

COMPTE RENDU SAE3.CYBER03

CONTEXTE

Votre responsable administration réseaux vous demande de concevoir et tester un nouveau réseau permettant d'accéder aux services et aux ressources de l'entreprise. Vous utiliserez toutes vos compétences pour faire évoluer le réseau.

VCENTER

Login : Sae_Etu1

Mot de passe : 6-j5r3^Q

NOM	MOT DE PASSE	ADRESSE IP
Serveur DNS Primaire : SAE3-SW16	etu1SAE3	192.168.108.1
Serveur DNS Secondaire : SAE3-SW16-sec	etu1SAE3	192.168.108.2
Client : SW16-Client	etu1SAE3	192.168.108.4

PARTIE DNS

Nous devons mettre en place un sous domaine du domaine « **sae** ». J'ai donc choisi le sous domaine **anguilet.sae**.

Après avoir obtenu mon sous domaine je dois passer à la création de mon serveur DNS. Pour cela, j'ai choisi de créer une machine Windows server 2016 sur laquelle j'allais y installer le rôle de serveur DNS. Je me suis rendu sur le site [VMware Compatibility](#) pour me servir des bonnes recommandations pour l'installation du système d'exploitation.

Storage		
BusLogic:	Not Supported	Virtual BusLogic Parallel SCSI adapter
IDE:	Supported	Virtual IDE adapter for ATA disks
LSI Logic:	Not Supported	Virtual LSI Logic Parallel SCSI adapter
LSI Logic SAS:	Supported	Virtual LSI Logic SAS adapter
NVMe:	Supported	NVMe Express Adapter
SATA:	Supported	Virtual SATA adapter
VMware Paravirtual:	Supported (Recommended)	VMware Paravirtual SCSI (PVSCSI) adapter

Networking		
e1000:	Not Supported	Emulated Intel 82545EM Gigabit Ethernet NIC
e1000e:	Supported	Emulated Intel 82574L Gigabit Ethernet Controller
Enhanced VMXNET:	Not Supported	Second generation VMware virtual NIC
Vlance:	Not Supported	Emulated AMD 79C970 PCnet32 Lance NIC
VMXNET:	Not Supported	VMware virtual NIC
VMXNET 3:	Supported (Recommended)	Third generation VMware virtual NIC

VMware Tools		
OSP Format Tools:	Not Supported	Operating System Specific Packages
Tools available for download:	Supported	The VMware Tools ISO is available for download from my.vmware.com
Tools bundled with host:	Supported	The VMware Tools ISO is bundled with host product

Back to Search Results

Nouvelle machine virtuelle

Type de provisionnement: Créer une machine virtuelle

Nom de la machine virtuelle:

Dossier:

Hôte:

Banque de données:

Nom du SE invité:

Sécurité basée sur la virtualisation: Désactivé

CPU:

Mémoire:

Cartes réseau:

Bâton de carte réseau 1:

Type de carte réseau 1:

Contrôleur SCSI 1:

Créer un disque dur 1: Nouveau disque virtuel

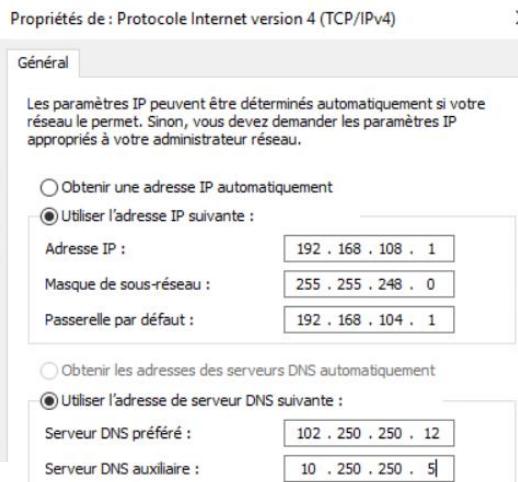
Capacité:

Banque de données:

Nœud de périphérique:

ANGUILET QUABEN Jonathan – C2

• Configuration IP de la machine



• Test de connectivité avec la passerelle

```
c:\ Administateur : Invité de commandes
microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\Administateur.WIN-RFEQ0ENER5>ping 192.168.104.1

Envoi d'une requête 'Ping' à 192.168.104.1 avec 32 octets de données :
Réponse de 192.168.104.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.104.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Après la configuration je me suis occupé de changer le nom de la machine et de la mettre dans mon sous domaine.



Lorsque l'on établit un réseau il est recommandé d'installer le service d'annuaire (AD DS) avant le service DNS (qui sera déployé lors de la mise en place de l'AD DS). En configurant d'abord l'AD DS, on établit la base pour une identification correcte des entités du domaine. Je vais donc passer à la configuration de l'AD DS sur mon serveur. Pour y arriver je me suis aidé de ce [tuto](#) sur le site it-connect.

The left screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' (Role and Feature Wizard) with the 'Progression de l'installation' (Installation Progress) step. It lists the following steps:

- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités
- AD DS
- Confirmation
- Résultats

The 'Fonctionnalités' step is currently selected. The right screenshot shows the 'Assistant Configuration des services de domaine Active Directory' (Active Directory Domain Services Configuration Wizard) with the 'Vérification de la configuration requise' (Check required configuration) step. It displays a summary of successful checks and some warnings:

- Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer... [Afficher plus](#)
- Configuration de déploiement
- Options du contrôleur de domaine
 - Options DNS
 - Options supplémentaires
 - Chemins d'accès
 - Examiner les options
 - Vérification de la configuration
- Installation
- Résultats

Warnings:

- Les contrôleurs de domaine Windows Server 2016 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.
- Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez
- Si vous cliquez sur Installer, le serveur redémarrera automatiquement à l'issue de l'opération de promotion.

ANGUILLET QUABEN Jonathan – C2

Mon AD DS a bien été créé.

The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' (User and Computers) snap-in. In the left navigation pane, under 'Utilisateurs et ordinateurs Active', there is a folder named 'Requêtes enregistrées' and a node labeled 'anguilet.sae'. In the main pane, a table lists the domain 'anguilet.sae' with its type as 'Domaine'.

Et par la même occasion mon DNS aussi, dans lequel une zone directe pour mon domaine a été ajoutée par défaut. J'ai créé un premier enregistrement de type A afin d'associer le nom de ma machine primaire à son adresse IP.

The screenshot shows the 'Gestionnaire DNS' (DNS Manager) snap-in. In the left navigation pane, under 'SAE3-SW16', there is a 'Zones de recherche directe' node containing a sub-node 'anguilet.sae'. In the main pane, a table lists several records for this zone, including an 'A' record for 'sae3-sw16' with the IP address '192.168.108.1'.

Ensuite j'ai ajouté une zone inversée qui va me servir à associer cette fois l'adresse IP de ma machine à son nom.

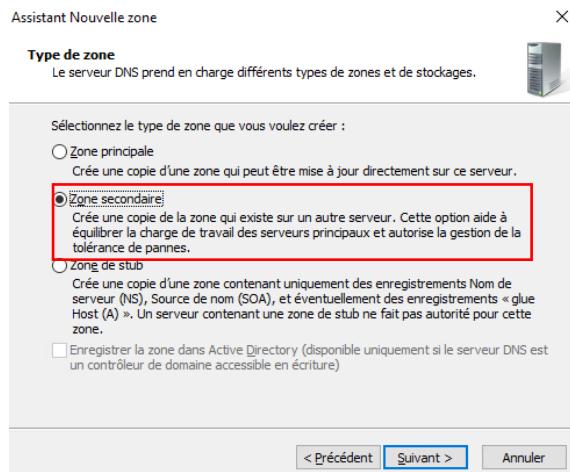
The screenshot shows the 'Gestionnaire DNS' snap-in. In the left navigation pane, under 'SAE3-SW16', there is a 'Zones de recherche inversée' node containing a sub-node '192.168.108.in-addr.arpa'. In the main pane, a table lists a 'PTR' record for the IP '192.168.108.1' with the name 'SAE3-SW16.anguilet.sae.'

Avant de continuer la gestion de mon DNS je vais créer un DNS Secondaire pour offrir au réseau une redondance en cas de panne du DNS principal. Pour cela je vais donc créer une deuxième machine Windows server 2016, qui n'aura comme utilité que son rôle de serveur DNS Secondaire.

The screenshot shows the 'Tableau de bord' (Dashboard) and 'PROPRIÉTÉS' (Properties) dialog boxes for the 'SAE3-SW16-sec' server. In the dashboard, under 'Serveur local', the 'DNS' option is selected. In the properties dialog, the 'Nom de l'ordinateur' is set to 'SAE3-SW16-sec' and the 'Domaine' is set to 'anguilet.sae'. On the right, the 'Général' tab of the 'Propriétés de : Protocole Internet version 4 (TCP/IPv4)' dialog box is shown, where the 'Utiliser l'adresse IP suivante' (Use the following IP address) option is selected with the IP '192.168.108.2' and subnet mask '255.255.248.0'.

ANGUILET QUABEN Jonathan – C2

Sur cette deuxième machine j'ai créé un serveur DNS dans lequel j'ai ajouté une zone secondaire.

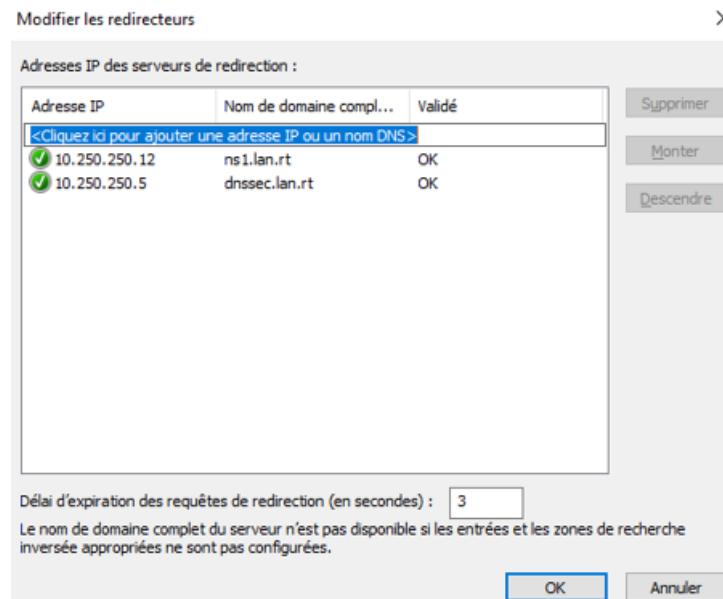


Je vais maintenant retourner sur mon DNS primaire pour terminer sa gestion en autorisant le transfert de zone et mettant en place des redirections vers les DNS de l'iut.

Le transfert est réussi (capture provenant du DNS Secondaire).

ANGUILET QUABEN Jonathan – C2

Mise en place des redirections vers les serveurs DNS de l'IUT.



Maintenant que la configuration de mon DNS est terminée je dois effectuer des tests pour vérifier son bon fonctionnement. Pour cela dans un premier temps j'ai créé une troisième machine Windows server 2016 qui fera office de client cette fois, sans aucun rôle installé.

• Tests NSLOOKUP

```
C:\Users\Administrateur.WIN-DRMCJ3J30JP>nslookup - 192.168.108.1
Serveur par défaut : SAE3-SW16.anguilet.sae
Address: 192.168.108.1

> set type=soa
> anguilet.sae
Serveur : SAE3-SW16.anguilet.sae
Address: 192.168.108.1

anguilet.sae
    primary name server = sae3-sw16.anguilet.sae
    responsible mail addr = hostmaster.anguilet.sae
    serial = 106
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
    expire = 86400 (1 day)
    default TTL = 3600 (1 hour)
sae3-sw16.anguilet.sae internet address = 192.168.108.1
```

```
> set type=ns
> anguilet.sae
Serveur : SAE3-SW16.anguilet.sae
Address: 192.168.108.1

