Millot Elisa – RT2 C1

Compte Rendu de la SAÉ3.CYBER.03 : Conception et déploiement d’un réseau sécurisé

Sommaire :

1. Introduction :

Contexte

Dans le cadre de la SAÉ3.CYBER.03, nous avons été sollicités pour concevoir et tester un nouveau réseau informatique pour une PME souhaitant moderniser son infrastructure et sécuriser ses services réseau. L'objectif principal était de répondre aux besoins décrits dans le cahier des charges, tout en mettant en œuvre des solutions techniques avancées.

Objectifs

- Moderniser les serveurs de l'entreprise en passant à Windows Server 2016 et/ou Debian 11.
- Mettre en place des services réseau avancés : DNS, DHCP, WiFi, AD DS, Radius.
- Assurer la sécurisation et la surveillance du réseau.
- Documenter les processus et valider les configurations via des tests.

Analyse et Préparation

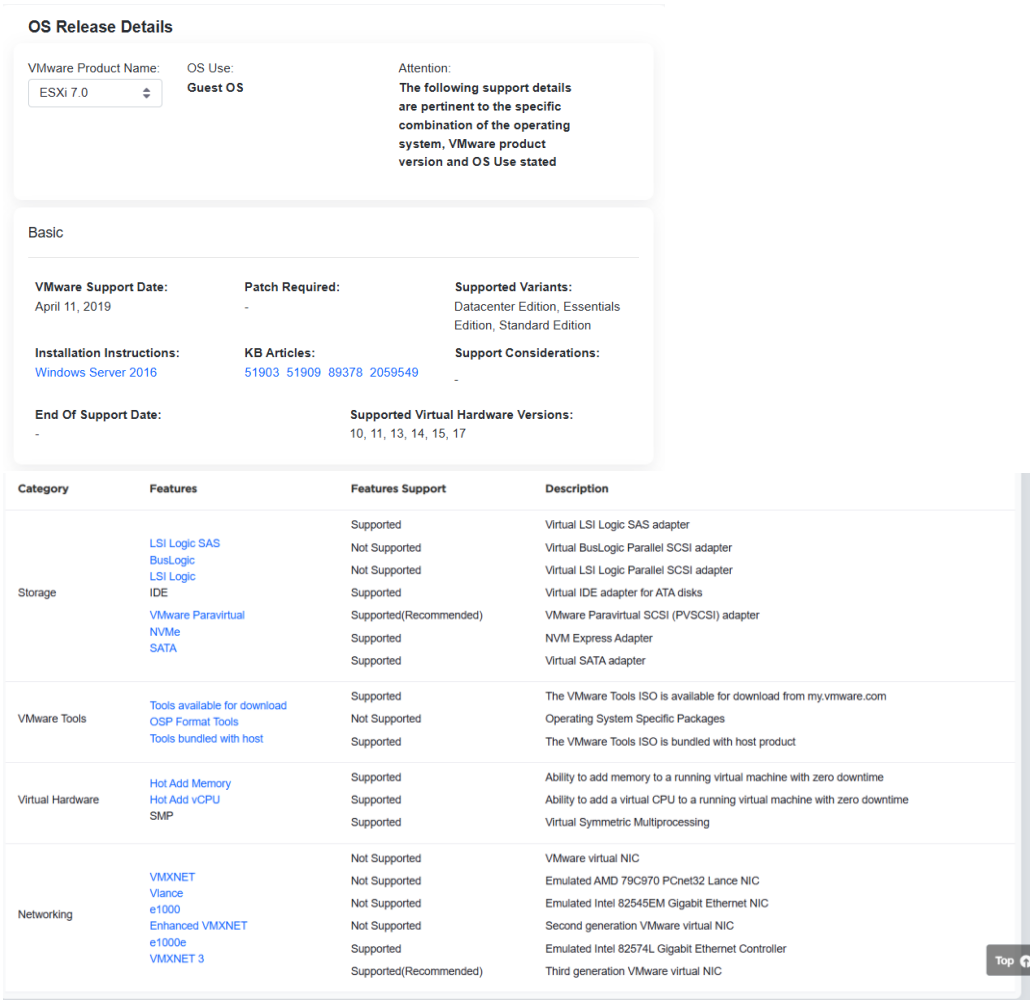
Étude du cahier des charges

Un brainstorming en cours a permis d'identifier les besoins techniques :

- Configuration Réseau (VLAN, OSPFv2, ACL, DHCP,)
- Sécurité réseau
- Hébergement Web, RDWeb et gestion du DNS

Création des VM

- Serveurs Windows 2016 créés sur VCenter.
- Configuration initiale : comptabilité des serveurs avec VCenter



OS Release Details

VMware Product Name: ESXi 7.0

OS Use: **Guest OS**

Attention: **The following support details are pertinent to the specific combination of the operating system, VMware product version and OS Use stated**

Basic

VMware Support Date: April 11, 2019

Patch Required: -

Supported Variants: Datacenter Edition, Essentials Edition, Standard Edition

Installation Instructions: Windows Server 2016

KB Articles: 51903 51909 89378 2059549

Support Considerations: -

End Of Support Date: -

Supported Virtual Hardware Versions: 10, 11, 13, 14, 15, 17

Category	Features	Features Support	Description
Storage	LSI Logic SAS	Supported	Virtual LSI Logic SAS adapter
	BusLogic	Not Supported	Virtual BusLogic Parallel SCSI adapter
	LSI Logic	Not Supported	Virtual LSI Logic Parallel SCSI adapter
	IDE	Supported	Virtual IDE adapter for ATA disks
	VMware Paravirtual	Supported(Recommended)	VMware Paravirtual SCSI (PVSCSI) adapter
	NVMe	Supported	NVM Express Adapter
	SATA	Supported	Virtual SATA adapter
VMware Tools	Tools available for download	Supported	The VMware Tools ISO is available for download from my.vmware.com
	OSP Format Tools	Not Supported	Operating System Specific Packages
	Tools bundled with host	Supported	The VMware Tools ISO is bundled with host product
Virtual Hardware	Hot Add Memory	Supported	Ability to add memory to a running virtual machine with zero downtime
	Hot Add vCPU	Supported	Ability to add a virtual CPU to a running virtual machine with zero downtime
	SMP	Supported	Virtual Symmetric Multiprocessing
Networking	VMXNET	Not Supported	VMware virtual NIC
	Vlance	Not Supported	Emulated AMD 79C970 PCnet32 Lance NIC
	e1000	Not Supported	Emulated Intel 82545EM Gigabit Ethernet NIC
	Enhanced VMXNET	Not Supported	Second generation VMware virtual NIC
	e1000e	Supported	Emulated Intel 82574L Gigabit Ethernet Controller
	VMXNET 3	Supported(Recommended)	Third generation VMware virtual NIC

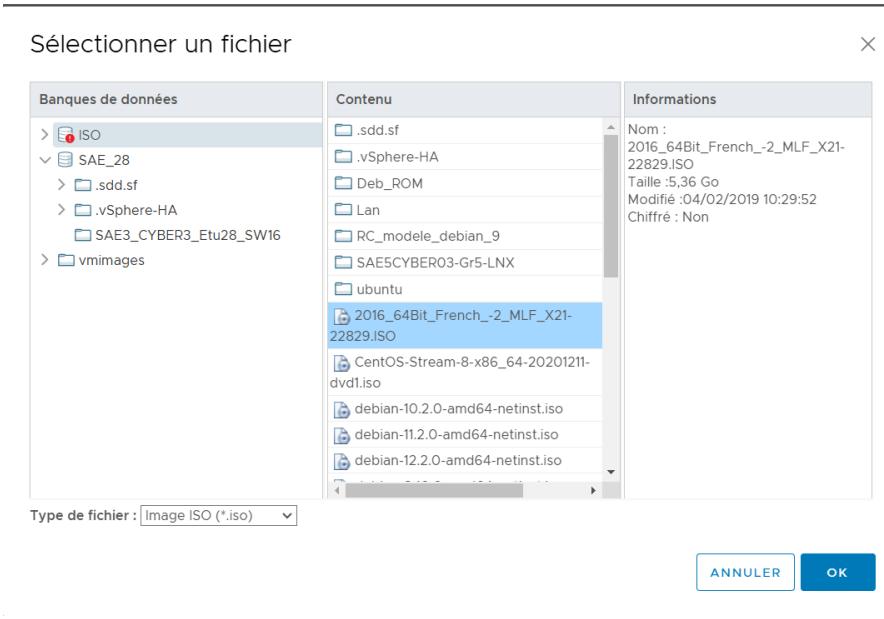
Top

Création Windows Serveur 2016 :

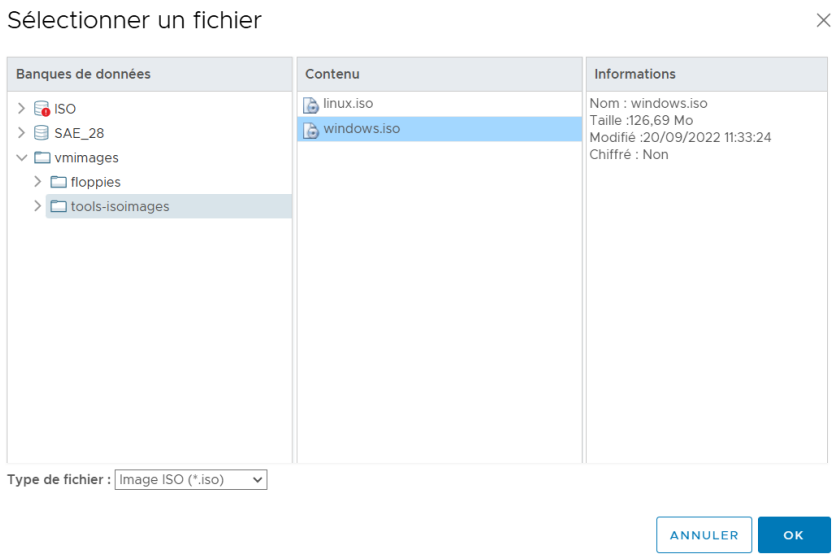
Type de provisionnement	Créer une machine virtuelle
Nom de la machine virtuelle	SAE3_CYBER3_Etu28_SW16
Dossier	Etudiant_28
Hôte	esx8.lan.rt
Banque de données	SAE_28
Nom du SE invité	Microsoft Windows Server 2016 ou version ultérieure (64 bits)
Sécurité basée sur la virtualisation	Désactivé
CPU	2
Mémoire	4 Go
Cartes réseau	1
Réseau de carte réseau 1	RT_VLAN704
Type de carte réseau 1	VMXNET 3
Contrôleur SCSI 1	Paravirtuel VMware
Créer un disque dur 1	Nouveau disque virtuel
Capacité	40 Go

Banque de données	SAE_28
Nœud de périphérique virtuel	SCSI(0 : 0)
Mode	Dépendant

Premier disque :

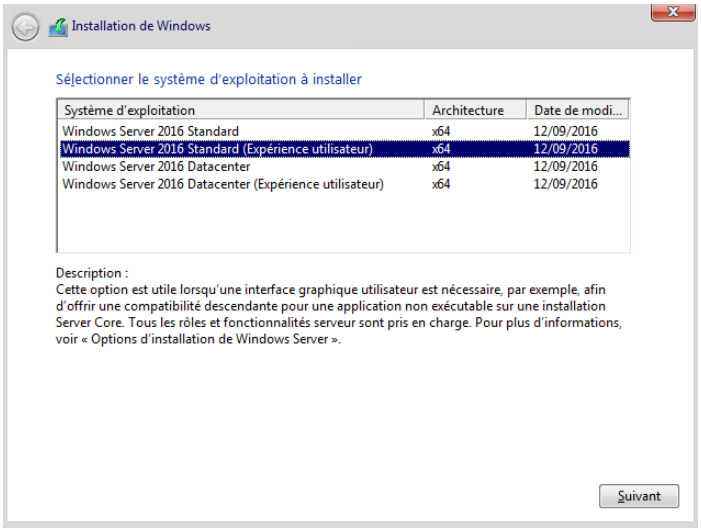


Deuxième disque :

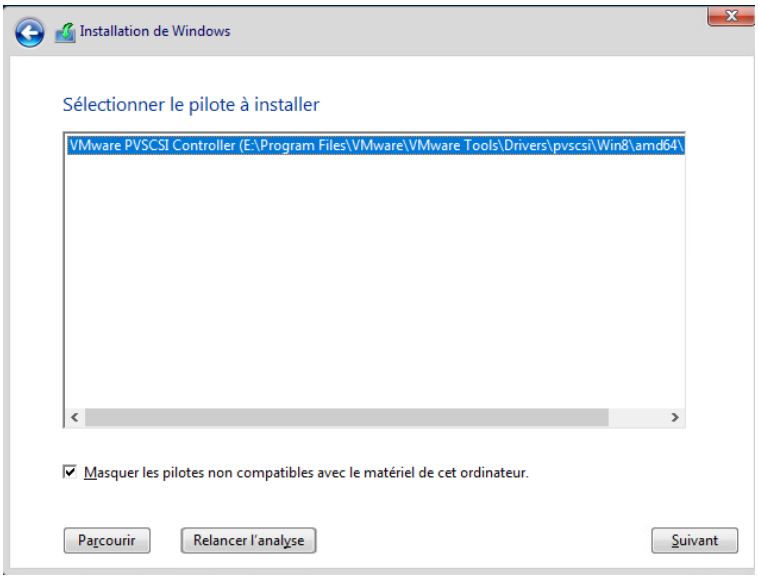


Pour installer les Tools Windows.

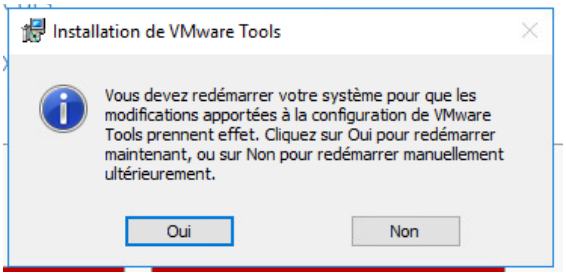
Ensuite nous lançons la machine, nous installons bien la version Windows Server 2016 (Expériences utilisateur) pour avoir la version graphique :



On sélectionne le pilote, on met « amd 64 » de « Win8 » pour le Serveur Windows 2016 parce qu'il y a une compatibilité entre ces versions de systèmes d'exploitation et de la similitude des architectures sous-jacentes.



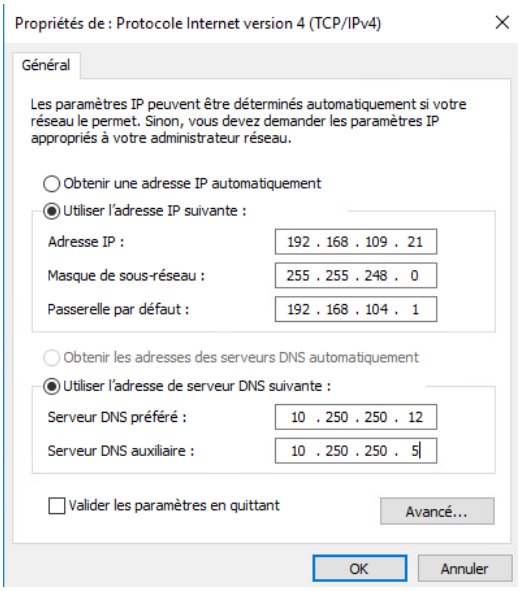
Quand c'est fini d'installer Windows Serveur 2016 et que nous avons mis le compte « Administrateur », installation des « VmTools »



Enfin nous mettons une adresse IP de notre réseau donnée. Sachant que j'ai :

Le réseau IP associé à ce vlan RT_VLAN704 est : 192.168.104.0/21.

- La passerelle a pour adresse IP : 192.168.104.1/21.
- Les serveurs DNS à utiliser sont : 10.250.250.12 et 10.250.250.5.
- La plage d'adresses IP que vous avez le droit d'utiliser est : 192.168.109.21/21 à 192.168.109.30/21

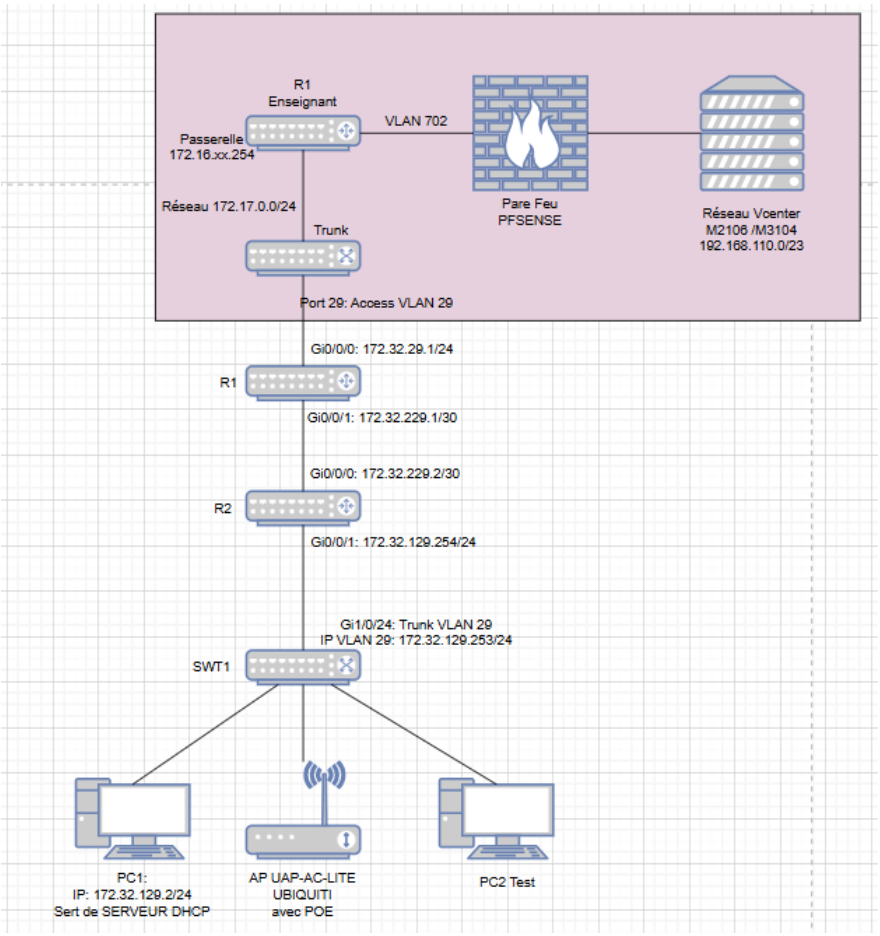


Dû à un grand nombre de service demander, j'ai créé par la suite une autre machine Windows Server 2016 ayant pour adresse IP : 192.168.109.22.

Diagramme réseau

Mon réseau du VLAN 29. J'avais comme informations :

- Vous utiliserez le Vlan 29
- Vous raccorderez votre routeur de tête, configuré par l'enseignant, R1, sur le port 29 du switch enseignant.
- Le réseau reliant votre routeur au switch enseignant et donc au routeur R1 enseignant est : 172.32.29.0/24
- L'interface de votre routeur de tête, sur ce réseau est : 172.32.29.1 et votre passerelle sur le routeur R1 enseignant est : 172.32.29.254
- Votre réseau connectant vos 2 routeurs entre eux est : 172.32.229. 0/30
- Votre réseau collaborateur (réseau privé) est : 172. 32.129.0/24.

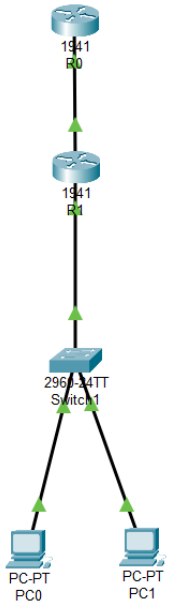


2. Mise en Place des Services Réseau

Réseau et VLAN

- Configuration des VLANs pour isoler les segments réseau.
- Implémentation d'OSPFv2 pour le routage dynamique.
- Sécurisation des équipements avec SSH et ACL.

