PROJET E5 BTS SIO SISR :

INFRASTRUCTURE RÉSEAU NOTATECH

Documentation de tests

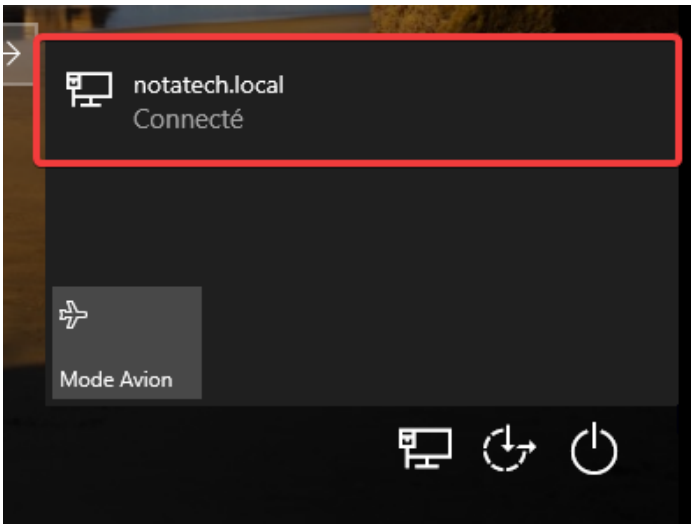
REDOULES CLÉMENT

Sommaire :

Test de connexion à l'AD avec une machine cliente et test des GPO mot de passe :

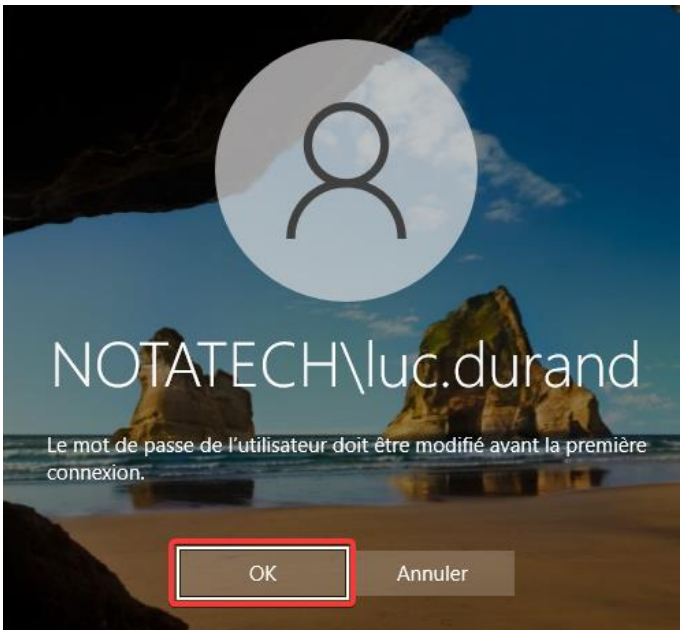
Dans cette partie nous allons tester la connexion à l'AD avec un compte de notre AD, dans notre cas ça sera le compte de Luc Durand que nous avons ajouté à notre AD précédemment.

Déjà nous observons que notre machine a bien récupéré le nom de domaine (je l'ai ajouté à notre domaine précédemment)

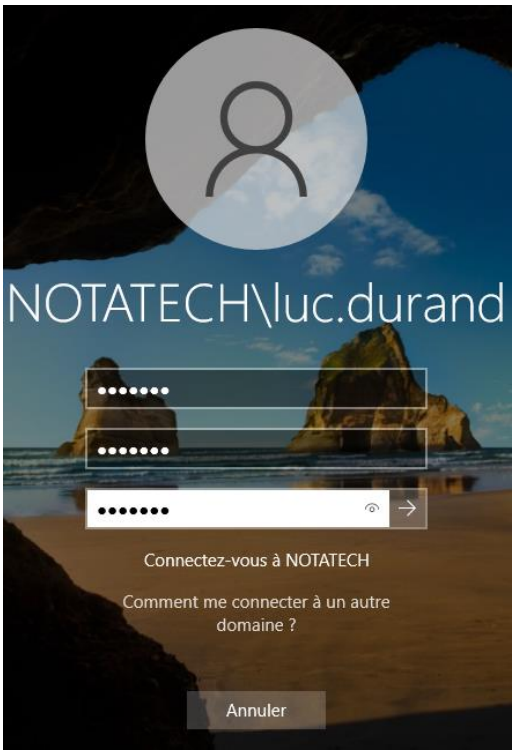


Ici je rentre l'identifiant **Prenom.nom** et ensuite le mot de passe générique **Root123** qu'on a configurer précédemment

