Configuring clustered Certification Authority

This lab is based on https://technet.microsoft.com/en-us/library/cc742450(v=ws.10).aspx#BKMK_DefiningNaming

Article

The following sections describe the installation and configuration of a certification authority (CA) on a failover cluster running on Windows Server® 2008/2012/2012R2.

- Define a naming convention to use in the cluster configuration.
- Set up the CA role service on the first cluster node.
- Set up the CA role service on the second cluster node.
- Set up the failover cluster feature on both cluster nodes.
- Create the failover cluster.
- Configure the failover cluster.
- Configure the certificate revocation list (CRL) distribution point.
- Create the CRL distribution point container in Active Directory® Domain Services (AD DS).
- Configure the CA in AD DS.
- Adjust the CA names in AD DS.

Defining a naming convention to use in the cluster configuration

Before you begin, you should plan the names to use during the installation procedure. It is important to properly define these names because they are used throughout the configuration.
The following named items are used in the subsequent sections and step-by-step procedures.

Item	Description	Configuration	Uses
Cluster node	Every computer running Windows has a name; therefore, computers acting as cluster nodes have a computer name.	The computer name is configured in the properties of a Windows–based computer. **LU-CA1** **LU-CA2**	The computer names of the nodes are permitted on access control lists (ACLs) in the following Active Directory objects in the configuration naming context under Services\Public Key Services: • Authority Information Access (AIA) – *CA name*

			• Enrollment Services – *CA name* • Enrollment Services – *KRA*
Cluster	The failover cluster has a unique name that is registered in AD DS.	The cluster name is configured when the failover cluster is set up. See step 8 in Setting up failover clustering. Already set **LU-CA**	The name of the cluster is used to refer to a specific cluster in the Failover Cluster Management snap-in. There is no dependency between this name and the CA.
Service	The service name represents the Domain Name System (DNS) name of the clustered CA service.	The service name is configured when the CA is set up as a clustered service. See step 5 inConfiguring AD CS as a cluster resource. Proposed name: **LU-CA-Cluster**	The service name appears as part of the CA configuration string. The service name is represented in the following Active Directory object in the configuration naming context under Services\Public Key Services: Certificate Revocation List (CRL) Distribution Point (CDP) – *Service name*. You can obtain the service name by opening a command prompt window and running the following command: **certutil -cainfo dns**.
CA	The CA is the actual name of the CA.	The name of the CA is configured when the CA service is installed. See step 12 in Setting up the CA role service on the first cluster node.	The CA name is part of the CA configuration string and is displayed as the node name in the Certification Authority snap-in. The name is written into the Issuer attribute on every issued certificate and is also used in the following Active Directory objects in the configuration naming context under Services\Public Key Services: • AIA – *CA name* • CDP – *Service name – CA name* • Certification Authorities – *CA name* • Enrollment Services – *CA name*

			• Key Recovery Agent (KRA) – *CA name* You can obtain the CA name by opening a command prompt window and running the following command: **certutil -cainfo name**.

Setting up the CA role service on the first cluster node

This section explains how to install AD CS on the first cluster node.
The configuration of the first cluster node includes the following tasks:

- Confirm that the shared disk is available to the node. (You will have Q: disk for quorum, And F: disk for shared files)

Note
The shared resources, such as the disk storage containing the CA database and log file, must be available to the CA during setup. Releasing these resources for setting up the second node is also important after the setup of this node is finished.

- Confirm that the network hardware security module (HSM) is available to the node. v
- Install the CA on the first node.
- Export the CA certificate (and, optionally, the private key) to share it with the second node.
- Shut down the CA service on the first node.
- Take the shared storage offline.
- Release the HSM from the first node. (no HSM in the lab)

To configure the first cluster node

1. Log on to the first server with permissions to install the first cluster node (LU-CA1, logicunion\administrator). To install an enterprise CA, you need to be a member of the Enterprise Admins group for the Active Directory domain. To install a stand-alone CA, you can log on as a member of the local Administrators group, but you will not be able to register the CA in the Active Directory configuration container.
2. Click **Start**, and then click **Server Manager**.
3. In the console tree, double-click **Storage**, and then click **Disk Management**. Confirm that the shared disk that is used for the CA is online.
4. In the console tree, double-click **Diagnostics**, and then click **Services**. If you are using a network HSM, confirm that the service that connects to the network HSM is running.
5. In the console tree, click **Roles**. On the **Action** menu, click **Add Roles**.
6. On the **Select Server Roles** page, click **Active Directory Certificate Services**, and then click **Next** twice.

