TP MULTI SITE

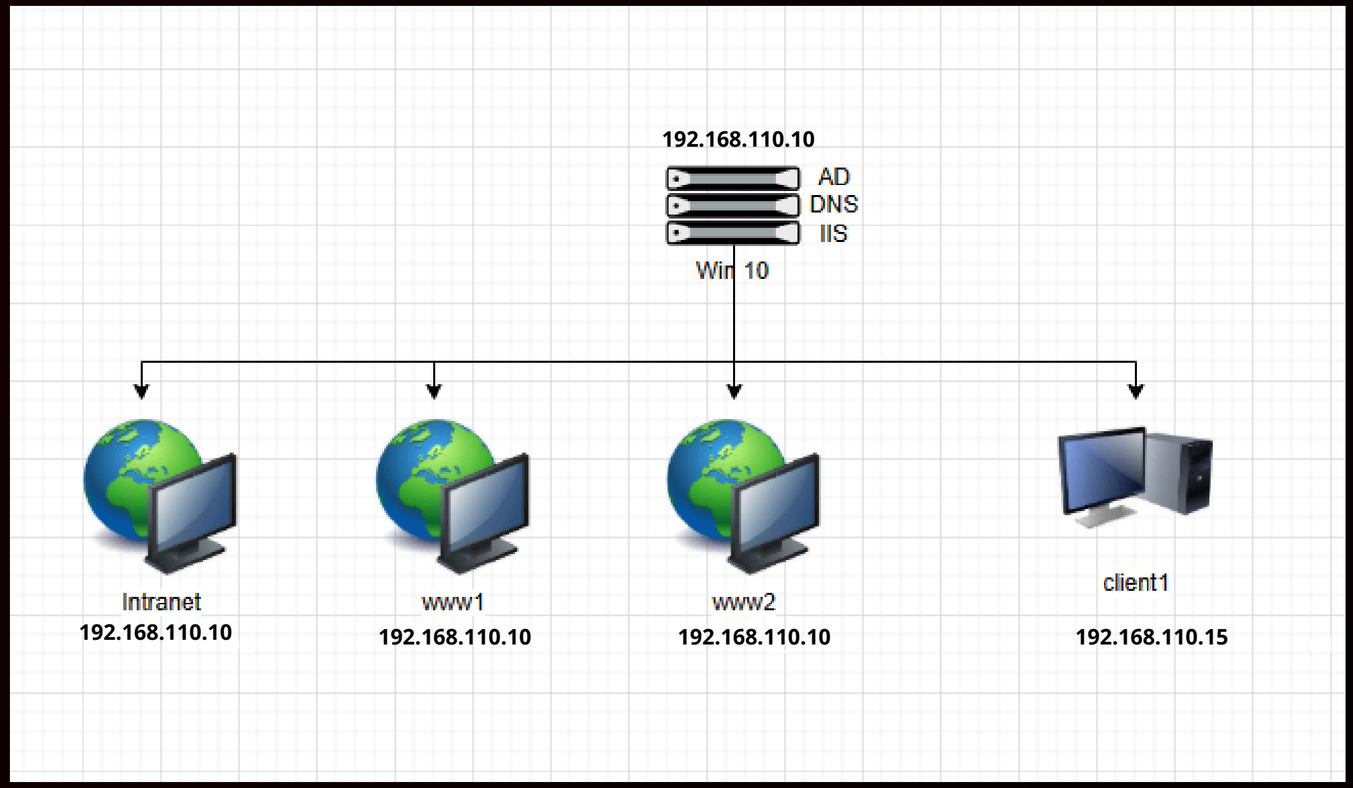
MISE EN PLACE D'UNE ARCHITECTURE MULTI-SERVEURS
WEB ET DNS SOUS WINDOWS SERVER

LUCA BONA

SOMMAIRE

LUCA BONA

SCHEMA

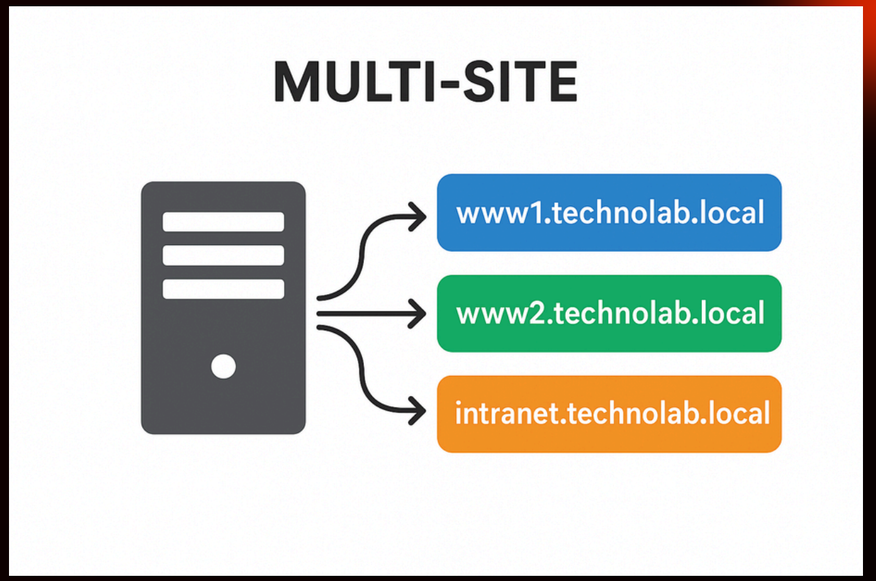

192.168.110.10
AD
DNS
IIS
Win 10
Intranet
192.168.110.10
www1
192.168.110.10
www2
192.168.110.10
client1
192.168.110.15

LE BUT

Le but du multi-site est de rendre plus claire et organisé notre infrastructure. Par exemple on peut separer les environnements (site test / intranet / production, renforcer la sécurité (https, authentification) mais aussi simplifier l'accés pour les utilisateurs qui n'ont pas besoin de retenir les adresses IP

