70-298

Designing Security for a MS Windows Server 2003 Network

Version 2.4

70-298

Total Questions : 96

Topic 1, Litware Inc., Scenario

Overview
Litware. Inc., is a manufacturer and wholesale distributor of hiking and climbing outdoor gear. The company recently merged with Contoso, Ltd.

Contoso, Ltd., provides fabrics to Litware, Inc.

Physical Locations
The Litware, Inc., main office is in Denver. The company has branch offices in Dallas, Boston, and San Francisco. The information technology (IT) department is located in the Denver office. The company's manufacturing plant is located in Dallas. The company's east coast sales and distribution center is located in Boston, and the west coast sales and distribution center is located in San Francisco. The Contoso, Ltd., main office is in Auckland.

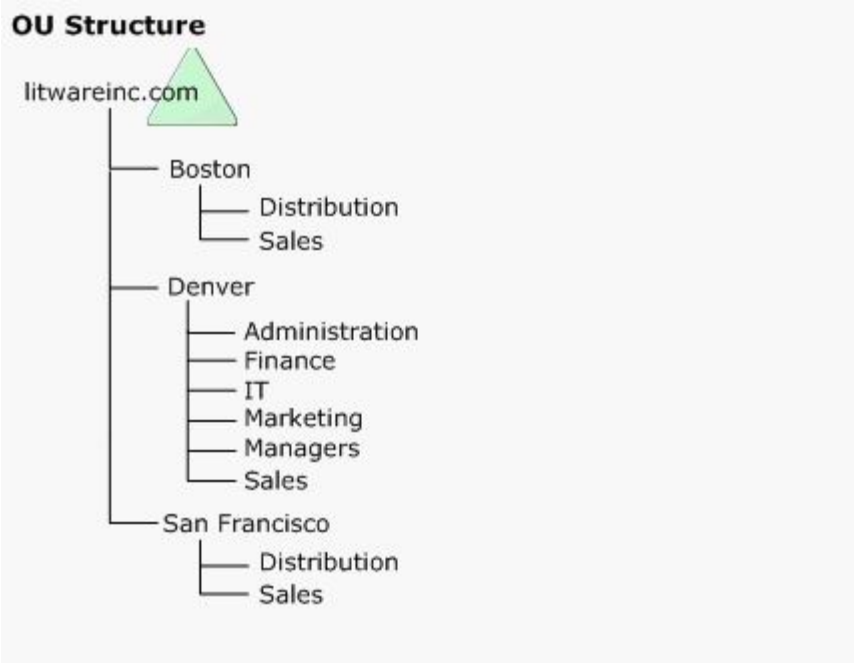
The company will open a new branch office in Singapore. This new office will be added to the contoso.com domain. Client computers in the Singapore office will run Windows XP Professional. An OU named Singapore Sales and Distribution will be added fro the contoso.com domain for the new branch office.

Computers and users in the Windows NT 4.0 domain will be migrated to an OU in the litwareinc.com domain. The firewall will be configured to allow PPTO and L2TP VPN traffic. Remote Desktop connections will be used for administration of servers and desktop client computers.