Dans un premier temps j'ai simulé mon réseau sur Cisco Packet Tracert ma partie de réseau :



Une fois ceci fait, j'ai mis ma configuration en vrai. Tout d'abord, j'ai configuré sur tous les routeur/switch les modes Privilèges et Consoles avec un mot de passe :

```
line cons 0
password password123
login
exit
enable password password123
```

Ensuite pour pouvoir se connecter en SSH :

```
ip domain name sae.local
crypto key generate rsa modulus 2048
username admin secret strongpassword123
line vty 0 4
login local
transport input ssh
exit
```

Ensuite sur le Routeur 1 (celui qui est connecter directement au switch enseignant). Je configure mes interfaces G0/0/0 qui est connecter au switch enseignant, nous mettons donc une adresse qui appartient au réseau, il est indiqué 172.32.29.1. Pour l'interface G0/0/1 nous avons un réseau entre les 2 routeurs qui est 172.32.229. 0/30 donc elle sera 172.32.229.1/30. Enfin je mets en places le protocoles OSPFV2.

```
interface GigabitEthernet0/0/0
ip address 172.32.29.1 255.255.255.0
no shutdown
exit

interface GigabitEthernet0/0/1
ip address 172.32.229.1 255.255.255.252
no shutdown
exit



router ospf 29
network 172.32.29.0 0.0.0.255 area 0
network 172.32.229.0 0.0.0.3 area 0
exit
```

Sur le Routeur 2 (entre notre Routeur 1 et notre switch) je configure mes interfaces, la Gi0/0/0 qui est connecter au Gi0/0/1 du Routeur 1, nous sommes donc dans le réseau entre les 2 routeurs, je lui donne donc l'adresse 172.32.29.2/30. L'autre interface est celle qui est connecter au switch, nous sommes donc dans notre réseau collaborateur (réseau privé) est : 172. 32.129.0/24. Nous mettons aussi du protocole OspfV2 pour avoir des routes.

```
interface GigabitEthernet0/0/0
ip address 172.32.229.2 255.255.255.252
no shutdown
exit

interface GigabitEthernet0/0/1
ip address 172.32.129.254 255.255.255.0
no shutdown
exit


router ospf 29
network 172.32.229.0 0.0.0.3 area 0
network 172.32.129.0 0.0.0.255 area 0
exit
```

Enfin sur le switch j'ai configuré mon VLAN 29 avec une adresse IP du réseau collaborateur. L'interface Gi1/0/24 est celle connecter au routeur, elle est donc en trunk. Les autres interfaces sont celle utiliser pour connecter les machines/point accès et d'autre matériel.

```
int vlan 29
 ip add 172.32.129.253 255.255.255.0
no sh

interface GigabitEthernet1/0/24
  switchport mode trunk
  switchport trunk allowed vlan 29
  switchport trunk native vlan 29

interface range GigabitEthernet1/0/1-23
  switchport mode access
  switchport access vlan 29
```

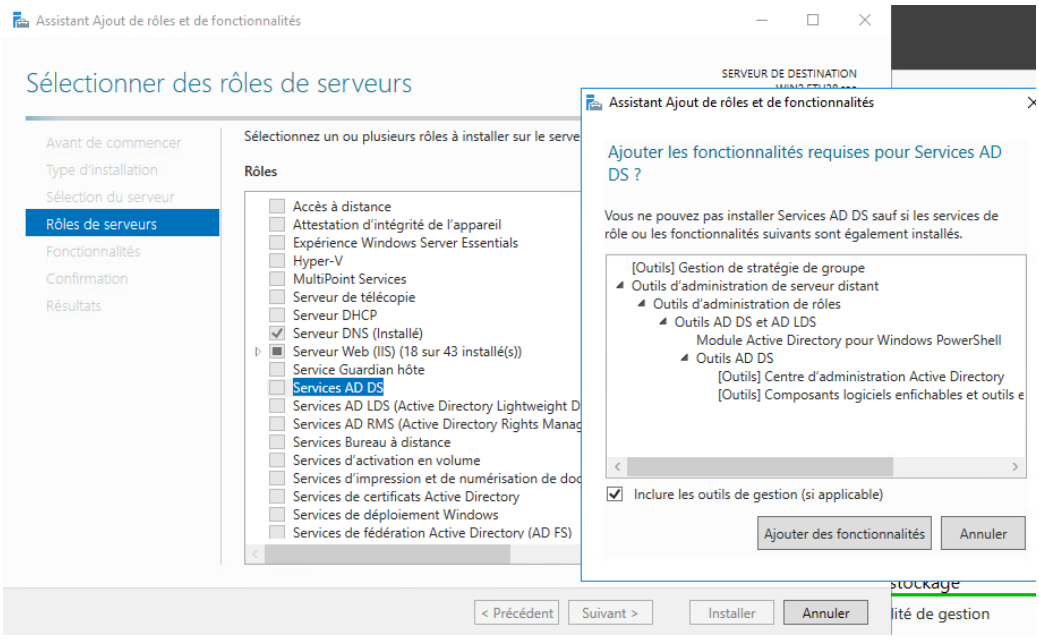
DNS

- Mise en place d'un serveur DNS primaire pour le sous-domaine ETU28.sae.
- Configuration des enregistrements A, NS, CNAME

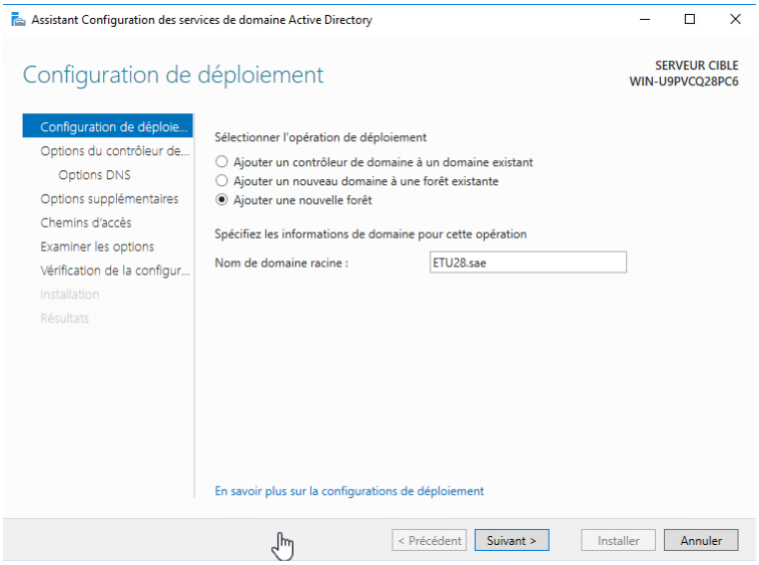
Pour installer le rôle DNS il est préconisé de l'installer grâce au rôle AD-DS qui l'installera par la suite, en mettant toutes les configurations pour que le DNS et AD-DS fonctionne. (https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/active-directory-integrated-dns-zones)

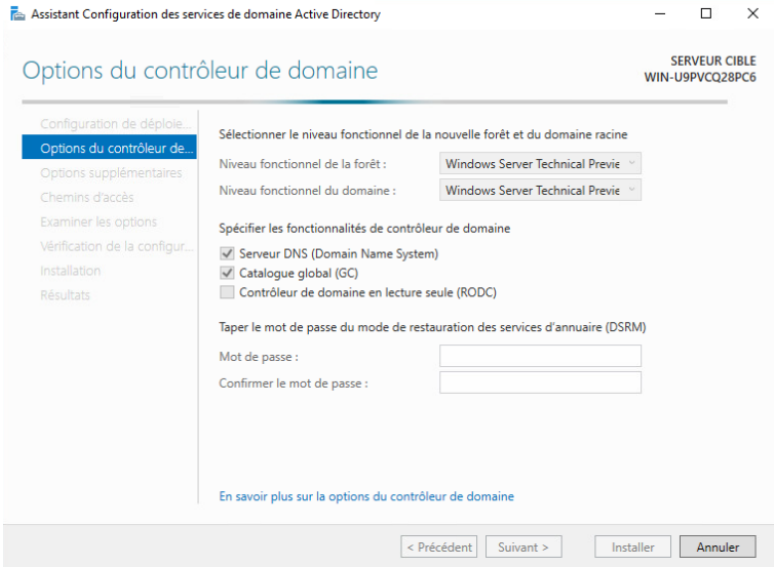
J'ai demandé un sous domaine ETU28 à l'adresse IP : 192.168.109.21 du domaine « sae ». J'ai donc comme domaine ETU28.sae.

On va donc dans « gérer », puis « Ajouter des rôles et es fonctionnalités ».

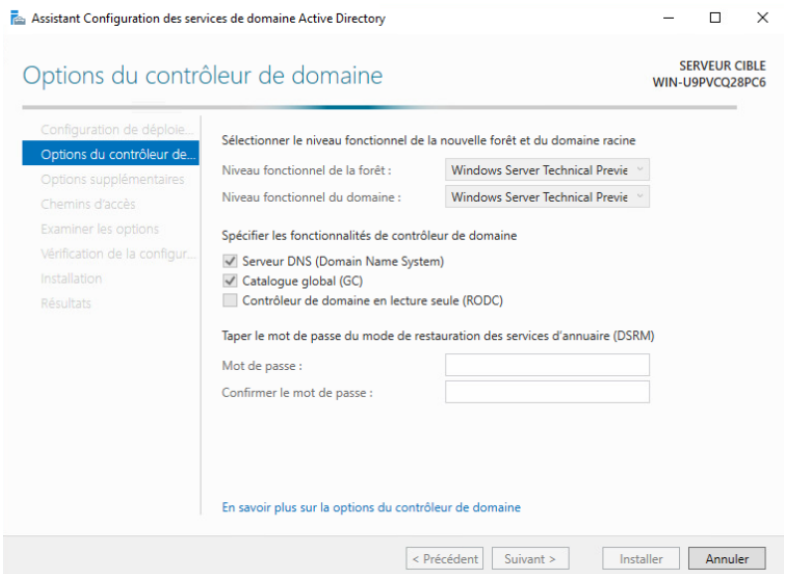


Quand c'est installer, nous mettons en place l'AD-DS en créant une nouvelle forêt. Comme notre domaine est « ETU28 » nous mettons le nom de domaine « ETU28.sae »

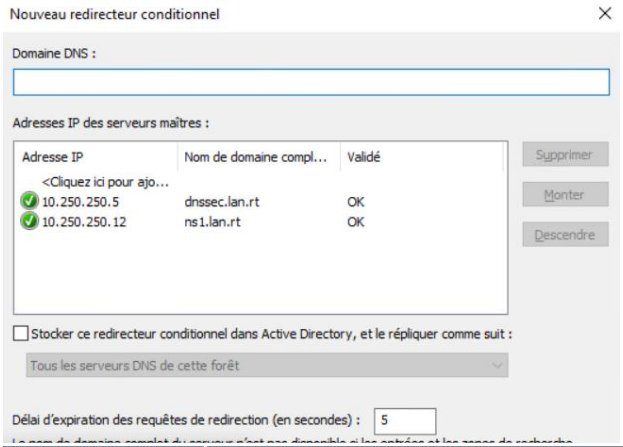


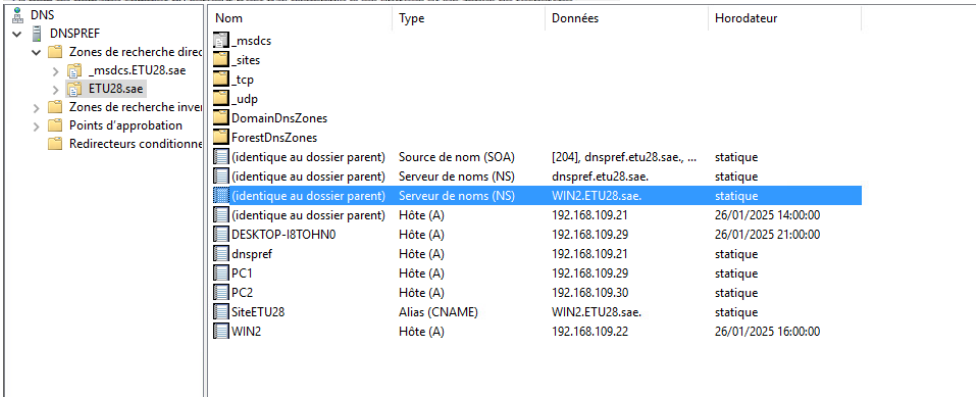


Mot de passe de restauration des services d'annuaire (DSRM) = SAEETU28-

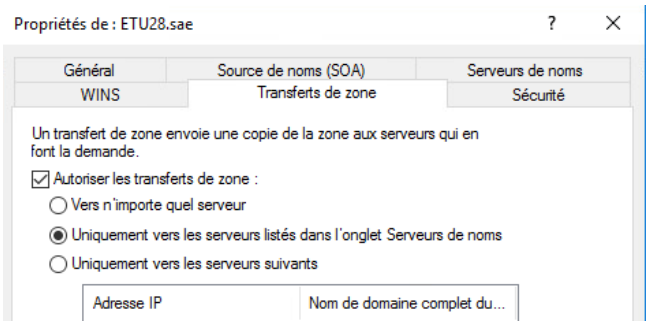


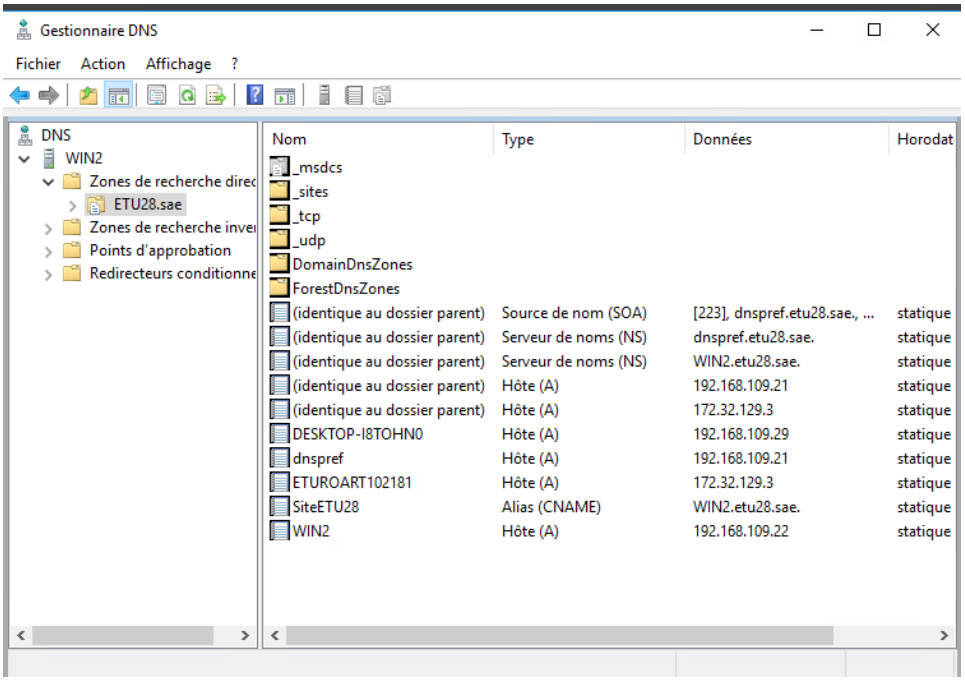
Une fois installer, nous allons dans le gestionnaire de serveur, en haut à droite « outil » puis « DNS », nous avons donc le « DNS » en place, il faudra donc mettre en place les hôtes de type A et les redirecteurs conditionnels vers les DNS de l'IUT.





Transfère de zone sur le deuxième serveur Windows 2016 :





DHCP

- Serveur DHCP configuré pour attribuer des adresses IP aux postes clients.

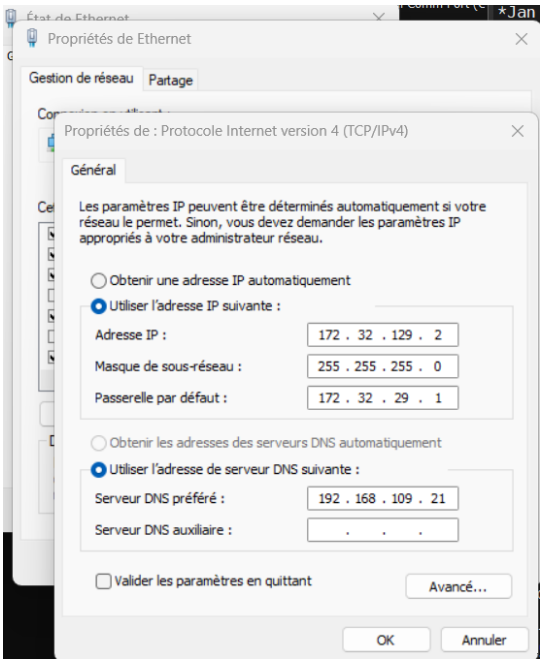
Tout d'abord, dans ma configuration de routeur, au niveau du routeur 2, j'ai mis en place une ACL

```
ip access-list extended BLOCK_DHCP
deny udp any any eq 67
deny udp any any eq 68
permit ip any any
exit

interface GigabitEthernet0/0/1
ip access-group BLOCK_DHCP out
exit
```

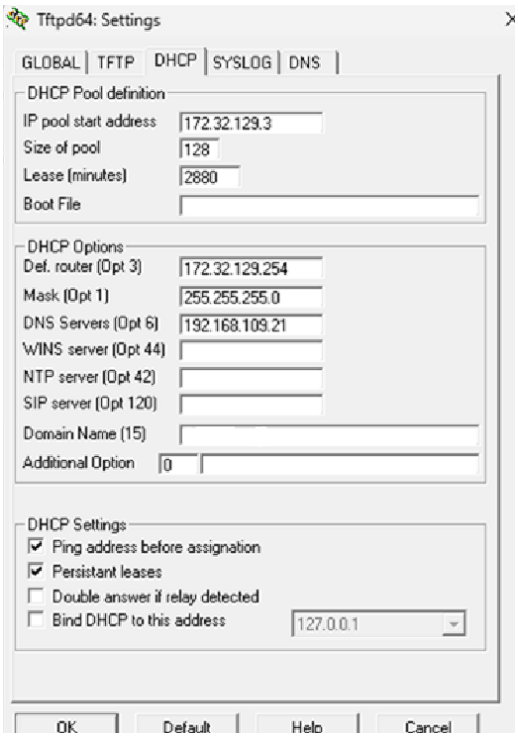
Cette configuration crée une liste de contrôle d'accès (ACL) **BLOCK_DHCP** qui bloque le trafic DHCP en filtrant les paquets UDP sur les ports 67 et 68 (utilisés par le protocole DHCP). Ensuite, l'ACL permet tout autre trafic IP.

L'ACL est appliquée à l'interface GigabitEthernet0/0/1, en filtrant le trafic sortant (**out**), empêchant ainsi les communications DHCP sortantes de cette interface. Cela bloque l'attribution d'adresses IP via DHCP sur cette interface spécifique.

Je vais ensuite utiliser mon pc, je lui attribuer une adresse IP et mon serveur DNS et je me connecte au switch.



Je lance TFTP64 en configurant le DHCP pour que mon pc puisse servir de serveur DHCP



A quoi sert le DHCP ?

Le DHCP sert à attribuer automatiquement des adresses IP aux machines, ce qui évite de le faire manuellement, une tâche longue et compliquée pour les moins habiles en informatique. Il

permet aussi au point d'accès d'obtenir une adresse IP du réseau, assurant son bon fonctionnement.

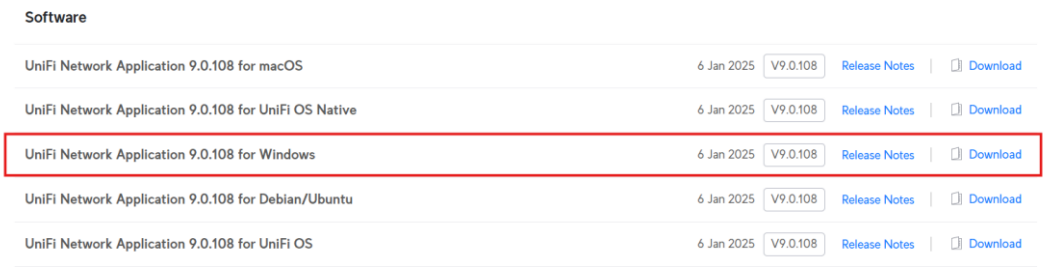
WiFi

- Comparaison entre UAP-AC-LITE Ubiquiti et AP 1702I Cisco.
- Configuration d'un contrôleur virtuel pour gérer deux SSID :
    - SSID entreprise avec authentification renforcée (Radius).
    - SSID invité avec restrictions (débit limité, accès web et mail uniquement).

Je commence par la comparaison entre UAP-AC-LITE Ubiquiti et AP 1702I Cisco. Avec un tableau

Critères	UAP-AC-LITE Ubiquiti	AP 1702I Cisco
Performances	Dual-band (2,4 GHz : 300 Mbps, 5 GHz : 867 Mbps) 1	Dual-band (2,4 GHz : 300 Mbps, 5 GHz : 867 Mbps) 1
Coût	Environ 100-120 € 1	Environ 350-400 €
Technologie	Wi-Fi 5 (802.11ac Wave 1) 1	Wi-Fi 5 (802.11ac Wave 1) 1
Nombre d'antennes	2x2 MIMO 1	2x2 MIMO 1
Portée	Environ 122 mètres en champ libre 1	Environ 100 mètres en champ libre
Facilité de gestion	Interface intuitive avec **UniFi Controller** (logiciel gratuit) 1	Gestion via **Cisco Controller** (complexe et coûteux)
Sécurité	WPA2, VLANs, gestion des invités 1	WPA2, VLANs, gestion des invités 1
Compatibilité	Compatibilité universelle (matériel varié) 1	Conçu pour les environnements Cisco
Fiabilité	Bonne pour les PME	Très fiable, adapté aux grandes entreprises 1
Durabilité	Robuste, adapté à un usage général 1	Très robuste, idéal pour des environnements exigeants
Fonctionnalités supplémentaires	Portail captif intégré, gestion centralisée via cloud 1	Gestion centralisée avancée, intégration avec des outils Cisco
Total:	**10**	**5**

Après avoir fait ce tableau, nous nous rendons compte que le meilleur à utiliser est le UAP-AC-LITE Ubiquiti. Je vais donc l'utiliser pour mettre en place le wifi. Je vais sur le site de « Unifi » (https://ui.com/download/unifi) et je descends jusqu'à « Software » pour prendre la dernière version de l'application.

