4/5/2021

Hands On Exercise

Chapter 8

Implementing Active Directory Certificate Services

(Part2)

El Adel, Taoufik
IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

Table 8-1 Activity requirements

Activity	Requirements	Notes
Activity 8-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1, ServerDM2, ServerSA1	
Activity 8-2: Installing the AD CS Role	ServerDC1, ServerDM1	
Activity 8-3: Creating an EFS Certificate Template	ServerDC1, ServerDM1	
Activity 8-4: Configuring EFS Certificate Autoenrollment	ServerDC1, ServerDM1	
Activity 8-5: Testing EFS Certificate Autoenrollment	ServerDC1, ServerDM1	
Activity 8-6: Installing the Web Enrollment Role Service	ServerDC1, ServerDM1	
Activity 8-7: Configuring an OCSP Response Signing Certificate Template	ServerDC1, ServerDM1	
Activity 8-8: Requesting the OCSP Response Signing Certificate	ServerDC1, ServerDM1	
Activity 8-9: Creating a Revocation Configuration for the OR	ServerDC1, ServerDM1	
Activity 8-10: Backing Up the CA Server and Archiving a Key	ServerDC1, ServerDM1	
Activity 8-11: Recovering a Lost Key	ServerDC1, ServerDM1	

Activity 8-7: Configuring an OCSP Response Signing Certificate template.

Time Required: 20 minutes
Objective: Configure an OCSP Response Signing Certificate template.
Required Tools and Equipment: ServerDC1, ServerDM1
Description: In this activity, you configure an online responder to field certificate status requests instead of requiring clients to download the CRL. You have already installed the Online Responder role service. Now you need to configure it.

1. On ServerDM1, in Server Manager, click the notifications flag, and click the **Configure Active Directory Certificate Services on the destination server** link. The AD CS Configuration Wizard starts. In the Credentials window, click **Next**.
2. In the Role Services window, click **Online Responder**, and then click **Next**. In the Confirmation window, click **Configure**. Click **Close**.
3. Open the Certification Authority console. Click to expand the server node. Right-click **Certificate Templates** and click **Manage**. In the right pane of the Certificate Templates console, right-click the **OCSP Response Signing** template and click **Duplicate Template**.
4. In the Properties of New Template dialog box, click the **General** tab, type **OCSP-2016** in the Template display name text box, and then click the **Publish certificate in Active Directory** check box.
5. Click the **Security** tab, and then click the **Add** button. In the Select Users, Computers, Service Accounts, or Groups dialog box, click **Object Types**. Click the **Computers** check box, and then click **OK**. Type **ServerDM1** and click **Check Names**. Click **OK**.
6. Click the **Enroll** and **Autoenroll** permissions in the Allow column, and then click **OK**. Close the Certificate Templates console.

7. The next step is to add the template to the CA. In the Certification Authority console, right-click **Certificate Templates**, point to **New**, and click **Certificate Template to Issue**.
8. In the Enable Certificate Templates list box, click **OCSP-2016**, and then click **OK**.
9. Next, you must inform the CA of the online responder's location. Right-click the CA server node and click **Properties**. Click the **Extensions** tab. Click the **Select extension** list arrow, and then click **Authority Information Access (AIA)**.
10. In the *Specify locations from which users can obtain the certificate for this CA* list box, click the entry starting with **http**. Click the **Include in the online certificate status protocol (OCSP) extension** check box (see Figure 8-21), and then click **OK**.

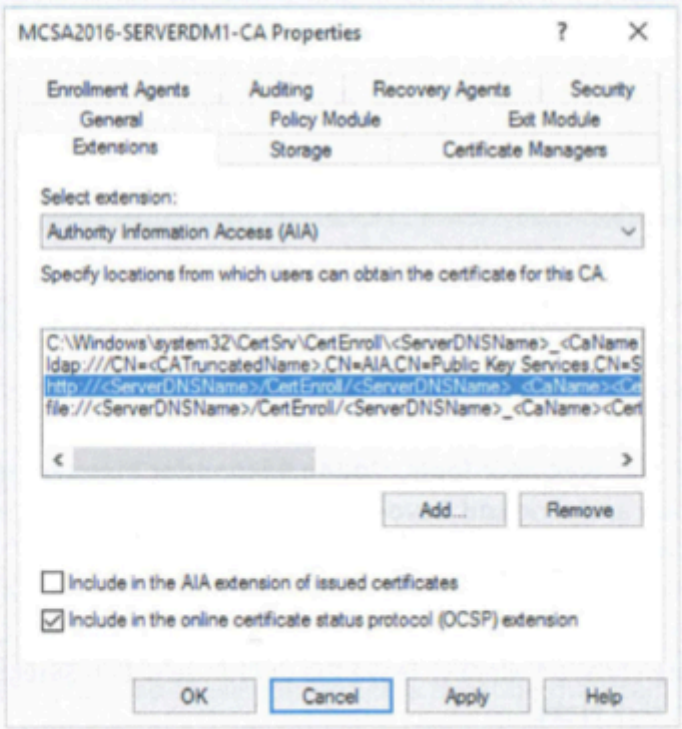


Figure 8-21 The Extensions tab

11. When you're prompted to restart Active Directory Certificate Services, click **Yes**.
12. Now the OR server (ServerDM1 in this case) must enroll in the signing certificate you configured earlier in this activity. You can do this by restarting the server or requesting it manually. The next activity goes through the steps to request the certificate manually so that the server doesn't have to be restarted. Continue to the next activity.