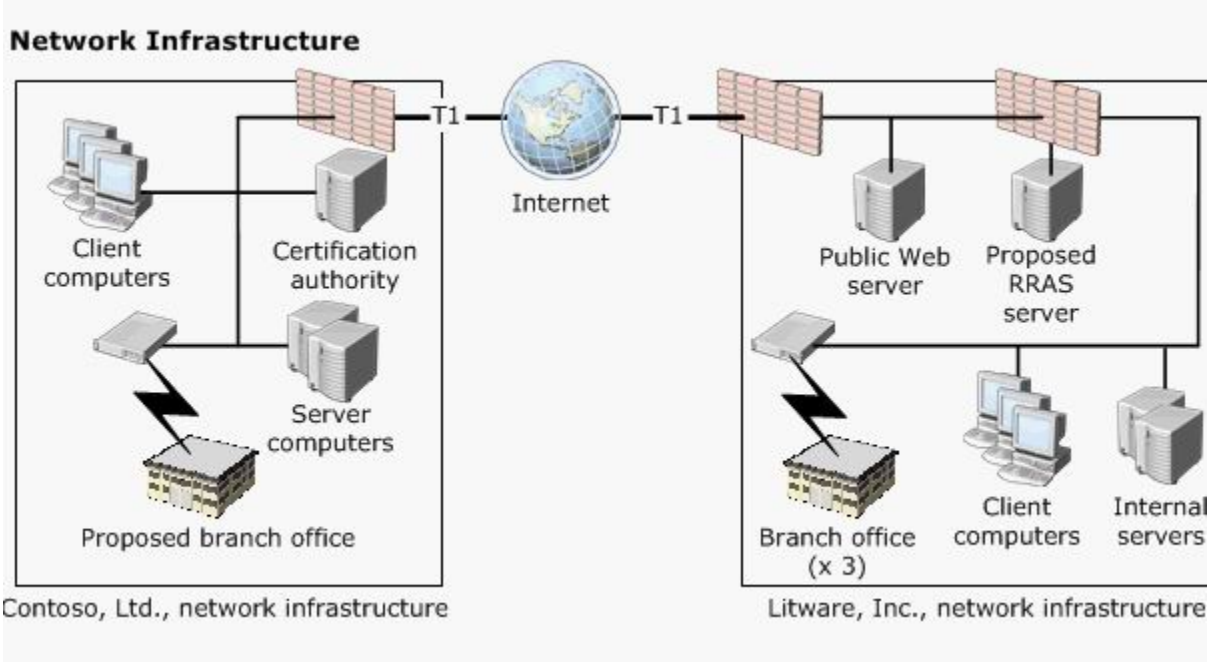
Routing and Remote Access servers in the branch offices will be taken offline. Administration of the remote access server in the Denver office will be managed by only administrators who specialize in remote access.

Business Processes
The IT staff in the Denver office managers the computers in the branch offices remotely. Each branch office has a desktop support technician.
All Litware, Inc., company data, including marketing, manufacturing, sales, financial, customer, legal, and development data must not be available to the public. This data is considered to be confidential.
The company's public Web site is hosted in the Denver office. The public Web site contains press releases and product information.
Each office has mobile sales users. These mobile users connect to a remote access server at the nearest branch office by using a dial-up connection.

Directory Services
The Litware, Inc., network consists of two domains. One domain is a Windows 2000 Active Directory domain.
The second domain is a Windows NT 4.0 domain. A two-way external trust relationship exists between the Active Directory domain and the Windows NT 4.0 domain.
The organizational unit (OU) structure for the Active Directory domain is shown in the OU Structure exhibit.



The Contoso, Ltd., network consists of a single Active Directory domain named contoso.com. All domain controllers run Windows Server 2003.
Network Infrastructure
The network infrastructure after the merger is shown in the Network Infrastructure exhibit.



The operating system installed on the client computers in each office is shown in the following table.

Office	Client operating system
Denver	Windows XP Professional
Boston	Windows XP Professional
San Francisco	Windows 2000 Professional
Dallas	Windows XP Professional and Windows NT Workstation 4.0
Auckland	Windows 2000 Professional and Windows XP Professional

All managers and mobile sales users have client computers that run Windows XP Professional.
All client computers run the latest service packs.

Problem Statements

The following business problems must be considered:

- IT administration is too complex and expensive.
- Remote access connections to the network are expensive.
- Remote access policies are not centralized.
- Employees are required to remember multiple passwords.
- It takes the Denver IT staff several days to fix account problems or problems with access to network resources.

Chief Executive Officer

Because we acquired Contoso, Ltd., we now hold the patent rights to a new fabric. We need to absolutely certain that our competitors do not obtain our development data or our research data. This information is secret, and it is critical to the success of our business.

Chief Information Officer

As the company grows, we need to find more cost effective methods to manage the network and to keep it more secure.
We need to enable a stronger authentication strategy for the network. We need to integrate Contoso, Ltd., into this strategy.

Denver IT Administrator

Currently, we allow only managers to use Encrypting File System (EFS) on local computers.
Sometimes we have problems with lost user profiles. We need to be able to restore access to encrypted files as quickly as possible.

I think we need a two-factor authentication method for the mobile sales users.
We need to limit unnecessary traffic across the WAN links.

We also need to track configuration changes on all domain controllers.
Network Manager (Litware, Inc.)

We simply do not have the IT staff to support all the branch offices and the newly acquired contoso.com domain. Currently, we rely on the desktop support technician at each branch office to perform minimal everyday administrative tasks, such as resetting passwords. Even though Contoso, Ltd., has its own IT staff, we are responsible for administration of the contoso.com domain.

We want to require all remote users to log on by means of a secure VPN connection. The solution must be easy to implement and also must reduce complexity for end users.
Also, we need to maintain both domains' servers and client computers with the latest updates and security patches. Denver IT staff must be able to control which updates and security patches are deployed to the other offices.

