



**83-640**

**Windows Server 2008 Active Directory, Configuring**

Q&A

DEMO Version

Copyright (c) 2010 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION 1**

Your company, Contoso, Ltd, has offices in North America and Europe. Contoso has an Active Directory forest that has three domains. You need to reduce the time required to authenticate users from the labs.eu.contoso.com domain when they access resources in the eng.na.contoso.com domain. What should you do?

- A. Decrease the replication interval for all Connection objects.
- B. Decrease the replication interval for the DEFAULTIPSITELINK site link.
- C. Set up a one-way shortcut trust from eng.na.contoso.com to labs.eu.contoso.com.
- D. Set up a one-way shortcut trust from labs.eu.contoso.com to eng.na.contoso.com.

**Answer: C**

**Explanation/Reference:**

A one-way, incoming, shortcut trust allows users in your domain (the domain that you are logged on to at the time that you run the New Trust Wizard) to more quickly access resources in another domain (which is nested within another domain tree) in your forest. For example, if you are the administrator of sales.wingtiptoys.com and users in that domain need to access resources in the marketing.tailspintoys.com domain (which is a child domain of the tailspintoys.com tree root domain), you can use this procedure to establish one side of the relationship so that users in your domain can more quickly access resources in the marketing.tailspintoys.com domain.

You can create this shortcut trust by using the New Trust Wizard in Active Directory Domains and Trusts or by using the Netdom command-line tool.

**QUESTION 2**

Your company has an Active Directory domain. You log on to the domain controller. The Active Directory Schema snap-in is not available in the Microsoft Management Console (MMC). You need to access the Active Directory Schema snap-in. What should you do?

- A. Register Schmmgml.dll.
- B. Log off and log on again by using an account that is a member of the Schema Administrators group.
- C. Use the Ntdsutil.exe command to connect to the Schema Master operations master and open the schema for writing.
- D. Add the Active Directory Lightweight Directory Services (AD LDS) role to the domain controller by using Server Manager.

**Answer: A**

**Explanation/Reference:****Regsvr32**

Registers .dll files as command components in the registry.

**QUESTION 3**

Your company has an Active Directory domain named contoso.com. The company network has two DNS servers named DNS1 and DNS2.

The DNS servers are configured as shown in the following table.

DNS1	DNS2
_msdcs.contoso.com contoso.com	.(root) _msdcs.contoso.com contoso.com

Domain users, who are configured to use DNS2 as the preferred DNS server, are unable to connect to Internet Web sites.

You need to enable Internet name resolution for all client computers.

What should you do?

- A. Create a copy of the .(root) zone on DNS1.
- B. Update the list of root hints servers on DNS2.
- C. Update the Cache.dns file on DNS2 Configure conditional forwarding on DNS1.
- D. Delete the .(root) zone from DNS2. Configure conditional forwarding on DNS2.

**Answer: D**

**Explanation/Reference:**

**Delete the .(root) zone**

When you install DNS on a Windows 2008 server that does not have a connection to the Internet, the zone for the domain is created and a root zone, also known as a **dot** zone, is also created. This root zone may prevent access to the Internet for DNS and for clients of the DNS. If there is a root zone, there are no other zones other than those that are listed with DNS, and you cannot configure forwarders or root hint servers. For these reasons, you may have to remove the root zone.

**Configure DNS Server Forwarders**

You can use this procedure to configure Domain Name System (DNS) server forwarders.

When you add a new domain controller that is a DNS server, if your network uses forwarding for recursive name resolution, configure DNS server forwarders based on the forwarding method that is established on your network. When forwarders are configured, a DNS server that receives a DNS query for a name for which it is not authoritative forwards the request to the DNS forwarder instead of using root hints. If your network uses forwarding, use the DNS snap-in to add the appropriate forwarders on the new domain controller. If you want the DNS Server service on the new domain controller to forward queries to different servers depending on the DNS suffix that is specified in the query, configure conditional forwarding appropriately.

**QUESTION 4**

Your company has a single Active Directory domain. All domain controllers run Windows Server 2003 You install Windows Server 2008 on a server. You need to add the new server as a domain controller in your domain.What should you do first?

- A. On the new server, run dcpromo /adv.
- B. On the new server, run dcpromo /createdcaccount.
- C. On a domain controller run adprep /rodcprep.
- D. On a domain controller, run adprep /forestprep.

**Answer: D**

**Explanation/Reference:**

**Adprep /forestprep**

Extends the Active Directory® schema and updates permissions as necessary to prepare a forest and domain for a domain controller that runs the Windows Server® 2008 operating system.

