|  |  |
| --- | --- |
| **Server & Cloud Security**  Diploma in CSF/IT  Oct 2022 | Week 3 |
| Practical |
| **Practical: HTTPS and Certificate Life Cycle** | |

Scenario

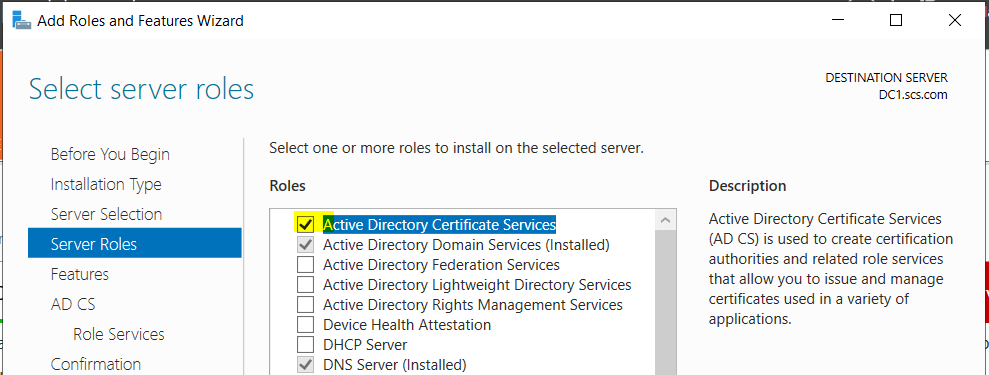
In this activity, you will explore the properties of different kinds of digital certificates and use Windows to request, issue, and revoke certificates.

Objectives

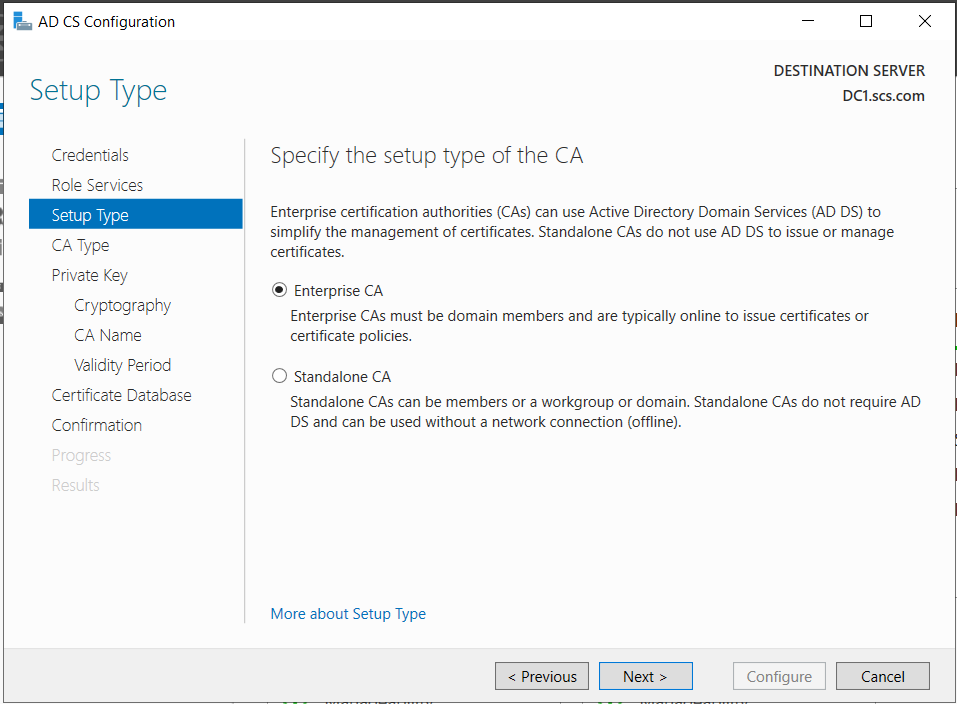
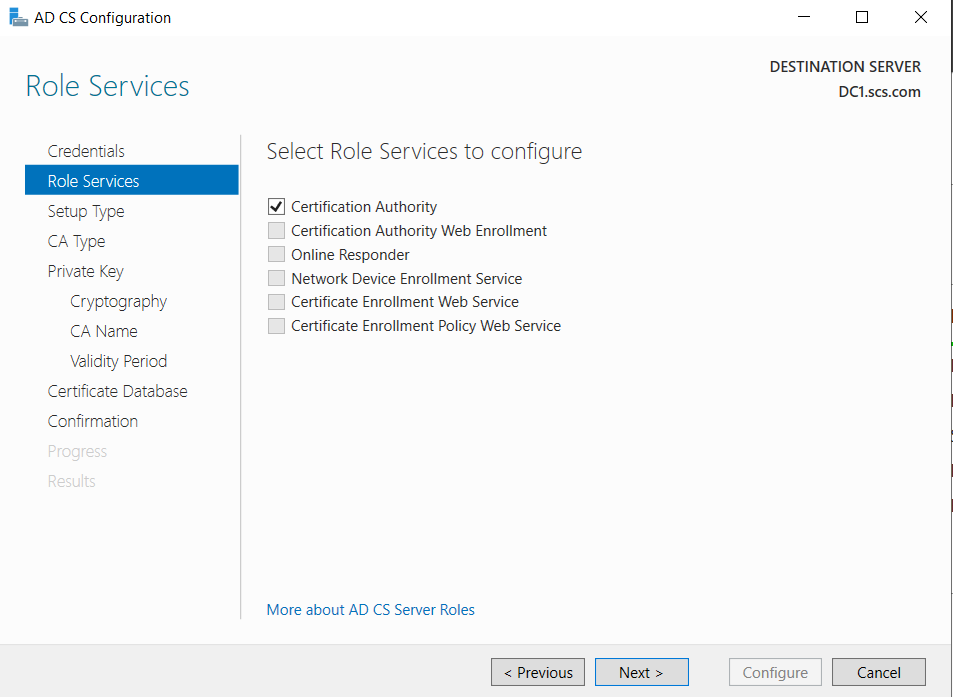
This activity is designed to test your understanding of the secure web communication using https and certificates.

