settings haven't been replicated to Branch2 as they are still receiving the old
notice.We need to force replication between the two sites to ensure that Branch2 receives the new GPO settings.
Incorrect Answers:
A:The Branch2 users still receive the old logon message.Therefore, this is not a permissions problem on the group
policy object.
B:This is unnecessary.
D:This would refresh the GPO from a Branch2 domain controller.We need to force replication to ensure that the Branch2 domain controllers have the latest GPO.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 5-4 to 5-9,5-25

QUESTION 98
You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain and two Active Directory sites. The sites are named Certkiller 1 and Certkiller 2. Each site contains two Windows Server 2003 domain controllers. All client computers on the network run Windows XP Professional. Administrators in Certkiller 1 manage all user and group administration on the network.
One of the executives located in the office at Certkiller 2 requires access to a network shared folder named ExecutiveData. This folder is located on a Windows Server 2003 member server at Certkiller 2. An administrator in Certkiller 1 adds the executive to an Active Directory global group that has access to the ExecutiveData shared folder.
The executive restarts her computer and logs back on to the domain. One hour later, the executive still

cannot access the shared folder. Other users in the same group can access the shared folder.
You need to ensure that the executive has immediate access to the ExecutiveData shared folder.
What should you do?
A.Modify the NTFS permissions on the ExecutiveData shared folder on the Windows Server 2003 member
server.
B.Configure one of the domain controllers in Certkiller 2 as a global catalog server.
C.Use Replication Monitor to force replication between domain controllers in the two sites.
D.Modify the share permissions on the ExecutiveData shared folder to give the user account explicit
permissions.

Answer: C

Explanation: The reason why the executive cannot access the folder is because replication did not yet occur.
Replication need to occur between Certkiller 1 and Certkiller 2 before the executive can access the folder.
Incorrect Answers:
A, D:This is not a permissions problem as other users can access the ExecutiveData shared folder.
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. However, this is a replication problem.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 5-4 to 5-8,5-25 to 5-37

QUESTION 99
You are the network administrator for Certkiller , which is located in New York. Certkiller owns a company
named Lucerne Publishing, which is located in London. The Certkiller network consists of a single Active
Directory forest that contains two domains.
Certkiller 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.
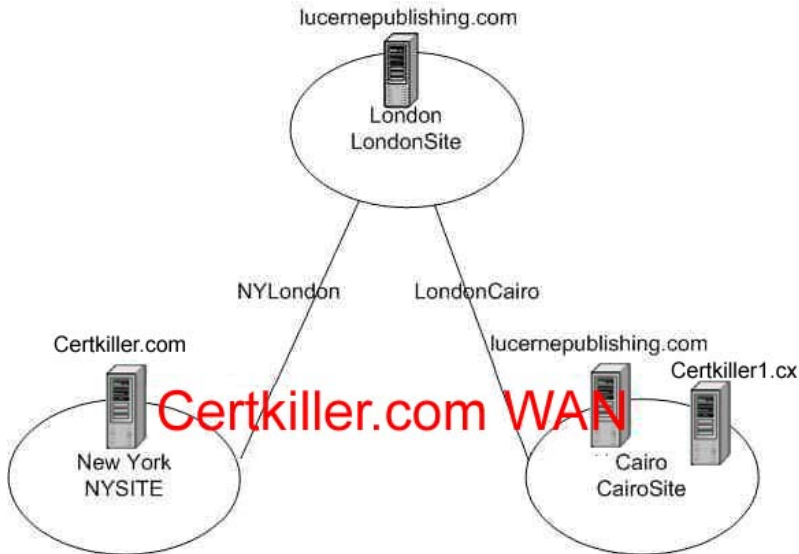
Both site links are configured to be transitive. The site links are configured as shown in the following table.

	NYLondon	**LondonCairo**
Cost	200	100
Interval	30 minutes	45 minutes
Schedule	11:00 P.M. 1:00 A.M. UTC	7:00 P.M. 9:00 P.M. UTC

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?

A.Replace the current site links with SMTPbased
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

Explanation: Replication is occurring through out the day. We need to reconfigure the replication schedule to prevent
this.

Incorrect Answers:

A:Replacing the links with SMTPbased
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 single paths in this
scenario.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 4-494-52,4-58
to 4-59

QUESTION 100
You are a network administrator for Certkiller .com. The network consists of two Active Directory domains with three sites. All servers run Windows Server 2003. Certkiller has offices in three cities and each office is configured as a separate site. The network configuration is shown in the exhibit.
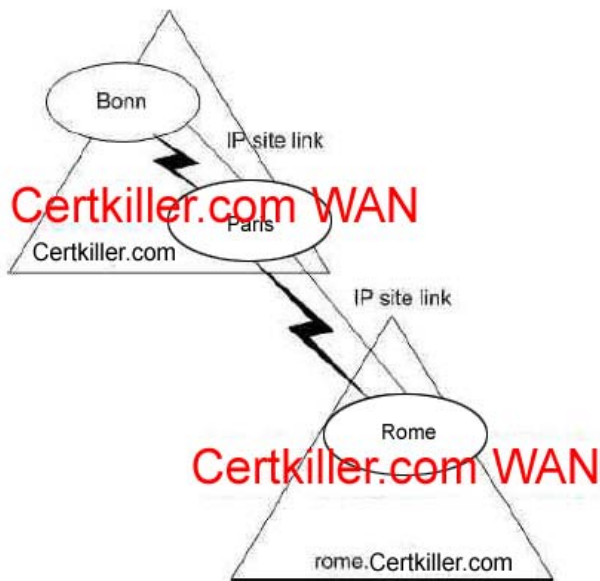
The company has 1,750 users in the Paris office, 1,750 users in the Rome office, and 25 users in the Bonn office. Global catalog servers are configured in each site. Automatic site link bridging is disabled.
A written company policy requires that no WAN connection exceed 70 percent peak utilization. You examine the WAN connection between the Rome and Paris offices and discover that the utilization reaches 95 percent during Active Directory replication.
You need to reduce the WAN traffic associated with the Active Directory replication on the connection between the Rome and Paris offices. You need to ensure that users in the Rome office can log on to the domain if a WAN connection fails.
What should you do?
A.Decrease the replication interval on the site link connecting the Paris and Rome sites.
B.Remove the global catalog server from the Rome office.Enable universal group membership caching in the Rome site.

C.Enable slow link detection in the Default Domain Policy Group Policy object (GPO) in the rome. Certkiller .com
domain.
D.Configure a site link bridge between the site link that connects the Rome and Paris sites and the site link that connects
the Paris and Bonn sites.

Answer: B

Explanation: The Global Catalog (GC) contains a full replica of all Active Directory objects in its host domain plus a
partial replica of all directory objects in every domain in the forest. A GC contains information about all objects in all
domains in the forest, so finding information in the directory does not require unnecessary queries across domains. A
single query to the GC produces the information about where the object can be found. It provides information about
objects that are located in other domains in the forest.
Universal group membership caching allows a site that does not contain a global catalog server to be configured to
cache universal group memberships for users who log on to the domain controller in the site. This ability allows a domain
controller to process user logon requests without contacting a global catalog server when a global catalog server is
unavailable. The cache is refreshed periodically as determined in the replication schedule.

Explanation:
A:Reducing the replication interval will reduce the amount of data that must be replicated at a time.
C, D:Enabling slow link detection or configuring a site link bridge will not reduce that amount of data that must be
replicated at a time.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 5-25 to 5-35,5-59 to 5-68

QUESTION 101
You are a network administrator for Certkiller , which has five regional offices and 3,000 branch offices. Each
branch office contains 10 users. Branch offices are connected to the nearest regional office by a 56Kbps
WAN connection.
The network consists of a single Active Directory forest that contains one domain for each regional office.
All servers run Windows Server 2003. Each branch office contains one domain controller that is configured
as an additional domain controller in the regional domain for the branch office. The site link between each
branch office and the corresponding regional domain is configured to replicate every 30 minutes.
Users in the branch office report that applications respond slowly when they access resources in the
corresponding regional office. You monitor the WAN connection that connects several of the branch offices

and discover that utilization increases from 30 percent to more than 90 percent on a regular basis.
You need to improve the response time of applications when they access resources in the regional office.
You need to ensure that users can log on without using cached credentials if the WAN connection fails.
What should you do?
A.Remove Active Directory from the file and print server in each branch office.
On the site link between each branch office and the corresponding regional office, increase the replication interval.
A.Enable universal group membership caching in each branch office.Configure the site link between each branch office
and the corresponding regional office to be available only during off-peak hours.
B.Configure the domain controller in each branch office as a global catalog server.
C.On the site link between each branch office and the corresponding regional office, decrease the replication interval.

Answer: D

Explanation: Response times for that application are slow because replication traffic is too much. Decreasing the
replication schedule will reduce the amount of replication traffic by allowing amounts of changes to be replicated.
Incorrect Answers:
A:Increasing the replication interval will increase the amount of changes that must be replicated at a time. This might
increase replication traffic.
B:We don't want to use cached credentials.
C: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.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 5-7 to 5-8
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 449-452,
458,458-459

QUESTION 102
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains three Windows Server 2003 domain controllers named Server CK1 , Server CK2 and Server CK3 . Server CK1 holds the schema master role and the domain naming master role. Server CK2 holds the relative ID (RID) master role. Server CK3 holds the PDC emulator master role and the infrastructure master role.
Server CK2 fails and cannot be restarted. You log on to Server CK3 as the administrator and seize the RID master role.
Later, Server CK2 is repaired and can be brought back online. You want Server CK2 to hold the RID master role again.
What should you do?
A.Restart Server CK2 while it is connected to the network.
Use the Ntdsutil utility and seize the RID master role.
Reconnect Server CK2 to the network.
A.Restart Server CK2 while it is disconnected from the network.
Use the Ntdsutil and seize the RID master role.
Reconnect Server CK2 to the network.
A.Reinstall Windows Server 2003 on Server CK2 .
Restore the system state from the most recent backup to Server CK2 .
Reconnect Server CK2 to the network.
A.Reinstall Windows Server 2003 on Server CK2 .
Promote Server CK2 to become a domain controller.
Transfer the RID master role to Server CK2 .

Answer: D

Explanation: A domain controller whose RID master role has been seized can only be brought back online by reinstalling Windows Server 2003.
Incorrect Answers:
A:Server CK2 was the RID master before it failed. That role was seized to Server CK3 . If we restart Server CK2 , there
will be two RID masters. Furthermore, we can only seize a role if the domain controller that holds that role fails.
B:We cannot seize the RID master role if Server CK2 is not connected to the network. Furthermore, we can only seize
a role if the domain controller that holds that role fails.
C:Server CK2 was the RID master before it failed. That role was seized to Server CK3 . However, if we bring Server CK2 back online, there will be two RID masters.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 517522

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 4-28,4-29

QUESTION 103
You are a network administrator for Acme. Acme consists of two subsidiaries named Litware Inc., and Certkiller GmBh. 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 Certkiller .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 Certkiller .com domain tree from a threemonthold
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 thenetdomcommand on a domain controller in Certkiller .com.
B.Use the Ntdsutil utility on a domain controller in litwareinc.com.
C.Use the ADSIEdit utility on a domain controller in Certkiller .com.
D.Run theldpcommand on a domain controller in litwareince.com.

Answer: C, D

Explanation: We need to edit a property of Active Directory.We can use a low level editor, such asAdsiEdit and ldp,to
do this.AdsiEdit is aMicrosoft Management Console (MMC) snapin
that acts as a lowlevel
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 agraphical tool that allows users to perform Lightweight
Directory Access Protocol (LDAP) operations, such as connect, bind, search, modify, add, and delete, against any
LDAPcompatible
directory, such as Active Directory. LDAP is an Internetstandard
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 commandline
utility performs database maintenance and clean up. However, it does not allow you to
add, move, or delete objects.
Reference:
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q216/9/93.

QUESTION 104

You are the network administrator for Acme. Acme consists of two subsidiaries named Certkiller and Fabrikam, Inc. The network consists of a single Active Directory forest that contains three domains. The domain and site configuration is shown in the exhibit.
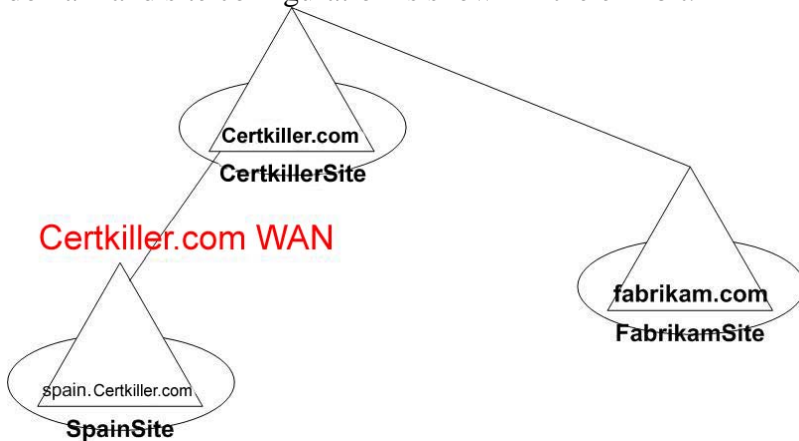
A computer named DC1.spain. Certkiller .com is a domain controller in the spain. Certkiller .com domain. DC1.spain. Certkiller .com is also a global catalog server and the preferred bridgehead server for SpainSite. The Active Directory database on DC1.spain. Certkiller .com contains 1 GB of data. The Spain departments in Certkiller are implementing an Active Directoryenabled
application. You expect size of the database on
DC1.spain. Certkiller .com to increase by 200 MB.
Active Directory stops responding on DC1.spain. Certkiller .com. You discover that the hard disk has less then 5 MB of space remaining.
You need to configure DC1.spain. Certkiller .com so that Active Directory can restart. You also need to configure the server so that additional space is available on the hard disk for the additional data that will be added to the Active Directory database.
What should you do?
A.Delete all log files that are located in the NTDS folder.
B.Install another hard disk in DC1.spain. Certkiller .com.
Use the Ntdsutil utility to move the database to the new hard disk.
A.Install another hard disk in DC1.spain. Certkiller .com.
Use the Ntdsutil utility to move the transaction logs to the new hard disk.
A.Configure another server in the site to operate as a preferred bridgehead server.
Configure DC1.spain. Certkiller .com so that it no longer operates as a preferred bridgehead server.

Answer: B

Explanation: Moving the Active Directory database to a new hard drive will ensure that there is adequate hard drive
space for the additional data that will be added to the Active Directory database. You can do this by using theNtdsutil

tool with thefilesswitch to move the Active Directory database to the new hard drive. TheNtdsutiltool provides management facilities for Active Directory. You can useNtdsutilto perform database maintenance of Active Directory,

manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.When used withy thefilesswitch,Ntdsutilprovides commands for managing the directory service database and log files.

To perform this operation you will need to restart the Domain Controller in Directory services restore mode. This

operation can not be performed in normal mode because the database and log are in use in normal mode.

Incorrect Answers:

A:Log files are important for recovery purposes. You should only delete the log files once a backup of the database has

been performed.Furthermore, the log files might no take up the required 250 MB that you must make provision for.

C:You could use theNtdsutiltool with thefilesswitch to move the log files to the new hard drive. The log files might no

take up the required 250 MB that you must make provision for. This is therefore not the best answer.

D:The location of the bridgehead server does not affect the size of the Active Directory database.

Reference:

David Watts & Will Willis, Windows Server 2003 Active Directory Infrastructure Exam Cram 2 (Exam 70294):Que

Publishing, Indianapolis, 2004, Chapter 10, Active Directory Maintenance.

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 707711

QUESTION 105

You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com.

The Active Directory database is contained on a Windows Server 2003 domain controller named Certkiller 1. The hard disk that contains the Active Directory database fails.

You restart Certkiller 1 in Directory Services Restore Mode. When prompted to log on, you type administrator@sales. Certkiller .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.Typesales\ administratoras your user name and enter your domain password.

B.Typeadministratoras your user name and enter the password that was associated with the local administrator account before you installed Active Directory.

C.Typeadministratoras your user name and enter your domain password.

D.Typeadministratoras your user name and enter the password that you supplied during the installation of Active

Directory.

Answer: D

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 suppliedduringthe 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:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 11, pp. 720,
731-741

QUESTION 106
You are the network administrator for Certkiller .com. 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
consists of a single Microsoft Exchange 2000 Server organization.
You need to create groups that can be used only to send email
messages to user accounts throughout
Certkiller . 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 email
groups for Certkiller .
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.
A.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.
A.Create universal distribution groups.
Make the appropriate users from each domain members of a universal distribution group.
A.Create universal security groups.
Make the appropriate users from each domain members of a universal security group.

Answer: A

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 in Universal groups as we want to reduce replication traffic.
D:We should not place user accounts directly in Universal groups as we want to reduce replication traffic. Furthermore,
we to use Distribution groups for email groups, not security groups.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, p. 8: 4
Schema classes and attributes, MS workshop 2209

QUESTION 107
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The domain contains Windows Server 2003 print servers and printer objects.
A group named PrinterSupport needs to be able to manage the printers and print queues in the domain. The
PrinterSupport group also needs to manage the printer objects in Active Directory. The PrinterSupport
group does not need to perform any other tasks.
You need to grant the PrinterSupport group only the permissions that it needs.
Which action or actions should you take? (Choose all that apply)
A.Make the PrinterSupport group a member of the Print Operators group on each print server.
B.Make the PrinterSupport group a member of the HelpServicesGroup on each print server.
C.Make the PrinterSupport group a member of the Power Users group on each print server.
D.Make the PrinterSupport group a member of the Server Operators group in the Builtin
container.
E.Make the PrinterSupport group a member of the Print Operators group in the Builtin

container.

Answer: E

Explanation: The builtin
Print Operators group is responsible formanaging only the printers and print queues in the
domain. We should thus add the PrinterSupport group to thePrint Operators group.
Incorrect Answers:
A:The PrinterSupport groupis responsible for
managing only the printers and print queues in the domain. Therefore they should be granted permissions at the
domain
level.
B:The HelpServicesGroup allows administrators to set rights common to all sup port
applications. By default, the
group has only one member, the account associated with Microsoft support applications, such as Microsoft
Remote
Assistance. Do not add users to this group, which is managed automatically by the Help And Support service.
C:Making thePrinterSupport group a member of the Power Users group would allow members of the
PrinterSupport
group full control of the entire domain.
D:The Server Operators group is responsible for managing all servers.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, pp. 8: 411
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/enus/
Default.asp?url=/resources/documentation/

QUESTION 108
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The functional level of the domain is Windows 2000 native. All servers run
Windows Server 2003.
Certkiller is adding 15 new servers to run a new application. Certkiller 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: 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
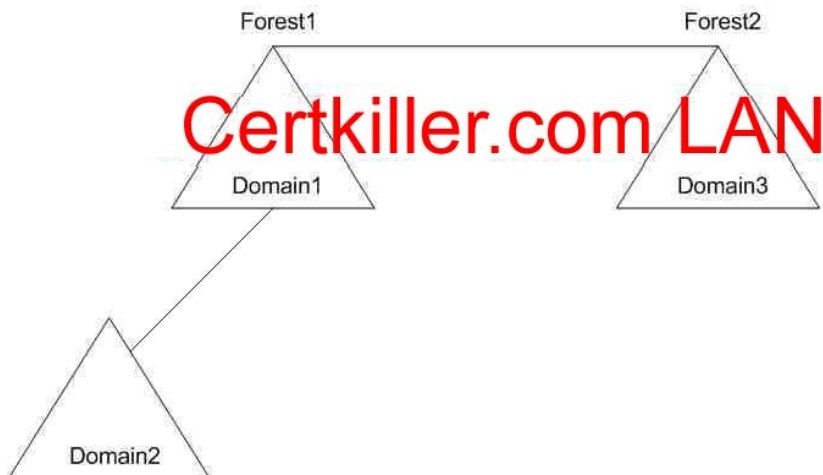Application OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-4 to 10-12,10-15 to 10-19,10-24 to 10-28.

QUESTION 109
You are the network administrator for Certkiller .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?
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 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 oneway
external trust relationship in which Domain2 trusts Domain3.

Answer: B
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:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 56-58, 402-406,407

QUESTION 110
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003.
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.
A.Grant the Server Access Team group permissions to modify computer objects in the Application OU.
B.Move the Server Access Team group object into the Application OU.
C.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

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-4 to 10-12,10-15 to 10-19,10-24 to 10-28

QUESTION 111
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
forest that contains three domains named Certkiller .com, child1. Certkiller .com, and child2. Certkiller .com. The
functional level of the forest is Windows 2003.
Both the child1. Certkiller .com domain and the child2. Certkiller .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 Certkiller .com domain.
Add both All_Accounting groups to the universal group.
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 domain local group in the Certkiller .com domain.
Add both All_Accounting groups to the domain local group.
A.Create a universal group in the Certkiller .com domain.

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

Answer: A

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 4-4 to 4-5
Walter Glenn, and Michael T. Simpson: MCSE Self
Windows Server 2003 Active Directory and Network Infrastructure, Microsoft Press, Redmond, Washington,
2004,
pp. 4-21 to 4-23,4-26 to 4-30
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 134-136

QUESTION 112
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
forest that contains five domains. The functional level of the forest is Windows 2000 native. You have not
configured any universal groups in the forest.
One domain is a child domain named usa. Certkiller .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
usa. Certkiller .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 theHKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailureskey to the registry on both domain controllers in Site1.
C.Add theHKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailureskey 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

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 nativemode domain,
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 nativemode
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\IgnoreGCFailureskey must be added to
the registry the both domain controllers in Site1, not the global catalog servers.

D:Raising thefunctional level of the forest to Windows Server 2003 won't solve the problem as Windows 2000 native
mode is sufficient.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-17 to 1-18,5-41 to 5-45,5-48 to 5-50
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 31, 543,
547,
550-552

QUESTION 113
You are a network administrator for Certkiller .com. Your network consists of a single Active Directory
domain named Certkiller .com. All servers run Windows Server 2003.
The company has users who work in the main office and users who work remotely by connecting to a server
running Routing and Remote Access. The company's written security policy requires that administrators in
the main office log on by using smart cards. The written security policy also requires that remote users use
smart cards to access network resources. No other users are required to use smart cards.
You issue portable computers that contain smart card readers to administrators and remote users. You issue
smart cards to administrators and remote users. Administrators and remote users report that they can log on
without using a smart card.
You need to ensure that only administrators are required to use smart cards when working in the main office.
You must also ensure that remote users are required to use smart cards when accessing network resources.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A.In the computer configuration settings of the Default Domain Policy Group Policy object (GPO), enable the
Interactive logon: Require smart cardsetting.
B.On the server running Routing and Remote Access, select theExtensible authentication protocol (EAP)check
box
and require smart card authentication.
C.In the properties of each administrator account, select theSmart Card Required for Interactive Logoncheck
box.
D.In the computer configuration settings of the Default Domain Controllers Policy Group Policy object (GPO),
enable
theInteractive logon: Requires smart cardsetting.
E.In the properties of each user account that requires remote access, select theSmart Card Required for
Interactive
Logoncheck box.

Answer: B, C

Explanation: We can require remote users to log on using smart cards only by configuring the RRAS server that

the
remote users connect to require smart card authentication.
We can configure the administrators' user accounts to require smart cards for interactive logons.This setting is defined in
the user properties in Active Directory Users and Computers.
Incorrect Answers:
A:This would require that all users log on using a smart card.
D:This would require that users use a smart card to log on to only the domain controllers. The administrators must use
smart cards to log on to any machine in the domain.
E:This would require that the remote users log on using a smart card to any machine. They don't need a smart card
logon if they are using a machine in the office.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 7-9 to 7-10.
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows Server 2003,
Sybex Inc. Alameda, 2003, p. 655

QUESTION 114
You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Most of the client computers are located in the offices of individual users. Some client computers are located in publicly accessible locations.
The company's written security policy includes the following requirements.
1.All users must use smart cards to log on to a client computer.
2.Users using the publicly accessible client computers must be logged off if the smart card is removed from the smart card reader.
You configure all user accounts to require smart cards for interactive logon. You create an organizational unit (OU) named Public.
You need to ensure that the appropriate result occurs on each client computer when a smart card is removed. You must achieve this goal without affecting other computers.
What should you do?
A.Place all computer accounts for the publicly accessible client computers in the Public OU.
Create a new Group Policy object (GPO) and link the GPO to the Public OU.
Configure theInteractive Logon: Smart card removal behaviorsetting toForce Logoff.
A.Place the user accounts of all users who use the publicly accessible client computers in the Public OU.
Create a new Group Policy object (GPO) and link the GPO to the Public OU.
Configure theInteractive logon: Smart card removal behaviorsetting toForce loggoff.
A.On the Default Domain Policy Group Policy object (GPO), configure the
Interactive logon: Smart card removal behaviorsetting toForce logoff.
B.On the Default Domain Controllers Policy Group Policy object (GPO), configure theInteractive logon: Smart card
removal behaviorsetting toForce Logoff.

Answer: A

Explanation:
public computers.The question states that users must be logged off if the smart card is removed from the smart card
reader.There is a specific setting in group policy for this.We can configure the Interactive Logon: Smart card removal
behaviour setting to Force Logoff.
Incorrect Answers:
B:This is a computer setting, not a user setting.
C:This will force logoff all users in the domain.Only users of the public computers should be logged off when they
remove their smart cards.
D:This will force logoff all users who log on to a domain controller.Only users of the public computers should be logged
off when they remove their smart cards.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-4 to 10-12,10-15 to 10-19,10-24 to 10-28

QUESTION 115
You are a network administrator for Certkiller . The network consists of a single Active Directory domain
named Certkiller .com. All servers run Windows Server 2003. Each client computer runs either Windows XP
Professional or Windows 2000 Professional.
The company requires that all users log on by using smart cards. You deploy Certificate Services and smart
card readers. You configure autoenrollment
to issue certificates to users. Users report that they cannot log
on by using a smart card.
You need to ensure that all users can log on by using a smart card.
What should you do?
A.In Active Directory Users and Computers, configure all user accounts to require a smart card for interactive
logon.
B.Configure the domain security policy to require smart cards for interactive logon.
C.Use the Certificate Services Web site to enroll each user for a smart card certificate.
D.Add a copy of the enterprise root certificate to the trusted root certification authorities store on each client
computer.

Answer: C

Explanation: Although the question says "you configure autoenrollment
to issue certificates to users", it doesn't say
what types of certificates were autoenrolled.
You can usethe Certificate Services Web site to enroll each user for a
smart card certificate.
The recommended method for enrolling users for smart cardbased

certificates and keys is through the Smart Card

Enrollment station that is integrated with Certificate Services in Windows 2000 Server and Windows 2000
Advanced

Server.

Incorrect answers:

A:This is not necessary. With this setting disabled, the users can log on using any method.

B:This is not necessary. With this setting disabled, the users can log on using any method.

D:In a single domain, the Certificate Authority would be trusted by the client computers in the domain.
Therefore, it is

not necessary to add a copy of the enterprise root certificate to the trusted root certification authorities store on
each

client computer.

Reference:

Martin Grasdal, Laura E. Hunter, Michael Cross, Laura Hunter, Debra Littlejohn Shinder, and Dr. Thomas W.
Shinder,

Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70293

Study Guide & DVD Training

System, Syngress Publishing, Inc., Rockland, MA, Chapter 12, p. 887

QUESTION 116

You are the administrator of the Certkiller company network.The network consists of a single Active
Directory domain named Certkiller .com.The network includes 20 servers running Windows Server 2003 and
400 client computers running Windows XP Professional.

A new written security policy specifies the following account polices:

1.User accounts must be automatically locked out in the event of three consecutive failed logon attempts
within a 30-minutes period.

2.Manual administrative action must be required to unlock a user account.

You configure a GPO linked to the domain with the following settings:

1.Account lockout threshold:3

2.Reset account lockout counter after 30 minutes.

You need to set the Account lockout duration so that manual administrative action must be required to
unlock a user account.

What setting should you use for the Account lockout duration?