Properties of New Template

Subject Name	Server	Issuance Requirements		
Compatibility	General	Request Handling	Cryptography	Key Attestation
Superseded Templates	Extensions	Security		

Group or user names:

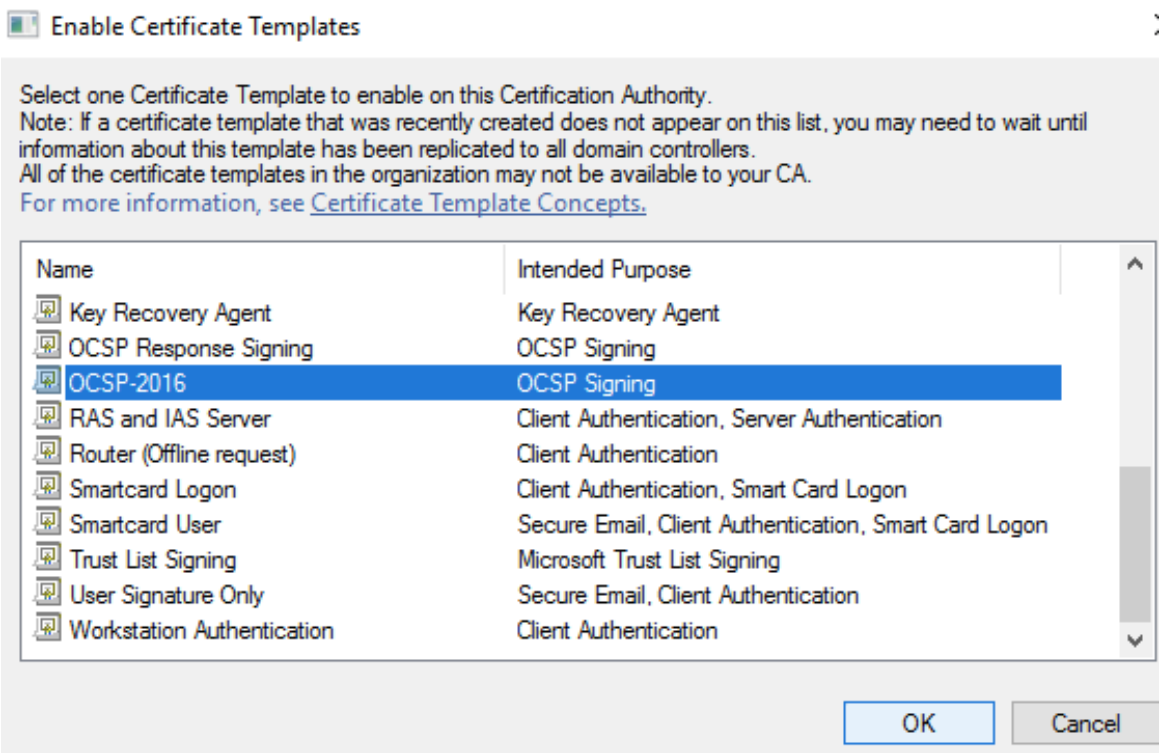
- Authenticated Users
- administrator
- Domain Admins (MCSA2016\Domain Admins)
- Enterprise Admins (MCSA2016\Enterprise Admins)
- SERVERDM1 (MCSA2016\SERVERDM1$)

