Documentation de test projets BTS

Fiche de tests

Nous allons maintenant vérifier si toutes les configurations faites précédemment fonctionnent.

Nous procèderons comme ceci :

1.Sécurité du réseau avec pfSense, Squid et SquidGuard

2. Serveur principal sous Windows Server 2019

3. Monitoring réseau avec Nagios

4. Gestion de la maintenance avec GLPI

5. Postes de travail collaborateurs

6. Sauvegarde cloud automatisée avec AWS et PowerShell

7. Redondance Active Directory et DNS

8. VPN Sécurisé avec OpenVPN

9. Surveillance et Sécurité du Réseau

9.1. Système de Détection d'Intrusion (IDS/IPS)

9.2. Analyse du Trafic avec Wireshark

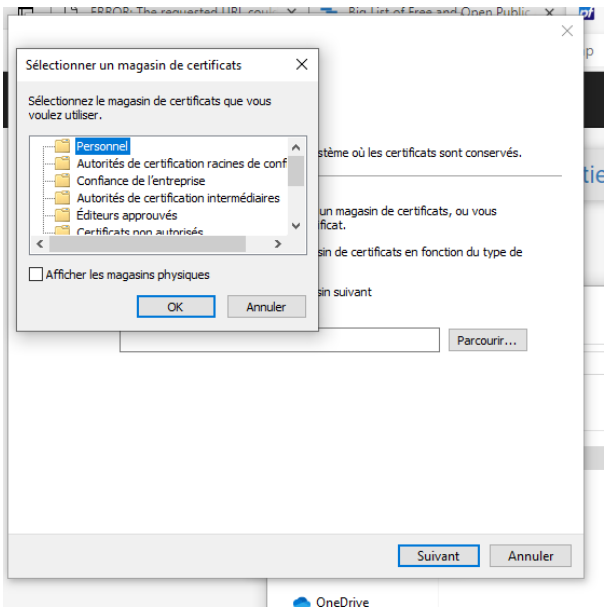
10. Stockage et Partage des Données

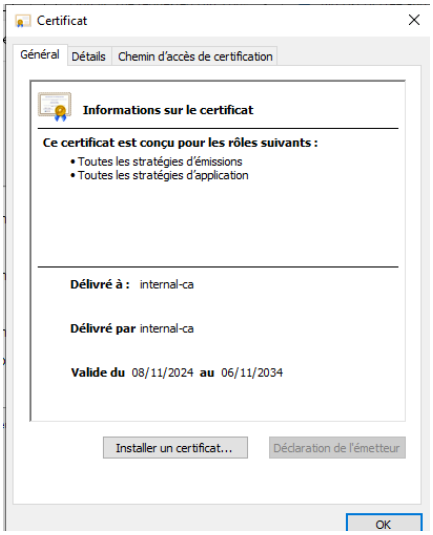
10.1. Infrastructure NAS avec TrueNAS

11. Messagerie d'entreprise via Zimbra

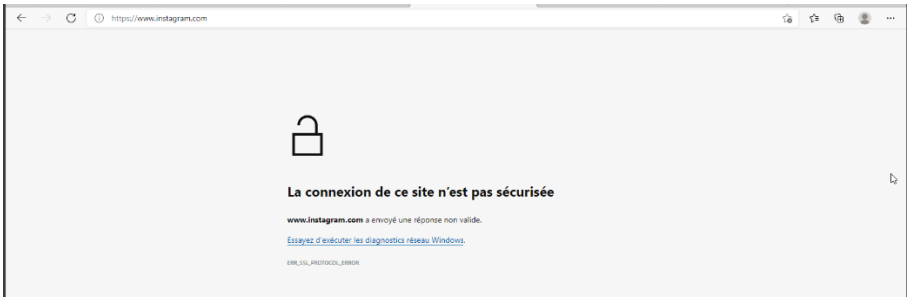
1 –

Tout d’abord nous nous rendons sur les postes de l’étude pour intégrer le certificat précédemment crée dans pfSense



