TP - Authentification SSO Windows

Table des matières

Le SSO, ou authentification unique (Single Sign-On), est une technologie qui permet à un utilisateur de s'authentifier une seule fois pour accéder à plusieurs applications, services ou systèmes sans avoir à se reconnecter à chaque fois

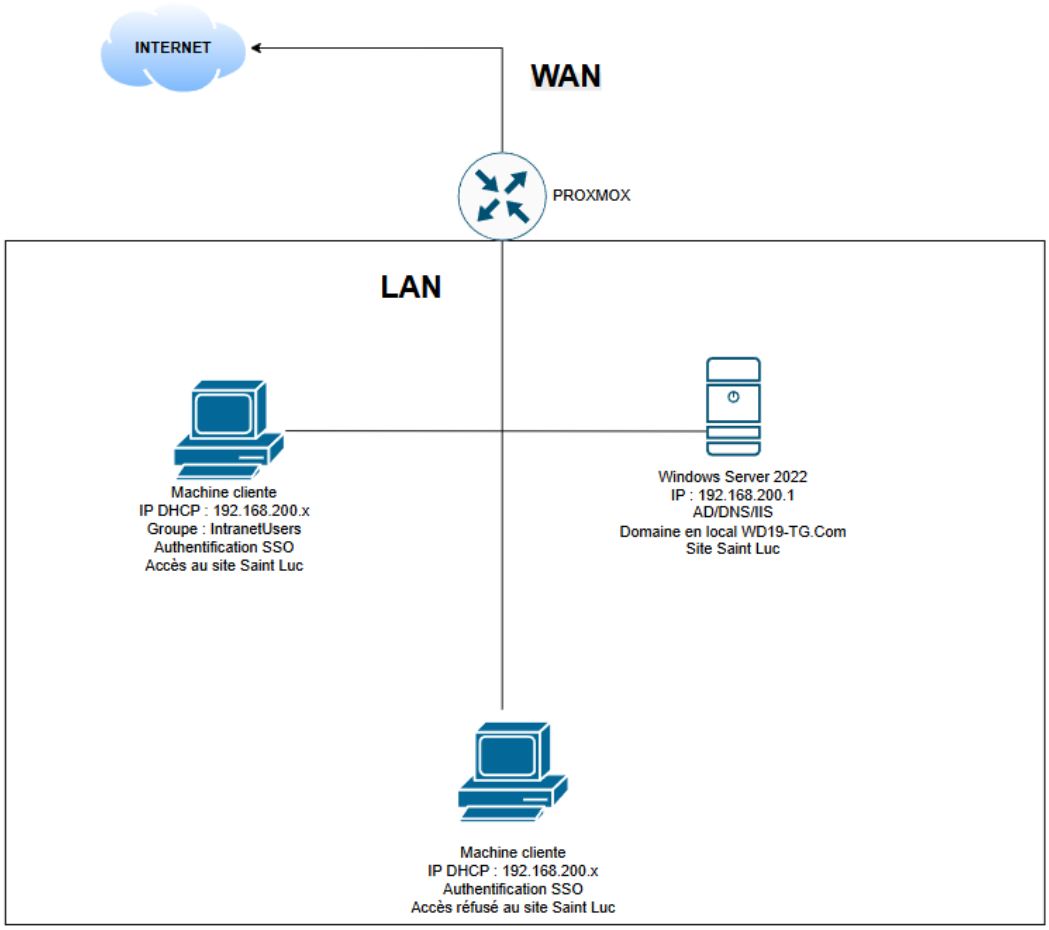
Prérequis :

- Un Windows server 2022
- Un domaine
- Un active directory et un DNS

Voir TP : AD DNS Windows Server-Thomas GRZESINSKI

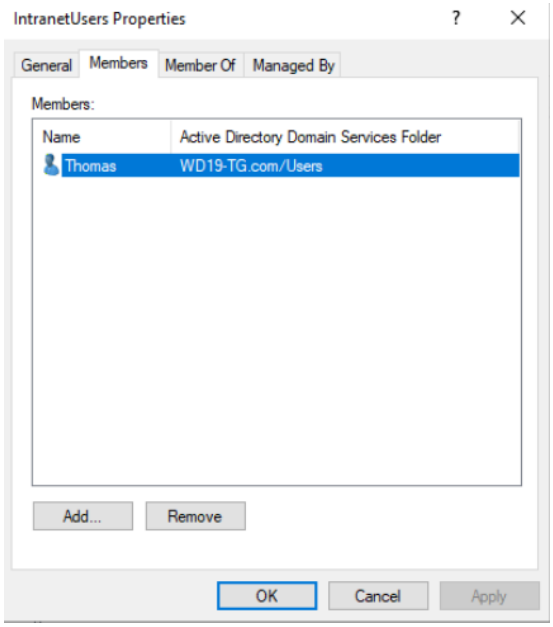
Contexte : Votre entreprise possède un domaine Active Directory. Vous devez créer un site intranet interne, qui ne soit accessible qu'aux employés connectés au domaine Windows, sans saisir à nouveau de mot de passe.