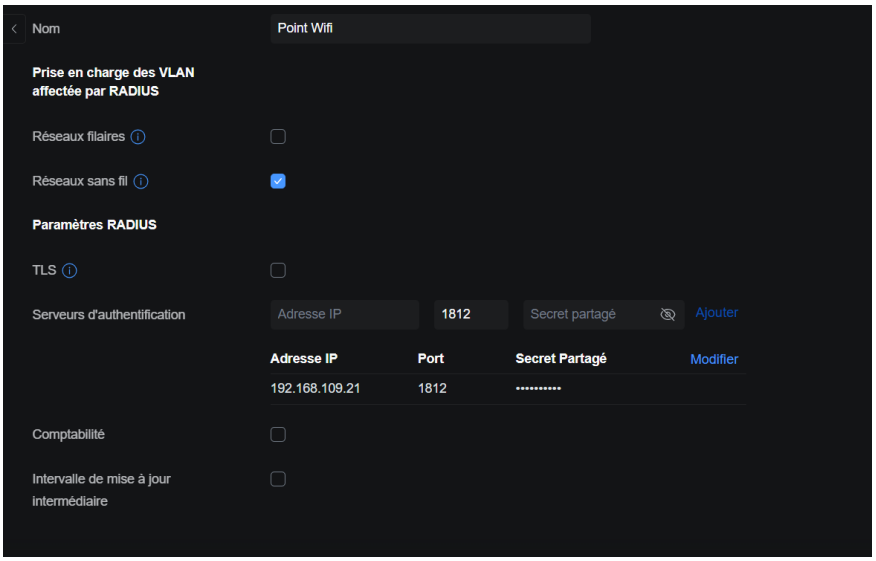


Une fois télécharger et installer nous pouvons lancer l'application :

Jusqu'à que l'application détecte un Ubiquiti sur le réseau

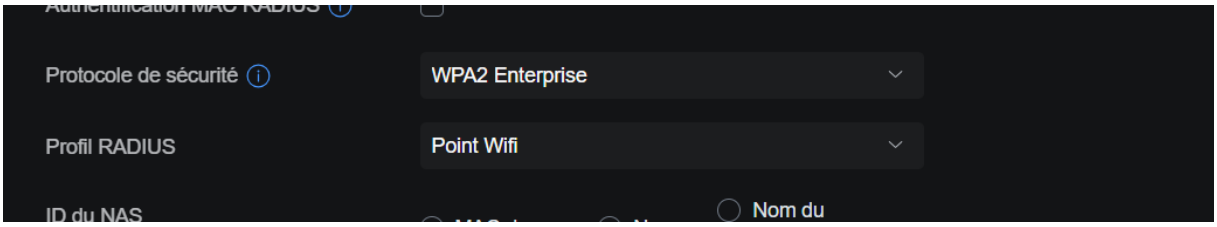
On se crée un compte sur le site internet Ubiquiti pour avoir un espace personnel. Enfin j'adopte la borne wifi que je possède.

Je vais modifier les paramètres pour faire en sorte d'avoir que le point d'accès et le radius sont lier :

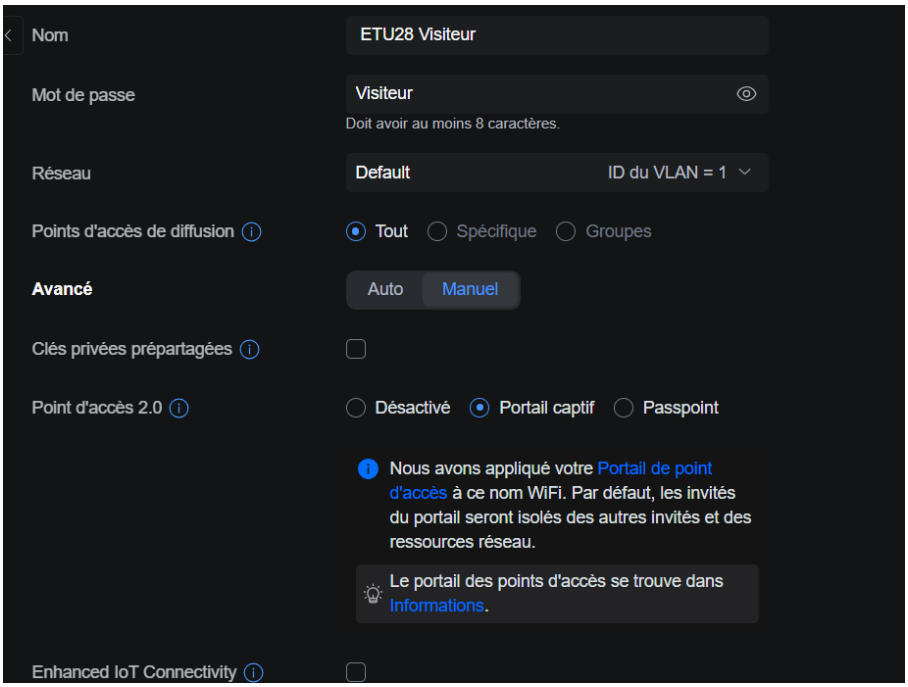


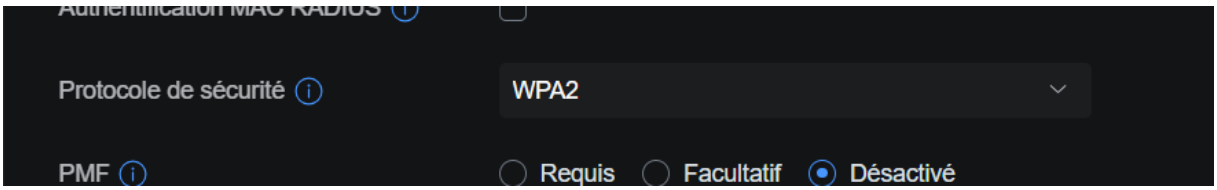
Je crée mes 2 réseaux qui sont visiteurs et personnel de l'entreprise :

Entreprise :



Visiteur :





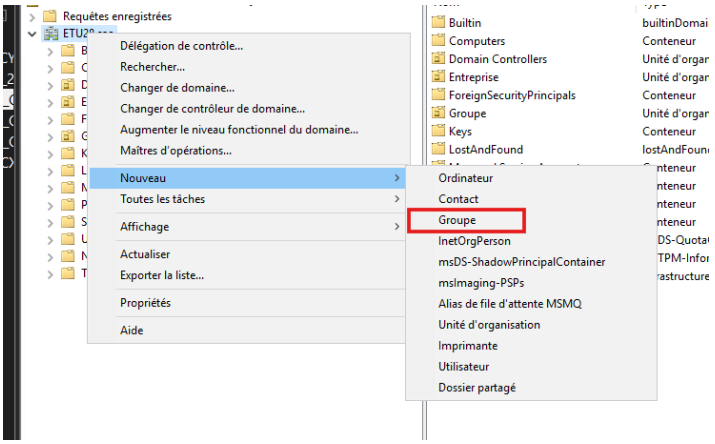
3. Services Avancés et Sécurité

AD DS et Radius

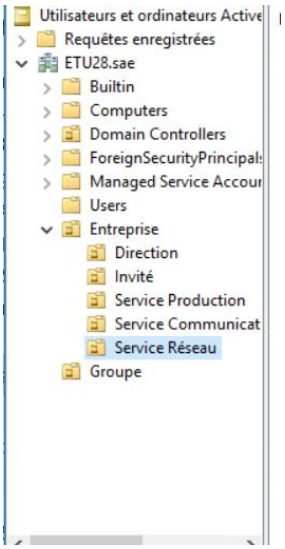
- Création d'une structure AD DS pour organiser les utilisateurs par service.
- Configuration d'un serveur Radius pour l'authentification WiFi.

AD-DS :

Comme nous avons installer AD-DS pour avoir le rôle « DNS », nous avons donc déjà le rôle d'installer sur notre machine, il faudra donc crée l'arborescence de l'entreprise. On peut faire ceci manuellement



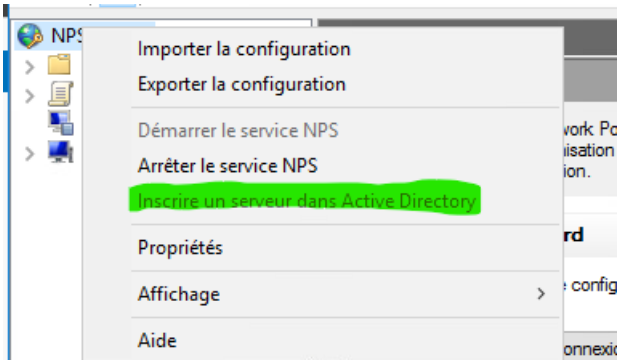
Je vais donc faires tout les groupes pour l'entreprise ou nous avons les groupes : « Direction », « Service Production », « Service Communication », « Service Réseau » et le groupe « Invité » qui nous serviras si des personnes extérieurs viennent dans l'entreprise, ça servira aussi pour la partie WIFI.

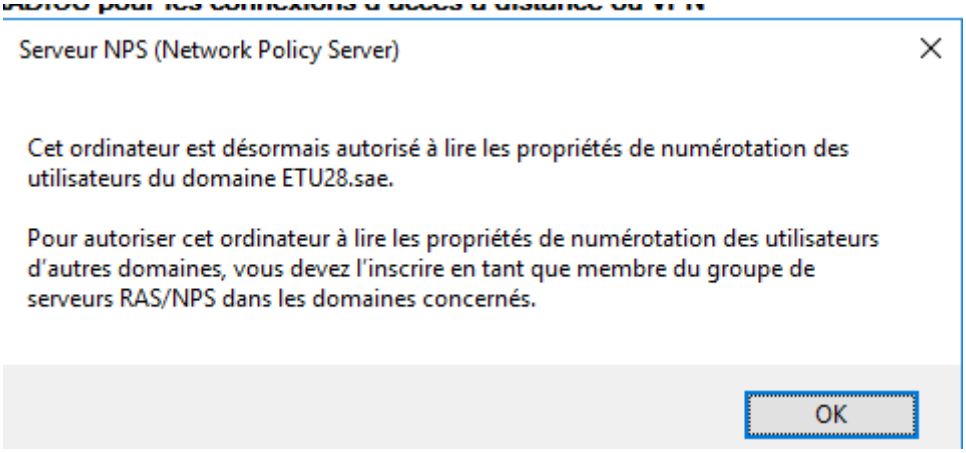


Par la suite j'ai optimisé tout cela grâce à un script PowerShell

Radius :

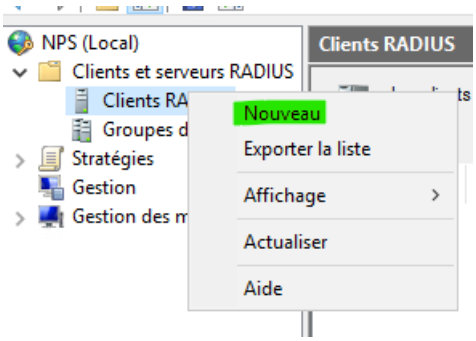
Je n'ai malheureusement pas réussi à le faire fonctionner, mais je vais quand même explique ce que j'ai fait. J'ai regardé énormément de tutoriel que ce soit écrit ou vidéo ça n'as pas fonctionner.
Dans un premier temps j'ai installé le rôle « Serveur NPS (Network Policy Server) ». J'ai lancer cet outil et j'ai fait :



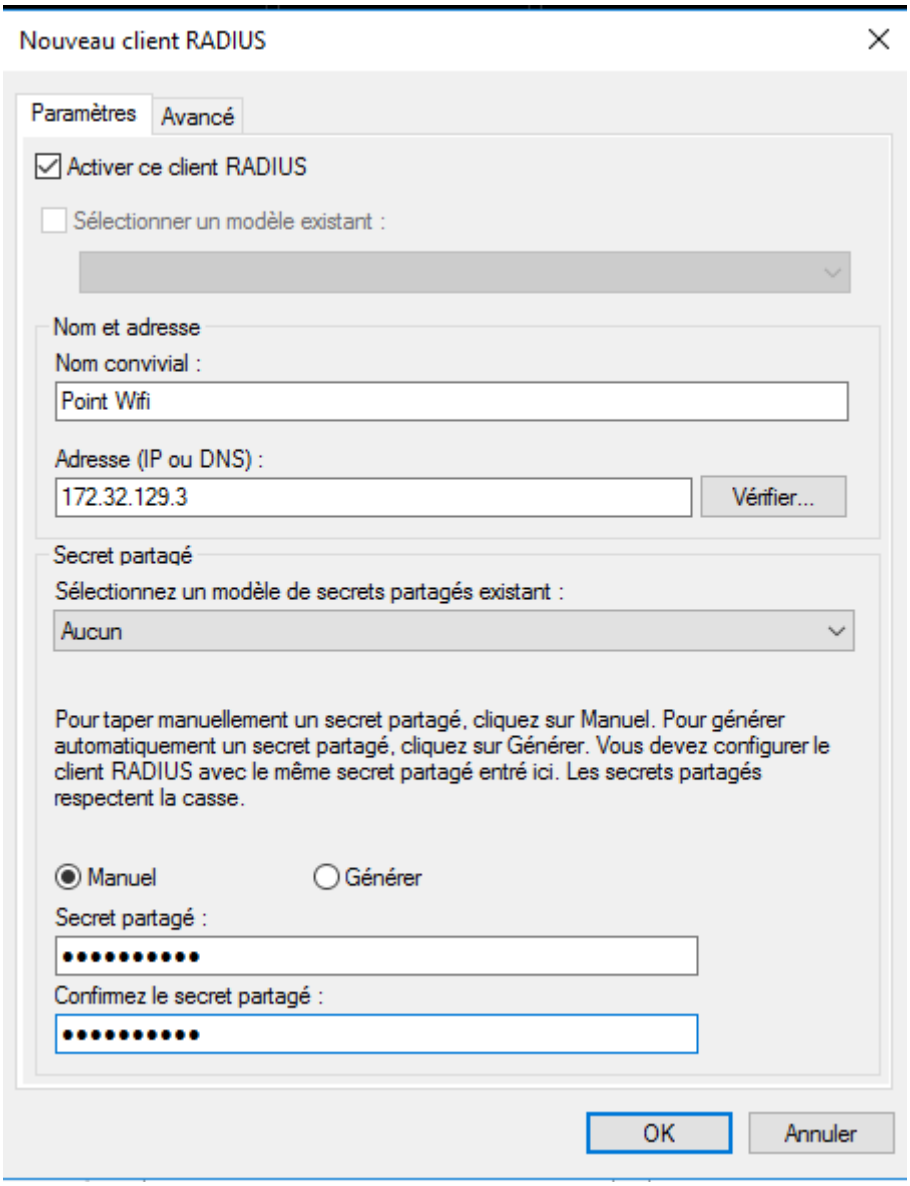


Pour qu'il puisse être relier à l'AD-DS car nous voulons nous connecter en WIFI avec nos comptes qui se trouve dans AD-DS.

Par la suite, j'ai mis un nouveau client RADIUS qui sera mon point d'accès :

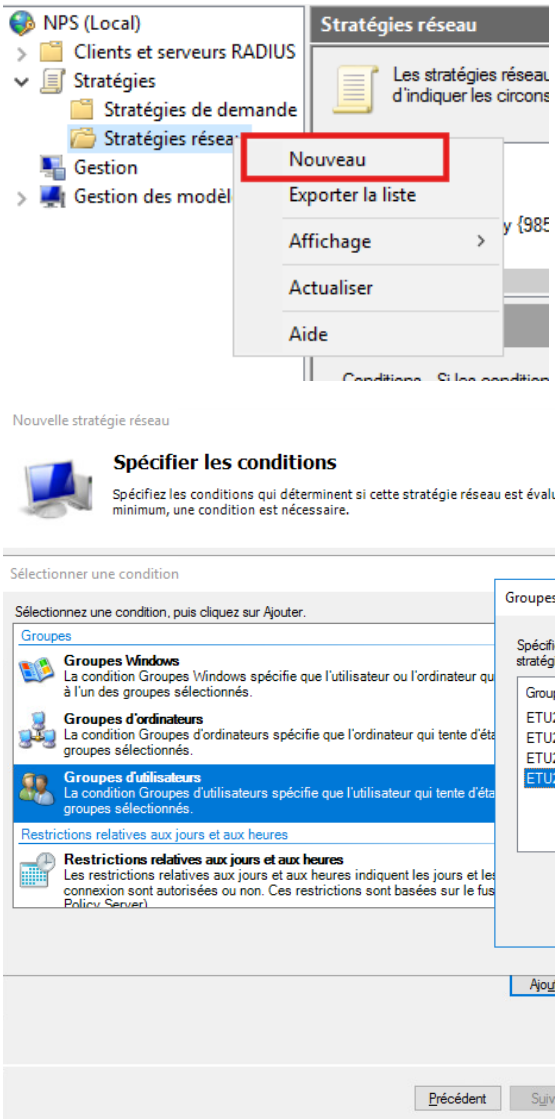


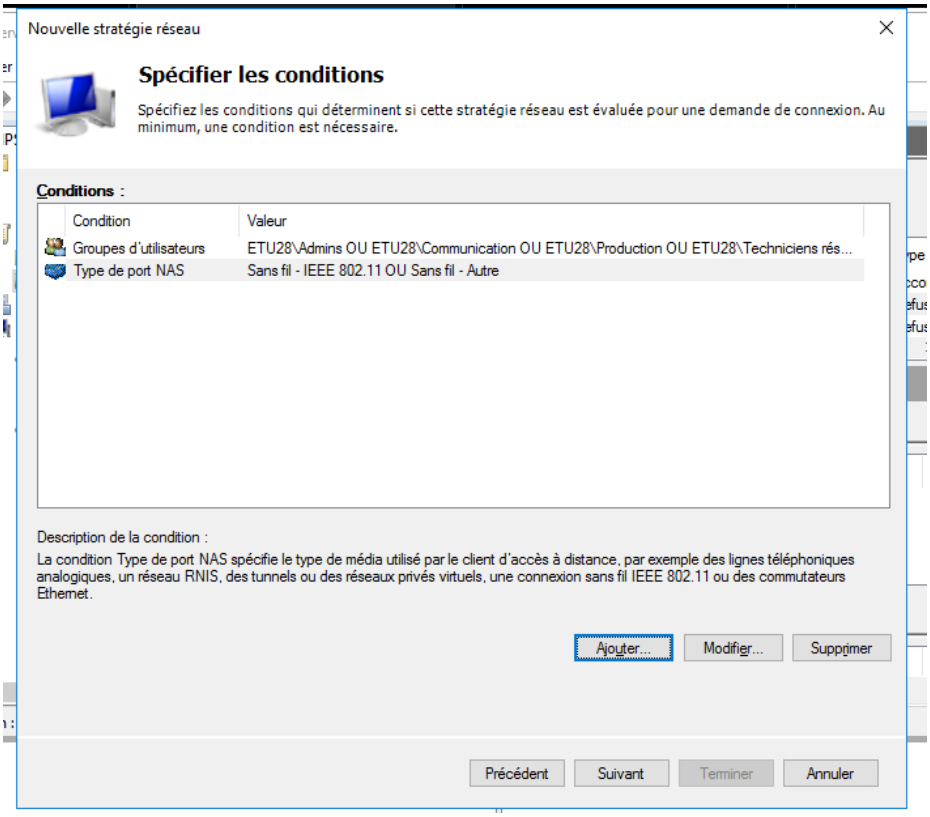
J’ai spécifié l’adresse IP de notre borne WIFI, comme nous sommes en DHCP, si l’adresse IP du point d’accès change, nous devrons donc le changer aussi ici.



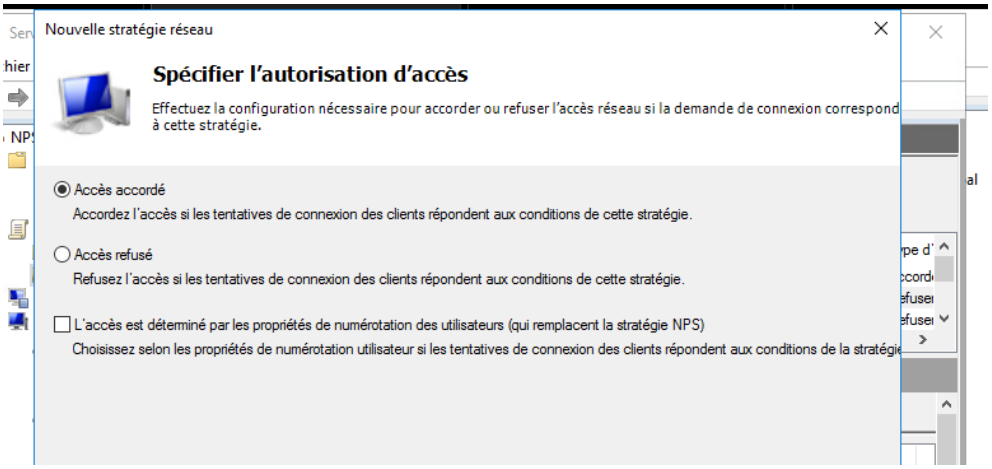
Secret partagé : PointAcces

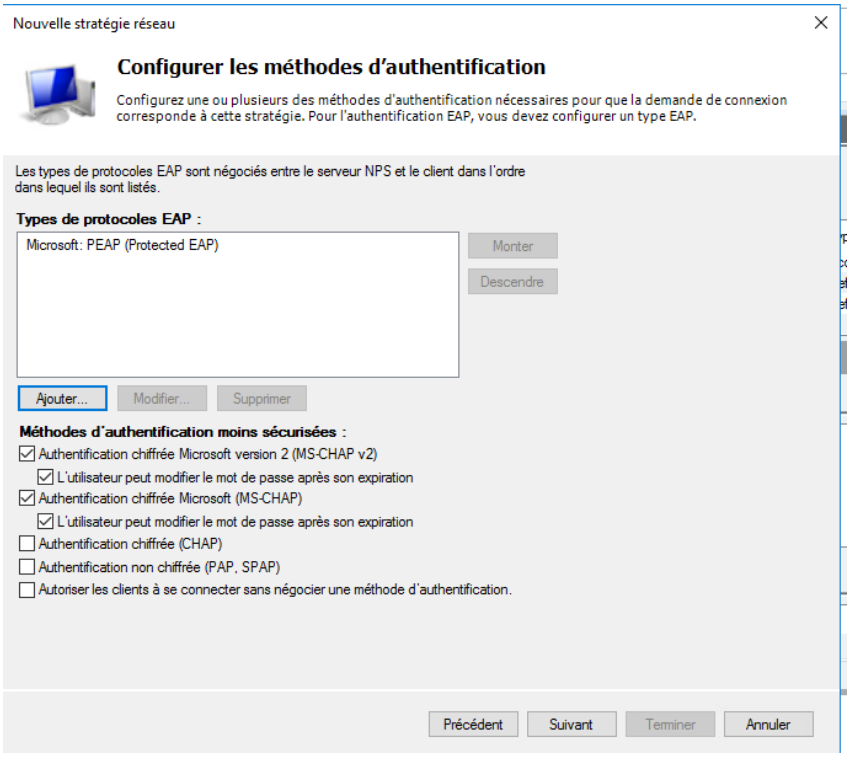
Ensuite dans Stratégies, je mets en place une nouvelle stratégies réseau. Je spécifie les conditions que je veux faire, qui sont les utilisateur auquel je veux pouvoir me connecter au wifi.


