02 - Concevoir et implémenter AD CS

Il est essentiel de s'assurer que vous concevez votre autorité de certification interne de façon optimale. Votre conception aura des implications significatives sur la sécurité et les aspects opérationnels de votre environnement d'infrastructure à clé publique.

Conception d'une hiérarchie basée sur AD CS

Avant d'implémenter AD CS, vous devez d'abord concevoir votre hiérarchie d'autorités de certification. Dans le cadre de votre conception, vous devez déterminer le nombre de niveaux d'autorité de certification dont vous avez besoin et quel sera le rôle de l'autorité de certification dans chaque niveau. Nous vous déconseillons de générer une hiérarchie d'autorités de certification de plus de trois niveaux, sauf si elle se trouve dans un environnement complexe, hautement sécurisé ou distribué. La plupart du temps, les hiérarchies d'autorités de certification ont deux niveaux, avec l'autorité de certification racine au niveau supérieur et une autorité de certification émettrice secondaire au deuxième niveau. En règle générale, vous utilisez l'autorité de certification racine pour générer la hiérarchie d'autorités de certification. Dans ce cas, l'autorité de certification racine reste hors connexion lorsque vous vous appuyez sur l'autorité de certification secondaire pour émettre et gérer des certificats.

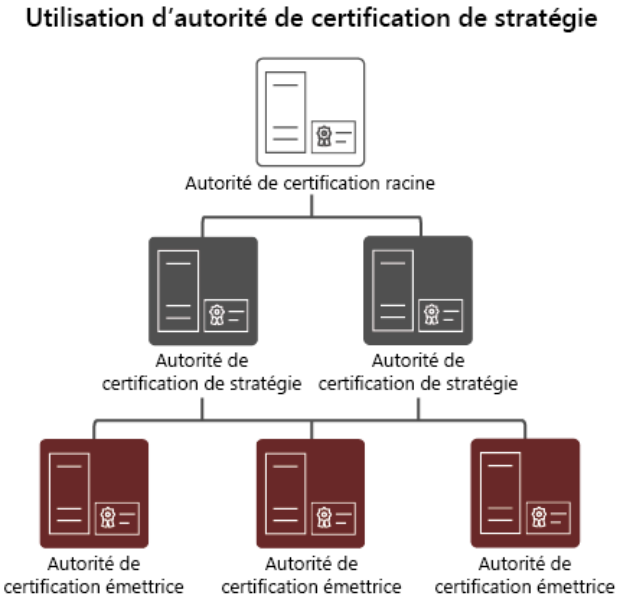
> **Notes**
>
> Une hiérarchie d'autorités de certification à plusieurs niveaux n'est pas obligatoire. Pour les environnements plus petits et moins complexes, vous pouvez implémenter une autorité de certification racine uniquement. Dans ce cas, l'autorité de certification racine fournit également la fonctionnalité d'émission et de gestion des certificats.