Pour faire simple : Le multi-site permet d'héberger plusieurs sites web distincts sur un même serveur ou sur plusieurs serveurs, chacun accessible avec son propre nom DNS (ex. www1.technolab.local, www2.technolab.local, intranet.technolab.local).

LES IP :
Windows Server : 192/168.110.10/24
Client Windows : 192.168.110.15/24

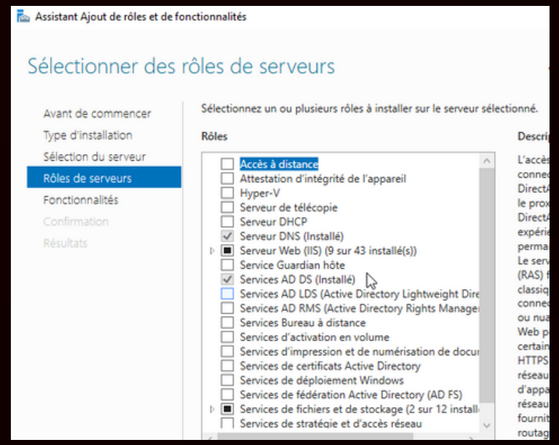


Pour mieux comprendre qu'est ce qu'un DNS, car ce tp tourne du DNS : voici une production expliquant qu'est ce que le DNS :

