Vendor: Microsoft

Exam Code: 70-299

Exam Name: Implementing and Administering Security in a Windows Server 2003 Network

Version: DEMO

1: You are a security administrator for your company. The network includes a public key infrastructure (PKI) that supports smart card logon. All client computers have smart card readers. Managers are issued smart cards. Managers are required to use smart cards when logging on to client computers. You need to ensure that managers are required to use a smart card when logging on to any client computer and that all other users are required to use a smart card when logging on to a client computer assigned to a manager. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A.On the properties of each user account used by a manager, select the Smart card required for interactive logon check box.

B.On the computer account for each manager's client computer, edit the DACL so that only managers are assigned the Allow - Allowed to authenticate permission.

C.Place all client computers used by managers in an organizational unit (OU). Link a new Group Policy object (GPO) to the OU. Configure the GPO to enforce the Interactive logon: Require smart card setting.

D.Place all client computers used by managers in an organizational unit (OU). Link a new Group Policy object (GPO) to the OU. Configure the GPO to set the startup type of the Smart Card service to Automatic.

Correct Answers: A C

2: You are a security administrator for your company. The network consists of an Active Directory forest that contains two domains. The domains are named treyresearch.com and litwareinc.com. All Active Directory domains are running at a Windows Server 2000 mixed mode functionality level. Employees in the help desk department need to modify certain attributes of employee user accounts that reside in the treyresearch.com domain. The help desk department user accounts reside in the litwareinc.com domain. You need to create a single group named Help Desk that contains all help desk department user accounts and that can be granted access to modify the employee user accounts in the treyresearch.com domain. What should you do?

A.Use a universal security group in the treyresearch.com domain named Help Desk.

B.Use a universal security group in the litwareinc.com domain named Help Desk.

C.Use a global security group in the litwareinc.com domain named Help Desk.

D.Use a global security group in the treyresearch.com domain named Help Desk.

Correct Answers: C

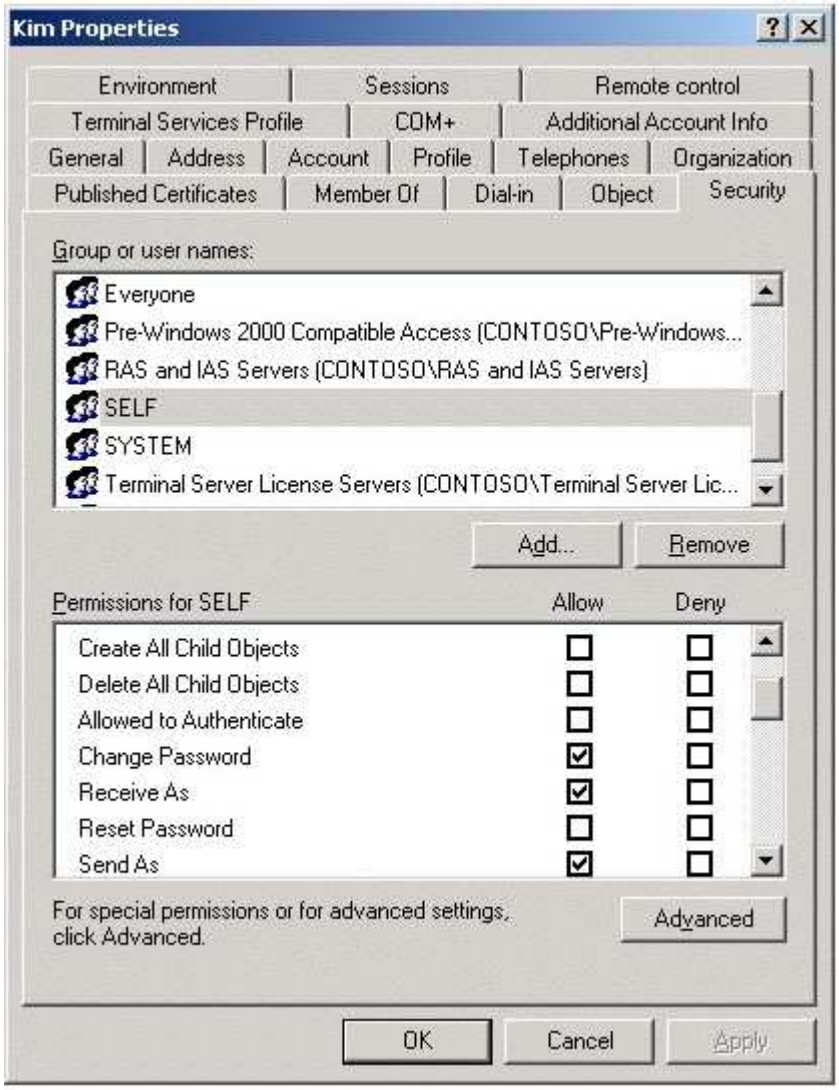
3: You are a security administrator for Contoso, Ltd. The network consists of a single Active Directory domain named contoso.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are members of the domain.