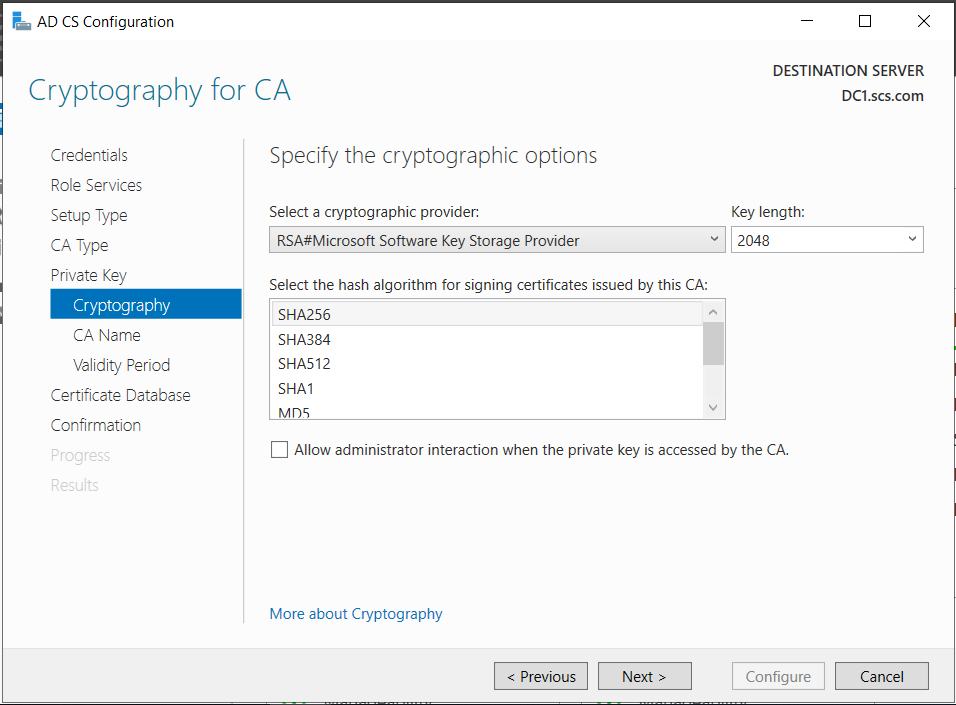
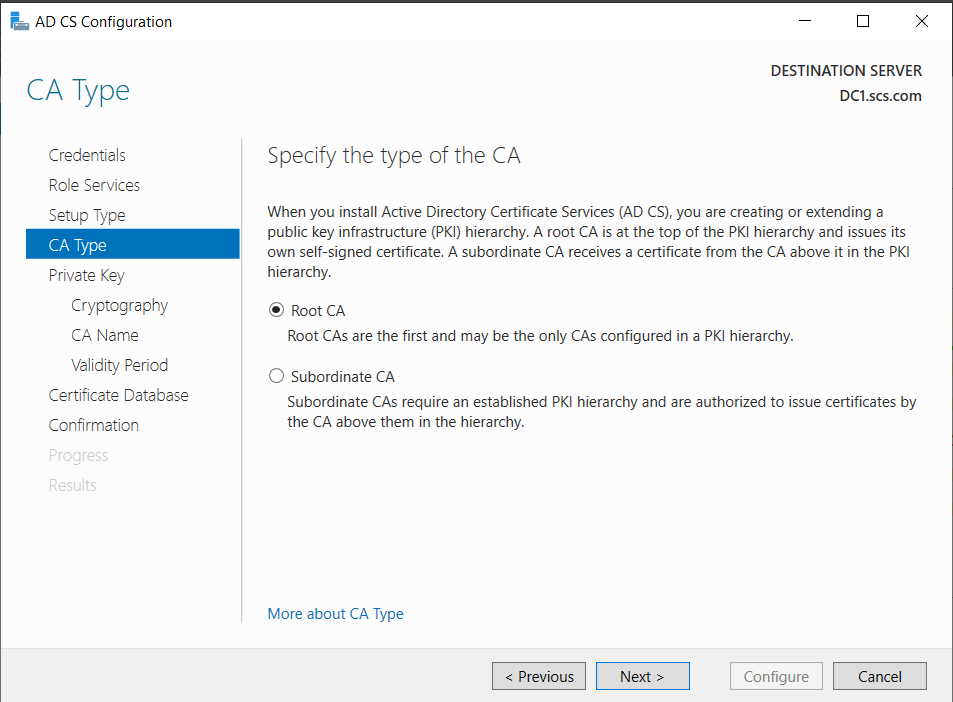
## Task 1: Setup Certificate Authority

