70-640$^{Q\&As}$

TS: Windows Server 2008 Active Directory Configuring

Pass Microsoft 70-640 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4lead.com/70-640.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Your network contains an Active Directory Rights Management Services (AD RMS) cluster.

You have several custom policy templates. The custom policy templates are updated frequently. Some users report that it takes as many as 30 days to receive the updated policy templates.

You need to ensure that users receive the updated custom policy templates within seven days.

What should you do?

A. Modify the registry on the AD RMS servers.

B. Modify the registry on the users\\' computers.

C. Change the schedule of the AD RMS Rights Policy Template Management (Manual) scheduled task.

D. Change the schedule of the AD RMS Rights Policy Template Management (Automated) scheduled task.

Correct Answer: B

Reference: http://technet.microsoft.com/en-us/library/cc771971.aspx

Configuring the AD RMS client The automated scheduled task will not query the AD RMS template distribution pipeline each time that this scheduled task runs. Instead, it checks updateFrequency DWORD value registry entry. This registry entry specifies the time interval (in days) after which the client should update its rights policy templates. By default the registry key is not present on the client computer. In this scenario, the client checks for new, deleted, or modified rights policy templates every 30 days. To configure an interval other than 30 days, create a registry entry at the following location: HKEY_CURRENT_USER\Software\Policies\Microsoft\MSDRM \TemplateManagement. In this registry key, you can also configure the updateIfLastUpdatedBeforeTime, which forces the client computer to update its rights policy templates.

QUESTION 2

Your company has an Active Directory domain.

You plan to install the Active Directory Certificate Services (AD CS) server role on a member server that runs Windows Server 2008 R2.

You need to ensure that members of the Account Operators group are able to issue smartcard credentials.They should not be able to revoke certificates.

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

A. Create an Enrollment Agent certificate.

B. Create a Smartcard logon certificate.

C. Restrict enrollment agents for the Smartcard logon certificate to the Account Operator group.

D. Install the AD CS role and configure it as an Enterprise Root CA.

E. Install the AD CS role and configure it as a Standalone CA.

F. Restrict certificate managers for the Smartcard logon certificate to the Account Operator group.

Correct Answer: BCD

http://technet.microsoft.com/en-us/library/cc753800%28v=ws.10%29.aspx AD CS: Restricted Enrollment Agent The restricted enrollment agent is a new functionality in the Windows Server?2008 Enterprise operating system that allows limiting the permissions that users designated as enrollment agents have for enrolling smart card certificates on behalf

of other users.

What does the restricted enrollment agent do?

Enrollment agents are one or more authorized individuals within an organization. The enrollment agent needs to be issued an enrollment agent certificate, which enables the agent to enroll for smart card certificates on behalf of users.

Enrollment agents are typically members of the corporate security, Information Technology (IT) security, or help desk teams because these individuals have already been trusted with safeguarding valuable resources. In some organizations,

such as banks that have many branches, help desk and security workers might not be conveniently located to perform this task. In this case, designating a branch manager or other trusted employee to act as an enrollment agent is required to

enable smart card credentials to be issued from multiple locations. On a Windows Server 2008 Enterprise-based certification authority (CA), the restricted enrollment agent features allow an enrollment agent to be used for one or many

certificate templates. For each certificate template, you can choose which users or security groups the enrollment agent can enroll on behalf of. You cannot constrain an enrollment agent based on a certain Active Directory?organizational unit

(OU) or container; you must use security groups instead. The restricted enrollment agent

is not available on a Windows

http://technet.microsoft.com/en-us/library/cc776874%28v=ws.10%29.aspx

Enterprise certification authorities

The Enterprise Administrator can install Certificate Services to create an enterprise certification authority (CA).

Enterprise CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail Extensions), authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport

Layer Security (TLS) and logging on to a Windows Server 2003 family domain using a smart card.

An enterprise CA has the following features:

An enterprise CA requires the Active Directory directory service. When you install an enterprise root CA, it uses Group Policy to propagate its certificate to the Trusted Root Certification Authorities certificate store for all users and computers

in the domain. You must be a Domain Administrator or be an administrator with write access to Active Directory to install an enterprise root CA.

Certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards. The enterprise exit module publishes user certificates and the certificate revocation list (CRL) to Active Directory. In order to publish

certificates to Active Directory, the server that the CA is installed on must be a member of the Certificate Publishers group. This is automatic for the domain the server is in, but the server must be delegated the proper security permissions to

publish certificates in other domains. For more information about the exit module, see Policy and exit modules.

An enterprise CA uses certificate types, which are based on a certificate template. The following functionality is possible when you use certificate templates:

Enterprise CAs enforce credential checks on users during certificate enrollment. Each certificate template has a security permission set in Active Directory that determines whether the certificate requester is authorized to receive the type of

certificate they have requested. The certificate subject name can be generated automatically from the information in Active Directory or supplied explicitly by the requestor.

The policy module adds a predefined list of certificate extensions to the issued certificate. The extensions are defined by the certificate template. This reduces the amount of information a certificate requester has to provide about the

certificate and its intended use. http://technet.microsoft.com/en-us/library/cc780501%28WS.10%29.aspx Stand-alone certification authorities

You can install Certificate Services to create a stand-alone certification authority (CA). Stand-alone CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail

Extensions) and authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

A stand-alone CA has the following characteristics:

Unlike an enterprise CA, a stand-alone CA does not require the use of the Active Directory directory service. Stand-alone CAs are primarily intended to be used as Trusted Offline Root CAs in a CA hierarchy or when extranets and the Internet

are involved. Additionally, if you want to use a custom policy module for a CA, you would first install a stand-alone CA and then replace the stand-alone policy module with your custom policy module.

When submitting a certificate request to a stand-alone CA, a certificate requester must explicitly supply all identifying information about themselves and the type of certificate that is wanted in the certificate request. (This does not need to be

done when submitting a request to an enterprise CA, since the enterprise user\\'s information is already in Active Directory and the certificate type is described by a certificate template). The authentication information for requests is obtained

from the local computer\\'s Security Accounts Manager database.

By default, all certificate requests sent to the stand-alone CA are set to Pending until the administrator of the stand-alone CA verifies the identity of the requester and approves the request. This is done for security reasons, because the

certificate requester\\'s credentials are not verified by the stand-alone CA.

Certificate templates are not used.

No certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards, but other types of certificates can be issued and stored on a smart card. The administrator has to explicitly distribute the stand-alone

CA\\'s certificate to the domain user\\'s trusted root store or users must perform that task themselves. When a stand-alone CA uses Active Directory, it has these additional features:

If a member of the Domain Administrators group or an administrator with write access to Active Directory, installs a stand-alone root CA, it is automatically added to the Trusted Root Certification Authorities certificate store for all users and

computers in the domain. For this reason, if you install a stand-alone root CA in an Active Directory domain, you should not change the default action of the CA upon receiving certificate requests (which marks requests as Pending).

Otherwise, you will have a trusted root CA that automatically issues certificates without verifying the identity of the certificate requester.

If a stand-alone CA is installed by a member of the Domain Administrators group of the parent domain of a tree in the enterprise, or by an administrator with write access to Active Directory, then the stand- alone CA will publish its CA

certificate and the certificate revocation list (CRL) to Active Directory.

QUESTION 3

Your company has a server that runs Windows Server 2008 R2. Active Directory Certificate Services (AD CS) is configured as a standalone Certification Authority (CA) on the server.

You need to audit changes to the CA configuration settings and the CA security settings.

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

A. Configure auditing in the Certification Authority snap-in.

B. Enable auditing of successful and failed attempts to change permissions on files in the %SYSTEM32%\CertSrv directory.

C. Enable auditing of successful and failed attempts to write to files in the %SYSTEM32%\CertLog directory.

D. Enable the Audit object access setting in the Local Security Policy for the Active Directory Certificate Services (AD CS) server.

Correct Answer: AD

http://technet.microsoft.com/en-us/library/cc772451.aspx Configure CA Event Auditing

You can audit a variety of events relating to the management and activities of a certification authority (CA):

Back up and restore the CA database.

Change the CA configuration.

Change CA security settings.

Issue and manage certificate requests.

Revoke certificates and publish certificate revocation lists (CRLs).

Store and retrieve archived keys.

Start and stop Active Directory Certificate Services (AD CS).

