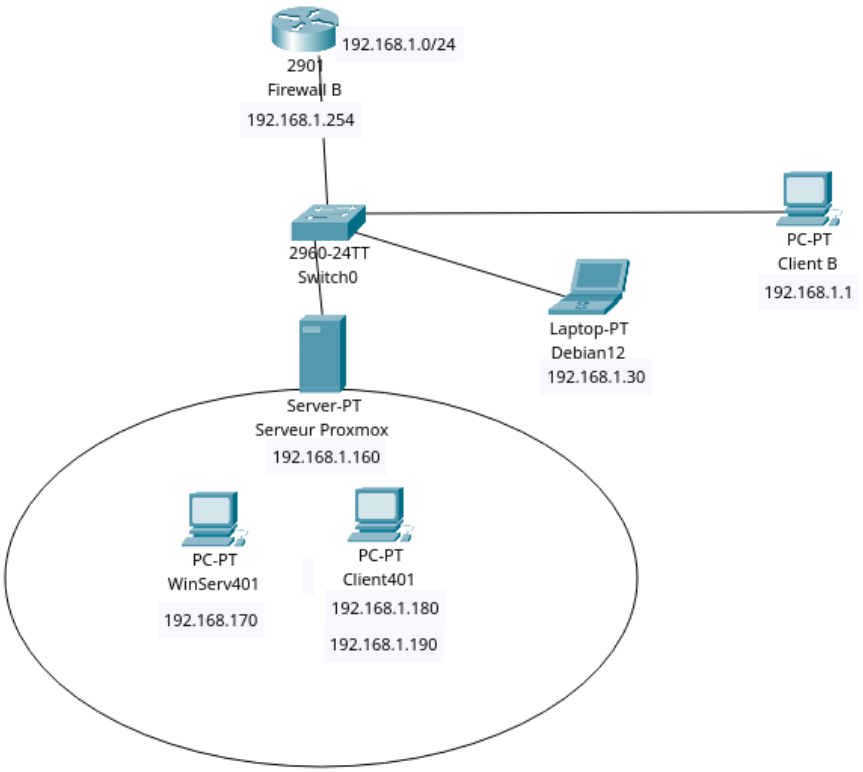
Rapport - tâche 11 : Mise en place d'une architecture Single Sign-On

Ardy : 15h - 89% | Erwann : 3h - 11%

Le Single Sign-On (SSO) ou Authentification unique en français, est une des méthodes d'authentification transparente. Cette méthode repose sur l'interrogation d'un annuaire par l'agent SSO afin d'authentifier un utilisateur sur le firewall. En effet, l'ouverture d'une session génère un événement d'authentification dans le domaine. Ce genre d'événements porte l'ID 4624 ou 4768. L'agent SSO va ensuite consulter les journaux d'événements du contrôleur de domaine et sur réception d'un nouvel événement, il transmet les informations liées à l'adresse IP et au login du client au firewall afin de les ajouter dans la table des utilisateurs authentifiés.
L'objectif de cette tâche est de permettre aux utilisateurs authentifiés de passer un proxy HTTP sans authentification explicite.



Il y a eu un oubli sur le schéma. La machine "Client" qui lui a fait office de client pour le test de connexion et de changement d'IP.

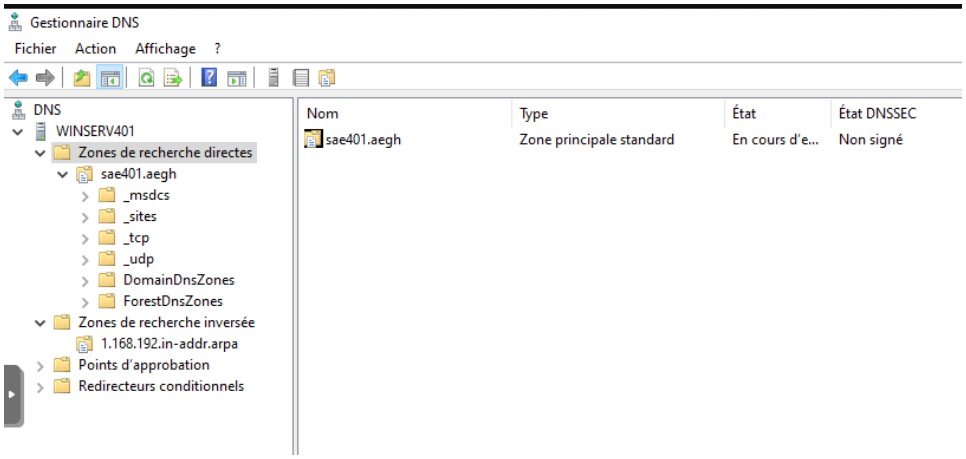
L'architecture demandée devrait se baser sur Active Directory, des services d'annuaire LDAP mis en œuvre par Microsoft pour les systèmes d'exploitation Windows. **Active Directory est un service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine. J'utiliserai AD pour désigner Active Directory.**
Vu que nous n'avions pas à disposition un serveur Windows dans notre réseau, j'ai décidé de le faire en environnement virtuel. J'ai alors installé un serveur Proxmox afin de créer un parc Windows où je mettrai un serveur Windows comme contrôleur de domaine AD.

