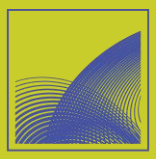


Jérémy OBJOIS

Projet StadiumCompany

2021-2023

La présente documentation a pour but de montrer la mise en place du projet scolaire StadiumCompany.

Table des matières

Section 1: Le contexte

Paragraphe 1: L'histoire de StadiumCompany

StadiumCompany est une société qui gère un grand stade.

Lors de la construction de ce stade, le réseau qui prenait en charge ses bureaux commerciaux et ses services de sécurité proposait des fonctionnalités de communication de pointe. Au fil des ans, la société a ajouté de nouveaux équipements et augmenté le nombre de connexions **sans tenir compte des objectifs** commerciaux généraux ni de la conception de l'infrastructure à long terme.

Certains projets ont été menés sans souci des conditionsde bande passante, de définition de priorités de trafic et autres, requises pour prendre en charge ce réseau critique de pointe.

À présent, la direction de StadiumCompany **veut améliorer la satisfaction des clients** en ajoutant des fonctions haute technologie et en permettant l'organisation de concerts, mais le réseau existant ne le permet pas.

La direction de StadiumCompany sait qu'elle ne dispose pas du savoir-faire voulu en matière de réseau pour prendre en charge cette mise à niveau. StadiumCompany décide donc de **faire appel à des consultants réseau** pour prendre en charge la conception, la gestion du projet et sa mise en œuvre.

Ce projet sera mis en œuvre suivant trois phases :

- **la première phase** consiste à planifier le projet et préparer la conception réseau de haut niveau
- **la deuxième phase** consiste à développer la conception réseau détaillée
- **la troisième phase** consiste àmettre en œuvre la conception

Après quelques réunions, StadiumCompany charge **NetworkingCompany**, une société locale spécialisée dans la conception de réseaux et le conseil, **de la phase 1** (la conception de haut niveau).

NetworkingCompany est une **société partenaire de Cisco Premier Partner**. Elle emploie 20 ingénieurs réseau qui disposent de diverses certifications et d'une grande expérience dans ce secteur.

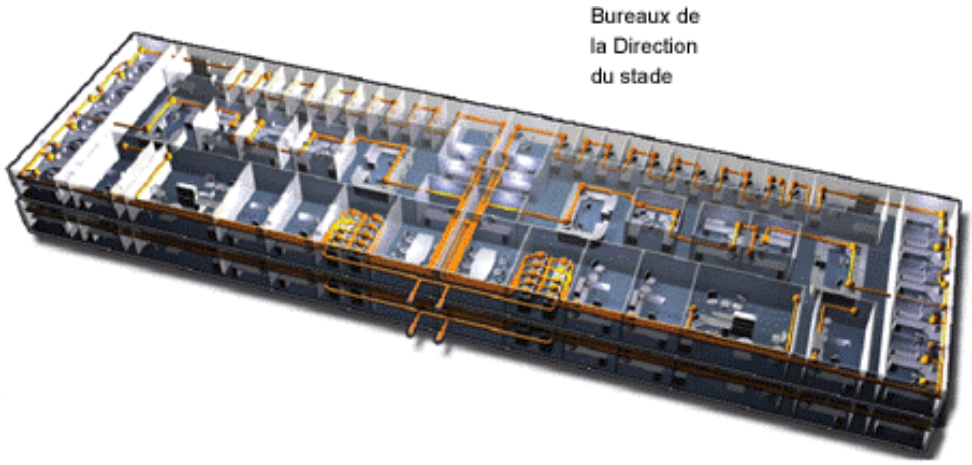
Pour créer la conception de haut niveau, NetworkingCompany a tout d'abord **interrogé le personnel du stade et décrit un profil** de l'organisation et des installations. C'est l'objet du paragraphe 2.

Paragraphe 2: L'organisation de StadiumCompany

StadiumCompany fournit l'infrastructure réseau et les installations sur le stade. StadiumCompany emploie **170 personnes** à temps plein :

- **35 dirigeants et responsables**
- **135 employés**

Environ **80 intérimaires sont embauchés** en fonction des besoins, pour des événements spéciaux dans les services installations et sécurité.



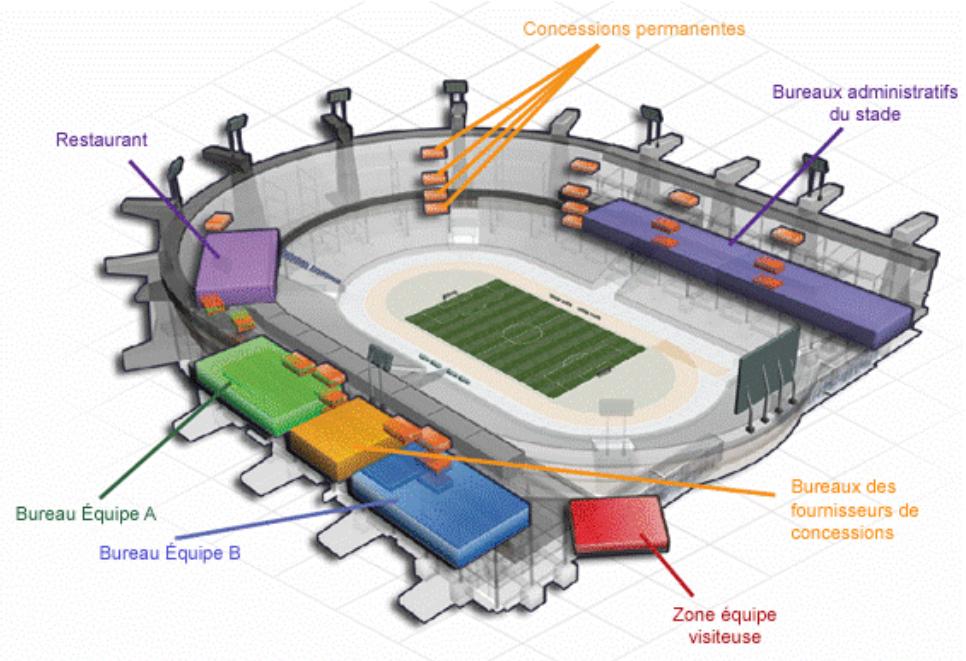
A) Les téléphones et les PCs de StadiumCompany

Tous les dirigeants et responsables de StadiumCompany utilisent des PC et des téléphones connectés à un PABX vocal numérique. À l'exception des préposés au terrain à temps plein et des gardiens, **tous les salariés** utilisent également des PC et des téléphones.

Cinquante téléphones partagés sont répartis dans le stade pour le personnel de sécurité. On compte également **12 téléphones analogiques**, certains prenant également en charge les télécopies et d'autres offrant un accès direct aux services de police et des pompiers. Le groupe sécurité dispose également de **30 caméras** de sécurité raccordées à un réseau distinct.

B) La prise en charge des installations déjà existantes

StadiumCompany propose des installations et une prise en charge de réseau pour **deux équipes de sports**(Équipe A et Équipe B), **une équipe « visiteurs »**, **un restaurant et un fournisseur de concessions**.



Le stade mesure environ 220 mètres sur 375. Il est construit sur deux niveaux.

En raison de la taille des installations, plusieurs locaux techniques connectés par **des câbles à fibre optique** sont répartis sur l'ensemble du stade.

Les vestiaires des équipes A et B et les salons des joueurs sont situés **au premier niveau** de la partie sud du stade. Les bureaux des équipes occupent une surface d'environ 15 mètres par 60 au deuxième niveau. **Le bureau et le vestiaire de l'équipe « visiteuse »** sont également situés au premier niveau.

Les bureaux de StadiumCompany se trouvent dans **la partie nord du stade**, répartis sur les deux niveaux. L'espace des bureaux occupe environ 60 mètres par 18 au premier niveau et 60 mètres par 15 au deuxième niveau.

Les équipes A et B sont engagées dans des compétitions sportives différentes, organisées à des dates différentes. Elles sont toutes les deux sous contrat avec StadiumCompany pour leurs bureaux et services au sein du stade.

1) L'organisation de l'équipe A

L'équipe A compte **90 personnes** :

- **4 dirigeants**
- **12 entraîneurs**
- **14 employés** *(y compris des médecins, kinés, secrétaires, assistants, comptables et assistantsfinanciers)*
- **60 joueurs**

L'équipe A dispose de 15 bureaux dans le stade pour ses employés non joueurs. Cinq de ces bureaux sont partagés. **24 PCs et 28 téléphones** sont installés dans les bureaux.

L'équipe A dispose également **d'un vestiaire des joueurs**, **d'un grand salon pour les joueurs** et **d'une salle d'entraînement**. Les employés non joueurs utilisent les locaux toute l'année. Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de **5 téléphones** et le salon des joueurs de **15 téléphones**. Des rumeurs indiquent que l'équipe A aurait récemment installé un concentrateur sans fil dans le salon des joueurs.

2) L'organisation de l'équipe B

L'équipe B compte **64 personnes** :

- **4 dirigeants**
- **8 entraîneurs**
- **12 employés** *(y compris des médecins, kinés, secrétaires, assistants, comptables et assistantsfinanciers)*
- **40 joueurs**

L'équipe B dispose de 12 bureaux dans le stade pour ses employés autres que les joueurs. Trois de ces bureaux sont partagés. **19 PCs et 22 téléphones** sont installés dans les bureaux.

L'équipe B dispose également **d'un vestiaire des joueurs** et **d'un grand salon pour les joueurs**. Les employés non joueurs utilisent les locaux toute l'année. Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de **5 téléphones** et le salon des joueurs de **15 téléphones**.

3) L'accueil de l'équipe « visiteuse »

L'équipe « visiteuse » dispose d'un vestiaire et **d'un salon équipés de 10 téléphones**.

Chaque équipe « visiteuse » demande des services provisoires le jour du match et quelques jours auparavant. Les équipes « visiteuses » passent également un contrat avec StadiumCompany pour les bureaux et services au sein du stade.

4) La prise en charge du fournisseur de concessions

Un fournisseur de concessions gère les services proposés lors des matchs et événements. Il compte 5 employés à temps plein. Ils occupent deux bureaux privés et deux bureaux partagés équipés de **cinq PCs et sept téléphones**. Ces bureaux se trouvent dans la partie sud du stade, entre les bureaux des équipes A et B.

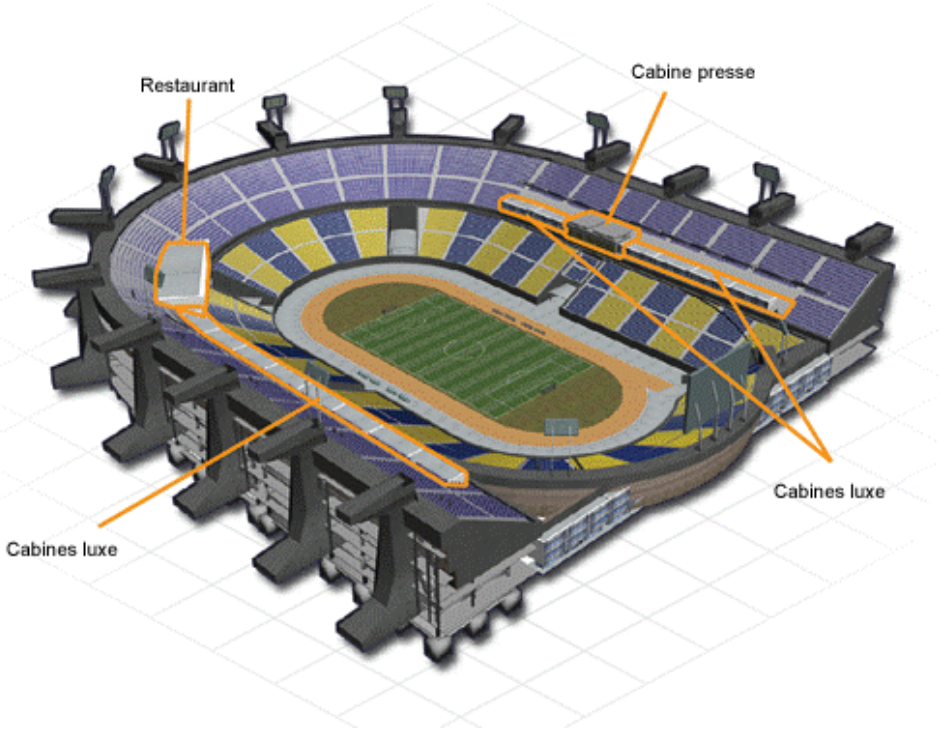
Deux employés à temps partiel prennent les commandes auprès des loges au cours des événements.

Le concessionnaire de services emploie des intérimaires saisonniers pour gérer 32 stands permanents et autres services répartis sur l'ensemble du stade. **Il n'y a actuellement aucun téléphone ni PC** dans les zones de vente.

5) L'organisation du restaurant de luxe

Le stade propose un restaurant de luxe ouvert toute l'année. En plus des salles et des cuisines, le restaurant loue des bureaux auprès de StadiumCompany. Les quatre dirigeants ont chacun un bureau privé. Les deux employés en charge des questions financières et comptables partagent un bureau.

Six PCs et téléphones sont pris en charge. **Deux téléphones** supplémentaires sont utilisés en salle pour les réservations.



6) La prise en charge des loges de luxe

Le stade compte 20 loges de luxe. StadiumCompany équipe **chaque loge d'un téléphone** permettant de passer des appels locaux et d'appeler le restaurant et le concessionnaire de services, soit **20 téléphones.**

7) L'organisation de la zone de presse

StadiumCompany propose un espace presse avec **trois zones partagées** :

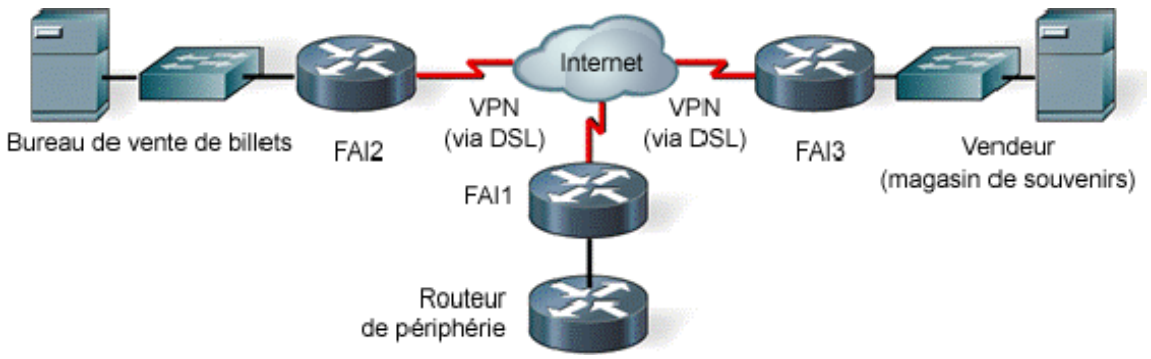
- **la zone presse écrite** accueille généralement 40 à 50 journalistes au cours d'un match. Cette zonepartagée est équipée de 10 téléphones analogiques et de deux ports de données partagés. On sait qu'un journaliste stagiaire apporte un petit point d'accès sans fil lorsqu'il couvre un match

- **la zone de presse pour les radios** peut accueillir 15 à 20 stations de radio. Elle est équipée de 10 lignes téléphoniques analogiques

- **la zone de presse télévisée** accueille généralement 10 personnes. Elle est équipée de 5 téléphones

8) La prise en charge des deux sites distants

StadiumCompany compte actuellement **deux sites distants** : **une billetterie en centre-ville** et **une boutique de souvenirs** dans une galerie marchande locale. Les sites distants sont connectés via un service DSL à un FAI local.



Le stade est connecté au FAI local à l'aide de FAI1, un routeur de services gérés qui appartient au FAI.

Les deux sites distants sont connectés au même FAI par les routeurs FAI2 et FAI3, fournis et gérés parle FAI. Cette connexion permet aux sites distants d'accéder aux bases de données situées sur les serveurs dans les bureaux de StadiumCompany.

StadiumCompany dispose également d'un routeur de périmètre, nommé Routeur de périphérie, connecté au routeur FAI1 du stade.

C) Les projets de StadiumCompany

StadiumCompany **veut ajouter à son réseau de nouveaux services**, tels que la vidéo.

La société envisage également de **remplacer le PABX vocal numérique existant**. Elle souhaiterait un meilleur accès à son réseau existant de caméras de sécurité.

Deux sites distants sont prévus dans le futur proche :

- **une société de production de films** a été engagée pour fournir des vidéos pendant et après les rencontres sportives et concerts. Elle doit se connecter au réseau du stade pour échanger des fichiers.
- **l'équipe A va ouvrir de nouveaux bureaux en dehors du stade**. Ces bureaux devront avoir accès aux mêmes ressources réseau que celles utilisées sur le réseau local du stade.

Section 2: Le cahier des charges

Cette année, vous allez intégrer la division du stade de StadiumCompagny. Vous serez **chargé de la maintenance des systèmes et réseaux informatiques**.

StadiumCompagny est composé de plusieurs sites :

- **Site 1** : **Stade** *(hébergement informatique, siège social et centre administratif)*
- **Site 2** : **Billetterie** *(vente des billets)*
- **Site 3** : **Magasin** *(vente des souvenirs)*

Les différentes solutions retenues pour l'étude du projet d'un point de vue général de StadiumCampagny pourront faire l'objet de documentations techniques en fonction de la complexité de leur mise en œuvre.

Mission 1 : Conception et prise en charge de StadiumCompany

Vous intégrez le service informatique du **centre administratif de stade**. Sur ce site sont effectuées toutes les opérations concernant la gestion du personnel et l'administration du stade.

On y trouve 7 grands services :

- **Service Administration** (170 personnes)
- **Service Équipe** (164 personnes)
- **Service WiFi** (100 personnes)
- **Service Caméra IP** (80 caméras)
- **Service VIP-Presse** (80 personnes)
- **Service Fournisseur** (44 personnes)
- **Service Restaurant** (14 personnes)

Le réseau de StadiumCompagny doit comporter **plusieurs périmètres de sécurité**:

- **l'adressage réseau et l'attribution de noms faciles à mettre à niveau** : **172.20.0.0/22**
- **un système de cloisonnement du réseau devra être testé** *(les commutateurs devront être facilement administrables afin de propager les configurations rapidement et aisément)*
- **une solution permettant l'interconnexion des différents sites** (stade, billetterie et magasin)
- **les différents commutateurs ainsi que le routeur doivent disposer de réglages de base homogènes**.
- **la solution doit se faire avec les équipements réseau CISCO**

Mission 2 : Administration et gestion des accès utilisateurs

Le StadiumCompany possède le nom de domaine StadiumCompany.com. Les principaux serveurs sont hébergés au stade au centre d'hébergement informatique. Selon les cas, certains services sont répliqués sur les sites eux-mêmes. Par exemple, les services d'annuaire Active Directory sont généralement répliqués sur le site de stade.

Le réseau de magasin et de la billetterie sont tous composés de la même manière :

- **X Postes pour les employés**

- **le site de stade dispose d'un service Active Directory, d'un service DHCP, et d'un DNS primaire** sur une machine sous Windows 2012 Server. Celle-ci permet aussi le stockage des fichiers utilisateurs. **Un serveur RSync et DNS secondaire sous Linux Debian**.

Paragraphe 1 : L'annuaire du site de stade (Active Directory)

Les utilisateurs sont authentifiés via le serveur **Active Directory du domaine stadiumcompany.com**. Il est configuré en regroupant les utilisateurs par service. Les UO suivantes sont présentes sur le serveur : Admin, WiFi…

Chaque UO contient les utilisateurs du service concerné :

- **un groupe d'utilisateurs dont le nom est au format G_xxxx où xxxx=le nom du service**

- **un groupe regroupant les utilisateurs avec pouvoir du service GP_Admin (directeurs et responsables notamment)**

- **une GPO permettant d'imposer des contraintes d'utilisation et d'habilitations sur les machines du réseau**

    - *Extrait d'une GPO : service équipes → gpo_equipes :*
    - *l'accès au panneau de configuration aux paramètres réseau est interdit*
    - *par un script de démarrage Equipesstart.bat permet la connexion des lecteurs réseau accédant aux dossiers partagés.*

- *Les utilisateurs démarrent avec un bureau imposé (barre de menu, fond d'écran...)*

Les utilisateurs ont **des logins construits** sur la base suivante - **pnom – p=première lettre du prénom et nom=nom de famille**. S'il y a homonymie, un chiffre de 1 à 10 sera ajouté.

Chaque utilisateur possède **un dossier personnel et un profil centralisé**.

Une stratégie de complexité des mots de passe est définie au niveau domaine.

Paragraphe 2 : Le serveur DNS

Les serveurs DNS sont configurés pour **résoudre la zone directe stadiumcompany**.com et la zone inverse du 172.20.0.10

Le serveur primaire est hébergé **sur une machine Windows 2012 Server** et le DNS secondaire sur une **Linux Debian**.

Paragraphe 3 : Le service DHCP

Une plage est définie sur le **172.20.0.10** avec des options de routeur renvoyant vers la passerelle/pare-feu IPCOP. Les serveurs DNS sont aussi transmis via les options DHCP.

Mission 3 : Sécurisation des communications entre sites

Une solution permettant l'administration à distance sécurisée et la sécurisation des interconnexions :

- La sécurité du système d'information devra être renforcée entre les différentssites
- Sécurisation des interconnexions entre le site du stade et les sites distants de billetterie et Magasin
- La solution retenue devra être administrable à distance via un accès sécurisé par SSH
- Mise en place d'un Firewall PFSENSE et portail captif

Mission 4 : Redondance et haute disponibilité

Vous intégrez le service informatique du **centre administratif de stade**. Sur ce site sont effectuées toutes les opérations concernant la gestion du personnel et l'administration du stade.

Solution permettant la redondance des services, la tolérance de panne et l'équilibrage des charges des éléments d'interconnexions de niveau 2 et 3.

- **la durée de l'interruption de service doit être minimale**
- **solution permettant d'améliorer la continuité de service des services existants en cas de panne de Commutateurs et liaisons d'accès (FAI)**
- **agrégation des liens entre les commutateurs et augmentation de la bande passante**

Mission 5 : Déploiement d'une solution d'accès sans fil des utilisateurs mobiles de StadiumCompany (WIFI)

Actuellement, le stade possède un accès aux différentes ressources de StadiumCompagny (fichiers, impression, internet, bases de données,). Mais cet accès n'est possible qu'à travers une liaison filaire. La direction du stade souhaite étendre aux services équipés d'un terminal Wifi.

StadimCompagny a fait l'acquisition de plusieurs Switchs compatibles PoE et des AP Cisco.Vous êtes chargé d'implémenter une solution d'accès sans fil pour les salariés du stade ainsiqu'aux visiteurs. Ces derniers n'auront accès qu'à la ressource internet mais d'une façon sécurisée (obligation légale).

Éléments du cahier des charges concernant les accès Wifi.

A chaque service est disposé d'un point d'accès 802.11 b/g/n PoE. Il y a un SSID non diffusépar VLAN sauf le Vlan visiteur.

La confidentialité est assurée par la norme WPA2 Enterprise sauf pour le dernier dans première temps, puis un renforcement de l'authentification dans un deuxième temps.

Prérequis :

- Le système d'information d'AP est opérationnel.

Modification à opérer :

- Proposer une solution d'accès Wifi pour le Vlan Wifi (stade-wifi)
- Proposer une solution d'accès Wifi pour les visiteurs

Mission 6 : Solution de gestion du Parc informatique

Le parc informatique de StadiumCompagny doit être inventorié. Pour cela, vous êtes chargé d'étudier une solution automatisée de gestion de parc.

Les objectifs de la gestion du parc

- **permettent aux administrateurs du parc de disposer d'un inventaire à jour de tous lespostes des services de stade**

- **fournir un outil d'helpdesk pour gérer les pannes (gestion des incidents)**

Mission 7 : Solution de supervision de l'infrastructure réseau et système permettant d'assurer l'anticipation des pannes

StadiumCompany recherche l'implémentation et la configuration d'une solution Open Source qui vise à superviser à distance les différents éléments actifs de l'infrastructure systèmes et réseaux du Stade avec gestion des alertes. Le but principal du projet est de pouvoir établir, choisir et installer une solution de surveillance des serveurs, routeurs, commutateurs, etc… qui remplit les conditions suivantes :

- Coûts financiers les plus réduits possibles
- Récupération des informations permettant la détection des pannes, l'indisponibilité des serveurs (Windows, Linux), routeurs, commutateurs, les états des imprimantes réseau et leurs services
- Des renseignements supplémentaires de monitoring sur la charge CPU, espace disque, mémoire disponible, input/output, processus en cours d'exécution, paquet perdu, temps moyen de parcours (round trip average), information d'état SNMP, trafic, bande passante consommée etc...
- Des renseignements supplémentaires de monitoring sur les services DNS, DHCP, http, SMTP, POP, IMAP, FTP
- Gestion des alertes
- Notification par mail ou SMS en cas de problème
- Générer des rapports sur le fonctionnement des serveurs par mois
- Générer des graphes (cartographie du réseau, ...)
- Une interface graphique claire pour l'interaction utilisateur/Logiciel

Mission 8 : Systèmes de gestion des événements et des informations de sécurité

Utilisation de Zimbra

Section 3 : Nos solutions

Mission 1 : Conception et prise en charge de StadiumCompany

Paragraphe 1 : L'adressage IP

A) Les définitions

Concernant l'adressage IP, il en existe deux types :

- **l'adressage IP statique**
- **l'adressage IP dynamique**

Une adresse IP statique est une adresse configurée manuellement **qui ne change pas**, autrement dit qui est attribuée en permanence sur des postes de travail.

Au contraire, **une adresse IP dynamique** est une adresse qui est **temporaire**. Dès lors qu'une machine se déconnecte, l'adresse IP peut être réattribuée à un autre équipement. Elle se manifeste grâce à un serveur DHCP.

B) Notre choix

Pour pouvoir **répartir au mieux les adresses IP** et avoir la possibilité de concevoir manuellement notre architecture, nous choisissons d'utiliser **l'adressage IP statique**, auquel nous ajoutons la création de **plusieurs VLANS**.

S'agissant **d'une adresse IP version 4**[1], répartie en 4 octets faisant au total 32 Bits, celle-ci est constituée :

[1] Nous écarterons ici l'adressage IP version 6.

- **d'une partie réseau**
- **d'une partie hôte**

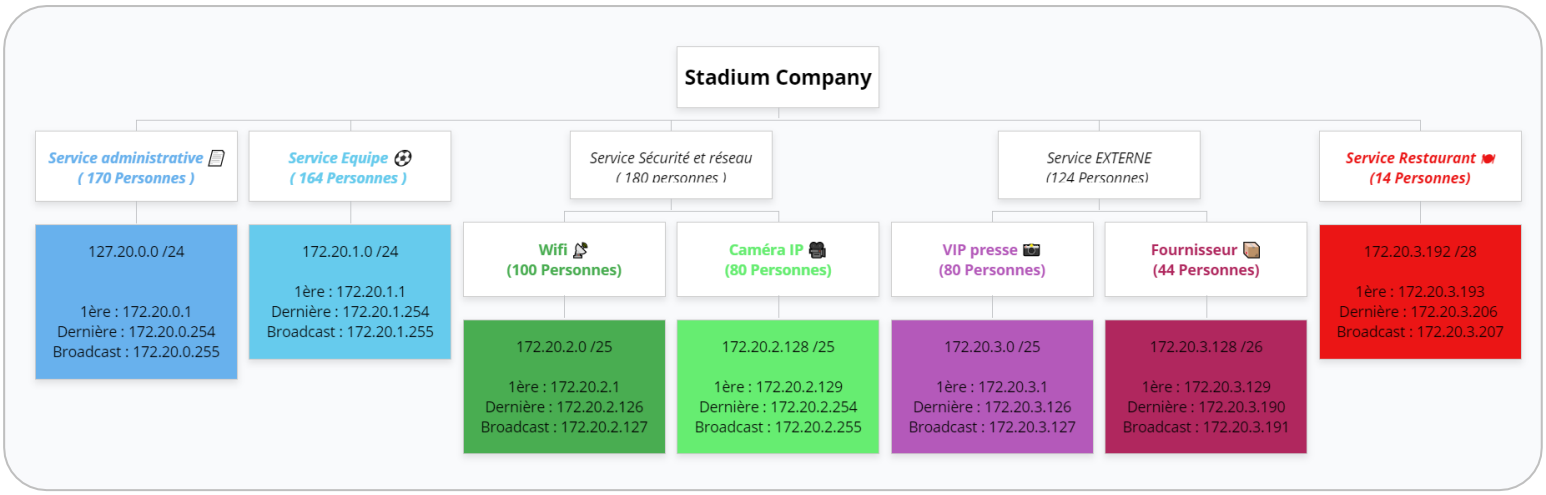
À cette adresse IP contenant les deux parties décrites, s'ajoute **un masque de sous-réseau**, permettant de définir la partie réseau et la partie hôte. Ce masque de sous-réseau peut s'écrire sous forme binaire, décimale ou CIDR (notation prenant en compte le dernier Bit utilisé).

En résumé, la fusion de l'adresse IP et du masque de sous-réseau nous permet d'obtenir **l'adresse de réseau**. En l'occurrence, dans notre cas, notre adresse de réseau est : **172.20.0.0 /24**.

C) La pratique

En répartissant les adresses IP en fonction du nombre d'utilisateurs et de notre adresse de réseau, nous obtenons **le tableau suivant** :

Les Services	Utilisateurs	CIDR	Adresse Réseau	Première adresse	Dernière adresse	Broadcast
Service Administratif	170	/24	172.20.0.0	172.20.0.1	172.20.0.254	172.20.0.255
Service Équipe	164	/24	172.20.1.0	172.20.1.1	172.20.1.254	172.20.1.255
Service Wifi	100	/25	172.20.2.0	172.20.2.1	172.20.2.126	172.20.2.127
Service Caméra IP	80	/25	172.20.2.128	172.20.2.129	172.20.2.254	172.20.2.255
Service VIPPresse	80	/25	172.20.3.0	172.20.3.1	172.20.3.126	172.20.3.127
Service Fournisseur	44	/26	172.20.3.128	172.20.3.129	172.20.3.190	172.20.3.191
Service Restaurant	14	/28	172.20.3.192	172.20.3.193	172.20.3.206	172.20.3.207



Paragraphe 2 : Les VLANS

A) Les définitions

Le **VLAN** (*Virtual Local Area Network, réseau local virtuel*) est un type de réseau local dans lequel **plusieurs machines informatiques sont connectées sur un même réseau avec des ports virtuels**.

Il existe 3 types de VLANS :

- **le VLAN de niveau 1 par ports**
- **le VLAN de niveau 2 par adresse MAC**
- **le VLAN de niveau 3 par adresse IP**

Le VLAN niveau 1 (par port) est créé en affectant **un VLAN à chaque port d'un commutateur**. En d'autres mots, l'appartenance d'une trame à un VLAN est déterminée par la connexion de la carte réseau du périphérique à un port du commutateur. Les ports étant affectés de manière statique à un VLAN.

Le VLAN niveau 2 (MAC) est créé en affectant **un VLAN à chaque adresse MAC**. En d'autres mots, l'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. L'affectation est faite de manière dynamique, les ports des commutateurs sont attribués à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.

Le VLAN niveau 3 (IP) est un VLAN dans lequel **les commutateurs apprennent automatiquement** la configuration des VLAN en accédant aux informations de la couche Transport.

B) Notre choix

Comme nous l'avons évoqué au paragraphe précédent, nous allons procéder à un adressage statique. Or, le VLAN qui se prête le mieux pour cela est le **VLAN de niveau 1 (par port)**.

De plus, d'une part ce type de VLAN a l'avantage **d'offrir une facilité de configuration**, d'autre part en cas de tentative d'attaque extérieure, le PC pirate ne pourra pénétrer le VLAN

qu'en se branchant sur un port tagué, c'est-à-dire sur un commutateur physique. Il s'agit donc **d'un type de VLAN sécurisé**.

Pour toutes ces raisons, notre choix se porte sur **le VLAN de niveau 1 (par port)**.

C) La pratique

1) La configuration initiale des deux switchs (mode trunk)

a) La configuration du Switch Server

Switch>**enable**

Switch#**configure terminal**

Switch(config)#**hostname SW-SRV**

SW-SRV(config)#**VTP mode server**

SW-SRV(config)#**VTP version 2**

SW-SRV(config)#**VTP domain stadiumcompany.com**

SW-SRV(config)#**interface range fa 0/22 – 24**

SW-SRV(config-if-range)#**switchport trunk encapsulation dot1Q**

SW-SRV(config if-range)#**switchport mode trunk**

SW-SRV(config if-range)#**no shutdown**

SW-SRV(config if-range)#**exit**

SW-SRV(config)#**exit**

SW-SRV#**show VTP status**

```
Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x03 0x39 0x96 0xD6 0x9C 0x4D 0xCF 0xD5
                                    0x31 0x4F 0x6D 0x77 0x71 0x95 0x21 0x9A
```


SW-SRV#**show interface trunk**

```
SW-SERVER#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1
```

b) La configuration du Switch Client

Switch>**enable**

Switch#**configure terminal**

Switch(config)#**hostname SW-CLIENT**

SW-CLIENT(config)#**VTP mode client**

SW-CLIENT(config)#**VTP version 2**

SW-CLENT(config)#**VTP domain stadiumcompany.com**

SW-CLENT (config)#**interface range fa 0/22 – 24**

SW-CLENT (config-if-range)#**switchport trunk encapsulation dot1Q**

SW-CLENT (config-if-range)#**switchport mode trunk**

SW-CLENT (config-if-range)#**no shutdown**

SW-CLIENT(config if-range)#**exit**

SW-CLIENT(config)#**exit**

SW-CLIENT#**show VTP status**

```
Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x03 0x39 0x96 0xD6 0x9C 0x4D 0xCF 0xD5
                                    0x31 0x4F 0x6D 0x77 0x71 0x95 0x21 0x9A
```

SW-CLIENT#**show interface trunk**

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/24      1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1
```

2) La création des VLANS

SW-SRV(config)#**VLAN 10**

SW-SRV(config-vlan)#**name administration**

SW-SRV(config-vlan)#**exit**

SW-SRV(config)#**VLAN 20**

SW-SRV(config-vlan)#**name equipes**

SW-SRV(config-vlan)#**exit**

SW-SRV(config)#**VLAN 30**

SW-SRV(config-vlan)#**name wifi**

SW-SRV(config-vlan)#**exit**

SW-SRV#**show VLAN**

```
10   administration                    active
20   equipes                           active
30   wifi                              active
```

SW-CLIENT#**show VLAN**

```
10   administration                    active
20   equipes                           active
30   wifi                              active
```

3) L'attribution des ports des VLANS

a) L'attribution des ports sur le Switch Server

SW-SRV(config)#**interface range fa 0/1 – 6**

SW-SRV(config-if-range)#**switchport access VLAN 10**

SW-SRV(config-if-range)#**no shutdown**

SW-SRV(config-if-range)#**exit**

SW-SRV(config)#**interface range fa 0/7 – 12**

SW-SRV(config-if-range)#**switchport access VLAN 20**

SW-SRV(config-if-range)#**no shutdown**

SW-SRV(config-if-range)**#exit**

SW-SRV(config)**#interface range fa 0/13 – 14**

SW-SRV(config-if-range)**#switchport access VLAN 30**

SW-SRV(config-if-range)**#no shutdown**

SW-SRV(config-if-range)**#exit**

SW-SRV(config)**#show VLAN**

10	administration	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6
20	equipes	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
30	wifi	active	Fa0/13, Fa0/14

b) L'attribution des ports sur le Switch Client

SW-CLIENT(config)**#interface range fa 0/1 – 6**

SW-CLIENT(config-if-range)**#switchport access VLAN 10**

SW-CLIENT(config-if-range)**#no shutdown**

SW-CLIENT(config-if-range)**#exit**

SW-CLIENT(config)**#interface range fa 0/7 – 12**

SW-CLIENT(config-if-range)**#switchport access VLAN 20**

SW-CLIENT(config-if-range)**#no shutdown**

SW-CLIENT(config-if-range)**#exit**

SW-CLIENT(config)**#interface range fa 0/13 – 14**

SW-CLIENT(config-if-range)**#switchport access VLAN 30**

SW-CLIENT(config-if-range)**#no shutdown**

SW-CLIENT(config-if-range)**#exit**

SW-CLIENT(config)#**show VLAN**

```
10   administration                   active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6
20   equipes                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
30   wifi                             active    Fa0/13, Fa0/14
```

En résumé :

VLANS	NOMS	PORTS
VLAN 10	administration	0/1 - 0/6
VLAN 20	equipes	0/7 - 0/12
VLAN 30	wifi	0/13 – 0/14
PORTS TRUNK	PORTS TRUNK	0/22 – 0/24

Paragraphe 3 : Le routage

A) Les définitions

1) Le routage statique

S'agissant du routage, il existe deux types de routage :

- **le routage statique**
- **le routage dynamique**

Le routage statique consiste à configurer un routeur en **saisissant manuellement les routes** permettant de structurer le réseau *(notamment par l'intermédiaire de port de sortie ou d'adresse IP de destination)*. Le routage statique n'est donc recommandé que lorsqu'il y a une connexion entre 10 routeurs au maximum.

Pour effectuer ce routage manuel, l'administrateur dispose de deux options :

- **soit au travers de la table de routage en utilisant la commande « route add »**
- **soit en utilisant la console du service « Routage et accès distant »**

2) Le routage dynamique

Contrairement au routage statique, **le routage dynamique** permet au routeur de **s'actualiser de manière automatique**, c'est-à-dire dynamique. De cette manière, les routeurs vont communiquer entre eux de manière automatique et calculer les routes les plus rapides pour que les informations soient délivrées de manière efficace.

Ainsi, dans un routage dynamique :

- **chaque routeur diffuse la liste des réseaux sur lesquels il est connecté**
- **chaque routeur met à jour automatiquement sa table de routage à partir des informations reçues depuis les autres routeurs**

Le routage dynamique utilise les protocoles suivants :

- **protocole RIP** (Routing Information Protocol)
- **protocole IGRP** (Interior Gateway Routing Protocol)
- **protocole EIGRP** (Enhanced Interior Gateway Routing Protocol)
- **protocole OSPF** (Open Shortest Path First)
- **protocole IS-IS** (Intermediate System-to-Intermediate System)
- **protocole BGP** (Border Gateway Protocol)

B) Notre choix

Le routage dynamique présente les avantages :

- **de permettre faciliter les échanges entre routeurs** *(car les données sont échangées de manière automatique)*
- **d'actualiser les tables de routage en cas de modification du réseau**

Pour autant, le routage dynamique :

- **consomme beaucoup de bande passante**
- **est plus difficile à initialiser**
- **peut représenter un problème de sécurité, car une attaque par un pirate permettrait de lire la topologie du réseau, voire de s'introduire dedans**

Le routage statique présente certes l'obligation de l'administrateur **à configurer toutes les routes manuellement** et à actualiser lui-même le routage, ce qui est plus long et difficile.

Mais il présente surtout les avantages :

- **d'économiser de la bande passante** (aucune donnée ne transite ente les routeurs pour les mettre à jour)

- **d'être sécurisé, car les routeurs ne communiquent pas d'informations sur le réseau**

- **de connaître parfaitement les routes et les flux de données par l'administrateur**

Ainsi, **nous choisirons le routage statique** car nous souhaitons paramétrer nous-mêmes les routes et que nous souhaitons protéger le réseau.

C) La pratique

1) La configuration des interfaces associées aux VLANS sur le routeur R1-Stade

Router>**enable**

Router#**configure terminal**

Router(config)#**hostname R1-Stade**

R1-Stade (config)#**interface fa 0/0**

R1-Stade (config-if)#**no shutdown**

R1-Stade (config-if)#**interface fa 0/0.10**

R1-Stade (config-subif)#**encapsulation dot1Q 10**

R1-Stade (config-subif)#**ip address 172.20.0.1 255.255.255.0**

R1-Stade (config-subif)#**no shutdown**

R1-Stade (config-subif)#**interface fa 0/0.20**

R1-Stade (config-subif)#**encapsulation dot1Q 20**

R1-Stade (config-subif)#**ip address 172.20.1.1 255.255.255.0**

R1-Stade (config-subif)#**no shutdown**

R1-Stade (config-subif)#**interface fa0/0.30**

R1-Stade (config-subif)#**encapsulation dot1Q 30**

R1-Stade (config-subif)#**ip address 172.20.2.1 255.255.255.128**

R1-Stade (config-subif)#**no shutdown**

2) La configuration des interfaces avec le routeur R2-Bill

R1-Stade (config-subif)**#interface fa0/1**

R1-Stade (config-subif-if)**#ip address 200.200.200.1 255.255.255.252**

R1-Stade (config-subif-if)**#no shutdown**

3) La configuration du routeur R2-Bill

Router>**enable**

Router**#configure terminal**

Router(config)**#hostname R2-Bill**

R2-Bill(config)**#interface fa 0/1**

R2-Bill(config-subif-if)**#ip address 200.200.200.2 255.255.255.252**

R2-Bill (config-if)**#no shutdown**

4) L'ajout des réseaux distants dans la table de routage du routeur R1-Stade et R2-Bill

R1-Stade(config)**#ip route 192.168.1.1 255.255.255.0 200.200.200.2**

R2-Bill(config)**#ip route 172.20.2.1 255.255.252.0 200.200.200.1**

R1-Stade**#show ip route**

```
     172.20.0.0/16 is variably subnetted, 6 subnets, 3 masks
C       172.20.0.0/24 is directly connected, GigabitEthernet0/0.10
L       172.20.0.1/32 is directly connected, GigabitEthernet0/0.10
C       172.20.1.0/24 is directly connected, GigabitEthernet0/0.20
L       172.20.1.1/32 is directly connected, GigabitEthernet0/0.20
C       172.20.2.0/25 is directly connected, GigabitEthernet0/0.30
L       172.20.2.1/32 is directly connected, GigabitEthernet0/0.30
     200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.200.200.0/30 is directly connected, GigabitEthernet0/1
L       200.200.200.1/32 is directly connected, GigabitEthernet0/1
```


R2-Bill#**show ip route**

