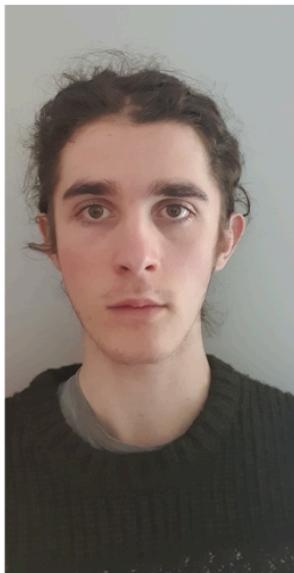


Dossier de projet



PANABIERES VINCENT

Administrateur d'infrastructure sécurisé

Titre professionnel : Administrateur d'infrastructures sécurisées

Nom : Panabieres

Prénom : Vincent

En Formation à La Plateforme_, 8 rue d'Hozier 13002 Marseille,

1.Introduction

1.1. Présentation personnelle

Je m'appelle Vincent PANABIERES, je suis actuellement en formation administrateur en infrastructures sécurisées à La Plateforme_.

Passionné par le monde de l'informatique depuis très jeune, après de nombreuses nombreuses heures de recherche dans le domaine de l'informatique je me suis tourné vers la cybersécurité et l'administration réseau et system.

Ce choix à était mûrement réfléchi, depuis petit étant attiré par l'informatique et la sécurité informatique je trouvais ce domaine passionnant.

Après une première année dans le cursus de la Plateforme_ j'ai décidé de continuer sur deux années en alternance afin d'intégrer un environnement professionnel et acquérir les compétences nécessaires à l'obtention du titre « Administrateur d'infrastructures sécurisées ».

1.2. Résumé

Durant mon alternance, j'ai eu l'opportunité d'intégrer un poste de support technique dans la société OPTIMALSI qui est une entreprise d'informatique et d'infogérance se basant sur Manosque

L'objectif de mes missions était d'assister au mieux les clients afin qu'ils puissent travailler dans un environnement de travail adéquat. Ainsi que d'administrer le parc informatique entièrement et de superviser la cybersécurité.

Mes missions consistaient à :

- Support technique téléphonique pour tout nos clients
- configuration gestion et mise en place de serveurs
- Supervision de la cybersécurité
- intervention sur site
- Vérification Backups

1.3. Summary in English.

During my work-study program, I had the opportunity to take on a technical support position at OPTIMALSI, an IT and managed services company based in Manosque.

The goal of my role was to provide the best possible assistance to clients so they could work in a suitable and efficient environment. I was also responsible for fully managing the IT infrastructure and overseeing cybersecurity.

My main tasks included:

- Providing technical support over the phone to all our clients
- Configuring, managing, and setting up servers
- Monitoring cybersecurity
- Performing on-site interventions
- Verifying backups

1.4. ENTREPRISE

OPTIMAL SI est une société de services informatiques et d'infogérance, fondée en 2010 (ou 2011 selon les sources) et basée à Manosque, en région PACA. Elle propose une offre globale à destination des TPE et PME, incluant l'infogérance, l'intégration de logiciels de gestion (comptabilité, paie, CRM), le développement sur mesure, la formation et le support technique .

L'entreprise met l'accent sur trois grands piliers :

- Un service personnalisé fondé sur la disponibilité, la compétence et la confiance,
- Une forte ancrage local, avec 100 % de ses collaborateurs recrutés dans la région PACA.,
- Et un engagement réel pour une informatique éco-responsable : cloud optimisé, recyclage des équipements, dématérialisation, formation des clients à des pratiques plus vertueuses.

Aujourd'hui, OPTIMAL SI se distingue par sa taille à dimension humaine (quelques collaborateurs), ses solutions sur mesure pour les PME et son approche alliant professionnalisme, proximité et durabilité.

1.5. Présentation de l'équipe

La société Optimalsi s'orchestre sur 3 axes majeurs, l'infrastructure et l'infogérance dans lequel je faisais partie ainsi que 2 techniciens, ensuite il y a la partie Logiciel qui est gérée par Bruno qui est le premier responsable. Cette axe se concentre sur la gestion des logiciels métier comme Sage, les logiciels de paiement ainsi qu'à la GED.

Et enfin il y a l'axe développement qui est géré par Jean-Claude, le deuxième responsable. Son rôle est de créer des programmes sur mesure sur demande du client.

Il y a aussi la partie commerce qui est gérée par Guillaume, son rôle est de fournir une solution adaptée pour chaque demande.

2.1. Mon rôle

Depuis mon intégration chez OPTIMALSI, j'évolue au sein du département Infrastructure, où je suis pleinement impliqué dans la gestion opérationnelle et technique des infrastructures systèmes, réseaux et sécurité, principalement pour le compte de nos clients professionnels. Mon rôle est varié et combine support utilisateur via ticketing, gestion de l'infrastructure cloud, sécurité des postes, sauvegardes, et interventions sur site.

Support technique – Ticketing (activité principale)

L'essentiel de mon activité quotidienne repose sur la gestion des tickets d'assistance, qui représente une part majeure de mon poste. À travers notre outil de ticketing interne, je suis en charge de :

- Réceptionner, analyser et traiter les demandes des clients (incidents, pannes, demandes de configuration ou d'évolution) ;
- Prioriser les tickets en fonction de l'urgence et de l'impact ;
- Assurer un suivi rigoureux des interventions, de l'ouverture à la clôture du ticket, en maintenant une communication claire avec le client ;
- Rédiger des comptes-rendus détaillés dans chaque dossier, afin d'assurer la traçabilité des actions menées ;

- Escalader les tickets complexes ou bloquants au bon niveau si nécessaire, tout en documentant précisément les étapes déjà effectuées.

Ce travail me permet de garder une vision globale de l'état des infrastructures clients, tout en apportant des solutions réactives et efficaces au quotidien.

Administration de l'infrastructure cloud – Nutanix

Parallèlement au support, je participe à l'administration de notre infrastructure cloud basée sur Nutanix, en réalisant notamment :

- Le déploiement, la configuration et la gestion des machines virtuelles ;
 - La surveillance des performances et de la disponibilité des services ;
 - Le maintien en conditions opérationnelles des environnements clients hébergés sur notre plateforme.
-

Gestion des sauvegardes clients

Je suis en charge de la gestion complète des sauvegardes, une mission essentielle pour garantir la sécurité des données :

- Planification, supervision et vérification des sauvegardes quotidiennes ;
- Réalisation de tests de restauration pour assurer la fiabilité ;

- Intervention rapide en cas d'échec ou de restauration d'urgence.
-

Sécurité des postes – Supervision via ESET

Afin d'assurer la cybersécurité, je supervise l'état des postes de travail à l'aide de la solution ESET :

- Suivi des alertes de sécurité, mises à jour, et scans réguliers ;
 - Gestion centralisée des politiques antivirus ;
 - Support auprès des utilisateurs en cas de menace détectée.
-

Interventions sur site

En complément de mes tâches à distance, je suis régulièrement amené à me déplacer chez les clients pour :

- Installer ou dépanner du matériel (PC, imprimantes, routeurs, etc.) ;
 - Configurer des équipements réseau ou des serveurs sur place ;
 - Réaliser des audits techniques et accompagnements personnalisés.
-

Autres responsabilités techniques

- Administration des services réseau : Active Directory, DNS, DHCP, etc. ;

- Support de niveau 2 et 3 selon la complexité des demandes ;
- Rédaction de documents techniques et procédures ;

2.2. Une journée type de travail

Au sein du département Infrastructure d'OPTIMALSI, mes journées s'organisent selon un ordre logique, orienté vers la supervision proactive des systèmes, la gestion des demandes clients, ainsi que les interventions techniques. Bien que certaines tâches soient récurrentes, d'autres dépendent de l'actualité des projets ou des urgences rencontrées.

Supervision quotidienne des infrastructures

Chaque matin débute par une phase essentielle de supervision. Je procède à une vérification complète de l'état des systèmes et des postes utilisateurs pour détecter tout dysfonctionnement ou alerte critique. Ce travail inclut la vérification des sauvegardes automatiques de la veille (succès, échecs, anomalies), le suivi des alertes de sécurité provenant de notre solution antivirus ESET, ainsi que le contrôle des éventuels problèmes de performance sur l'infrastructure (notamment au niveau des machines virtuelles hébergées sur notre environnement Nutanix).

À l'issue de cette analyse, je rédige un rapport interne détaillant les incidents ou points de vigilance identifiés. Les problèmes détectés font immédiatement l'objet d'un traitement prioritaire afin de garantir la stabilité et la sécurité des environnements clients.

Configuration et intégration de nouveaux clients

Lorsqu'un nouveau client rejoint OPTIMALSI, je participe à la mise en place de son environnement technique. Cela comprend la création de machines virtuelles sur la plateforme Nutanix, la configuration des ressources (CPU, RAM, stockage, réseau), l'activation des sauvegardes, la mise en place des outils de sécurité, ainsi que l'intégration des utilisateurs dans l'Active Directory. J'interviens également dans la configuration des services réseaux (DHCP, DNS, partages de fichiers, droits d'accès, etc.) en fonction des besoins spécifiques du client.

Cette phase inclut également la rédaction de la documentation technique pour assurer un suivi clair et permettre une bonne continuité dans la gestion du compte client.

Support utilisateur via le système de ticketing

Une part importante de ma journée est consacrée à la gestion des tickets d'assistance technique. C'est une activité centrale de mon poste. J'interviens sur des tickets de niveau 1, 2 et parfois 3, selon la complexité des demandes. Ces tickets peuvent concerner des problèmes logiciels, des incidents liés à l'infrastructure (accès réseau, droits utilisateurs, imprimantes, services partagés...), ou encore des besoins de configuration ponctuels.

Mon rôle consiste à analyser chaque demande, apporter une solution dans les meilleurs délais, documenter chaque action réalisée, et assurer un suivi clair et professionnel jusqu'à la résolution complète du problème.

Interventions sur site (selon les besoins)

Enfin, selon les cas, je suis amené à me déplacer chez les clients pour effectuer des interventions sur site. Ces déplacements peuvent concerner l'installation ou le dépannage de matériel (postes de travail, imprimantes,

routeurs, etc.) , la vérification de l'état du réseau local, ou encore l'accompagnement des utilisateurs sur place. Ces interventions permettent de mieux comprendre l'environnement réel du client, d'installer des solutions adaptées et de maintenir une relation de proximité.

2.4. Mon future

Actuellement en alternance au sein de l'entreprise OPTIMALSI, je souhaite poursuivre mon parcours professionnel dans la continuité de cette expérience formatrice. Mon objectif à court et moyen terme est de rester dans l'entreprise pendant encore trois à quatre ans après l'obtention de mon diplôme. Cette période me permettra de continuer à développer mes compétences techniques en infrastructure, de gagner en responsabilité, et de consolider mon autonomie sur des projets d'envergure.

OPTIMALSI m'offre un environnement de travail stimulant et varié, dans lequel je peux approfondir mes connaissances tout en étant au contact direct des clients, des environnements cloud, de la cybersécurité et du support technique. En restant plusieurs années supplémentaires, je souhaite maîtriser pleinement les outils et les méthodes utilisés en production, tout en continuant à apprendre aux côtés d'une équipe expérimentée.

À plus long terme, j'ai pour ambition de partir travailler à l'étranger, dans un pays anglophone, afin de perfectionner mon anglais professionnel, de sortir de ma zone de confort et de découvrir une nouvelle culture et un autre mode de travail. Cette expérience internationale me permettra d'acquérir une ouverture d'esprit, une capacité d'adaptation et une richesse humaine précieuse pour la suite de ma carrière. Je suis convaincu que travailler à l'étranger est un excellent moyen de progresser aussi bien sur le plan technique que personnel.

En résumé, mon projet post-diplôme s'inscrit dans une double logique : capitaliser sur l'expérience acquise chez OPTIMALSI dans un premier temps, puis m'enrichir par une expérience professionnelle à l'international, avant de potentiellement revenir en France avec un profil plus complet et tourné vers l'avenir.

3. PROJET FERME RDS

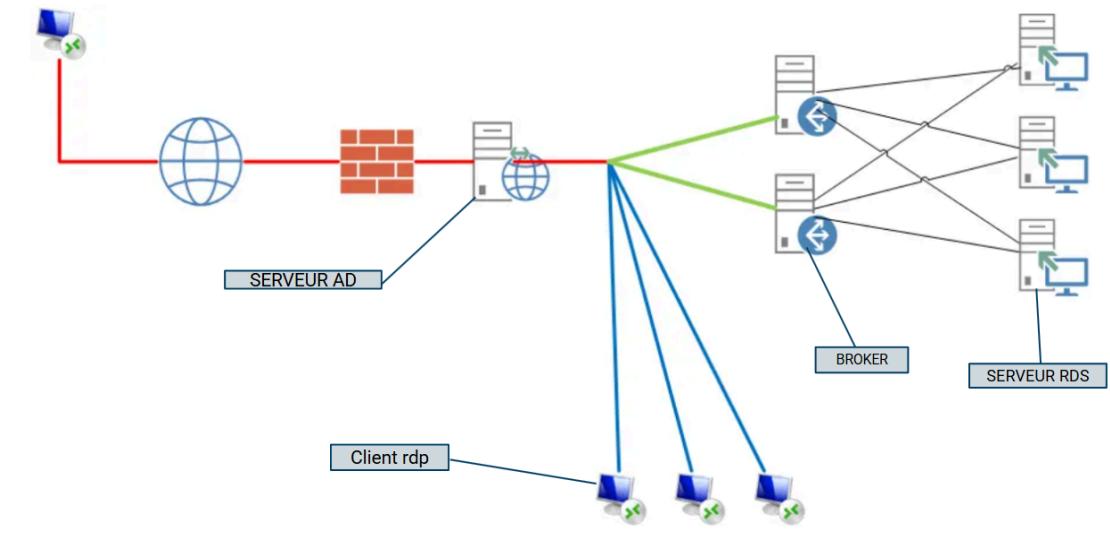
3.1 EXPLICATION D'UNE FERME RDS ET SON BUT

Maintenant passons au projet, une ferme RDS (Remote Desktop Services) est un ensemble de serveurs configurés pour fournir des bureaux à distance ou des applications virtualisées à plusieurs utilisateurs simultanément. Elle permet aux utilisateurs d'accéder à un environnement Windows complet, hébergé sur des serveurs, via une simple connexion réseau.

Concrètement, une ferme RDS comprend généralement :

- Un ou plusieurs serveurs hôtes de session (où les utilisateurs se connectent),
- Un broker (gestionnaire de connexions) qui distribue les sessions,
- Et parfois une passerelle RDS pour l'accès à distance sécurisé.

Cela permet aux entreprises de centraliser les ressources, de sécuriser les données et de simplifier la gestion des postes de travail.



La ferme RDS est le plus souvent utilisée pour des entreprises de taille moyenne (environ 40 utilisateurs), le but principal étant de répartir au mieux les utilisateurs dans les différents serveurs afin d'avoir des performances stables lors de l'utilisation.

Context :

Nous avons un nouveau client de taille moyenne qui souhaite un serveur de travail pour tous ses collaborateurs.

Il nous faut créer une ferme RDS afin d'administrer au mieux ce nouveau client.

Pour ceci il nous faut mettre en place :

- 2 serveurs RDS
- 1 serveur Broker
- 1 serveur Active Directory
- 1 firewall Hardware
- Mise en place des logiciels de surveillance
- Mise en place des sauvegardes local

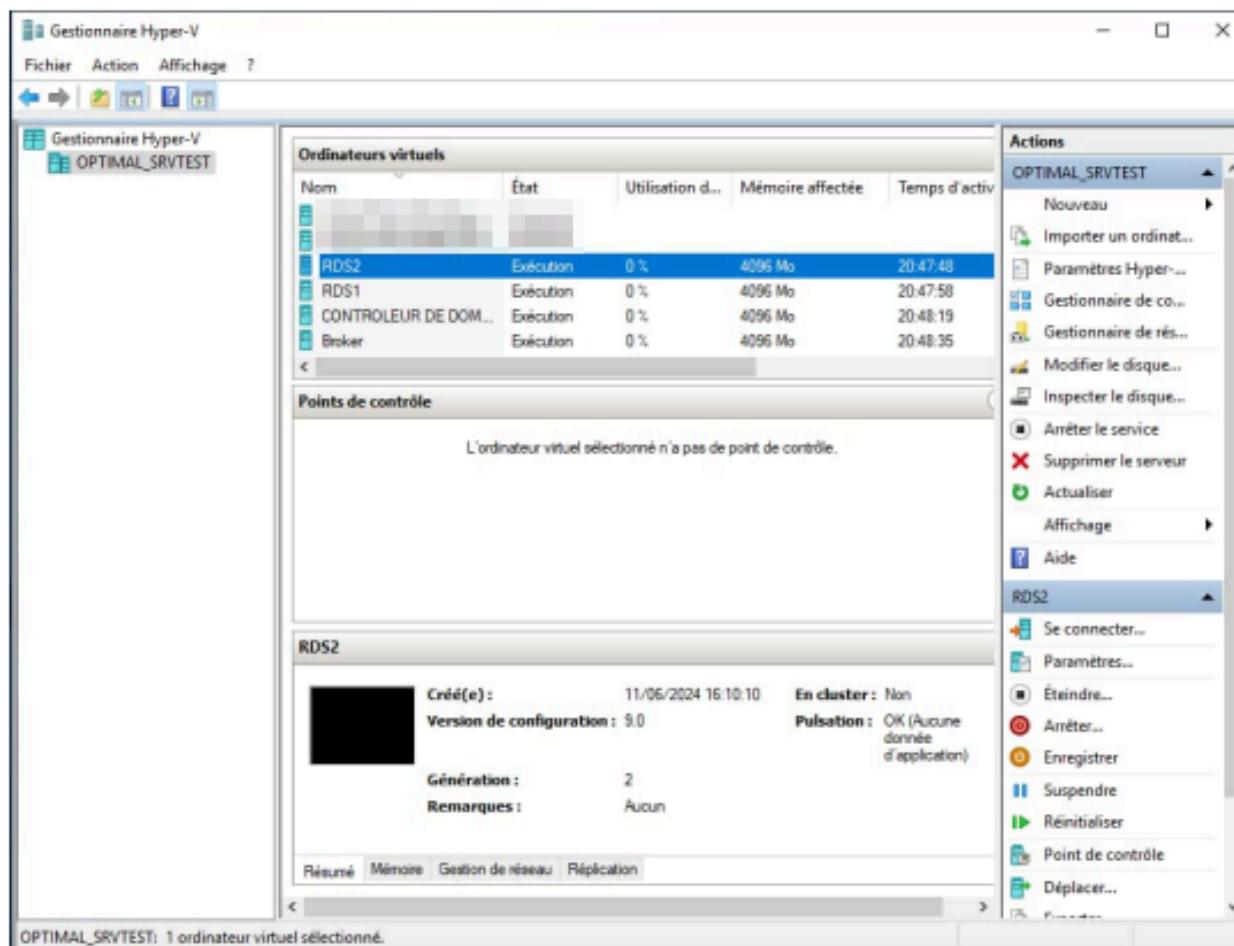
3.2 Crédation des VMs

Pour commencer nous allons créer les 4 VMs qui seront nécessaires à la mise en place.

La base matérielle étant un DELL poweredge r360 avec Windows Server 2019 d'installé ainsi que le rôle HYPER V natif.

