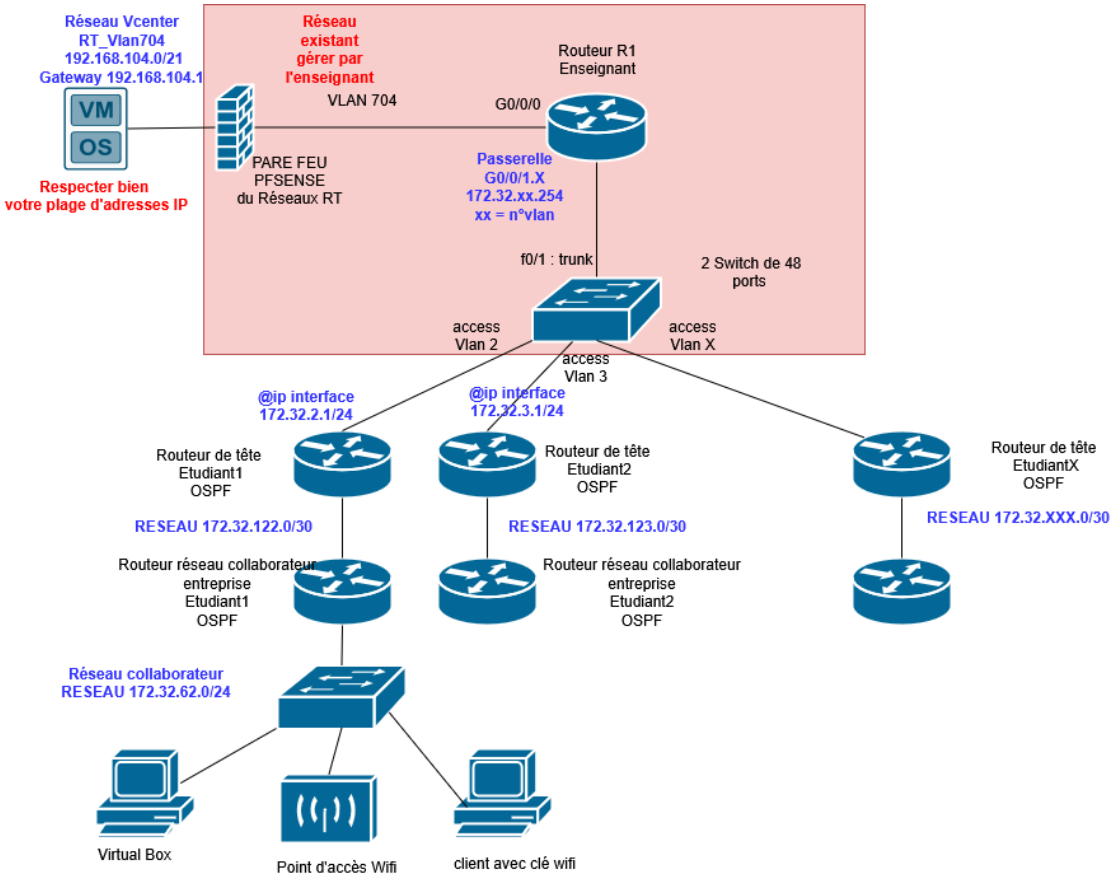
SAE3.CYBER.03



Jordão Mbambu

Table des matières

Contexte

Mon responsable administration réseaux, me demande de concevoir et tester un nouveau réseau permettant d'accéder aux services et aux ressources de l'entreprise.

Les services réseaux de l'entreprise fonctionnent encore sur des Windows serveur 2008 et sur des serveurs Linux Debian 7.

Il me demande de passer au minima, sur des serveurs Windows 2016 et Debian 11.

Planning initial

Planning SAE Cyber3	
Parties	**Nombre d'heures**
Virtualisation	1h
DNS	30min
Réseaux	2h
AD ou LDAP	30min
DHCP	30min
WiFi	2h
Radius	1h
Web	30min
RDS	2h
Veille Techno	4h
Test + Corrections	2h
Total	16h

Apprentissages Critiques

– AC21.01 | Configurer et dépanner le routage dynamique dans un réseau (**OSPFv2**)

– AC21.03 | Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée (**Serveur AD Windows sur VSphere**)

– AC21.04 | Déployer des services réseaux avancés (**NPS et Radius**)

– AC22.02 | Mettre en place un accès distant sécurisé (**SSH, RDS**)

– AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau (**Zabbix, Grafana, Wazuh**)

– AC24.03Cyber | Sécuriser les services (**Mots de Passe)**

– AC24.06Cyber | Comprendre des documents techniques en anglais (**Lire la doc officielle des logiciels utilisé**)

Partie Virtualisation

Dans le cadre donné, j'ai choisi les versions Windows server 2022 et Debian 12 car sont l'une des dernières versions dans leurs systèmes respectifs, cela me permettra d'être à jour et sécurisé au niveau de failles logiciel**les**.

Ensuite je regardé VMware compatibility guide – Guest OS (https://compatibilityguide.broadcom.com/search?program=software&persona=live&column=osVendors&order=asc) pour installer mes machines de la façon la plus propre.

VirtualHardware Storage Networking Confidential ComputingVMwareTools Customization

Features	Release	VMware Product
Hide	ESXi 9.0	ESXi

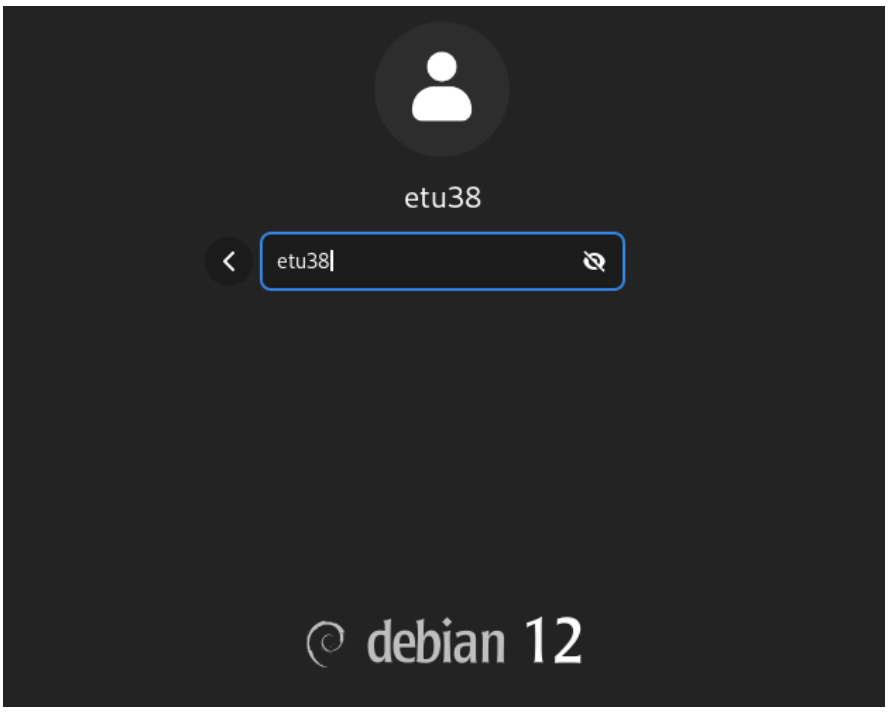
Category	Features	Features Support	Description
Storage	BusLogic	Not Supported	Virtual BusLogic Parallel SCSI adapter
	IDE	Supported	Virtual IDE adapter for ATA disks
	NVMe	Supported	NVM Express Adapter
	SATA	Supported	Virtual SATA adapter
	VMware Paravirtual	Supported(Recommended)	VMware Paravirtual SCSI (PVSCSI) adapter
	LSI Logic SAS	Supported	Virtual LSI Logic SAS adapter
	LSI Logic	Supported	Virtual LSI Logic Parallel SCSI adapter
Virtual Hardware	Hot Add vCPU	Supported	Ability to add a virtual CPU to a running virtual machine with zero downtime
	Hot Add Memory	Supported	Ability to add memory to a running virtual machine with zero downtime
	SMP	Supported	Virtual Symmetric Multiprocessing
Customization	Guest Customization	Supported	Customize the guest operating system of a virtual machine
VMware Tools	open-vm-tools	Supported(Recommended)	Operating System provides open-vm-tools
Networking	e1000e	Supported	Emulated Intel 82574L Gigabit Ethernet Controller
	VMXNET 3	Supported(Recommended)	Third generation VMware virtual NIC

Maintenant que j'ai les recommandation , j'ai ensuite crée mes machines virtuelles :

Ex : SAE3_CYBER3_Etu8_SW22

Provisioning type	Create a new virtual machine
Virtual machine name	SAE3_CYBER3_Etu38_SW22
Folder	Etudiant_38
Host	esx8.lan.rt
Datastore	SAE_38
Guest OS name	Microsoft Windows Server 2016 or later (64-bit)
Virtualization Based Security	Disabled
CPUs	2
Memory	4 GB
NICs	1
NIC 1 network	RT_VLAN704
NIC 1 type	VMXNET 3
SCSI controller 1	VMware Paravirtual
Create hard disk 1	New virtual disk
Capacity	40 GB
Datastore	SAE_38