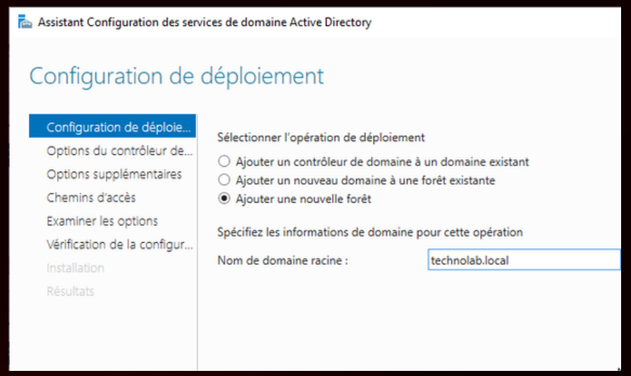
TP_DNS

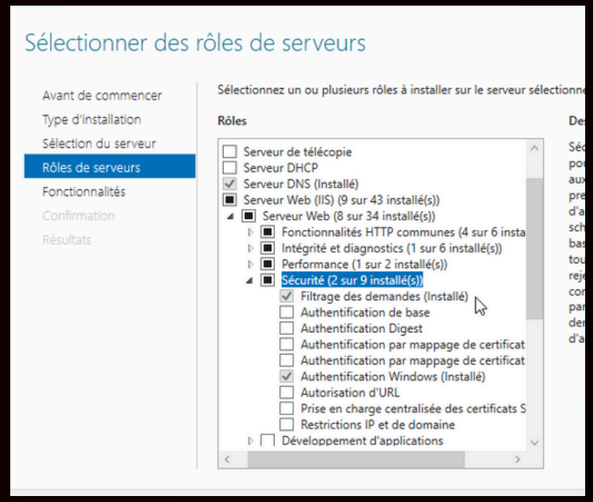
ACTIVE DIRECTORY

Pour commencer, je vais installer toutes les options dont j'aurai besoin, c'est-à-dire l'AD, le DNS et le serveur web IIS.



J'ajoute mon domain



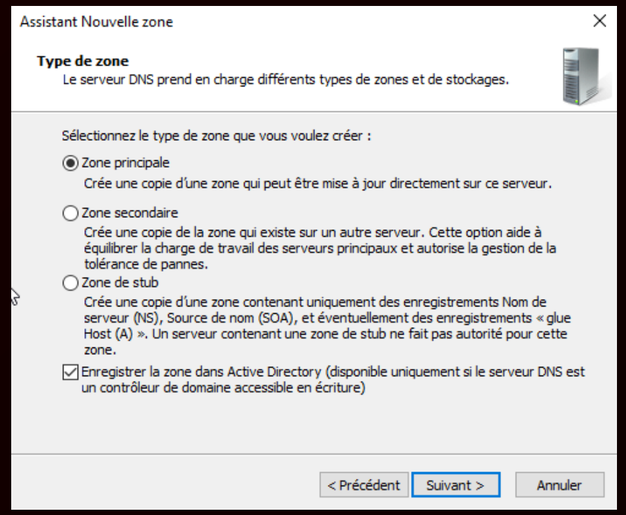


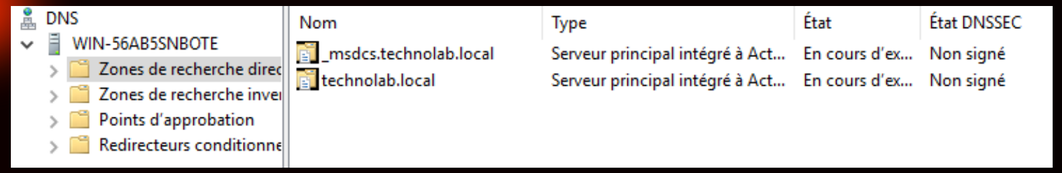
Ensuite, il faut installer "Authentification Windows". Cela servira à créer un site avec accès contrôlé : seules les personnes possédant un identifiant valide pourront y accéder.

LUCA BONA

DNS

Il faut créer une nouvelle zone DNS.