A.2

B.3

C.99

D.999

E.0

F.31

Answer: E

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.
Incorrect Answers:
A:This will set the account lockout duration to 2 minutes.
B:This will set the account lockout duration to 3 minutes.
C:This will set the account lockout duration to 99 minutes
D:This will set the account lockout duration to 999 minutes
F:This will set the account lockout duration to 31 minutes
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290):Managing and Maintaining a
Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, Washington, 2004,p. 340

QUESTION 117
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003.
Certkiller 's written security policy requires the following account polices:
1.User accounts must be automatically locked out in the event of three consecutive failed logon attempts within a 30-minutes period.
2.Manual administrative action must be required to unlock a user account.
You need to configure the account polices 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:
The Account lockout duration security setting determines the number of minutes a locked-outaccount remains locked out before automaticallybecoming 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 thresholdsecurity 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 avalue 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 aftersecurity 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:
Dan Holme and Orin Thomas, MCSA/MCSE SelfPaced
Training Kit (Exam 70290):
Managing and Maintaining a
Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, Washington, 2004,p. 340
Microsoft Official Curriculum 1558, Advanced Administration of Microsoft Windows 2000 Module 7: Advanced
Administration of User Accounts and Groups, pp. 6-10.

QUESTION 118
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003. The domain contains Windows Server 2003 computers and Windows XP Professional computers. The domain consists of the containers shown in the exhibit.

All production server computer accounts are located in an organizational unit (OU) named Servers. All production client computer accounts are located in an OU named Desktops. There are Group Policy objects (GPOs) linked to the domain, to the Servers OU, and to the Desktop OU.
The company recently added new requirements to its written security policy. Some of the new requirements apply to all of the computers in the domain, some requirements apply to only servers, and some requirements apply to only client computers. You intend to implement the new requirements by making modifications to the existing GPOs.
You configure 10 new Windows XP Professional computers and 5 new Windows Server 2003 computers in order to test the deployment of settings that comply with the new security requirements by using GPOs. You use the Group Policy Management Console (GPMC) to duplicate the existing GPOs for use in testing.
You need to decide where to place the test computer accounts in the domain. You want to minimize the amount of administrative effort required to conduct the test while minimizing the impact of the test on production computers. You also want to avoid linking GPOs to multiple containers.
What should you do?
A.Place all test computer accounts in the Certkiller .com container.
B.Place all test computer accounts in the Computers container.

C.Place the test client computer accounts in the Desktops OU and the test server computer accounts in the Servers
OU.
D.Create a child OU under the Desktops OU for the test client computer accounts.
Create a child OU under the Servers OU for the test server computer accounts.
A.Create a new OU named Test under the Certkiller .com container.
Create a child OU under the Test OU to test client computer accounts.
Create a second child OU under the Test OU to test server computer accounts.

Answer: E

Explanation: To minimize the impact of the test on production computers, we can create a test OU with child OUs for
the servers and the client computer accounts. Settings that should apply to the servers and client computers can be
applied to the Test OU, and settings that should apply to the servers or the client computers can be applied to the
appropriate child OUs.
Incorrect Answers:
A:You cannot place computer accounts directly under the domain container. They must be in an OU or in a built in
container such as the Computers container.
B:We need to separate the servers and the client computers into different OUs.
C:This solution would apply the new settings to existing production computers.
D:This could work but you would have more group policy links. For example, the GPO settings that need to apply to
the servers and the client computers would need to be linked to both OUs. It would easier to link the GPO to a single
parent OU.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 5, p.
408

QUESTION 119
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The company contains several departments. One of these departments is sales.
A group named Sales Admin 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 Certkiller 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.
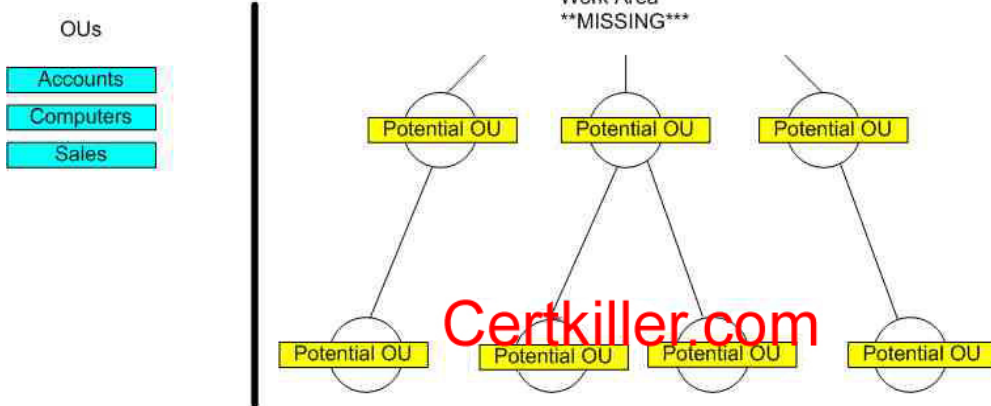
Answer:

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23
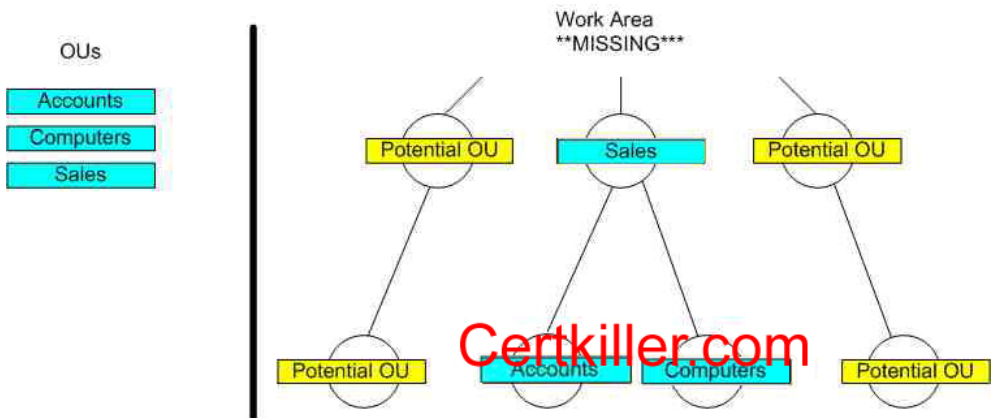

QUESTION 120
You are a member of the Enterprise Admins group in Certkiller 's Windows 2003 network. The network consists of a single domain named Certkiller .com. The Bonn office has its own organizational unit (OU) named Bonn.
You hire an employee named Sophie as a LAN administrator for the Bonn office. Sophie needs to create child OUs for the Bonn OU. She also needs to verify the existence of the OUs she creates. You need to grant Sophie the minimum permissions on the Bonn OU so that she can accomplish these tasks.

Which permissions should you grant?
A.Read All Properties, Create Organizational Unit Object, Write All Properties.
B.Read All Properties, List Contents, Create Organizational Unit Objects.
C.List Contents, Create All Child Objects.
D.Write All Properties, All Extended Rights.

Answer: B.

Explanation: The minimum permission required to create OUs in the Create Organizational Unit Objects permission.To
verify the OUs, she needs the Read and List permissions.
Incorrect Answers:
A:The write permission will allow a user to create or modify any object in the OU.
C:The Create All Child Objects will allow a use to create any object in the OU.
D:The write permission will allow a user to create or modify any object in the OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 9-18 to 9-20,9-23 to 9-26

QUESTION 121
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. All servers run Windows Server 2003. Each department in Certkiller has an
organizational unit OU for all its resources and accounts.
Certkiller 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 now 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

Work Area

GPO creation team

Support staff

Make users members of Group Policy Creator Owners.

Drag action here

Drag action here

Assign the **Allow - Read** and the **Allow Write** permissions to the **gPlink** property of the departmental Ous.

Drag action here

Drag action here

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

Certkiller.com

Answer:

Explanation:

Possible Actions

Work Area

GPO creation team

Support staff

Make users members of Group Policy Creator Owners.

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 **gPlink** property of the departmental Ous.

Drag action here

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

Certkiller.com

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

The GPO creation team must link the GPO to any departmental OU. The desktop support staff must be able use the
GPO but are not allowed to create any GPOs themselves. Thus, the GPO creation team must be members of the Group
Policy Cerator Owners group, and the desktop support staff must haveAllow - ReadandAllow -

Writepermissions
to thegPLinkandgPOptionsattributes of the departmental OUs.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-40 to 10-41

QUESTION 122
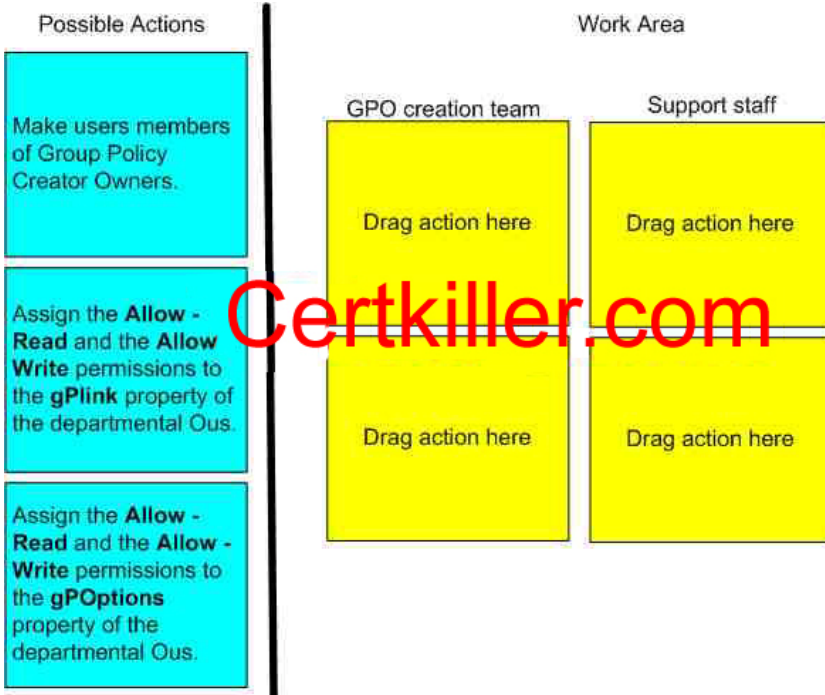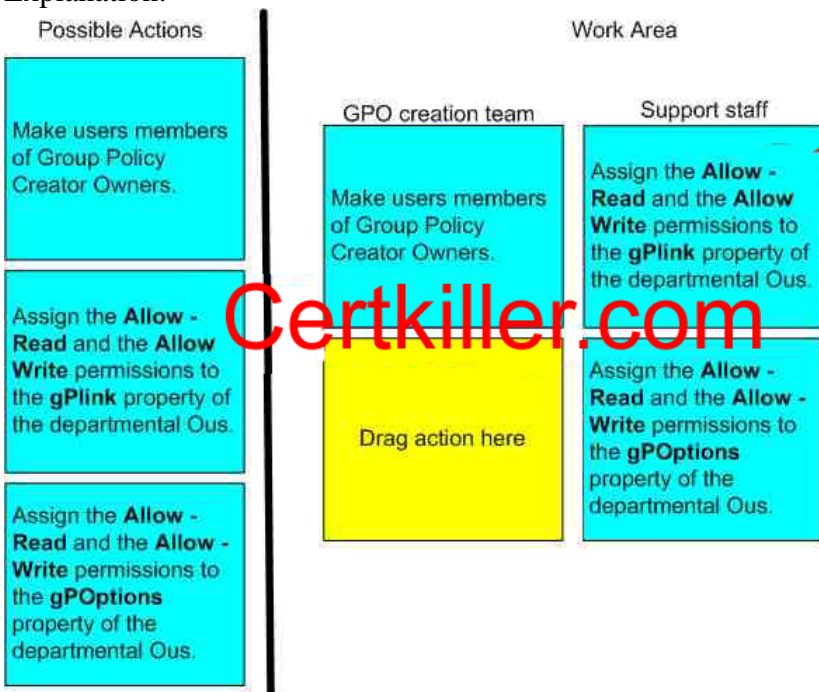You are the network administrator for Certkiller .com. Certkiller has one main office and 11 branch offices.
The network consists of a single Active Directory domain named Certkiller .com. The domain contains an
organizational unit (OU) named BranchOffices. The BranchOffices OU contains an OU for each 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.
Certkiller 's written security policy states the following requirements:
1.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.
2.Members of the BranchOffice Admins group must not be able to block the inheritance of GPOs at the
individual branch office OUs.
3.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.
A.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.
A.In the Group Policy Management Console (GPMC), remove the BranchOffice Admins group from
thePermissions
tab for the BranchOffices OU.
Add the BranchOffice Admins group to the LinkGPOs permission in theDelegationtab for the BranchOffices
OU.
Configure the permissions to apply the BranchOffice Admins container only.
A.In the Group Policy Management Console (GPMC), remove the BranchOffice Admins group from
thePermissions
tab for the BranchOffices OU.
Add the BranchOffice Admins group to the LinkGPOs permission in theDelegationtab for the BranchOffices
OU.
Configure the permissions to apply the BranchOffice Admins container and all child containers.

Answer: A

Explanation: We need to restrict the administrative abilities of the BranchOffice Admins group at the Branch level. The
gPOptionsattribute 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 thegPOptionsattribute.
C, D:TheBranchOffice Admins group must be able to administrate at the branch level. We should not remove them
from theDelegationtab for the BranchOffices OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-16 to 10-20,10-40 to 10-41

QUESTION 123
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. User and group objects for the sales department are located in an
organizational unit (OU) named Sales.
Peter and Mary are administrators for Certkiller . 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

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 Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 9-18 to 9-20,9-23 to 9-26

QUESTION 124

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The relevant portion of the organizational unit (OU) structure is shown in the exhibit.

Certkiller '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.

Certkiller 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?

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.

A.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.

A.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.

A.On the Sales OU, block the inheritance of permissions.

Copy all existing permissions.

On the Sales OU, grant junior managers the permissions to enable and disable accounts.

Answer: A

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:Youwant 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.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 9-18 to 9-20,9-23 to 9-26

QUESTION 125
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com.
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 global group and members of the Executive global group. The help desk employees must not have any other administrative rights in the domain.
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.
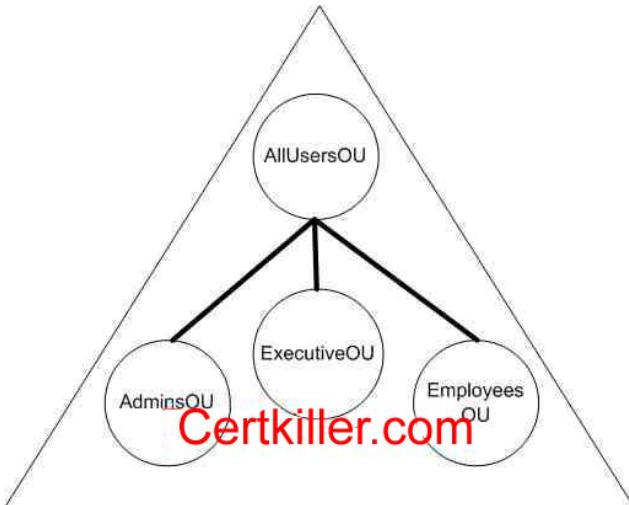
You need to configure the permissions for the help desk employees as defined by the written domain administration policy.

What should you do?

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

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 AllUsersOU 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:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 56-58,

402-406,407

QUESTION 126

You are the network administrator for Certkiller .com. The network consists of a single Active Directory

forest that contains three domains named Certkiller .com, usa. Certkiller .com, and europe. Certkiller .com. The functional level of the forest is Windows Server 2003.

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 Certkiller .com domain. All user accounts for the help desk department users are members of the HD_Users group.
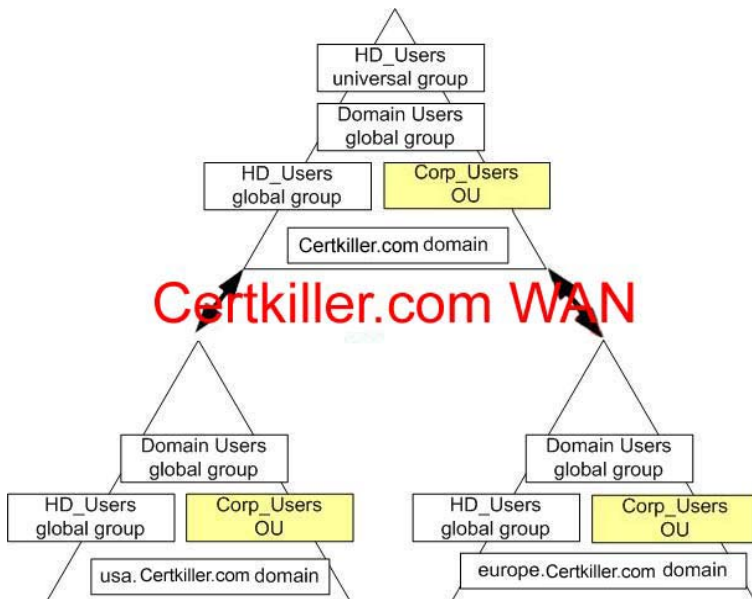
You need to delegate the required authority for resetting passwords to the users in the help desk department.

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

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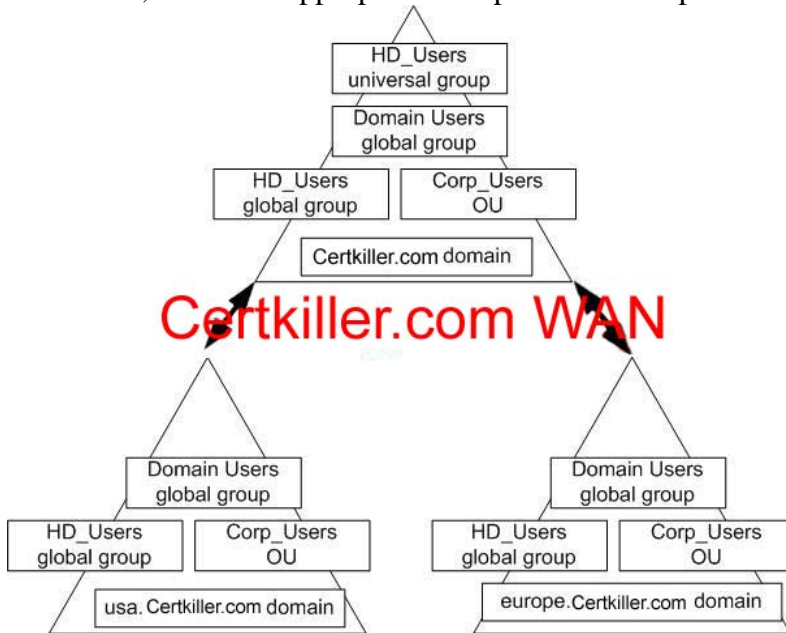
Answer:

Explanation:
We need to delegate the required authority for resetting passwords for the Corp_Users OU 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:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 408411
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 127
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .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 nonMicrosoft
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 Certkiller .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.
A.Create a new domain under the Certkiller .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.
A.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.
A.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

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 thelocaluser 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 thelocaluser accounts.The local user accounts
are not objects in Active Directory and so cannot be moved to an OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 6-3 to 6-9,10-20

QUESTION 128
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The domain contains 2,250 user accounts. Each user account has the
appropriate permissions for resource access. All user accounts are in the Users container.
Certkiller has five departments. To support Certkiller 's structure, you must place the existing user accounts
in organizational units (OUs) arranged by department.
You create five OUs in the domain, with one OU for each department. The human resources manager sends
you a file in the commaseparated
value (CSV) file format. The CSV file lists each user's full name, account
logon name, and department. You expect to receive CSV files containing new and updated information every
two weeks.
You need to place the user accounts in the correct OUs. You must not make changes that require the
permissions on resources to be changed. You must deploy the changes in the minimum amount of time and
by changing the minimum amount of administrative effort.
What should you do?
A.Create a script that reads the CSV file and uses ADSI to move user accounts to the correct OUs.
B.Create a script that reads the CSV file and updates the Department attribute of each user account to the name
of the
correct OU.
C.Create a security group for each department.
Move the security group objects to the correct OUs.
Make each user account a member of the security group for the user's department.
A.In Active Directory Users and Computers, create a new user account for each user in the correct OU, then
delete the
corresponding user object in the Users container.
B.In Active Directory Users and Computers, select all of the user accounts from one department and move them
to the
correct OU.
Repeat this process for each of the other departments.

Answer: A

Explanation: Creating a script to automate the updates and moves is the easiest way to handle the administrative
tasks
on an ongoing basis.
Incorrect Answers:
B:The department attribute is an information attribute. It doesn't represent the OU. Thus ensuring that the
department
attribute is correct won't more the accounts to the appropriate OU.
C, D, E:This could work but would require much more administrative effort.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 3-12,7-17
Michael Cross, Jeffery
A. Martin, Todd

QUESTION 129
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
forest that contains a single domain named Certkiller .com. Organizational units (OUs) in the domain are
configured as shown in the Domain Structure exhibit.
The exhibit shows the following OU structure:
-IT Users OU-
------Service Desk Staff OU.
------Domain Admins OU.
All client computers run Windows XP Professional. All client computer accounts are located in the Certkiller
Computers OU.
Your user account is a member of the Domain Admins security group. All user accounts that are members of
the Domain Admins security group are located in the Domain Admins OU.
All service desk users have user accounts that are members of the SrvDeskGrp security group. All accounts
that are members of this group are located in the Service Desk Staff OU.
You use the Group Policy Management Console (GPMC) to create a Group Policy object (GPO) named
Install Admin Tools. You configure the GPO as follows:
1.In the GPO, create a software installation package that assigns the Windows Server 2003 Administration
Tools Pack (adminpak.msi) to users.
2.Link the GPO to the IT Users OU.
3.Remove the Authenticated Users builtin
group from the list of users and groups that were delegated
permissions for the GPO.
4.Assign the SrvDeskGrp security the Allow Read
permission for GPO.
Service desk users report that the administrative tools needed for their job are not installed. You use the
GPMC to examine the history of Group Policy application for one of the affected users. The relevant results
are shown in the GPMC exhibit.
MISSING
You also discover that when you log on to a computer normally used by a service desk user, the
administrative tools are automatically available for you.
You need to ensure that administrative tools can also be installed by Group Policy for all users with accounts
in the IT Users OU, without increasing the administrative privileges of any users.
What should you do?
A.Link the Install Admin Tools GPO to the Service Desk Staff OU.
Move the computer accounts for computers used by service desk users to the Service Desk Staff OU.
A.Change the security filtering on the Install Admin Tools GPO to grant the SrvDeskGrp security group the
ability to
apply the GPO.
B.Move the SrvDeskGrp security group to the Domain Admins OU.
C.Modify the GPO to assign the Administration Tools Pack to computers instead of to users.

Answer: B

Explanation: You need to assign theAllow Apply
Group Policypermission, not just theAllow Readpermission,
to theSrvDeskGrp group.
Incorrect Answers:
A:Linking theInstall Admin Tools GPO to the Service Desk Staff OU on its own won't help. The SrvDeskGrp would
still only haveAllow Readpermissions.
C:Making the SrvDeskGrp a member of theDomain Admins OU would give them too much permissions.
D:The GPO should apply to users not computers because we are controlling application based on user groups.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 130
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory
domain named Certkiller .com. Three security groups named Accounts, Processors, and Management are
located in an organizational unit (OU) named Accounting. All of the user accounts that belong 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:
1.You need to ensure that the GPO applies to all user accounts that are members of the Processors group.
2.You need to prevent the GPO from applying to any user account that is a member of the Accountants
group.
3.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 theDeny Readand
theDeny Apply
Group Policypermissions.
Modify the DACL of the GPO to assign the users who are in both the Accountants and Management security
groups
theAllow Readand
theAllow Apply
Group Policypermissions.
A.Modify the discretionary access control list (DACL) settings of the GPO to assign the Accountants and
Management
security groups theDeny Readand
theDeny Apply
Group Policypermissions.

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 theAllow Readand
theAllow Apply Group Policypermissions.
A.Modify the discretionary access control list (DACL) settings of the GPO to assign the Accountants security group the
Deny Readand theDeny Apply Group Policypermissions.
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 theAllow Readand
theAllow Apply Group Policypermissions.
A.Modify the discretionary access control list (DACL) settings of the GPO to assign the Accountants security group the
Deny Readand theAllow Apply Group Policypermissions.
Modify the DACL settings of the GPO to assign the Management security group theDeny Readand
theDeny Apply Group Policypermissions.

Answer: C

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 thediscretionary access control list (DACL) settings of the GPO to assign the
Accountants security group theDeny- Readand theDeny- Apply Group Policypermissions.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 modifyingthe DACL settings of the GPO to add the Processors group and assign theAllow Readand
theAllow Apply Group Policypermissions.
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 theAllow- ReadandtheAllow- Apply Group
Policypermissions.
Incorrect Answers:
A, B, D:Assigning theManagement security groups theDeny Readand
theDeny Apply
Group Policypermissions
will prevent the members that are members of both the Management and Processors group from receiving the
GPO.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf

QUESTION 131

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All user accounts for the research and development department are located in an organizational unit (OU) named PBUsers.
A Group Policy object (GPO) named UserRights is linked to the domain. The following user settings are enabled in the UserRights GPO:
1.Prohibit user configuration of offline files.
2.Remove Add or Remove Programs.
3.Remove Display in Control Panel.
You need to allow all users in the PBUsers OU to remove programs by using Add or Remove Programs in Control Panel. The other policy settings must continue to apply.
What should you do?
A.Enable theBlock Policy Inheritancesetting on the PBUsers OU.
B.Create a new GPO that disables theRemove Add or Remove Programssetting. Link the GPO to the PBUsers OU.
C.Assign the user accounts in the PBUsers OU theDeny Apply
Group Policypermission for the UserRights GPO.
D.Assign the user accounts in the PBUsers OU theDeny Write
GPlinkpermission for the PBUsers OU.

Answer: B

Explanation: A GPO linked to an OU will override the settings from a GPO linked to the domain.Therefore, we can
create a GPO thedisables theRemove Add or Remove Programssetting and link it to the PBUsers OU.
Incorrect Answers:
A:The question states that the other settings from the domain GPO must apply.Therefore, we cannot block policy
inheritance.
C:The question states that the other settings from the domain GPO must apply.Denying the users the Apply Group
Policy permission will prevent the settings from the domain GPO from being applied.
D:This setting has no effect on the application of the GPOs.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-23 to 10-24

QUESTION 132

You are the network administrator for Certkiller .com. The network consists of a Single Active Directory domain named Certkiller .com 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.

A.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.

A.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.