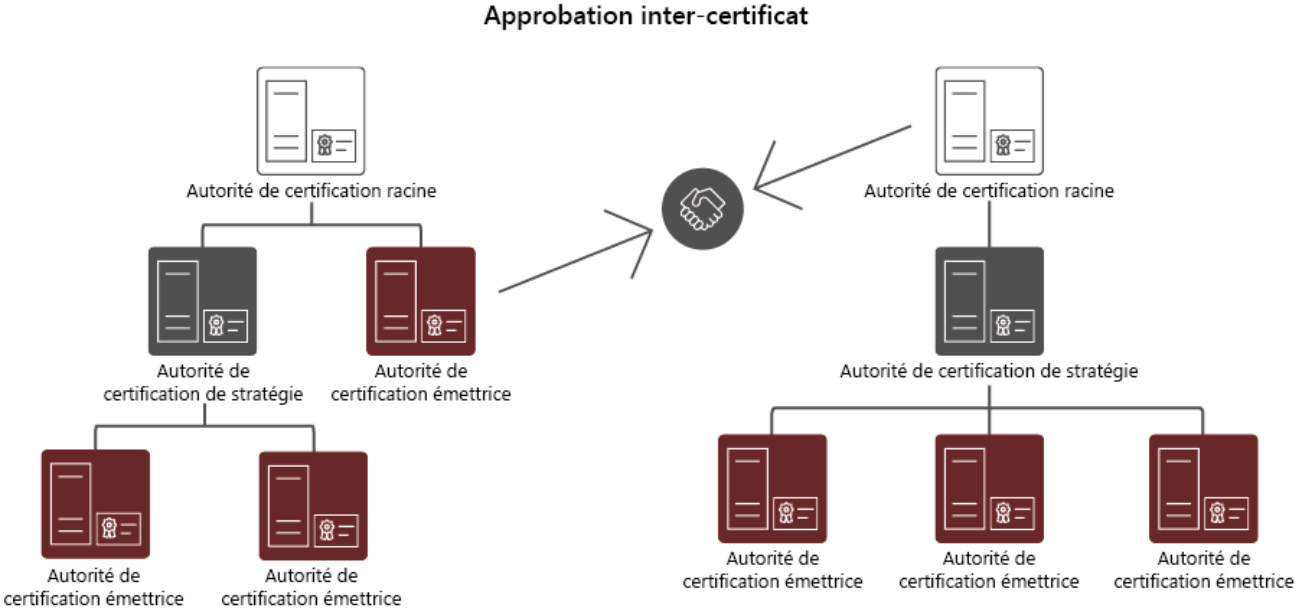
Voici quelques conceptions d'autorité de certification plus complexes :

- Hiérarchies d'autorités de certification avec une autorité de certification de stratégie. Les autorités de certification de stratégie sont des autorités de certification secondaires se trouvant directement sous l'autorité de certification racine et au-dessus des autres autorités de certification secondaires dans une hiérarchie d'autorités de certification. Vous utilisez des autorités de certification de stratégie pour émettre des certificats d'autorité de certification pour leurs autorités de certification secondaires. Les certificats d'autorité de certification reflètent les stratégies et les procédures qu'une organisation implémente pour sécuriser son infrastructure à clé publique, les processus qui valident l'identité des détenteurs de certificats et les processus qui appliquent les procédures de gestion des certificats. Une autorité de certification de stratégie émet un certificat uniquement vers d'autres autorités de certification. Les autorités de certification qui reçoivent ces certificats doivent respecter et appliquer les stratégies définies par

l’autorité de certification de stratégie. L’utilisation d’autorités de certification de stratégie n’est pas obligatoire, à moins que des divisions, des secteurs ou des emplacements différents de votre organisation ne nécessitent des stratégies et des procédures d’émission différentes. Par exemple, une organisation peut implémenter une autorité de certification de stratégie pour tous les certificats qu’elle émet en interne pour les employés et une autre autorité de certification de stratégie pour tous les certificats qu’elle émet pour les sous-traitants.

- Hiérarchies d’autorités de certification avec certification croisée de confiance. Dans ce scénario, deux hiérarchies d’autorités de certification indépendantes inter-opèrent lorsqu'une autorité de certification dans une hiérarchie émet un certificat d’autorité de certification croisée pour une autorité de certification dans une autre hiérarchie. Dans ce cas, vous établissez une confiance mutuelle entre des hiérarchies d’autorités de certification différentes.





Le tableau suivant détaille les différences les plus importantes entre les autorités de certification autonomes et d'entreprise.