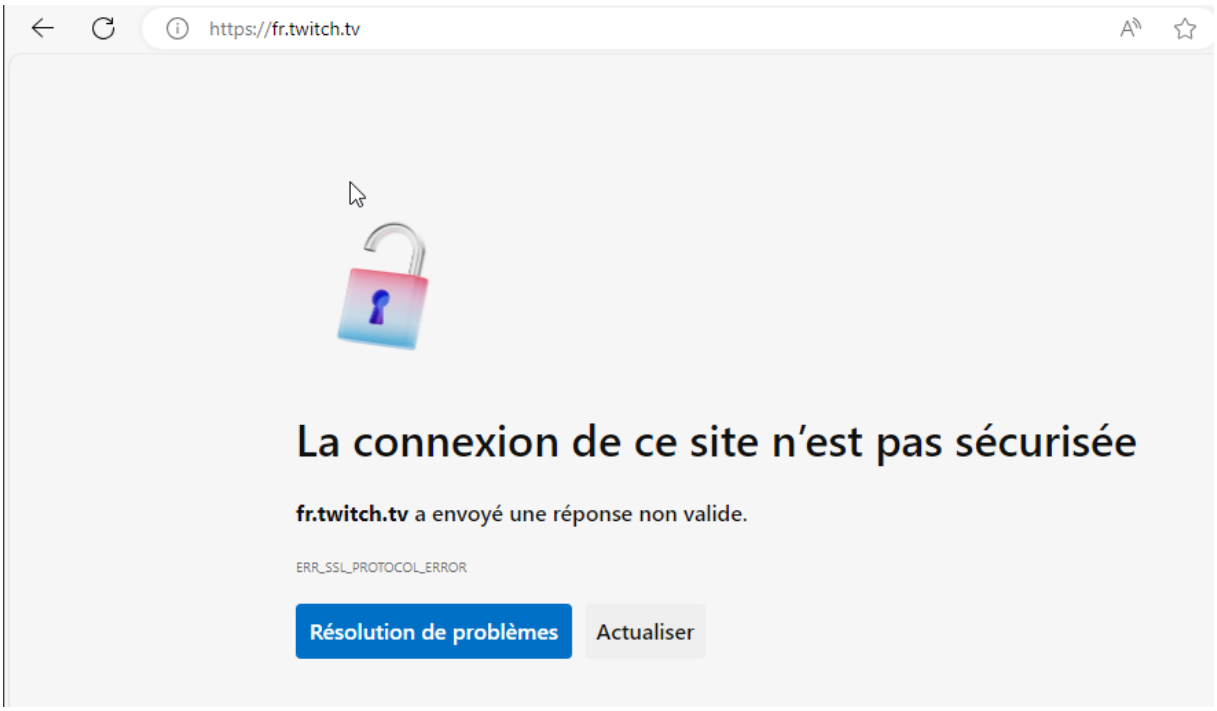


Le certificat est bien intégré, nous pouvons maintenant essayer d’accéder aux sites bloqués

