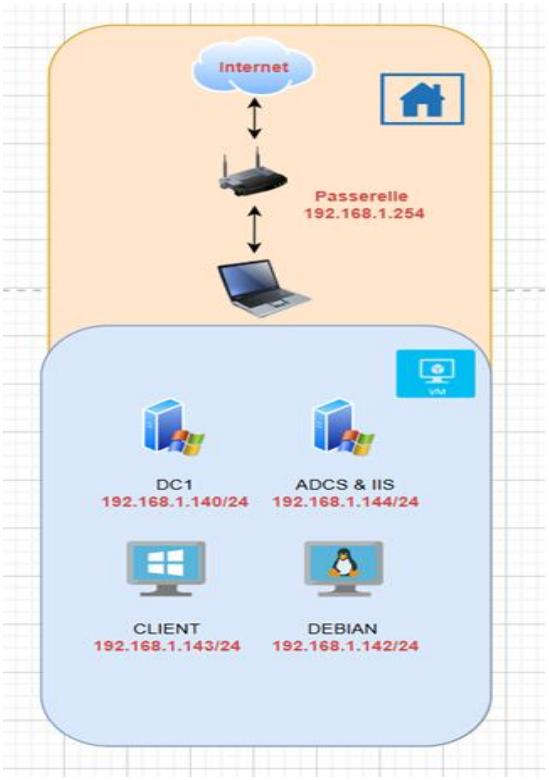
Dans le cadre d'un TP au CEFIM, j'ai mis en place une architecture composé de plusieurs machines virtuelles, dont un serveur central, puis j'ai installé une infrastructure à Clé publique (PKI). Cette PKI gère les certificats numériques, assurant l'authentification sécurisée et le chiffrement des communications au sein de l'architecture, simulant ainsi un environnement sécurisé pour des échanges de données.

Dans ce TP PKI, nous allons démontrer comment mettre en place une PKI sur Windows Server et configurer Easy-RSA sur Debian.

Cette infrastructure contient :

- 1 Windows Server 2019 « DC01 » contrôleur de domaine ais.local
- 1 Windows Server « CA » Autorité de certification d'entreprise + rôle IIS installé et configuré
- 1 Debian 12 « DEBIAN » avec Apache2 installé
- 1 Windows 10 « Client-10 » qui servira de station cliente pour les différents tests

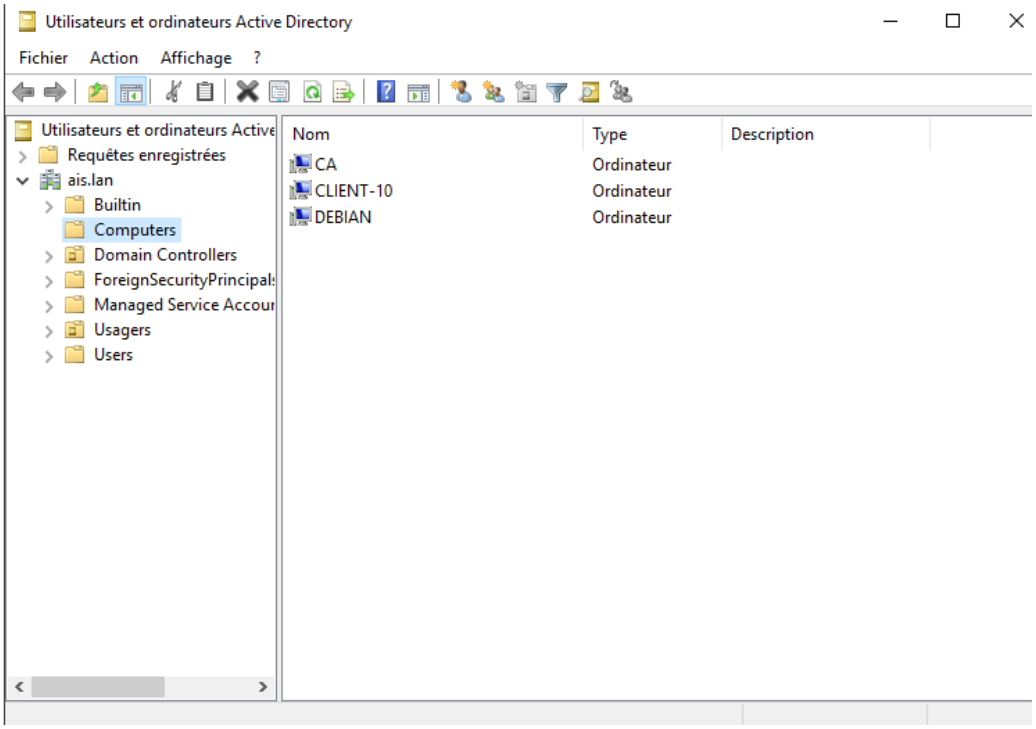
Voici l'infrastructure sous forme de schéma présentant les informations de chaque machine :



