Microsoft 70-648

TS: Upgrading from Windows Server 2003 MCSA to, Windows Server 2008, Technology Specializations

Version: 46.0

Topic 1, Volume A

QUESTION NO: 1

Your network contains an Active Directory domain. The relevant servers in the domain are configured as shown in the following table:

Server name	Operating System	Server role
Server1	Windows 2008	Domain controller
Server2	Windows 2008 R2	Enterprise root certification authority (CA)
Server3	Windows 2008 R2	Network Device Enrollment Service (NDES)

You need to ensure that all device certificate requests use the MD5 hash algorithm.

What should you do?

A. On Server2, run the Certutil tool.
B. On Server1, update the CEP Encryption certificate template.
C. On Server1, update the Exchange Enrollment Agent (Offline Request) template.
D. On Server3, set the value of the HKLM\Software\Microsoft\Cryptography\MSCEP\ HashAlgorithm \HashAlgorithm registry key.

Answer: D
Explanation:

QUESTION NO: 2

Your network contains an Active Directory domain. You have a server named Server1 that runs Windows Server 2008 R2. Server1 is an enterprise root certification authority (CA). You have a client computer named Computer1 that runs Windows 7. You enable automatic certificate enrollment for all client computers that run Windows 7.

You need to verify that the Windows 7 client computers can automatically enroll for certificates.

Which command should you run on Computer1?

A. certreq.exe retrieve
B. certreq.exe submit

C. certutil.exe getkey
D. certutil.exe pulse

Answer: D

Explanation:

QUESTION NO: 3

Your network contains two Active Directory forests named contoso.com and adatum.com. The functional level of both forests is Windows Server 2008 R2. Each forest contains one domain. Active Directory Certificate Services (AD CS) is configured in the contoso.com forest to allow users from both forests to automatically enroll user certificates.

You need to ensure that all users in the adatum.com forest have a user certificate from the contoso.com certification authority (CA).

What should you configure in the adatum.com domain?

A. From the Default Domain Controllers Policy, modify the Enterprise Trust settings.
B. From the Default Domain Controllers Policy, modify the Trusted Publishers settings.
C. From the Default Domain Policy, modify the Certificate Enrollment policy.
D. From the Default Domain Policy, modify the Trusted Root Certification Authority settings.

Answer: C

Explanation:

QUESTION NO: 4

You have a server named Server1 that has the following Active Directory Certificate Services (AD CS) role services installed:

- Enterprise root certification authority (CA)
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

You create a new certificate template. External users report that the new template is unavailable when they request a new certificate. You verify that all other templates are available to the external users.

You need to ensure that the external users can request certificates by using the new

template.

What should you do on Server1?

A. Run iisreset.exe /restart.
B. Run gpupdate.exe /force.
C. Run certutil.exe dspublish.
D. Restart the Active Directory Certificate Services service.

Answer: A
Explanation:

QUESTION NO: 5

Your network contains an enterprise root certification authority (CA).

You need to ensure that a certificate issued by the CA is valid.

What should you do?

A. Run syskey.exe and use the Update option.
B. Run sigverif.exe and use the Advanced option.
C. Run certutil.exe and specify the -verify parameter.
D. Run certreq.exe and specify the -retrieve parameter.

Answer: C
Explanation:

QUESTION NO: 6

You have an enterprise subordinate certification authority (CA). The CA issues smart card logon certificates.

Users are required to log on to the domain by using a smart card.

Your company's corporate security policy states that when an employee resigns, his ability to log on to the network must be immediately revoked.

An employee resigns.

You need to immediately prevent the employee from logging on to the domain.

What should you do?

A. Revoke the employee's smart card certificate.
B. Disable the employee's Active Directory account.
C. Publish a new delta certificate revocation list (CRL).
D. Reset the password for the employee's Active Directory account.

Answer: B
Explanation:

QUESTION NO: 7

Your network contains a server that runs Windows Server 2008 R2. The server is configured as an enterprise root certification authority (CA).

You have a Web site that uses x.509 certificates for authentication. The Web site is configured to use a manyto-one mapping.

You revoke a certificate issued to an external partner.

You need to prevent the external partner from accessing the Web site.

What should you do?

A. Run certutil.exe -crl.
B. Run certutil.exe -delkey.
C. From Active Directory Users and Computers, modify the membership of the IIS_IUSRS group.
D. From Active Directory Users and Computers, modify the Contact object for the external partner.

Answer: A
Explanation:

QUESTION NO: 8
You have an Active Directory domain that runs Windows Server 2008 R2.

You need to implement a certification authority (CA) server that meets the following requirements:

- Allows the certification authority to automatically issue certificates
- Integrates with Active Directory Domain Services

What should you do?