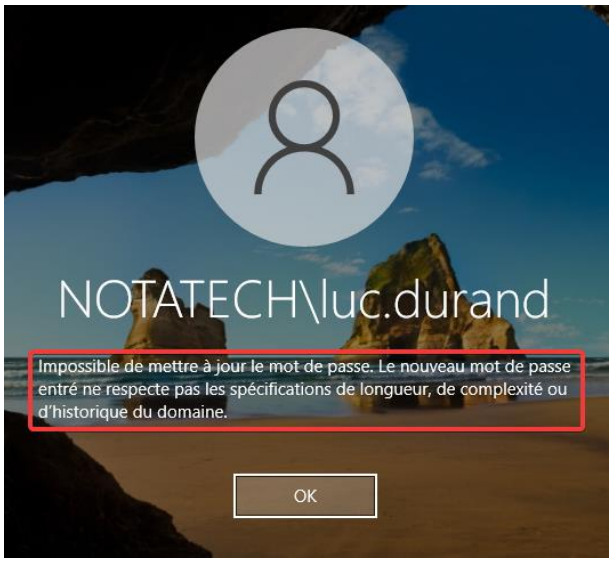
Ensuite ici on voit que notre configuration **« l'utilisateur devra changer de mot de passe »** fonctionne bien car on nous demande de changer de mot de passe



Ensuite ici je rentre un mot de passe ne respectant pas les exigences de mots de passe des GPO pour tester mes GPO mot de passe, le mot de passe est simplement **Root123**



On voit donc que les GPO fonctionnent bien car on nous signale que **le mot de passe ne respecte pas les exigences de mot de passe du domaine**



Je rentre donc un mot de passe **Complexe**

Et la connexion se fait ensuite bien avec un mot de passe changé

Test DHCP PfSense :

Dans cette partie nous allons voir si notre machine a bien reussit a joindre notre serveur DHCP et a avoir une IP dans la plage configuré avec les bons DNS et la bonne passerelle

Je fais donc un **ipconfig /all** pour voir tous les paramètres réseaux que ma machine a récupérée, on peut voir que déjà la machine est bien connecté au DNS **Notatech.local** ensuite au niveau de **l'adresse IP** on peut voir que notre machine a bien récupérée l'adresse **192.168.1.103/24** et la passerelle a bien été défini en **192.168.1.1** qui est l'adresse de notre **PfSense**

```
C:\Windows\system32>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . . : DESKTOP-G0EHVTQ
   Suffixe DNS principal . . . . . . . . : notatech.local
   Type de noeud. . . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . . : Non
   Liste de recherche du suffixe DNS.: notatech.local

Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : notatech.local
   Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . . . . . . . : 00-0C-29-E7-D4-01
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::cde2:2195:a30:4502%13(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.103(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : vendredi 22 novembre 2024 16:13:44
   Bail expirant. . . . . . . . . . . . . : vendredi 22 novembre 2024 18:00:30
   Passerelle par défaut. . . . . . . . . : fe80::20c:29ff:fe5c:41bc%13
                                    192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . : 117443625
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2E-D1-65-47-00-0C-29-E7-D4-01
```