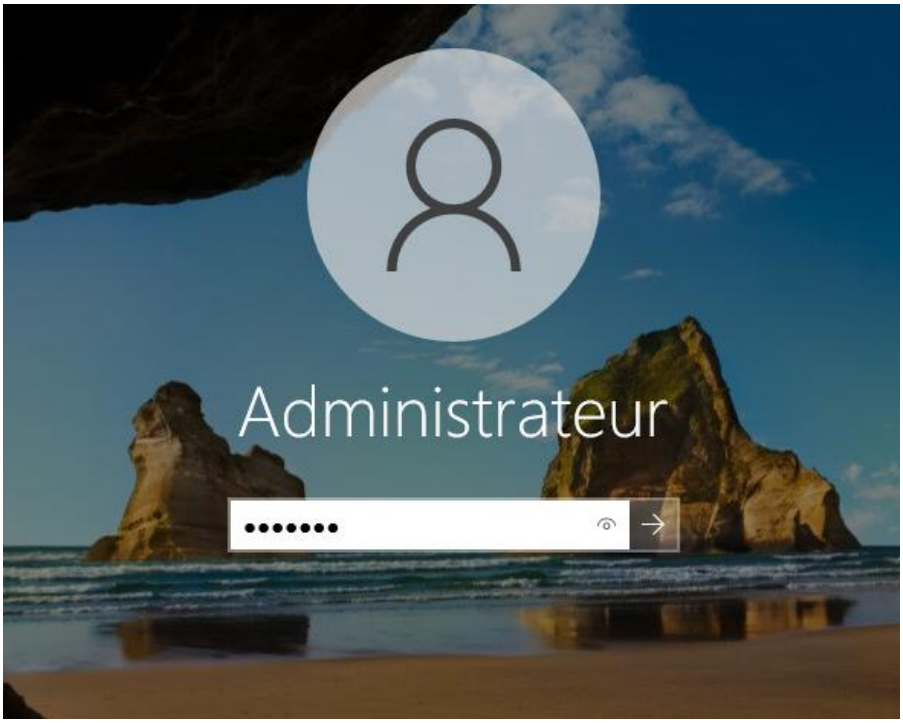
Vérification de l'installation et configuration réseau :



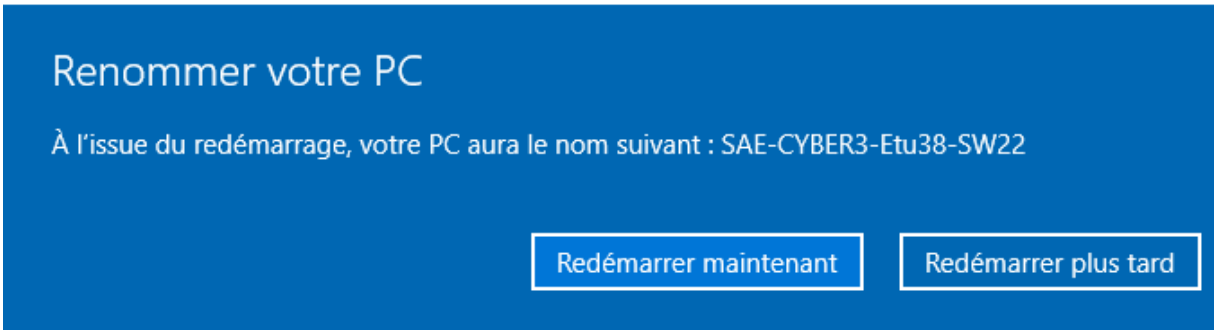
```
etu38@SAE3-CYBER3-Etu38-Deb:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:91:37:89 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 192.168.108.185/21 scope global ens192
       valid_lft forever preferred_lft forever
etu38@SAE3-CYBER3-Etu38-Deb:~$ cat /etc/resolv.conf
nameserver 10.250.250.12
nameserver 10.250.250.5
etu38@SAE3-CYBER3-Etu38-Deb:~$ ip route
default via 192.168.104.1 dev ens192
192.168.104.0/21 dev ens192 proto kernel scope link src 192.168.108.185
```

Changement du nom de l'hôte windows (SAE-CYBER3-Etu38-SW22)

Cette configuration a une limite des caractères , c'est la raison pour laquelle j'ai mis SAE au lieu de SAE3



Renommer votre PC



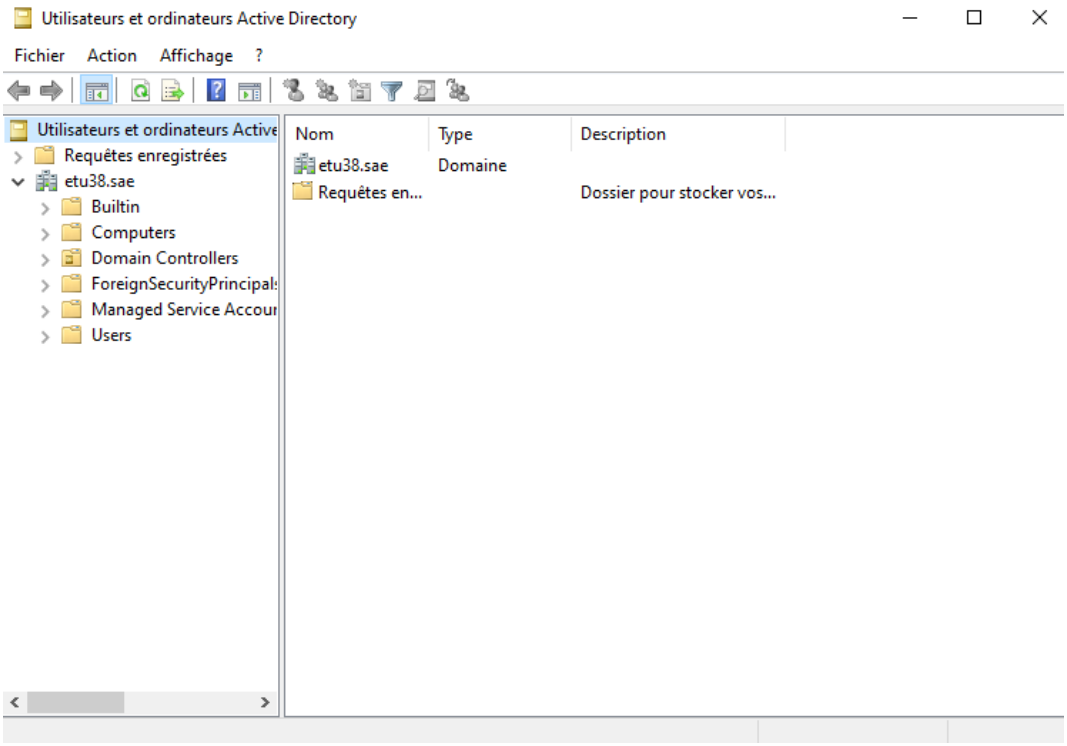

```
C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . : WIN-02E7AS198VO
   Suffixe DNS principal . . . . . . . :
   Type de noeud. . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . : Non

Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Adaptateur Ethernet vmxnet3
   Adresse physique . . . . . . . . . . . : 00-50-56-91-A4-90
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::1cf5:ebb:5083:a31b%15(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.108.186(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.248.0
   Passerelle par défaut. . . . . . . . . : 192.168.104.1
   IAID DHCPv6 . . . . . . . . . . . : 100683862
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-30-9A-B5-23-00-50-56-91-A4-90
   Serveurs DNS. . .  . . . . . . . . . : 10.250.250.12
                                 10.250.250.5
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

C:\Users\Administrateur>
```

Partie AD + DNS

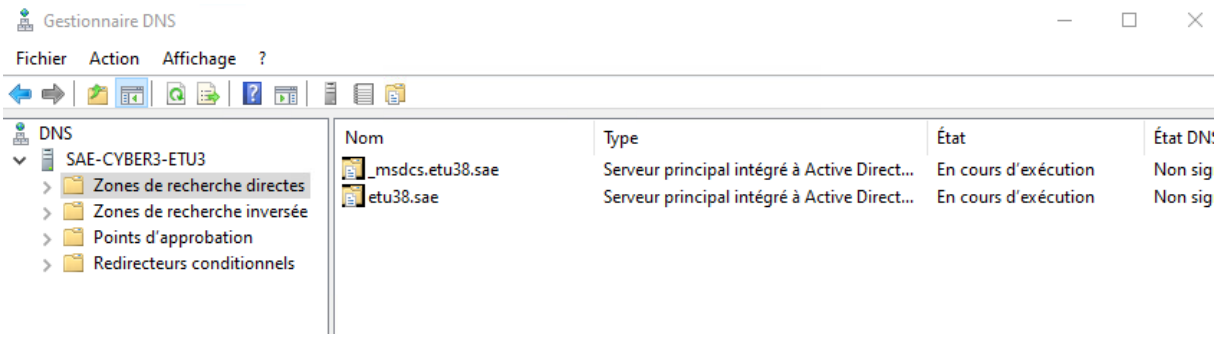
D'après le site https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/deploy/install-a-new-windows-server-2012-active-directory-forest--level-200-

Dès qu'on crée une nouvelle foret , il crée automatiquement le DNS , alors ce n'est pas nécessaire de créer le DNS avant

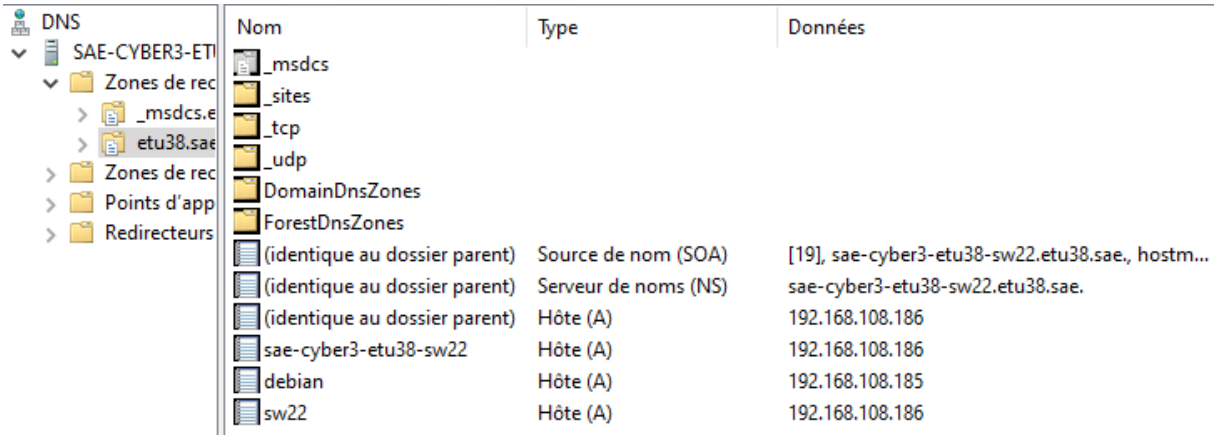
Ce site explique aussi la procédure pour créer une nouvelle forêt sur un active directory, je choisis etu38.sae comme nom de domaine