NPS (Local)
Clients et serveurs RADIUS
Stratégies
Stratégies de demande
Stratégies réseau
Gestion
Gestion des modèl
Stratégies réseau
Les stratégies réseau
d'indiquer les circons
Nouveau
Exporter la liste
Affichage
Actualiser
Aide
Nouvelle stratégie réseau
Spécifier les conditions
Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.
Sélectionner une condition
Sélectionnez une condition, puis cliquez sur Ajouter.
Groupes
Groupes Windows
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qu
à l'un des groupes sélectionnés.
Groupes d'ordinateurs
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'éta
groupes sélectionnés.
Groupes d'utilisateurs
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'éta
groupes sélectionnés.
Restrictions relatives aux jours et aux heures
Restrictions relatives aux jours et aux heures
Les restrictions relatives aux jours et aux heures indiquent les jours et les
connexion sont autorisées ou non. Ces restrictions sont basées sur le fus
Policy Server).
Ajouter...
Modifier...
Supprimer
Précédent
Suivant
Terminer
Annuler
Groupes d'utilisateurs
Spécifiez l'appartenance aux groupes nécessaire pour correspondre à cette stratégie.
Groupes
ETU28\Admins
ETU28\Communication
ETU28\Production
ETU28\Techniciens réseau
Ajouter des groupes...
Supprimer
OK
Annuler



Enfin je spécifie l'autorisation d'accès et les méthodes d'authentification





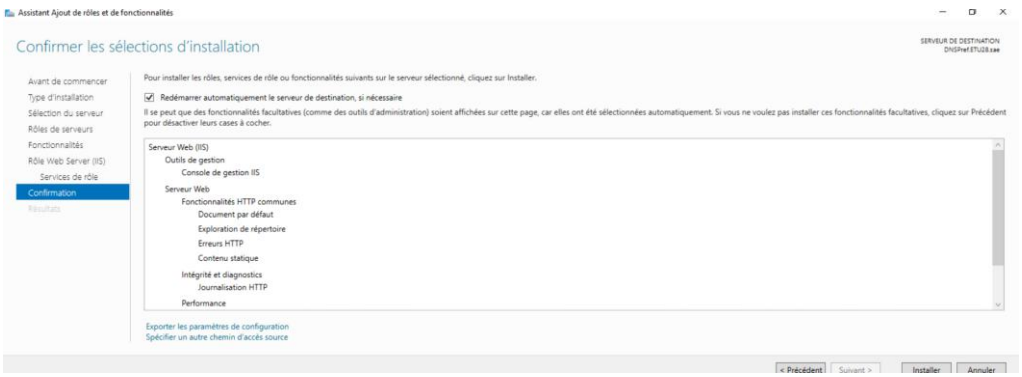
Service Web

- Installation du rôle IIS
- Modification nom du domaine (CName)
- Installation du rôle RDP pour le RDWeb

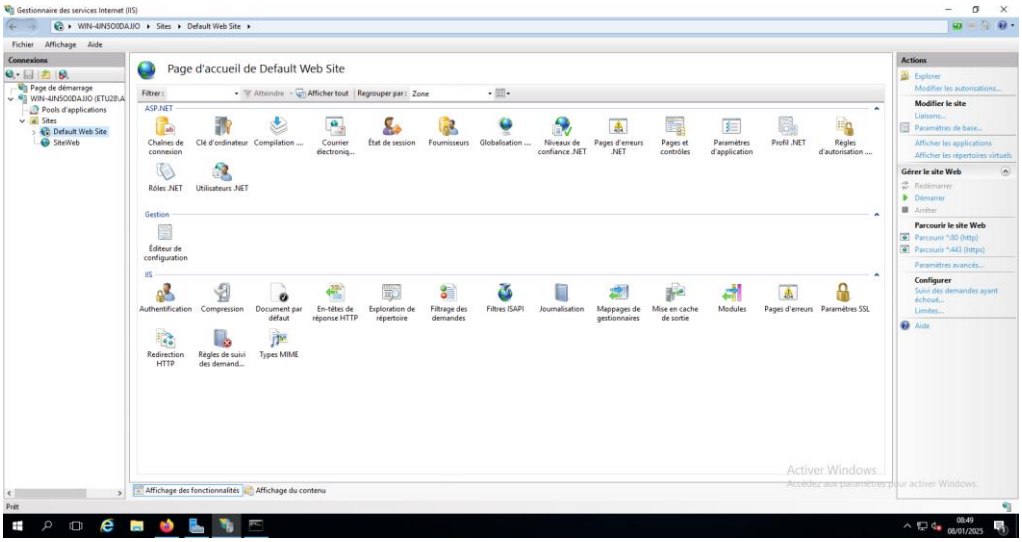
ISS :

Nous avons besoin d'un site internet pour le service communication, au lieu qui l'héberge chez des fournisseurs de domaine (Comme OVH) on va l'héberger sur notre Windows Serveur 2016.

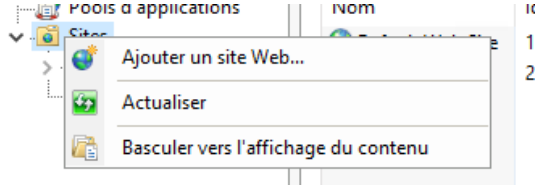
Dans un premier temps nous allons installer le rôle IIS



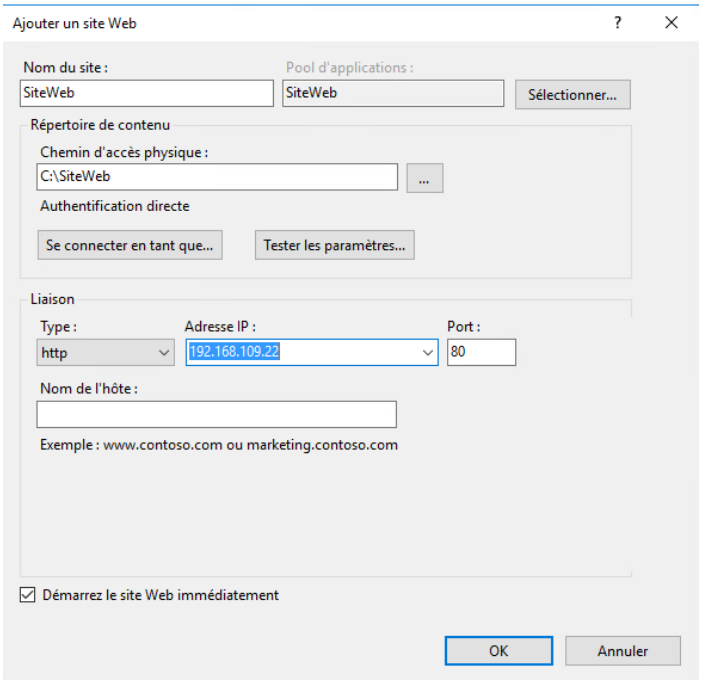
Quand ceci est fait, nous allons dans « Gestionnaires des services Internet (IIS) ». Nous devons avoir ceci :



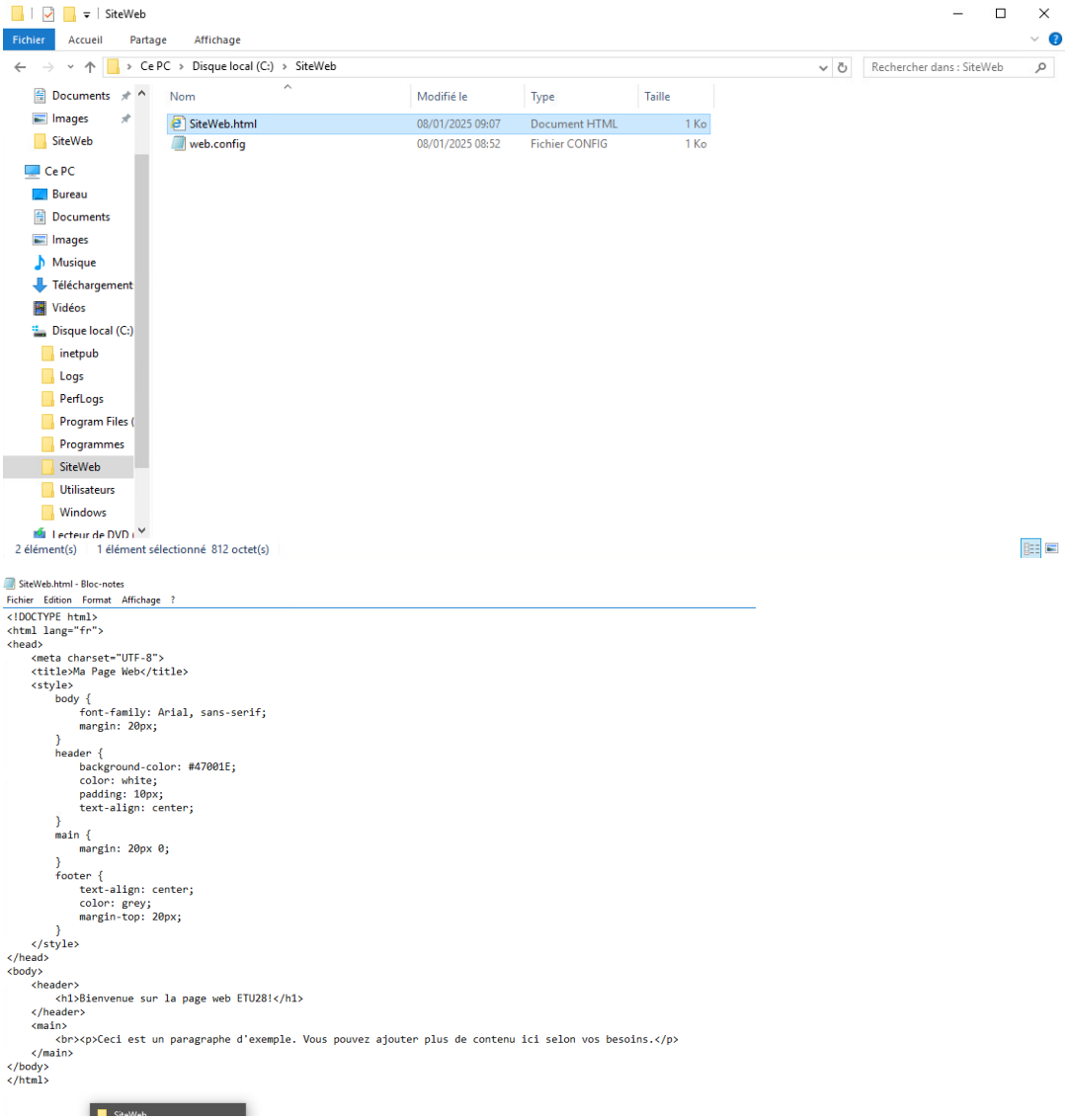
Je vais arrêter par la suite le site par défaut pour en cliquant dessus à gauche, plus dans l'onglet de droit je clique sur « Arrêter ».
Après je vais crée un nouveau site WEB en faisant clic droit sur « Sites » puis « Ajouter un site Web… »



Je mets le nom du site, le chemin d'accès physique, l'adresse IP de notre machine, comme IIS est mis sur la deuxième Windows Serveur 2016, nous avons l'adresse IP 192.168.109.22.



On crée un fichier html dans le fichier et ensuite on met les codes pour la page :

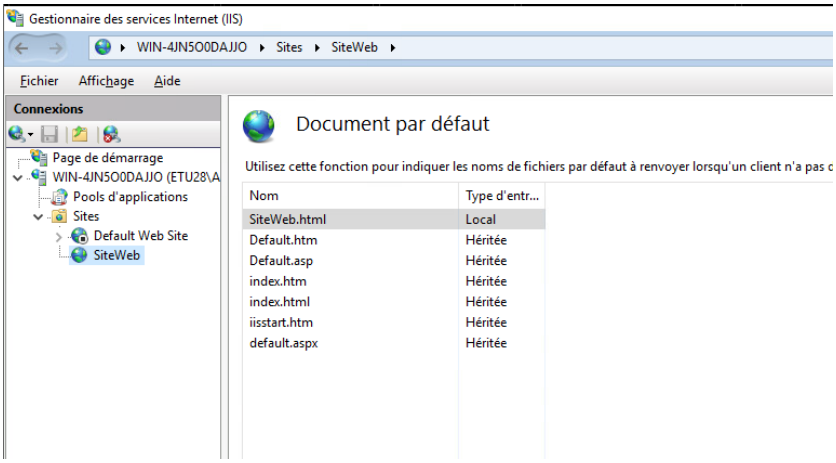


SiteWeb.html - Bloc-notes

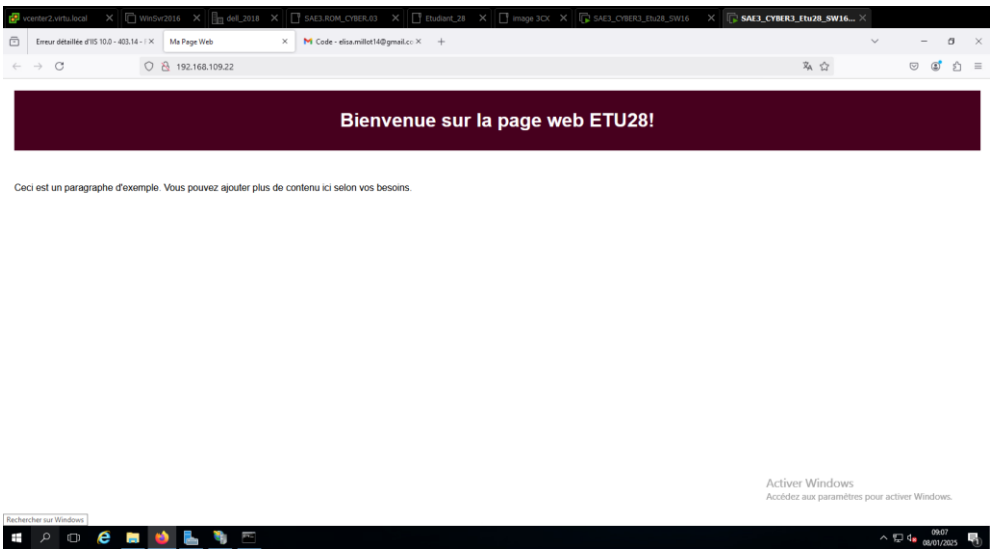
Fichier Edition Format Affichage ?

```
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <title>Ma Page Web</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            margin: 20px;
        }
        header {
            background-color: #47001E;
            color: white;
            padding: 10px;
            text-align: center;
        }
        main {
            margin: 20px 0;
        }
        footer {
            text-align: center;
            color: grey;
            margin-top: 20px;
        }
    </style>
</head>
<body>
    <header>
        <h1>Bienvenue sur la page web ETU28!</h1>
    </header>
    <main>
        <br><p>Ceci est un paragraphe d'exemple. Vous pouvez ajouter plus de contenu ici selon vos besoins.</p>
    </main>
</body>
</html>
```

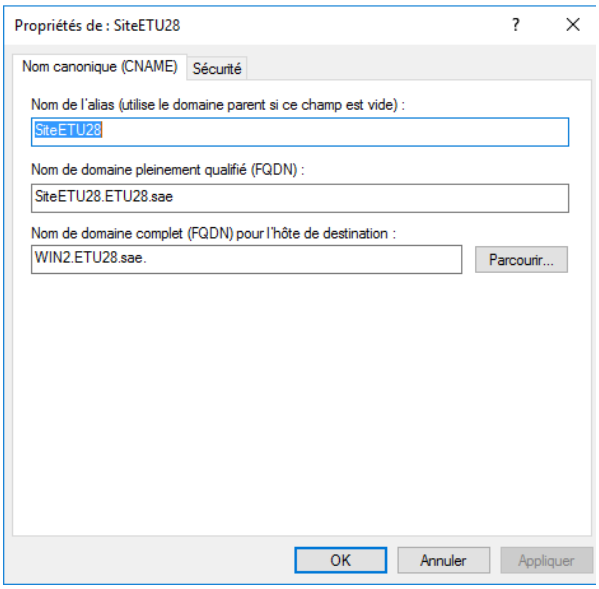
On retourne sur le « Gestionnaire des services Internet (IIS) », puis « SiteWeb » et « Document par défaut » nous mettons le fichier qu'on vient de crée en haut pour qu'il le sélectionne



Enfin quand on tape notre adresse IP sur internet nous tombons bien sur la page que nous venons de faire



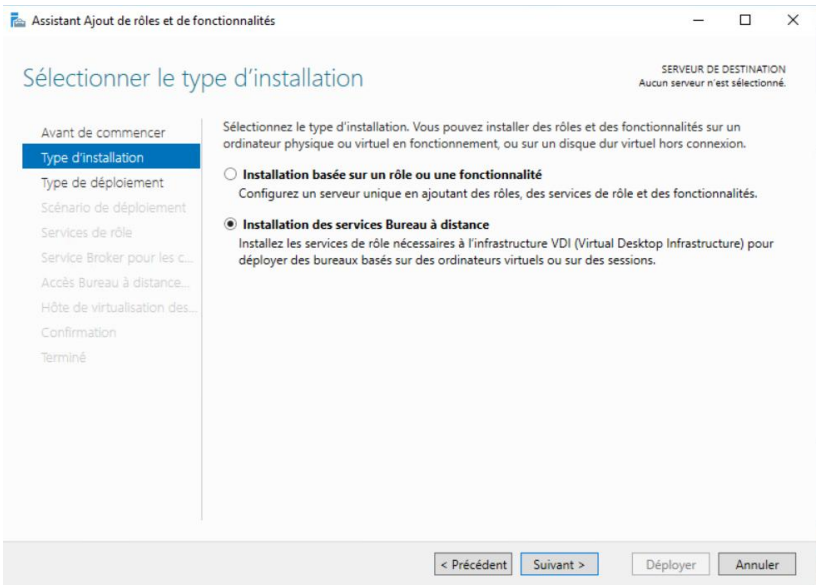
Pour finir, nous allons crée un CNAME dans notre DNS pour faire en sorte que quand on tape seulement « SiteETU28 » sur internet et ça nous met notre site. Pour cela nous allons sur le DNS, j'avais déjà créé précédemment un hôte de type A de mon deuxième serveur Windows 2016, j'ai seulement besoin de crée mon CNAME :



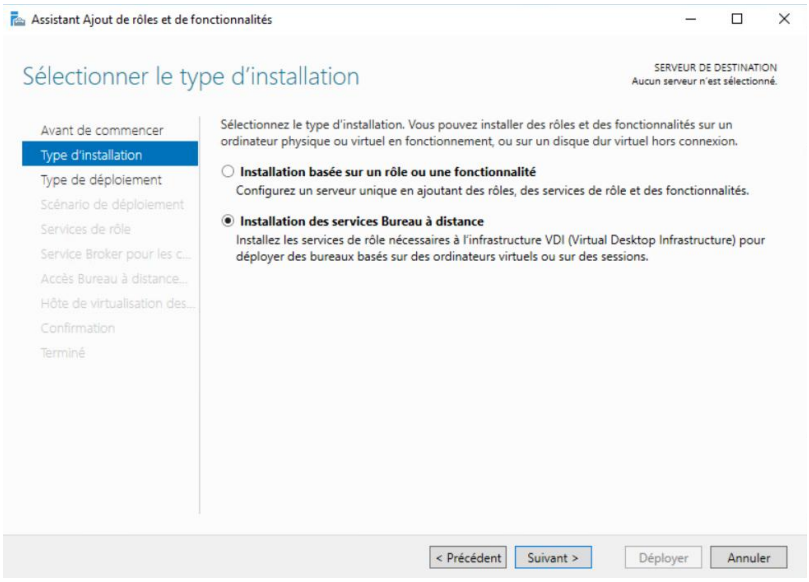
RDWeb :

Maintenant mise en place du RDWeb (https://rdr-it.com/deployer-un-serveur-rds-service-de-bureau-a-distance/) :