```
     200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.200.200.0/30 is directly connected, GigabitEthernet0/0/1
L       200.200.200.2/32 is directly connected, GigabitEthernet0/0/1
```

Dans la réalisation présentée ci-dessus, les interfaces FastEthernet ont été remplacées par des interfaces GigabitEthernet. Toutefois, le principe reste le même.

Mission 2 : Administration et gestion des accès utilisateurs

Dans un premier nous allons déployer et configurer l'AD, le DNS puis le DHCP sur le Windows server 2016

Paragraphe 1 : L'installation de l'Active Directory

A) La définition de l'active Directory

L'Active Directory (ou AD) est **un service d'annuaire** développé par Microsoft pour les réseaux de domaine Windows.

Il est inclus dans la plupart des systèmes d'exploitation Windows Server en tant **qu'ensemble de processus et de services**.

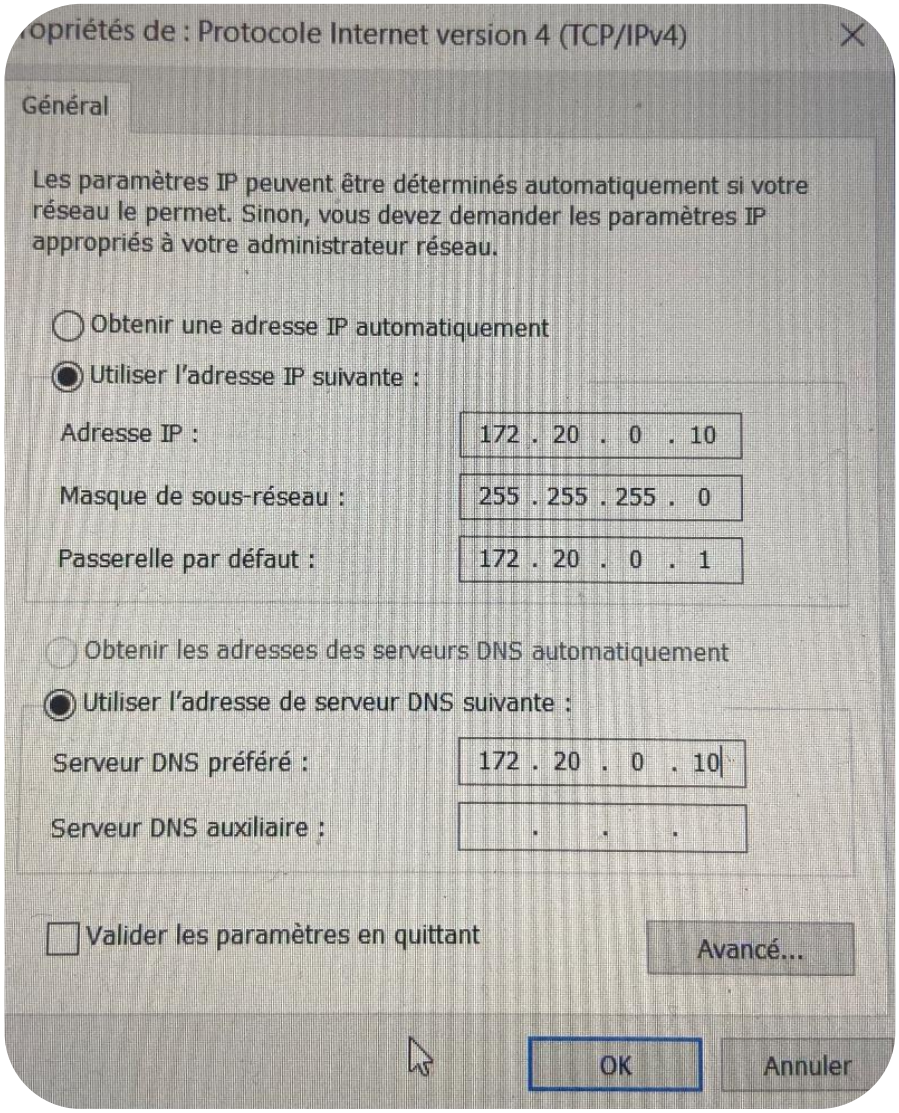
Son objectif principal est de fournir des services centralisés **d'authentification et d'identification**.

Active Directory permet également :

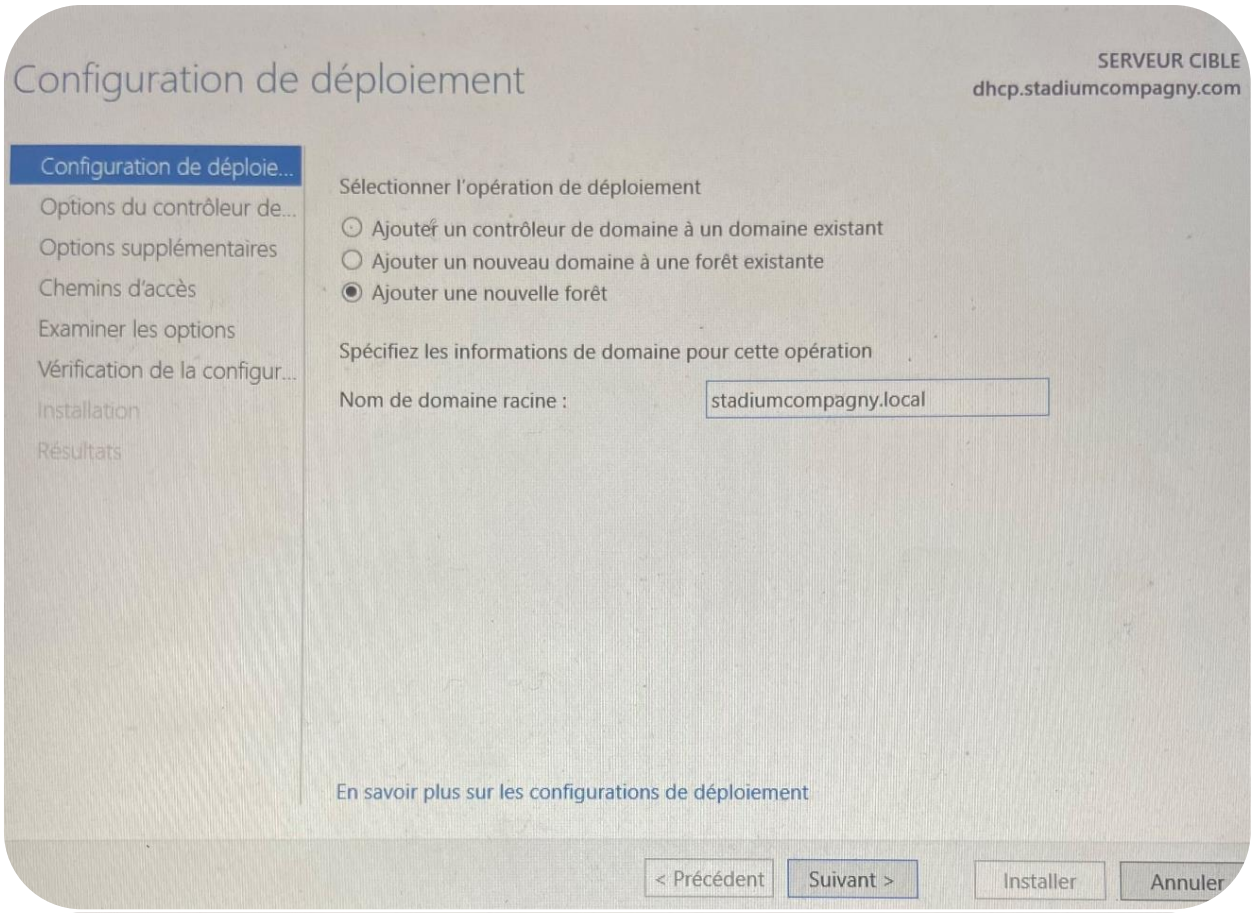
- **d'attribuer et d'appliquer des stratégies**
- **d'installer des mises à jour critiques par les administrateurs**
- **de distribuer des logiciels.**
- **de répertorier les éléments d'un réseau** *(exemples : les comptes des utilisateurs , les postes de travail, les imprimantes, les serveurs et les dossiers partagés…)*

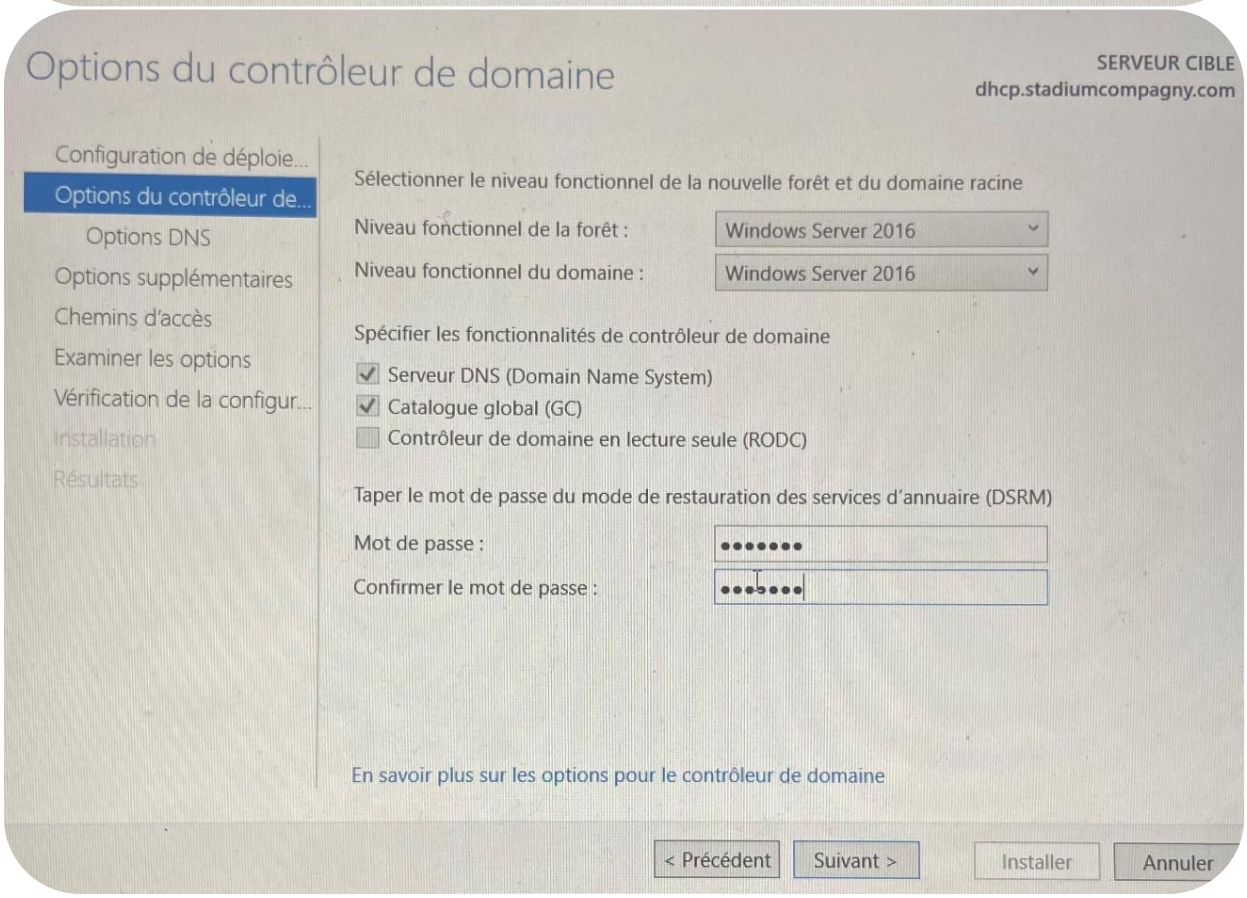
B) La pratique

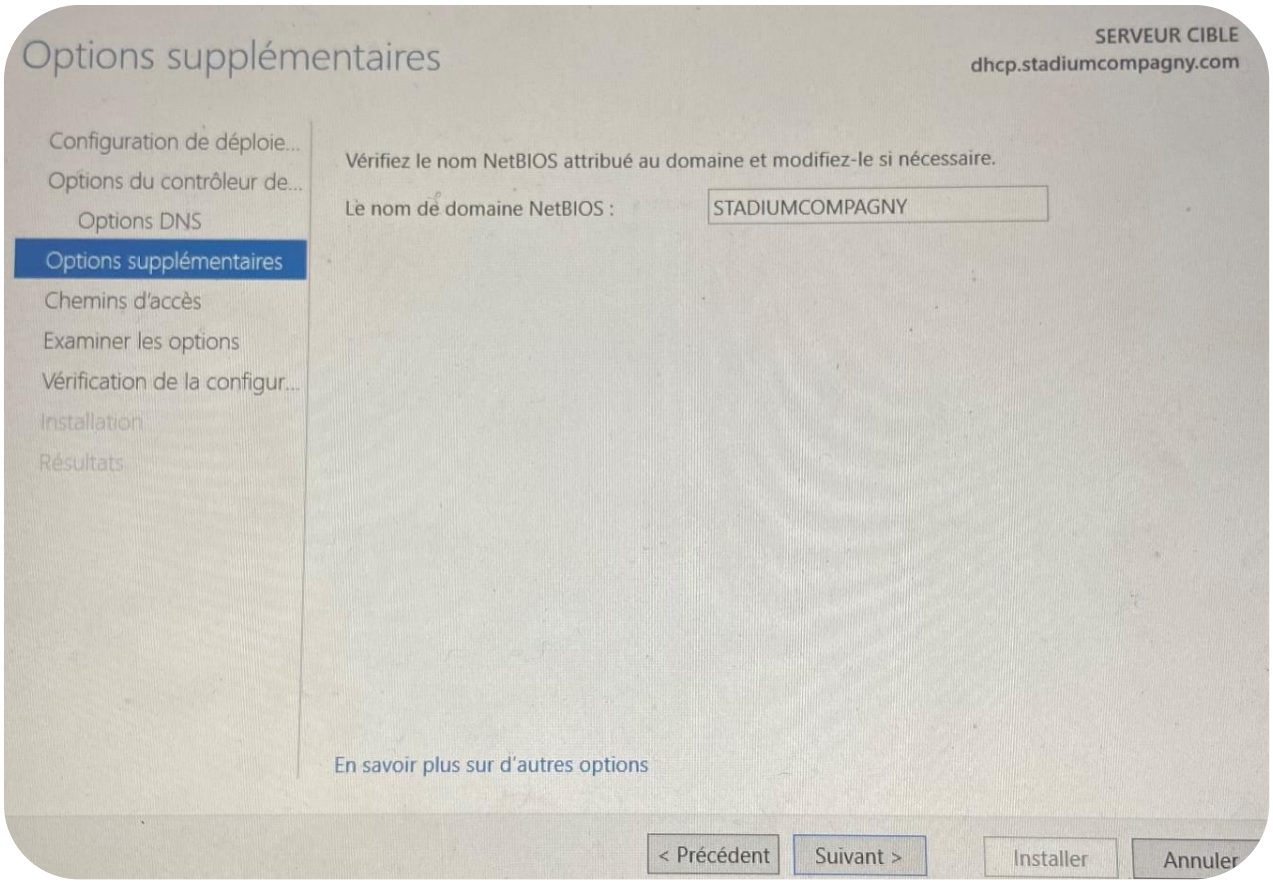
Conformément au cahier des charges, nous allons mettre l'adresse IP du serveur sur **172.20.0.10**.

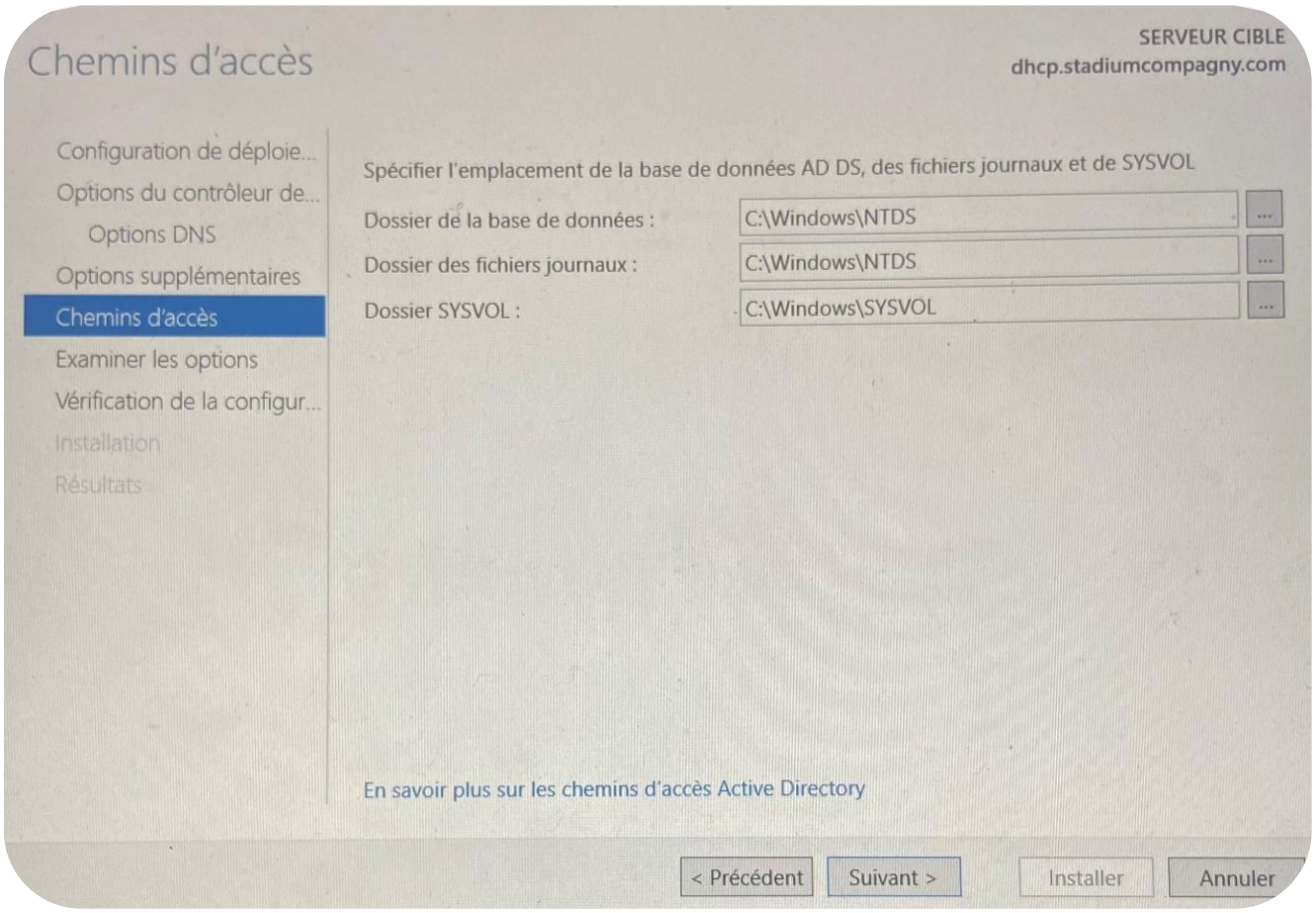


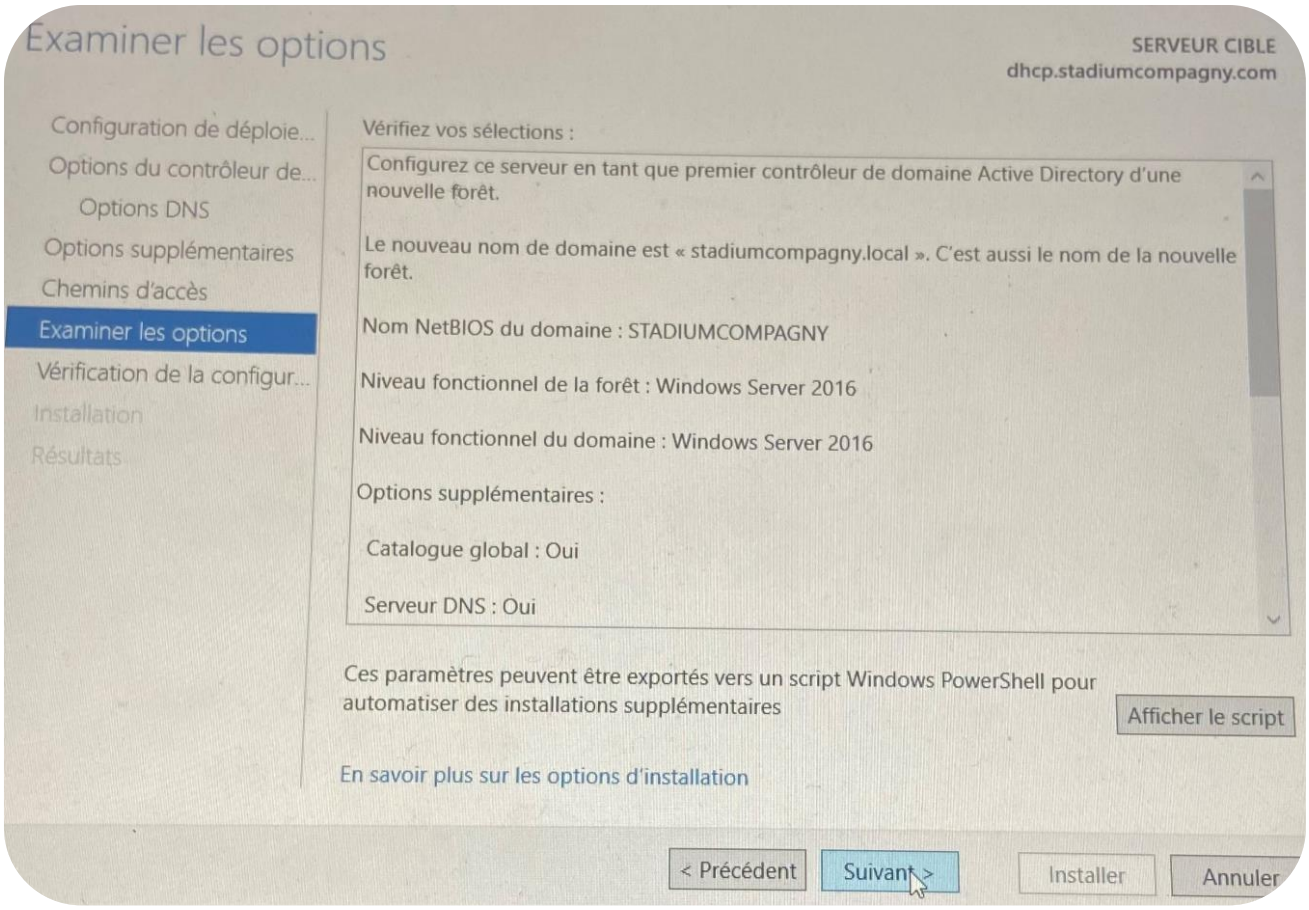
- Une fois que cela a été fait, nous procédons à la configuration du domaine stadiumcompagny.local.

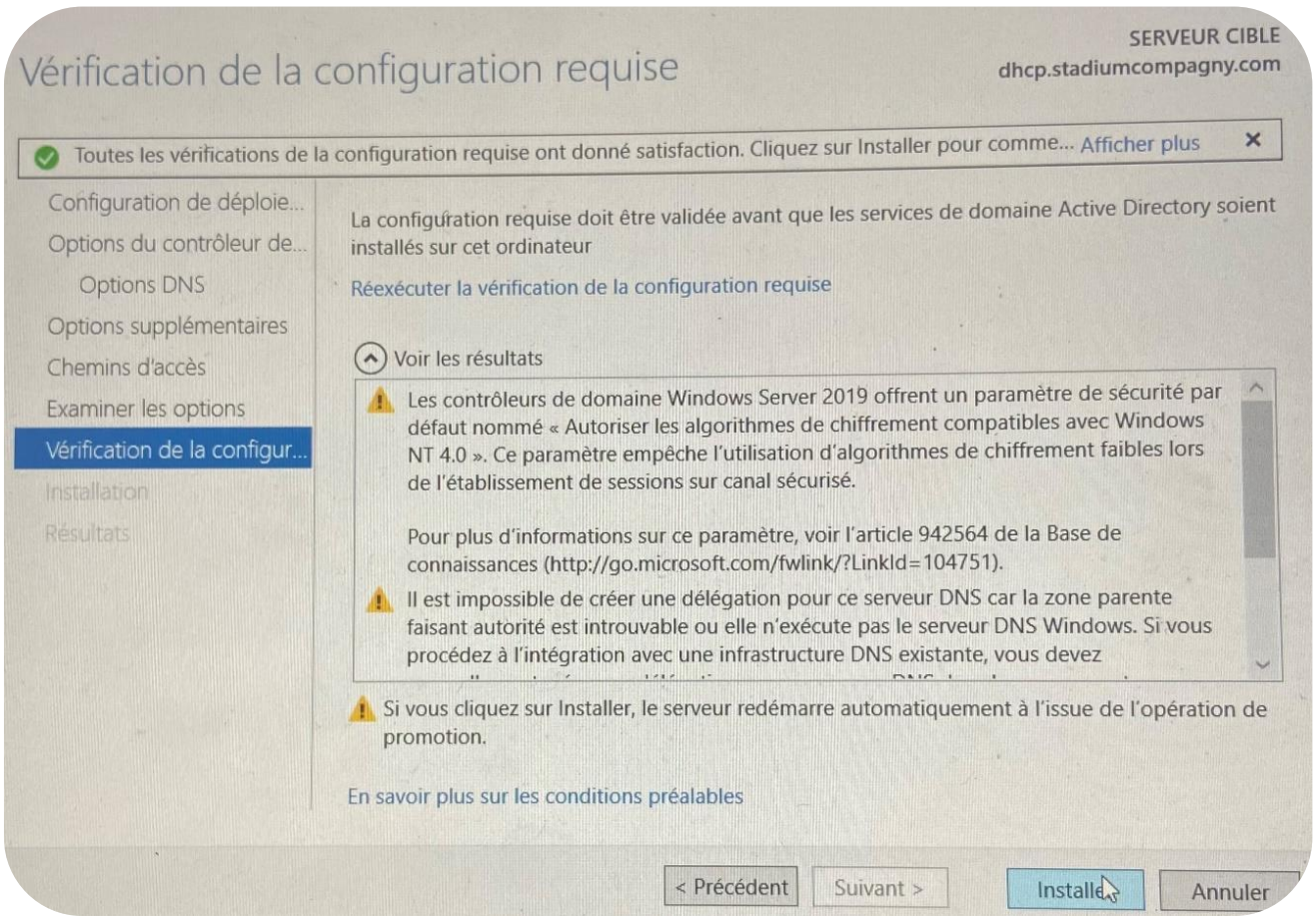

Configuration de déploiement
SERVEUR CIBLE
dhcp.stadiumcompagny.com
Configuration de déploie...
Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner l'opération de déploiement
Ajouter un contrôleur de domaine à un domaine existant
Ajouter un nouveau domaine à une forêt existante
Ajouter une nouvelle forêt
Spécifiez les informations de domaine pour cette opération
Nom de domaine racine :
stadiumcompagny.local
En savoir plus sur les configurations de déploiement
< Précédent
Suivant >
Installer
Annuler

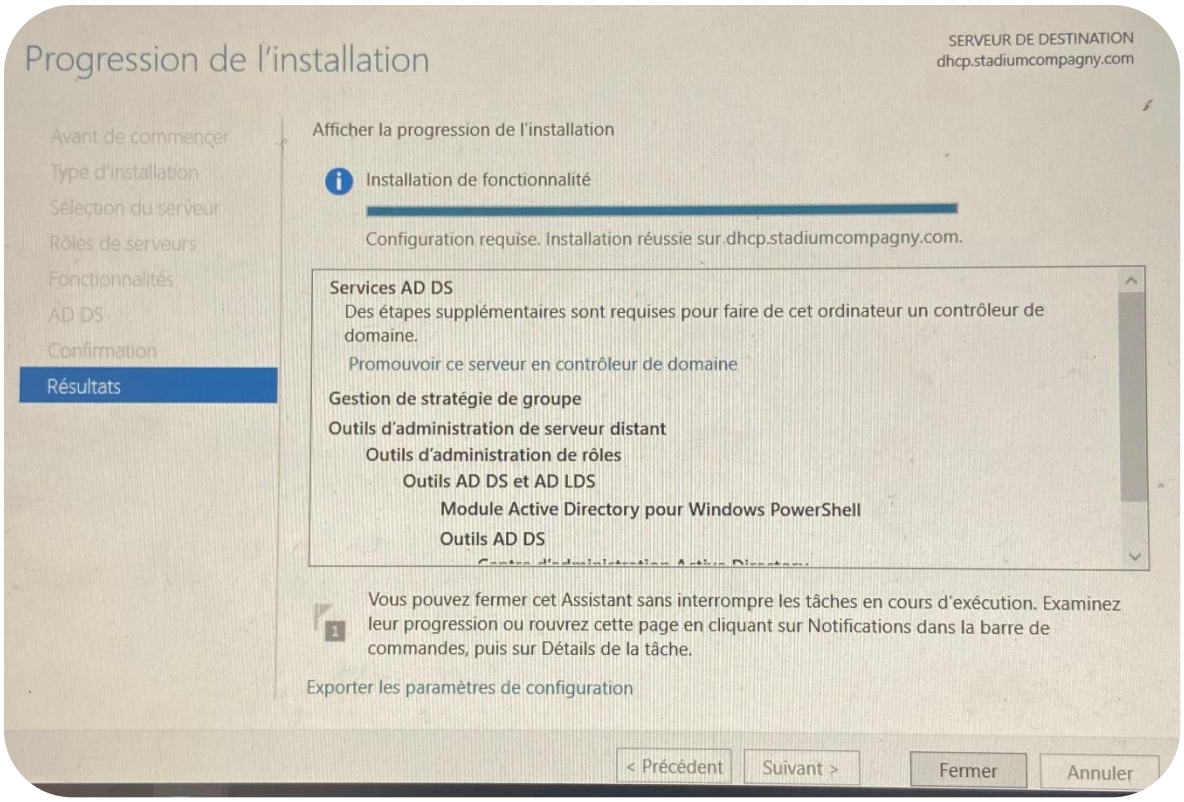

Options du contrôleur de domaine
SERVEUR CIBLE
dhcp.stadiumcompagny.com
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine
Niveau fonctionnel de la forêt :
Windows Server 2016
Niveau fonctionnel du domaine :
Windows Server 2016
Spécifier les fonctionnalités de contrôleur de domaine
Serveur DNS (Domain Name System)
Catalogue global (GC)
Contrôleur de domaine en lecture seule (RODC)
Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)
Mot de passe :
Confirmer le mot de passe :
En savoir plus sur les options pour le contrôleur de domaine
< Précédent
Suivant >
Installer
Annuler


Options supplémentaires
SERVEUR CIBLE
dhcp.stadiumcompagny.com
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.
Le nom de domaine NetBIOS :
STADIUMCOMPAGNY
En savoir plus sur d'autres options
< Précédent
Suivant >
Installer
Annuler


Chemins d'accès
SERVEUR CIBLE
dhcp.stadiumcompagny.com
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL
Dossier de la base de données :
C:\Windows\NTDS
Dossier des fichiers journaux :
C:\Windows\NTDS
Dossier SYSVOL :
C:\Windows\SYSVOL
En savoir plus sur les chemins d'accès Active Directory
< Précédent
Suivant >
Installer
Annuler


Examiner les options
SERVEUR CIBLE
dhcp.stadiumcompagny.com
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez vos sélections :
Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.
Le nouveau nom de domaine est « stadiumcompagny.local ». C'est aussi le nom de la nouvelle forêt.
Nom NetBIOS du domaine : STADIUMCOMPAGNY
Niveau fonctionnel de la forêt : Windows Server 2016
Niveau fonctionnel du domaine : Windows Server 2016
Options supplémentaires :
Catalogue global : Oui
Serveur DNS : Oui
Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires
Afficher le script
En savoir plus sur les options d'installation
< Précédent
Suivant >
Installer
Annuler


Vérification de la configuration requise
SERVEUR CIBLE
dhcp.stadiumcompagny.com
Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... Afficher plus
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur
Réexécuter la vérification de la configuration requise
Voir les résultats
Les contrôleurs de domaine Windows Server 2019 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.
Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?LinkId=104751).
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 redémarre automatiquement à l'issue de l'opération de promotion.
En savoir plus sur les conditions préalables
< Précédent
Suivant >
Installer
Annuler



L'Active Directory est désormais installée.

Paragraphe 2 : L'application du NAT et du relais DHCP sur le routeur R1-Stade

A) L'application du NAT sur le routeur R1-Stade

R1-Stade(config)#**interface fa0/1**

R1-Stade(config)#**ip nat outside**

R1-Stade(config)#**interface fa0/0.10**

R1-Stade(config)#**interface fa0/0.20**

R1-Stade(config)#**interface fa0/0.30**

R1-Stade(config)#**ip nat inside**

R1-Stade(config)#**accesslist 10 permit 172.20.0.0 0.0.0.255**

R1-Stade(config)#**accesslist 20 permit 172.20.1.0 0.0.0.255**

R1-Stade(config)#**accesslist 30 permit 172.20.2.0 0.0.0.127**

R1-Stade(config)**#ip nat inside source list 10 interface fa0/1 overload**

R1-Stade(config)**#ip nat inside source list 20 interface fa0/1 overload**

R1-Stade(config)**#ip nat inside source list 30 interface fa0/1 overload**

R1-Stade(config)**#ip route 0.0.0.0 0.0.0.0 10.0.228.1**

#show ip nat translation

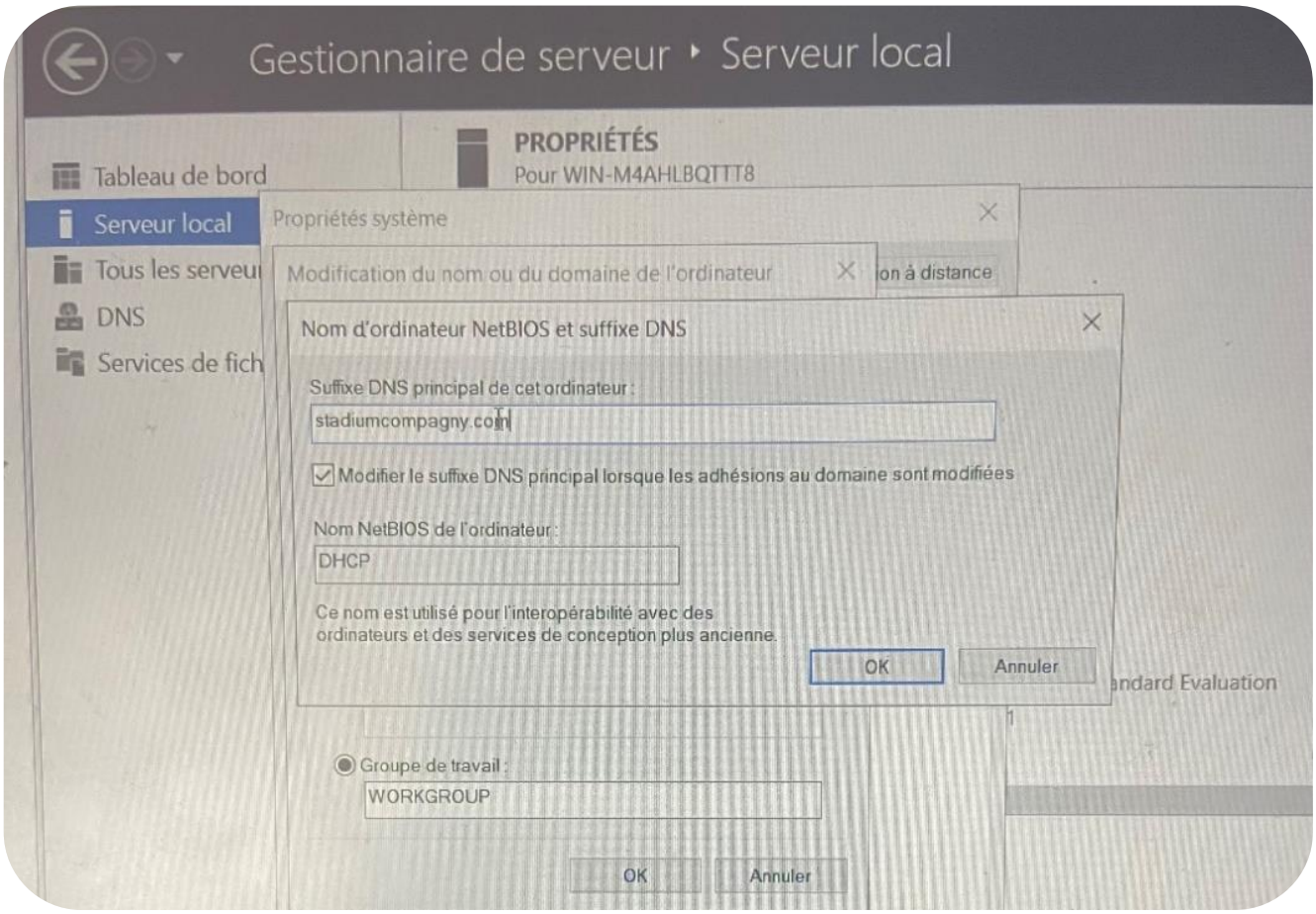
B) L'application du relais DHCP sur le routeur R1-Stade

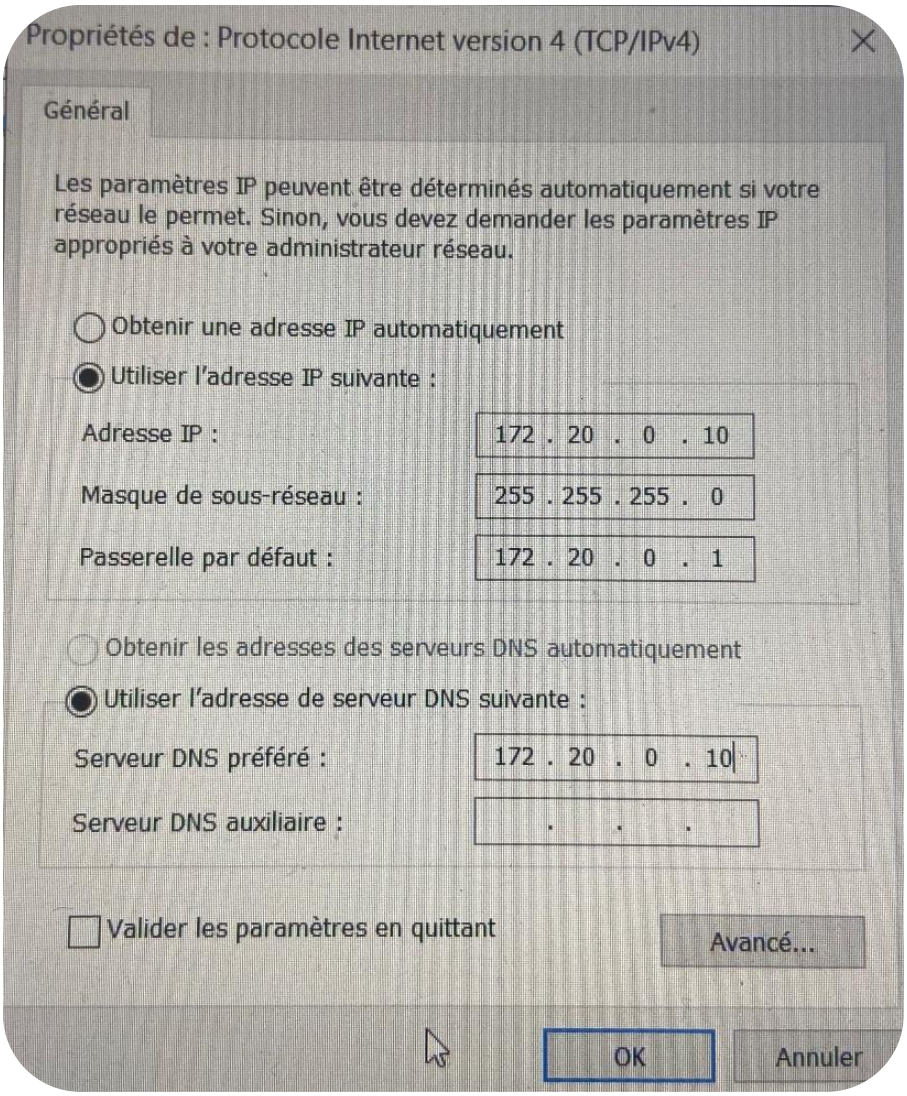
R1-Stade(config)**#inteface fa0/0.20**

R1-Stade(config)**#interface fa0/0.30**

R1-Stade(config)**#ip helper-address 172.20.0.10**

Paragraphe 3 : La mise en place du DNS sur Windows Server 2016



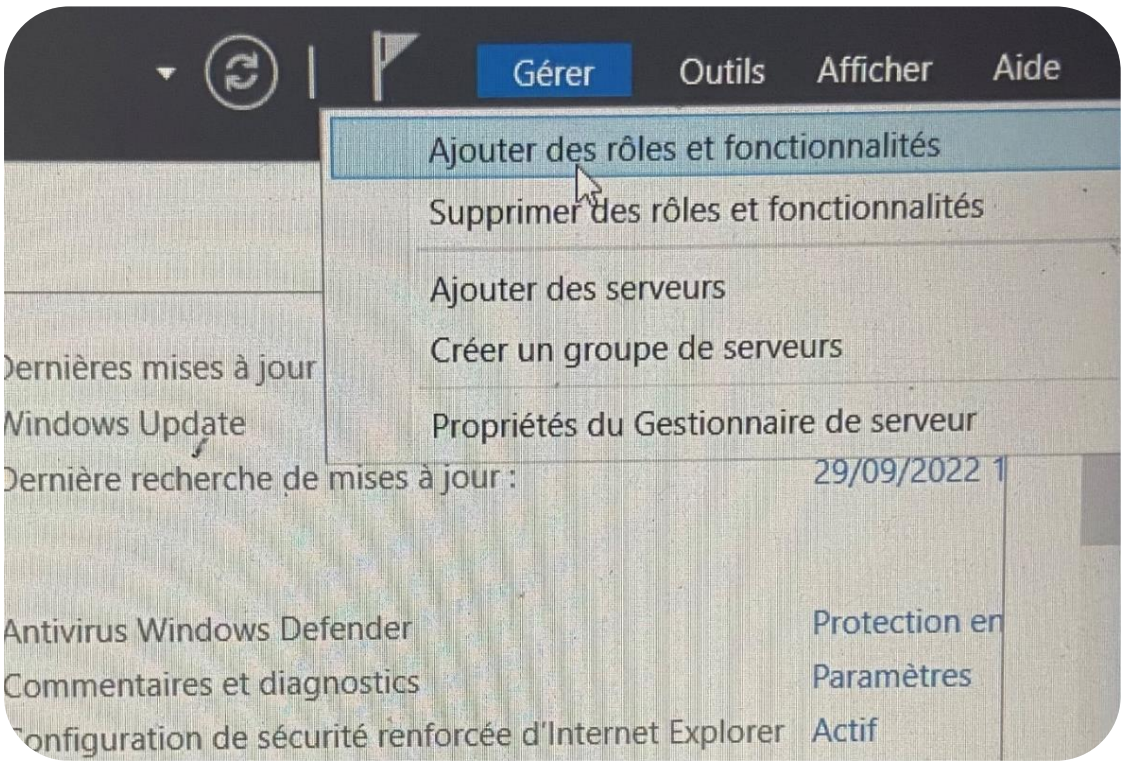


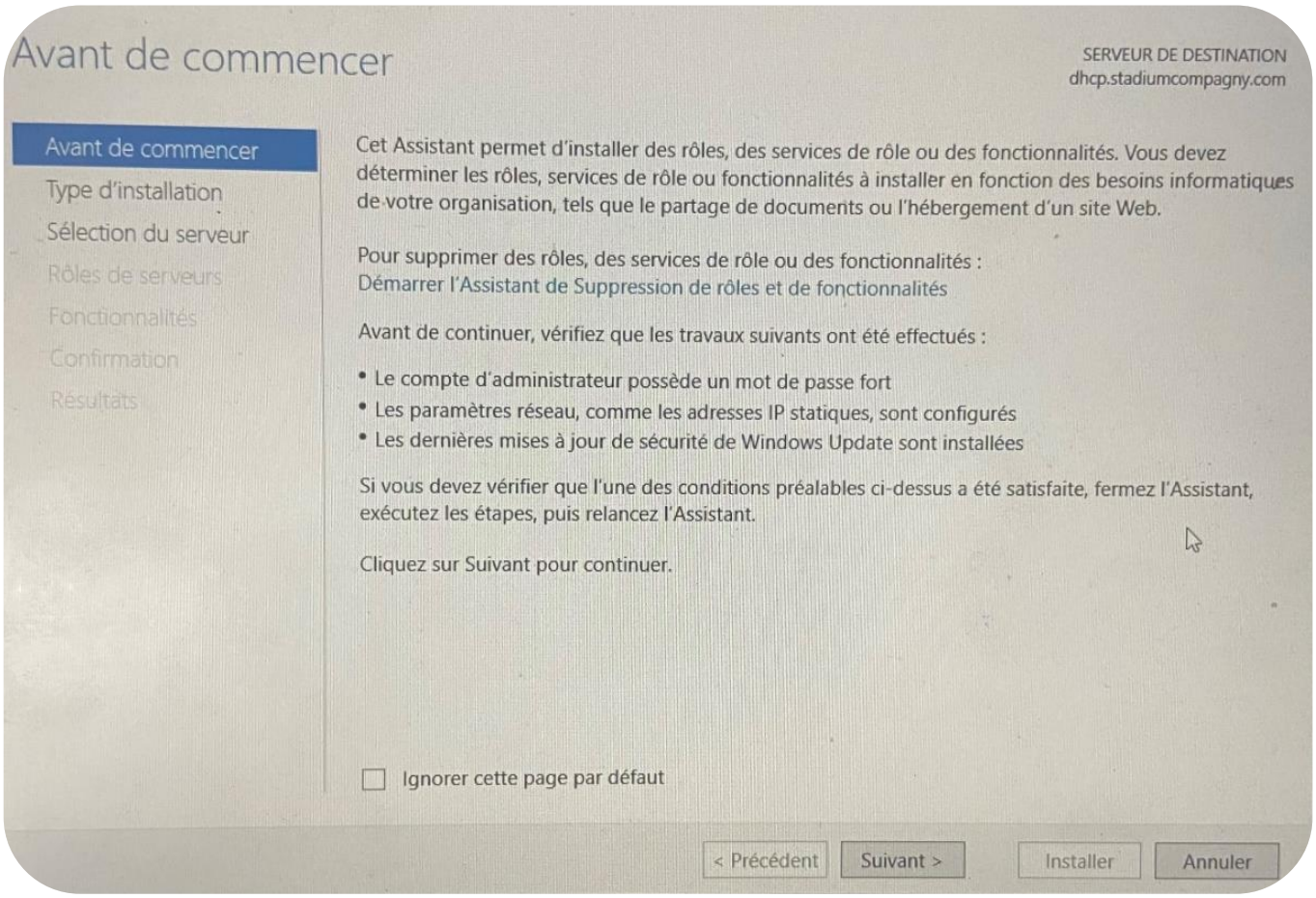
Paragraphe 4 : La mise en place du rôle DHCP sur Windows Server 2016

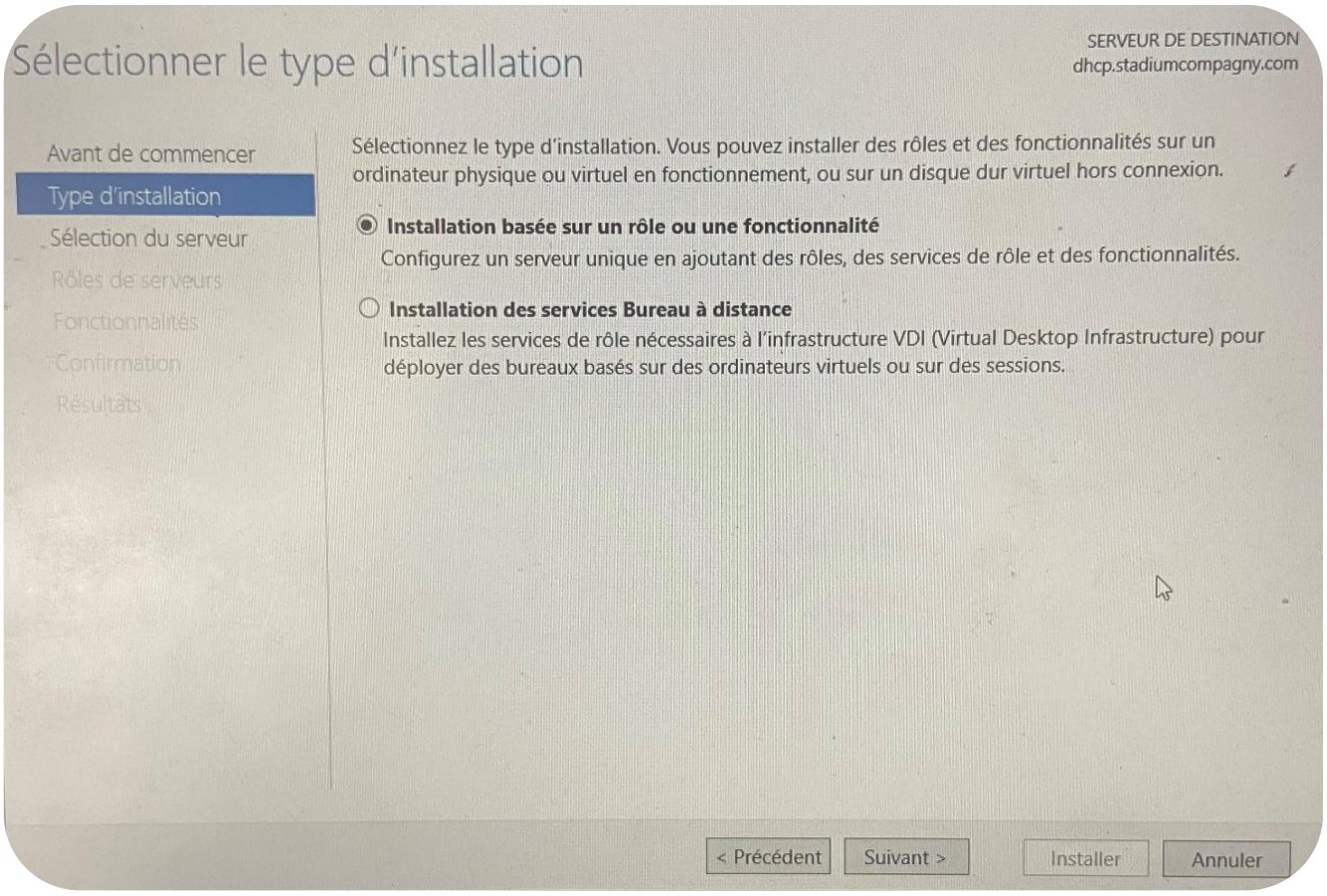
Nous allons intégrer le DHCP sur le Windows server 2016.

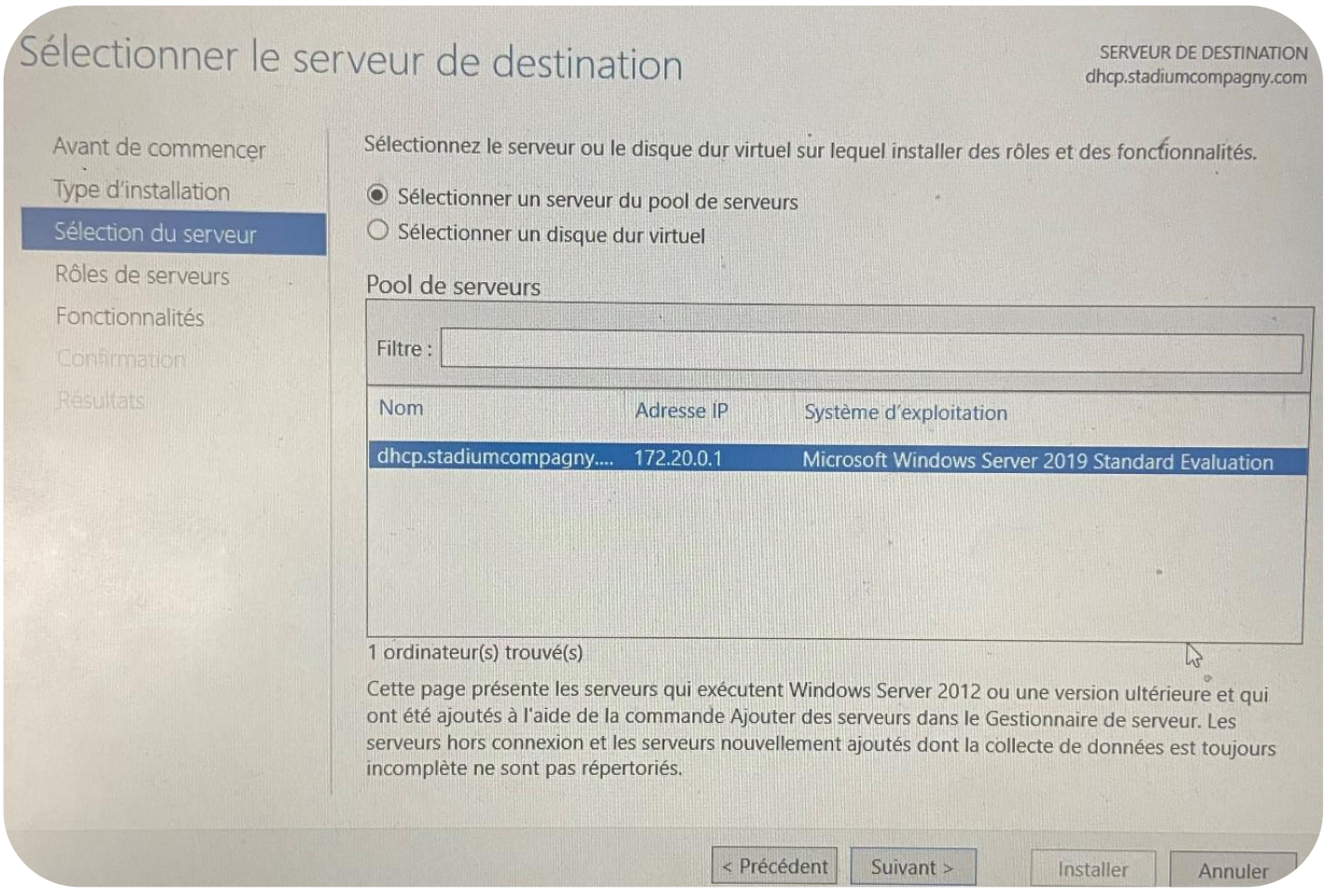
- Sur le gestionnaire du serveur, nous allons **dans les outils**, puis sur « **DHCP** ».

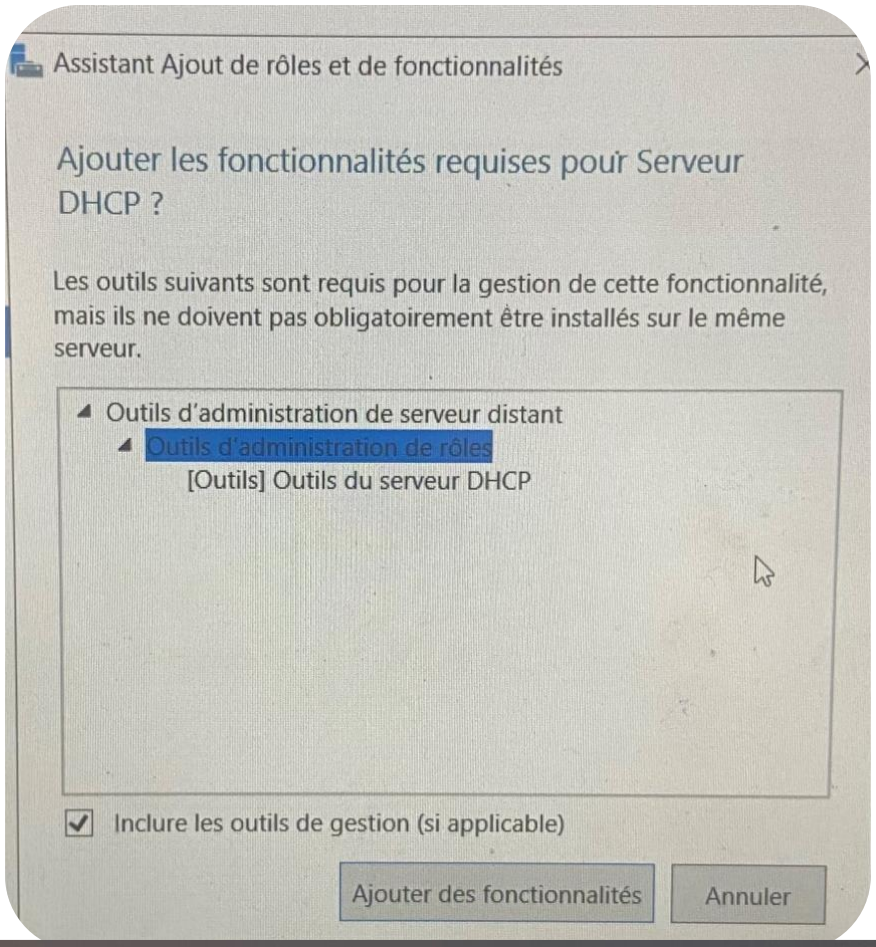
A) La création initiale du rôle DHCP

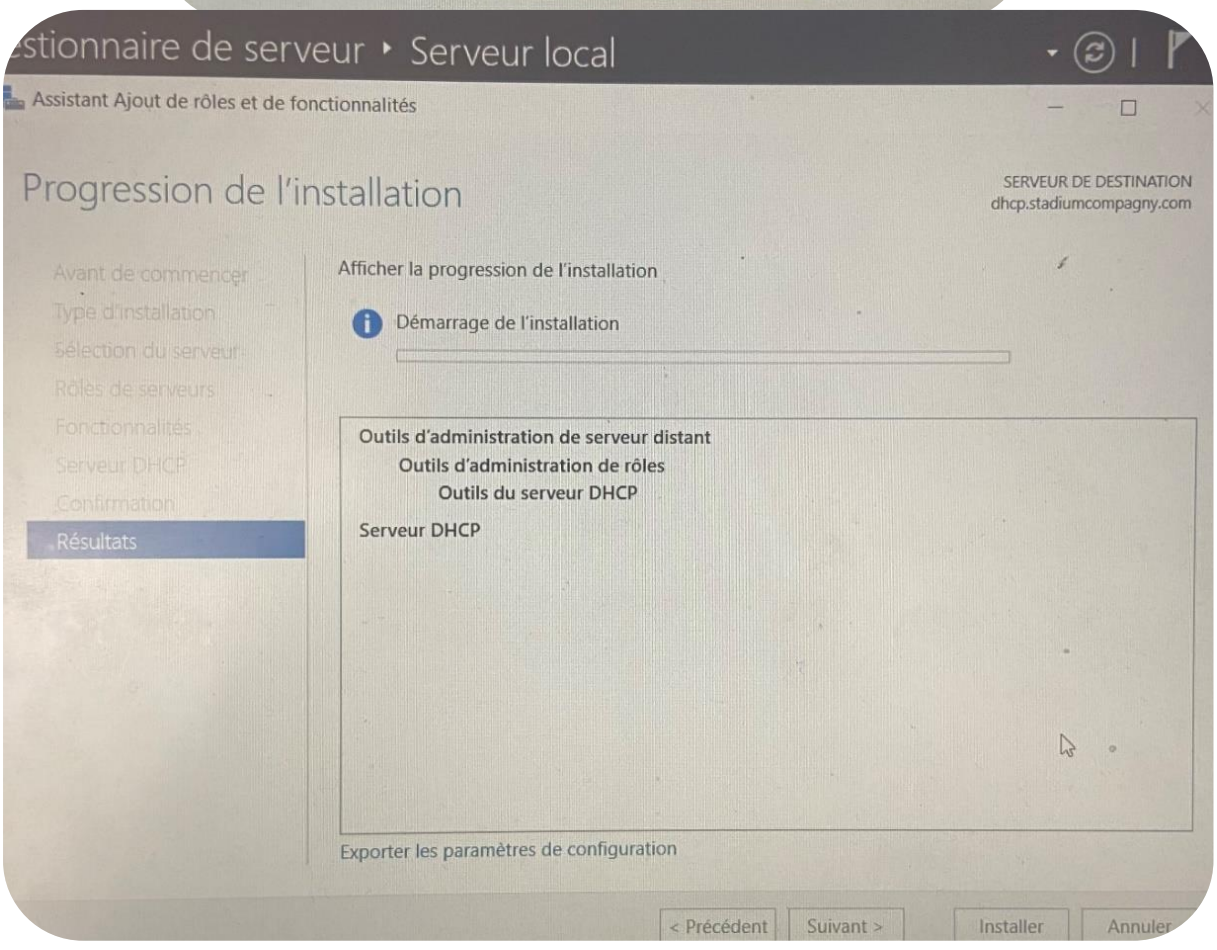


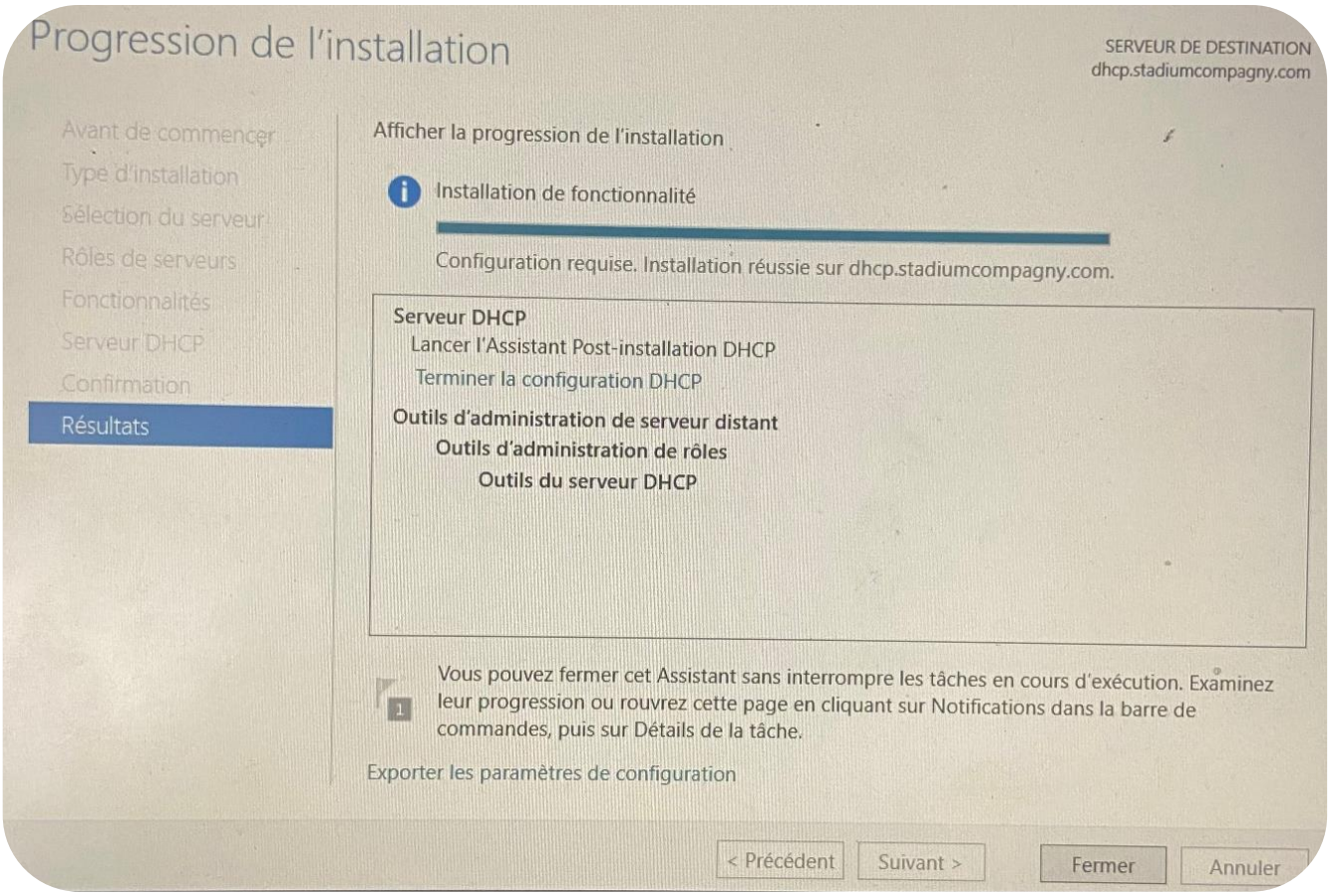


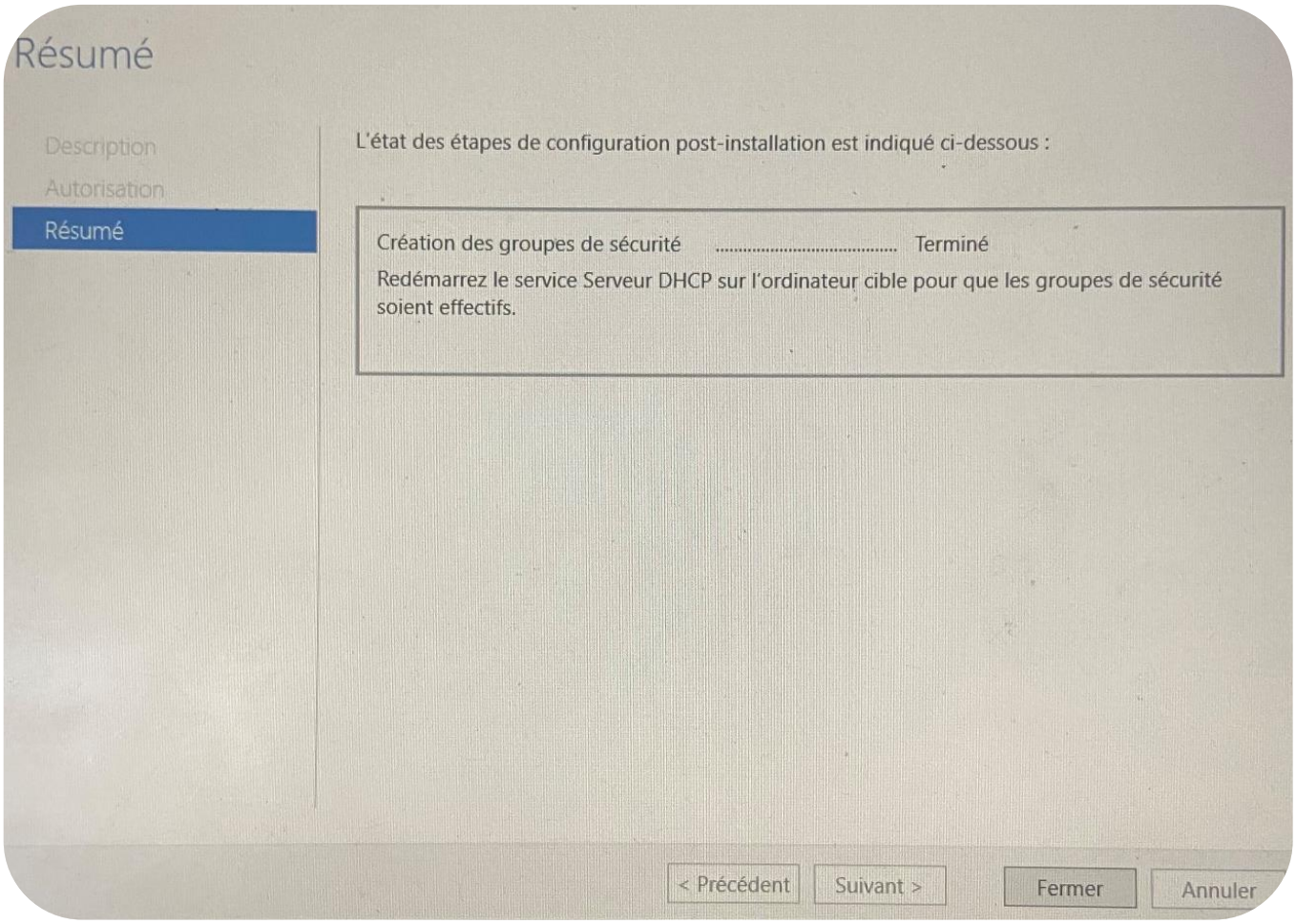

Sélectionner le type d'installation
SERVEUR DE DESTINATION
dhcp.stadiumcompagny.com
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.
< Précédent
Suivant >
Installer
Annuler


Sélectionner le serveur de destination
SERVEUR DE DESTINATION
dhcp.stadiumcompagny.com
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
dhcp.stadiumcompagny....
172.20.0.1
Microsoft Windows Server 2019 Standard Evaluation
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Serveur DHCP ?
Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.
Outils d'administration de serveur distant
Outils d'administration de rôles
[Outils] Outils du serveur DHCP
Inclure les outils de gestion (si applicable)
Ajouter des fonctionnalités
Annuler


stionnaire de serveur ‣ Serveur local
Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DESTINATION
dhcp.stadiumcompagny.com
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
Confirmation
Résultats
Afficher la progression de l'installation
Démarrage de l'installation
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils du serveur DHCP
Serveur DHCP
Exporter les paramètres de configuration
< Précédent
Suivant >
Installer
Annuler

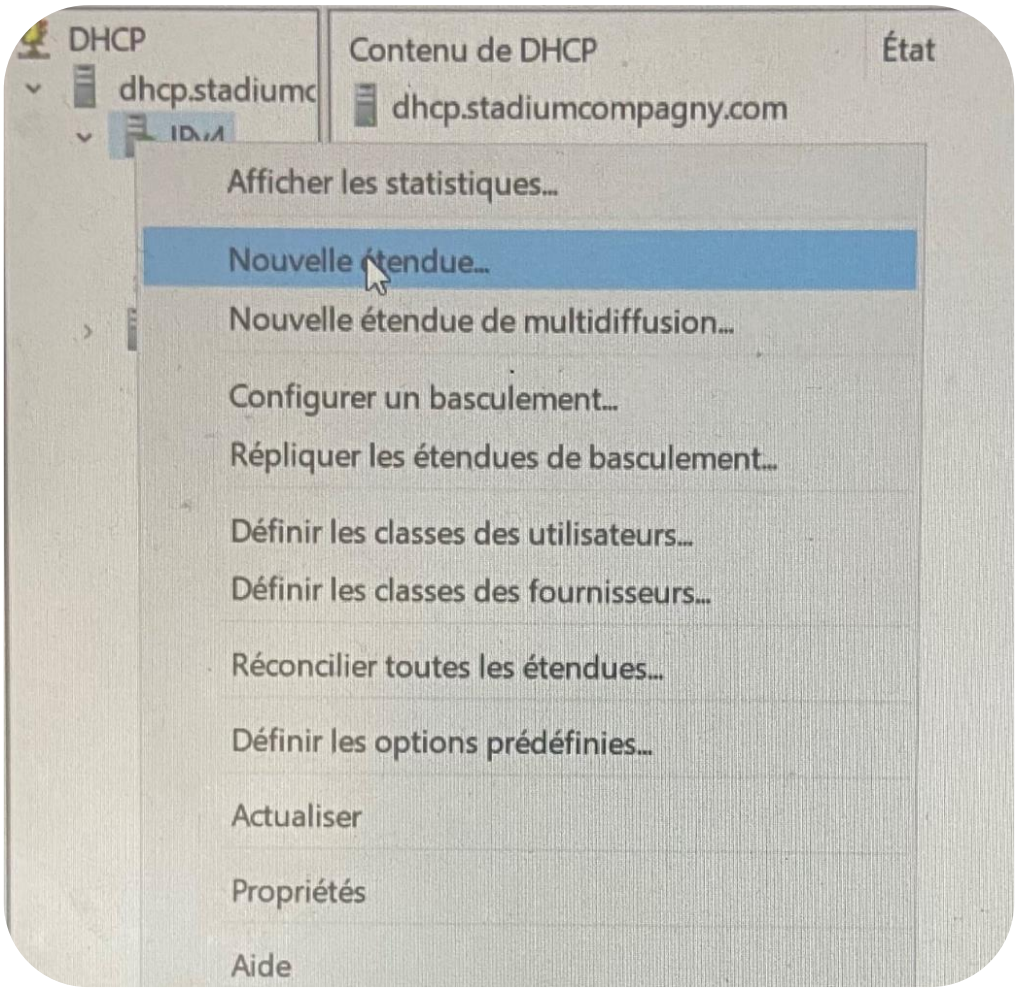

Progression de l'installation
SERVEUR DE DESTINATION
dhcp.stadiumcompagny.com
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
Confirmation
Résultats
Afficher la progression de l'installation
Installation de fonctionnalité
Configuration requise. Installation réussie sur dhcp.stadiumcompagny.com.
Serveur DHCP
Lancer l'Assistant Post-installation DHCP
Terminer la configuration DHCP
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils du serveur DHCP
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.
Exporter les paramètres de configuration
< Précédent
Suivant >
Fermer
Annuler


Résumé
Description
Autorisation
Résumé
L'état des étapes de configuration post-installation est indiqué ci-dessous :
Création des groupes de sécurité ..... Terminé
Redémarrez le service Serveur DHCP sur l'ordinateur cible pour que les groupes de sécurité soient effectifs.
< Précédent
Suivant >
Fermer
Annuler

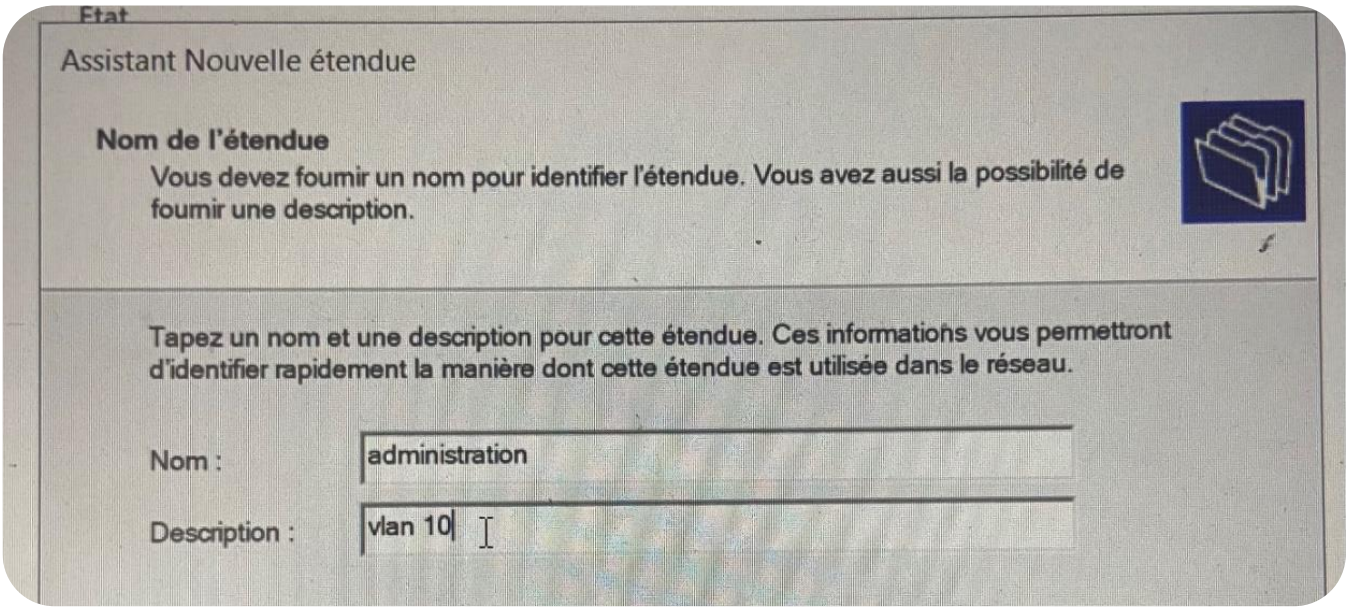
B) L'ajout d'étendues sur le service DHCP

- Le service DHCP étant installé sur le serveur Windows, nous allons à présent **ajouter les différentes étendues**.

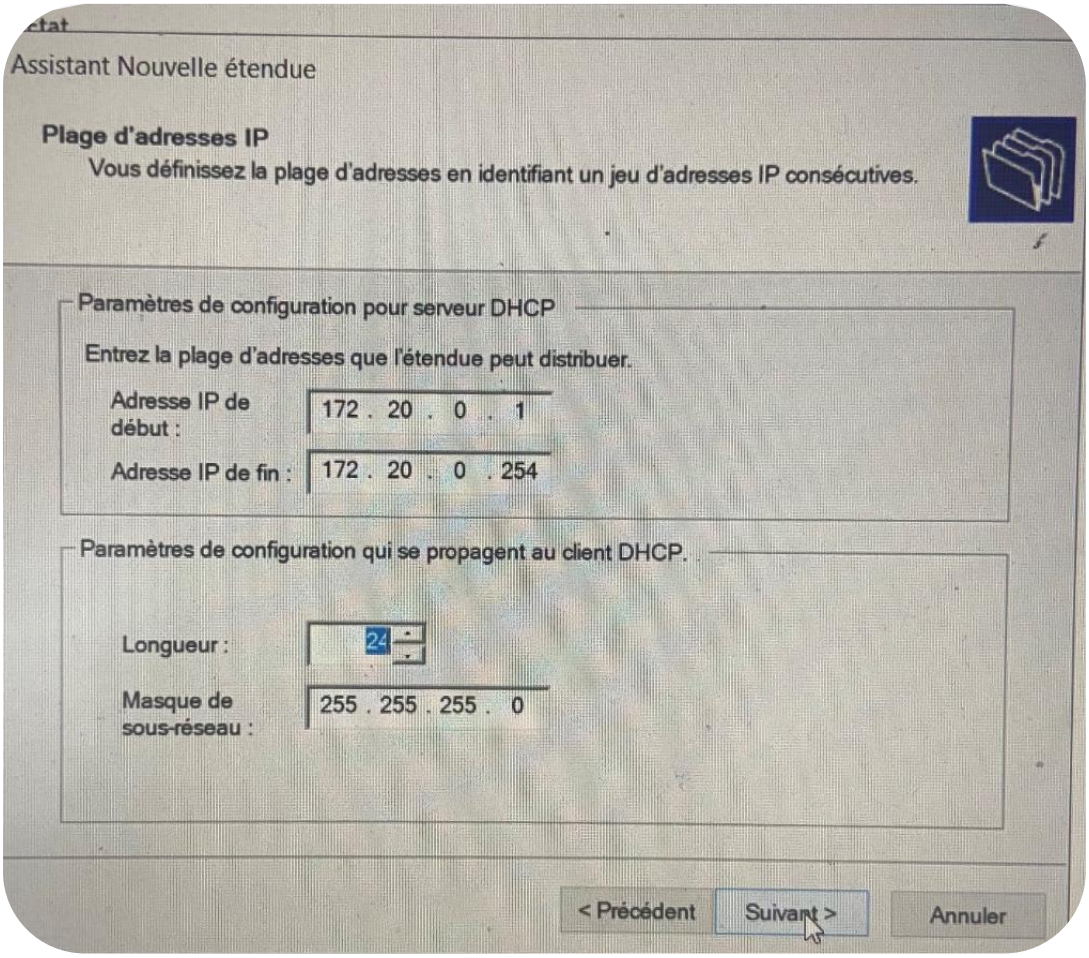
1) L'étendue administration



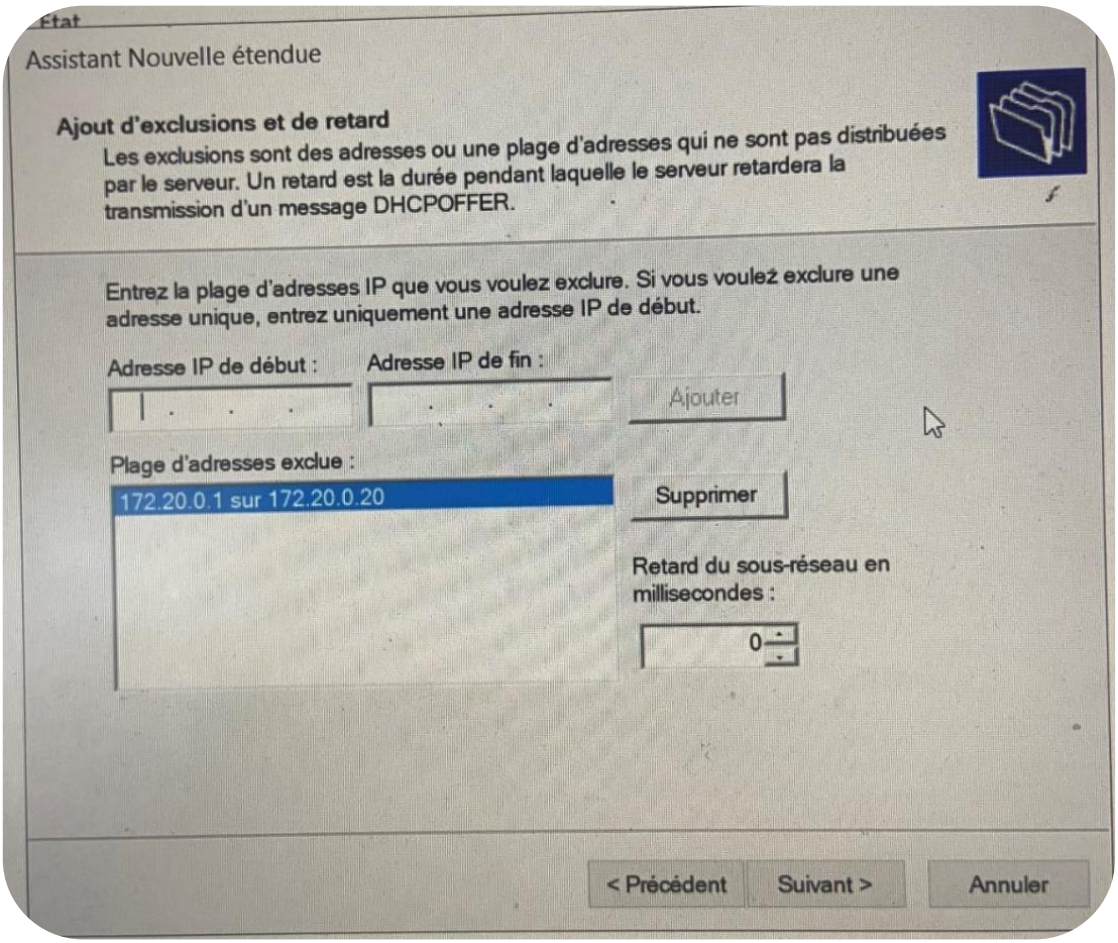
- Nous définissons **le nom de l'étendue** pour le VLAN 10 : administration.



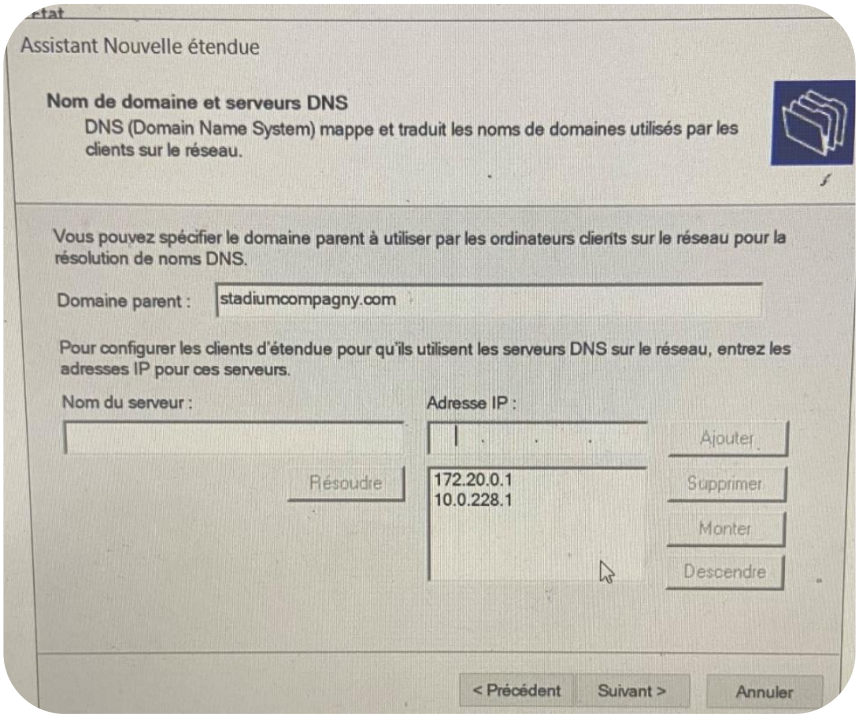
- Puis nous paramétrons **l'adressage** de notre service DHCP.



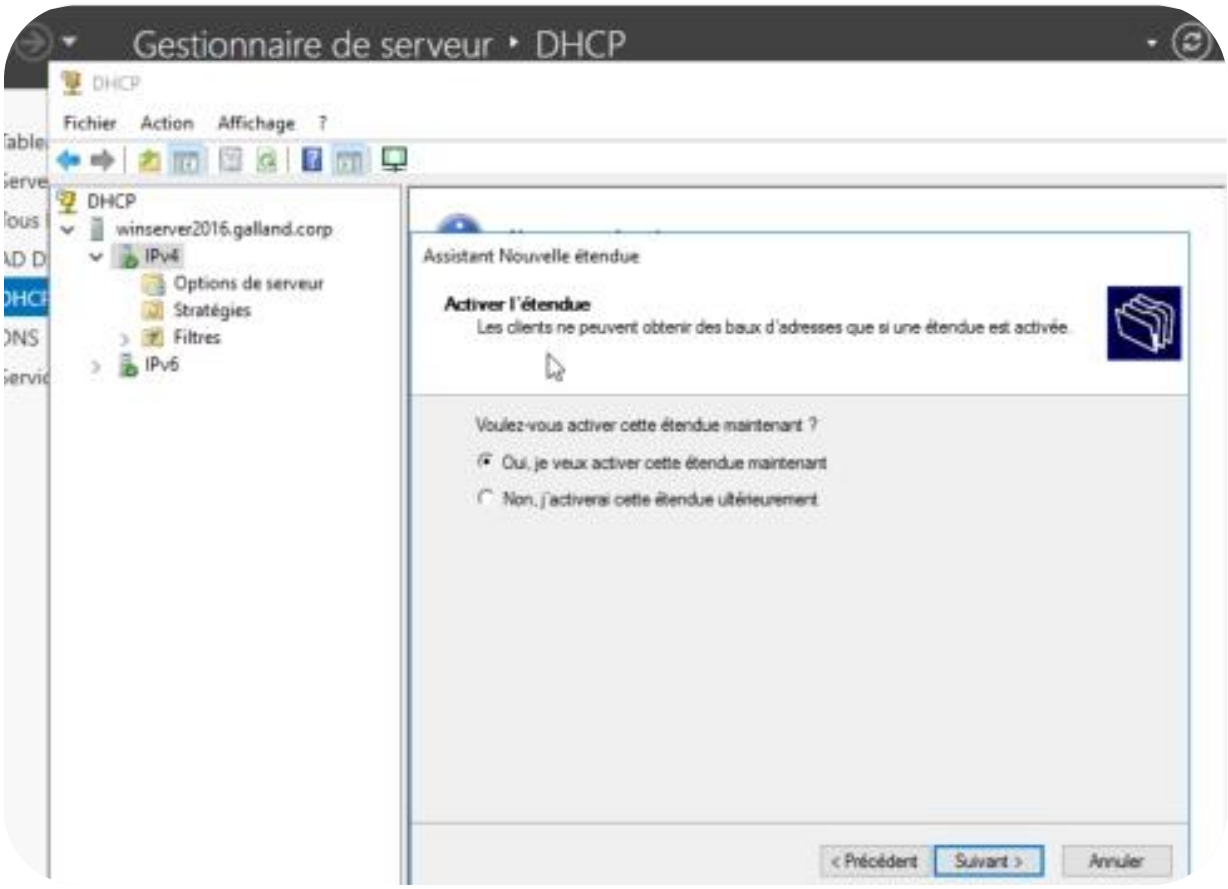
- Nous y ajoutons la plage d'adresses IP que **nous allons exclure**.



- Nous indiquons **le nom du domaine** et **les adresses DNS** pour pouvoir connecter les machines au réseau.

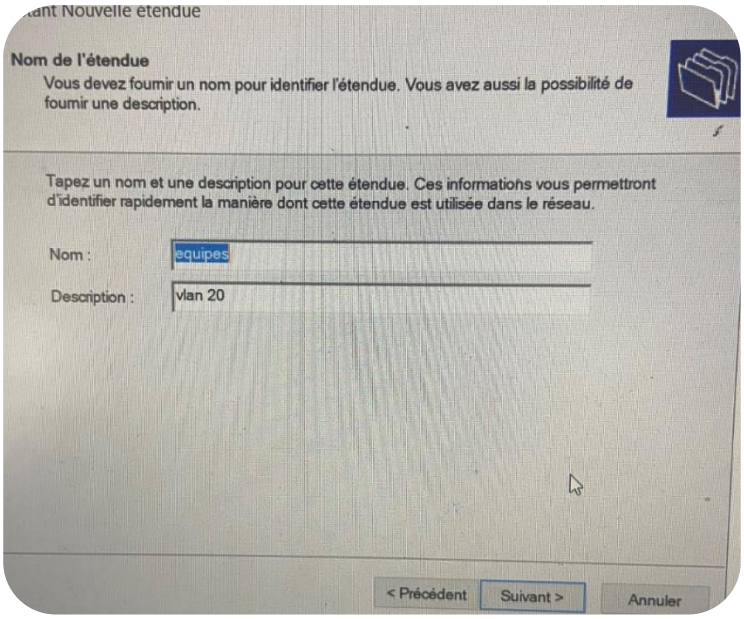


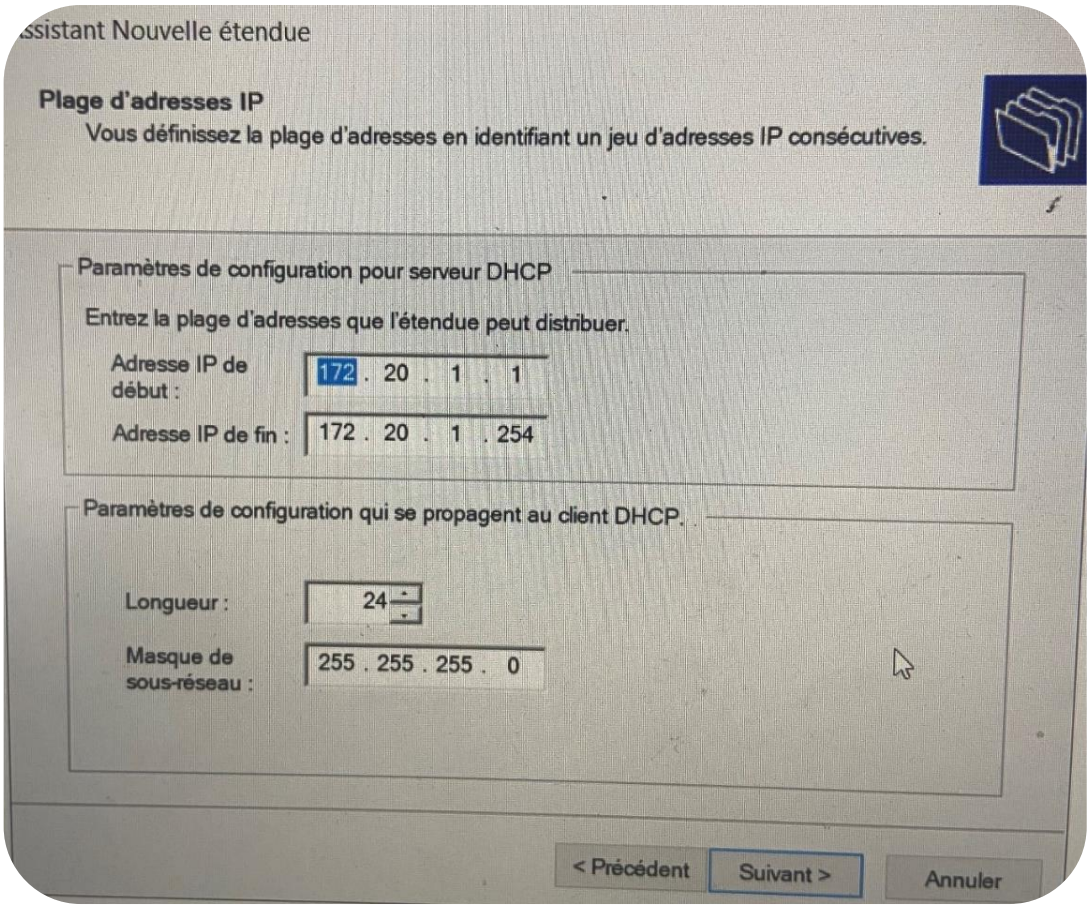
- Enfin, **nous activons l'étendue**.

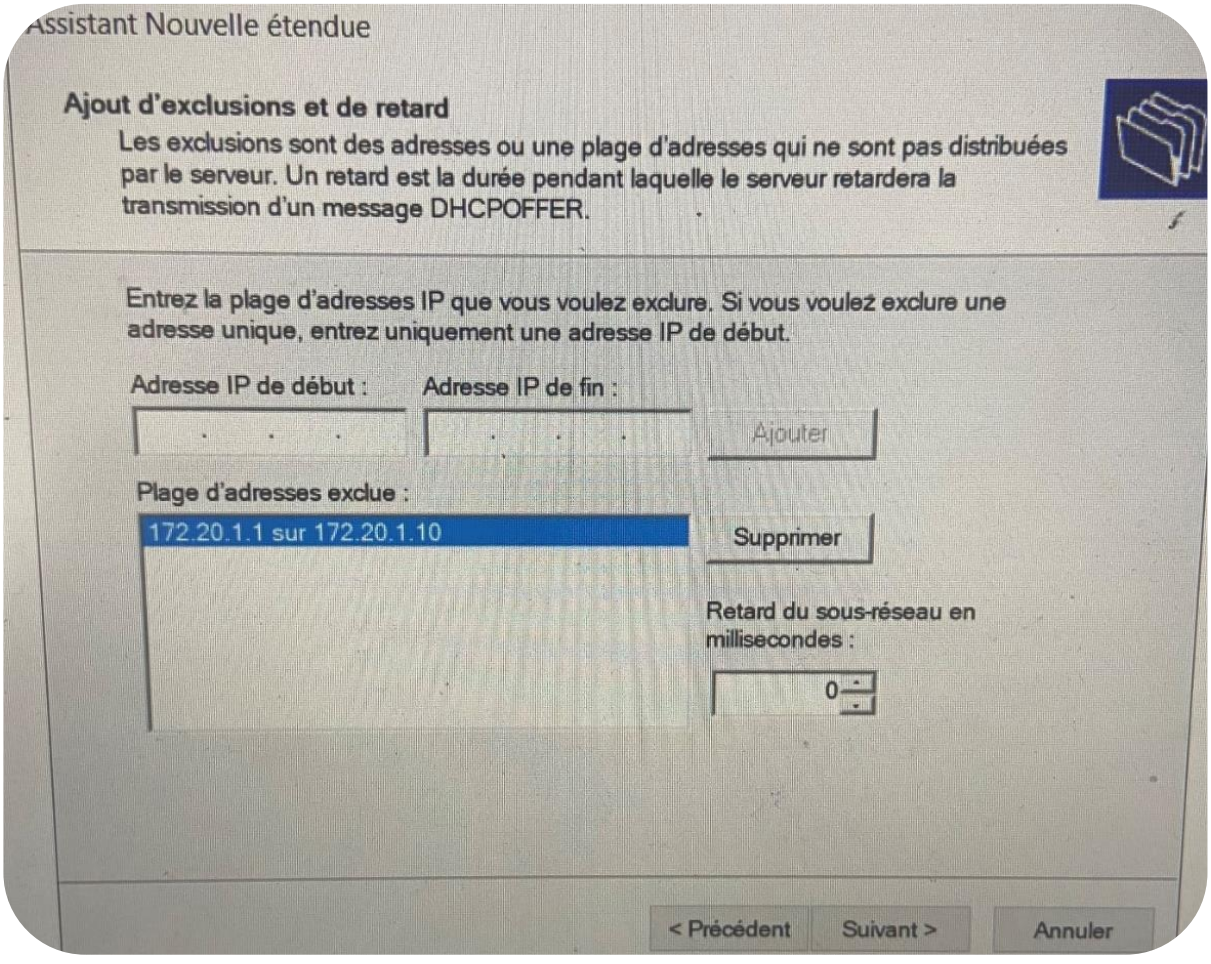


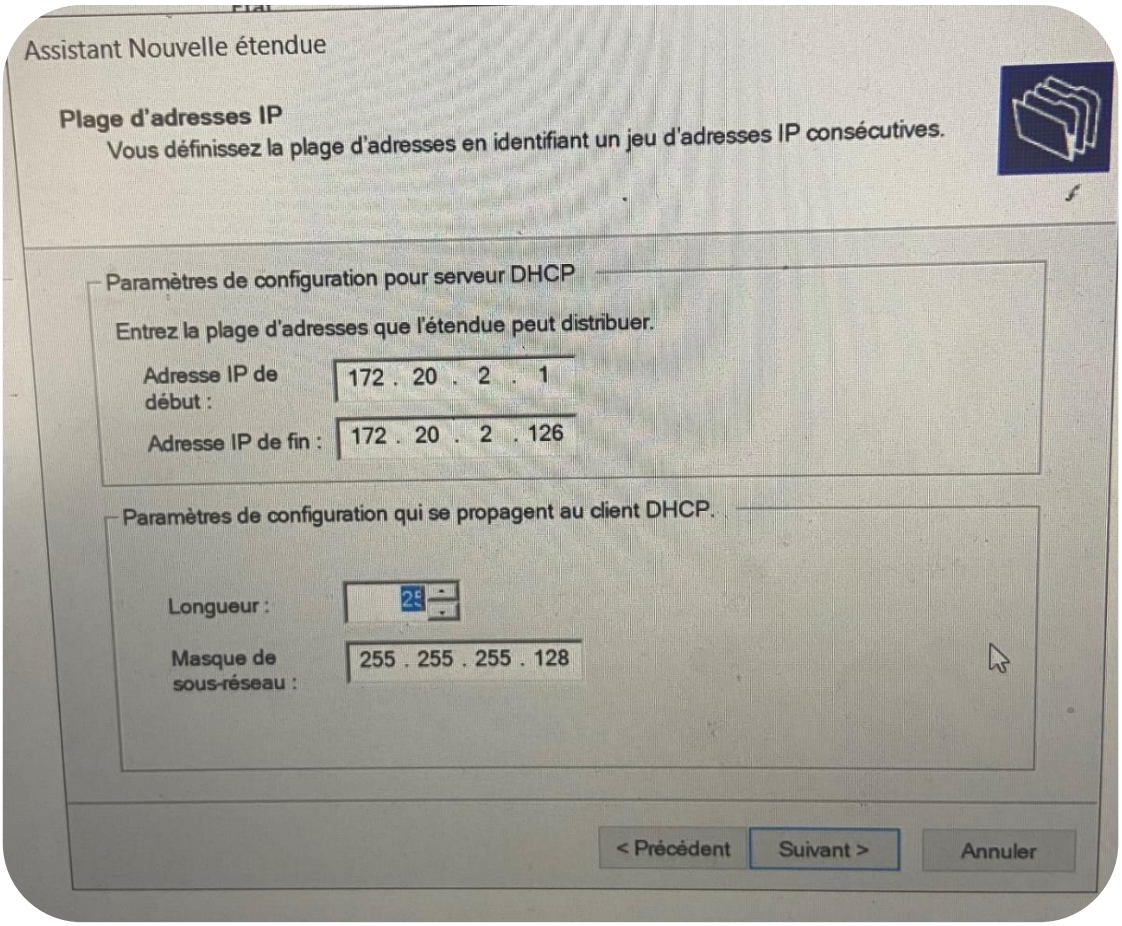
- Nous faisons **la même chose pour les deux autres étendues** : ici « Equipes ».

2) L’étendue equipes



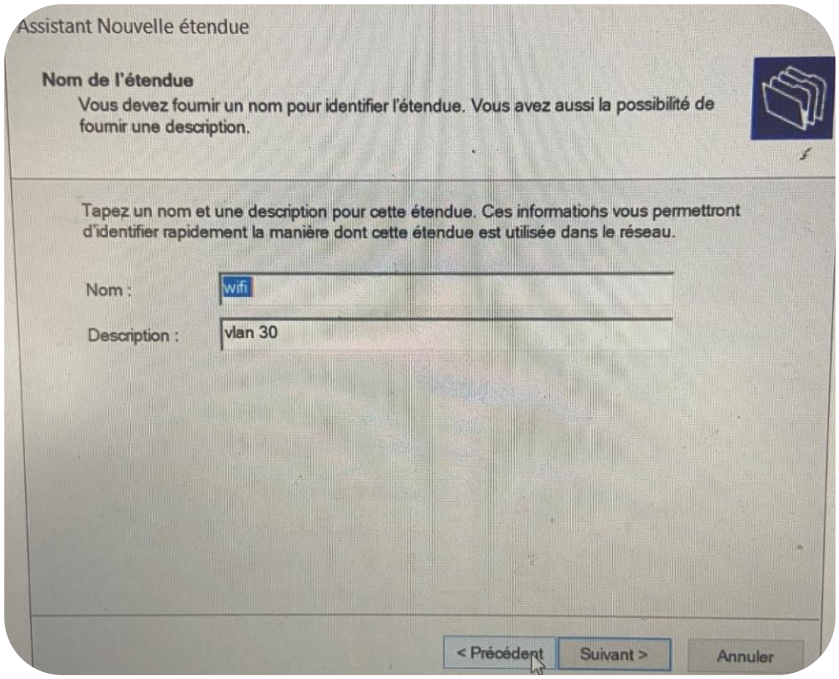

ssistant Nouvelle étendue
Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.
Paramètres de configuration pour serveur DHCP
Entrez la plage d'adresses que l'étendue peut distribuer.
Adresse IP de début :
172 . 20 . 1 . 1
Adresse IP de fin :
172 . 20 . 1 . 254
Paramètres de configuration qui se propagent au client DHCP.
Longueur :
24
Masque de sous-réseau :
255 . 255 . 255 . 0
< Précédent
Suivant >
Annuler

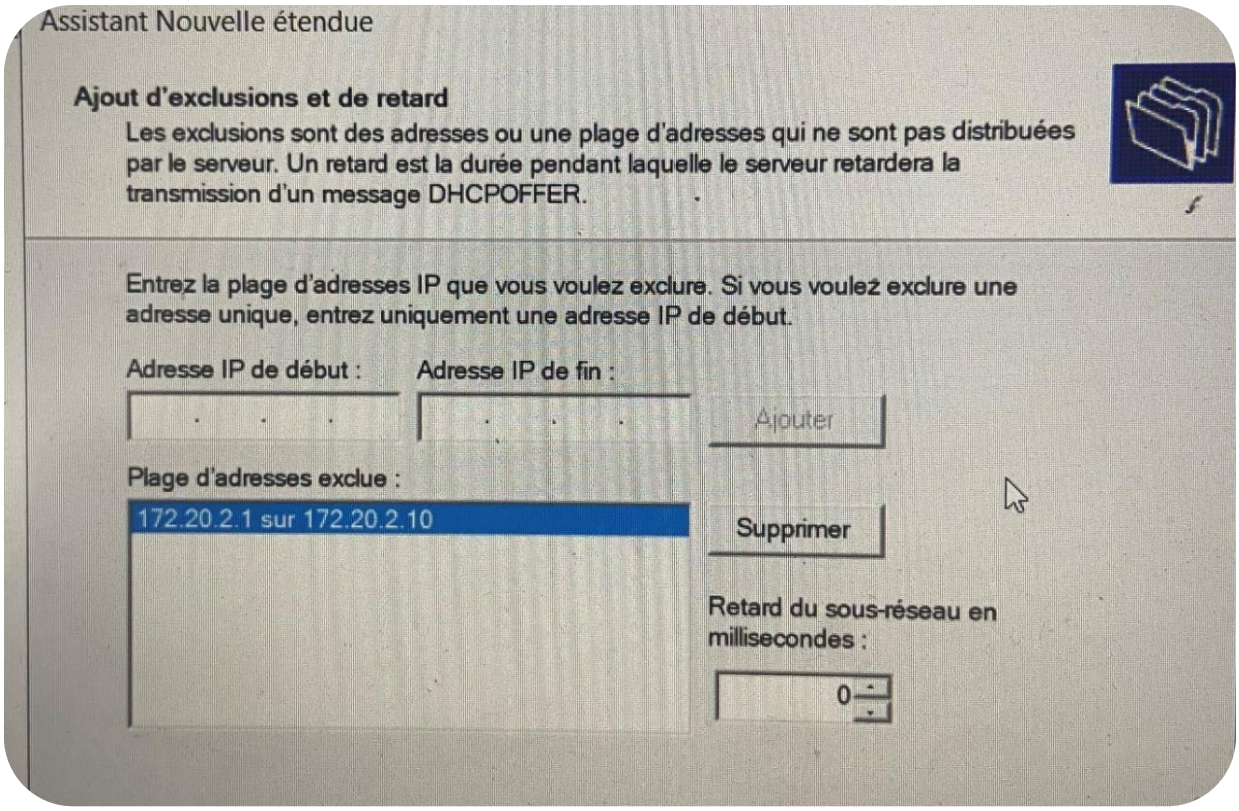

Assistant Nouvelle étendue
Ajout d'exclusions et de retard
Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCPOFFER.
Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.
Adresse IP de début :
Adresse IP de fin :
Ajouter
Plage d'adresses exclue :
172.20.1.1 sur 172.20.1.10
Supprimer
Retard du sous-réseau en millisecondes :
0
< Précédent
Suivant >
Annuler

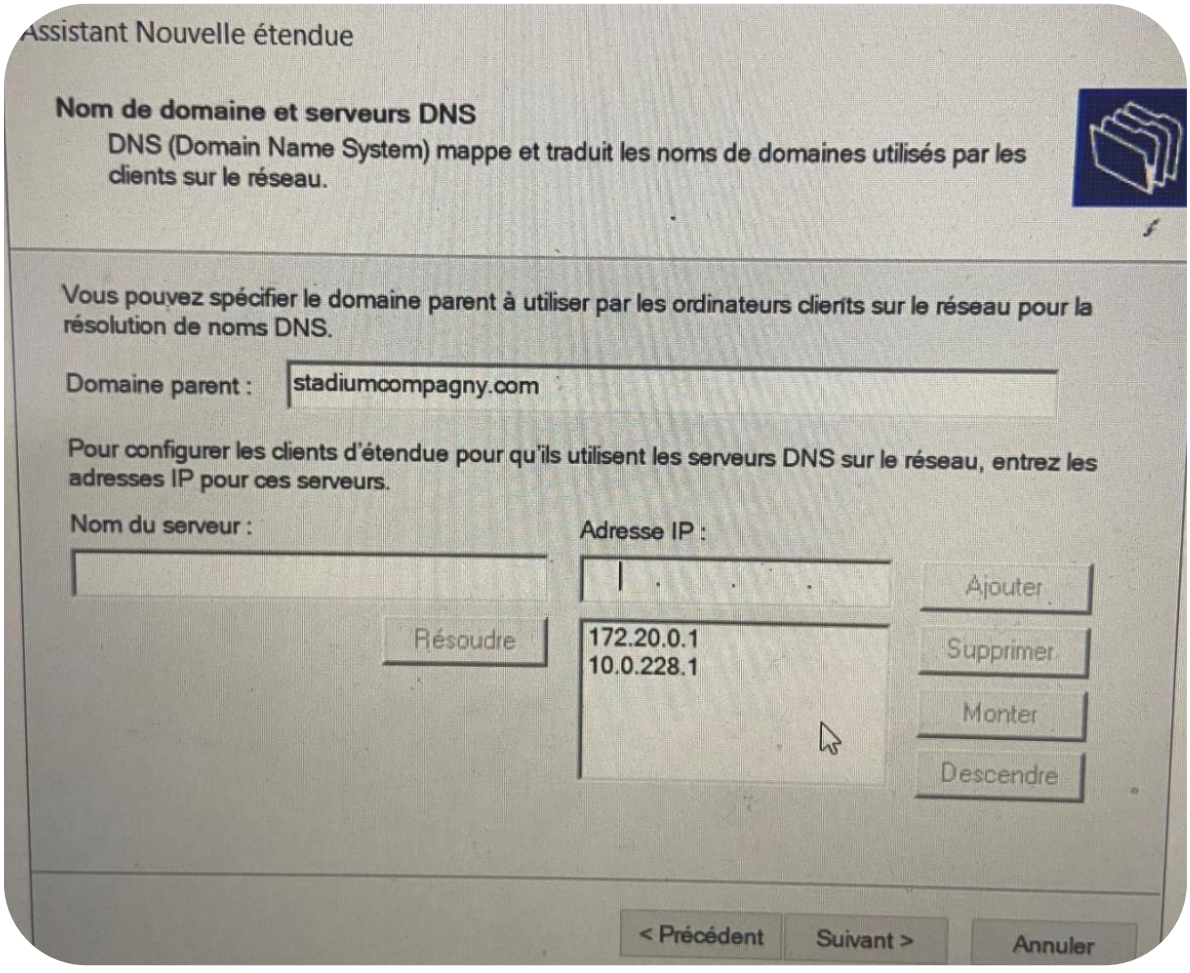


3) L'étendue WIFI

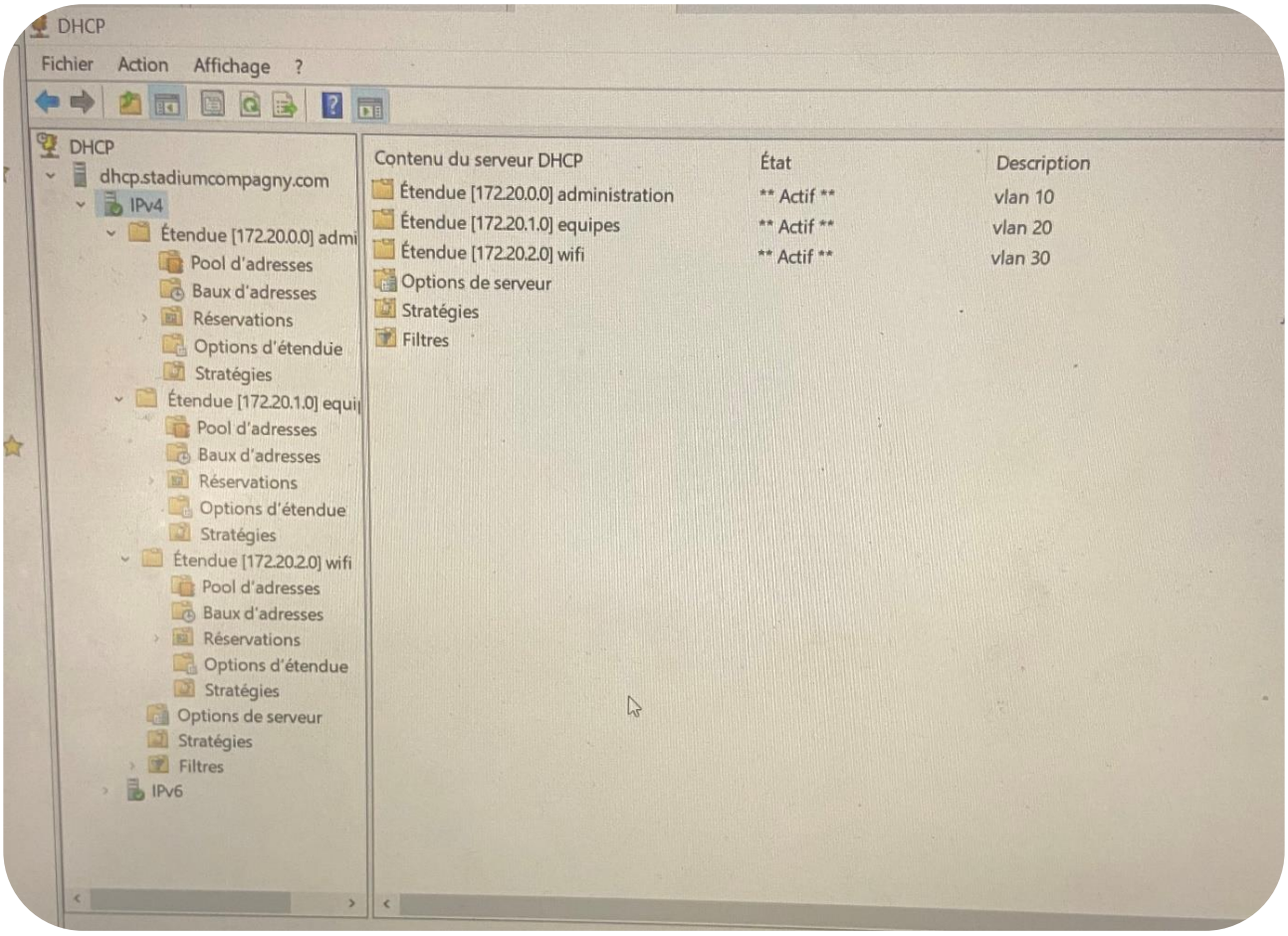
- Il nous reste à configurer **l'étendue Wifi**.

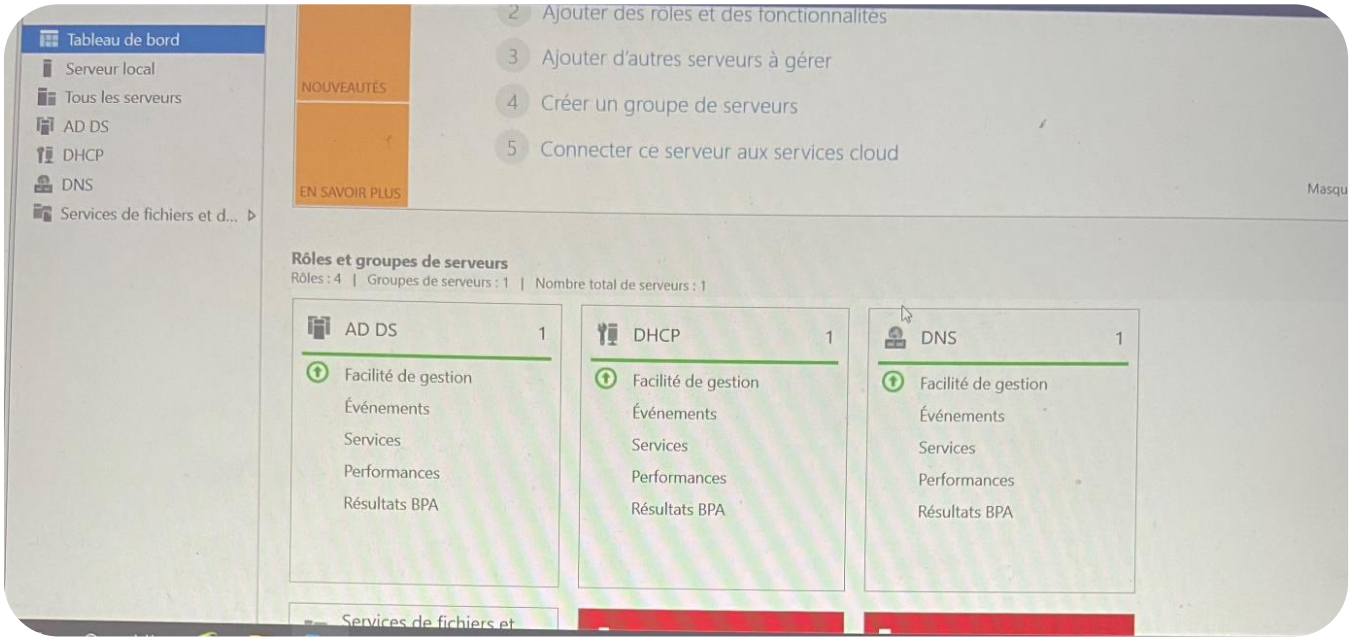



Assistant Nouvelle étendue
Ajout d'exclusions et de retard
Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCPOFFER.
Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.
Adresse IP de début :
Adresse IP de fin :
Ajouter
Plage d'adresses exclue :
172.20.2.1 sur 172.20.2.10
Supprimer
Retard du sous-réseau en millisecondes :
0


Assistant Nouvelle étendue
Nom de domaine et serveurs DNS
DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.
Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.
Domaine parent :
stadiumcompagny.com
Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.
Nom du serveur :
Adresse IP :
Ajouter
Résoudre
172.20.0.1
10.0.228.1
Supprimer
Monter
Descendre
< Précédent
Suivant >
Annuler

- Enfin, nous constatons bien **la présence des trois étendues** dans notre console DHCP.



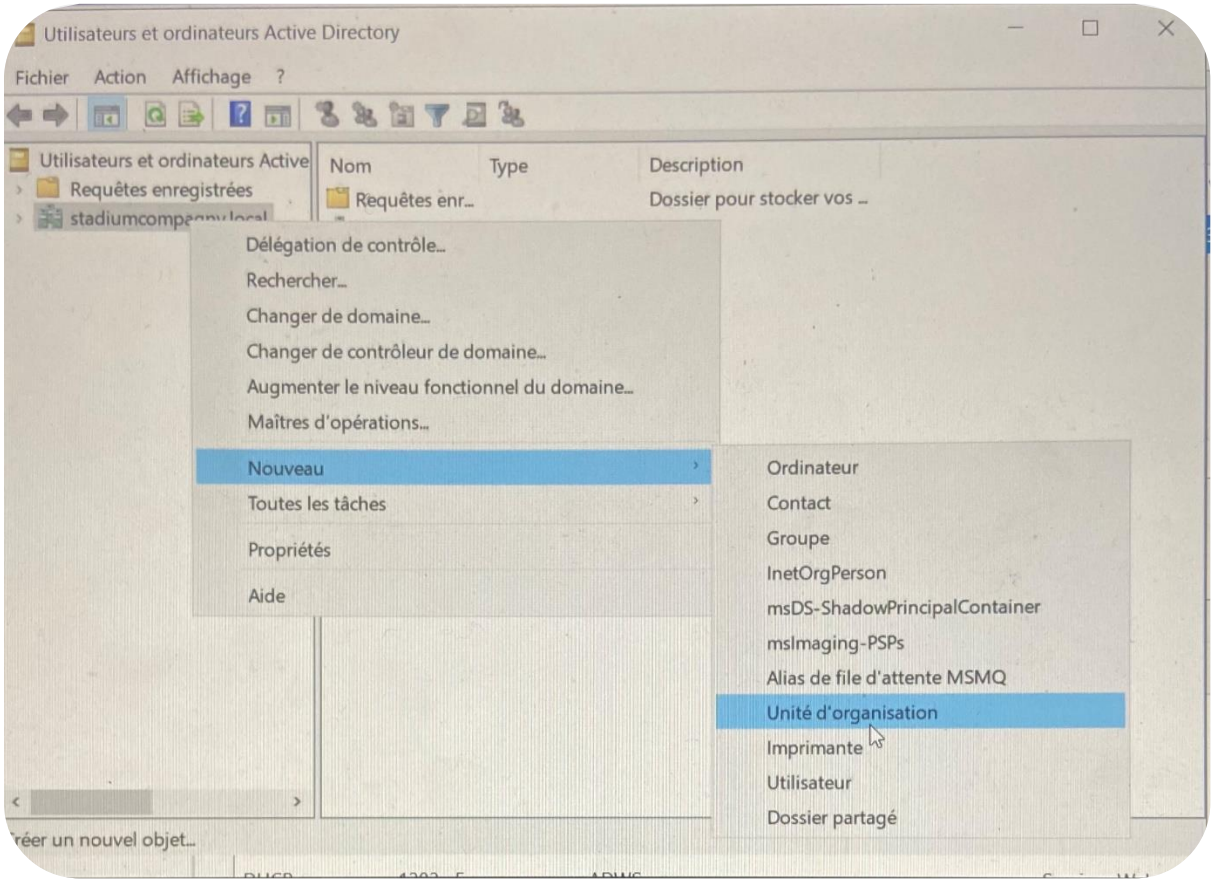


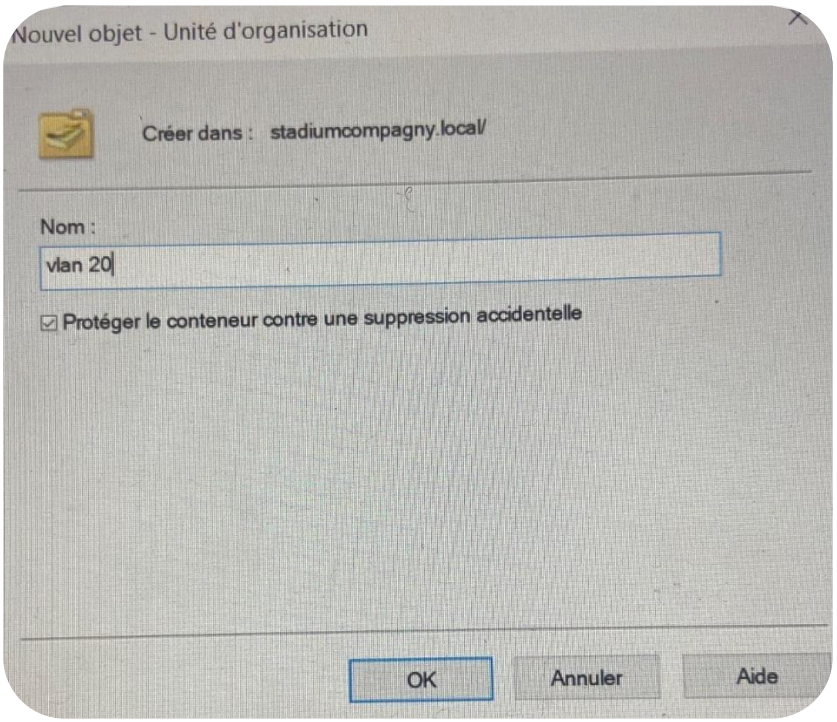
Ainsi, les services AD, DHCP et DNS sont correctement installés.

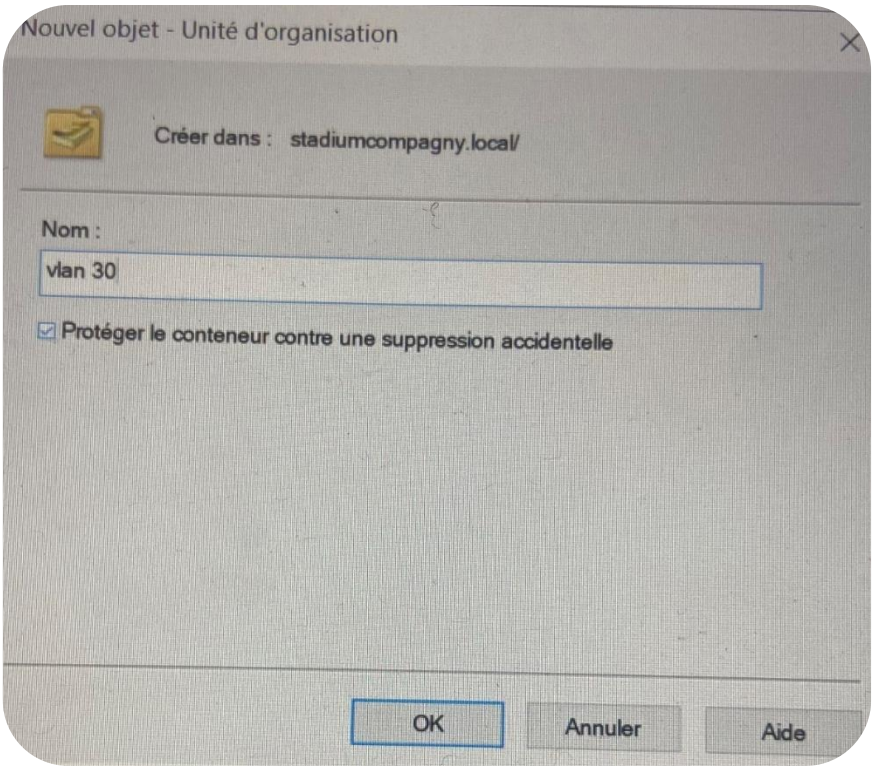
Paragraphe 5 : La création des unités d'organisation

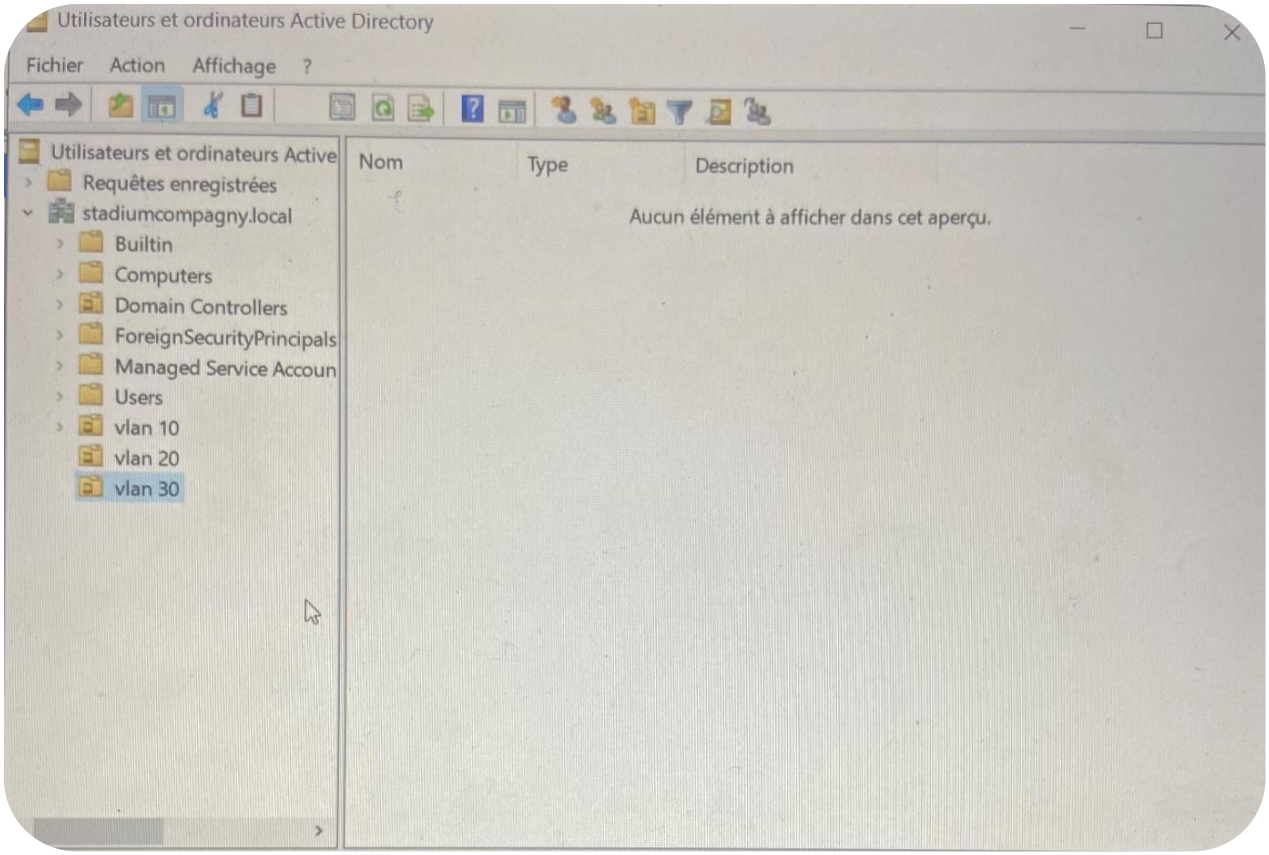
A) La création des unités d'organisation

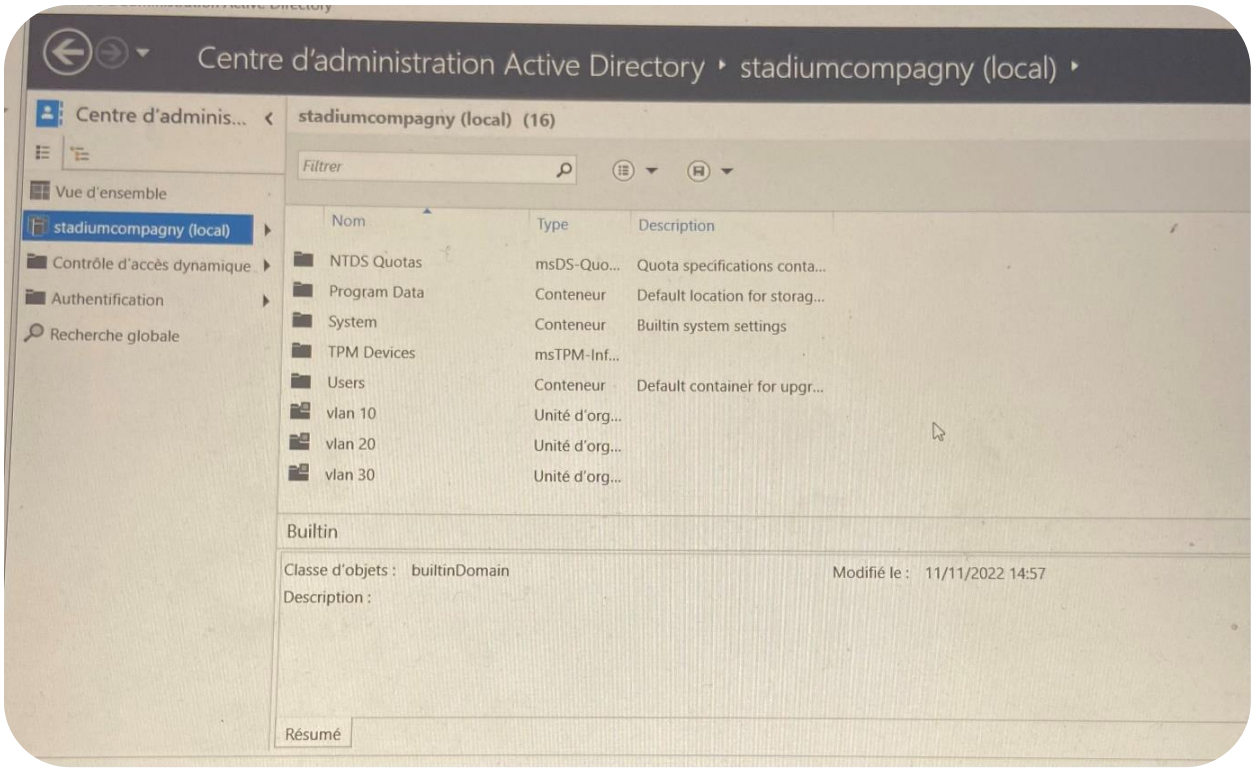
- Nous allons créer une **nouvelle unité d'organisation** qui correspond aux VLANs





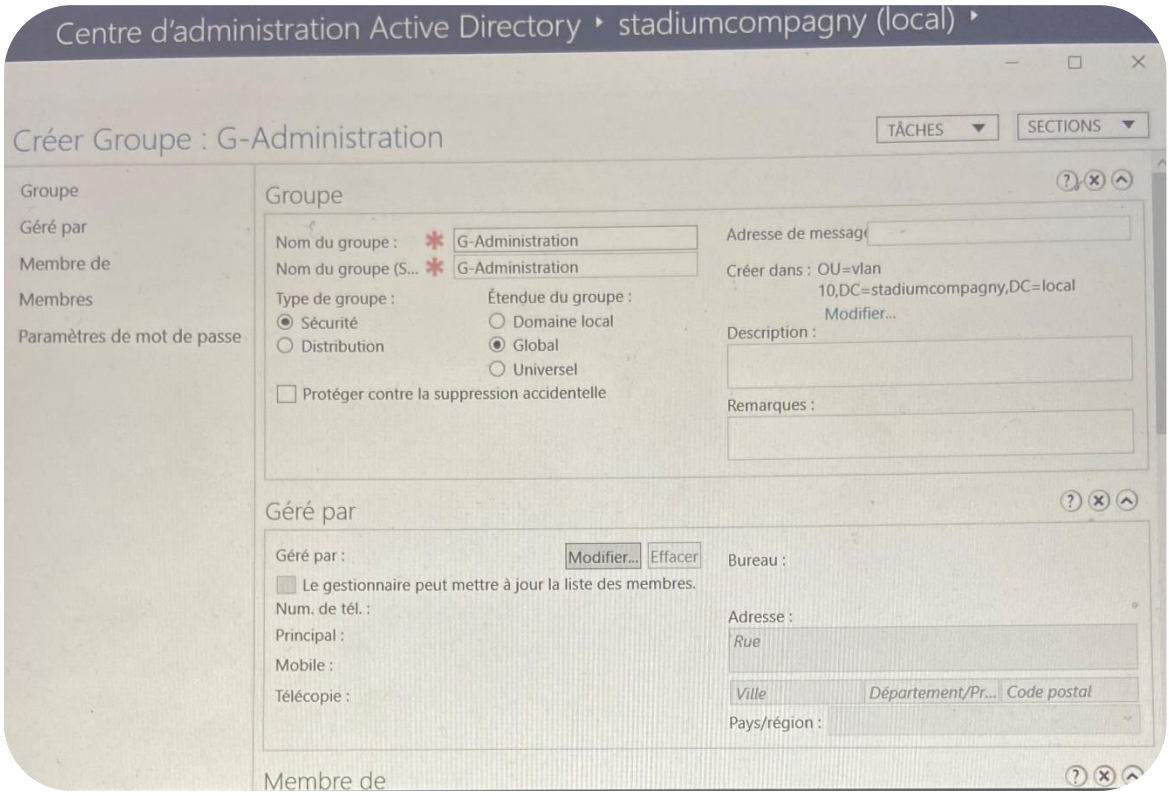

Nouvel objet - Unité d'organisation
Créer dans : stadiumcompagny.local/
Nom :
vlan 30
Protéger le conteneur contre une suppression accidentelle
OK
Annuler
Aide

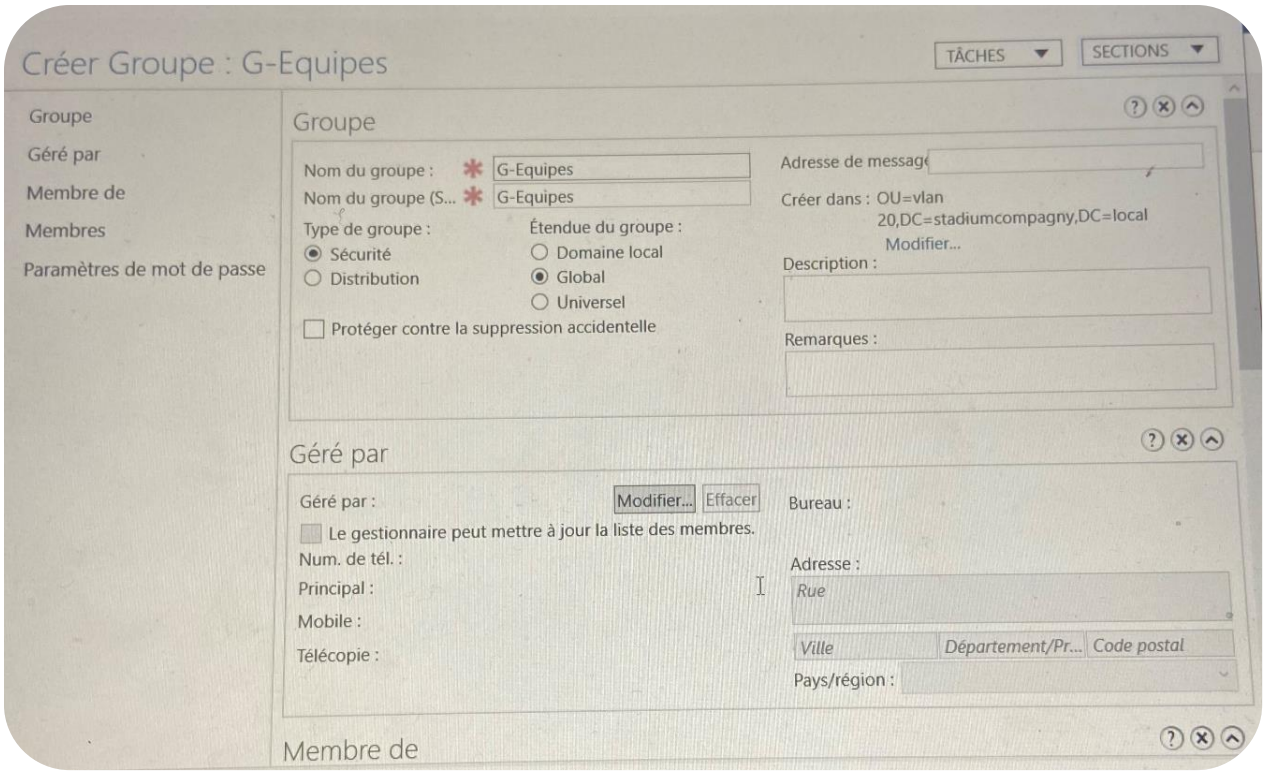

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
stadiumcompagny.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accoun
Users
vlan 10
vlan 20
vlan 30
Nom
Type
Description
Aucun élément à afficher dans cet aperçu.

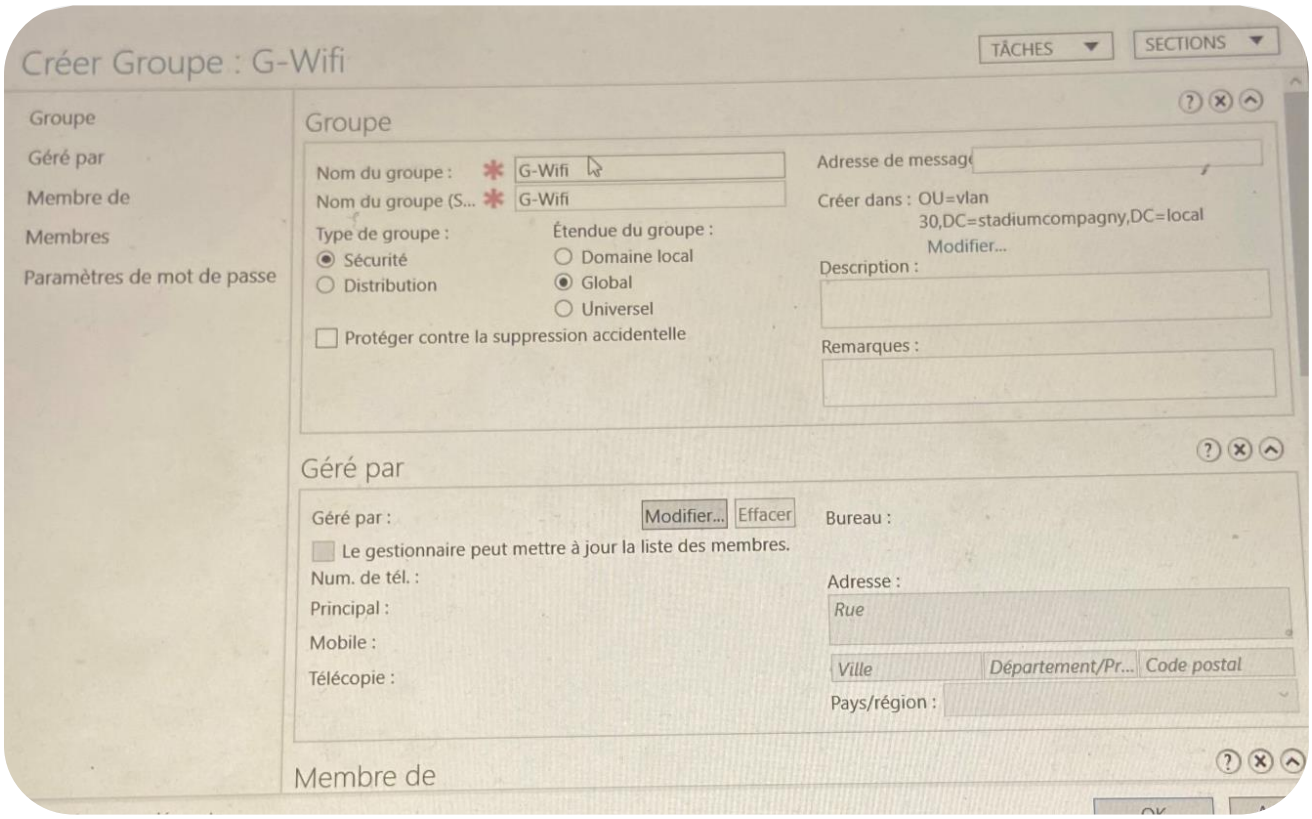


B) La création des groupes

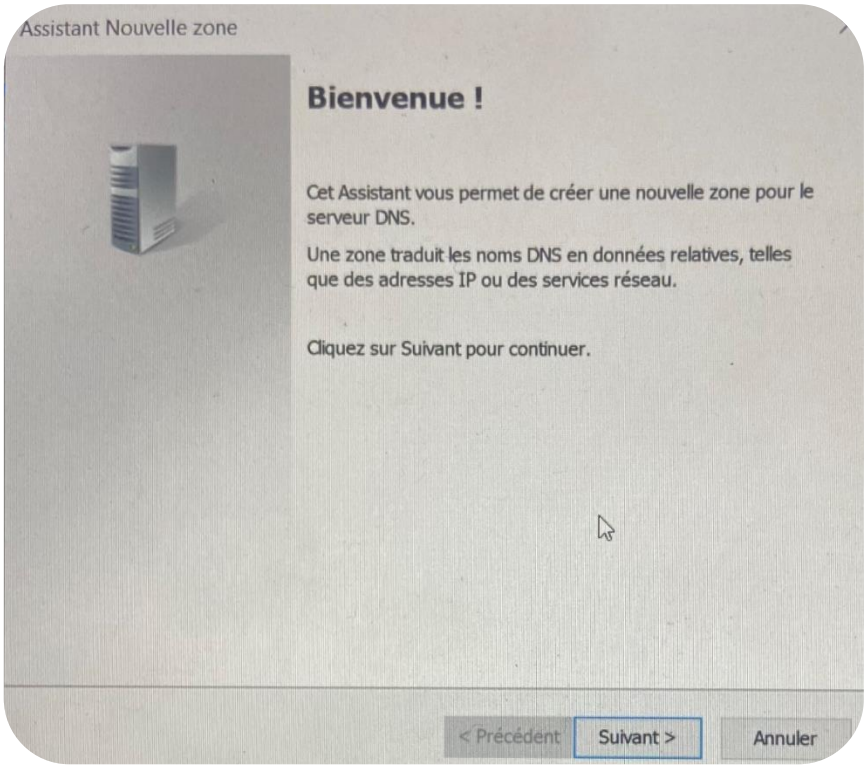
- **Chaque UO contient les utilisateurs du service concerné**, un groupe d'utilisateurs dont le nom est au format G_xxxx où xxxx=le nom du service.

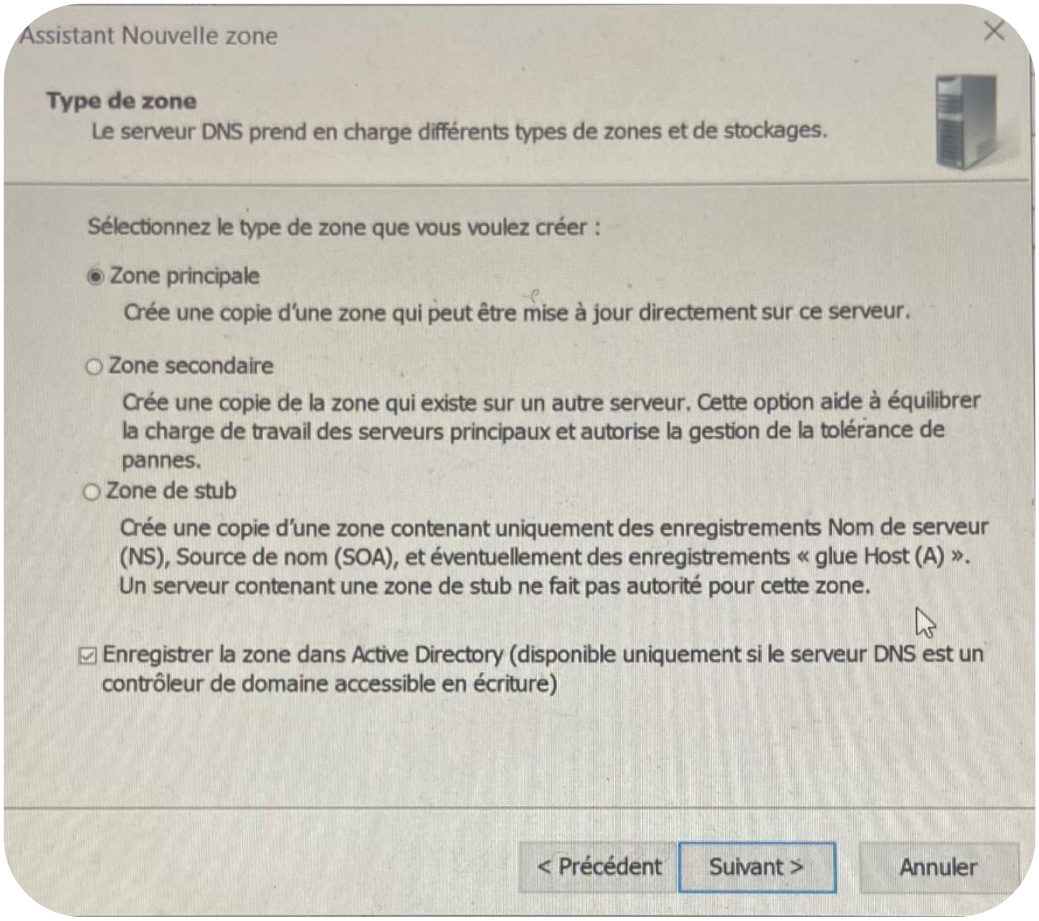


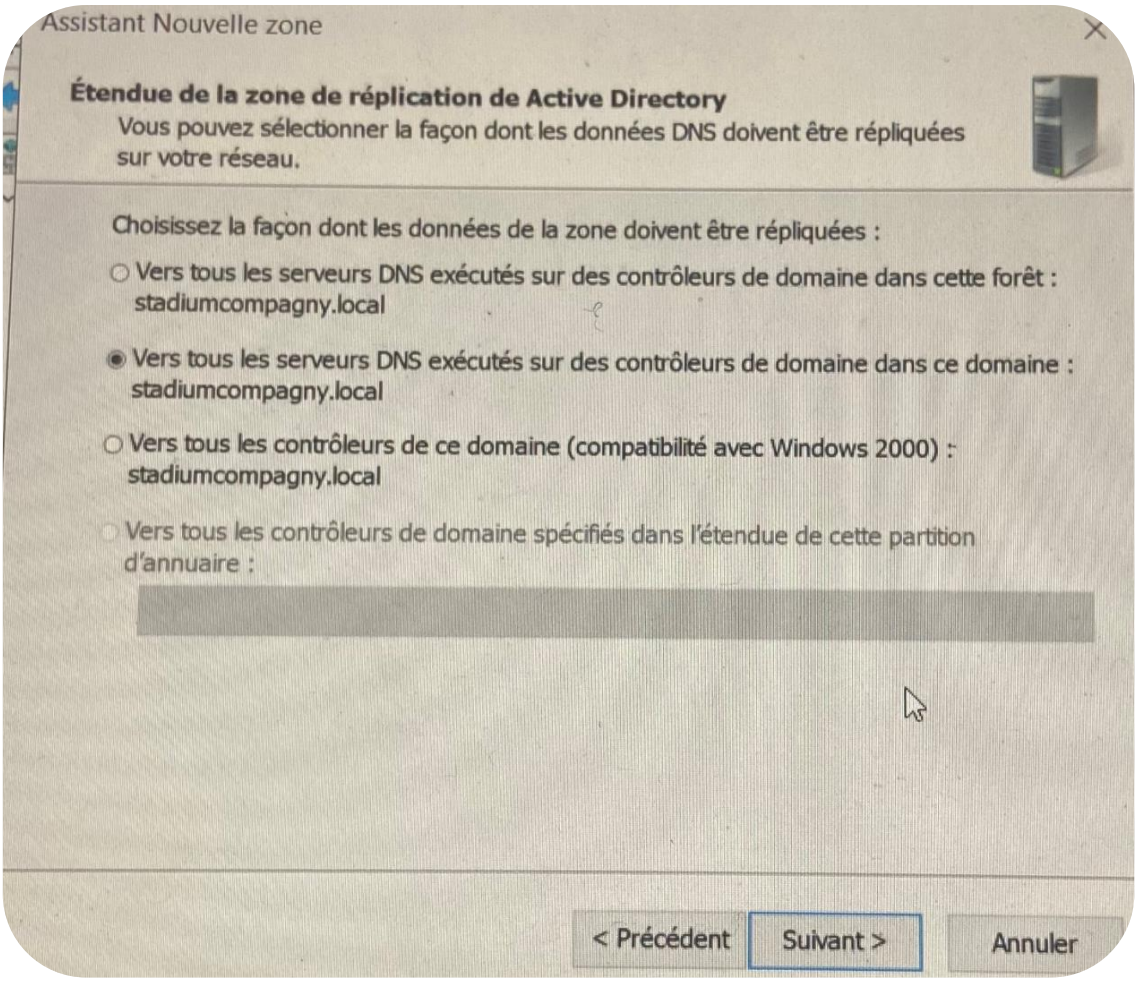

Créer Groupe : G-Equipes
TÂCHES
SECTIONS
Groupe
Géré par
Membre de
Membres
Paramètres de mot de passe
Groupe
Nom du groupe : G-Equipes
Nom du groupe (S... G-Equipes
Type de groupe :
Sécurité
Distribution
Étendue du groupe :