Schéma réseau :

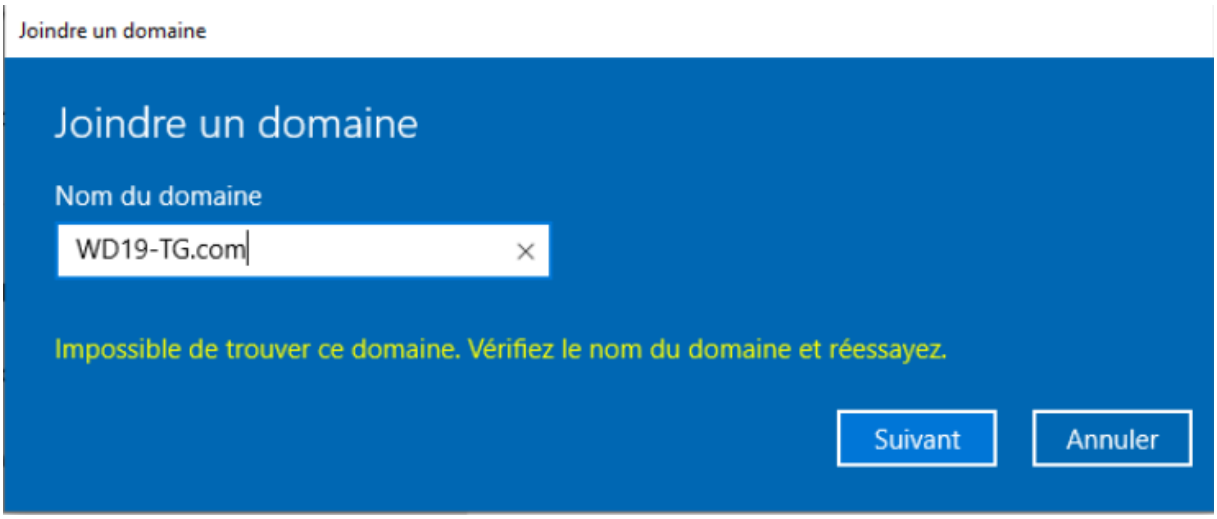


Etape 1 - Préparation Active directory :

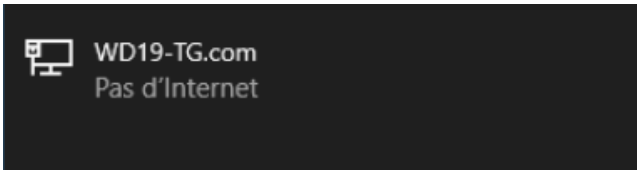
- Créer un utilisateur dans l'AD et un groupe IntranetUsers
- Ajouter votre utilisateur au groupe



- Pour ajouter votre machine cliente au domaine, vous devriez aller dans système -> Comptes -> Accès pro ou scolaire
  - Ajouter un active directory

