Installation d'Active Directory Certificate Services

Sommaire :

I. Présentation du projet :

Dans le cadre de ce projet, l'objectif principal est de mettre en place **Active Directory Certificate Services (ADCS)** sur un serveur Windows. ADCS permet de créer et de gérer des certificats numériques dans un environnement Active Directory, garantissant ainsi la sécurité des communications et l'authentification des utilisateurs et des services.

L'utilisation des certificats numériques est essentielle pour assurer la confidentialité et l'intégrité des données échangées sur un réseau. Grâce à l'ADCS, il est possible de gérer les demandes de certificats, de les émettre, de les révoquer, et d'assurer une gestion centralisée des certificats pour les utilisateurs et les ordinateurs de l'organisation.

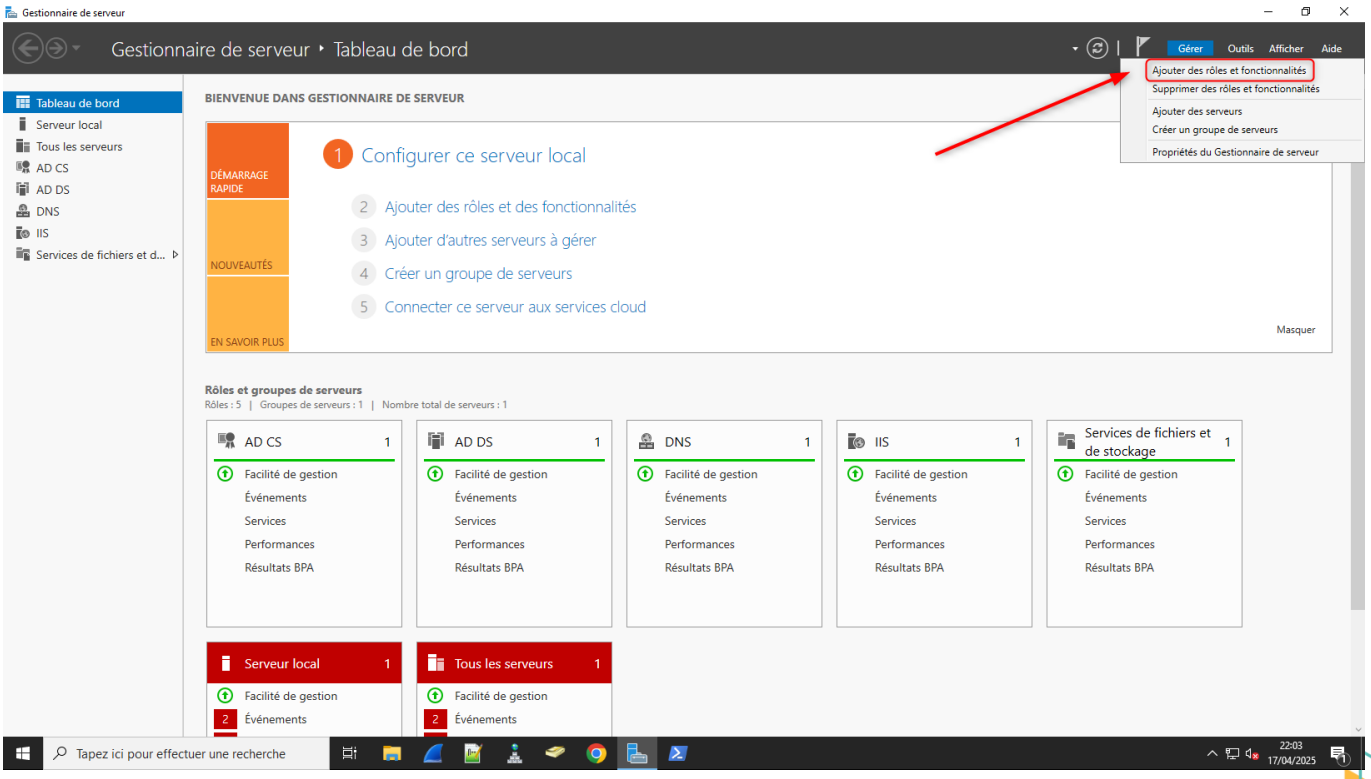
Ce projet vise à :

- Installer et configurer le rôle **ADCS** sur un serveur Windows.
- Créer une autorité de certification (CA) interne pour gérer la délivrance des certificats.
- Mettre en place des certificats pour des services spécifiques comme l'authentification des utilisateurs, le chiffrement des communications, et la signature des données.