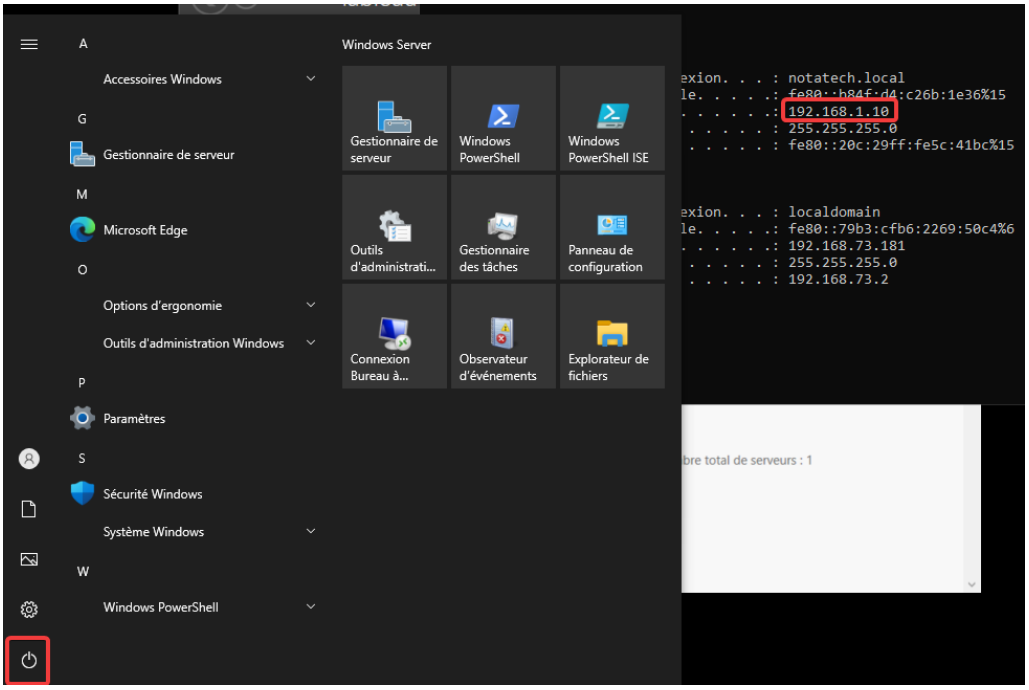
Et finalement on voit qu'au niveau des serveurs DNS notre machine a bien récupérée les adresses de nos 2 serveurs AD en redondance **192.168.1.10** et **192.168.1.5**

```
Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . . . . . . . : 117443625
DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2E-D1-65-47-00-0C-29-E7-D4-01
Serveurs DNS. . .  . . . . . . . . . . : 192.168.1.10
                                    192.168.1.5
NetBIOS sur Tcpip. . . . . . . . . . . : Active
Liste de recherche de suffixes DNS propres à la connexion :
                                    notatech.local
```

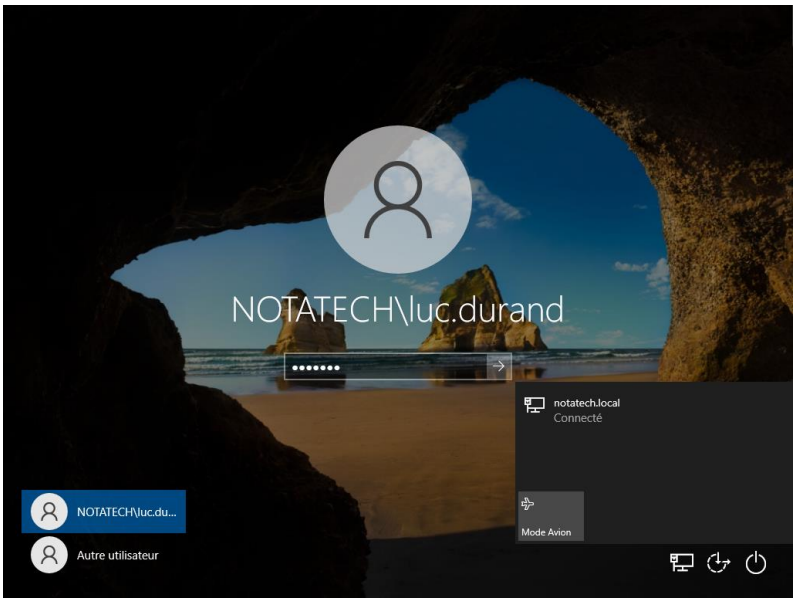
Test de la redondance :

Dans cette partie nous allons tester la redondance de nos 2 serveurs AD, je vais tout simplement éteindre mon serveur AD principal et voir si je peux toujours me connecter a mon domaine