Caractéristique	Autorité de certification autonome	Autorité de certification d'entreprise
Utilisation classique	Vous utilisez généralement une autorité de certification autonome pour les autorités de certification hors connexion.	Vous utilisez généralement une autorité de certification d'entreprise pour émettre des certificats pour les utilisateurs, les ordinateurs et les services. Vous ne pouvez pas l'utiliser en tant qu'autorité de certification hors connexion.
Dépendances AD DS	Une autorité de certification autonome ne dépend pas d'AD DS.	Une autorité de certification d'entreprise s'appuie sur AD DS comme sa base de données de configuration et d'inscription. Une autorité de certification d'entreprise utilise également AD DS pour publier des certificats et leurs métadonnées.
Méthodes de demande de certificat	Les utilisateurs peuvent demander des certificats auprès d'une autorité de certification autonome à l'aide d'une procédure manuelle ou d'une inscription via le web.	Les utilisateurs peuvent demander des certificats auprès d'une autorité de certification d'entreprise à l'aide de l'inscription manuelle, de l'inscription via le web, de l'inscription automatique, de l'inscription pour le compte de et des services web.
Méthodes d'émission de certificat	Un administrateur d'autorité de certification doit approuver toutes les demandes manuellement.	L'autorité de certification peut émettre des certificats ou refuser automatiquement l'émission de certificats en fonction d'une configuration personnalisée définie par l'administrateur de l'autorité de certification.

Une autorité de certification racine d'entreprise est le choix le plus courant lors du déploiement d'une autorité de certification unique dans un environnement AD DS. Si vous déployez une hiérarchie à deux niveaux avec une autorité de certification secondaire dans un environnement AD DS, vous devez envisager d'utiliser une autorité de certification racine autonome en tant qu'autorité de certification racine. Cela vous permet de la mettre hors connexion sans affecter le processus de gestion des certificats pour les utilisateurs de domaine et les appareils joints à un domaine.

Un autre point à prendre en compte est le type d'installation du système d'exploitation. L'Expérience utilisateur et les scénarios d'installation Server Core prennent en charge AD CS. Server Core minimise la surface potentielle du pirate et la surcharge de maintenance du système d'exploitation, ce qui en fait le choix optimal pour AD CS dans un environnement d'entreprise.

De plus, vous devez garder à l'esprit que vous ne pouvez pas modifier les noms d'ordinateur, le nom de domaine ou l'appartenance à un domaine d'ordinateur après avoir déployé une autorité de certification de n'importe quel type sur cet ordinateur. Par conséquent, il est important de configurer ces paramètres avant le déploiement.

Certaines considérations spécifiques au déploiement d'une autorité de certification racine autonome hors connexion sont également disponibles :

- Avant d'émettre un certificat secondaire à partir de l'autorité de certification racine, assurez-vous de fournir au moins un point de distribution de liste de révocation de certificats (CDP) et un emplacement AIA qui seront disponibles pour tous les clients. Cela est dû au fait que, par défaut, le CDP et l'AIA se trouvent sur une autorité de certification racine autonome elle-même. Par conséquent, lorsque vous déconnectez l'autorité de certification racine du réseau, une vérification de la révocation échoue, car le CDP et les emplacements AIA ne sont pas accessibles. Lorsque vous définissez ces emplacements, vous devez copier manuellement les informations de liste de révocation de certificats et d'AIA à cet emplacement.
- Définissez une période de validité pour les listes de révocation de certificats que l'autorité de certification racine publie sur une longue période de temps, un an par exemple. Cela signifie que vous devrez activer l'autorité de certification racine une fois par an pour publier une nouvelle liste de révocation de certificats, puis que vous devrez la copier dans un emplacement disponible pour les clients. Si vous ne le faites pas, après l'expiration de la liste de révocation de certificats de l'autorité de certification racine, les vérifications de révocation de tous les certificats échoueront également.
- Utilisez Stratégie de groupe pour publier le certificat d'autorité de certification racine dans un magasin d'autorités de certification racine approuvé sur tous les ordinateurs serveurs et clients. Vous devez le faire manuellement, car une autorité de certification autonome ne peut pas le faire automatiquement, contrairement à une autorité de certification d'entreprise. Vous pouvez également publier le certificat d'autorité de certification racine sur AD DS à l'aide de l'outil en ligne de commande `certutil`.