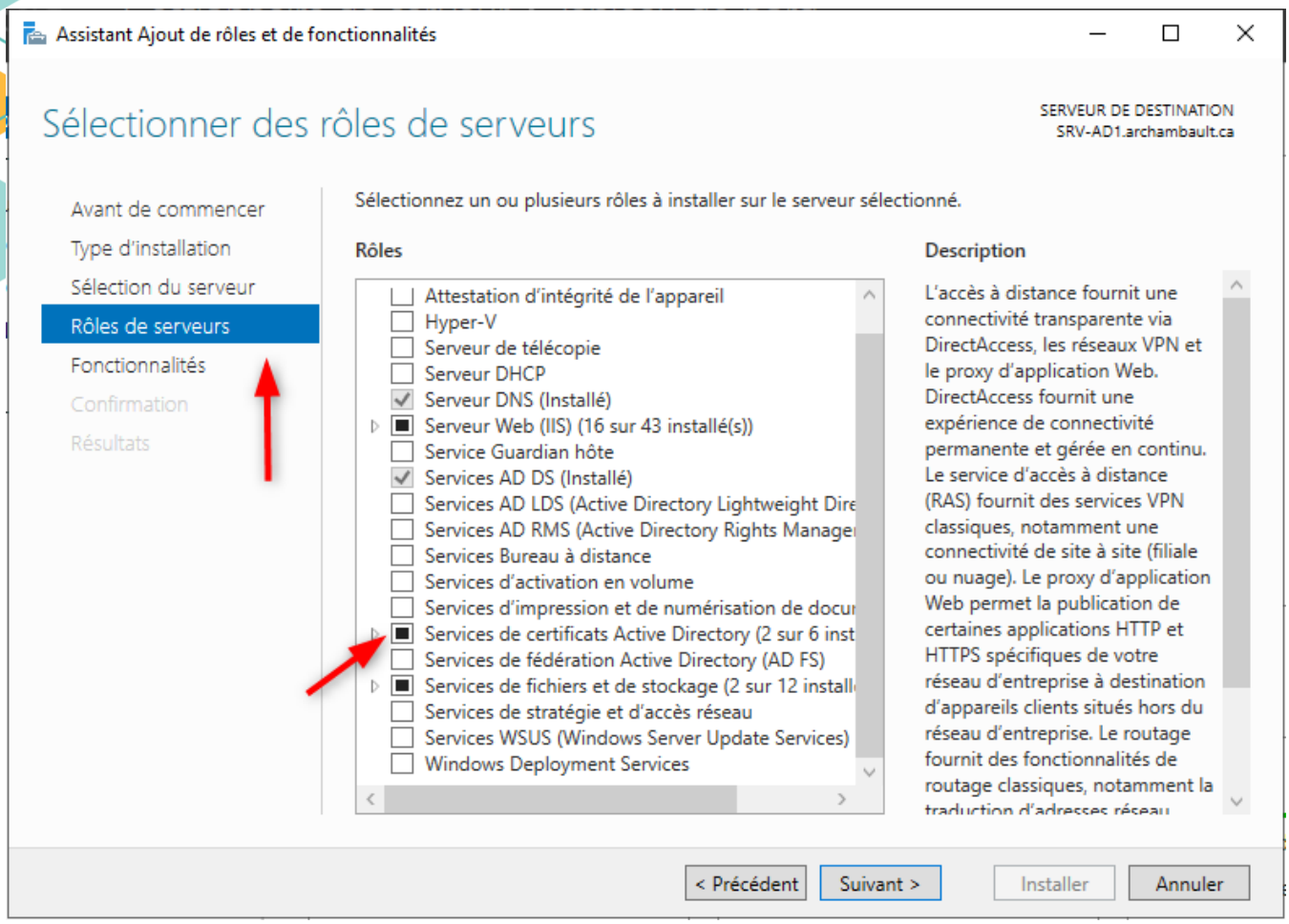
Le projet s'inscrit dans un contexte de renforcement de la sécurité du réseau, avec une gestion centralisée des certificats permettant de garantir une meilleure gestion de la sécurité des communications entre les différents composants de l'infrastructure réseau.