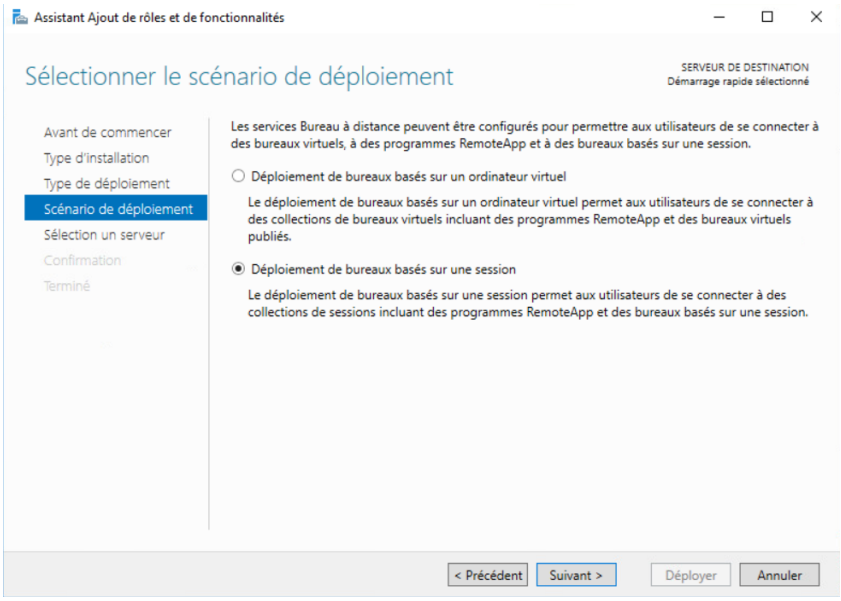
Nous allons dans « Gérer » puis « Ajouter un rôle ou une fonctionnalité » et on sélectionne « Installation des services Bureau à distance »



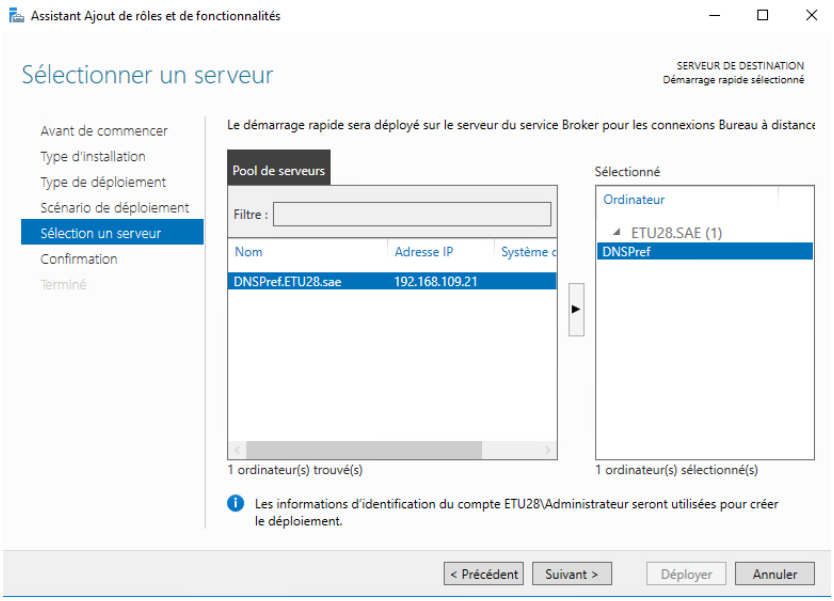
Ensuite on sélectionne « Démarrage rapide »



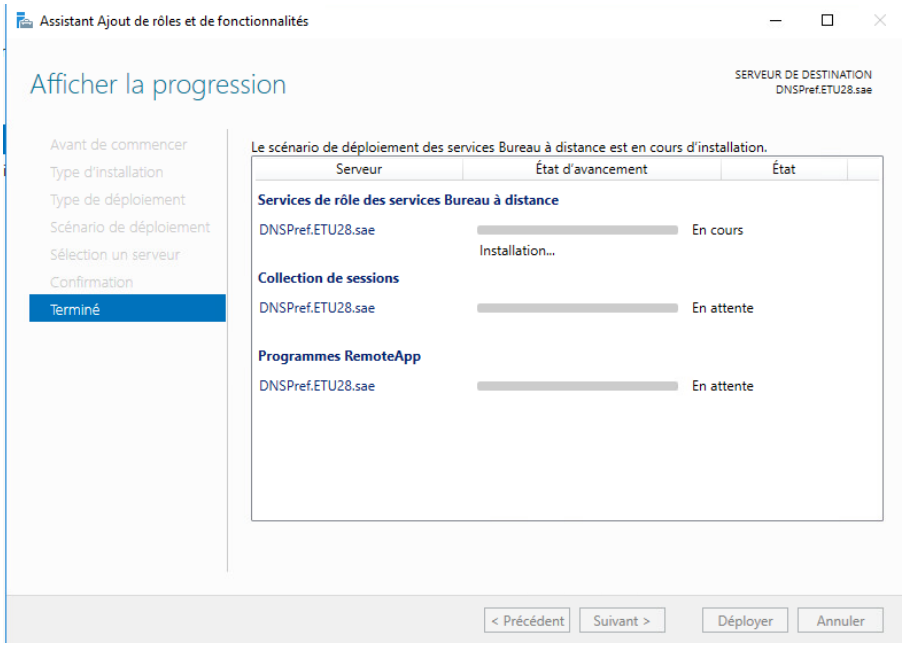
On sélectionne « Déploiement de bureau basés sur une session » car nous mettons en lien avec les comptes qu'on va crée dans l'AD-DS selon leur service ils n'auront pas les mêmes applications

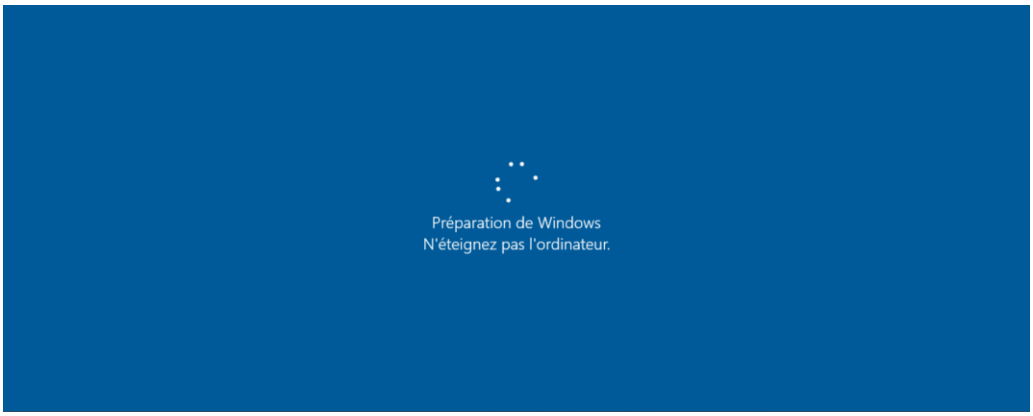


On sélectionne le serveur sur le quel nous voulons que ça soit déployer, ici je mets mon serveur principal

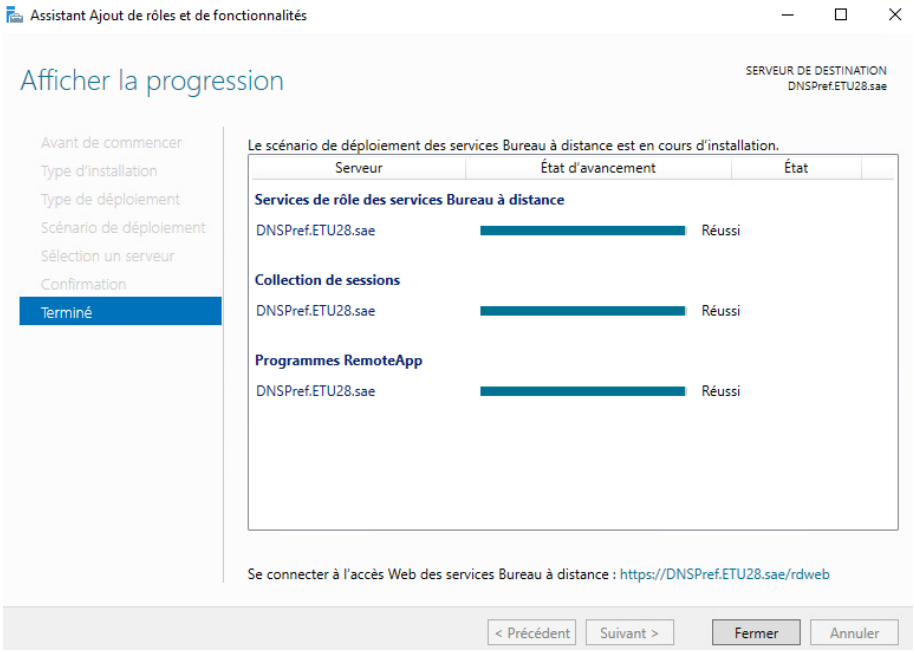


Et nous installons le service, un redémarrage est nécessaire pour mettre en place.

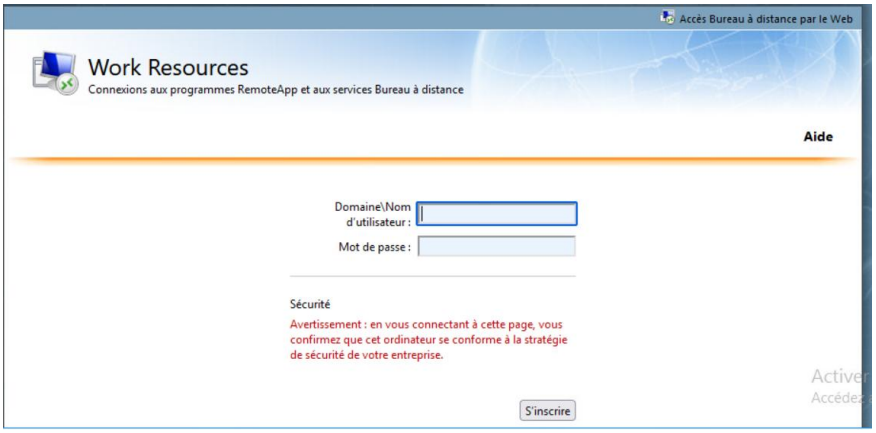




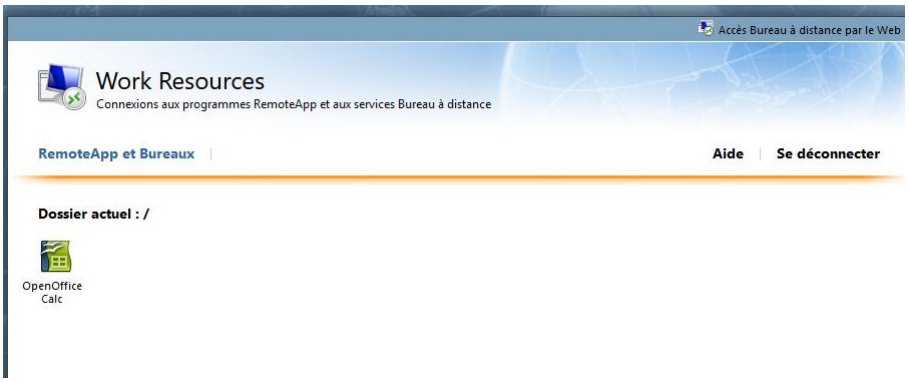
Une fois l'installation terminer, nous avons notre accès Web des service bureau à distance



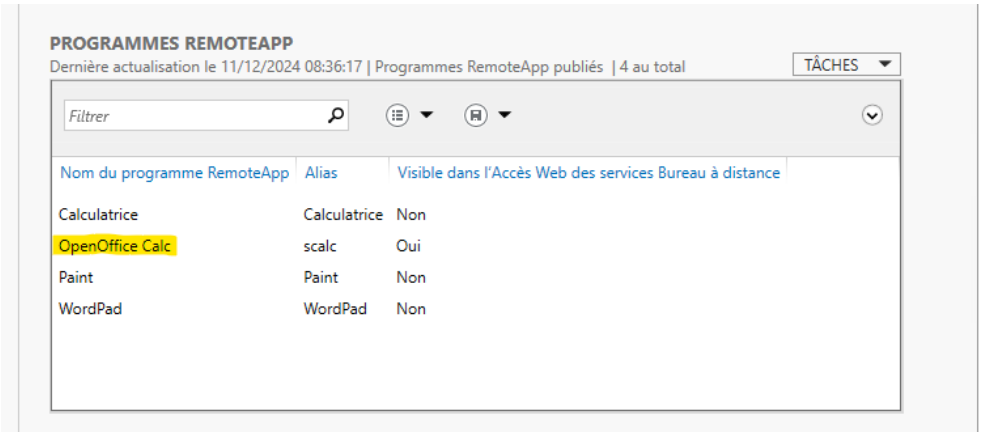
Je vais tester de me connecter sur le site avec un compte que j'ai créé sur AD-DS



Et nous accédons à cette page

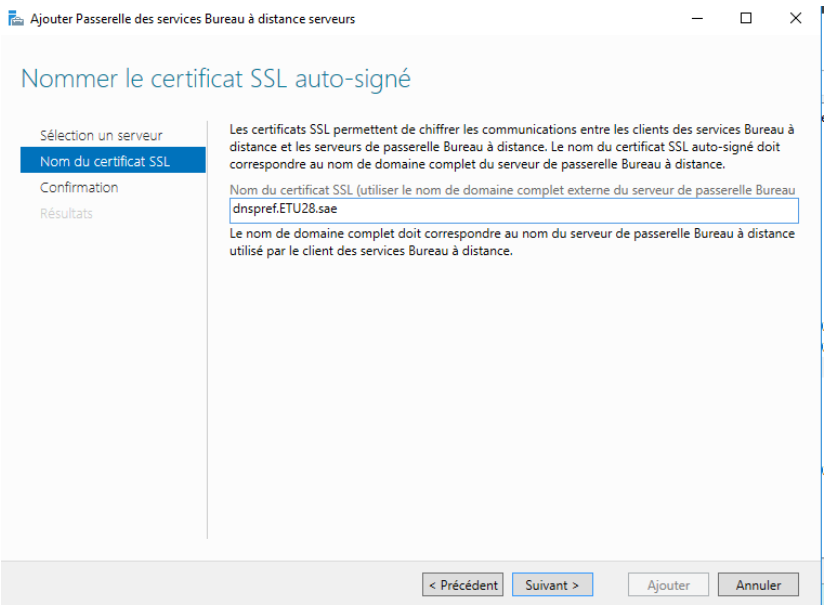


Le service RDWeb fonctionne donc bien, nous pouvons mettre en place les options pour répondre au cahier des charges. Pour cela :

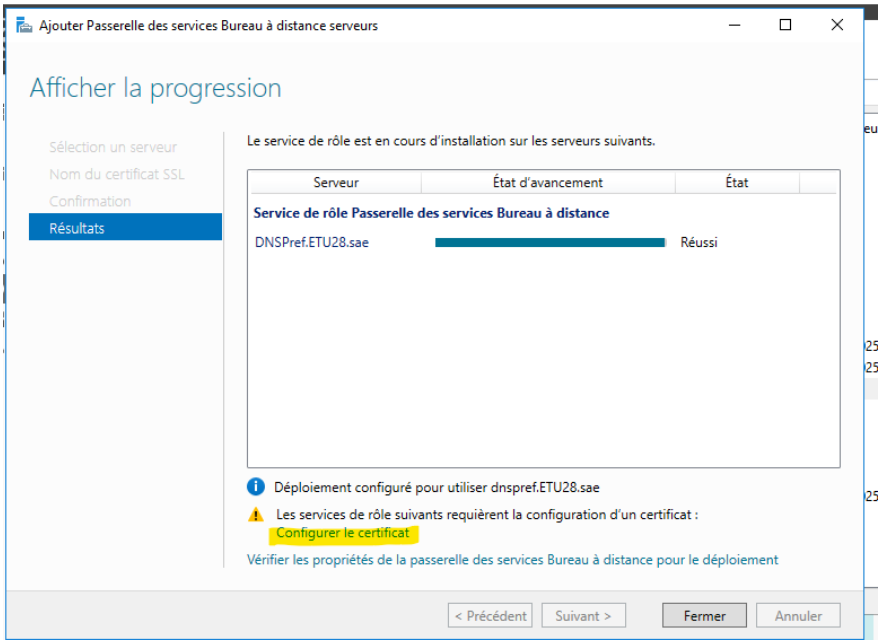


Je télécharge les applications que je dois mettre dans le RemoteAPP, j'ai téléchargé OpenOffice et Wireshark, je n'arrivais pas à installer « Acrylic ».

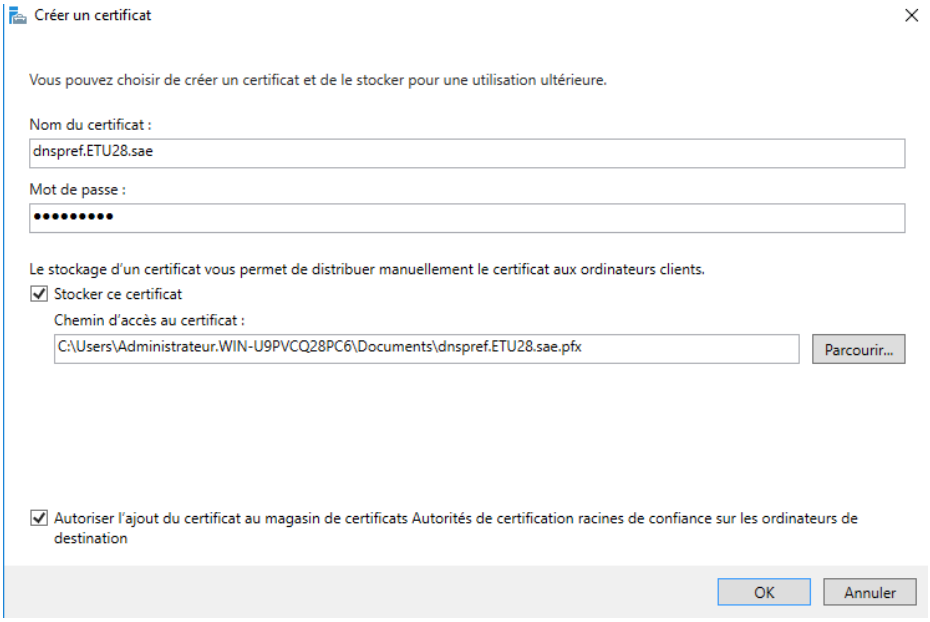
Je vais mettre en place le certificat SSL. Un certificat SSL auto-signé dans le RDWEB sert à chiffrer les communications entre les utilisateurs et le portail d'accès distant (Remote Desktop Web Access), garantissant ainsi la confidentialité des données échangées. Bien qu'il ne soit pas validé par une autorité de certification, il offre une protection basique contre l'interception des données lors des connexions.

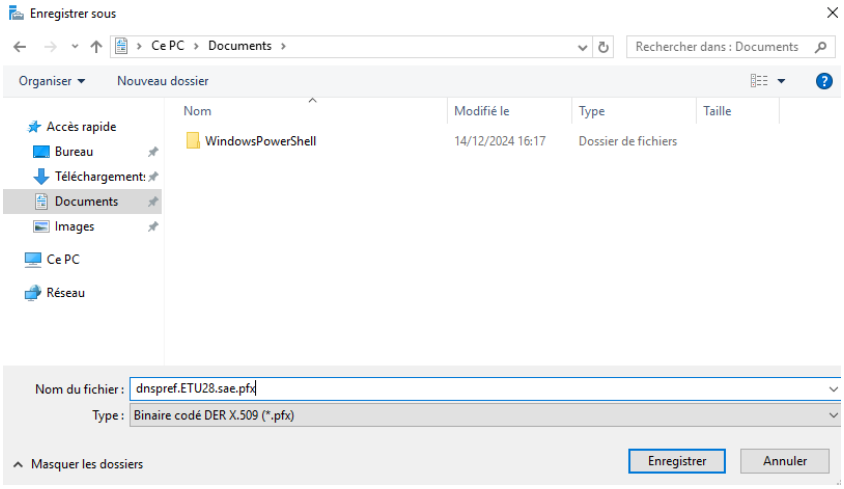


Je vais maintenant configurer le certificat.