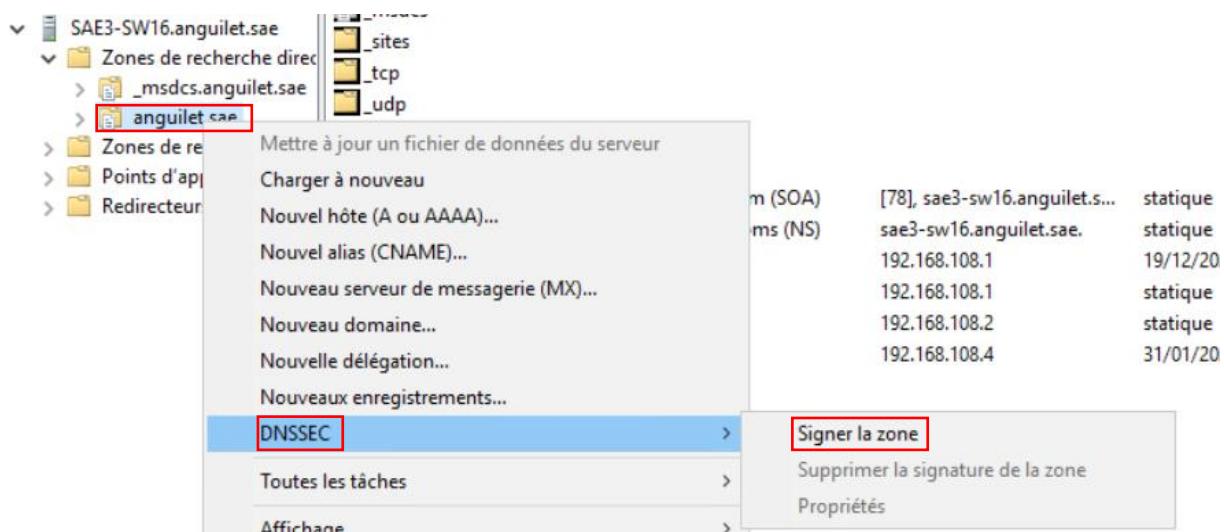
anguilet.sae      nameserver = sae3-sw16-sec.anguilet.sae
anguilet.sae      nameserver = sae3-sw16.anguilet.sae
sae3-sw16-sec.anguilet.sae      internet address = 192.168.108.2
sae3-sw16.anguilet.sae      internet address = 192.168.108.1
>
```

ANGUILET QUABEN Jonathan – C2

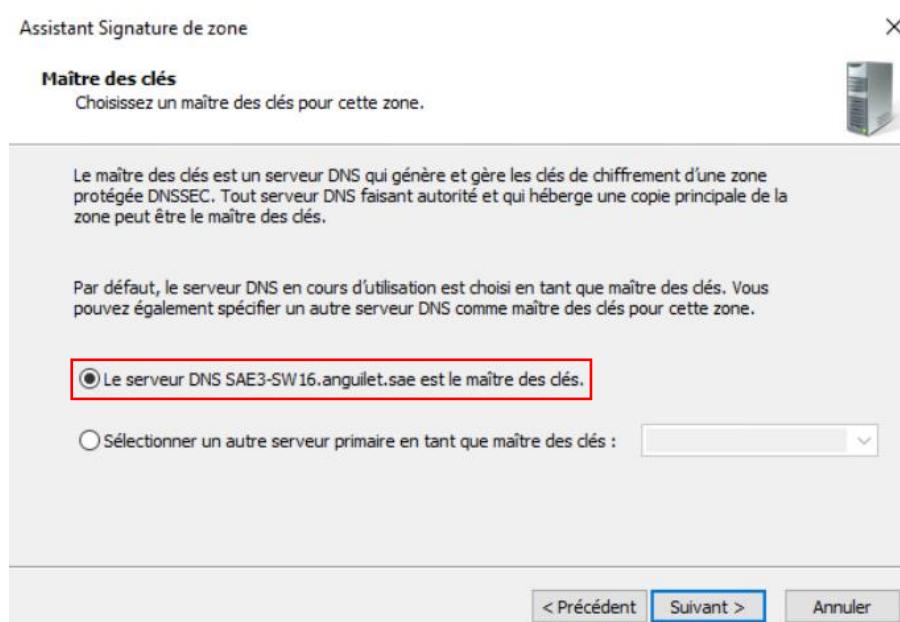
Comme on peut le voir lorsque je veux vérifier quel serveur fait autorité dans mon domaine avec la commande **set type=SOA** on voit bien qu'il s'agit de mon serveur DNS primaire et lorsque je veux vérifier la liste des serveurs de noms en tapant la commande **set type=ns** mes serveurs primaire et secondaire sont affichés.

Dans le but de sécuriser au maximum le réseau, j'ai pris l'initiative de mettre en place un DNSSEC afin de signer les enregistrements DNS de ma zone directe. Cette configuration permettra d'empêcher d'éventuels attaquants d'usurper l'identité de mon serveur DNS puisqu'ils ne pourront pas présenter des enregistrements signés. Je me suis aidé de ce [tuto](#) pour y arriver.

Pour commencer je vais signer la zone.

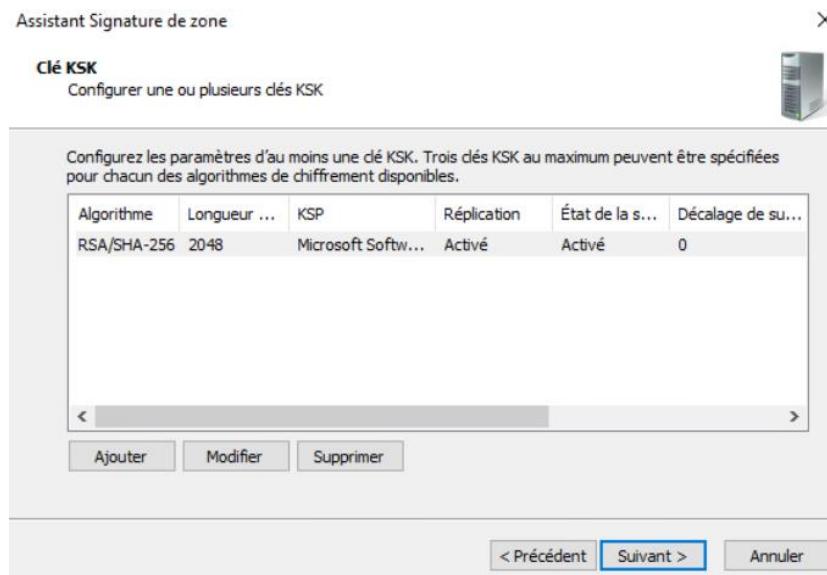
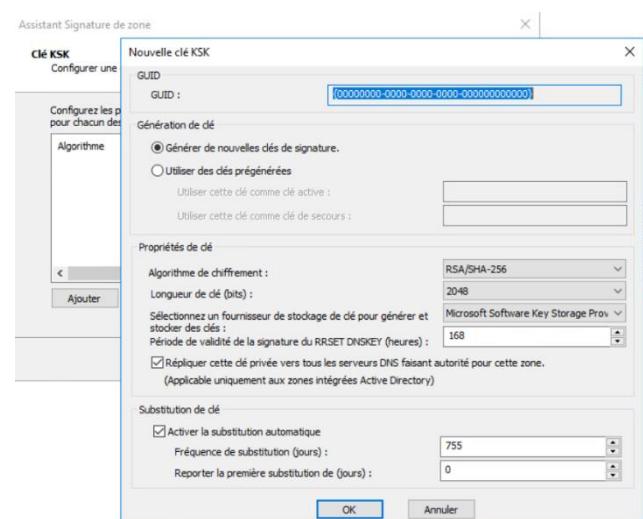
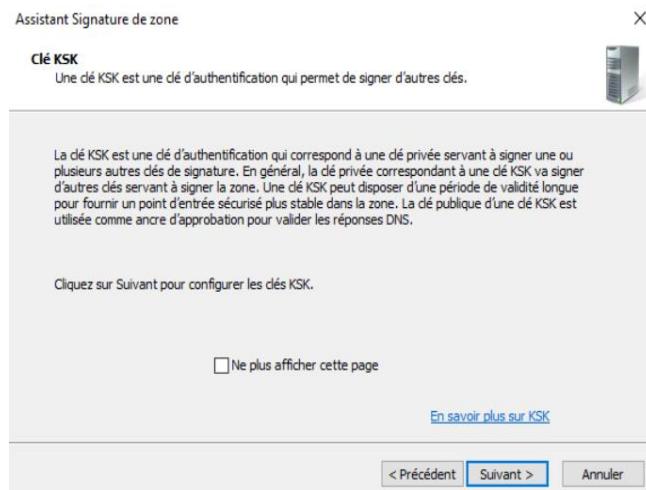


Ensuite j'ai choisi mon serveur primaire comme maître des clés qui vont être créées.

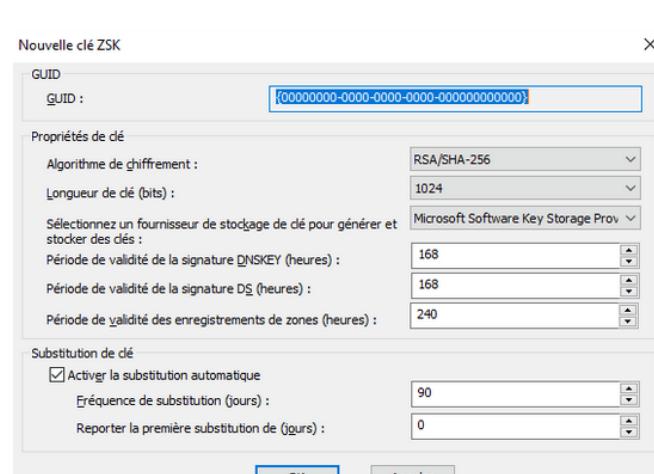
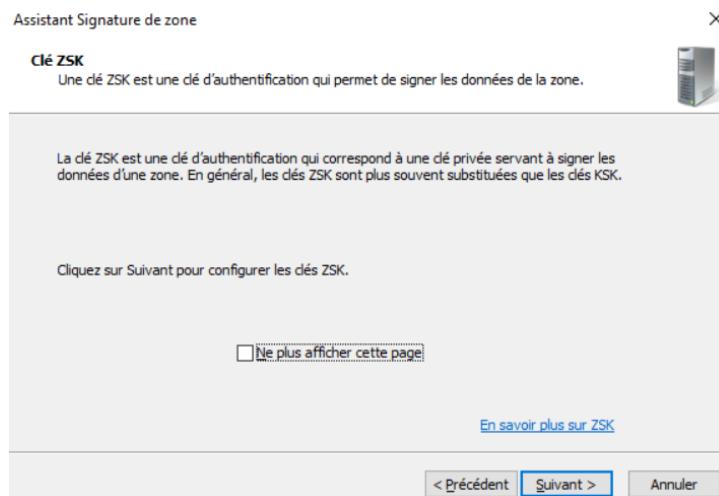


ANGUILLET QUABEN Jonathan – C2

Création de la première clef.

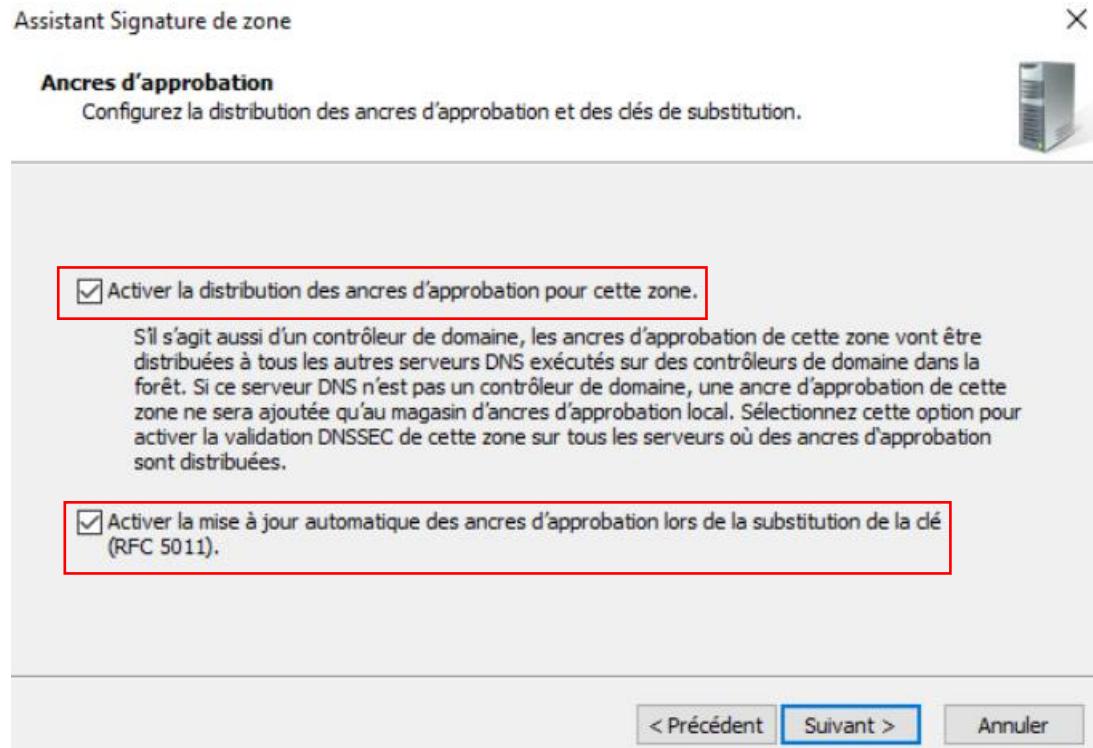


Création de la seconde clef.

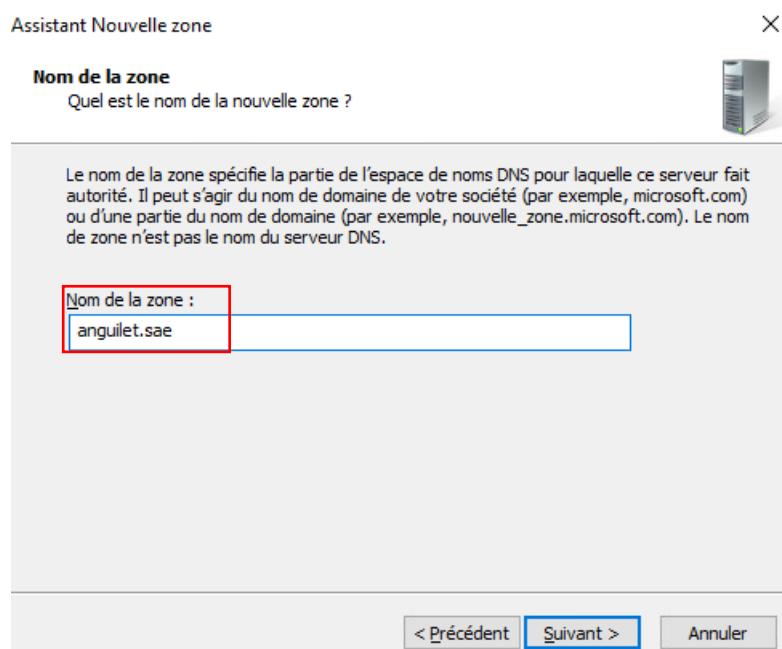


ANGUILET QUABEN Jonathan – C2

Il faut activer la distribution des ancles d'approbation pour la zone qui va être signée pour ne pas avoir à le faire manuellement par la suite ainsi que la mise à jour automatique des ancles d'approbation lors de la substitution de la clef.

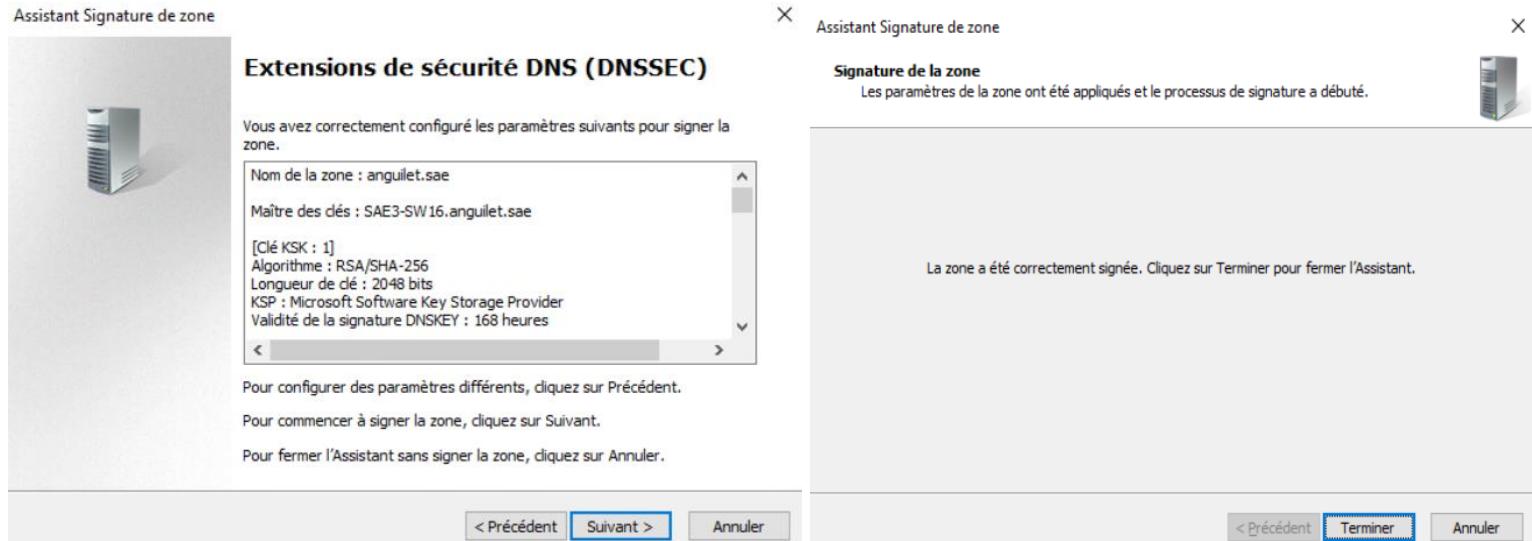


J'ai donc logiquement ajouté le nom de ma zone directe comme zone principale.



ANGUILET QUABEN Jonathan – C2

La première partie de la mise en place du DNSSEC est terminée.

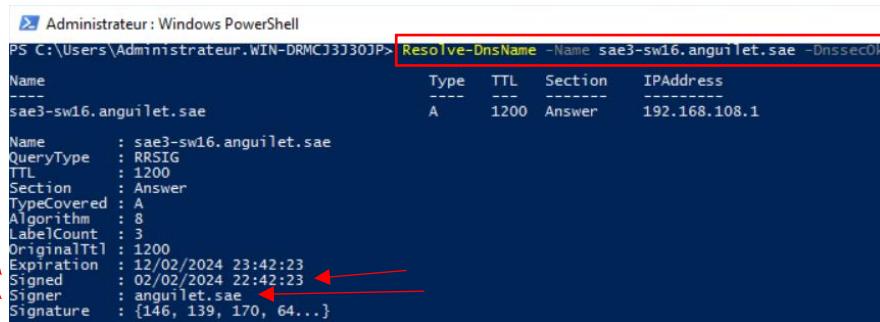


Comme nous pouvons le voir les enregistrements de ma zone directe sont désormais signés.

DNS	Nom	Type	Données	Horodateur
SAE3-SW16	_msdcs			
SAE3-SW16.anguilet.sae	_sites			
Zones de recherche directe	_tcp			
_anguilet.sae	_udp			
DomainDnsZones				
ForestDnsZones				
(identique au dossier parent)	Source de nom (SOA)		[80], sae3-sw16.anguilet.s...	statique
(identique au dossier parent)	Serveur de noms (NS)		sae3-sw16.anguilet.sae.	statique
(identique au dossier parent)	Hôte (A)		192.168.108.1	03/02/2024 00:00:00
(identique au dossier parent)	RR Signature (RRSIG)		[A][Inception(UTC): 02/02...	statique
(identique au dossier parent)	RR Signature (RRSIG)		[NS][Inception(UTC): 02/0...	statique
(identique au dossier parent)	RR Signature (RRSIG)		[SOA][Inception(UTC): 02/...	statique
(identique au dossier parent)	RR Signature (RRSIG)		[DNSKEY][Inception(UTC):...	statique
(identique au dossier parent)	RR Signature (RRSIG)		[DNSKEY][Inception(UTC):...	statique
(identique au dossier parent)	RR Signature (RRSIG)		[NSEC3PARAM][Inception...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)		[256][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)		[256][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)		[257][DNSSEC][RSA/SHA-...	statique

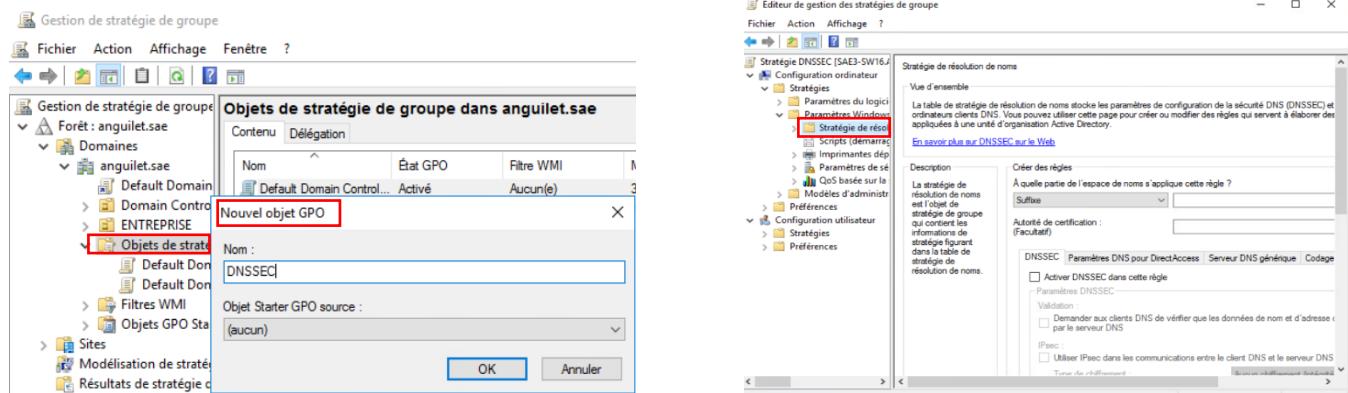
Il est possible de tester que la signature fonctionne de plusieurs manières, j'ai choisi de le faire en utilisant le PowerShell pour interroger mon serveur DNS. Pour ça je me suis rendu sur la machine client et j'ai utilisé la commande **Resolve-DnsName**. On voit bien que la réponse du DNS a été signée.

ANGUILET QUABEN Jonathan – C2

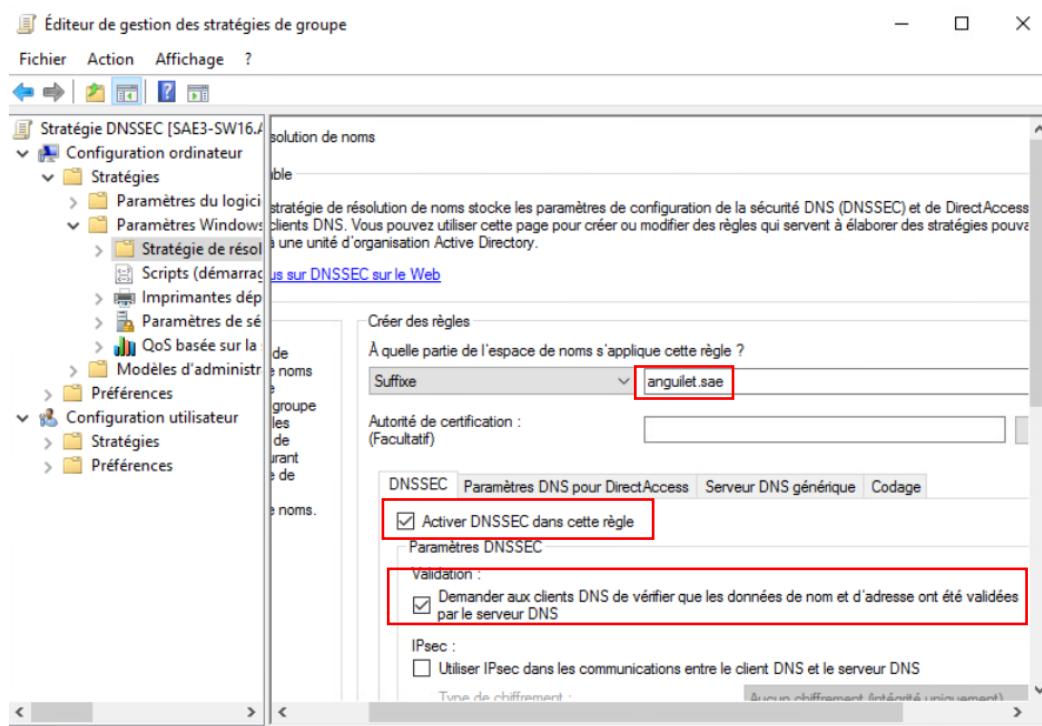