Au cours de ce projet, j'ai d'abord installé l'ensemble des machines virtuelles nécessaire, y compris le service Active Directory Certificate services (ADCS) et le rôle Internet Information Services (IIS). Il est recommandé de configurer les rôles dans des serveurs différents mais par soucis de performance de mon ordinateur, j'ai dû mettre les deux rôles dans un même serveur.

Cela est recommandé afin d'isoler les services et renforce la sécurité, d'améliorer les performances et de simplifier la gestion comme déployer des mises à jour plus ciblée.

Pour commencer, j'ai mis dans le domaine, les 3 machines pour avoir une gestion centralisée des utilisateurs et la configuration des ordinateurs et des services.



C'est un peu plus complexe de mettre une machine DEBIAN dans un domaine d'un Windows Serveur mais voici les configurations et les commandes pour intégrer une machine Linux dans le domaine :

Nous mettons bien évidemment les configurations IP pour que notre serveur puisse communiquer avec les autres machines sur le réseau ou Internet.

On modifie dans le fichier /etc/network/interfaces :

Nous modifions aussi le fichier /etc/resolv.conf car nous devons spécifier l'adresse IP de votre Windows Server (qui héberge le contrôleur de domaine) liées à la résolution DNS (Domain Name System).

Une fois que les configurations ont été enregistrés, nous pourrons contacter notre contrôleur de domaine :

apt update

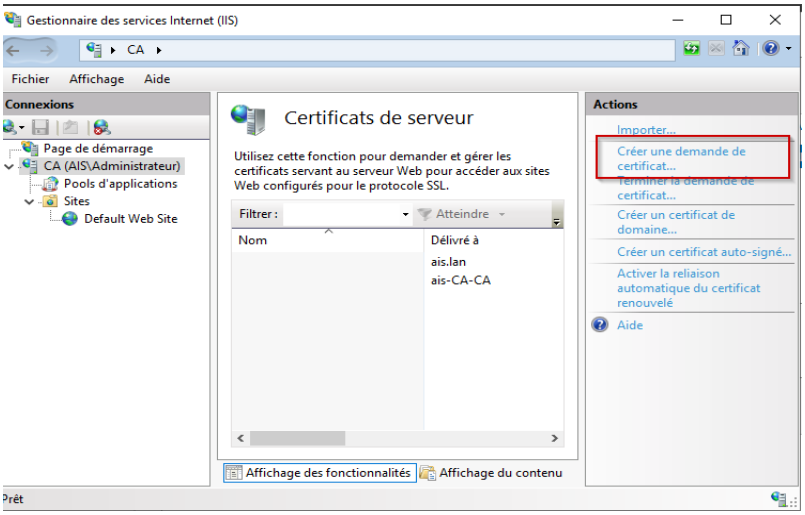
apt install realmd sssd samba adcli krb5-user