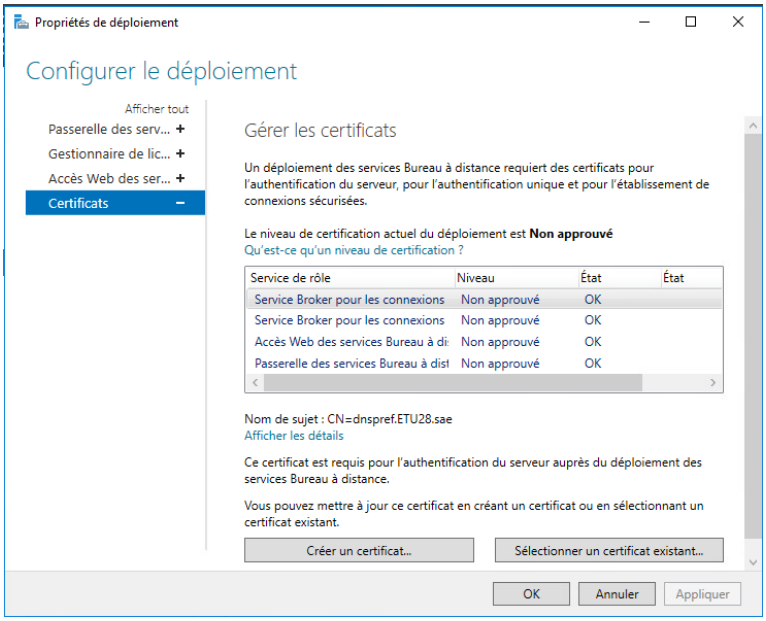


Je vais crée le certificat que je vais utiliser par la suite

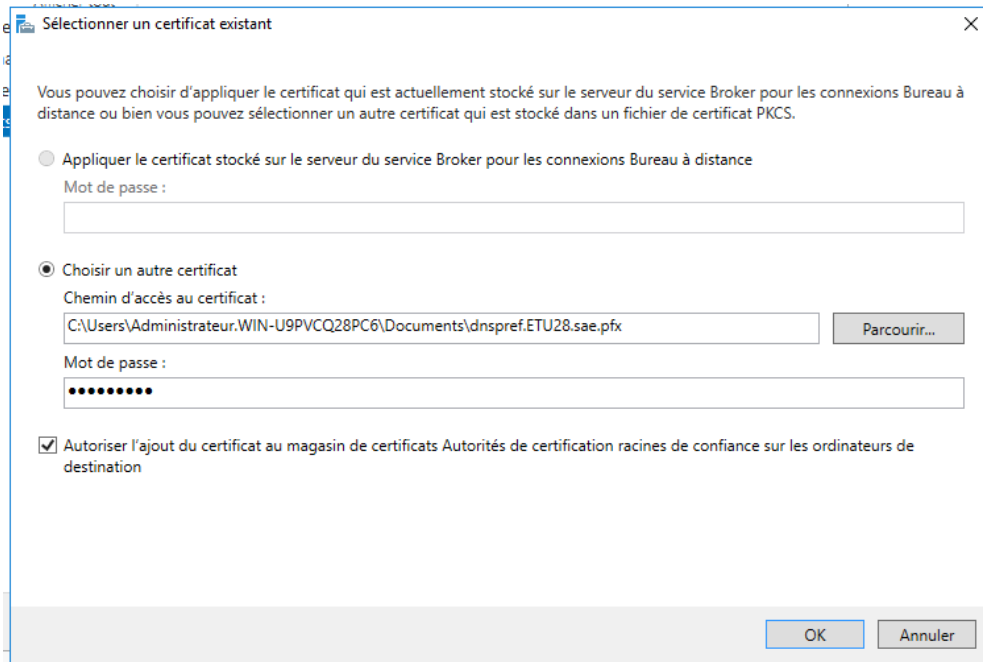




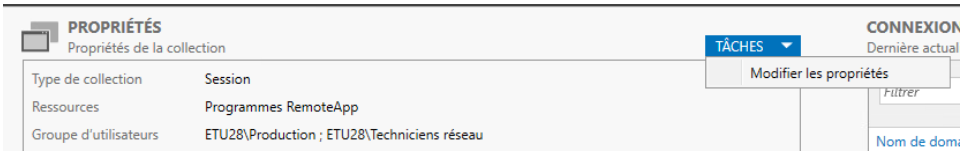
Nous allons après dans l'onglet « Certificats » et pour chaque « Service de rôle » je vais leur attribuer le certificat que je viens de crée et de télécharger sur ma machine



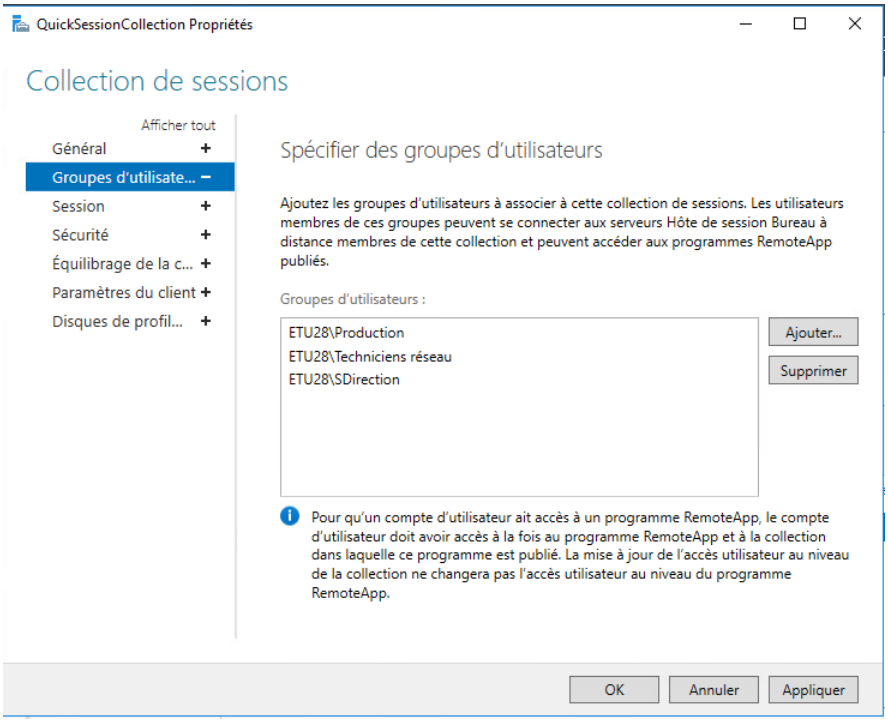
On sélectionne donc « Sélectionner u certificat existant... »



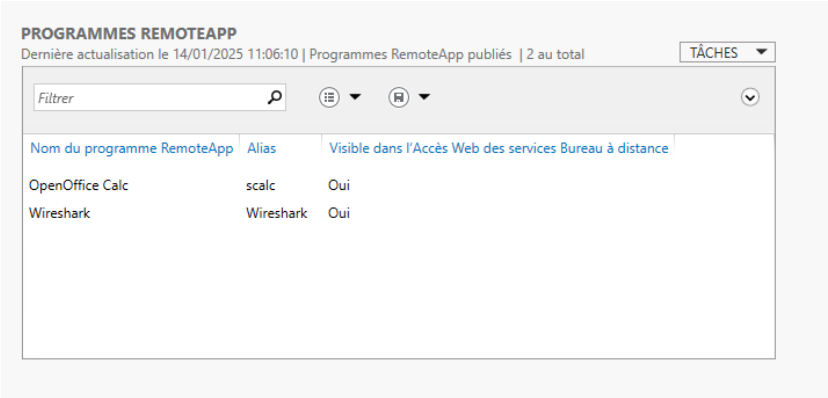
Enfin pour mettre en places, que l'application soit disponible pour qu'un seul service je vais dans « QuickSessionCollexion »

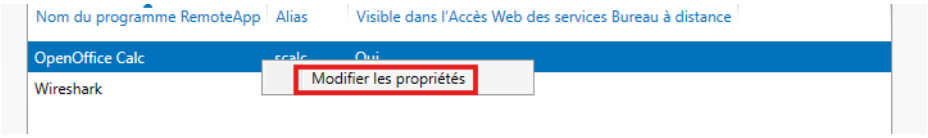


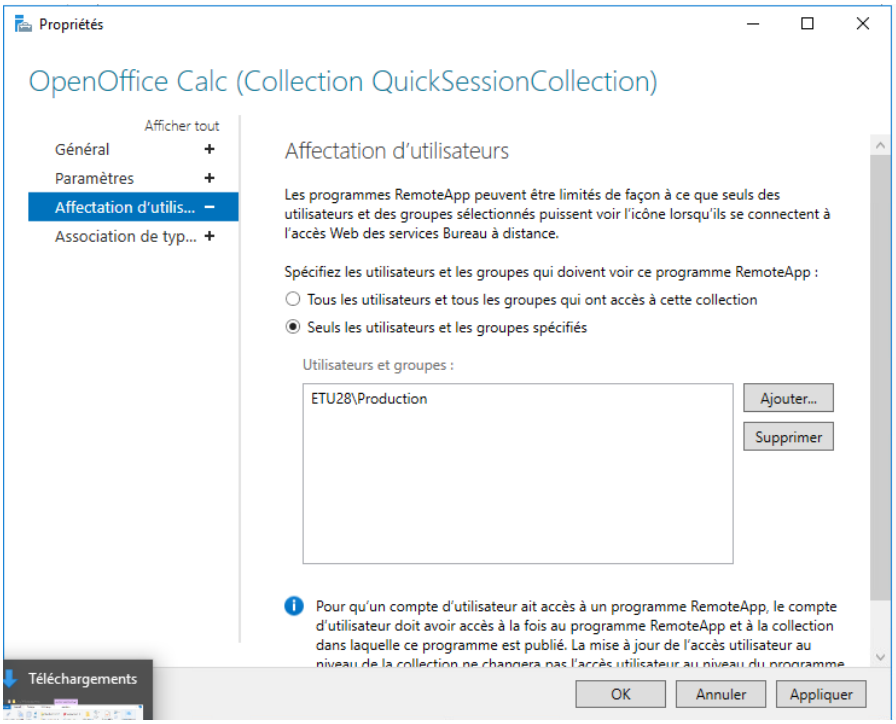
Dans « Modifier les propriétés » je vais dans « Groupes d'utilisateurs » et je séléctionne

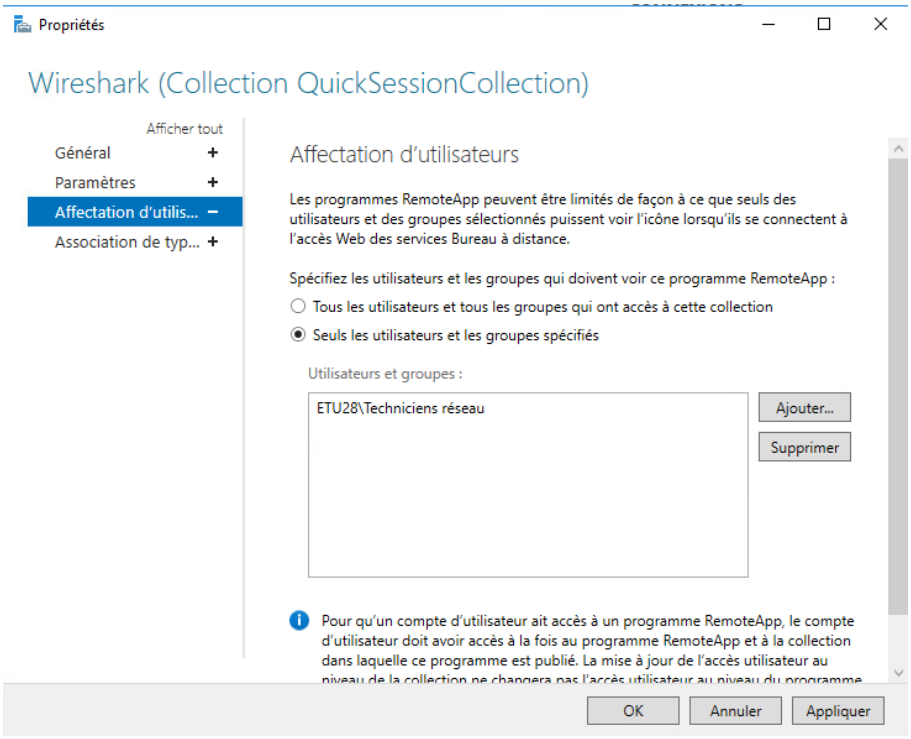


Maintenant nous allons attribuer chaque application au groupe qui doit pouvoir accès.
« OpenOffice Calc » doit être accessible seulement pour le service production, « Wireshark » est seulement pour le service réseau.









Surveillance

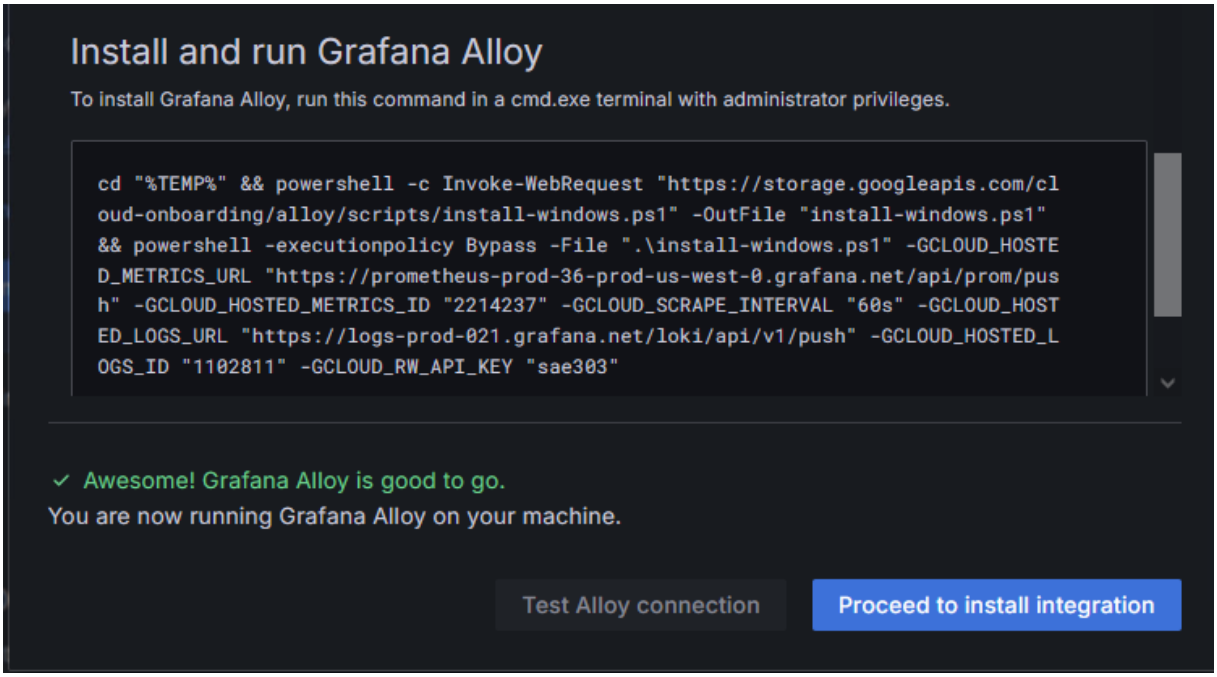
- Installation et utilisation de Grafana
- Mise en place de Prometheus, Alloy & Windows exporter
- Intégration à Windows active directory

J'ai décider de faire mon grafana sur le cloud, car nous avons un module qui s'appelle « Windows Active directory » pour avoir les informations dans l'AD-DS mais qui comporte aussi Prometheus.

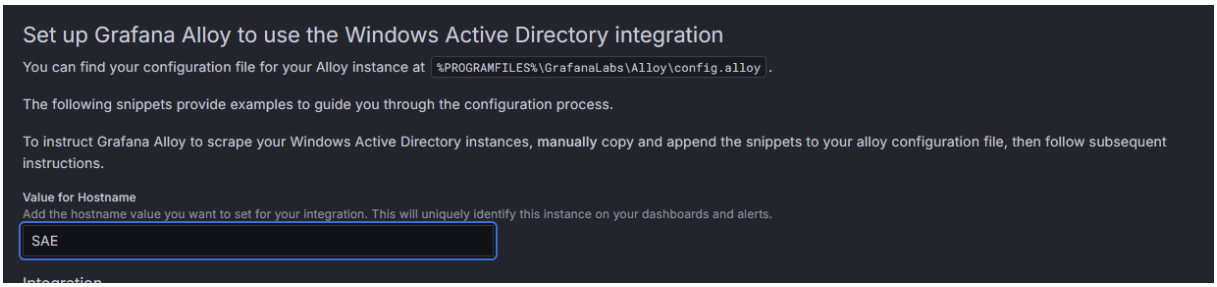
J'ai suivi ce tutoriel :

https://grafana.com/docs/grafana-cloud/monitor-infrastructure/integrations/integration-reference/integration-windows-active-directory/

J'ai installé Alloy :



J'ai modifié le fichier de configuration de Alloy :



Les modifications du fichier Alloy permet de mettre Prometheus pour surveiller l'état d'une machine et de Loki

```
prometheus.exporter.windows "integrations_windows_exporter" {
        enabled_collectors = ["ad", "cpu", "cs", "logical_disk", "net", "os", "service", "system", "textfile", "time", "diskdrive"]

        dfsr {
                sources_enabled = [""]
        }

        exchange {
                enabled_list = [""]
        }

        mssql {
                enabled_classes = [""]
        }
}

discovery.relabel "integrations_windows_exporter" {
        targets = prometheus.exporter.windows.integrations_windows_exporter.targets

        rule {
                target_label = "job"
                replacement  = "integrations/windows_exporter"
        }

        rule {
                target_label = "instance"
                replacement  = "SAE"
        }
}

prometheus.scrape "integrations_windows_exporter" {
        targets    = discovery.relabel.integrations_windows_exporter.output
        forward_to = [prometheus.relabel.integrations_windows_exporter.receiver]
        job_name   = "integrations/windows_exporter"
}

prometheus.relabel "integrations_windows_exporter" {
        forward_to = [prometheus.remote_write.metrics_service.receiver]

        rule {
                source_labels = ["volume"]
```

Administrateur : Invite de commandes - prometheus.exe --config.file=prometheus.yml

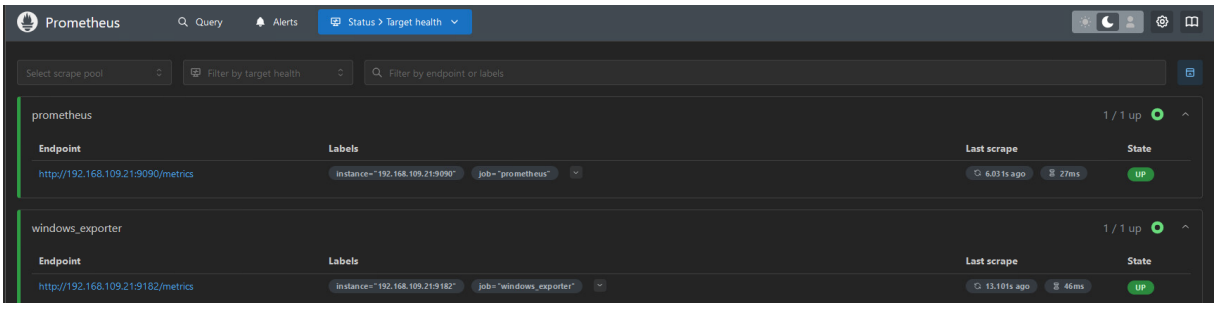
```
loki.process "logs_integrations_integrations_windows_exporter_application" {
        forward_to = [loki.write.grafana_cloud_loki.receiver]

        stage.json {
                expressions = {
                        level  = "levelText",
                        source = "source",
                }
        }

        stage.labels {
                values = {
                        level  = null,
                        source = null,
                }
        }
}

loki.relabel "logs_integrations_integrations_windows_exporter_application" {
        forward_to = [loki.process.logs_integrations_integrations_windows_exporter_application.receiver]

        rule {
                source_labels = ["computer"]
                target_label  = "agent_hostname"
        }
}

loki.source.windowsevent "logs_integrations_integrations_windows_exporter_application" {
        locale                 = 1033
        eventlog_name          = "Application"
        bookmark_path          = "./bookmarks-app.xml"
        poll_interval          = "0s"
        use_incoming_timestamp = true
        forward_to             = [loki.relabel.logs_integrations_integrations_windows_exporter_application.receiver]
        labels                 = {
                instance = "SAE",
                job      = "integrations/windows_exporter",
        }
}

loki.process "logs_integrations_integrations_windows_exporter_system" {
```

Enfin nous installons prometheus et windows_exporter :

Dans la configuration de Prometheus nous modifions seulement :

```
scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: "prometheus"
    static_configs:
      - targets: ["192.168.109.21:9090"]

  - job_name: 'windows_exporter'
    static_configs:
      - targets: ['192.168.109.21:9182']
```

Pour avoir accès aux informations de windows_exporter sur le site :



Et enfin nous lançons wndows_exporter avec :

```
PS C:\Users\Administrateur.WIN-U9PVCQ28PC6\Downloads> .\windows_exporter-0.30.1-amd64.exe --collectors.enabled="ad,cpu,cs,logical_disk,net,os,service,system"
```

Et en parallèle :

```
C:\Users\Administrateur.WIN-U9PVCQ28PC6\Downloads\prometheus-3.1.0.windows-amd64\prometheus-3.1.0.windows-amd64>prometheus.exe --config.file=prometheus.yml
```

Nous avons bien nos informations qui apparaisse sur le Grafana cloud, si l'administration a besoin d'avoir accès au Grafana je les mettrais en collaborateur sur le cloud.