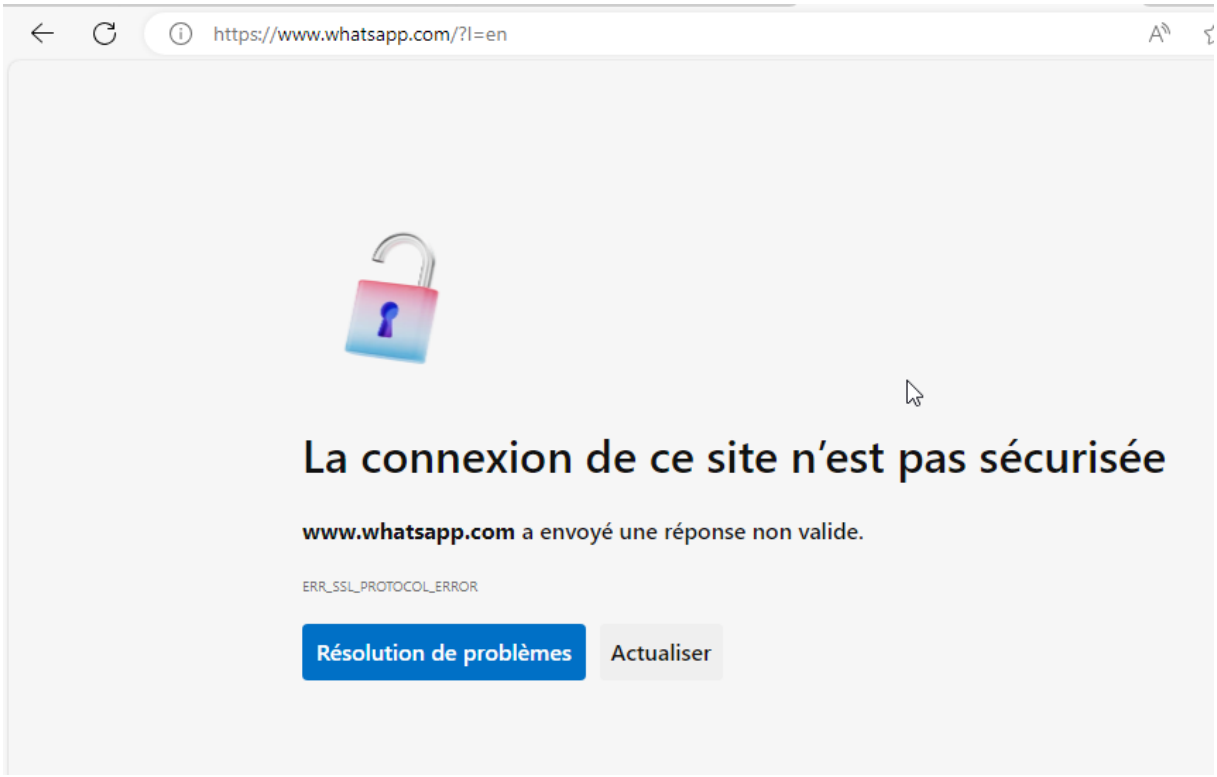


Ici instagram est bien bloqué

Egalement pour Twitch.tv

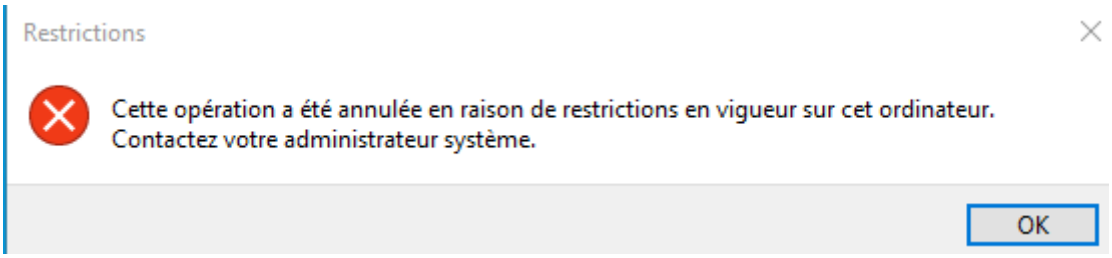


Egalement whatsapp

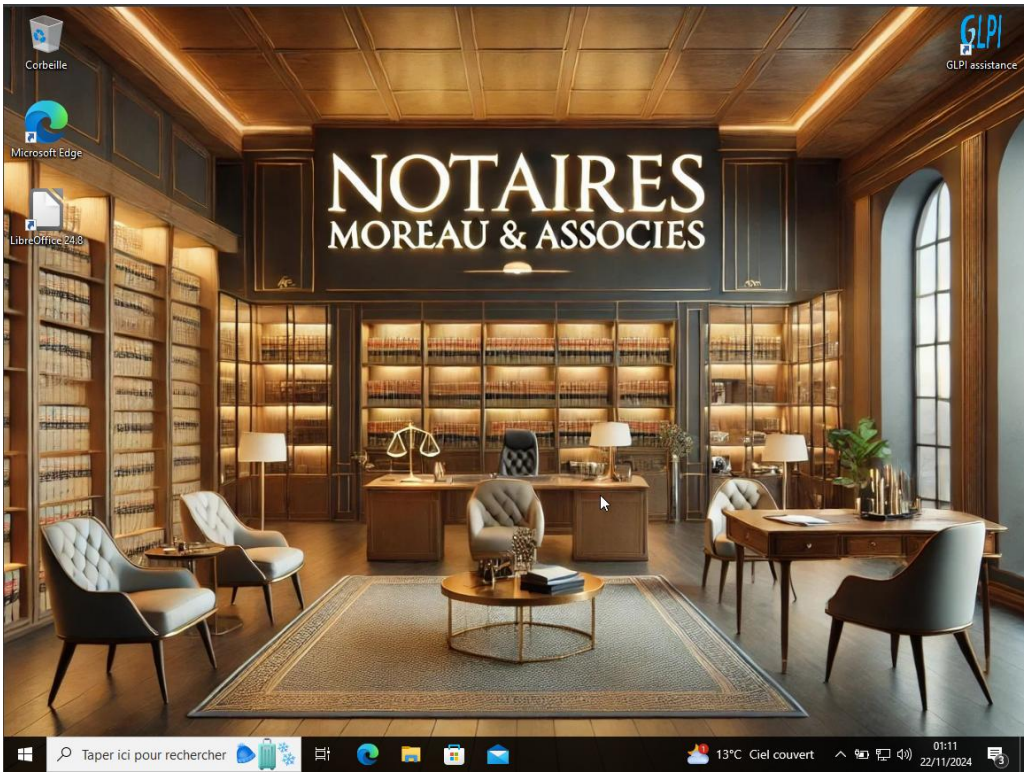


2. Serveur principal sous Windows Server 2019

On voit que notre GPO dédié au menu exécuter fonctionne

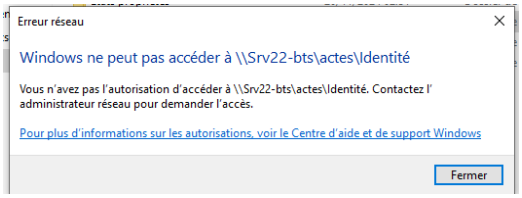


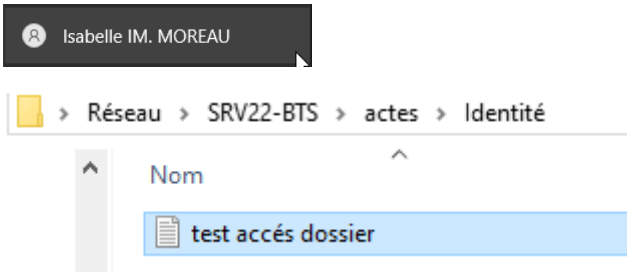
Ainsi que nos fond d'écrans



Maintenant vérifions les autrisation d'accés aux dossiers sensibles

Ici nous pouvons voir que sophie marin n'a pas accès au dossier tandis que Isabelle Moreau si





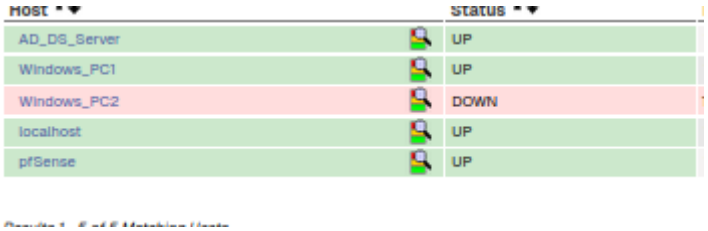
Ainsi nous bloquons l'accès aux donnés sensible en fonctions des demandes de la cliente.

