Managing the Life Cycle of a Certificate in Windows Server

Scenario

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

Objectives

This activity designed to test your understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

- 3.9 Given a scenario, implement public key infrastructure.

Lab

- DC1 VM
- MS1 VM
- Kali VM
- pfSense VM

Task 1

Browse Certificate Server properties

In the first part of this activity, you will examine the certificate server. Open **Certificate Services** on DC1 and locate the root certificate.

1. On the **DC1** VM, select **CTR+ALT+DEL**, and then sign in as **CONTOSO\Administrator** with the password **Pa$$w0rd**.

2. In **Server Manager**, select **Tools > Certification Authority**.

3. Right-click the server (**contoso-DC1-CA**) and select **Properties**.

4. On the **General** tab, note the root certificate (Certificate #0).

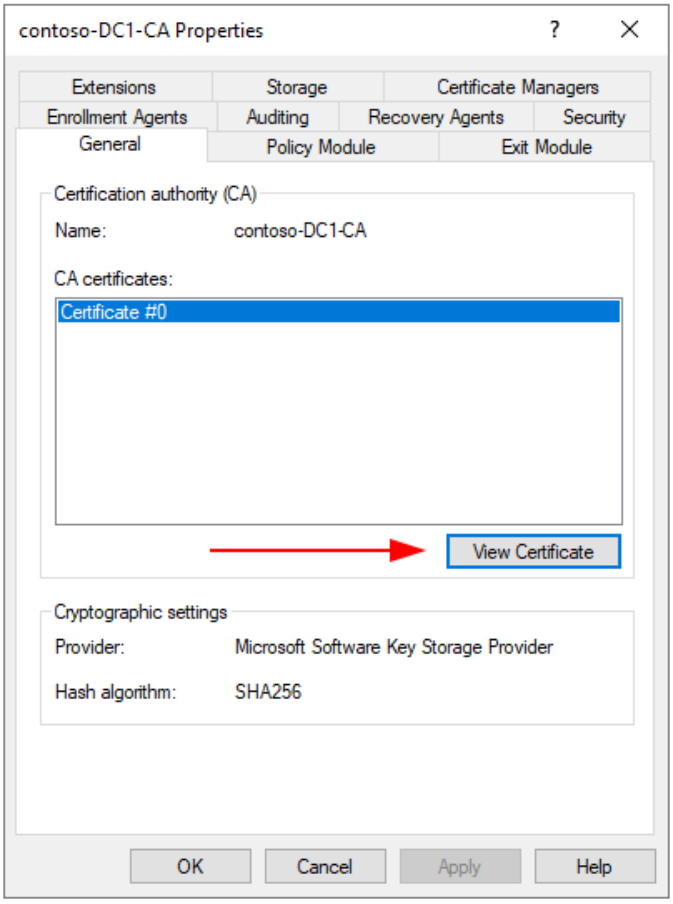

Figure 1.1 – contoso-DC1-CA properties window.

5. Select the **View Certificate** button.

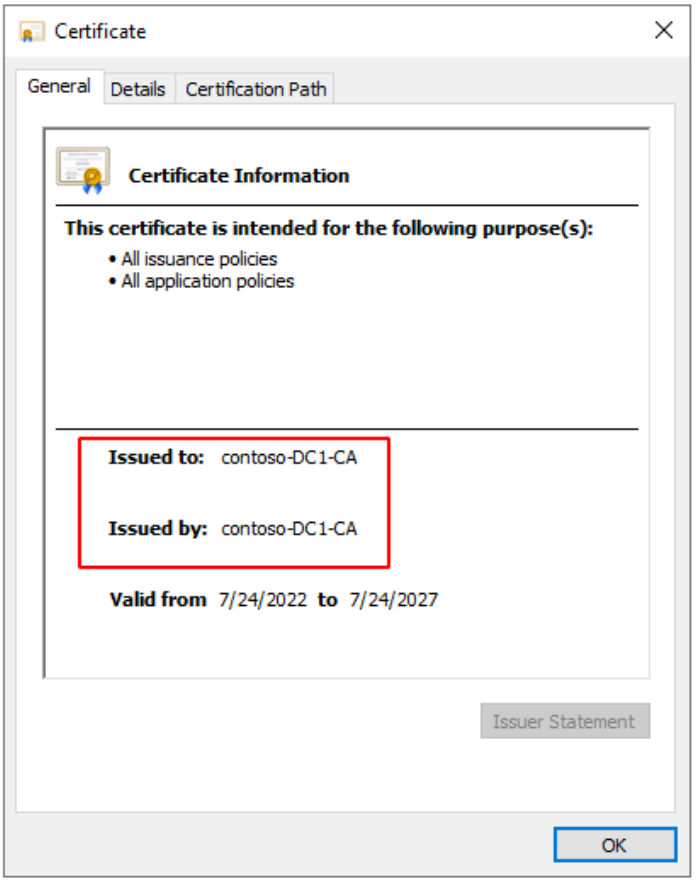

Figure 1.2 – The contoso-DC1-CA Self Signed Certificate.

