

Installation de l'autorité de certification racine

Je m'inspire de cette documentation, très complète : [Offline Root CA Setup | docs.mjcb.io](https://docs.mjcb.io/Offline-Root-CA-Setup/)

Un livre papier/kindle existe, je le recommande très fortement.

Cette documentation est en cours de rédaction.

J'utilise ici les bonnes pratiques de Microsoft qui consiste à mettre en place 2 serveurs :

- Un serveur Windows Server 2022 qui aura le rôle d'autorité de certification racine, qui sera par la suite éteint,
- Un deuxième serveur Windows Server 2022 qui aura le rôle d'autorité de certification intermédiaire, en ligne en permanence, qui délivrera les certificats clients.

On commence par mettre en place l'autorité de certification racine, qui sera par la suite offline.

A la racine du C:, on ajoute un fichier CAPolicy.inf :

```
[Version]
Signature = "$Windows NT$"

[PolicyStatementExtension]
Policies = AllIssuancePolicy, InternalPolicy
Critical = FALSE

; AllIssuancePolicy is set to the OID of 2.5.29.32.0 to ensure all certificate templates are
available.
[AllIssuancePolicy]
OID = 2.5.29.32.0

[InternalPolicy]
OID = 1.2.3.4.1455.67.89.5
Notice = "The Khroners Labs Certification Authority is an internal resource. Certificates that
are issued by this Certificate Authority are for internal usage only."
```

```
URL = http://pki.ad.khroners.fr/cps.html
```

```
[Certsrv_Server]
```

```
; Renewal information for the Root CA.
```

```
RenewalKeyLength = 4096
```

```
RenewalValidityPeriod = Years
```

```
RenewalValidityPeriodUnits = 10
```

```
; Disable support for issuing certificates with the RSASSA-PSS algorithm.
```

```
AlternateSignatureAlgorithm = 0
```

```
; The CRL publication period is the lifetime of the Root CA.
```

```
CRLPeriod = Years
```

```
CRLPeriodUnits = 10
```

```
; The option for Delta CRL is disabled since this is a Root CA.
```

```
CRLDeltaPeriod = Days
```

```
CRLDeltaPeriodUnits = 0
```

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
SRV-ROOT35-01.ad.khroners.fr

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD CS

Services de rôle

Confirmation

Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- ☐ Attestation d'intégrité de l'appareil
- ☐ Hyper-V
- ☐ Serveur de télécopie
- ☐ Serveur DHCP
- ☐ Serveur DNS
- ☐ Serveur Web (IIS)
- ☐ Service Guardian hôte
- ☐ Services AD DS
- ☐ Services AD LDS (Active Directory Lightweight Directory Services)
- ☐ Services AD RMS (Active Directory Rights Management Services)
- ☐ Services Bureau à distance
- ☐ Services d'activation en volume
- ☐ Services d'impression et de numérisation de documents
- ☒ Services de certificats Active Directory
- ☐ Services de fédération Active Directory (AD FS)
- ☒ Services de fichiers et de stockage (1 sur 12 installés)
- ☐ Services de stratégie et d'accès réseau
- ☐ Services WSUS (Windows Server Update Services)
- ☐ Windows Deployment Services

Description

Les services de certificats Active Directory (AD CS) servent à créer des autorités de certification et les services de rôle associés pour émettre et gérer les certificats utilisés dans diverses applications.

< Précédent

Suivant >

Installer

Annuler

Sélectionner des services de rôle

SERVEUR DE DESTINATION
SRV-ROOT35-01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD CS

Services de rôle

Confirmation

Résultats

Sélectionner les services de rôle à installer pour Services de certificats Active Directory

Services de rôle

- ☒ **Autorité de certification**
- ☐ Inscription de l'autorité de certification via le Web
- ☐ Répondeur en ligne
- ☐ Service d'inscription de périphérique réseau
- ☐ Service Web Inscription de certificats
- ☐ Service Web Stratégie d'inscription de certificats

Description

Une autorité de certification sert à émettre et gérer des certificats. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.

< Précédent

Suivant >

Installer

Annuler

On configure le rôle :

SERVEUR DE DESTINATION
SRV-ROOT35-01

Informations d'identification

Informations d'identificati...