A.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: 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 theAllow Read
and Apply Group Policypermissions 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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 133

You are a network administrator for Certkiller .com. 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. Certkiller .com domain. All other user accounts and resources are in the Certkiller .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. Certkiller .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.
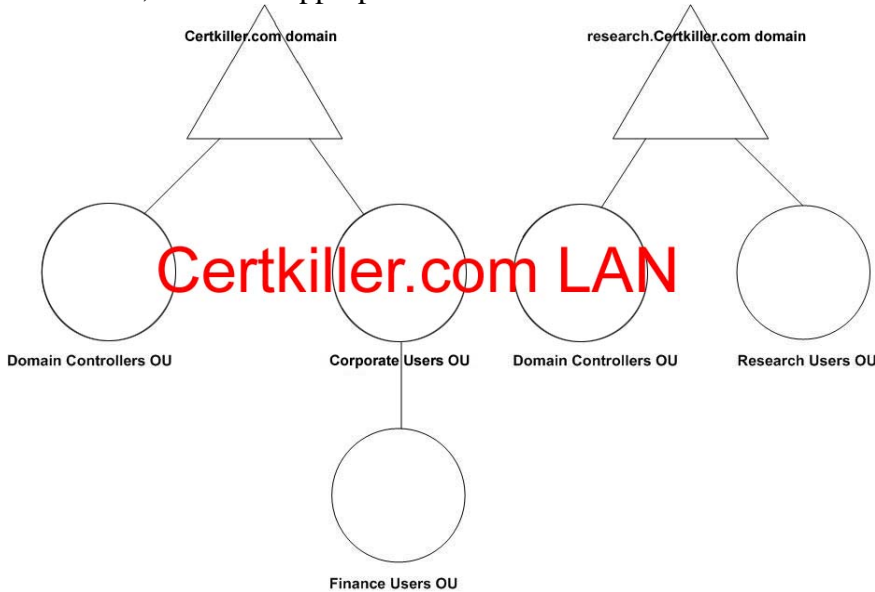
Answer:
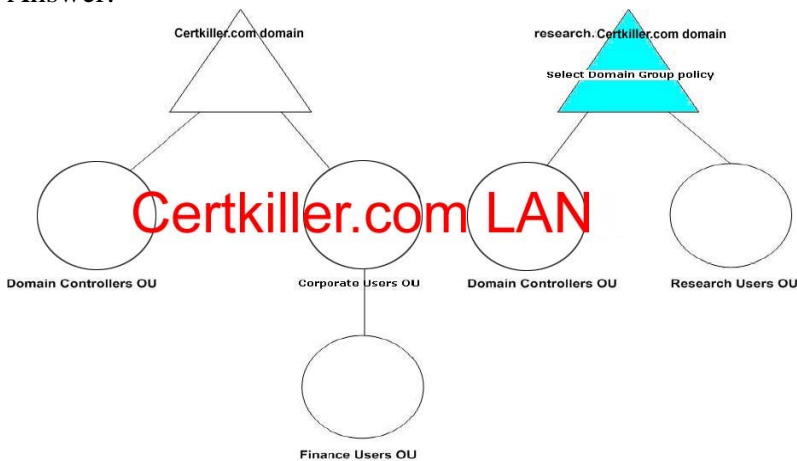
Explanation:

Select the research. Certkiller .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. Certkiller .com contains only research users so

applying the policy at the domain level will not affect any other others.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-31 to 10-44

QUESTION 134
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .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.
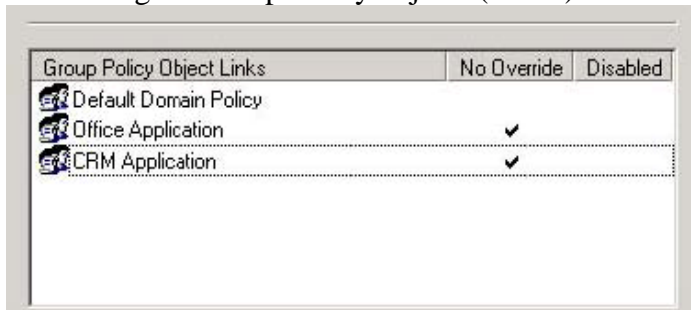
The Office Applications GPO has only the Microsoft Office applications listed as allowed applications. The
CRM Application GPO has only the CRM application listed as an allowed application. The CRM
Application GPO has security settings so that it applies only to members of the CRM Users security group.
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:
1.All users must be able to run the Microsoft Office applications.
2.Members of the CRM Users security group must be able to run the CRM application.
3.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)
A.Configure the Default Domain Policy GPO so that the CRM application is published to the members of the
CPM
Users security group.
B.Disable theNo Overridesetting for the CRM Application GPO. Leave the CRM Application GPO linked to
the
domain.
C.Reorder the GPOs so that the CRM Application GPO is higher in the list than the Office Application 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 theBlock Policy inheritancesetting 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: C, E

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 theNo Overridesetting 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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-20 to 10-21,11-6,12-3 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 135
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. You are testing Group Policy objects (GPOs) on an organizational unit (OU) named Test. The Test OU contains a Windows XP Professional client computer that you use as a test computer.
The domain contains a group named Security. You create a new GPO and configure the Computer Configuration section to grant the Security group the Change the system time user right.
You log on to the test computer and discover that the setting you set through the GPO is not in effect.
You need to apply the GPO settings immediately.
What should you do?
A.Log off the test computer and log on again.
B.Log off the test computer.
Create a test user account in the Test OU and then log on as the test user account.
A.On the test computer, run thegpresultcommand.

B.On the test computer, run thegpupdate /forcecommand.

Answer: D

Explanation: GPOs are applied when users log on and when the computer is booted up. GPOs are set to reapply refreshed at a given interval. However, you can use thegpupdate /forcecommandto apply the GPO immediately with
out having to reboot the computer.
Incorrect Answers:
A, B:The computer configuration settings are applied when the computer boots, not at log on.
C:The Gpresult commandline
tool allows you to create and display an RSoP query, which can be used to analyze the
cumulative effects of GPOs, through the command line. It also provides general information about the operating system,
user, and computer.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-15 to 10-17,10-44,1-14,1-16,11-19 to 11-22
www.microsoft.com/technet/treeview/default.asp?url=/ technet/prodtechnol/winxppro/proddocs/refrGP.asp

---

QUESTION 136
You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All file servers have computer accounts in an organizational unit (OU) named CompanyServers. All users have user accounts in an OU named CompanyUsers.
For all users and administrators, the My Documents folder is redirected to a shared folder on a file server named Certkiller 1.
The company wants to limit the amount of disk space that can be used by each user. Each user must be allowed to use a maximum of 2 GB of storage on Certkiller 1.
You need to limit disk space usage on Certkiller 1 to 2 GB per user. Administrators must not have these limits.
What should you do?
A.Create a Group Policy object (GPO) linked to the CompanyUsers OU. In the GPO, enable disk quotas.
B.Create a Group Policy object (GPO) linked to the CompanyUsers OU. In the GPO, enable a size limit on user profiles
C.Create a Group Policy object (GPO) linked to the CompanyServers OU. In the GPO, enable disk quotas.
D.Create a Group Policy object (GPO) linked to the CompanyServers OU. In the GPO, enable a default cache size for
offline files.

Answer: B

Explanation: To prevent users, computers, and groups from creating an unlimited number of objects in Active Directory, Windows Server 2003 has added quotas. Active Directory quotas are used to limit how many objects are

owned in a particular directory partition. While quotas can be applied to almost every user, computer, and group,
Domain Administrators and Enterprise Administrators are exempted from these limits. The quotas that are used to limit
the ability of a user, computer, or group from creating too many objects in Active Directory should not be confused with
disk quotas, which are also available on Windows Server 2003 servers (regardless of the functionality level being used).
The new Active Directory quotas (not to be confused with disk quotas) are defined as the number of objects that can
be owned by a given user in a given directory partition. Domain Admins and Enterprise Administrators are exempt from
only the original operations do. Quota administration is performed through a set of commandline tools, including dsadd,
dsmod, dsget, and dsquery. No graphical interface exists for quota administration.
Disk quotas can be used to limit the amount of hard disk space that can be used on a volume that's formatted in NTFS.
The NTFS file system is more advanced than other file systems such as FAT or FAT32, which can also be used to
format volumes. By using disk quotas on an NTFS volume, administrators can prevent users from filling up the hard disk
with an unlimited number of files.
Incorrect answers:
A:Making use of disk quotas will not have the desired effect.
C:The CompanyServers OU is the wrong organizational unit to link the GPO to.
D:First, this is the wrong to link the newly created GPO to this particular organizational unit and furthermore, the GPO
should not be one of enabling a default cache size for offline files.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 1, p. 69 &
Chapter 4, p. 250

QUESTION 137
You are a network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
You use a Group Policy object (GPO) to change the default storage location of the My Documents folder for all user accounts. The GPO redirects the My Documents folder to
\\SERVER1\USERFILES\%USERNAME%. The Redirect the folder back to the local user profile location when policy is removed option is selected. The network does not use roaming user profiles.
The My Documents folders of several users are very large and consume too much disk space on Server1.

As a result, users report slow response times for shared files.
You need to ensure that the My Documents folder for each user is stored and maintained on the user's client computer. You must not affect any other policies.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)
A.Change the redirection setting in the GPO toNot configured.
Run thegpupdatecommand on Server1.
A.Change the redirection setting in the GPO toNot Configured.
Include anxcopycommand in each user's logon script to move the files.
A.Copy all settings in the GPO except the redirection setting to a new GPO.
Delete the existing GPO.
A.In the GPO, change the specified path to %USERPROFILE%\My Documents.
B.Configure all shared folders on Server1 to automatically make all files available offline.
After the files are cached on the client computer, delete the files from the server.

Answer: A, D

Explanation: There is no roaming profile so we can remove the redirection setting. The gpupdate will ensure that the
altered GPO is applied immediately.
Incorrect Answers:
B:The xcopy command will copy the files from Server1 to the local computer. This will consume network bandwidth. It
is thus not the best answer.
C:We don't need to create a new GPO, just change the one setting.
E:The files will still be stored on Server1 but will be available for use on the local computer when the computer is
disconnected from the network. This won't ensure that the files are stored on the local computer.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 11-28 to 11-48

QUESTION 138
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. 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 Certkiller expands, user accounts for users other than support staff might be created in OUs other than the UserAccounts OU.
A written Certkiller policy states that all users, including support staff, must comply with the following rules:
1.Users are not allowed to use offline files.
2.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 Certkiller 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.

Answer:

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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-40 to 10-41

QUESTION 139
You are the network administrator for Certkiller that has a main office and many small branch offices.
Certkiller 's network consists of a single Active Directory domain named Certkiller .com. 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 Certkiller 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
accounts
into the new OU.
Block GPOs from applying to the new OU.
A.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.
A.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.
A.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 accounts does not
apply to
the new GPO.

Answer: D

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'sUserAccounts OU which contains all user accounts for the branch. We can
ensure that
this GPO doesn't apply to the administrator by assigning theDeny Apply
Group policyto the administrator account in
each branch.
Incorrect Answers:
A, C:The GPO must be linked to the users not the computers.
B:Simplyassigning theDeny Apply

Group policyto the administrator account will ensure that the administrator can't
have the GPO settings.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-40 to 10-41

QUESTION 140
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The domain contains one domain controller. All servers run Windows Server
2003. All client computers run Windows XP Professional. Certkiller 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 Certkiller .com.
In the Certkiller .com folder, create a folder named Policies.
A.In the SYSVOL folder, create a folder named System State.
In the System State folder, create a folder named Policies.
A.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.
A.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.
A.Use Active Directory Users and Computers to open each GPO.
Close each GPO without changing any settings.
A.Use Active Directory Users and Computers to open each GPO.
Change at least one setting in each GPO before closing it.

Answer: A, D, F

Explanation: A globally unique identifier (GUID) is a 128bit
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

the other computers 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 Certkiller .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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 1: 32, 3: 52

QUESTION 141

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. The organizational unit (OU) structure is shown in the exhibit.

The File Servers OU subtree contains 20 file and print servers. All of Certkiller 's user accounts are in the User Accounts OU subtree. Certkiller uses Group Policy objects (GPOs) linked to the 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 Certkiller .com. Certkiller 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?

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

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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-16 to 10-20, 10-23,10-36

QUESTION 142

You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.

Certkiller operates a call center in which 200 users use Windows XP Professional computers to access email,

Certkiller 's intranet, and a database application.All client computers are configured identically. The call center users do not use computers outside of the call center.

A written Certkiller policy states that call center users are not allowed to install or run additional applications

or to change the desktop settings on their computers.
You need to prevent call center users from changing the configuration of the call center computers. Your
solution must not restrict users in other parts of Certkiller from making changes to computers outside the
call center.
What should you do?
A.Place all of the computer accounts for call center computers in an organizational unit (OU) named Call
Center
Computers.
Create a Group Policy object (GPO) that includes the appropriate restrictions in the User Configuration section.
Link the GPO to the Call Center Computers OU.
A.Place all of the user accounts for call center users in an organizational unit (OU) named Call Center Users.
Create a Group Policy object (GPO) that includes the appropriate restrictions in the User Configuration section.
Link the GPO to the Call Center Users OU.
A.Place all of the user accounts for call center users in a security group named Call Center Users.
Change the default user rights assignment on the call center computers so that the Call Center Users group has
only the
Allow log on locallyright.
A.Place all of the user accounts for call center users in a security group named Call Center Users.
Configure these accounts so that all users use a common roaming profile stored on a file server.
Assigns the Call Center Users group theAllow Full
Controlpermission for the roaming profile folder.

Answer: B

Explanation: To restrict call center users from running certain applications and changing their desktops, we
need to
configure the required restrictions in a GPO and have it applied to all call center users. This can be achieved by
placing
all call center users in an OU and applying the GPO to that OU.
Incorrect Answers:
A:The GPO should apply to the users, not the computers.
C:achieved simply by restricting them to the local computer.
D:A roaming profile will not prevent users from running unauthorized applications. Furthermore,
grantingAllow Full
Controlpermission for the roaming profile folderwould allow them to change their desktop settings.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-16 to 10-20,10-40 to 10-41

QUESTION 143
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. All servers run Windows Server 2003.
The company decides to make five Windows XP Professional computers available in a public area for use by
visitors. These computers are to be used only for browsing public Web sites, A Web browser is the only
application that will be run on these computers.

You make these computers members of the Active Directory domain. You create a new organizational unit (OU) named Restricted Computers and place the five computer accounts in this OU. You configure these computers to automatically log on a user named Restricted User each time the computer is started. The Restricted User account does not have administrative rights on the computer or on the domain.
You need to configure the five computers so that they can access public Web sites but cannot run other applications. The restrictions must not affect other users or computers on the network.
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) and link it to the domain.
Configure the user settings in the GPO to allow only Internet Explorer to run.
Configure the computer settings in the GPO to enable loopback mode.
A.Create a Group Policy object (GPO) and link it to the Restricted Computers OU.
Configure the user settings in the GPO to allow only Internet Explorer to run.
Configure the GPO to apply only to the Restricted User account.
A.Create a Group Policy object (GPO) and link it to the Restricted Computers OU.
Configure the GPO to contain a Restricted Groups policy that places all users in the local Guests group of each of the
five Windows XP Professional computers.
A.Create a Group Policy object (GPO) and link it to the domain.
Configure the user settings in the GPO to allow only Internet Explorer to run.
Configure the GPO to apply only to the Restricted User account.
A.Create a Group Policy object (GPO) and link to the Restricted Computer OU.
Configure the user settings in the GPO to allow only Internet Explorer to run.
Configure the computer settings in the GPO to enable loopback mode.

Answer: D, E

Explanation: The computers are configured to automatically log on the Restricted User account each time the computers start.We can configure a GPO toallow only Internet Explorer to run.We can link the GPO to the domain and
use security permissions to ensure that the policy applies only to the Restricted User account.This will ensure that the
GPO only affects the restricted computers.
The restricted computers are in the Restricted Computers OU.Therefore, another solution would be to link the GPO to
the Restricted Computers OU, thus ensuring that no other computers are affected by the GPO.Although the Internet
Explorer settings are in the user part of a GPO, and this solution applies the GPO to computers (not users), we can
apply the user settings to the Restricted User account by using loopback mode.
For loopback processing, you can choose whether to replace or merge userspecific
policy. The replace mode replaces
all of a user's normal policy settings with those defined in the user configuration of the GPOs that apply to the computer
object (the loopback settings). Merge mode merges the user's normal policy settings and the loopback settings. In the

case where a policy item in the user's normal policy conflicts with the loopback settings, the loopback settings are
applied.
Incorrect Answers:
A:If we apply the GPO to the domain and use loopback mode, the settings will apply to all the computers in the domain. We should restrict the GPO to only the Restricted Computers.
B:We would need to use loopback mode to apply the GPO to the Restricted Users. This ensures that users receive
their policy regardless of the machine they use to log in.
C:The computers are configured to log on the Restricted Users account, not the guest account. In Windows Server
2003, the guest account is disabled by default.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows Server 2003,
Sybex Inc. Alameda, 2003,p. 784

QUESTION 144
You are a network administrator for Certkiller that operates a call center. The network consists of a single Active Directory domain named Certkiller .com. 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.

Work Area	
Allow Cross-Forest User Policy and Roaming User Profiles	Disabled
Group Policy slow link detection	Enabled
Turn off Resultant Set of Policy logging	Disabled
Remove users ability to invoke machine policy refresh	Enabled
Disallow Interactive Users from generating Resultant Set of Policy...	Enabled
Registry policy processing	Disabled
Internet Explorer Maintenance policy processing	Disabled
Software Installation policy processing	Disabled
Folder Redirection policy processing	Disabled
Scripts policy processing	Disabled
Security policy processing	Disabled
IP Security policy processing	Disabled
Wireless policy processing	Disabled
EFS recovery policy processing	Disabled
Disk Quota policy processing	Disabled
Always use local ADM files for Group Policy Object Editor	Enabled

Answer:

Explanation: Select "Registry policy processing: Disabled"
The Call Center computers OU have a GPO linked to it that will ensure that any user logging on to these computers will
receive a restricted desktop. Access control entries are set in the registry. However, if managers are to perform managerial tasks then they do not need to be hampered with a restricted desktop if you enable the registry policy
processing setting.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 2: 49

QUESTION 145
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All file servers have computer accounts in an organizational unit (OU) named CompanyServers. All users have user accounts in an OU named CompanyUsers.
For all users and administrators, the My Documents folder is redirected to a shared folder on a file server named Certkiller 1.
The company wants to limit the amount of disk space that can be used by each user. Each user must be allowed to use a maximum of 2 GB of storage on Server1.
You need to limit disk space usage on Server1 to 2 GB per user. Administrators must not have these limits. What should you do?
A.Create a Group Policy object (GPO) linked to the CompanyUsers OU. In the GPO, enable disk quotas.
B.Create a Group Policy object (GPO) linked to the CompanyUsers OU. In the GPO, enable a size limit on user profiles
C.Create a Group Policy object (GPO) linked to the CompanyServers OU. In the GPO, enable disk quotas.
D.Create a Group Policy object (GPO) linked to the CompanyServers OU. In the GPO, enable a default cache size for
offline files.

Answer: B

Explanation:
To prevent users, computers, and groups from creating an unlimited number of objects in Active Directory, Windows
Server 2003 has added quotas. Active Directory quotas are used to limit how many objects are owned in a particular
directory partition. While quotas can be applied to almost every user, computer, and group, Domain Administrators and
Enterprise Administrators are exempted from these limits. The quotas that are used to limit the ability of a user, computer, or group from creating too many objects in Active Directory should not be confused with disk quotas, which
are also available on Windows Server 2003 servers (regardless of the functionality level being used).
The new Active Directory quotas (not to be confused with disk quotas) are defined as the number of objects that can
be owned by a given user in a given directory partition. Domain Admins and Enterprise Administrators are exempt from
only the original operations do. Quota administration is performed through a set of commandline
tools, including dsadd,
dsmod, dsget, and dsquery. No graphical interface exists for quota administration.
Disk quotas can be used to limit the amount of hard disk space that can be used on a volume that's formatted in NTFS.
The NTFS file system is more advanced than other file systems such as FAT or FAT32, which can also be used to
format volumes. By using disk quotas on an NTFS volume, administrators can prevent users from filling up the hard disk
with an unlimited number of files.
Incorrect answers:
A:Making use of disk quotas will not have the desired effect.
C:The CompanyServers OU is the wrong organizational unit to link the GPO to.
D:First, this is the wrong to link the newly created GPO to this particular organizational unit and furthermore, the GPO
should not be one of enabling a default cache size for offline files.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 1, p. 69 &
Chapter 4, p. 250

QUESTION 146
You are the network administrator for Certkiller .com. The network consists of a single Active Directory

domain named Certkiller .com. The domain contains an organizational unit (OU) named Accounting.
A user named Jack works in the accounting department. A user account for Jack is located in the Accounting OU.
You create three Group Policy objects (GPOs) and link them to the Accounting OU. The three polices are shown in the Accounting Properties exhibit.

You run Resultant Set of Policy (RSoP) in logging mode for Jack's user account. The results for the policies that apply to Jack's user account are shown in the RSoP Settings exhibit.
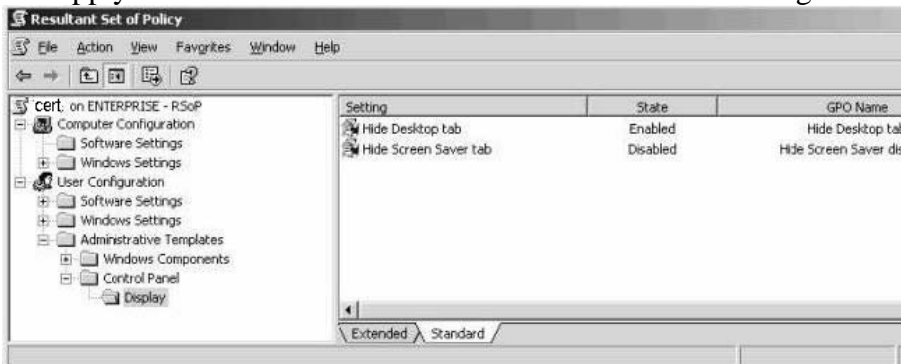
You need to ensure that the Desktop tab and the Screen Saver tab are disabled.
What should you do?
A.Move the Hide Screen Saver disabled GPO higher in the priority list in theGroup Policy Object Linksarea of the
Accounting Propertiesdialog box.
B.Move the Hide Screen Saver disabled GPO lower in the priority list in theGroup Policy Object Linksarea of the
Accounting Propertiesdialog box.
C.Disable theBlock Policy inheritancesetting on the Accounting OU.
D.Click theOptionsbutton in theAccounting Propertiesdialog box and enable theNo Overridesetting on the Hide desktop tab GPO.

Answer: B

Explanation: The Desktop tab is hidden, so we just need to hide the Screen Saver tab.With the current settings, the

Hide Screen Saver Enabled policy is applied first.It is then overwritten by the Hide Screen Saver Disabled policy.The
result being that the Screen Saver tab is no longer hidden.We can rectify this by moving the Hide Screen Saver disabled
GPO lower in the priority list in theGroup Policy Object Linksarea of theAccounting Propertiesdialog box.This will
mean that that the Hide Screen Saver Disabled policy is applied first and is then overwritten by the Hide Screen Saver
Enabled policy.
Incorrect Answers:
A:The Hide Screen Saver disabled GPO is already higher in the priority list than the Hide Screen Saver Enabled GPO.
It needs to be lower.
C:The problem is caused by the OU policies.Unblocking inheritance won't affect the OU policies.
D:This won't affect the policies applied at this OU level.This would only affect child OUs if they existed.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-13 to 11-23

QUESTION 147

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All computers are members of the domain. All servers run Windows Server 2003. All client computers run Windows XP Professional.
The network contains desktop client computers and portable client computers. The portable computers include both laptop computers and tablet computers. Client computer accounts are located in various organizational units (OUs) organized by department and division, along with desktop computer accounts.
A written company policy requires that no portable computer is to be left unattended and logged on to the network, unless protected by a password. Users are not allowed to override this requirement. This requirement does not apply to desktop computers because those computers are located in secured offices.
You need to configure your network so that portable computers comply with the written requirement.
What should you do?
A.Create a Group Policy object (GPO) that specifies a logon script.
Link this GPO to the domain.
Configure the logon script to read the Oeninfo.info file for manufacturer and model information, and set the screen saver
properties if the manufacturer and model number indicates one of the portable computers.
A.Create a Group Policy object (GPO) that specified a logon script.
Link this GPO to the domain.
Configure the logon script to make a WMI query for manufacturer information and update the user's profile information
in Active Directory if the user is using a portable computer.
A.Create a Group Policy object (GPO) that specifies a passwordprotected
screen saver.
Link this GPO to the domain.
Use a WMI filter to query for the hardware chassis type information to ensure that the GPO applies only to the

portable
computers.
A.Create a Group Policy object (GPO) that specified a passwordprotected
screen saver.
Link this GPO to the domain.
Use a WMI filter to query for the specific edition of Windows XP Professional installed on the computer to ensure that
the GPO applies only to the portable computers.

Answer: C

Explanation: We can use a WMI filter to query for the hardware chassis type information to ensure that the GPO
applies only to the portable computers.
Incorrect Answers:
A:This is a very difficult and impractical way of doing it.
B:Updating the user profile would not achieve anything.
D:The desktops would probably have the same version of XP as the laptops.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-20 to 10-21,1-16

QUESTION 148
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .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 computers.
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.
A.Create a group that includes the Windows XP Professional computers.
Assign the group theDeny General
Resultant Set of Policy(Logging)permission.
A.Create a group that includes the Windows 2000 Professional computers.
Assign the group theDent Apply

Group Policypermission.

Answer: A, B

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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-20 to 10-21,11-6

QUESTION 149
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com.
The following table shows the types and quantities of Windows Server 2003 Web and database servers in the domain.

Server type	Quantity
Nonproduction test Web server	2
Nonproducation test database server	2
Production Web server	10
Production database server	10

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.
Certkiller plans to use Group Policy objects (GPO) to centrally apply security settings to the Web and database server computers. The settings need to be applied as follows:
1.Some security settings need to apply to all Web and database servers.
2.Some security settings need to apply to the nonproduction servers only.
3.Some security settings need to apply to the production servers only and must not be overridden.
4.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 ***missing***

What should you do?

A.Create two toplevel

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.

A.Create two toplevel

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.

A.Create a toplevel

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.

A.Create a toplevel

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 unde r both the Nonproduction OU and the Production OU.

Answer: D

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 nonproduction 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.

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 Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 6-3 to 6-9,6-16 to 6-23

QUESTION 150

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains three domains named Certkiller .com, texas. Certkiller .com, and dakota. Certkiller .com. The

functional level of the forest is Windows Server 2003.

Both texas. Certkiller .com and dakota. Certkiller .com contain employee user accounts, client computer accounts,
and resource server computer accounts. The domain named Certkiller .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.
Certkiller 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 toplevel
OU for each server role under the Certkiller .com domain.
Create a toplevel
OU named Servers under the texas. Certkiller .com domain.
Create a toplevel
OU named Servers under the dakota. Certkiller .com domain.
A.Create a toplevel
OU named Servers under the texas. Certkiller .com domain.
Create a child OU for each server role under the Servers OU.
Create a toplevel
OU named Servers under the Dakota. Certkiller .com domain.
Create a child OU for each server role under the Servers OU.
A.Create a toplevel
OU named Servers under the Certkiller .com domain.
Create a child OU for each server role under the Servers OU.
A.Create a toplevel
OU for each server role under the texas. Certkiller .com domain.
Create a toplevel
OU for each server role under the dakota. Certkiller .com domain.

Answer: B

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,
dakota. Certkiller .com and texas. Certkiller .com.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 dakota. Certkiller .com and texas. Certkiller .com, because the resource servers
are in those domains.
C:We need a top level OU for all the resource servers in dakota. Certkiller .com and texas. Certkiller .com, so we can apply
group policies to all the servers.

D:We need a top level OU for all the resource servers in dakota. Certkiller .com and texas. Certkiller .com, so we can apply
group policies to all the servers.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 406, 408-411,
576-584

QUESTION 151
You are the administrator of the Certkiller company network. The network consists of a single Active Directory domain Certkiller .com. The network includes 50 servers running Windows Server 2003 and 1000 client computers running Windows XP Professional.
All client computers are in an organisational unit (OU) named Clients. All server computers are in an organisational unit (OU) named Servers.
You discover that most of the servers are running the SMTP service and the Telnet service. These services are not required and should be disabled.
What is the easiest way to ensure that the services are always disabled on the servers?
A.Use gpedit.msc to create a Group Policy object (GPO) to apply a logon script that disables the unnecessary services.
Link the GPO to the Servers OU.
A.Use gpedit.msc to create a Group Policy object (GPO) and import the Hisecws.inf security template.
Link the GPO to the Servers OU.
A.Use gpedit.msc to create a Group Policy object (GPO) to set the startup type of the unnecessary services to Disabled.
Link the GPO to the Servers OU.
A.Use gpedit.msc to create a Group Policy object (GPO) to apply a startup script to stop the unnecessary services.
Link the GPO to the Servers OU.

Answer: C

Explanation: The servers have been moved to an OU. This makes it easy for us to configure the servers using a group
policy. We can simply assign a group policy to the Servers OU to disable the services.
Incorrect Answers:
A:The logon script would only run when someone logs on to the servers. It's likely that the servers will be running with
no one logged in.
B:TheHisecws.inf security template is designed for workstations, not servers.
D:The startup script would only run when the servers are restarted. A group policy would be refreshed at regular
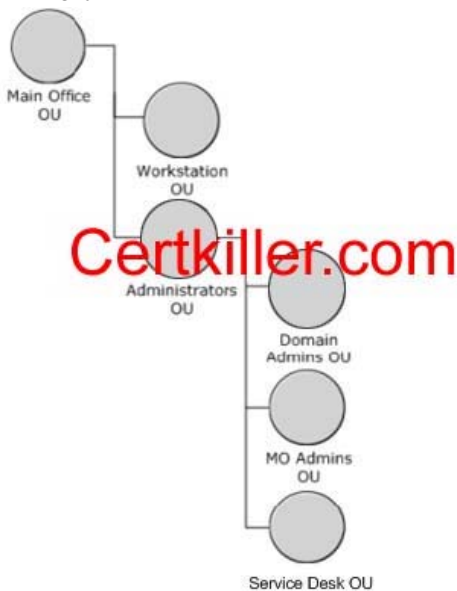
intervals.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 13: 85-86

QUESTION 152
Exhibit

You are a network administrator for Certkiller .com. The user accounts for all service desk users are members of a global group named Service Desk and are located in ServiceDesk OU.
A GPO named Admin Tools assigns the Windows Server 2003 Administration Tools Pack to users. You link the GPO to the Administrators OU.
The administrative tools are not installed on the client computers used by the service desk users. These users require the administrative tools.
You use the Group Policy Management Console (GPMC) to examine how the Group Policy is applied to the ServiceDesk OU. You discover that the inheritance of GPOs is blocked for the ServiceDesk OU.
You need to ensure that the administrative tools are installed on the client computers used by the service desk users. You also need to ensure that the client computers used by the service desk users are not modified in any other way.
What should you do?
A.Link the Admin Tools GPO to the ServiceDesk OU.
B.Link the Admin Tools GPO to the domain.
C.Configure the Admin Tools GPO to apply to the Service Desk global group.
D.Create a new GPO that assigns the Windows Server 2003 Administration Tools Pack to computers. Link the new
GPO to the ServiceDesk OU.