realm discover ais.lan

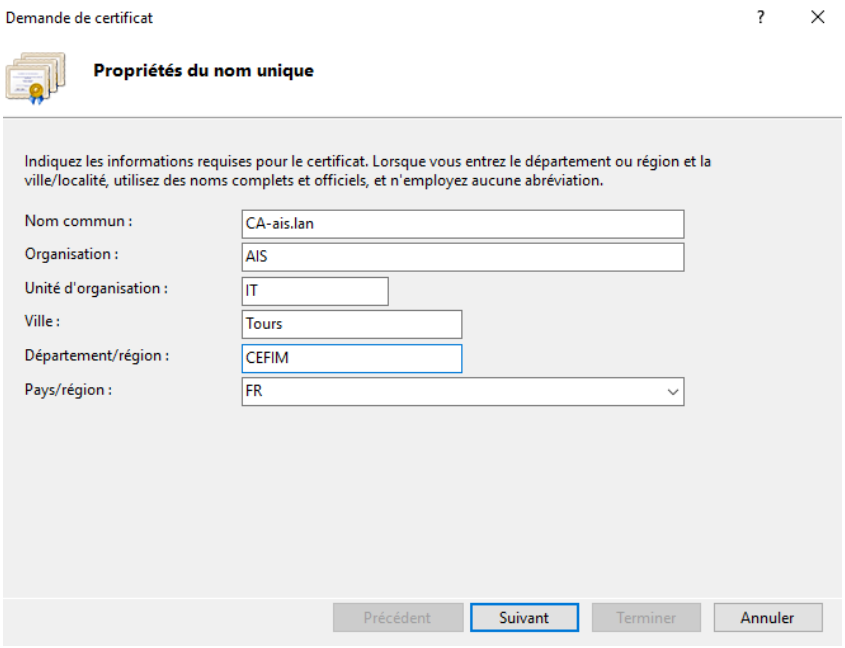
realmjoin —user=Administrateur ais.lan

ADCS : installer un Certificat Webserver dans IIS (PARTIE WINDOWS SERVER)

Dans la console de gestion de IIS, ouvrir la console *Certificat*, faire un clic-droit et sélectionner *Créer une demande de certificat* :



Renseigner les informations suivantes. Sélectionner le paramétrage ci-dessous :

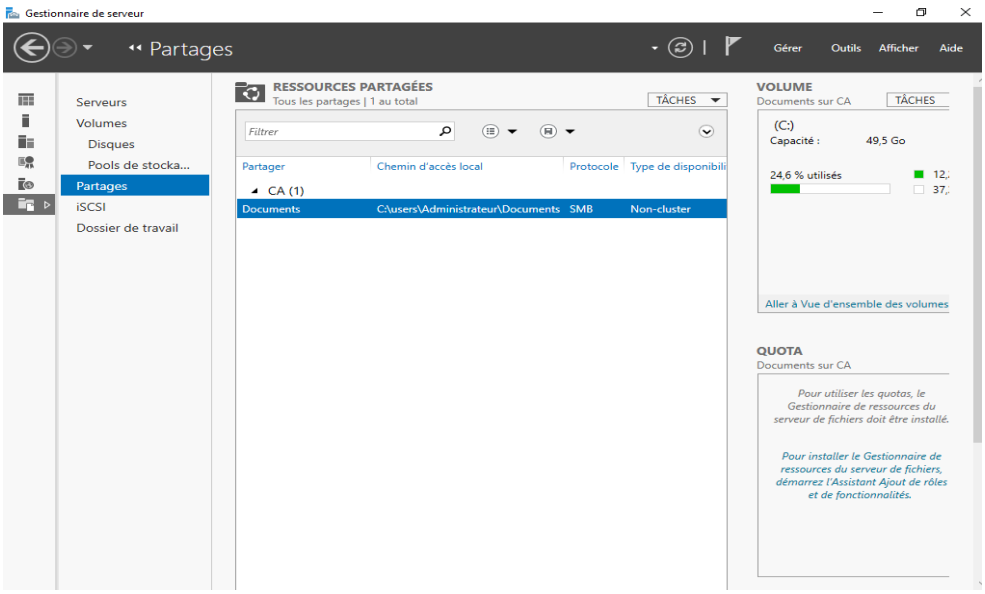


Renseigner le dossier et de nom où se trouvera la requête.

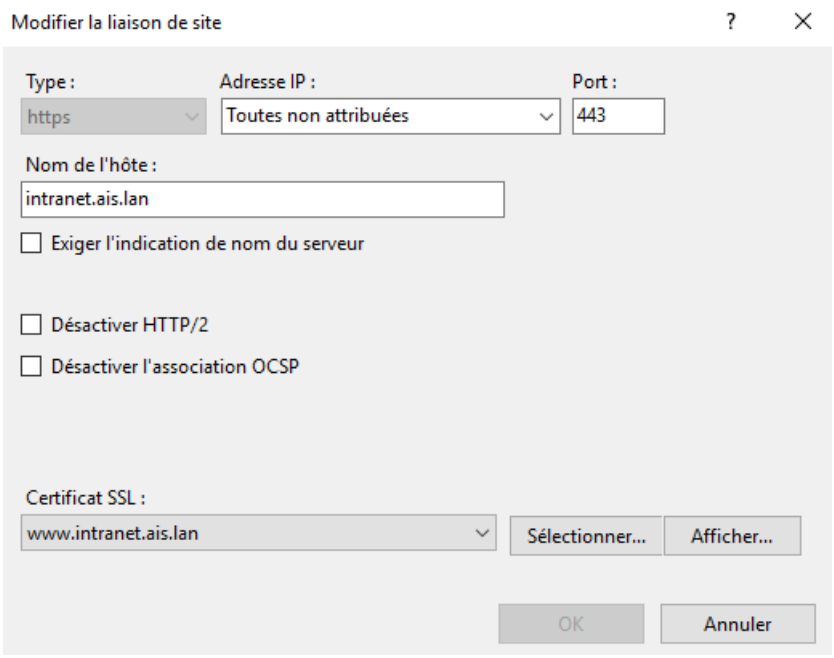
\\CA\Documents

Récupérer la requête via partage réseau (SMB)

