

Lesson 19: Installing and Configuring Active Directory Certificate Services

MOAC 70-412: Configuring Advanced
Windows Server 2012 Services

Overview

- Objective 6.2 – Install and configure Active Directory Certificate Services (AD CS).
 - Install an Enterprise Certificate Authority (CA)
 - Configure CRL distribution points
 - Install and configure Online Responder
 - Implement administrative role separation
 - Configure CA backup and recovery

Understanding the Active Directory Certificate Services

Lesson 19: Installing and Configuring Active
Directory Certificate Services

Active Directory Certificate Services (AD CS)

- **Active Directory Certificate Services (AD CS)** is a server role that allows you to issue and manage digital certificates as part of a public key infrastructure.
- A **Public key infrastructure (PKI)**
 - Is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates.
 - Consists of certification authorities (CAs) and registration authorities that verify and authenticate the validity of each entity involved in an electronic transaction through the use of public key cryptography.
- Within the PKI, the **certificate authority (CA)** binds a public key with respective user identities and issues digital certificates containing the public key.

Digital Certificate

- A **digital certificate**
 - Is an electronic document that contains an identity, such as a user or organization name, along with a corresponding public key.
 - Can also be used for authentication because digital certificates are used to prove a person's or computer's identity.
 - Is similar to a driver's license or passport because it contains a user's photograph and thumbprint leaving no doubt about the user's identity.