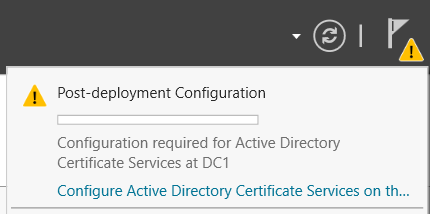
Sign in to DC1 server and add a new server role “Active Directory Certificate Services” to it. Your DC1 server will be worked as the Domain Controller as well as the Certificate Authority in your environment.



Configure the rest of the parameters as shown in the below screenshots.





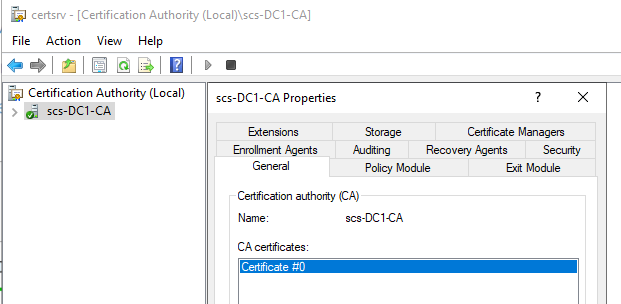


Your DC1 server is now the root CA in your environment.

## Task 2: Browse Certificate Server properties

Open **Certificate Services** on DC1 and locate the root certificate.

1. Sign in to the DC1 VM.
2. In Server Manager, select **Tools→Certification Authority**.
3. Right-click your server (**eg. Scs-DC1-CA**) and select **Properties**.



1. On the **General** tab, note the root certificate (Certificate #0).
2. Which of the following is the identity of the cryptographic provider?
3. Microsoft Software Key Storage Provider
4. Microsoft Smart Card Key Storage Provider
5. Microsoft Platform Crypto Provider

Ans: A

1. Select the **View Certificate** button.

This is the CA server's proof of identity. Note that it is self-signed (issued to itself by itself) because this is the root certification authority. If you were to create subordinate CAs, they would be issued with certificates signed by this server.

1. What is the purpose of this certificate? (Choose two)
2. All issuance policies
3. Proves your identity to a remote computer
4. All application policies
5. Ensures the identity of a remote computer

Ans: A and C

A CA has been installed with the DC to minimize the number of VMs required for the labs. This configuration is NOT something that should ever be done in a production environment. A root CA must be installed to a standalone server with no other roles configured on it. The root CA is very commonly kept offline, except when signing or revocation actions have to be performed. The task of issuing certificates is delegated to an intermediate CA (but again that should not be installed on the same machine as the DC).

1. Close the **Certificate** window, and then select **Cancel** to close the **Properties** window.

Task 3: Browse Certificate Services components

Browse the components used to issue and revoke certificates.