```
PS C:\Users\Administrateur.WIN-DRMCJ3J30JP> Resolve-DnsName -Name sae3-sw16.anguilet.sae -DnssecOk
Name          : sae3-sw16.anguilet.sae
Type          : A
TTL           : 1200
Section       : Answer
TypeCovered   : A
Algorithm     : 8
LabelCount    : 3
OriginalTtl   : 1200
Expiration    : 12/02/2024 23:42:23
Signed        : 02/02/2024 22:42:23
Signer        : anguilet.sae
Signature     : {146, 139, 170, 64...}
```

Par défaut Windows accepte les réponses DNS non signées pour tous les domaines. Cela signifie que les machines de mon domaine sont en mesure d'accepter une réponse non signée. Pour forcer l'utilisation du DNSSEC pour mon domaine une GPO doit être déployée. Je vais l'appeler **DNSSEC**.



J'ai créé une nouvelle règle.



ANGUILET QUABEN Jonathan – C2

La règle apparaît dans la table de stratégie de résolution de noms.

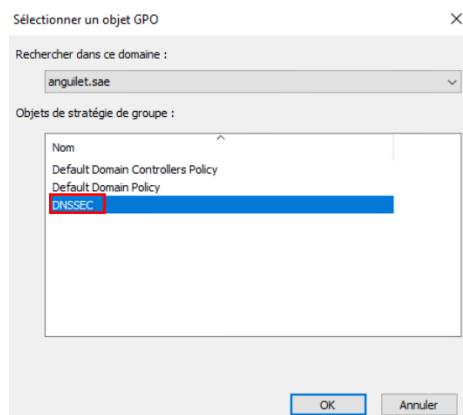
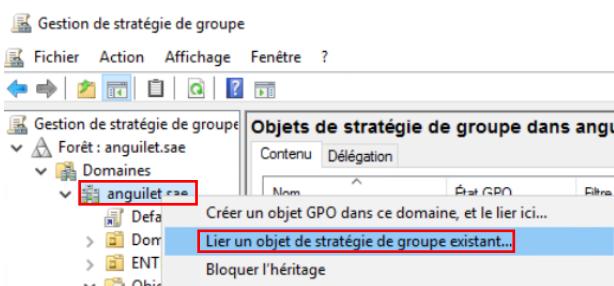
Table de stratégie de résolution de noms

Espace de... .anguilet.sae	Auto... Oui	DNSSE... Oui	DNSSEC ... Non	DNSSEC (... Non)	DirectAc... Non	DirectAc... Non	DirectAc... Non	DirectAc... Non	Serveur

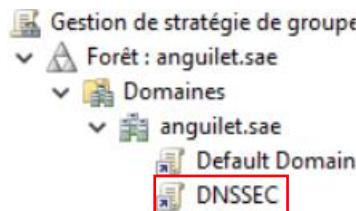
Supprimer une règle

Appliquer

La GPO est prête, je vais maintenant créer une liaison pour l'appliquer aux machines de mon domaine.



La liaison a bien été créée.



Maintenant place au test. Je vais à nouveau utiliser la commande **Resolve-DnsName** sur la machine Client, mais à la fin de la commande je n'ajouterais pas **-DnssecOk**, pour vérifier que Windows a bien compris avec la GPO qu'il doit obtenir des réponses signées pour la zone directe de mon serveur DNS primaire.