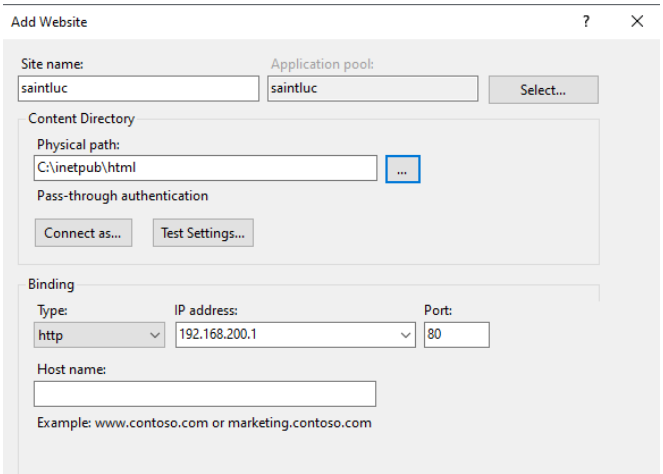


- Vous êtes enfin raccordé au domaine

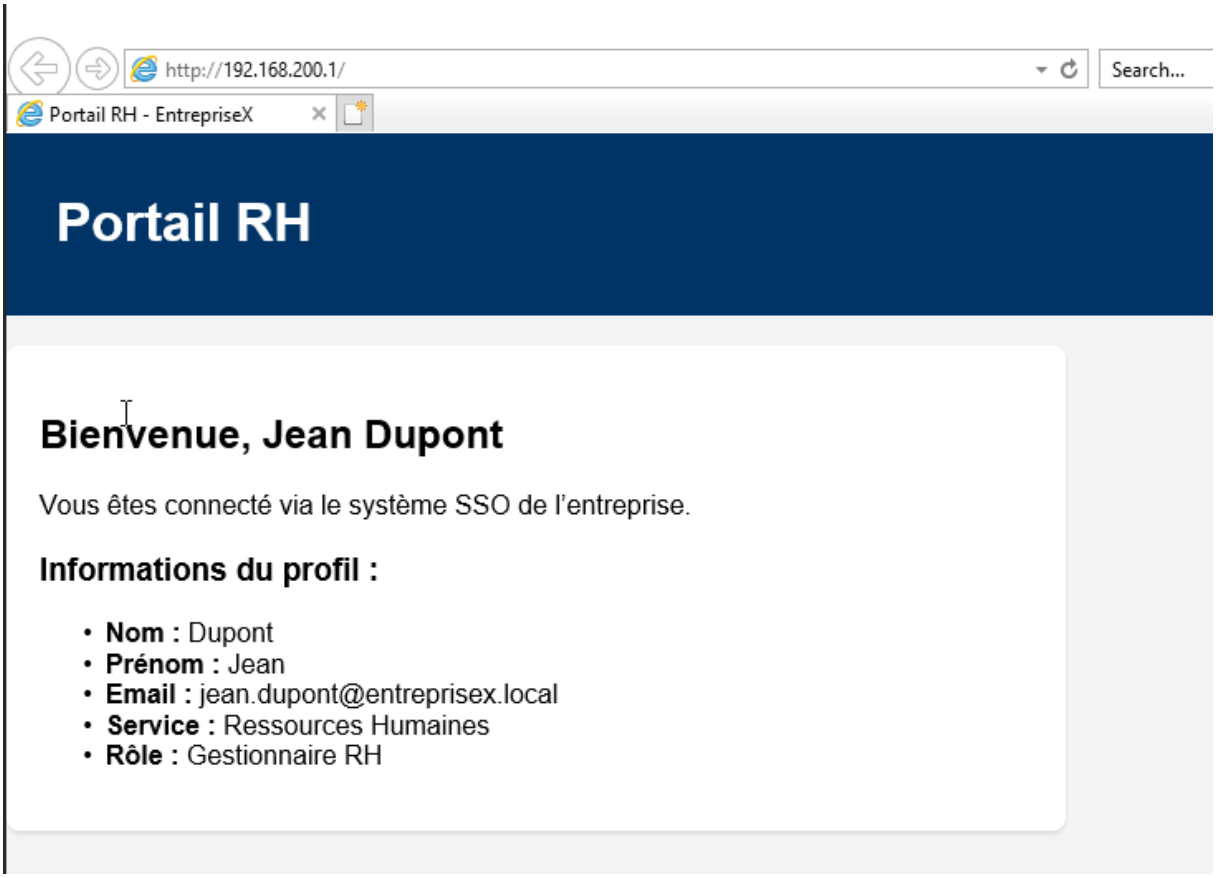


Etape 2 - Serveur IIS :

- Créer un dossier ISS dans le dossier C
- Maintenant il vous faudra installer le services IIS dans le gestionnaire du Windows serveur.
- Lancer le service
- Un site par défaut est déjà configuré sur le serveur
- Créer un deuxième site par défaut
- Pour ajouter un nouveau serveur web faites un clic droit sur « Sites » et ensuite faites ajouté site

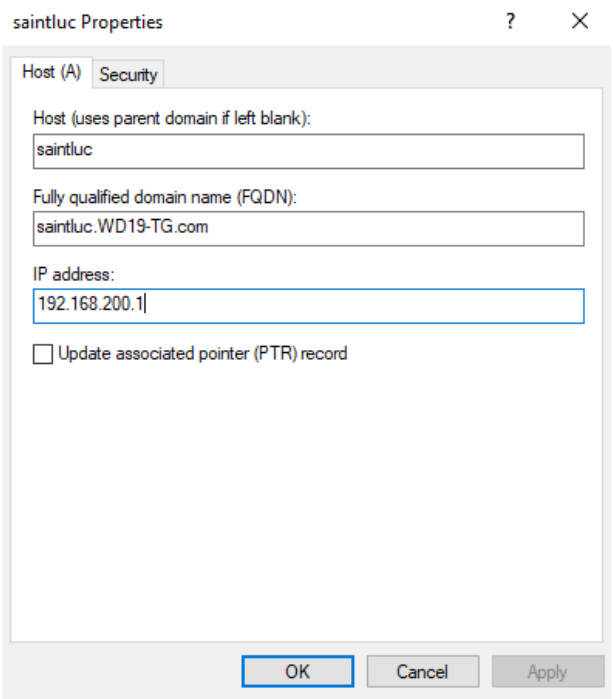


- Lancer le site web pour faire un test



Nous allons maintenant mettre en place une redirection DNS pour notre site internet, ceci permettra aux utilisateurs d'accéder directement au site internet par un nom de domaine et nom une adresse IP.