The company has a main office and three branch offices. Each office is configured as an Active Directory site. Each site contains domain controllers.

A domain user named Kim reports that she forgot her password. She works in one of the branch offices. A desktop support technician in the main office resets Kim's password, enables the User must change password at next logon option on Kim's user account, and then tells Kim the new password.

Kim attempts to log on by using her new password and reports that she cannot change the password at logon.

You investigate the problem. Kim's user account is not locked out, and it is not disabled. Permissions for the user account are shown in the exhibit. (Click the Exhibit button.) You need to ensure that Kim can log on and change her password.
What should you do?



A.Assign the SELF group the Allow - Reset Password permission for Kim's user account.
B.Assign the SELF group the Allow - Allowed to Authenticate permission for Kim's user account.
C.Assign the Everyone group the Allow - Allowed to Authenticate permission for Kim's user account.
D.Enable the Let Everyone permissions apply to anonymous users security setting in the domain.
E.Reset Kim's password on a domain controller in her branch office.
Correct Answers: E

4: You are a security administrator for your company. The network consists of two Active Directory domains. These domains each belong to separate Active Directory forests. The domain named graphicdesigninstitute.com is used primarily to support company employees. The domain named fineartschool.net is used to support company customers. The functional level of all domains is Windows Server 2003 interim mode. A one-way external trust relationship exists in

which the graphicdesigninstitute.com domain trusts the fineartschool.net domain.
A Windows Server 2003 computer named Server1 is a member of the fineartschool.net domain. Server1 provides customers access to a Microsoft SQL Server 2000 database. The user accounts used by customers reside in the local account database on Server1. All of the customer user accounts belong to a local computer group named Customers. SQL Server is configured to use Windows Integrated authentication.
Your company has additional SQL Server 2000 databases that reside on three Windows Server 2003 computers. These computers are member servers in the graphicdesigninstitute.com domain. The company's written security policy states that customer user accounts must reside on computers in the fineartschool.net domain.
You need to plan a strategy for providing customers with access to the additional databases. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?
A.Create a new user account in the fineartschool.net Active Directory domain for each customer. Create a universal group in the fineartschool.net domain. Add the new customer domain user accounts as members of the new universal group. Assign this group permissions to access the databases.
B.Create a new user account in the fineartschool.net Active Directory domain for each customer. Create a global group in the fineartschool.net domain. Add the new customer domain user accounts as members of the new global group. Assign this group permissions to access the databases.
C.Create a new user account in the graphicdesigninstitute.com Active Directory domain for each customer. Create a global group in the fineartschool.net Active Directory domain. Assign the new global group permissions to access the databases.
D.Create a new user account in the graphicdesigninstitute.com Active Directory domain for each customer. Create a universal group in the fineartschool.net Active Directory domain. Assign the new universal group permissions to access the databases.
Correct Answers: B