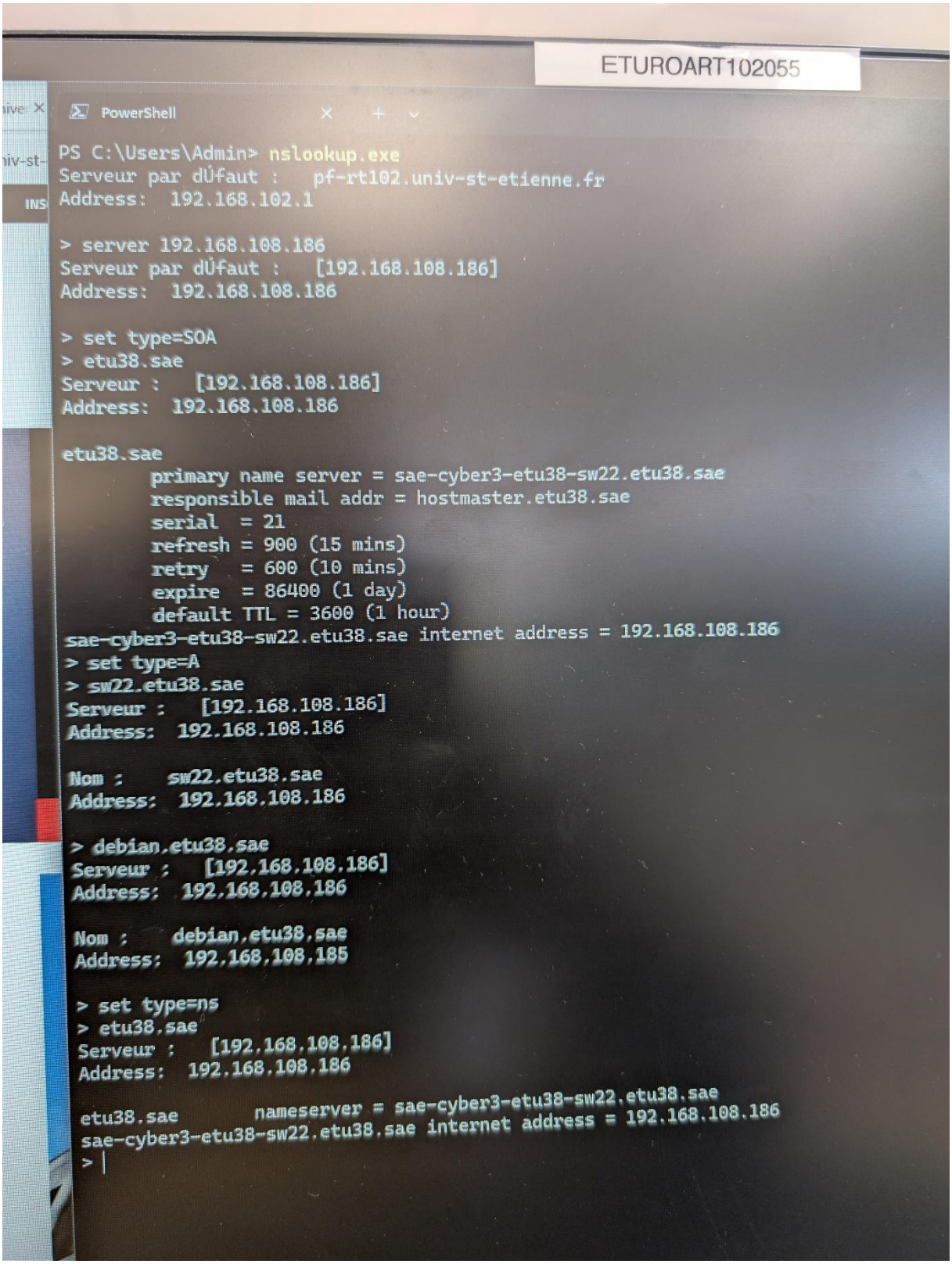
Je peux regarder maintenant le DNS qui a été créée :



J'ajoute des enregistrements A pour mes machines :



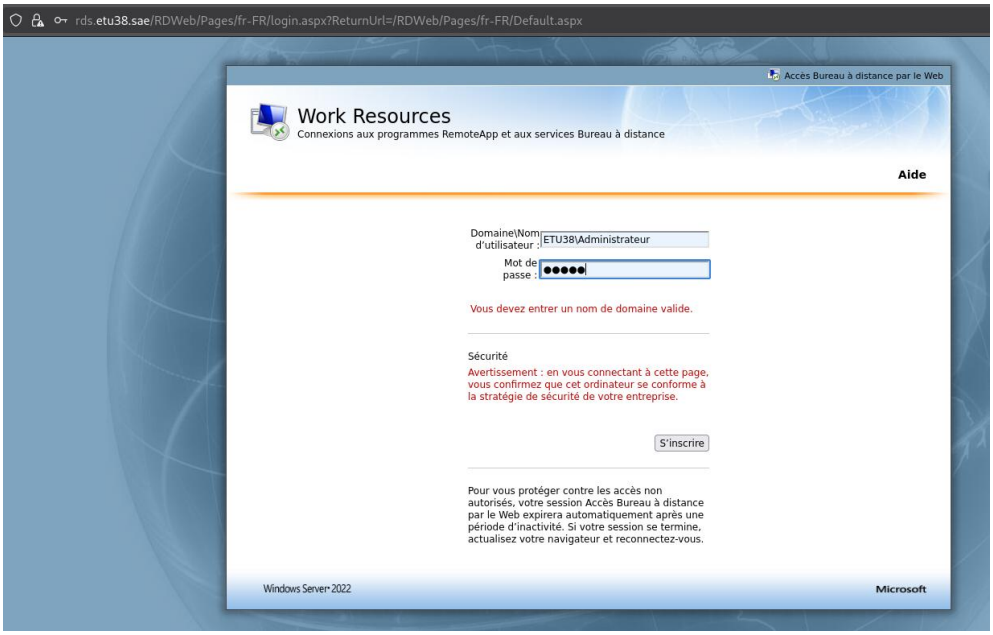
Je vérifie le bon fonctionnement du DNS ,dans un pc de l'IUT :

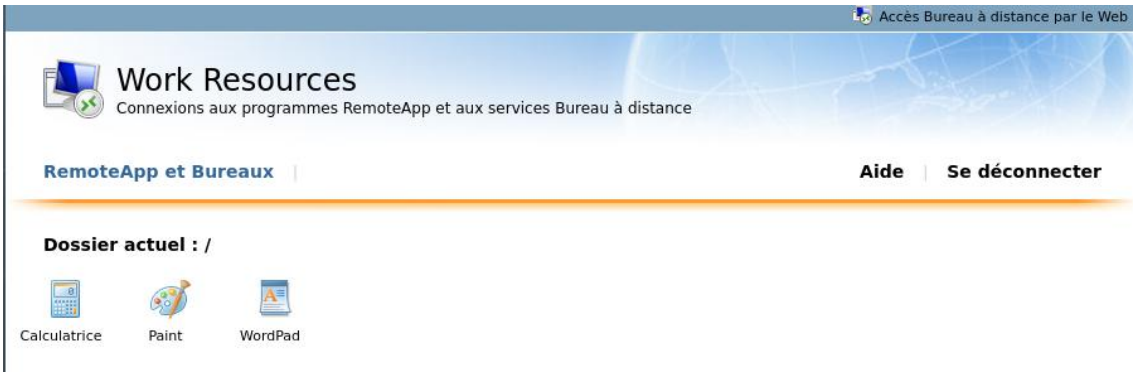


Partie RDS

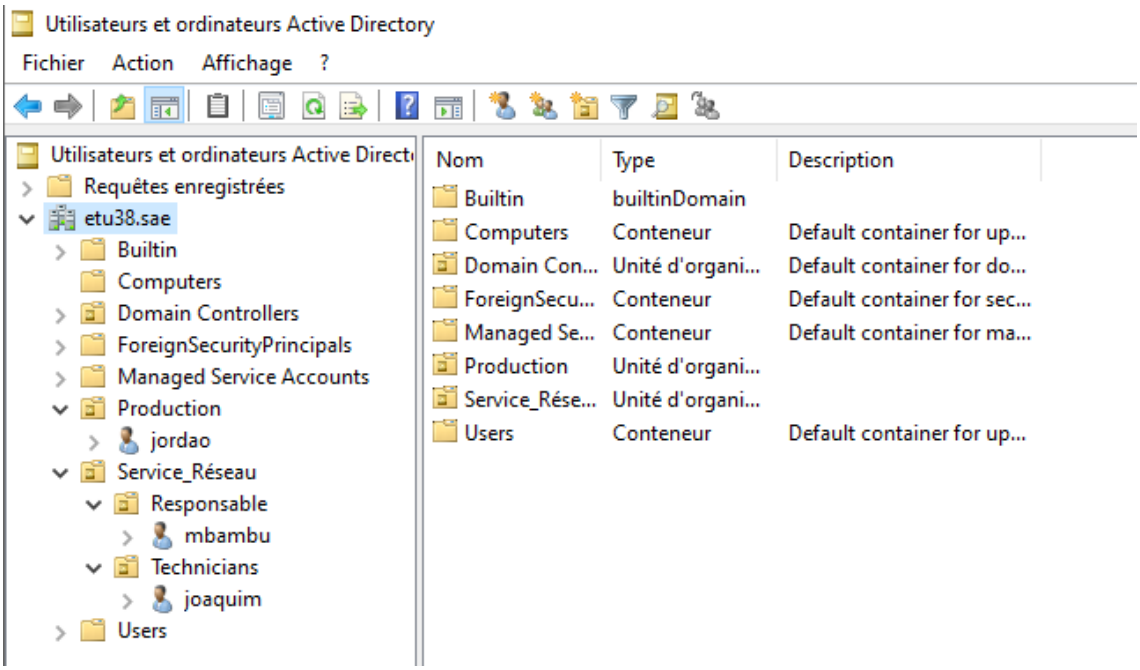
Pour installer le service RDS , j'ai suivi le tutoriel :

https://rdr-it.com/windows-serveur-2025-installer-le-role-adds-et-configurer-un-domaine-active-directory/