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.

NOTE: 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).

6. Close the **Certificate** window, and then select **Cancel** to close the **contoso-DC1-CA Properties** window.

TIP: When you are inspecting the configuration, it is a good practice to **Cancel** boxes to close them, rather than selecting **OK** and implementing an inadvertent change.

Task 2

Browse Certificate Services components

Browse the components used to issue and revoke certificates.

1. In the **Certification Authority** console, expand the server **contoso-DC1-CA** to view the sub-folders.

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

2. Select **Issued Certificates**. The domain controller certificates issued to the host server are displayed.

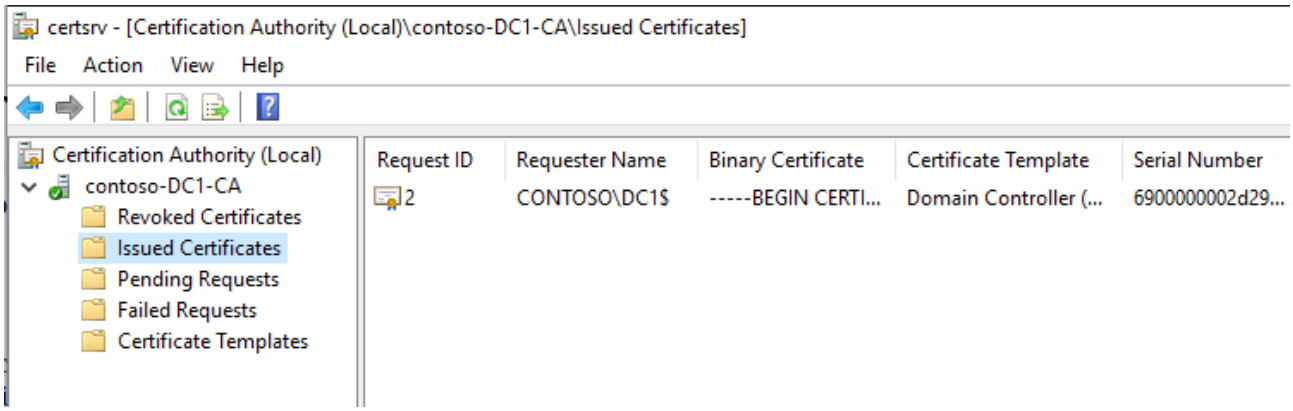

Figure 2.1 – Issued Certificates folder.

3. If there is more than one certificate, select the one with the most current Certificate Effective Date, and then right-click this certificate and select **Open**.