To configure CA event auditing

1.

Open the Certification Authority snap-in.

2.

In the console tree, click the name of the CA.

3.

On the Action menu, click Properties.

4.

On the Auditing tab, click the events that you want to audit, and then click OK.

5.

On the Action menu, point to All Tasks, and then click Stop Service.

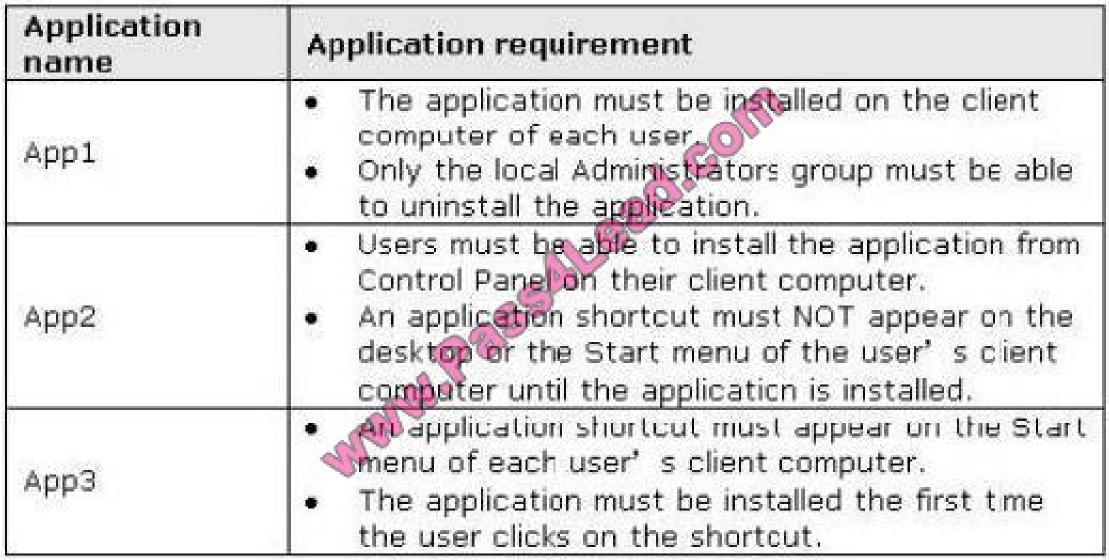
6.

On the Action menu, point to All Tasks, and then click Start Service.

Additional considerations To audit events, the computer must also be configured for auditing of object access. Audit policy options can be viewed and managed in local or domain Group Policy under Computer Configuration\Windows Settings\Security Settings\Local Policies.

QUESTION 4

Your network contains an Active Directory forest named contoso.com. You need to use Group Policies to deploy the applications shown in the following table.

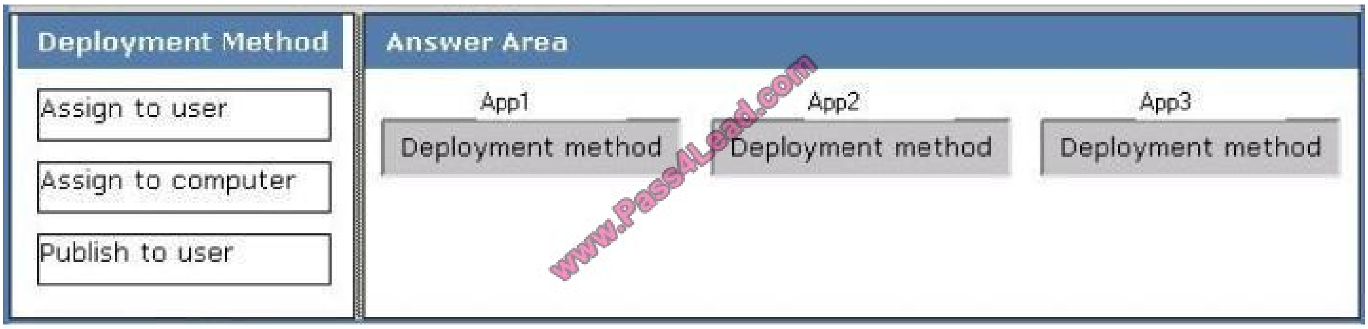


Application name	Application requirement
App1	• The application must be installed on the client computer of each user. • Only the local Administrators group must be able to uninstall the application.
App2	• Users must be able to install the application from Control Panel on their client computer. • An application shortcut must NOT appear on the desktop or the Start menu of the user’ s client computer until the application is installed.
App3	• An application shortcut must appear on the Start menu of each user’ s client computer. • The application must be installed the first time the user clicks on the shortcut.