II. Mise en place d'Active Directory Certificate Services :

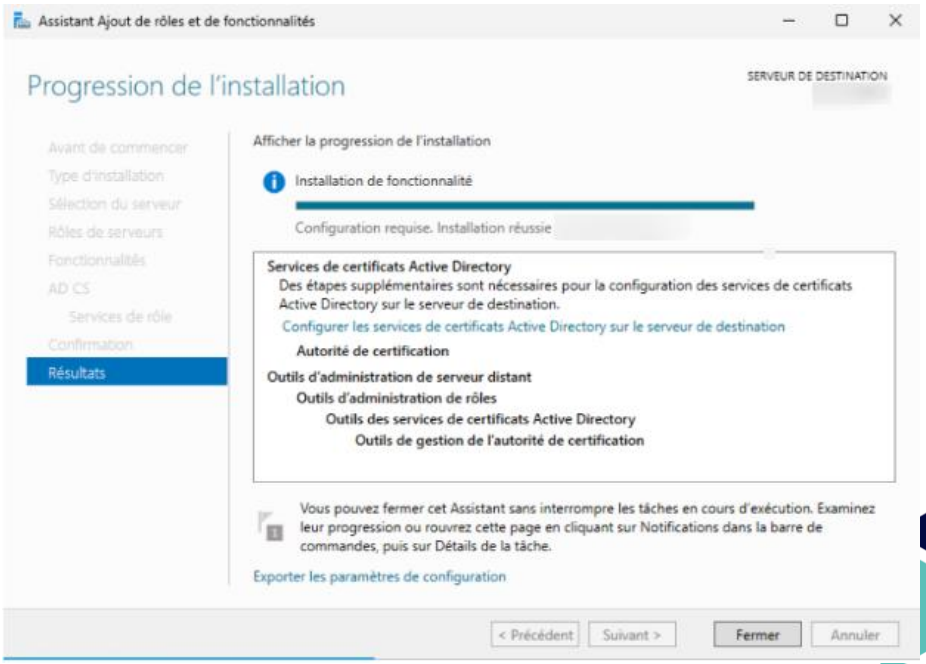
Sur un Windows Serveur 2022 du domaine, ici basé sur mon serveur AD, il suffit de cliquer dans le gestionnaire de serveurs sur Ajouter des rôles et des fonctionnalités :