3. Monitoring réseau avec Nagios

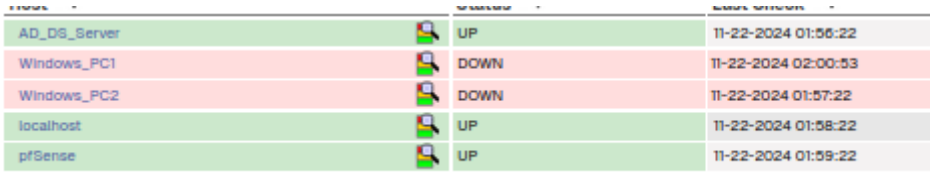
Pour se faire nous allons déconnecter le pc 2 du réseau et ainsi voir si effectivement il apparait comme étant down et donc non fonctionnel sur nagios

La vm est éteinte

Et le pc est répertorié comme down dans nagios



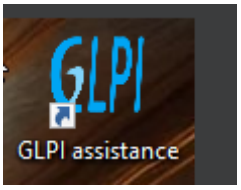
Ainsi que le pc 1



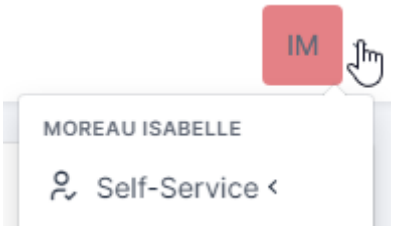
Ainsi nous pouvons nous assurer du bon état des services et des equipements

4. Gestion de la maintenance avec GLPI

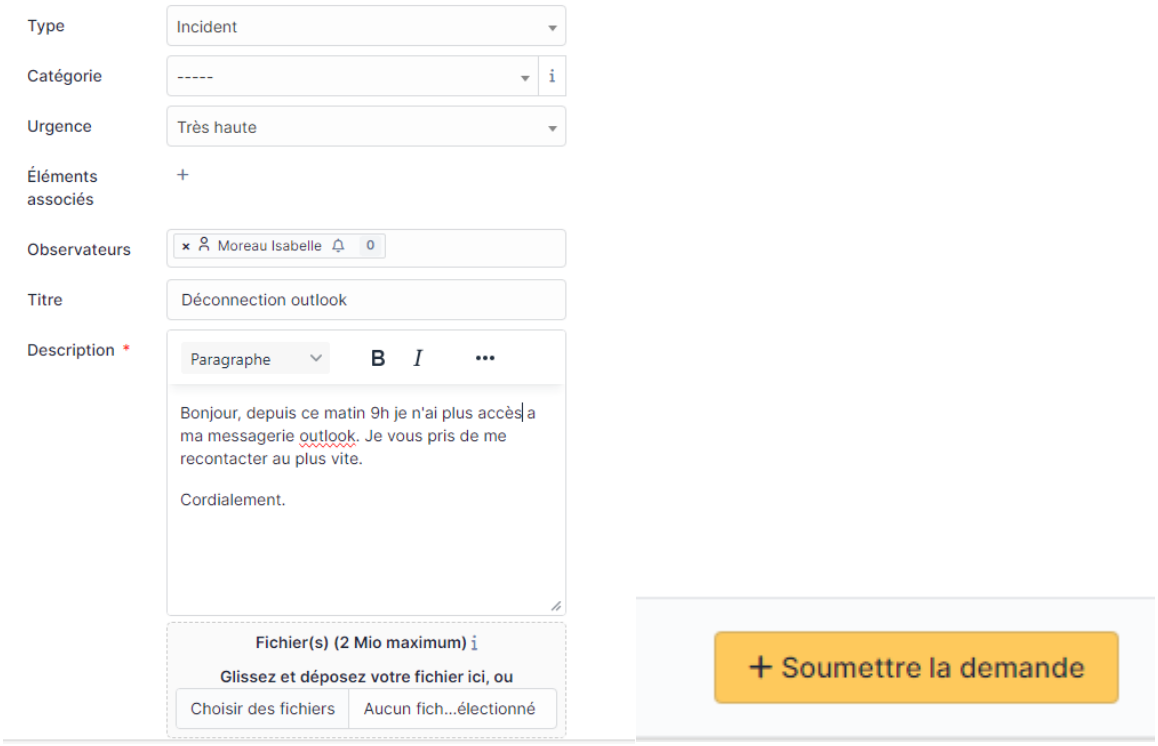
Nous allons nous connecter sur le compte glpi de la cliente et créer un ticket de demande support en passant par le raccourcie préalablement appliqué sur le bureau du poste de la cliente.