Nous commençons par créer les 4 serveurs que nous allons nommer :

- RDS1
- RDS2
- broker
- CONTRÔLEUR DE DOMAINE



La mise en place des Windows server se fait par un fichier .iso personnalisé, qui ignore la plupart des instructions de configuration fournies.

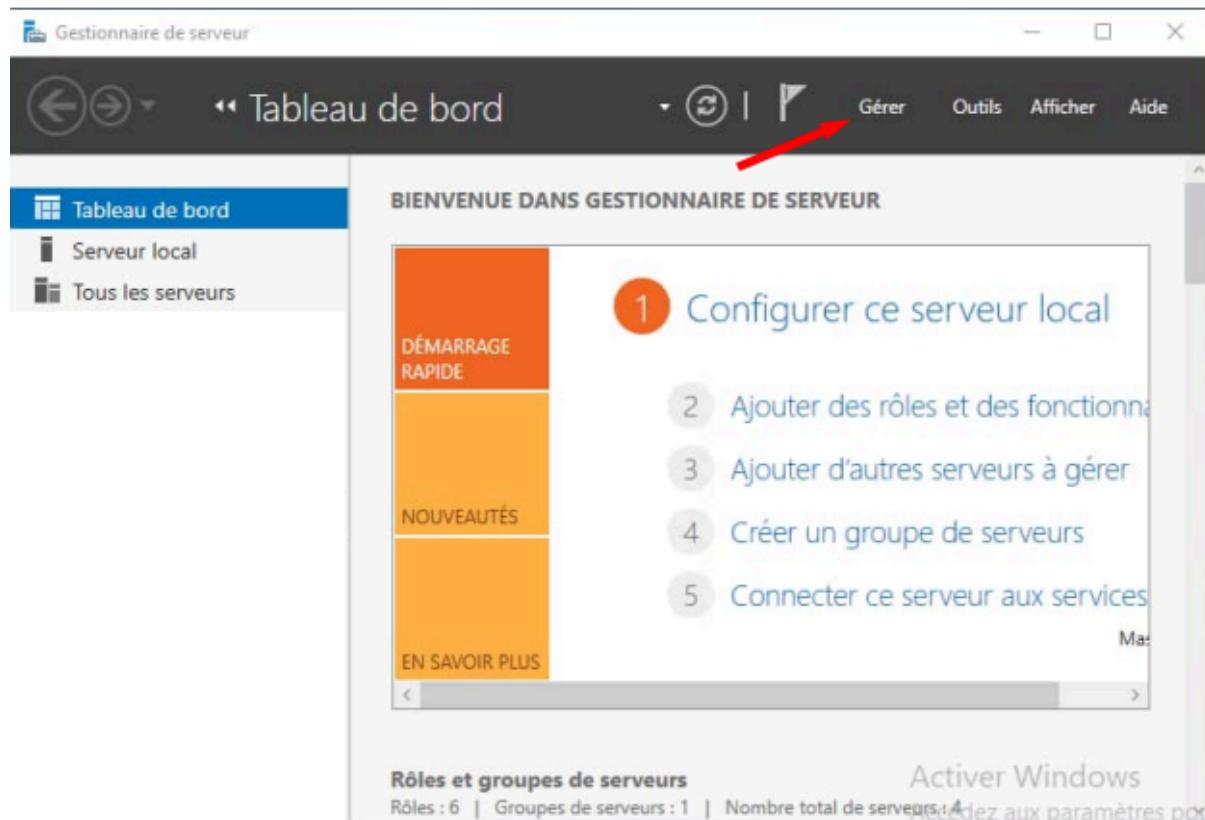
Les serveurs RDS ont le rôle de bureau à distance natif.

3.3 Configuration de l'Active Directory et du domaine.

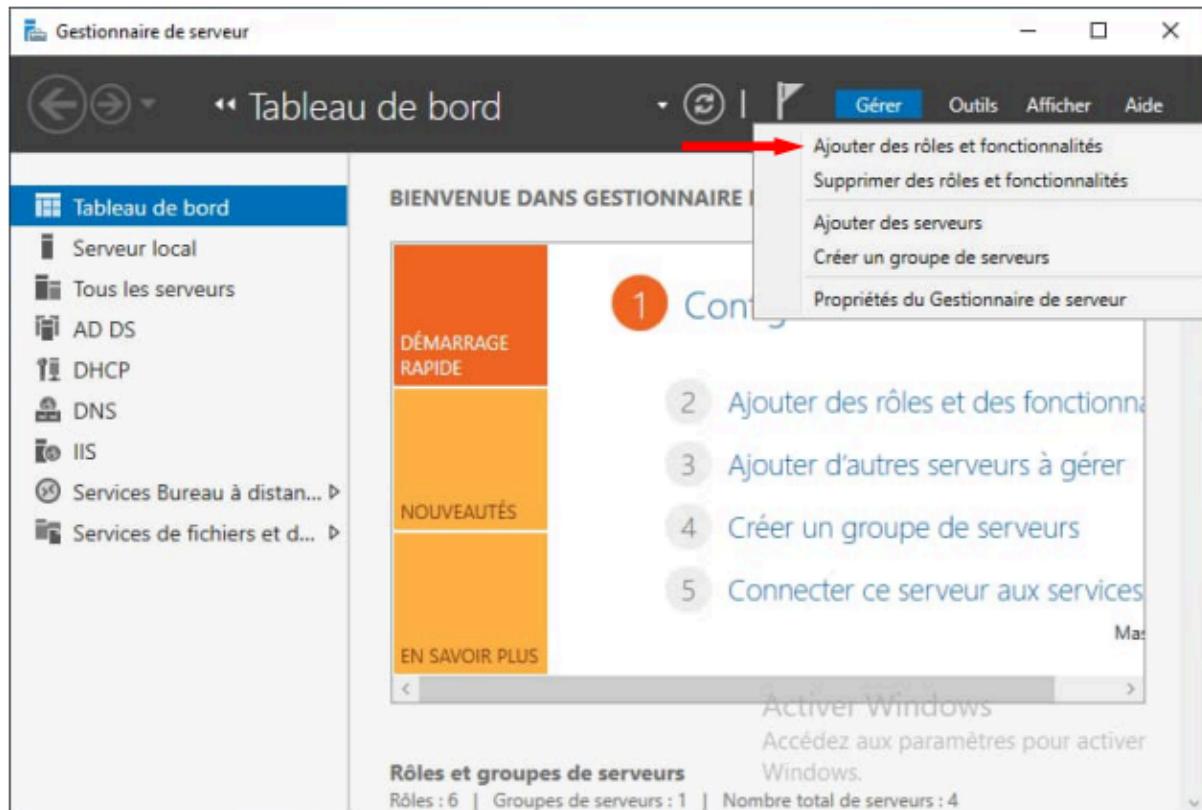
3.3.1 Installation du rôle de contrôleur de domaine

Une fois le serveur contrôleur de domaine installé nous pouvons configurer notre domaine pour ceci il nous faut nous connecter au serveur avec les codes administrateur.

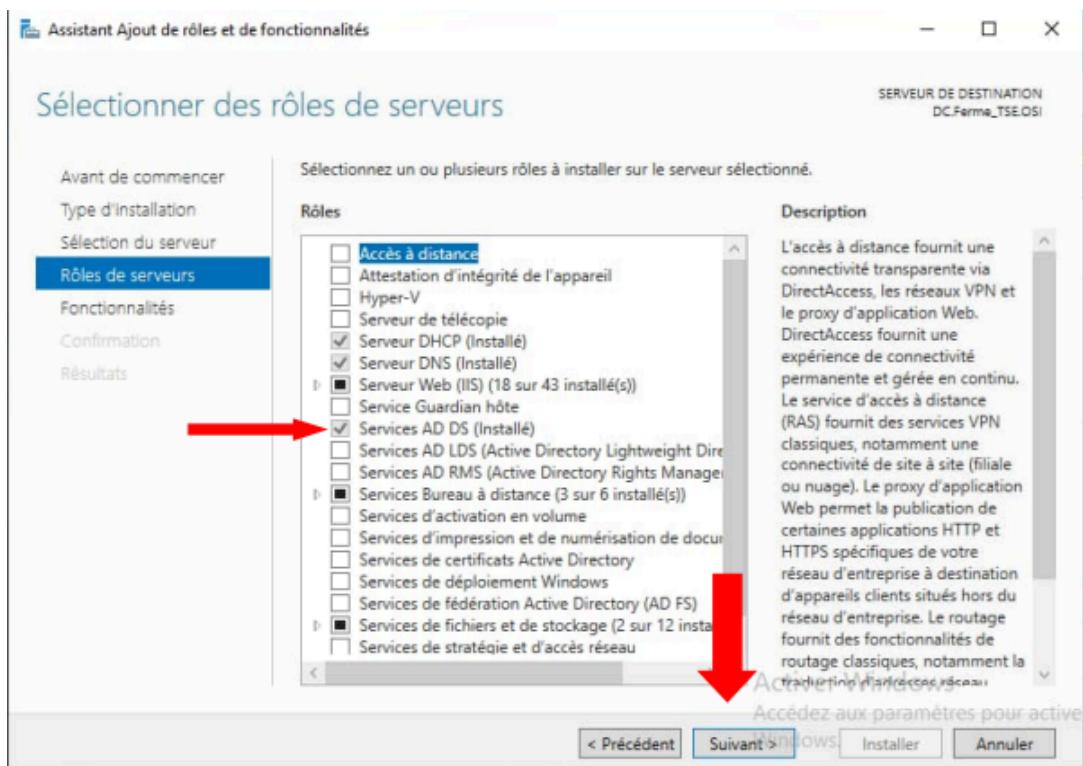
Une fois connecté nous lançons le gestionnaire de serveur et nous cliquons sur gérer.



Nous cliquons ensuite sur "ajouter des rôles et fonctionnalités"



Puis nous installons le rôle 'Service AD DS'



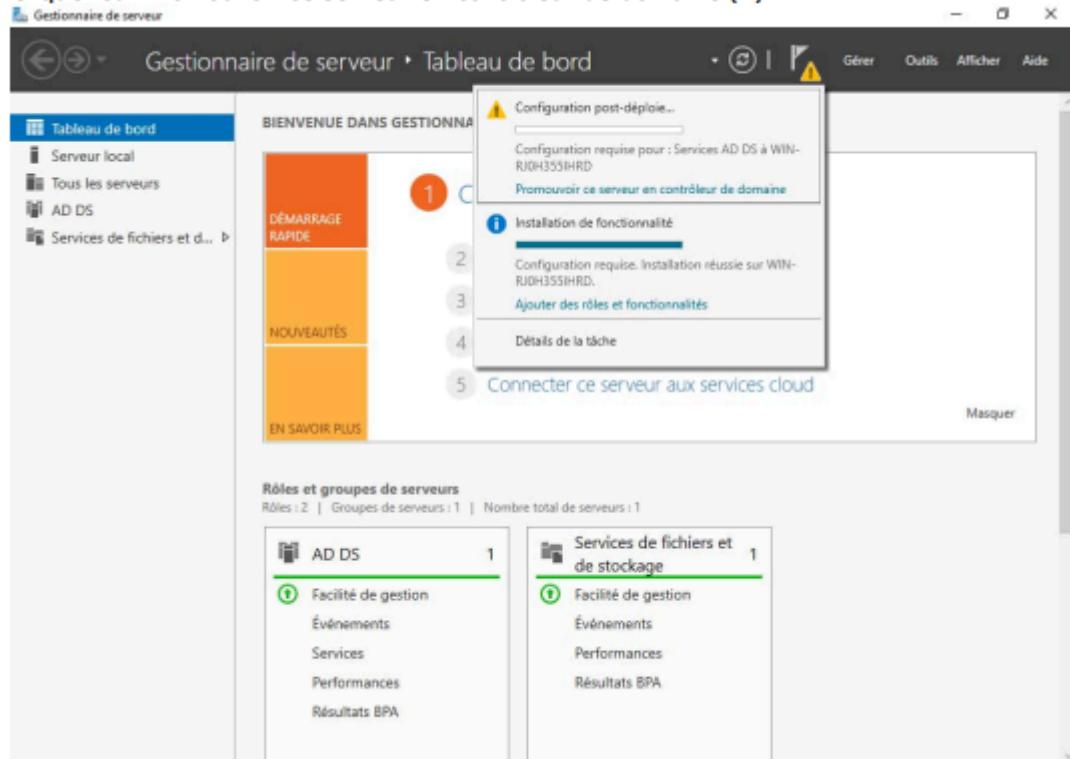
Nous redémarrons le serveur et le rôle est bien installé.

3.3.2 Création du domaine

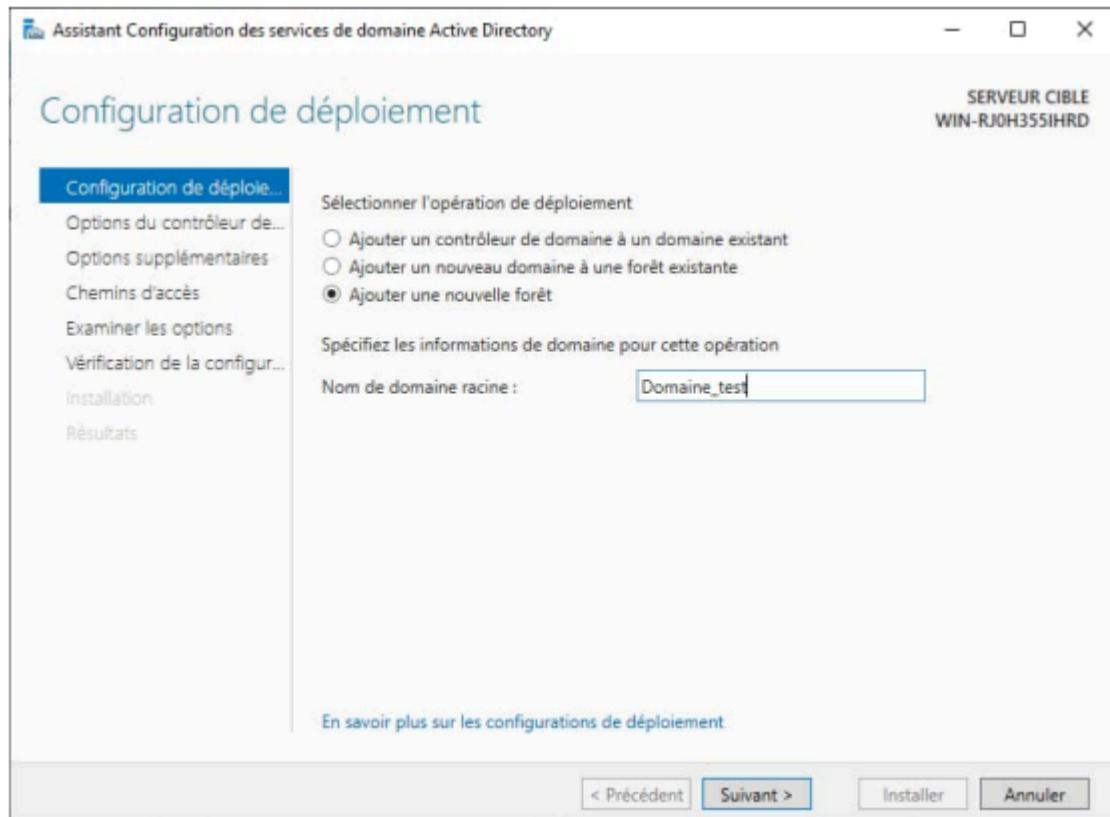
Maintenant que serveur a bien le rôle de contrôleur de domaine il nous faut en créer un.

Pour ce faire nous allons dans le gestionnaire de serveur et en haut à droite de l'écran un point d'exclamation est apparu.

Cliquer sur Promouvoir ce serveur en contrôleur de domaine (1)



Nous allons maintenant promouvoir le serveur en tant que contrôleur de domaine.



Nous entrons dans le nom que nous souhaitons. A noter que le nom donné à cette étape-ci ne peut pas être changé sous peine de devoir désinstaller le rôle et de le réinstaller de nouveau.

Le nom donné ici est : Domaine_test

Après avoir promu le serveur nous pouvons voir que l'application "active directory" est bien présente sur le serveur.

4. PARAMÉTRAGE RÉSEAU

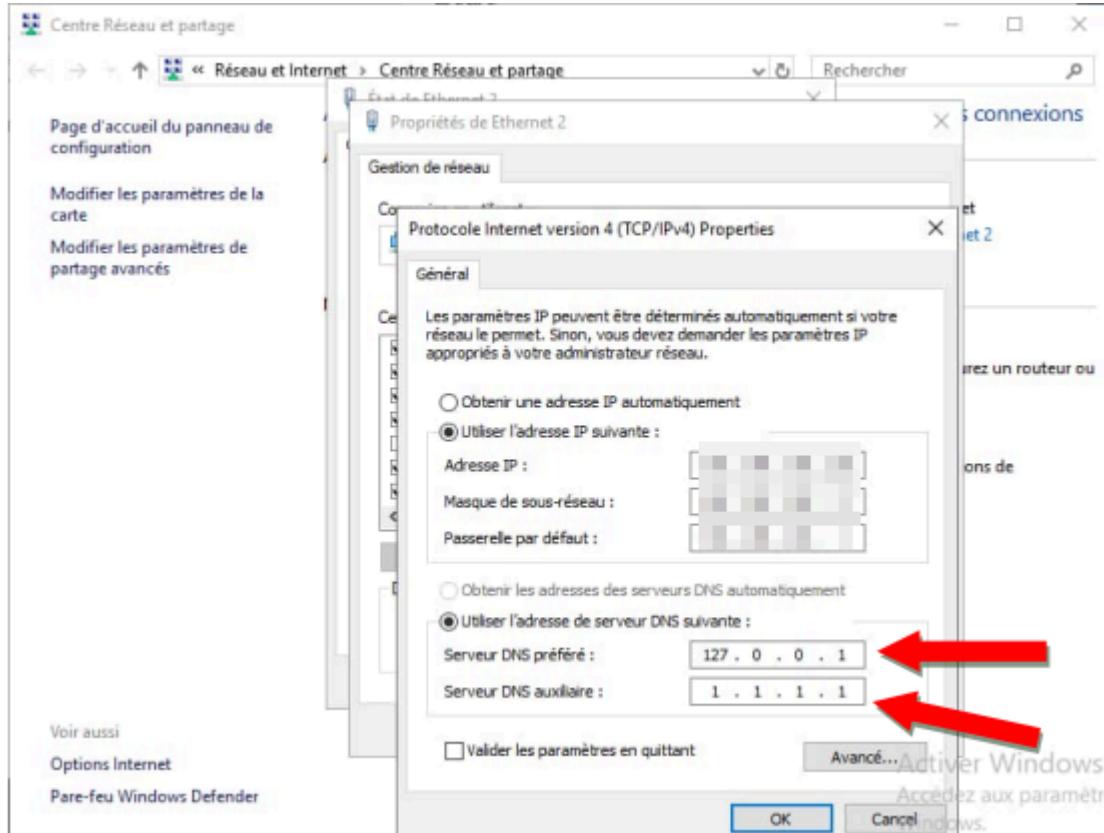
4.1 Configuration réseau

Maintenant il nous faut connecter les serveurs au réseau de l'entreprise en fixant l'adresse ip.

Pour ce faire, nous avons besoin de connaître la plage IP du routeur du client.

Nous allons donc nous connecter à tous les serveurs et leur enregistrer l'adresse ip que nous souhaitons.

Dans un premier temps nous allons le faire pour l'active directory.