5: You are a security administrator for your company. The company has one main office and five branch offices. Network administrators work in the main office and each branch office. Network administrators in the main office frequently create scripts that automate common administrative tasks. You review each script to ensure it does not introduce security vulnerabilities. Scripts that do not introduce security vulnerabilities are considered approved. Occasionally, branch office administrators modify these scripts and distribute the modified scripts to other branch office administrators. Branch office administrators often report that they accidentally run a modified version of a script. You need to ensure that branch office administrators can verify which scripts are approved scripts. What should you do?
A.Maintain a list of the dates that the approved scripts were last modified. Instruct branch office administrators to verify the file modification date.
B.Digitally sign all approved scripts. Instruct branch office administrators to verify the signature before using a script.
C.Distribute all approved scripts to branch office administrators in an e-mail message.
D.Place all approved scripts on a file server in the main office. Assign all branch office

administrators only the Allow - Read permission for the folder that contains the approved scripts. Instruct administrators to copy scripts from this file server.

Correct Answers: B

6: You are a security administrator at your company. The network consists of a single Active Directory domain. The network contains Windows 2000 Professional client computers and Windows Server 2003 computers. Three Windows Server 2003 computers are named CA1, CA2, and CA3.

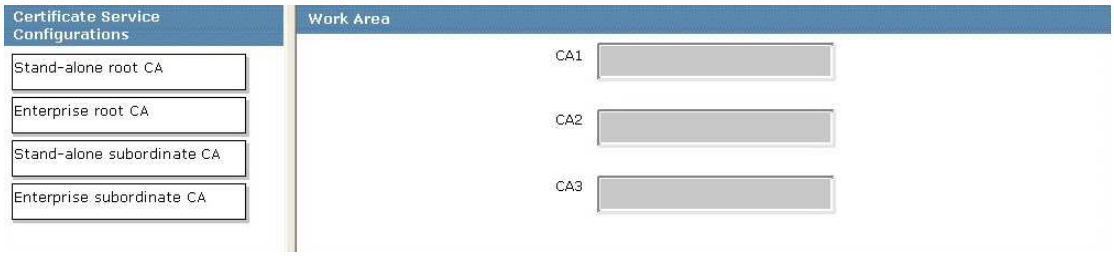
You want to implement a public key infrastructure (PKI) to support the security requirements in your company. All certification authorities (CAs) must belong to the same CA hierarchy.

You plan to install Certificate Services on CA1 first. CA1 will not be connected to the network and will be stored in a locked cabinet in the company data center. You plan to use CA2 to issue certificates for IPSec and Encrypting File System (EFS). You will configure CA2 to automatically issue these certificates. You plan to use CA3 to issue certificates that enable business partners to authenticate to your IIS Web site. CA3 will not be a member of the Active Directory domain.

You need to configure Certificate Services on each server to fulfill the server's designated role.

What should you do?

To answer, drag the appropriate Certificate Services configuration roles to the correct server locations in the work area.



Correct Answers: See Full Version

7: You are a security administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003.

You company uses the Internet to sell products. Customers place and view the status of orders by using a Web application named App1. App1 is hosted on a Windows Server 2003 computer that runs IIS. Users access App1 by using various Web browsers. You configure SSL for connections to App1.

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

All users must enter a user name and password when they access App1.

All users must use the same authentication method.

All users must use credentials in the company's domain.

You need to configure IIS to support the required authentication.

What should you do ?

To answer, configure the appropriate option or options in the dialog box in the work area.

Correct Answers: See Full Version

8: You are a security administrator for your company. The network consists of a single Active Directory domain. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional. Users store files on a server named Server1. These files are confidential and must be encrypted at all times while on Server1. You configure a new certification authority (CA) and issue certificates that support Encrypting File System (EFS) to all users. Users report that they cannot encrypt files that are stored on Server1. They report that they can encrypt files that are stored locally on their client computers. You need to ensure that users can encrypt files that are stored on Server1. What should you do?

