

TP 04 : Cryptologie

Luka VALENCELLE

Allan ETTINGER

Table des matières

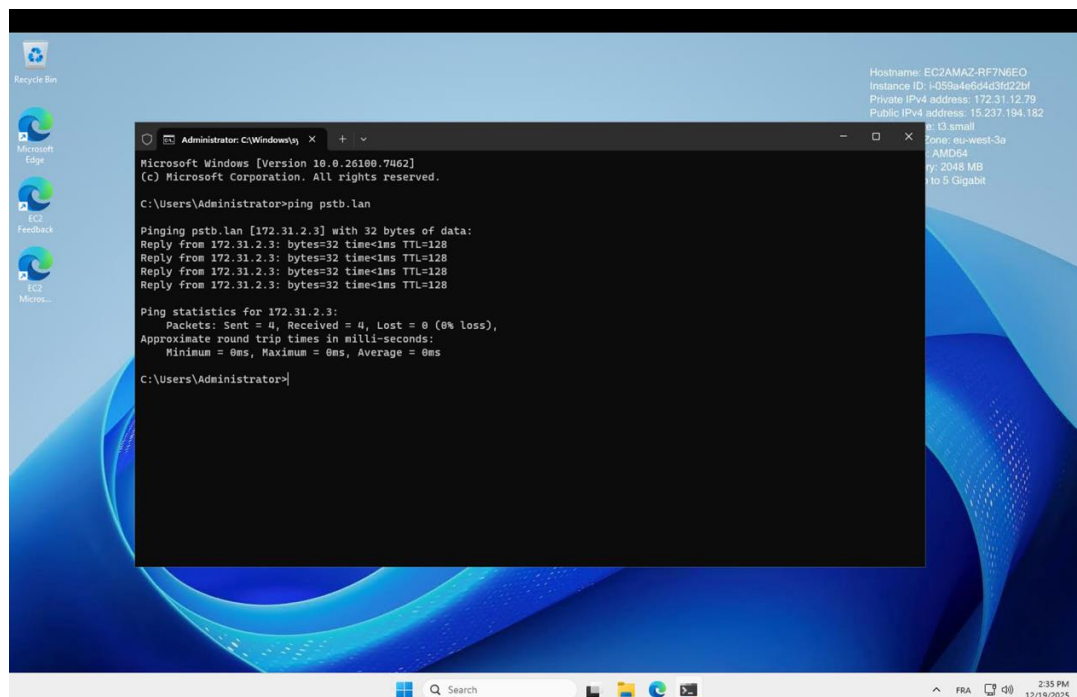
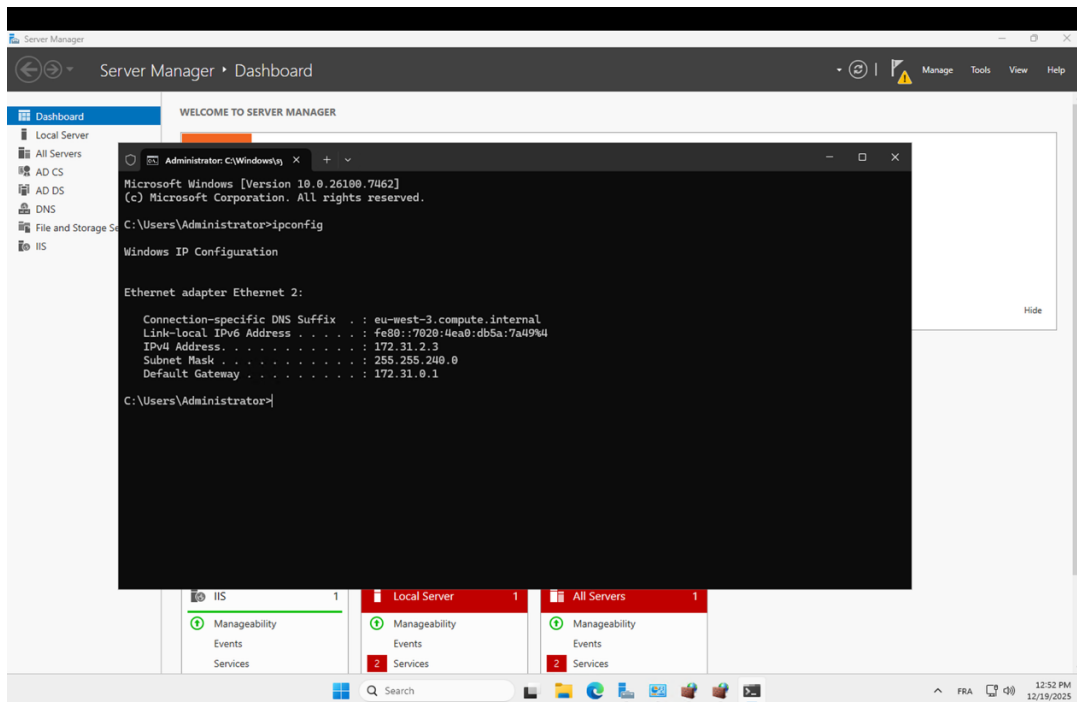
<i>Installation d'un serveur et d'un client.....</i>	<i>3</i>
<i>Certificat de l'autorité</i>	<i>4</i>
<i>Installation manuelle du certificat.....</i>	<i>4</i>
<i>Demande de certificat.....</i>	<i>5</i>
Demande depuis la console IIS.....	5
Demande depuis la console MMC	5
<i>Auto enroll</i>	<i>6</i>
<i>Sauvegarde de l'AD CS</i>	<i>7</i>