Dans le centre réseau et partage nous configurons de la sorte :

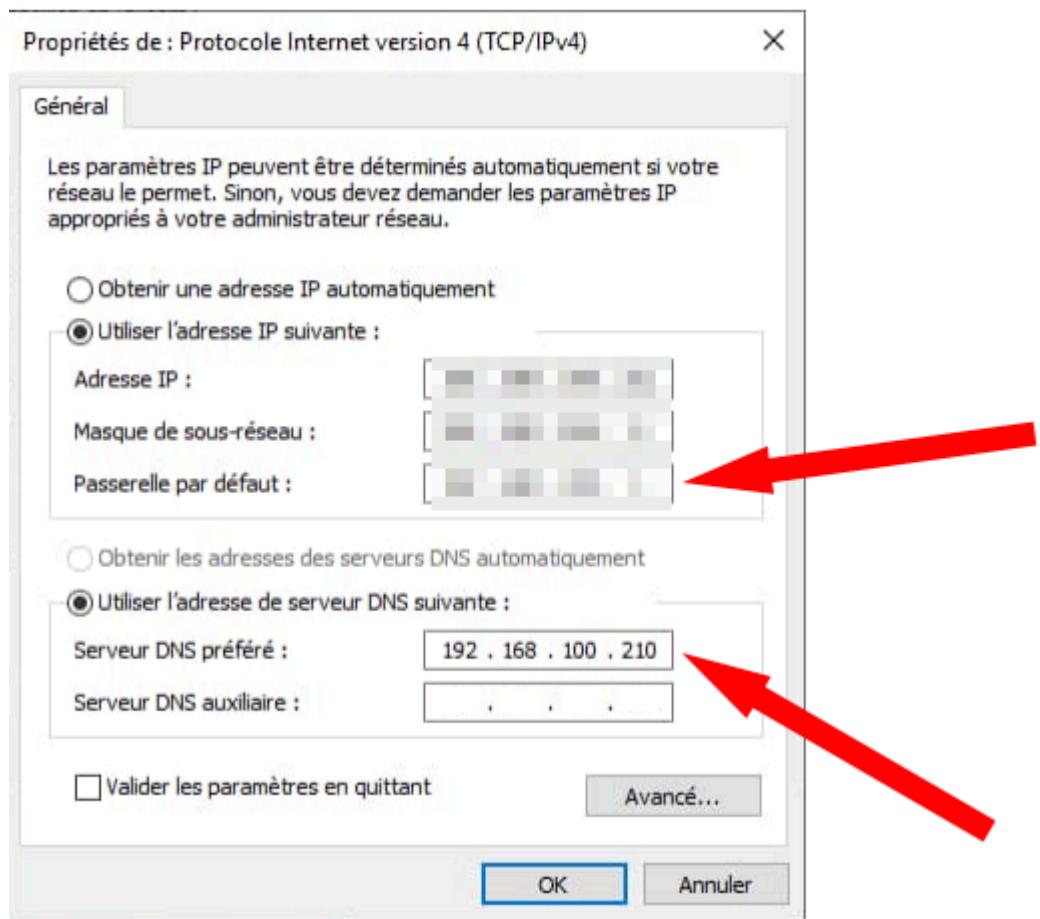
- adresse ip : l'adresse que nous voulons
- Masque de sous-réseau : ne change pas
- passerelle par défaut : l'adresse ip du routeur du client

-Serveur DNS préféré : 127.0.0.1 pour que le contrôle de domaine pointe sur lui même

De ce fait, nous pouvons faire la liaison entre les serveurs et le contrôleur de domaine.

Maintenant nous allons faire la même chose pour les serveurs RDS et le serveur broker.

La configuration devrait ressembler à ceci :



Dans la même optique que pour le contrôleur de domaine nous allons configurer IPv4 pour tous les autres serveurs :

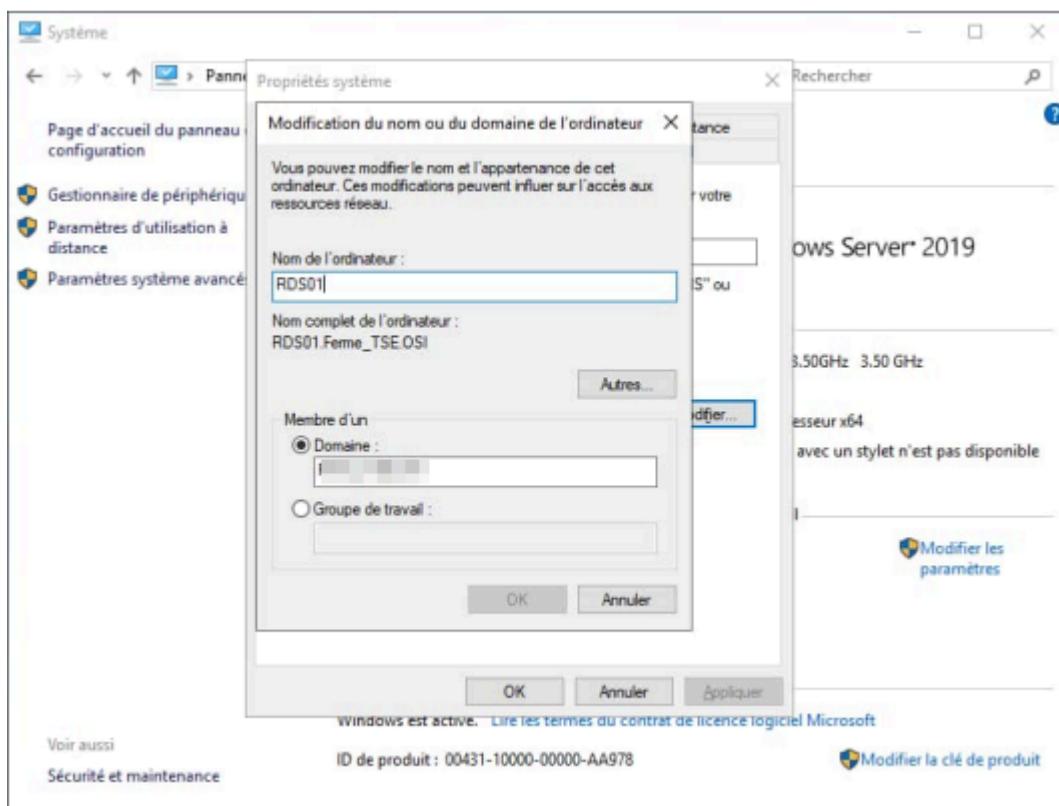
- Adresse IP: adresse ip différente à chaque fois pour éviter les conflits d'IP
- Masque de sous-réseau : ne change pas
- Passerelle par défaut : l'adresse IP du routeur du client

-Serveur DNS préféré : l'adresse ip du contrôleur de domaine qui a été configurée tout à l'heure.

4.2 Connexion au domaine

Maintenant que les serveurs ont leurs ip de fixé nous pouvons entrer les VMs dans le domaine que nous avons créé précédemment.
Pour ce faire nous allons passer sur tous les serveurs (sauf l'active directory).

Pour cela nous allons aller dans les paramètres système de chaque machine et les rentrer dans le domaine.



Entrer le mot de passe administrateur du contrôleur de domaine qui a été configuré lors de la création du domaine.

Après avoir fait cela pour toutes les machines votre domaine est prêt et vos VMs devraient apparaître dans votre Active directory.

5. INSTALLATION DU BROKER

5.1 Ajout des serveurs

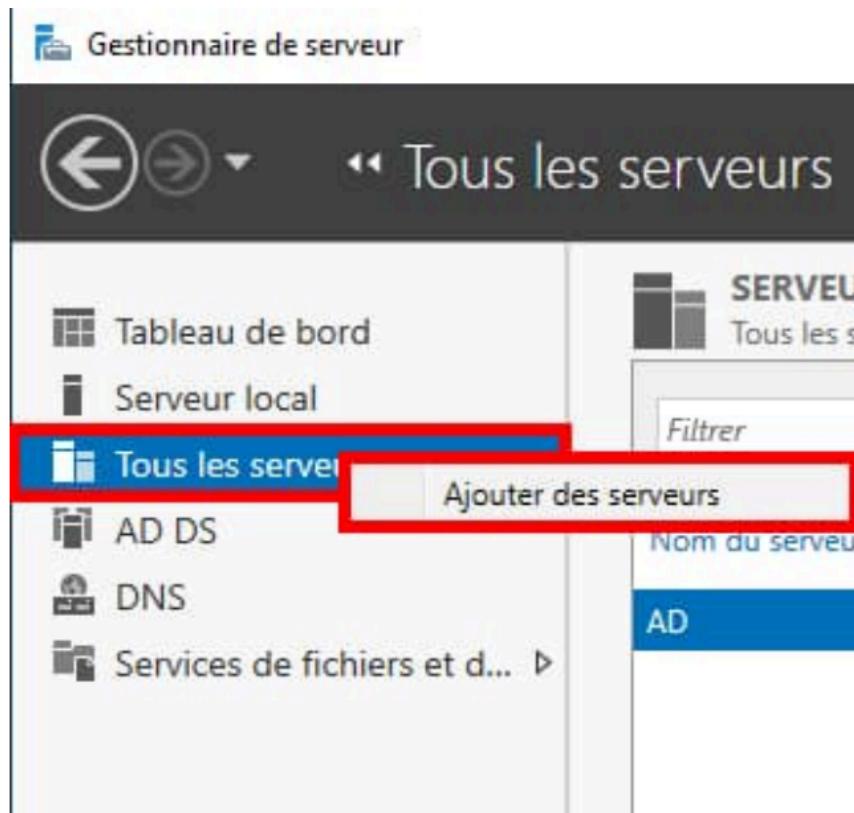
5.1.1 Crédit pool de serveur

Le broker RDS gère la répartition et la connexion des utilisateurs aux serveurs disponibles dans la ferme, assurant ainsi une distribution équilibrée des sessions.

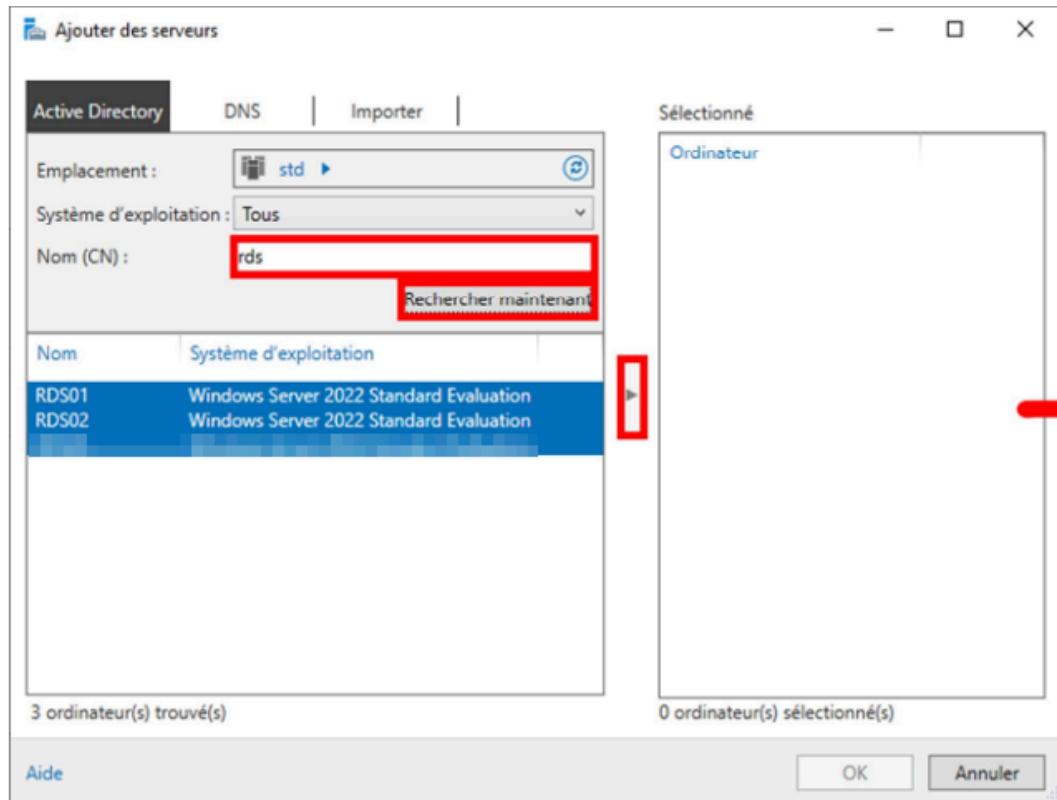
Il permet aussi de reconnecter un utilisateur à sa session existante pour garantir la continuité du travail.

Pour le mettre en place nous allons dans un premier temps nous connecter au serveur AD et créer un pool de serveur.

Dans le gestionnaire de serveur nous allons cliquer sur "ajouter des serveurs" comme montré dans la capture d'écran :



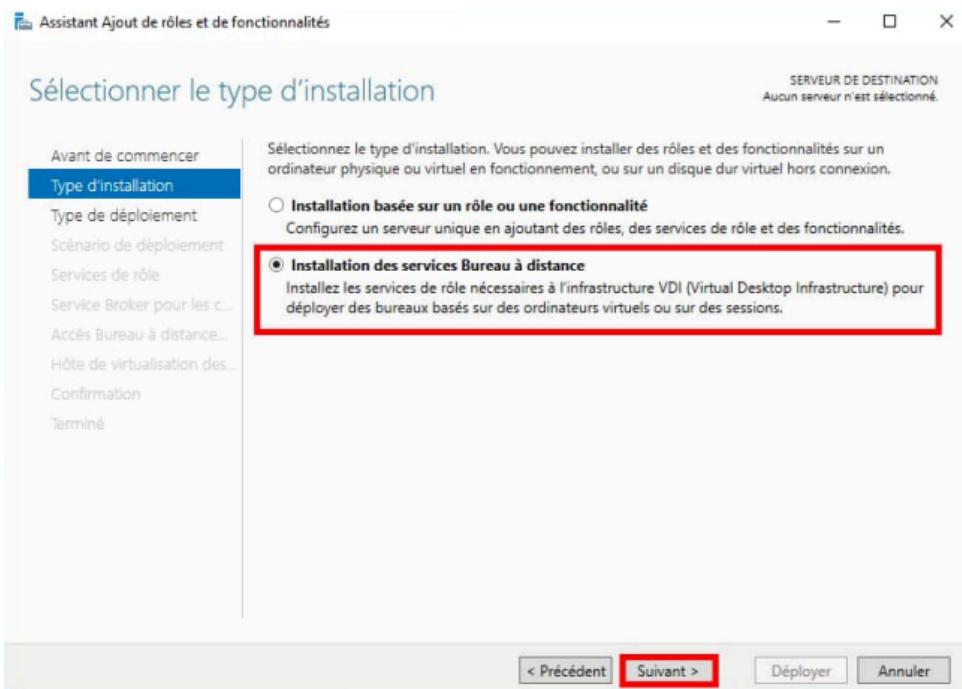
Nous allons ensuite donner un nom au pool de serveur et ensuite sélectionner les serveurs et les ajouter



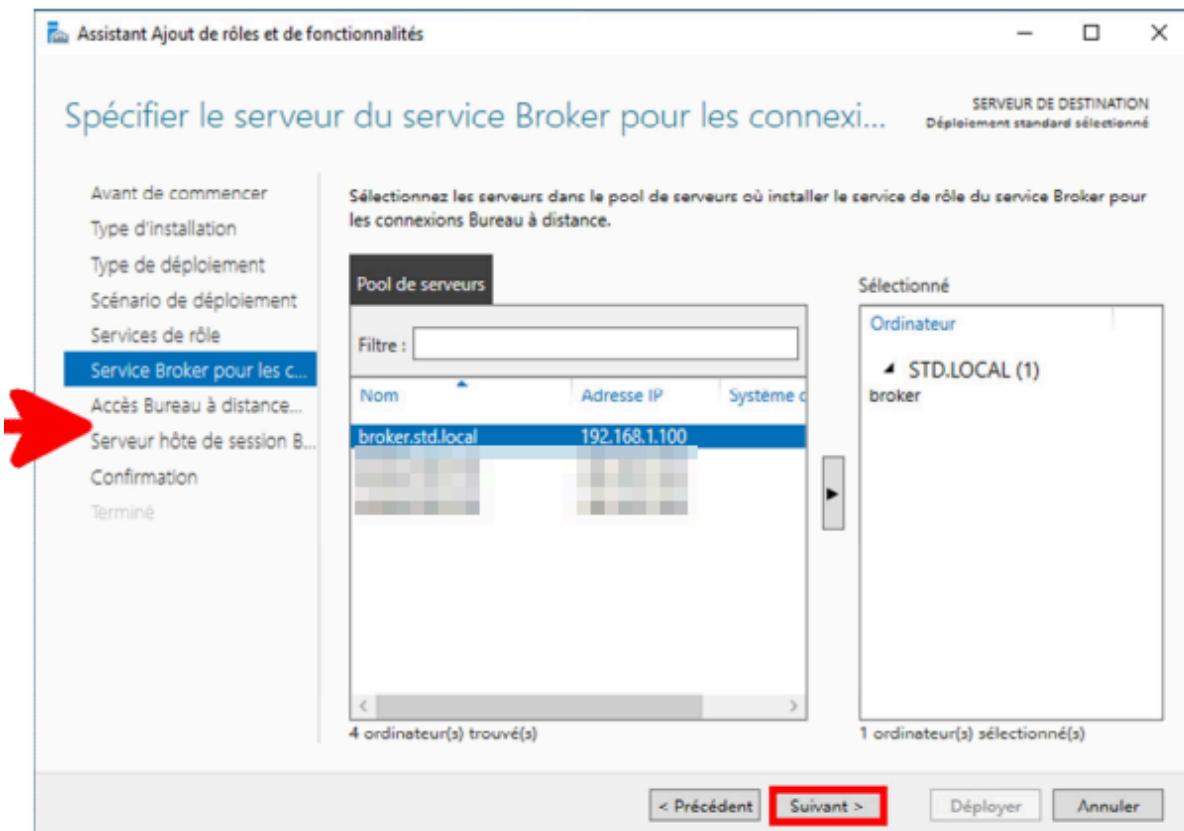
5.1.2 Installation du broker

Nous allons maintenant configurer le broker afin qu'il puisse faire la répartition sur les deux autres serveurs.

Une fois dessus nous allons installer un rôle broker, pour ce faire nous allons aller dans le gestionnaire de serveur et installer le rôle de bureau à distance :



Nous allons ensuite choisir quel serveur va recevoir le rôle de "broker" et "d'accès au bureau à distance"



Une fois installé le broker est en service mais ne sait toujours pas sur quel serveur va-il répartir les utilisateurs.