- Lancer le service DNS
- Ajouter un alias



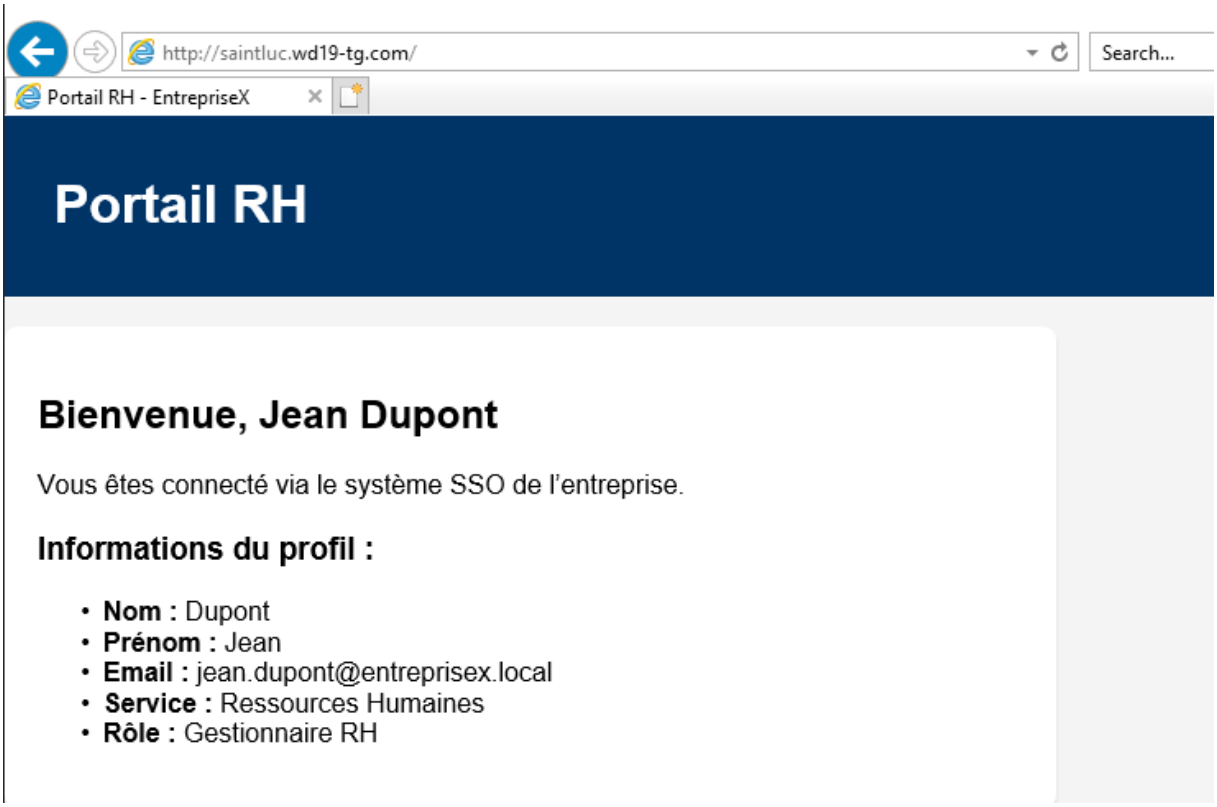
- Vérification :

```
C:\Users\Administrator>ping saintluc.WD19-TG.com

Pinging saintluc.WD19-TG.com [192.168.200.1] with 32 bytes of data:
Reply from 192.168.200.1: bytes=32 time<1ms TTL=128
Reply from 192.168.200.1: bytes=32 time<1ms TTL=128
Reply from 192.168.200.1: bytes=32 time<1ms TTL=128
Reply from 192.168.200.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.200.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

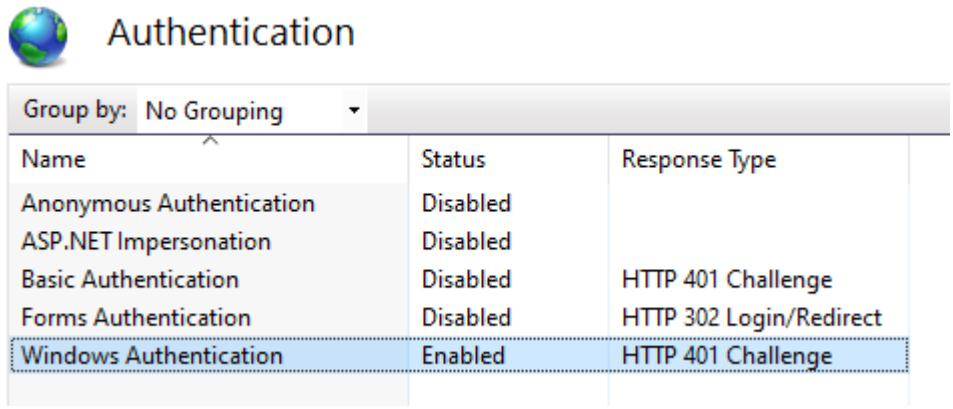
- Sur un navigateur internet entre le DNS pour vérifier son fonctionnement



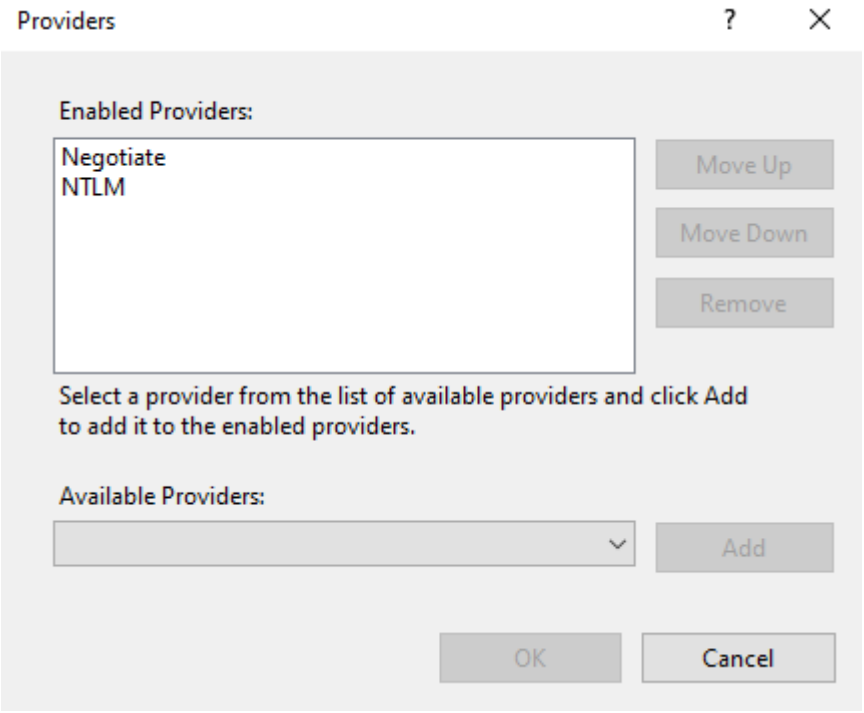
Etape 3 - Configurer l'authentification Windows :

- Sur votre site web dans votre IIS
- Aller dans autorisation

- Désactiver l'authentification anonyme et activer l'authentification Windows