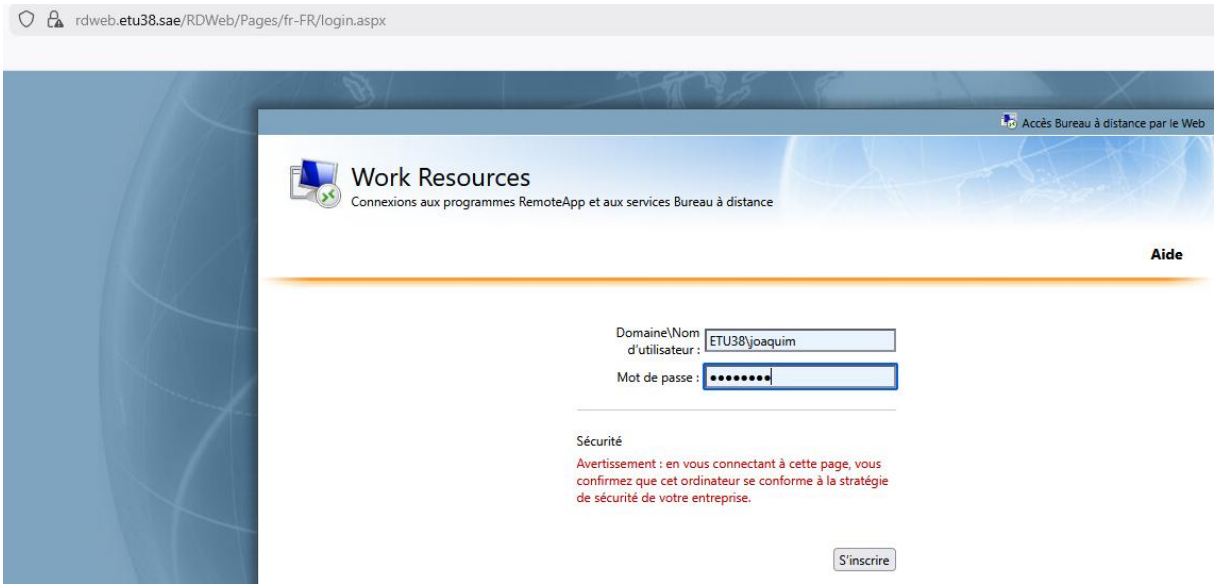


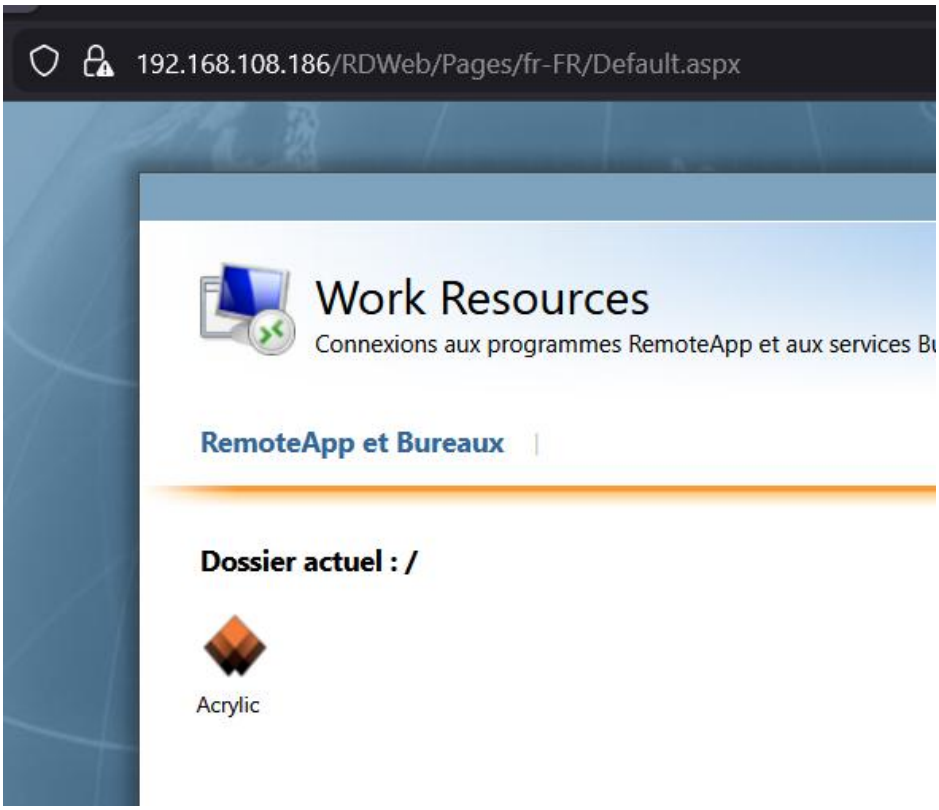


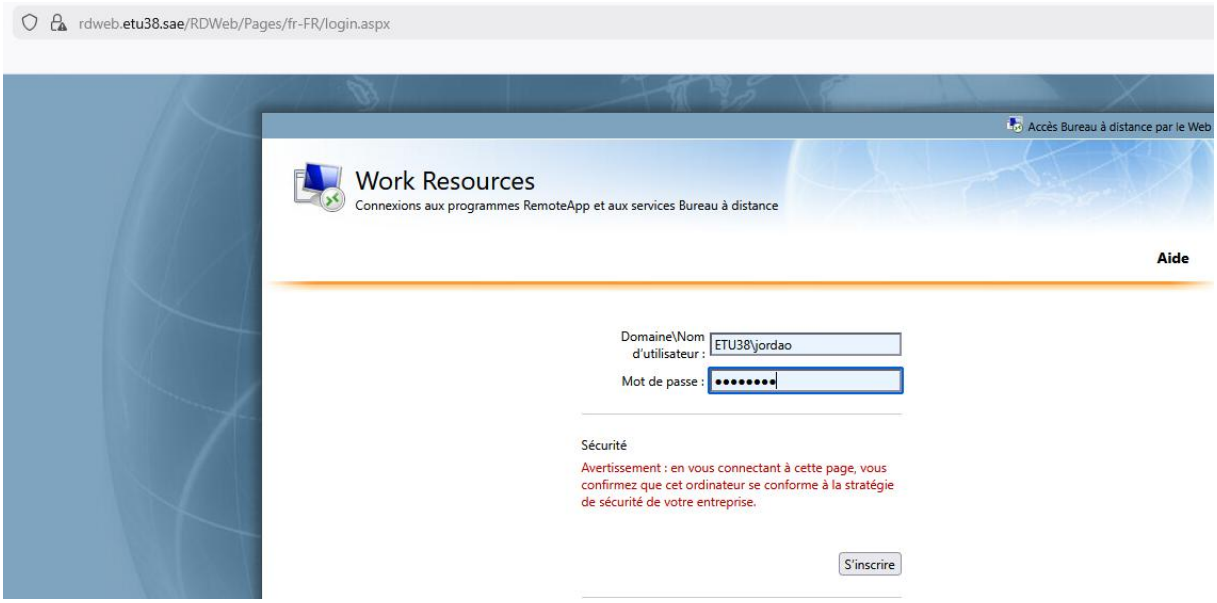
Création des OU et utilisateurs

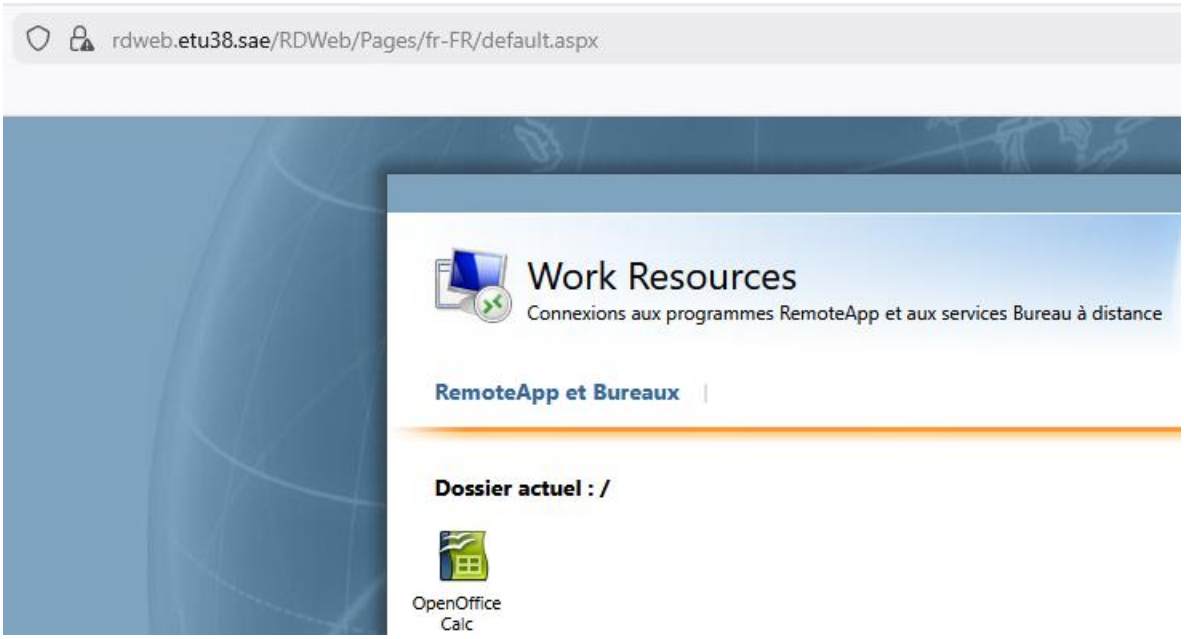


Ensuite j'ai mis en place les application demandées, acrylic pour les techniciens réseaux et Calc pour la Production respectivement