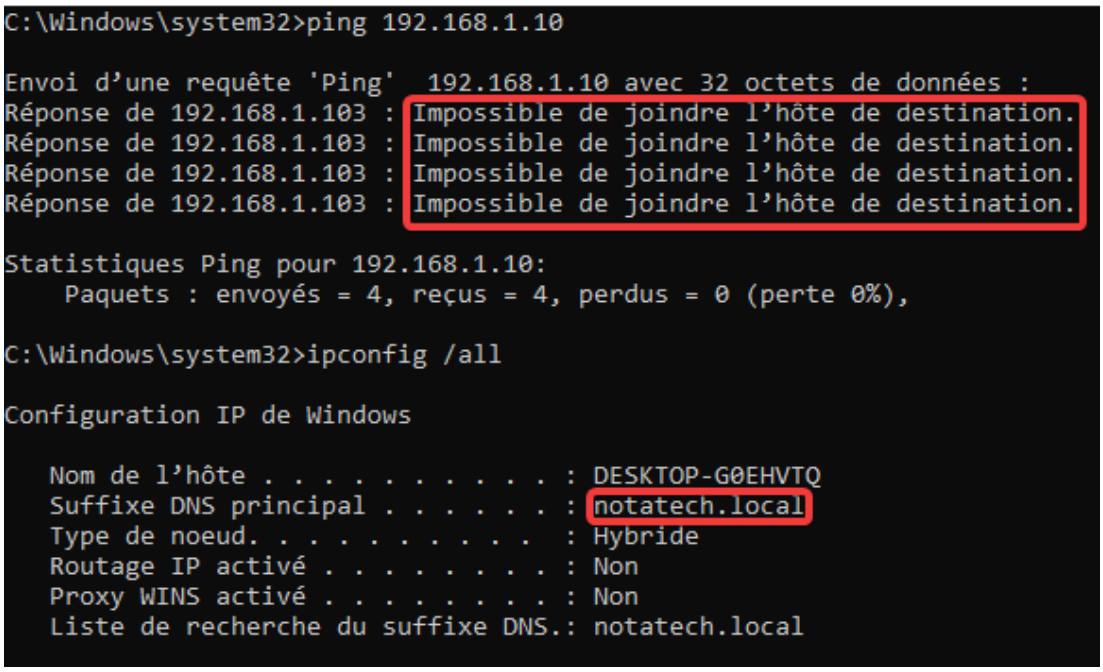
Je commence donc par éteindre mon premier serveur AD en **192.168.1.10**



Ensuite j'allume une machine cliente pour tester la connexion a l'AD, on peut déjà voir que notre machine a bien récupérée la connexion réseau et le domaine **notatech.local**



Je me connecte donc avec les identifiants de session de **Luc Durand** et on peut voir que la connexion s'est bien faite, j'ouvre donc une fenêtre **CMD** pour faire un **ping** vers notre serveur AD éteint et on peut voir qu'il est bien éteint est que la redondance est effective car la machine a bien réussi à joindre le domaine.

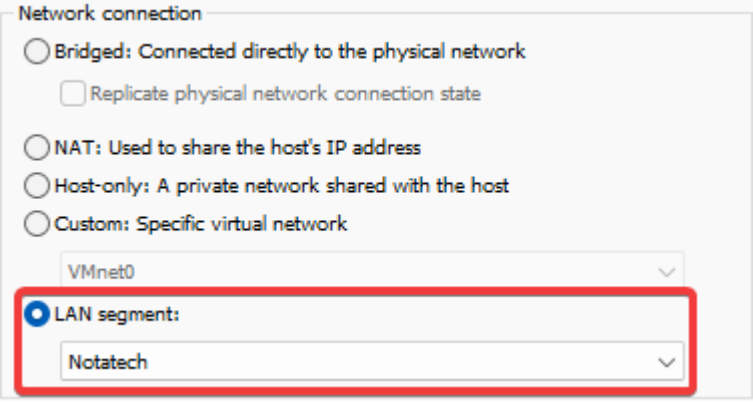


Notre redondance est donc bien effective

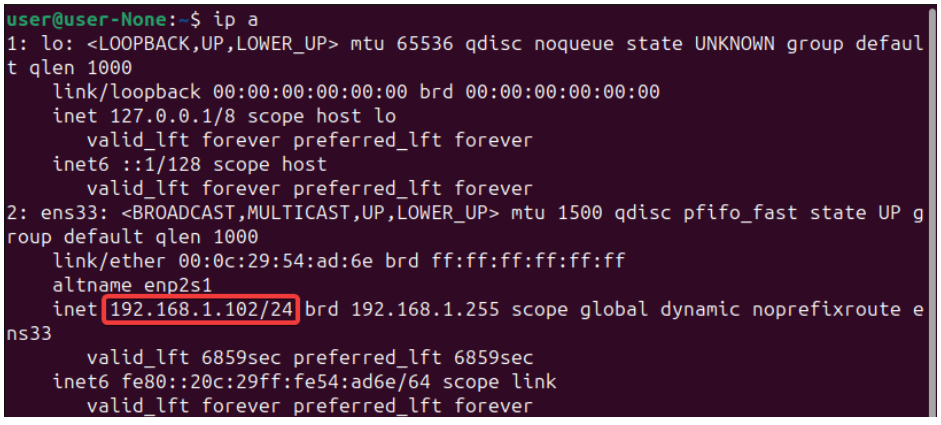
Test de notre IDS/IPS Suricata :