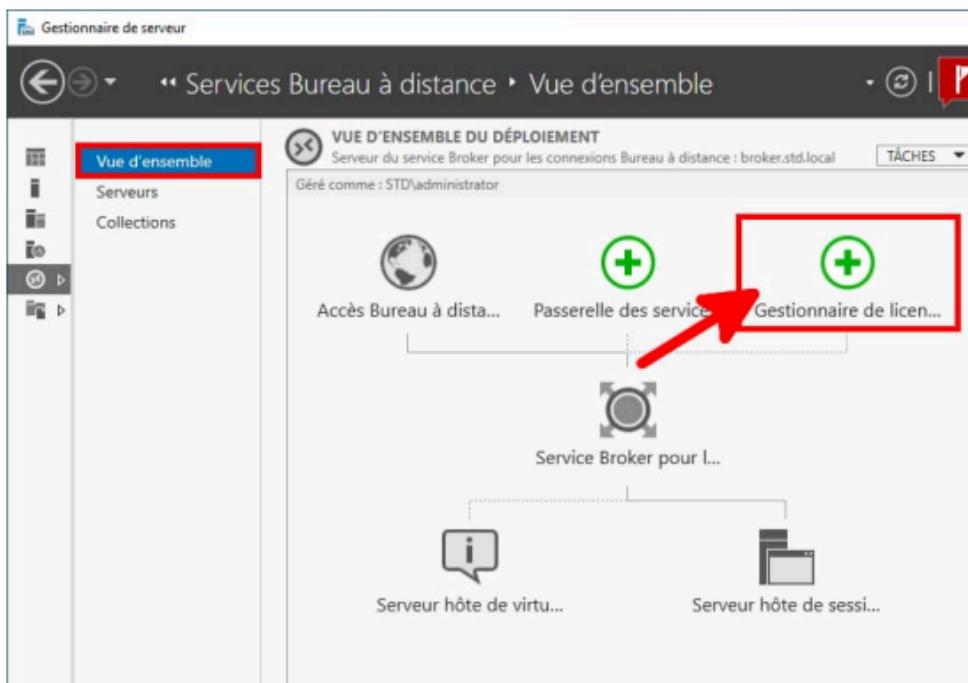
5.2 POST-INSTALL

5.2.1 Serveur de licence + CAL RDS

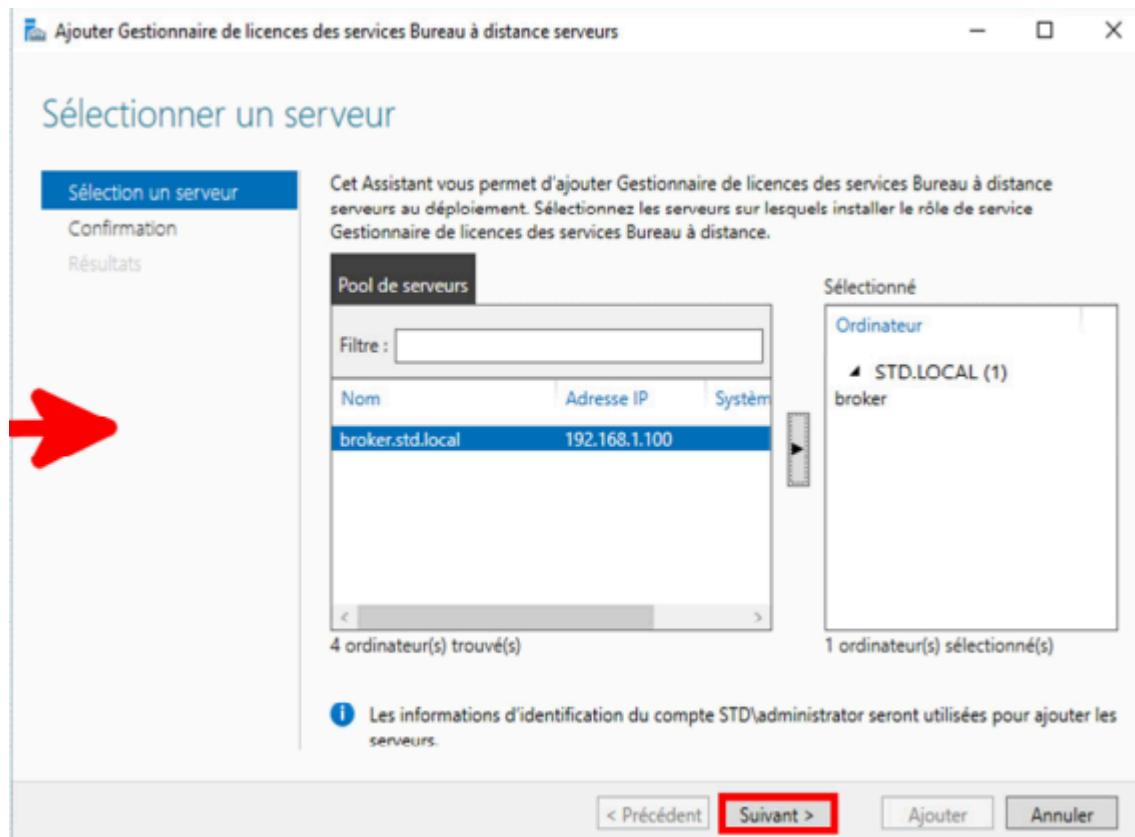
Une fois le rôle de broker installé il nous faut un gestionnaire de licence afin de pouvoir un CAL RDS.

Un CAL RDS (Client Access License Remote Desktop Services) est une licence qui autorise un utilisateur ou un appareil à se connecter légalement à un serveur Remote Desktop Services. Elle est obligatoire pour chaque connexion à distance afin de respecter les règles de licence Microsoft.

Pour ce faire toujours sur le serveur broker nous allons aller dans le gestionnaire de serveur et sur service de bureau à distance que nous avons installé précédemment et enfin sur gestionnaire de licence:

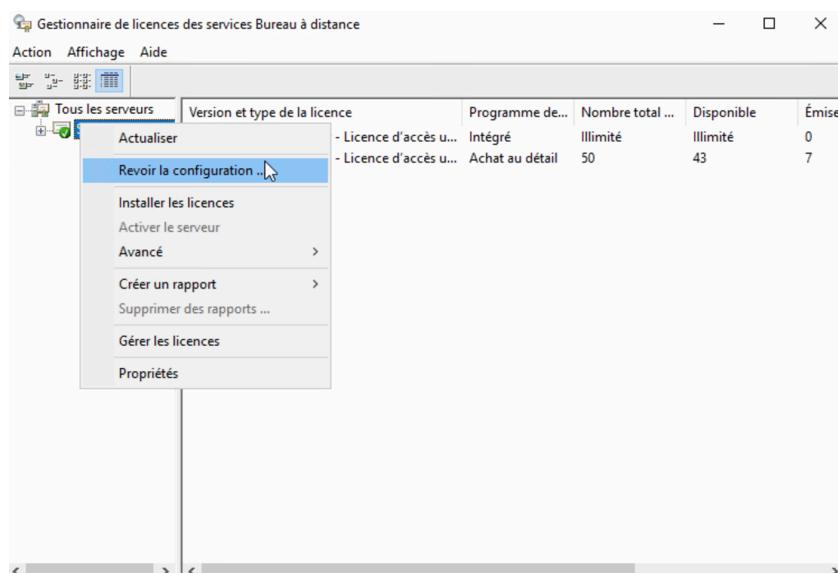


De là, nous pouvons installer le gestionnaire de licence sur le serveur broker.



Après avoir redémarré le serveur nous pouvons installer un CAL RDS.

Pour se faire nous allons aller dans la recherche windows et ouvrir l'application "Gestionnaire des licences de bureau à distance"

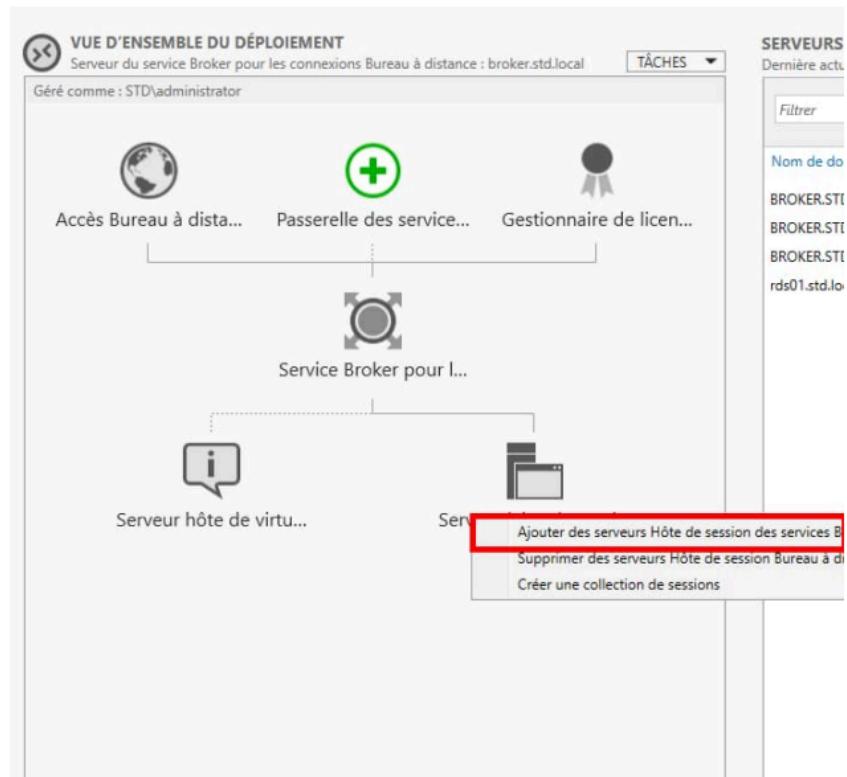


A noter que la CAL est achetée à l'avance et installable en allant sur "installer les licences".

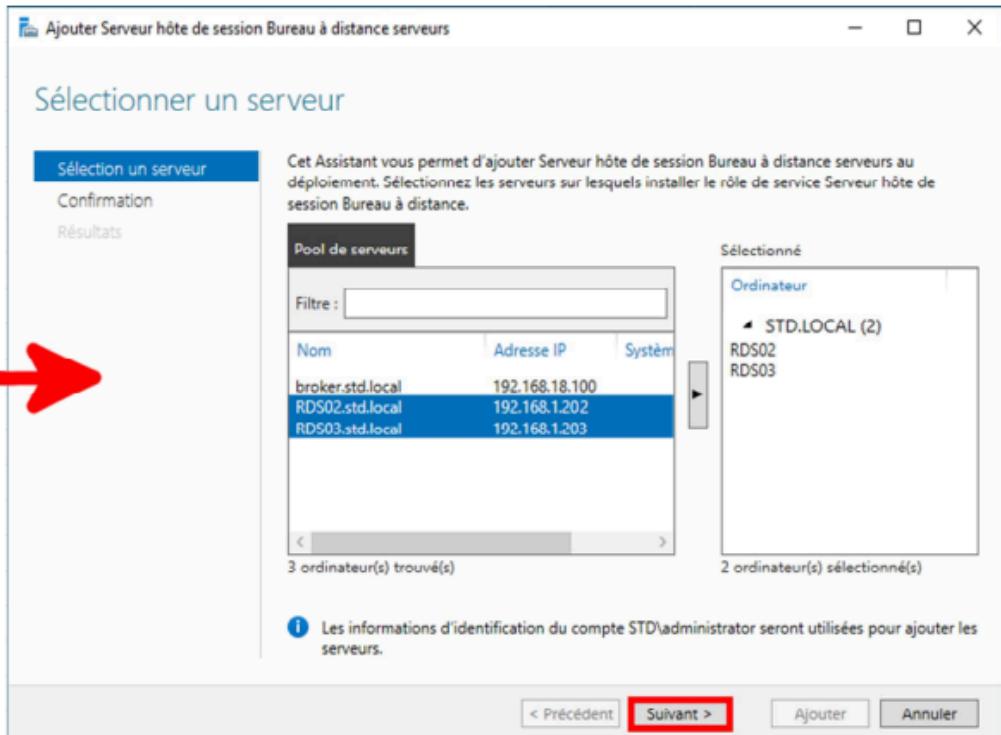
5.2.2 Ajout des serveurs Hôtes de sessions

Nous allons maintenant pouvoir ajouter les serveurs hôtes de sessions, ce qui veut dire que nous allons donner l'instruction au broker dans quels serveurs il doit répartir les utilisateurs.

Pour cela toujours sur le serveur broker nous allons aller dans "serveur hôte de session".



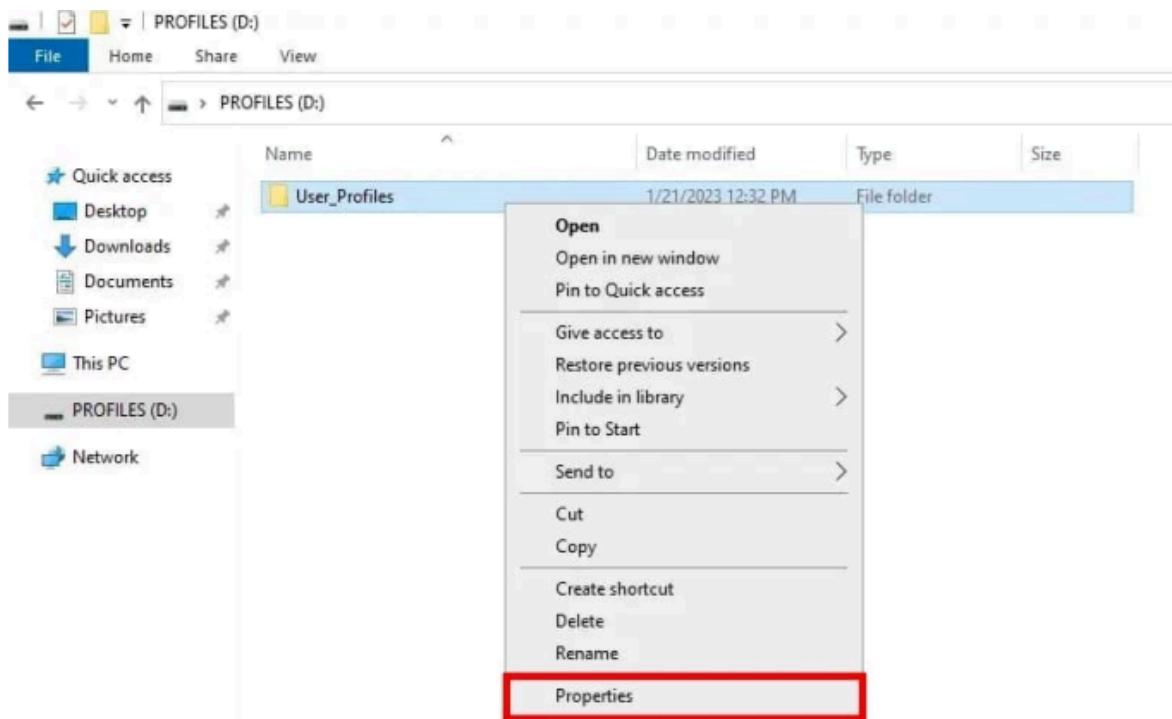
Nous allons maintenant choisir nos deux serveurs RDS présents dans le pool que nous avons créé précédemment.



5.2.3 Mettre en place le partage des dossiers utilisateurs

Toujours sur le serveur broker nous allons mettre en place les dossiers de profile car oui si les utilisateurs se connectent sur deux serveurs différents ils leurs faut récupérer leurs environnement de bureau ainsi que leurs travail.

Pour cela nous allons créer un dossier partagé sur le serveur broker qui servira de "C:\users"



Nous créons donc un dossier "User_Profiles" que nous allons partager sur le réseau.

A screenshot of the 'Sharing and Security' dialog box for the 'User_Profiles' folder. At the top, it says 'Choose people on your network to share with' and 'Type a name and then click Add, or click the arrow to find someone.' A red arrow points to the 'Name' column in the table below. The table lists two entries: 'Administrator' with 'Read/Write' permission and 'Owner' status, and 'Administrators' with 'Owner' status. At the bottom, there is a link 'I'm having trouble sharing' and a 'Share' button which is also highlighted with a red box, along with a 'Cancel' button.

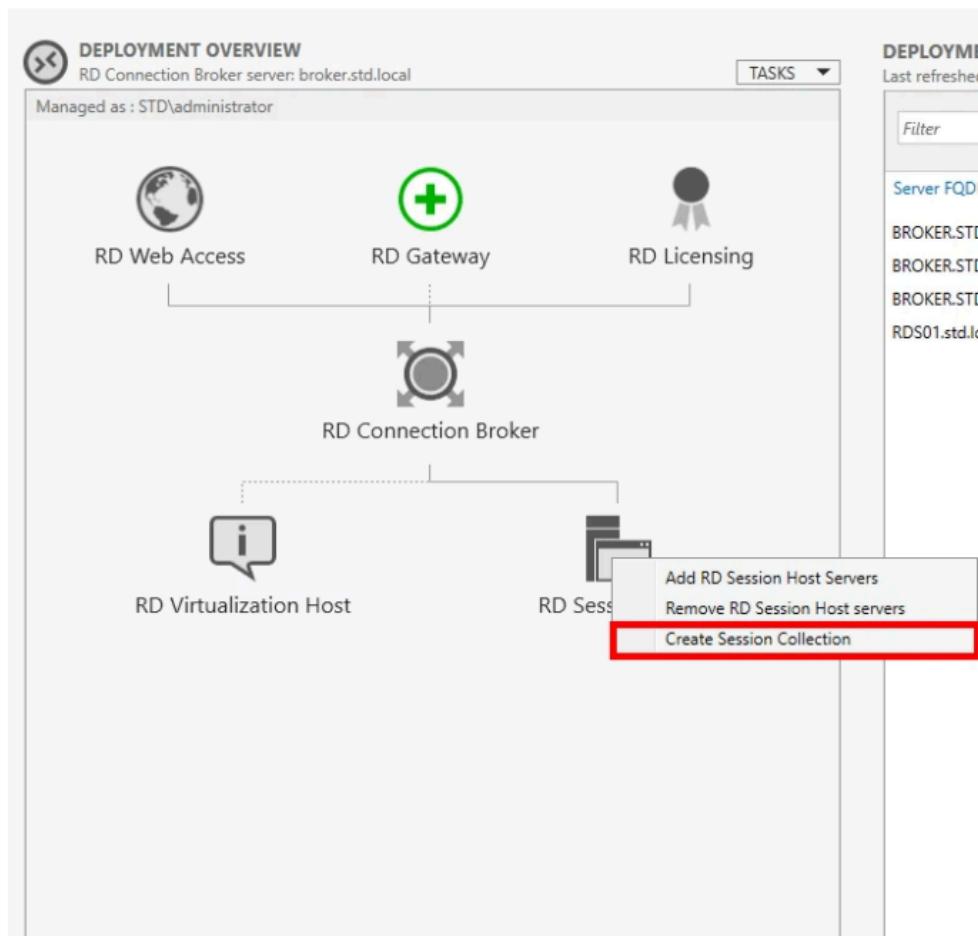
Notons que le dossier racine ne sera accessible que par les utilisateurs ayant le rôle administrateur.