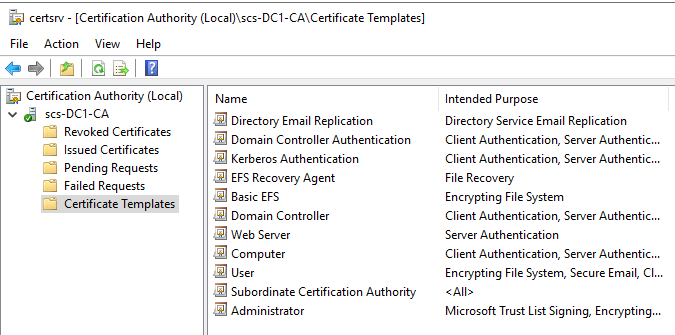
1. In the *Certification Authority* console, expand the server to view the subfolders.

Note that there are folders for revoked and issued certificates and pending and failed requests.

1. Select **Issued Certificates**. The domain controller certificates issued to the host server are displayed.
2. Select the certificate with the most current *Certificate Effective Date*, and then right-click this certificate and select **Open**.
3. You should be able to see one certificate issued by your CA.
4. Select **OK** to close the Certificate dialog box.
5. Select the **Certificate Templates** folder.

It may take several seconds for the Certificate Templates folder to populate.

This snap-in shows the various kinds of certificates that can be issued, such as for server authentication, user authentication, and another specialist uses. As well as different usage profiles, certificate templates can represent different ways of allowing subjects to be enrolled with that type of certificate.



1. Which of the following templates should you choose if you need to configure Server Authentication?
2. Subordinate Certification Authority
3. Basic EFS
4. Domain Controller
5. Web Server

Ans: D

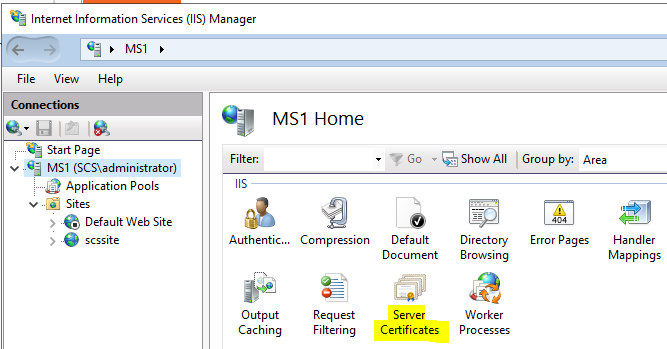
1. What certificate provides Encrypting File System, Secure Email, Client Authentication for employee accounts?
2. Computer
3. Kerberos Authentication
4. Web Server
5. User

Ans: D

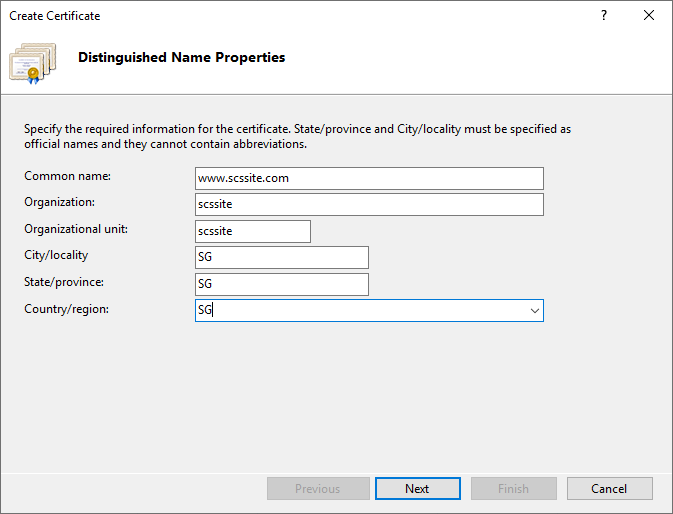
## Task 4: Request a server certificate

In the next part of this activity, you will request a certificate for the MS1 member server and use it to configure a secure web service. You will then explore options for revoking the certificate. In this step, use IIS Manager on the MS1 VM to request a new certificate.

1. Sign in to MS1 VM.
2. In Server Manager, select **Tools→Internet Information Services (IIS) Manager**.
3. In the Connections pane, select the **MS1** server icon. In the Home pane, open the **Server Certificates** applet.