Answer: A

Explanation: The question stated that Block Policy Inheritance is enabled for the ServiceDesk OU. Given the

exhibit

that shows the OU structure of Certkiller and also that the Admin Tools GPO is linked to the Administrators OU, you

should then link the Admin Tools GPO to the ServiceDesk OU to ensure that administrative tools are also installed on

the ServiceDesk OUs client computers without changing the client computers in any other way.

Incorrect answers:

B:That GPO should be linked to the ServiceDesk OU and not the domain. If linked to the domain then it will apply to

unnecessary computers as well. The question states that the administrative tools installed should be used by the service

desk users' client computers and that these computers should not be modified in any other way.

C: A global group can contain accounts and groups from the domain in which it is created, and be assigned permissions

to resources in any domain in a tree or forest. Because it only applies to the domain in which it's created, this type of

group is commonly used to organize accounts that have similar access requirements. Having the Admin Tools GPO only

applied to the Service Desk global group would not necessarily have the desired effect then.

D:There is no need to create a new GPO since there is already a GPO called Admin Tools that serves the same purpose.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 9: 18-19

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 2, p. 134

QUESTION 153

You are the network administrator for Certkiller . The network consists of two Active Directory forests, each consisting of a single domain. The functional level of both forests is 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.

You are using the test forest to test Group Policy objects (GPOs) that manage administrative templates before they are implemented in the production forests. This testing includes changes to the Default Domain Policy GPO and the Default Domain Controllers Policy GPO.

You need to be able to restore the Default Domain Policy and Default Domain Controllers Policy GPOs for the test domain to the settings used in the production forest. You want to accomplish this task by using the minimum amount of administrative effort.

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

A.Run thedcgpofix /bothcommand in the test domain.

B.Back up the Default Domain Policy and Default Domain Controllers Policy GPOs from the production domain by
using the Group Policy Management Console (GPMC).
C.Import the Default Domain Policy and Default Domain Controllers Policy GPOs into the test domain by using the
Group Policy Management Console (GPMC) and a migration table.
D.Back up the original GptTmpl.inf files for the Default Domain Policy and Default Domain Controllers Policy GPOs
from the production forests.
E.Restore the backed up GpTmpl.inf files to the test domain.
F.Increment the version in the Gpt.ini files for the Default Domain Policy and Default Domain Controllers Policy GPOs.

Answer: B, C

Explanation: We can use theGroup Policy Management Console (GPMC) to back up the GPOs from the production
domain and import them into the test lab.The GPMC lets administrators manage Group Policy for multiple domains and
sites within one or more forests, all in a simplified user interface (UI) with draganddrop
support. Highlights include
new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These
operations are fully scriptable, which lets administrators customize and automate management.
When we do the restore process, we need to restore both policies Domain and DCS.Therefore, for the DC's we will
need to use a migration table, to migrate the security principals.
If we install GPMC in the default path we need to execute from C:\Program Files\GPMC\Scripts
The script:CreateMigrationTable.wsf.
This script Creates migration tables that can be edited and used to map paths and security principals to new values
when importing and copying GPOs across domains.
Incorrect answers:
A:The Dcgpofix command restores Group Policy Objects (GPOs) to the state they where in when initially installed.By
restoring these GPOs to their original states, any changes that were made to them are lost. This is not what is required in
this scenario.
D:There is no need to backup files for the Default Domain Policy and the Default Domain Controllers Policy GPO from
the production forest. This will result in unnecessary administrative effort.
E:Since the test domain is used to test the settings and what is needed is to apply these settings to the production
domain then all that is necessary is to back up the Default Domain Policy and Default Domain Controllers Policy GPOs
from the production domain by using the Group Policy Management Console (GPMC) and then to import it into the test
domain.

F:This option will result in too much administrative effort being applied when all that is needed is to back up the Default
Domain Policy and Default Domain Controllers Policy GPOs from the production domain by using the Group Policy
Management Console (GPMC) and then to import it into the test domain.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 1, p. 46
MS White Paper: Migrating GPOs Across Domains with GPMC
http://www.microsoft.com/windowsserver2003/docs/MigGPOs.doc

QUESTION 154
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. There is an organizational unit (OU) named DocProcessing. The DocProcessing OU contains user accounts for users in the document processing department.
You create a Group Policy object (GPO) and link it to the DocProcessing OU. You configure the GPO to publish a graphics application. Some of the users in the document processing department report that the application is not available from the Start menu, and other users report that the graphics application was installed successfully after they double-clicked a graphics application document.
You need to ensure that all users in the DocProcessing OU can successfully run the graphics application. What should you do?
A.Instruct users who report a problem to run thegpupdatecommand on their computers.
B.Instruct users who report a problem to install the application by using Add or Remove Programs in Control Panel.
C.Run the Resultant Set of Policy (RSoP) tool on the domain controllers on the network.
D.Run thegpresultcommand on each client computer and domain controller on the network.

Answer: B

Explanation: You havepublishedthe applications to users.This setting makes the application available for users to
install.In order to install a published application, users need to use the Add or Remove Programs applet in Control
Panel, which includes a list of all published applications that are available for them to install.
Users in the document processing department report that the application is not available from theStart menu.It won't be
available in the start menu because the application was published, not assigned.
Incorrect Answers:
A:This will refresh the group policy.It won't make the application available in the start menu.
C:This will display the resultant policy.It won't make the application available in the start menu.
D:This will display the resultant policy.It won't make the application available in the start menu.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 18: 15

QUESTION 155
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. An organizational unit (OU) named Sales contains two child OUs named Accounts Payable and Accounts Receivable.
You need to deploy an accounting application to all user accounts in the Sales and Accounts Receivable OUs. You do not want to deploy the application to the user accounts in the Accounts Payable OU. In addition, you have a graphics application that you need to deploy to all user accounts in the Accounts Payable OU only.
You need to configure your Group Policy object (GPO) structure to achieve these goals.
What should you do?
A.Create a GPO named Software Distribution and link it to the Sales OU.
Configure the GPO to deploy both the accounting and the graphics applications.
Enable theNo Overridesetting on the GPO.
On the Accounts Payable OU, enable theBlock Policy inheritancesetting.
A.Create a GPO named Software Distribution and link it to the Sales OU.
Configure the GPO to deploy both the accounting and the graphics applications.
Modify the discretionary access control list (DACL) settings of the GPO to assign the Authenticated Users group the
Deny Readand theDeny Apply Group Policypermissions.
A.Create a GPO named Graphics and link it to the Sales OU.
Configure the GPO to deploy the graphics application.
Create a GPO named Accounting Software and link it to the Accounts Payable OU.
Configure the GPO to deploy the accounting application.
On the Accounts Payable OU, enable theBlock Policy inheritancesetting.
A.Create a GPO named Accounting Software and link it to the Sales OU.
Configure the GPO to deploy the accounting application.
Create a GPO named Graphics and link it to the Accounts Payable OU.
Configure the GPO to deploy the graphics application.
On the Accounts Payable OU, enable theBlock Policy inheritancesetting.

Answer: D

Explanation: We need to deploy an accounting application to all user accounts in the Sales and Accounts Receivable
OUs but not to the user accounts in the Accounts Payable OU. Instead we want to deploy a graphics application to all
user accounts in the Accounts Payable OU.
applies the graphics GPO to the Accounts Payable OU. We aren't concerned about the Accounts Receivable OU because that OU is a child OU of the Sales OU so it will get the settings applied at the parent OU. The Accounts Payable OU is also a child OU of the Sales OU so we must prevent it from getting the accounts application form the

Sales OU by setting the Accounts Payable OU to Block Policy Inheritance.
Incorrect Answers:
A, B, C:The graphics application must be deployed only to the Accounts Payable OU. Therefore we should apply it to
the Accounts Payable OU and not the Sales OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 156
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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.
Certkiller requires all client computers to run antivirus software. Certkiller licenses an antivirus application that is installed on a file server named Certkiller 1. An unattended installation can be performed on each client computer by running the setup command from a shared folder on Certkiller 1.
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 thesetupcommand to install the antivirus application if it is not currently
installed.
Instruct all users to restart their client computers.
A.Create a Group Policy object (GPO) linked to the domain.
Use the GPO to launch a startup script that runs thesetupcommand to install the antivirus application if it is not currently
installed.
Instruct all users to restart their client computers.
A.Create a batch file that runs thesetupcommand.
Send this batch file in an email
message to all users.
Instruct all users to run this batch file.
A.Use Remote Assistance to run thesetupcommand on each client computer.

Answer: B
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 registrybased 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 emailing

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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-40 to 10-41

Dan Holme and Orin Thomas, MCSA/MCSE SelfPaced

Training Kit (Exam 70290):

Managing and Maintaining a

Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, Washington, 2004,pp. 2-19 to 2-24

QUESTION 157

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

Event Properties

Event

Date: 3/22/2003   Source: Application Management
Time: 10:26:03 PM   Category: None
Type: Error   Event ID: 102
User: Certkiller\newuser
Computer: Certkiller1

Certkiller.com

Description:

The install of application Windows Server 2003 Administration Tools Pack from policy FileInstall failed. The error was : The installation source for this product is not available. Verify that the source exists and that you can access it.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ⦿ Bytes ○ Words

You need to ensure that users can install the application.
What should you do?
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 theAlways install with elevated privilegessetting.
D.Assign the users theAllow Readpermission
for the .msi file.

Answer: D

Explanation: To assign the application to users, the users need at leastAllow Readpermission
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 haveAllow Read
permissions.
C:Users need theAllow-Readpermission to the msi file.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-16 to 10-20,10-40 to 10-41

QUESTION 158
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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

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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-23 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 159

You are the network administrator for Certkiller .com. Your network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. You use Group Policy objects (GPOs) to distribute software.

Certkiller 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: 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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 12-3 to 12-10

QUESTION 160
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory
domain named Certkiller .com 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 CK1 .
All users in Certkiller 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 CK1 , their assigned applications are not available.
You need to configure your network so that the applications are available to users when they connect to
CK1 . 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 CK1 . 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

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 Server.

D: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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-23 to 12-10,12-13 to 12-28,12-34 to 12-39


QUESTION 161
You are the Network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003.The user accounts for the processing department are located in an Organizational Unit (OU) named processing.
You need to deploy an application to all users in the processing department. You create a Group Policy Object (GPO) and link it to the processing OU. You place the .msi file for the application in a shared folder on the network. You configure the User Configuration section of the GPO to deploy the application.
You need to ensure that the application is immediately ready for use when a user logs on to a client computer. You also need to prevent any user from continuing to use the application if the user's user account is moved to another OU.
What should you do?
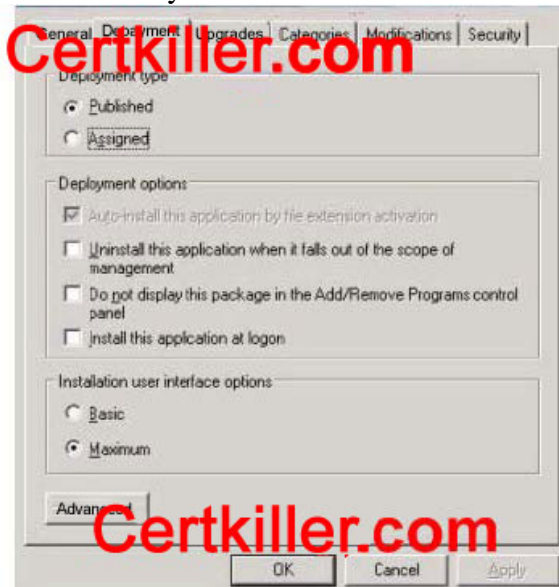
Answer:
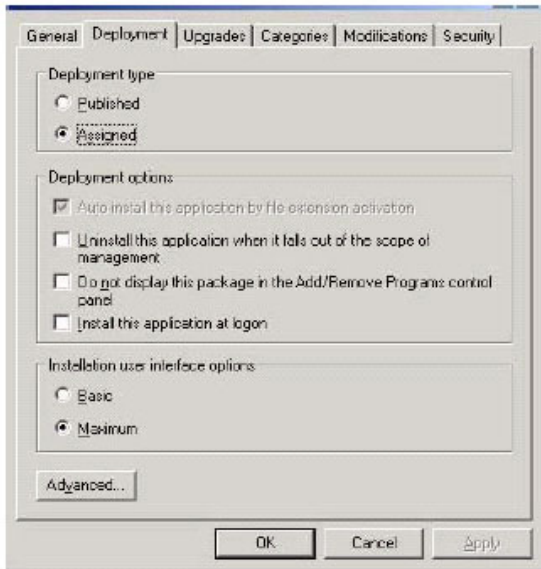
Explanation:
Select the following check boxes:
1.Assigned.
2.Uninstall this application when it falls out of the scope of management.
3.Install this application at logon.
4.Basic
We need to assign the application to the users and select the "Install this application at logon" option to ensure that the
application is immediately ready for use when a user logs on to a client computer.
To prevent any user from continuing to use the application if the user's user account is moved to another OU, we need
to select the "Uninstall this application when it falls out of the scope of management" option.
The "Basic" option ensures that the application installs with minimal (or no) user intervention.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-23 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 162
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. User accounts for users in the finance department are in an organizational unit (OU) named Finance. You use Group Policy objects (GPOs) to manage these user accounts.
Users in the finance department need a new application installed on their computers. Several of these users volunteer to be pilot users to test the application before it is deployed throughout the department.
You configure a GPO to install the application. You create a group named PilotUsers in the Finance OU. You make the pilot users' user accounts members of the PilotUsers group. The pilot users' user accounts are also in the Finance OU.
You need to allow only the pilot users to test the application.
What should you do?

A.Assign the PilotUsers group theAllow Readand
theAllow Writepermissions
for the gPLink property of the
Finance OU.
B.Assign the PilotUsers group theAllow Readand
theAllow Apply
Group Policypermissions for the GPO.Remove
the Authenticated Users group's permissions to apply the GPO.
C.Assign the PilotUsers group theAllow Generate
Resultant Set of Policy (Logging)permissions for the Finance
OU.
D.Assign the PilotUsers group theAllow Generate
Resultant Set of Policy (Planning)permission for the Finance
OU.

Answer: B

Explanation: We need to install the application for the pilot users only.We can do this by assigning the
PilotUsers group
theAllow Readand
theAllow Apply
Group Policypermissions for the GPO.To prevent the GPO applying to the
other finance users, we need to remove the Authenticated Users group's permissions to apply the GPO.
Incorrect Answers:
A:We need to assign permissions to apply the group policy, not link the policy.
C:This will allow the PilotUsers group to run RSoP in logging mode.It won't configure the GPO to apply to just
the pilot
users.
D:This will allow the PilotUsers group to run RSoP in planning mode.It won't configure the GPO to apply to
just the
pilot users.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 408411

QUESTION 163
You are the network administrator for Certkiller . The network consists of a single Active Directory domain
named Certkiller .com. All member servers run Windows Server 2003. All client computers run Windows XP
Professional. All client computer accounts in the domain are located in an organizational unit (OU) named
Workstations.
You need to distribute a new application to all client computers on the network. You create a Group Policy
object (GPO) that includes the application package in the software installation settings of the Computer

Configuration section of the GPO. You assign the GPO to the Workstations OU.
Several days later, users report that the new application is still not installed on their client computers.
You need to ensure that the application is installed on all client computers.
What should you do?
A.Instruct users to restart their client computers.
B.Instruct users to run Windows Update on their client computers.
C.Instruct users to force a refresh of the computer policy settings on their client computers.
D.Instruct users to force a refresh of the user policy settings on their client computers.

Answer: A

Explanation: When an application is assigned to a computer, the software is deployed when it is safe to do so (that is,
when the operating system files are closed). This generally means that the software will be installed when the computer
starts up, which ensures that the applications are deployed prior to any user logging on. For this scenario, we need to
tell the users torestart their client computers.
Incorrect Answers:
B:Windows Update is used to update the operating system with the latest security patches etc.
C:You applied the policy several days ago. The client computers should have the GPO by now.
D:The setting isn't in the user section of the group policy.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 10, p.
646

QUESTION 164
You are a network administrator for Certkiller . The network consists of a single Active Directory domain
named Certkiller .com. All servers run Windows Server 2003.
A Group Policy object (GPO) named Software Restrictions prevents users from running unauthorized
applications. This restriction does not apply to users who are local administrators on their client computers.
Developers at the company create a new application for internal users. An administrator installs the
application on a number of computers by running the Setup.exe file supplied by the developers. However,
when users try to run the new application, they report that they cannot do so.
You need to ensure that all users can run the new application. You also need to ensure that unauthorized
applications cannot run.
What should you do?
A.Install the application on computers that require its use.Create a WMI filter on the Software Restrictions GPO
that
detects where the software is installed and prevents the GPO from being applied.
B.Create a security group that contains all users who need to use the application.Modify the security settings on

the
Software Restrictions GPO so that its effects are bypassed for members of this group.
C.Create a hash value for the application's executable code file, and revise the Software Restrictions GPO to allow
executable code files that match the hash value to run.
D.Repackage the application as an .msi package and use a new GPO to assign the package to the computers that require the application.

Answer: C

Explanation: We have a software restrictions policy that only allows authorised applications to run.The new application
isn't authorised, so we need to authorise it by creating a hash value of the program file and modify the software restrictions policy to permit the users to run the application.
Incorrect Answers:
A:The GPO prevents users running unauthorized software.Therefore, this GPO must be applied at all times we cannot
use a WMI filter to prevent the application of the GPO.
B:The GPO prevents users running unauthorized software.
Therefore,this GPO must be applied at all times we
cannot use security filtering to prevent the application of the GPO
to the users who require access to the new application.
D:Windows clients support setup.exe files.As long as the setup.exe file is written correctly, the users would be able to
use the application.The users in this scenario cannot run the program because the software restrictions group policy is
preventing them running the application.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 10, p. 647
MS knowledge Base Article Q324036HOW TO: Use Software Restriction Policies in Windows Server 2003

QUESTION 165
You are the Network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. The domain contains 300 user accounts and 325 computer accounts.
Different users on the network need different applications based on the department in which they work. All of these applications are packaged as .msi files.Many of the applications are updated every year.
You receive many support calls from users who need to have applications reinstalled because of damaged installations. The company decides that the cost of installing and maintaining these many applications is too high.

You need to implement a technology that will enable you to lower the cost of deploying user applications
while minimizing user down time.
What should you do?
A.Configure Group Policy Objects (GPOs) to assign applications to user accounts.
B.Install servers running Remote Installation Services on the network.
C.Place a server running Software Update Services (SUS) on the network and configure a GPO to enable updates for
all client computers.
D.Install Microsoft Operations Manager and enable SNMP on the client computers.

Answer: A

Explanation:
You can use the Software Installation extension of Group Policy to centrally manage software distribution in your
organization. You can assign and publish software for groups of users and computers using this extension.
When you assign applications to users or computers, the applications are automatically installed on their computers at
logon (for userassigned
applications) or startup (for computerassigned
applications.)
When assigning applications to users, the default behavior is that the application will be advertised to the computer the
next time the user logs on. This means that the application shortcut appears on theStartmenu, and the registry is updated
with information about the application, including the location of the application package and the location of the source
files for the installation. With this advertisement information on the user's computer, the application is installed the first
time the user tries to use the application. In addition to this default behavior, WindowsXP Professional and Windows
Server2003 clients support an option to fully install the package at logon, as an alternative to installation upon first use.
Note that if this option is set, it is ignored by computers running Windows2000, which will always advertise user-assigned applications.
When assigning applications to computers, the application is installed the next time the computer boots up. Applications
assigned to computers are not advertised, but are installed with the default set of features configured for the package.
Assigning applications through Group Policy requires that the application setup is authored as a Windows Installer (.msi)
package.
Incorrect answers:
B:Installing servers that runs Remote Installation Services will contribute to downtime on the network. The question
pertinently states to minimize downtime.

C:This is not a matter of running updates on the network for all the client computers to receive updates. The question
states that full applications needs to be reinstalled and this is conceptually different from running updates.
D:Enabling SNMP on the client computers will not accomplish the task at hand.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, p. 10: 12

QUESTION 166
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. All servers run Windows Server 2003.
You configure a certification authority (CA) to issue smart card authentication certificates. Users who have
administrative responsibilities are required to have two accounts. One account is for general computer use.
The other account is an administrative account that has administrative privileges and is used only when
performing administrative tasks.
You decide to deploy smart cards to all users in your company. You issue one smart card to each user for
general computer use. You enroll each user for a smart card authentication certificate.
You need to plan smart card access for users who have administrative responsibilities.
What should you do?
A.Issue an additional smart card to users who have administrative responsibilities.Enroll each user's
administrative
account for a smart card authentication certificate.Instruct users to use this card when logging on to perform
administrative tasks.
B.Enroll each user's administrative account for a smart card authentication certificate.When prompted, store the
certificate on the existing smart card.Instruct users to use this card when logging on to perform all tasks.
C.Configure Group Policy to autoenroll administrative users for certificates.Instruct these users to log on by
using their
nonadministrative accounts.
D.Issue a master card to users who have administrative responsibilities.Instruct users to use this card when
logging on to
perform administrative tasks.

Answer: B

Explanation: It is possible to store multiple certificates on a smart card.The user can select an account when
he/she logs
on.
Incorrect Answers:
A:It is not necessary to issue additional smart cards.A single smart card can store multiple certificates.
C:This answer won't work.The users need to log on using their administrative accounts to do administrative
work.A
certificate needs to be created for the administrative account and stored on a smart card.
D:It is not necessary to issue additional smart cards.A single smart card can store multiple
certificates.Furthermore, this
answer seems to suggest having multiple smart cards with a single "master" certificate mapped to a single

"master"
administrative account.
Reference:
Martin Grasdal, Laura E. Hunter, Michael Cross, Laura Hunter, Debra Littlejohn Shinder, and Dr. Thomas W. Shinder,
Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70293
Study Guide & DVD Training
System, Syngress Publishing, Inc., Rockland, MA 02370 Chapter 12, pp. 898
Craig Zacker, MCSE SelfPaced
Training Kit (Exam 70-293):Planning and Maintaining a Microsoft Windows Server
2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, Chapter 11
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active
Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 3, pp.
14-18

QUESTION 167
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. All servers run Windows Server 2003.
You install Certificate Services and configure an offline root certification authority (CA). You also configure
an enterprise subordinate CA in the domain.
Employees in the marketing department use a public key infrastructure (PKI) enabled application to store
secure marketing data. Employees require a certificate that supports client authentication to gain access to
this application. User objects for employees in the marketing department are stored in an organizational unit
(OU) named Marketing.
You create a Group Policy object (GPO) that configures users for autoenrollment, and you link the GPO to
the Marketing OU. You create a duplicate of the User certificate template named Employee and assign
permission to allow autoenrollment for users in the marketing department. You configure the Employee
template to prompt the user during enrolment.
An employee in the marketing department named David Lindberg reports that when he attempts to use the
marketing application, he receives a message stating that he does not have a client authentication
certificate. David is unable to use the marketing application. You examine David Lindberg's user object,
shown in the exhibit.
MISSING
You need to ensure that David can use the marketing application.
What should you do?
A.Edit David Lindberg's user object to include an email
address.
B.Add David Lindberg's user object to the Cert Publishers domain local group.
C.On David Lindberg's computer, use the Web enrolment tool to connect to the subordinate CA and download a
copy
of the subordinate CA's certificate.
D.On David Lindberg's computer, use the Web enrolment tool to connect to the subordinate CA and download

the
most recent certificate revocation list (CRL).

Answer: D

Explanation:
CAs can revoke as well as issue certificates. After a certificate is revoked, it needs to be published to a
CRL distribution point. Clients check the CRL periodically before they can trust a certificate. Following this
reasoning it
could be that his certificate could have been revoked. To make sure that he can use the marketing application he
should
make use of the Web enrolment tool to connect to the subordinate CA and download the latest CRL.
Incorrect answers:
A:This is probably a case of a revoked CA and editing Lindberg's user object to include an email
address will not
address the issue at hand.
B:This will not ensure that David will be able to make use of the marketing application.
C::You should not be downloading a copy of
CRL from the subordinate CA.
Reference:
Martin Grasdal, Laura E. Hunter, Michael Cross, Laura Hunter, Debra Littlejohn Shinder, and Dr. Thomas W.
Shinder,
Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70293
Study Guide & DVD Training
System, Syngress Publishing, Inc., Rockland, MA, Chapter 12, p. 909

QUESTION 168
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. All client computers run Windows XP Professional.
A written Certkiller 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.
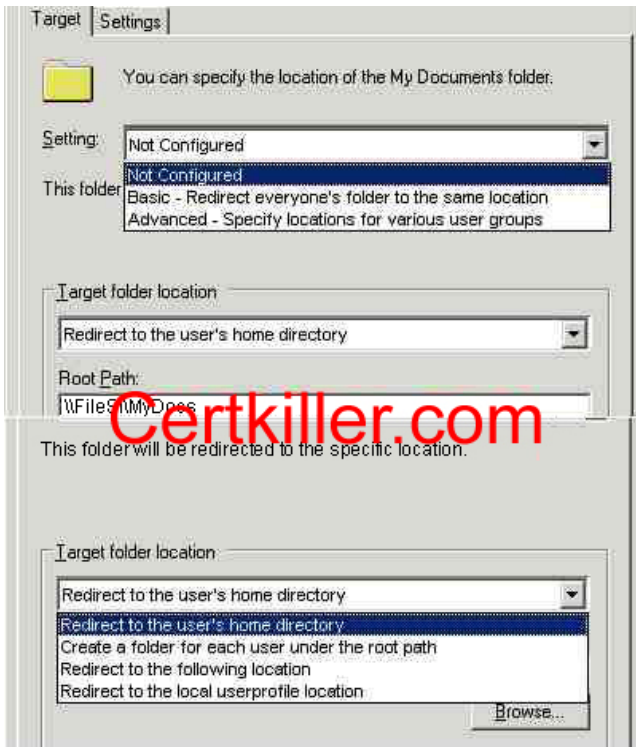
Answer:

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 Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 11-28 to 11-48

QUESTION 169
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain with two sites. The two sites are named Certkiller 1 and Certkiller 2. Certkiller 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 256Kbps
leased line. In addition, Certkiller 1 and Certkiller 2 are
connected by a site link. Certkiller 1 has 1,000 users and Certkiller 2 has 15 users. There are no domain controllers in Certkiller 2.
You create a Group Policy object (GPO) to redirect the My Documents folder. You link the GPO to the domain. Users in Certkiller 1 have their folders redirected successfully, but users in Certkiller 2 do not.
You need to ensure that users in Certkiller 2 have their folders redirected.
What should you do?
A.Combine Certkiller 1 and Certkiller 2 into a single site.

B.Enable loopback processing inMergemode in the GPO.
C.Remove the link for the GPO from the domain.Link the GPO to Certkiller 1 and to Certkiller 2.
D.Create a new GPO that disables Group Policy slow link detection.Link the new GPO to Certkiller 2.