4. Select **OK** to close the Certificate dialog box.

5. Select the **Certificate Templates** folder.

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

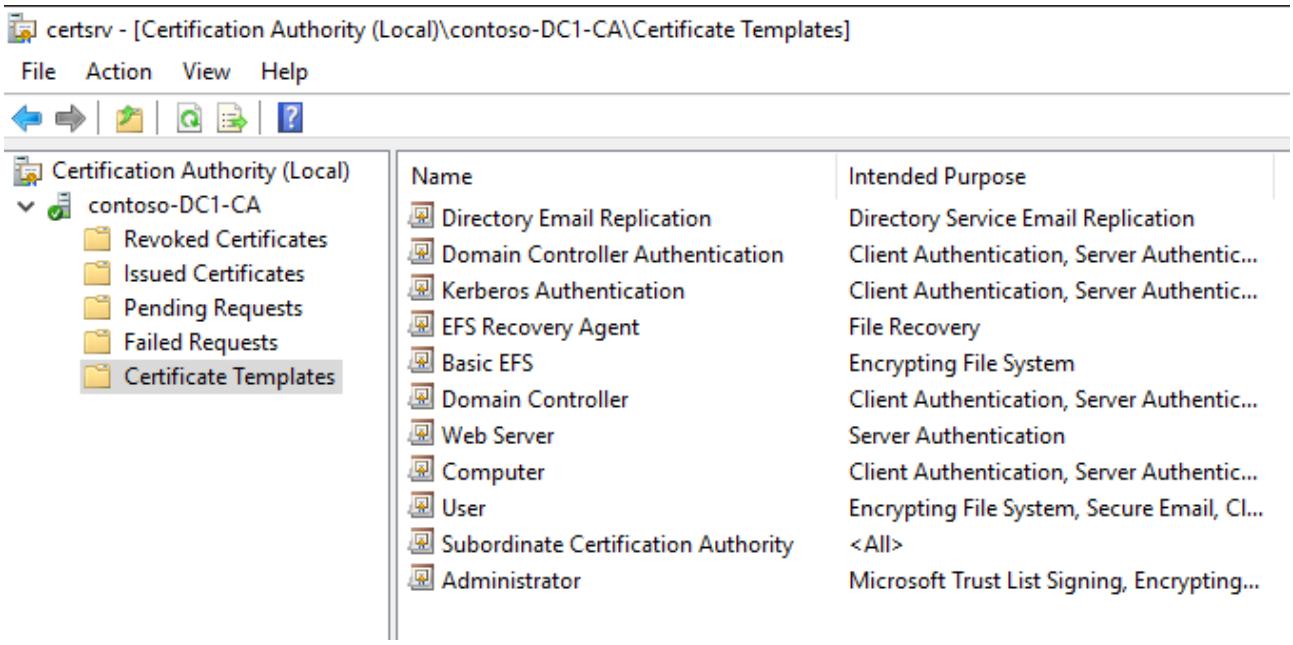

Figure 2.2 – Certificate Templates folder.

This snap-in shows the various kinds of certificates that can be issued, such as for server authentication, user authentication, and other 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.

Task 3

Request a server certificates

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. Select the **MS1** VM, select **CTRL+ALT+DEL**, and then sign in as **CONTOSO\Administrator** with the password **Pa$$w0rd**.

2. In **Server Manager**, select **Tools > Internet Information Services (IIS) Manager**.

3. In the **Connections** pane, select the **MS1** server icon. In the MS1 Home pane, open the **Server Certificates** applet.