5.2.4 ajout d'une collection

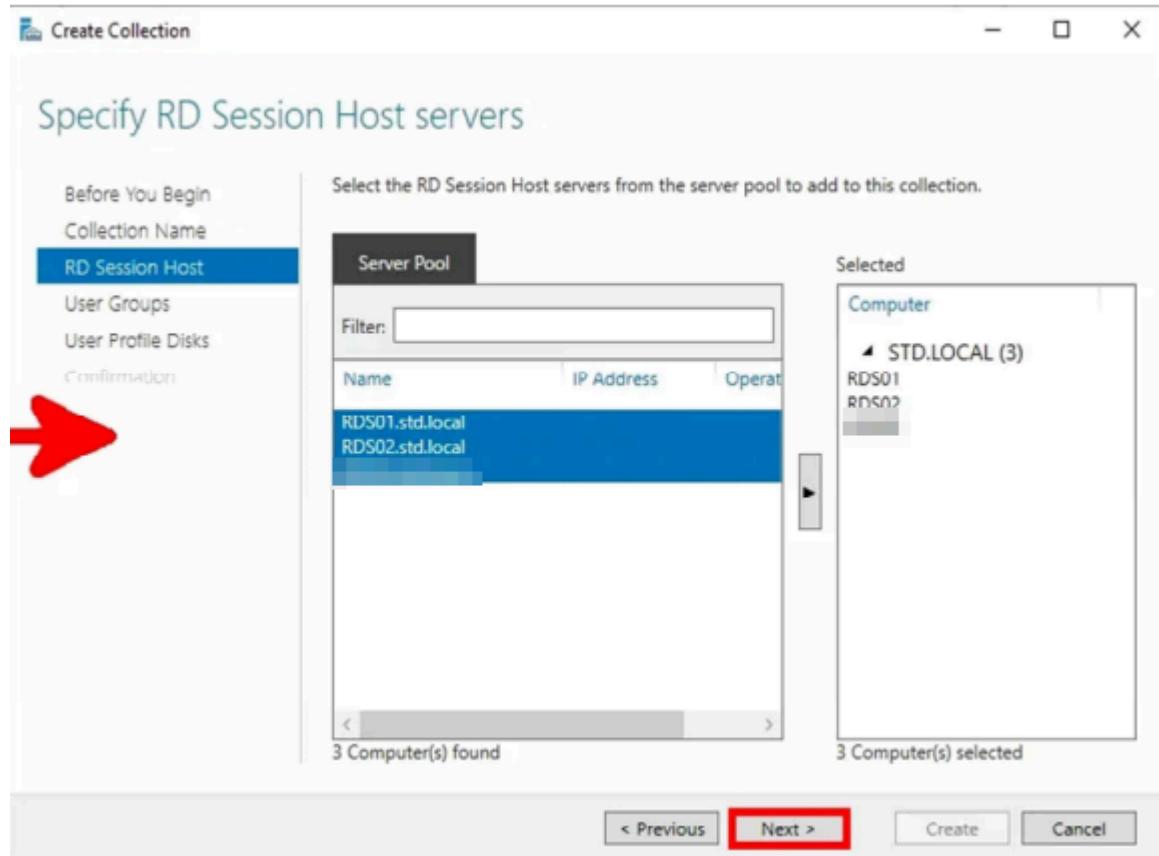
Il nous faut maintenant pouvoir lier ce dossier au dossier utilisateur de la ferme.

Pour ce faire nous allons créer une collection, son rôle est de pouvoir faire en sorte que le dossier que nous avons créé puisse être reconnu par la ferme en tant que dossier profile.

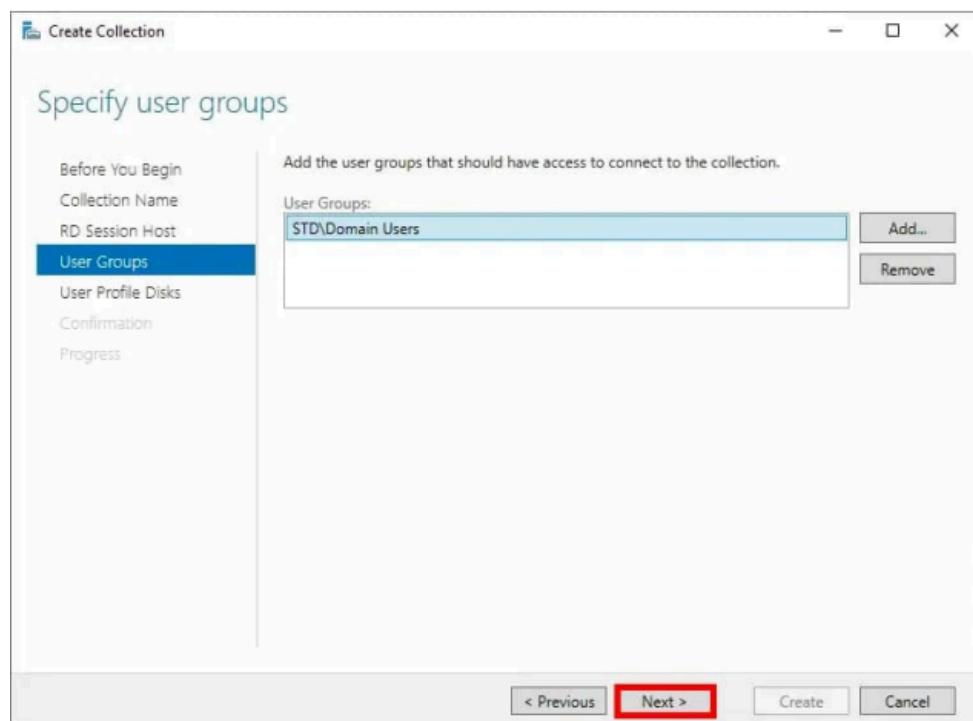
Nous allons donc, toujours sur le serveur broker, sur le rôle bureau à distance et "create session collection".



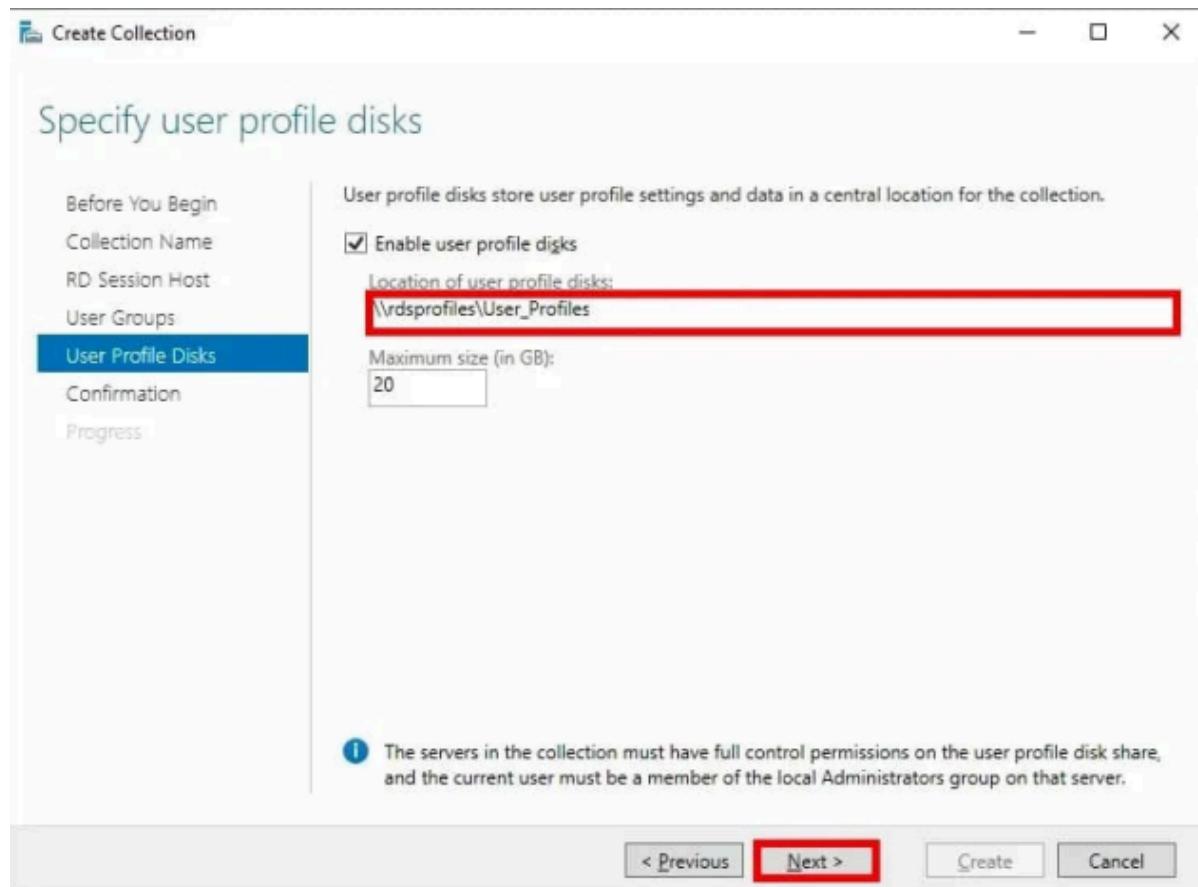
Nous ajoutons donc nos serveurs RDS en tant que host de ces dossiers:



Nous sélectionnons les utilisateurs, ici les utilisateurs du domaine:



Et enfin nous donnons le chemin réseau du dossier partagé que nous avons créé:



A noter que la taille maximale du disque profile peut être changé et ne demande qu'une simple manipulation.

Pour l'exemple, nous avons mis 20go.

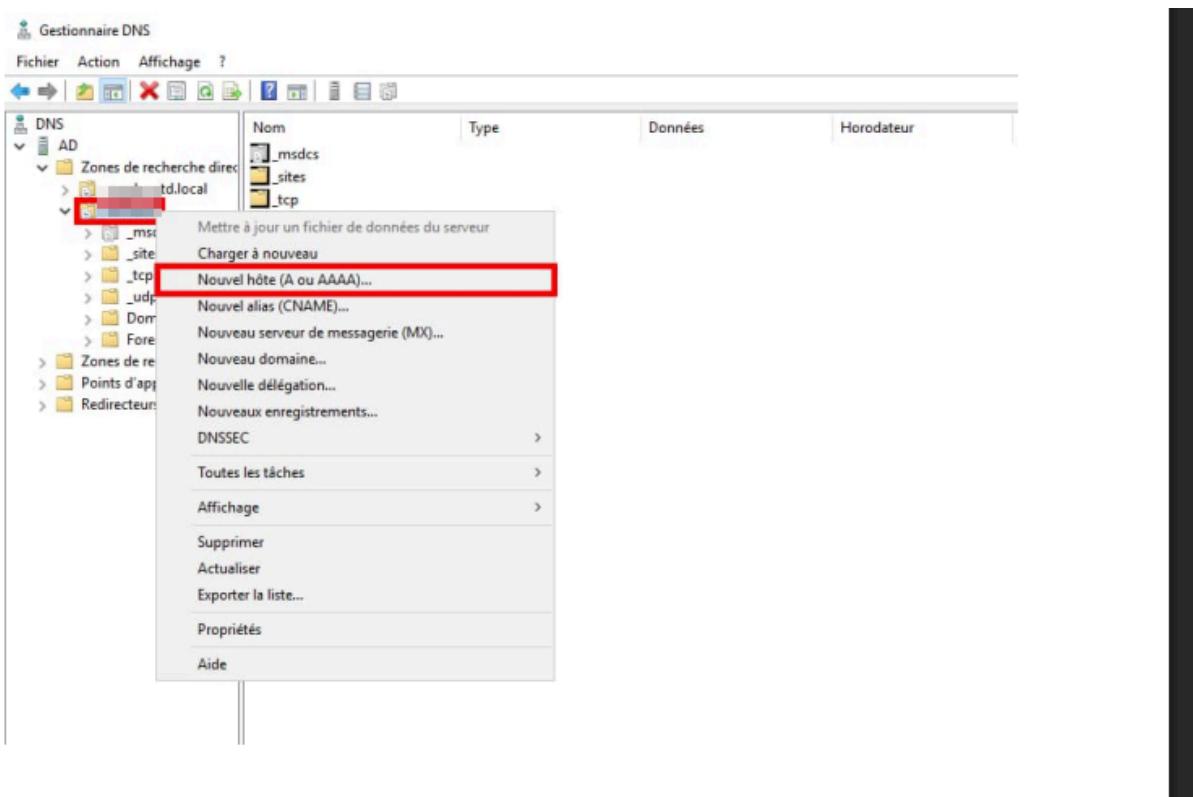
Après avoir fait cela chaque utilisateurs aura son dossier profile qui devrait apparaître en tant que disque "User_Profiles"

5.3 Client RDS

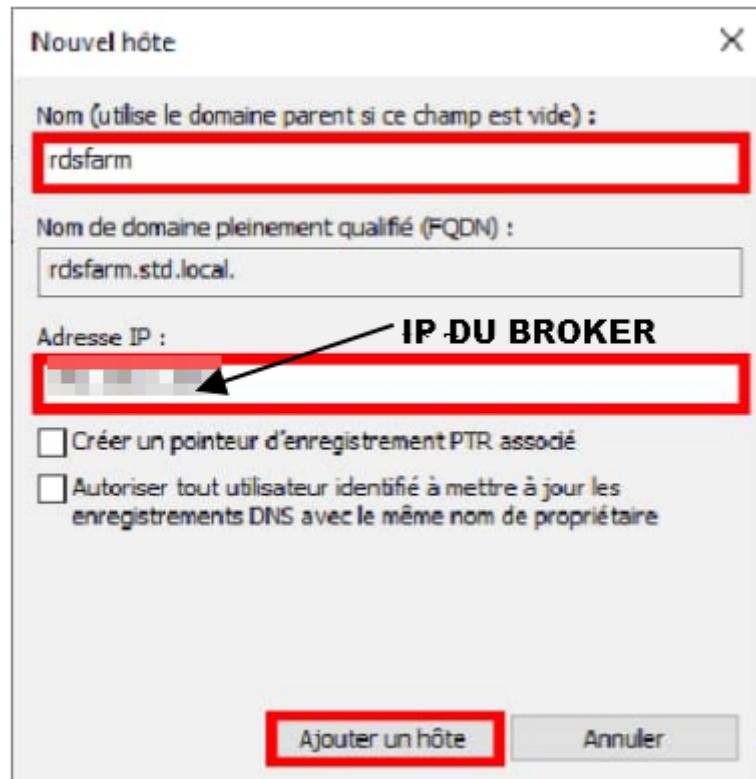
5.3.1 Configuration des entrées DNS

Maintenant nous devons mettre en place des entrées DNS pour que les utilisateurs puissent se connecter aux serveurs en passant par le nom de domaine.

Pour ce faire nous allons aller dans le gestionnaire DNS, sur le serveur AD et créer un nouvel hôte dans le domaine local.



Nous allons maintenant associer le nom de domaine du broker avec son ip:



6. TESTS

Nous allons maintenant tester la ferme RDS, pour ceci nous allons créer un utilisateur classique sans droits administrateur.

Nous mettons donc l'entrée DNS du broker que nous avons créé précédemment:

Ici l'utilisateur créé est : r.marsh

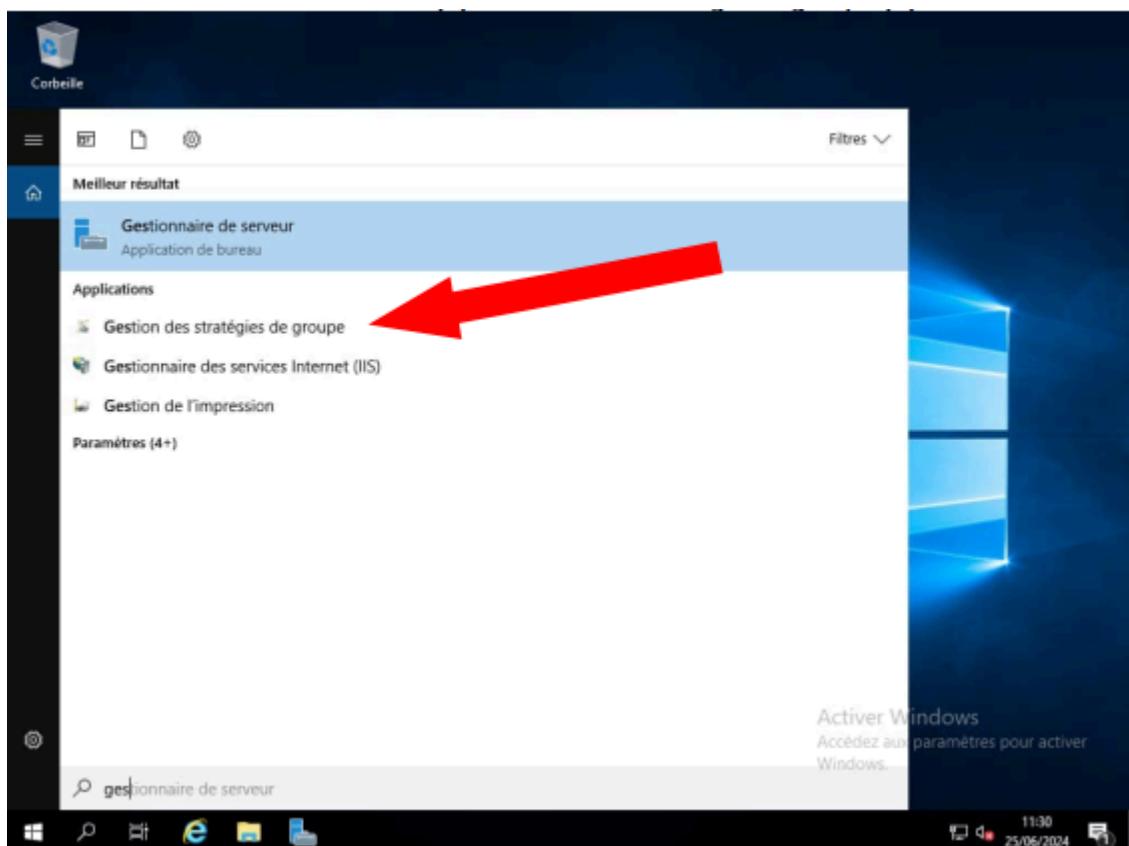


7. Mise en place GPO

Maintenant que notre ferme fonctionne, nous pouvons maintenant l'administrer.

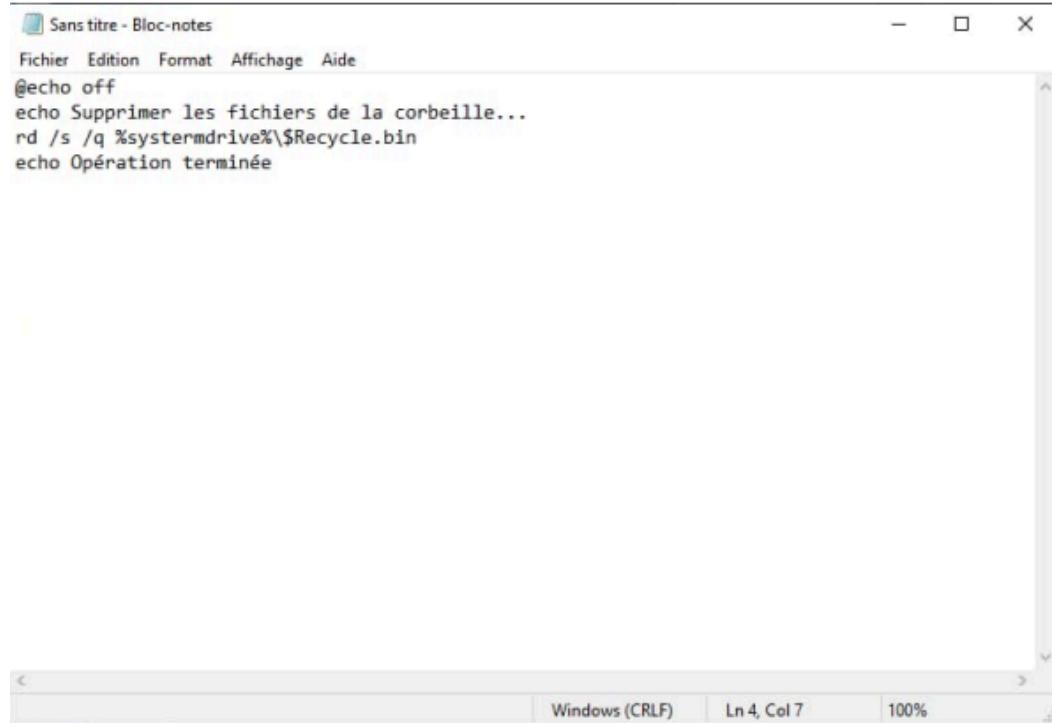
Nous allons donc dans un premier temps mettre en place une GPO qui est un ensemble de règles dans un environnement Windows permettant de contrôler la configuration des utilisateurs et des ordinateurs d'un domaine. Il est utilisé pour appliquer automatiquement des paramètres de sécurité, de réseau ou logiciels via Active Directory.