```
PS C:\Users\Administrateur.WIN-DRMCJ3J30JP> Resolve-DnsName -Name sae3-sw16.anguilet.sae
Name                                Type    TTL     Section      IPAddress
----                                --     --      -----      -----
sae3-sw16.anguilet.sae                A      1200   Answer      192.168.108.1

Name      : sae3-sw16.anguilet.sae
QueryType : RRSIG
TTL       : 1200
Section   : Answer
TypeCovered : A
Algorithm : 8
LabelCount : 3
OriginalTtl : 1200
Expiration : 12/02/2024 23:42:23
Signed    : 02/02/2024 22:42:23
Signer    : anguilet.sae
Signature : {146, 139, 170, 64...}
```

ANGUILET QUABEN Jonathan – C2

La commande **Get-DnsClientNrpPolicy -Effective** (que j'ai tapé sur le serveur DNS primaire lui-même cette fois) permet de s'assurer que la stratégie mise en place soit bien appliquée.

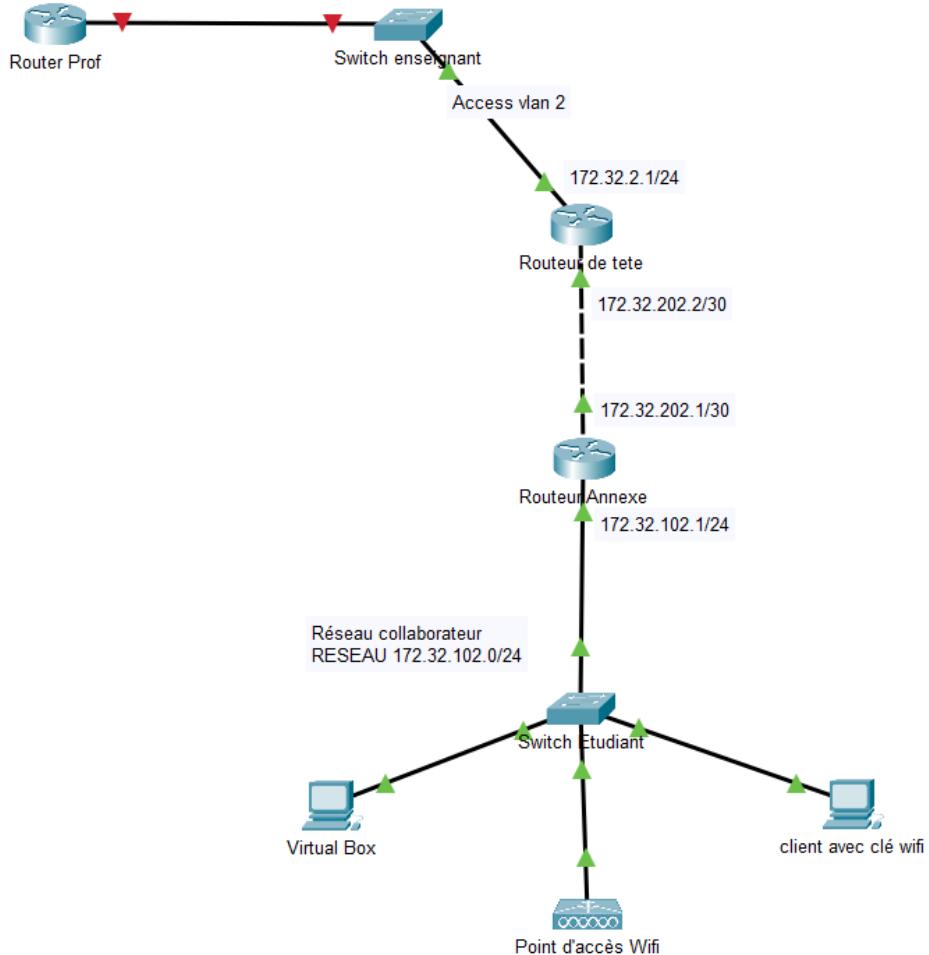
```
PS C:\Users\Administrateur.WIN-RFE0Q0ENER5> get-DnsClientNrpPolicy -Effective

Namespace : .anguilet.sae
QueryPolicy : QueryIPv6Only
SecureNameQueryFallback : FallbackPrivate
DirectAccessIPsecCARestriction :
DirectAccessProxyName :
DirectAccessDnsServers :
DirectAccessEnabled : False
DirectAccessProxyType :
DirectAccessQueryIPsecEncryption :
DirectAccessQueryIPsecRequired :
NameServers :
DnsSecIPsecCARestriction :
DnsSecQueryIPsecEncryption :
DnsSecQueryIPsecRequired : False
DnsSecValidationRequired : True
NameEncoding :
```

La mise en place complète de mon DNS est donc terminée.

PARTIE RÉSEAU

- Réseau Simulé sous Packet Tracer



ANGUILLET QUABEN Jonathan – C2

Pour cette partie, le travail demandé est de mettre en œuvre sur mes 2 routeurs de l'OSPFv2 pour pouvoir remonter jusqu'au routeur enseignant. Sans oublier que mes équipements réseaux doivent être accessibles à distance via un protocole sécurisé. Avant de commencer voici quelques informations importantes pour cette partie.

VLAN attribué :	VLAN2
Plage d'IP utilisables :	192.168.108.1 – 192.168.108.10/21
Réseau liant Routeur de tête au Routeur prof :	172.32.2.0/24
Interface du Routeur de tête reliée au R. prof :	172.32.2.1/24
Passerelle sur Routeur prof :	172.32.2.254/24
Réseau entre mes 2 routeurs :	172.32.202.0/30
Réseau Collaborateur :	172.32.102.0/24

J'ai commencé mes configurations réseaux en commençant par configurer mon **Switch**, puis mon **Routeur annexe** et en dernier mon **Routeur de tête** qui est relié au **Routeur prof** par l'intermédiaire du **Switch enseignant**.

➤ SWITCH ÉTUDIANT

```
!
interface GigabitEthernet0/0
  vrf forwarding Mgmt-vrf
  no ip address
  shutdown
!
interface GigabitEthernet1/0/1
  switchport access vlan 2
  switchport mode access
```

➤ ROUTEUR ANNEXE

```
!
interface GigabitEthernet0/0/0
  ip address 172.32.202.1 255.255.255.252
  negotiation auto
!
interface GigabitEthernet0/0/1
  ip address 172.32.102.1 255.255.255.0
  negotiation auto
```

```
!
router ospf 2
  network 172.32.102.0 0.0.0.255 area 0
  network 172.32.202.0 0.0.0.3 area 0
,
```

ANGUILLET QUABEN Jonathan – C2

➤ ROUTEUR DE TETE

```
!
interface GigabitEthernet0/0/0
 ip address 172.32.2.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/0/1
 ip address 172.32.202.2 255.255.255.252
 negotiation auto
!
!
router ospf 2
 network 172.32.2.0 0.0.0.255 area 0
 network 172.32.202.0 0.0.0.3 area 0
```

Maintenant on va vérifier que mon OSPFv2 a été bien configuré avec un **Show ip route**. Le routage dynamique est bien fonctionnel dans mon réseau.

➤ ROUTEUR ANNEXE

```
Router2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
      n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      H - NHRP, G - NHRP registered, g - NHRP registration summary
      o - ODR, P - periodic downloaded static route, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 172.32.202.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.32.202.2, 00:00:14, GigabitEthernet0/0/0
      172.32.0.0/16 is variably subnetted, 51 subnets, 3 masks
O     172.32.2.0/24
      [110/2] via 172.32.202.2, 00:00:18, GigabitEthernet0/0/0
O     172.32.3.0/24
      [110/3] via 172.32.202.2, 00:00:14, GigabitEthernet0/0/0
O     172.32.4.0/24
      [110/3] via 172.32.202.2, 00:00:14, GigabitEthernet0/0/0
O     172.32.5.0/24
      [110/3] via 172.32.202.2, 00:00:14, GigabitEthernet0/0/0
O     172.32.6.0/24
      [110/3] via 172.32.202.2, 00:00:14, GigabitEthernet0/0/0
O     172.32.7.0/24
      [110/3] via 172.32.202.2, 00:00:14, GigabitEthernet0/0/0
```

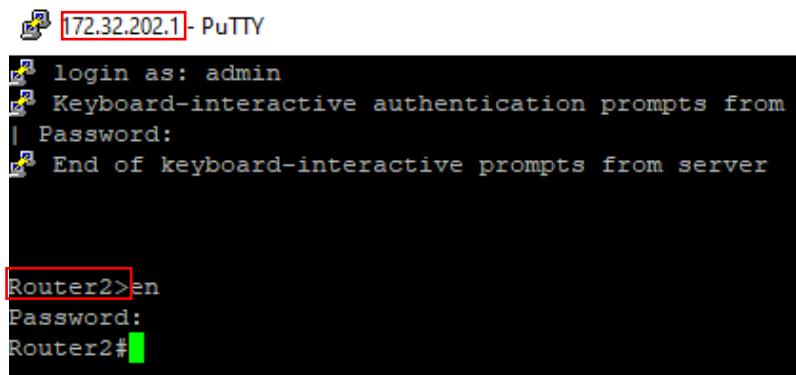
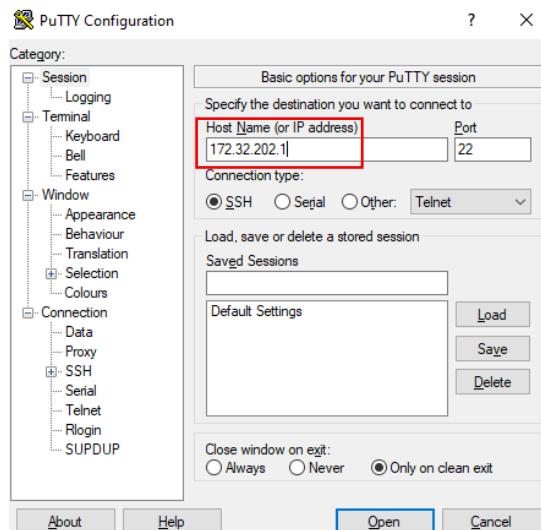
Place aux tests de vérification du protocole sécurisé SSH. (Tous les mots de passe de mes 3 équipements réseau sont : **root** et les utilisateurs : **admin**).

ANGUILET QUABEN Jonathan – C2

```
Router2>en
Router2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config) line cons 0
Router2(config-line)#pass root
Router2(config-line)#enable secret root
Router2(config)#ip domain-name anguilet.sae
Router2(config)#crypto key generate rsa
The name for the keys will be: Router2.anguilet.sae
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
* Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

Router2(config)#
*Feb 5 11:38:06.641: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named Router2.anguilet.sae has been generated or imported by crypto-engine
*Feb 5 11:38:06.645: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Feb 5 11:38:06.758: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named Router2.anguilet.sae.server has been generated or imported by crypto-engine
Router2(config)#ip ssh version 2
Router2(config)username admin secret root
Router2(config)#
*Feb 5 11:38:31.622: %AAA-5-USER_RESET: User admin failed attempts reset by console
Router2(config)line vty 0 15
Router2(config-line)#login local
Router2(config-line)#transport input ssh
```



PARTIE DHCP

Le protocole DHCP dans un réseau est très important, encore plus lorsque le réseau est grand. Il sert à attribuer automatiquement une adresse IP à un appareil connecté au réseau dans une plage d'adresses IP établie au préalable par l'administrateur.

Afin de ne pas altérer le fonctionnement du réseau de l'entreprise lors de la mise en place de mon DHCP il est impératif de le mettre en place sur mon **Routeur annexe**. N'étant pas directement connecté au réseau de l'entreprise il n'y a donc aucun risque.

Pour le réaliser j'ai utilisé la commande **Ip dhcp pool**, puis j'ai donné le nom **reseaucol** à ce pool. J'ai ensuite mentionné mon réseau qui est **172.32.102.0** avec son masque et ajouté comme passerelle l'adresse de l'interface de mon **Routeur annexe**

ANGUILET QUABEN Jonathan – C2

reliée à mon réseau collaborateur. Pour finir j'ai renseigné l'adresse IP de mes serveurs DNS primaire et secondaire et mon nom de domaine.