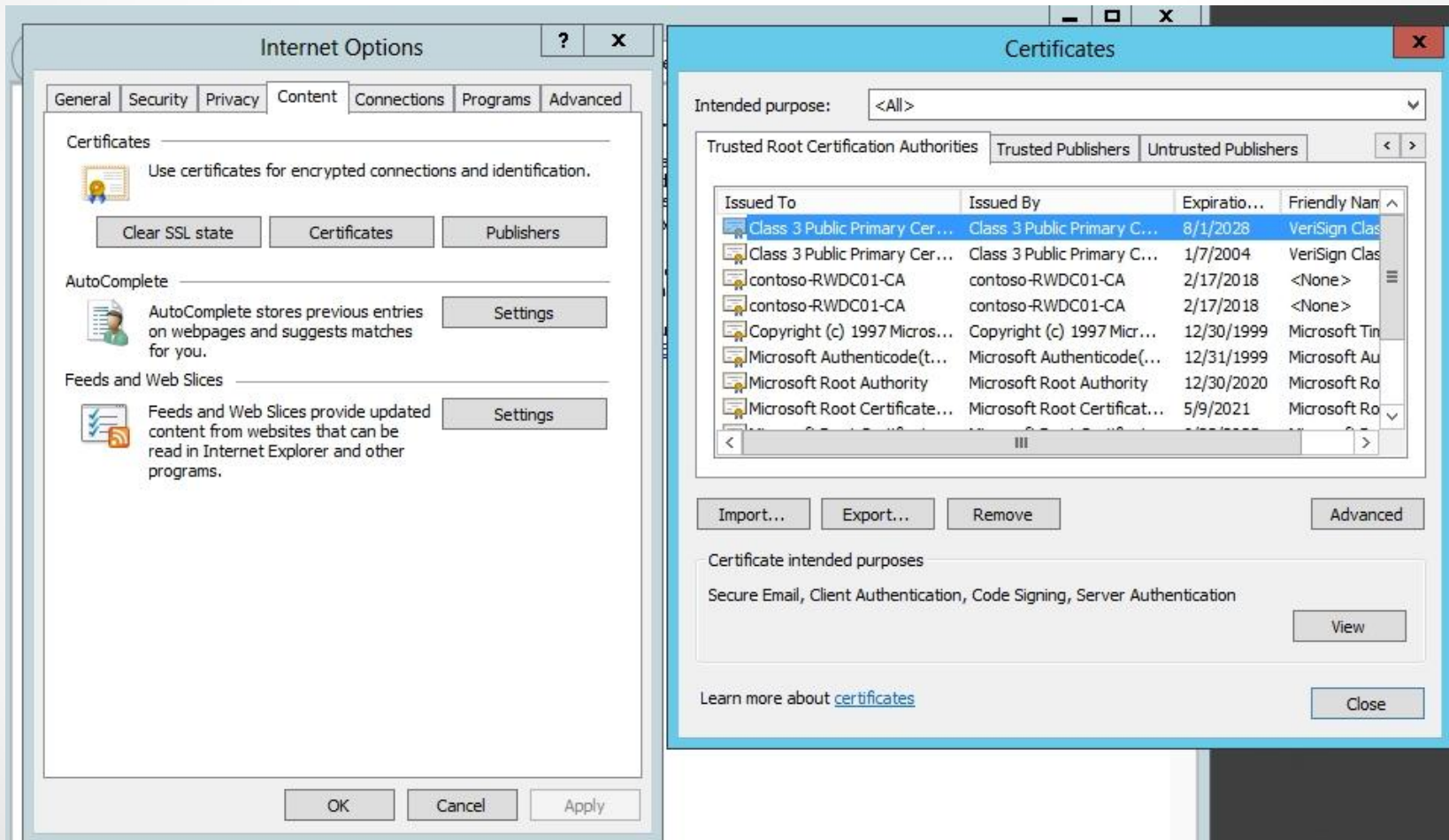
Benefits of the PKI

- **Confidentiality:** The PKI allows you to encrypt data that is stored or transmitted.
- **Integrity:** A digital signature identifies whether the data is modified while the data is transmitted.
- **Authenticity:** A message digest is digitally signed using the sender's private key. Because the digest can be decrypted only with the sender's corresponding public key, it proves that the message can come only from the sending user (non-repudiation).

Trusting CA

- For the PKI system to work, the CA must be trusted.
- Typically within an organization, you can install a CA on Windows Server, and it would be trusted within your organization.
- If you require a CA that is trusted outside your organization, you have to use a trusted third-party CA.
- Established commercial CAs charge to issue certificates that will automatically be trusted by most web browsers.

Trusting CA



Certificate Authority

- The CA is a Windows Server 2012 server role that
 - Verifies the identity of the certificate requestors.
 - Issues certificates to requesting users, computers, and services.
 - Manages certificate revocation.

Certificate Authority

- Role services of the AD CS role include:
 - **CA**: The component that issues certificates to users, computers, and services and manages certificate validity.
 - **CA Web Enrollment**: The component that provides a method to issue and renew certificates for users, computers, and devices that are not joined to the domain, are not connected directly to the network, or are for users of non-Windows operating systems.
 - **Online Responder**: The component that configures and manages Online Certificate Status Protocol (OCSP), which is used to validate and revoke certificates.

Certificate Authority

- **Network Device Enrollment Service:** The component that can be used to assign certificates to routers, switches, and other network devices.
- **Certificate Enrollment Web Service:** The component that allows computers to connect to a CA using a web browser to request, renew, and install issued certificates; retrieve CRLs; download a root certificate; and enroll over the Internet or across forests.
- **Certificate Authority Policy Web Service:** The component that enables users to obtain certificate enrollment policy information.

Certificate Authority

- When you install a CA, you have the following choices:
 - Stand-alone CA or Enterprise CA
 - Root CA or Subordinate CA

Stand-Alone CA

- The ***stand-alone CA*** works without Active Directory and does not need Active Directory.
- However, the server can be a member of a domain.
- Users can request certificates using a manual procedure or web enrollment, where they identify information and specify the certificate they need.
- By default, all certificate requests submitted to stand-alone CAs are held in a pending queue until a CA administrator approves them.
- However, you can configure stand-alone CAs to issue certificates automatically upon request, but this is less secure and is usually not recommended.

Enterprise CA

- An **enterprise CA** requires Active Directory and is typically used to issue certificates to users, computers, devices, and servers for an organization.
- Users can request certificates using manual enrollment, web enrollment, auto-enrollment, or an enrollment agent.
- Because information for a user or computer can be retrieved from Active Directory, templates can be used to generate certificates with the appropriate attributes for the specified certificate type.

Root CA

- The **root CA** is at the top of the certificate hierarchy.
- Because everything branches from the root, it is trusted by all clients within an organization.
- Smaller organizations may only have one CA; larger organizations could have a root CA with multiple subordinate CAs.
- Although the enterprise CA can issue certificates to end users, it is usually used to issue certificates to subordinate CAs.

Subordinate CAs

- There is only one root CA, but there can be one or more **subordinates CAs**.
- The number of subordinate CAs needed is determined by geographical location and number of clients.
- If a CA is compromised, all certificates issued by the CA and any subordinate CAs under the compromised CA (including any corresponding issued certificates) are also considered compromised.

AIA and CRL Distribution Points

- After a CA is installed, and before the CA issues any certificates, you must configure the **Authority Information Access (AIA) extension** and **CRL distribution point (CDP) extension**.
- They are necessary to validate the certificates.
- The AIA extension specifies where to find up-to-date certificates for the CA.
- The CDP extension specifies where to find up-to-date CRLs that are signed by the CA.
- These extensions apply to all certificates that are issued by that CA.