Pour ce faire nous allons aller dans le gestionnaire des stratégies de groupe:



Nous allons en créer une qui nous servira à faire un vidage entier de la corbeille à chaque déconnexion de chaque utilisateur.

Pour ce faire nous créons un fichier .bat via le bloc note et nous allons y entrer le script suivant :



```
Sans titre - Bloc-notes
Fichier Edition Format Affichage Aide
@echo off
echo Supprimer les fichiers de la corbeille...
rd /s /q %systemdrive%\$Recycle.bin
echo Opération terminée
```

The screenshot shows a Windows Notepad window titled "Sans titre - Bloc-notes". The menu bar includes "Fichier", "Edition", "Format", "Affichage", and "Aide". The main text area contains a batch script. The script starts with "@echo off", followed by "echo Supprimer les fichiers de la corbeille...", then "rd /s /q %systemdrive%\\$Recycle.bin", and finally "echo Opération terminée". The status bar at the bottom indicates "Windows (CRLF)", "Ln 4, Col 7", and "100%".

Ceci n'est qu'un exemple de GPO dites "classique" que nous pouvons appliquer à un domaine.

Mais nous pouvons en créer beaucoup d'autres comme un GPO qui déconnectera les utilisateurs inactifs depuis un certain temps.

Voici une liste des GPO que nous avons créé et que nous avons attribué à notre domaine:

The screenshot shows the Windows Group Policy Management console window. The left pane displays the navigation tree under 'Forêt : Ferme_TSE.OSI'. The 'Domaines' node is expanded, showing the 'Ferme_TSE.OSI' domain with its sub-objects: Default Domain Policy, GPO_LIMITATION_CONNEXION, GPO_MESSAGE_BIENVENUE, GPO_VIDAGE_AUTO_TEMP, GPO_VIDAGE_COREILLE, Domain Controllers, OU_FERME, Objets de stratégie de groupe, Filtres WMI, and Objets GPO Starter. Below these are 'Sites', 'Modélisation de stratégie de groupe', and 'Résultats de stratégie de groupe'. The right pane is titled 'Objets de stratégie de groupe dans Ferme_TSE.OSI' and contains a table listing 12 Group Policies. The table columns are 'Nom', 'État GPO', 'Filtre WMI', 'Modifié le', and 'Propriétaire'. The table data is as follows:

Nom	État GPO	Filtre WMI	Modifié le	Propriétaire
Default Domain Control...	Activé	Aucun(e)	12/06/2024 13:3...	Admins du domaine (...)
Default Domain Policy	Activé	Aucun(e)	12/06/2024 10:2...	Admins du domaine (...)
GPO_7-ZIP	Activé	Aucun(e)	20/06/2024 15:5...	Admins du domaine (...)
GPO_CCleaner	Activé	Aucun(e)	20/06/2024 10:3...	Admins du domaine (...)
GPO_CHROME	Activé	Aucun(e)	21/06/2024 14:5...	Admins du domaine (...)
GPO_LIMITATION_C...	Activé	Aucun(e)	19/06/2024 09:4...	Admins du domaine (...)
GPO_MESSAGE_BIE...	Activé	Aucun(e)	20/06/2024 09:4...	Admins du domaine (...)
GPO_Vidag_Corbelle...	Activé	Aucun(e)	25/06/2024 12:1...	Admins du domaine (...)
GPO_VIDAGE_AUTO...	Activé	Aucun(e)	20/06/2024 09:4...	Admins du domaine (...)
GPO_VIDAGE_COREI...	Activé	Aucun(e)	20/06/2024 09:4...	Admins du domaine (...)
GPO_WALLPAPER	Activé	Aucun(e)	19/06/2024 17:0...	Admins du domaine (...)
GPO_WALLPAPER_D...	Activé	Aucun(e)	19/06/2024 17:0...	Admins du domaine (...)

In the bottom right corner of the main pane, there is a 'Activer Windows' button with the sub-instruction: 'Accédez aux paramètres pour activer Windows.'

At the bottom of the window, a status bar indicates '12 objet(s) de stratégie d'.

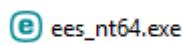
8. Mise en place antivirus

8.1 Installation de l'application

A Optimalsi pour sécuriser tous nos utilisateurs nous utilisons ESET ESET qui est un antivirus léger et rapide qui protège contre les virus, malwares, ransomwares et autres menaces. Il analyse en temps réel et met à jour régulièrement sa base de données pour bloquer les attaques.

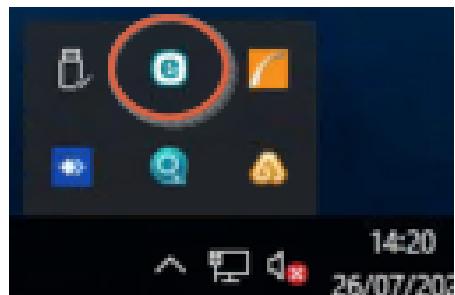
Nous allons donc l'installer sur nos VMs.

Pour ce faire nous prenons le fichier .exe d'installation:



Nous installons donc l'antivirus sur toutes les machines en y mettant la licence commandée avec l'installation.

Nous redémarrons le VMs pour chaque installation et nous vérifions que toutes aient bien ESET d'installés:



Nous lançons également un premier scan afin de sécuriser le tout.

8.2 Vérification liaison avec console ESET

Maintenant que nous avons installé l'antivirus nous devons nous assurer qu'il est bien lié à la console.

Pour ce faire nous allons nous connecter à www.eset.com avec les codes administrateur.

Nous cherchons maintenant si les serveurs sont apparus

The screenshot shows the ESET Security Console interface. At the top, a green bar displays a checkmark icon and the text "Vous êtes protégé". Below this, a section titled "Statistiques de protection du système de fichiers" provides the following data:

Statistique	Valeur
Infecté :	0
Nettoyé :	0
Propre :	15 248 239
Total :	15 248 239

At the bottom of the interface, there is a summary of server details:

Version du produit	12.0.12004.0
Nom de serveur	HYPERV
Système	Windows Server 2019 Standard 64-bit (10.0.17763)
Ordinateur	Intel(R) Xeon(R) E-2236 CPU @ 3.40GHz (3408 MHz), 32358 MB RAM
Durée d'exécution du serveur	53 jours, 20 heures, 35 minutes

Nous pouvons voir que les serveurs sont remontés, voici une capture d'écran de L'HYPER V que nous avons utilisé.

La console ESET centralise la gestion de la sécurité des postes du réseau. Elle affiche en temps réel l'état de protection des appareils, les menaces détectées, l'état des mises à jour, et permet d'appliquer des politiques de

sécurité à distance. On peut y créer des tâches (analyses, redémarrages, mises à jour), surveiller les événements de sécurité, générer des rapports détaillés, et recevoir des alertes en cas d'incident.

Elle nous sert principalement pour la sécurité logiciel et voir l'activité des utilisateurs.

9. Mise en place des applications de surveillance

9.1 Installation Noip

Zabbix est une solution open source de supervision réseau et système. Elle permet de surveiller en temps réel la disponibilité, les performances et l'état des serveurs, équipements réseau, applications, etc. Zabbix collecte des données, génère des alertes en cas de problème, et fournit des tableaux de bord et rapports détaillés.

Notre ferme RDS n'étant pas sur le Cloud Nutanix pour donc connecter la ferme à notre Proxi zabbix il nous faut donc utiliser No-ip pour attribuer un nom de domaine à une adresse ip dynamique.

Pour ce faire nous allons dans un premier temps nous connecter à www.my.noip.com afin de commencer la configuration.

Nous allons dans le menu DDNS & Remote Access -> No-IP Hostnames et cliquer sur « Create Hostname »

The screenshot shows the No-IP web interface. On the left sidebar, under 'DDNS & Remote Access' (marked with a red box and number 1), there is a link 'No-IP Hostnames' (marked with a blue box and number 2). The main content area is titled 'Hostnames' and shows the path 'My No-IP > Hostnames'. A large green button labeled 'Create Hostname' (marked with a blue circle and number 3) is prominently displayed. Below it is a form field labeled 'Hostname' with a dropdown arrow.

La page suivante s'affiche, renseignons les informations demandées :

- Hostname : Le hostname doit respecter la nomenclature suivante : <id SAGE du client>-optimalsi
- Domain : Le domaine à utiliser est : « ddns.net ».
- Record Type : DNS HOST (A).
- IPV4 Address : l'adresse IP par défaut.

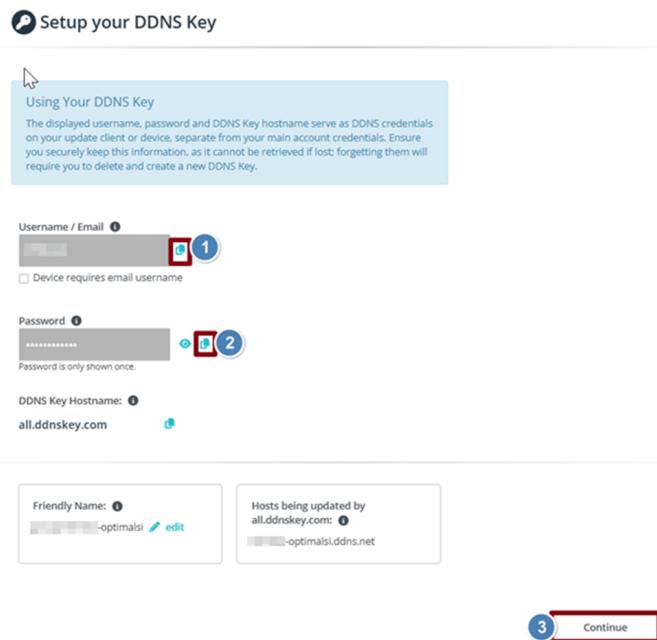
Cliquer sur « Create Hostname with DDNS Key ».

The screenshot shows the 'Create a Hostname' configuration form. At the top, there is a green button '+ Create a Hostname'. The form fields are as follows:

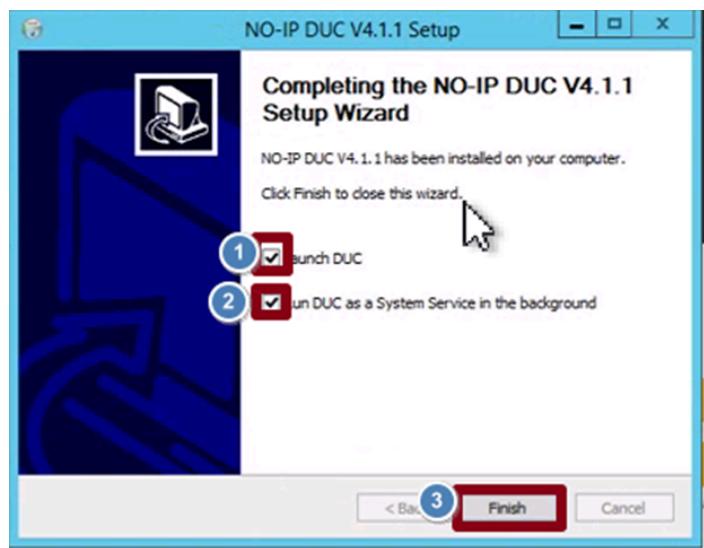
- Hostname** (1): optimalsi. A note below says: 'The name may not be greater than 49 characters.'
- Domain** (2): ddns.net. A note below says: 'Run Dynamic DNS on your own domain'
- Record Type** (3): DNS Host (A)
- IPV4 Address** (4): 192.168.1.100
- Wildcard**: Enable Wildcard
- MX Records**: + Add MX Records

At the bottom right, there are two buttons: 'Cancel' and 'Create Hostname with DDNS Key' (5), which is highlighted with a red box.

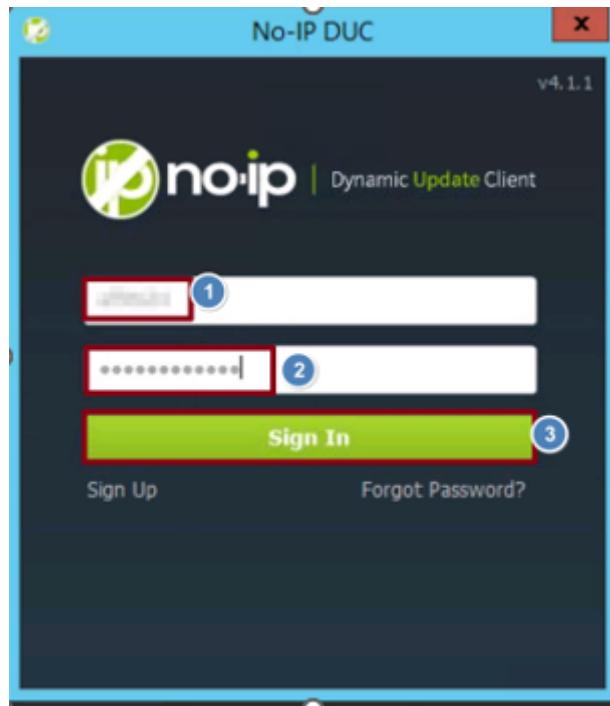
Suite à cela nous générerons la Clé DDNS qui est une authentification sécurisée utilisée pour mettre à jour automatiquement l'adresse IP dynamique avec le nom de domaine No-IP.



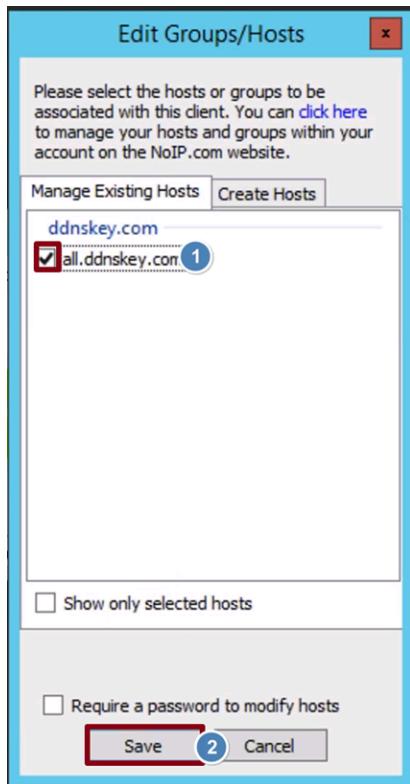
Après avoir fait cela, nous pouvons maintenant installer l'agent NoIP sur les VMs.



Une fois cela fait nous pouvons nous connecter avec la clé DDNS créée précédemment:



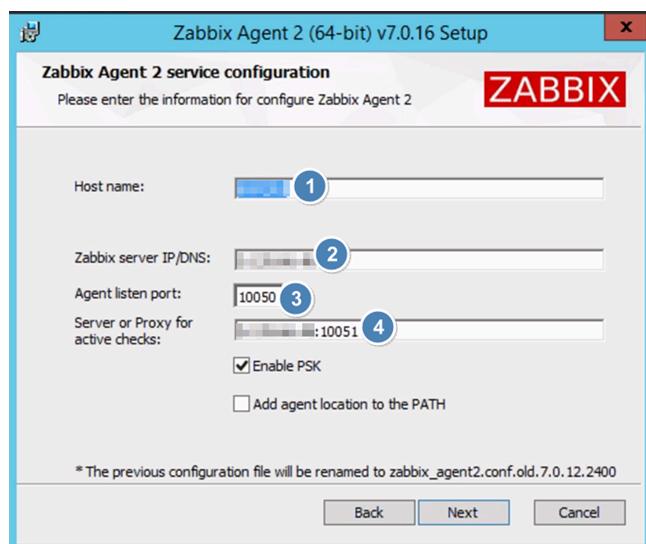
Nous pouvons nous connecter et nous pouvons voir que l'IP dynamique fonctionne correctement:



9.2 Installation ZABBIX

Maintenant nous pouvons passer à l'installation de zabbix.

Pour cela nous prenons l'application .exe que nous allons installer sur tous les serveurs.



Suite à cela il nous suffit de créer le host dans le proxy en choisissant le template que nous utilisons pour les Serveur physique one premise suite à cela zabbix et nos l'agent zabbix sont bien installé et fonctionnent correctement:

The screenshot shows the 'Host' tab selected in the Zabbix interface. The form fields are as follows:

- Host name:** Services Docker home
- Visible name:** Services Docker home
- Groups:** A dropdown menu with a search bar containing 'type here to search'. A 'Select' button is next to it.
- Interfaces:** A table with one row:

Agent	IP address	DNS name	Connect to	Port	Default
Agent	127.0.0.1	docker.home.khroners.fr	IP	DNS	10050
- Description:** An empty text area with an 'Add' link above it.
- Monitored by proxy:** A dropdown menu set to '(no proxy)'.
- Enabled:** A checked checkbox.
- Buttons:** 'Add' (blue) and 'Cancel' (white).

10. Mise en place Backups

Conformément à notre contrat de service, nous avons mis en œuvre une stratégie de sauvegarde locale automatisée sur le serveur On-Premise. Cette configuration garantit la protection des données critiques en cas de défaillance ou d'incident.

Sauvegardes locales – Serveur On-Premise :

Les sauvegardes sont effectuées automatiquement vers un NAS dédié, avec une rétention de 15 jours. Cela permet de restaurer rapidement les données en cas de perte ou de défaillance locale, tout en maintenant l'activité sans interruption.

Nous utilisons l'application Hornetsecurity pour la gestion et la supervision des sauvegardes sur les serveurs On-Premise.

Sauvegardes cloud :

Pour les environnements hébergés dans le cloud NUTANIX, nous utilisons Veeam, une solution fiable et éprouvée, permettant une sauvegarde sécurisée des machines virtuelles, avec des options avancées de restauration et de rétention selon les besoins.