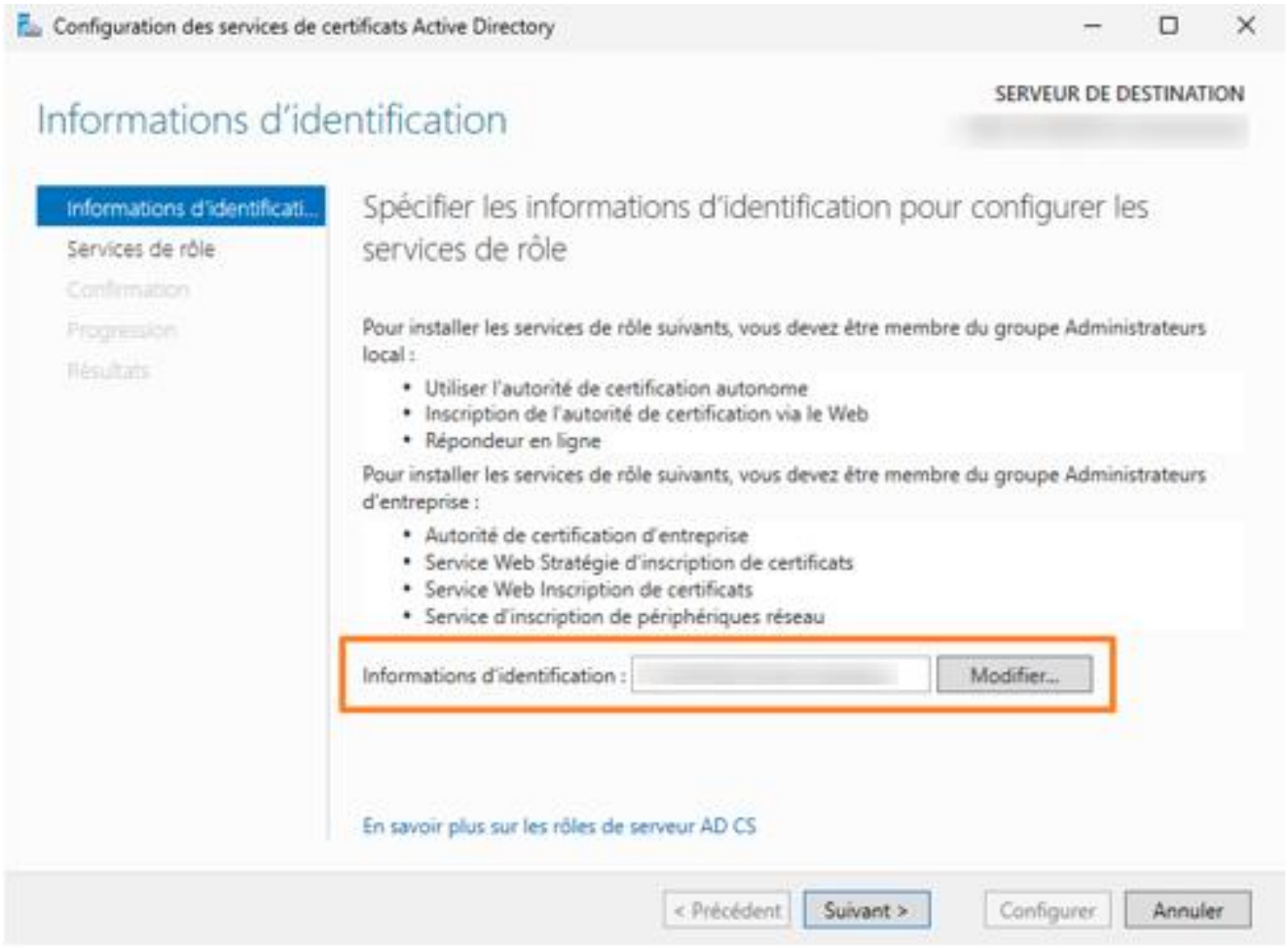
Puis sélectionner le serveur, faire suivant et saisir dans la partie Rôles de serveurs « Services de certificats Active Directory.



Sur la partie service de rôle cocher l'option Autorité de certification :