Adprep.exe is a command-line tool that is available on the Windows Server 2008 installation disc in the \sources\adprep folder, and it is available on the Windows Server 2008 R2 installation disk in the \support\adprep folder. You must run **adprep** from an elevated command prompt. To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

**QUESTION 5**

Your company has an Active Directory domain. All servers run Windows Server 2008. Your company uses an Enterprise Root certificate authority (CA). You need to ensure that revoked certificate information is highly available. What should you do?

- A. Implement an Online Certificate Status Protocol (OCSP) responder by using Network Load Balancing.
- B. Implement an Online Certificate Status Protocol (OCSP) responder by using an Internet Security and Acceleration Server array.
- C. Publish the trusted certificate authorities list to the domain by using a Group Policy Object (GPO).
- D. Create a new Group Policy Object (GPO) that allows users to trust peer certificates. Link the GPO to the domain.

**Answer: A**

**Explanation/Reference:**

**What does OCSP support do?**

The use of Online Responders that distribute OCSP responses, along with the use of CRLs, is one of two common methods for conveying information about the validity of certificates. Unlike CRLs, which are distributed periodically and contain information about all certificates that have been revoked or suspended, an Online Responder receives and responds only to requests from clients for information about the status of a single certificate. The amount of data retrieved per request remains constant no matter how many revoked certificates there might be.

In many circumstances, Online Responders can process certificate status requests more efficiently than by using CRLs. For example:

Clients connect to the network remotely and either do not need nor have the high-speed connections required to download large CRLs.

A network needs to handle large peaks in revocation checking activity, such as when large numbers of users log on or send signed e-mail simultaneously.

An organization needs an efficient means to distribute revocation data for certificates issued from a non-Microsoft CA.

An organization wants to provide only the revocation checking data needed to verify individual certificate status requests, rather than make available information about all revoked or suspended certificates.

**Who will be interested in this feature?**

This feature applies to organizations that have PKIs with one or more Windows-based CAs.

Adding one or more Online Responders can significantly enhance the flexibility and scalability of an organization's PKI; therefore, this feature should interest PKI architects, planners, and administrators.

In order to install an Online Responder, you must be an administrator on the computer where the Online Responder will be installed.

**QUESTION 6**

You have a Windows Server 2008 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 AD CS 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 Certification Authority Web Enrollment Role Service on a member server.
- D. Configure the Certification Authority Web Enrollment Role Service on a domain controller.

**Answer: C**

**Explanation/Reference:**

Active Directory Certificate Services (AD CS) Web enrollment support can be installed on any computer running Windows Server 2008 R2 Standard, Windows Server 2008 R2 Enterprise, Windows Server 2008 R2 Datacenter, Windows Server 2008 Standard, Windows Server 2008 Enterprise, or Windows Server 2008 Datacenter. The certificate enrollment data can come from a certification authority (CA) on a computer running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003, or from a non-Microsoft CA.

The following procedure can be used if none of the AD CS role services (such as a CA) have been installed on this computer.

Membership in **Domain Admins**, or equivalent, is the minimum required to complete this procedure. For more information, see Implement Role-Based Administration.

**To install Web enrollment support**

Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.

Click **Manage Roles**. Under **Active Directory Certificate Services**, click **Add role services**. If a different AD CS role service has already been installed on this computer, select the **Active Directory Certificate Services** check box in the **Role Summary** pane, and then click **Add role services**.

On the **Select Role Services** page, select the **Certification Authority Web Enrollment** check box.

Click **Add required role services**, and then click **Next**.

On the **Specify CA** page, if a CA is not installed on this computer, click **Browse** to select the CA that you

want to associate with Web enrollment, click **OK**, and then **Next**.

Click **Next**, review the information listed, and click **Next** again.

On the **Confirm Installation Options** page, click **Install**.

When the installation is complete, review the status page to verify that the installation was successful.

#### **Additional considerations**

Installation of the Web enrollment pages configures the computer as a registration authority. This computer is also known as a "CA Web proxy" or a "Web enrollment station."

#### **QUESTION 7**

Your company uses a Windows 2008 Enterprise certificate authority (CA) to issue certificates. You need to implement key archival. What should you do?

- A. Archive the private key on the server.
- B. Apply the Hisecdc security template to the domain controllers.
- C. Configure the certificate for automatic enrollment for the computers that store encrypted files.
- D. Install an Enterprise Subordinate CA and issue a user certificate to users of the encrypted files.