```
!
ip dhcp pool reseaucol
 network 172.32.102.0 255.255.255.0
 domain-name anguilet.sae
 dns-server 192.168.108.1 192.168.108.2
 default-router 172.32.102.1
```

Maintenant nous allons vérifier que le DHCP est bien fonctionnel en connectant un PC physique à mon switch étudiant.

Le PC physique a bien récupéré une adresse IP dans mon pool et a par la même occasion intégré mon domaine.

Paramètres IP

Attribution d'adresse IP : Automatique (DHCP)

Propriétés

Vitesse de connexion (Réception/ Transmission) :	1000/1000 (Mbps)
Adresse IPv6 locale du lien :	fe80::aa9c:eb3b:7cd:bab4%14
Adresse IPv4 :	172.32.102.2
Serveurs DNS IPv4 :	192.168.108.1 192.168.108.2
Suffixe DNS principal :	anguillet.sae
Fabricant :	Intel
Description :	Intel(R) Ethernet Connection (17) I219-LM
Version du pilote :	12.19.2.50
Adresse physique (MAC) :	64-4E-D7-69-3A-AE

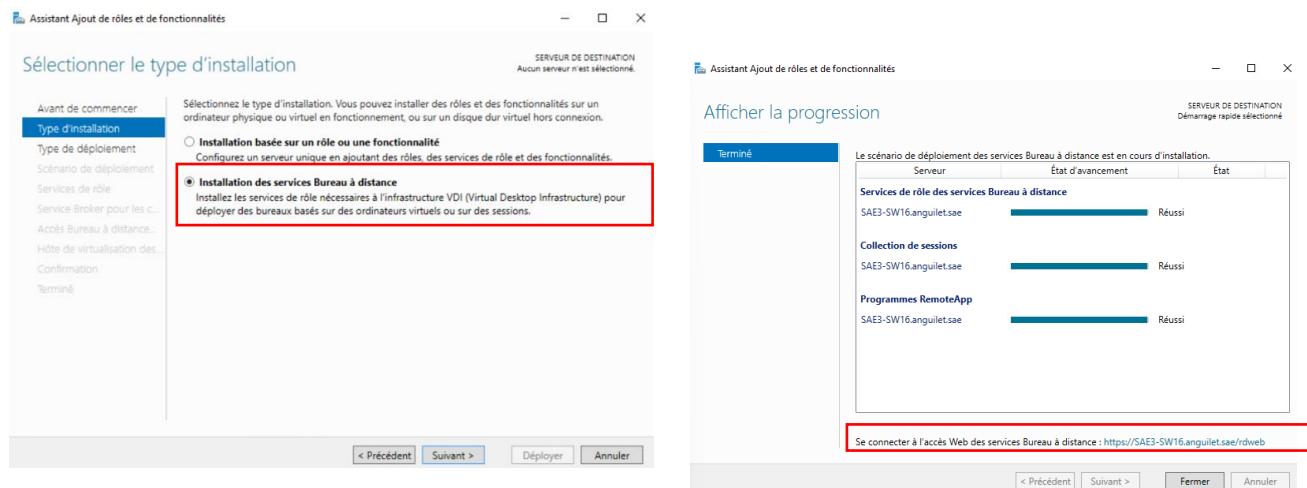
ANGUILET QUABEN Jonathan – C2

D'ailleurs pour qu'il puisse intégrer mon domaine il fallait dans un premier temps désactiver les pare-feu Windows sur mon serveur primaire.

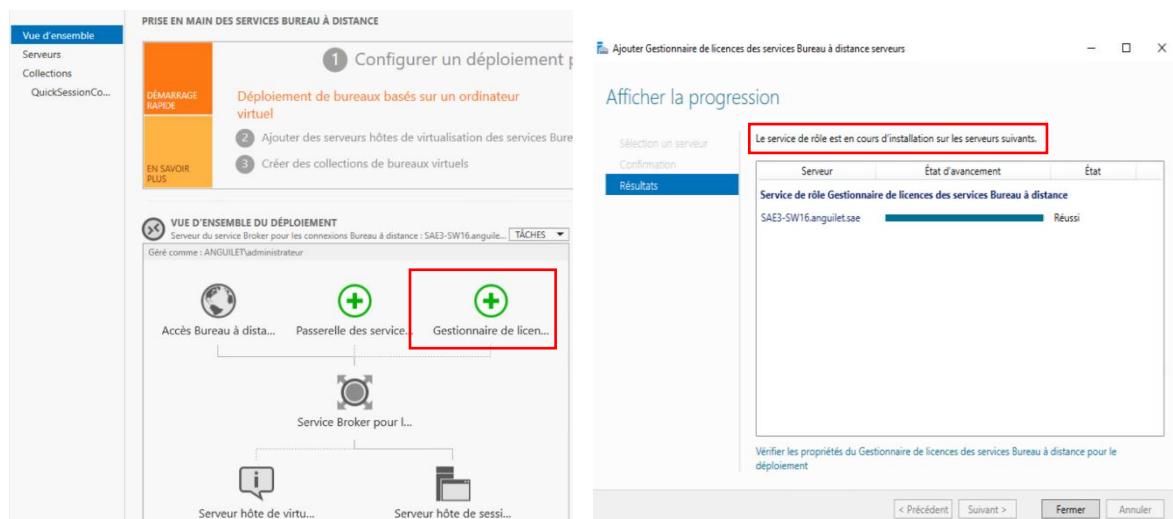
PARTIE WEB

Pour cette partie, il est demandé dans un premier temps de tester si on peut héberger le nouveau site de l'entreprise sur un serveur local et dans un second temps d'organiser le service AD DS créé de telle sorte que les techniciens et la production puissent utiliser leurs applications logicielles à distance depuis un navigateur. On précise que les techniciens doivent accéder au logiciel **Acrylic** et la production au logiciel **Calc**.

Pour commencer cette partie je vais mettre en place le RDS en installant les services de Bureau à distance. Je vais m'aider de ce [tuto](#).

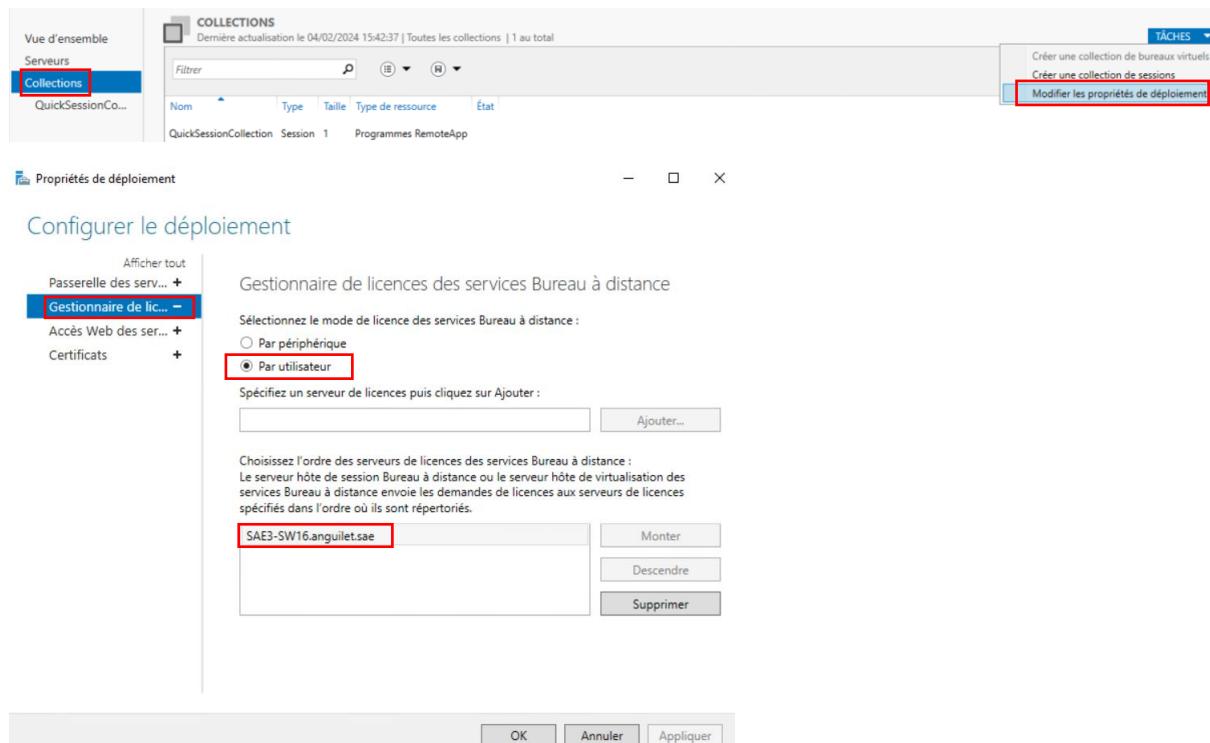


Maintenant que les services de bureau à distance sont installés il va falloir faire les configurations nécessaires pour réaliser le travail demandé, à savoir dans un premier temps ajouter un serveur de gestionnaire de licence de services de bureau à distance.

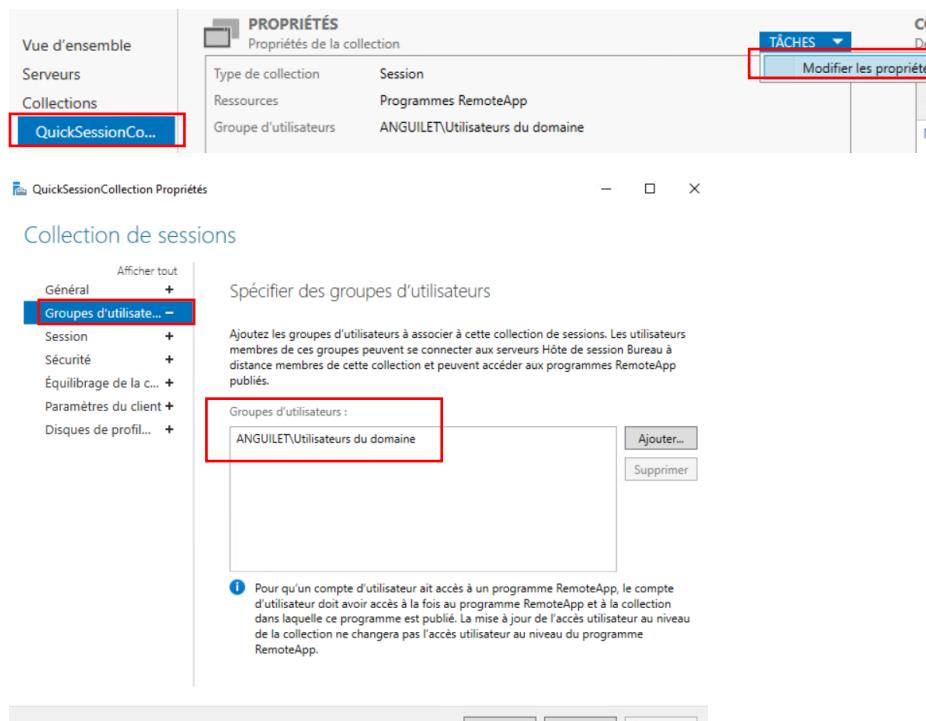


ANGUILET QUABEN Jonathan – C2

Je vais modifier les paramètres de déploiement pour préciser au serveur RDS qu'il doit fonctionner en attribuant des licences par utilisateur qui se connecte et non par périphérique.



Il faut ensuite passer à la configuration de la collection de mon RDS, pour spécifier quels groupes auront le droit d'accéder à cette collection. J'ai choisi d'autoriser l'accès à tous les utilisateurs du domaine **anguilet.sae** dans un premier temps.



ANGUILET QUABEN Jonathan – C2

Lorsque j'accède à l'onglet **QuickSessionCollection**, je peux voir la liste des applications présentes.

PROGRAMMES REMOTEAPP

Dernière actualisation le 04/02/2024 15:42:37 | Programmes RemoteApp publiés | 5 au total

Nom du programme RemoteApp	Alias	Visible dans l'Accès Web des services Bureau à
AcrylicWiFiSnifferControl	AcrylicWiFiSnifferControl	Oui
Calculatrice	Calculatrice	Oui
Paint	Paint	Oui
scalc	scalc	Oui
WordPad	WordPad	Oui

Celles qui nous intéressent sont **Acrylic** et **scalc**. Rappelons que seuls les **techniciens** ont le droit d'avoir accès à **Acrylic** et la **production** à **scalc**.

Pour cela il faut donc que je puisse mettre en place des O.U, donc je vais mettre en place une OU que je vais appeler **ENTREPRISE**, et deux sous OU que je vais appeler respectivement **PRODUCTION** et **TECHNICIEN** dans mon AD DS.

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active

- Requêtes enregistrées
- anguilet.sae
 - Builtin