Answer: D

Explanation: The users in Certkiller 2 receive their GPOs from domain controllers in Certkiller 1.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 Certkiller 2, 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 11-28 to 11-48

QUESTION 170
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Each client computer runs Windows NT Workstation 4.0, Windows 2000 Professional, or Windows XP Professional. The computer accounts for all client computers are located in an organizational unit (OU) named CompanyComputers. All user accounts are located in an OU named Certkiller Users.
Certkiller has a written policy that requires a logon banner to be presented to all users when they log on to any client computer on the network. The banner must display a warning about unauthorized use of the computer.
You need to ensure when a user logs on to a client computer.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A.Create a Group Policy object (GPO) that includes the appropriate settings in the interactive logon section.Link the
GPO to the domain.
B.Create a script that presents the required warning.Create a Group Policy object (GPO) that will cause the script to
run during the startup process.Link the GPO to Certkiller Users OU.
C.Create a system policy file named Ntconfig.pol that includes the appropriate settings.Place a copy of this file in the
appropriate folder on the domain controller.
D.Create a batch file named Autoexec.bat that presents the required warning.Copy the file to root folder on the system
partition of all computers affected by the policy.

Answer: A, C

Explanation: We need to configure a GPO to display the logon message that will apply to the Windows 2000 and
Windows XP clients. We need to configure a system policy to display the logon message that will apply to the Windows
NT clients.
This policy is created with System policies and the System Policy Editor, System policies are used by network
administrators to configure and control individual users and their computers. Administrators use
POLEDIT.EXE to set
Windows NT profiles that are either network or
userbased.
Using this application, you can create policies, which are
either local or networkdriven,
that can affect Registry settings for both hardware and users. The file created to apply
the policy is named NTConfig.pol.
Incorrect Answers:
B, D:Scripts and Autoexec.bat is processed at startup rather than at logon.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-3 to 10-12,10-16 to 10-20

QUESTION 171
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The network also consists of two sites named Certkiller 1 and Certkiller 2. 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.

Name	GPO section	Policy	Setting
GPO1	User Configuration	Prevent changing wallpaper	Disabled
GPO2	Computer Configuration	Minimum password length equals 8 characters	Enabled
GPO3	User Configuration	Screen Saver	Disabled

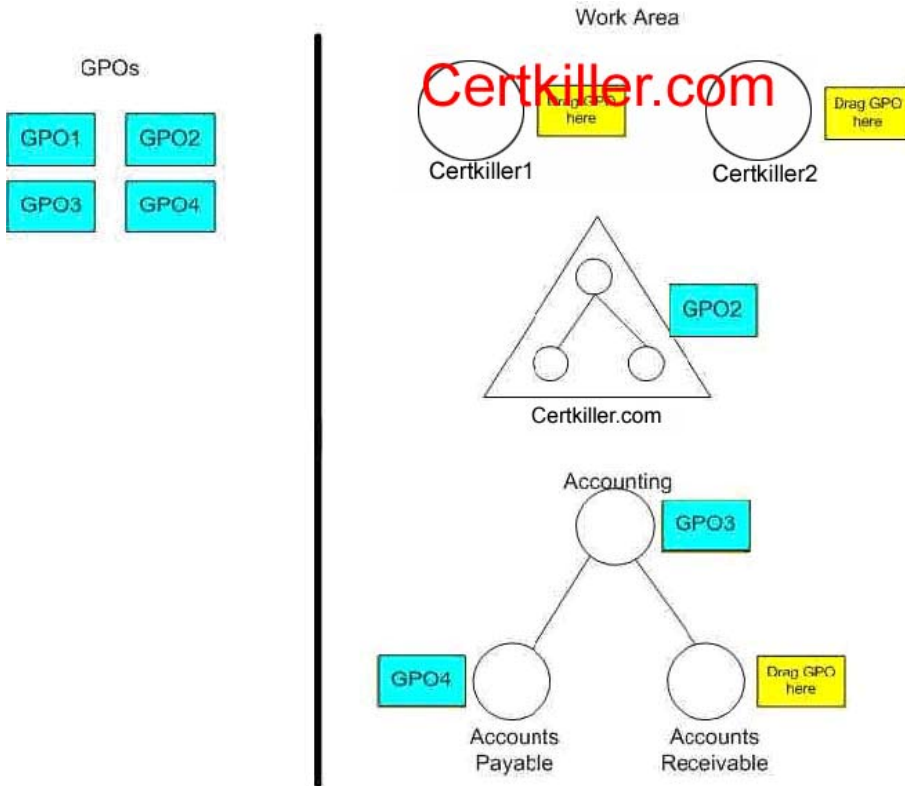| GPO4	User Configuration	Prevent changing wallpaper	Enabled

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.
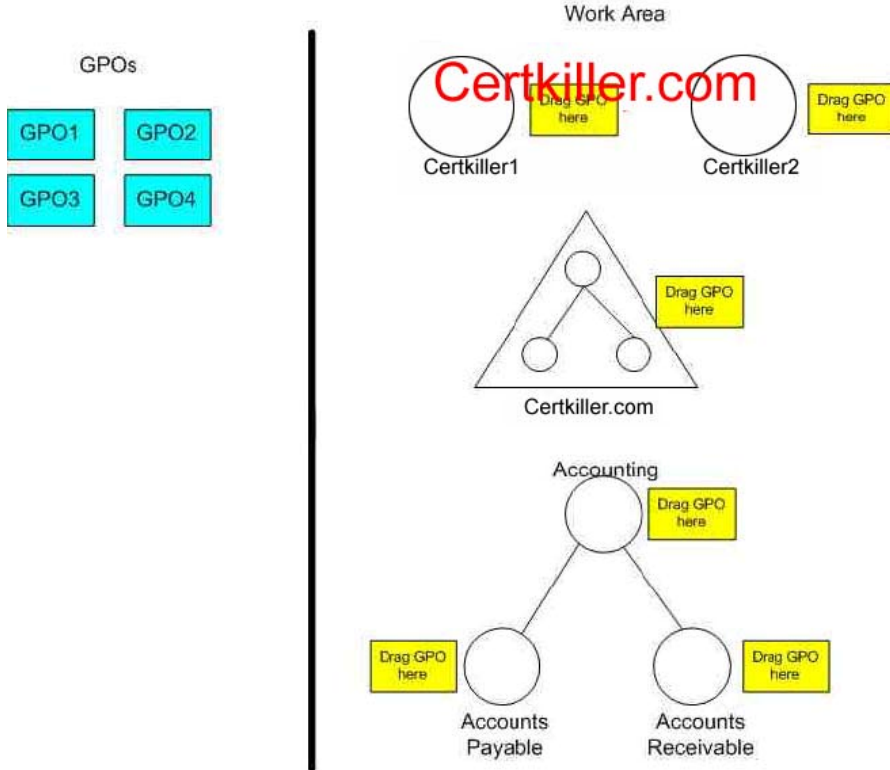
Answer:

Explanation:
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 isPrevent changing wallpaper. This must be enabled.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-16 to 10-20,10-41

QUESTION 172
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The domain contains an organizational unit (OU) named Accounting.
A user named Marie works in the accounting department. A user account for Marie is located in the
Accounting OU.

You create a Group Policy object (GPO) and link it to the Accounting OU. You configure the GPO to require complex passwords. Marie reports that the policy is not in effect.
You run Resultant Set of Policy (RSoP) in logging mode for Marie's user account. The results for the password policies are shown in the exhibit.

You need to ensure that the complex password policy is applied to the Accounting OU.
What should you do?
A.Enable theBlock Policy inheritancesetting on the Accounting OU.
B.Modify the Default Domain Policy GPO to enforce complex passwords.
C.Run thegpupdatecommand on Marie's client computer.
D.Disable the User Configuration section of the GPO linked to the Accounting OU.

Answer: B

Explanation: The exhibit shows that thePassword must meet complexity requirementssetting is disabled. We need
to enable this setting.
Incorrect Answers:
A, D:ThePassword must meet complexity requirementssetting is applied by the Default Domain Policy GPO. It is
not applied at the Accounting OU.
C:The Gpresult commandline
tool allows you to create and display an RSoP query, which can be used to analyze the
cumulative effects of GPOs, through the command line. It also provides general information about the operating system,
user, and computer.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-8 to 10-15

QUESTION 173
You are the network administrator for Certkiller .com. 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 Certkiller Users.

A written Certkiller 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 Certkiller Users OU. The setting in the Password Policy section of the Password Policies GPO are shown in the exhibit.

Policy	Policy Setting
Enforce password history	1 passwords remembered
Maximum password age	60 days
Minimum password age	0 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

You discover that users are creating simple passwords that do not meet the complexity requirements.
You need to ensure that Certkiller 's password requirements are enforced.
What should you do?
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

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-40 to 10-41

QUESTION 174
You are the network administrator for Certkiller .com. The network consists of as ingle Active Directory forest that contains an empty root domain named Certkiller .com and a child domain named research. Certkiller .com.
You need to implement secure password protection for the accounts located in the research. Certkiller .com domain.

What should you do?

A.Configure the Default Domain Policy Group Policy object (GPO) of the research. Certkiller .com domain to enable the
Password must meet complexity requirementspolicy.

B.Configure the Default Domain Controllers Policy Group Policy object (GPO) of the research. Certkiller .com domain to
enable thePassword must meet complexity requirementspolicy.

C.Configure the Default Domain Policy Group Policy object (GPO) of the Certkiller .com domain to enable thePassword
must meet complexity requirementspolicy.Enable theNo Overridesetting on the GPO.

D.Configure the Default Domain Controllers Policy Group Policy object (GPO) of the Certkiller .com domain to enable
thePassword must meet complexity requirementspolicy.Enable theNo Overridesetting on the GPO.

Answer: A

Explanation: GPOs are applied at the level at which they are linked. Thepassword 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:Thepassword policy must be configured at the domain level, i.e., Certkiller .com and not research. Certkiller
.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:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-41 to 10-42

QUESTION 175
You are the network administrator for Certkiller , a company that has a single office. The network consists of
a single Active Directory domain named Certkiller .com and a single site. All servers run Windows Server
2003.
All file and print servers and application servers are located in an organizational unit (OU) named Servers. A
server support team handles daily support issues for the file and print servers and application servers. All of
the server support team's user accounts are located in the OU named SST.
You are responsible for managing security for Certkiller 's servers. You create a group named ServerSupport
that includes all the user accounts of the server support team.
You need to ensure that members of the server support team can log on locally to only the file and print
servers and the application servers.
What should you do?

A.Create a Group Policy object (GPO) to grant the ServerSupport group theAllow log on locallyuser right.Link
the
GPO to the SST OU.

B.Create a Group Policy object (GPO) to grant the ServerSupport group theAllow log on locallyuser right.Link
the
GPO to the Servers OU.

C.Assign the ServerSupport group theAllow Full
Controlpermission for the Servers OU.
D.Assign the ServerSupport group theAllow Full
Controlpermission for the Computers container.

Answer: B

Explanation: All file and print servers and application servers are located in an organizational unit (OU) named
Servers.
Therefore, we can simply a Group Policy object (GPO) to grant the ServerSupport group theAllow log on
locallyuser
right and link the GPO to the Servers OU.
Incorrect Answers:
A:The GPO needs to be linked to the OU containing the computer accounts for the servers.
C:This would allow the ServerSupport group to create objects in the OU, and to modify the permission on
existing
objects.This is more 'permission' than necessary.
D:This would allow the ServerSupport group to create objects in the computers container, and to modify the
permission on existing objects.This would have no effect on the servers because they are in a separate OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 176
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The network contains 10 domain controllers and 50 servers in application
server roles. All servers run Windows Server 2003.
The application servers are configured with custom security settings that are specific to their roles as
application servers. Application servers are required to audit account logon events, object access events,
and system events. Application servers are required to have passwords that meet complexity requirements,
to enforce password history, and to enforce password aging. Application servers must also be protected
against maninthemiddle
attacks during authentication.
You need to deploy and refresh the custom security settings on a routine basis. You also need to be able to
verify the custom security settings during audits.
What should you do?
A.Create a custom security template and apply it by using Group Policy.
B.Create a custom IPSec policy and assign it by using Group Policy.
C.Create and apply a custom Administrative Template.
D.Create a custom application server image and deploy it by using RIS.

Answer: A

Explanation: The easiest way to deploy multiple security settings to a Windows 2003 computer is to create a
security

template with all the required settings and import the settings into a group policy.We can also use secedit to analyse the
current security settings to verify that the required security settings are in place.
Incorrect Answers:
B:An IPSec policy will not configure the required auditing policy.
C:We need a security template, not an administrative template.
D:This will create multiple identical machines.We cannot use RIS images in this scenario.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 13-57 to 13-66

QUESTION 177
You are the network administrator for Certkiller .com. The company has a main office and six branch offices. Each branch office employs fewer than 15 users.
The network consists of a single Active Directory domain named Certkiller .com configured as a single site. All servers run Windows Server 2003. Domain controllers are located in the main office. All branch offices are connected to the main office by WAN connections.
All users are required to change their password every 10 days. They are further restricted from reusing a password until after they have used five different passwords. You discover that users in the branch office can log on by using recently expired passwords and access local resources during a WAN connection failure that lasts for 24 hours or longer.
You need to ensure that users can log on to the domain only by using a current password.
What should you do?
A.Enable universal group membership caching in the site.
B.Instruct all users to log on by using their principal names (UPNs).
C.In Active Directory Users and Computers, require all users to change their passwords to the next time they log on to
the domain.
D.Configure the Default Domain Policy Group Policy object (GPO) to prevent logon attempts that use cached credentials.

Answer: D

Explanation: When the client computers are unable to contact a domain controller at the main office, the users are being
logged on using 'cached credentials'.This means that the client computer remembers that the user successfully authenticated with the domain controller recently, so the client computer assumes it is ok to log the user on again after
failing to contact a domain controller.We can disable this behaviour using a group policy.
Incorrect Answers:
A:Enabling universal group caching won't prevent the logons.
B:This won't prevent the users' ability to log on.
C:This won't prevent the users' ability to log on.
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE SelfPaced Training Kit (Exam 70-290):Managing and Maintaining a

Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, Washington, 2004,p. 5-19
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,2004, p. 5-41
Walter Glenn, and Michael T. Simpson; MCSE Self
Windows Server 2003 Active Directory and Network Infrastructure, Microsoft Press, Redmond, Washington,
2004,
pp. 5-11

QUESTION 178
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory
domain named Certkiller .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

Explanation: Given the organization structure of the company and the security concerns, the way to ensure htat
membership of the HRManagers group in each application servers is as secure as possible, you need to place
restrictions on the group membership by creating a GPO that configures resticted groups for each HRManagers
group
and link 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: (i) Local groups can contain local user
accounts from
the computer where you create the local group. (ii) Local groups cannot be members of any other group.This
option are
thus not a viable option in the light of the security concerns and the nature of the HRManagers group.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, p. 8: 6

QUESTION 179
You are the network administrator for Acme. The company consists of two subsidiaries named Litware Inc.,
and Certkiller . Litware, Inc., has an office in Los Alamos. Certkiller has two offices, one in New Delhi and the
other in Berlin.
The network consists of two Active Directory forests. A forest trust relationship exists between the two
forests. One forest contains one domain named LosAlamos.litwareinc.com. The other forest contains two
domains named NewDelhi. Certkiller .com and Berlin. Certkiller .com. All three offices are connected by two
128Kbps
connections. All servers run Windows Server 2003.
The network uses roaming profiles and Group Policy objects (GPOs). Occasionally, users need to work at an
office other than their usual office. Users must have the same desktop, no matter where they log on to the
network.
You need to ensure that the user's profile and the GPO settings that apply to the user's account will apply
wherever the user logs on to the network.
What should you do?
To answer, drag the appropriate configuration or configurations to the correct policy or policies in the work
area.

Configuration Select from these

Enabled

Certkiller.com

Disabled

Not configured

Place here

Wait for remote user profile — place here

Group Policy slow link detection — place here

Allow Cross-Forest User Policy and User Roaming Profiles — place here

Answer:

Configuration Select from these

Enabled

Certkiller.com

Disabled

Not configured

Place here

Wait for remote user profile	Enabled
Group Policy slow link detection	Enabled
Allow Cross-Forest User Policy and User Roaming Profiles	Enabled

Explanation:
The question states that when a user logs on in the other forest to the one where his user account resides, the user
MUST have his desktop settings and group policy settings.The first setting, "Wait for remote user profile" should be
enabled so that the client computer waits to load the remote profile, no matter how long it takes.To enable the roaming
profiles and group policy settings to apply to the user across a forest link, we should enable the third setting, "Allow
CrossForest
User Policy and User Roaming Profiles".
We need to prevent the speed of the link affecting the policies that are applied.However, we can't do this by simply
disabling the slow link detection, because a disabled slow link detection policy will use a default setting of 512Kbps (our
link is slower than that, so some group policy settings won't apply).We need to enable the policy and enter a connection
speed of 0.This disables the setting in such a way that all group policies will be applied across the slow link, no matter
how long they take to load.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, p. 588

QUESTION 180
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com Windows Server 2003 domain controllers are located in two sites named Certkiller 1 and Certkiller 2. 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.
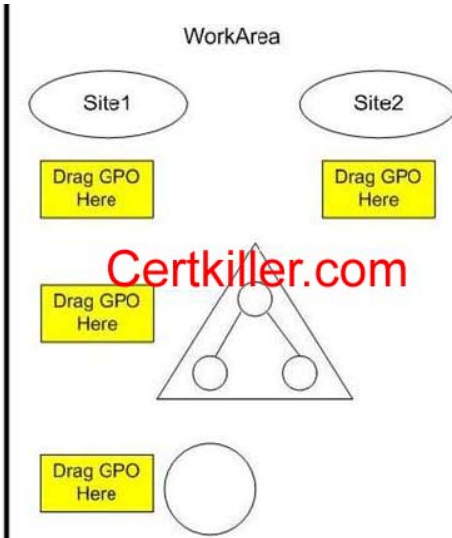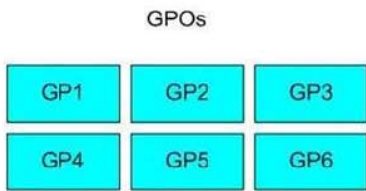You need to deploy an antivirus application to all computers on the network without user intervention. You also need to deploy a special accounting application to user accounts in the Accounting OU without user intervention. The accounting application must be available to users in the accounting department 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.

Name	GPO section	Policy setting
GPO1	Computer Configuration	Assign the antivirus application
GPO2	User Configuration	Assign the antivirus application
GPO3	Computer Configuration	Assign the accounting application
GPO4	User Configuration	Assign the accounting application
GPO5	User Configuration	Publish the antivirus application
GPO6	User Configuration	Publish the accounting application

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.

WorkArea

GPOs

| GP1 | GP2 | GP3 |
| GP4 | GP5 | GP6 |

Site1   Site2

Drag GPO Here   Drag GPO Here

Drag GPO Here

Certkiller.com

Drag GPO Here

Answer:

WorkArea

GPOs

| GP1 | GP2 | GP3 |
| GP4 | GP5 | GP6 |

Site1   Site2

Drag GPO Here   Drag GPO Here

GP1

Certkiller.com

GP4
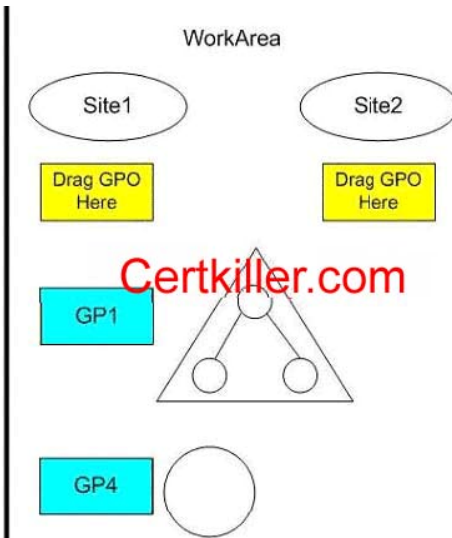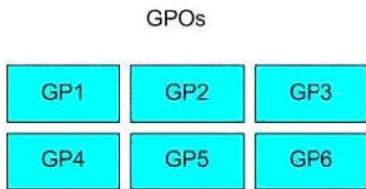
Explanation:
We need to apply the antivirus application to all computers on the network. This means we should configure Computer
Configuration section of the GPO to assign the antivirus application and link the GPO at the Domain level. Applications
can only be assigned to computers they cannot be published 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-23 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 181
You are the network administrator for Certkiller .com. Your network consists of a single Active Directory
domain named Certkiller .com. 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.
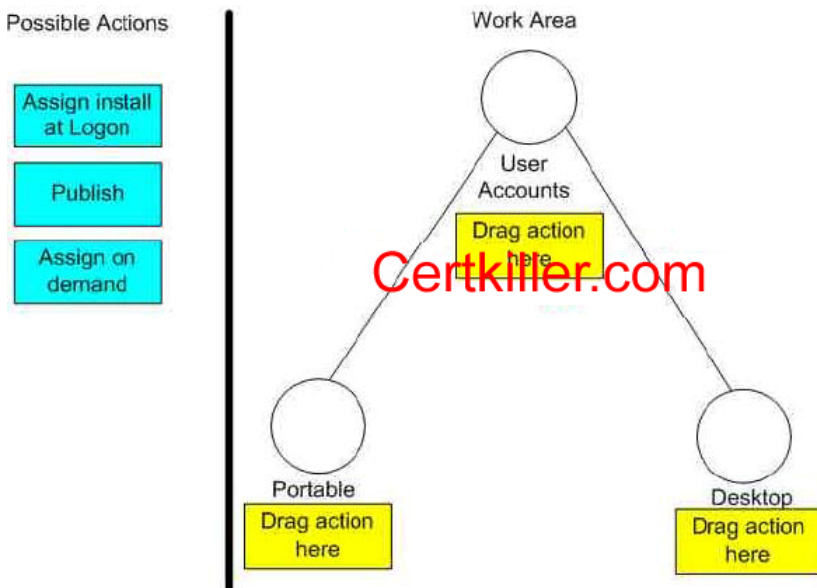
Answer:

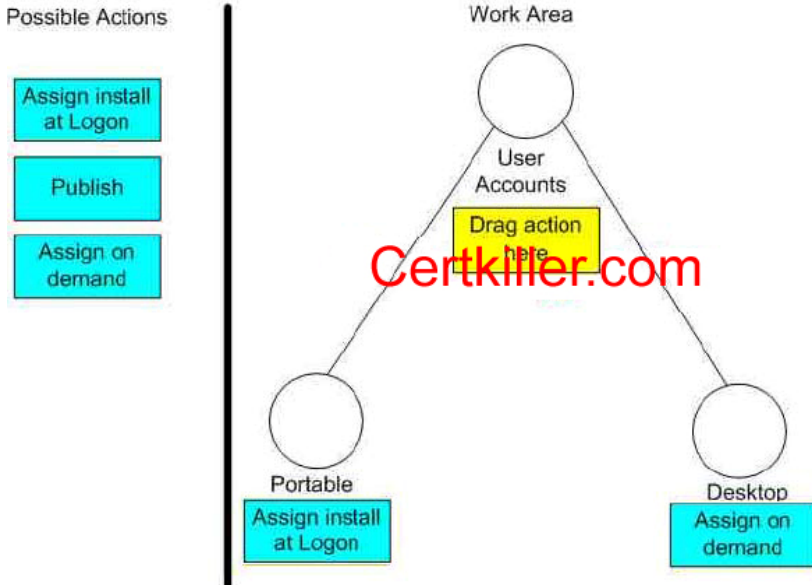Explanation:
The application must be installed on all client computers. However, some computers are portable computers. We
therefore should not apply the GPO at the domain level but at the OU level because we can only have the application
installed on the portable computers when users log on to the network 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:

Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-40 to 10-41

QUESTION 182
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain with a single site. All client computers in the domain run Windows XP Professional. The relevant
portion of the organizational unit (OU) structure is shown in the OU structure exhibit.
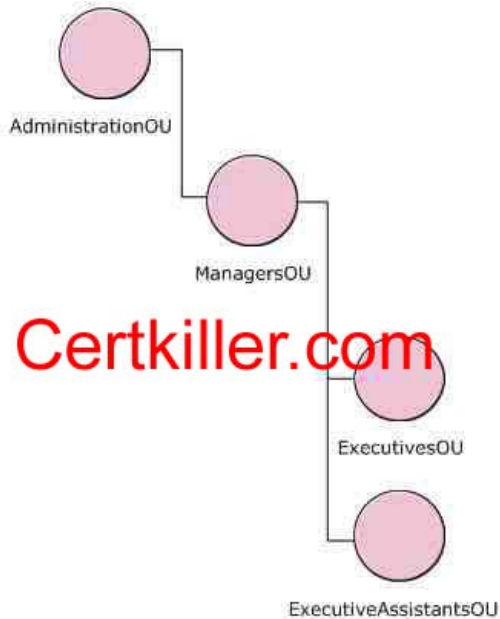
The user accounts for all managers are located in Managers OU.

You need to deploy a new application. You create a new Group Policy object (GPO) that assigns the .msi application package to user accounts. You link the GPO to the domain. You configure the permissions on the GPO as shown in the Security Settings exhibit.
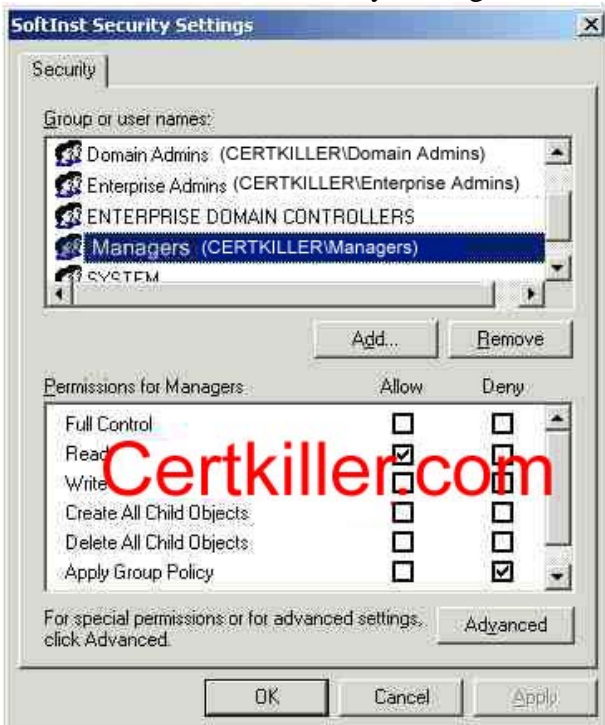
You then remove the Authenticated Users builtin
group from the permissions on the GPO.

The application package is installed on the client computers of all users who are not managers. Managers indicate that they want to have the application installed as well.

You need to configure the GPO so that the application is installed on the manager's computers.

What should you do?
A.Modify the permissions on the GPO by selecting theAllow Apply
Group Policypermission check box for the
Managers global group.
B.Modify the permissions on the GPO by clearing theDeny Apply
Group Policypermission check box for the
Managers global group.
C.Remove the link between the GPO and the domain.Link the GPO to Managers OU.
D.Remove the link between the GPO and the domain.Link the GPO to the site that contains the domain
controller.

Answer: A

Explanation: The Managers group hasDeny Apply
Group Policypermission. This prevents them from having the
GPO applied to them. We should assign them theAllow Apply
Group Policypermission.
Incorrect Answers:
B:TheAllow Apply
Group Policypermission needs to be explicitly granted. Thus, clearing theDeny Apply
Group
Policypermission check box won't do.
C, D:The Managers group hasDeny Apply
Group Policypermission. This prevents them from having the GPO
applied to them and is not dependant on which container the GPO is linked to.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 183
You are the network administrator for Certkiller .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. The TerminalServers 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 Readand
theAllow Apply
Group Policypermissions.
D.Modify the discretionary access control list (DACL) settings of the GPO to assign the computer accounts in the
TerminalServers OU theAllow Readand
theAllow Apply
Group Policypermissions.