Cette architecture est mise en place dans le réseau du firewall B (192.168.1.0/24).
Adressage IP :

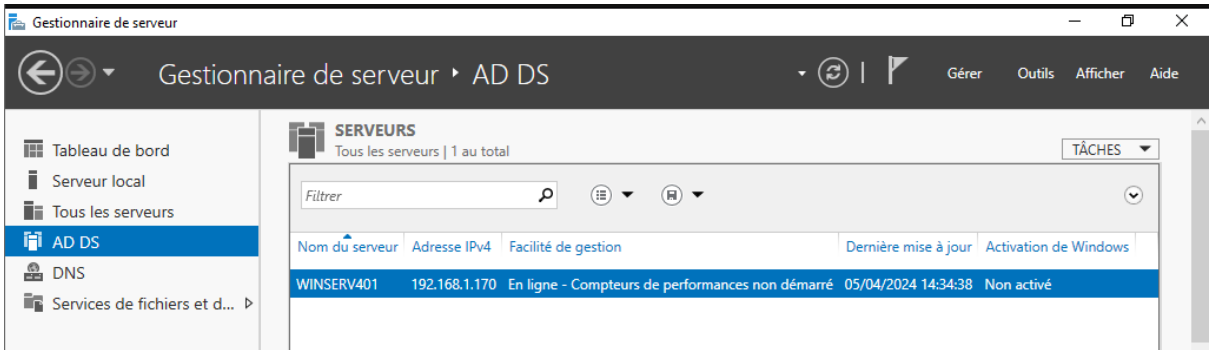
Client B =====> 192.168.1.1
Debian12 =====> 192.168.1.30 (pour configurer les VM)
Serveur Proxmox =====> 192.168.1.160
WinServ401 =====> 192.168.1.170
Client401 =====> 192.168.1.180
Client =====> 192.168.1.190 et 192.168.1.200

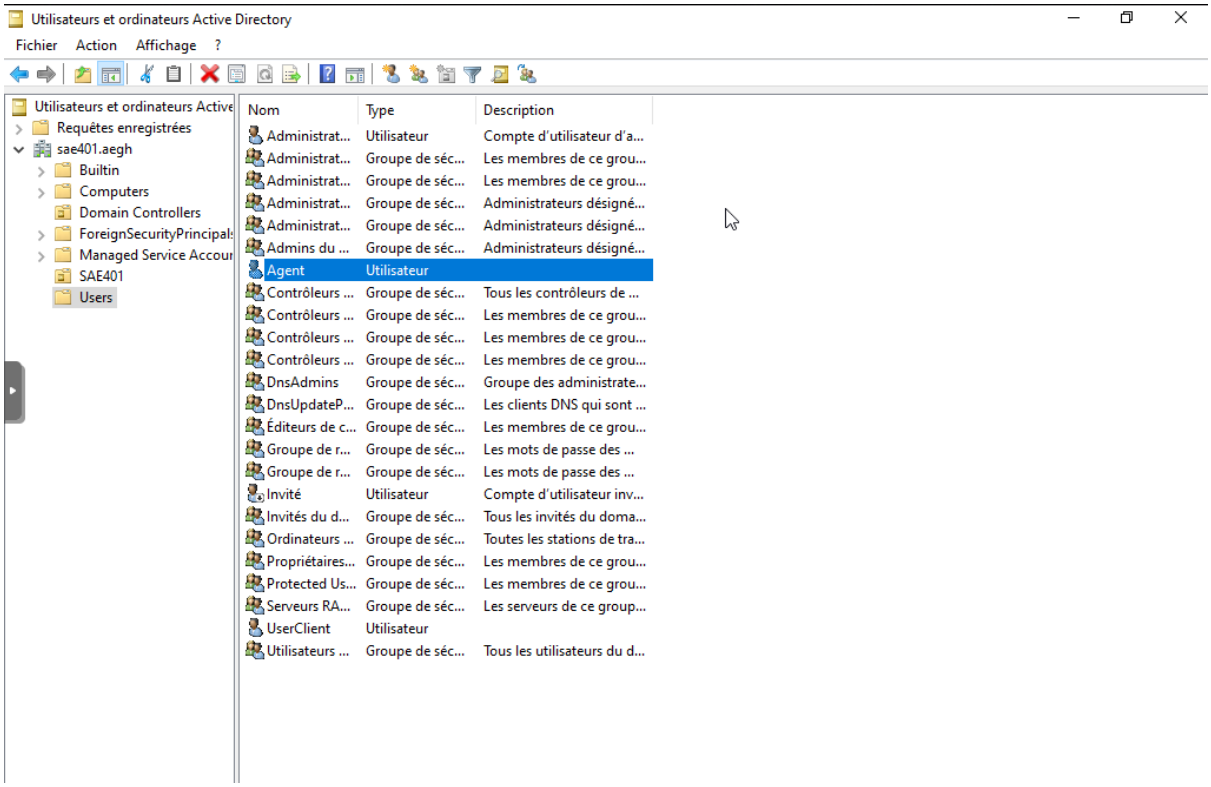
1. Installation d'un serveur AD

L'installation du serveur Windows étant terminée, je réalise d'abord une configuration IP statique correcte et je modifie le nom de mon serveur en "WinServ401". Avant de mettre en place AD, je mets en place le service DNS pour la résolution de nom dont AD pourra se baser dessus.



Cette capture a été prise après l'installation du rôle ADDS, ce qui explique la présence de répertoires de domaine. On note également la résolution inverse des adresses (nécessaire pour le changement d'adresses).
J'installe alors le rôle ADDS et promeus mon serveur en tant que contrôleur de domaine AD. Une fois l'installation réalisée, le rôle ADDS s'ajoute à la console de gestion du serveur au côté du rôle DNS.