10.1 Mise en place NAS

Pour mettre en place les sauvegardes locales de notre ferme RDS nous devons configurer un NAS dans lequel nous y allons stocker les données

Pour ce faire nous nous munissons un NAS QNAP TS-453S Pro



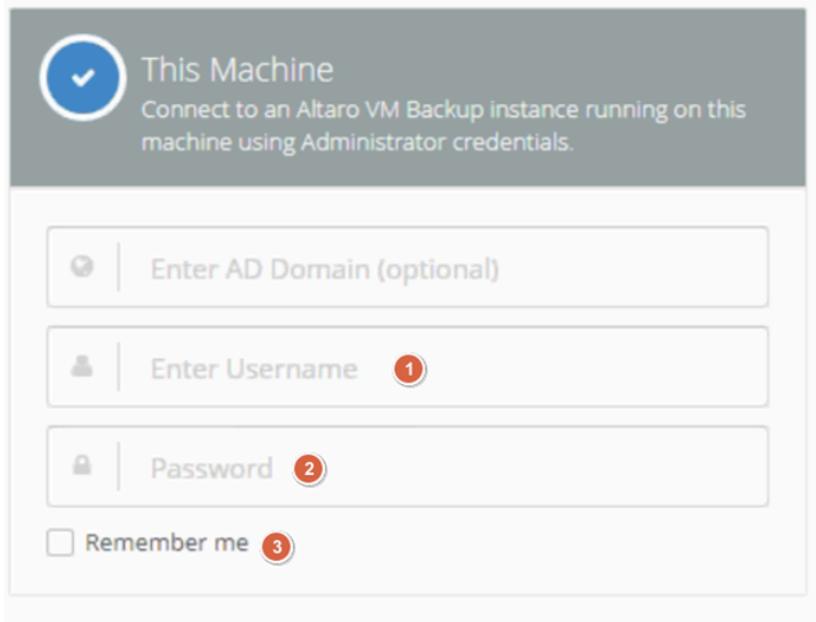
Nous commençons par le configurer et mettre en place un dossier partagé que nous allons mettre sous le nom "altaro_backup"

10.2 Configuration Hornetsecurity

Dans un premier temps nous allons installer l'application Hornetsecurity sur notre Hyper V grâce au .exe fourni

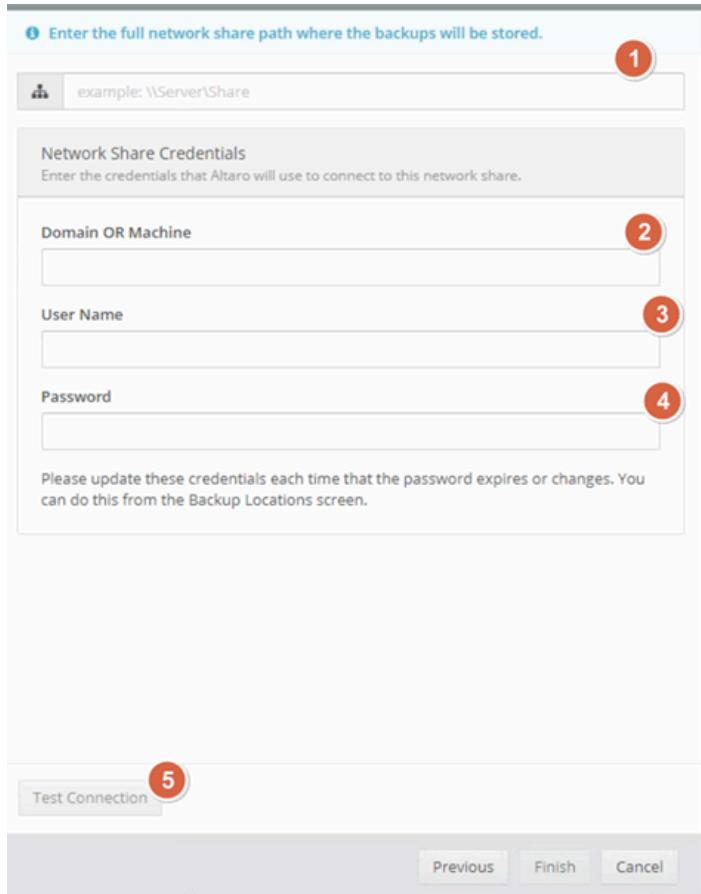


Une fois installé sur l'HYPER V nous nous connectons à l'interface grâce aux codes administrateur de l'utilisateur local de la machine



Afin de pouvoir configurer les Backups nous allons dans backup locations et nous allons ensuite ajouter le NAS que nous avons configuré plus tôt.

En cliquant sur “add backup location” nous pouvons ajouter notre NAS



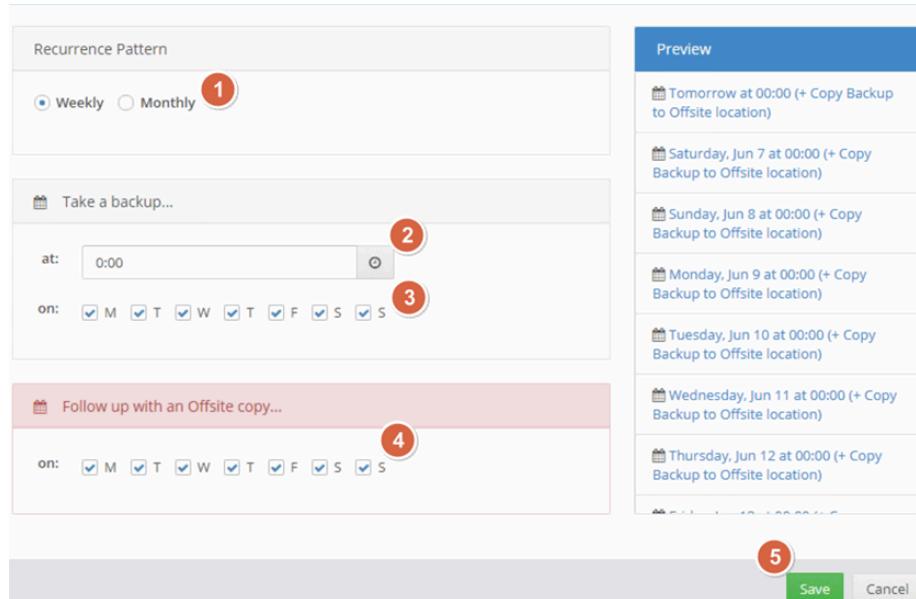
Sur cette page nous allons entrer le chemin réseau du dossier partagé que nous avons créé sur le NAS(1), nom de la machine(2) , l'utilisateur administrateur du NAS(3) et enfin son mot de passe(4).

Afin de s'assurer que la connexion est stable et le canal d'écoute est sécurisé nous cliquons sur “test connection”(5)

Une fois cela fait nous avons ajouté notre repository

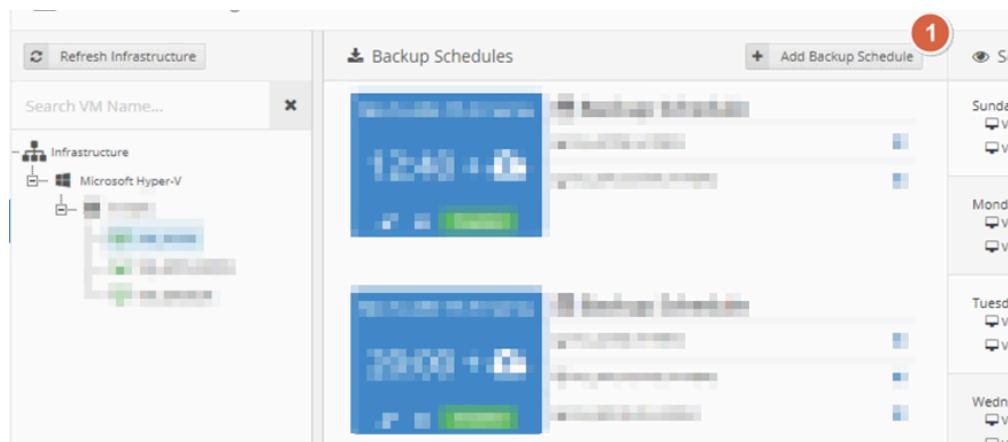
Nous pouvons maintenant mettre en place un schedule pour les sauvegardes

Pour cela nous allons aller dans “backup schedule” et créer deux événements

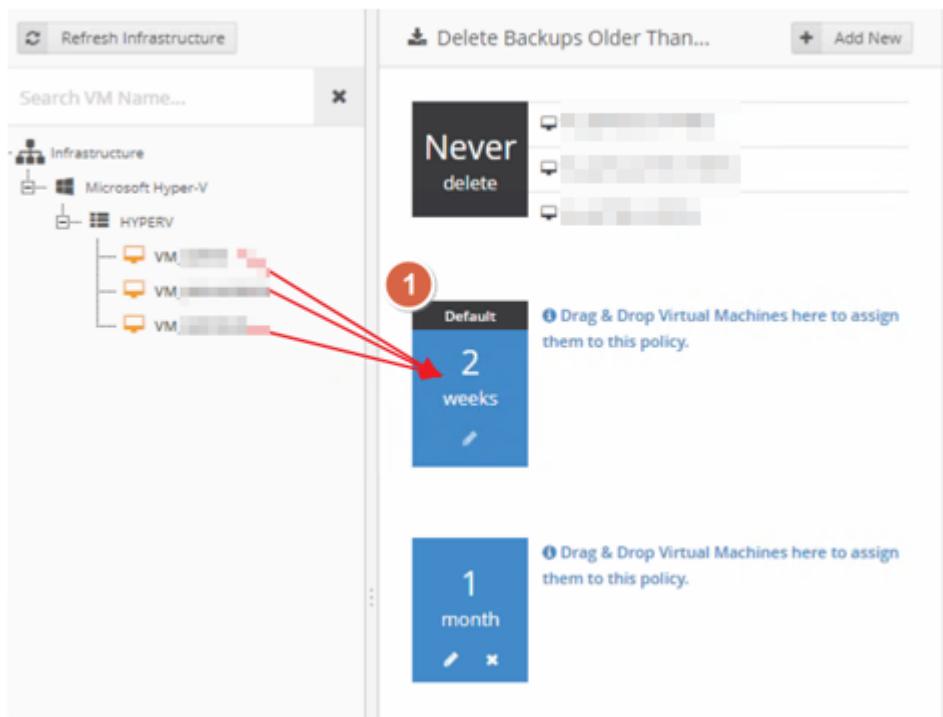


Nous allons en créer un pour 12H tous les jours et un pour 0H00 tous les jours.

Notons que le scheduler peut changer en fonction des horaires de travail des clients.



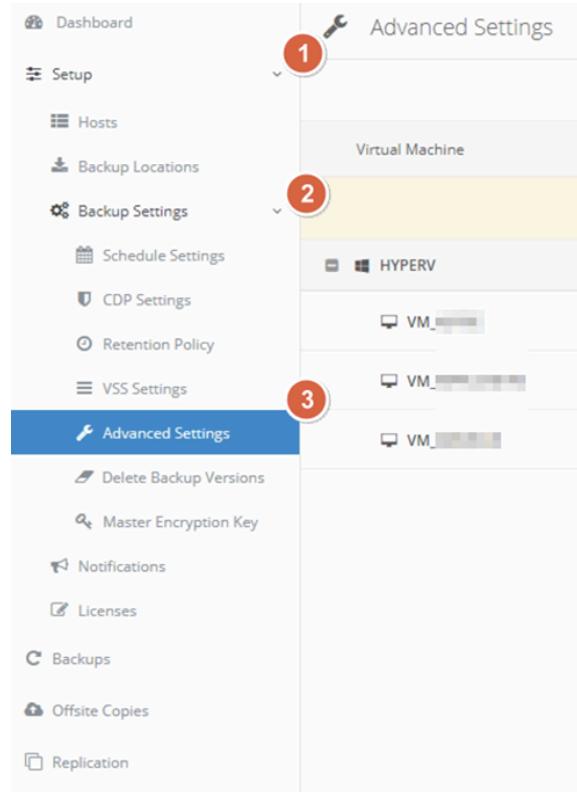
Maintenant passons à la politique de rétention, pour cela nous allons dans l'onglet “retention policy”.



et nous mettons une rétention de 2 semaines ouvrable afin d'être en raccord avec le contrat de sauvegarde.

A noter que tout comme le scheduler, la politique de rétention peut changer en fonction du client et de son contrat.

Maintenant que cela est fait il nous faut sécuriser le transfert de données pour cela nous allons dans Advanced Settings



de la nous allons mettre en place du encryption des données en cochant les cases correspondantes pour toutes les VMs:

Virtual Machine	Deduplication	Encryption	Exclude ISOs	Use CBT	Excluded Drives
HYPERV	<input checked="" type="checkbox"/>	<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
VM_ADTSE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Exclude Drives...
VM_APPLICATIFS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Exclude Drives...
VM_SERVEUR	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Exclude Drives...

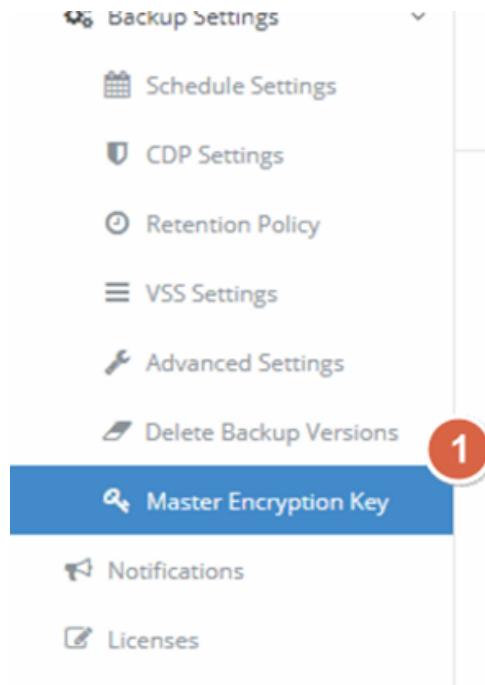
En faisant cela nous garantissons un hachage des données et faite de manière avec un chiffrement AES 256 bits en provenance de l'HYPER V.

Pour récupérer la clé de chiffrement il nous faut configurer un Master Encryption Key.

Lorsqu'une sauvegarde est lancée, Altaro chiffre les données directement sur l'hôte source, avant qu'elles ne soient transférées vers la destination (NAS). Cela garantit que les données sont protégées en transit et au repos.

Cette clé doit être configuré de la manière suivante :

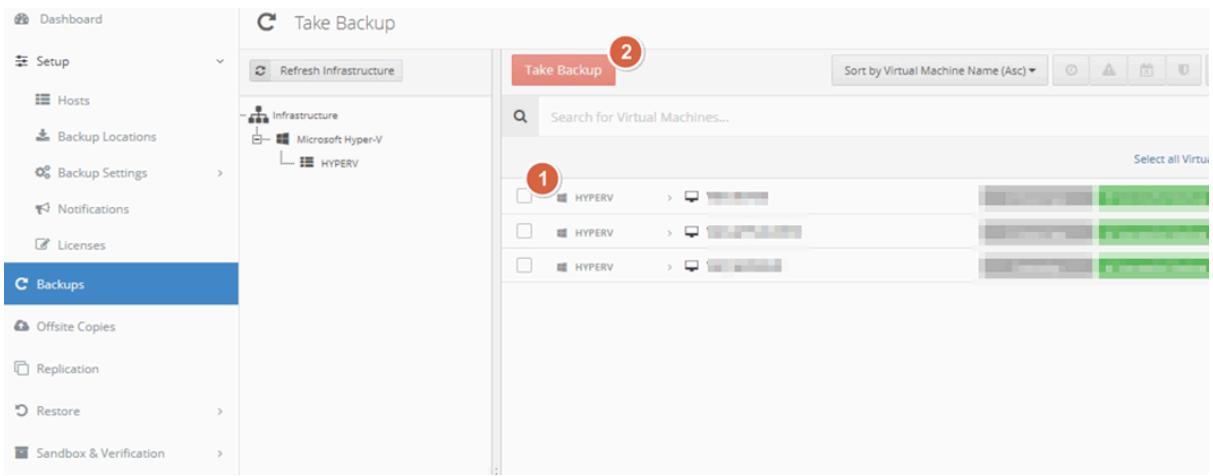
Tout d'abord nous allons dans l'onglet "Master Encryption Key"



De là, nous pouvons la configurer et la stocker précieusement.

Noter que la clé est indispensable pour la restauration, sans elle il est impossible de faire quoi que ce soit.

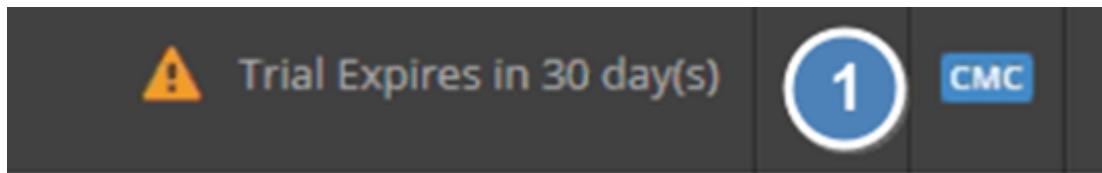
Maintenant que tout est configuré nous pouvons lancer un premier backup afin de créer les fichier de configuration en allant dans l'onglet "backups"



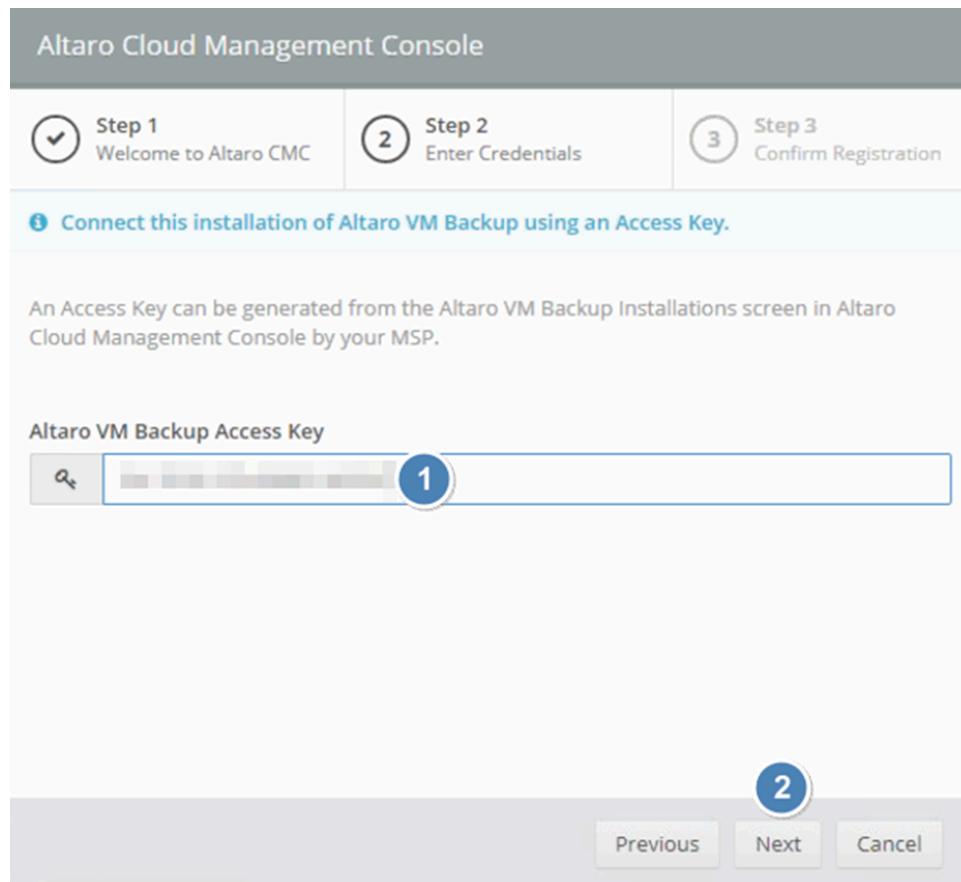
10.3 Liaison avec la console HORNET

A présent nous devons faire la liaison entre cette interface et la console HORNET centralisée afin de pouvoir avoir des informations si une sauvegarde n'a pas fonctionné.

Pour cela nous allons cliquer sur "CMC" en haut de l'interface.