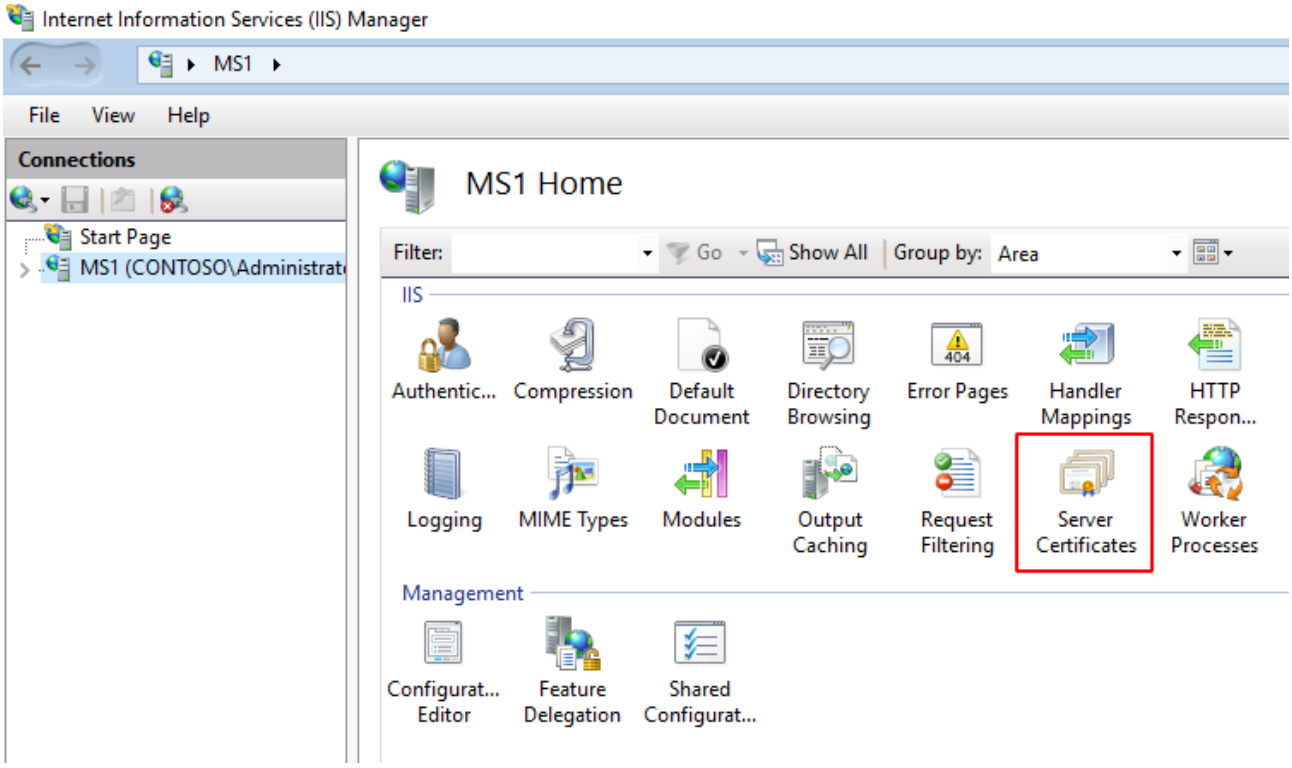

Figure 3.1 – Server Certificates applet.

4. In the Actions pane, select **Create Domain Certificate**.

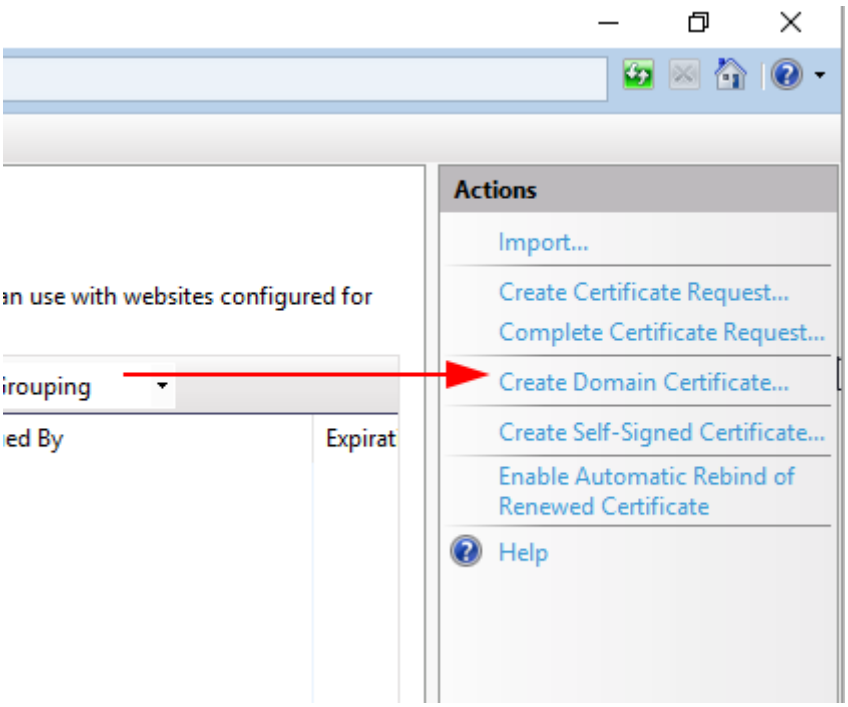

Figure 3.2 – Selecting Create Domain Certificate.

Complete the Create Certificate wizard by entering the following information:

- Common Name: **support.contoso.local**
- Organization: **CONTOSO**
- Organizational Unit: **Web services**
- City/locality, State/province: Enter your location or just **Cloud** for each.

5. Select **Next**.

6. On the Online Certification Authority page, select the **Select** button, then select **contoso-DC1-CA** and select **OK**.

7. In the Friendly name box, type **Support-CA** and select **Finish**.

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

Task 4

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** to show the Default Web Site node. Right-click **Default Web Site** and select **Edit Bindings**.