On arrive sur le compte de la cliente

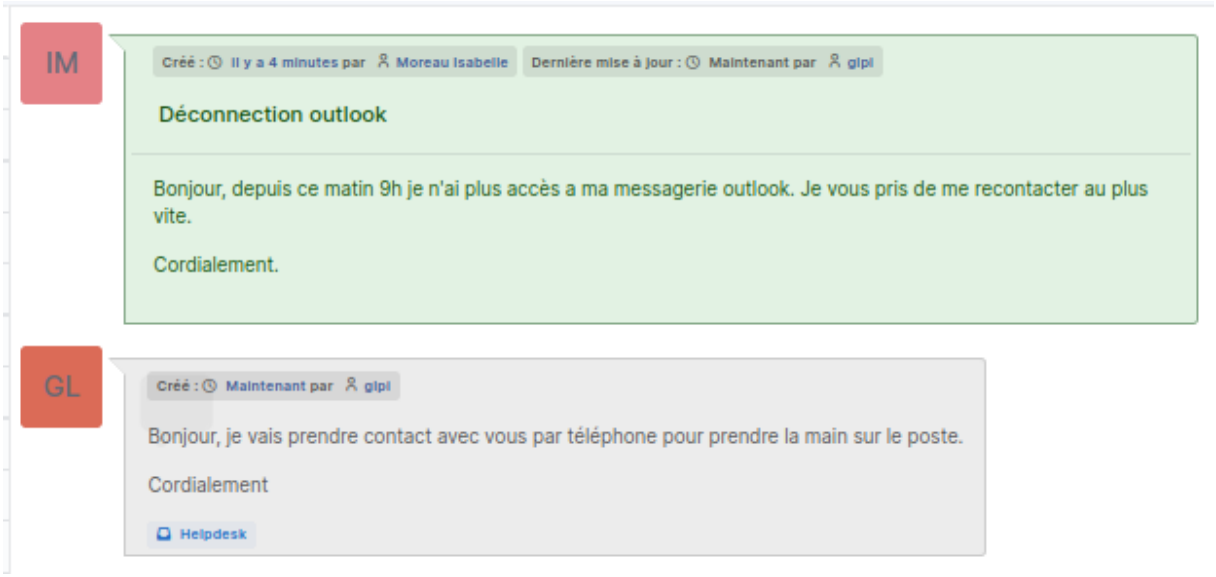


On crée un ticket



On se rend sur un compte administrateur

Nous avons un ticket



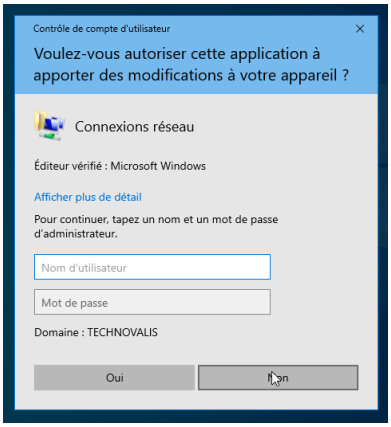
Nous pouvons voir que tout fonctionne correctement, nous pouvons facilement communiquer pour agir le plus rapidement possible pour ainsi débloquer la cliente.

5. Postes de travail collaborateurs

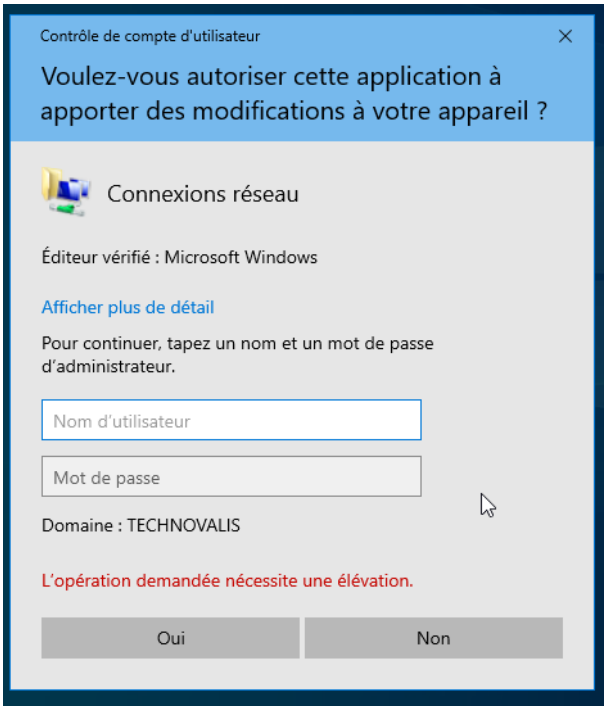
Nous allons nous rendre sur le poste de Sophie Marin pour faire les vérifications nécessaires

La cliente n'est pas administrateur, elle ne peut pas faire ce qu'elle veut sur son poste comme demandé.

Nous allons tenter de mettre le poste en ip fixe par exemple.



La cliente rentre ses identifiants de sessions



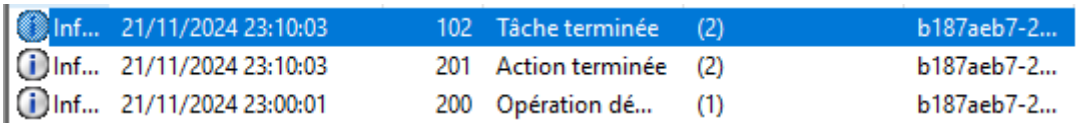
Elle ne peut pas, seule le compte technovalis ainsi que le compte de la Notaire de l'étude peuvent accéder à cette console, donc pour toutes les modifications sur le poste, la cliente devra faire la demande auprès de la notaire.

Bien sur c'est un exemple, une collaboratrice n'irait pas changer l'ip du pc, cependant nous ne pouvons écarter les potentiels erreurs de manipulations.

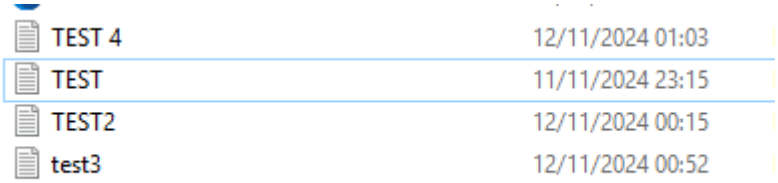
6. Sauvegarde cloud automatisée avec AWS et PowerShell

Pour ce test nous allons créer des fichiers test, lancer la tache planifiée manuellement et vérifier si ceux-ci apparaissent bien dans le bucket de sauvegarde de l'étude dans AWS.