7. On the **Select Role Services** page, select the **Certification Authority** role service, and then click **Next**. Do not select any other role services. Only the CA role service is supported in a clustered environment.
8. Select the setup type for the CA, and click **Next**.
9. Select the CA type for the CA, and click **Next**.
10. Select **Create a new private key**, and click **Next**.
11. If you are using a network HSM, select the cryptographic service provider (CSP) provided by the HSM vendor from the list and set the desired key length. Click **Next**.
12. Enter the CA name, and click **Next**. For more information about the CA name, see Defining a naming convention to use in the cluster configuration.
13. If you are configuring a root CA, define the validity period. If you are using a subordinate CA, choose whether to submit the request online or save it to a file. Click **Next**.
14. Change the default paths for the database and log files to the desired location on the shared storage drive that you set up in Preparing the CA Cluster Environment. Click **Next**, and then click **Install**.
15. After the CA installation is complete, open the Certification Authority snap-in. In the console tree, select the CA node. On the **Action** menu, click **All Tasks**, and then click **Backup CA**.
16. On the **Welcome** page of the CA Backup Wizard, click **Next**. Select **Private key and CA certificate**, and provide a directory name where you want to temporarily store the CA certificate and optionally the key. Click **Next**.
17. Provide a password to protect the CA key, click **Next**, and then click **Finish**.
18. If you are using a network HSM, a warning message will display telling you that the private key cannot be exported. This is expected behavior because the private key will never leave the HSM. Click **OK**.
19. While the CA is selected in the console tree, on the **Action** menu, click **All Tasks**, and then click **Stop Service**.
20. Detach the shared storage from the cluster node. In the Server Manager console tree, double-click **Storage**, and then click **Disk Management**. Change the state of the disk containing the CA database to offline. Then, release the HSM from the cluster node.
21. In the console tree, double-click **Diagnostics**, and click **Services**. If you are using a network HSM, select the service that works with the HSM. On the **Action**menu, click **Stop**. Log off from the first cluster node.

The installation of the CA on the first node is now complete.

Setting up the CA role service on the second node

This section explains how to set up the second cluster node. The configuration of the second node is slightly different from the first node. Some configuration settings are already defined on the first node so they only need to be applied on the second node.

The configuration of the second node includes the following tasks:

- Confirm that the shared disk is available to the node.
- Confirm that the network HSM is available to the node.
- Import the CA certificate into the local computer certificate store.
- Associate the CA certificate with the key material stored in an HSM (this step is optional).
- Install AD CS on the second node.

The following procedure describes these tasks in greater detail.

To set up the CA role service on the second node

1. Log on to the cluster node with the same permissions used to install the first cluster node(LU-CA2, logicunion\administrator). To install an enterprise CA, log on as a member of the Enterprise Admins group to the Active Directory domain. To install a stand-alone CA, you can log on as a member of the local Administrators group, but you will not be able to register the CA in the Active Directory configuration container.

2. Open Server Manager. In the console tree, double-click **Storage**, and click **Disk Management**. Verify that the shared disk that is used for the CA is online.
3. In the console tree, double-click **Diagnostics**, and click **Services**. If you are using a network HSM, confirm that the service that connects to the network HSM has started.
4. Open the Certificates snap-in for the computer account.
5. In the console tree, double-click **Certificates (Local Computer)**, and click **Personal**.
6. On the **Action** menu, click **All Tasks**, and then click **Import** to open the Certificate Import Wizard. Click **Next**.
7. Enter the file name of the CA certificate that was previously created on the first node, and click **Next**. If you click **Browse** to find the certificate, change the file type to **Personal Information Exchange (*.pfx,*.p12)**.
8. Type the password that you have previously used to protect the private key. The password is required even if there is no private key in the .pfx file. Do not mark this key as exportable. Click **Next**.
9. Place the certificate in the **Personal** certificate store, and click **Next**. To complete the certificate import process, click **Finish**, and then click **OK**.
10. If you are using a network HSM, you must repair the association between the certificate and the private key that is stored in the HSM. In the Certificates snap-in, double-click **Personal Certificates**, and select the certificate that you just imported.
11. On the **Action** menu, click **Open**. Click the **Details** tab, copy the serial number to the Clipboard, and then click **OK**.
12. Open a command prompt window, type **certutil –repairstore My "{Serialnumber}"** and then press ENTER.
13. Open Server Manager, select the **Roles** node, and on the **Action** menu, click **Add Roles**.
14. On the **Select Server Roles** page, select **Active Directory Certificate Services**, and click **Next** twice.
15. On the **Select Role Services** page, select **Certification Authority**, and click **Next**. The CA role service is the only AD CS role service that can be configured to use clustering.
16. Select the same setup type for the CA that you used for the first node, and click **Next**.
17. Select the same CA type for the CA that you used for the first node, and click **Next**.
18. Select **Use existing private key**, select **Select a certificate and use its associated private key**, then click **Next**.
19. Select the CA certificate that was generated on the first node, and click **Next**.
20. Change the default paths for the database. In the dialog box stating that an existing database was found, select **Yes** to overwrite it. Click **Next** to continue.
21. Click **Install**. To finish the role installation, click **Close**. Log off from the second cluster node.