Installation d'un serveur et d'un client

Pur cette réalisation, Windows Server 2025 a été installé en tant que serveur et promu en tant que contrôleur de domaine.

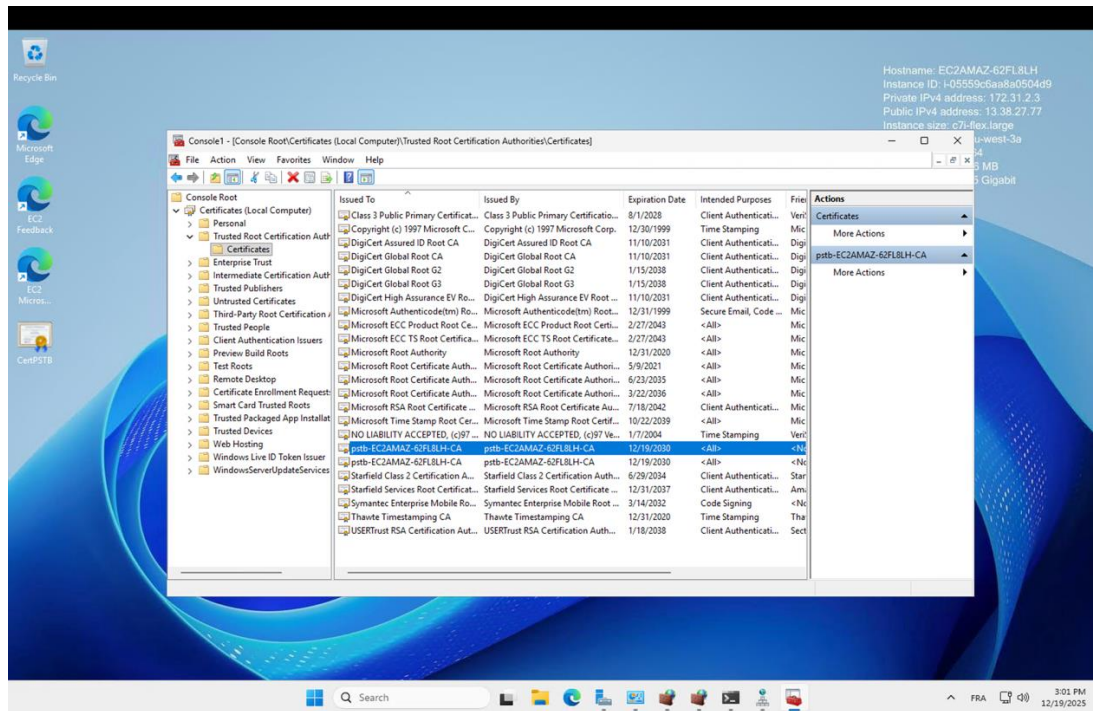
Sur ce dernier ont été installé les rôles AD CS et IIS. L'Autorité de Certification à par la suite été configurée.