A. Purchase a certificate from a third-party certification authority. Import the certificate into the computer store of the schema master.
B. Install and configure the Active Directory Certificate Services server role as a Standalone Root CA.
C. Purchase a certificate from a third-party certification authority. Install and configure the Active Directory Certificate Services server role as a Standalone Subordinate CA.
D. Install and configure the Active Directory Certificate Services server role as an Enterprise Root CA.

Answer: D
Explanation:

QUESTION NO: 9

Your company has an Active Directory forest. You plan to install an Enterprise certification authority (CA) on a dedicated stand-alone server.

When you attempt to add the Active Directory Certificate Services (AD CS) server role, you find that the

Enterprise CA option is not available.

You need to install the AD CS server role as an Enterprise CA.

What should you do first?

A. Add the DNS Server server role.
B. Join the server to the domain.
C. Add the Web Server (IIS) server role and the AD?CS server role.
D. Add the Active Directory Lightweight Directory Services (AD?LDS) server role.

Answer: B
Explanation:

QUESTION NO: 10

You have a Windows Server 2008 R2 that has the Active Directory Certificate Services server role installed.

You need to minimize the amount of time it takes for client computers to download a certificate revocation list (CRL).

What should you do?

A. Install and configure an Online Responder.
B. Install and configure an additional domain controller.
C. Import the Root CA certificate into the Trusted Root Certification Authorities store on all client workstations.
D. Import the Issuing CA certificate into the Trusted Root Certification Authorities store on all client workstations.

Answer: A
Explanation:

QUESTION NO: 11

You have a Windows Server 2008 R2 Enterprise Root CA . Security policy prevents port 443 and port 80 from being opened on domain controllers and on the issuing CA

You need to allow users to request certificates from a Web interface. You install the Active Directory Certificate Services (AD CS) server role.

What should you do next?

A. Configure the Online Responder Role Service on a member server.
B. Configure the Online Responder Role Service on a domain controller.
C. Configure the Certificate Enrollment Web Service role service on a member server.
D. Configure the Certificate Enrollment Web Service role service on a domain controller.

Answer: C
Explanation:

QUESTION NO: 12

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.

Answer: A,D
Explanation:

QUESTION NO: 13

Your company has an Active Directory domain. You install an Enterprise Root certification authority (CA) on a member server named Server1.

You need to ensure that only the Security Manager is authorized to revoke certificates that are supplied by Server1.

What should you do?

A. Remove the Request Certificates permission from the Domain Users group.
B. Remove the Request Certificates permission from the Authenticated Users group.
C. Assign the Allow - Manage CA permission to only the Security Manager user account.
D. Assign the Allow - Issue and Manage Certificates permission to only the Security Manageruser account.

Answer: D
Explanation:

QUESTION NO: 14

You have a Windows Server 2008 R2 Enterprise Root certification authority (CA).

You need to grant members of the Account Operators group the ability to only manage Basic EFS certificates.

You grant the Account Operators group the Issue and Manage Certificates permission on the CA.

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

A. Enable the Restrict Enrollment Agents option on the CA .
B. Enable the Restrict Certificate Managers option on the CA .
C. Add the Basic EFS certificate template for the Account Operators group.
D. Grant the Account Operators group the Manage CA permission on the CA .
E. Remove all unnecessary certificate templates that are assigned to the Account Operators group.

Answer: B,C,E
Explanation:

QUESTION NO: 15

You have two servers named Server1 and Server2. Both servers run Windows Server 2008 R2. Server1 is configured as an enterprise root certification authority (CA). You install the Online Responder role service on Server2.

You need to configure Server1 to support the Online Responder.

What should you do?

A. Import the enterprise root CA certificate.
B. Configure the Certificate Revocation List Distribution Point extension.
C. Configure the Authority Information Access (AIA) extension.
D. Add the Server2 computer account to the CertPublishers group.

Answer: C
Explanation: To configure online responder role service on S1, you should configure AIA extension.
The authority information access extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may

include on-line validation services and CA policy data. (The location of CRLs is not specified in this extension; that information is provided by the cRLDistributionPoints extension.) This extension may be included in subject or CA certificates, and it MUST be non-critical

QUESTION NO: 16

Your company has an Active Directory domain. All servers run Windows Server 2008 R2. Your company runs an Enterprise Root certification authority (CA).

You need to ensure that only administrators can sign code.

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

A. Publish the code signing template.
B. Edit the local computer policy of the Enterprise Root CA to allow users to trust peer certificates and allow only administrators to apply the policy.
C. Edit the local computer policy of the Enterprise Root CA to allow only administrators to manage Trusted Publishers.
D. Modify the security settings on the template to allow only administrators to request code signing certificates.

Answer: A,D
Explanation:

QUESTION NO: 17

Your company has an Active Directory domain. All servers run Windows Server 2008 R2. Your company uses an Enterprise Root certification authority (CA) and an Enterprise Intermediate CA.

The Enterprise Intermediate CA certificate expires.

You need to deploy a new Enterprise Intermediate CA certificate to all computers in the domain.

What should you do?