On installe le rôle : Service de fichier



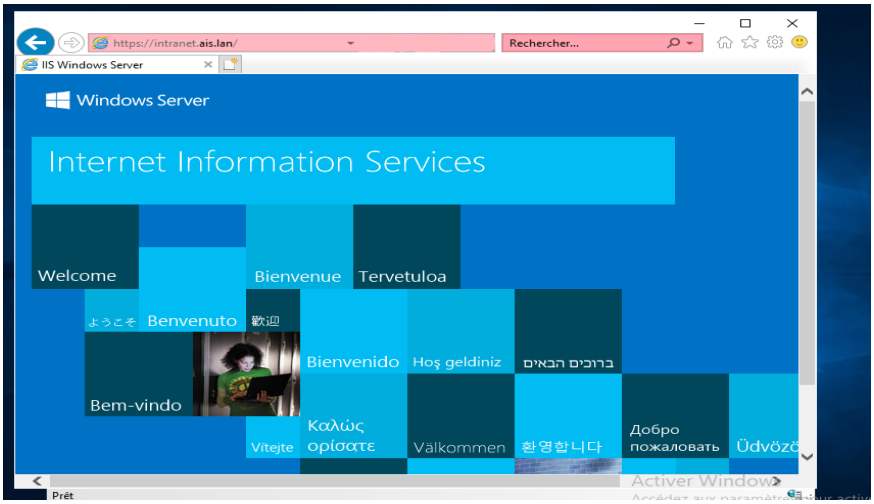
Sur IIS : Ajouter le certificat SSL :



Maintenant, tapez votre nom de domaine dans le navigateur web "Internet Explorer" de votre serveur et cliquez sur le petit cadenas qui s'affiche dans la barre d'adresse.

Comme vous pouvez le voir, votre navigateur n'a pas affiché d'avertissement concernant votre certificat car celui-ci est signé par votre autorité de certification.

Etant donné que le certificat de votre autorité de certification se trouve dans la liste des autorités de confiance de votre serveur, le certificat est considéré comme valide.



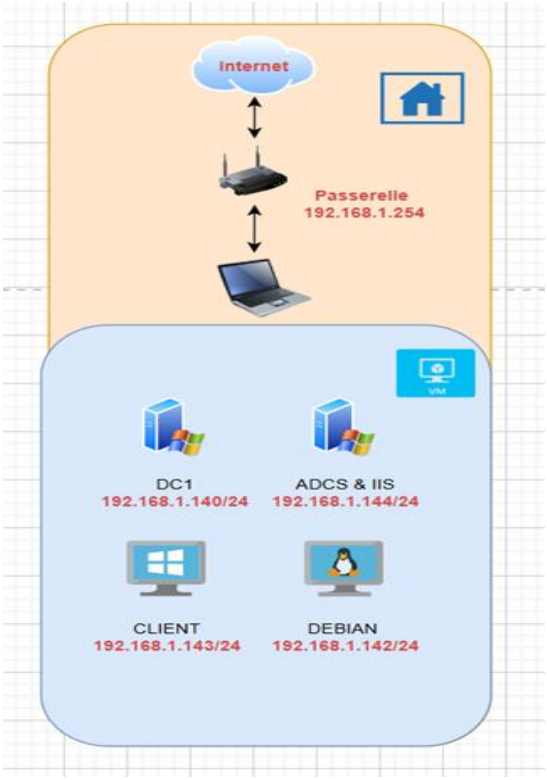
Dans le cadre d’un TP au CEFIM, j’ai mis en place une architecture composé de plusieurs machines virtuelles, dont un serveur central, puis j’ai installé une infrastructure à Clé publique (PKI). Cette PKI gère les certificats numériques, assurant l’authentification sécurisée et le chiffrement des communications au sein de l’architecture, simulant ainsi un environnement sécurisé pour des échanges de données.

Dans ce TP PKI, nous allons démontrer comment mettre en place une PKI sur Windows Server et configurer Easy-RSA sur Debian.