Answer: A

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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-20,10-40 to 10-41,1-23 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 184
You are a network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers are Windows XP Professional computers that are members of the domain.
Certkiller wants to install a new application on only the computers where it is required. However, once installed on a particular computer, the application can be used by any user logged on to that computer.
The application is installed by using a Windows Installer package. You copy the .msi file to a shared folder on a file server. The shared folder is configured so that members of the Domain Admins group have the Allow Full
Control permission, and no other permissions are granted.
Certkiller wants to automate installation as much as possible. Users must not be able install unauthorized copies of the application.
You need to ensure that the application will be deployed in accordance with Certkiller 's requirements. You create a security group and assign this group the Allow Read
permission for the shared folder that contains

the .msi file.
Which two additional courses of action should you take? (Each correct answer presents part of the solution.
Choose two)
A.Make all users of the application members of the security group.
B.Make all unauthorized computers members of the security group.
C.Create a Group Policy object (GPO) that assigns the application to users.Link the GPO to the domain.Set
permissions on the GPO so that it applies only to the security group you created.
D.Create a Group Policy object (GPO) that publishes the application to users.Link the GPO to the domain.Set
permissions on the GPO so that it applies only to the security group you created.
E.Create a Group Policy object (GPO) that assigns the application to computers.Link the GPO to the
domain.Set
permissions on the GPO so that it applies only to the security group you created.

Answer: A, C

Explanation: A security group is a collection of users who have specific rights and permissions to resources.
Rather
than giving rights to perform certain tasks to individual users, and then setting permissions as to what resources
that user
can access, the rights and permissions are applied to the group. Any users who are members of the group then
acquire
this same level of security access. In doing so, collections of users are handled as a single unit, rather than as
individuals.
Thus to ensure that you accomplish the task at hand and staying within the requirements of the company, you
should
make all users of this particular application members of a security group and then create a GPO that will assign
the
application to these users. Obviously you need to link the GPO to the domain and then set the relevant
permissions to
apply to only the newly created security group.
Incorrect Answers:
B:If we created a security group that contains all unauthorized computers, we would need to apply theDeny
Apply
Group **Policy**permission to that security group. The latter is not one of the options.
D: We need to assign the application to users, not publish it. Assigned applications appear on the user's desktop,
or start
menu, which is part of the user profile. This means that the application will not be available to other users who
log on to
the computer.
E: Assigning the application to computers would be wrong since it is users that you need to take into account
and it
could be that users have roaming profiles which might cause them to use all computers besides their own as
well.
Reference:
Michael Cross, Jeffery
A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 2, pp.
131-133
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-23 to 12-10, 12-13 to 12-28,12-34 to 12-39

QUESTION 185
You are the administrator of the Certkiller company network.The network consists of a single Active
Directory domain named Certkiller .com.The network includes 20 servers running Windows Server 2003 and
400 client computers running Windows XP Professional.All client computers are in 12 organisational units
(OU) organised by company department.All member server computer accounts are in an organisational unit
(OU) named Servers.All user accounts are in an organisational unit (OU) named Employees.
You need to install an application on all client computers in the domain.The application must not be installed
on any 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.Use gpedit.msc to create a Group Policy object (GPO) to assign the application to the computers.Link this
GPO to
the domain.Configure the Domain Controllers OU and the Servers OU to block policy inheritance.
B.Use gpedit.msc to create a Group Policy object (GPO) to assign the application to the computers.Link this
GPO to
the domain.Configure permissions on the GPO so that all servers and domain controller accounts are denied the
permissions to read and apply the GPO.
C.Use gpedit.msc to create a Group Policy object (GPO) to assign the application to the users.Link this GPO to
the
domain.Configure the Domain Controllers OU and the Servers OU to block policy inheritance.
D.Use gpedit.msc to create a Group Policy object (GPO) to assign the application to the users.
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

Explanation: The software can be installed on all the client computers, but not the domain controllers or
member
servers.Because the client computers are in 12 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 permissionsto read
and
apply the GPO 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:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-23 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 186

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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 user accounts must have passwords that are at least eight characters in length and most 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 polices need to be linked to the same location, use the source labelled Both GPOs.

GPOs

Software GPO

Password GPO

Both GPOs

Active Directory

Certkiller.com

Drag GPO Here

Certkiller.com

Accounting

Drag GPO Here

Research

Drag GPO Here

Drag GPO Here

AP

AR

Answer:

GPOs

Software GPO

Password GPO

Both GPOs

Active Directory

Certkiller.com

Password GPO

Certkiller.com

Accounting

Software GPO

Research

Drag GPO Here

Drag GPO Here

AP

AR

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
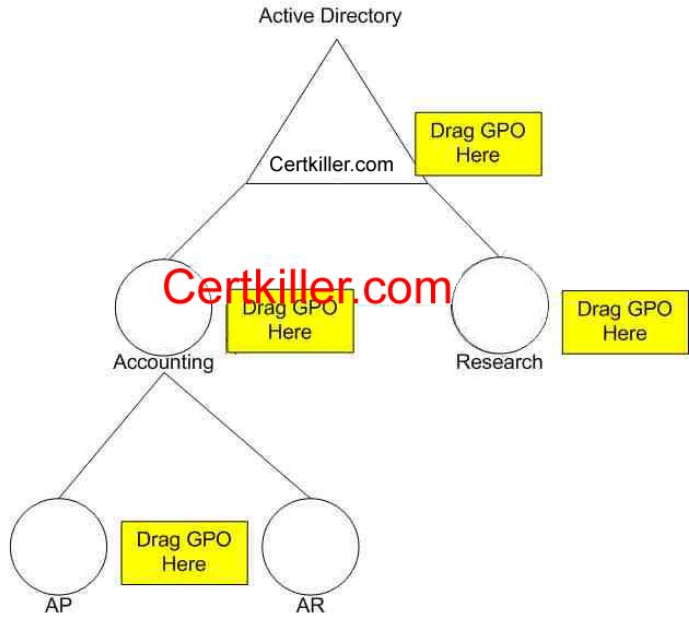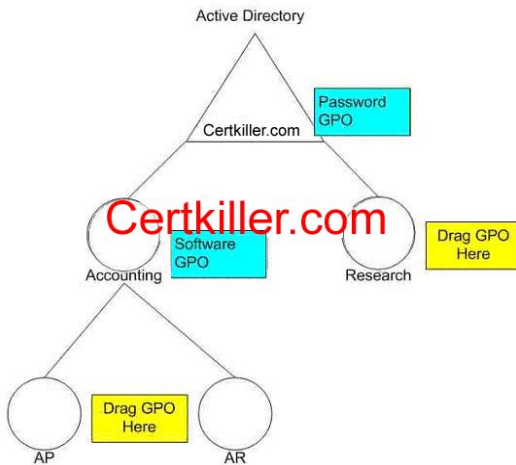users. You plan to create a GPO named Software to install the accounting application.The software GPO can be
applied to the Accounting OU.This GPO will also apply to the AP and AR OUs (which also contain accounts users).
The research department user accounts must have passwords that are at least eight characters in length and most be
changed every 30 days. There are no specific password requirements for any other users in the Certkiller .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.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-23 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 187
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows 2000 mixed. The domain includes an organizational unit (OU) named Marketing. Computer accounts for client computers in the marketing department are located in the Marketing OU. Each client computer runs Windows NT Workstation 4.0, Windows 2000 Professional, or Windows XP Professional.
You need to automatically deploy a new software package to all Windows 2000 Professional client computers in the Marketing OU. You create a Group Policy object (GPO) and link it to the Marketing OU.
What else should you do?
A.Configure the GPO to assign the software package under the Computer Configuration section, under Software
Settings.Modify the discretionary access control list (DACL) of the GPO to assign the Authenticated Users group the
Allow-Readand theDeny- Apply Group Policypermissions.
B.Configure the GPO to assign the software package under the Computer Configuration section, under Software
Settings.Configure a WMI filter to include Windows 2000 Professional.
C.Configure the GPO to assign the software package under the Computer Configuration section, under Software
Settings.Disable Computer Configuration settings on the GPO.
D.Configure the GPO to publish the software package under the User Configuration section, under Software
Settings.
Modify the discretionary access control list (DACL) of the GPO to assign only the Windows 2000 Professional computer accounts theAllow Readand theAllow Apply Group Policypermissions.

Answer: B

Explanation: This question is tricky because Windows 2000 clients cannot process WMI filters.They will ignore the
filters and install the software.However, the Windows XP clients will process the WMI filter and so will not install the
software.
The NT clients will not process the group policy at all, and so will not install the software.This fulfils the requirements in
the question.
Incorrect Answers:
A:This will deny the group policy, so the policy will not apply to anyone.
C:This will disable the part of the GPO with the required settings.Therefore, the software won't install on any computers.
D:The software needs to be assigned to the computers, not the users.This answer could work if the software was

assigned under the Computer Configuration section, but it's an impractical way of doing it.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-20 to 10-21,11-6

QUESTION 188
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains 10 file servers running Windows Server 2003.All the file servers are located in an organizational unit (OU) named TK.
You discover that a virus is infecting files on the file servers.You locate an antivirus application that will remove the virus and install a patch that prevents the virus from reinfecting
the servers.The application and
its updates are available as .msi files.The file servers must remain available because users are currently using the file servers for critical processes.
You need to ensure that the file servers are protected from viruses. You want to accomplish this task by using the minimum mount of administrative effort.
Which action or actions should you take to achieve this goal?
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.

Actions, Select from these	Place here
Create a Group Policy Object (GPO) to set the Group Policy refresh interval to be 0, and link the GPO to the CKOU	Place first action here
Create a Group Policy Object (GPO) to distribute the antivirus .msi files, and link the GPO to the CKOU.	Place second action here
Log on interactively and install the .msi file on each server	Place third action here
Log on interactively and run the secedit/ overwrite command on each server	Place fourth action here

Answer:

Explanation:
First action:Log on interactively and install the .msi file on each server.
When assigning applications to computers, the application is installed the next time the computer boots up. Applications
assigned to computers are not advertised, but are installed with the default set of features configured for the package.
The question states thatthe file servers must remain available because users are currently using the file servers for critical processes.For this reason, we cannot use a group policy to assign the software (we cannot reboot
the computers).Therefore, we must manually install the software on the computers.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 1-23 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 189

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

Certkiller wants all users to have Microsoft Word available on their client computers. Certkiller does not want to install Word on domain controller 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 servers 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

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:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 600-604
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 12-13 to 12-28

QUESTION 190
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. One of the domain controllers is configured as a subordinate enterprise certification authority (CA). Certkiller also has an offline root C
A. All
client computers run Windows XP Professional.
Certkiller does business with a distributor named Coho Vineyard. Users at Certkiller frequently access secured Web sites at Coho Vineyard. These sites are secured by using certificates issued by an enterprise CA at Coho Vineyard.
Users at Certkiller report that they receive security alerts from the Web browser whenever they try to access secured Web sites at Coho Vineyard. Users can access the sites after they acknowledge the warnings, but many choose to cancel the operation in order to be sure that the network is secure.
You need to configure the Certkiller network to prevent these security alerts from appearing when accessing the secured Web sites at Coho Vineyard.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A.Obtain a copy of the Coho Vineyard root certificate from Coho Vineyard.
B.Issue a certificate to the Coho Vineyard Web server from the Certkiller enterprise CA.
C.Import the certificate into the Trusted Root Certification Authorities section of the Default Domain Policy Group
Policy object (GPO).
D.Place the Coho Vineyard secured Web sites in the list of trusted sites in the Internet Explorer Maintenance section of
the Default Domain Policy Group Policy object (GPO).

Answer: A, C

Explanation: The certificate is issue by another entity, we need to trust the certificates issued by that entity. To do this
we need to place a copy of the certificate inTrusted Root Certification Authorities section of the Default Domain Policy
Group Policy object (GPO).
Incorrect Answers:
B:There is already a certificate issued by the Cohovinyards C
A. we do not need to issue another certificate.
D:The Internet Explorer Maintenance section of theDefault Domain Policy Group Policy object is not responsible for
maintaining certificates. It is used to administer and customize Internet Explorer on Windows Server 2003 computers.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 460-464, 470-473.
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,p.13-9

QUESTION 191
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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 NetworkSecurity.
B.Link NetworkSecurity to the Processing OU.Remove the link from NetworkSecurity to the domain.
C.Modify the discretionary control list (DACL) for NetworkSecurity to assign all computer accounts on the Processing
OU theAllow Readand theAllow Supply Group Policypermissions.
D.Modify the discretionary access control list (DACL) for NetworkSecurity to assign the Authenticated Users group
theDeny Apply Group Policypermission and to assign all of the computer accounts in the Processing OU theAllow Readand
theAllow Apply Group Policypermissions.

Answer: B

Explanation: We need to ensure that the NetworkSecurity GPO is applied to computers in the Processing OU; however, the NetworkSecurity GPO is linked to the domain. We should link the NetworkSecurity GPO to the Processing OU, not the domain.
Incorrect Answers:
A:Linking theNetworkSecurity GPO to the Processing OU won't work if the NetworkSecurity GPO is still linked to the
domain. We need to also remove the link to the domain.
C, D:The NetworkSecurity GPO is linked to the domain and is thus applied to all computers. Assigning all computer
accounts on the Processing OU theAllow Readand
theAllow Supply
Group Policypermissions won't stop the
GPO from applying to all computers in the domain.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 192
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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 securityrelated
registry entries to all of the computer accounts in the Accounting
OU. You create an ADM template named CustomSecuritySettings that includes the security-related registry entries.
You need to import the CustomSecuritySettings template into the Custom ADM Template GPO so that you can enable the new policy settings in the CustomSecuritySettings template.
Where should you import the CustomSecuritySettings template?
To answer, select the appropriate section of the GPO in the dialog box.
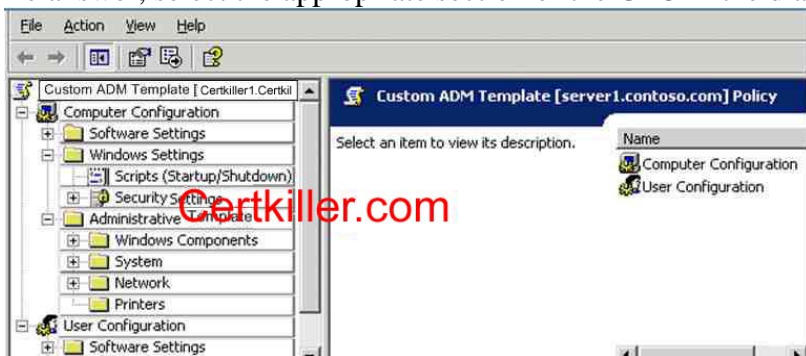
Answer:

Explanation: Select "Security Settings" under Computer Configuration.

To import theCustomSecuritySettingssecurity template into the Custom ADM Template GPO, in the console where
you manage local or nonlocal Group Policy settings, click the Custom ADM Template GPO to which you want to
import the security template. Then, in the console tree, right-clickSecurity Settings, and then clickImport Policy. In
theImport Policy Fromdialog box, click theCustomSecuritySettingssecurity template you want to import, and then
clickOpen.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 13-57 to 13-65,13-65-13-66

QUESTION 193
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain.
All servers run Windows Server 2003. All client computers run Windows XP Professional. All computer accounts for the client computers are located in an organizational unit (OU) named Workstations.
Certkiller 's written security policy states the following requirements:
1.Users must be members of the local Power Users group on all client computers.
2.Users must not be members of the local Administrators group on any client computers.
3.Users must not have any administrative rights to member servers or domain controllers in the domain.
4.The Power Users group membership cannot be modified by members of the local Administrators group on any client computer.
You need to provide automatic assignments of required group memberships for the users on the client computers.
What should you do?
A.Create a logon script that adds the Domain Users group to the local Power Users group when the user logs on.Link
the logon script to the Workstations OU.
B.Create a startup script that adds the Domain Users group to the local Power Users group when the client computer
starts.Link the startup script to the Workstation OU.
C.Create a new Group Policy object (GPO) named GPO1.Configure the Restricted Groups option in GPO1 to add the
Domain Users group to the Power Users group.Link GPO1 to the Workstation OU.
D.Create a new Group Policy object (GPO) named GPO1.Configure the Restricted Groups option in GPO1 to add the
Domain Users group to the Power Users group.Link GPO1 to the domain.

Answer: C

Explanation: We need to move all users to the Power users group. We can do this by usingthe Restricted Groups
option of a GPO to add the Domain Users group to the Power Users group. Restricted Groups ensures that group
memberships are set as specified. Groups and users not specified in Restricted Groups are removed from the

group. In
addition, the reverse membership configuration option ensures that each restricted group is a member of only those
groups specified in the Member Of column. This GPO must be linked to all client computers as users must not have any
administrative rights to member servers or domain controllers in the domain. The client computers are in the Workstations OU.
Incorrect Answers:
A,B:Usingthe Restricted Groups option would be a better solution than using logon scripts or startup scripts.
D:We should link the GPO the Workstations OU, not the domain as it should only be applied to client computes and
not server computers. Linking the GPO to the domain will result in the GPO being applied to client computers as well as
to server computers.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-40 to 10-41,13-6 to 13-7

QUESTION 194
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers that are not domain controllers are located in an organizational unit (OU) named Servers.
The security department is responsible for defining security requirements for servers. You are responsible for configuring Certkiller 's servers. The security department provides you with security settings that you must apply to new and existing servers that are not domain controllers. You configure a Windows Server 2003 computer named Certkiller 1 with these settings.
You need to apply the security settings in compliance with the security department's requirements.
What should you do?
A.Export the security settings for Certkiller 1.Import the settings to a Group Policy object (GPO) linked to the Servers
OU.
B.Create a script by running thenetsh dumpcommand on Certkiller 1.Create a Group Policy object (GPO), link to the
GPO to the Servers OU, and configure the GPO to apply the script as a startup script.
C.Configure Synchronization Manager on Certkiller 1 to perform a synchronization task daily.
D.Export the security settings for Certkiller 1.Configure File Replication service (FRS) to copy the .ini file to the
systemroot on each server.

Answer: A

Explanation: You need to apply the settings to all servers that are not domain controllers. All these servers are in the
Servers OU and you have applied the security settings to Certkiller 1. All you need to do now is export the settings to a

custom template and import to a GPO that is linked to the Servers OU.
Incorrect Answers:
B:Thenetsh dumpcommand dumps the network configuration to a file, not the security settings.
C:We need to apply the security settings to the other servers. This can't be accomplished by synchronizing.
D:Copying the exported file to the systemroot of each server will not apply the settings to the server. We need to apply
it through a GPO.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-40 to 10-41,13-57 to 13-62

QUESTION 195
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The domain contains an organizational unit (OU) named Research. All users
who have user accounts in the Research OU use portable computers that run Windows XP Professional.
You create a Group Policy object (GPO) named PowerManagement and link it to the Research OU. You
configure the PowerManagement GPO to enable the Prompt for password on resume from hibernate
/suspend policy.
A user named Sandra has a user account in the Research OU. Sandra reports that she is not prompted for a
password when her computer resumes hibernation.
You need to ensure that Sandra immediately has password protection for her portable computer when
resuming from hibernation mode.
What should you do?
A.Instruct Sandra to run thegpupdatecommand from her computer.
B.Instruct Sandra to run thegpresultcommand from her computer.
C.Instruct Sandra to send a Remote Assistance invitation to you.Take control of Sandra's compute and run
thesecedit
/analyzecommand.
D.Instruct Sandra to send a Remote Assistance invitation to you.Take control of Sandra's computer and run the
gpresultcommand.

Answer: A

Explanation: Although the GPO has been configured, some laptops may have not been online to be updated
with the
GPO policy or there could have been network connectivity problems that prevented some laptops from getting
the
policy. All problems aside, Sandra's laptop should get the update at the next GPO refresh interval or Sandra can
get
refresh immediately by running the gpupdate command form her computer.
Incorrect Answers:
B, D:The Gpresult commandline
tool allows you to create and display an RSoP query, which can be used to analyze
the cumulative effects of GPOs, through the command line. It also provides general information about the
operating

system, user, and computer.

C:The secedit command has been replaced by gpupdate in Windows Server 2003.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-44 to 10-21,11-4,11-6,11-19 to 11-22

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,p. 797

QUESTION 196

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. Each client computer runs either Windows 2000 Professional or Windows XP Professional.

All desktop computers have computer accounts in an organizational unit (OU) named Certkiller Desktops, and all portable computers have computer accounts in an OU named Certkiller Portables. All employees have user accounts in an OU named Certkiller Users.

A written Certkiller policy requires that different Encrypting File System (EFS) policies be applied to portable computers and to desktop computers. In addition, policy settings in the Default Domain Policy Group Policy object (GPO) must apply to all computers.

You create two new GPOs named DesktopEFSPolicy and PortableEFSPolicy to be applied to desktop computers and portable computers, respectively. You configure each GPO to contain the policy settings required by the written Certkiller policy.

You need to ensure that the written Certkiller policy is enforced.

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

A.Link the DesktopEFSPolicy GPO to the Certkiller Desktops OU.Link the PortableEFSPolicy GPO to the Certkiller

Portables OU.

B.In the Default Domain Policy GPO, assign the Domain Users security group theDeny Full

Controlpermission.

Assign the Domain Admins security group theAllow Full

Controlpermission.

C.Link the DesktopEFSPolicy GPO and the PortableEFSPolicy to the domain.Configure the Certkiller Desktops OU

and the Certkiller Portables OU to block Group Policy inheritance.

D.Enable theNo Overridesetting for the Default Domain Policy GPO, the DesktopEFSPolicy GPO, and the PortableEFSPolicy OU.

Answer: A, D

Explanation: You want the Default Domain Policy settings to apply to all computers, so you must configure the No

Override, or else lower GPO settings with the Block Policy Inheritance will negate the particular policy from above.

Also the same is true for the OU level GPOS that are configured. Any lower GPOs configured on child OUs with Block

Policy inheritance will negate policy from a higher level set GPO policy.

Incorrect Answers:

B:The GPO must be applied based to computer type, not user group.

C:Lower GPO settings with the Block Policy Inheritance will negate the particular policy from above.

Reference:

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-16 to 10-20,10-40 to 10-41

QUESTION 197

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. One of the domain controllers is configured as an enterprise root certification authority (CA). All client computers run Windows XP Professional.

Certkiller uses IPSec to secure communications between computers in Certkiller and computers at other companies. These IPSec connections require computer certificates. Your IPSec policies require every computer to be able to make an IPSec connection when connecting to other computers.

You need to configure the network so that all computers can make IPSec connections.

What should you do?

A.In the computer settings section of the Default Domain Policy Group Policy object (GPO), configure the domain

members to always digitally encrypt or sign secure channel data.

B.Create a new automatic certificate request in the computer settings section of the Default Domain Policy Group Policy

object (GPO),

C.Obtain a new computer certificate from a public C

A. Import a copy of this certificate into the Trusted Root

Certification Authorities section of the Default Domain Policy Group Policy object (GPO).

D.Issue a new computer certificate from your enterprise C

A. Place a copy if this certificate on an internal Web page.

Instruct users to install this certificate in their trusted certificate store the first time they need to make an IPSec connection.

Answer: D

Explanation: Enterprise CAs is integrated into the Active Directory directory service. They use certificate templates,

publish their certificates and CRLs to Active Directory, and use the information in the Active Directory database to

approve or deny certificate enrollment requests automatically. Because the clients of an enterprise CA must have access

to Active Directory to receive certificates, enterprise CAs are not suitable for issuing certificates to clients outside the

enterprise.Enterprise CAs requires and uses Active Directory to issue certificates, often automatically. AN IPSec

connection comprises of two modes: Main mode and Quick mode.

Main Mode is the first part of an IPSec connection. In Main Mode, each computer authenticates to the other and then

IKE is used to calculate the master key. All other keys are generated from the master key. An IKE security association

(SA) is created over which Quick Mode can be negotiated.

Quick Mode is the second phase of IPSec. In Quick Mode, agreement is reached for the encryption, integrity algorithms, and other policy settings. Two SAs are created, one incoming and one outgoing.

Incorrect answers:

A:Always digitally encrypting or signing secure channel data does not necessarily ensure the ability to make IPSec

connections.

B:An automatic certificate request in the computer settings section of the Default Domain GPO is not the solution.

C:Obtaining a new certificate from a public CA is not going to ensure that all computers will have the ability to make

IPSec connections. What is needed is to have a new computer certificate issued from your enterprise CA which should

be installed on users' trusted certificate store.

Reference:

J. C. Mackin, Ian McLean, MCSA/MCSE selfpaced

training kit (exam 70291):

Implementing, Managing, and

Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington,

2004, p.11: 88

James Chellis, Paul Robichaux, and Matthew Sheltz, MCSA/MCSE: WindowsServer 2003 Network Infrastructure

Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2004,p. 11: 15

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, p. 612

QUESTION 198

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

User accounts are configured as local administrators so that users can install software. A desktop support team supports end users. The desktop support team's user accounts are all members of a group named Support.

You create a software restriction policy that only prevents users from running registry editing tools by file hash rule. You apply the policy to all user accounts in the domains.
The desktop support team reports that when they attempt to run registry editing tools, they receive the following error message:
"Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator".
You need to ensure that only the desktop support team can run registry editing tools.
What should you do?
A.Configure the software restriction policies to be enforced for all users except local administrators.
B.Make users members of the Power Users group instead of the Administrators group.
C.Use a logon script to copy the registry editing tools to the root of drive C.Assign the Domain Admins group theAllow
Readpermission
for the registry editing tools in the new location.
D.Filter the software restriction policy to prevent the Support group from applying the policy.

Answer: D

Explanation: We can prevent the software restriction policy from applying to the support group by simply assigning the
support group the Deny Read
and/or the Deny Apply
group policy permission.
Incorrect answers:
A:Theusers are local administrators. The policy must apply to the local administrators.
B:The policy applies to all users. It will still apply to the support group. Changing the local users group membership will
have no effect on the policy.
C:The software restriction policy is using a hash rule to prevent the use of the registry editing tools. It doesn't matter
where the tools are located, they still won't run.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, pp. 591-593

QUESTION 199
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 computers and Windows XP Professional client computers. The domain contains two organizational units (OUs) named Sales and Marketing. Both OUs have multiple Group Policy Objects (GPOs) linked to them.
The Sales OU needs to be moved under the Marketing OU.

You need to find out which objects in the Sales OU are adversely affected by GPOs linked to the Marketing OU.
You need to achieve this goal without disruption to users.
What should you do?
A.Use Resultant Set of Policy (RSoP) in logging mode for the Marketing OU.Review the policy results for the users in
the OU.
B.Use Resultant Set of Policy (RSoP) in logging mode for the Sales OU.Review the policy results for the users in the
OU.
C.Use Resultant Set of Policy (RSoP) in planning mode for the Marketing OU.Choose the Sales OU to simulate policy
settings.
D.Use Resultant Set of Policy (RSoP) in planning mode for the Sales OU.Choose the Marketing OU to simulate policy
settings.

Answer: D

Explanation: We need to view the effective group policy without actually applying the group policy and disrupting the
users.For this, we can use RSoP in planning mode.In this mode, you can determine how policy settings are applied to a
target, and then analyze the results before deploying a change to Group Policy.
In logging mode, you can assess which policy settings have been applied or failed to apply to a particular target (users
or computers in Active Directory). Group Policy clientside
extensions have a WMI interface that writes information
(known aslogging mode data)about their policy settings to a CIMOM database. You can use the RSoP user interface to
query the CIMOM database for policy information
Incorrect Answers:
A:We need to use planning mode, not logging mode.
B:We need to use planning mode, not logging mode.
C:We need to test the effects of applying the Marketing OU policies to the Sales OU, not vica versa.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, p. 591
MS Knowledge Base article323276:HOW TO: Install and Use RSoP in Windows Server 2003
Server Help:RSoP overview

QUESTION 200
You are the network administrator for Fabrikam, Inc. The network consists of a single Active Directory domain named Certkiller .com that 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.
A new user named Dr. King reports that his Windows desktop is different from others in the company and that he does not have access to the same applications as other users. You discover that none of the user settings from any GPOs are in effect in Dr. King's computer after Dr. King logs on. You instruct Dr. King to run the gpresult command, and he reports that he receives the following error message: "INFO: The group policy object does not exist".
You run the gpotool command on the domain controller and receive the output shown in the exhibit.

You need to ensure that Group Policy settings can be applied correctly.
What should you do?
A.Run thegpupdate /forcecommand on the domain controller.
B.Run thegpupdate /forcecommand on Dr. King's computer.
C.Restore the system state on the domain controller from a valid backup.
D.Restore the backup state on Dr. King's computer from a valid backup.