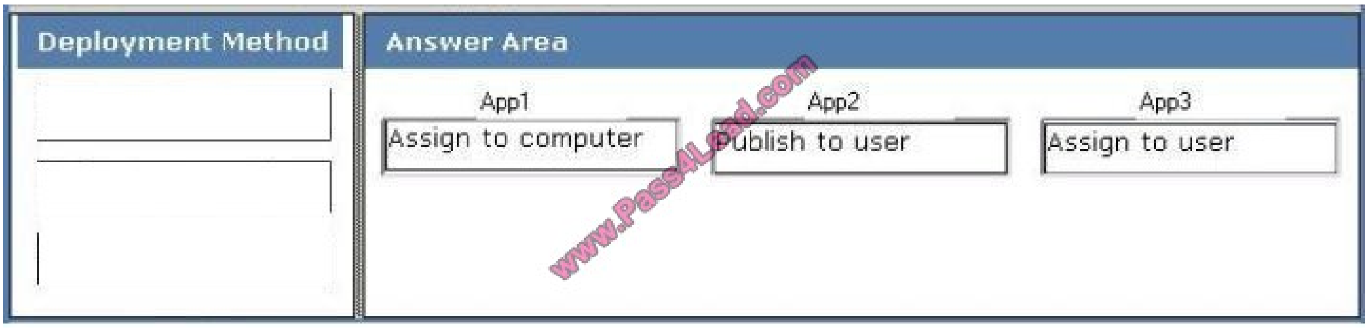
What should you do?

To answer, drag the appropriate deployment method to the correct application in the answer area.

Select and Place:



Correct Answer:



App1: Assign to computer

App2: Publish to user

App3: Assign to user

Reference:

technet.microsoft.com/en-us/library/cc783502.aspx

Software installation 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.

Assigning Applications

When you assign applications to users or computers, the applications are automatically installed on their computers at logon (for user-assigned applications) or startup (for computer-assigned 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 the Start menu, 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, Windows XP Professional and Windows Server

2003 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 Windows 2000, 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.

Publishing Applications

You can also publish applications to users, making the application available for users to install.