Ensuite, Windows 11 a été installé en tant que client sur une autre machine et cette machine a été jointe au domaine.



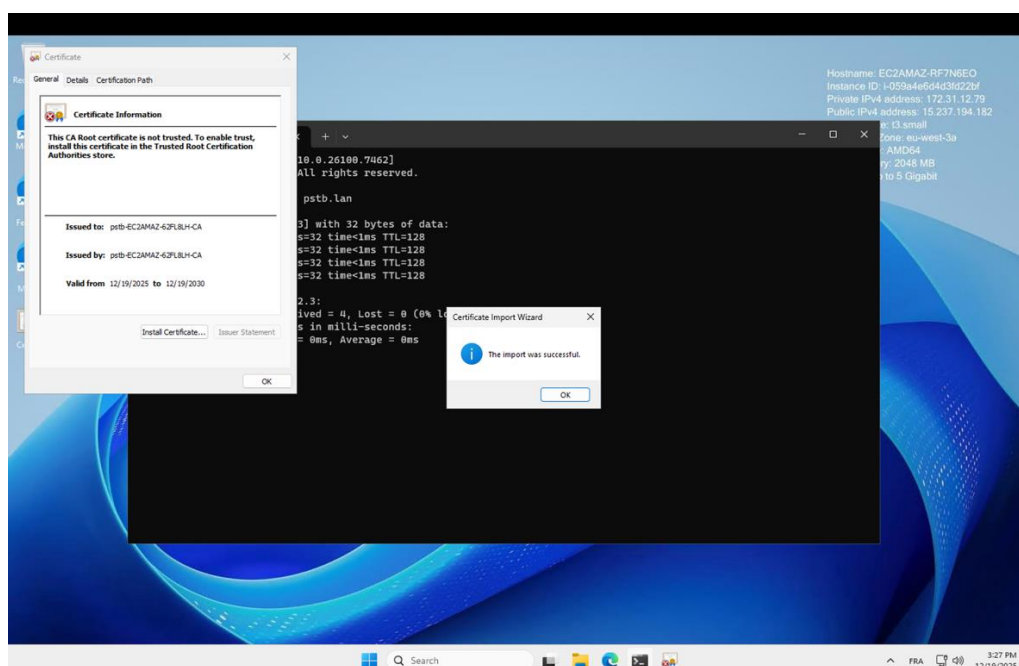
Certificat de l'autorité

Ici, nous avons d'abord exporté notre certificat root sur le bureau avant de générer des certificats avec l'autorité de certifications afin d'éviter les messages d'erreur dans les navigateurs et de permettre le bon fonctionnement des services.