Setting up failover clustering

Failover clustering support is a feature in Windows Server 2008/2012/2012R2 Enterprise. The following steps must be completed on both cluster nodes.
(Already done in the lab)

To set up failover clustering on a server

1. Log on to the cluster node as a member of the local Administrators group.
2. Open Server Manager. In the console tree, click **Features**, and on the **Action** menu, click **Add Features**.
3. In the list of available features, select **Failover Clustering**, and click **Next**. Click **Install**, and then click **Close**.
4. Log on to the second cluster node (the storage should still be attached to that node). Click **Start**, point to **Run**, type **Cluadmin.msc**, and then click **OK**.
5. If the **Before you begin** page appears, click **Next**. Enter the cluster node name (computer name) of the first cluster node, and click **Add**.
6. Enter the name of the second cluster node, click **Add**, and then click **Next** to continue.
7. To test the cluster, click **Yes**, and click **Next** twice. Keep the default option to **Run all tests**, and click **Next** twice. Verify the cluster test report, and click**Finish**.
8. Provide the cluster name. This name is not relevant for the later CA configuration. View the cluster setup information page, and click **Finish**.

Configuring AD CS as a cluster resource

Before closing the Failover Cluster Management snap-in, configure AD CS as a cluster resource.

To configure AD CS as a cluster resource

1. In the console tree of the Failover Cluster Management snap-in, click **Services and Applications**.
2. On the **Action** menu, click **Configure a service or Application**. If the **Before you begin** page appears, click **Next**.
3. In the list of services and applications, select **Generic Service**, and click **Next**.
4. In the list of services, select **Active Directory Certificate Services**, and click **Next**.
5. Choose the service name, and click **Next**. For more information about the service name, see Defining a naming convention to use in the cluster configuration.
6. Select the disk storage that is still mounted to the node, and click **Next**.
7. To configure a shared registry hive, click **Add**, type **SYSTEM\CurrentControlSet\Services\CertSvc**, and then click **OK**. Click **Next** twice.
8. Click **Finish** to complete the failover configuration for AD CS.
9. In the console tree, double-click **Services and Applications**, and select the newly created clustered service.
10. In the details pane, click **Generic Service**. On the **Action** menu, click **Properties**.
11. Change the **Resource Name** to **Certification Authority**, and click **OK**.

You can now move the CA between both nodes.

If you have installed a service to access the network HSM, you should create a dependency between the CA and the network HSM service.

To create a dependency between a CA and the network HSM service (Informative – No HSM)

1. Open the Failover Cluster Management snap-in. In the console tree, click **Services and Applications**. In the details pane, select the previously created name of the clustered service. On the **Action** menu, click **Add a resource**, and then click **Generic Service**.
2. The new resource wizard appears. In the list of available services, select the name of the service that was installed to connect to your network HSM. Click**Next** twice, and then click **Finish**.
3. Under **Services and Applications** in the console tree, click the name of the clustered services.
4. In the details pane, select the newly created **Generic Service**. On the **Action** menu, click **Properties**.
5. On the **General** tab, rename the service name if desired, and click **OK**. Confirm that the service is online.
6. In the details pane, select the service previously named **Certification Authority**. On the **Action** menu, click **Properties**.
7. On the **Dependencies** tab, click **Insert**, select the network HSM service from the list, and then click **OK**.

Configuring the CRL distribution point

In the default CA configuration, the server's short name is used as part of the CRL and authority information access path. When a CA is running on a failover cluster, the server's short name must be replaced with the cluster's short name in the CRL and authority information access URL. To publish the CRL in AD DS, the CRL distribution point container must be added manually.

Note
All CA configuration tasks should be performed on the active cluster node. You must restart the CA service after changing the CRL and authority information access.

To change the configured CRL distribution points

1. Log on to the active cluster node as a member of the local Administrators group.
2. Click **Start**, point to **Run**, type **regedit**, and then click **OK**.