Lorsque l'on arrive dans le planificateur de tache nous pouvons voir que la tache de 23h s'est bien appliquée

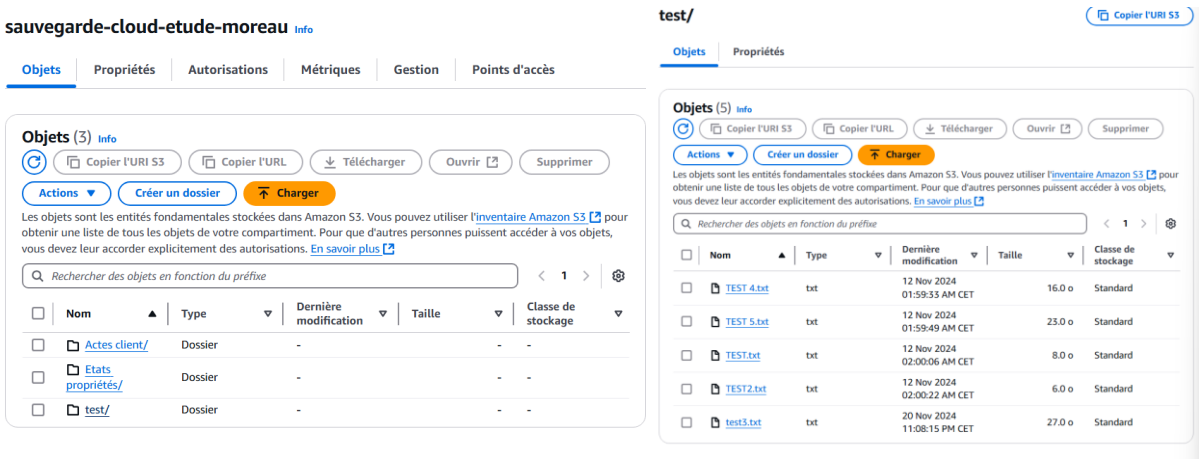


Nous allons essayer avec des fichier text test



On lance manuellement la tache

On se rend ensuite dans AWS et nous pouvons observer dans le bucket de sauvegarde de l'étude que les fichiers sont bien sauvegardés dans le cloud



Nous pouvons remarquer que les sauvegarde sont incrémentielles.

Ainsi, la sauvegarde quotidienne fonctionne sans soucis et sont bien envoyé tout les soir a 23h dans le cloud pour ne pas générer la production.

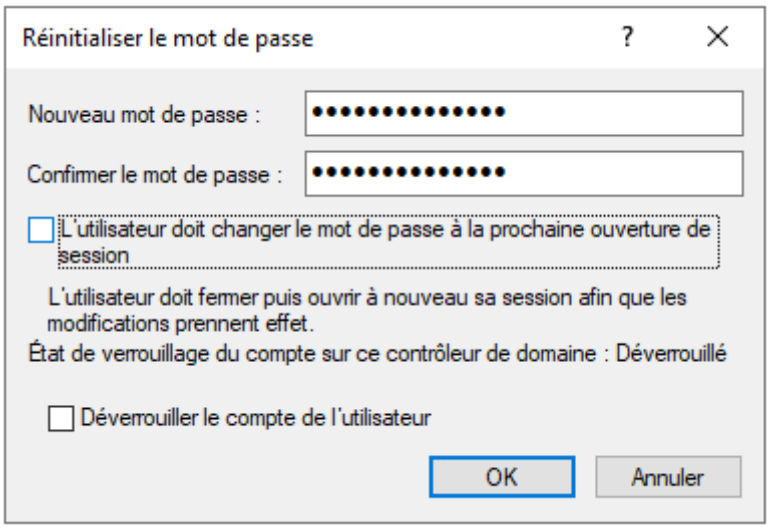
7. Redondance Active Directory et DNS

En premier lieu nous allons éteindre le serveur principal et voir si le serveur secondaire prend le relais.

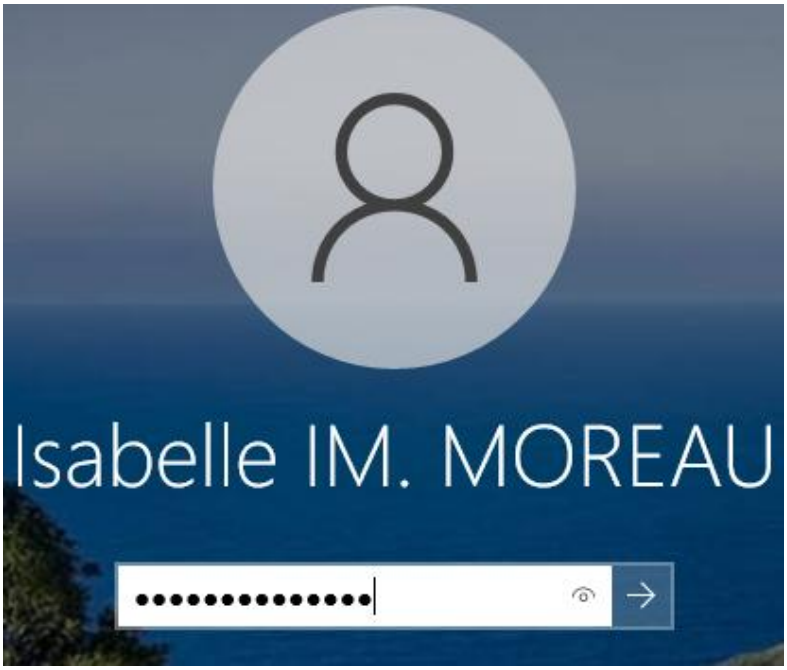
```
C:\Users\i.moreau>nslookup technovalis.local 192.168.2.6
Serveur :   SRVBACKUP.technovalis.local
Address:  192.168.2.6

Nom :    technovalis.local
Addresses:  192.168.2.4
          192.168.2.6
```