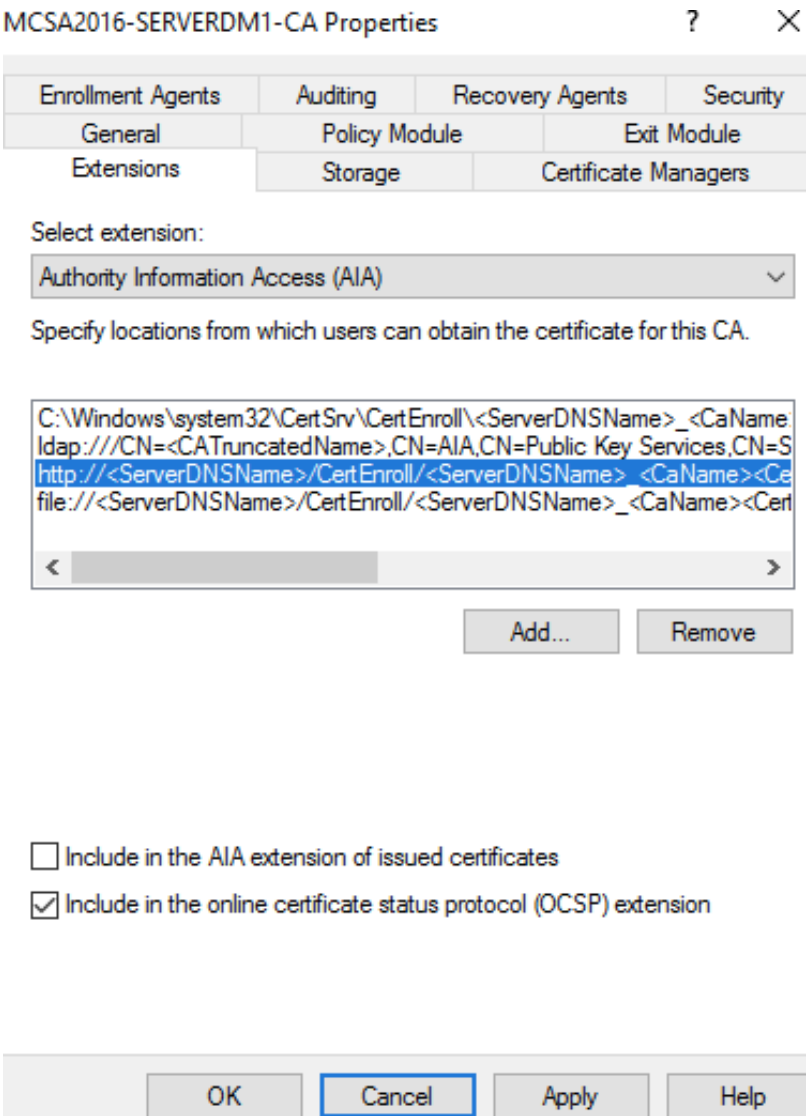
Add... Remove

Permissions for SERVERDM1	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☐	☐
Enroll	☑	☐
Autoenroll	☑	☐

For special permissions or advanced settings, click Advanced.

Advanced

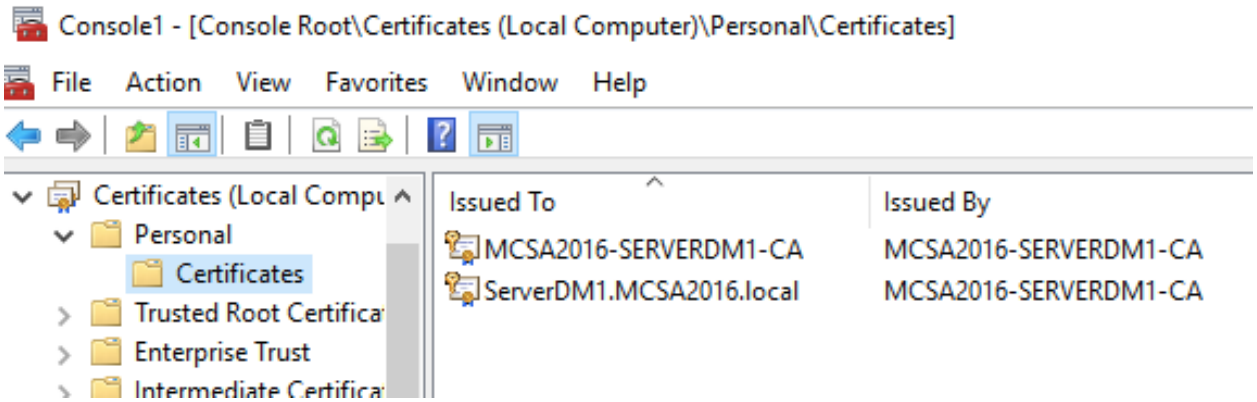

Enable Certificate Templates
Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.
Name
Intended Purpose
Key Recovery Agent
Key Recovery Agent
OCSP Response Signing
OCSP Signing
OCSP-2016
OCSP Signing
RAS and IAS Server
Client Authentication, Server Authentication
Router (Offline request)
Client Authentication
Smartcard Logon
Client Authentication, Smart Card Logon
Smartcard User
Secure Email, Client Authentication, Smart Card Logon
Trust List Signing
Microsoft Trust List Signing
User Signature Only
Secure Email, Client Authentication
Workstation Authentication
Client Authentication
OK
Cancel



Activity 8-8: Requesting the OCSP Response Signing Certificate

Time Required: 10 minutes
Objective: Request the OCSP Response Signing certificate.
Required Tools and Equipment: ServerDC1, ServerDM1
Description: In this activity, to avoid restarting the OR server, you request the OCSP Response Signing certificate in the Certificates snap-in.