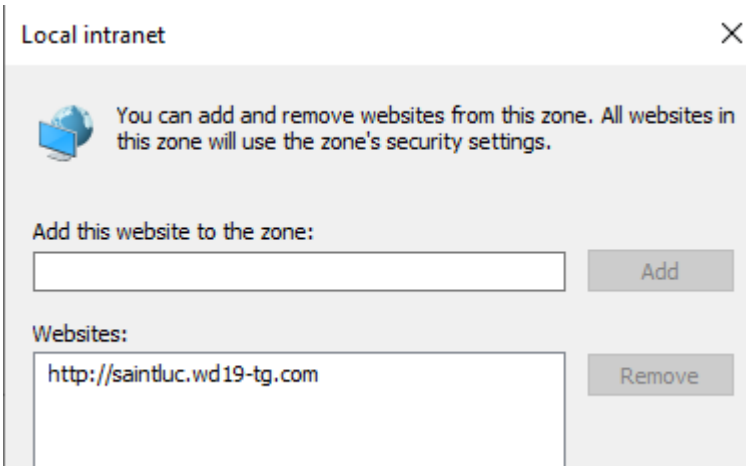


- Maintenant sur l'onglet "providers" à droite de Windows Authentification assurez-vous que ceci est configuré dans le bon ordre :

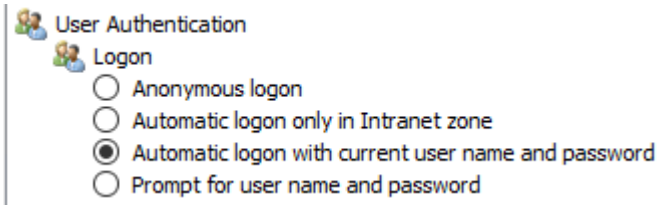


- Ensuite il vous faudra aller dans les options de vos options Internet
- Aller dans sécurité
- Local intranet

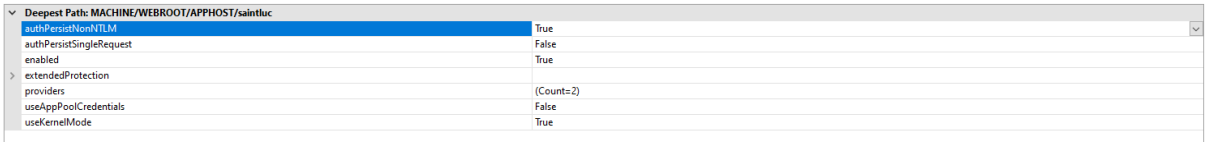
- Dans sites ajouté votre site internet



- Ensuite dans personnalisé choisissez la connexion automatique de l'utilisateur et de son mot de passe par session Windows



- Ensuite retourner sur votre site internet dans la config IIS et aller dans
- Configuration Editor
- Aller dans le chemin system.webServer/security/authentication/windowsAuthentication
- Activer le mode Kernel



Maintenant dans une invite de commande enregistrer a nouveau le nom d'hote et le http de votre site internet avec ses commandes :

