Key Archival and Recovery

The key archive stores a certificate's subject name, public key, private key, and supported cryptographic algorithms in its CA database. This procedure can be performed manually or automatically, depending on the configuration. If the certificate template requires key archiving, then the process requires no manual intervention. However, key archiving can also be performed manually if the private key is exported and then sent to an administrator for import into the CA database.

There is also a Key Recovery Agent template available in the standard templates within Active Directory Certificate Services. The Key Recovery Agent template enables Domain Admins and Enterprise Admins to export private keys. Additionally, you can add other accounts and groups to have the necessary permissions (Read and Enroll) through the Security tab of the template.

The Key Recovery Agent template also needs to be enabled, as with other certificate templates, through the Certification Authority tool by selecting Certificate

Template To Issue. See "Publishing a Certificate Template" earlier in this chapter for more details on enabling a certificate template on a CA.

With the Key Recovery Agent template in place, the following process must take place for key archiving and recovery:

1. Request a key recovery agent certificate using the Certificates snap-in.
2. Issue the key recovery agent certificate using the Certification Authority tool.
3. Retrieve the enrolled certificate using the Certificates snap-in.
4. Configure the CA for key archiving and recovery.

The final step, configuring the CA for key archiving and recovery, takes place in the Properties dialog box of each CA that will need to archive and recover keys. Specifically, the Recovery Agents tab configures the behavior of the CA when a request includes key archiving.

Each Key Recovery Agent certificate should be added using the Add button on the Recovery Agents tab.

Task 1--Creating a Key Recovery Agent account

Configure and add the Key Recovery Agent certificate template as a template that can be issued by the enterprise CA.

Important

- Perform the following procedures at the domain controller.

1. Verify who can enroll the Key Recovery Agent template

a. Log on as Administrator@adventure-works.com.

b. Click **Start**, click **Run**, type **certtmpl.msc** and then press Enter.

c. In the console tree, click **Certificate Templates**.

d. In the details pane, right-click **Key Recovery Agent** and click **Properties**.

e. In Key Recovery Agent **Properties**, click the **Security** tab.

By default, the security groups can enroll the Key Recovery Agent certificate template are Domain Administrators and Enterprise Administrators.

f. If you want another recovery agent, click **Add** to add the user and grant that user **Read** and **Enroll** permissions.

2. Change the default issuance behavior of the Key Recovery Agent template

a. In Key Recovery Agent **Properties**, click the **Issuance Requirements** tab.

b. Clear the **CA certificate manager approval** check box and click **OK**.

c. Close **Certificate Templates**.

3. Configure the EntCA certification authority to issue Key Recovery Agent certificates.

a. On the **Administrative Tools** menu, click **Certification Authority**.

b. In the console tree, double-click **EntCA**, and then click **Certificate Templates**.

c. Right-click **Certificate Templates**, then click **New**, and then click **Certificate to Issue**.

d. In **Select Certificate Template**, click **Key Recovery Agent**, and then click **OK**.

Task 2--Acquiring the Key Recovery Agent certificate

In this series of steps, you will acquire a Key Recovery Agent Certificate for the purpose of recovering private keys.

Important

- Perform the following procedures at the domain controller.

1. Create an MMC console with the Certificates snap-in loaded.

a. Ensure that you are logged on as administrator@adventure-works.com.

b. On the taskbar, click the **Start** button, and then click **Run**.

c. In **Run**, type **mmc**, and then click **OK**.

d. On the **File** menu, click **Add/Remove Snap-in**.

e. In **Add/Remove Snap-in**, click **Add**.

f. In the **Add Stand-alone Snap-in**, click **Certificates**, and then click **Add**.

g. In **Certificates**, click **User account** and then click **Finish**.

h. Click **Close**, and then click **OK**.