1. On ServerDM1, right-click **Start**, click **Run**, type **MMC** in the Open text box, and press **Enter**. Click **File, Add/Remove Snap-in** from the MMC menu.
2. Click **Certificates**, and then click the **Add** button. In the Certificates snap-in dialog box, click the **Computer account** option button, and then click **Next**. In the Select Computer dialog box, leave the default selection **Local computer**, click **Finish**, and then click **OK**.
3. In the left pane, click to expand the **Certificates** node and the **Personal** folder, and then click **Certificates**. Notice that two certificates are issued to this computer.
4. Right-click the **Certificates** folder, point to **All Tasks**, and click **Request New Certificate** to start the Certificate Enrollment Wizard. Click **Next** twice.
5. In the Request Certificates window, click the **OCSP-2016** check box, click the **Enroll** button, and then click **Finish**.
6. Click the **Certificates** folder again. You should see the new OCSP-2016 certificate in the list (scroll to the right to see the template from which the certificate was created).
7. The last step is configuring the certificate. Right-click the **OCSP Signing** certificate, point to **All Tasks**, and click **Manage Private Keys**.
8. In the Security tab, click **Add**. In the *Enter the object names to select* text box, type **Network Service**, click **Check Names**, and then click **OK**. Click **OK**, and then close the MMC. Click **No** when prompted to save the console.
9. Continue to the next activity.



Certificate Enrollment

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

Active Directory Enrollment Policy		
OCSP-2016	STATUS: Succeeded	Details

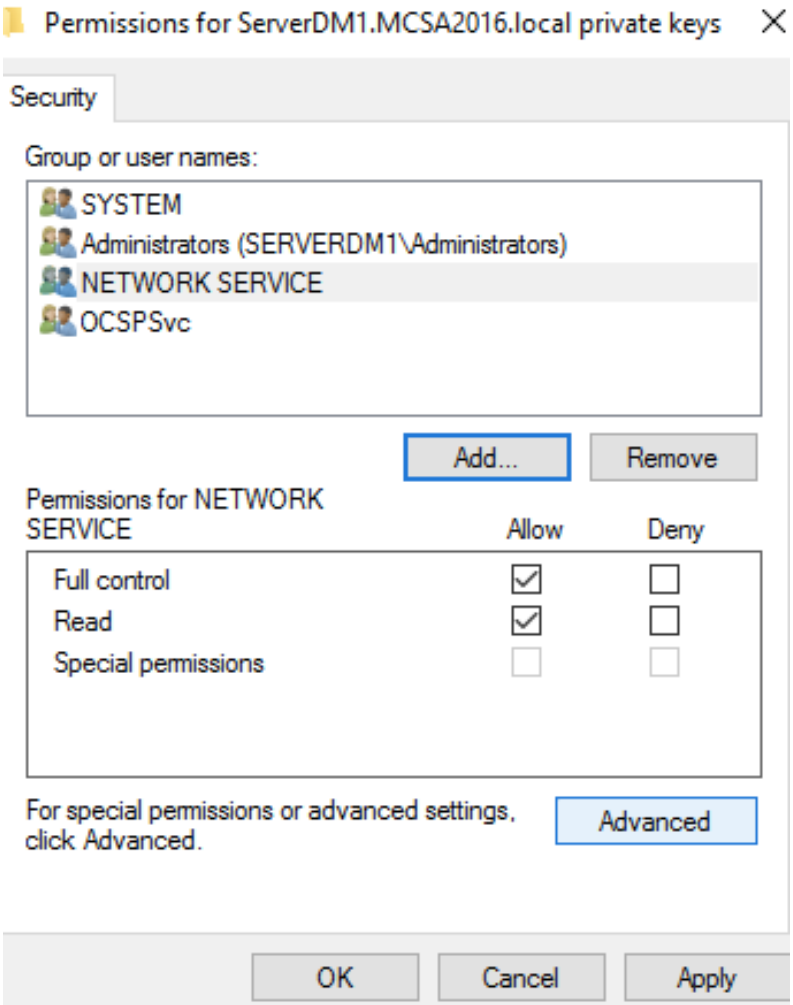
Finish

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

File Action View Favorites Window Help

- Certificates (Local Compu
  - Personal
    - Certificates
  - Trusted Root Certifica
  - Enterprise Trust

Issued To	Issued By
MCSA2016-SERVERDM1-CA	MCSA2016-SERVERDM1-CA
ServerDM1.MCSA2016.local	MCSA2016-SERVERDM1-CA
ServerDM1.MCSA2016.local	MCSA2016-SERVERDM1-CA



Activity 8-9: Creating a Revocation Configuration for the OR

Time Required: 10 minutes
Objective: Create a revocation configuration.
Required Tools and Equipment: ServerDC1, ServerDM1
Description: You're almost finished configuring the online responder. The last task is creating the revocation configuration so that the CA can direct clients where and how to get their CRL.