Answer: C

Explanation: We can see from the exhibit that there is a problem with the group policy.It seems to have become corrupted.To restore the group policy, we'll need to restore the system state data on a domain controller.
Incorrect Answers:
A, B:Thegpupdate /force
D:The GPO resides on the domain controller, not on the local computer.
Reference:
Microsoft Knowledge Base Article 216359:Troubleshooting Group Policy Application Problems.
Microsoft Knowledge Base Article 250842:Troubleshooting Group Policy Application Problems.
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 11-3,11-19 to 11-22
Michael Cross, Jeffery
A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active
Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 620-626

QUESTION 201
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com All client computers run Windows XP Professional.
Certkiller 's main office is located in Cape Town. You are a network administrator at Certkiller 's branch office
in Nairobi. You create a Group Policy object (GPO) that redirects the Start menu for users in the Nairobi
branch office to a shared folder on a file server.
Server user in Nairobi report that many of the programs that they normally use are missing from their Start
menus. The programs were available on the Start menu the previous day, but did not appear when the users
logged on today.
You log on to one of the client computers. All of the required programs appear on the Start menu. You verify
that users can access the shared folder on the server.
You need to find out why the Start menu changed for these users.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose
two)
A.In the Group Policy Management Console (GPMC), select the file server that hosts the shared folder and a
user
account that is in the Domain Admins global group and run Resultant Set of Policy (RSoP) in planning mode.
B.In the Group Policy Management Console (GPMC), select one of the affected user accounts and run
Resultant Set of
Policy (RSoP) in logging mode.
C.On one of the affected client computers, run thegpresultcommand.
D.On one of the affected client computers, run thegpupdatecommand.
E.On one of the affected client computers, run theseceditcommand.

Answer: B, C

Explanation: We need to view the effective group policy settings for the users or the computers that the users
are using.
We can use gpresult of RSoP.Gpresult displays Group Policy settings and Resultant Set of Policy (RSoP) for a
user or
a computer.
RSoP provides details about all policy settings that are configured by an Administrator, including
Administrative
Templates, Folder Redirection, Internet Explorer Maintenance, Security Settings, Scripts, and Group Policy
Software
Installation.
Incorrect Answers:
A:We need to test the effective policy from a user's computer, not the file server.
D:Gpupdate is the tool used to refresh the policy settings in Windows XP and Windows Server 2003.
E:Secedit is the tool used to refresh the policy in Windows 2000 professional and server editions.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 11-3,11-19 to 11-22

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 620-626

QUESTION 202

You are the administrator of the Certkiller company network.The network consists of a single active directory domain.The network includes 10 servers running Windows Server 2003 and 500 client computers running Windows XP Professional.

You create a Group Policy object (GPO) that redirects the Start menu for users to a shared folder on a file server.

Some users report that many of the programs that they normally use are missing from their Start menus.

You log on to a client computer named Client1.All of the required programs appear on the Start menu.The users are able to connect to the shared folder.You suspect that changes made to one of more GPOs are causing the problem.

You need to find out why some Start menu items are not appearing for some users.

What should you do?

A.On the file server that hosts the shared folder, run thegpresultcommand.

B.On one of the affected client computers, run thegpresultcommand.

C.On one of the affected client computers, run thegpupdatecommand.

D.On one of the affected client computers, run theseceditcommand.

Answer: B

Explanation: Because you can apply overlapping levels of policies to any computer or user, the Group Policy feature

generates a resulting set of policies at logon.Gpresultdisplays the resulting set of policies that were enforced on the

computer for the specified user at logon.

Incorrect Answers:

A:We need to run the gpresult command on one of the affected client computers, not the server that hosts the shared

folder.

C:The gpudate command refreshes the group policies applied to a computer or user.We need to use the gpresult command to determine the result of all the policies that apply to the computer.

D:The secedit command is the command line version of the Security Configuration and Analysis utility.This has nothing

to do with the effects of group policies.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

QUESTION 203

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

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

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

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

You need to create one or more Group Policy objects (GPOs) to implement the security settings. You want to
minimize the amount of administrative effort required when changes are requested by the various operations
groups.
What should you do?
A.Create a GPO and import the following templates in the following order: Baseline.inf, Certkiller
Sec.inf.Create a GPO
for each server role and import only the specific template for that role into each respective GPO.
B.Create a GPO and import the following templates in the following order: Certkiller Sec.inf,
Baseline.inf.Create a GPO
for each server role and import only the specific template for that role into each respective GPO.
C.Create a GPO for each server role and import the following templates in the following order: Baseline.inf,
specific
server role template, Certkiller Sec.inf.

D.Create a GPO and import the following templates in the following order: Certkiller Sec.inf, Certkiller DB.inf, Certkiller File.inf, Baseline.inf.

Answer: A

Explanation: Windows Server 2003 processes GPOs from the bottom of the list to the top of the list, with the topmost
GPO having the final authority. Because policies contained in GPOs will, by default, overwrite policies of previously
applied, we would need to import the Baseline.inf before the Certkiller Sec.inf template.
Incorrect Answers:
B:Because policies contained in GPOs will, by def
import the Baseline.inf before the Certkiller Sec.inf template.
C, D:Because we need to import templates specific to each of two server roles, we need a separate GPO for each
server role.
Reference:
Dan Holme, and Orin Thomas, MCSA/MCSE SelfPaced Training Kit: Upgrading Your Certification to Microsoft
Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296,Chapter 5

QUESTION 204
You are the network administrator for Certkiller .com. 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 theDeny Readpermission
for unused GPOs.
B.Assign the Testuser account theDeny Write
gpoLinkpermission for the domain.
C.Create a GPO to enable theNegative DC Discovery Cache Setting, specify the setting to be 60 seconds, and
apply it to the client computers.
D.Create a GPO to enable theGroup Policy refresh interval for computerssetting, specify the update rate to be 120
minutes, and apply it to the client computers.

Answer: A

Explanation: Group Policy is still processed but not applied when theDeny Apply
Group Policypermission is
assigned. TheDeny Readpermission
will ensure that the GPO is not processed. This will improve logon times.
Incorrect Answers:
B:There is notWrite gpoLinkpermission.
C:TheNegative DC Discovery Cache Settingspecifies 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:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-20,10-40 to 10-41

QUESTION 205
You are the network administrator for Certkiller .com. 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 Lisa is transferred out of the engineering department. The user account for Lisa is moved into
an OU named Research. Lisa reports that the application is still installed on her computer.
You must ensure that that the application is automatically uninstalled from Lisa'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 Lisa's user account back into the Engineering OU.Configure the software installation package so that the
software is uninstalled when Lisa's user account falls out of the scope of management.Ensure that Lisa logs on to the
network.Move Lisa's user account back into the Research OU.
B.Move Lisa's user account back into the Engineering OU.Modify the GPO so that the software installation package is
removed.Ensure that Lisa logs on to the network.Move Lisa's user account back to the Research OU.
C.Move the client computer object for Lisa's computer out of the EngineeringWorkstations OU.
D.Remove Lisa from the Engineers global group.

Answer: A

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 Lisa's user account back into the Engineering OU so that the application
applies to her again and Lisa must log on to the network for the GPO to apply. Then we can move Lisa's user account
back into the Research OU.The application will no longer apply to Lisa 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:The application applies to users not computers; theref
D:The GPO is applied at the OU. TheEngineers global group is not in the Engineering OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 12-3 to 12-10,12-16 to 12-20

QUESTION 206
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. All servers run Windows Server 2003. You deploy an application by using a
Group Policy object (GPO) that publishes an .msi file.
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: D, E

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 a
.msp file, or a .mst file.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 1-23 to 1-28,2-34 to 12-39

QUESTION 207
You are the network administrator for Certkiller .com. You are responsible for planning the deployment and configuration of applications by using Group Policy objects (GPOs). Your network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All user accounts are located in an organizational unit (OU) named Accounts. All client computers run Windows XP Professional and are located in an OU named Workstations.
All managers in the company need to use a management application. This application is sent by a hyperlink contained in an email
message to the users who require it. The managers need this application regardless of
the computer that they are using at any given time.
A software update for the application is now available.
You need to update the application on all computers that have the application installed.
What should you do?
A.Configure a GPO to install the software update by using a WMI filter. Link the GPO to the Accounts OU.
B.Configure a GPO that requires the installation of the software update. Link the GPO to the Workstations OU.
C.Create a .zap file for the software update, and configure a GPO to install the .zap file. Link the GPO to the Accounts
OU.
D.Configure a GPO to enable automatic updates and to install the software update. Link the GPO to the Workstations
OU.

Answer: B

Explanation: Configuring a GPO that requires the installation of the software update and linking that GPO to the
Workstations OUwill install the update only on workstations on which the application is installed.If the application is not
installed, the update will not be installed.
Incorrect Answers:
A:WMI filtering can be used to restrict the GPO scope to certain groups.
C:The manager requires the application regardless of what computer he uses. We should therefore link the GPO to the
computer container.
D:Automatic updates can only be configured for Windows Updates, not for applications.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-20 to 10-21,11-6,12-3 to 12-10,12-13 to 12-28,12-34 to12-39

QUESTION 208
You are the network administrator for Certkiller .com. The network consists of a singe Active Directory
domain. All servers run Windows Server 20003.
You create a Group Policy object (GPO) to publish an .msi file that installs a graphics application. The
company approve the use of a new graphics application to replace the old graphics application. The new

application is installed by using an .msi file. Current users can continue to use the old application, or they can start using the new application whenever they choose. To prevent support issues, both applications must not be installed at the same time.

You need to configure the user accounts so that users can migrate to the new application.

What should you do?

A.Create a new GPO to publish the new application. Configure the link for the new GPO to have a higher priority than
the GPO that installs the old application.

B.Create a new GPO to assign the new application. Disable the GPO that installed the old application.

C.Create a new GPO to publish the new application. Configure the GPO to upgrade and replace the existing application with the new application, but do not make it a requirement.

D.Copy the .msi file for the new application to the same location as the .msi file for the old application.

Answer: C

Explanation: We need to publish the application rather than assign it.If we assigned it, the new application will automatically install.The users must be able to use the old application if they want to.Publishing the application will give
the users the choice.They can install the new application by using the Add/Remove Programs control panel applet.To
prevent users running the old version and the new version, we can configure the published application to replace the old
version.

Incorrect Answers:

A:This will not cause the new application to replace the old application when it is installed.

B:If we assigned it, the new application will automatically install.The users must be able to use the old application if they
want to.

D:This will not install the new application or replace the old one.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 12-3 to 12-10,12-13 to 12-28,12-34 to 12-39

QUESTION 209

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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 Certkiller Computers.

Certkiller requires all computers to be kept uptodate
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 Certkiller Computers 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 Certkiller Computers 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: B, D

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 internalserver 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 Certkiller Computers 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 Certkiller Computers OU and not the domain.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-40 to 10-41
Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290):Managing and Maintaining a
Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, Washington, 2004, pp. 9-14 to 9-16

QUESTION 210
You are the network administrator for Certkiller .com. Certkiller consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computer accounts for the client computers are located in an organizational unit (OU) named Computer Accounts. All user accounts are located in an OU named User Accounts.
Software Update Services (SUS) is installed on your network. The SUS infrastructure is shown in the exhibit.
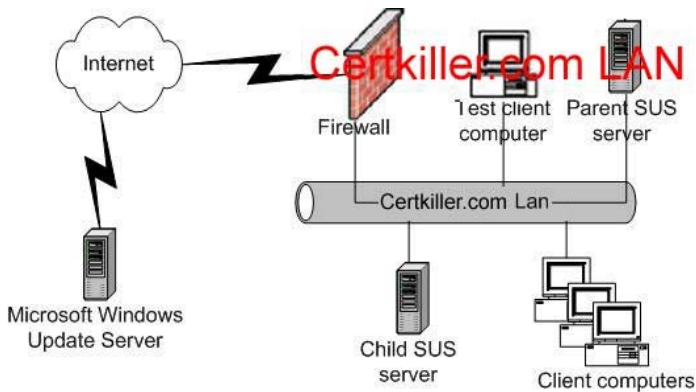
Updates that are deployed must not cause any conflicts or errors on the client computers.
You need to configure the client computers to download approved updates from the correct server.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A.Create a Group Policy object (GPO) to set the default package location to be the internal interface of the firewall.
B.Create a Group Policy object (GPO) to set the default package location to be the child SUS server.
C.Create a Group Policy object (GPO) to set the update service location to be the child SUS server.
D.Create a Group Policy object (GPO) to set the update service location to be the Microsoft Windows Update server.
E.Link the Group Policy object (GPO) to the User Accounts OU.
F.Link the Group Policy object (GPO) to the Computer Accounts OU.

Answer: C, F

Explanation: You will need to specify the child SUS server and to link the policy to the computer accounts OU.Only
approved updates can be downloaded and installed from the child SUS server.
Incorrect Answers:
A, B:We should use the update package not the default package.
D:Only approved updates must be downloaded. Specifying theMicrosoft Windows Update server will mean that all
updates will be downloaded.
E:Updates are applied tot the computer, not the user account.
Reference:
Dan Holme and Orin Thomas, MCSA/MCSE SelfPaced
Training Kit (Exam 70290):
Managing and Maintaining a
Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, Washington, 2004, pp. 9-14
to 9-16

QUESTION 211
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The domain controllers are located in three Active Directory sites. The domain
contains an organizational unit (OU) named Marketing. The Marketing OU contains two child OUs named
Sales and Research.
You need to disable the Windows Update service on all computers in the domain, with the exception of

computers in the Sales OU. You want to use the minimum number of Group Policy object (GPOs).
What should you do?
A.Create a GPO and link it to the domain.Configure the GPO to disable Windows Update under the User
Configuration section of the GPO.On the Sales OU, enable theBlock Policy inheritancesetting.
B.Create a GPO and link it to the domain.Configure the GPO to disable Windows Update under the User
Configuration section of the GPO.Enable theNo Overridesetting on the GPO.
C.Create a GPO and link it to all three Active Directory sites.Configure the GPO to disable Windows Update
under the
User Configuration section of the GPO.On the Sales OU, enable theBlock Policy inheritancesetting.
D.Create a GPO and link it to all three Active Directory sites.Configure the GPO to disable Windows Update
under the
User Configuration section of the GPO.Enable theNo Overridesetting on the GPO.

Answer: A

Explanation: You want to Windows update to run only on computers in the Sales OU. To do this you must
create two
GPOs: one for the domain and one for the Sales OU. Configure the domain GPO todisable Windows Updateand
block
policy inheritance on the GPO for the Sales OU.Windows Update is enabled by default so blocking inheritance
will
ensure that it is still applied to the Sales OU.
Incorrect Answers:
B:The no override option on the domain GPO will ensure that the settings in the domain GPO are not blocked at
the lower
level GPOs. This will mean that Windows Update is disabled for the entire domain.
C:This will work but creating a GPO at the domain level todisable Windows Update would require less
administrative
effort. This is thus not the best option.
D:Creating a GPO at the domain level todisable Windows Update would require less administrative effort.
Also,the no
override option on the Active Directory sites will ensure that the settings in the domain GPO are not blocked at
the
lower level GPOs. This will mean that Windows Update is disabled for all the sites.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 10-40 to 10-41

QUESTION 212
You are a network administrator for Certkiller . The network consists of a single Active Directory domain
Certkiller .com. The network contains Web servers that run Windows Server 2003.
You use Sysprep to create a baseline image for Web servers. You instruct a technician to install Windows
Server 2003 on 20 new Web servers by using the baseline image.
A new service pack is subsequently released.
You need to install the new service pack on all Web servers. You want to achieve this goal by using the

minimum amount of administrative effort.

What should you do?

A.Copy the service pack installation files to a shared folder.Install the service pack on each Web server from the shared

folder.

B.Create an organizational unit (OU) named Web servers.Create a Group Policy object (GPO) to assign the service

pack package to users.Link the GPO to the Web Servers OU.Move the Web servers into the Web Servers OU.

C.Create an organizational unit (OU) named Web Servers.Create a Group Policy object (GPO) to assign the service

pack package to computers.Link the GPO to the Web Servers OU.Move the Web servers into the Web Servers OU.

D.Create a Cmdlines.txt file for use with the baseline Sysprep image in order to run the service pack package.

Answer: C

Explanation: Aservice pack

is a software update package provided by Microsoft for one of its products. A service pack contains a collection of

fixes and enhancements packaged into a single self-installing archive file.

To distribute a service pack, create a shared folder and either extract the service pack to that folder or copy the

contents of the service pack CD to the folder. Then, using the Active Directory Users And Computers snapin,

create or select an existing GPO. Click Edit and the Group Policy Object Editor console appears, focused on the selected

GPO. Expand the Computer Configuration\Software Settings node. Right-click Software Installation and choose New,

then Package. Enter the path to the service pack's Update.msi file. Be certain to use a UNC format (for example,

\\Server\Share) and not a local volume path, such as Drive:\Path. In the Deploy Software dialog box, select Assigned.

Close the Group Policy Object Editor console. Computers within the scope of the GPO-in the site, domain, or OU

branch to which the policy is linked-automatically deploy the service pack at the next startup.

You can create a baseline security configuration in a GPO directly, or import a security template into a GPO. Link the

baseline security GPO to OUs in which member servers' computer objects exist.

Incorrect Answers:

A:Installing the service pack on each server would require a lot of administrative effort.

B:Service packs must be applied to the computers not the users.

D:Service packs can be applied without running the Sysprep image.

Reference:

Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293):Planning and Maintaining a Microsoft Windows Server

2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, Glossary.

Dan Holme and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290):Managing and Maintaining a

Microsoft Windows Server 2003 Environment, Microsoft Press, Redmond, Washington, 2004,Chapter 9

Dan Holme, and Orin Thomas, MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft
Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Microsoft Press, Redmond, Washington, 2004, Chapter 9.

QUESTION 213
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains an organizational unit (OU) named TerminalServers. You create two Group Policy objects (GPOs) named Certkiller Settings and SecuritySettings and link them to the domain. You then create another GPO named TS_Settings and link it to the TerminalServers OU.
Users report that when they run Internet Explorer on a terminal server, they cannot access approved Web sites. Users did not encounter any problems with running Internet Explorer on the terminal servers before the GPOs were created and linked.
You need to find out which GPO is the cause of the problem.
What should you do?
A.Log on to a terminal server and run thesecedit /analyzecommand.
B.Log on to a domain controller and run thequery termservercommand.
C.Log on to a domain controller and run Resultant Set of Policy (RSoP) in planning mode against the client computers.
D.Log on to a domain controller and run Resultant Set of Policy (RSoP) in logging mode against a terminal server.

Answer: D

Explanation: Use RSoP in logging mode to view the actual policy settings for a user on a computer. You can use RSoP
in logging mode to discover which policy settings are actually in effect for a particular user or computer, and find the
specific GPOs that applied those settings. You can also use the presult.exe commandline
tool to generate RSoP logging
data in a text format. Since the GPOs have been applied to the TerminalServers OU, you should run RSoP in logging
mode against a terminal server.
Incorrect Answers:
A:Thesecedit /analyzecommandallows you to analyze the security settings on a computer by comparing them against
the baseline settings in a database. It is not used to troubleshoot GPO application.
B:Thequery termservercommand displays a list of all terminal servers on the network.
C:Use the Resultant Set of Policy (RSoP) tool in planning mode to see the effects of group policy settings prior to
implementation. However, the GPOs have been applied to the TerminalServers OU, not the client computers. We
should run RSoP against the terminal servers.
Reference:
Michael Cross, Jeffery
A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, pp.
629,
631
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp. 11-3 to 11-24

QUESTION 214
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. The domain includes a Windows Server 2003 computer that runs Terminal
Services. The terminal server has a computer account in an organizational unit (OU) named Terminal
Servers.
A Group Policy object (GPO) named TS Settings is linked to the Terminal Servers OU. This GPO is
configured with settings that must apply when users are logged on to the terminal server. The company
wants users to have their normal settings when connected to the terminal server, except settings that
conflicts with the settings in the TS Settings GPO.
You discover that when users are logged on to the terminal server, they receive only the settings from the
TS Settings GPO, without any of their own settings.
You use the Group Policy Management Console (GPMC) to examine the configuration of the TS Settings
GPO. The relevant portion of the configuration is shown in the exhibit.
****MISSING****
You need to ensure that policy settings apply properly to users logging on the terminal server.
What should you do?
A.Enable theBlock Policy inheritancesetting for the Terminal Servers OU.
B.Disable theNo Overridesetting for the TS Settings GPO.
C.Modify the TS Settings GPO to use loopback processing inMergemode.
D.Disable theOnly allow local profilessetting in the TS Settings GPO.

Answer: B

Explanation: Group policies set toNo Overridecannot be blocked.This is part of the problem. Therefore you
should
disable the No Override setting for the TS settings GPO in order to ensure that policy settings apply properly to
users
logging on the terminal server.
Incorrect Answers:
A:Enabling theBlock Policy inheritance
setting for the Terminal Servers OU will prevent the application of GPOs higher in the hierarchy from being
inherited by
the Terminal Servers OU. Thus, only the TS Settings GPO will be applied.
C:Loopback is a new Group Policy setting that provides alternatives to the default method of obtaining the
ordered list
of GPOs whose user configuration settings affect a user. By default, a user's settings come from a GPO list that

depends
on the user's location in Active Directory. Loopback operates in replace mode or merge mode. In merge mode, user
settings that do not conflict with computer settings are applied. If there is a conflict between the two, the computer
settings override the user settings.
D:TheOnly allow local profilesis a new Group Policy option that permits a computer to ignore user settings in roaming
profiles.By default, when roaming profile users log on to a computer, their roaming profile is copied to the local
computer. If they have previously logged on to this computer, the roaming profile is merged with the local profile. When
the users log off this computer, the local copy of their profile, including any changes they have made, is merged with the
server copy of their profile. IftheOnly allow local profilessetting is enabled,the user receives a local profile, rather than
the roaming profile.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 582, 590
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004,pp.10-16 to 10-17,10-19 to 10-20
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/enus/
Default.asp?url=/resources/documentation/

QUESTION 215
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All users have user accounts in an organizational unit (OU) named CompanyUsers. The CompanyUsers OU is configured as shown in the exhibit.
MISSING
You discover that no Group Policy settings are being applied to most users when they log on to client computers in the domain. When administrators log on, they receive the appropriate Group Policy settings. You examine the event log on one of the client computers. You find the error message shown in the Event Properties exhibit:
MISSING
You need to correct the problem in the network so that Group Policy settings are applied for all users. What should you do?
A.Assign the SYSTEM account theAllow Full
Controlpermission for child objects in the CompanyUsers OU.
B.Assign the Authenticated Users group theAllow Read,
theAllow Read

All Properties, and theAllow List
Contentspermissions for the CompanyUsers OU.
C.Assign the Everyone group theAllow Readand
theAllow Apply
Group Policypermissions for the Default Domain
Controllers Policy Group Policy object (GPO).
D.Assign the Domain Users group theAllow Full
Controlpermission for the Default Domain Policy Group Policy
object (GPO).

Answer: C

Explanation: The Read permission allows the viewing of objects and associated object attributes, the object owner,
and Active Directory permissions. Note that the Apply Group Policy permission is not available for the local GPO. The
policies in a nonlocal
GPO apply only to users who have Read and Apply Group Policy permissions for the GPO set
to Allow.
On computers running Windows Server 2003, the Everyone group members include Authenticated Users and Domain
Guests. On computers running earlier versions of the operating system, members include Authenticated Users and
Domain Guests, plus Anonymous Logon.
Default Domain Controllers Policy GPO is linked to the Domain Controllers
OU, and it generally affects only domain
controllers, because computer accounts for domain controllers are kept exclusively in the Domain Controllers OU.
Incorrect answers:
A, D:Groups or users that have been grantedFull Controlpermission for a folder can delete files and subfolders within
that folder, regardless of the permissions protecting the files and subfolders. This is not what is required.
B:These permissions will not correct the problem that is being experiences.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond,
Washington, 2004, p. 9: 18

QUESTION 216
You are the network administrator for Certkiller GmBh. The network consists of a single Active Directory
domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP
Professional. The Active Directory structure is shown in the Active Directory exhibit.

The company's written policy states that users in the manufacturing department are given only restricted access to settings and applications on their computers. The written policy also states that this limitation does not apply to members of a security group named Managers.
You create a Group Policy object (GPO) named Restricted Settings and link the GPO to the domain. This GPO contains the policy settings required by the written company policy.
You discover that the restricted settings apply to all users. You examine the Restricted Settings GPO by using the Group Policy Management Console (GPMC). The relevant information is shown in the GPMC exhibit.

You need to configure the network so that the written policy is enforced correctly.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A.Unlink the Restricted Settings GPO from the domain.Link it to the Manufacturing organizational unit (OU).
B.Unlink the Restricted Settings GPO from the domain.Link it to the Company Users organizational unit (OU).
C.Assign the Authenticated Users group to theDeny Apply
Group Policypermission for the Restricted Settings
GPO.
D.Assign the Managers group theDeny Apply
Group Policypermission for the Restricted Settings GPO.

Answer: A, D

Explanation: The question states that the restricted settings should apply to users in the Manufacturing OU.The policy is
currently linked to the domain which is why it is being applied to all users in the domain.We should unlink the policy
from the domain and link it to the Manufacturing organizational unit (OU).

Members of the Managers group should not receive the settings from the OU.We can fulfil this requirement by assigning
the Managers group theDeny Apply
Group Policypermission for the Restricted Settings GPO.
Incorrect Answers:
B:The restricted settings should apply to users in the Manufacturing OU, not the Company Users OU.
C:This would prevent the policy applying to all users. The policy should apply to users in the Manufacturing OU.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-41,10-42,10-20 to 10-21

QUESTION 217
You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .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.
Certkiller 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 doubleclick
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 theProhibit User Installssetting in the
Windows Installer section of the computer settings.
D.Modify the Default Domain Policy Group Policy object (GPO) and enable theAlways install with elevated privilegessetting in the Windows Installer section of the computer settings.

Answer: A, D

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 theAlways install with elevated privilegessetting 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 toenable theAlways install with elevated privilegessetting rather than disable theProhibit User Installs
setting.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70294:
Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 10, p. 656
Group policy help: StepbyStep
Guide to Software Installation and Maintenance
http://www.microsoft.com/windows2000/techinfo/planning/management/swinstall.asp

QUESTION 218
You are the network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .com. 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.

Location	GPO name	GPO configuration	Setting
Domain	ScreenSaver	Hide Screen Saver tab	Disabled
Sales OU	Display and Wallpaper	Hide Screen Saver tab	Enabled
Sales OU	Display and Wallpaper	Set Active Desktop Wallpaper to	Enabled
		c:\WINNT\web\wallpaper	\bliss.jpg
Sales OU	Wallpaper	Set Active Desktop Wallpaper to	Enabled
		c:\WINNT\web\wallpaper	\autumn.jpg

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 theNo Overridesetting for the Display and Wallpaper GPO.
B.Disable theNo Overridesetting on the ScreenSaver GPO.Reorder the Wallpaper GPO to be first in the list.
C.Create a GPO and link it to the DefaultFirstSiteName.
Configure the GPO to set the Active Desktop Wallpaper to
c:\WINNT\web\wallpaper\autumn.jpg.
D.Disable theBlock Policy inheritancesetting 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

Explanation: TheNo Overridesetting on the Screensaver GPO is causing all computers in the domain to display the
Screensaver tab.We want to hide the screensaver tab for the Sales OU, so we'll have to remove theNo 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 theDisplay 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
theNo Overridesetting for the Display and Wallpaper GPO won't result in it being applied.
C:AGPO linked to the Site is applied first and will be overwritten by subsequent GPOs applied at the lower levels.
D:Group policies set toNo Override Block Policy inheritancesetting on the Sales
OU does not affect the ScreenSaver GPO. This is part of the problem.
Reference:
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-3 to 10-12,10-16 to 10-20

QUESTION 219
Exhibit, Active Directory

Exhibit, GPMC

Sandra reports that the Run command does not appear on her Start menu, even though she is in the OU named Administration.
You discover that the Default Domain Policy GPO is removing the Run command from Sandra's Start menu. There is also a GPO named AdministativeSettings linked to the Administration OU that has the "Remove Menu from Start Menu" setting disabled.
To investigate the problem, you use the Group Policy Management Console (GMPC). The relevant information is shown in the exhibit.
You need to correct the application of policy settings so that the accounts in the Administrative OU receive the settings from the GPO linked to that OU. You need to accomplish this task without affecting any other policies.
What should you do?
A.Disable theNo Overridesetting in the Default Domain Policy GPO.
B.Disable the user configurationsetting in the Default Domain Policy GPO.
C.Enable theBlock Policy inheritancesetting for the Administrative OU.
D.Enable theNo Overridesetting for the AdministrativeSettings GPO.
E.Link the AdministrativeSettings GPO to the domain instead of the Administration OU. Modify the security settings so
that the GPO applies to accounts contained in the Administrative OU.