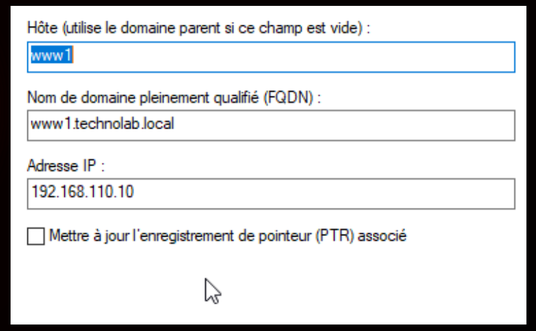




Ensuite, faites un clic droit sur “technolab.local” pour créer votre hôte “A ou AAAA”.

Vérification de la liaison entre le serveur Windows et le client Windows.

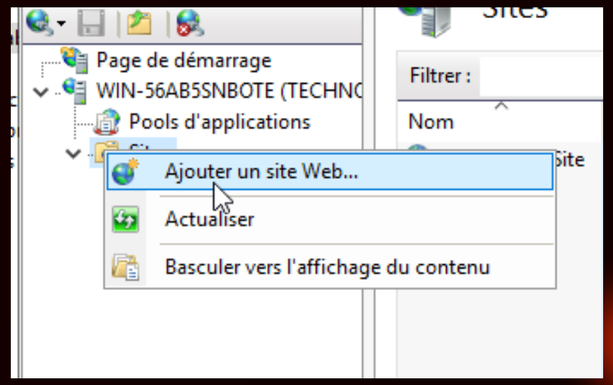
```
C:\Users\sio>ping technolab.local

Envoi d'une requête 'ping' sur technolab.local [192.168.110.10] avec 32 octets de données :
Réponse de 192.168.110.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.110.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.110.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.110.10 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.110.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```



SERVER IIS

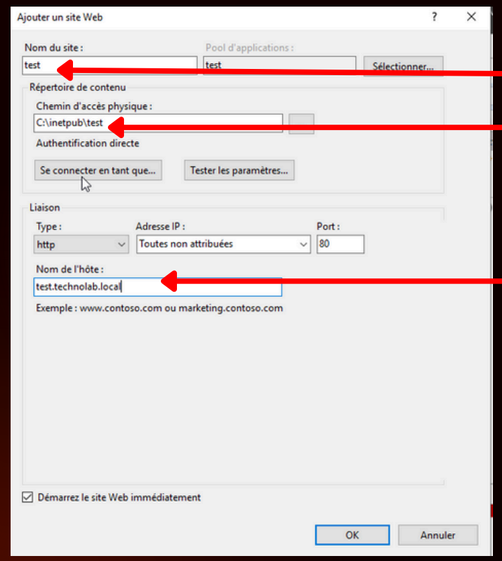
01

Depuis votre Gestionnaire de serveur, rendez-vous dans le Gestionnaire des services Internet (IIS), puis ajoutez un site web.