1. On ServerDM1, in Server Manager, click **Tools, Online Responder Management** from the menu. Right-click **Revocation Configuration** and click **Add Revocation Configuration**. In the Add Revocation Configuration Wizard's Getting started window, click **Next**.
2. In the Name the Revocation Configuration window, type **ORServerDM1** in the Name text box. The name should describe the online responder function and include the server name. Click **Next**.
3. In the Select CA Certificate Location window, leave the default selection **Select a certificate for an Existing enterprise CA**, and then click **Next**.
4. In the Choose CA Certificate window, click **Browse** next to the *Browse CA certificates published in Active Directory* text box. The Select Certification Authority message box opens. Because there's only one choice, click **OK**. The Online Responder Signing certificate is loaded automatically. Click **Next**.
5. In the Select Signing Certificate window (see Figure 8-22), accept the defaults, and then click **Next**.

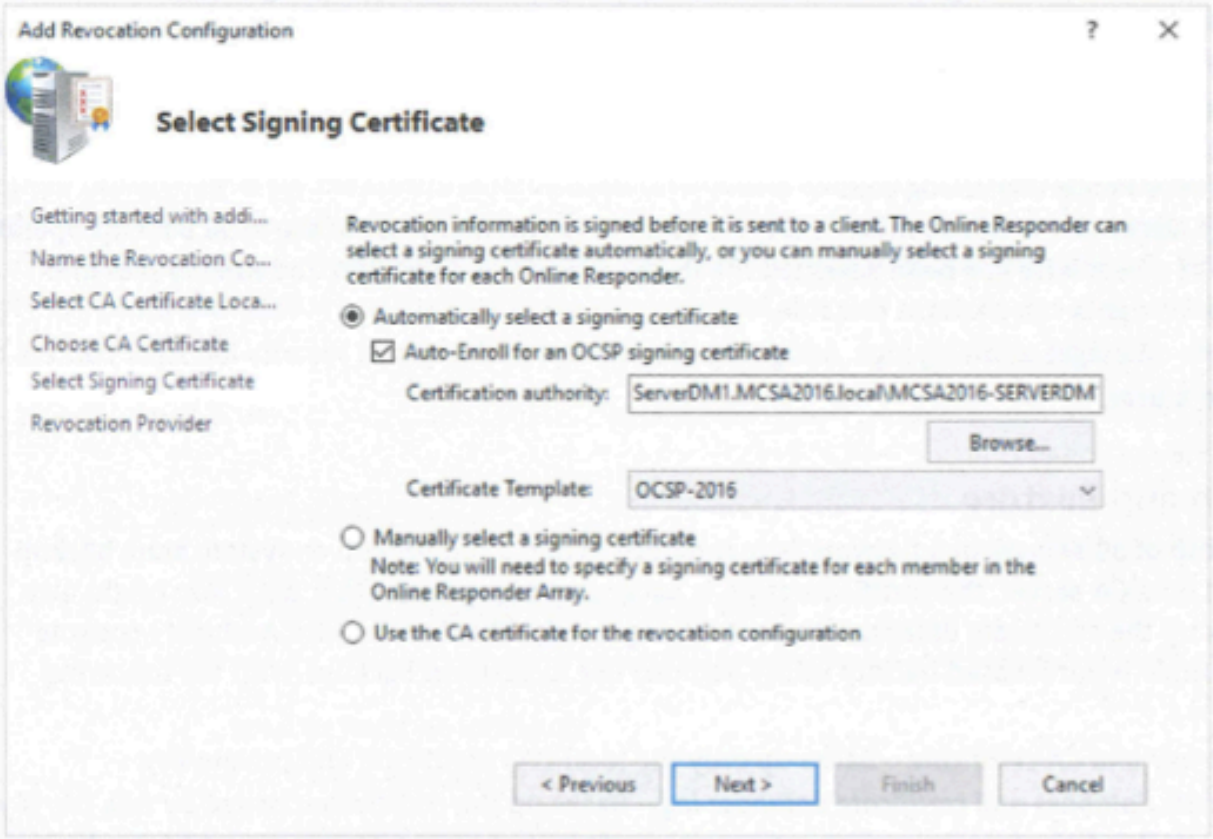


Figure 8-22 The Select Signing Certificate window

6. In the Revocation Provider window, click the **Provider** button, and then click **Add**. Type **http://ServerDM1.MCSA2016.local/CertEnroll/MCSA2016-ServerDM1-CA.crl**, and click **OK**.
7. Under the Delta CRLs text box, click **Add.** In the Add/Edit URL text box, type **http://ServerDM1.MCSA2016.local/CertEnroll/MCSA2016-ServerDM1-CA.crl**, and then click **OK** twice. In the wizard's final window, click **Finish**.
8. Read the information on the Online Responder Configuration window, close all open windows, and continue to the next activity.