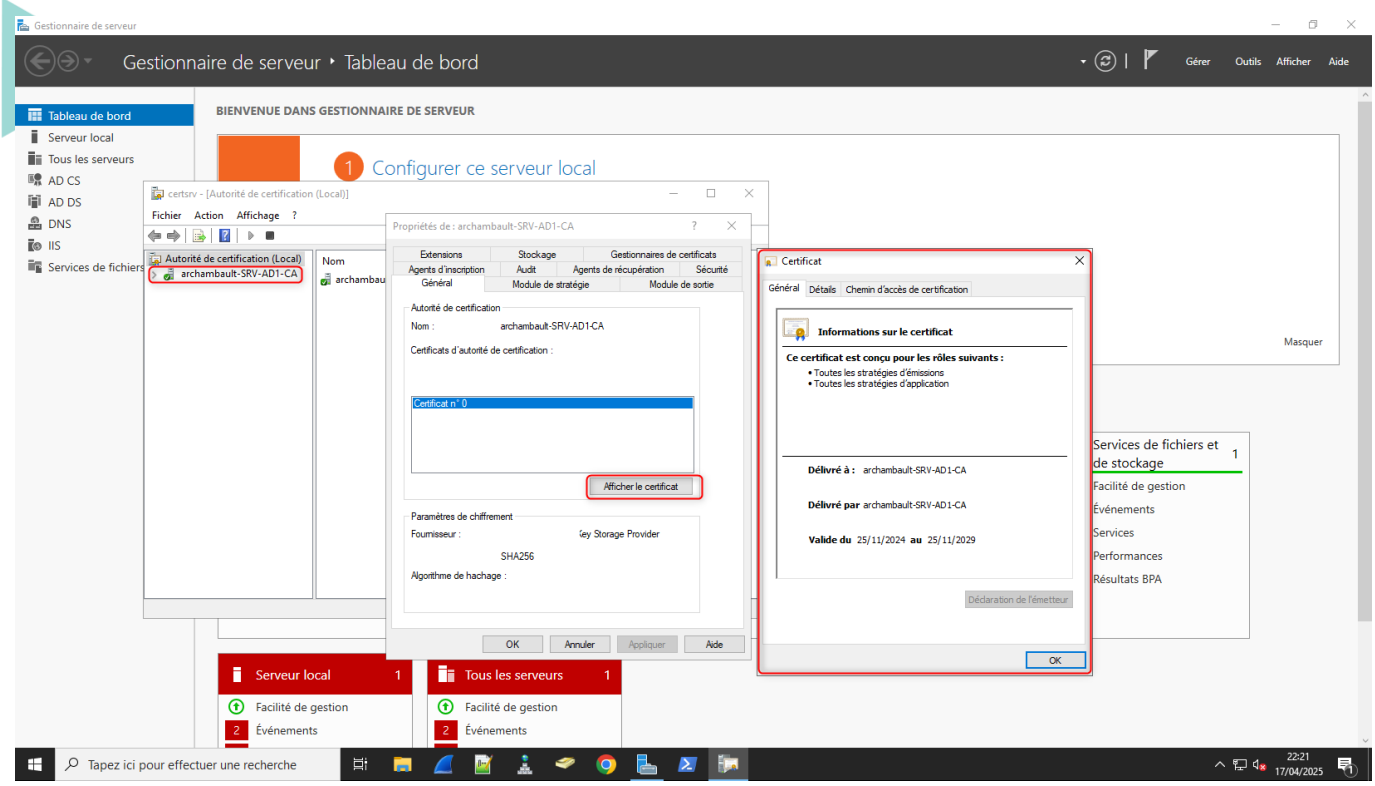
Une fois l'installation terminée, continuer et créer l'autorité de certification et saisir le compte d'identification :



Continuer les différentes étapes en venant déclarer les paramètres spécifiques à cette autorité de certification.