192.168.108.186/RDWeb/Pages/fr-FR/Default.aspx
Work Resources
Connexions aux programmes RemoteApp et aux services Bu
RemoteApp et Bureaux
Dossier actuel : /
Acrylic


rdweb.etu38.sae/RDWeb/Pages/fr-FR/login.aspx
Accès Bureau à distance par le Web
Work Resources
Connexions aux programmes RemoteApp et aux services Bureau à distance
Aide
Domaine\Nom d'utilisateur :
ETU38\jordao
Mot de passe :
Sécurité
Avertissement : en vous connectant à cette page, vous confirmez que cet ordinateur se conforme à la stratégie de sécurité de votre entreprise.
S'inscrire


rdweb.etu38.sae/RDWeb/Pages/fr-FR/default.aspx
Work Resources
Connexions aux programmes RemoteApp et aux services Bureau à distance
RemoteApp et Bureaux
Dossier actuel : /
OpenOffice Calc

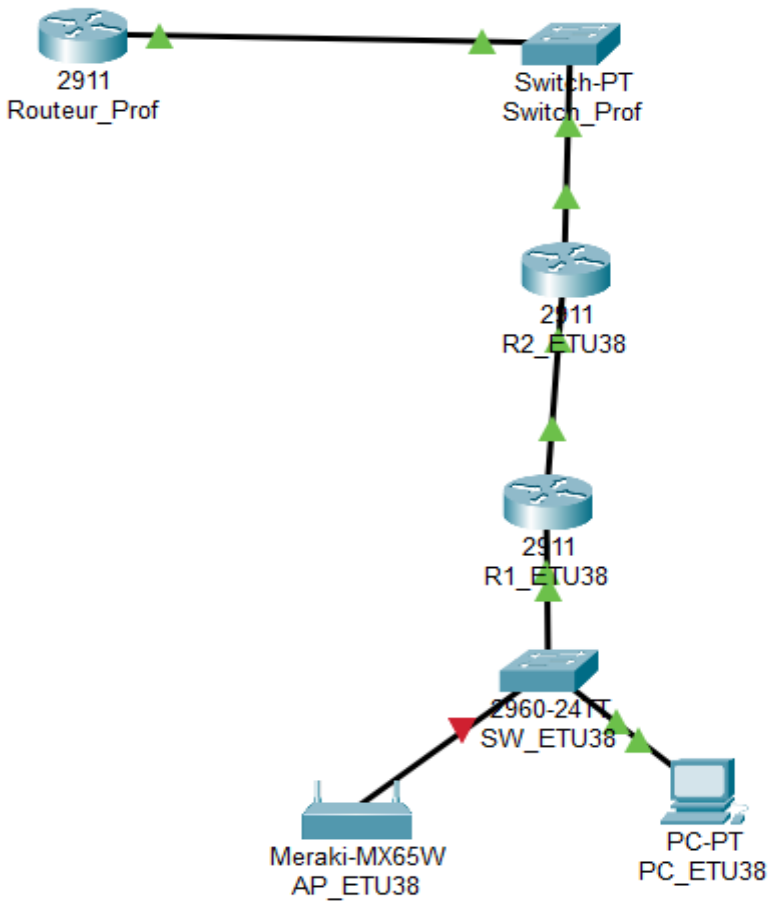
Partie Réseau + DHCP

J'ai réussi à configurer mon réseau avec **OSPv2** pour le routage dynamique, **SSH** comme protocole de contrôle à distance sécurisé, **DHCP** (sur le Switch) pour attribuer des addresses automatiques pour les machines presentes dans le réseau, surtout pour l'AP.

Pour isoler mon réseau des autres étudiants tout en restant connecté à la baie de virtualisation VMWare j'ai utilisé des **ACL** pour autoriser le traffic exterieur du routeur du prof et de l'internet, mais j'ai interdit tous les réseaux exterieures en 172.32.0.0/16 (notre supernetting)

Les commandes de configuration se trouvent dans le fichier **Partie_Réseaux+DHCP.md**

Après la configuration, les tests de communication avec Vcenter a été un succès.



Partie Wi-Fi

Tableau comparatif

Dans un premier temps j'ai dû faire le choix entre Ubiquiti UAP-AC-LITE et et Cisco Aironet 1702I, Pour cela je fais un tableau comparatif avec les avantages et inconvénients de chacun.

Tableau Comparatif

Critères	Ubiquiti UAP-AC-LITE	Cisco Aironet 1702I
STATUT SUPPORT 2025	✅ ACTIF / SUPPORTÉ	❌ FIN DE VIE (EOL)
Date de fin de support	Non annoncée (Toujours maintenu)	30 Avril 2024 (Plus de support)
Année de sortie	2015	2014
Sécurité Wi-Fi	WPA2 / WPA3 (via mise à jour)	WPA2 uniquement (Pas de WPA3)
Nombre d'antennes	2 × 2 MIMO	2 × 2 MIMO
Port Ethernet	1× Gigabit RJ45	1× Gigabit RJ45
Alimentation	PoE 24V passif (ou 802.3af sur versions récentes)	PoE 802.3af
Rayon de couverture	~110 m	~120 m
Contrôleur Wi-Fi (2025)	UniFi Network (v8+) : Moderne & Gratuit	Obsolète : Vieux WLC matériel ou VM requis
Licence	Aucune	Souvent nécessaire (MAJ/Fonctions)
Facilité d'administration	Très simple	Complexe (Expertise Cisco requise)
Fonctionnalités entreprise	Bonne	Excellente (mais datée)
Isolation client	Oui	Oui
ACL & trafic avancé	Basique	Très avancé
Intégration RADIUS	Oui	Oui
Support technique	Communautaire + docs	Inexistant (Fin du contrat TAC)
Prix du contrôleur	0€	Élevé (occas) ou complexe à virtualiser
Profil d'usage 2025	Prod (PME/ TPE / SOHO)	Lab

Le Cisco Aironet 1702I est en fin de vie , cela veut dire qu'à chaque nouvelle vulnérabilité lié à un protocole Wi-Fi on aura pas le droit à une correction ou update de la part de Cisco , contrairement à Ubiquiti qui rendra disponible tous les mises à jour de sécurité.

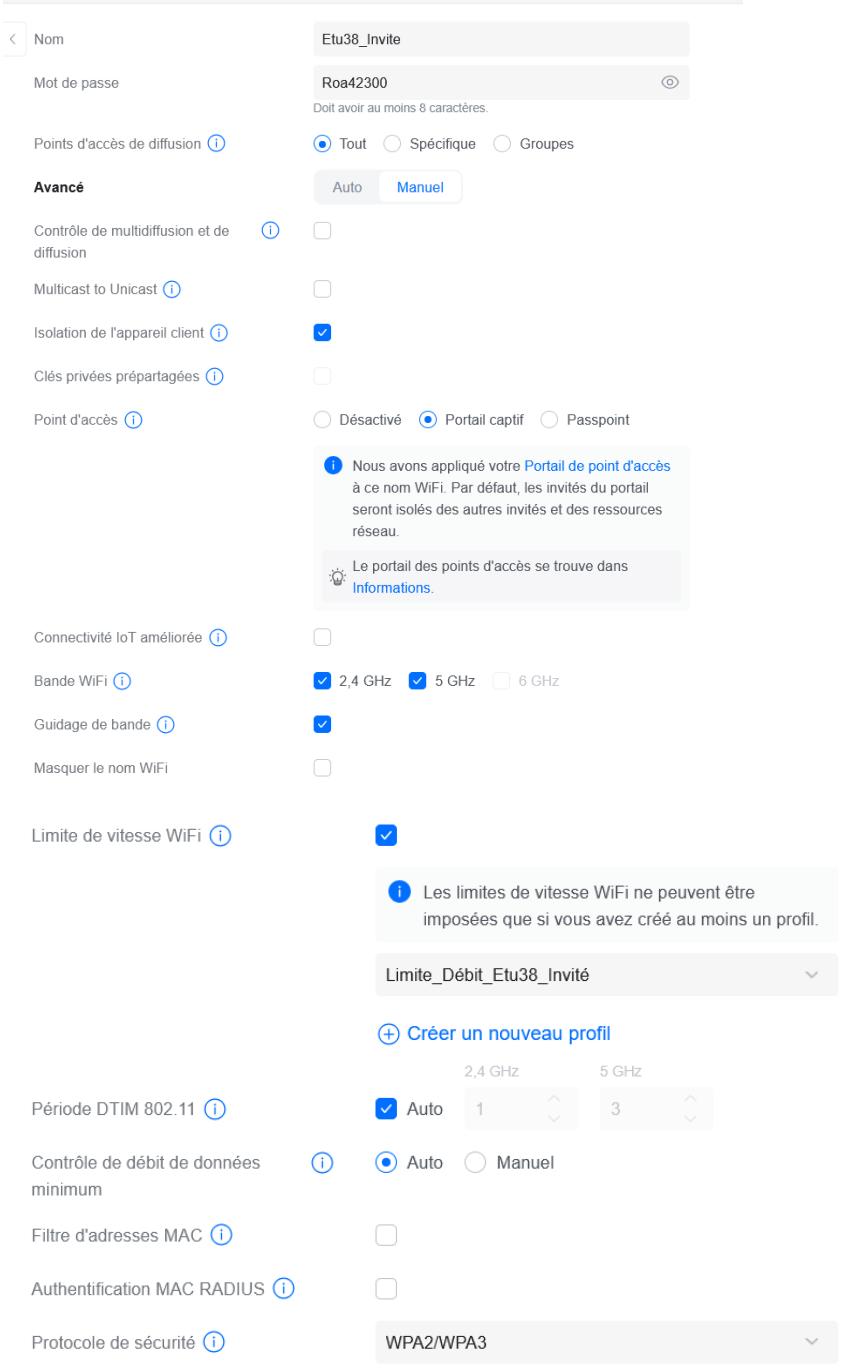
Le Cisco Aironet 1702I ne supporte le WPA3 , il ne fonctionne que sur le WPA2, donc, ça lui rend vulnerables à des attaques wifi comme « Pass-The-Hash » qui permettront à un attaquant de récuperer le hash et ensuite cracker le mot de passe.