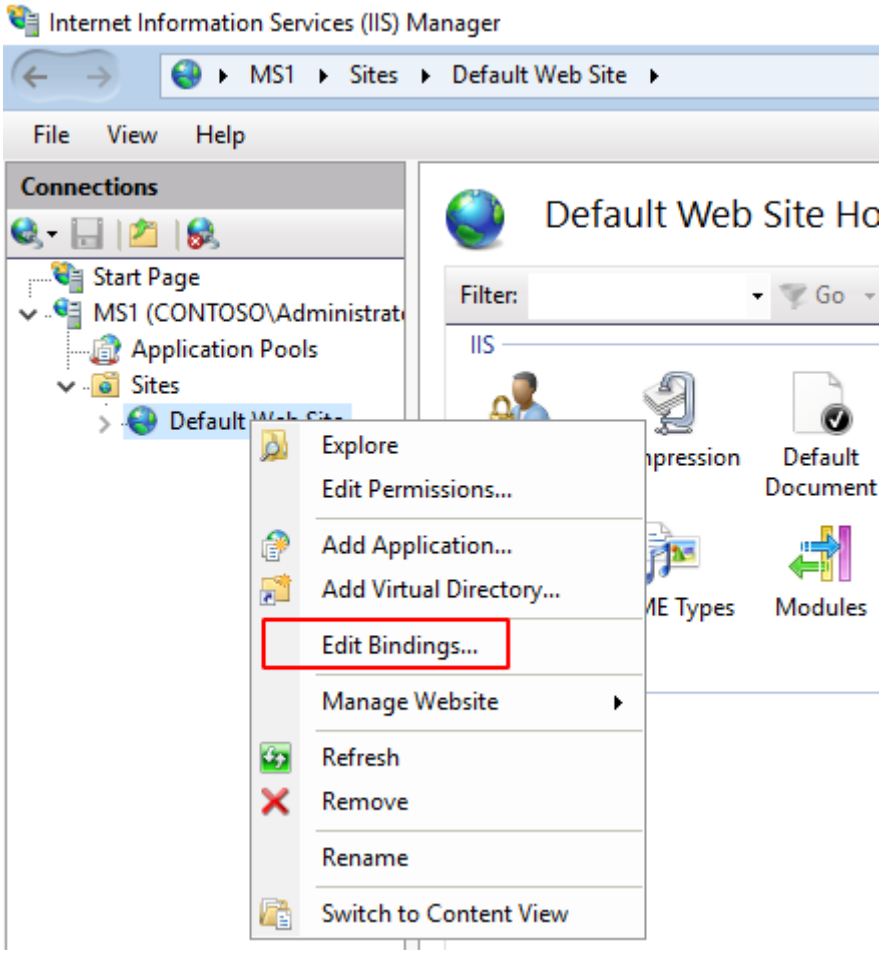

Figure 4.1 – Default Web Site context menu.