Add Revocation Configuration ?

Select Signing Certificate

- Getting started with addi...
- Name the Revocation Co...
- Select CA Certificate Loca...
- Choose CA Certificate
- Select Signing Certificate
- Revocation Provider

Revocation information is signed before it is sent to a client. The Online Responder can select a signing certificate automatically, or you can manually select a signing certificate for each Online Responder.

(●) Automatically select a signing certificate

[x] Auto-Enroll for an OCSP signing certificate

Certification authority: ServerDM1.MCSA2016.local\MCSA2016-SERVERDM

Browse...

Certificate Template: OCSP-2016

( ) Manually select a signing certificate

Note: You will need to specify a signing certificate for each member in the Online Responder Array.

( ) Use the CA certificate for the revocation configuration

< Previous | Next > | Finish | Cancel

ocsp - [Online Responder: ServerDM1.MCSA2016.local]

File Action View Help

- Online Responder: ServerDM1.MCS
  - Revocation Configuration
  - Array Configuration

Online Responder Configuration

Use this snap-in to configure and manage one or more certificate revocation responders.

Overview

The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities.

Use this tool to:

- Manage certificate revocation configurations for an Online Responder Array.
- Monitor the operating status of each member of an Online Responder Array.
- Manage Online Responder Array members.

Revocation Configuration Status

The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members.

Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here.

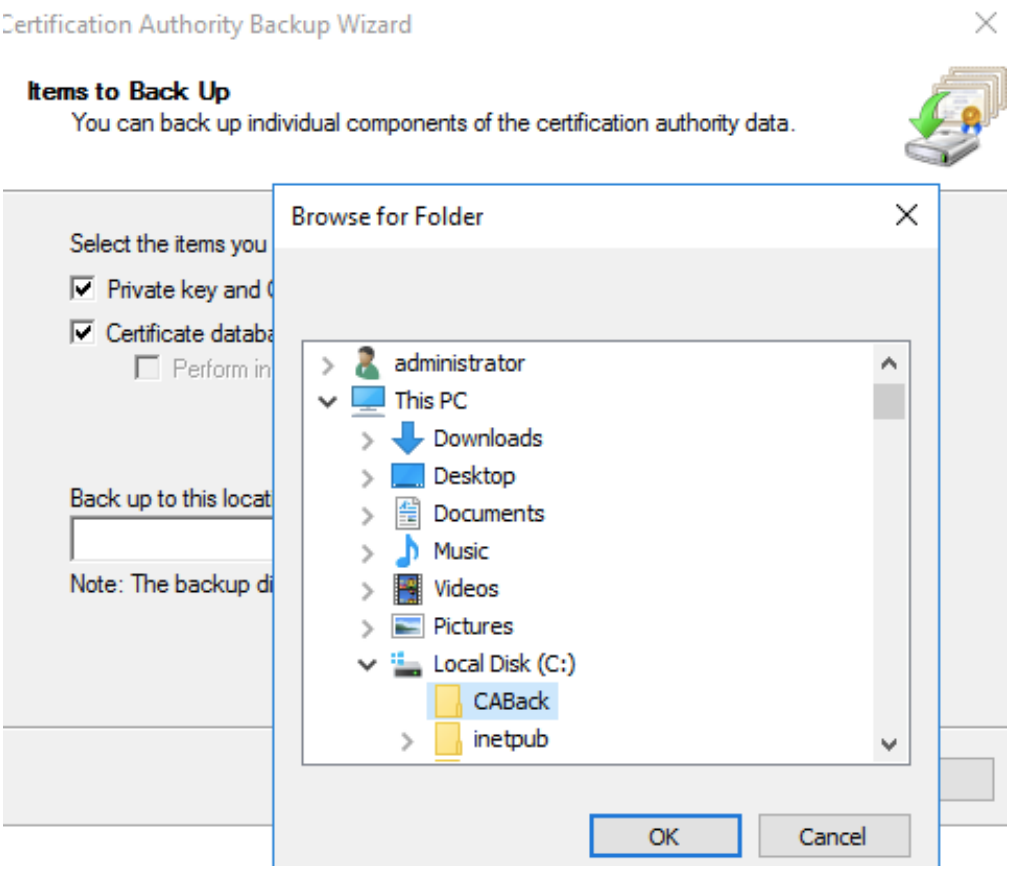
For more information, see Verifying that a revocation configuration is functioning properly.