Sur l'image ci-dessus, on voit l'arborescence résultant de la mise en place du rôle ADDS. Un utilisateur spécifique a été créé pour permettre à l'agent SSO de contacter le contrôleur de domaine. En effet, cet utilisateur :

- **fait parti du groupe "Lecteurs de journaux d'événements"**
- **peut ouvrir une session comme un service**

J'ai également activé l'audit d'ouverture de session.

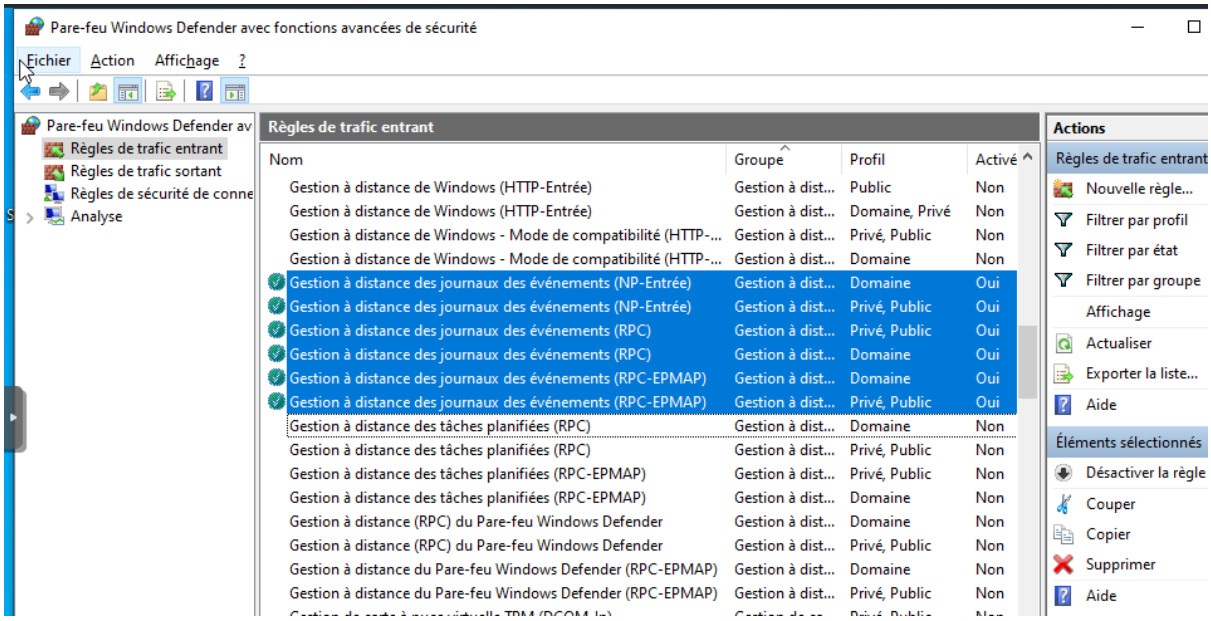
2. Installation de l'Agent SSO sur une machine

Cette installation se fait en deux phases.

a) Sur la machine

J'ai décidé d'installer l'agent SSO sur une autre machine que le contrôleur de domaine, cette machine étant bien sûr membre du domaine. Il faut ensuite autoriser depuis les fonctions avancées de sécurité Windows Defender, trois règles de trafic entrant :

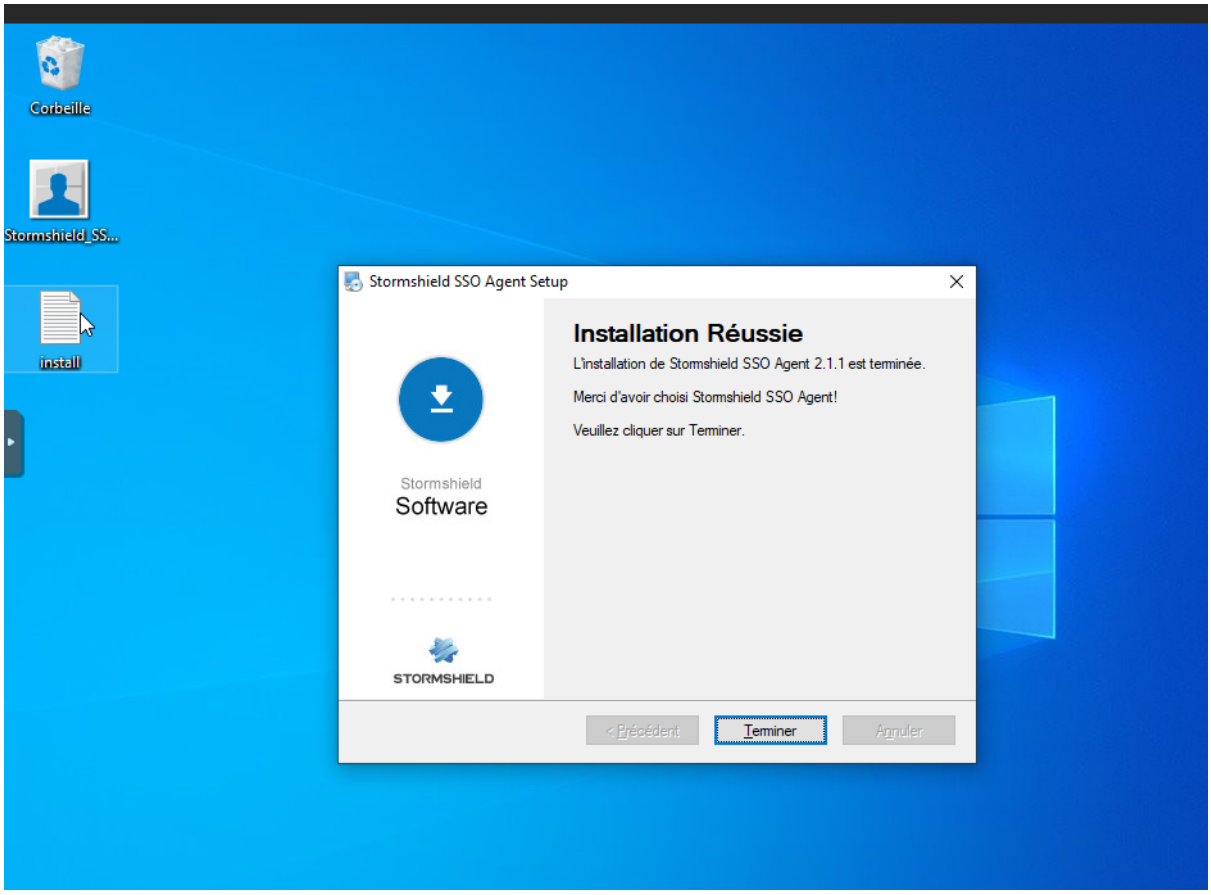
- **Gestion à distance des journaux des événements (NP-Entrée) ;**
- **Gestion à distance des journaux des événements (RPC) ; et**
- **Gestion à distance des journaux des événements (RPC-EMAP)**