C'est pour cette raison que j'ai choisi comme matériel « Ubiquiti UAP AC-LITE »

Wi-Fi Invité

J’ai crée un WI-FI invité, avec un portail captif et un mot de passe, en utilisant le protocole de sécurité **WPA2/WPA3**

En plus les clients connectés au WI-FI invité auront une limite de bande passante.



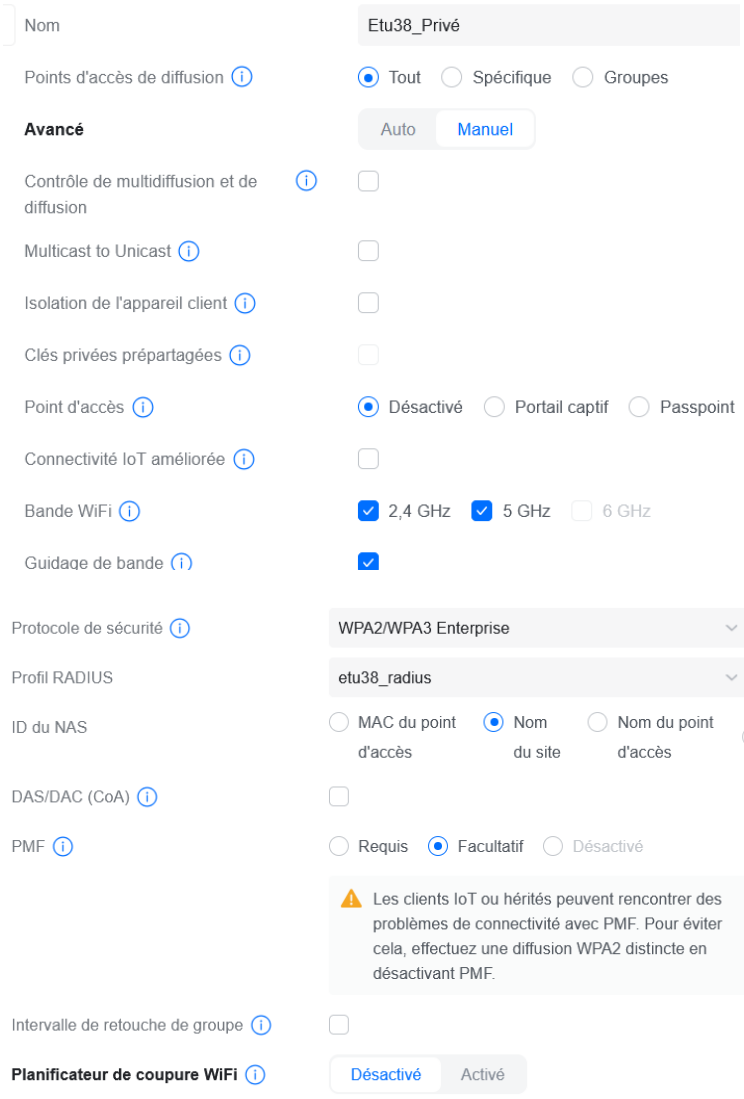
Limite de vitesse WiFi

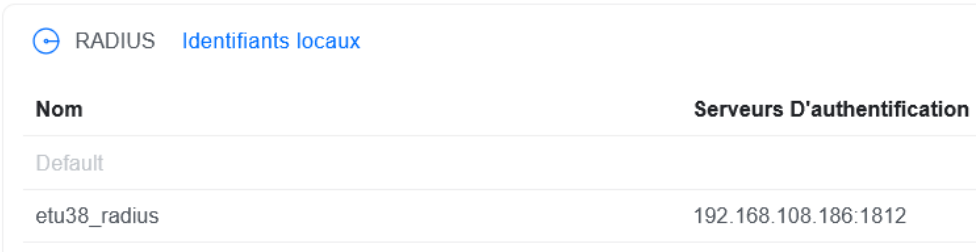
Nom	Limite De Bande Passante De Téléversement	Limite De Bande Passante De Téléchargement
Default	Illimité	Illimité
Limite_Débit_Etu38_Invité	↓ 100 Mbps	↑ 100 Mbps

Test

WI-FI Privé

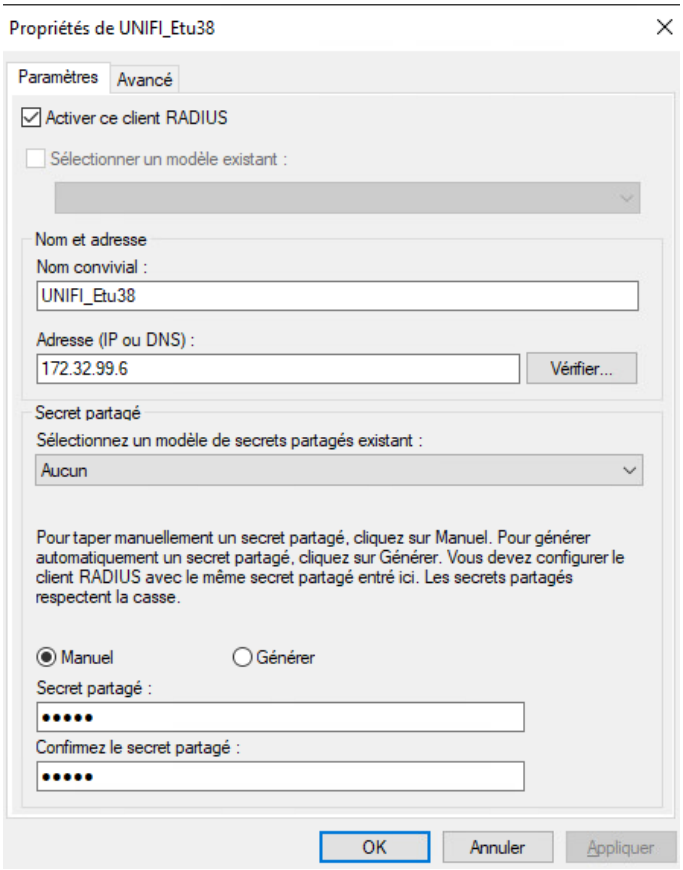
Pour le Wi-Fi privé, j'ai utilisé le protocole de sécurité WPA2/WPA3 Entreprise et un serveur radius pour l'authentification.