```
C:\Users\Administrator>setspn -a http/saintluc.WD19-TG.com WDS2019-ThomasG
Checking domain DC=WD19-TG,DC=com

Registering ServicePrincipalNames for CN=WDS2019-THOMASG,OU=Domain Controllers,DC=WD19-TG,DC=com
        http/saintluc.WD19-TG.com
Updated object

C:\Users\Administrator>setspn -a HOST/saintluc.WD19-TG.com WDS2019-ThomasG
Checking domain DC=WD19-TG,DC=com

Registering ServicePrincipalNames for CN=WDS2019-THOMASG,OU=Domain Controllers,DC=WD19-TG,DC=com
        HOST/saintluc.WD19-TG.com
Updated object
```

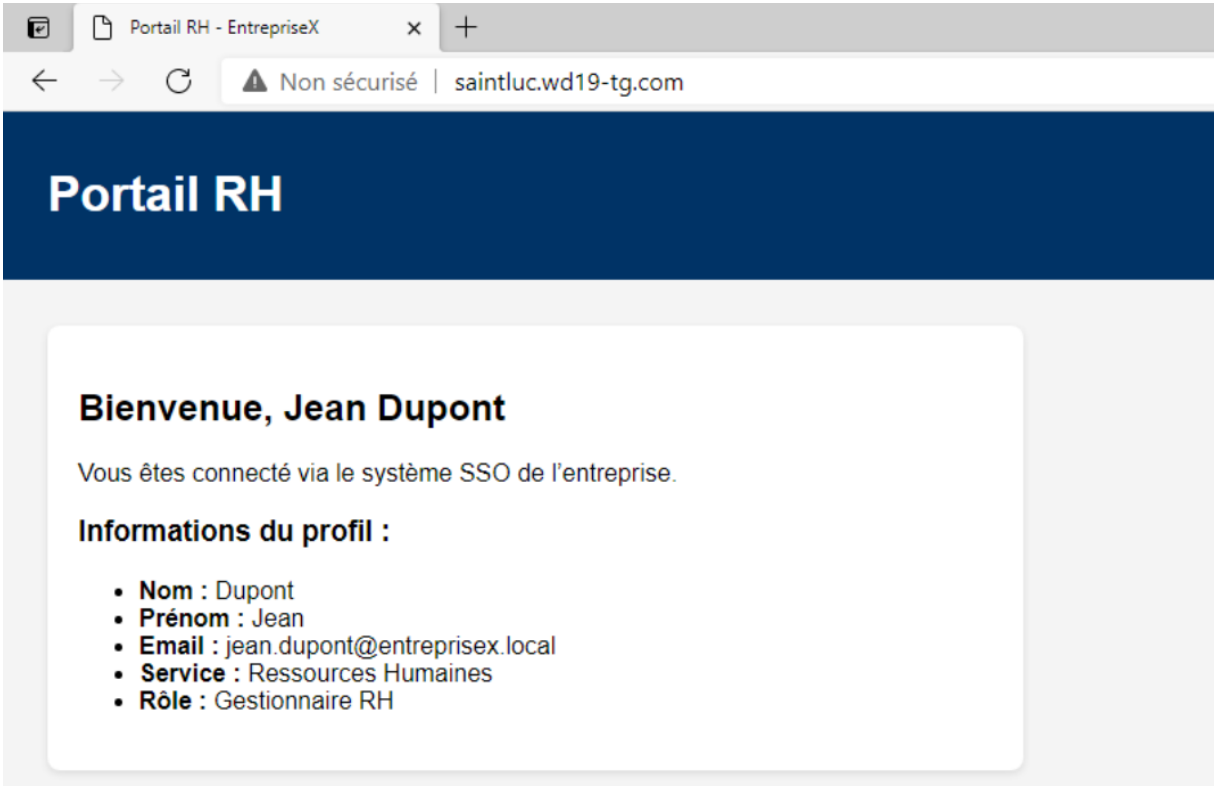
- Elles permettent de mettre à jour les SPN* présentent dans votre serveur
- Vérifier si cela a bien été pris en compte avec cette commande :