2. Acquire a Key Recovery Agent certificate.

a. In the newly-created MMC console, in the console tree, double-click **Certificates (Current User)**.

b. In the console tree, right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.

c. In the Certificate Request Wizard, click **Next**.

d. In **Certificate Template**, select **Key Recovery Agent**, and then click **Next**.

e. In the **Certificate Friendly Name and Description**, in **Friendly name**, type **Key Recovery**, and then click **Next**.

f. In **Completing the Certificate Request Wizard**, click **Finish**.

g. In the console tree, double-click **Personal** and then click the Certificates folder.

h. Ensure that a certificate with the friendly name of "Key Recovery" exists.

i. Close the console without saving changes.

Task 3--Configuring the CA to allow key recovery

In this series of steps, you configure the EntCA enterprise CA to use the Recovery Agent certificate acquired in Task 2. The CA must load the public key for the Key Recovery Agent to be used for encrypting the recovery data.

Important

- Perform the following procedures at the domain controller.

1. Configure the Recovery Agent to be the Administrator's Key Recovery Agent certificate.

a. Ensure that you are logged on as Administrator@adventure-works.com.

b. In **Administrative Tools**, open **Certification Authority**.

c. In the console tree, click **EntCA**.

d. Right-click **EntCA**, and then click **Properties**.

e. On EntCA **Properties**, on the **Recovery Agents** tab, click **Archive the key** and then click **Add**.

f. In **Key Recovery Agent Selection**, click the certificate that is displayed, and then click **OK**.

g. When prompted to restart the CA, click **Yes**.

2. Open the Certificates console, focused on the local computer.

a. On the taskbar, click the **Start** button, and then click **Run**.

b. In **Run**, type **mmc**, and then click **OK**.

c. On the **File** menu, click **Add/Remove Snap-in**.

d. In **Add/Remove Snap-in**, click **Add**.

e. In **Add Standalone Snap-in**, click **Certificates**, and then click **Add**.

f. In **Certificates**, click **Computer account** and then click **Next**.

g. In **Select Computer**, click **Local Computer**, and then click **Finish**.

h. Click **Close**, and then click **OK**.

3. Verify the installation of the KRA certificate.

a. In the console tree, double-click **Certificates (Local Computer)**, double-click **KRA**, and then click **Certificates**.

b. In the details pane, double-click the certificate.

The intended use of the certificate is Key Recovery Agent and the certificate is issued to Administrator. This procedure ensures that the Key Recovery Agent has been successfully configured, and then click **OK**.

d. Close the console without saving changes.

Task 4--Creating a new certificate template that allows key archiving

In this series of steps, you will define a new template that allows Key Archival by using the Certificate Templates console. This will allow key recovery in the domain in the event that the private key is lost or corrupted at the client computer.

Important

- Perform the following procedures at the domain controller.

1. Open the Certificate Templates console.

a. Log on as Administrator@adventure-works.com.

b. On the taskbar, click the **Start** button, and then click **Run**.

c. In **Run**, type **mmc**, and then click **OK**.

d. On the **File** menu, click **Add/Remove Snap-in**.

e. In **Add/Remove Snap-in**, click **Add**.

f. In **Add Standalone Snap-in**, click **Certificate Templates**, and then click **Add**.

g. Click **Close**, and then click **OK**.

2. Create a duplicate of the Users certificate template with the following properties:

- Template is named "Archive User"
- Key archival is enabled

a. In the console tree, click **Certificate Templates**.

b. In the details pane, right-click the **User** template, and click **Duplicate Template**.

c. In the **Properties** of New Template dialog box, in the **General** tab, in the **Display name** box, type **Archive User**.

d. In the **Request Handling** tab, enable the **Archive subject's private key** option.

The archive key option makes it possible for the Key Recovery Agent to recover the private key from the certificate store.

e. Click the **Security** tab.

Domain Administrators and Domain Users can enroll for this certificate. These permissions were copied from the Users certificate template.

f. Click **OK**.

g. Close the console without saving changes.

Task 5--Acquiring a User certificate that has an archived key

In this series of tasks, you configure the EntCA certification authority to issue Archive User certificates. Using a newly created account, you will acquire an Archive User certificate and record the certificate's serial number for later usage.