Domaine local
Global
Universel
Protéger contre la suppression accidentelle
Adresse de messag
Créer dans : OU=vlan
20,DC=stadiumcompagny,DC=local
Modifier...
Description :
Remarques :
Géré par
Géré par :
Modifier...
Effacer
Le gestionnaire peut mettre à jour la liste des membres.
Num. de tél. :
Principal :
Mobile :
Télécopie :
Bureau :
Adresse :
Rue
Ville
Département/Pr...
Code postal
Pays/région :
Membre de

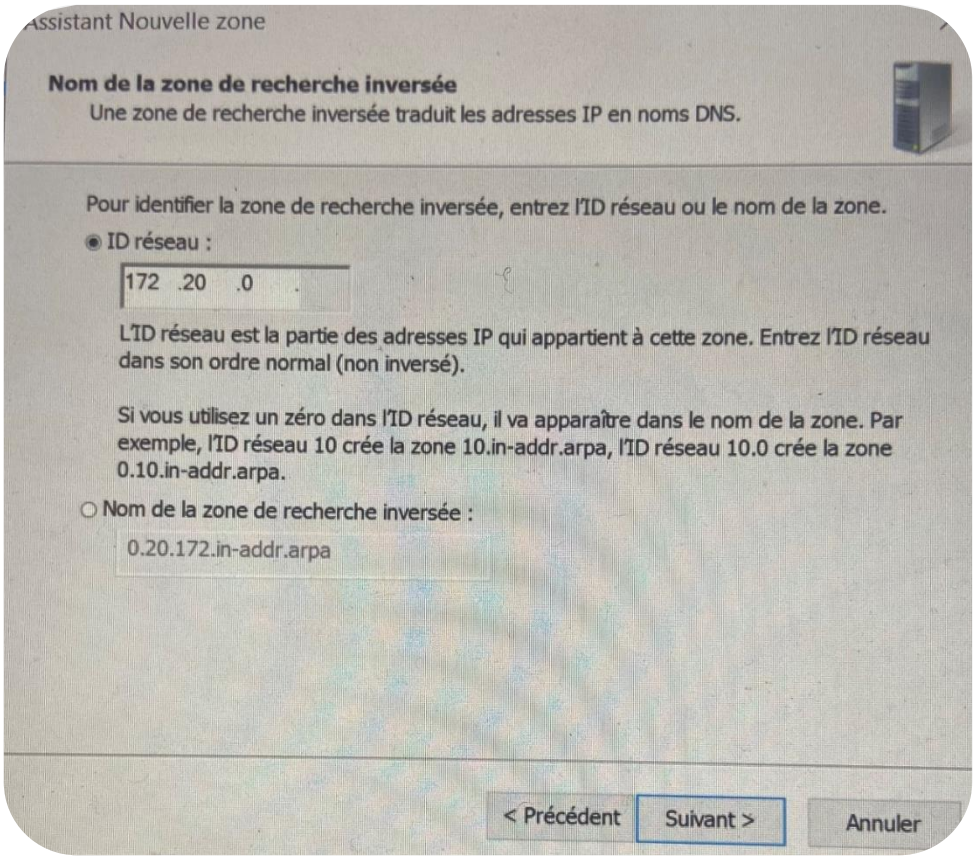

Créer Groupe : G-Wifi
TÂCHES
SECTIONS
Groupe
Géré par
Membre de
Membres
Paramètres de mot de passe
Groupe
Nom du groupe : G-Wifi
Nom du groupe (S... G-Wifi
Type de groupe :
Sécurité
Distribution
Étendue du groupe :
Domaine local
Global
Universel
Protéger contre la suppression accidentelle
Adresse de messag
Créer dans : OU=vlan
30,DC=stadiumcompagny,DC=local
Modifier...
Description :
Remarques :
Géré par
Géré par :
Modifier...
Effacer
Le gestionnaire peut mettre à jour la liste des membres.
Num. de tél. :
Principal :
Mobile :
Télécopie :
Bureau :
Adresse :
Rue
Ville
Département/Pr...
Code postal
Pays/région :
Membre de

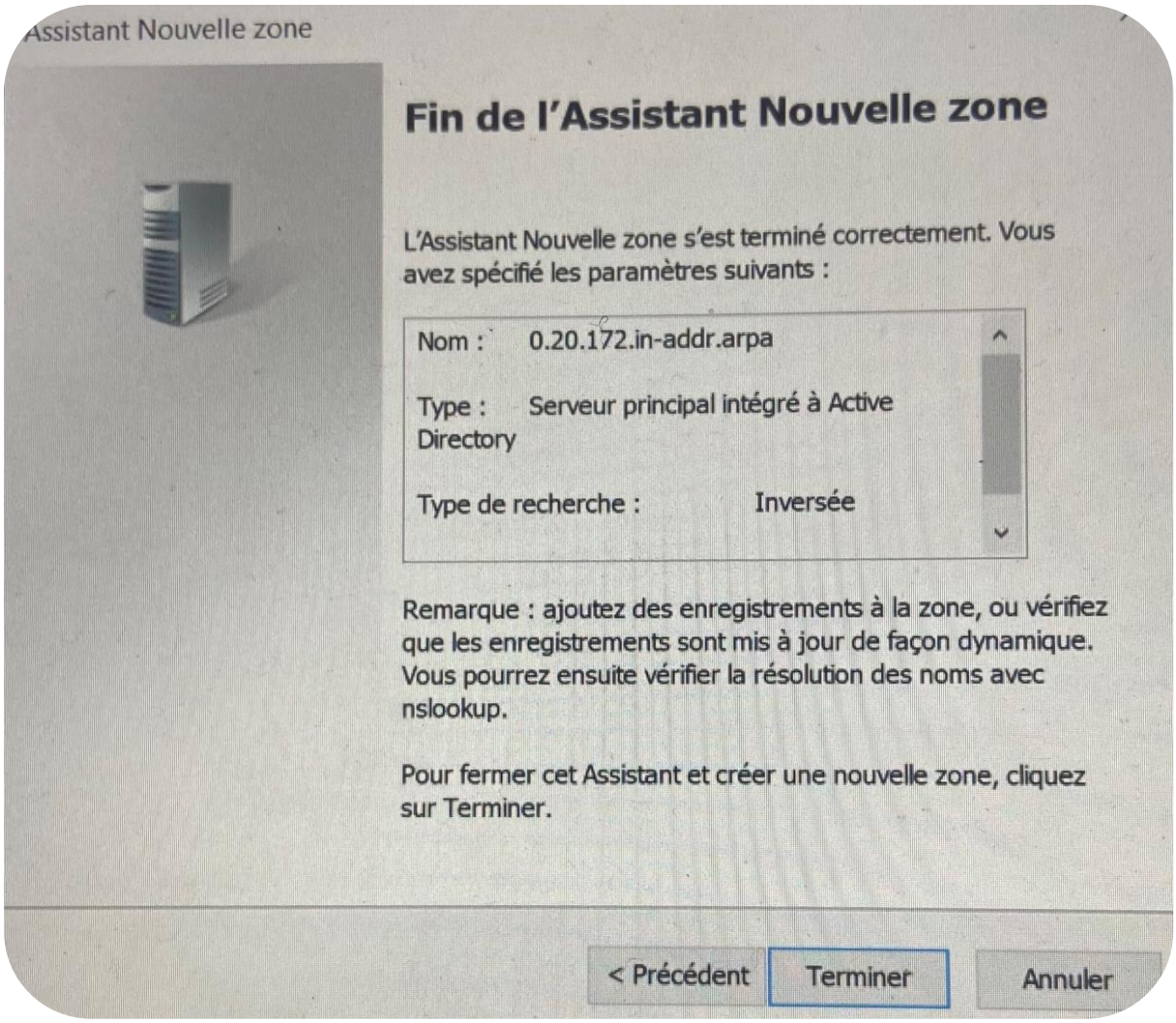
C) La configuration de la zone de réplication d'Active Directory






Assistant Nouvelle zone
Étendue de la zone de réplication de Active Directory
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.
Choisissez la façon dont les données de la zone doivent être répliquées :
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : stadiumcompagny.local
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : stadiumcompagny.local
Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : stadiumcompagny.local
Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :
< Précédent
Suivant >
Annuler


Assistant Nouvelle zone
Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.
Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.
ID réseau :
172 .20 .0
L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).
Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.
Nom de la zone de recherche inversée :
0.20.172.in-addr.arpa
< Précédent
Suivant >
Annuler


Assistant Nouvelle zone
Fin de l'Assistant Nouvelle zone
L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :
Nom : 0.20.172.in-addr.arpa
Type : Serveur principal intégré à Active Directory
Type de recherche : Inversée
Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.
Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.
< Précédent
Terminer
Annuler

Mission 3 : Sécurisation des communications entre sites

Paragraphe 1 : Test et comparaison des solutions

A) Accès à distance

1) SSH et son fonctionnement

SSH :
Il s'agit d'un protocole permettant à un client d'ouvrir une session interactive sur une machine distante afin d'envoyer des commandes ou des fichiers de manière sécurisée :

- Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité. Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être.

SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. À ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou open source.

Fonctionnement :
L'établissement d'une connexion SSH se fait en plusieurs étapes :

- Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé.

- Dans un second temps le client s'authentifie auprès du serveur pour obtenir une session.

L'authentification :

Une fois que la connexion sécurisée est mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès. Il existe plusieurs méthodes :

- la méthode la plus connue est le traditionnel mot de passe. Le client envoie un nom d'utilisateur et un mot de passe au serveur au travers de la communication sécurisée et le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide

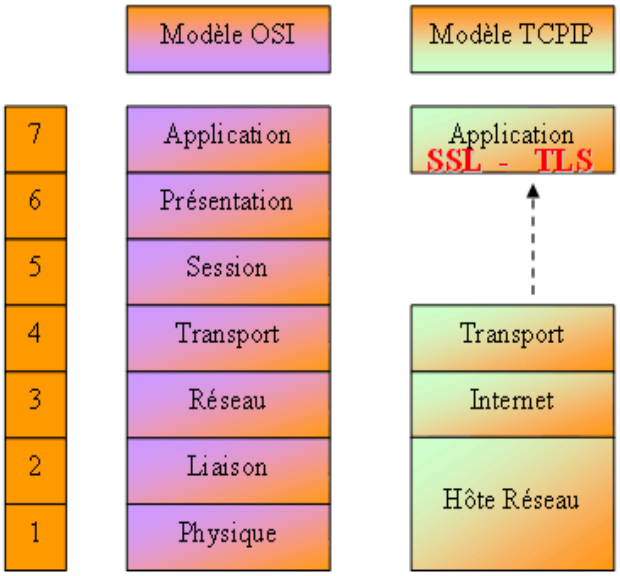
- une méthode moins connue mais plus souple est l'utilisation de clés publiques. Si l'authentification par clé est choisie par le client, le serveur va créer un challenge et donner un accès au client si ce dernier parvient à déchiffrer le challenge avec sa clé privée

2) SSL et TLS fonctionnement et Implémentation

Positionnement SSL :

SSL signifie Secure Sockets Layer et son équivalent actuel TLS signifie Transport Secured Layer. Ils sont tous les deux des protocoles situés entre le niveau Transport et Application. Ainsi, on retrouve leur positionnement sur le schéma suivant représentant le modèle OSI et TCP/IP.

Positionnement de SSL et TLS



SSL et TLS se comportent en effet comme une couche intermédiaire supplémentaire, car ils sont indépendants du protocole utilisé au niveau application. Cela signifie donc qu'il peut aussi bien être employé pour sécuriser une transaction web, l'envoi ou la réception d'email, etc. SSL et TLS sont donc transparents pour l'utilisateur et ne nécessitent pas l'emploi de protocoles de niveau Application spécifiques.

Fonctionnalité SSL :

- Authentification : Le client doit pouvoir s'assurer de l'identité du serveur. Depuis SSL 3.0, le serveur peut aussi demander au client de s'authentifier. Cette fonctionnalité est assurée par l'emploi de certificats.

- Confidentialité : Le client et le serveur doivent avoir l'assurance que leur conversation ne pourra pas être écoutée par un tiers. Cette fonctionnalité est assurée par un algorithme de chiffrement.

- Identification et intégrité : Le client et le serveur doivent pouvoir s'assurer que les messages transmis ne sont ni tronqués ni modifiés (intégrité), qu'ils proviennent bien de l'expéditeur attendu. Ces fonctionnalités sont assurées par la signature des données.

SSL et TLS reposent donc sur la combinaison de plusieurs concepts cryptographiques, exploitant à la fois le chiffrement asymétrique et le chiffrement symétrique.

SSL et TLS se veulent en outre évolutifs, puisque le protocole est indépendant des algorithmes de cryptage et d'authentification mis en œuvre dans une transaction. Cela lui permet de s'adapter aux besoins des utilisateurs et aux législations en vigueur. Cela assure de plus une meilleure sécurité, puisque le protocole n'est pas soumis aux évolutions théoriques de la cryptographie.

Fonctionnement :

Le protocole SSL et TLS se décompose en deux couches principales (quatre en réalité) :

- SSL et TLS Handshake Protocol choisissent la version de SSL et TLS qui sera utilisée, réalise l'authentification par l'échange de certificats et permet la négociation entre le client et le serveur d'un niveau de sécurité au travers du choix des algorithmes de cryptage. C'est le protocole de configuration de la transaction.

- SSL et TLS Record Protocol encapsule et fragmente les données. C'est le protocole de transmission des données. Dans une première phase, le client et le serveur vont effectuer la négociation an de configurer la transaction et d'échanger les clés de chiffrement. Puis ils effectueront l'échange de données proprement dit.

Comme il a été mentionné ci-dessus, SSL et TLS sont des protocoles transparents pour l'utilisateur, situés entre les couches Application et Transport. De nombreux protocoles peuvent donc exploiter SSL et TLS, tels HTTP (HTTPS), LDAP (LDAPS), etc.

Cependant, si SSL et TLS sont transparents au niveau des protocoles, il ne l'est pas au niveau des applications qui l'exploitent. Celles-ci nécessitent donc individuellement des aménagements pour prendre en compte SSL et TLS. L'une des faiblesses de SSL et TLS est de donc disposer d'un nombre encore relativement réduit d'implémentations.

Implémentation de SSL et TLS :

Implémentations dans les navigateurs web

La majeure partie des implémentations de SSL et TLS se trouve dans les navigateurs et serveurs web. Le serveur apache, notamment, peut exploiter SSL grâce à une implémentation basée sur OpenSSL.

OpenSSL

Implémenté en C, OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques (une de cryptographie générale et une implémentant le protocole SSL), ainsi qu'une commande en ligne. OpenSSL supporte SSL 2.0, SSL 3.0 et TLS 1.0. OpenSSL est distribué sous une licence de type apache.

a) SSL et TLS plus que d'autres solutions

D'autres protocoles permettent d'assurer la sécurité sur le réseau. Bien que proposant des fonctionnalités concurrentes de SSL et TLS, ils sont plutôt considérés comme complémentaires.

SSH est un protocole de niveau application qui propose une alternative sécurisée aux utilitaires classiques (rlogin, rsh, telnet) qui n'offrent pas de confidentialité. La possibilité d'exploiter un mécanisme de tunneling rend SSH, comme SSL et TLS compatible avec les autres protocoles de niveau application déjà existant. Tout comme SSL et TLS, SSH assure l'authentification des machines, la confidentialité et l'intégrité des données. Il assure aussi l'authentification des utilisateurs par mot de passe.

SSH souffre de faiblesses par rapport SSL et TLS : il n'intègre pas la notion de certificats X509 v3, nécessite l'installation d'une application cliente spécifique (pas de transparence). De plus, la notion de tunneling reste difficile à appréhender.

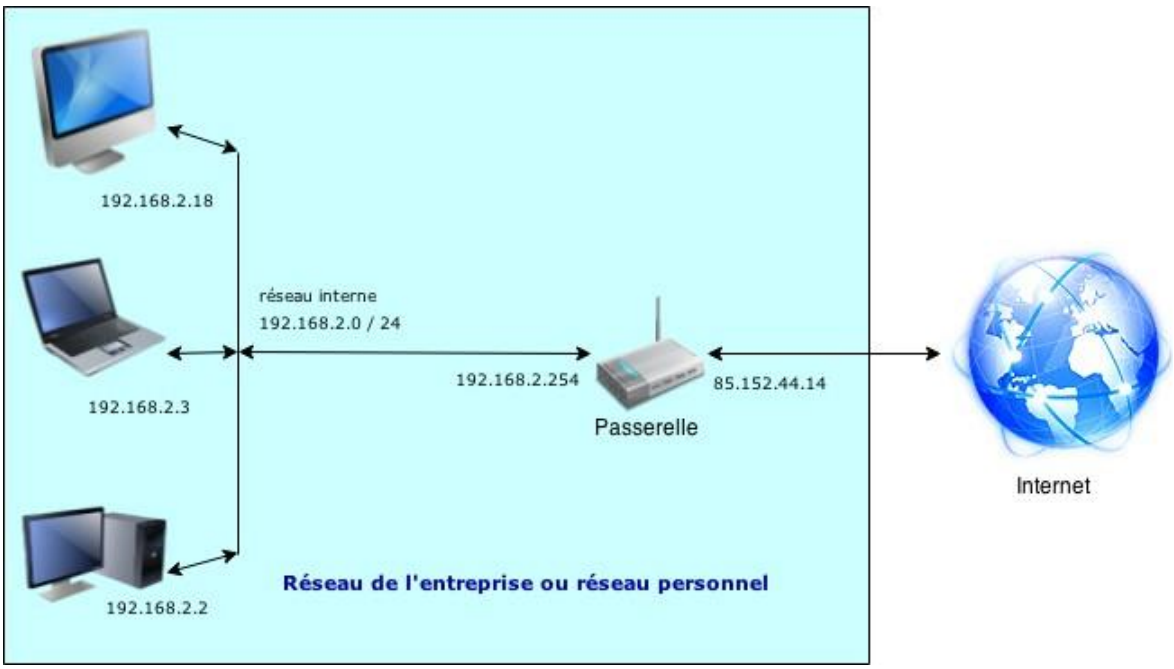
Cependant, SSH est moins vulnérable que SSL et TLS en matière d'identification du client. En effet, la protection du certificat sur un poste client ne peut pas toujours être correctement assurée.

B) Accès internet

La fonction NAT traduit les adresses privées internes en une ou plusieurs adresses publiques pour le routage sur Internet. La fonction NAT remplace l'adresse source IP privée contenue à l'intérieur de chaque paquet par une adresse IP enregistrée publiquement avant d'envoyer le paquet sur Internet.

Les petites et moyennes entreprises se connectent à leurs fournisseurs de services Internet via une connexion unique. Le routeur de périphérie local configuré à l'aide de la fonction NAT se connecte au fournisseur de services Internet. Les entreprises plus grandes peuvent disposer de plusieurs connexions à des FAI, et le routeur de périphérie situé à chacun de ces emplacements exécute la fonction NAT.

L'utilisation de la fonction NAT sur les routeurs de périphérie permet de renforcer la sécurité. Les adresses privées internes se traduisent chaque fois en adresses publiques différentes. Ceci permet de dissimuler la véritable adresse des hôtes et serveurs de l'entreprise. La plupart des routeurs qui implémentent la fonction NAT bloquent également les paquets en provenance de l'extérieur du réseau privé, sauf si ces paquets constituent une réponse à une demande émise par un hôte interne.

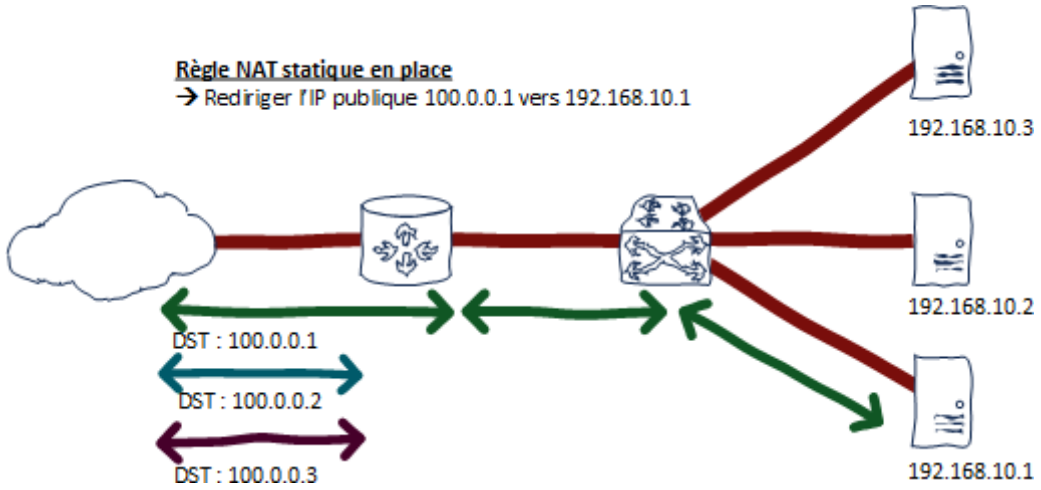


a) Le NAT statique

On va parler de NAT ou de translation d'adresse statique quand il s'agit d'effectuer une conversion des paquets d'un point à un autre de façon constante et systématique. Un point peut être une IP, on va alors dire au routeur que tous les paquets arrivant sur une IP externe donnée seront à traduire pour être transmis à une IP interne. On peut également identifier un point comme étant une IP et un ou plusieurs port(s) précis. Certains paquets, avec pour port de destination un certain port, vont alors être redirigés vers une certaine IP interne et les paquets avec un autre port ne seront pas redirigés ou alors vers une autre machine.

Techniquement, le routeur va, à la réception d'un paquet depuis l'extérieur, modifier le champ "IP destination" qui va passer de l'IP externe du routeur à l'IP du serveur en interne, c'est ici qu'agit la translation d'adresse. On peut également parler de NAT de destination.

On effectue donc une association entre une IP dite publique (externe) et une IP privée (interne) pour tout ou partie des ports sur lesquels arrivent les paquets sur l'interface "publique" ou externe du routeur. Voici l'illustration d'un routage statique "un à un", c'est-à-dire une association IP à IP de tous les ports du routeur coté public vers une IP privée :



Le NAT statique permet donc de rendre une machine présente dans un LAN ou une DMZ disponible depuis internet. Cela ne va pas dans le sens premier de la création du NAT qui est d'économiser des adresses IPv4 car l'association d'une IP publique vers une IP privée est en un à un. On parle également de redirection de port lorsque l'on va rediriger uniquement un port de l'IP externe vers un port (le même ou un autre) d'une IP interne. Si l'on décide de faire une redirection du port 80 vers notre serveur web en DMZ, on va dire au routeur que toutes les requêtes ayant pour port destination le port 80 (HTTP) seront à réécrire pour aller vers l'IP de notre serveur web qui est en interne.

b) Le NAT dynamique

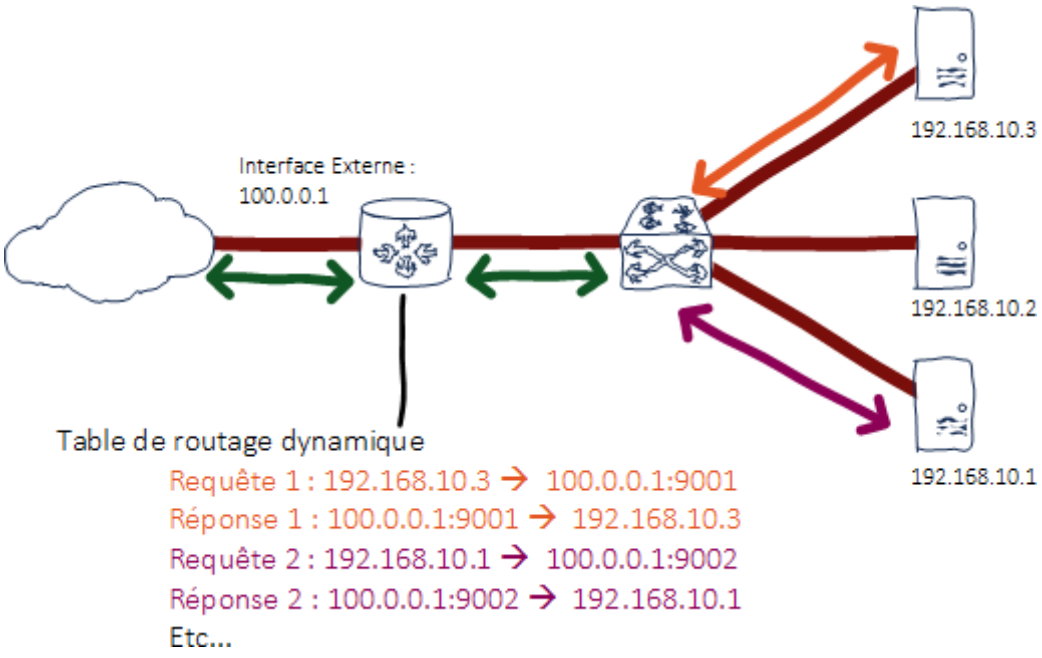
La translation d'adresse dynamique fonctionne elle dans l'autre sens et c'est le but premier de la création du NAT. Il permet de mettre, aux yeux des éléments qui sont du côté de l'interface externe, un ensemble de machines derrière une ou plusieurs IPs. Si l'on dispose par exemple d'une plage IP de 8 adresses comme 100.0.0.0/29 sur internet mais que l'on a 500 machines dans notre LAN, nous ne pourrons pas les rendre toutes disponibles sur internet en même temps car à force il n'y aurait plus assez d'adresses IPv4 (il n'en reste déjà plus !). Le NAT dynamique va alors nous permettre de traduire les 500 adresses IP internes dans le lot des 8 adresses que nous avons sur internet. Cela est dit "dynamique" car le routeur va utiliser