2. Select the **Add** button.

3. In the Add Site Binding dialog box, from the Type Box, select **https**.

4. In the Host name box, type **support.contoso.local**

5. From the SSL certificate box, select **Support-CA**

6. Select **OK**.

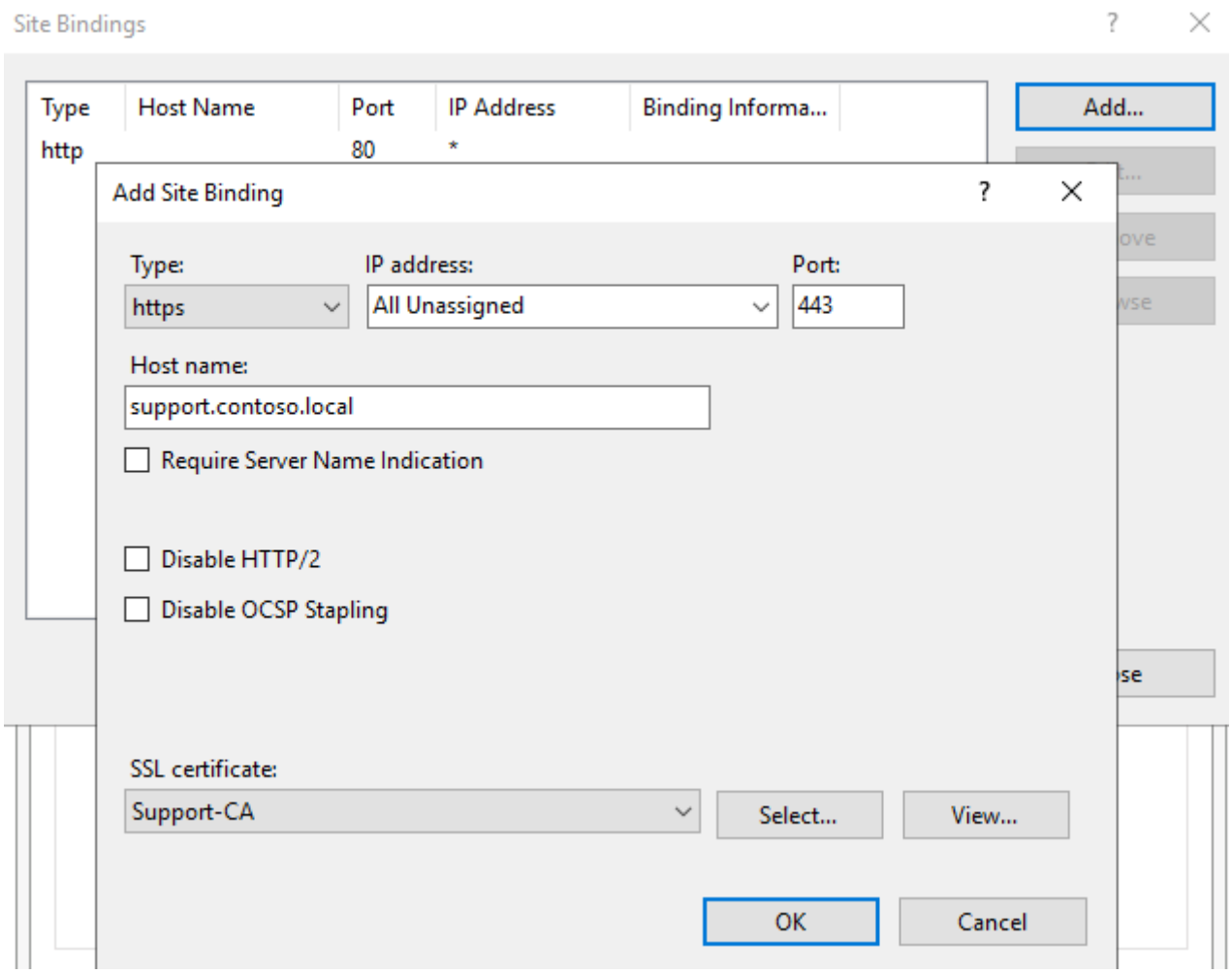

Figure 4.2 – Add Site Binding window.

7. In the Site Bindings dialog box, select the **http** entry, then select **Remove**. Confirm by selecting **Yes**. Select the **Close** button.

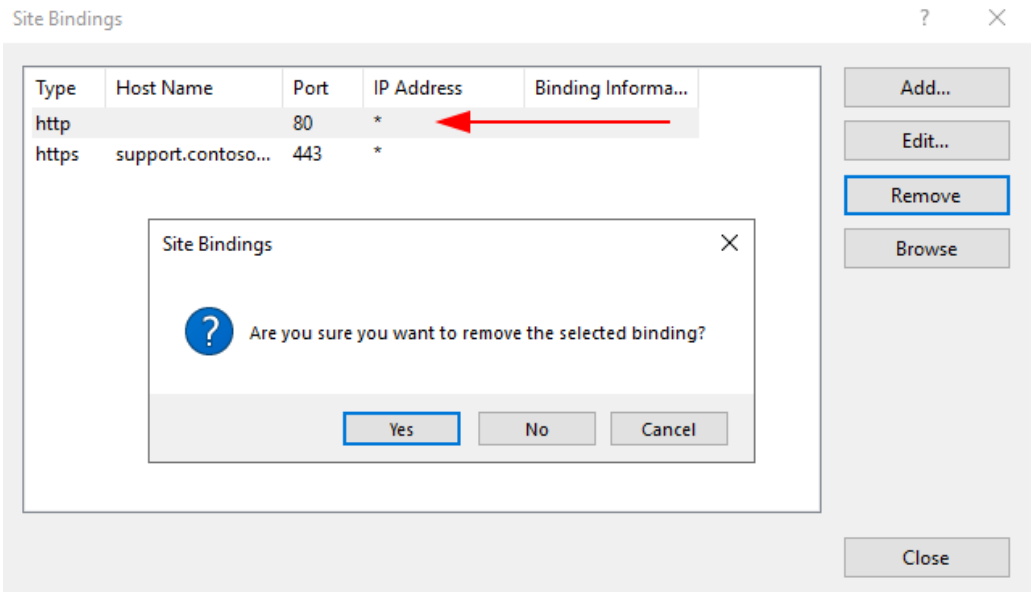

Figure 4.3 – Removing http binding.