A présent il nous reste qu'à entrer les codes administrateur de la console ainsi que la Master Encryption Key que nous avons configuré :



De la liaison est faite il nous faut la vérifier en nous connectant à la console

The screenshot shows a list of managed hosts in the Altaro Cloud Management Console. There are four entries, each with a green checkmark icon and a host icon. The hosts listed are: 'MD-ESXI-I05.LAB.COM' (Managed Host), 'MD-ESXI-I08.LAB.COM' (Managed Host), 'MD-ESXI-I02.LAB.COM' (Managed Host), and 'MD-ESXI-I07.LAB.COM' (Managed Host). Each entry has a blue progress bar to its right. A horizontal progress bar at the bottom indicates the process is 100% complete.

Nous pouvons voir que toutes nos VM sont bien remontées dans la console, nous avons donc fini de configurer les Backups locaux.

MISE EN PLACE FIREWALL HARDWARE

Dans le cadre d'un projet d'infrastructure pour notre nouveau client, une ferme RDS (Remote Desktop Services) a été mise en place afin de permettre un accès distant sécurisé.

Pour assurer la sécurité périphérique du réseau, un pare-feu SonicWall TZ 350 a été installé et configuré. Nous allons donc expliquer chaque étape de la mise en service, de l'ouverture de la boîte à la configuration complète du système.

1.Déballage du matériel et branchement

Voici le matériel que nous avons à disposition pour la mise en place:



Nous avons donc à disposition un Sonicwall TZ 350 NA

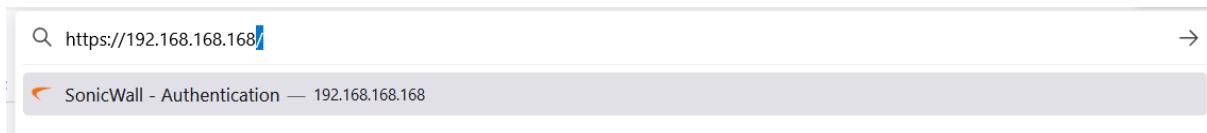
Le SonicWall TZ 350 est un pare-feu de nouvelle génération destiné aux petites entreprises et bureaux distants. Il offre une protection complète contre les menaces (malwares, intrusions, ransomware) grâce à l'inspection approfondie des paquets (DPI).

Afin de pouvoir configurer le Firewall il nous faut le brancher et prendre l'accès via l'interface web :

- X0 : vers le PC de configuration (LAN)
- X1 : vers le réseau (WAN)



Après cela nous pouvons nous connecter au sonicwall en entrant l'adresse ip : 192.168.168.168 sur un navigateur web



De la cette page apparaît :

The screenshot shows the SonicWall TZ 270W dashboard. At the top, there's a header with tabs for HOME, MONITOR, DEVICE, NETWORK, OBJECT, and POLICY. Below the header, there are sections for Device, Summary, Network, Threat, Front, Back, Storage, and a Refresh button. The main area features a large SONICWALL logo and a 270W model identifier. It includes a network interface status bar with icons for U0, SS, W0, X0-X7, and U0. Below this are four main panels: GENERAL (with fields like Name, Friendly Name, Product Code, Serial Number, Authentication Code, Firmware Version, ROM Version, System Time, Up Time, Primary WAN, and Connections), SYSTEM STATUS (with graphs for Management Plane and Data Plane), SYSTEM USAGE (showing 137.64 Kbps Bandwidth and 43 Active Connections), and NETWORK INTERFACES (listing various ports with their status and IP addresses). Red circles numbered 1 and 2 highlight specific fields in the GENERAL and AUTHENTICATION sections respectively.

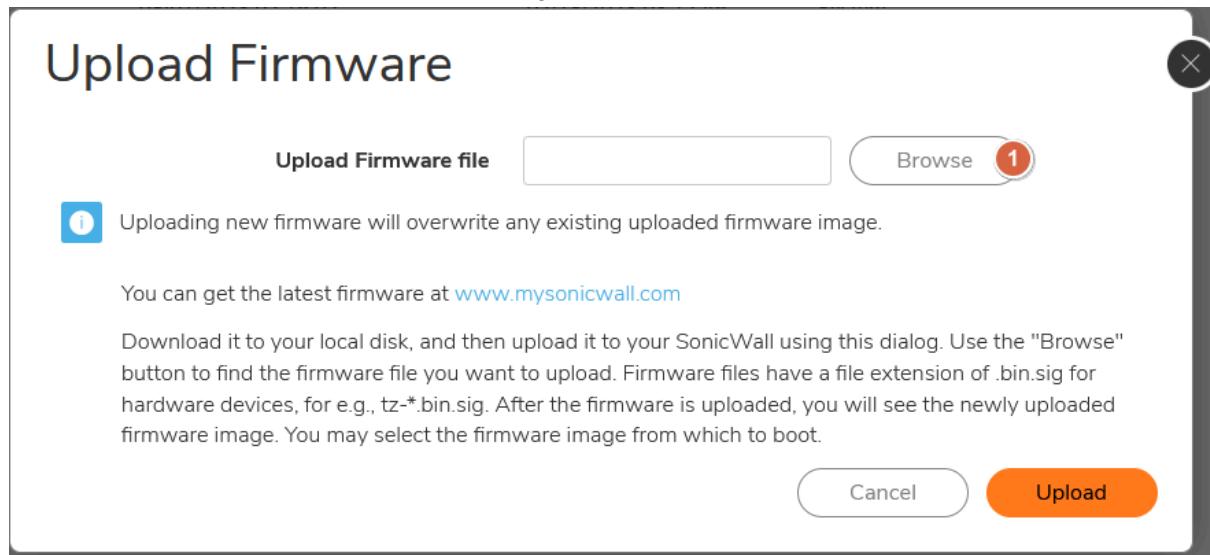
2. Mise à jour firmware + sauvegarde firmware local et cloud

Il nous faut maintenant mettre à jour le firmware de la machine car sans cela nous sommes à la merci des attaques.

Pour cela nous allons télécharger le fichier de mise à jour sur le site officiel de sonicwall auquel nous pouvons accéder grâce au compte administrateur.

The screenshot shows a software update page for a SonicWall device. At the top, there are tabs for Informations sur le produit, Licences, Firmware, and Sauvegardes cloud. The Firmware tab is active, showing a warning icon and the message "Version mise à jour disponible". It lists the current version (7.0.1-5095) and the latest version (7.0.1-5145). The Sauvegardes cloud tab shows the cycle of life for the firmware. Below these tabs, there's a section for Téléchargements disponibles with a link to "sw_tz_270w_eng.7.0.1-5145-R5175.bin.sig". This file was published on Oct 16, 2023, and has a size of 223.89 MB. A red circle with the number 1 is placed over the download link.

Suite à cela nous allons mettre à jour le sonicwall :



Après un redémarrage, le firewall est à jour.

A noter qu' une mise à jour est disponible toutes les deux semaines, il nous faut donc assurer une surveillance de toutes nos Sonicwall.

Maintenant nous allons sauvegarder ce firmware en local et sur le cloud pour garantir une restauration rapide en cas de défaillance ou de mauvaise mise à jour, tout en assurant une protection contre les pertes de données dues à des incidents physiques ou techniques.

Pour cela nous allons dans l'onglet "create Backup" et nous activons le backup local et Cloud

The screenshot shows the 'Create Backup' interface. At the top, there are tabs for 'Firmware & Local Backups' (which is selected), 'Cloud Backups', and 'Settings'. Below the tabs are three rows of backup information:

#	FIRMWARE VERSION	CONFIGURATION BACKUP DATE	FIRMWARE LOAD DATE	USERNAME	COMMENTS	BACkUP TYPE	ACTIONS
1	Current Firmware Version ✓ SonicOS 7.0.0-R906	05/26/2023 05:51:42	01/31/2023 16:20:27	System	This is the current firmware.		
2	Backup created with version SonicOS 7.0.0-R906 (1 Configuration Files available)			admin	This is a backup on Local Storage.		
	sonicwall-20201201083915-20220303080650	03/03/2022 09:06:50		admin			

At the top right, there are buttons for 'Create Backup', 'Import/Export Configuration', and 'Upload Firmware'.

3.Configuration réseau

Maintenant il nous faut configurer le X0, pour cela nous allons dans l'interface réseau et nous configurons l'adresse ip ainsi que le masque de sous-réseau avec une plage qui n'est pas celle du routeur du client.

Exemple :

- ip du routeur : 192.168.0.1
- ip du sonicwall : 192.168.1.254

General Advanced

INTERFACE 'X0' SETTINGS

Zone: LAN

Mode / IP Assignment: Static IP Mode

IP Address: 192.168.1.254 (1)

Subnet Mask: 255.255.255.0 (2)

Default Gateway (Optional): 0.0.0.0

Comment:

Domain Name:

Add rule to enable redirect from HTTP to HTTPS:

MANAGEMENT

HTTPS: (3)

Ping:

SNMP:

SSH:

USER LOGIN

HTTP:

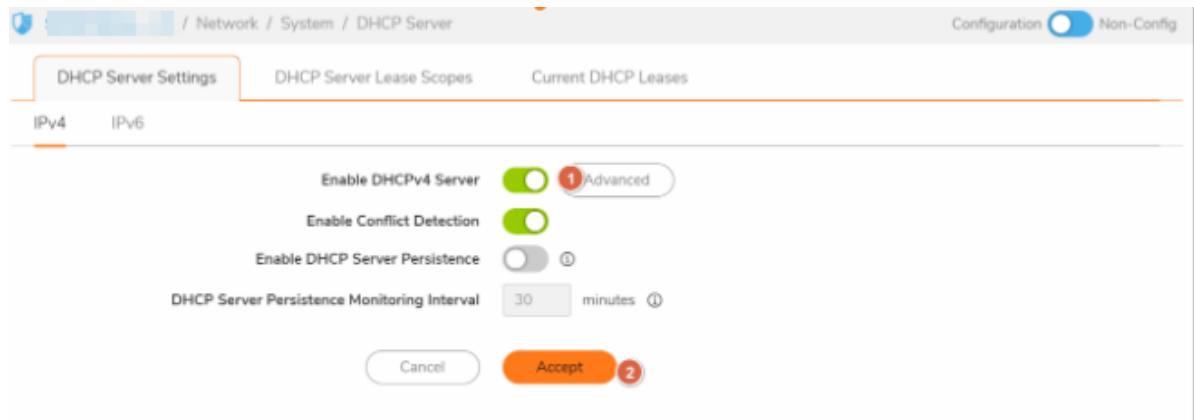
HTTPS:

Cancel OK (4)

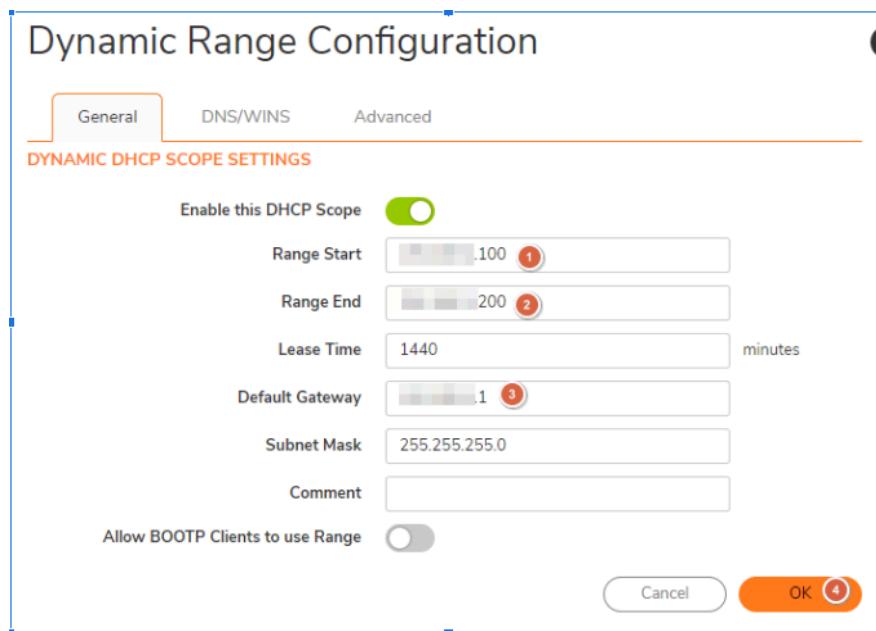
A noter que le WAN prendra le réseau du routeur il n'est donc pas nécessaire de la configurer.

Maintenant que notre plage IP est bien annoncée nous pouvons configurer le DHCP.

Pour cela nous allons activer le "DHCPv4 server" dans les paramètres réseaux :



Il nous faut maintenant mettre en place une plage DHCP duquel les machines auront une adresse ip attribués ainsi que la Default Gateway qui est l'adresse IP du routeur du client :



Ici la plage se trouve entre 100 - 200 ce qui permet de réservé les adresses IP situées en dehors de cette plage (par exemple de 2 à 99) pour des équipements à IP fixe comme les serveurs, imprimantes ou caméras. Cela évite les conflits d'adresses et assure une meilleure organisation du réseau.

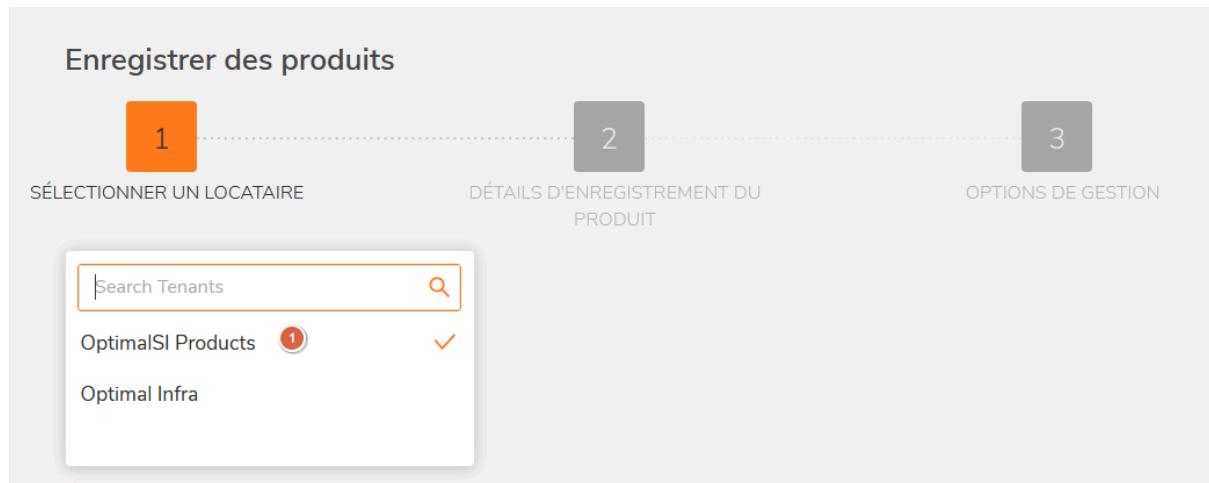
3. Mise en place des licences de sécurité

Pour lier un SonicWall TZ350 à votre compte MySonicWall, commencez par accéder à l'interface web du pare-feu via son adresse IP.

Une fois connecté, rendez-vous dans le menu "System" puis "Licensing", où vous serez invité à vous connecter avec vos identifiants MySonicWall.

Après authentification, l'appareil sera automatiquement enregistré sur votre compte, ce qui permet d'activer les services sous licence (comme les mises à jour de sécurité, l'analyse des menaces, ou le VPN) et de gérer l'appareil à distance depuis le portail MySonicWall.

MySonicWall est une plateforme en ligne sécurisée qui centralise la gestion des pare-feu et autres dispositifs SonicWall. Elle permet d'enregistrer les appareils, d'activer les licences (comme les services de sécurité et VPN) et d'accéder à des mises à jour & rapports depuis un tableau de bord unique. Grâce à MySonicWall, l'administration à distance, le suivi des abonnements et l'analyse centralisée des menaces sont simplifiés.

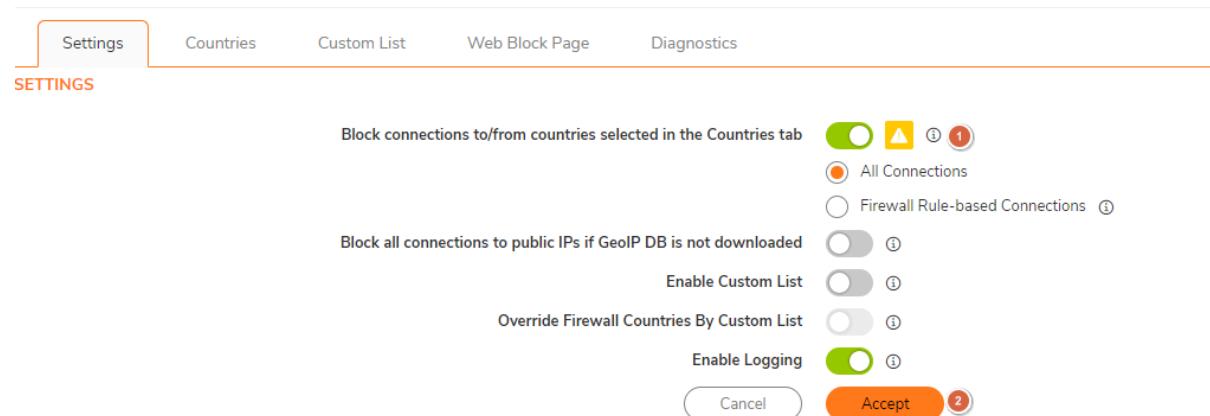


4.Configuration du Goip filter

Une fois les licences de sécurité installé nous pouvons mettre le Geo-ip filter

Le Geo-IP Filter sur un pare-feu SonicWall permet de bloquer automatiquement les connexions entrantes ou sortantes en fonction du pays d'origine ou de destination de l'adresse IP. Il peut être configuré pour bloquer tout le trafic provenant de certains pays ou seulement sur des règles précises. Une liste d'exclusion permet également d'autoriser certaines adresses IP spécifiques, même si elles viennent de pays bloqués.

Pour mettre cela en place nous allons dans les paramètres et nous activons le filtrage par pays :



Suite à cela nous allons bannir les pays que nous voulons bloquer :

The screenshot shows the SonicWall TZ350's administrative interface for managing country policies. The 'Blocked Countries' section lists China (1) and Russian Federation (2), both marked with red circles. A green toggle switch below the panels is set to 'Block all Unknown countries'. A 'Geo-IP Exclusion Object' dialog box is open, showing a dropdown menu and two buttons: 'Cancel' and 'Accept' (3).

Ici nous avons banni la Chine et la Fédération de Russie.

A noter que cette configuration est un exemple pour un client dit "classique", d'autres technologies peuvent être installé en fonction du contrat du client ainsi que sa vulnérabilité.

Le SonicWall TZ350 intègre plusieurs technologies de cybersécurité avancées pour protéger les réseaux des petites entreprises :

Il dispose d'un moteur d'inspection approfondie des paquets (DPI) capable d'analyser tout le trafic, y compris le contenu chiffré via TLS/SSL. Il intègre également un système de prévention des intrusions (IPS), un antivirus réseau, un anti-spyware, un filtrage web par catégories, ainsi qu'un système de détection et de blocage des malwares connus et inconnus grâce à la technologie Capture ATP (sandboxing dans le cloud). Enfin, il prend en charge des VPN SSL/IPSec sécurisés, la gestion des accès via des règles granulaires, et une protection contre les attaques par déni de service (DoS et DDoS).

L'ensemble est administrable via une interface centralisée ou par le portail MySonicWall.