02

Enfin, finalisez la création de votre site web. Pour le chemin d'accès, rendez-vous dans C:\inetpub puis créez un dossier portant le nom de votre site.



Nom du site local

Lien d'acces physique(repertoir du site)

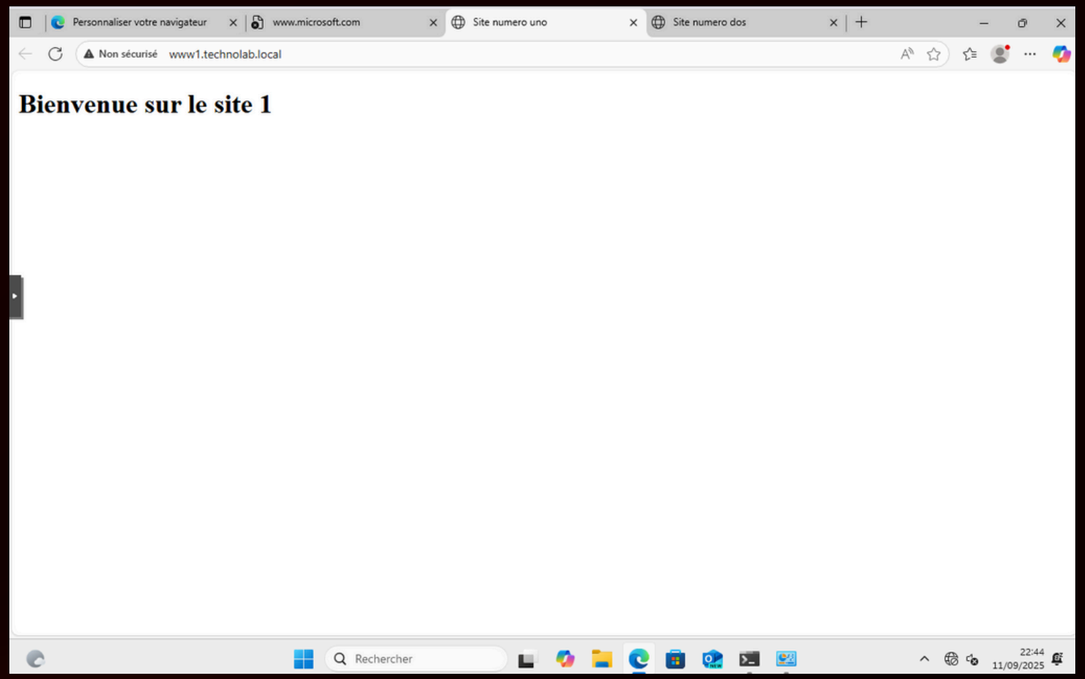
URL

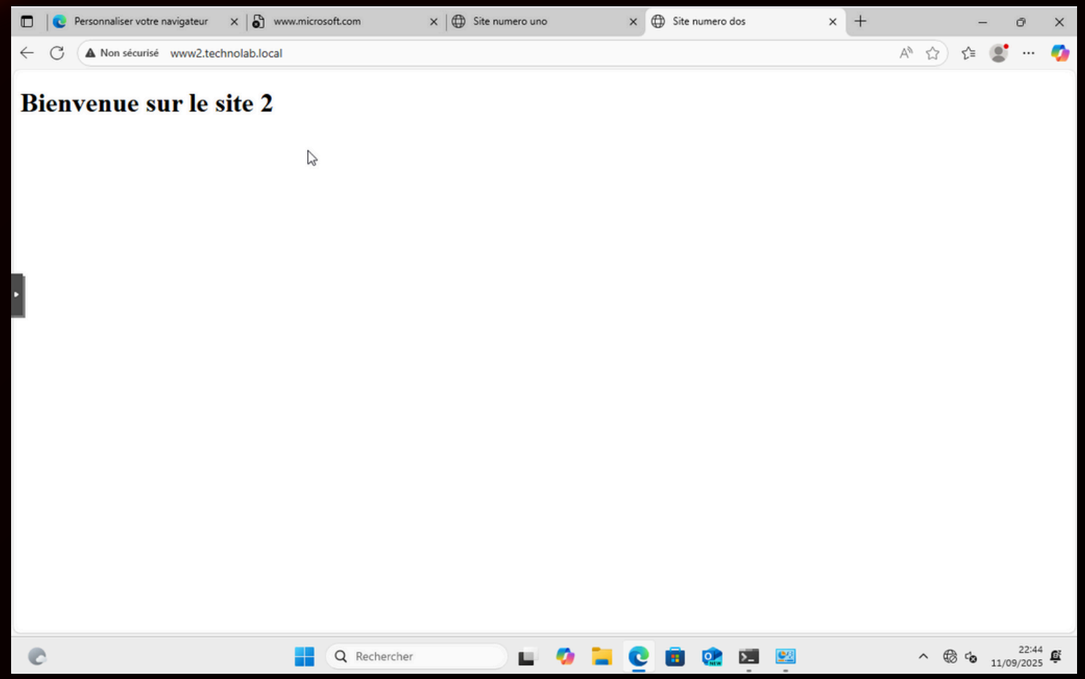
03

Personellement j'ai creé le site 1 et site 2

Ceci est une demonstration

En ajoutant un fichier HTML dans le dossier physique du site, vous pourrez avoir une interface lors de la connexion aux différents sites.

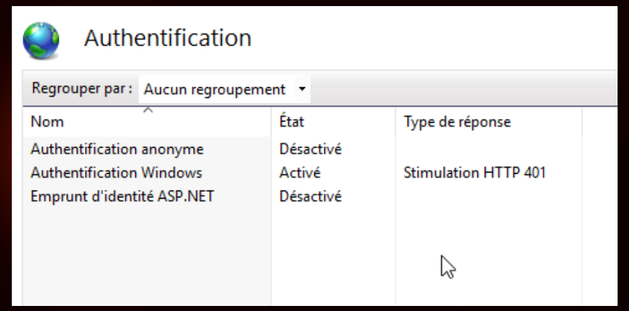




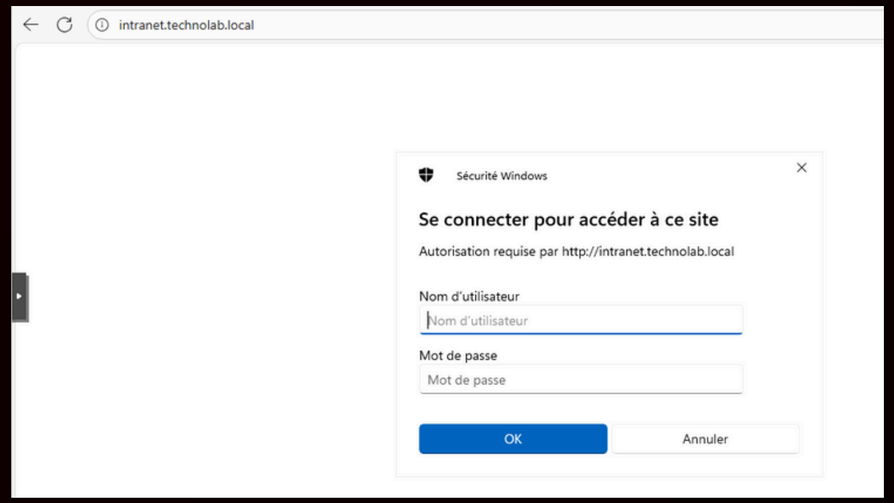
AUTHENTIFICATION

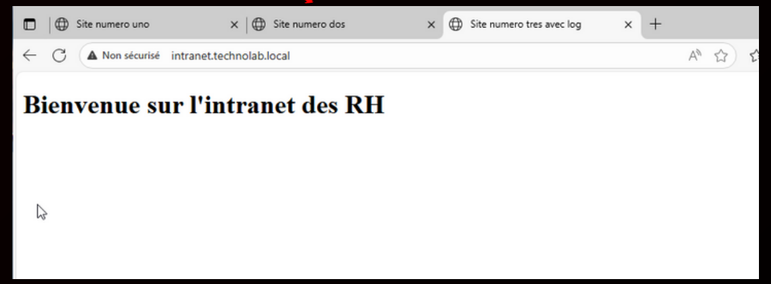
En créant le nouveau site “Intranet”, après avoir installé l’authentification Windows et créé mon utilisateur sio2025 pour se connecter au site, il ne me reste plus qu’à vous montrer comment procéder.