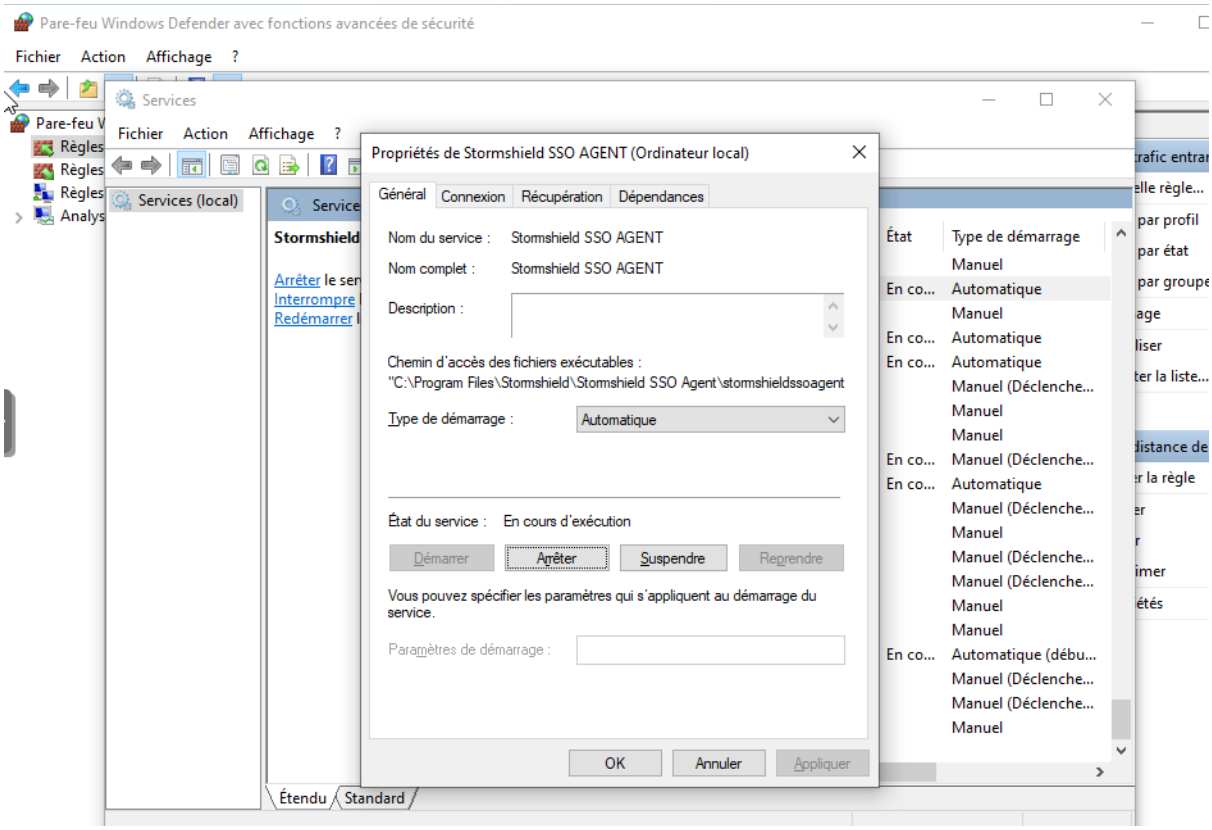
Je récupère par la suite l'exécutable de l'agent SSO fourni. Je lance l'assistant d'installation puis je procède, selon les étapes, de la manière suivante :

- **je renseigne un compte dédié ;**
- **je rentre les informations du compte ; et**
- **je crée la clé de chiffrement SSL (clé pré-partagée).**

Je rappelle que le compte est celui qui a été mentionné plus haut.