Dans cette partie nous allons tester notre IDS/IPS que nous avons configurer sur notre PfSense précédemment, pour ce faire nous allons faire une machine ubuntu sur laquelle nous allons essayer d'installer Nmap, ce qui devrait être bloqué, et ensuite voir les alertes de notre Suricata générée par notre réseau

Je commence donc par démarrer une machine ubuntu que j'ai au préalable mit sur le **LAN segment « Notatech »**



Déjà en faisant **ip a** nous pouvons voir que la machine Ubuntu a bien récupérée une adresse avec notre **DHCP**



Ensuite je fais donc cette commande pour mettre à jour les paquets de ma machine ubuntu et installer le package **Nmap** pour pouvoir utiliser cet outil qui permet de faire des scans réseaux

```
ubuntu@ubuntu:~$ sudo apt update && sudo apt install nmap -y
```

On peut voir déjà que mes téléchargements sont bloqués

```
E: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/universe/libl/liblinear
/liblinear4_2.3.0%2bdfsg-5build1_amd64.deb  Unable to connect to archive.ubuntu.
com:http:
E: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/main/libs/libssh2/libss
h2-1t64_1.11.0-4.1build2_amd64.deb  Unable to connect to archive.ubuntu.com:http
:
E: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/universe/n/nmap/nmap-co
mmon_7.94%2bgit20230807.3be01efb1%2bdfsg-3build2_all.deb  Unable to connect to a
rchive.ubuntu.com:http:
E: Failed to fetch http://archive.ubuntu.com/ubuntu/pool/universe/n/nmap/nmap_7.
94%2bgit20230807.3be01efb1%2bdfsg-3build2_amd64.deb  Unable to connect to archiv
e.ubuntu.com:http:
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-mis
sing?
```

Ensuite quand je vais dans mes alertes sur mon interface WEB **PfSense** on voit que les recherches internet par exemple sont référencés, et nous permet de bloquer le site ou de ne rien faire

11/22/2024 19:12:45	3	UDP	Generic Protocol Command Decode	142.250.75.227	443	192.168.1.103	51061	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:12:45	3	UDP	Generic Protocol Command Decode	142.250.75.227	443	192.168.1.103	51061	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:12:45	3	UDP	Generic Protocol Command Decode	142.250.75.227	443	192.168.1.103	51061	1:2231000	SURICATA QUIC failed decrypt

Ensuite pour l'interface **WAN** On voit aussi que les alertes **suricata** se font bien

11/22/2024 19:49:01	3	UDP	Generic Protocol Command Decode	192.168.73.181	59696	2.18.40.151	443	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:49:01	3	UDP	Generic Protocol Command Decode	192.168.73.181	59696	2.18.40.151	443	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:48:02	3	UDP	Generic Protocol Command Decode	192.168.73.181	60369	2.18.40.151	443	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:48:02	3	UDP	Generic Protocol Command Decode	192.168.73.181	60369	2.18.40.151	443	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:47:01	3	UDP	Generic Protocol Command Decode	192.168.73.181	49152	2.18.40.143	443	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:47:01	3	UDP	Generic Protocol Command Decode	192.168.73.181	49152	2.18.40.143	443	1:2231000	SURICATA QUIC failed decrypt
11/22/2024 19:46:01	3	UDP	Generic Protocol Command Decode	192.168.73.181	61363	2.18.40.143	443	1:2231000	SURICATA QUIC failed decrypt

Conclusion :

Cette documentation de tests met en évidence les différentes validations effectuées sur l'infrastructure réseau de Notatech. Les tests de connexion à l'AD, des GPO, du DHCP, de la redondance et de l'IDS/IPS montrent que les configurations mises en place fonctionnent comme attendu, garantissant la stabilité, la sécurité et l'efficacité du réseau.

Ces résultats confirment que l'infrastructure répond aux exigences d'un projet professionnel et est prête à être exploitée dans un environnement de production.