 - Computers
 - Domain Controllers
 - ENTREPRISE
 - PRODUCTION
 - TECHNICIEN

Dans chaque sous OU j'ai créé un groupe et un utilisateur appartenant à ce groupe (**Les mots de passe des deux utilisateurs sont : Root123**).

Sous OU PRODUCTEUR

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active

- Requêtes enregistrées
- anguilet.sae
 - Builtin
 - Computers
 - Domain Controllers
 - ENTREPRISE
 - PRODUCTION
 - TECHNICIEN

Sous OU TECHNICIEN

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

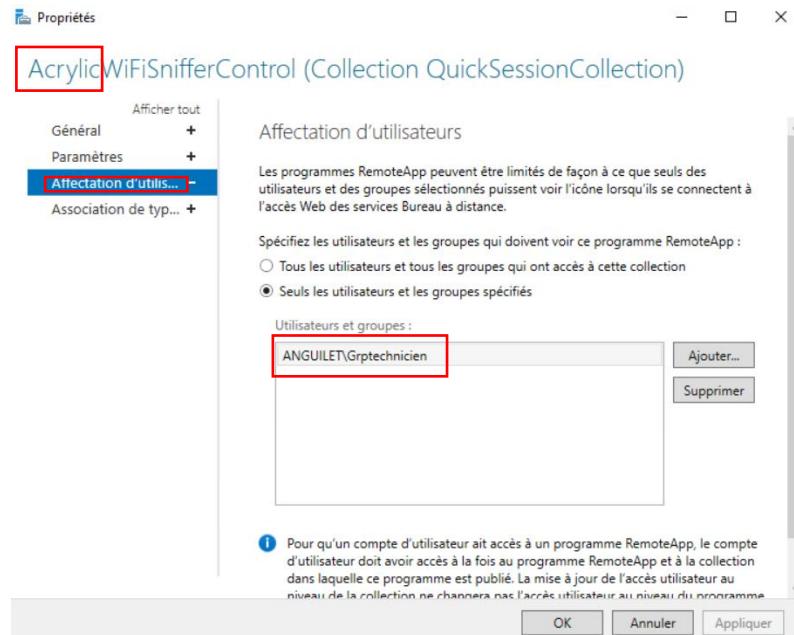
Utilisateurs et ordinateurs Active

- Requêtes enregistrées
- anguilet.sae
 - Builtin
 - Computers
 - Domain Controllers
 - ENTREPRISE
 - PRODUCTION
 - TECHNICIEN

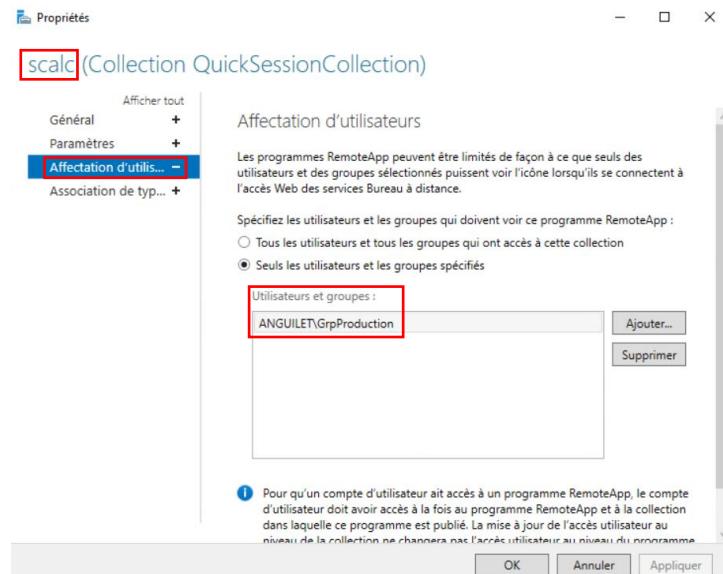
ANGUILET QUABEN Jonathan – C2

Maintenant je retourne dans le service de Bureau à distance pour donner à chaque groupe son droit d'accès à son application.

➤ Acrylic pour les Techniciens.

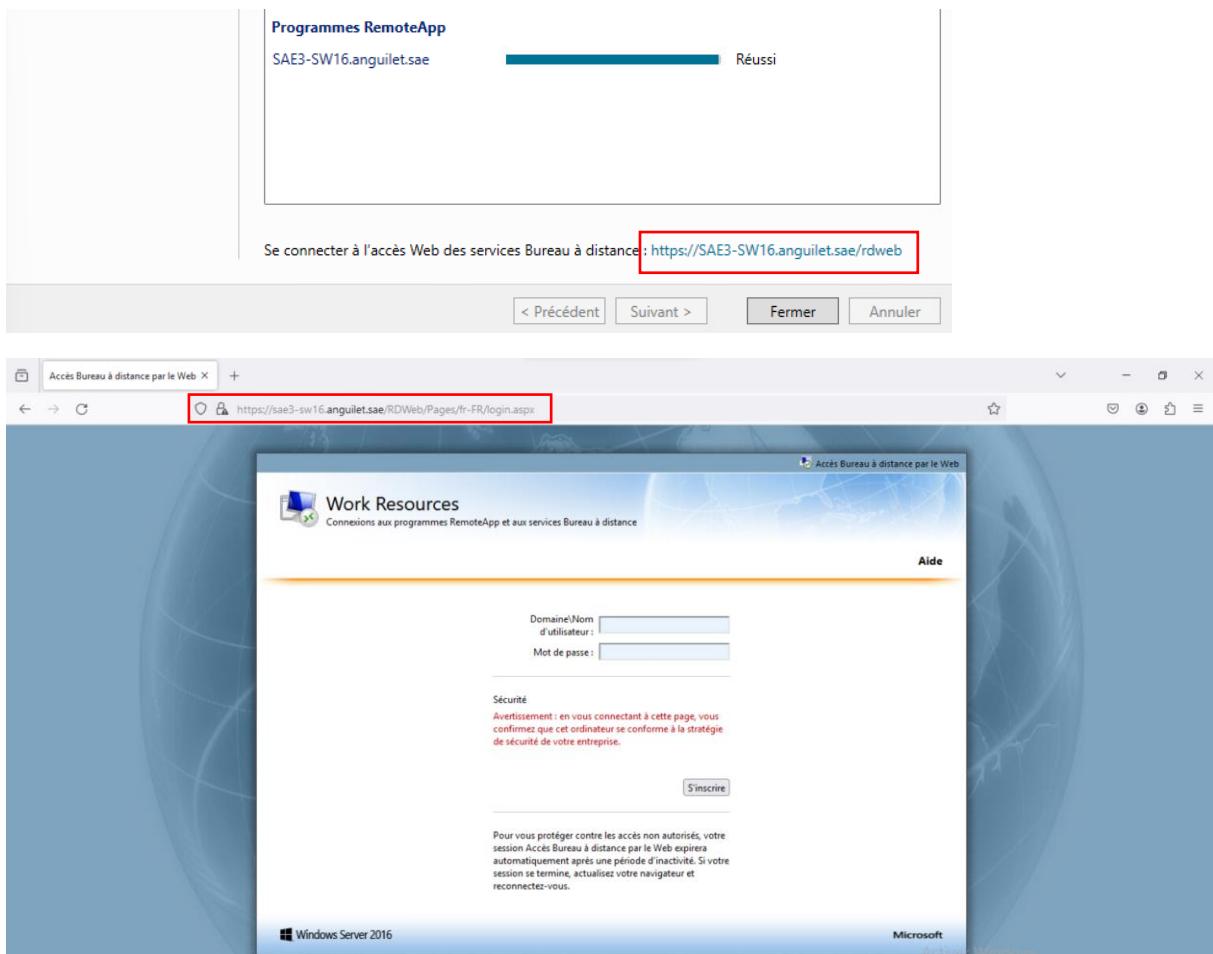


➤ Scalc pour la production.

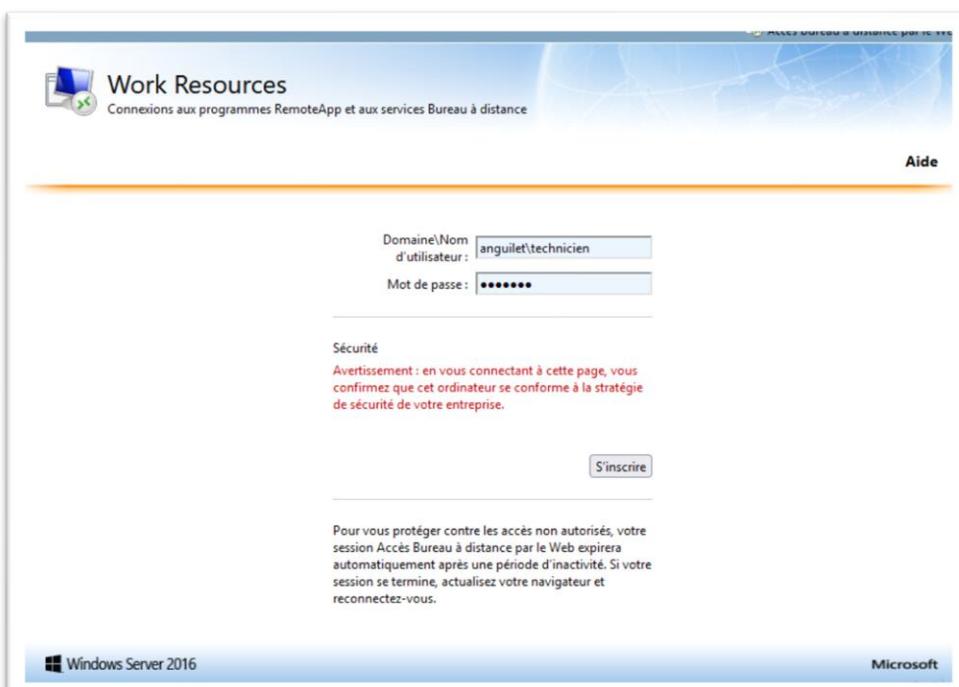


Afin d'effectuer des tests, j'ai utilisé le lien qui m'a été fourni lors de l'installation du RDS.

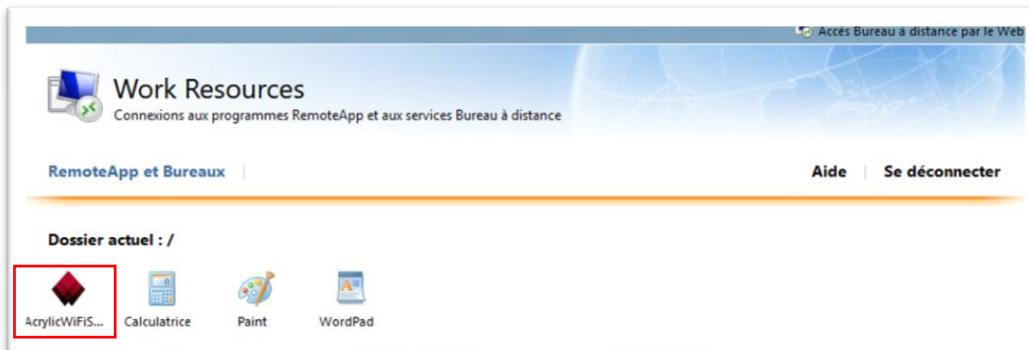
ANGUILET QUABEN Jonathan – C2



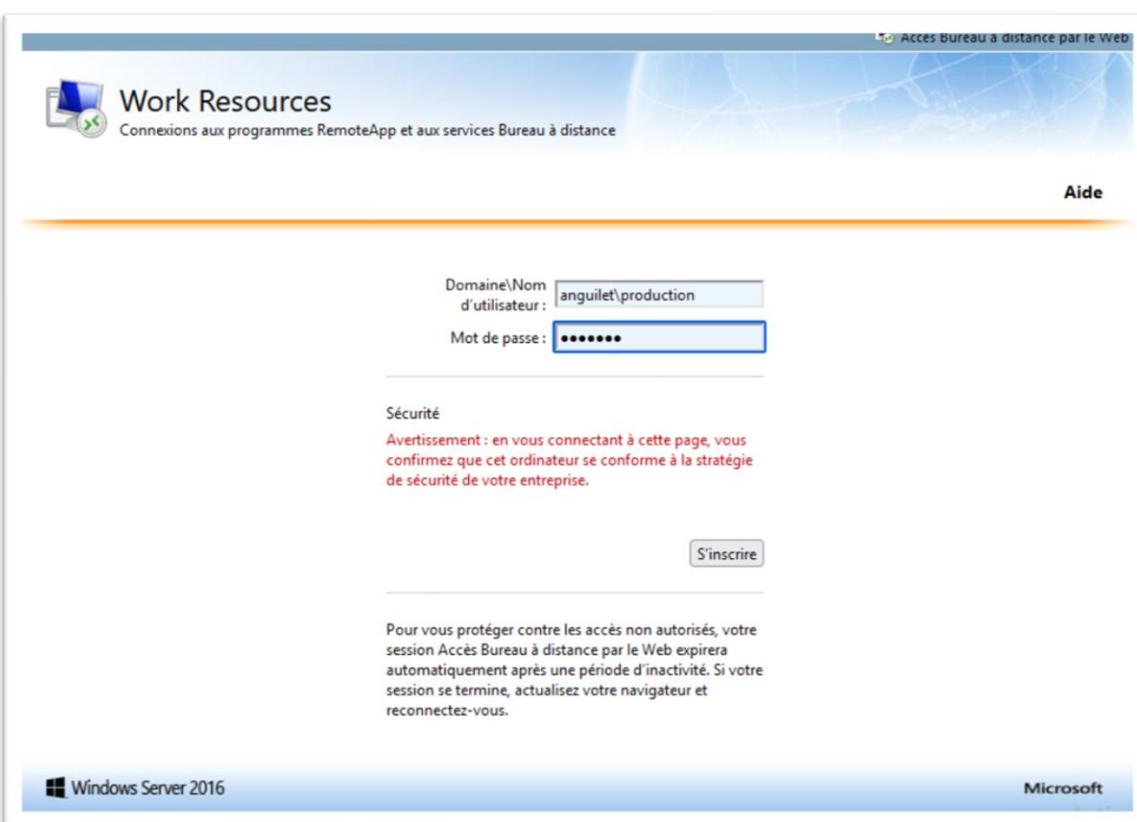
Je vais dans un premier temps me connecter avec un utilisateur du groupe technicien (**mdp : Root123**). On rappelle qu'il ne doit pas avoir accès à **scalc**.



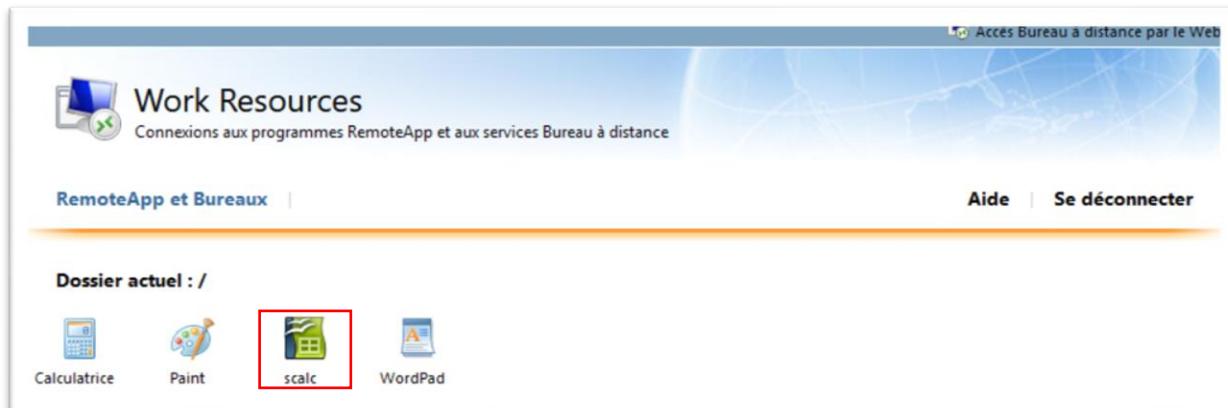
ANGUILET QUABEN Jonathan – C2



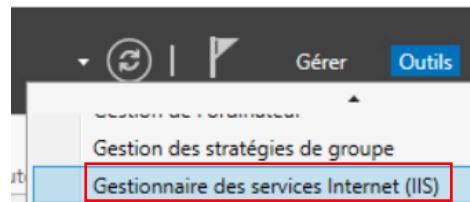
Au tour d'un utilisateur du groupe production, qui ne doit pas avoir accès à **Acrylic**.



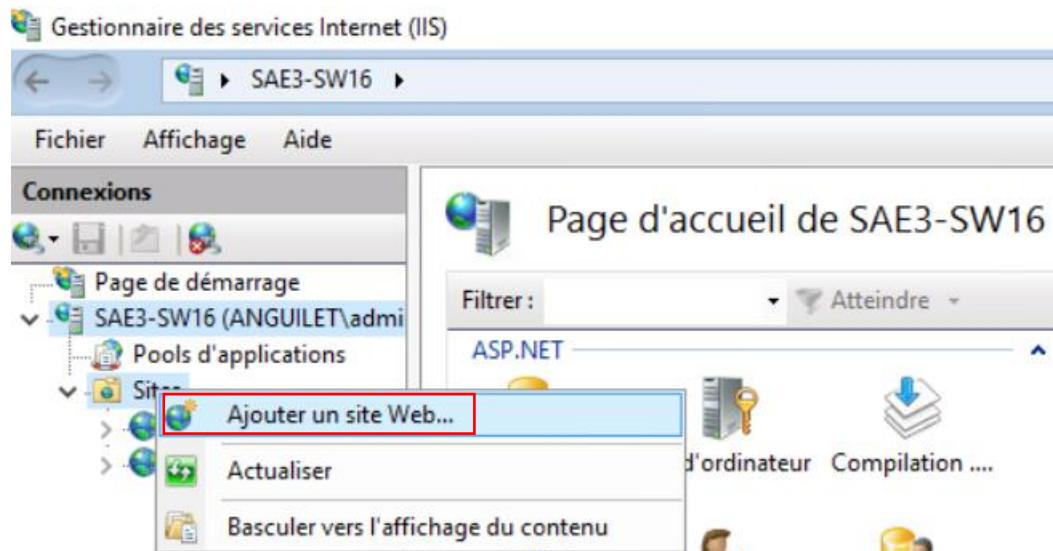
ANGUILET QUABEN Jonathan – C2



Pour pouvoir héberger le nouveau site de l'entreprise sur un serveur local je me suis servi du serveur IIS qui a été déployé lorsque j'ai installé les services de bureau à distance.



J'ai effectué un clic droit sur le dossier **sites** pour y ajouter un nouveau site web que j'ai nommé **anguilet.sae**.



Dans les paramètres avancés du site **anguilet.sae** j'ai pu retrouver son chemin d'accès physique afin de pouvoir l'éditer.

ANGUILET QUABEN Jonathan – C2

The screenshot shows the IIS Manager interface. On the left, under 'Connexions', there is a tree view with 'Page de démarrage', 'SAE3-SW16 (ANGUILET)', 'Pools d'application', 'Sites', and two entries: 'anguilet.sae' (selected and highlighted with a red box) and 'Default Web Site'. On the right, the 'Paramètres avancés' (Advanced Settings) window is open for the selected site. The 'Général' section contains the following settings:

Chemin d'accès physique	C:\inetpub\wwwroot
Identificateur	2
Informations d'identification du	
Informations d'identification du	ClearText
Liaisons	https:192.168.108.1:443:anguilet.sae
Nom	anguilet.sae
Pool d'applications	anguilet.sae
Préchargement Activée	False

J'ai bien retrouvé le fichier au chemin indiqué. Je vais maintenant le personnaliser un minimum.

The screenshot shows two windows. On the left, a File Explorer window shows the directory structure: 'Ce PC > Disque local (C:) > inetpub > wwwroot'. Inside 'wwwroot', there are several files and folders, including 'aspnet_client', 'f', and 'iisstart' (which is highlighted with a red box). On the right, a Notepad window titled 'iisstart' shows the XML content of the file:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD
<html xmlns="http://www.w3.org/1999/
<head>
<meta http-equiv="Content-Type" co
<title>SAE3.CYBER.ANGUILET</title>
```