Authority Information Access (AIA) Extension

- The AIA extension specifies the locations from which users can obtain the certificate for this CA.
- Certificate chaining is a process that builds one or more certificate paths, which trace to the self-signed or root certificate and help determine whether a digital certificate can be trusted or not.

Certificate Revocation List (CRL)

- The **Certificate Revocation List (CRL)**
 - Is a digitally signed list issued by a CA containing a list of certificates issued by the CA that have been revoked.
 - Includes all individual revoked certificates including the serial number of the certificate, the date that the certificate was revoked, and the revocation reason.
- The application uses a CDP to check the CRL for a revoked certificate.
- The CDP is a certificate extension that indicates where the certificate revocation list for a CA can be retrieved.

Certificate Revocation List (CRL)

The image shows two overlapping windows from the Windows Certificate Authority console. The background window is titled 'certsrv - [Certification Authority (Local)]' and displays a tree view with 'contoso-RWDC01-CA-1' selected. Overlaid on this is a dialog box titled 'Add Location'. The dialog contains the following text: 'A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.' Below this is a 'Location:' text box, a 'Variable:' dropdown menu with '<CaName>' selected, and an 'Insert' button. A 'Description of selected variable:' section shows: 'Used in URLs and paths', 'Inserts the DNS name of the server', and 'Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix>'. At the bottom are 'OK' and 'Cancel' buttons.

The foreground window is titled 'contoso-RWDC01-CA-1 Properties'. It has a tabbed interface with 'General' selected. Under the 'Extensions' tab, 'CRL Distribution Point (CDP)' is selected in a dropdown menu. Below the dropdown is a list of CRL locations. The first location is highlighted and contains the following text: 'C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>\ldap://CN=<CATruncatedName><CRLNameSuffix>_CN=<ServerShortName>http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaFile>file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaFile>'. Below the list are 'Add...' and 'Remove' buttons. At the bottom of the window are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Online Responder

- An Online Responder is a trusted server that runs the Online Responder service and Online Responder Web proxy to receive and respond to individual client requests for information about the status of a certificate.
- It implements the **Online Certificate Status Protocol (OSCP)** protocol, which allows a recipient of a certificate to submit a certificate status request to a responder by using the Hypertext Transfer Protocol (HTTP).

Online Responder

- Online Responder receives and responds only to individual requests from clients for information about the status of a certificate, unlike certificate revocation lists (CRLs), which are distributed periodically and contain information about all certificates that have been revoked or suspended.
- Online Responder can process certificate status requests more efficiently than by using CRLs.