- Autorité racine
- Génération de clé privé
- Options de chiffrement

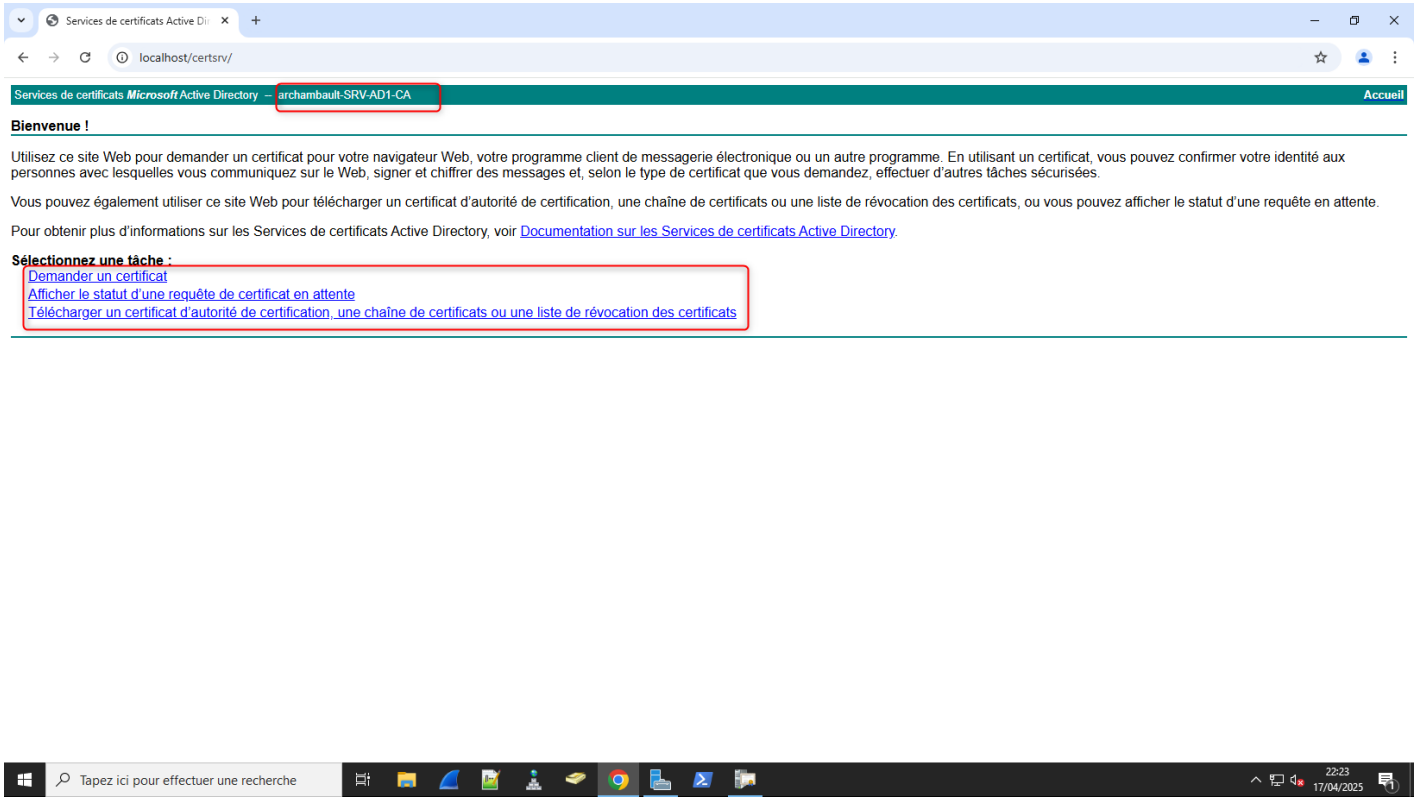
Une fois l'autorité de certification créée, il est possible de retrouver le certificat dans la console Autorité de certification.



Ce certificat sera à distribuer sur toutes les machines qui auront accès sur des sites certifiés par cette autorité de certification.

III. Accès au site et aperçu :

Il est possible d'accéder au site de l'autorité de certification en saisissant : IPDUSERVEUR/certsrv



Depuis cette console, il est possible de :

- Signer des nouveaux certificats.
- Afficher le statut d'une requête de certificat.
- Télécharger le certificat de l'autorité de certification, une chaine de certificats ou une liste de révocation de certificats.

IV. Compétences mises en œuvre :

Compétence du référentiel	Mise en œuvre dans le projet
Gérer le patrimoine informatique	Installation d'un service de gestion et de sécurisation basé sur une autorité de certification.
Mettre à disposition des utilisateurs un service informatique	Mise en place d'un service permettant d'avoir une authentification forte sur les services interne. Chiffrement des communications des services.