ISLEVER

72-640

TS: Windows Server 2008 Active Directory, Configuring

DEMO

https://www.islever.com/72-640.html

https://www.islever.com/microsoft.html

Note: The answer is for reference only, you need to understand all question.

QUESTION 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

Question 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

Question 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

Question 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

Question 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

Question 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

Question 7
You add an Online Responder to an Online Responder Array. You need to ensure that the new Online Responder resolves synchronization conflicts for all members of the Array.

What should you do?

A. From Network Load Balancing Manager, set the priority ID of the new Online Responder to 1.
B. From Network Load Balancing Manager, set the priority ID of the new Online Responder to 32.