01 - Explorer les notions de base de l’infrastructure à clé publique et d’AD CS

Pour obtenir des certificats pour votre infrastructure AD DS, vous pouvez les demander auprès d’une autorité de certification publique ou les émettre à l’aide de votre propre infrastructure. Pour implémenter votre propre autorité de certification, vous pouvez utiliser AD CS, qui est le chemin que Contoso a choisi de prendre. AD CS est une technologie d’identité dans Windows Server qui vous permet d’implémenter une infrastructure à clé publique pour votre **organisation**.

Qu’est-ce que l’infrastructure à clé publique ?

L’infrastructure à clé publique est une combinaison de logiciels, de technologies de chiffrement, de processus et de services qui permet à une organisation de sécuriser ses données, ses communications et ses transactions commerciales. L’infrastructure à clé publique s’appuie sur l’échange de certificats numériques entre les utilisateurs authentifiés et les ressources approuvées. Vous utilisez des certificats pour sécuriser les données et gérer les informations d’identification des utilisateurs et des ordinateurs à la fois dans et en dehors de votre organisation.

Qu’est-ce qu’AD CS ?

Vous pouvez implémenter une solution d’infrastructure à clé publique à l’aide du rôle Windows Server AD CS. AD CS fournit tous les composants liés à l’infrastructure à clé publique sous forme de services de rôle. Chaque service de rôle est responsable d’une partie spécifique de l’infrastructure de certificat tout en travaillant ensemble pour former une solution complète.

Le rôle AD CS comprend les services de rôle suivants :

- Autorité de certification. Les principaux objectifs des autorités de certification sont d’émettre des certificats, de révoquer des certificats et de publier des informations d’accès aux informations de l’autorité (AIA) et de révocation. La première autorité de certification que vous déployez devient la racine de votre infrastructure à clé publique interne. Par la suite, vous pouvez déployer des autorités de certification secondaires, positionnées dans la hiérarchie d’infrastructure à clé publique, avec l’AC racine en haut. Les autorités de certification secondaires approuvent implicitement l’AC racine et, par implication, les certificats qu’elle émet.

> **Vous avez la possibilité de déployer plusieurs hiérarchies d’autorités de certification internes, chacune avec sa propre racine.**

- Inscription en ligne de l'autorité de certification. Ce composant fournit une méthode pour émettre et renouveler des certificats dans des scénarios où les utilisateurs utilisent des appareils qui ne sont pas joints au domaine ou qui exécutent des systèmes d’exploitation autres que Windows.
- Répondeur en ligne. Vous pouvez utiliser ce composant pour configurer et gérer la vérification de la validation et de la révocation du protocole OCSP. Un répondeur en ligne décode les requêtes d’état de révocation pour des certificats spécifiques, évalue l’état de ces certificats et retourne une réponse signée avec les informations d’état de certificat demandées.
- Service d’inscription de périphérique réseau (SCEP). Avec ce composant, les routeurs, commutateurs et autres périphériques réseau peuvent obtenir des certificats auprès d’AD CS.
- Service d'enrôlement Web pour certificats (CES). Ce composant fonctionne en tant que client proxy entre un ordinateur exécutant Windows et l’autorité de certification. CES permet aux utilisateurs, aux ordinateurs ou aux applications de se connecter à une autorité de certification à l’aide de services web pour :
  - Demander, renouveler et installer les certificats émis.
  - Récupérer les listes de révocation de certificats (CRL).
  - Télécharger un certificat racine.
  - S’inscrire sur Internet ou entre des forêts.
  - Renouveler automatiquement des certificats pour des ordinateurs qui font partie de domaines AD DS non approuvés ou qui ne sont pas joints à un domaine.
- Service Web de politique d’inscription de certificats. Ce composant permet aux utilisateurs d’obtenir des informations sur la stratégie d’inscription de certificats. Associé à CES, il permet l’inscription de certificats basée sur des stratégies dans des scénarios où les appareils utilisateur ne sont pas joints au domaine ou ne peuvent pas se connecter à un contrôleur de domaine.

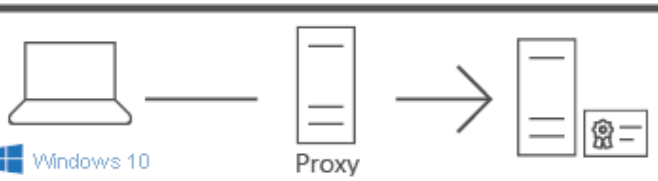
CA

CA Inscription par le web

Répondeur en ligne

Périphérique réseau
Service d'inscription

Inscription de certificats
Service web



Inscription de certificats
Service web de stratégie