dynamiquement différentes correspondances IP:ports pour faire suivre les paquets et les échanges qui transitent sur les translations interne et externe.

Le NAT dynamique dans son utilisation courante peut également être appelé NAT de source car on va effectuer une translation d'adresse (un changement d'information dans les paquets IP) de l'adresse source des paquets, les faisant passer des IPs internes vers l'IP externe du routeur.

Le routeur va alors avoir une table de translation qui va être générée via un mécanisme de PAT (Port Address Translation), on va affecter un échange depuis une IP interne vers externe à un port sur l'interface externe. Nous allons prendre un exemple avec une seule adresse IP externe et trois postes situés dans le LAN.

Si les trois postes décident d'aller sur internet. Le routeur va enregistrer que l'IP interne 192.168.10.3 va être translatée en 100.0.0.1:9001 (par exemple), le second échange sera translaté en 100.0.0.1:9002 pour les ports sources coté internet. Ainsi, quand la réponse d'internet reviendra sur le port 100.0.0.1:9001, le routeur saura qu'il faut renvoyer ces paquets vers 192.168.10.3. C'est une affectation, qu'elle soit par port ou par IP+port, qui est dynamique et éphémère, car générée sur demande jusqu'à la fin d'un échange de paquet ou d'une connexion :



Nous avons donc bien un fonctionnement qui nous permet d'avoir plusieurs postes "se faisant passer" pour une seule IP coté internet, une correspondance IP_externe:port <–> IP interne est faite pour chaque requête à l'inverse du NAT statique ou une correspondance IP à IP ou IP:port à IP:port est fait de façon automatique et constante.

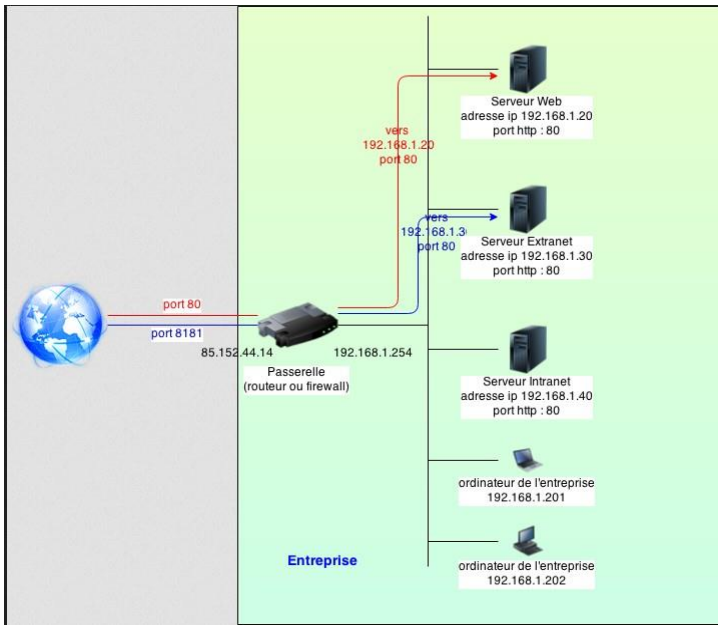
c) Le PAT

Une des variantes les plus répandues de la fonction NAT dynamique est connue sous le nom de fonction traduction d'adresses de port (PAT, Port Address Translation), également appelée surcharge NAT.
La fonction PAT traduit dynamiquement plusieurs adresses locales internes en une seule adresse publique. Lorsqu'un hôte source envoie un message à un hôte de destination, il utilise une combinaison d'adresse IP et de numéro de port pour suivre chaque conversation individuelle. Dans la fonction PAT, le routeur de passerelle traduit la combinaison de l'adresse source locale et du numéro de port en une seule adresse IP globale et un numéro unique de port supérieur à 1024.

Une table dans le routeur contient une liste des combinaisons d'adresses IP internes et de numéros de ports qui sont traduites en adresse externe.

Bien que chaque hôte se traduise par la même adresse IP globale, le numéro de port associé à la conversation est unique.

Pour accéder aux différents services proposés par vos serveurs, les ordinateurs externes vont utiliser l'adresse publique de votre réseau mais en appelant des protocoles et donc des ports différents.



Comme il existe plus de 64000 ports disponibles, il est peu probable qu'un routeur vienne à manquer d'adresses.

La fonction PAT traduit de multiples adresses locales en une seule adresse IP globale. Lorsqu'un hôte source envoie un message à un hôte de destination, il utilise une combinaison d'adresse IP et de numéro de port pour effectuer le suivi de chaque conversation individuelle

avec l'hôte de destination. Dans la fonction PAT, la passerelle traduit la combinaison d'adresse source locale et de port dans le paquet en une adresse IP globale unique et un numéro de port unique supérieur à 1024. Bien que chaque hôte soit traduit par la même adresse IP globale, le numéro de port associé à la conversation est unique.

Le trafic de réponse est adressé à l'adresse IP et au numéro de port traduit utilisés par l'hôte. Une table dans le routeur contient une liste des combinaisons d'adresses IP internes et de numéros de ports qui sont traduits en adresse externe. Le trafic de réponse est transféré à l'adresse interne et au numéro de port approprié. Comme il existe plus de 64 000 ports disponibles, il est fort improbable qu'un routeur manque d'adresses, alors qu'il s'agit d'une éventualité avec la fonction NAT dynamique.

C) ACL

1) Définition

Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :
-L'adresse d'origine
-L'adresse de destination le numéro de port.
-Les protocoles de couches supérieures
-D'autres paramètres (horaires par exemple)Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers.

Les ACLs sont associées à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certaines conditions faisant partie de la liste de contrôle d'accès.

Les ACL peuvent être créés pour tous les protocoles routés. Il faut donc définir une liste de contrôle d'accès dans le cas de chaque protocole activé dans une interface pour contrôler le flux de trafic acheminé par cette interface.

2) Vérifications des paquets

Lorsque le routeur détermine s'il doit acheminer ou bloquer un paquet, la plate-forme logicielle Cisco IOS examine le paquet en fonction de chaque instruction de condition dans l'ordre dans lequel les instructions ont été créées.

Si le paquet arrivant à l'interface du routeur satisfait à une condition, il est autorisé ou refusé (suivant l'instruction) et les autres instructions ne sont pas vérifiées.
Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est jeté. Ceci est le résultat de l'instruction implicite deny any à la fin de chaque ACL.

3) Création des ACL – Généralités

Pour créer une liste de contrôle d'accès, il faut :

- Créer la liste de contrôle d'accès en mode de configuration globale.
- Assigner cette ACL à une interface

D) VPN

1) IPsec

IPSEC est une suite de protocoles destinés à sécuriser la couche Réseau (Network layer) de la suite TCP/IP.

IPSEC comprend trois sous-protocoles : AH, ESP et IKE.

- Le protocole AH (Authentication Header) définit les fonctionnalités d'authentification, de contrôle d'intégrité et de protection contre le rejeu de trafic.

- Le protocole ESP (Encapsulating Security Payload) définit les mêmes fonctionnalités et y ajoute la garantie de confidentialité par le chiffrement.

- Le protocole IKE (Internet Key Exchange) enfin définit les méthodes d'échange de clefs entre hôtes.

Avantages :

- IPSEC est une modification de la suite TCP/IP. Les fonctionnalités qu'il offre sont donc mises en œuvre directement au sein du noyau des machines hôtes. Cela signifie que les performances ne sont pas dégradées autant qu'elles peuvent l'être dans le cadre d'un VPN SSL/TLS. Cela signifie surtout qu'il n'est pas nécessaire d'installer des programmes clients ou serveurs sur chaque membre du VPN.

- Tout système d'exploitation - et plus précisément toute suite TCP/IP - qui intègre les fonctionnalités IPSEC est nativement interopérable. Il n'est pas nécessaire de choisir une solution IPSEC unique pour tous les membres du VPN.

Inconvénients :

- Les solutions IPSEC ont encore la réputation d'être moins faciles à paramétrer que leurs "homologues" SSL/TLS. L'infrastructure réseau sous-jacente peut constituer un point bloquant notamment en cas de translation d'adresse.

- IPSEC étant une modification de la suite TCP/IP, il est nécessaire de modifier le noyau du système d'exploitation de l'hôte. Ce point cependant est tempéré par le fait que les dernières versions des OS les plus couramment utilisés intègrent par défaut IPSEC dans le noyau.

2) VPN SSL/TLS

Le protocole SSL, actuellement dans sa version 3, a été initialement développé par la société Netscape pour sécuriser les transactions électroniques. L'IETF a repris son développement et a normalisé le protocole sous le vocable Transport Layer Security (TLS) dans la RFC2246. Dans le langage courant, SSLv3 et TLS sont souvent synonymes.

Sans entrer dans le détail, le protocole SSL/TLS s'insert entre la couche Application et la couche Transport du modèle OSI/TCPIP et concerne donc les protocoles TCP et UDP. Il est lui-même composé de deux sous-protocoles : TLS Handshake et TLS Record.

TLS Record prend en charge le chiffrement - symétrique - des données et le contrôle de leur intégrité.

TLS Handshake prend en charge l'authentification de chaque partie, la négociation des algorithmes de chiffrement er de signature ainsi que les échanges des clefs de session qui sont utilisés par le protocole TLS Record, ainsi que la remontée d'alertes.

Avantages :

- D'une manière générale, les VPN SSL/TLS sont mis en œuvre par des programmes qui s'exécutent en mode Utilisateur (user). Ils ne nécessitent donc pas de modification ni de recompilation du noyau du système d'exploitation hôte. De ce fait, ils sont également plus facilement portés d'un OS à l'autre.

- Ce mode d'exécution permet également de cloisonner (chroot) ces programmes et de les faire tourner avec des privilèges système réduits.

- Un VPN SSL/TLS s'appuie sur une connexion réseau TCP/IP “normale” en ce sens qu'il encapsule le trafic chiffré dans un paquet IP “classique”. La nature et la topologie des réseaux sous-jacents sont donc sans impact sur le VPN y compris en cas de translation d'adresse (NAT).

Inconvénients :

- Les VPN SSL/TLS supposent l'installation de logiciels clients sur les machines membres du VPN. Comme ce type de VPN n'est pas normalisé (Note : le protocole SSL/TLS l'est quant à lui), il n'y a aucune garantie d'interopérabilité entre différentes solutions logicielles.

- Dans la plupart des cas, les solutions VPN SSL/TLS utilisent des interfaces réseau virtuelles de type tun/tap. Ces interfaces redirigent le trafic émis par les applications vers les programmes VPN. Chaque paquet émis et reçu passe ainsi plusieurs fois dans le noyau avant d'être effectivement transmis sur le réseau, ce qui peut impacter plus ou moins sensiblement les performances générales de la solution.

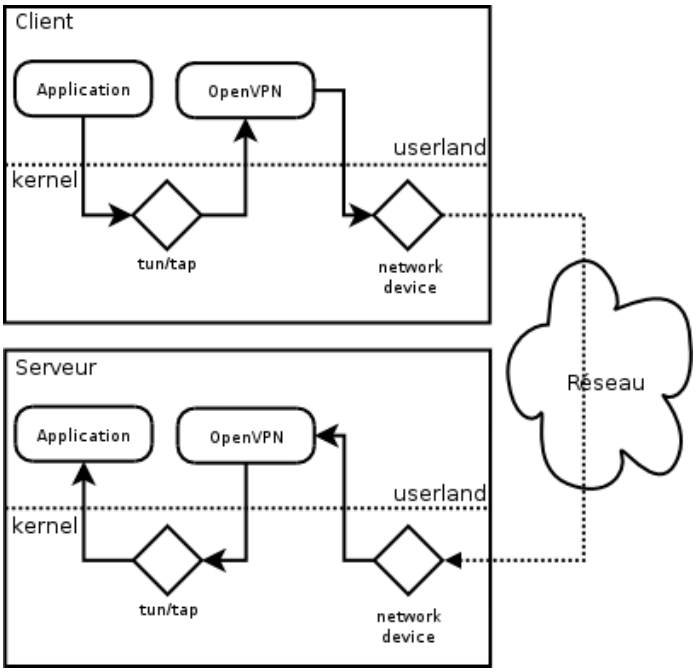
3) Open VPN

OpenVPN est un projet initié par James Yonan en 2001 qui permet de créer des VPN SSLT/TLS entre machines qui utilisent ce logiciel distribué sous licence GPL.

À l'origine “simple” tunnel IP sur UDP, OpenVPN est devenu au fil des années une solution client/serveur complète qui offre toutes les fonctionnalités et les garanties que l'on est en droit d'attendre d'un tel produit.

Le principe de fonctionnement d'OpenVPN est le suivant : une interface réseau virtuelle de type TUN (pour les tunnels IP) ou TAP (pour les tunnels Ethernet) est utilisée pour rediriger le trafic émis ou reçu par les applications d'une machine hôte vers un démon OpenVPN. Ce démon assure le chiffrement des données ainsi transmises grâce à une liaison (le tunnel) établi entre un client et un serveur. Sur ce dernier, un démon OpenVPN effectue les mêmes opérations.

Le schéma ci-dessous illustre ce mode de fonctionnement :



En plus du chiffrement, le démon OpenVPN apporte les fonctions d'authentification forte mutuelle de chaque partie : le client s'authentifie auprès du serveur et vice versa.

OpenVPN utilise les fonctions cryptographiques fournies par la bibliothèque OpenSSL.

OpenVPN s'appuie indifféremment sur UDP ou TCP comme protocole de transport. L'utilisation du protocole UDP repose sur l'extension DTLS (Datagram Transport Layer Security) fournie par la bibliothèque OpenSSL depuis la version 0.9.8.

OpenVPN est supporté par les systèmes d'exploitation les plus couramment utilisés : Linux, Solaris, *BSD, MS Windows et Mac OS X.

Modes de sécurité :

Lors de l'utilisation de clefs statiques, les deux passerelles VPN partagent la même clef pour chiffrer et déchiffrer les données. Dans ce cas, les configurations seront très simples mais le problème peut venir du fait qu'il est parfois nécessaire de transmettre la clef (à travers un canal sécurisé bien sûr) à quelqu'un dont vous n’avez pas confiance à l'autre bout du tunnel.

L'infrastructure à clef publique (PKI pour Public Key Infrastructure en anglais) est utilisée pour résoudre ce problème. Elle est basée sur le fait que chaque partie possède deux clefs, une clef publique connue de tout le monde et une clef privée tenue secrète. Ce processus est utilisé par OpenSSL, la version gratuite et open source intégrée à OpenVPN, pour authentifier les machines VPN avant le chiffrement des données.

Les avantages des deux modes :		
Mode OpenVPN :	Clefs partagées	SSL
Mode de cryptographie :	Symétrique	Asymétrique/Symétrique
Implémentation :	Plus facile	Plus compliquée
Vitesse :	Plus rapide	Plus lente
Consommation CPU :	Plus petite	Plus grand
Échange des clefs :	OUI	NON
Renouvellement des clefs :	NON	OUI
Authentification des passerelles :	NON	OUI

Paragraphe 2 : Choix des solutions

A) Accès à distance

Nous utiliserons le SSH, qui permet d'avoir une connexion distante en mode terminale (ou console) de manière sécurisée grâce aux algorithmes proposés (RSA, DSA, …)

B) Accès Internet

Nous utiliserons le SSH, qui permet d'avoir une connexion distante en mode terminale (ou console) de manière sécurisée grâce aux algorithmes proposés (RSA, DSA, …)

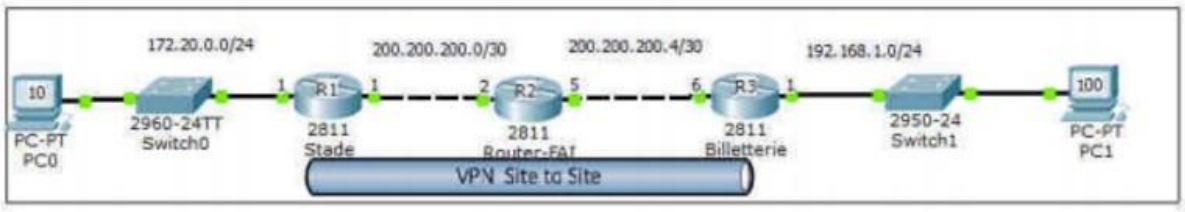
C) Accès à distance

Nous utiliserons et mettrons en place IPSec, c'est le seul capable de crypter les données échangées.

Paragraphe 3 : Projet

A) Objectifs du projet

Mise en place des outils de sécurité au sein de l'infrastructure Stadiumcompany.



B) Planning

1) Configuration SSH sur le routeur

Configurez les informations de base du routeur et de l'interface :