3. Expand the following containers in the registry: **HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration**.
4. Select the name of the CA in the **Configuration** container.
5. In the right pane, open **CRLPublicationURLs** to edit this entry.
6. In the second line, replace **%2** with the service name that was defined in step 5 of Configuring AD CS as a cluster resource. The service name also appears in the Failover Cluster Management snap-in under **Services and Applications**.
7. After the new path is entered, set all publishing options to be the same as the default LDAP URL; either completely remove the default entry or remove all the publish options.
8. Open a command prompt window, type **net stop certsvc && net start certsvc**, and press ENTER to restart the CA service.
9. At the command prompt, type **certutil -CRL**, and press ENTER to update the CRL with the new settings applied previously.

> Note
>
> If you receive an error stating "Directory object not found," complete the following procedure to create the CRL dist AD DS.

To create the CRL distribution point container in AD DS

1. At the command prompt, type **cd %windir%\System32\CertSrv\CertEnroll**, and press ENTER. The CRL file created by the certutil –CRL command should be located in this directory.
2. To publish the CRL in AD DS, type **certutil -f -dspublish** "*CRLFile.crl*", and press ENTER.

Configuring the CA in AD DS

You need to complete three procedures to configure the CA in AD DS:

- Enable both cluster nodes to update the CA certificate when required.
- Give both nodes permissions on the Enrollment container.
- Give both nodes permissions on the KRA container.

To enable both cluster nodes to update the CA certificate when required

1. Log on to the computer as a member of the Enterprise Admins group, and open the Active Directory Sites and Services snap-in.
2. In the console tree, select the top node. On the **View** menu, click **Show services node**.
3. In the console tree, double-click **Services**, double-click **Public Key Services**, and then click **AIA**.
4. In the details pane, select the CA name as it appears in the Certification Authority snap-in.
5. On the **Action** menu, click **Properties**. Click the **Security** tab, and then click **Add**.
6. Click **Object Types**, select **Computers**, and then click **OK**.
7. Type the computer name of the second cluster node as the object name, and click **OK**.
8. Confirm that the computer accounts of both cluster nodes have **Full Control** permissions, and then click **OK**.

To give both nodes permissions on the Enrollment container

1. Log on to the computer as a member of the Enterprise Admins group, and open the Active Directory Sites and Services snap-in.

2. In the console tree, select the top node. On the **View** menu, click **Show services node**.
3. In the console tree, double-click **Services**, double-click **Public Key Services**, and then click **AIA**.
4. In the console tree, click **Enrollment Services**. In the details pane, select the CA name.
5. On the **Action** menu, click **Properties**. Click the **Security** tab, and then click **Add**.
6. Click **Object Types**, select **Computers**, and click **OK**.
7. Type the computer name of the second cluster node as the object name, and click **OK**.
8. Confirm that the computer accounts of both cluster nodes have **Full Control** permissions, and then click **OK**.

To give both nodes permissions on the KRA container

1. Log on to the computer as a member of the Enterprise Admins group, and open the Active Directory Sites and Services snap-in.
2. In the console tree, select the top node. On the **View** menu, click **Show services node**.
3. In the console tree, double-click **Services**, double-click **Public Key Services**, and then click **KRA**.
4. In the details pane, select the CA name.
5. On the **Action** menu, click **Properties**. Click the **Security** tab, and then click **Add**.
6. Click **Object Types**, select **Computers**, and then click **OK**.
7. Type the computer name of the second cluster node as object name, and click **OK**.
8. Confirm that the computer accounts of both cluster nodes have **Full Control** permissions, and then click **OK**.

Adjusting the DNS name for the CA in AD DS

When the CA service was installed on the first cluster node, it created the Enrollment Services object and put its own fully qualified domain name (FQDN) into that object. Since the CA can operate on both cluster nodes, the DNS host name of the Enrollment Services object needs to be changed to the service name of the CA.

To adjust the DNS name for the CA in AD DS

1. Log on to the computer as a member of the Enterprise Admins group, and open the ADSI Edit snap-in.
2. In the console tree, click **ADSI Edit**. On the **Action** menu, click **Connect to**.
3. In the list of well-known naming contexts, select **Configuration**, and click **OK**.
4. In the console tree, double-click **Configuration**, **Services**, and **Public Key Services**, and then click **Enrollment Services**.
5. In the details pane, select the name of the cluster CA. On the **Action** menu, click **Properties**.
6. Select the attribute **dNSHostName**, and click **Edit**.
7. Enter the service name of the CA as shown in the Failover Cluster Manager under **Failover Cluster Management**, and click **OK** twice. Close ADSI Edit.