8. Switch to the **DC1** VM and observe the new certificate in the Issued Certificates folder.

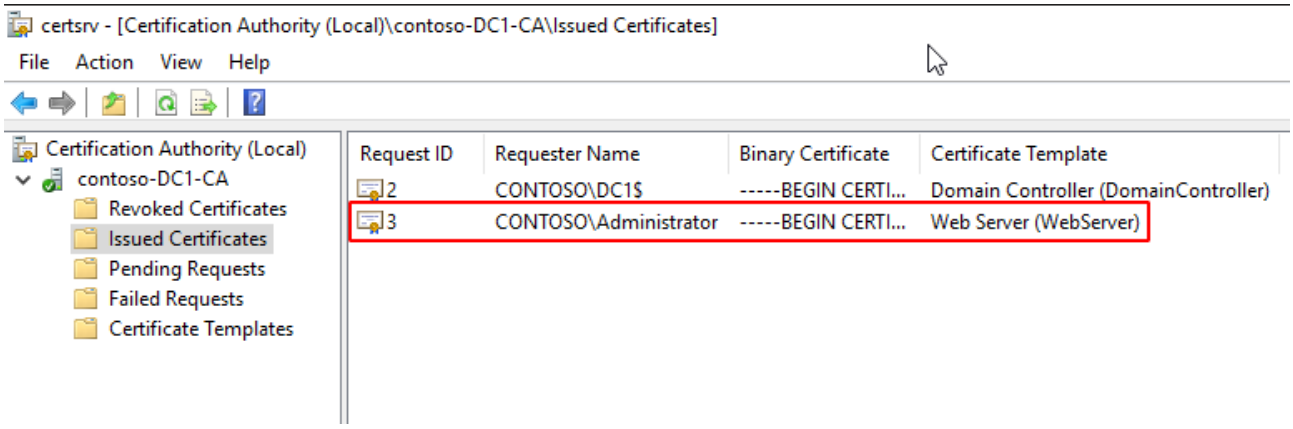

Figure 4.4 – Issued Certificates window.

NOTE: The Policy Module tab in the CA server properties dialog box is used to configure whether all certificates must be manually approved or not. Individual certificate templates can be set up to auto-issue or require administrator approval.

Task 5

Test secure web services

Test the certificate by browsing the website from the Kali VM.

1. Select the **Kali** VM and sign in as **kali** with the password of **Pa$$w0rd**.

2. Use the **Firefox** web browser to connect to **https://support.contoso.local**

A security warning is displayed. Firefox doesn't trust the certificate. Firefox has a list of pre-configured trusted root certificates, and the **contoso-DC1-CA** is not on that list. Root Certificate Authorities can be added to the browser.

NOTE: If you try to connect to the server using an incorrect link, an error is displayed because the URL would not match the subject name configured in the certificate. For example, an attempt to connect to https://ms1.contoso.local or https://192.168.1.2 will also result in a security warning.

3. Navigate through the interface to accept the risk of connecting to a site with an untrusted root certificate.

The page should show correctly.

4. To the **left** of the **https://support.contoso.local** URL, select the padlock icon to display certificate information. Expand the message for more information on the certificate.