```
R-Stade>en
R-Stade#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-Stade(config)#ip domain-name stadiumcompany.com
R-Stade(config)#username admin privilege 15 password cisco
R-Stade(config)#int fa 0/0
R-Stade(config-if)#no shut
R-Stade(config-subif)#int fa 0/0.4
R-Stade(config-subif)#encapsulation dot1Q 10
R-Stade(config-subif)#ip address 172.20.0.1 255.255.255.0
R-Stade(config-subif)#no shut
R-Stade(config-subif)#exit
R-Stade(config)#int fa 0/1
R-Stade(config-if)#ip address dhcp
R-Stade(config-if)#no shut
```

Lignes de terminal VTY entrantes afin de valider Telnet et SSH :

```
R-Stade(config)#line vty 0 4
R-Stade(config-line)#privilege level 15
R-Stade(config-line)#login local
R-Stade(config-line)#transport input telnet ssh
R-Stade(config-line)#exit
```


2) Mise en place du NAT/PAT

Paramétrage des interfaces :

```
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config)#int fa 0/1
Router(config-if)#ip add dhcp
Router(config-if)# ip nat outside
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa 0/0.10
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.20
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.30
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.40
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.50
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.100
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.200
Router(config-subif)#ip nat inside
```

Vérification des access-list :

```
Router#sh access-lists
Standard IP access list 10
    10 permit 172.20.0.0, wildcard bits 0.0.0.255


Standard IP access list 20
    10 permit 172.20.1.0, wildcard bits 0.0.0.255
Standard IP access list 30
    10 permit 172.20.3.0, wildcard bits 0.0.0.127
Standard IP access list 40
    10 permit 172.20.3.128, wildcard bits 0.0.0.63
Standard IP access list 50
    10 permit 172.20.3.192, wildcard bits 0.0.0.31
Standard IP access list 98
    10 permit 172.20.2.0, wildcard bits 0.0.0.127
Standard IP access list 99
    10 permit 172.20.2.128, wildcard bits 0.0.0.127
```

Traduction des adresses depuis un client :

```
Router#sh ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
icmp 172.20.90.75:1   172.20.1.100:1     8.8.8.8:1          8.8.8.8:1
udp 172.20.90.75:137  172.20.1.100:137   64.4.23.145:137    64.4.23.145:137
udp 172.20.90.75:137  172.20.1.100:137   64.4.23.155:137    64.4.23.155:137
udp 172.20.90.75:137  172.20.1.100:137   111.221.77.167:137 111.221.77.167:137
udp 172.20.90.75:137  172.20.1.100:137   157.55.130.145:137 157.55.130.145:137
udp 172.20.90.75:137  172.20.1.100:137   157.55.130.151:137 157.55.130.151:137
udp 172.20.90.75:137  172.20.1.100:137   157.55.235.141:137 157.55.235.141:137
udp 172.20.90.75:137  172.20.1.100:137   157.55.235.165:137 157.55.235.165:137
udp 172.20.90.75:137  172.20.1.100:137   157.56.52.15:137   157.56.52.15:137
udp 172.20.90.75:137  172.20.1.100:137   157.56.52.17:137   157.56.52.17:137
udp 172.20.90.75:137  172.20.1.100:137   157.56.52.45:137   157.56.52.45:137
udp     172.20.90.75:137            172.20.1.100:137            213.199.179.148:137
213.199.179.148:137
udp     172.20.90.75:137            172.20.1.100:137            213.199.179.165:137
213.199.179.165:137
udp     172.20.90.75:137            172.20.1.100:137            213.199.179.172:137
213.199.179.172:137
udp      172.20.90.75:1581          172.20.1.100:1581           46.236.190.182:65444
46.236.190.182:65444
udp      172.20.90.75:1581          172.20.1.100:1581           101.184.60.230:9180
101.184.60.230:9180
udp 172.20.90.75:1581  172.20.1.100:1581  155.4.21.64:52189  155.4.21.64:52189
```

C) Mise en place du VPN

1) Routeur R1

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip address 172.20.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip address 200.200.200.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

Les interfaces sont configurées, maintenant je vais faire un routage EIGRP. D'autres choix étaient possibles comme le routage OSPF ou statiques.