Je me suis rendu sur la machine client pour le tester, et donc le nouveau site de l'entreprise est hébergé en local.

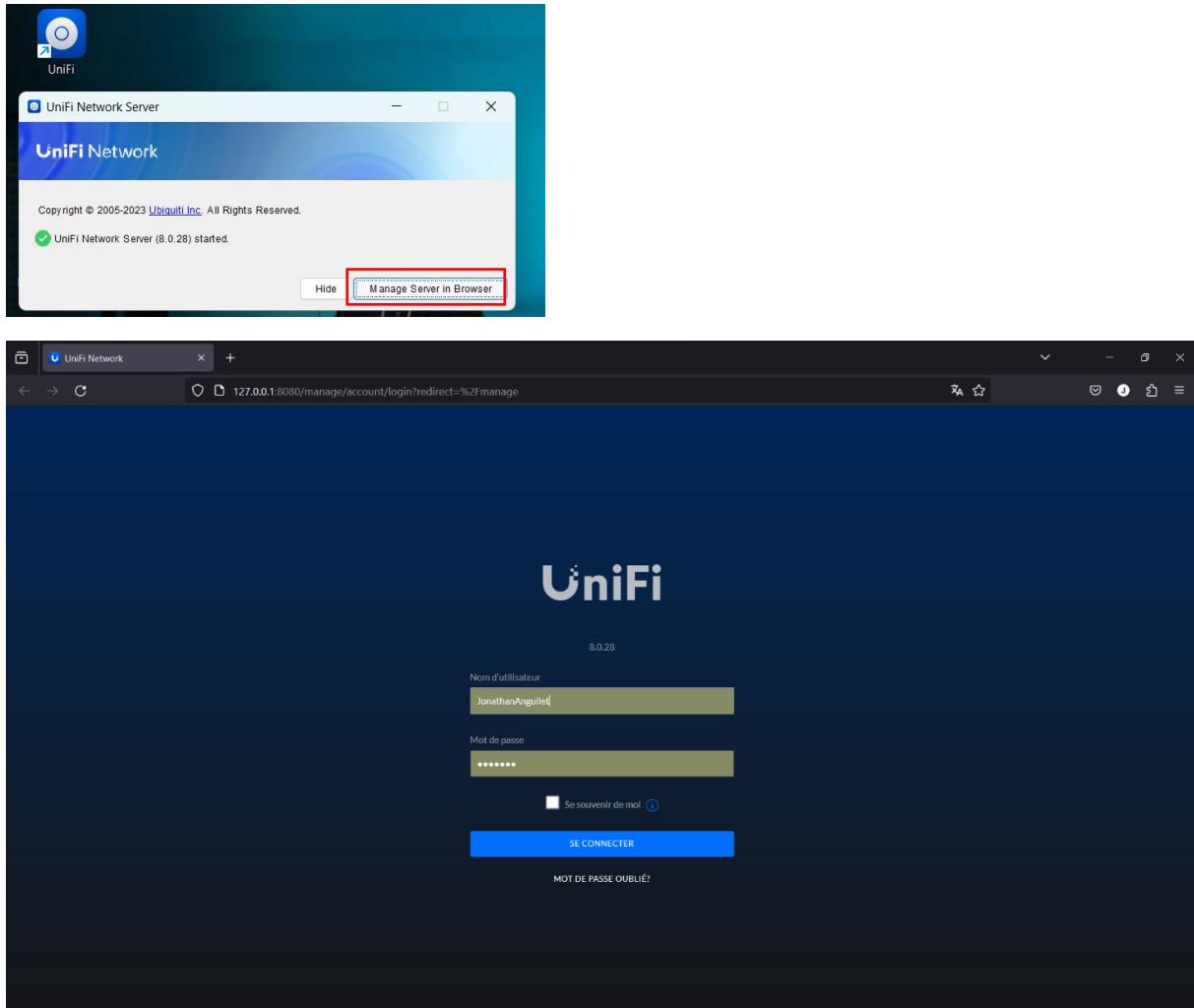


PARTIE WIFI

Pour cette partie, le travail à réaliser est de créer 1 SSID pour les membres de l'entreprise et 1 SSID invité pour les visiteurs.

ANGUILLET QUABEN Jonathan – C2

J'ai choisi d'utiliser l'AP UAP-AC-LITE UBIQUITI. Dans un premier temps j'ai dû créer un compte sur unifi puis m'y connecter.



Le DHCP que j'ai mis en place a attribué une adresse IP à l'AP qui est **172.32.102.3**.

Type	Name	Application	Status	IP Address	Uplink	Parent Device	Ch. 2.4 GHz	Ch. 5 GHz	Connected	Experience	24HR Usage	Download	Upload
UAP-AC-Lite	Network	Offline	172.32.102.2	-	-	-	-	-	0	No Clients	-	10 bps	101
UAP-AC-Lite	Network	Up to date	172.32.102.3	GbE	-	6 (20 MHz)	48 (40 MHz)	1	Excellent	2.70 MB	1.27 Kbps	15	

Ensuite je suis passé à la création des deux réseaux wifi. Un pour les invités et un pour les employés.