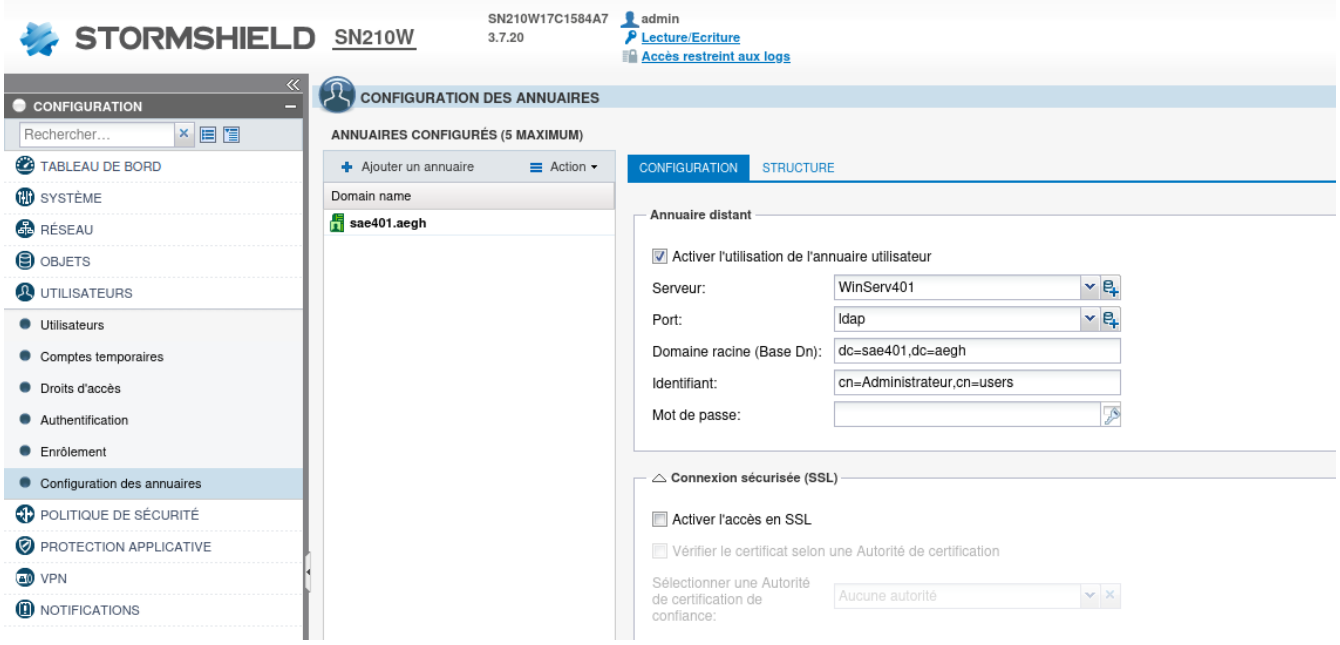


Je me rends ensuite dans les Services Windows, pour démarrer le service “Stormshield SSO Agent”.