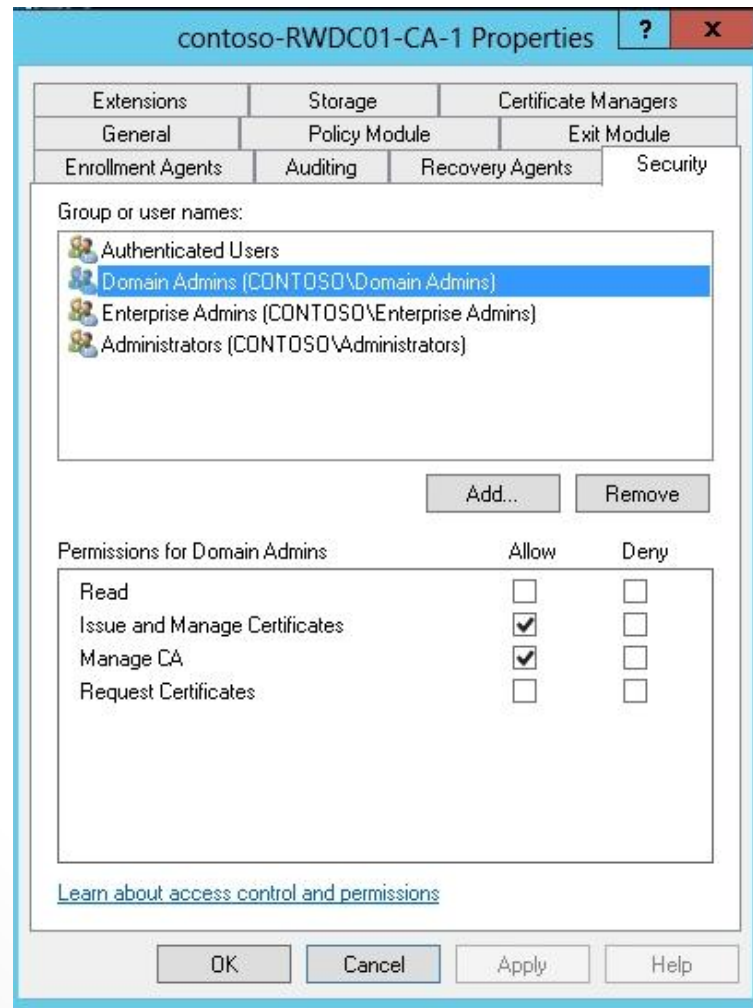
Administrative Role Separation

- Because certificates and CAs are important security tools used for a company, you need to consider using separation of duties to maintain the security of PKI infrastructure.
- You can use role-based administration to organize CA administrators into separate, predefined CA roles, each with his or her own set of tasks.

CA Administrator

- The **CA administrator** configures and maintains the CA. CA administrators have the ability to assign all other CA roles and renew the CA certificate.
- The Allow Manage CA permission allows the CA administrator to
 - Configure policy and exit modules.
 - Start and stop the AD Certificate Services service.
 - Configure AD CS roles and CA extensions.
 - Define key recovery agents.
 - Configure certificate manager restrictions.
 - Delete one or more records in the CA database.
 - Modify Certificate Revocation List (CRL) publication schedules.
 - Read records and configuration information in the CA database.

Modifying the CA Permissions



Certificate Manager

- The **certificate manager** issues and manages certificates, and approves certificate enrollment and revocation requests.
- To make a user a certificate manager, you just have to grant Allow Issue and Manage Certificates.
- Certificate managers can
 - Perform bulk deletions in the CA database.
 - Issue, approve, deny, revoke, reactivate, and renew certificates.
 - Recover archived keys.
 - Read records and configuration information in the CA database.

Backup Operator

- The **backup operator** backs up and restores files and directories.
- Backup operators are assigned using Active Directory Users and Computers or Computer Management.
- Backup operators can
 - Back up and restore the system state, including CA information.
 - Start and stop the AD CS service.
 - Possess the system backup user right.
 - Read records and configuration information in the CA database.

Auditors


- **Auditors** manage and read security logs on a computer running the AD CS role.
- Because auditors have the system audit user right, they can
 - Configure audit parameters.
 - Read audit logs.
 - Possess the system audit user right.
 - Read records and configuration information in the CA database.
- By default, the local administrator holds the system audit user rights. In addition to audit events, the computer must also be configured for auditing of object access using a group policy.

CA Backup and Recovery

- You can back up the entire server by backing up all files and the system state using Windows Backup.
- However, you can back up a CA without having to back up the entire server on which the CA is installed.
- You just need to back up the private and public key for the CA and the certificate database (including the certificate database logs).
- To perform a backup or restore, you must be a CA administrator, a member of the Backup Operators group, or equivalent.

CA Backup and Recovery

Certification Authority Backup Wizard X

Items to Back Up
You can back up individual components of the certification authority data. 

Select the items you wish to back up:

- Private key and CA certificate
- Certificate database and certificate database log
 - Perform incremental backup

Back up to this location:

Note: The backup directory must be empty.

Lesson Summary

- Active Directory Certificate Services (AD CS) is a server role that allows you to issue and manage digital certificates as part of a public key infrastructure.
- Public key infrastructure (PKI) is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates.
- Within the PKI, the certificate authority (CA) binds a public key with respective user identities and issues digital certificates containing the public key.

Lesson Summary

- A digital certificate is an electronic document that contains an identity, such as a user or organization name, along with a corresponding public key. Because a digital certificate is used to prove a person's identity, it can also be used for authentication.
- The stand-alone CA works without Active Directory and does not need Active Directory. Users can request certificates using a manual procedure or web enrollment, where they identify information and specify the certificate they need.
- An enterprise CA requires Active Directory and is typically used to issue certificates to users, computers, devices, and servers for an organization.

Lesson Summary

- A Certificate Revocation List (CRL) is a digitally signed list issued by a CA containing a list of certificates issued by the CA that have been revoked.
- An Online Responder is a trusted server that runs the Online Responder service and Online Responder Web proxy to receive and respond to individual client requests for information about the status of a certificate.
- You can back up a CA without having to back up the entire server on which the CA is installed. You just need to back up the private and public key for the CA and the certificate database (including the certificate database logs).

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make backup copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.