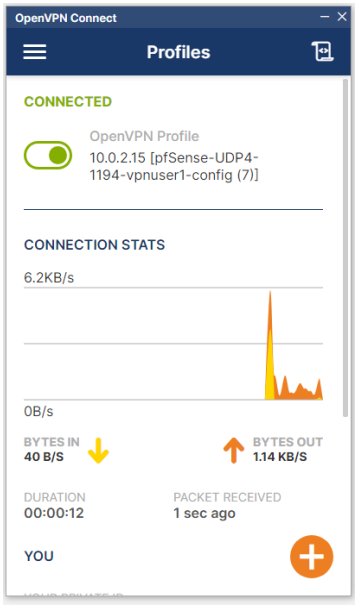
Il prend bien le relai, maintenant nous allons tenter la modification des identifiant d'un utilisateur.



Les identifications utilisateur ont bien été modifiés



8. VPN Sécurisé avec OpenVPN



On arrive bien à se connecter à notre server VPN.

9. Système de Détection d'Intrusion (IDS/IPS)

2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_sip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_sip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_sip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_sip) Method is unknown

Notre système de détection d'intrusion fonctionne correctement, des alertes commencent à remonter

9.2. Analyse du Trafic avec Wireshark

Analyse du Trafic avec Wireshark

Je lance wireshark sur l'interface Ethernet puis je tente de faire un ping depuis une autre machine.

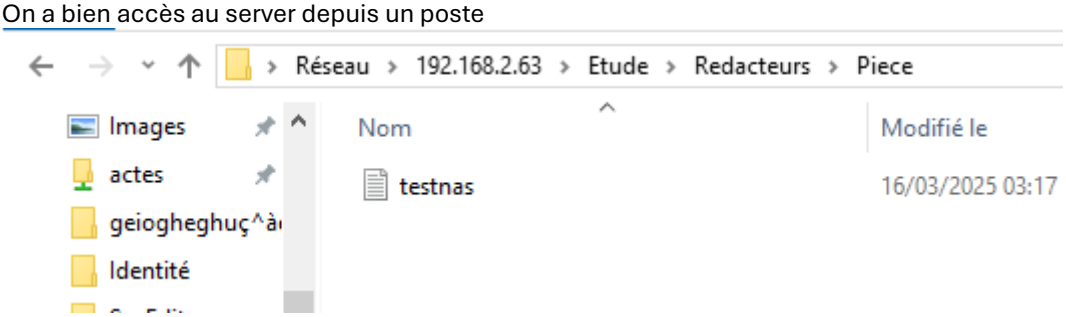
La trame icmp du ping remonte bien.

```
└  68 8.190140    192.168.2.50    192.168.2.4    ICMP    101 Destination unreachable (Port unreachable)
```