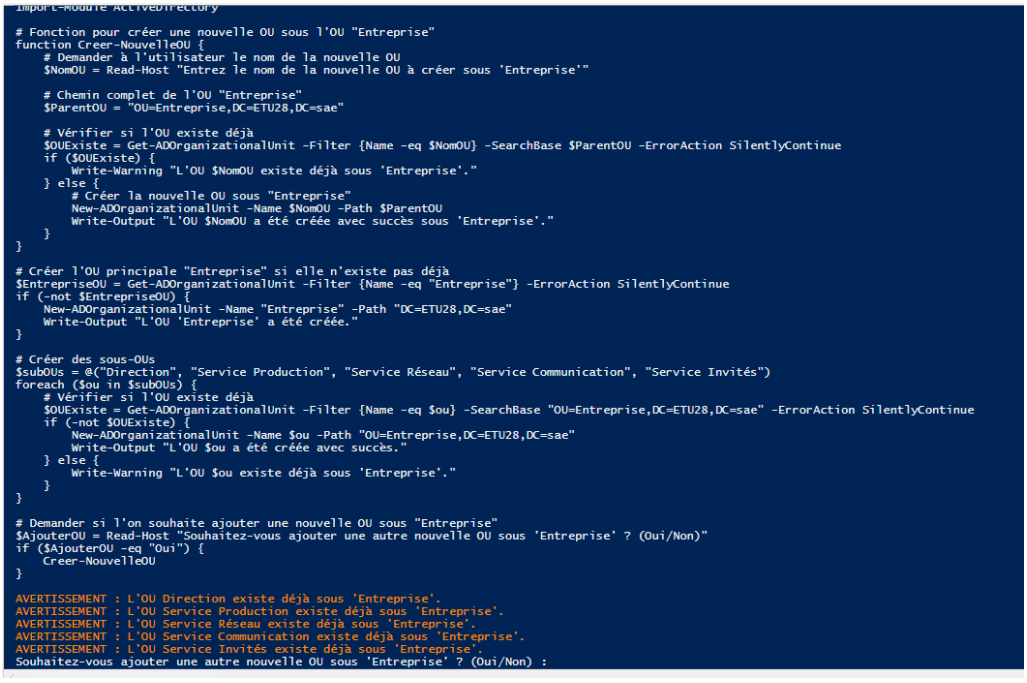
Automatisation (PowerShell et GPO)

- Scripts PowerShell utilisés pour :
    - Créer des utilisateurs et les affecter à des groupes.
    - Configurer des GPO pour restreindre ou permettre certains accès réseau.

Je voulais faire dans un premier temps un fichier EXCEL où nous rentrons les informations des personnes qui était dans l'entreprise et grâce à une commande et les informations dans le Excel ça puisse remplir l'AD-DS. Mais je n'ai pas réussi et je perdais trop de temps, je suis donc passée à un autre moyen.

J'ai créé 3 scripts PowerShell :

Le premier sert à crée la structure entière de l'entreprise, si mon serveur windows venait à planter, ou tout autre soucie, je peux recrée facilement et rapidement la structure de l'entreprise.



```
Import-Module ActiveDirectory

# Fonction pour créer une nouvelle OU sous l'OU "Entreprise"
function Creer-NouvelleOU {
    # Demander à l'utilisateur le nom de la nouvelle OU
    $NomOU = Read-Host "Entrez le nom de la nouvelle OU à créer sous 'Entreprise'"

    # Chemin complet de l'OU "Entreprise"
    $ParentOU = "OU=Entreprise,DC=ETU28,DC=sae"

    # Vérifier si l'OU existe déjà
    $OUExiste = Get-ADOrganizationalUnit -Filter {Name -eq $NomOU} -SearchBase $ParentOU -ErrorAction SilentlyContinue
    if ($OUExiste) {
        Write-Warning "L'OU $NomOU existe déjà sous 'Entreprise'."
    } else {
        # Créer la nouvelle OU sous "Entreprise"
        New-ADOrganizationalUnit -Name $NomOU -Path $ParentOU
        Write-Output "L'OU $NomOU a été créée avec succès sous 'Entreprise'."
    }
}

# Créer l'OU principale "Entreprise" si elle n'existe pas déjà
$EntrepriseOU = Get-ADOrganizationalUnit -Filter {Name -eq "Entreprise"} -ErrorAction SilentlyContinue
if (-not $EntrepriseOU) {
    New-ADOrganizationalUnit -Name "Entreprise" -Path "DC=ETU28,DC=sae"
    Write-Output "L'OU 'Entreprise' a été créée."
}

# Créer des sous-OUs
$subOUs = @("Direction", "Service Production", "Service Réseau", "Service Communication", "Service Invités")
foreach ($ou in $subOUs) {
    # Vérifier si l'OU existe déjà
    $OUExiste = Get-ADOrganizationalUnit -Filter {Name -eq $ou} -SearchBase "OU=Entreprise,DC=ETU28,DC=sae" -ErrorAction SilentlyContinue
    if (-not $OUExiste) {
        New-ADOrganizationalUnit -Name $ou -Path "OU=Entreprise,DC=ETU28,DC=sae"
        Write-Output "L'OU $ou a été créée avec succès."
    } else {
        Write-Warning "L'OU $ou existe déjà sous 'Entreprise'."
    }
}

# Demander si l'on souhaite ajouter une nouvelle OU sous "Entreprise"
$AjouterOU = Read-Host "Souhaitez-vous ajouter une autre nouvelle OU sous 'Entreprise' ? (Oui/Non)"
if ($AjouterOU -eq "Oui") {
    Creer-NouvelleOU
}

AVERTISSEMENT : L'OU Direction existe déjà sous 'Entreprise'.
AVERTISSEMENT : L'OU Service Production existe déjà sous 'Entreprise'.
AVERTISSEMENT : L'OU Service Réseau existe déjà sous 'Entreprise'.
AVERTISSEMENT : L'OU Service Communication existe déjà sous 'Entreprise'.
AVERTISSEMENT : L'OU Service Invités existe déjà sous 'Entreprise'.
Souhaitez-vous ajouter une autre nouvelle OU sous 'Entreprise' ? (Oui/Non) :
```

Le deuxième script permet de crée les groupes dans chaque OU que nous avons créé précédemment.

```
PS C:\Users\Administrateur.WIN-U9PVCQ28PC6>
# Importer le module ActiveDirectory
Import-Module ActiveDirectory

# Liste des groupes et de leurs OUs correspondantes
$groupOU = @{
    "Admins"            = "OU=Direction,OU=Entreprise,DC=ETU28,DC=sae"
    "Techniciens réseau" = "OU=Service Réseau,OU=Entreprise,DC=ETU28,DC=sae"
    "Communication"      = "OU=Service Communication,OU=Entreprise,DC=ETU28,DC=sae"
    "Production"         = "OU=Service Production,OU=Entreprise,DC=ETU28,DC=sae"
    "SInvités"           = "OU=Service Invités,OU=Entreprise,DC=ETU28,DC=sae"
}

# Créer les groupes dans les OUs spécifiées
foreach ($group in $groupOU.Keys) {
    $OU = $groupOU[$group]

    # Vérifier si le groupe existe déjà dans l'OU
    $ADGroup = Get-ADGroup -Filter {Name -eq $group} -SearchBase $OU -ErrorAction SilentlyContinue
    if ($ADGroup) {
        Write-Warning "Le groupe $group existe déjà dans l'OU $OU."
    } else {
        # Créer le groupe dans l'OU correspondante
        New-ADGroup -Name $group `
                    -GroupScope Global `
                    -GroupCategory Security `
                    -Path $OU

        Write-Output "Groupe $group créé dans l'OU $OU."
    }
}

Write-Output "Les groupes ont été créés avec succès dans leurs OUs respectives."




AVERTISSEMENT : Le groupe Communication existe déjà dans l'OU OU=Service Communication,OU=Entreprise,DC=ETU28,DC=sae.
AVERTISSEMENT : Le groupe Production existe déjà dans l'OU OU=Service Production,OU=Entreprise,DC=ETU28,DC=sae.
AVERTISSEMENT : Le groupe Techniciens réseau existe déjà dans l'OU OU=Service Réseau,OU=Entreprise,DC=ETU28,DC=sae.
AVERTISSEMENT : Le groupe SInvités existe déjà dans l'OU OU=Service Invités,OU=Entreprise,DC=ETU28,DC=sae.
AVERTISSEMENT : Le groupe Admins existe déjà dans l'OU OU=Direction,OU=Entreprise,DC=ETU28,DC=sae.
Les groupes ont été créés avec succès dans leurs OUs respectives.

PS C:\Users\Administrateur.WIN-U9PVCQ28PC6>
```

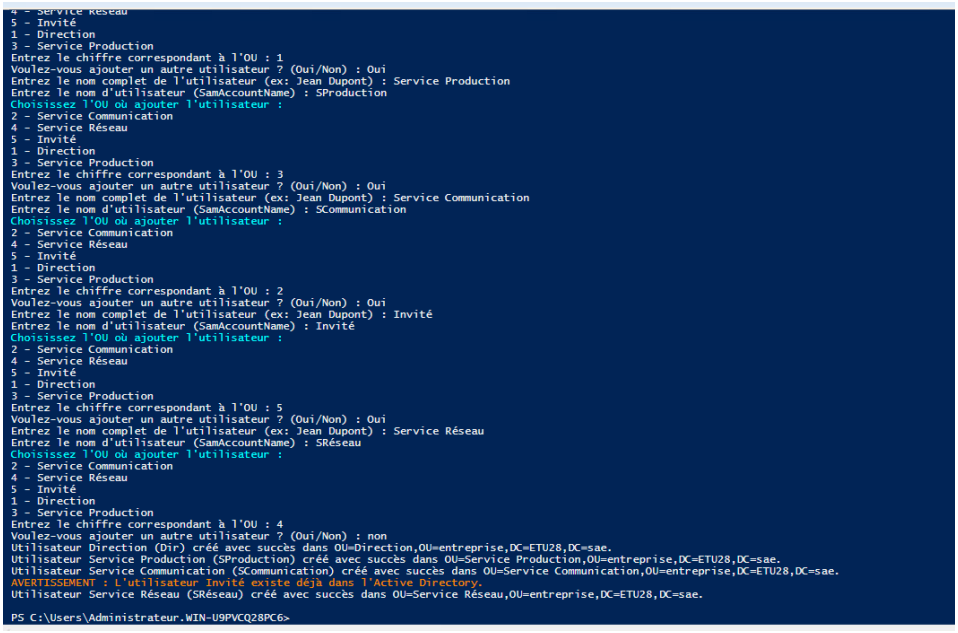
Et le dernier script permet de crée les utilisateurs et de les rangés selon ou nous voulons.

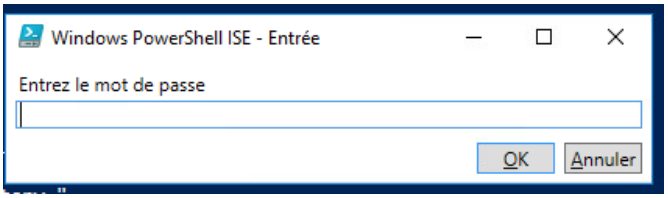
```
PS C:\Users\Administrateur.WIN-U9PVCQ28PC6>
# Liste des OUs disponibles sous ETU28.sae et leurs groupes associés
$ListeOUs = @{
    "1" = @{
        "Path"  = "OU=Direction,OU=entreprise,DC=ETU28,DC=sae"
        "Group" = "Admins"
    }
    "2" = @{
        "Path"  = "OU=Service Communication,OU=entreprise,DC=ETU28,DC=sae"
        "Group" = "Communication"
    }
    "3" = @{
        "Path"  = "OU=Service Production,OU=entreprise,DC=ETU28,DC=sae"
        "Group" = "Production"
    }
    "4" = @{
        "Path"  = "OU=Service Réseau,OU=entreprise,DC=ETU28,DC=sae"
        "Group" = "Techniciens réseau"
    }
    "5" = @{
        "Path"  = "OU=Service Invités,OU=entreprise,DC=ETU28,DC=sae"
        "Group" = "SInvités"
    }
}

# Fonction pour afficher les choix d'OU
function Choisir-OU {
    Write-Host "Choisissez l'OU où ajouter l'utilisateur :" -ForegroundColor Cyan
    $ListeOUs.GetEnumerator() | ForEach-Object {
        Write-Host "$($_.Key) - $($_.Value.Path.Split(',')[0].Split('=')[1])"
    }
    do {
        $Choix = Read-Host "Entrez le chiffre correspondant à l'OU"
    } while (-not $ListeOUs.ContainsKey($Choix))
    return $ListeOUs[$Choix]
}
```

```
# Initialisation d'une liste vide pour stocker les utilisateurs
$Utilisateurs = @()

do {
    # Demander les informations pour chaque utilisateur
    $NomComplet = Read-Host "Entrez le nom complet de l'utilisateur (ex: Jean Dupont)"
    $NomUtilisateur = Read-Host "Entrez le nom d'utilisateur (SamAccountName)"
    $MotDePasse = Read-Host "Entrez le mot de passe (Complexe)" -AsSecureString

    # Choix de l'OU
    $OUSelection = Choisir-OU
    $OUPath = $OUSelection.Path
    $Group = $OUSelection.Group

    # Ajouter les informations dans la liste
    $Utilisateurs += [PSCustomObject]@{
        NomComplet     = $NomComplet
        NomUtilisateur = $NomUtilisateur
        MotDePasse     = $MotDePasse
        OU             = $OUPath
        Groupe         = $Group
    }

    # Demander si un autre utilisateur doit être ajouté
    $AjouterAutre = Read-Host "Voulez-vous ajouter un autre utilisateur ? (Oui/Non)"
} while ($AjouterAutre -eq "Oui")
```

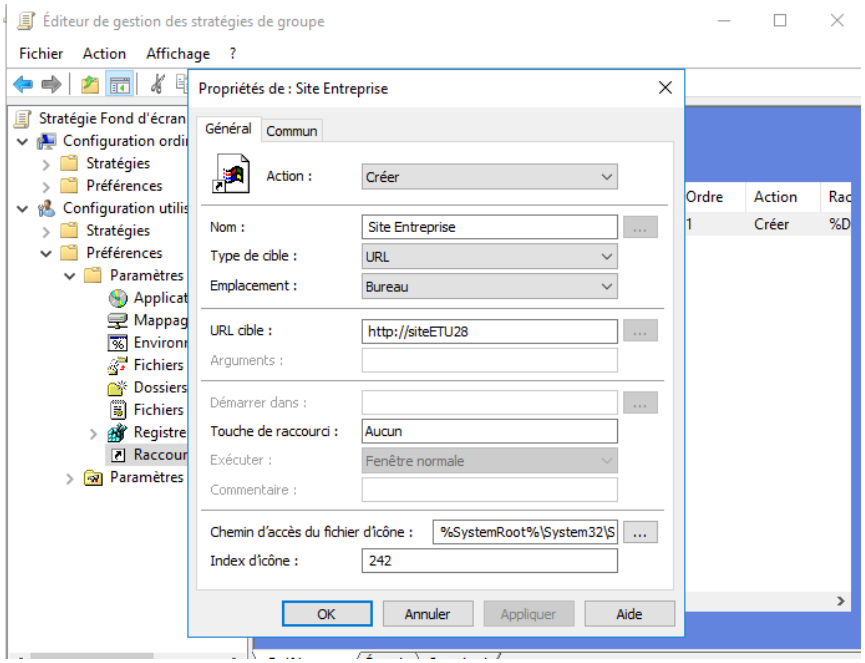
```
# Parcourir la liste des utilisateurs pour les ajouter dans Active Directory
foreach ($Utilisateur in $Utilisateurs) {
    $NomComplet     = $Utilisateur.NomComplet
    $NomUtilisateur = $Utilisateur.NomUtilisateur
    $MotDePasse     = $Utilisateur.MotDePasse
    $OUPath         = $Utilisateur.OU
    $Group          = $Utilisateur.Groupe

    # Vérifier si l'utilisateur existe déjà dans Active Directory
    $ADUser = Get-ADUser -Filter {SamAccountName -eq $NomUtilisateur} -ErrorAction SilentlyContinue
    if ($ADUser) {
        Write-Warning "L'utilisateur $NomUtilisateur existe déjà dans l'Active Directory."
    } else {
        # Créer l'utilisateur dans Active Directory
        try {
            New-ADUser -Name $NomComplet `
                       -SamAccountName $NomUtilisateur `
                       -UserPrincipalName "$NomUtilisateur@etu28.sae" `
                       -AccountPassword (ConvertTo-SecureString -String $MotDePasse -AsPlainText -Force) `
                       -Enabled $true `
                       -ChangePasswordAtLogon $true `
                       -Path $OUPath `
                       -GivenName ($NomComplet.Split(" ")[0]) `
                       -Surname ($NomComplet.Split(" ")[1])
            Write-Output "Utilisateur $NomComplet ($NomUtilisateur) créé avec succès dans $OUPath."

            # Ajouter l'utilisateur au groupe associé
            Add-ADGroupMember -Identity $Group -Members $NomUtilisateur
            Write-Output "L'utilisateur $NomUtilisateur a été ajouté au groupe $Group."
        } catch {
            Write-Error "Erreur lors de la création de l'utilisateur $NomUtilisateur ou de son ajout au groupe $Group : $_"
        }
    }
}

Entrez le nom complet de l'utilisateur (ex: Jean Dupont) : |
```

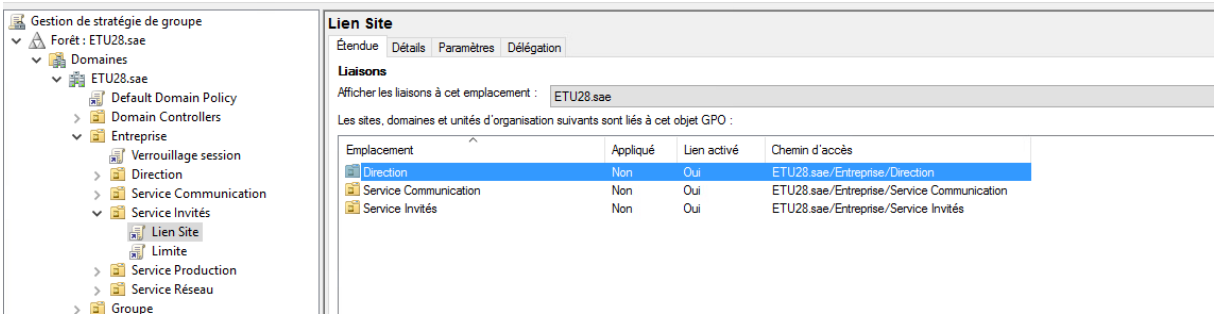
Donc j’ai entrée tout mes utilisateurs grâce à mon script :



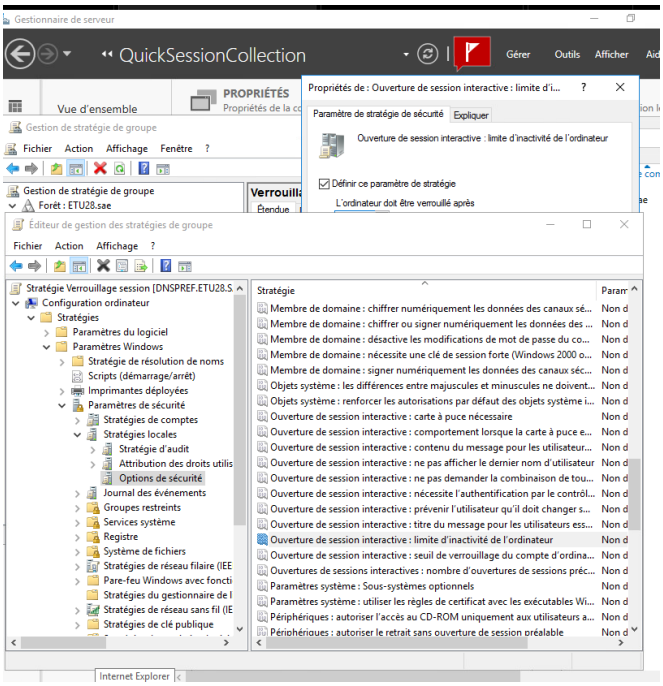


Les GPO j'ai fait par interface graphique. J'ai fait en sorte d'avoir le futur site de l'entreprise directement sur le bureau ? Seulement pour les comptes qui se trouve dans les groupes invités, communication & direction.





J'ai fait comme autre GPO, le verrouillage de session au bout de 600secondes d'inactivité sur l'ordinateur pour toutes l'entreprise.