We need a public key infrastructure (PKI) that is not vulnerable to compromise. We also need a PKI that will allow only specific administrators to control the enrollment of smart card certificates.

Business Drivers
The following business drivers must be considered:

- The network environment must be more secure and it must be standardized. The network management must be minimized.
- Universal principal names (UPN) single sign-on must be provided to all users.

The relevant portion of the company's written security policy includes the following requirements:

- Only managers and executives must be able to access the Customer Information folder.
- Only managers and executives must be able to access research and product development information.
- Only managers must be able to encrypt files stored on file servers or on their local computers.
- Sales users must be able to encrypt the offline files cache.
- Users must not be able to log on interactively to client computers by using accounts that have administrative privileges.
- Two-factor authentication is required to perform administrative tasks.
- All Terminal Services connections must require encryption.
- Remote access users must use only L2TP VPN connections to connect to the internal network.

Topic 1, Litware, Inc (4 Questions)

QUESTION NO: 1
You need to design a remote access solution for the mobile sales users in the litwareinc.com domain. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure autoenrollment for user certificates and computer certificates.
B. Configure Web enrollment for user certificates and computer certificates.
C. Configure a Certificate Services hierarchy in the litwareinc.com domain.
D. Configure qualified subordination between the litwareinc.com and the contoso.com domains.
E. Configure PEAP authentication on the remote access servers.

Answer: A, C
Explanation: Auto-enrollment features are set by CA administrators in the certificate templates. A user who is authorized to use these Certificate templates will be auto-enrolled.

- Each office has mobile sales users. These mobile users connect to a remote access server at the nearest branch office by using a dial-up connection.
- Remote access connections to the network are expensive.
- Remote access policies are not centralized.
- We need **a two-factor authentication** method for the mobile sales users.
- We want to require all remote users to log on by means of a secure VPN connection. **The solution must be easy to implement** and also must reduce complexity for end users.

Considering the above, you should configure autoenrollment for user certificates and computer certificates and you should also configure Certificate Services hierarchy in the litwareinc.com domain.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 181

QUESTION NO: 2
You need to design an administrative control strategy for Denver administrators.
What should you do?

A. Create a security group named HelpDesk.
Add the HelpDesk group to the Enterprise Admins group in both domains.
B. Create a security group named HelpDesk.
Add the HelpDesk group to the Domain Admins groups in both domains.
C. Add the Domain Admins group in the litwareinc.com domain to the Domain Admins group in the contoso.com domain.
Delegate full control of the litwareinc.com domain to the Domain Admins group in the contoso.com domain.
D. Create a security group named HelpDesk for each office.
Delegate administrative tasks to their respective OU or domain.
Delegate full control of the contoso.com domain to the Domain Admins group from the litwareinc.com domain.

Answer: D
Explanation: When designing a delegation strategy, you should be aware that there are two types of administrators, Service Administrators and Data Administrators. Service Administrators are responsible for the overall integrity and availability of Active Directory; they maintain network services and functions for the entire user base. Data administrators are responsible for specific objects stored within Active Directory such as user and group accounts and the like. You should create your Active Directory design so that these two tasks can be separated and managed by two different people or job functions. When designing a delegation strategy, it's also imperative that you analyze your business needs for autonomy versus isolation. For example, your Human Resources department might require full and unshared control over their portion of the Active Directory and all of their network resources, with strict policies on security. In this case, the only way to give them this level of control is by creating a separate forest for them. Another department might be more willing to accept shared administration of their resources, in which case they would fall under the category of autonomy. At this point, you can create a separate domain or OU to subdivide their resources for them. Delegation of administration can be set the forest level, domain level, and OU level. The higher the level, the more isolated the administrative model. Conversely, the lower the level of delegation, the more it tends toward autonomous administration.

- The Litware, Inc., main office is in Denver.
- The information technology (IT) department is located in the Denver office.
- Currently, we rely on the desktop support technicians at each branch office to perform minimal everyday administrative tasks, such as resetting passwords.
- Even though contoso, Ltd., has its own IT staff, we are responsible for administration of the contoso.com domain.

As the situation is, the best administrative strategy would be to create a security group for each office and then delegate administrative tasks to their respective OU or domain. Then you should delegate full control of the contoso.com domain to the Domain Admins group of the litwareinc.com domain.