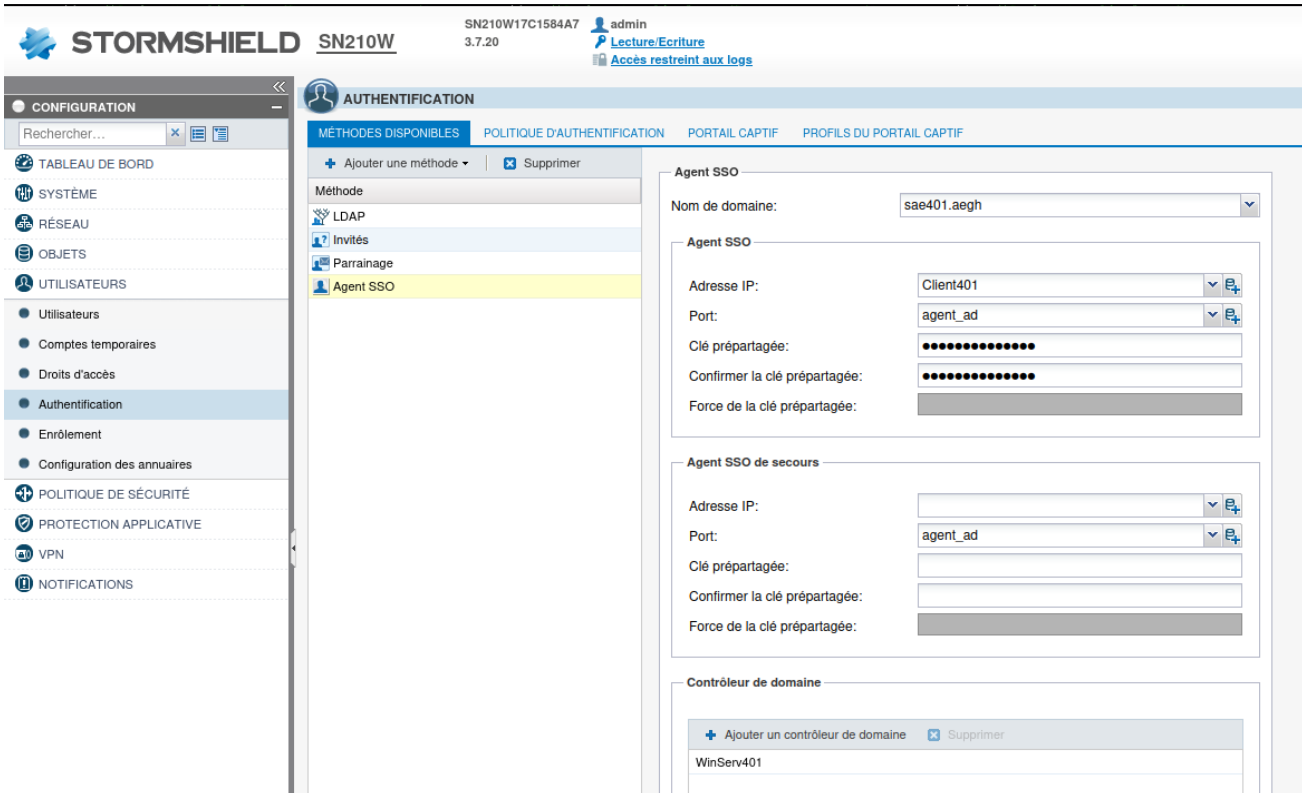


b) Sur le firewall

La phase du firewall consiste essentiellement à configurer les fonctionnalités requises pour finaliser la mise en place de l'architecture.
Je crée deux objets réseau de type machine afin d'identifier facilement l'agent SSO et le contrôleur de domaine respectivement **Client401 et WinServ401.**
Ensuite je renseigne l'annuaire AD concerné dans **Configuration > Utilisateurs > Configuration des annuaires.**



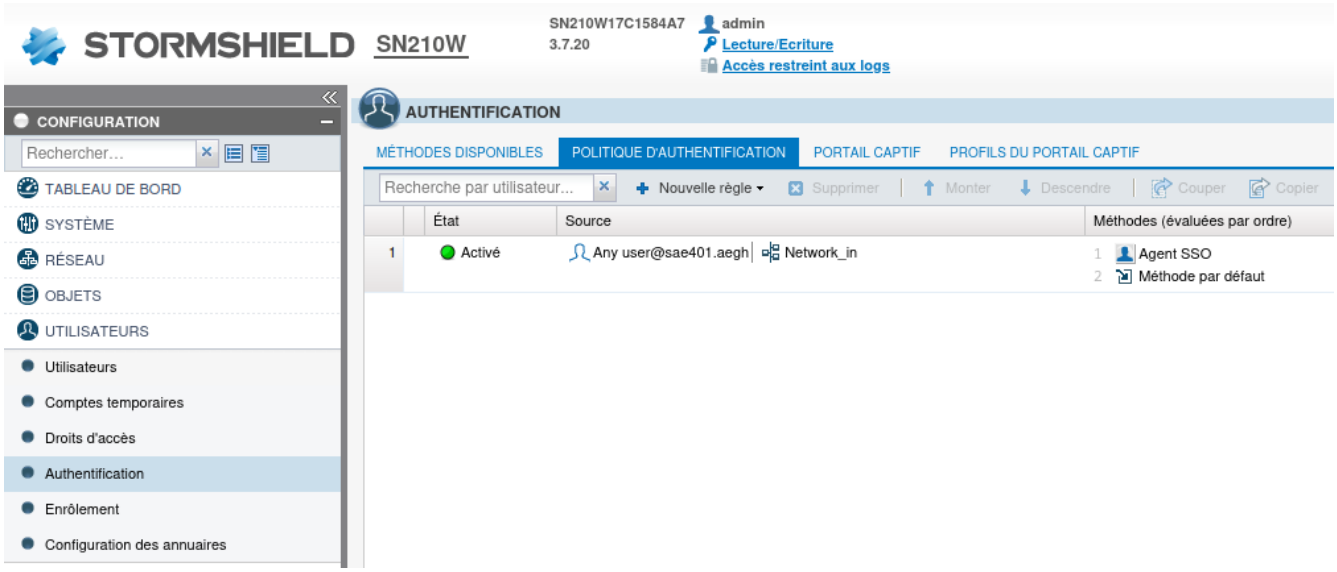
Les informations du compte Administrateur ont été renseignées pour la configuration de l'annuaire. Ne reste plus qu'à configurer la méthode et la politique d'authentification.
Je me rends donc dans **Configuration > Utilisateurs > Authentification.**



Des méthodes par défaut existent. Sur l'image ci-dessus, j'ai ajouté la méthode "Agent SSO" et j'ai rentré les informations demandées :

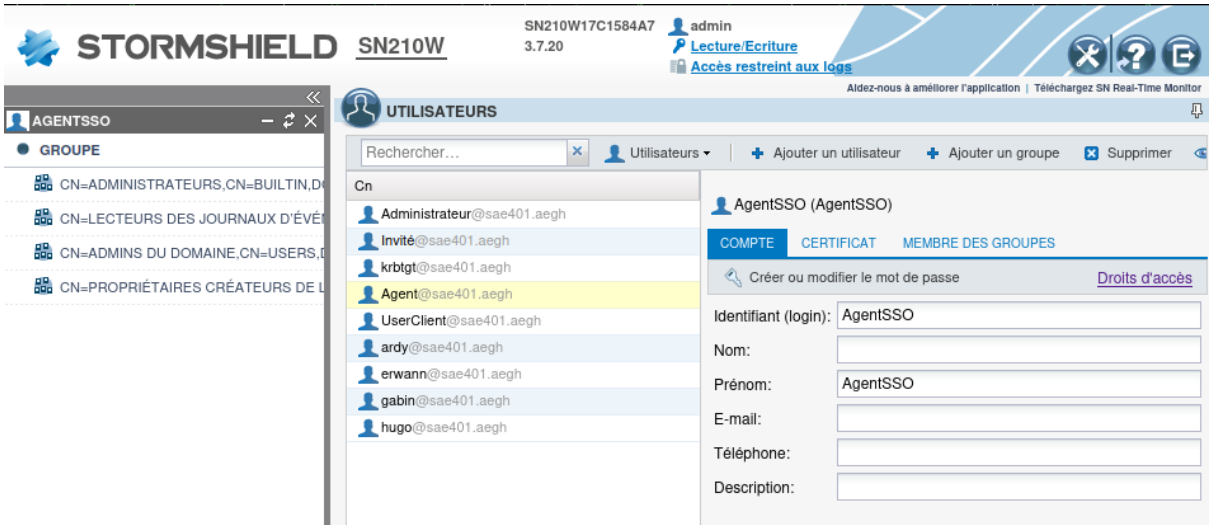
- **"sae401.aegh" nom de domaine ;**
- **"Client401" est l'objet désignant la machine qui héberge le service SSO**
- **"agent_ad" est un objet de port par défaut ;**
- **la clé de chiffrement utilisée lors de l'installation du SSO**
- **"WinServ401" contrôleur de domaine**