Answer: A

Explanation: The Default Domain Policy GPO is linked to the domain, and it affects all users and computers in the domain (including
computers that are domain controllers) through Group Policy inheritance. You thus need to disable the No Override

setting in this Default Domain Policy GPO if you want to correct the application of policy settings appropriately without

affecting any other policies.

Incorrect answers:

B:Disabling use configuration setting is not going to correct the application of policy settings in the Administrative OU.

C:The question states that you should correct the application of policy settings therefore, we cannot block policy

inheritance.

D:Group policies set to No Override cannot be blocked. This is part of the problem.

E:This option will affect the other policies and the question clearly states that you should correct the application of the

policy settings without affecting the other policies.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 10: 4

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294:

Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory

Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 582, 590

QUESTION 220

You are the network administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The domain includes an OU named Accounting. The user accounts for all users in the accounting department are in the Accounting OU.

You create a GPO and link it to Accounting. You configure the GPO to display the company logo as the desktop wallpaper for all clients computers in the Accounting OU.

The users in the accounting department report that they do not see the company logo as the desktop wallpaper. You suspect that a policy that has higher precedence is conflicting with the one you recently created.

You need to find out why the desktop wallpaper is not applying the client computer.

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

A.Use Resultant Set of Policy (RSOP) in planning mode. Expand the Administrator Templates and view the state of the

Active Desktop Wallpaper.

B.Use Resultant Set of Policy (RSOP) in logging mode. Expand the Administrator Templates and view the properties of

the Active Desktop Wallpaper.

C.Run the gpupdate /Target: User command from your computer.

D.Run the gpresult /Z command on a computer in the accounting department.

Answer: B, D.

Explanation: We need to view the effective group policy settings for the users or the computers that the users are using.

We can use gpresult or RSoP.The gpresult command displays Group Policy settings and Resultant Set of Policy (RSoP)

for a user or a computer.Resultant Set of Policy (RSoP) is an addition to Group Policy provides details about all policy

settings that are configured by an Administrator, including Administrative Templates, Folder Redirection, Internet

Explorer Maintenance, Security Settings, Scripts, and Group Policy Software Installation.

RSoP consists of two modes: Planning mode and logging mode. With planning mode, you can simulate the effect of

policy settings that you want to apply to a computer and user. Logging mode reports the existing policy settings for a

computer and user that are currently logged on.

Incorrect answers:

A:Running RSoP in planning mode will simulate the effect of policy settings that you want to apply to a computer and

user. This does not allow you to see the existing policy settings for that computer or user.

C:The gpupdate command will refresh a new policy that needs to be applied immediately. This is not what is required.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 11: 5

QUESTION 221

You are the network administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains an organizational unit (OU) named Research. All users who have user accounts in the Research OU use portable computers that run Windows XP Professional. You create a Group Policy object (GPO) named PowerManagement and link it to the Research OU. You configure the PowerManagement GPO to enable the Prompt for password on resume from hibernate /suspend policy.

A user named Jack has a user account in the Research OU. Jack reports that she is not prompted for a password when her computer resumes hibernation.

You need to ensure that Jack immediately has password protection for her portable computer when resuming from hibernation mode.

What should you do?

A.Instruct Jack to run thegpupdatecommand from her computer.

B.Instruct Jack to run thegpresultcommand from her computer.

C.Instruct Jack to send a Remote Assistance invitation to you.

Take control of Jack's compute and run thesecedit /analyzecommand.

A.Instruct Jack to send a Remote Assistance invitation to you.

Take control of Jack's computer and run thegpresultcommand.

Answer: A

Explanation: Although the GPO has been configured, some laptops may have not been online to be updated with the
GPO policy or there could have been network connectivity problems that prevented some laptops from getting the
policy. All problems aside, Jack's laptop should get the update at the next GPO refresh interval or Jack can get refresh
immediately by running the gpupdate command from her computer.
Incorrect answers:
B:The gpresult command will yield a text report of the resultant set of policy, i.e. the policy that is already applied. You
rather want to enforce a new GPO and that can be done through the use of the gpupdate command that enforces a
GPO without having to restart the computer.
C:This command is usually utilized when analyzing system security on a large number of computers. This will not ensure
that Jack will have immediate password protection for her portable computer when resuming from hibernation mode.
She needs to have the GPO updated on her computer.
D:This would be the wrong command to use (see B explanation). First sending Remote Assistance invitation is not an
immediate process as is required by the question.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, p. 623
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 10-44 to 10-21,11-4,11-6,11-19 to 11-22

QUESTION 222
You are the network administrator for Certkiller .com. Certkiller has offices in New York, Copenhagen, and Ankara. The network consists of a single Active Directory domain and three sites. The sites are named NYsite, CopSite, and AnkSite.
Certkiller is adding a new division at the New York office for publishing fiction books. You create a new organizational unit (OU) named Fiction for the fiction division. You add a new network segment and subnet for the fiction division. You plan to place new Windows XP Professional computers for the fiction division in the new subnet. You also plan to add a new domain controller to NYSite.
You need to ensure that users in the fiction division use the domain controllers in the New York office when logging on to the network.
What should you do?
A.Decrease the metric for the default gateway on the new Windows XP Professional computers.

B.Create a new subnet object for the new subnet.Add the new subnet object to NYSite.
C.Configure the location attribute for the new Windows XP Professional computers to be NYSite.
D.Move the domain controller objects for the domain controllers in the New York office to the Fiction OU.

Answer: B

Explanation:
Subnets can be associated with a site by using subnet objects. This will ensure that users on a particular subnet log on to
a domain controller in a particular site.
Incorrect Answers:
A:This won't accomplish anything.
C:The location attribute is for information only. It will not link the computer to the site.
D:This will give the administrators of the Fiction OU control over the domain controllers in the New York office. It
won't ensure that the users on the new subnet logon to the domain controller in the New York office.
Reference:
J. C. Mackin, Ian McLean, MCSA/MCSE selfpaced
training kit (exam 70291):
Implementing, Managing, and
Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond,
Washington,
2004, p. 2: 27-30
Walter Glenn, and Michael T. Simpson; MCSE Self
Windows Server 2003 Active Directory and Network Infrastructure, Microsoft Press, Redmond, Washington,
2004,
p. 58

QUESTION 223
You are a consultant for several different companies. You design the security policies for the computers
running Windows 2003 Server and Windows 2000 Professional in your customers' networks.
You use these security policies to configure a server named Server1. You want to deploy the security
configuration on Server1 to computers in your customer's networks by using the least amount of
administrative effort.
What should you do first?
A.Create a Group Policy Object (GPO) that configures the security settings for all computers to match the
settings on
Server1, and then link the GPO to the domain.Export the console list to a file.
B.In the Security Configuration and Analysis snapin,
analyze Server1 and export the security template in a file.
C.In the System Information snapin,
save the system summary as a system information file.
D.In the Security Templates snapin,
export the console list to a file.

Answer: B

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

QUESTION 224
You are a network administrator for Certkiller .com. The network consists of a single Active Directory
domain named Certkiller .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 Certkiller 1. All DNS servers contain Active Directoryintegrated
zones.
Other administrators report that they cannot connect to Certkiller 1 when attempting to perform Active
Directory administration. They report they can perform these tasks locally at Certkiller 1. 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 Certkiller 1 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 Certkiller 1.
D.Configure Certkiller as a local bridgehead server for the EastCoast site.

Answer: B

Explanation: Certkiller 1 is a domain controller.We know this because administrators are trying to perform Active
Directory administration on Certkiller 1.File and print resources on Certkiller 1 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 Certkiller 1 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 Certkiller 1.

D: Certkiller 1 does not need to be a bridgehead server to enable the administrators to access it.

Reference:

Craig Zacker, MCSE Self-PacedTraining Kit (Exam 70-293):Planning and Maintaining a Microsoft Windows Server

2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 4: 12

QUESTION 225

You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest root domain is contoso.com. Contoso, Ltd., recently merged with another company named Certkiller , whose network consists of a single Active Directory forest. The functional level of the Certkiller forest is Windows Server 2003.

The forest root domain for Certkiller is Certkiller .com. You need to create a forest trust relationship between the two forests. Each company has dedicated connections to the Internet.

You need to configure DNS to support the forest trust relationship. You want to maintain Internet name resolution capability for each company's network.

What should you do?

A.Configure the contoso.com DNS servers to forward to the Certkiller .com DNS servers.Configure the Certkiller .com

DNS servers to forward to the contoso.com DNS servers.

B.Configure conditional forwarding of Certkiller .com on the contoso.com DNS servers to the Certkiller .com DNS servers.

Configure conditional forwarding of contoso.com on the Certkiller .com DNS servers to the contoso.com DNS servers.

C.Configure a standard primary zone for Certkiller .com on one of the contoso.com DNS servers.Configure a standard

primary zone for contoso.com on one of the Certkiller .com DNS servers.

D.Configure an Active Directoryintegrated

zone for Certkiller .com on the contoso.com DNS servers.Configure an

Active Directoryintegrated

zone for contoso.com on the Certkiller .com DNS servers.

Answer: B

Explanation: A conditional forwarder is a DNS server on a network that is used to forward DNS queries

according to
the DNS domain name in the query. For example, a DNS server can be configured to forward all the queries it receives
for names ending with widgets.example.com to the IP address of a specific DNS server or to the IP addresses of multiple DNS servers.
Incorrect Answers:
A:We don't want ALL resolution requests to be forwarded to the other DNS servers.
C:We can't host primary zones on multiple servers.
D:We can't host Active Directory integrates zones on DNS servers in different forests.
Reference:

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 4-58,4-61
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows Server 2003,
Sybex Inc. Alameda, 2003, pp. 8-9,460-464
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003,pp. 367-369

QUESTION 226
You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains three domains. Each domain contains domain controllers that run Windows 2000 Server and domain controllers that run Windows Server 2003. The DNS Server service is installed on all domain controllers. All client computers run Windows XP Professional.
You need to add an additional DNS zone that is hosted on at least one DNS server on each domain. You want to configure the zone to allow secure updates only.
What should you do?
A.Configure the new zone on DNS servers in the root domain.Configure stub zones that refer to DNS servers in another two domains.
B.Configure the new zone as a primary zone on one DNS server.Configure other DNS servers in the three domains as
secondary servers for this zone.Enable the DNS Security Extensions (DNSSEC) protocol.
C.Configure the new zone as an Active Directoryintegrated
zone on DNS servers in the three domains.Store the zone
data in the DNS directory partition named DomainDNSZones.
D.Configure the new zone as an Active Directoryintegrated
zone on DNS servers in the three domains.Store the zone
data in the DNS directory partition named ForestDNSZones.

Answer: D

Explanation: To enable secure updates, we need an Active Directory integrated zone.To replicate to the DNS

servers

in the other domains, the zone must be installed on a Windows 2003 domain controller in each domain.During the

configuration of the zone, you can select the option to replicate the zone information to all domain controllers in the

Incorrect Answers:

A:We need Active Directory integrated zones, not stub zones.

B:Secondary zones are not writeable and so cannot accept updates.

C:If we store the zone data in the DNS directory partition named DomainDNSZones, it will only be replicated in a

single domain, not the entire forest.

Reference:

J. C. Mackin, Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291):Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington,

2004,pp. 5-25,6-22

QUESTION 227

You are the network administrator for Certkiller .com. The network consists of a single Active Directory forest that contains one domain named Certkiller .com.

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

You install a new standalone

Windows Server 2003 computer named CK1 . You plan to make CK1 the first

domain controller in the NA. Certkiller .com domain. You configure CK1 with a static IP configuration.

You run the Active Directory Installation Wizard on CK1 . The wizard prompts you for the network

credentials to use to join the NA. Certkiller .com domain to Certkiller .com.

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

You need to be able to promote CK1 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 CK1 to use a WINS server that contains entries for the Certkiller .com domain

controllers.

B.Configure the client DNS settings on CK1 to use a DNS server that is authoritative for the Certkiller .com domain.

C.Configure the DNS Server service on CK1 to have a zone for NA. Certkiller .com.

D.Configure CK1 to be a member server in the Certkiller .com domain.

Answer: B

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. CK1 is a Windows Server 2003 computer.

C:NA. Certkiller .com does not yet exist.

D:We want to install CK1 as a domain controller for the na. Certkiller .com domain. Making CK1 a member server would

me demoting the server and then promoting it again al a later point. This does not make sense.

Reference:

Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293):Planning and Maintaining a Microsoft Windows Server

2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, p.4: 6

Jill Spealman, Kurt Hudson & Melissa Craf

and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004,pp. 4-6 to 4-9,4-17

QUESTION 228

You are the network administrator for Acme. The network consists of a single Active Directory forest root domain named acme.com. The functional level of the forest is Windows Server 2003.

A Windows Server 2003 domain controller named DC1.acme.com is the Active Directory-integrated DNS server for acme.com. All servers and client computers in the acme.com domain use DC1.acme.com as their DNS server for name resolution.

Acme acquires a company named Certkiller . The Certkiller network consists of a single Active Directory forest root domain named Certkiller .com. The functional level of this domain is Windows Server 2003.

A Windows Server 2003 domain controller named DC1. Certkiller .com is the Active Directory-integratedDNS server for Certkiller .com. All servers and client computers in the Certkiller .com domain use DC1. Certkiller .com

as their DNS server for name resolution.

You create a two-way forest trust relationship with forest-wide authentication between acme.com and Certkiller .com.

You need to ensure that all users in both companies can log on to both forest root domains. You need to achieve this goal without adversely affecting Internet access.
What should you do?
A.Set theStub Zoneas the zone type for the acme.com domain on DC1.acme.com and for the Certkiller .com domain on
DC1. Certkiller .com.
B.Select theDo not use recursion for this domaincheck box on DC1. Certkiller .com and on DC1.acme.com.
C.Add the fully qualified domain name (FQDN) and the IP address of DC1. Certkiller .com to theRoot hintslist in
DC1.acme.com.Add the FQDN and the IP address of DC1.acme.com to theRoot hintslist on DC1. Certkiller .com.
D.Configure conditional forwarding on DC1.acme.com to forward all requests for resources in the Certkiller .com domain
to DC1. Certkiller .com.Configure conditional forwarding on DC1. Certkiller .com to forward all requests for resources in the
acme.com domain to DC1.acme.com.

Answer: D

Explanation: To log on to a computer in acme.com with a user account in Certkiller .com, the acme.com DNS server
needs to be able to locate a domain controller in Certkiller .com to authenticate the login.You can useConditional
forwardingwhich enables a DNS server to forward DNS queries based on the DNS domain name in the query.
Conditional forwarding in Windows Server 2003 DNS eliminates the need for secondary zones by configuring DNS
servers to forward queries to different servers based on the domain name.
Incorrect Answers:
A:A stub zone is a copy of a zone containing only those resource records necessary to identify the authoritative DNS
servers for the master zone
B:Recursion is the process of a DNS server querying other DNS servers on behalf of an original querying client. If
recursion is disabled, the client performs iterative queries by using root hint referrals from the DNS server. Iteration
refers to the process of a DNS client making repeated queries to different DNS servers.
C:Root hints is a list of preliminary resource records used by the DNS service to locate servers authoritative for the root
of the DNS domain namespace tree.
Reference:
Mark Minasi, Christa Anderson, Michele Beveridge, C.
A. Callahan & Lisa Justice, Mastering Windows Server 2003,
Sybex Inc. Alameda, 2003, pp. 451

QUESTION 229
You are the security analyst for Certkiller .com. The network consists of a single Active Directory domain

named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP
Professional. The perimeter network contains an application server, which is accessible to external users.
You view the logs on your intrusiondetection
system (IDS) and on the router and discover that very large
numbers of TCP SYN packets are being sent to the application server. The application server is responding
with SYNACK
packets to several different IP addresses, but is not receiving ACK responses. You note that
all incoming SYN packets appear to be originating from IP addresses located within the perimeter network's
subnet address range. No computers in your perimeter network are configured with these IP addresses. The
router logs show that these packets are originating from locations on the Internet.
You need to prevent this type of attack from occurring until a patch is made available from the application
vendor. Because of budget constraints, you cannot add any new hardware or software to the network. Your
solution cannot adversely affect legitimate traffic to the application server.
What should you do?
A.Relocate the application server to the company intranet.Configure the firewall to allow inbound and outbound
traffic
on the ports and protocols used by the application.
B.Configure network ingress filters on the router to drop packets that have local addresses but that appear to
originate
from outside the company network.
C.Create access control lists (ACLs) and packet filters on the router to allow perimeter network access to only
authorized users and to drop all other packets originating from the Internet.
D.Configure the IDS on the perimeter network with a response rule that sends a remote shutdown command to
the
application server in the event of a similar denialofservice
attack.

Answer: B

Explanation: In an ideal world, each router would be configured with ingress filters that would drop packets
arriving
from "internal" networks whose source address was not a member of the set of network addresses that this
router
serves. The majority of routers could be so configured. These ingress filters should be required as part of a
"good
neighbor policy." Ingress filters would not totally eliminate denial of service attacks but could greatly reduce
such
attacks. An attacker could still spoof an address within a local subnet, but that would permit backtracking
the packets
to the source subnet.
Incorrect Answers:
A:There is no firewall mentioned in the question.
C:This option could also work, but it involves extra administration.
D: The question clearly states; "Your solution cannot adversely af
option would.
Reference:

Martin Grasdal, Laura E. Hunter, Michael Cross, Laura Hunter, Debra Littlejohn Shinder & Dr. Thomas W. Shinder,
Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training
System, Syngress Publishing, Inc., Rockland, MA, Chapter11, p. 783
http://securityresponse.symantec.com/avcenter/security/content/9011.html

---

QUESTION 230
You are the network administrator for Certkiller . You need to test a new application.
The application requires 2 processors and 2 GB of RAM. The application also requires shared folders and installation of software on client computers.
You install the application on a Windows Server 2003 Web Edition computer and install the application on 20 test client computers.
You then discover that only some of the client computers can connect and run the application. You turn off some computers and discover that the computer that failed to open the application can now run the application. You need to identify the cause of the failure and update your test plan.
What should you do?
A.Increase the maximum number of worker processes to 20 for the default application pool
B.Use add/remove programs to add the application server windows component
C.Change the application pool to identify the local service for the default application pool
D.Change the test server OS to Window Server 2003 Standard Edition or Enterprise

Answer: D

Explanation: Although Windows Server 2003 Web Edition supports up to 2GB of RAM, it reserves 1GB of it for the
operating system; only 1GB of
Standard Edition or Enterprise Edition to support enough RAM.
Incorrect Answers:
A,C: The application requires 2 GB of
operating system so only 1GB of RAM is available for the application. So, changing the application pool won't resolve
this problem.
B:The application server component includes IIS and ASP. These would be part of the default installation on a Web
Server.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 1, p. 75

QUESTION 231
You are the network admin for litware inc. The company's written security policy requires that you maintain a copy of all private keys issued by Certkiller 's enterprise root CA
You create a duplicate of the user template named Employee and configure the template as shown in the Employee Properties exhibit:

You configure the CA to archive private keys by using a Key Recovery Agent Certificate.
You create a test user account named Peter and request a new employee certificate. You issue the certificate to Peter. You reinstall the OS on your test computer and attempt to recover Peter's private key. Your attempt fails and generates the following error message:
C:\ certutil Getkey
CertUtil: GetKeycommand
failed
CertUtil: Cannot find object or property.
You need to ensure that future attempts to recover private keys associated with Employee certificates succeed
What should you do?
A.Using Group Policy, deploy a copy of the key recovery agent certificate to all client computers.
B.In the Employee template, select the Archive subject's encryption private key check box.
C.In the employee template, select the Allow private key to be exported check box.
D.Run the certutil dspublish
command to publish the Key Recovery Agent certificate to Active Directory.

Answer: C

Explanation: The Request Handling tab has options including minimum key size and certificate purpose. The certificate
purpose can be encryption, signature, or signature and encryption. There is also an option to allow the export of the
private key.
Incorrect Answers:

A:Key recovery is deployed via the Certificate Services
B:You are attempting to recover the key, not archive it
D:This option will not work since the certutil command is not responding positively.
Reference:
Martin Grasdal, Laura E. Hunter, Michael Cross, Laura Hunter, Debra Littlejohn Shinder, and Dr. Thomas W. Shinder,
Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70293
Study Guide & DVD Training
System, Syngress Publishing, Inc., Rockland, MA, 2004, Chapter 12

QUESTION 232
You are the network administrator for Certkiller . The network consists of a single Active Directory forest that contains a single domain named Certkiller .com. All servers run Windows Server 2003, and all client computers run Windows XP Professional.
In a test lab that contains a separate forest, you develop and test a Group Policy object (GPO) that you need to apply to all computers and users in the domain.
You need to implement the new GPO on the network. You want to accomplish this task by using the minimum amount of administrative effort.
What should you do?
A.Use a Distributed File System (DFS) to replicate the GPO information in the SYSVOL shared folder from the test
lab to the domain.
B.Use the Group Policy Management Console (GPMC) to back up the GPO from the test lab and import it into the
domain.
C.Copy the Group Policy Template (GPT) files in the SYSVOL shared folder from the test lab to the domain.
D.Use Active Directory Users and Computers to create a new GPO linked to the domain.
In the new GPO, include all of the settings that exist in the GPO in the test lab.

Answer: B

Explanation: The GPMC lets administrators manage Group Policy for multiple domains and sites within one or more
forests, all in a simplified user interface (UI) with draganddrop
support. Highlights include new functionality such as
backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations are fully scriptable,
which lets administrators customize and automate management.
We can use theGroup Policy Management Console (GPMC) to back up the GPO from the test lab and import it into
the domain.
Incorrect answers:
A:DFS allows you to redirect specific folders like My Documents out to a highavailability
network location where each
user's files can be backed up and protected. This is not what is desired.
C:This option is not the way to implement a new GPO on a network.

D:This is one way of implementing the GPO but with much more administrative effort than is necessary.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active
Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 4, pp.
328,
361
MS White Paper: Migrating GPOs Across Domains with GPMC
http://www.microsoft.com/windowsserver2003/docs/MigGPOs.doc

QUESTION 233
You are the network administrator for Certkiller . All Web servers on the network run Windows 2000 Server.
The Web servers run several applications, including a collaborative Webbased
application that uses
ASP.NET and Web Distributed Authoring and Versioning (WebDAV).
You plan to migrate the Web servers to Windows Server 2003. You use the Configure Your Server Wizard to
configure a Windows Server 2003 computer as an application server, and you enable ASP.NET in the
process.
You install the Webbased
application on the server.
Users now report that when they attempt to access the collaborative Webbased
application, they receive the
error message shown in the exhibit.

The page cannot be found

The page you are looking for might have been removed, had its name changed, or
is temporarily unavailable.

Please try the following:

- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the Back button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

You need to enable the collaborative Webbased
application to function on Windows Server 2003 while
maintaining Web server security.
What should you do?
A.Use IIS Manager to disable anonymous access.
B.Use IIS Manager to allow the WebDAV Web service extension and to allow Httpext.dll.
C.Use IIS Manager to grant the users of the Webbased
application permissions for the default Web site.
D.Use IIS Manager to allow the Active Server Pages Web service extension and to allow Asp.dll.

Answer: D

Explanation: By default, when Internet Information Services (IIS) is installed on any version of the Microsoft Windows
Server 2003 family, IIS only serves static content (HTML). When you request dynamic content, such as Active Server
Pages (ASP) or ASP.NET pages, you receive one of the following error messages:
HTTP Error 404 File - Not Found
-or-
HTTP Error 404- File or Directory not found
To permit IIS to serve other types of content, the administrator must unlock this content in the Web service extensions
node in the IIS management console. To do this, either enable a preexisting
Web service extension or add a new Web
service extension.
Incorrect Answers:
A:This is not a permissions problem.You can run ASP content with anonymous access enabled if you want to.
B:Webdav is used to access files over http.It is not required to run ASP content.
C:This is not a permissions problem.A permissions problem would return a different error message.
Reference:
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 3

QUESTION 234
You are a systems engineer for Certkiller . The network consists of a single Active Directory domain named
Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. The
network contains 20 servers that run Terminal Services. All user productivity applications are hosted on
these servers. Several of these applications are legacy applications that require users to control the file
system and application registry settings.
Currently, Terminal Services is configured to allow administrators to remotely view and control users'
Terminal Services sessions for support and training purposes. The managers of the human resources and
finance departments inform you that confidential information was compromised when administrative
personnel viewed user sessions without the knowledge or permission of the users. The managers direct you
to change the Terminal Services configuration to ensure that administrators can never view or control a
user's session without the user's permission. You modify the Default Domain Policy Group Policy object
(GPO) as shown in the exhibit.
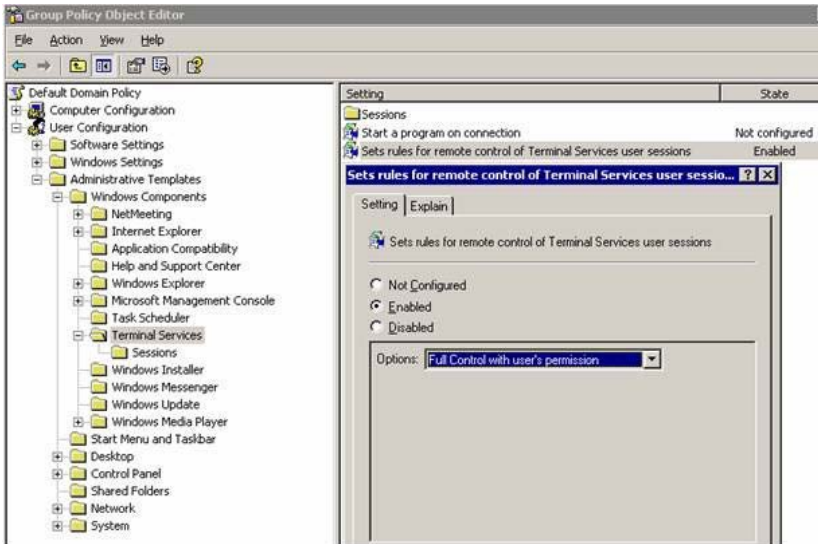
You attempt to establish remote control of user's Terminal Services session and find out that you can do so without the user's permission.
You need to configure Terminal Services to require the users' permission before an administrator can remotely view or control the session. You need to accomplish this task as quickly as possible and by using the minimum amount of administrative effort. Your configuration must also automatically apply to any new terminal servers that are installed in the network.
What should you do?
A.In the Computer Configuration section of the Default Domain Policy GPO, disable theUsers can connect remotely
using Terminal Servicesoption.
B.In the Computer Configuration section of the Default Domain Policy GPO, enable theSets rules for remote control
of Terminal Services user sessions option and specifyFull Control with user's permission.
C.In the Terminal Services Configuration tool, select theUse remote control with the following settingsoption and
select theRequire user's permissioncheck box.
D.In the Terminal Services Configuration tool, set thePermission compatibilityoption toFull Security.In the connection properties, remote theAllow Full
Controlpermission from the Administrators group.

Answer: B

Explanation: Group policies are collections of user and computer configuration settings that can be linked to computers,
sites, domains, and OUs to specify the behavior of users' desktops.TheDefault Domain Policy GPO is linked to the
domain, and it affects all users and computers in the domain (including computers that are domain controllers) through
Group Policy inheritance. Thus to require that an administrator can remotely control or view the session and apply it to
all new terminal servers that are installed on the network with the least amount of administrative effort, you

should enable
the Sets rules for remote control of Terminal Services user sessions with the Full Control with user's permission setting in
the Default Domain Policy GPO.
Incorrect answers:
A:The Computer configuration section of the Default Domain Policy GPO is the correct location to be configured.
However, disabling the Users can connect remotely using Terminal Services is not the correct setting.
C:This option will require more than is necessary administrative effort.
D:There is no need to configure the Terminal Services Configuration tool and its settings since all that is required is to
enable the Sets rules for remote control of Terminal Services user sessions with the Full Control with user's permission
setting in the Default Domain Policy GPO.
Reference:
Jill Spealman, Kurt Hudson & Melissa Craf
and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, p. 1: 43
Michael Cross, Jeffery
A. Martin, Todd
A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.
Shinder, MCSE: Exam 70-294:Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory
Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 2, pp. 122-126 & Chapter 9, pp. 628-630