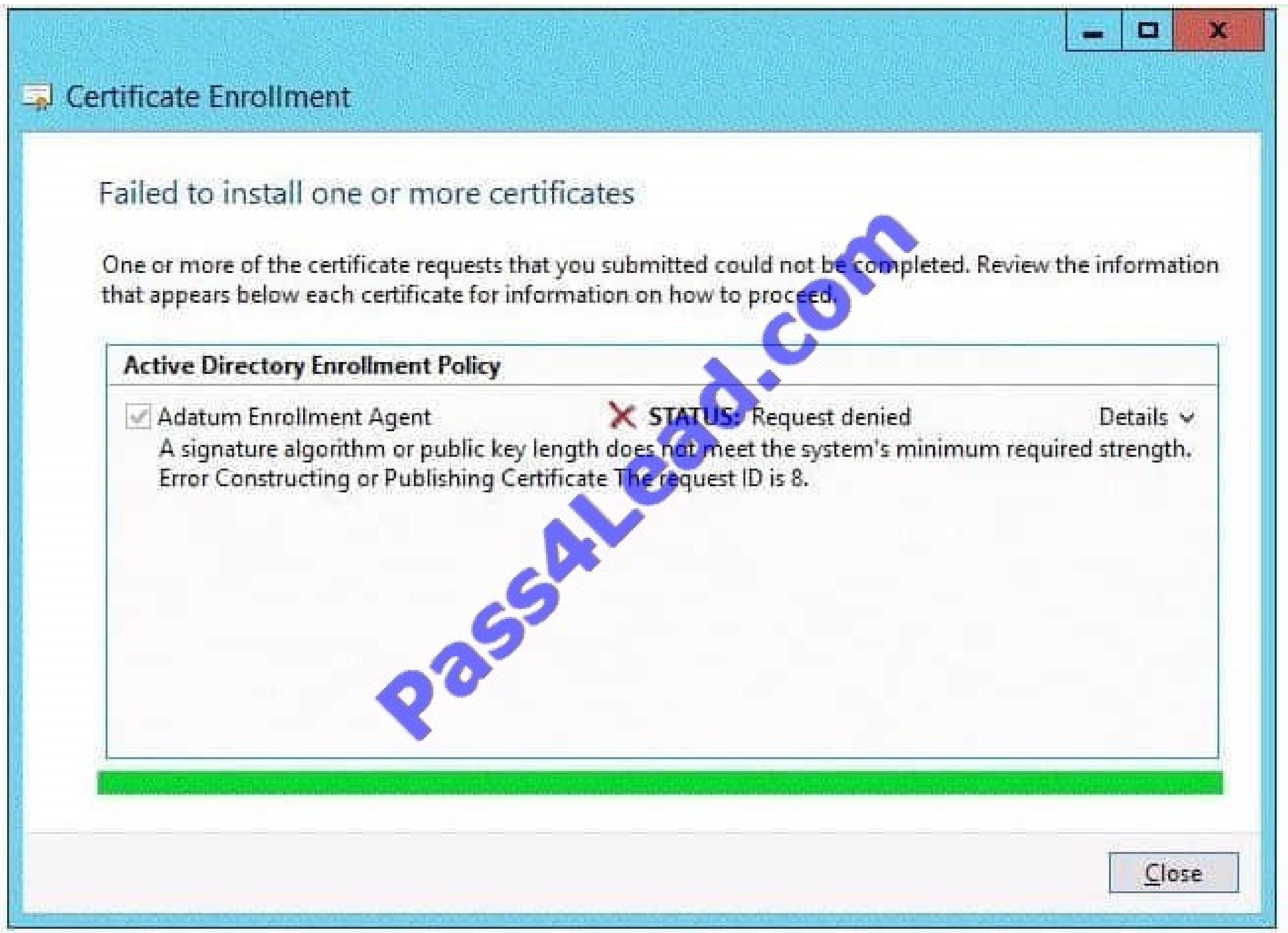
To install a published application, users can use Add or Remove Programs in Control Panel, which includes a list of all published applications that are available for them to install.

Alternatively, if the administrator has selected the Auto-install this application by file extension activation feature, users can open a document file associated with a published application. For example, double clicking an .xls file will trigger the

installation of Microsoft Excel, if it is not already installed. Publishing applications only applies to user policy; you cannot publish applications to computers.

QUESTION 5

Your network contains an Active Directory domain named adatum.com. The domain contains an enterprise certification authority (CA). When submitting a request for a certificate based on the EnrollmentAgent template, you receive the error message shown in the exhibit. (Click the Exhibit button.)



Failed to install one or more certificates

One or more of the certificate requests that you submitted could not be completed. Review the information that appears below each certificate for information on how to proceed.

Active Directory Enrollment Policy

☑ Adatum Enrollment Agent ☒ **STATUS:** Request denied Details ⌄

A signature algorithm or public key length does not meet the system's minimum required strength. Error Constructing or Publishing Certificate The request ID is 8.

You need to ensure that you can enroll for the certificate successfully. What should you modify?

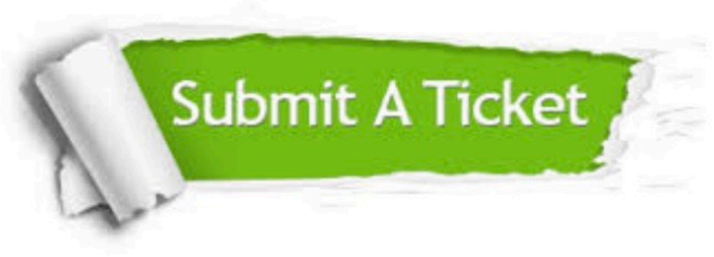
A. the Security settings of the issuing CA

B. the Cryptography settings of the certificate template

C. the Security settings of the certificate template

D. the Enrollment Agents settings of the issuing CA

Correct Answer: B


Submit A Ticket

100%