Important

- Perform the following procedures at the domain controller.

1. Configure EntCA to issue the new Archive User certificate template.

a. Ensure that you are logged on as Administrator@adventure-works.com, with a password of **password**.

b. From **Administrative Tools**, open **Certification Authority**.

c. In the console tree, double-click **EntCA**, and then click **Certificates Templates**.

d. Right-click Certificate Templates, click **New**, and then click **Certificate to Issue**.

e. In **Select Certificate Template**, click **Archive User** and then click **OK**.

The Archive User certificate template now appears in the details pane.

f. Close **Certification Authority**.

2. Create a new user account

a. In **Administrative Tools**, open **Active Directory Users and Computers**.

b. Double-click adventure-works.com.

c. In **Users**, create a user account with the following properties:

- First name: Mike
- Last name: Danseglio
- User logon name: Mikedan
- Password: password
- Member of: Server Operators
- E-mail: Mikedan

d. Click **Next**, and then click **Finish**.

e. Double-click the **Mikedan** account, and then select the **Member of** tab.

f. Click **Add**, in **Select Groups**, type **Server Operators**, click **Check Names**, and then click **OK**.

g. Click **OK** to close **Properties**.

h. Close **Active Directory Users and Computers**.

i. Close all open windows and log off of the computer.

3. Log in to the network as Mikedan@adventure-works.com and open the Certificates console.

Note

- Mikedan was added to the Server Operators group so he can log on locally to the domain controller.

a. Log on as Mikedan@adventure-works.com.

b. On the taskbar, click the **Start** button, and then click **Run**.

c. In **Run**, type **mmc**, and then click **OK**.

d. From the **Console** menu, click **Add/Remove Snap-in**.

e. In **Add/Remove Snap-in**, click **Add**.

f. In **Add Stand-alone Snap-in**, click **Certificates**, click **Add**, and then click **OK**.

4. Use the Certificates MMC to acquire an Archive User certificate

a. In the newly-created MMC console, in the console tree, double-click **Certificates (Current User)**.

b. In the console tree, right-click **Personal**, click **All Tasks**, and then click **Request New Certificate**.

c. In the Certificate Request Wizard, click **Next**.

d. On **Certificate Template**, select the **Archive User** certificate, and then click **Next**.

e. On **Certificate Friendly Name and Description**, in **Friendly name**, type **Archive User**, and then click **Next**.

f. On **Completing the Certificate Request Wizard**, click **Finish**.

g. On **Certificate Request Wizard**, click **Install Certificate** and then click **OK**.

h. Double-click **Personal**, and then click **Certificates**.

i. In the details pane, double-click the certificate with the friendly name of **Archive User**.

j. In **Certificate**, click the **Details** tab.

Note that the certificate template that used to generate this certificate was ArchiveUser, then click **OK**.

k. Close the new console without saving changes

l. Close all windows and log off of the computer.

Task 6--Performing a Key Recovery

In this series of tasks, you will perform a key recovery by using Certutil.exe.

For more information on Certutil, see Certutil.

Important

- Perform the following procedures at the domain controller.

1. Log on to the network as Administrator and ensure that the private key is still recoverable by viewing the **Archived Key** column in the Certification Authority console.

a. Log on as Administrator@adventure-works.com.

b. From **Administrative Tools**, open **Certification Authority**.

c. In the console tree, double-click **EntCA**, and then click **Issued Certificates**.

d. From the **View** menu, click **Add/Remove Columns**.

e. In **Add/Remove Columns**, in **Available Column**, select **Archived Key**, and then click **Add**. Archived Key should now appear in **Displayed Columns**.

f. Click **OK** and then, in the details pane, scroll to the right and confirm that the last issued certificate to Mikedan has a **Yes** value in the Archived Key column.