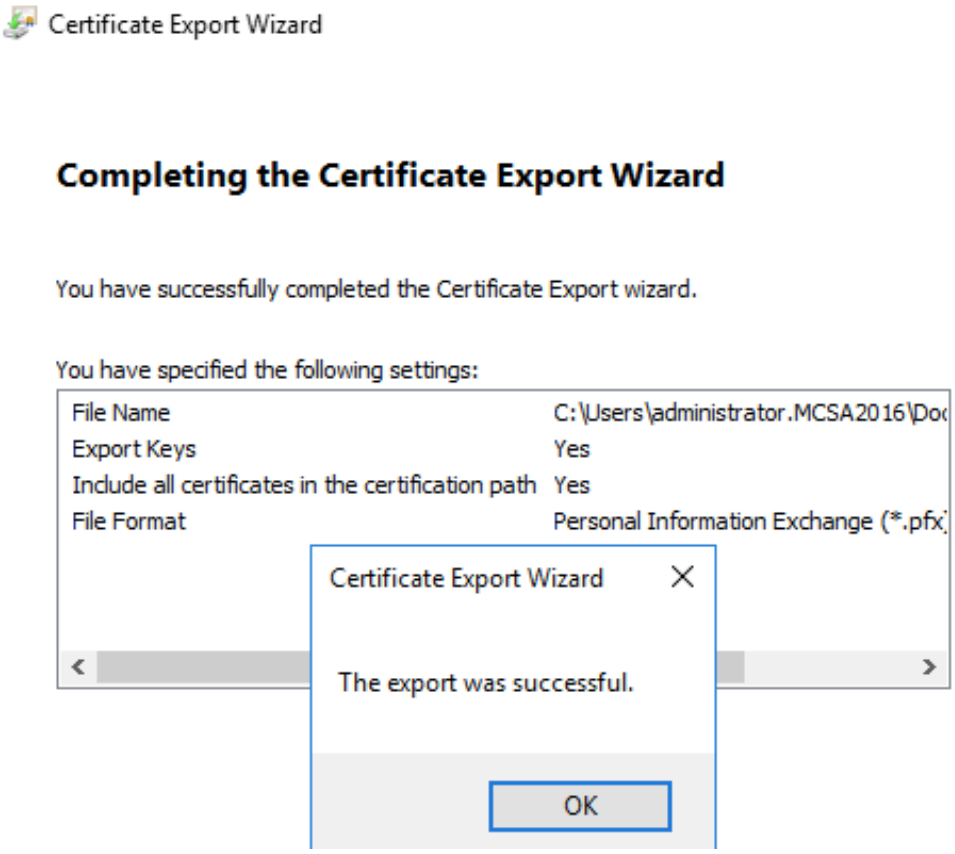
ORServerDM1	Working

Activity 8-10: Backing up the CA Server and Archiving a Key.

Time Required: 10 minutes
Objective: Back up the CA server and archive a private key.
Required Tools and Equipment: ServerDC1, ServerDM1
Description: In this activity, you perform a backup of the CA certificate, private key, and certificate database. Then, you archive a private key.

1. First, you need to create a folder for storing the backup. Normally, this folder is on another server or removable media. For this activity, on ServerDM1, create a folder named **CABack** in the root of the C drive.
2. Open the Certification Authority console. Right-click the CA server node, point to **All Tasks**, and click **Back up CA** to start the Certification Authority Backup Wizard. Click **Next** in the welcome window.
3. In the Items to Back Up window, click **Private key and CA certificate** and **Certificate database and certificate database log**.
4. Click the **Browse** button next to the *Back up to this location* text box. In the Browse For Folder dialog box, navigate to and click the **CABack** folder you just created, and click **OK**. Click **Next**.
5. In the Password and Confirm password text boxes, type **Password01**, and then click **Next**. In the Completing the Certification Authority Backup Wizard window, click **Finish**. The backup begins.
6. When the backup is finished, close the Certification Authority console. Next, you'll archive a private key using the Certificates snap-in.
7. Open an MMC and add the **Certificates** snap-in to it using the default options. In the left pane, click to expand the Certificates node and the **Personal** folder, and then click the **Certificates** folder.
8. Right-click the certificate, point to **All Tasks**, and click **Export**. In the Certificate Export Wizard's welcome window, click **Next**.
9. Click the **Yes, export the private key** option button, and then click **Next**.
10. In the Export File Format window, leave the **Personal Information Exchange - PKCS 12 (.PFX)** option button selected, and then click **Next**.
11. In the Security window, click the **Password** check box, type **Password01** in the Password text box and the Confirm password text box, and then click **Next**.
12. In the File to Export window, click **Browse**. Note which folder is selected as the destination folder (by default, it is the Documents folder). Type **EFSCert** in the File name text box, and click **Save**. Click **Next**.
13. In the Completing the Certificate Export Wizard window, click **Finish**. Click **OK** in the success message. Leave the Certificates snap-in open and continue to the next activity.