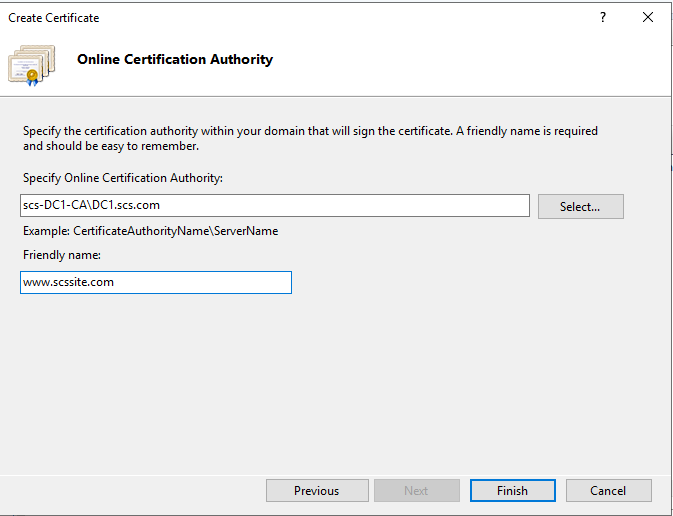


1. In the Actions pane, select **Create Domain Certificate**. Complete the Create Certificate wizard by entering the following information:



Put your full URL as the Common Name.

1. Select **Next**.
2. On the Online Certification Authority page, select the **Select** button, then select your CA and select **OK**.
3. In the Friendly name box, type your website again and select **Finish**.

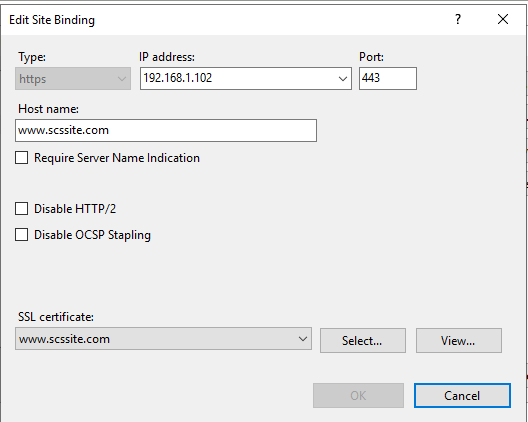


After a few seconds, the certificate request will be granted.

Task 5: Bind certificate to HTTPS port

Bind the certificate to a secure HTTPS port on a website.

1. In *IIS Manager*, expand the server, then **Sites**. Right-click your web site and select **Edit Bindings**.
2. Select the **Add** button.
3. Choose “https” as Type and key in the relevant parameters similar to the below.

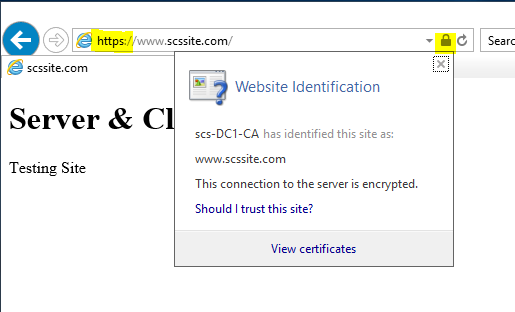


1. Switch to the DC1 VM and observe the **Web Server** certificate in the **Issued Certificates** folder.
2. Which certificate template was used?
3. Computer
4. Web Server
5. Domain Controller
6. Basic EFS

Ans: B

## Task 6: Test secure web services

Test the certificate by browsing the website from the DC1. Make sure you can access the website using https connection.



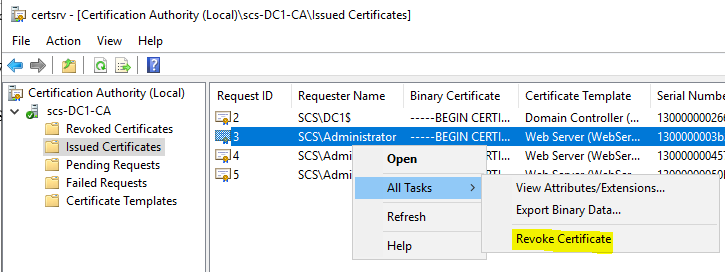
1. Is your connection to the server encrypted?
2. Yes
3. No

Ans: A

## Task 7: Revoke certificate (Optional, For Information Only)

Use DC1 to revoke the certificate if the certificate is no longer needed.

1. Switch to the DC1 VM and observe the web server certificate in the **Issued Certificates** folder. Right-click the certificate and select **All Tasks→Revoke Certificate**.
2. From the Reason code box, select **Cease of Operation**. Leave the date and time set to the current time and select **Yes** to confirm.



--END OF PRACTICAL--