```
R1(config)#router eigrp 1
R1(config-router)#network 172.20.0.0 0.0.0.255
R1(config-router)#network 200.200.200.0 0.0.0.3
R1(config-router)#exit
```

Configuration :

Nous commencerons par configurer notre PC et notre serveur en leur attribuant la bonne configuration réseau.

Nous attaquerons ensuite la configuration du routeur R1 :

Première étape :
Commençons par notre routeur R1, vous devez vérifier que l'IOS de vos routeurs supporte le VPN. On active ensuite les fonctions crypto du routeur :

```
R1(config)#crypto isakmp enable
```

```
Cette fonction est activée par défaut sur les IOS avec les options cryptographiques.
Sinon :
R-Stade#boot sy
R-Stade#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R-Stade(config)#boo
R-Stade(config)#boot sy
R-Stade(config)#boot system fla
R-Stade(config)#boot system flash:c2801-adventerprisek9-mz.124-16.bin
R-Stade(config)#^Z
R-Stade#wr
```

Deuxième étape :
Nous allons configurer la police qui détermine quelle encryptions on utilise, quelle HASH, l'authentification etc.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
```

Ensuite nous configurons la clef :

```
R1(config)#crypto isakmp key  iris123  address  200.200.200.6
```

ou `R1(config)#crypto isakmp key 6  iris123  address 200.200.200.6`

Quatrième étape :
Configuration des options de transformations des données :

```
R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
```

esp : Signifie Encapsulation Security Protocol

Cinquièmes Étapes est la création des ACL qui va déterminer le trafic autorisé :

```
R1(config)#access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0255
```


Enfin on configure la crypto map qui va associer l'acces-list, le trafic, et la destination :

```
R1(config)#crypto map stade 10 ipsec-isakmp
R1(config-crypto-map)#set peer 200.200.200.6
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
```

2) Routeur R2

Même procédure pour notre routeur R2 :
On commence par le Hostname :

```
Router#configure terminal
Router(config)#hostname R2
```

Nous configurons ensuite les adresses IP des deux interfaces :

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip address 200.200.200.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface FastEthernet 0/1
R2(config-if)#ip address 200.200.200.5 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage.

```
R2(config)#router eigrp 1
R2(config-router)#network 200.200.200.0 0.0.0.3
R2(config-router)#network 200.200.200.4 0.0.0.3
R2(config-router)#exit
```

La configuration de base de notre routeur R2 est terminée.

3) Routeur R3

Même procédure pour notre routeur R3 :
On commence par le Hostname :

```
Router#configure terminal
Router(config)#hostname R3
```

Nous configurons ensuite les adresses IP des deux interfaces :

```
R3(config)#interface FastEthernet 0/0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface FastEthernet 0/1
R3(config-if)#ip address 200.200.200.6  255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
```

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage.

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.1.0 0.0.0.255
R3(config-router)#network 200.200.200.4 0.0.0.3
R3(config-router)#exit
```

La configuration de base de notre routeur R3 est terminée.

Test de fonctionnement :

```
PC> ping 192.168.1.100
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=12ms TTL=126
Reply from 192.168.1.100: bytes=32 time=11ms TTL=126
Reply from 192.168.1.100: bytes=32 time=12ms TTL=126
Reply from 192.168.1.100: bytes=32 time=13ms TTL=126
Ping statistics for 192.168.1.100:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% l
oss),
Approximate round trip times in milli-seconds:
   Minimum = 11ms, Maximum = 13ms, Average = 12ms
```

Nous avons ping depuis le PC du réseau local du stade vers le PC du réseau local de la billetterie

L'ensemble des équipements interconnectés répondent bien entre eux. La base du réseau est en place. Grâce à la mise en place d'un serveur de domaine, les ordinateurs des différents VLANs pourront être intégré au domaine « stadiumcompany.local» et profiter des dossiers partagés sur le serveur. Le serveur DHCP distribuera les adresses IP automatiquement aux ordinateurs qui se connecteront sur le réseau. Des groupes d'utilisateurs ont été créés selon les services occupés par les utilisateurs. Ainsi seuls les utilisateurs du VLAN 10ont accès au partage « G-administration », et ainsi de suite.

Paragraphe 4 : Firewall PFSENSE et portail captif

1) Installation

1. Introduction

PfSense est un pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient pour la sécurisation d'un réseau d'entreprise.
Prérequis pour une machine PfSense

	Configuration minimale	Configuration recommandée
Processeur	600 MHz	1 GHz
Mémoire vive	512 Mo	1 Go
Stockage	> 6 Go	

2. Infrastructure

Pour notre Labo :il faut 3 machines
-Machine Pfsense FreeBSD dans le réseau Wan
Nom du serveur : heimdall
Adresse IP : DHCP/NAT

-Une machine avec active directory et DNS (nom du domaine Dns et active directory est sitka.local) dans le réseau sitka_lan
-une machine Debian dans le réseau opt_lan

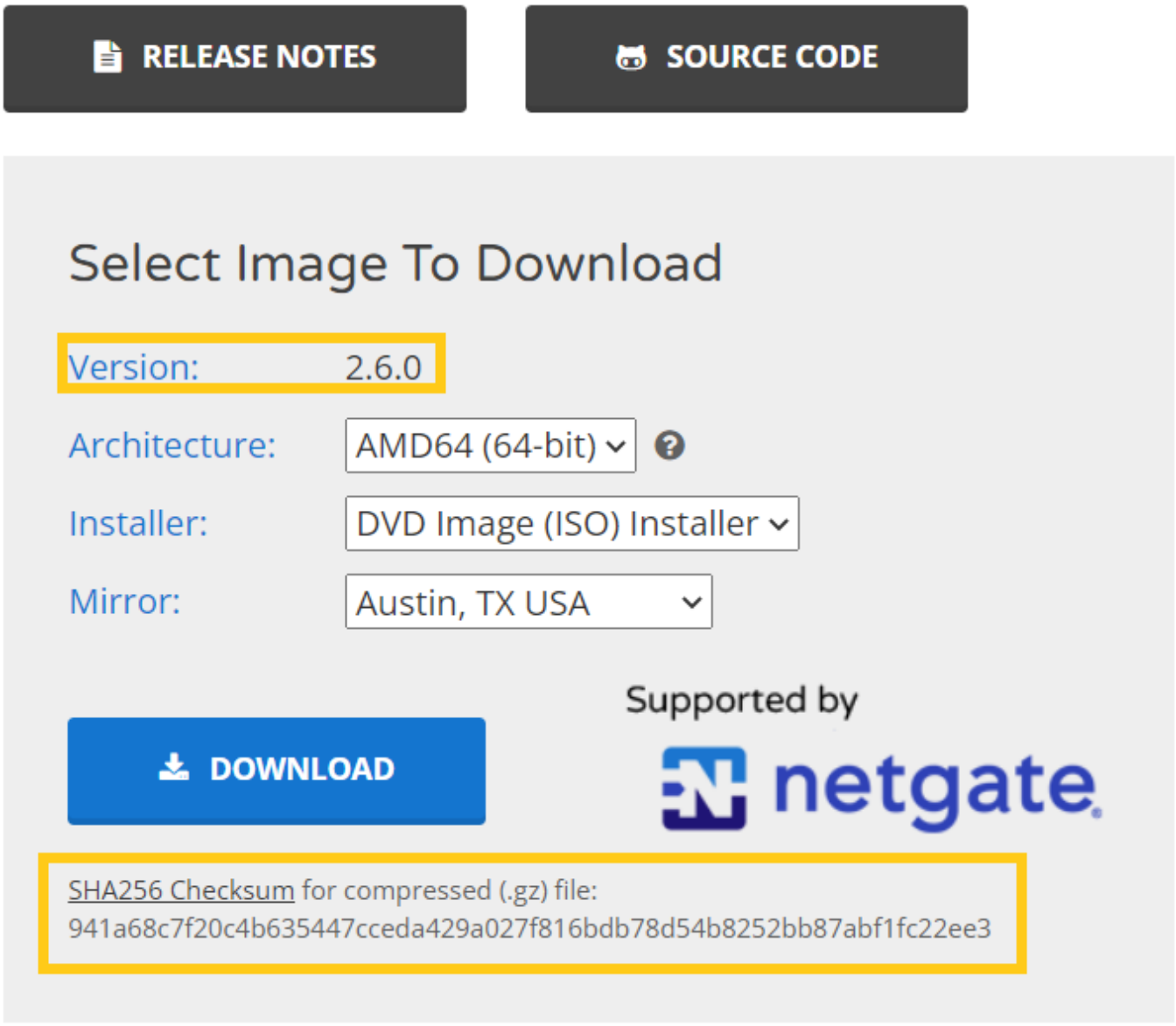
-Machine AD dans le réseau sitka_lan
Nom du serveur : hermes
Adresse IP : 172.20.0.14
Net masque : 255.255.255.0
Passerelle : 172.20.0.250
DNS : adresse de votre serveur DNS

-Une machine Debian ou Ubuntu et Windows dans le réseau opt_lan
Adresse IP : DHCP

3. Installation de pfsense

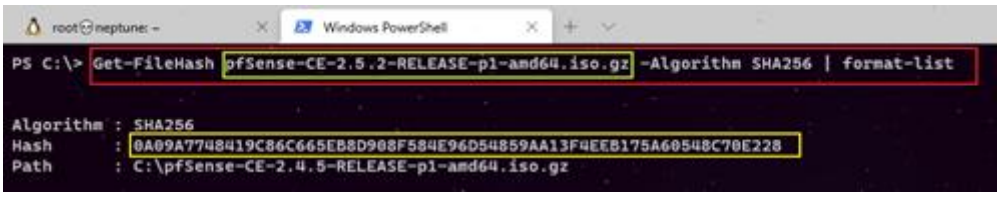
a. Téléchargement de pfsense

Pour installer pfSense il faut télécharger l'iso d'installation sur le site officiel à l'adresse :
https://www.pfsense.org/download/
Le lien de téléchargements est ci-dessous
https://atxfiles.netgate.com/mirror/downloads/pfSense-CE-2.6.0-RELEASE-amd64.iso.gz



b. Vérification de l'intégrité du fichier téléchargé pfsense

Une fois le fichier télécharger on va vérifier l'integrité du fichier telechargé avec la commande :
Get-FileHash pfSense-CE-2.6.0-RELEASE-p1-amd64.iso.gz -Algorithm SHA256 | format-list

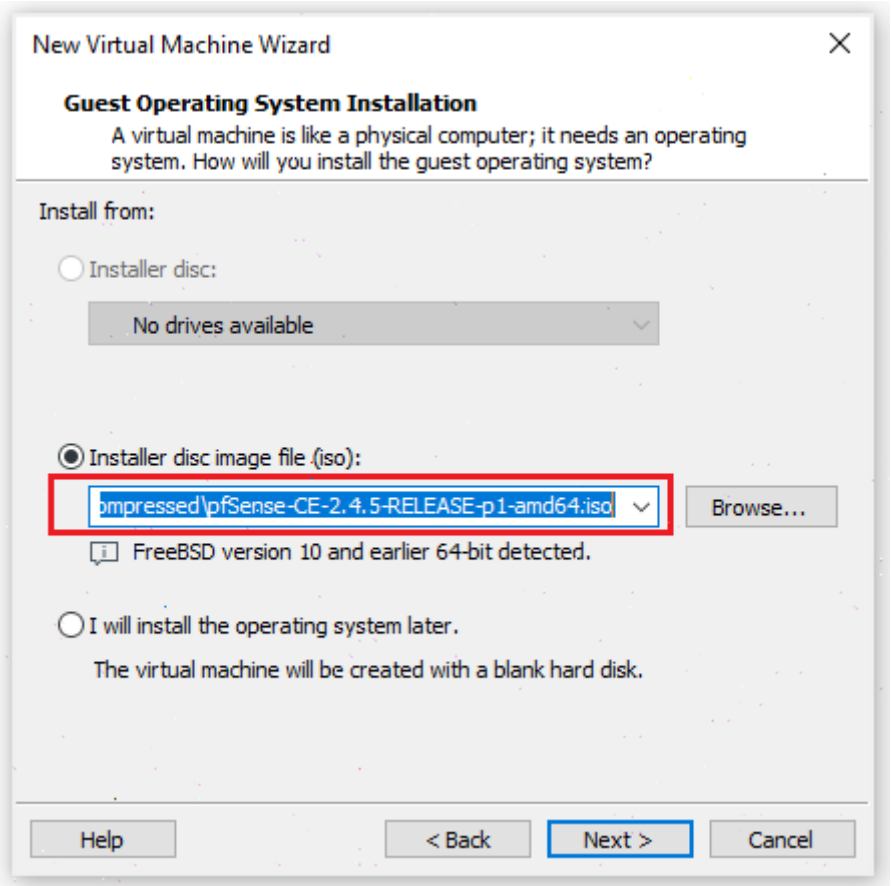


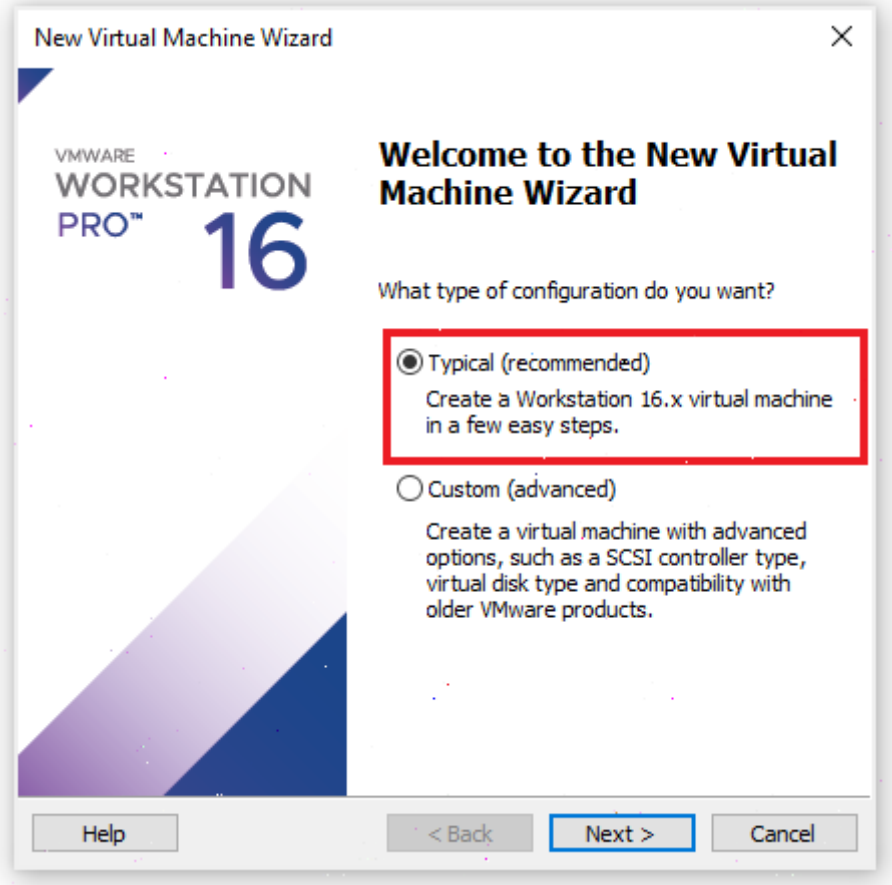
Comparer les deux empreintes **1** et **2** si les deux empreinte sont identique ceci implique que le fichier telechargé et intègre

c. Lancement de l'installation

il faut maintenant dézziper notre fichier pour avoir l'iso et lancer l'installation sur vmware

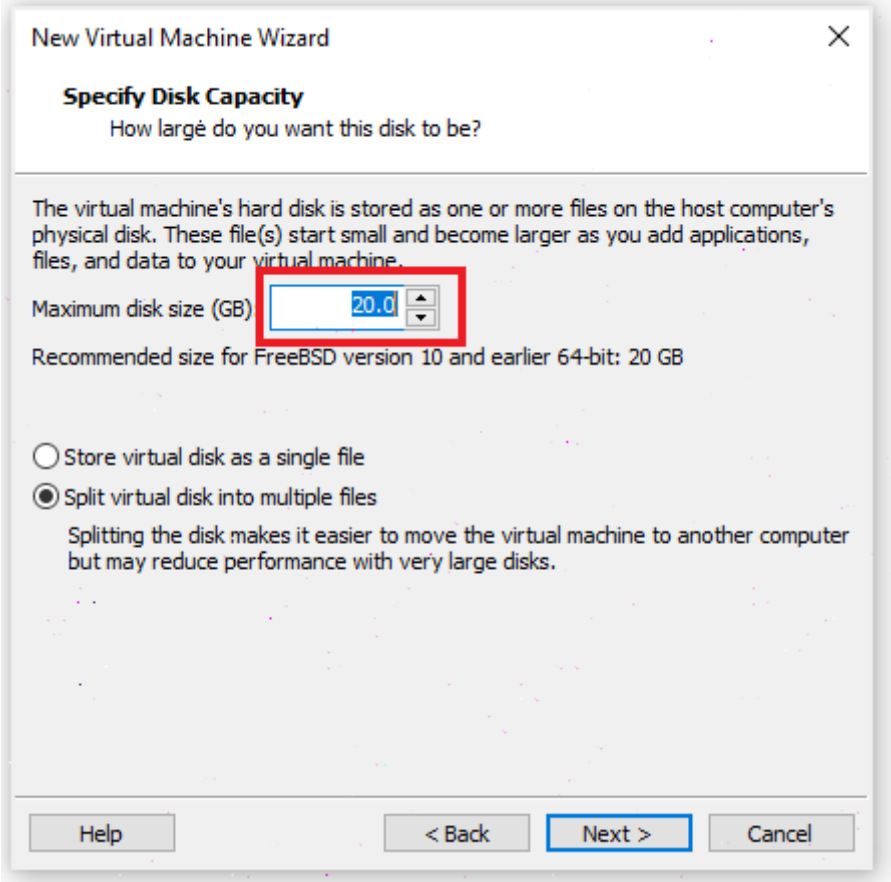
On pointe vers le fichier iso de pfsense

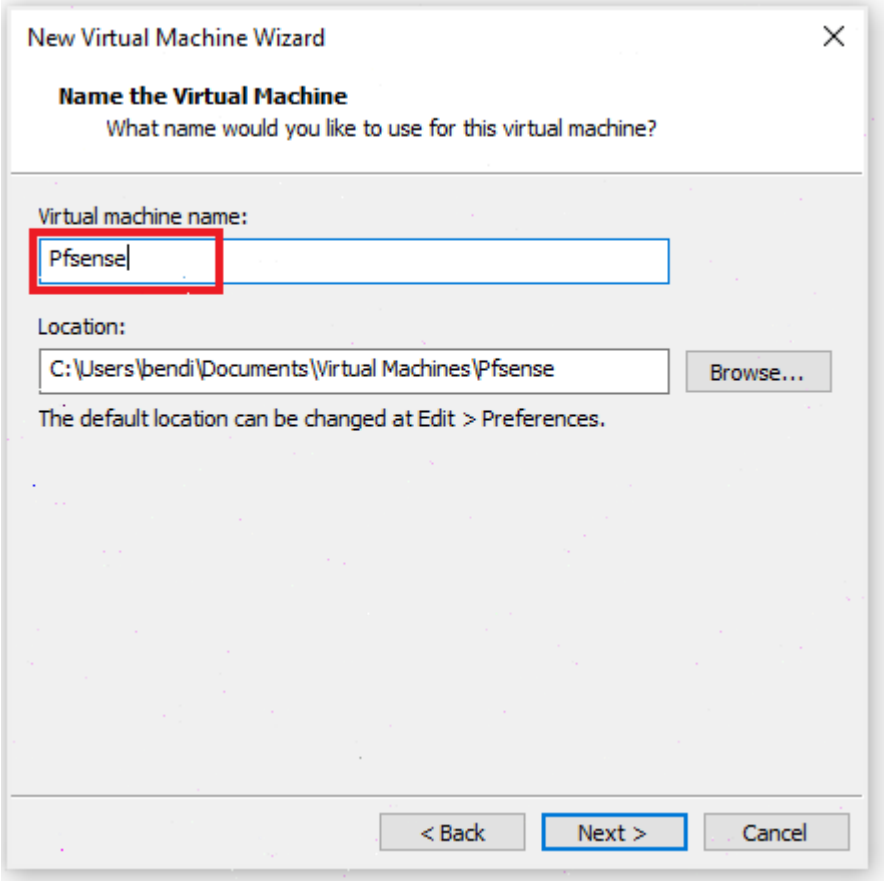

New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
No drives available
Installer disc image file (iso):
ompressed\pfSense-CE-2.4.5-RELEASE-p1-amd64.iso
Browse...
FreeBSD version 10 and earlier 64-bit detected.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
VMWARE
WORKSTATION
PRO™
16
Welcome to the New Virtual Machine Wizard
What type of configuration do you want?
Typical (recommended)
Create a Workstation 16.x virtual machine in a few easy steps.
Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
Help
< Back
Next >
Cancel

On choisit pfsense comme nom

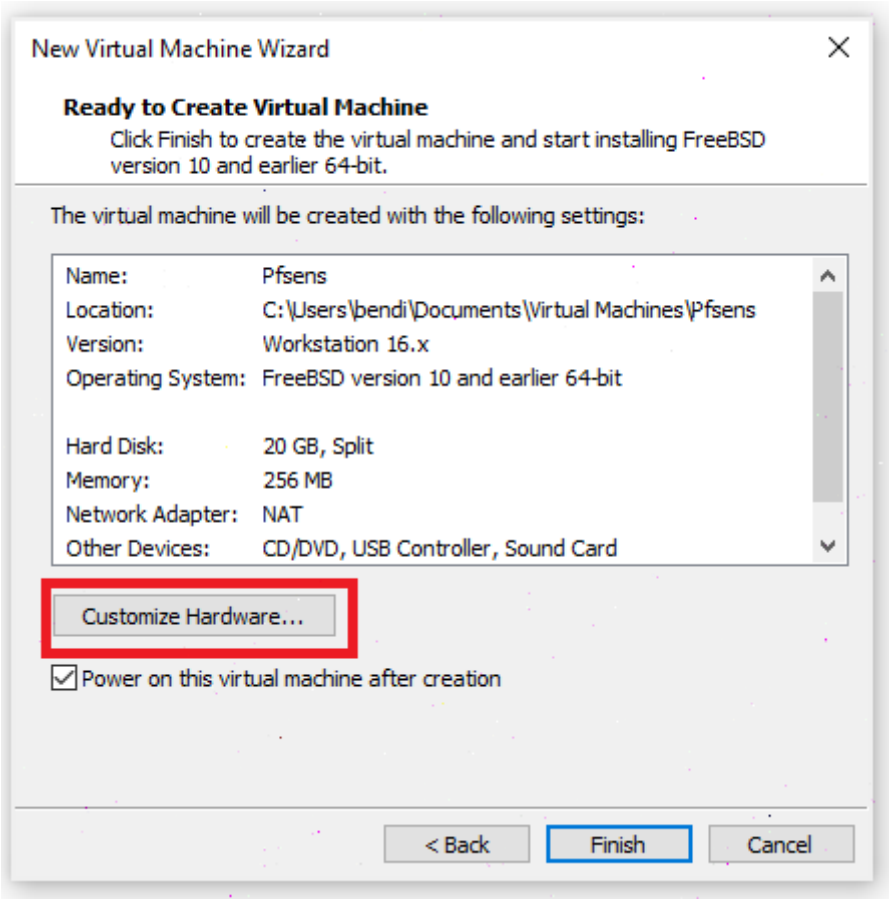
On laisse 20 gb par défaut

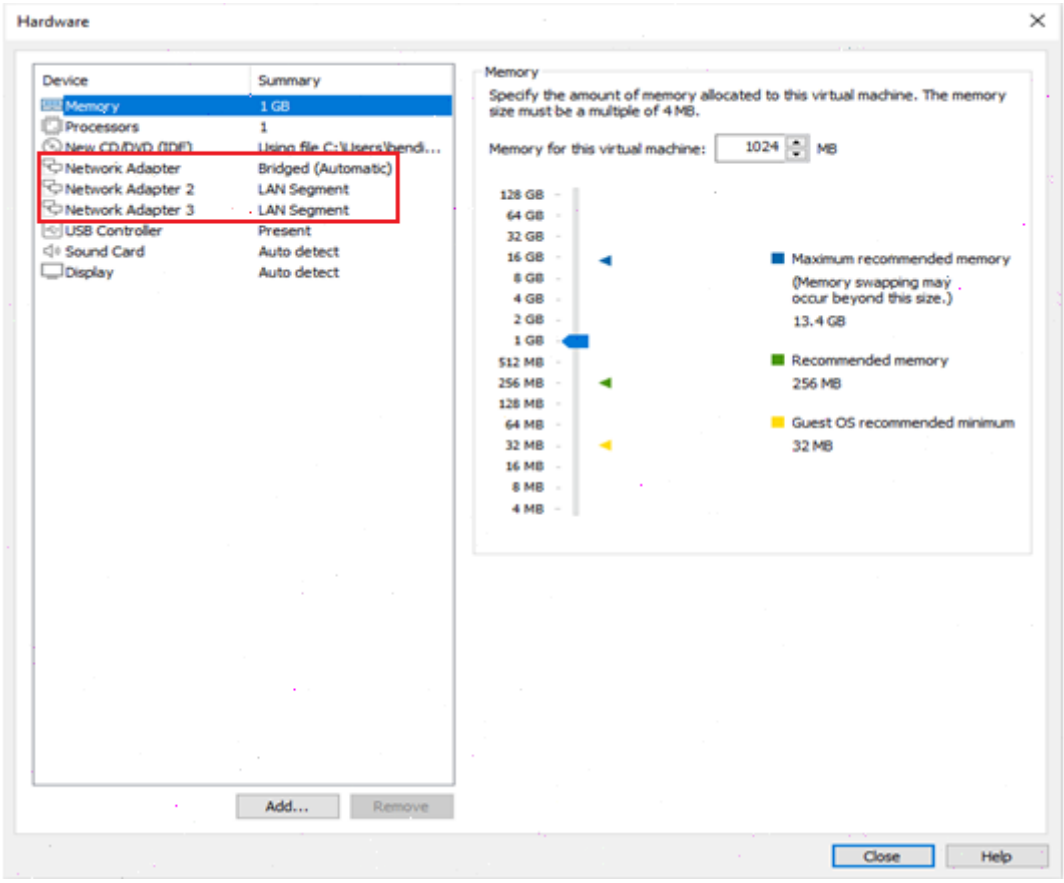




Pour cette étape On mettra en place 3 cartes
Network Adapter en bridge----------à192.168.1.0/24
Network Adapter2 en Lan_1----------à172.20.0.0/24
Network Adapter3 en Lan_2----------à192.168.2.0/24
On mettra 1GB de mémoire

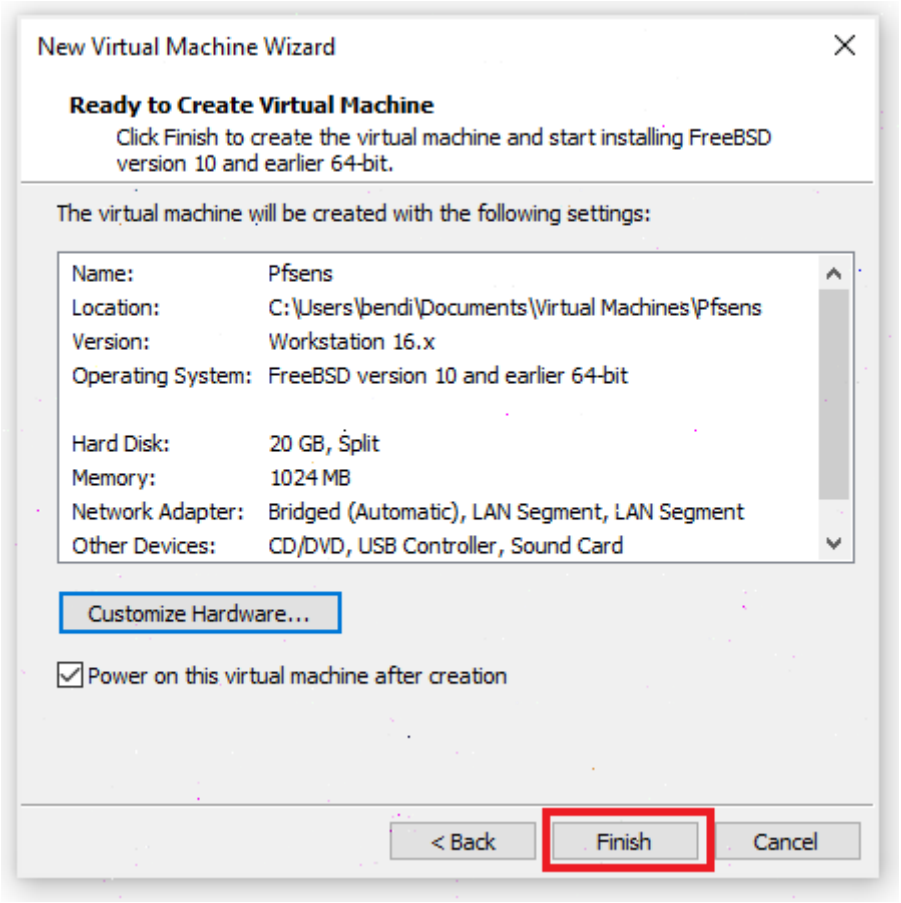
```
WAN (wan)       -> em0        -> v4: 192.168.1.250/24
LAN (lan)       -> em1        -> v4: 172.20.0.250/24
OPT1 (opt1)     -> em2        -> v4: 192.168.2.250/24
```




Hardware
Device
Summary
Memory
1 GB
Processors
1
Network Adapter
Bridged (Automatic)
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine:
1024
MB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
13.4 GB
Recommended memory
256 MB
Guest OS recommended minimum
32 MB
Close
Help

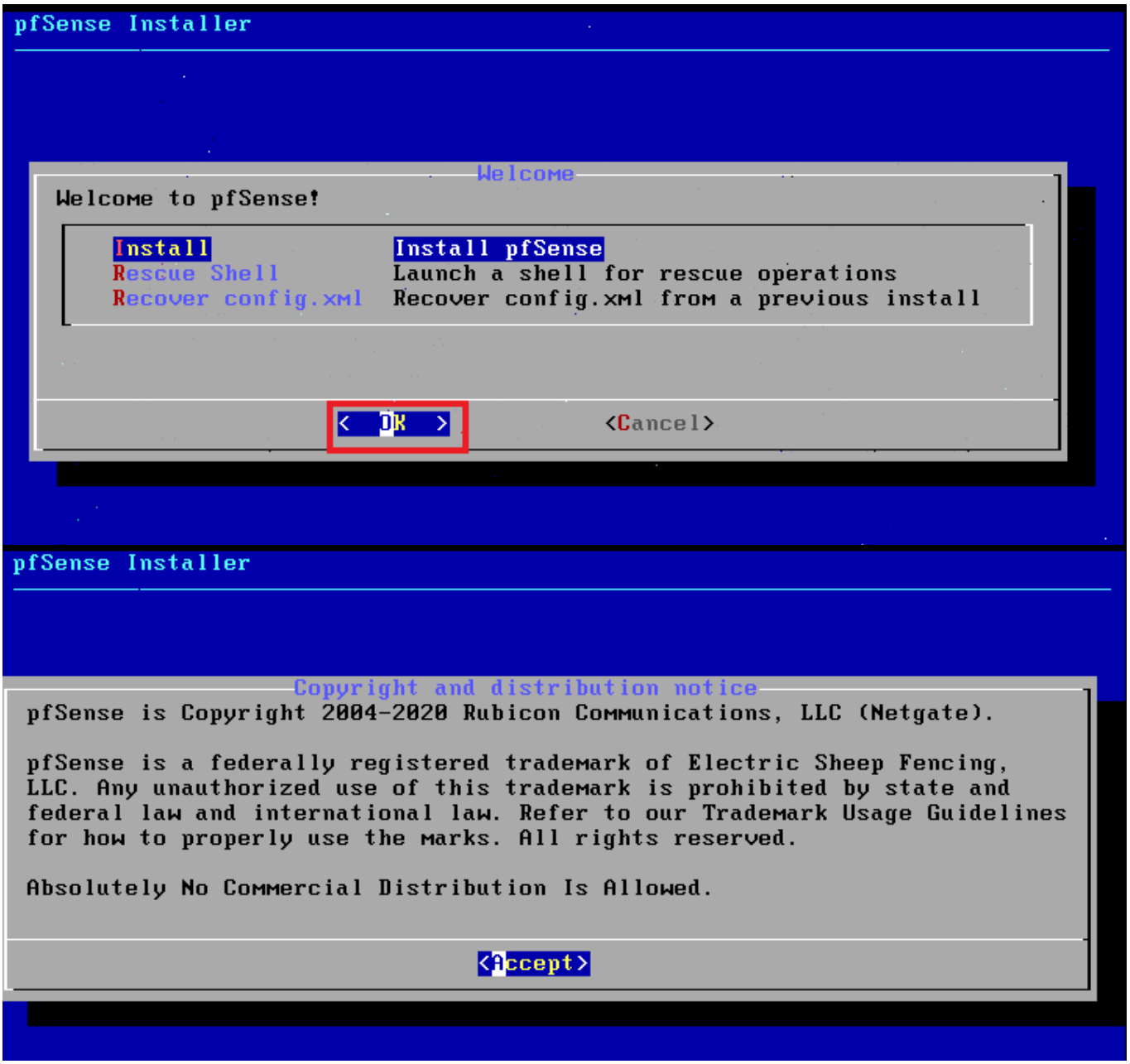
©

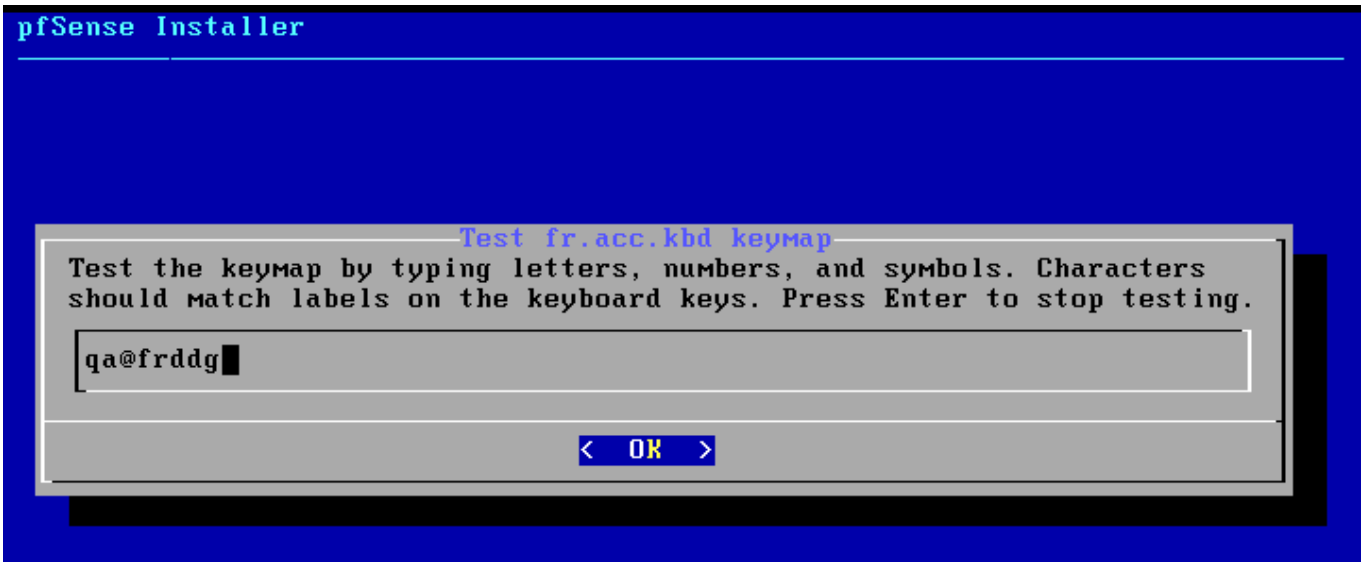
On clique sur finish et on commence l'installation



On accepte le contrat

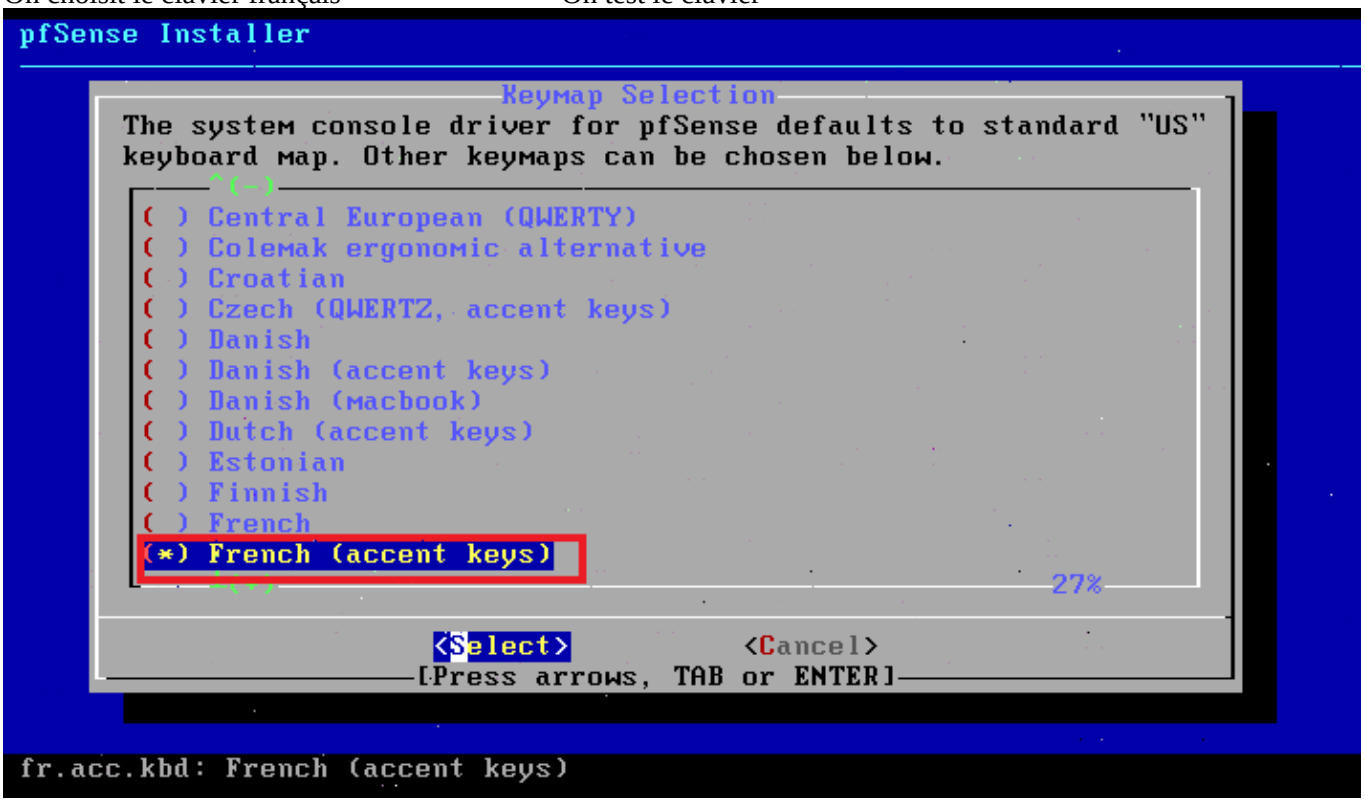
On sélectionne Install puis ok


pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
< OK >
<Cancel>
pfSense Installer
Copyright and distribution notice
pfSense is Copyright 2004-2020 Rubicon Communications, LLC (Netgate).
pfSense is a federally registered trademark of Electric Sheep Fencing, LLC. Any unauthorized use of this trademark is prohibited by state and federal law and international law. Refer to our Trademark Usage Guidelines for how to properly use the marks. All rights reserved.
Absolutely No Commercial Distribution Is Allowed.
<Accept>



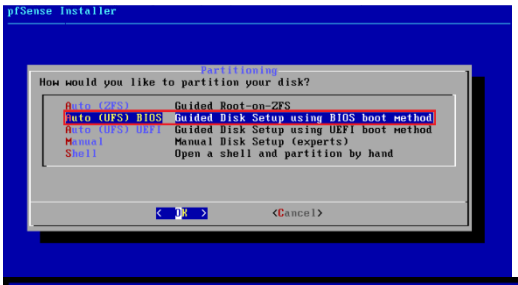
On choisit le clavier français

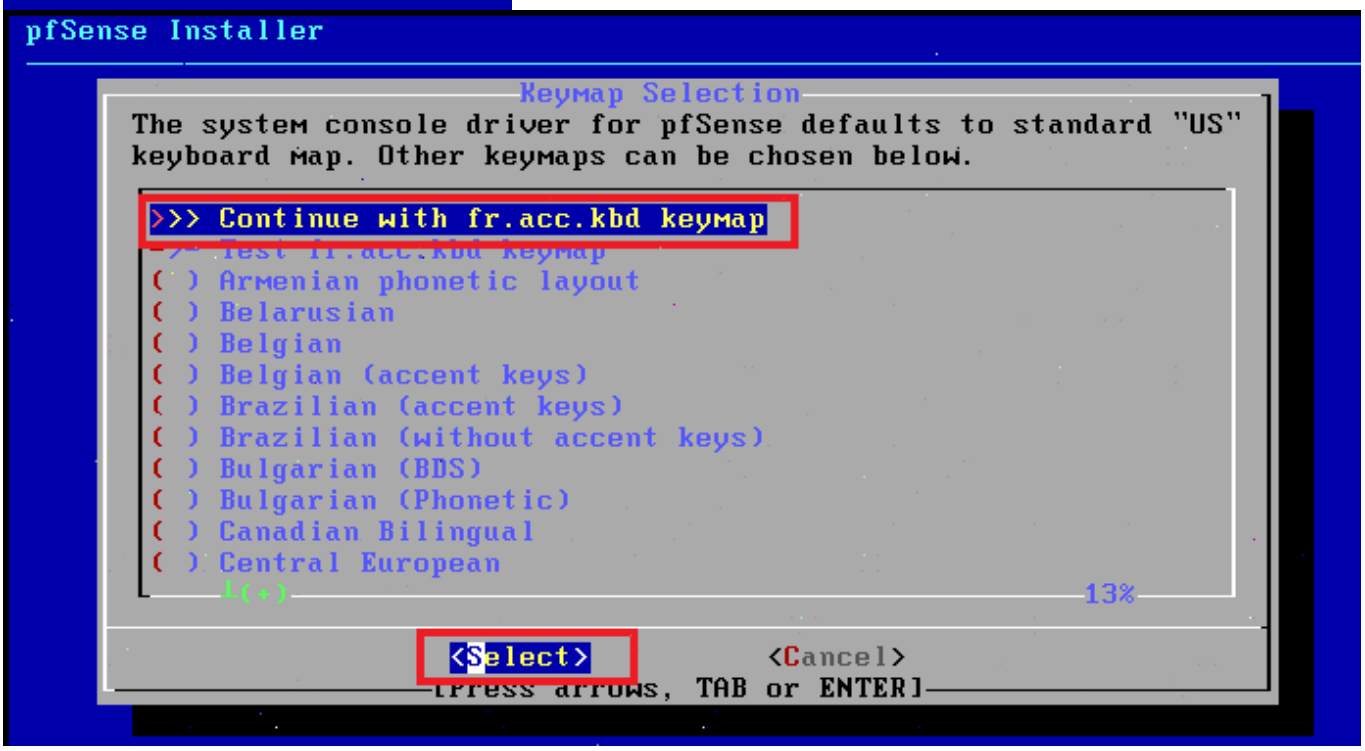
On test le clavier



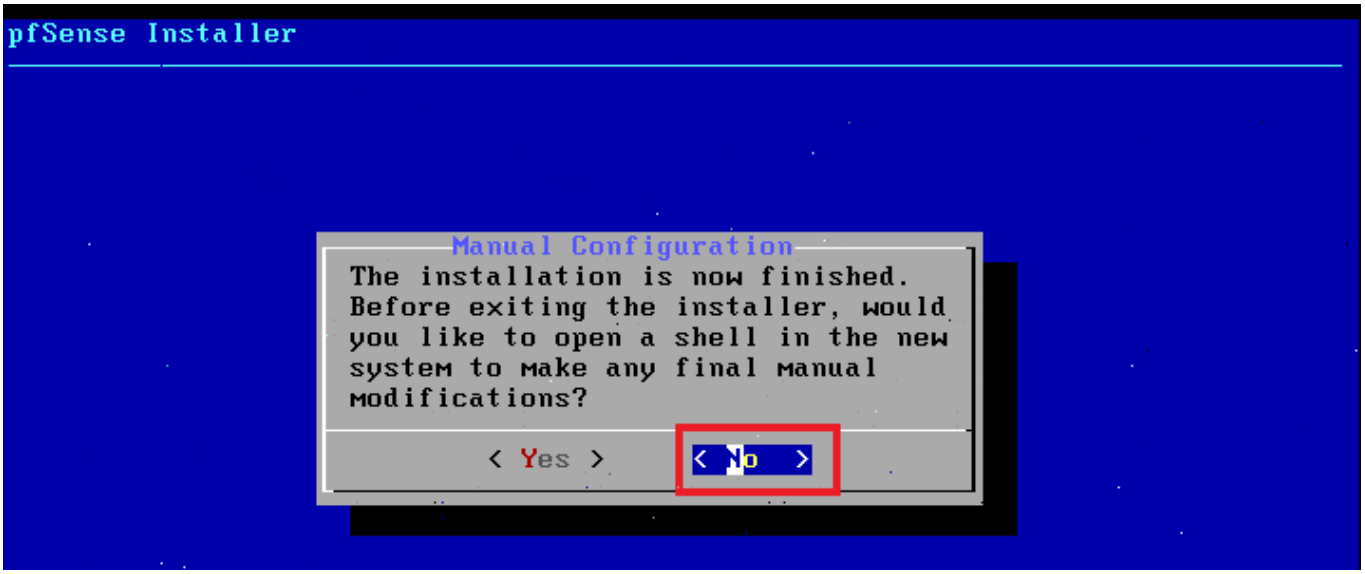
Puis on continue l'installation

On choisit le système UFS pour créer nos partitions



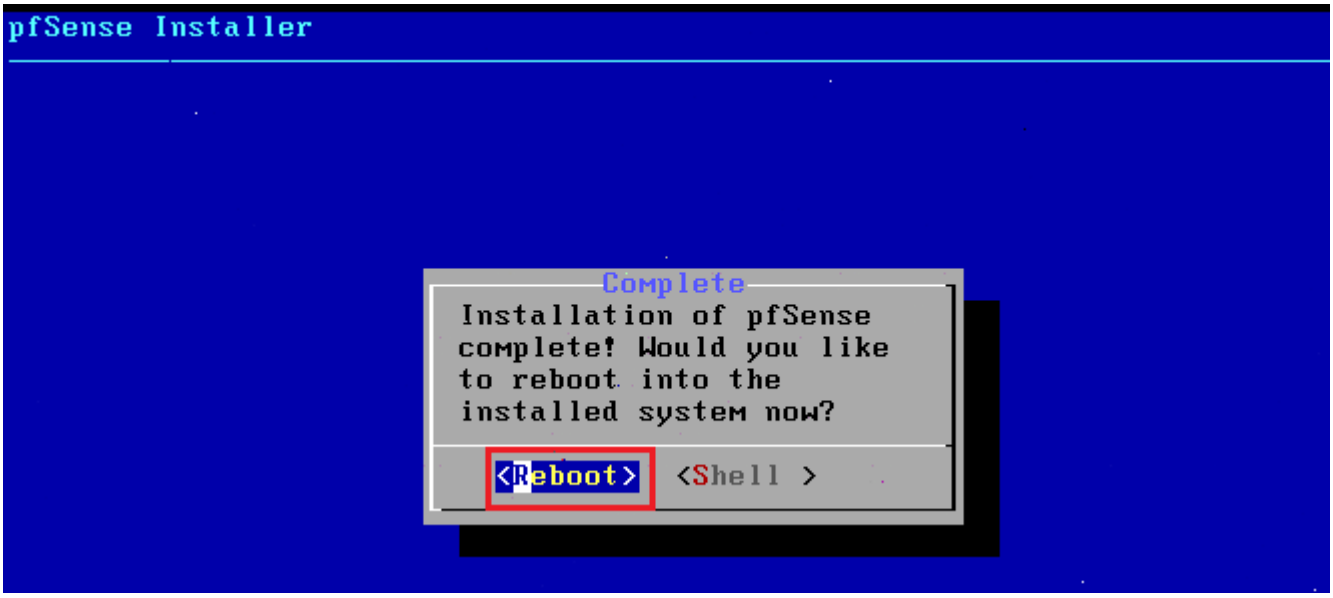


On nous demande si on veut aller sur le Shell

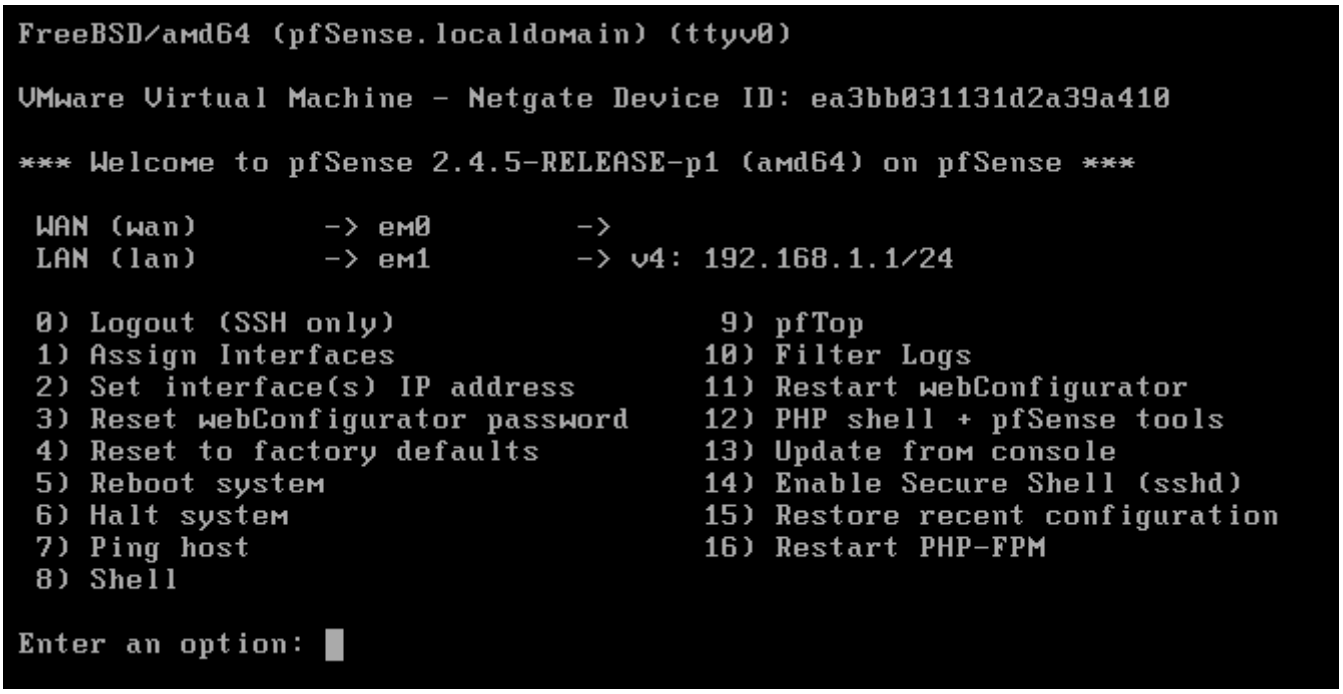


pour d'autres manipulations on dit non

Puis on redémarre la machine



Une fois la machine a redemarrer on tombe sur l'interface menu
On remarque qu'il ya que deux interfaces qui sont reconnue **em0** et **em1** et que le clavier est en qwerty malgré notre choix pendant l'installation d'un clavier français

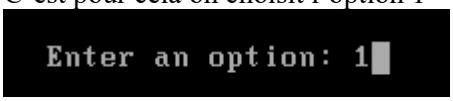


4. Configuration post installation

Mannuellement on va mettre notre clavier en français mais temporairement car en redemarrant notre serveur le clavier redevient en qwerty ; on le configurera d'une façon permanente avec l'interface web:
On choisit **l'option 8** pour demarrer le shell puis on tape la commande suivante
`#kbdcontrol -l fr` ou `#kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd`

a. Déclaration des interfaces

Maintenant on va déclarer nos trois interfaces : Wan, lan et opt1 :
C'est pour cela on choisit l'option 1



Après il faut prendre les choix encadrés en rouge

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
OPT1 -> em2

Do you want to proceed [y|n]? y
```