Sur la page d’accueil d’IIS, en cliquant sur votre site “Intranet”, vous verrez dans le tableau de bord l’option “Authentification”. Une fois dessus, désactivez l’authentification anonyme et activez l’authentification Windows.



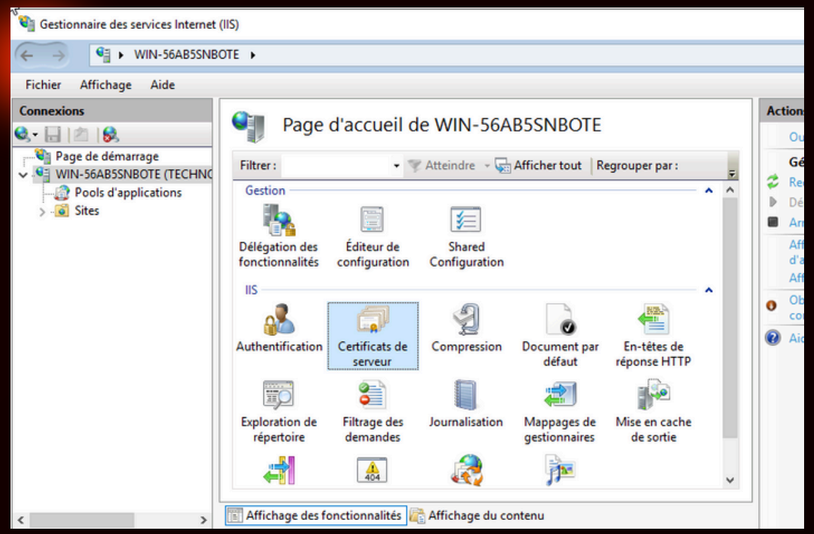
En se connectant au site, il demande bien un accès. Pour pouvoir consulter le site, il faut que l’utilisateur appartienne au domaine et dispose des bons droits, sinon il ne pourra pas y accéder.





SÉCURISATION SSL

01

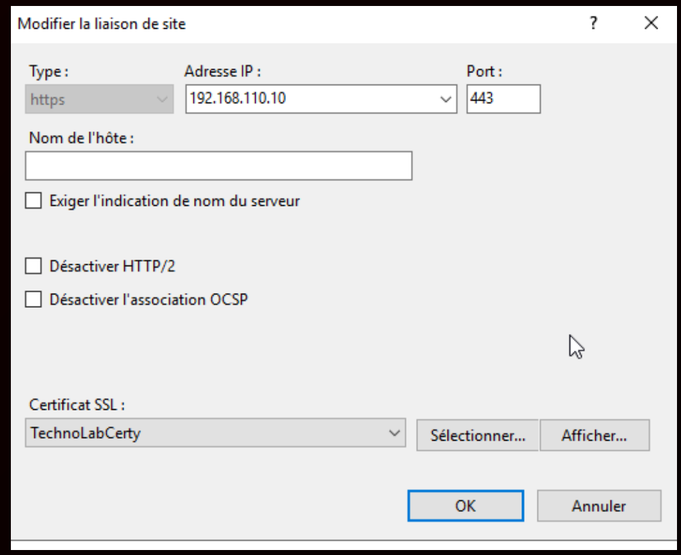


Rendez-vous dans l'onglet de votre serveur, puis cliquez sur **Certificats de serveur.**

02

Créez votre certificat auto-signé.

03



Une fois votre certificat généré, rendez-vous sur le site web que vous souhaitez sécuriser, faites un clic droit dessus, puis Modifier les liaisons.
Ajoutez une liaison en HTTPS et n'oubliez pas de sélectionner votre certificat SSL.

04

CONCLUSION

La mise en place d'un DNS interne rend l'utilisation du réseau beaucoup plus simple, car les utilisateurs n'ont plus besoin de retenir des adresses IP compliquées. Ils peuvent accéder aux sites avec des noms clairs comme www1.technolab.local.

L'utilisation de plusieurs serveurs permet aussi de mieux organiser les services de l'entreprise. Chaque serveur a un rôle précis, ce qui évite les conflits, limite les surcharges et facilite la gestion au quotidien.

Enfin, l'ajout de l'authentification et du chiffrement (HTTPS) rend l'accès aux sites plus sûr. Cela garantit que seuls les collaborateurs autorisés peuvent consulter certains services et que les échanges sont protégés. Cette architecture constitue donc une base solide pour une future mise en production.