Services de rôle

Confirmation

Progression

Résultats

Spécifier les informations d'identification pour configurer les services de rôle

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :

- Utiliser l'autorité de certification autonome
- Inscription de l'autorité de certification via le Web
- Répondeur en ligne

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise :

- Autorité de certification d'entreprise
- Service Web Stratégie d'inscription de certificats
- Service Web Inscription de certificats
- Service d'inscription de périphériques réseau

Informations d'identification : SRV-ROOT35-01\CA-Admin

Modifier...

[En savoir plus sur les rôles de serveur AD CS](#)

< Précédent

Suivant >

Configurer

Annuler

SERVEUR DE DESTINATION
SRV-ROOT35-01

Services de rôle

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Sélectionner les services de rôle à configurer

- ☒ Autorité de certification
- ☐ Inscription de l'autorité de certification via le Web
- ☐ Répondeur en ligne
- ☐ Service d'inscription de périphériques réseau
- ☐ Service Web Inscription de certificats
- ☐ Service Web Stratégie d'inscription de certificats

[En savoir plus sur les rôles de serveur AD CS](#)

< Précédent

Suivant >

Configurer

Annuler

Type d'installation

SERVEUR DE DESTINATION
SRV-ROOT35-01

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier le type d'installation de l'AC

Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.

☐ Autorité de certification d'entreprise

Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.

☒ Autorité de certification autonome

Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).

[En savoir plus sur le type d'installation](#)

< Précédent

Suivant >

Configurer

Annuler

Type d'autorité de certification

SERVEUR DE DESTINATION
SRV-ROOT35-01.ad.khroners.fr

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

☒ Autorité de certification racine

Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.

☐ Autorité de certification secondaire

Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

[En savoir plus sur le type d'autorité de certification](#)

< Précédent

Suivant >

Configurer

Annuler

Clé privée

SERVEUR DE DESTINATION
SRV-ROOT35-01.ad.khroners.fr

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

☒ Créer une clé privée

Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

☐ Utiliser la clé privée existante

Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.

☐ Sélectionner un certificat et utiliser sa clé privée associée

Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.

☐ Sélectionner une clé privée existante sur cet ordinateur

Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

[En savoir plus sur la clé privée](#)

< Précédent

Suivant >

Configurer

Annuler

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION
SRV-ROOT35-01

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement :

RSA#Microsoft Software Key Storage Provider

Longueur de la clé :

4096

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :

SHA256

SHA384

SHA512

SHA1

☐ Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.[En savoir plus sur le chiffrement](#)

< Précédent

Suivant >

Configurer

Annuler

Nom de l'autorité de certification

SERVEUR DE DESTINATION
SRV-ROOT35-01

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

Suffixe du nom unique :

Aperçu du nom unique :

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent

Suivant >

Configurer

Annuler

Période de validité

SERVEUR DE DESTINATION
SRV-ROOT35-01

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

10

Années



Date d'expiration de l'AC : 30/09/2033 18:57:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

[En savoir plus sur la période de validité](#)

< Précédent

Suivant >

Configurer

Annuler

Base de données de l'autorité de certification

SERVEUR DE DESTINATION
SRV-ROOT35-01

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats :

C:\Windows\system32\CertLog

Emplacement du journal de la base de données de certificats :

C:\Windows\system32\CertLog

[En savoir plus sur la base de données de l'autorité de certification](#)

< Précédent

Suivant >

Configurer

Annuler

```
certutil.exe -setreg CA\DSConfigDN "CN=Configuration,DC=ad,DC=khroners,DC=fr"
certutil.exe -setreg CA\ValidityPeriodUnits 5
certutil.exe -setreg CA\ValidityPeriod "Years"
certutil.exe -setreg CA\CRLPeriodUnits 52
certutil.exe -setreg CA\CRLPeriod "Weeks"
certutil.exe -setreg CA\CRLOverlapPeriodUnits 12
certutil.exe -setreg CA\CRLOverlapPeriod "Hours"
net stop CertSvc
net start CertSvc
```

[Offline Root CA Setup | docs.mjcb.io](https://docs.mjcb.io)

Revision #6

Created 27 September 2023 05:49:23 by Khroners

Updated 5 October 2023 22:21:26 by Khroners