Enfin, je définis une règle dans la politique d'authentification qui va autoriser le trafic dédié à la méthode d'authentification Agent SSO configurée en amont.

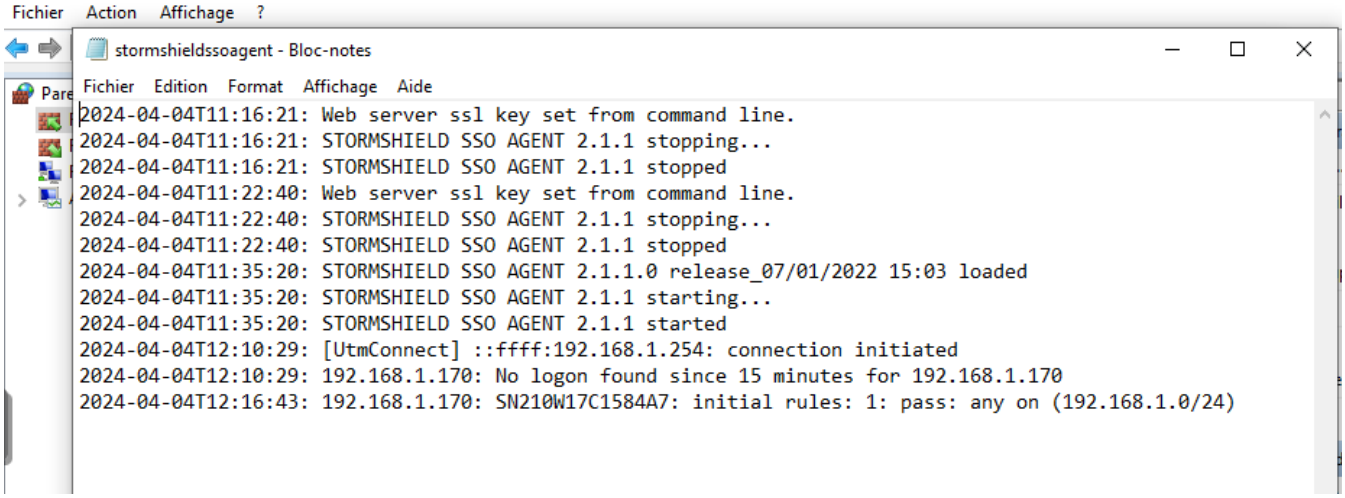


La méthode d'authentification Agent SSO se base sur les événements d'authentification collectés par le contrôleur de domaine. Ceux-ci n'indiquent pas l'origine du trafic, la politique ne peut être spécifiée avec des interfaces d'où "Network_in".

L’image ci-dessous confirme l'opérationnalité de notre annuaire.



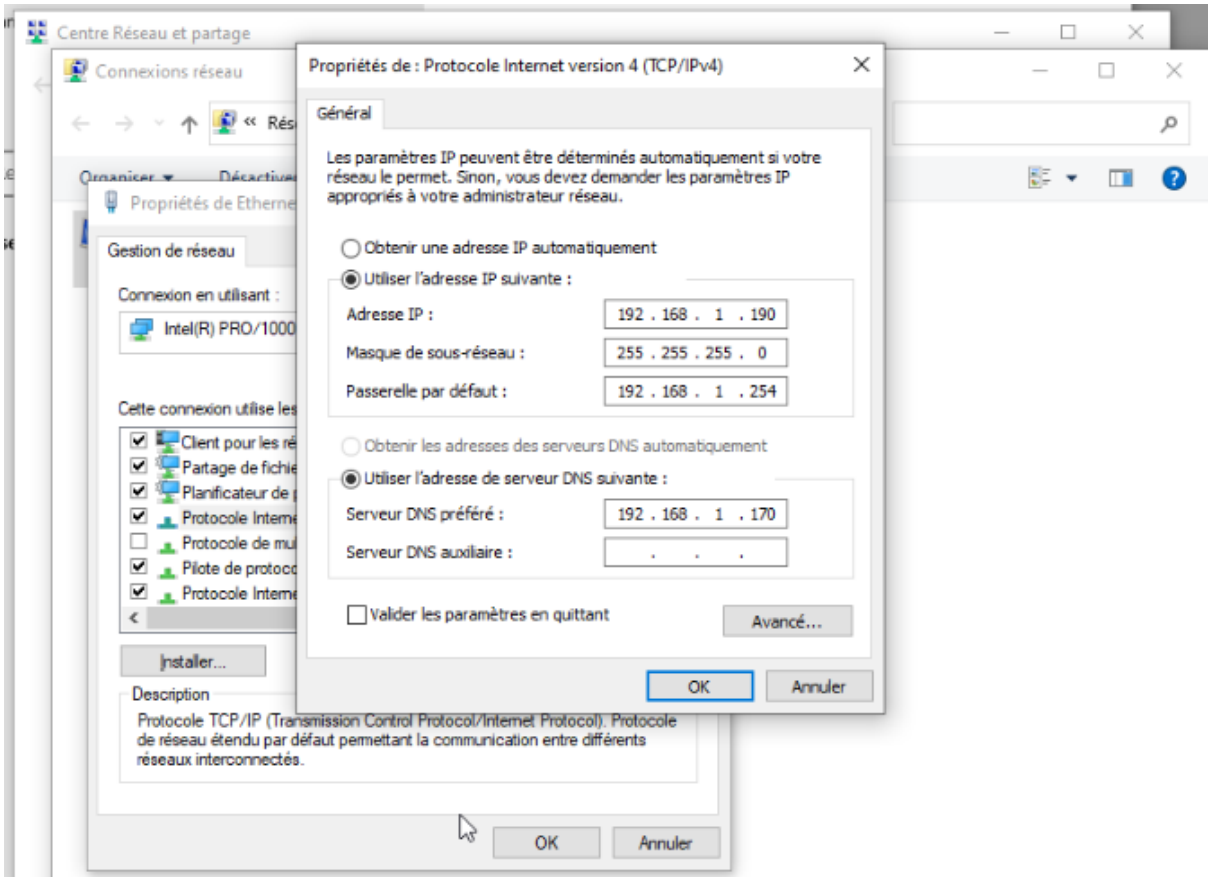
On vérifie le fonctionnement de notre installation depuis la machine hébergeant le service SSO grâce au fichier de log.