Atelier

Objectif

- Configurer les composants requis pour une autorité de certification racine d’entreprise.
- Déployer une autorité de certification racine d’entreprise.

Étapes :

Créer une VM MOD-Win2022

- Installer Windows Server 2022 (GUI)
- Autonome (workgroup), mis à jour, utilitaires....

Cloner la VM MOD-Win2022 en VM Win2022-DC1

- sysprep :

```
%WINDIR%\system32\sysprep\sysprep.exe /generalize /reboot /oobe
```

- Adressage IP statique : 10.14.0.10
- Nom d'hôte (Alias) : srvdc1
- Suffixe DNS principal (FQDN) : staff.local
- Test avec nslookup

Rôle AD DS

- Installer et configurer AD DS
- Promouvoir srvdc1 en tant que DC
- DDNS intégré à l'AD avec mises à jour sécurisées uniquement

Cloner la VM MOD-Win2022 en VM Win2022-root-CA

- sysprep :

```
%WINDIR%\system32\sysprep\sysprep.exe /generalize /reboot /oobe
```

- Adressage IP statique : 10.14.0.11/16
- Nom d'hôte (Alias) : srvca
- Suffixe DNS principal (FQDN) : staff.local
- Intégration au domaine AD
- Test avec nslookup

Rôle AD CS

- Installer AD CS avec le gestionnaire de serveur :
  Ajout du rôle Services de certificats Active Directory
- Configurer les services de certificats AD
  - Informations d'identification pour configurer les services de rôle : `administrateur@staff.local`
  - services de rôle à configurer :
    - `Autorité de certification`
    - `Inscription de l'autorité de certification via le web`
  - Type d'installation de l'CA :
    - `Autorité de certification d'entreprise`
    - `Autorité de certification racine`
    - Spécifier le type de la clé privé : `Créer une clé privée`
      - Longueur de la clé : 4096
      - Algorithme de hachage pour signer les certificats émis : SHA512
    - Spécifier le nom de l'CA :
      - Nom commun : cefim-srv-CAroot
      - Suffixe de nom logique : dc=staff,dc=local
        - Aperçu du nom unique : cn=staff-srv-CAroot,dc=staff,dc=local
    - Spécifier la période de validité : 10 ans
    - Spécifier les emplacements des bases de données : pas de modification
    - Lire attentivement le résumé avant de cliquer sur le bouton **Configurer**
    - Processus de création puis **Fermer**
- Vérification
  - Nouvelle console : `Autorité de certification` = Outil pour gérer le CA
  - Bouton droit sur le nom du CA, onglet `Général` :
    - `Afficher le certificat` pour voir la date de validité,
    - Onglet `Détails` pour voir les informations saisies
  - Onglet `Extensions` :
    - CDP (Points de distribution de liste de révocation des certificats)
      Publication des révocations
    - AIA (Accès aux informations de l'autorité)
  - Sur l'annuaire AD, lancer `utilisateurs et ordinateurs AD`
    Dans le conteneur `Users`, nous avons le groupe Domaine Local de type sécurité `Editeurs de certificats` qui a un membre, un compte ordinateur utile uniquement pendant l'installation. Supprimez-le.
  - Console ADSIedit, faire bouton droit sur `Configuration`
    - Choisir `Paramètres`

    - Sélectionnez le contexte d'attribution de noms connu : `Configuration`
      CN=Configuration...
      CN=Services
      CN=Public Key Services
      CN=Certification Authorities
      -> où on retrouve l'autorité de certification d'entreprise DONC le CA est inscrite dans l'AD
- WIN+R mmc
    - Ajouter le snap-in, `Certificats
    - Un compte d'ordinateur local puis **Ok**
    - Dans le nœud `Certificats Autorités de certification racines de confiance`
        - `Certificats` -> où on voit le CA que nous avons installés