Cette infrastructure contient :

- 1 Windows Server 2019 « DC01 » contrôleur de domaine ais.local
- 1 Windows Server « CA » Autorité de certification d'entreprise + rôle IIS installé et configuré
- 1 Debian 12 « DEBIAN » avec Apache2 installé
- 1 Windows 10 « Client-10 » qui servira de station cliente pour les différents tests

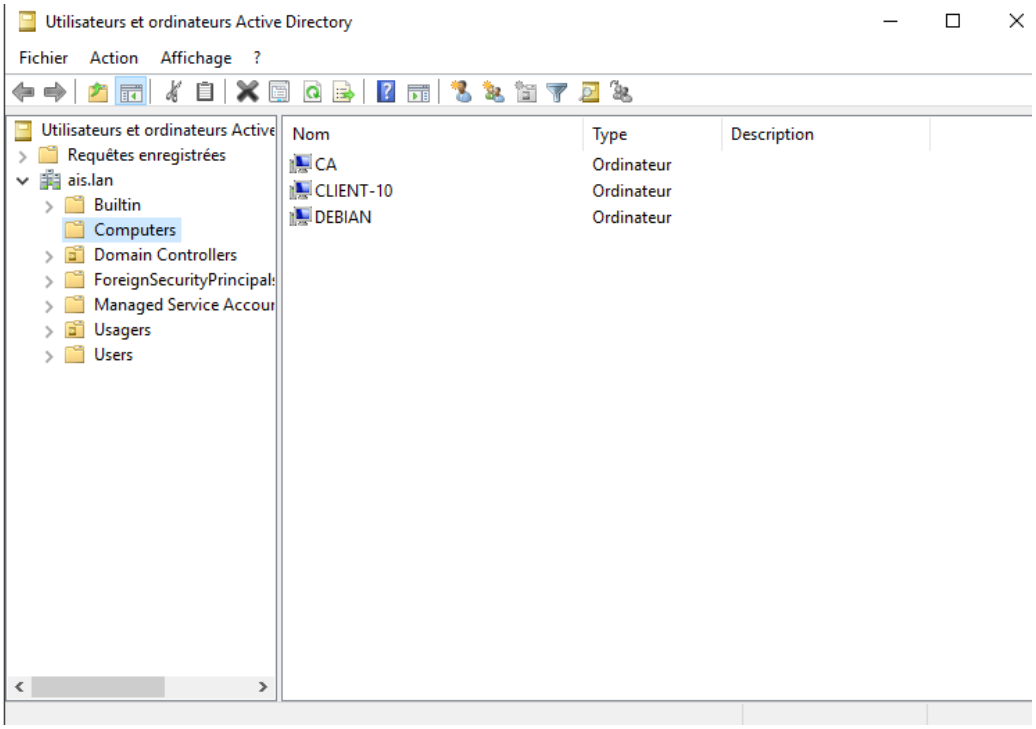
Voici l'infrastructure sous forme de schéma présentant les informations de chaque machine :



Au cours de ce projet, j'ai d'abord installé l'ensemble des machines virtuelles nécessaire, y compris le service Active Directory Certificate services (ADCS) et le rôle Internet Information Services (IIS). Il est recommandé de configurer les rôles dans des serveurs différents mais par soucis de performance de mon ordinateur, j'ai dû mettre les deux rôles dans un même serveur.

Cela est recommandé afin d'isoler les services et renforce la sécurité, d'améliorer les performances et de simplifier la gestion comme déployer des mises à jour plus ciblée.

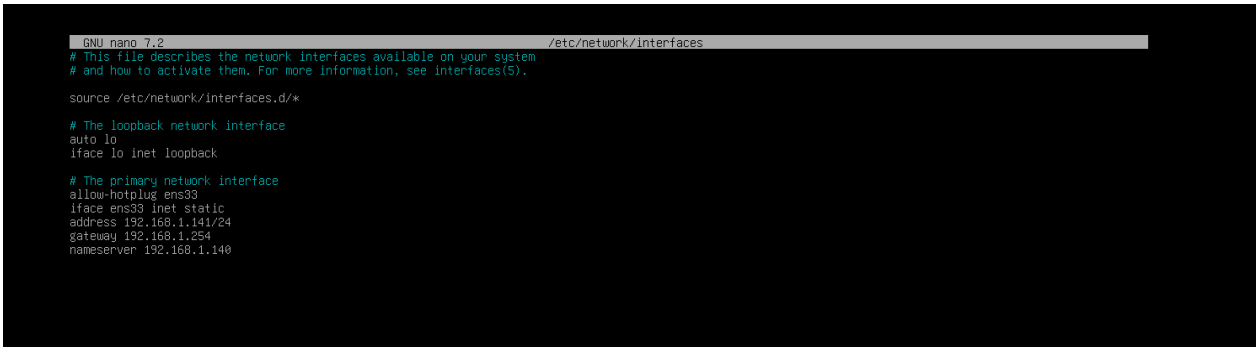
Pour commencer, j'ai mis dans le domaine, les 3 machines pour avoir une gestion centralisée des utilisateurs et la configuration des ordinateurs et des services.