A la fin on doit avoir le résultat suivant

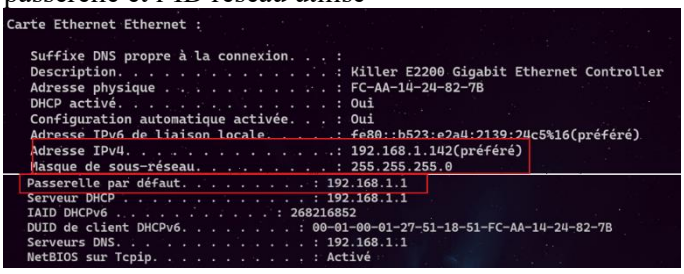
```
WAN (wan)       -> em0        ->
LAN (lan)       -> em1        -> v4: 192.168.1.1/24
OPT1 (opt1)     -> em2        ->
```

Maintenant on va affecter les adresses IP à nos trois interfaces,

b. Assignement des adresses aux interfaces wan, lan et opt1

- L'interface Wan.

Le choix de des adresses qu'on va affecter à cette interface dépend de la configuration de notre box internet c'est pour cela il faut faire une **ipconfig /all** sur la machine physique pour déterminer la passerelle et l'ID réseau utilisé



Donc notre réseau est

Id réseau **192.168.1.0/24**

DNS/Passerelle **192.168.1.1**

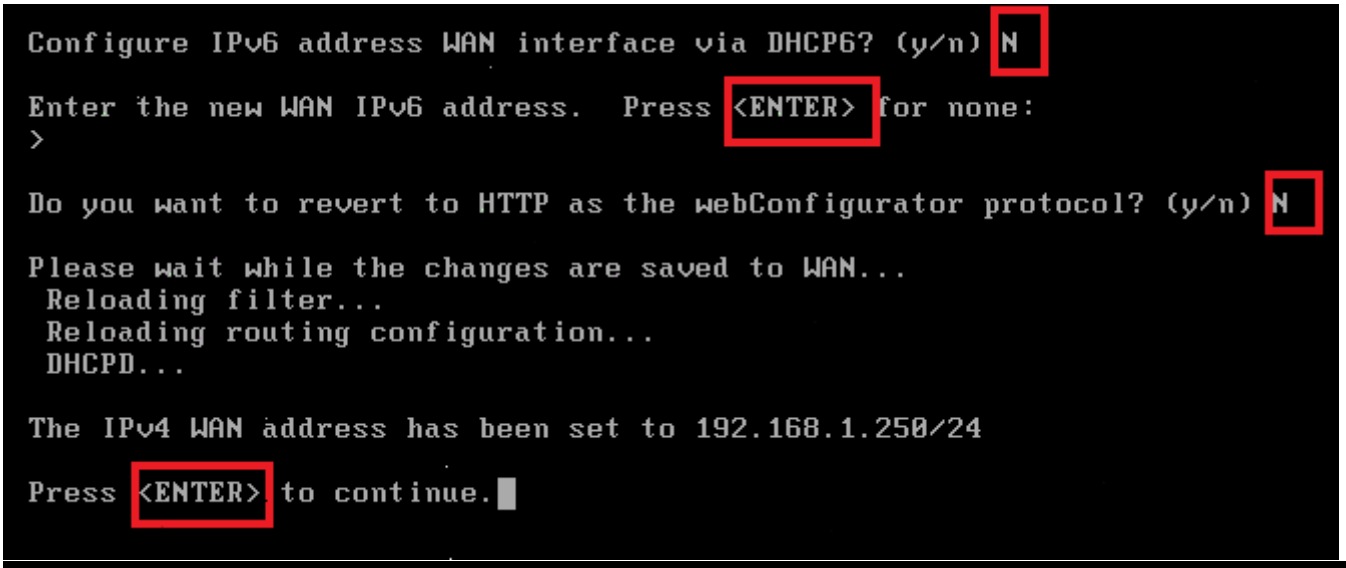
On choisit l'option 2

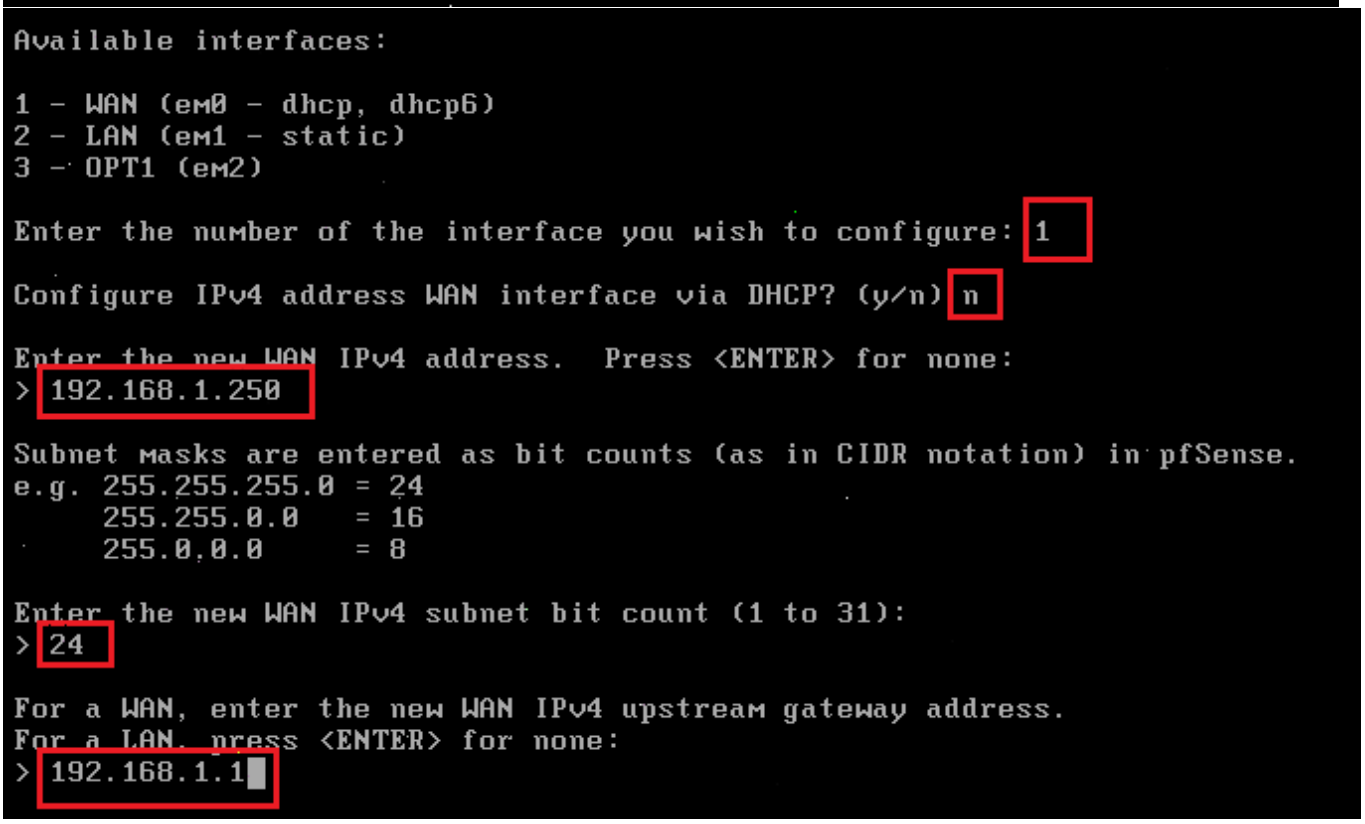
```
Enter an option: 2
```

Et on fait les choix suivants

@ip :192.168.1.250

Masque de sous réseau 255.255.255.0
Passerelle 192.168.1.1
Pas de DHCP IPv5
Pas de IPv6
Pas de DHCP6
Le webconfigurateur pour des raisons de sécurité il est préférable de ne pas le mettre sur l'interface Wan



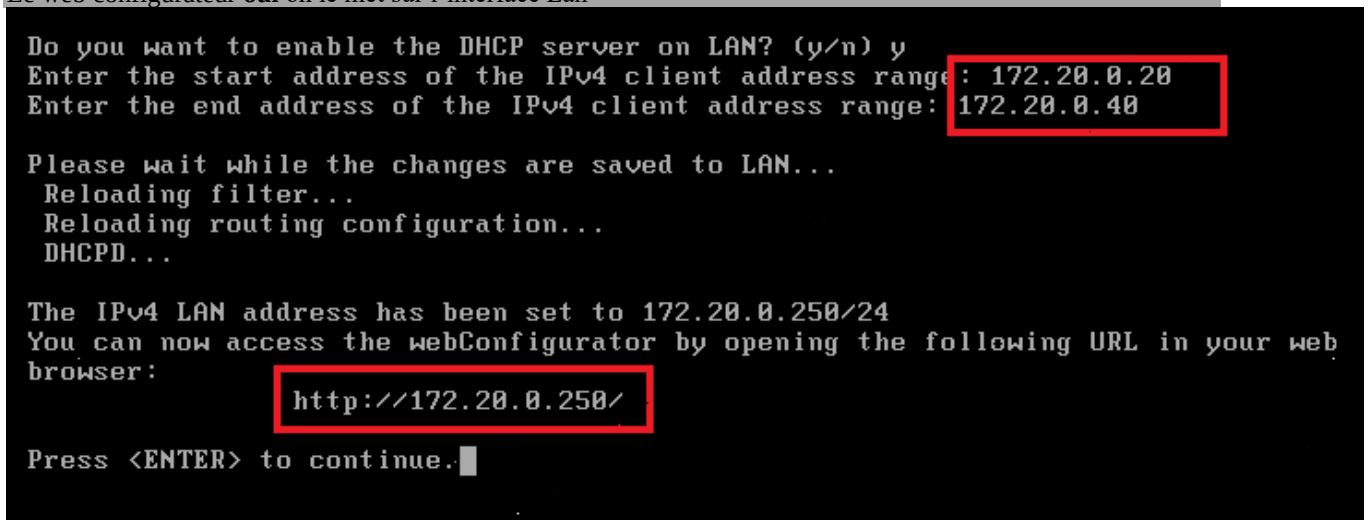


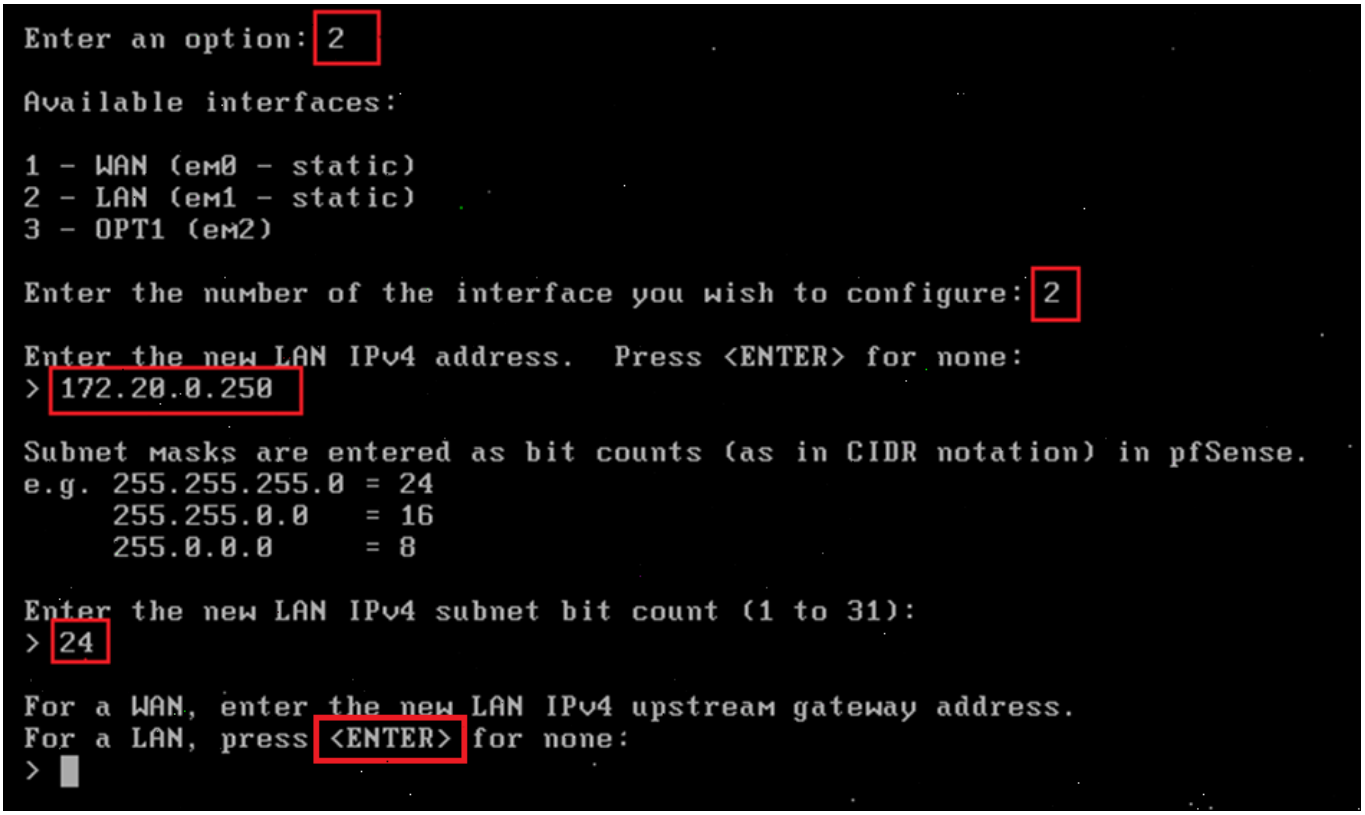
- L'interface lan

Et on fait les choix suivants

@ip :172.20.0.250
Masque de sous réseau 255.255.255.0
Passerelle : non
DHCP IPv5 oui on crée un étendu de : 172.20.0.20--à172.20.0.30
Pas de IPv6