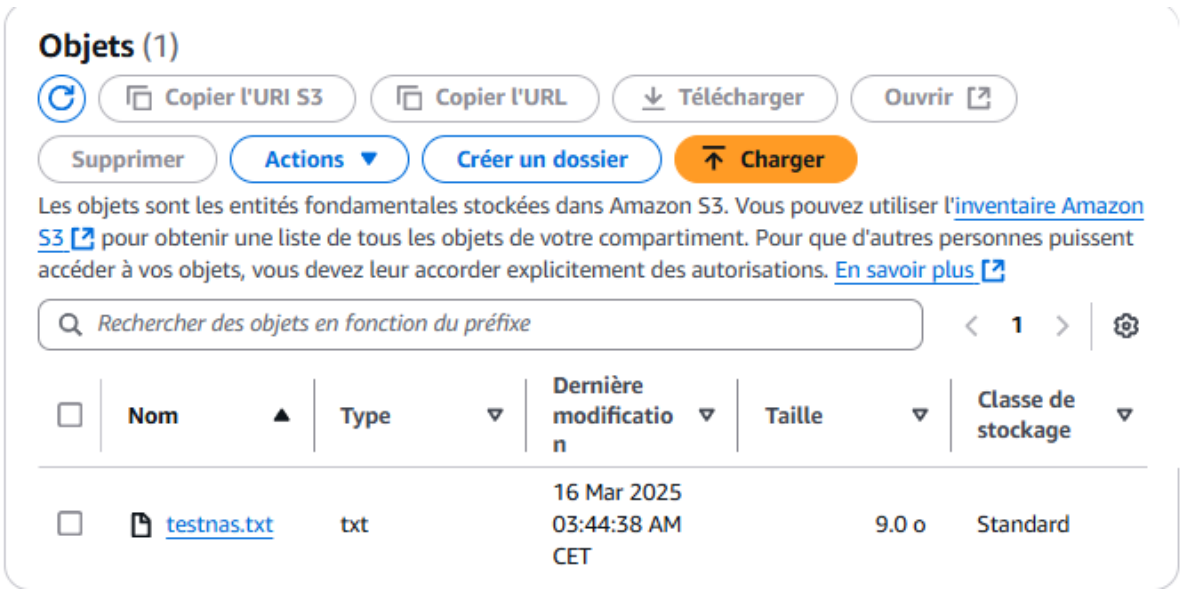
10. Infrastructure NAS avec TrueNAS

Je test sur un poste client l'accès au nas depuis l'explorateur de fichier

On a bien accès au server depuis un poste



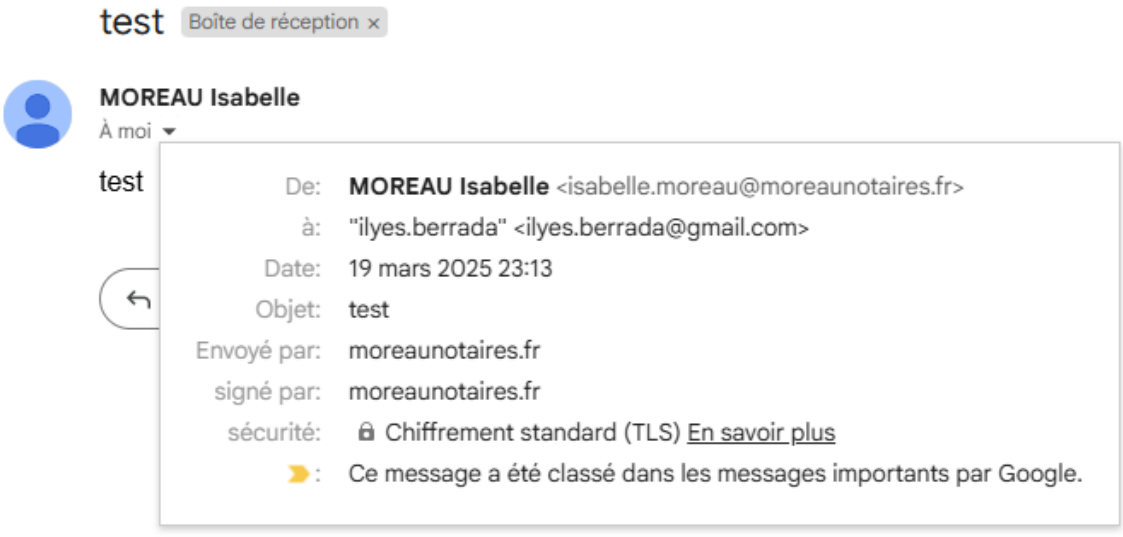
De plus la sauvegarde cloud du serveur de stockage se fait bien comme le montre la console AWS



11. Messagerie d’entreprise

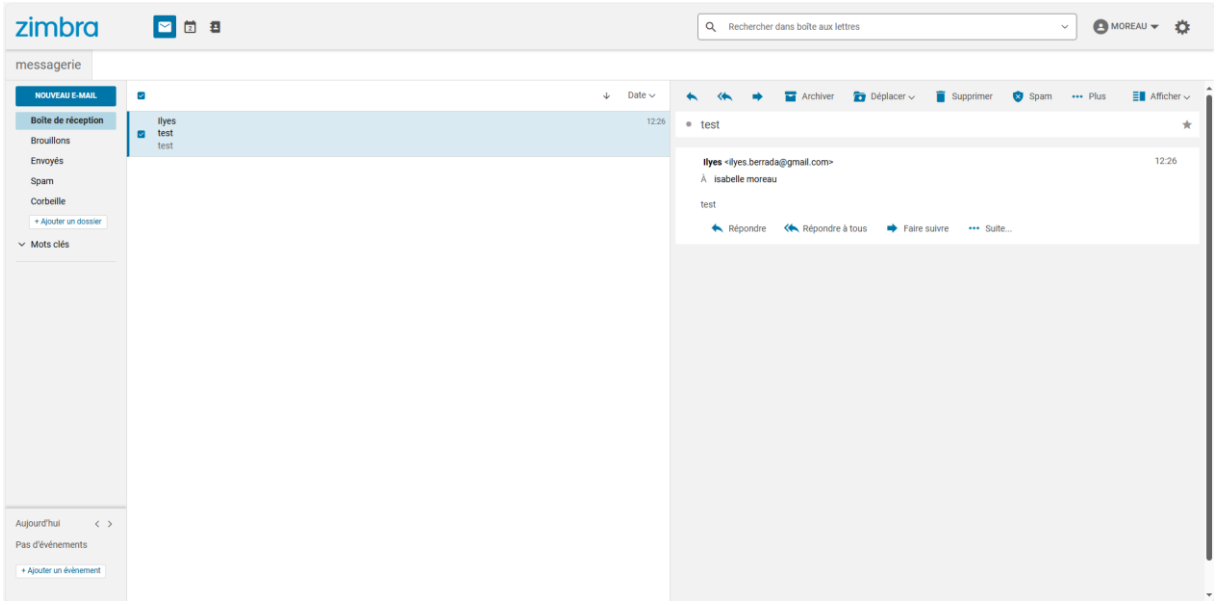
La cliente se rendre sus zimbra pour pouvoir s’y connecter

Une fois ici on va se connecter et simplement faire un test d’envoi réception vers une adresse gmail, plus précisément la mienne



Nous pouvons voir que l’envoi de mail fonctionne bien.

Ainsi que la réception.


zimbra
Rechercher dans boîte aux lettres
MOREAU
messagerie
NOUVEAU E-MAIL
Boîte de réception
Brouillons
Envoyés
Spam
Corbeille
+ Ajouter un dossier
Mots clés
Aujourd'hui
Pas d'événements
+ Ajouter un évènement
Date
Archiver
Déplacer
Supprimer
Spam
Plus
Afficher
Ilyes
test
test
12:26
test
Ilyes <ilyes.berrada@gmail.com>
12:26
À isabelle moreau
test
Répondre
Répondre à tous
Faire suivre
Suite...