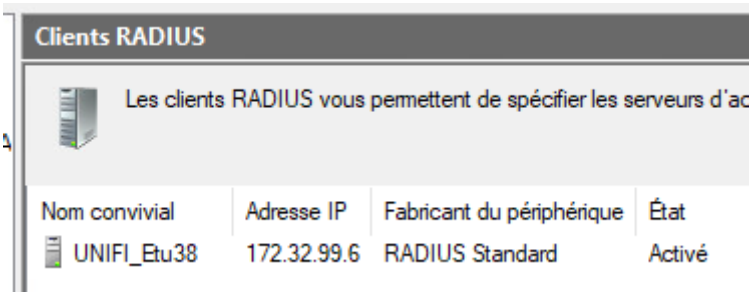




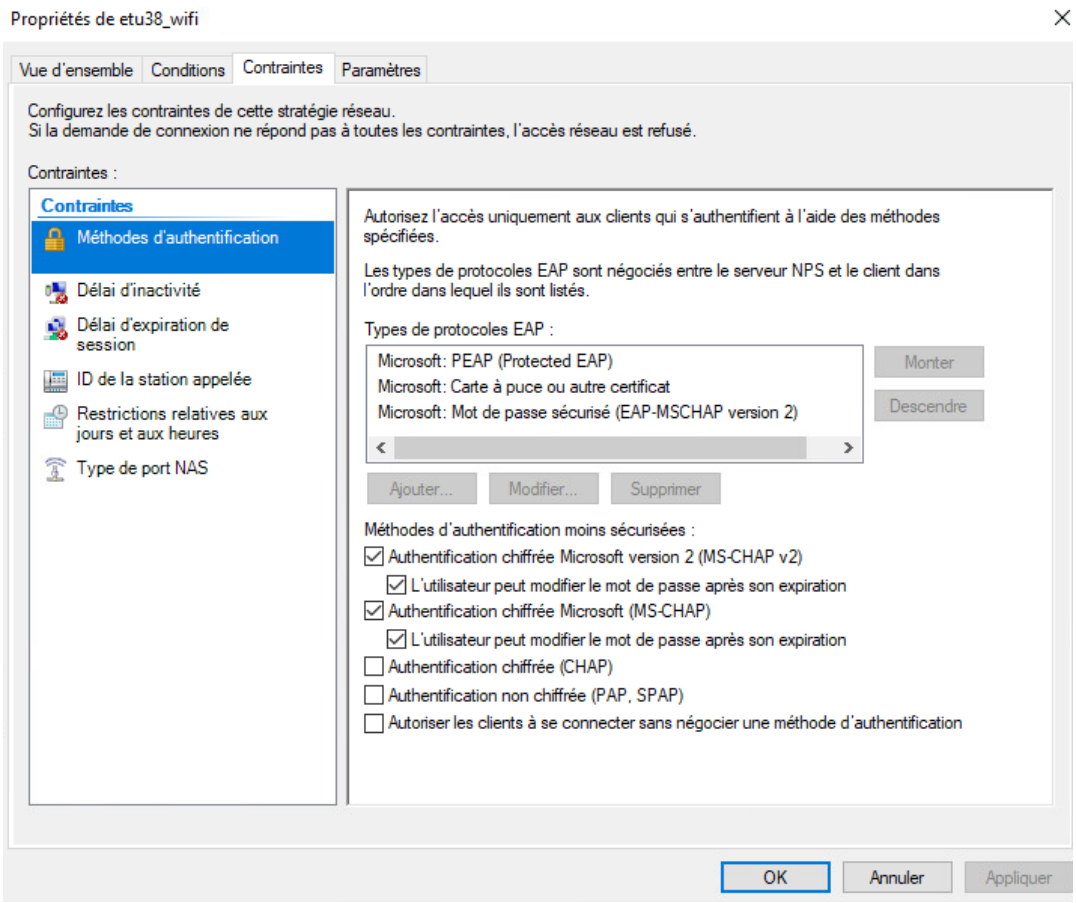
Partie Radius

On ajoute notre client radius dans le serveur NPS

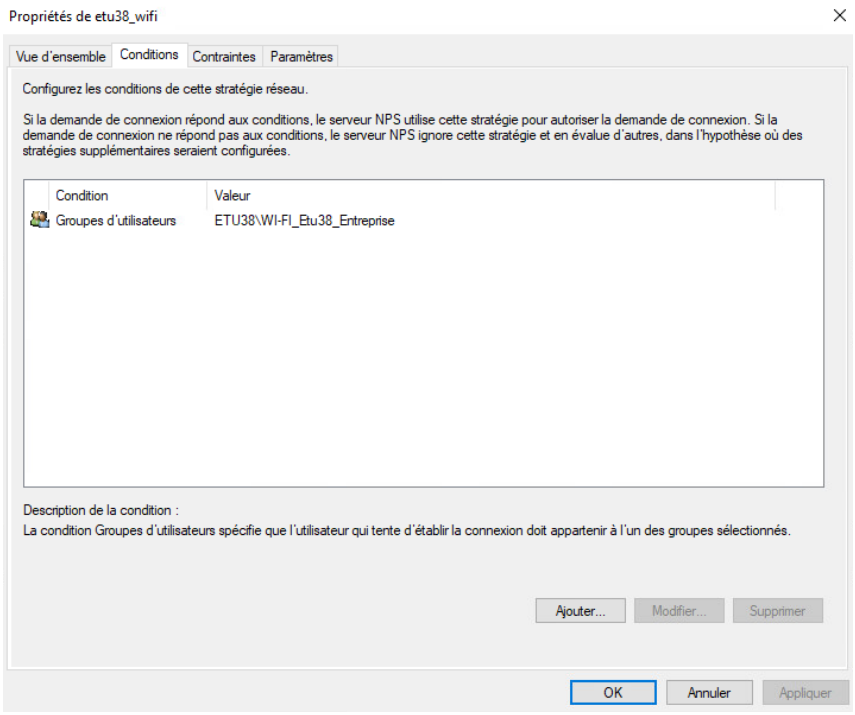




On ajoute une stratégie réseau dans notre serveur Radius pour autoriser les protocoles de connexion utilisés par le WI-FI.

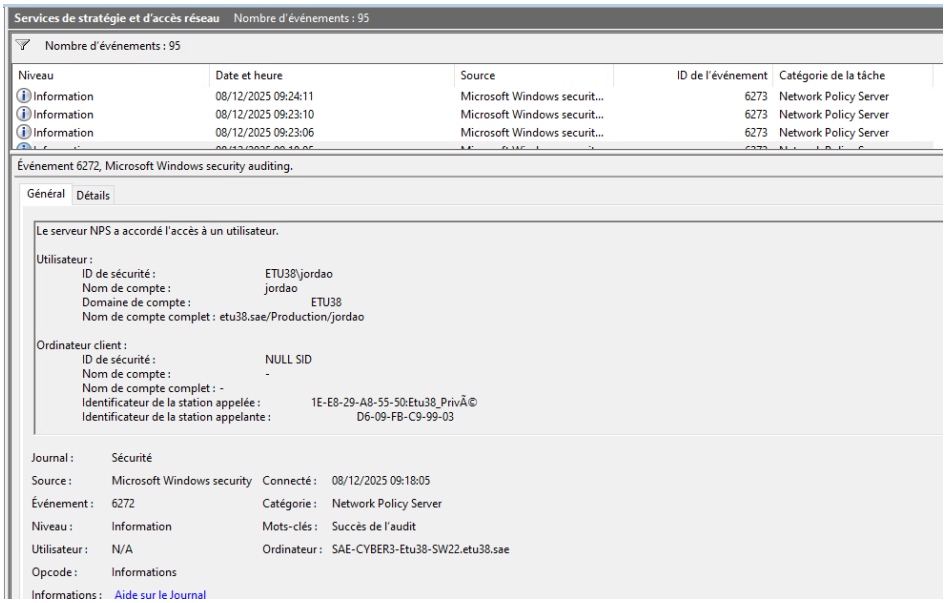


En plus de ça on ajoute aussi un groupe destiné pour la connexion WI-FI



Test

Maintenant on peut se connecter dans notre WI-FI privé , et vérifier que l'authentification au niveau du Radius a été un succès .

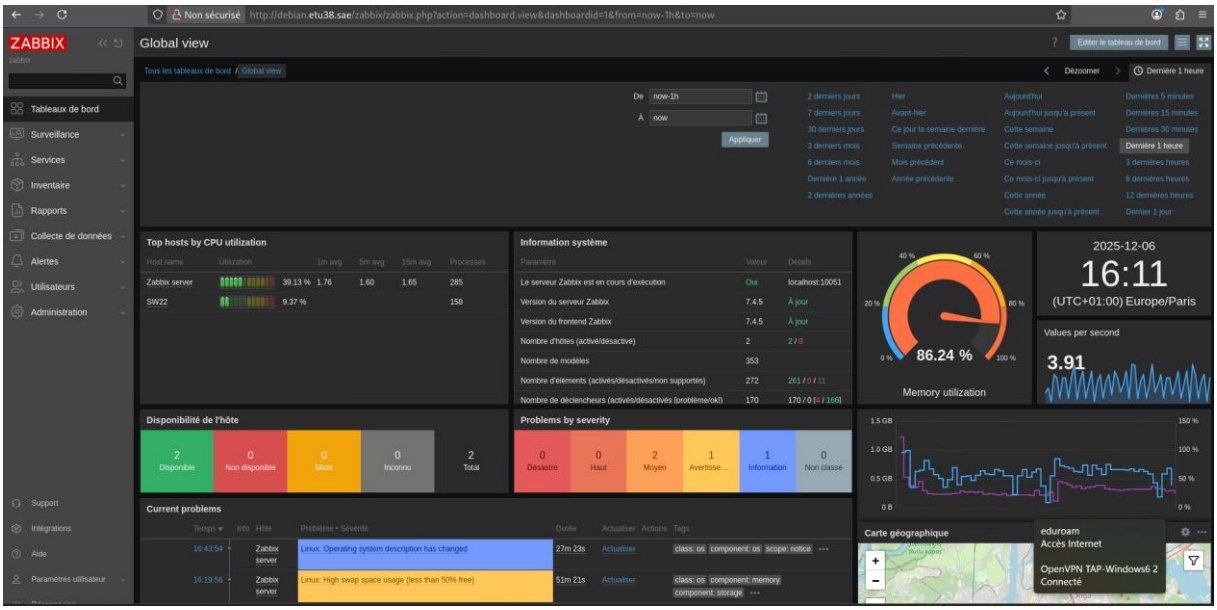


Veille Technologique

Zabbix

En suivant les instructions du site officiel de Zabbix j'ai installé Zabbix et j'ai monitoré les machines SW22 et Debian.

https://www.zabbix.com/download?zabbix=7.4&os_distribution=debian&os_version=12&components=server_frontend_agent&db=mysql&ws=apache