**Answer:** A

#### **Explanation/Reference:**

Active Directory Certificate Services (AD CS) requires key recovery agent certificates, exchange (XCHG) certificates, and keys in order to support key archival. The functioning of key recovery agent certificates, XCHG certificates, and the cryptographic service providers (CSPs) needed to create them is critical to a public key infrastructure.

#### **QUESTION 8**

Your company has an Active Directory domain. You plan to install the Active Directory Certificate Service (AD CS) role on a member server that runs Windows Server 2008. 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. Install the AD CS role and configure it as an Enterprise Root CA.
- B. Install the AD CS role and configure it as a Standalone CA.
- C. Restrict enrollment agents for the Smartcard logon certificate to the Account Operator group.
- D. Restrict certificate managers for the Smartcard logon certificate to the Account Operator group.
- E. Create a Smartcard logon certificate.
- F. Create an Enrollment Agent certificate.

**Answer:** ACE

#### **Explanation/Reference:**

##### **Requirements**

Smart Card Authentication to Active Directory requires that Smartcard workstations, Active Directory, and Active Directory domain controllers be configured properly. Active Directory must trust a certification authority to authenticate users based on certificates from that CA. Both Smartcard workstations and domain controllers must be configured with correctly configured certificates.

As with any PKI implementation, all parties must trust the Root CA to which the issuing CA chains. Both the domain controllers and the smartcard workstations trust this root.

##### **Active Directory and domain controller configuration**

Required: Active Directory must have the third-party issuing CA in the NTAAuth store to authenticate users to active directory.

Required: Domain controllers must be configured with a domain controller certificate to authenticate smartcard users.

Optional: Active Directory can be configured to distribute the third-party root CA to the trusted root CA store of all domain members using the Group Policy.

##### **Smartcard certificate and workstation requirements**

Required: All of the smartcard requirements outlined in the "Configuration Instructions" section must be met, including the text formatting of the fields. Smartcard authentication fails if they are not met.  
 Required: The smartcard and private key must be installed on the smartcard.

### QUESTION 9

Your company has a server that runs Windows Server 2008. Certification Services is configured as a stand-alone 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 Services 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 Certification Services server.

**Answer:** AD

**Explanation/Reference:**

#### **Auditing certification services**

This security policy setting determines whether the operating system generates events when Active Directory Certificate Services (AD CS) operations are performed, such as:

AD CS starts, shuts down, is backed up, or is restored.

- Certificate revocation list (CRL)-related tasks are performed.
- Certificates are requested, issued, or revoked.
- Certificate manager settings for AD CS are changed.
- The configuration and properties of the certification authority (CA) are changed.
- AD CS templates are modified.
- Certificates are imported.
- A CA certificate is published to Active Directory Domain Services.
- Security permissions for AD CS role services are modified.
- Keys are archived, imported, or retrieved.
- The OCSP Responder Service is started or stopped.

Monitoring these operational events is important to ensure that AD CS role services are functioning properly.

Event volume: Low to medium on servers hosting AD CS role services

Default: Not configured

#### **Audit object access setting**

This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified. If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.

To set this value to **No auditing**, in the **Properties** dialog box for this policy setting, select the **Define these policy settings** check box and clear the **Success** and **Failure** check boxes.

Note that you can set a SACL on a file system object using the **Security** tab in that object's **Properties** dialog box.

**Default:** No auditing.

#### **Configuring this security setting**

You can configure this security setting by opening the appropriate policy and expanding the console tree as such: Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\

### QUESTION 10

Your company has an Active Directory forest that contains multiple domain controllers. The domain controllers run Windows Server 2008.

You need to perform an authoritative restore of a deleted organizational unit and its child objects.

Which four actions should you perform in sequence? (To answer, move the appropriate four actions from the list of actions to the answer area, and arrange them in the correct order.)

Ordered List Title	Answer Choices Title
<div style="border: 1px solid gray; height: 260px; width: 100%;"></div>	<p>Use the Nldsutil utility to mark the organizational unit as authoritative.</p> <p>Use the Dsadd utility to recreate the organizational unit.</p> <p>Restart the domain controller in safe Mode.</p> <p>Restore the system state data to a date before the organizational unit was deleted.</p> <p>Restart the domain controller.</p> <p>Restart the domain controller in Directory Services Restore Mode (DSRM).</p>
<< Move Remove >>	

**Answer:**

Restart the domain controller in Directory Services Restore Mode (DSRM).

Restore the system state data to a date before the organizational unit was deleted.

Use the Nldsutil utility to mark the organizational unit as authoritative.

Restart the domain controller.

**Explanation/Reference:**