Installation manuelle du certificat

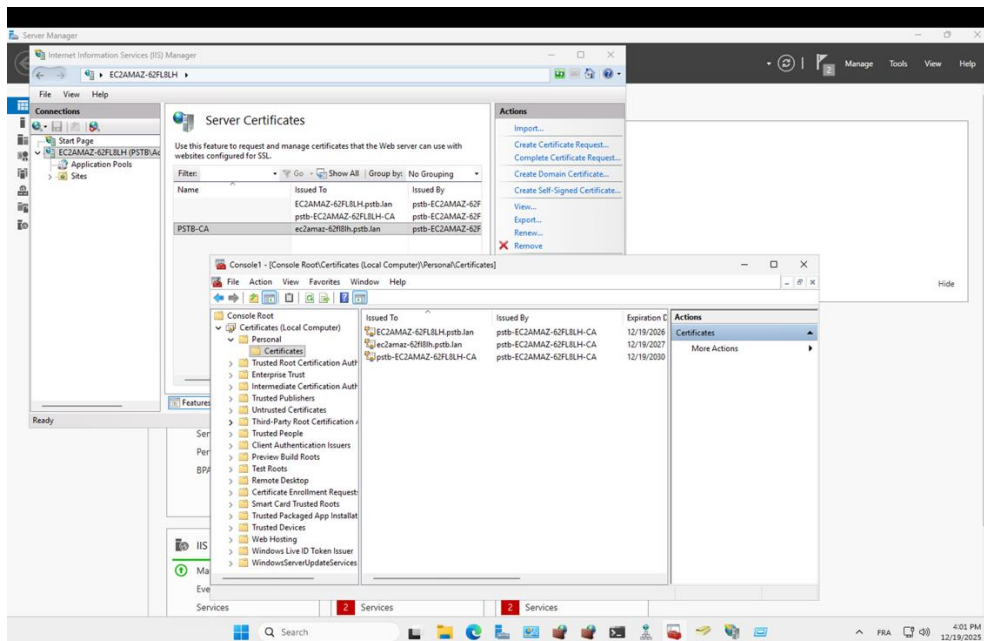
Dans un premier temps, nous avons copié le certificat du serveur au client via RDP. Ensuite, nous avons pu procéder à l'installation manuelle du certificat.



Demande de certificat

Demande depuis la console IIS

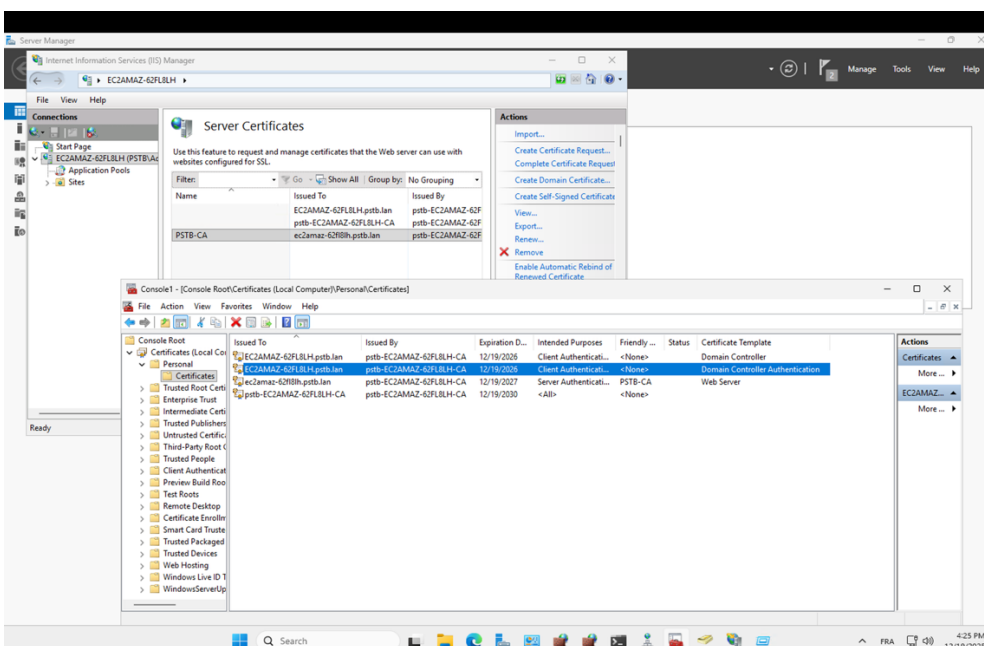
Nous commençons par faire une demande de certificat depuis la console IIS. Le certificat est ensuite disponible depuis la console IIS ou depuis le magasin de certificats.



Demande depuis la console MMC

Tentons maintenant de faire une demande de certificat depuis la console MMC. Ce moyen est assez pratique et facile d'utilisation avec l'assistant.