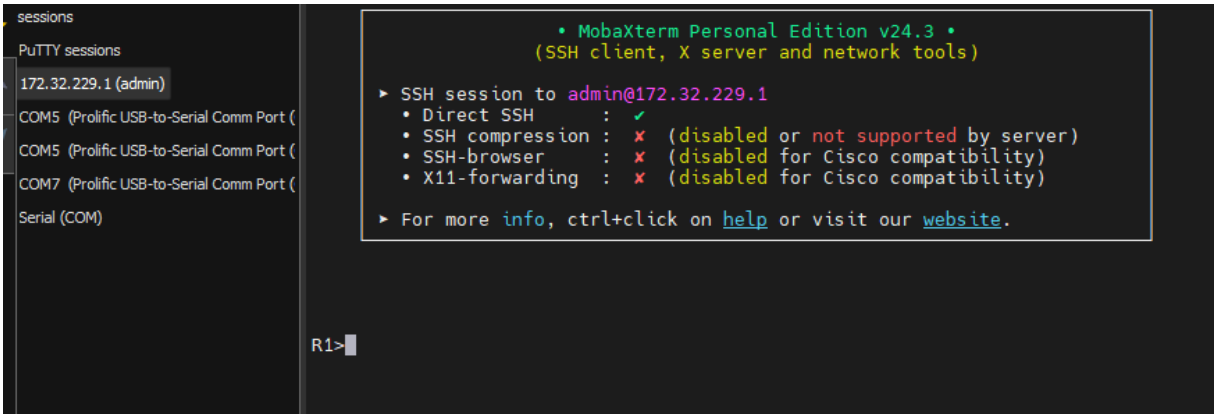


4. Tests et Résultats

Tests fonctionnels

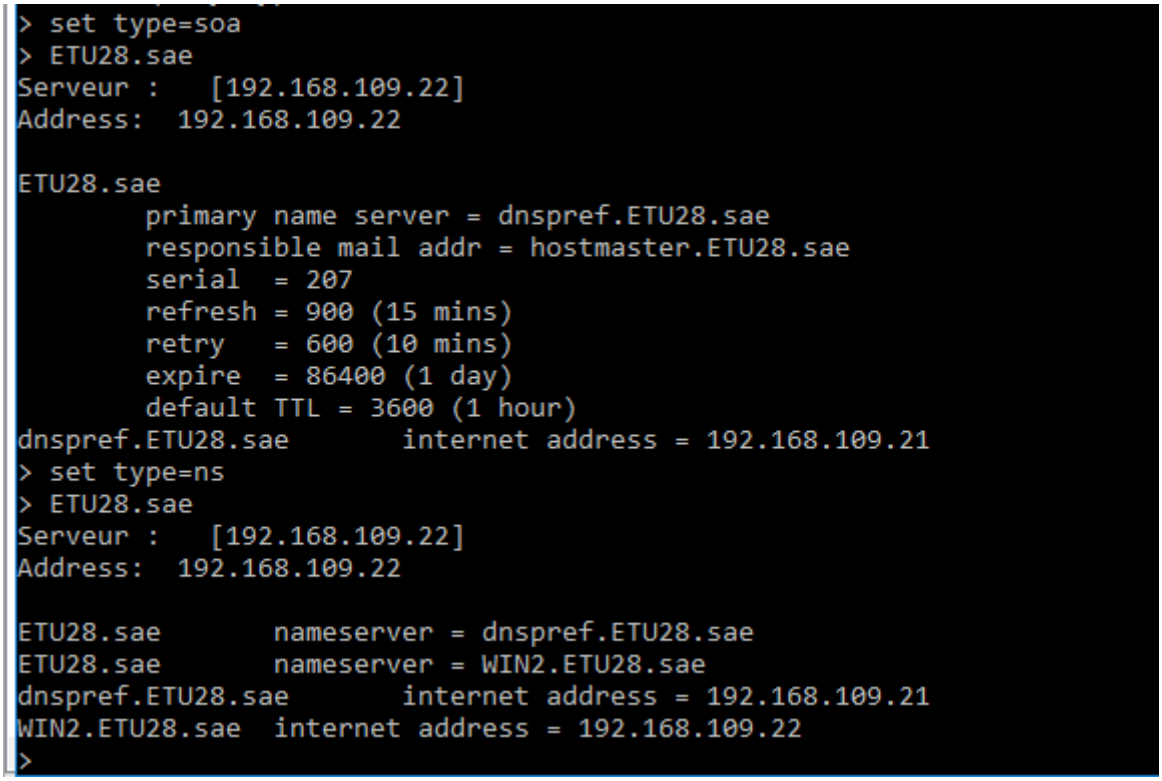
- Réseau, connexion en SSH

Nous nous connectons au R1 grâce à IP 172.32.229.1, la création du SSH étant identique sur l'autre routeur et switch, la connexion fonction avec les IP qui se trouve sur les interfaces.



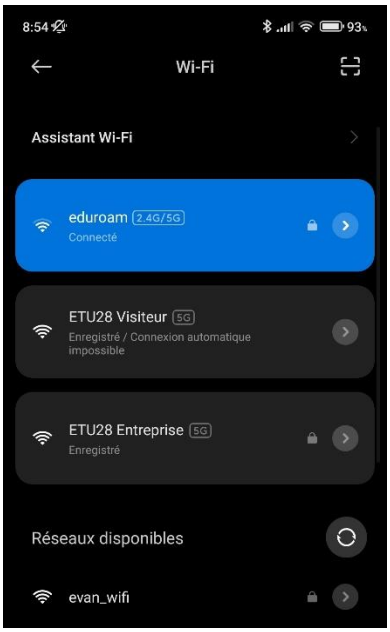
- Résolution DNS, attribution DHCP, accès WiFi validés.

DNS :

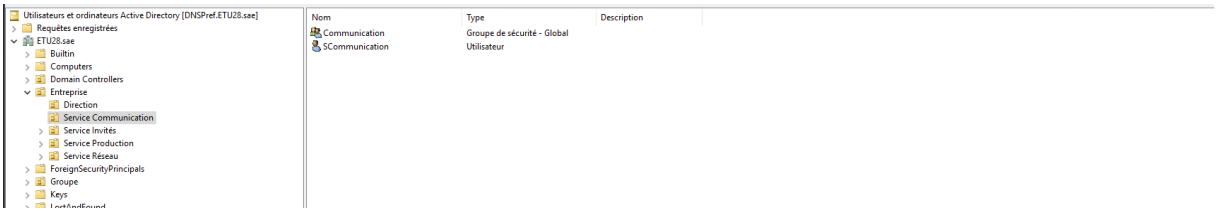


DHCP :

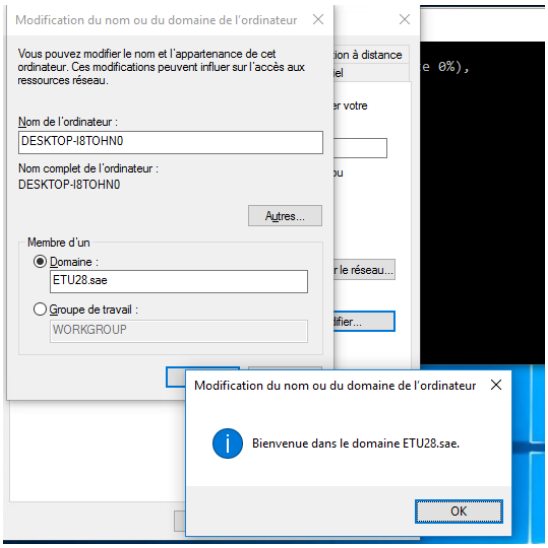
Wifi :



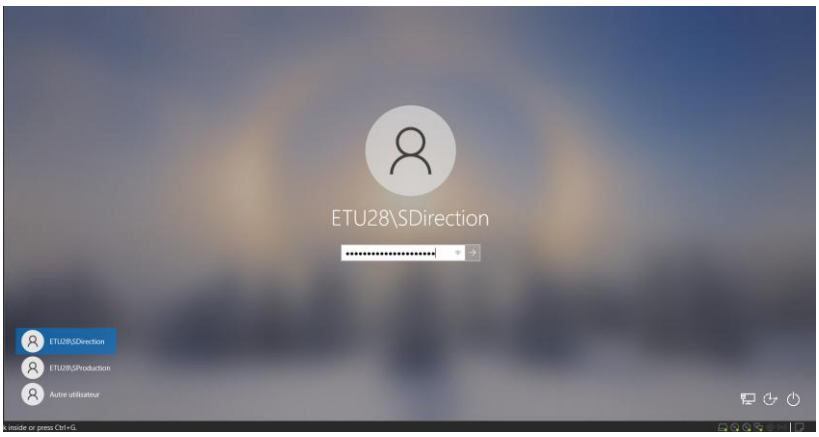
- Vérification que les scripts de l'AD-DS crée bien les OU, Groupes et Utilisateurs.



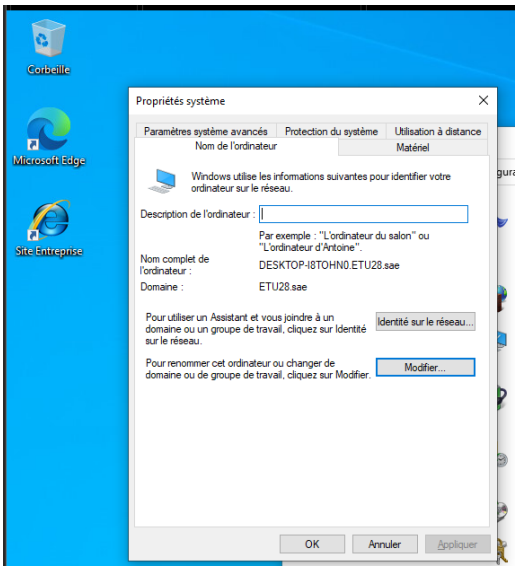
- Intégration d'une machine virtuelle et d'un pc de l'IUT dans AD-DS et les GPO



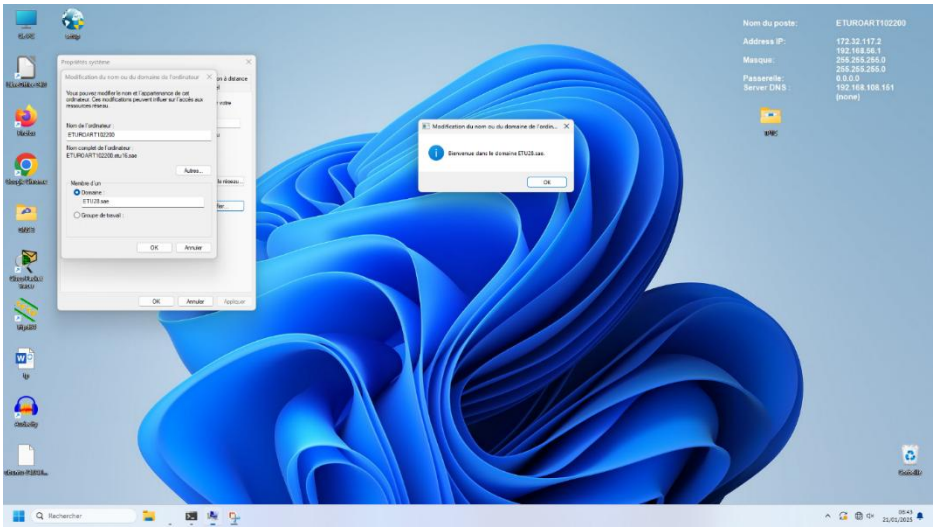
Redémarrage



Après redémarrage pour l'intégration dans AD-DS. Connexion avec l'utilisateur Direction, nous voyons que nous avons notre GPO:

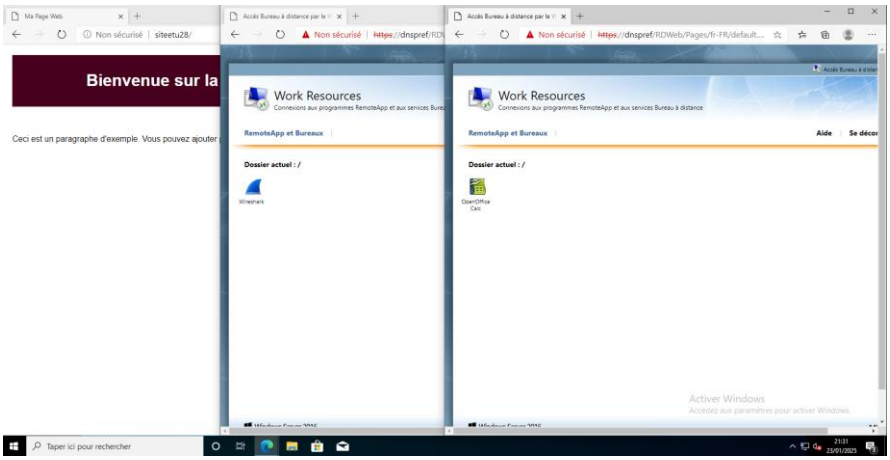


Même chose pour une machine physique qui se trouvais sur le réseau de IUT

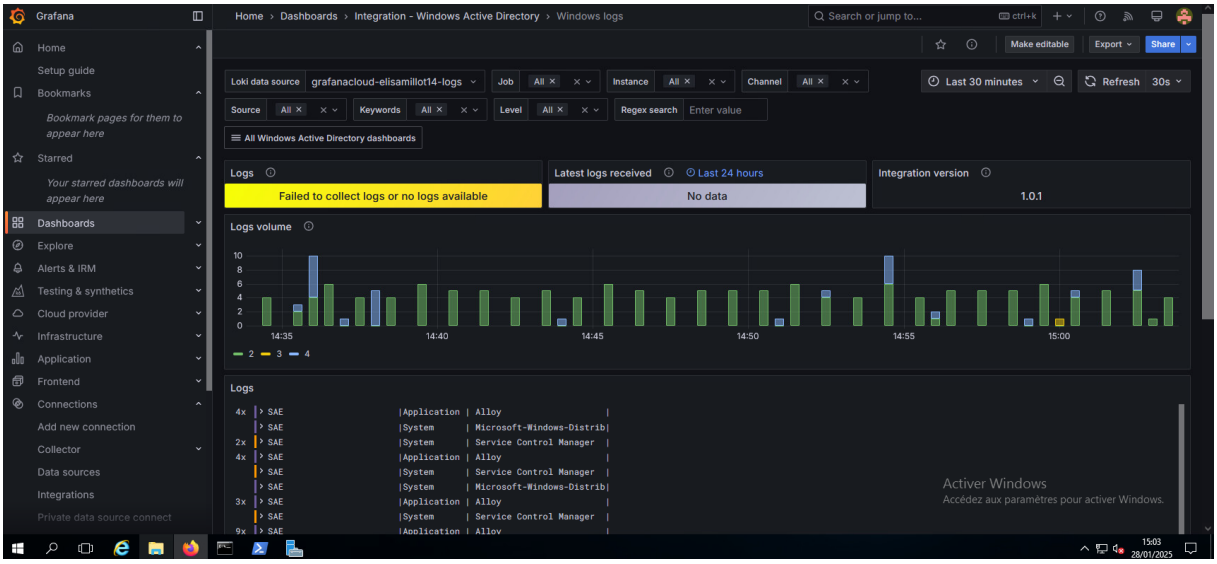


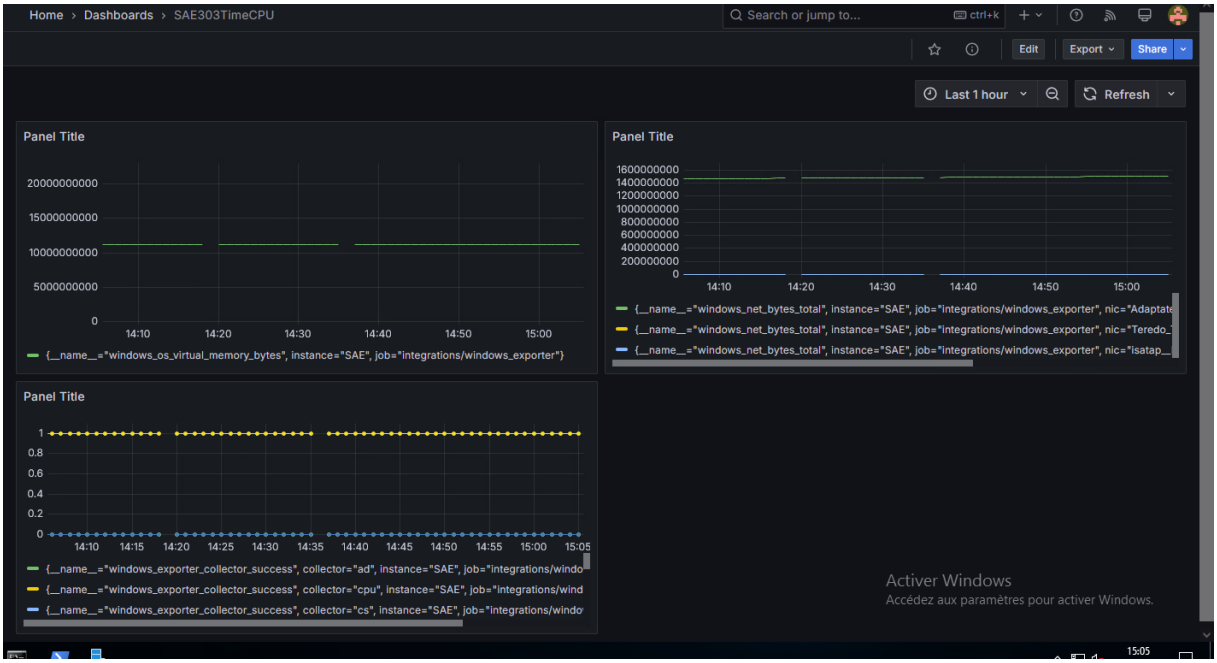
- Accès distant aux logiciels et site web.

A droite notre site internet, nous avons aussi une connexion au RDWeb avec un compte Réseau et un autre avec le service Production.



- Surveillance Grafana :





5. Problème rencontrée et solutions & amélioration :

Problèmes rencontrés et solutions

Correction des passerelles pour assurer la communication entre les VM et le pare-feu

Lors de la configuration initiale, certaines VM ne parvenaient pas à communiquer avec le réseau en raison d'une mauvaise du pare-feu et configuration des passerelles. Ce problème a été résolu en ajustant les paramètres réseau sur les interfaces concernées, en s'assurant que les VLANs et les routes OSPF étaient correctement définis. Cela a permis une communication fluide entre les différents équipements du réseau et les VM.

Mise en place de TFTPD64 avec le serveur DHCP et blocage DHCP sur le réseau via ACL

Pour déployer un serveur DHCP fonctionnel, TFTPD64 a été configuré pour attribuer des adresses IP dynamiques aux postes clients. Cela a permis d'assurer une distribution efficace des adresses sans intervention manuelle. Afin d'éviter que le DHCP interfère avec d'autres parties du réseau, des ACL (Access Control Lists) ont été mises en place sur le routeur 2. Ces ACL bloquent les paquets DHCP sur les ports 67 et 68, empêchant ainsi les demandes DHCP de se propager au-delà du segment réseau défini. Cette solution garantit que seules les machines autorisées reçoivent des adresses IP depuis le serveur DHCP configuré.

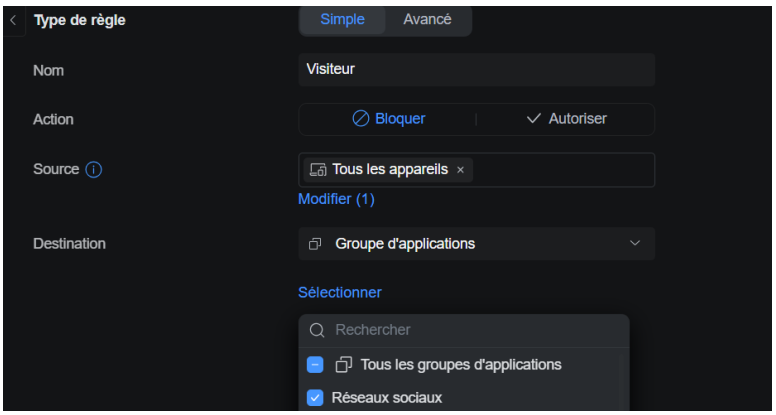
Améliorations à apporter

Faire fonctionner le serveur Radius

D'après certains tutoriels trouver il aurait fallu installer AD-CS qui est un serveur de certification. Le serveur Radius n'a pas pu être testé avec des certificats, mais une configuration potentiellement complète a été mise en place. Il est probable que l'utilisation des certificats permette de finaliser l'intégration avec succès.

Configuration Wi-Fi sécurisée

Pour le Wi-Fi, il reste à tester son intégration avec Radius. Une fois en place, il serait intéressant de configurer une restriction d'accès aux réseaux sociaux depuis l'interface de gestion Unifi, dans la section Sécurité. Cela renforcerait la productivité en limitant l'utilisation non professionnelle du réseau.



Redondance des services AD-DS

Pour améliorer la robustesse de l'infrastructure, il serait utile d'ajouter un deuxième contrôleur de domaine pour garantir la redondance en cas de panne du serveur principal. Cette configuration améliorerait la disponibilité des services comme l'authentification et le DNS.

Résolution des problèmes de transfert d'informations entre Prometheus et Grafana Cloud

Bien que Windows Exporter soit correctement configuré pour récupérer les informations de l'Active Directory et que ces données soient visibles sur Prometheus, elles n'arrivent pas jusqu'à Grafana Cloud. Ce problème nécessite une analyse approfondie de la configuration du fichier Prometheus (prometheus.yml) pour s'assurer que les endpoints sont correctement définis et accessibles depuis Grafana Cloud. Une vérification des permissions et des paramètres d'intégration côté Grafana Cloud pourrait également résoudre cette limitation. Cela permettrait d'avoir une vue complète des performances et des alertes directement sur Grafana Cloud, facilitant ainsi la supervision centralisée du réseau.

6. Conclusion :

Conclusion

Cette SAE a été enrichissante, bien que certains aspects aient manqué de clarté, notamment autour du Radius et du Wi-Fi. Concernant le Wi-Fi, le manque de pratique a été un frein, car je n'ai pu assister au seul TP sur le sujet. Même en consultant les comptes rendus de mes collègues, il m'a manqué des informations pour finaliser cette partie. Néanmoins, cette SAE m'a permis de développer des compétences techniques variées et essentielles, allant de la configuration réseau à l'automatisation des tâches administratives. Les nombreux aspects couverts montrent l'importance d'une bonne planification et d'une compréhension approfondie des systèmes pour déployer un réseau sécurisé et fonctionnel.

7. Annexe :

Fichier AD-DS.txt comportant les 3 scripts permettant de crée les OU, les Groupes et les Utilisateurs.

Fichier Réseau.txt comportant les 3 configurations du routeur 1 (Connecter au réseau enseignant), routeur 2 et le switch.

Mot de passe Serveur Windows 2016 : SAE3.328-

Mot de passe compte sur l'AD-DS : NouveauMotDePasse123 !