```
PS C:\Users\Administrator> setspn -L WDS2019-ThomasG
Registered ServicePrincipalNames for CN=WDS2019-THOMASG,OU=Domain Controllers,DC=WD19-TG,DC=com:
        http/saintluc.WD19-TG.com
```

SPN (Service Principal Name) est un identificateur unique pour une instance de service dans un environnement Active Directory, utilisé par l'authentification Kerberos pour associer un service à un compte de connexion*

Etape 4 - Tester la connexion :

- Test avec l'utilisateur Thomas crée



- Notre utilisateur peut donc accéder directement au site sans devoir entrer des identifications sur le site.
- Maintenant nous allons limiter l'accès au groupe IntranetUsers

Il n'y a pas de saisie de mot de passe car lorsque l'authentification Windows est activée, si l'utilisateur est déjà connecté à un domaine Windows, le navigateur peut automatiquement transmettre ses informations d'identification.

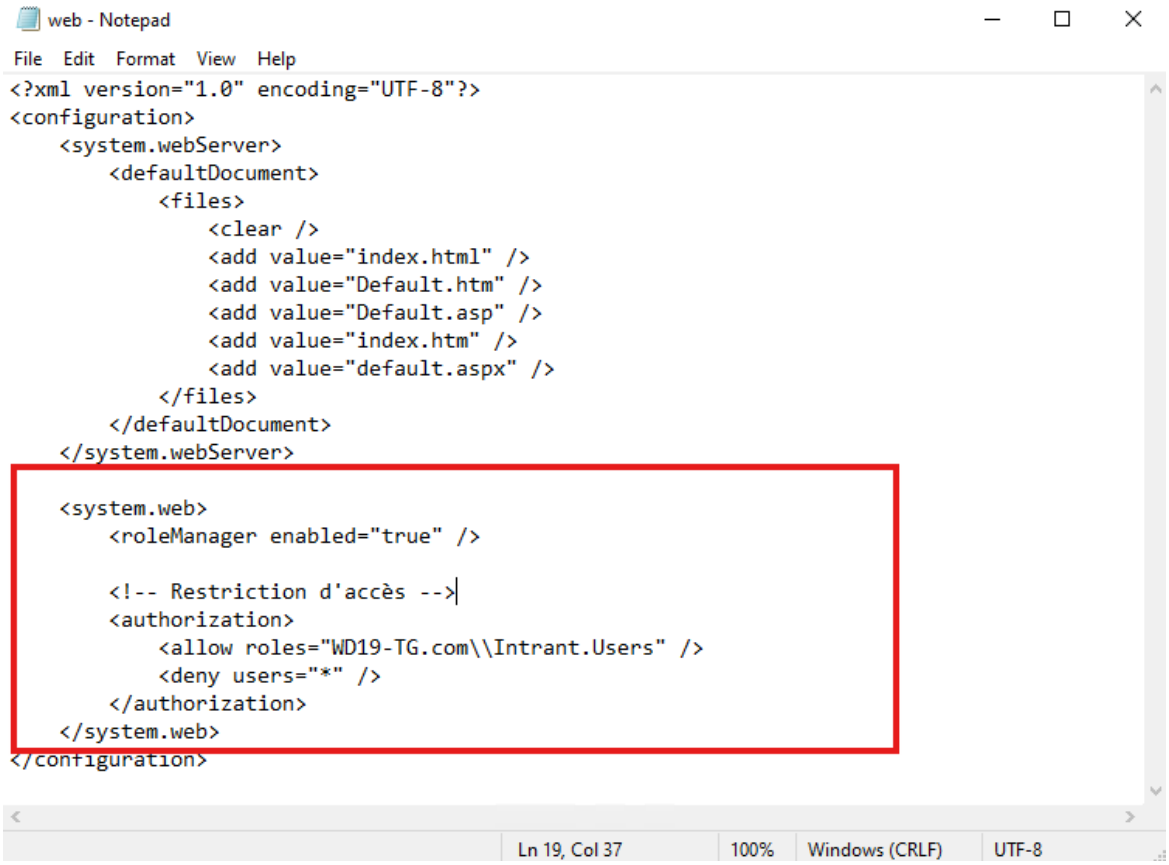
Ce comportement fait partie du mécanisme de Single Sign-On (SSO), qui permet une authentification transparente, sans devoir ressaisir ses identifiants.

Active Directory (AD) et Kerberos jouent des rôles fondamentaux dans le SSO sous Windows. AD est la base de données de sécurité centralisée : il stocke les comptes, les secrets associés aux utilisateurs, les politiques, etc. Kerberos est le protocole d'authentification par défaut dans un domaine : après la connexion de l'utilisateur sur la machine, il délivre un ticket d'authentification (TGT), puis des tickets de service pour