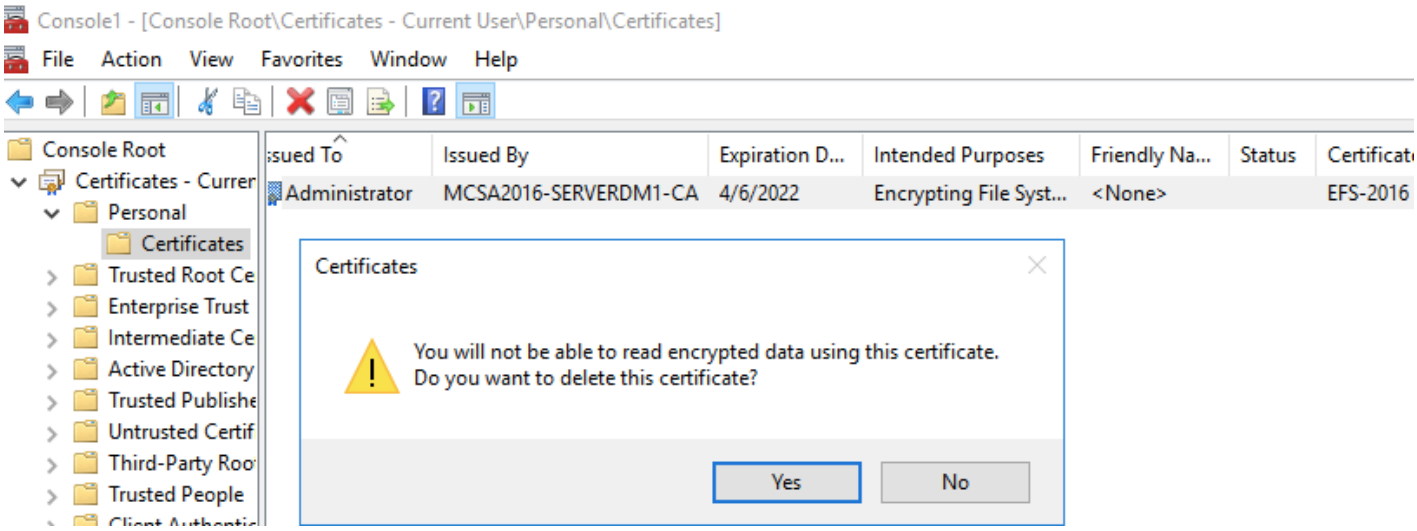

Certification Authority Backup Wizard
Items to Back Up
You can back up individual components of the certification authority data.
Select the items you
Private key and
Certificate databa
Perform in
Back up to this locat
Note: The backup di
Browse for Folder
administrator
This PC
Downloads
Desktop
Documents
Music
Videos
Pictures
Local Disk (C:)
CABack
inetpub
OK
Cancel



Activity 8-11: Recovering a lost key

Time Required: 15 minutes
Objective: Recover a lost key.
Required Tools and Equipment: ServerDC1, ServerDM1
Description: In this activity, you recover your private key from an archived backup.

1. First, you delete your existing certificate and key. On ServerDM1, in the left pane of the Certificates snap-in, click the **Certificates** folder, if necessary. Right-click the **EFS-2016 certificate** and click **Delete**.
2. In the message box explaining that you can't decrypt data encrypted with this certificate, click **Yes**.
3. Right-click the **Certificates** folder, point to **All Tasks**, and click **Import**. (Note that you can request a new certificate, but it can't decrypt data encrypted with the deleted certificate.)
4. The Certificate Import Wizard starts. Click **Next**.
5. In the File to Import window, click **Browse**. In the File types list box, click **Personal Information Exchange**. Click the **EFSCert** certificate that you exported in the previous activity, and then click **Open.** Click **Next.**
6. In the Private key protection window, type **Password01** in the Password text box, and then click the **Mark this key as exportable** check box. If you don't select this check box, you can't export the key again. Click **Next**.
7. In the Certificate Store window, accept the default **Personal** option, and then click **Next**.
8. In the Completing the Certificate Import Wizard window, click **Finish**. In the success message box, click **OK**. You see your EFS-2016 certificate displayed in the Certificates folder.
9. Shut down all computers.



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••••

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\administrator.MCSA2016\Documents\EFSCert

Finish Cancel

Certificate Import Wizard

The import was successful.

OK

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificates - Currer
    - Personal
      - Certificates
    - Trusted Root Ce
    - Enterprise Trust
    - Intermediate Ce

Issued To	Issued By	Expiration ...	Intended Purposes	Friendly Na...	Status	Certificate Te..
Administrator	MCSA2016-SERVERDM1-CA	4/6/2022	Encrypting File Syst...	<None>		EFS-2016
MCSA2016-SE...	MCSA2016-SERVERDM1-CA	4/5/2026	<All>	<None>		