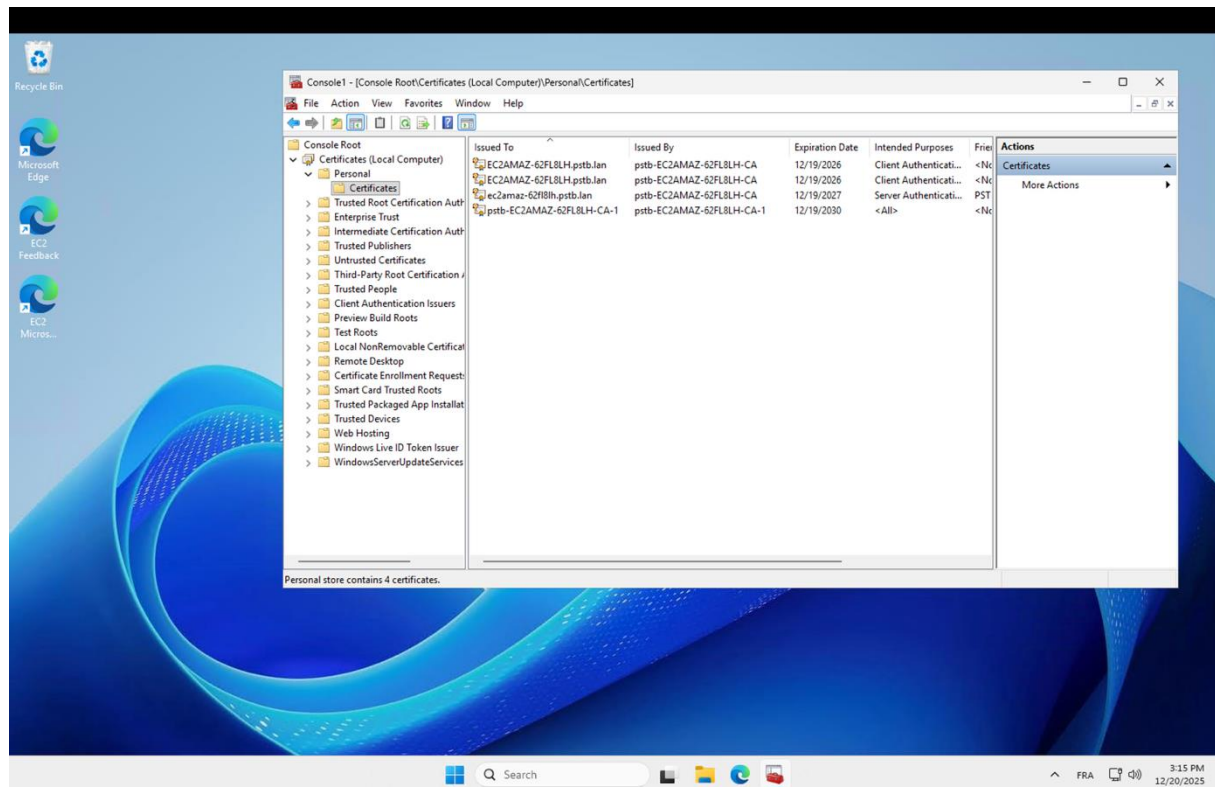
On peut ensuite voir que le certificat apparaît bien dans les certificats disponibles.



Auto enroll

Une GPO Auto-Enrollment a été créée et liée au domaine, permettant aux utilisateurs et ordinateurs membres du domaine de recevoir automatiquement leurs certificats.

Sur un poste client membre du domaine, connecté avec un utilisateur AD, le certificat a été généré automatiquement et est visible dans le magasin de certificats.



Sauvegarde de l'AD CS

Cette dernière étape du consiste à effectuer la sauvegarde de l'Autorité de Certification.

Depuis la console AD CS, nous avons utilisé l'option Tasks → Back Up CA, ce qui permet de sécuriser la base de données de la CA ainsi que la clé privée.

Cette sauvegarde garantit que l'ensemble des certificats délivrés et les paramètres de la CA peuvent être restaurés en cas de problème, assurant la continuité du service.