ANGUILLET QUABEN Jonathan – C2

Name	Network	Broadcasting APs	Clients (Peak)	Security	Experience
ANGUILLET-invité	Default	UAP-AC-Lite	0 (1)	Open	N/A
ANGUILLET-Employés	Default	UAP-AC-Lite	0 (0)	WPA Enterprise	N/A

[Create New](#) [Manage](#)

Radios [Go To Radio Manager](#)

Channelization [Optimize Now](#)

➤ Configuration du SSID invité.

Name: ANGUILLET-invité

Broadcasting APs: [Devices](#) [Groups](#)

Name	Model	IP Address
<input type="checkbox"/> UAP-AC-Lite	UAP AC Lite	172.32.102.2
<input checked="" type="checkbox"/> UAP-AC-Lite	UAP AC Lite	172.32.102.3

[Advanced](#) [Auto](#) [Manual](#)

Private Pre-Shared Keys:

Hotspot Portal:

We have applied your [Hotspot Portal](#) to this WiFi name.
By default, portal guests will be isolated from other
guests and network resources.

RADIUS MAC Authentication:

Security Protocol: [Open](#)

PMF: Required Optional Disabled

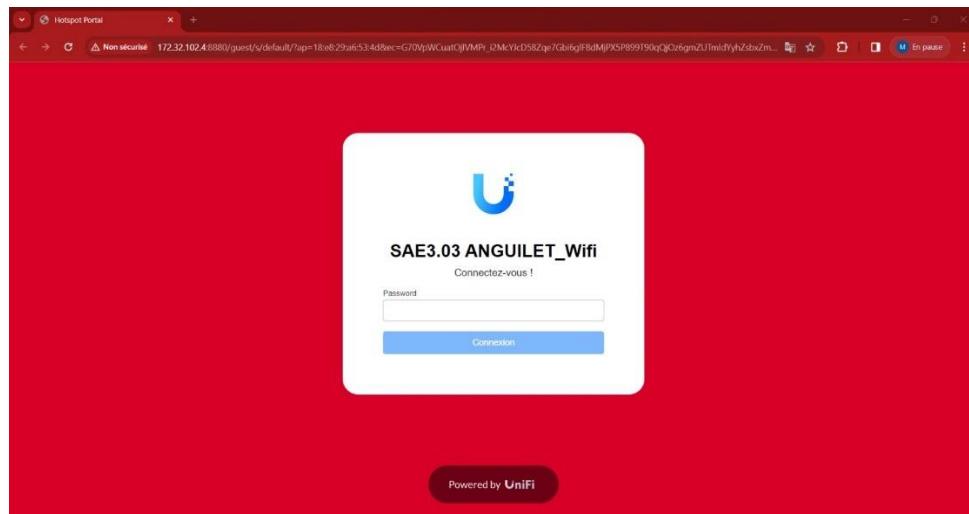
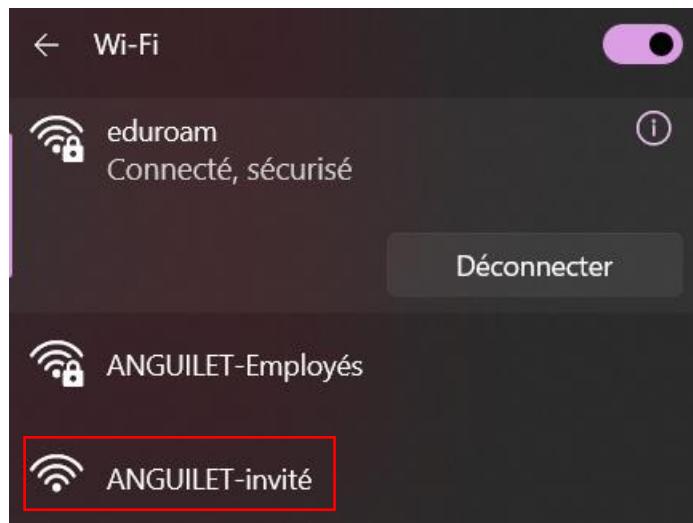
WiFi Scheduler: [Off](#) [On](#)

ANGUILET QUABEN Jonathan – C2

➤ Configuration du portail captif.

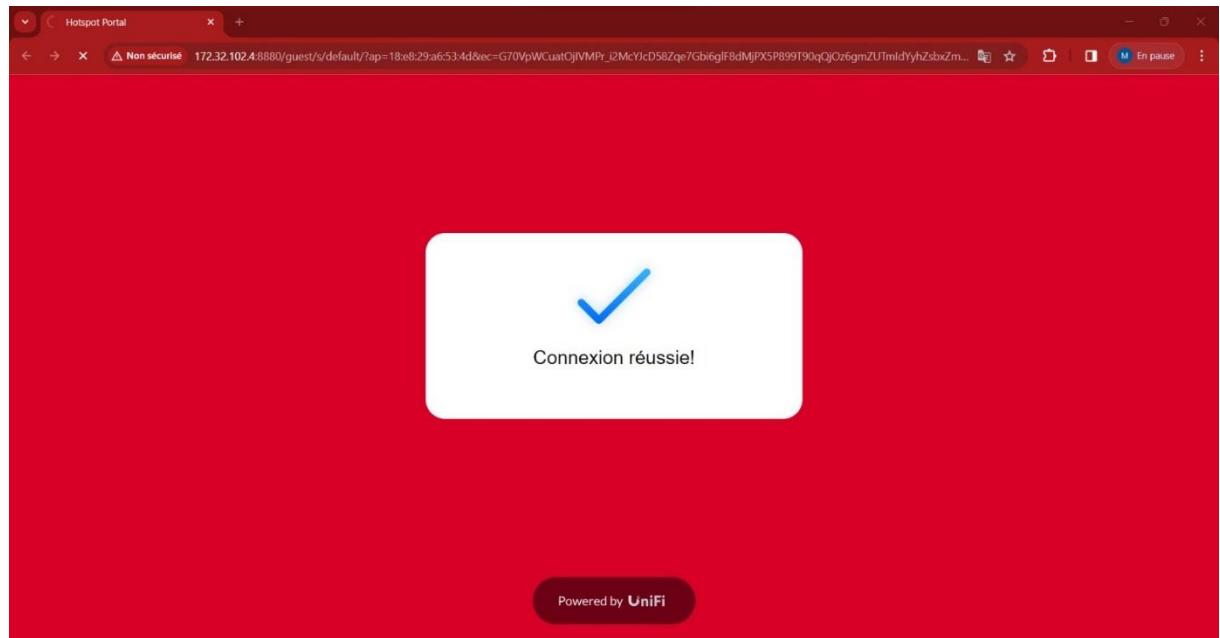
The screenshot shows the UniFi Network interface under the 'Network' tab. The 'Landing Page' tab is active. A sidebar on the left contains icons for various network components. The main area features a preview of a captive portal landing page with a red background, a blue UniFi logo, and the text 'SAE3.03 ANGUILLET_Wifi' and 'Connectez-vous !'. It includes a password input field and a 'Connexion' button. To the right, the 'Authentication Methods' section is expanded, showing options like Facebook, Password (highlighted with a red border), Payment, Vouchers, and RADIUS. An 'Edit' button is visible next to the Password option. Below this is the 'One Way Methods' section with an 'External Portal Server' option.

➤ TEST CONNEXION WIFI INVITÉ



ANGUILET QUABEN Jonathan – C2

MOT DE PASSE : Root1234.

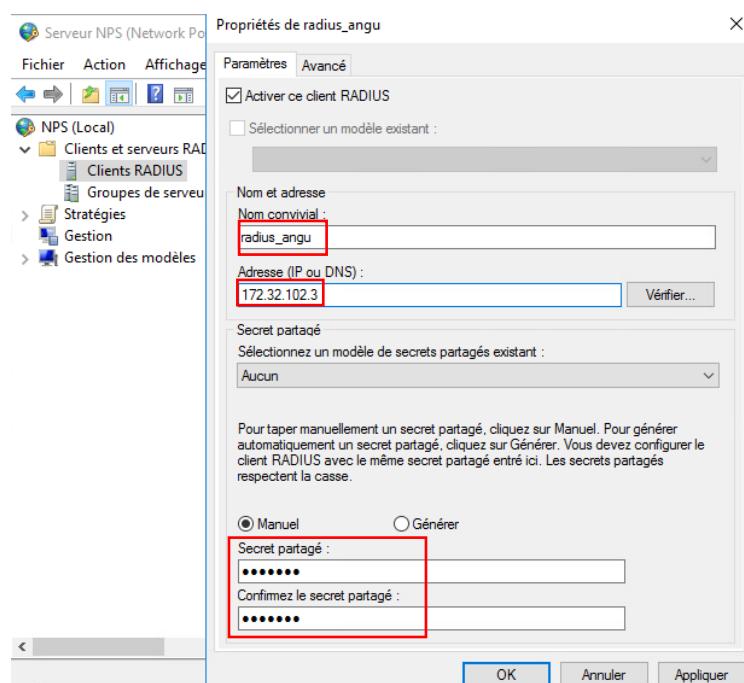


PARTIE AUTHENTIFICATION WIFI

Pour cette partie je vais utiliser un serveur radius pour gérer l'accès au point d'accès wifi. J'utiliserai le service AD DS pour jumeler un annuaire utilisateur au serveur radius.

Pour l'installation de radius je me suis servi de ce [tuto](#).

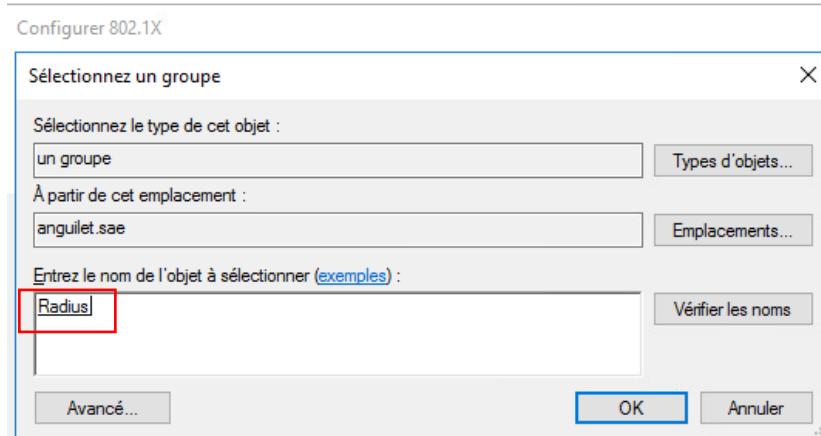
Sur RADIUS j'ai installé un client avec l'adresse IP de mon point d'accès et une clef partagée.



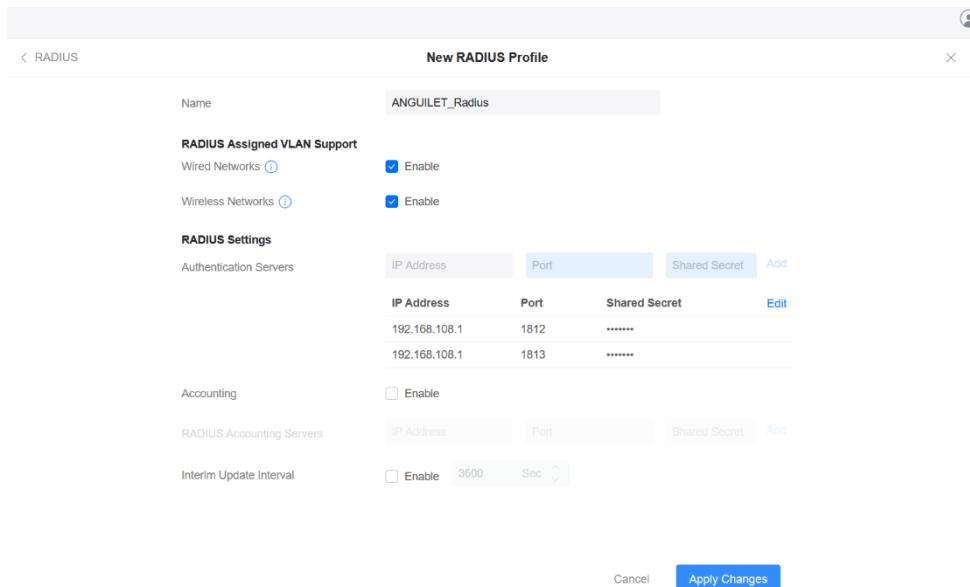
ANGUILET QUABEN Jonathan – C2



J'ai mis en place un groupe d'utilisateurs pour RADIUS que j'ai créé au préalable dans l'AD.



Pour lier le serveur RADIUS au point d'accès j'ai configuré un profil RADIUS sur lequel j'ai renseigné l'adresse IP de mon serveur RADIUS ainsi que la clef partagée que j'ai créée sur ce même serveur.



ANGUILET QUABEN Jonathan – C2

➤ TEST CONNEXION WIFI Employés

LOGIN : tech

MOT DE PASSE : Root1234.