Reference:
Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 8, pp. 497-498

QUESTION NO: 3

You need to design a PKI for Litware, Inc.
What should you do?

A. Add one offline stand-alone root certificate authority (CA).
Add two online enterprise subordinate CAs.
B. Add one online stand-alone root certification authority (CA).
Add two online enterprise subordinate CAs.
C. Add one online enterprise root certification authority (CA).
Add one offline enterprise subordinate CA.
D. Add one online enterprise root certification authority (CA).
Add two online enterprise subordinate CAs.

Answer: A
Explanation: The root CA is the top of the CA hierarchy and should be trusted at all times. The certificate chain will ultimately end at the root CA. The enterprise can have a root CA as enterprise or a stand-alone CA. The root CA is the only entity that can self sign, or issue self certificates in the enterprise. Windows Server 2003 only allows one machine to act as the root CA. The root CA is the most important CA. If the root CA is compromised, all the CAs in the enterprise will be compromised. Therefore, it is a good practice to disconnect the root CA from the network and use a subsidiary CA to issue certificates to users. Any CAs that is not the root CA is classified as subordinate CAs. The first level of subordinate CAs will obtain their certificates from the root CA. These servers are commonly referred to as intermediary or policy CAs. They will pass on the certificate information to the issuing CAs down the chain. They are referred to as intermediary because they act as a "go-between" with the root CA and the issuing CAs.

You need to protect the root. Install the root CA as a Windows Server 2003 stand-alone root CA. This type of CA does not need to be on the network. Take the root CA offline. When the root CA is not connected to the network, it cannot be attacked across the network.

- We need a public key infrastructure (PKI) that is not vulnerable to compromise. We also need a PKI that will allow only specific administrators to control the enrollment of smart card certificates.

Incorrect answers:
It is best practice to have a root CA offline. Thus these options will leave your network vulnerable.

Reference:
Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 3, p. 159, 181

QUESTION NO: 4
You need to design an EFS strategy to address the Denver IT administrator's concerns.
What should you do?

A. Configure key archival on each certification authority (CA).
B. Configure a certificate trust list (CTL) that includes the root certification authority (CA) certificate.
C. Create a security group named Managers.
Assign the appropriate NTFS permissions to the Managers group for the managers' data in Denver.
Add the Managers security group to the Restricted Groups in the Default Domain Policy object (GPO=.
D. Configure IPSec certificate autoenrollment on the Default Domain Policy Group Policy object (GPO):
Configure an IPSec policy on the Managers OU.

Configure the IPSec policy to use certificate authentication.

Answer: A
Explanation: Safely storing and archiving recovery agent credentials will ensure that you're always able to decrypt important files even after you've changed recovery agents. Files that might sit dormant for some time might need to be decrypted long after the file's owner leaves the company, so archiving is a critical step.
Thus a Windows Server 2003 Enterprise Edition computer with the certificates services can be configured to issue EFS certificates with a **file archival property**. Especially when you take into account the relevant pieces of information from the case study mentioned below:

- Currently, we allow only managers to use Encrypting File System (EFS) on local computers. Sometimes we have problems with lost user profiles. We need to be able to restore access to encrypted files as quickly as possible.
- I think we need a two-factor authentication method for the mobile sales users.
- We need to limit unnecessary traffic across the WAN links.
- We also need to track configuration changes on all domain controllers.

Incorrect answers:
* The CTL documents the trusted certificates of the enterprise. This signed list is issued by the CAs. However, this is not what is needed by Denver IT administrator.
The other options will not address the concerns stated.

Reference:
Elias N. Khnaser, Susan Snedak, Chris Peiris and Rob Amini, MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapters 3 & 9, pp. 157-159, 181, 565-569

Topic 2, Humongous Insurance, Scenario

Overview
Humongous Insurance provides property and casualty insurance to customers in North America and Europe.