C’est un peu plus complexe de mettre une machine DEBIAN dans un domaine d’un Windows Serveur mais voici les configurations et les commandes pour intégrer une machine Linux dans le domaine :

Nous mettons bien évidemment les configurations IP pour que notre serveur puisse communiquer avec les autres machines sur le réseau ou Internet.

On modifie dans le fichier /etc/network/interfaces :



Nous modifions aussi le fichier /etc/resolv.conf car nous devons spécifier l'adresse IP de votre Windows Server (qui héberge le contrôleur de domaine) liées à la résolution DNS (Domain Name System).

Une fois que les configurations ont été enregistrés, nous pourrons contacter notre contrôleur de domaine :

apt update

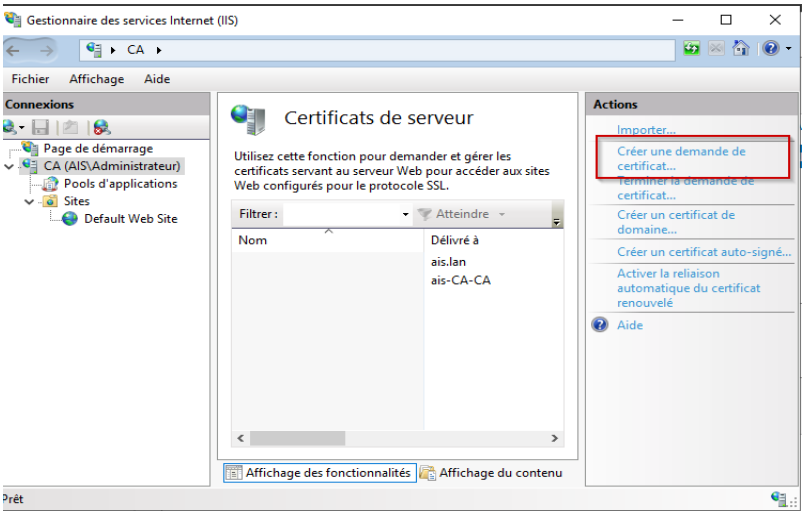
apt install realmd sssd samba adcli krb5-user

realm discover ais.lan

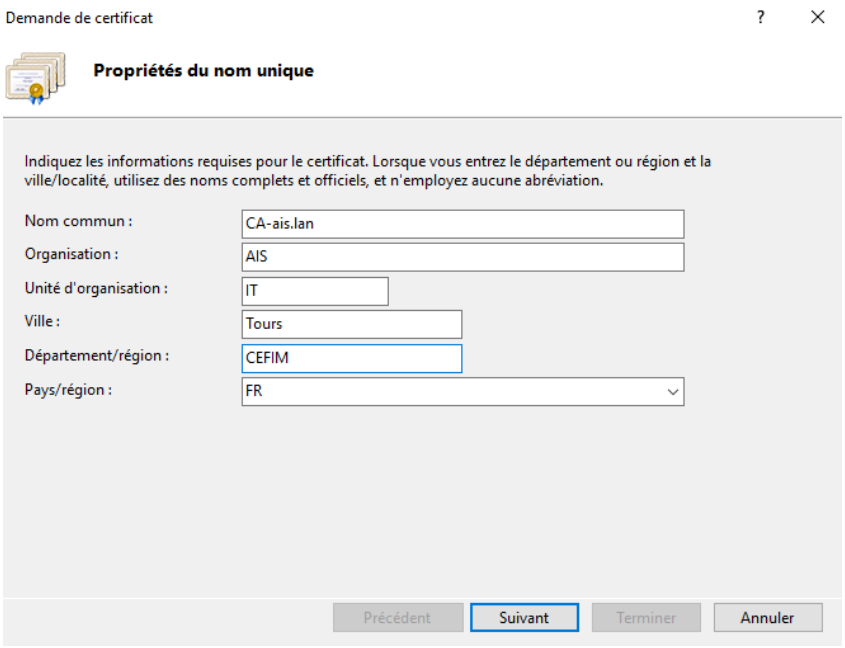
realmjoin —user=Administrateur ais.lan

ADCS : installer un Certificat Webserver dans IIS (PARTIE WINDOWS SERVER)