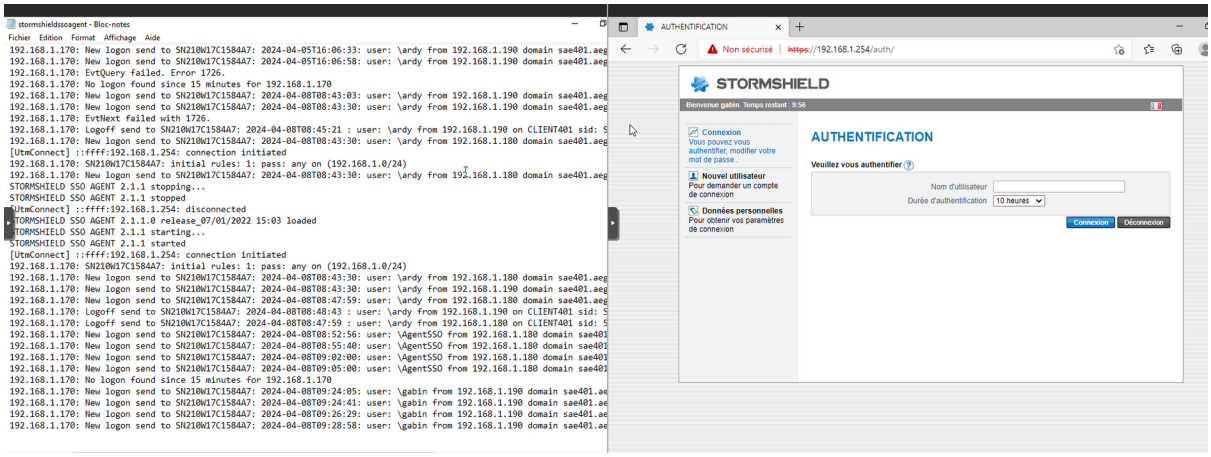


Une fois l’architecture en place, on n’a plus qu’à configurer une autre machine pour réaliser le test.

3. Configuration d’une machine cliente et changement d’adresses IP.

La configuration ici ne consiste qu’à mettre cette machine dans le domaine. Vu que nous n'avons pas de serveur DHCP, on réalise premièrement une configuration réseau statique puis modifions le nom et le domaine de cette machine. Ce qui donne





Sur la dernière image. On peut vérifier les logs sur le client SSO et l'utilisateur qui est directement authentifié sur le firewall.

Remarque : Cette représentation ne traduisait pas une situation réelle. Et lors de la validation par M. Bourgeois, nous avons mis en place une règle traduisant une situation normale de la vie où un utilisateur ouvrant une session dans le domaine pouvait accéder à Internet et un autre hors domaine qui était interdit. Cela illustre la validation de l'architecture SSO.

Le changement d’adresse IP se remarque lors de requêtes DNS de la part du SSO. Ce qui permet au firewall d’associer la nouvelle IP à l’utilisateur. Ce changement se fait grâce à zone de recherche inverse.

```
 No logon found since 15 minutes for 192.168.1.170
 No logon found since 15 minutes for 192.168.1.170
 No logon found since 15 minutes for 192.168.1.170
 No logon found since 15 minutes for 192.168.1.170
 No logon found since 15 minutes for 192.168.1.170
:ffff:192.168.1.254: disconnected
 EvtQuery failed. Error 1722. To connect to the remote computer, the remote computer must enable the "Remote Event Log
 Logoff send to SN210W17C1584A7: 2024-04-05T14:30:54 : user: \ardy from 192.168.1.180 on CLIENT401 sid: S-1-5-21-394490
 New logon send to SN210W17C1584A7: 2024-04-05T12:55:06: user: \ardy from 192.168.1.190 domain sae401.aegh on CLIENT401
```

Conclusion

Le Single Sign-On est une méthode d’authentification transparente facilitant l’expérience utilisateur. Cette méthode connecte un utilisateur à d’autres applications dès l’ouverture de session. Mais elle ne supporte pas la connexion Multi-users sur une IP.