Note

- A certificate template must have been modified so that the Archive bit and Mark Private Key as Exportable attributes were enabled. The private key is only recoverable if there is data in the Archived Key column.

g. Double-click the **Archive User** certificate.

h. Click the **Details** tab

Write down the serial number of the certificate. (Do not include spacing between digit pairs.) This is required for recovery.

The serial number will be a hexadecimal string that is 20 characters long. The serial number of the private key is the same as the serial number of the certificate. For the purposes of this walkthrough, the serial number will be referred to as *serialnumber*.

i. Click **OK**.

j. Close **Certification Authority**.

2. Recover the private key into a BLOB output file by using certutil.exe.

a. On the taskbar, click the **Start** button, click **Run**, type **cmd**, then click **OK**.

This opens a command prompt window.

b. Type **cd ** and then press ENTER.

c. Ensure that you are in the **c:** directory.

d. At the command prompt, type:

Certutil -getkey *serialnumber* **outputblob**

e. At the command prompt, type **dir outputblob**

Note

- If the file *outputblob* does not exist, you probably typed the serial number incorrectly for the certificate.

The *outputblob* file is a PKCS#7 file containing the KRA certificates and the user certificate and chain. The inner content is an encrypted PKCS#7 containing the private key (encrypted to the KRA certificates).

3. Recover the original private/public key pair using Certutil.exe

a. On the taskbar, click the **Start** button, click **Run**, type **cmd**, then click **OK**.

This opens a command prompt window.

b. At a command prompt, type:

Certutil -recoverkey outputblob Mikedan.pfx

c. When prompted, enter the following information:

Enter new password: **password**

Confirm new password: **password**

d. Type **exit**, and then press ENTER.

e. Close all windows and log off as the current user.

Task 7--Importing the recovered private key

In this series of tasks, you will restore the recovered private key in Mike's certificate store by importing the Mikedan.pfx file.

Important

- Perform the following procedures at the domain controller.

1. Log on as Mikedan@adventure-works.com and start the Certificates mmc.

a. Log on as Mikedan@adventure-works.com, with a password of *password*.

b. On the taskbar, click the **Start** button, and then click **Run**.

c. In **Run**, type **mmc**, and then click **OK**.

d. On the **File** menu, click **Add/Remove Snap-in**.

e. In **Add/Remove Snap-in**, click **Add**.

f. In **Add Standalone Snap-in**, click **Certificates**, click **Add**,and then click **OK**.

2. Delete all certificates issued by EntCA to simulate a re-installed computer.

a. Right-click **Certificates (Current User)**, and then click **Find Certificates**.

b. In **Find Certificates**, in **Contains**, type **EntCA** and then click **Find Now**.

c. In **Find Certificates**, on the **Edit** menu, click **Select All**.

d. In **Find Certificates**, on the **File** menu, click **Delete**.

e. In Certificates, click **Yes**.

f. In Root Certificate Store, click **Yes**.

g. Close **Find Certificates**.

3. Import the certificate at c:\Mikedan.pfx and let the certificates be placed automatically.

a. In the console tree, right-click **Personal** and then click **All Tasks** and then click **Import**.

b. In the Certificate Import Wizard, click **Next**.

c. On **Files to Import**, in the **File name** box, type **c:\Mikedan.pfx**, and then click **Next**.

d. In **Password**, type **password** and then click **Next**.

e. On **Certificate Store**, click **Automatically select the certificate store based on the type of certificate** and then click **Next**.

f. On **Completing the Certificate Import Wizard**, click **Finish**

g. If the **Root Certificate Store** dialog box appears, click **Yes**.

h. In **Certificate Wizard Import**, click **OK**.

Two certificates were imported. The Archive User certificate for Mike is located in the Personal certificates store and the EntCA certificate is located in the Trusted Root Certification Authorities store.

4. Verify the serial number of the imported certificate.

a. In the console tree, double-click **Personal** and then click **Certificates**.

b. Double-click the certificate

c. In **Certificate**, click the **Details** tab. Verify that the serial number matches the original.

d. Close all open windows and log off of the network.