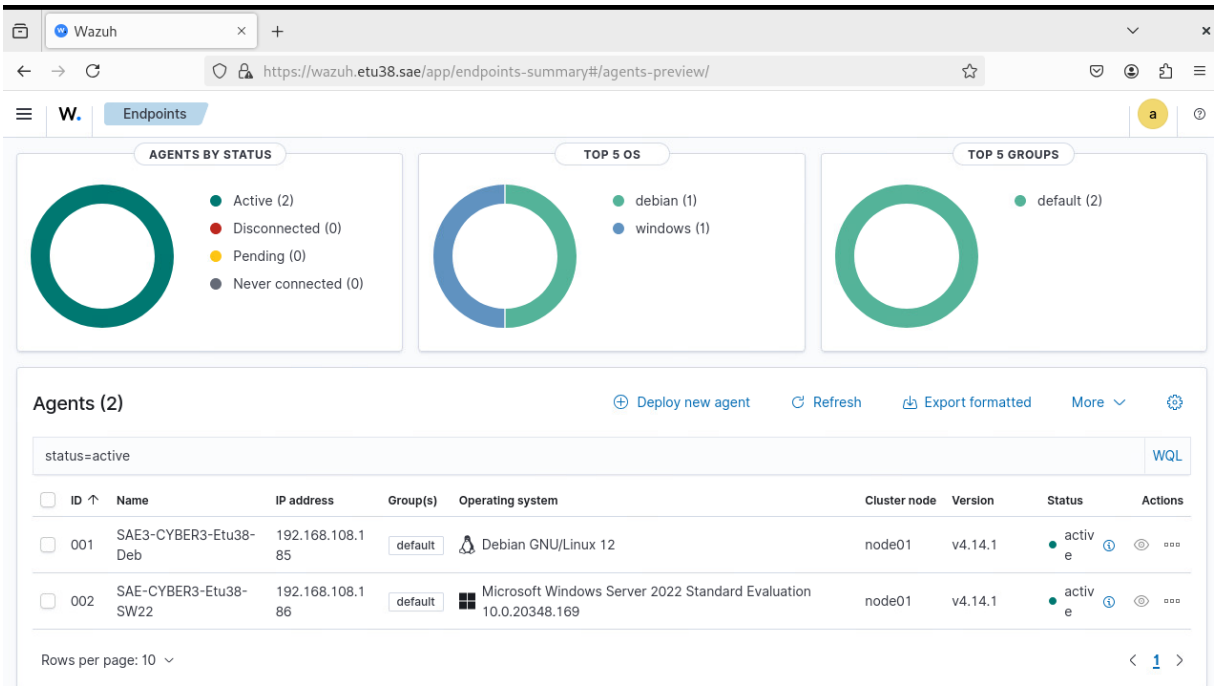
Grafana

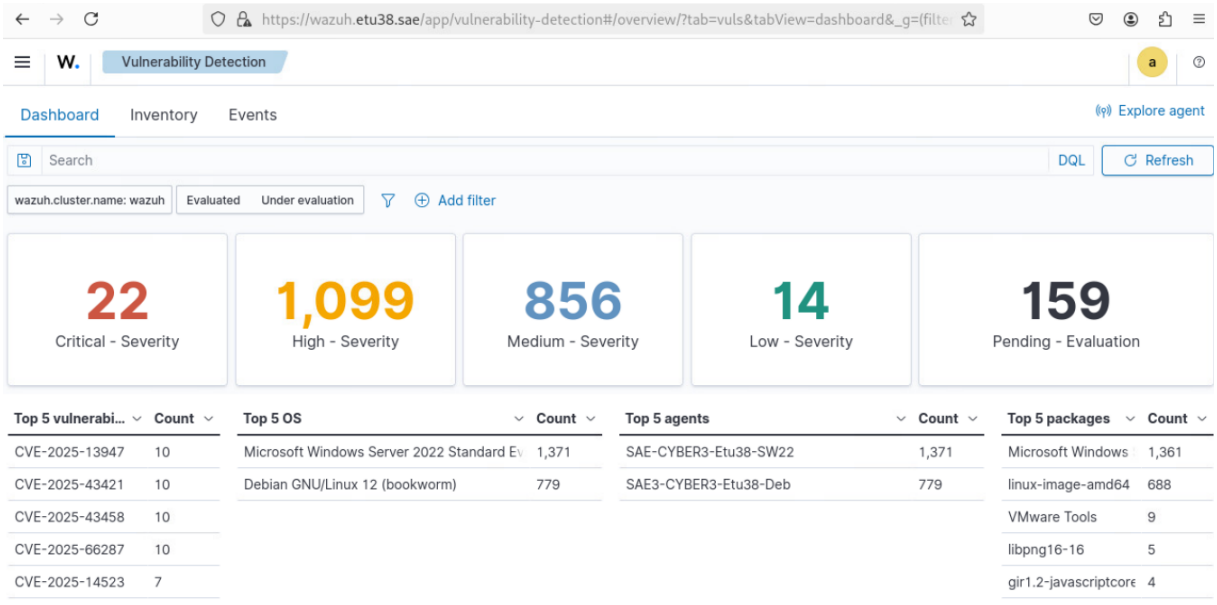
Pour améliorer l'affichage de ces données, j'ai installé grafana en suivant les orientations officielles de la documentation(https://grafana.com/docs/grafana/latest/setup-grafana/installation/debian/)

Prise d’initiative

Wazuh

Dans le but de sécuriser les infrastructures présentes, j’ai installé wazuh grâce aux consignes de la documentation officielle(https://documentation.wazuh.com/current/quickstart.html) ,pour la collecte de logs et recherche des vulnérabilités présentes dans nos serveurs installés.





Analyse Réflexive

AC24.02Cyber | Mettre en œuvre les outils fondamentaux de sécurisation d'une infrastructure du réseau

1. Avant l'action

Révision des notions de sécurité réseau

Préparation à l'utilisation d'outils de supervision et de détection

2. Pendant l'action

Installation et configuration de Wazuh (détection d'intrusion)

Mise en place de Zabbix et Grafana (supervision et visualisation)

Sécurisation des accès via SSH

3. Après l'action

Maîtrise des outils de sécurisation et de supervision

Meilleure compréhension de la détection des incidents de sécurité

Réfléchir aux moyens d'améliorer la sécurité globale de l'infrastructure

Planning Final

Heures Passés sur chaque partie	
Parties	**Nombre d'heures**
Virtualization	1h30
DNS	30min
Réseaux	1h
AD ou LDAP	30min
DHCP	30min
WiFi	3h
Radius	1h
Web	30min
RDS	2h
Veille Techno	5h
Test + Corrections	4h
Total	19h30min

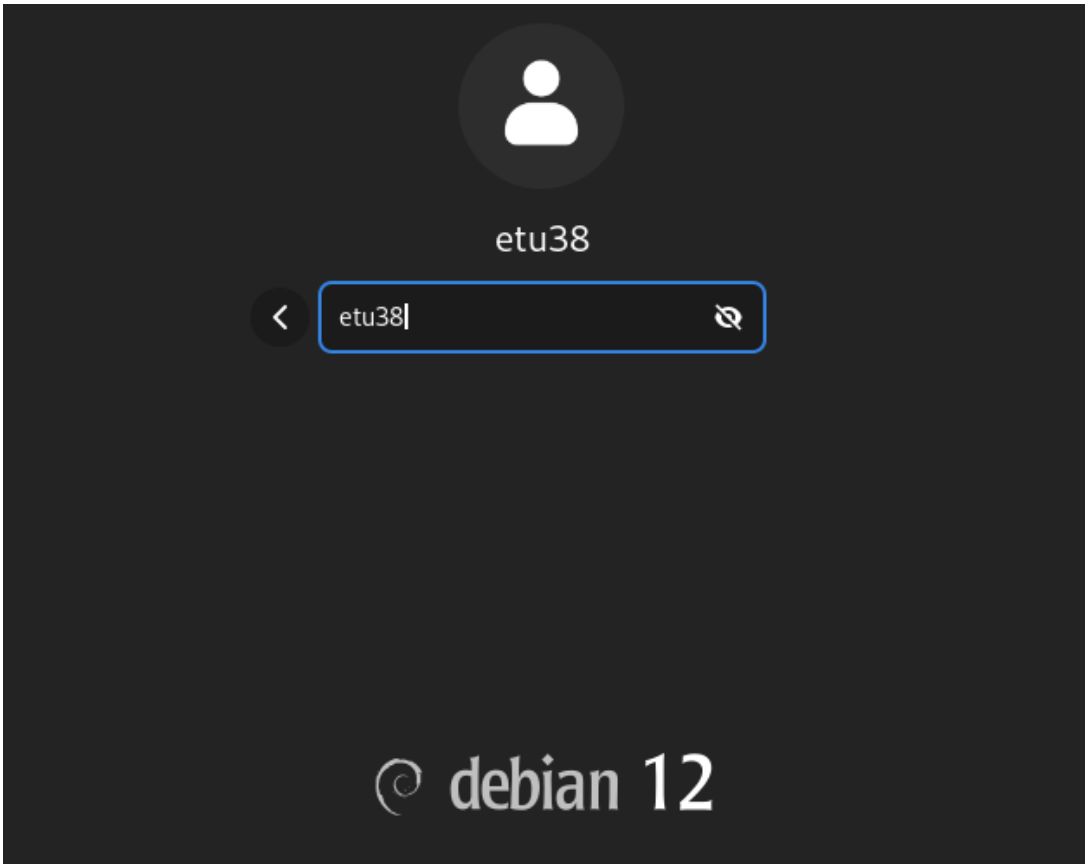
Pendant cette SAE, j'ai trouvé quelques blocages que j'ai dû surmonter, et cela m'a coûté plus de temps que prévu.

Erreurs trouvées et surmontées

Debian sans interface GUI

```
etu38@SAE3-CYBER3-Etu38-Deb:~$ sudo apt update
Ign :1 cdrom://[Debian GNU/Linux 12.2.0 _Bookworm_ - Official amd64 NETINST with firmware 20231007-1
0:28] bookworm InRelease
Err :2 cdrom://[Debian GNU/Linux 12.2.0 _Bookworm_ - Official amd64 NETINST with firmware 20231007-1
0:28] bookworm Release
  Veuillez utiliser apt-cdrom afin de faire reconnaître ce cédérom par votre APT. apt-get update ne
peut être employé pour ajouter de nouveaux cédéroms
Lecture des listes de paquets... Fait
E: Le dépôt cdrom://[Debian GNU/Linux 12.2.0 _Bookworm_ - Official amd64 NETINST with firmware 20231
007-10:28] bookworm Release n'a pas de fichier Release.
N: Les mises à jour depuis un tel dépôt ne peuvent s'effectuer de manière sécurisée, et sont donc dé
sactivées par défaut.
N: Voir les pages de manuel d'apt-secure(8) pour la création des dépôts et les détails de configurat
ion d'un utilisateur.
etu38@SAE3-CYBER3-Etu38-Deb:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=6.59 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=6.62 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=6.67 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 6.594/6.628/6.667/0.030 ms
etu38@SAE3-CYBER3-Etu38-Deb:~$ _
```

Pour résoudre ce problème j'ai du actualiser les liens présents dans le fichier **/etc/apt/sources.list**



Possibilité d’améliorations

-UNIFI Security Gateway

– Serveur NAS (backup)

– Un AD Secondaire (Redondance AD)

– VRF (Redondance Réseau)

– Clé SSH

Conclusion

Pour conclure, cette SAE m'a permis de répondre aux exigences de modernisation de l'infrastructure de l'entreprise. Nous sommes passés d'un environnement obsolète à une architecture sécurisée et supervisée, basée sur Windows Server 2022 et Debian 12.

J'ai pu consolider mes compétences en virtualisation et en services réseaux critiques (DNS, DHCP, Radius), tout en allant plus loin grâce à la mise en place d'une supervision moderne avec Zabbix et Grafana, et d'une détection d'intrusion avec Wazuh.

Bien que fonctionnelle, cette infrastructure pourrait encore évoluer, notamment par l'ajout de redondance pour garantir une haute disponibilité des services. Ce projet a été une excellente mise en situation professionnelle, confirmant l'importance de la rigueur et de la veille technologique dans notre métier.