Dans la console de gestion de IIS, ouvrir la console *Certificat*, faire un clic-droit et sélectionner *Créer une demande de certificat* :



Renseigner les informations suivantes. Sélectionner le paramétrage ci-dessous :

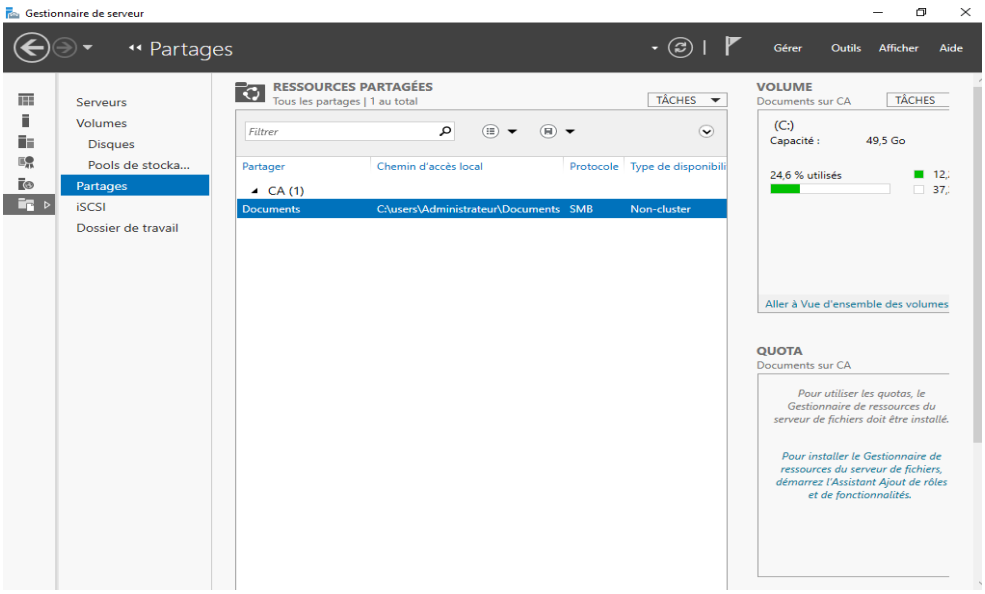


Renseigner le dossier et de nom où se trouvera la requête.

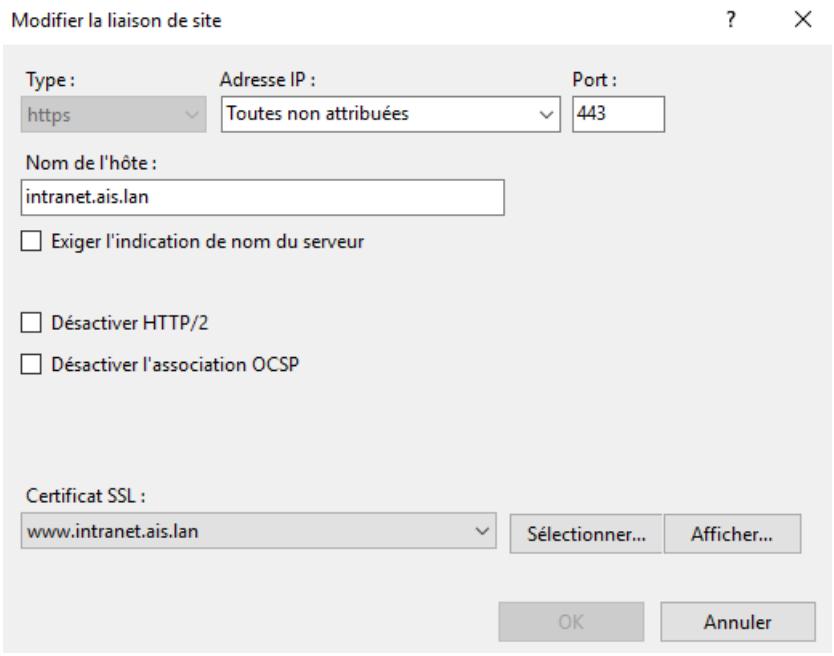
\\CA\Documents

Récupérer la requête via partage réseau (SMB)