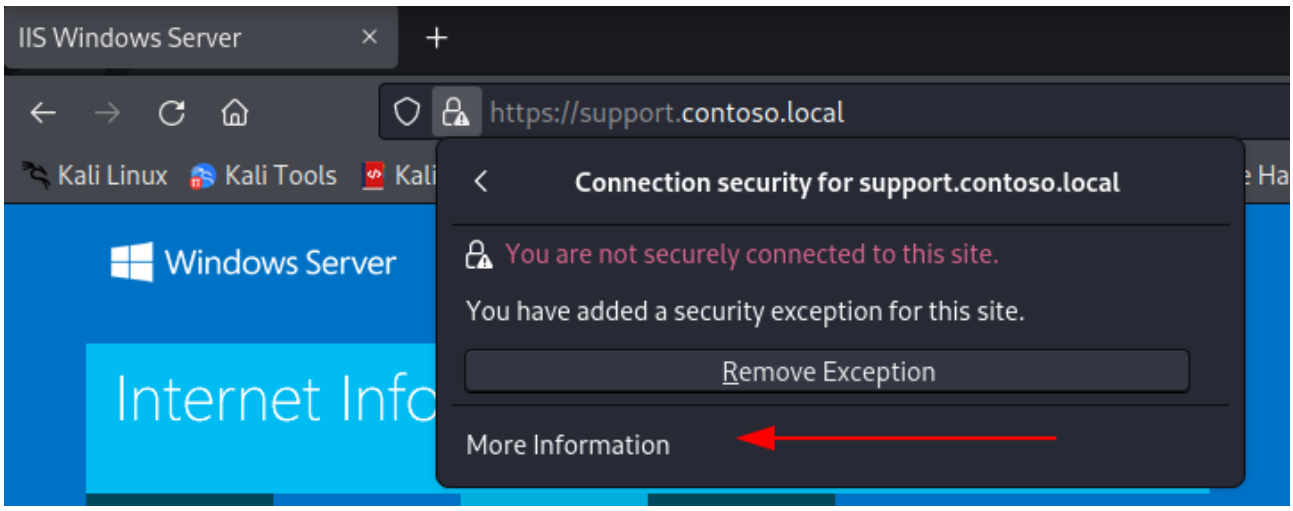

Figure 5.1 – Selecting more information about the certificate.

5. Close the **Firefox** web browser.

Task 6

Revoke certificate

Use DC1 to revoke the certificate and observe the effect on browsing the website.

1. Switch to the **DC1** VM. If necessary, select the web certificate in the **Issued Certificates** folder.

2. Right-click the certificate and select **All Tasks > Revoke Certificate**.

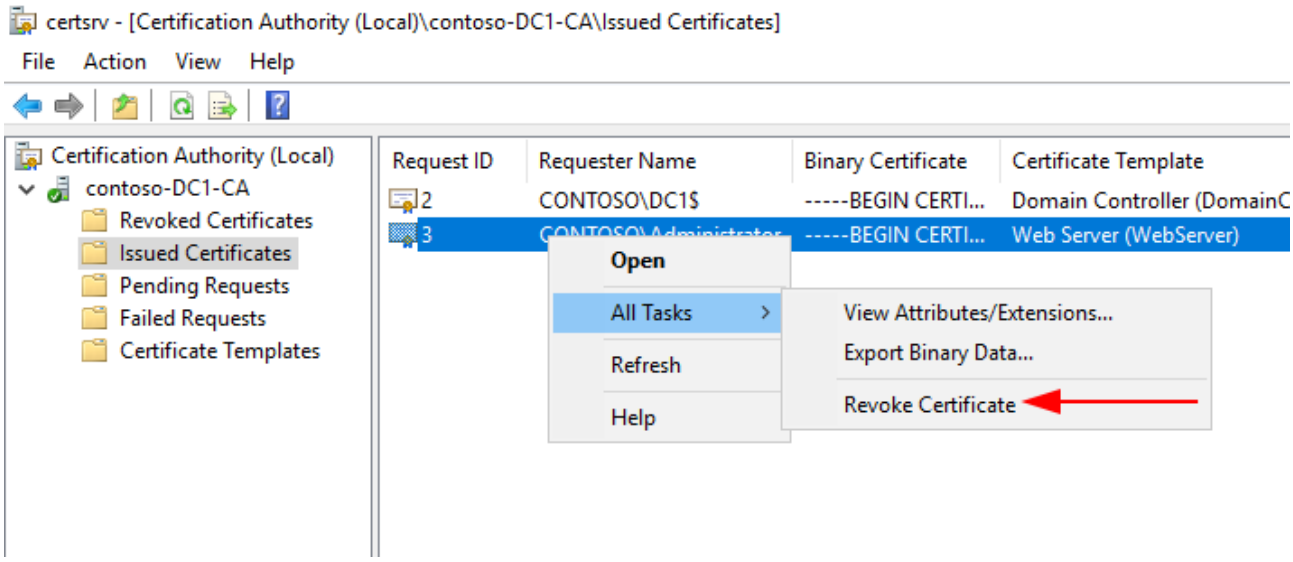

Figure 6.1 – Revoke a Certificate.

3. From the Reason code box, select **Cease of Operation**. Leave the date and time set to the current time and select **Yes** to confirm.

TIP: If you were to right-click the **Revoked Certificates** folder and select **Properties**, you would see that the next publication of a delta CRL is set for the next day.

NOTE: If you were to return to the web client and attempt a new HTTPS connection, it will still succeed. There is no certificate warning displayed because the updated CRL has not yet been published. If you want to revoke certificates very quickly, you have to configure the CRL publishing periods before you issue certificates. The problem with publishing CRLs more often is that it consumes more bandwidth and slows down client access.

4. Close the **certsrv** console.