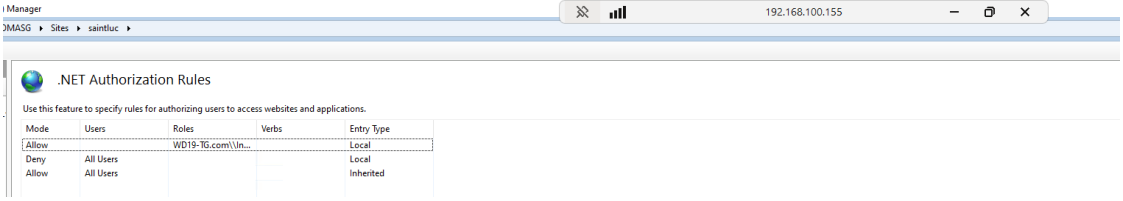
les ressources demandées. Grâce à cela, l'utilisateur peut accéder à plusieurs ressources sans avoir à se reconnecter à chaque fois.

Etape 5 - Limiter l'accès au groupe :

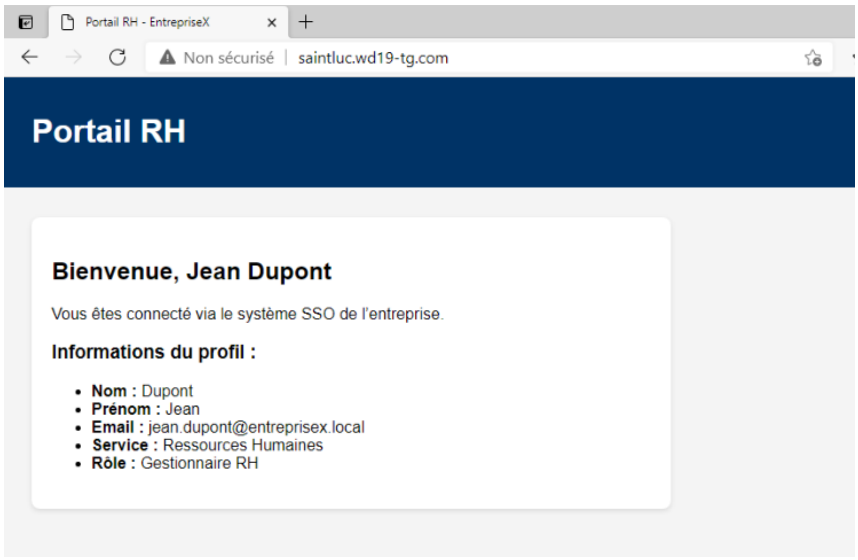
- Pour des raisons de sécurités et de confidentialités il vaut mieux donc restreindre l'accès à certains utilisateurs
- Aller sur votre IIS
- Dans autorisation
- Aller dans son explorateur de fichier
- Aller sur le fichier web
- Appliquer une règle comme quoi vous autorisez l'accès au groupe intranet et vous refusez l'accès aux autres utilisateurs



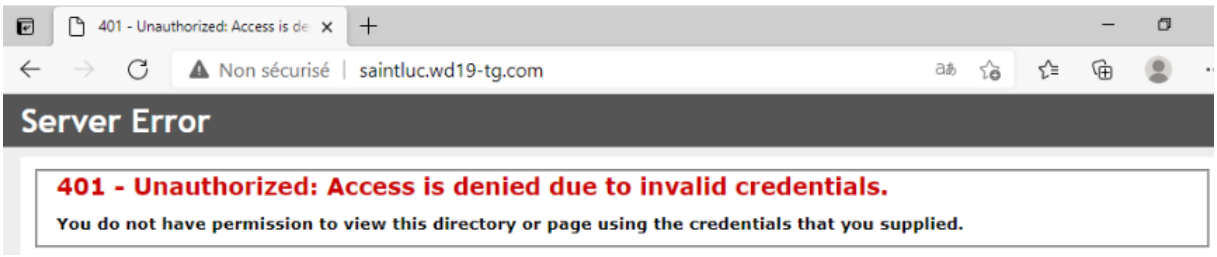
- La règle s'applique dans les règles du site dans .NEt Authorization Rules



- La règle Allow All user ne peut être supprimé depuis l'interface, donc c'est pour cela que l'on a précisé dans le fichier que l'on refusé l'accès à tous les utilisateurs. Pour que l'on puisse "surchargé" localement sans casser l'héritage
- Connexion automatique pour l'utilisateur Thomas



- Refus par l'utilisateur test



- Votre serveur est donc configuré reposant sur le principe de SSO

Source : TP-Service WEB/DNS/Routage -Thomas GRZESINSKI