On installe le rôle : Service de fichier



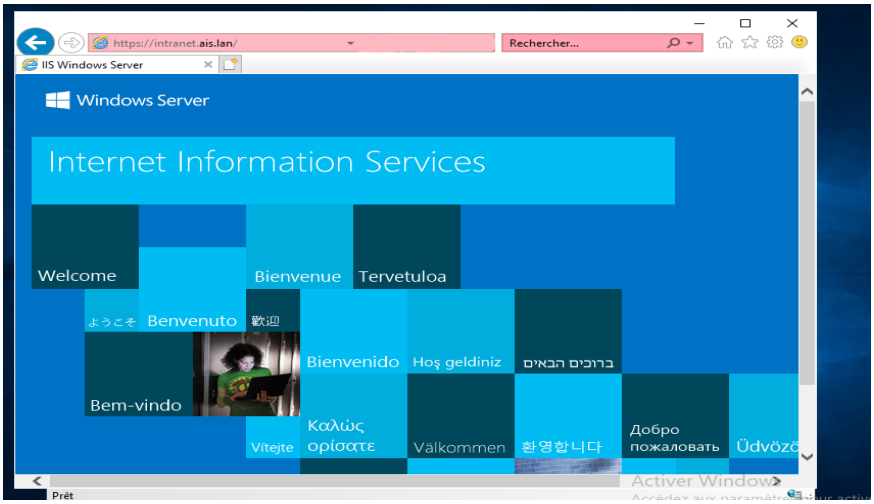
Sur IIS : Ajouter le certificat SSL :



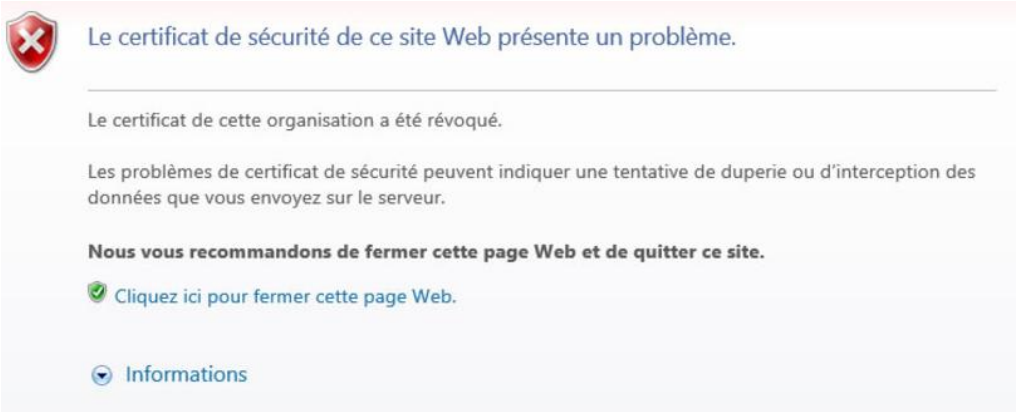
Maintenant, tapez votre nom de domaine dans le navigateur web "Internet Explorer" de votre serveur et cliquez sur le petit cadenas qui s'affiche dans la barre d'adresse.

Comme vous pouvez le voir, votre navigateur n'a pas affiché d'avertissement concernant votre certificat car celui-ci est signé par votre autorité de certification.

Etant donné que le certificat de votre autorité de certification se trouve dans la liste des autorités de confiance de votre serveur, le certificat est considéré comme valide.



Si vous avez ce message d'erreur lorsque vous essayez de voir le certificat :

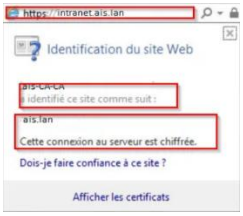


Vide le cache de CRL (les listes de révocations de certificats) du disque dur :

```
certutil -URLCache CRL –delete
```

Invalide l'utilisation des CRL en cache dans la mémoire et sur le disque dur :

```
certutil –setreg chain\ChainCacheResyncFiletime @now
```



Notre autorité de certification est maintenant configurée et prête à agir en tant que racine de confiance pour tous les systèmes que vous souhaitez configurer pour l'utiliser. Vous pouvez ajouter le certificat de l'autorité de certification à vos serveurs OpenVPN, serveurs Web, messagerie, etc. Tout utilisateur ou serveur qui doit vérifier l'identité d'un autre utilisateur ou serveur de votre réseau doit avoir une copie du fichier ca.crt importé dans le magasin de certificats de son système d'exploitation.