Physical Locations
The company's main office is located in New York. The company has three branch offices in the following locations:

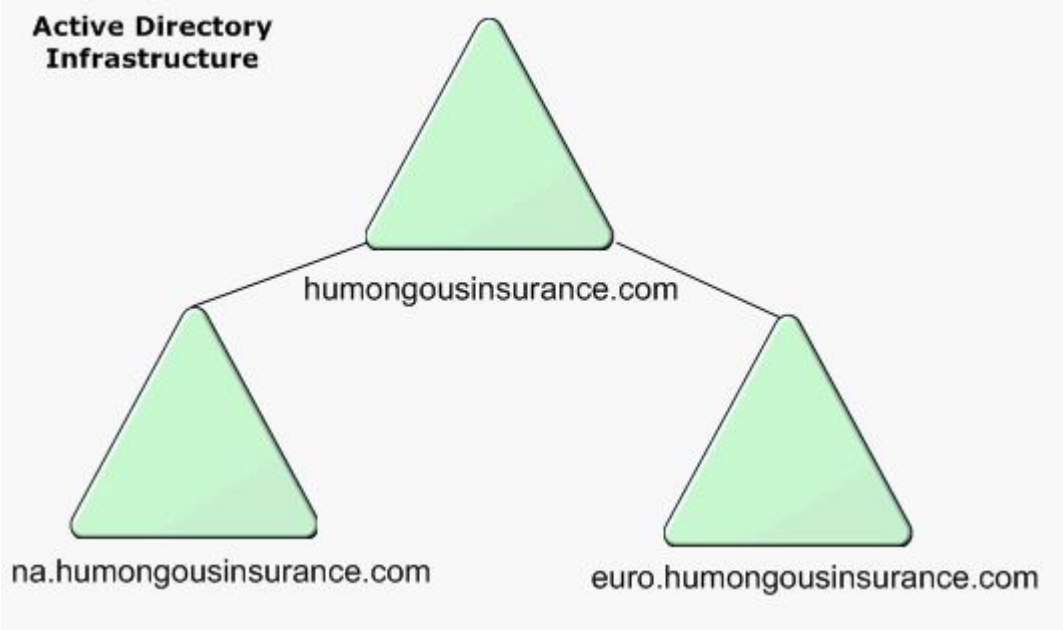
- Seattle
- London
- Madrid

Planned Changes
Humongous Insurance is entering into a join venture with Contoso, Ltd., a worldwide asset management company. The Contoso, Ltd., network consists of a single Windows 2000 Active Directory domain. Contoso, Ltd., does not plan to upgrade its servers to Windows Server 2003.

The collaboration between the two companies will take place entirely over the Internet. Users from both companies will access a shared folder name Customer Data, which will be located on a Windows Server 2003 computer on the Humongous Insurance internal network.

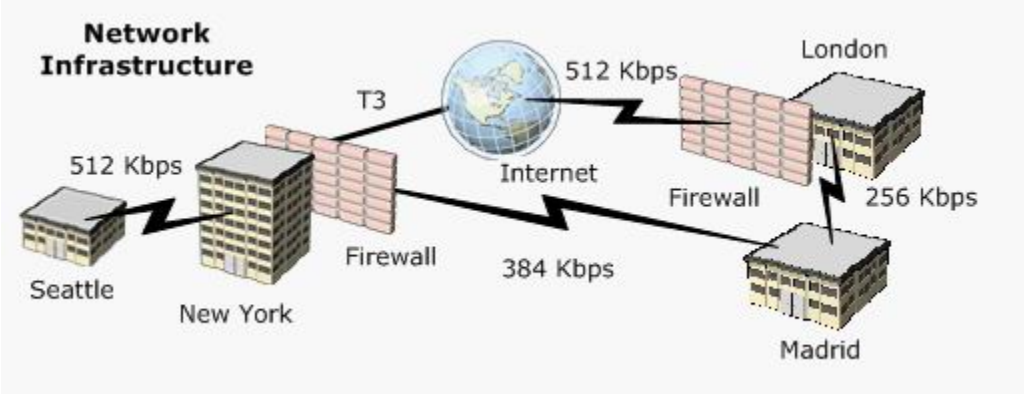
All Humongous Insurance client computers in Madrid will be upgraded to Windows XP Professional.

Directory Services
The existing Active Directory forest for Humongous Insurance is shown in the **Active Directory Infrastructure** exhibit.



The Humongous Insurance network consists of a single Windows Server 2003 Active Directory forest. The forest contains three domains named humongousinsurance.com, na.humongousinsurance.com, and euro.humongousinsurance.com

Network Infrastructure
The company's existing network infrastructure is shown in the **Network Infrastructure** exhibit



A Windows Server 2003 Web server is located in the New York office perimeter network. All client computers in North America run Windows XP Professional. Each office contains a domain controller. The domain controllers also serve as file and print servers.

Problem Statements
The following business problems must be considered:

- It is difficult to maintain all client computers with the latest security patches.
- Unauthorized users have modified the registry on some servers. Unauthorized users must not be able to modify the registry on company servers.