A.Enroll Server1 for a Computer certificate that supports file encryption.

B.Configure a new EFS recovery agent. Deploy the EFS recovery agent by using Active Directory.

C.Configure the Server1 computer account to be trusted for delegation.

D.Enroll each client computer for a Computer certificate that supports file encryption.

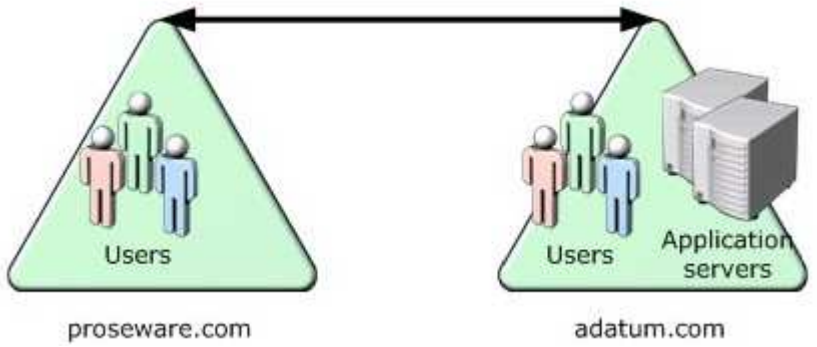
Correct Answers: C

9: You are a security administrator for your company. The network consists of two Active Directory domains named adatum.com and proseware.com. These domains are in the same Active Directory forest. The adatum.com Active Directory domain operates at a Windows 2000 mixed mode domain functional level. The proseware.com Active Directory domain operates at a Windows 2000 native mode domain functional level.

An application runs on four Windows Server 2003 computers. These computers are domain member servers in the adatum.com Active Directory domain. Authorized users in both the adatum.com and the proseware.com domains require access to this application. The network is depicted in the exhibit. (Click the Exhibit button.)

You need to plan an authorization model to control user access to the application. You will place adatum.com user accounts in a group named Adatum AppUsers. You will place proseware.com user accounts in a group named Proseware AppUsers. You will use a group named AppResources to assign permissions that allow access to the application. You need to choose the appropriate types of groups to implement your plan.

Which three types of groups should you choose? (Each correct answer presents part of the solution. Choose three.)



A.Use a global group named Adatum AppUsers in the adatum.com domain.

B.Use a domain local group named Adatum AppUsers in the adatum.com domain.

C.Use a global group named Proseware AppUsers in the proseware.com domain.

D.Use a domain local group named Proseware AppUsers in the proseware.com domain.

E.Use a global group named AppResources that contains the Adatum AppUsers and the Proseware AppUsers groups in the adatum.com domain.

F.Use a global group named AppResources that contains the Adatum AppUsers and the Proseware AppUsers groups in the proseware.com domain.

G.Use a domain local group named AppResources that contains the Adatum AppUsers and the Proseware AppUsers groups in the adatum.com domain.

H.Use a domain local group named AppResources that contains the Adatum AppUsers and the Proseware AppUsers groups in the proseware.com domain.

Correct Answers: A C G

10: You are a security administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. The company occasionally experiences downtime because of malicious Internet worms that arrive as Microsoft Visual Basic Scripting Edition (VBS) files. You examine several client computers and discover that VBS files are downloaded by using Microsoft Outlook, instant messaging, or peer-to-peer file sharing programs. You need to prevent users from running VBS files regardless of how they arrive on client computers. What should you do?

A.Use a software restriction policy to disable all unauthorized scripts.

B.Use an Administrative Template to ensure that Outlook and Internet Explorer are in the

Restricted Sites security zone.

C.Use a centralized logon script to rename the Wscript.exe file on each computer to contain a nonexecutable extension.

D.Use a file system security policy to assign the Deny - Execute permission for the Wscript.exe file.

Correct Answers: A