Pas de DHCP IPV6
Le web configurateur **oui** on le met sur l'interface Lan





- L'interface opt

@ip :192.168.2.250
Masque de sous réseau 255.255.255.0
Passerelle : non
Pas de DHCP IPv5
Pas de IPv6
Pas de DHCP6

```
Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) n

Please wait while the changes are saved to OPT1...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT1 address has been set to 192.168.2.250/24

Press <ENTER> to continue.


Enter an option: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.2.250

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```


2) Portail captif

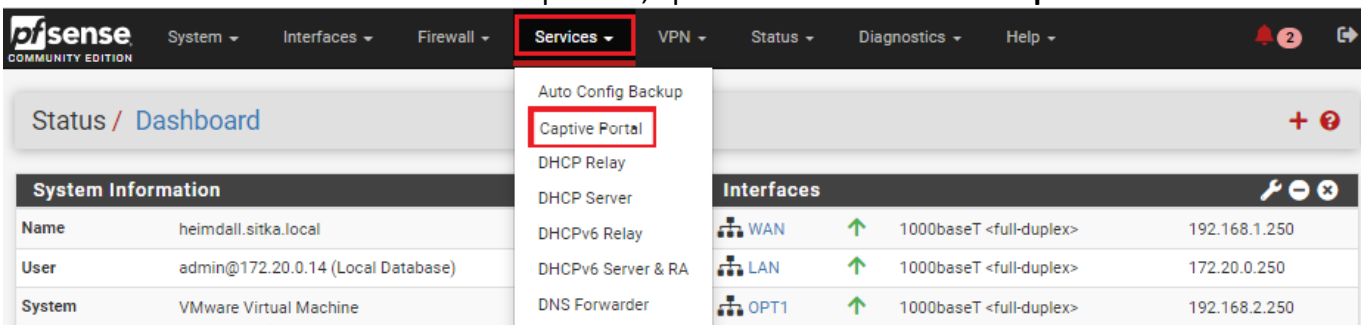
Portail Captive

1. **Introduction**

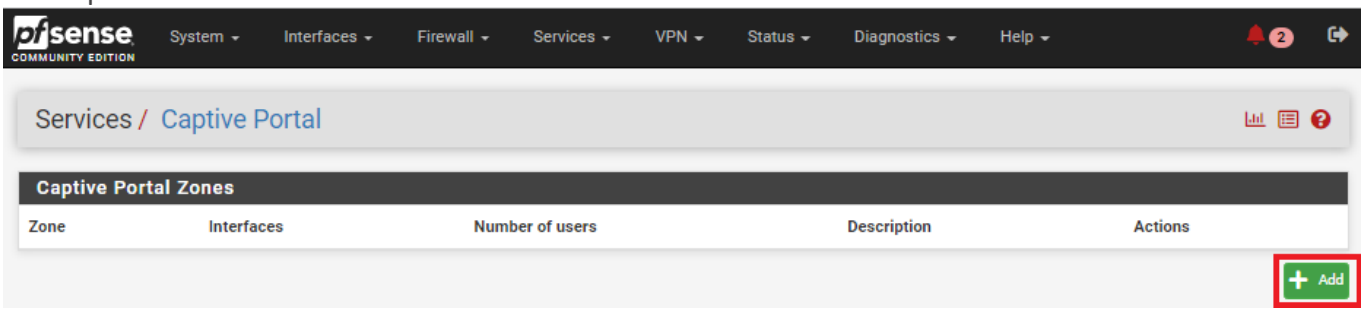
Le portail captif est un moyen qui force les clients d'un réseau de passer par une page Web d'authentification pour pouvoir se connecter à Internet.
Il est utilisé dans des réseaux assurant un accès public comme certain espace de la SNCF, les hôtels, les établissement scolaires …

2. **Activation du portail captive**

On se connecte sur l'interface de web de pfsense, après on va sur **Services + Captive Portal**

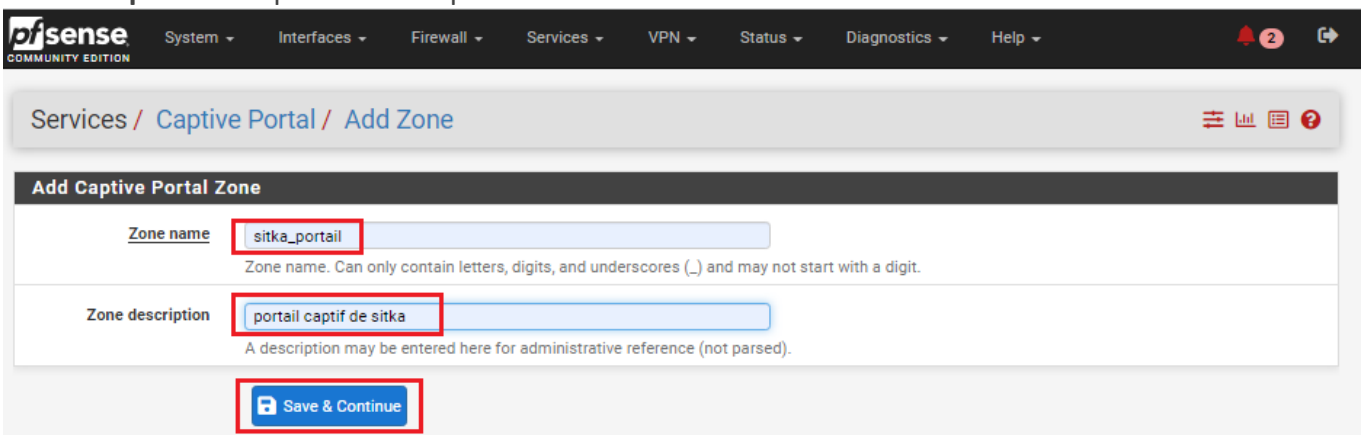


On clique sur **Add**

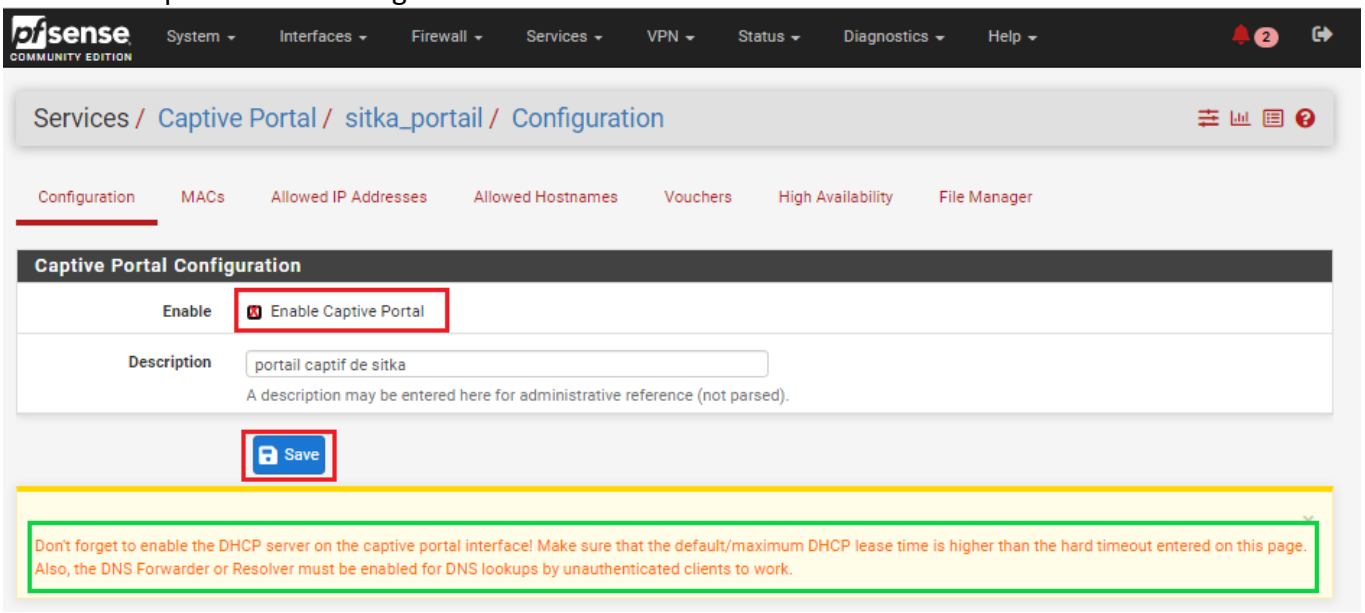


On renseigner le Nom du Portail Captif et sa description :
Sitka_portal pour le nom de la zone

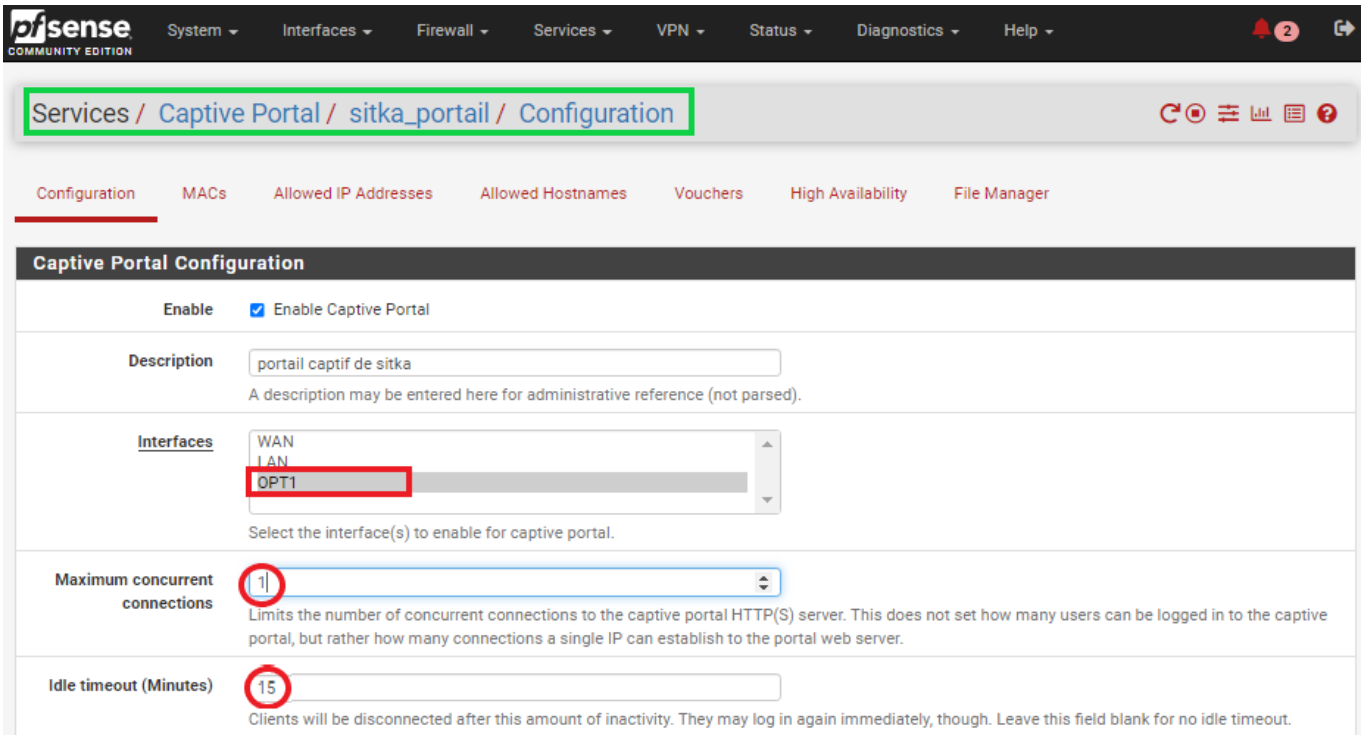
Portail captive sitka pour la description de la zone



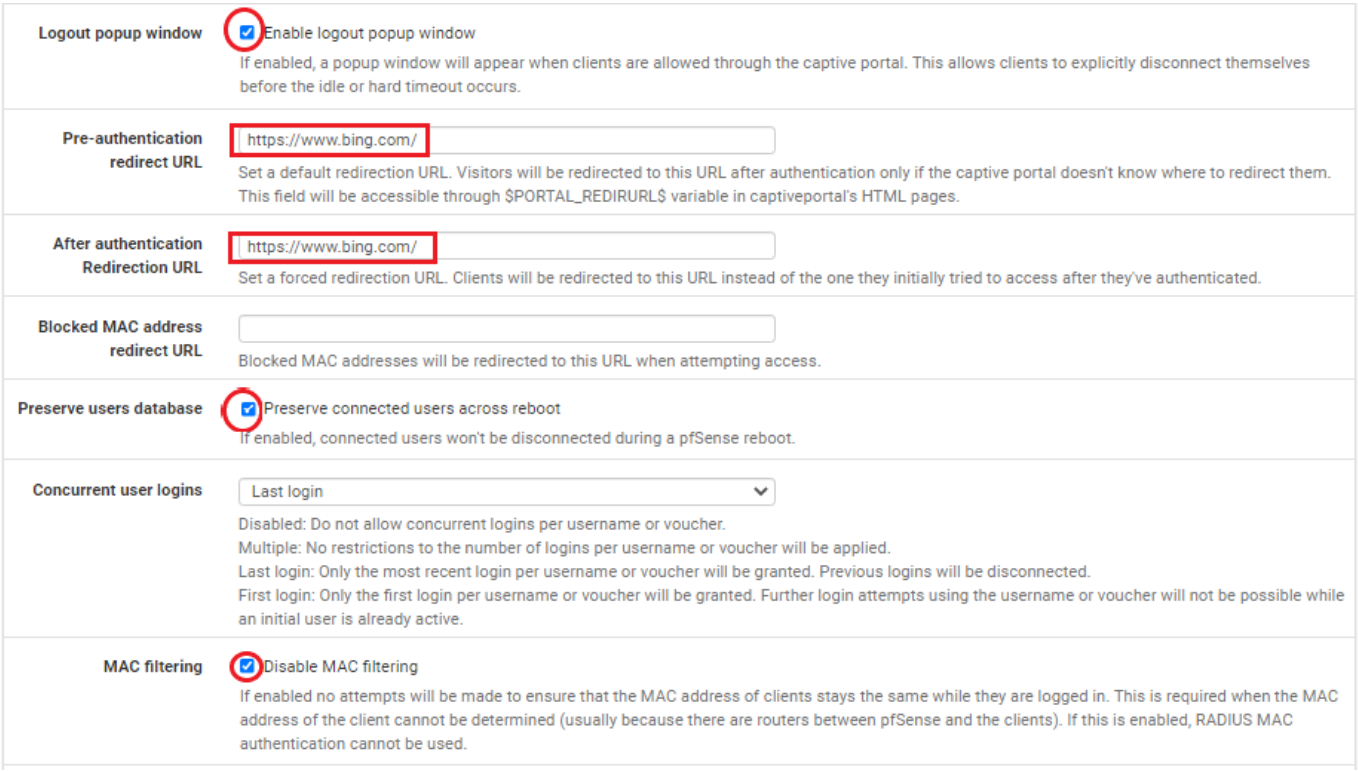
On active le portail et on enregistre



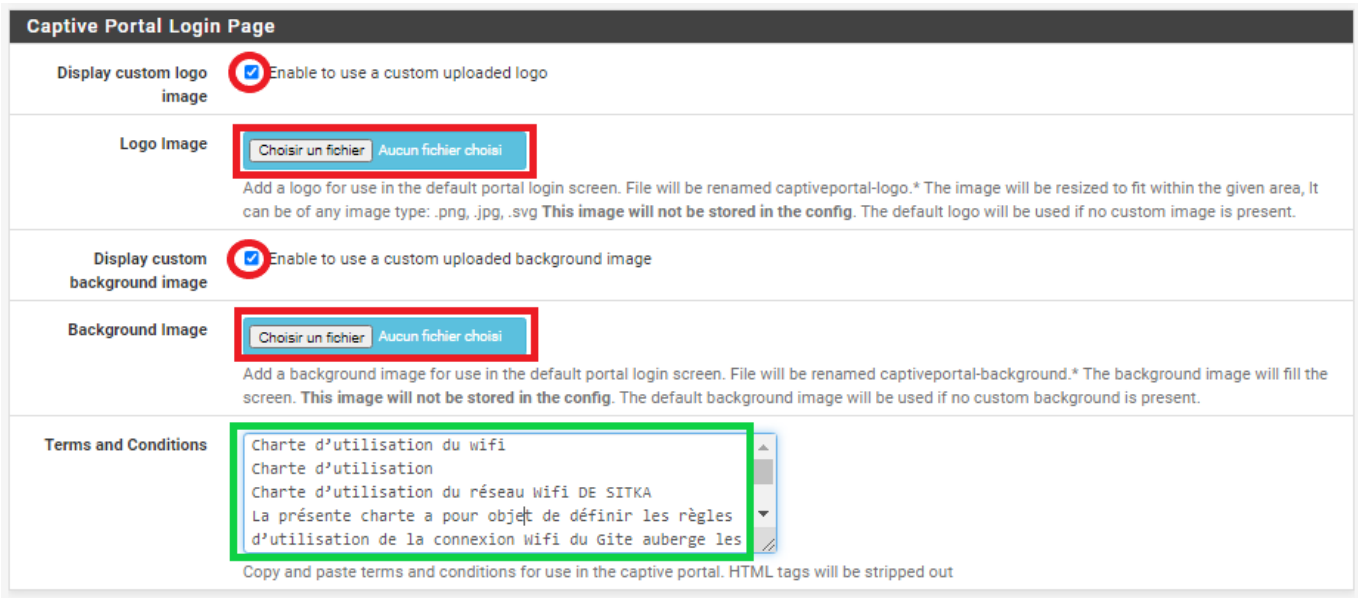
- On active **Enable Captive Portal**
- On sélectionne l'interface **Opt1**
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur)
- Idle timeout (Minutes) on choisit **15**:(Les clients seront déconnectés après cette période d'inactivité)



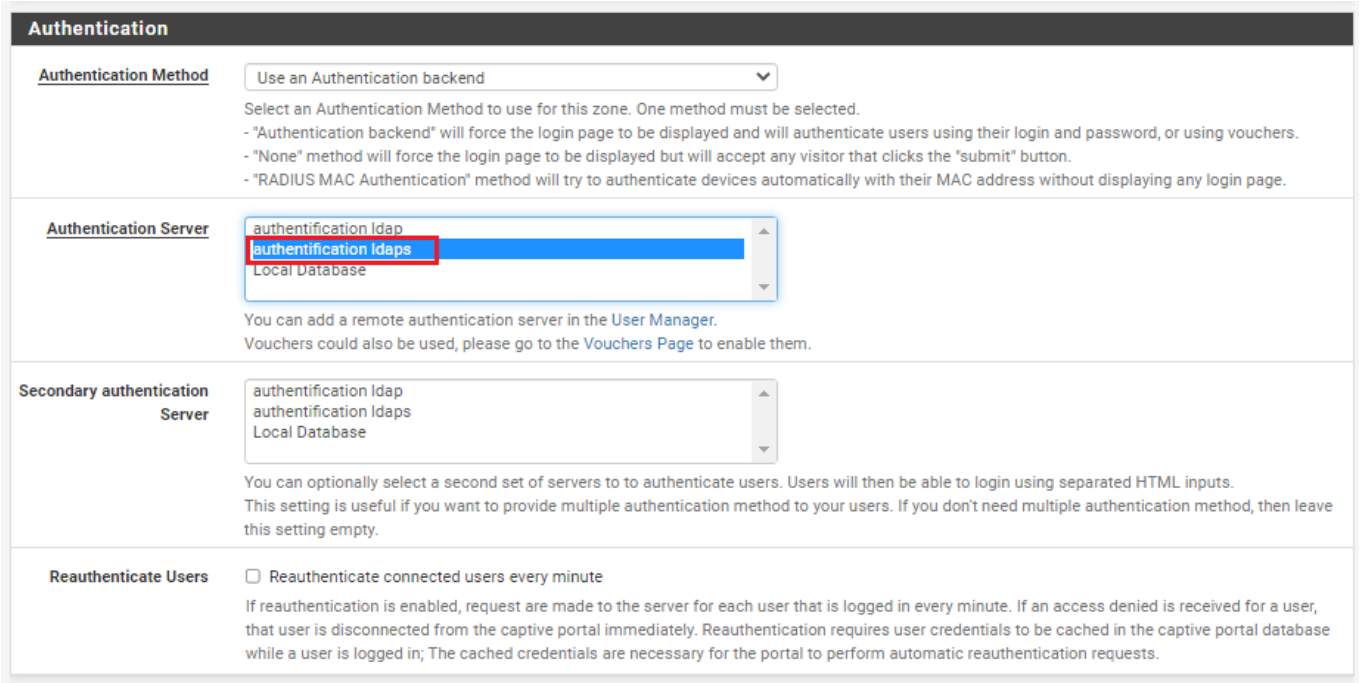
- Définir **After authentication Redirection URL** (**URL HTTP** de redirection Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont tenté d'accéder après s'être authentifiés)
- Activer **Disable Concurrent user logins** (seule la connexion la plus récente par nom d'utilisateur sera active)
- Activer **Disable MAC filtering** (lorsque l'adresse MAC du client ne peut pas être déterminée)



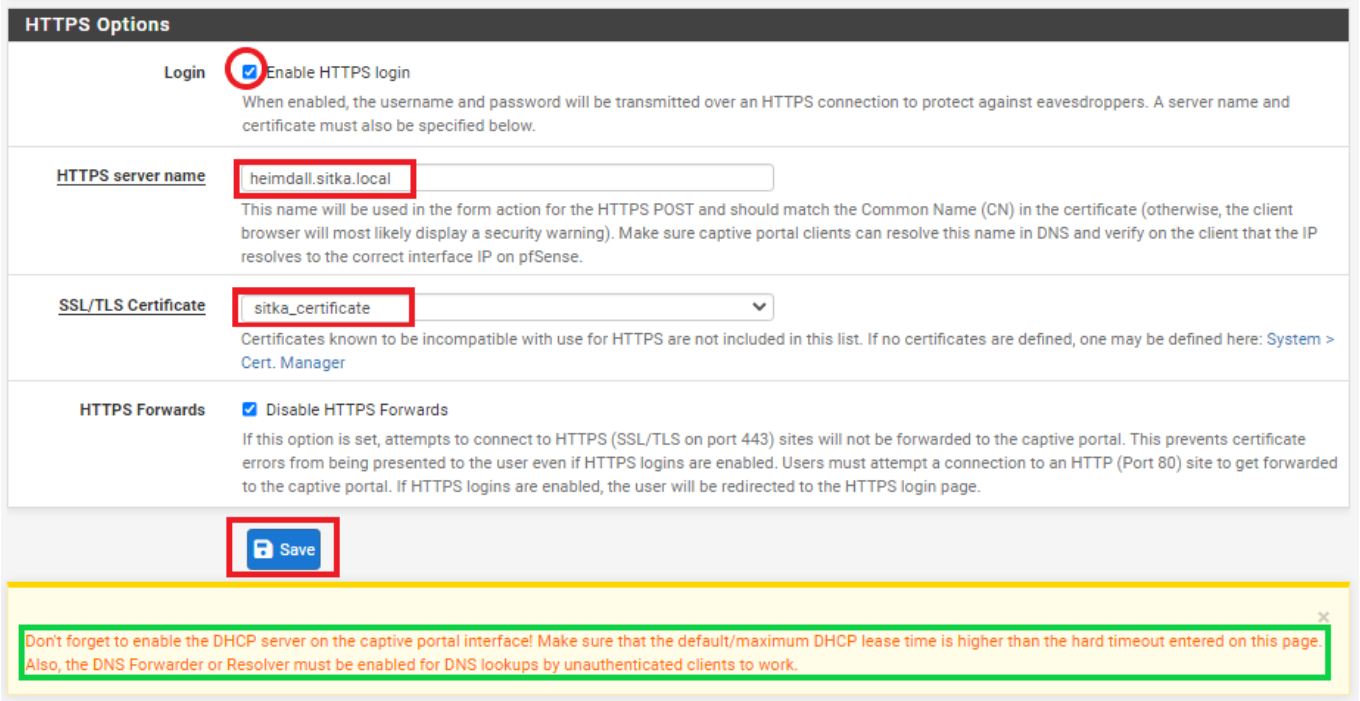
On peut choisir un logo et une image d'arrière-plan ainsi qu'un charte de connexion



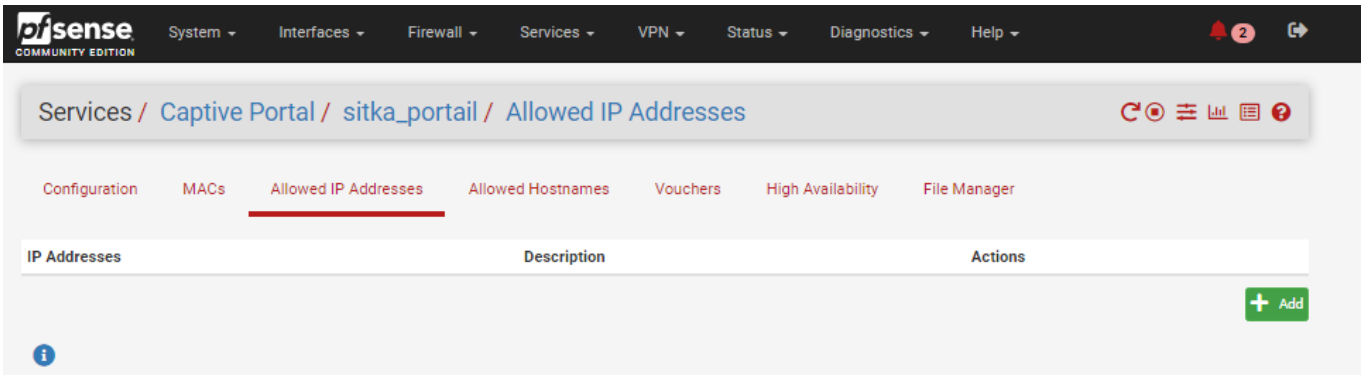
- On sélectionne **Use an Authentication backend**
- On sélectionne **Authentification LDAPS** comme méthode d'authentication

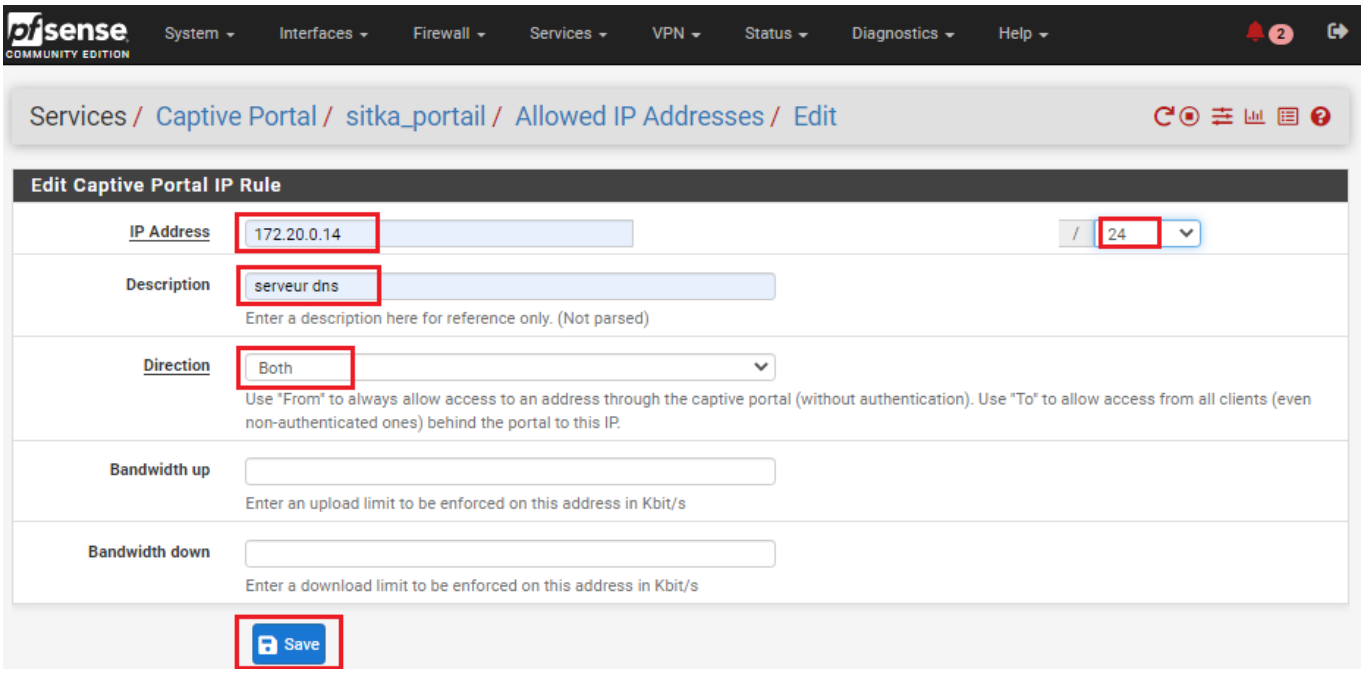


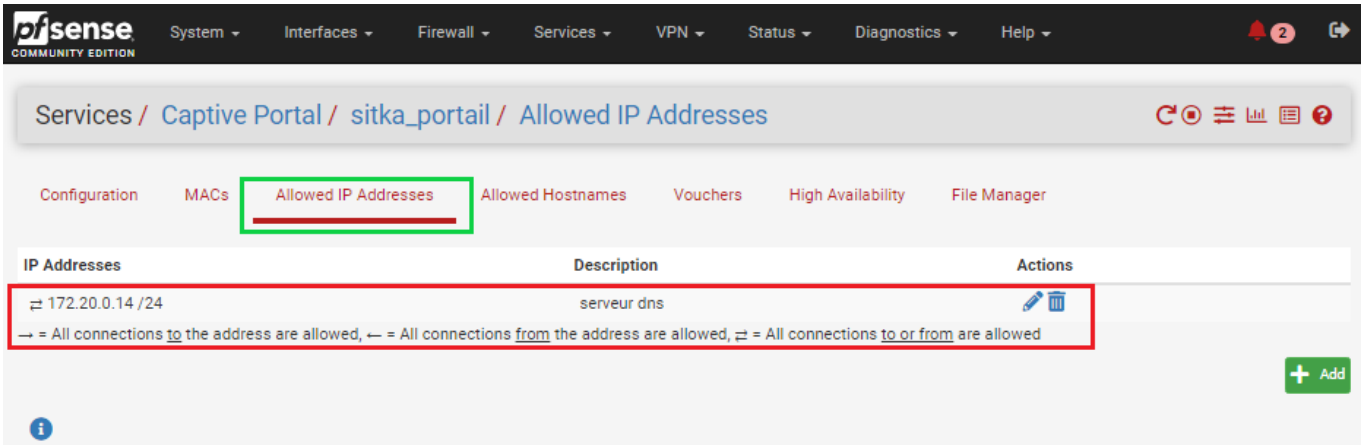
On active ssl pour notre portail active



Les clients ont besoin d'une résolution DNS donc on va autoriser cette résolution en autorisant l'adresse IP du DNS 172.20.0.14

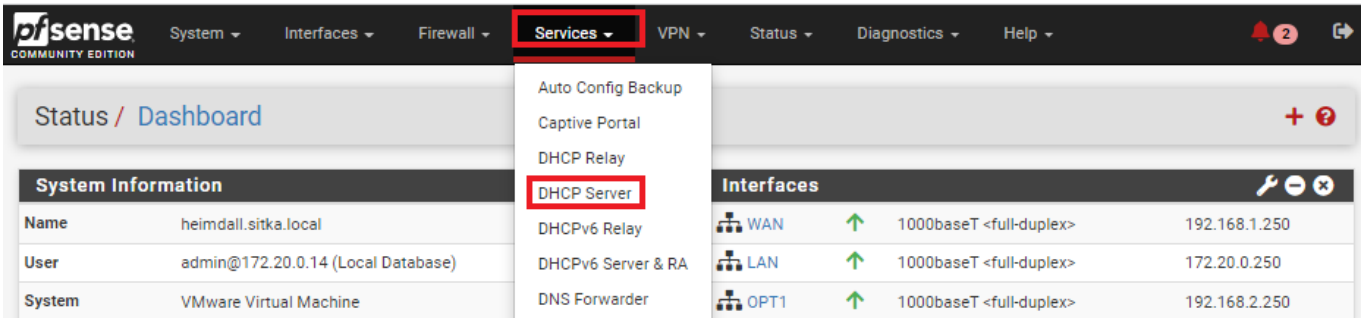




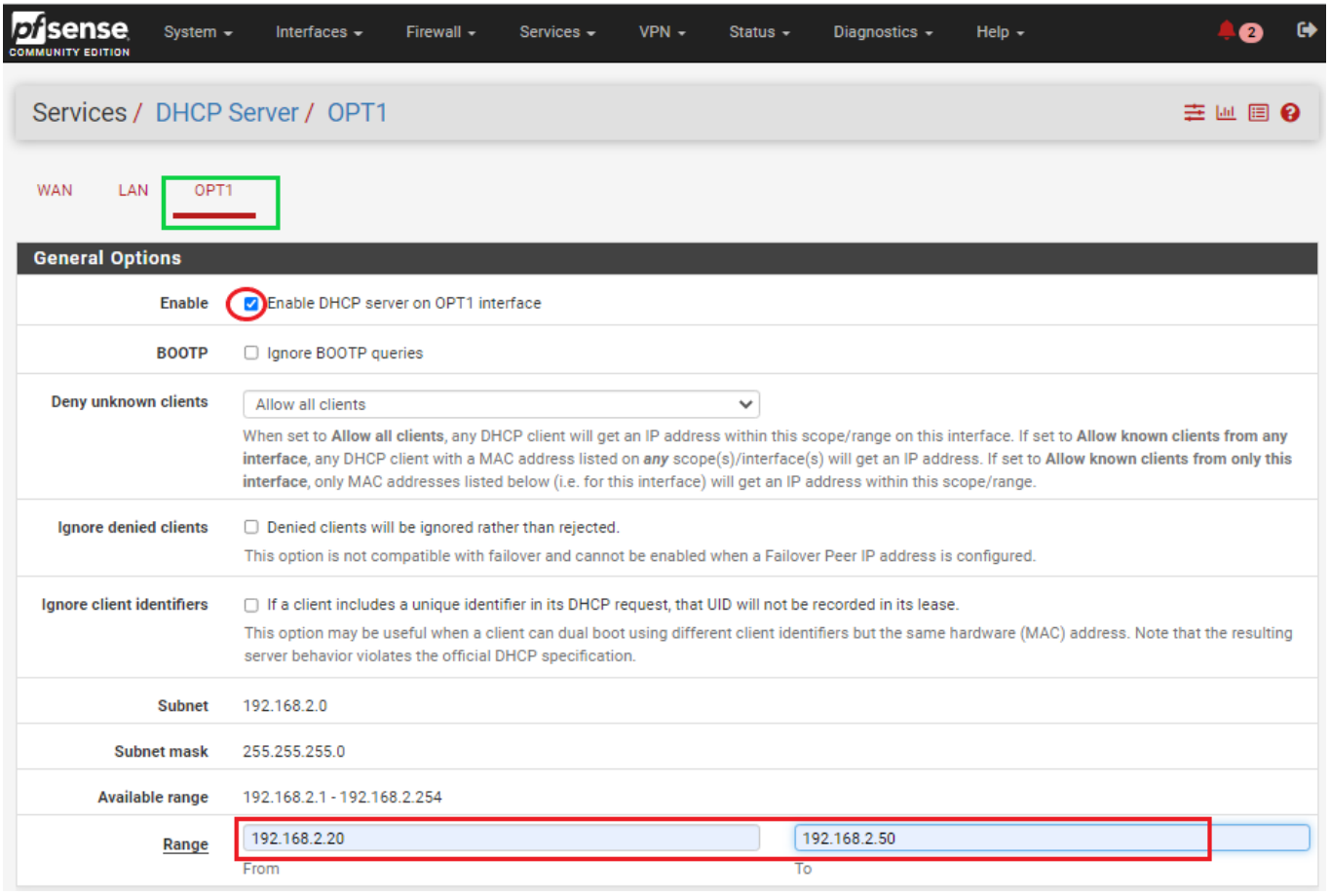


3. **Configuration du DHCP**

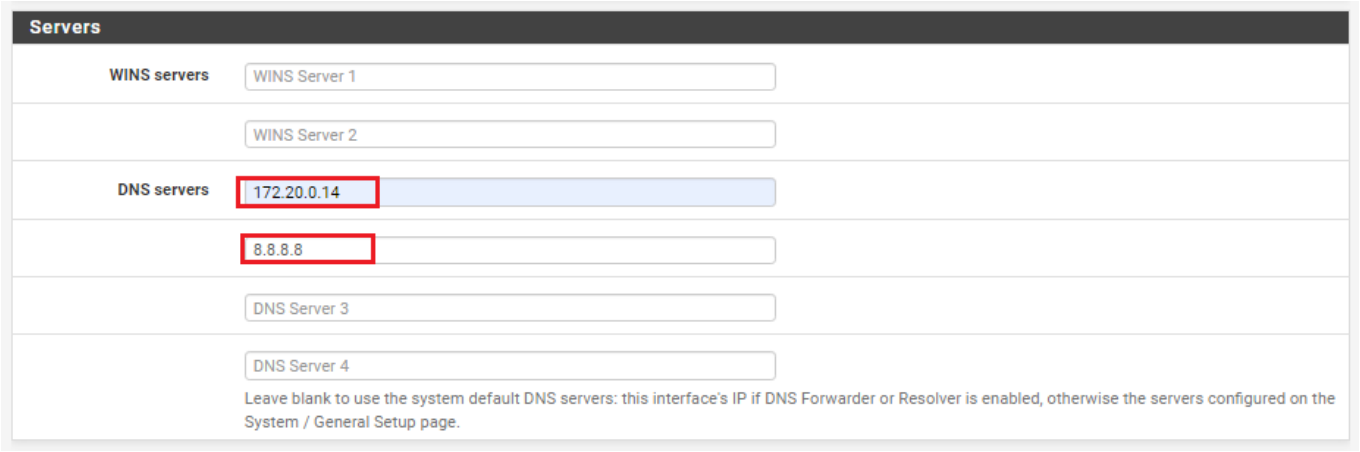
Maintenant On va activer le DHCP sur l'interface opt1



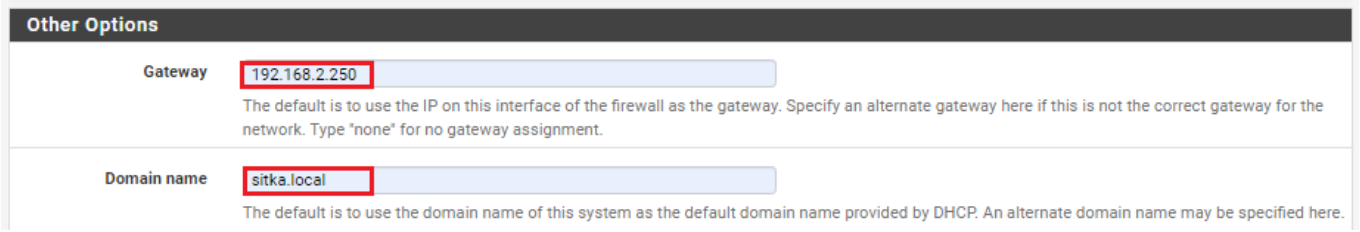
On déclare notre étendue



On rentre l'adresse de notre DNS

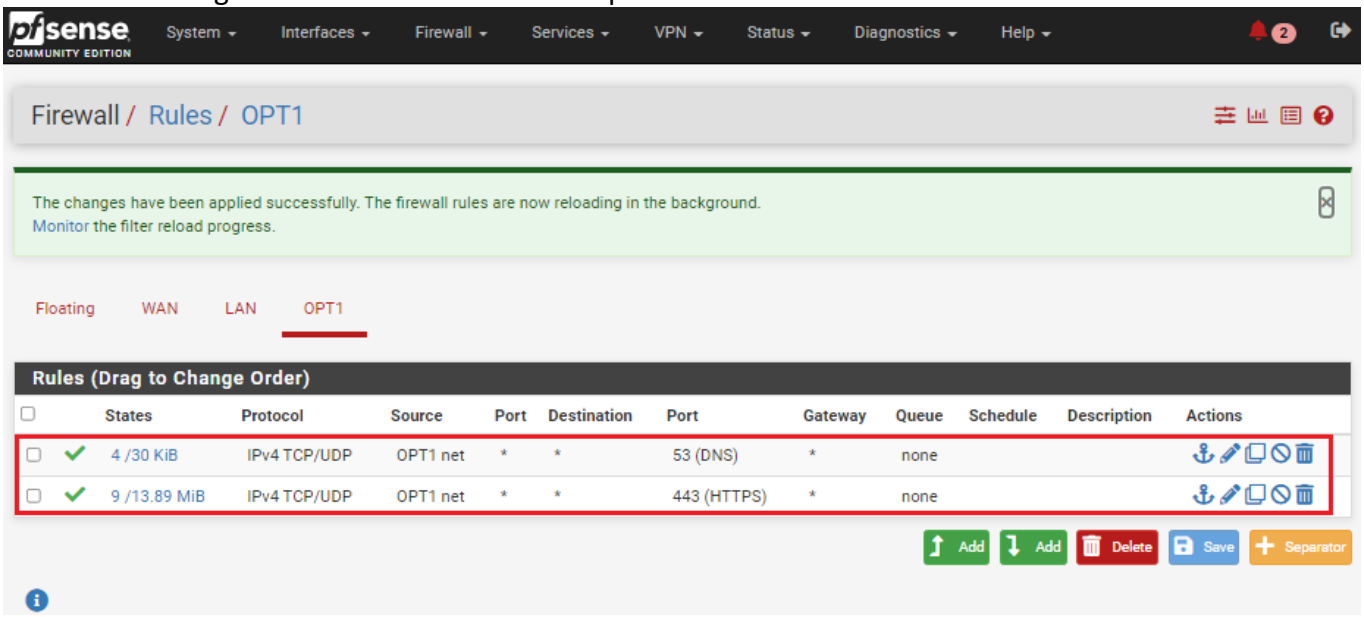


On rentre l'adresse de la passerelle et du nom de domaine



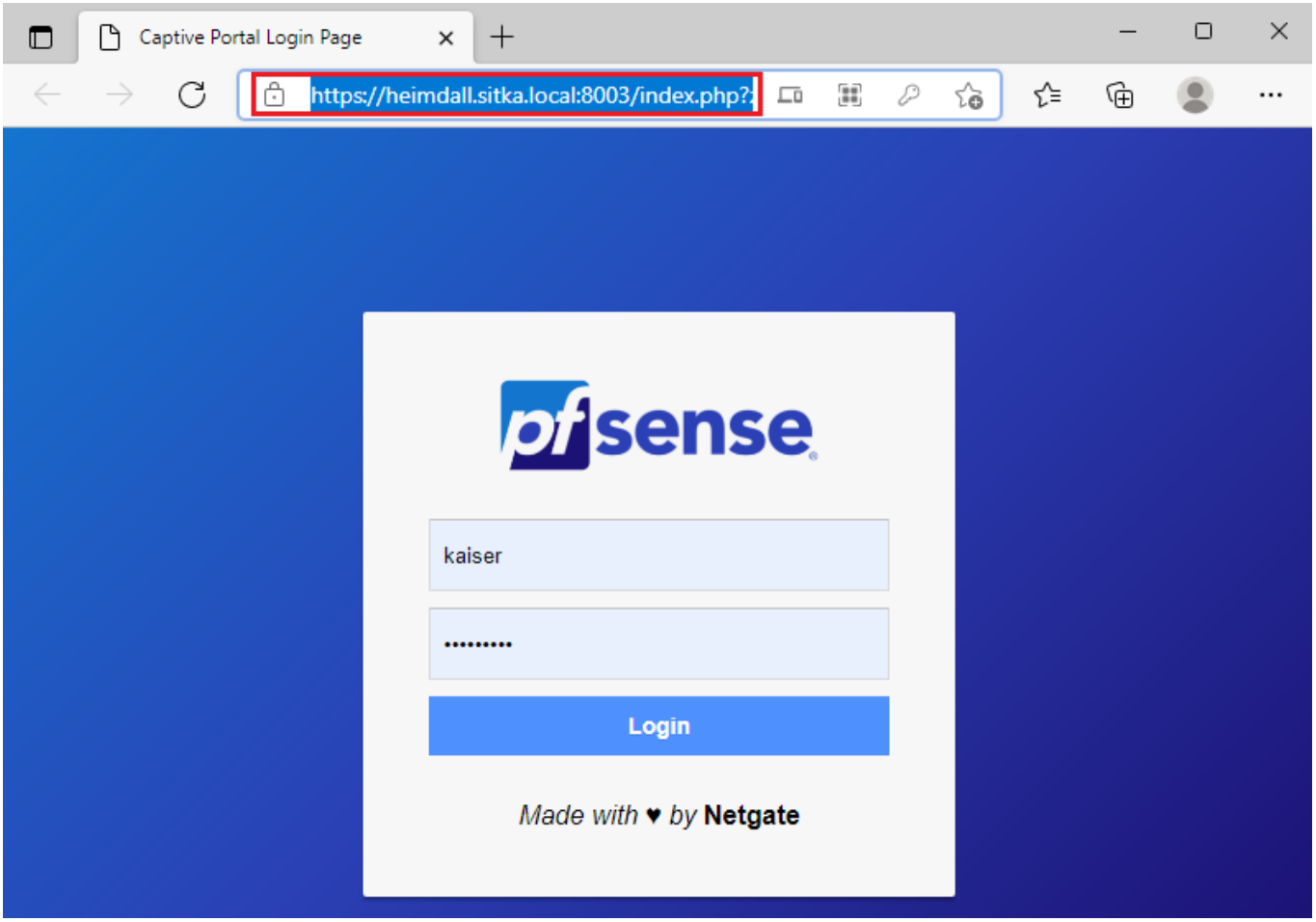
4. Création des règles sur le firewall

On Cree deux règles autorisant le DNS et le https

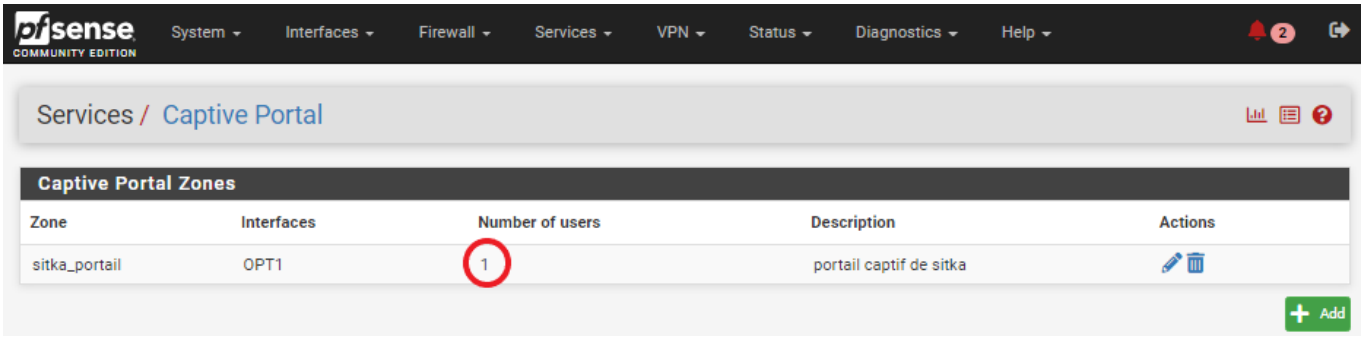


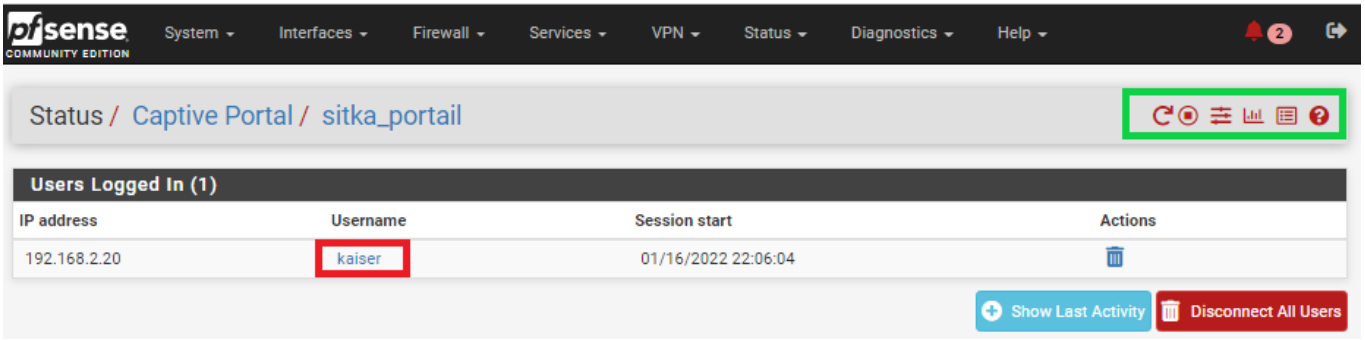
5. Test de notre portail captive

On fait notre test de connexion

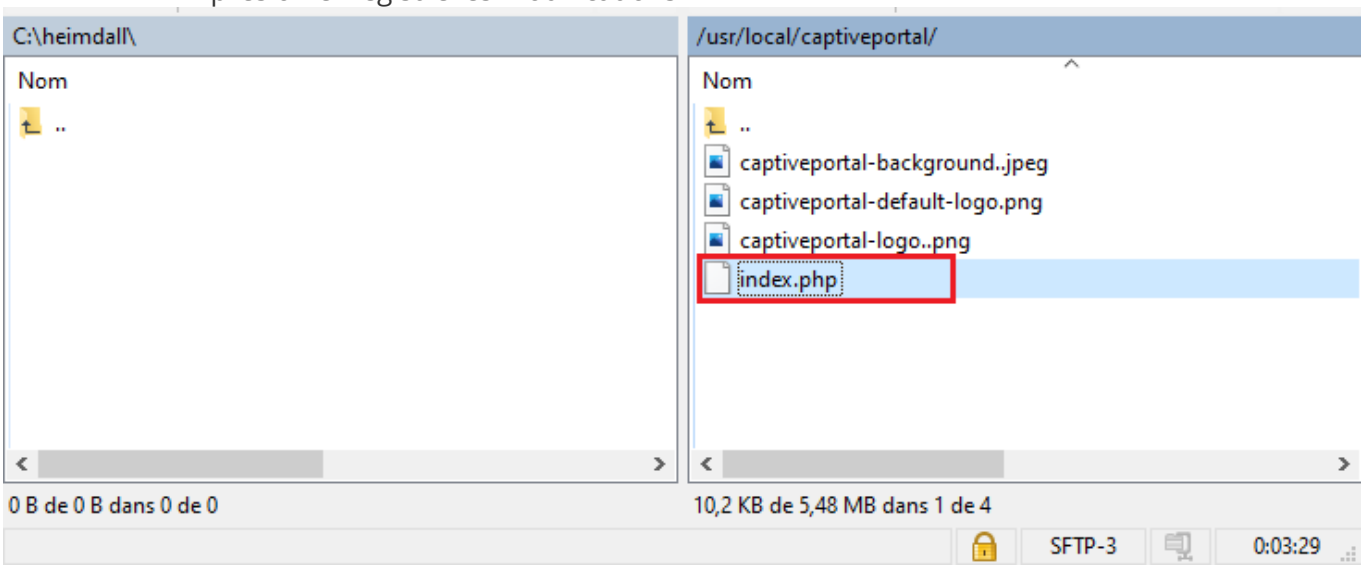


Sur pfsense on peut vérifier les connexions



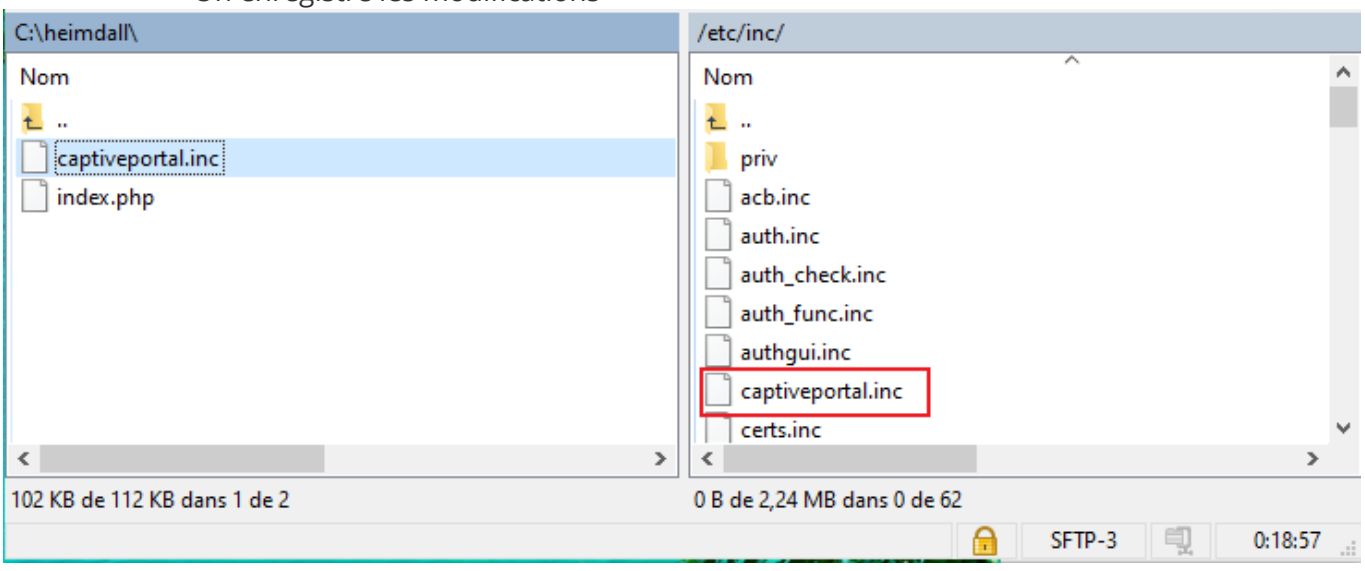


- On chercher **You are connected** et remplacer par **Vous êtes connecté**
- On chercher **Disconnecting…** et **You have been disconnected** et on remplacer par **Déconnexion…** et **Vous êtes déconnecté**
- On cherche **Invalid credentials specified** et on remplace **par Les informations saisies sont invalides,** il y a 2 lignes à modifier
- Après on enregistre les modifications



Maintenant on va sur /etc/inc puis et on ouvre captiveportal.inc

- On chercher Captive Portal login Page et on remplacer par : Portail Captif de sitka
- On chercher Login et Made with … by … Netgate et on remplacer par Connexion et Connectez-vous avec votre compte LDAPS
- On chercher User et Password et on Remplace par Utilisateur et Mot de Passe
- On rechercher Logout et Click the button below to disconnect on remplace par **Déconnexion et Cliquez sur le bouton ci-dessous pour vous déconnecter**
- On enregistre les modifications



3) Snort IDS-IPS

1. Introduction

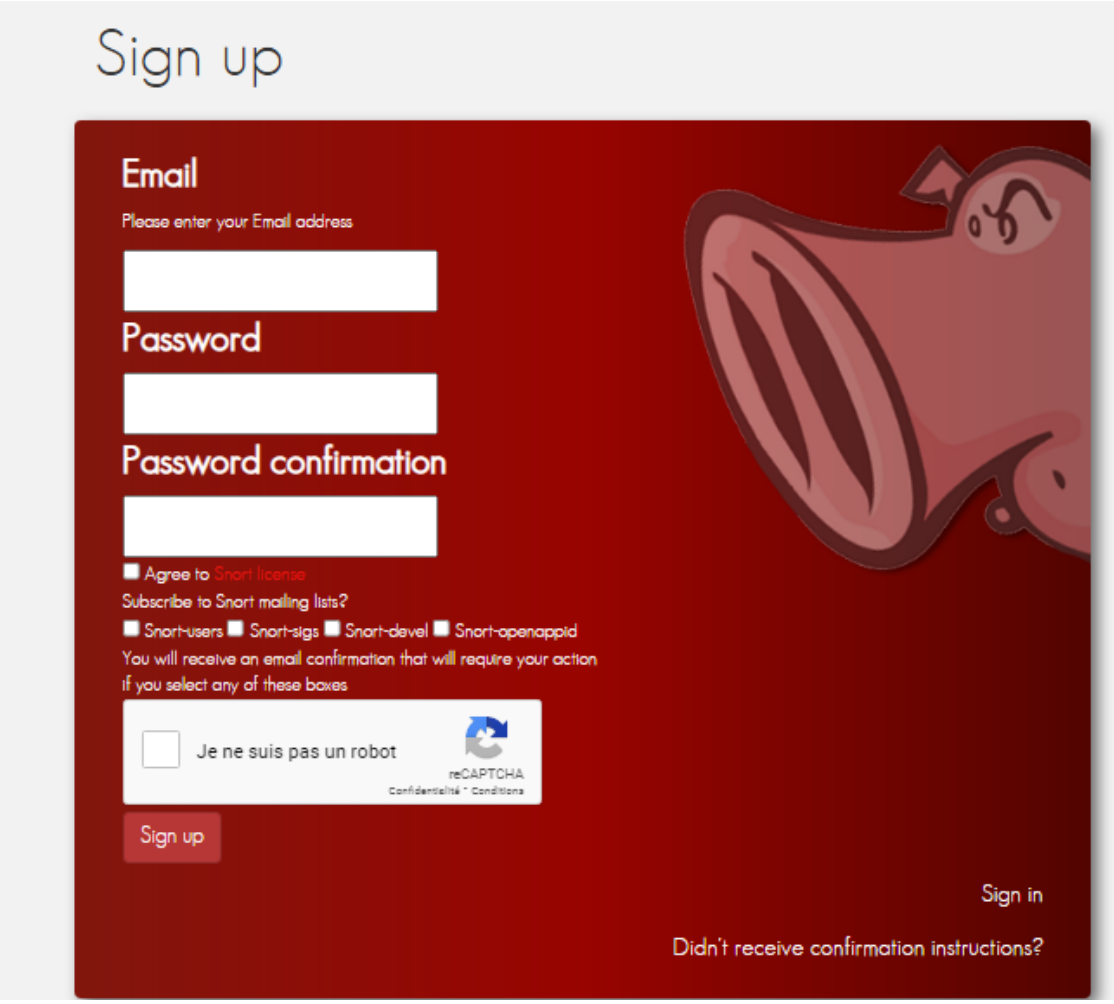
Dans cette partie consacrée à Pfsense on va voir comment installer le package Snort sur PfSense, et ainsi un IDS voir même un IPS !
On va d'abord voire un peu ce qu'est un IDS et un IPS et la différence entre eux.
Les IDS (Intrusion Detection Systems) n'a pas comme rôle de bloquer les attaques, IDS utilisent une base de données d'attaques afin de :

- Analyser et surveiller le trafic réseau pour détecter une cyberattaque.
- Détecter les violations de la politique de sécurité,
- Détecter les malwares et les scanners de port.

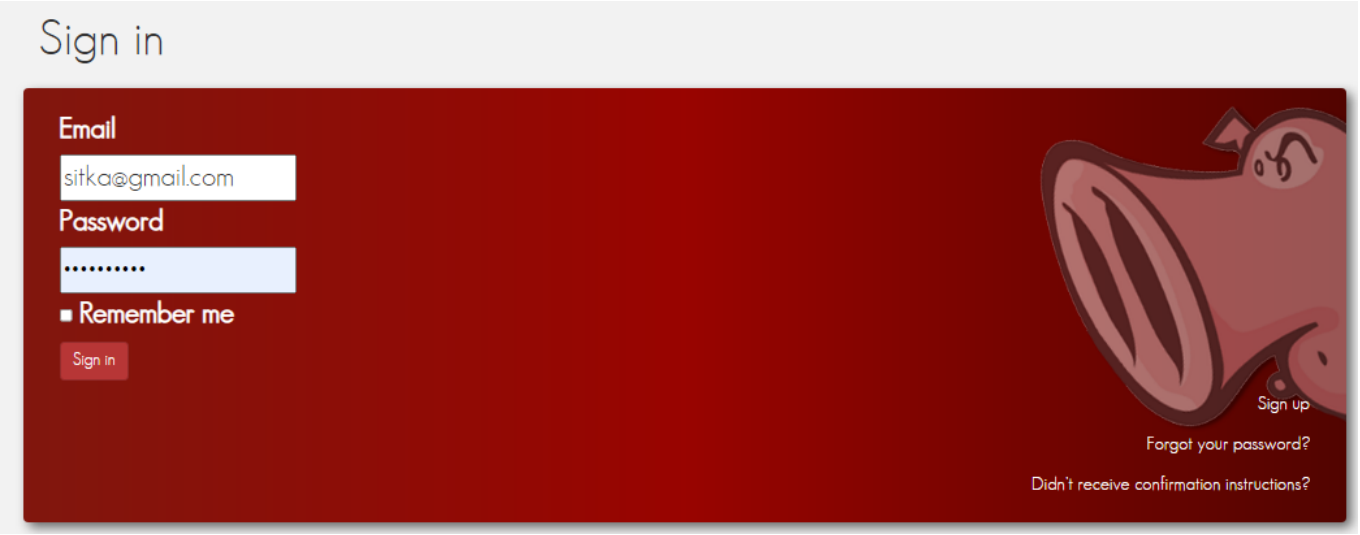
Les IPS (Intrusion Prevention Systems): Les IPS bloquent et rejettent les paquets réseau en utilisant un profil de sécurité en cas de menaces .

2. Création d'un compte dans Snort

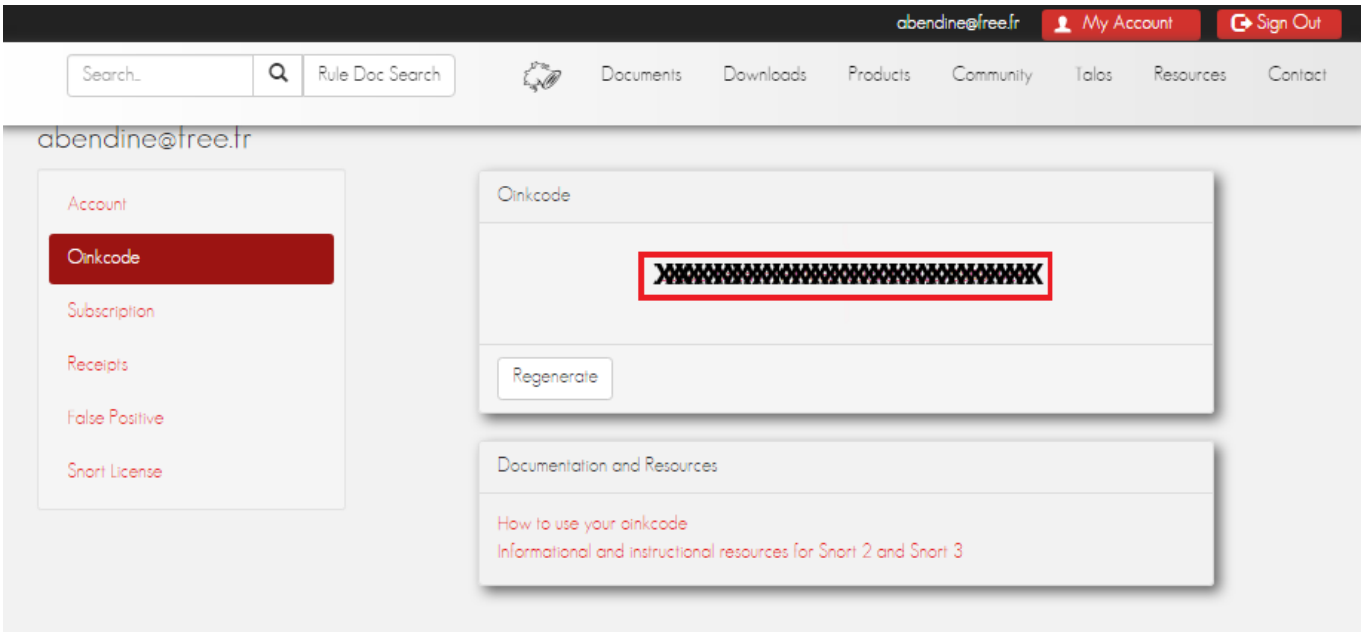
Il faut créer un compte sur le site officiel de Snort (https://www.snort.org/users/sign_up)
, car Snort va nous fournir une clé (**Snort Oinkmaster Code)** qui nous servira à la mise à jour des règle Snort.
Une fois le formulaire d'inscription est rempli il faut se rendre sur la messagerie qu'on a renseigné dans notre formulaire d'inscription pour confirmer notre inscription à partir du mail envoyé par Snort.



Une fois L'inscription confirmé on se rend sur le site de Snort https://www.snort.org/et on se connecte avec nos identifiants

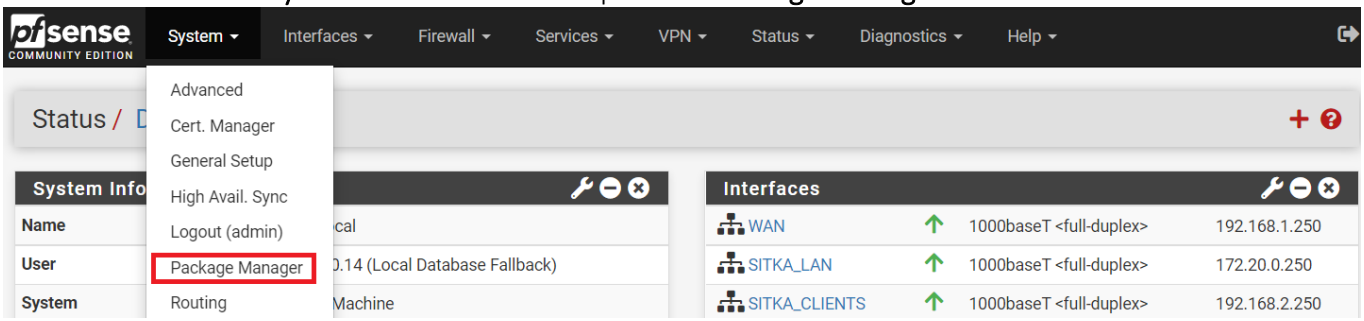


Une fois connecté on va dans le menu Oincode pour récupérer le code de téléchargement et de mise à jour des règles Snort

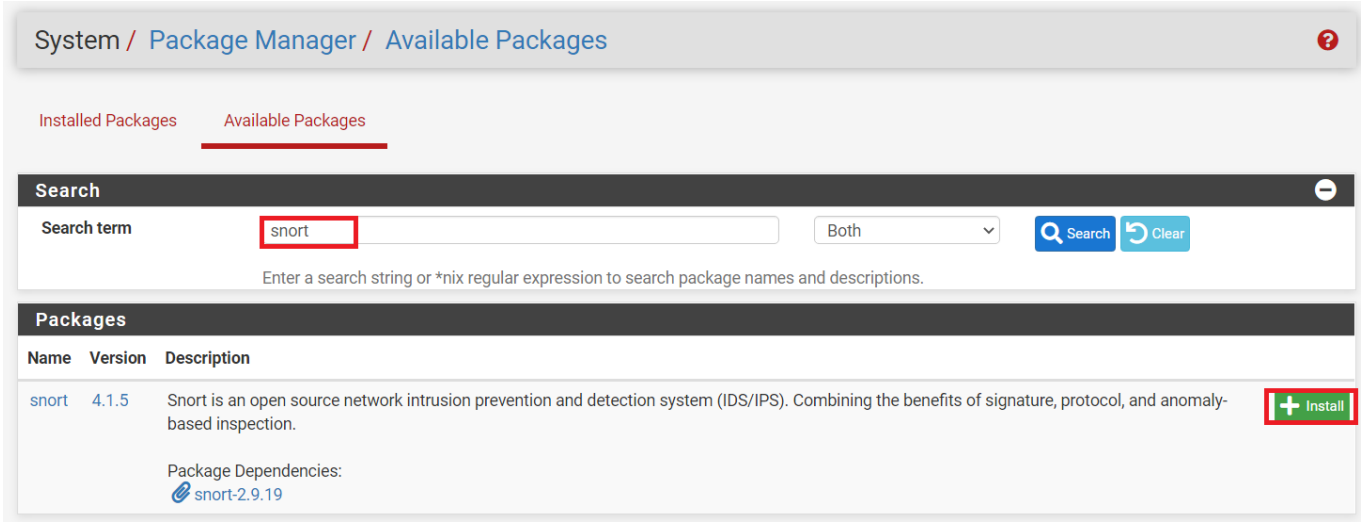


3- Installation de Snort

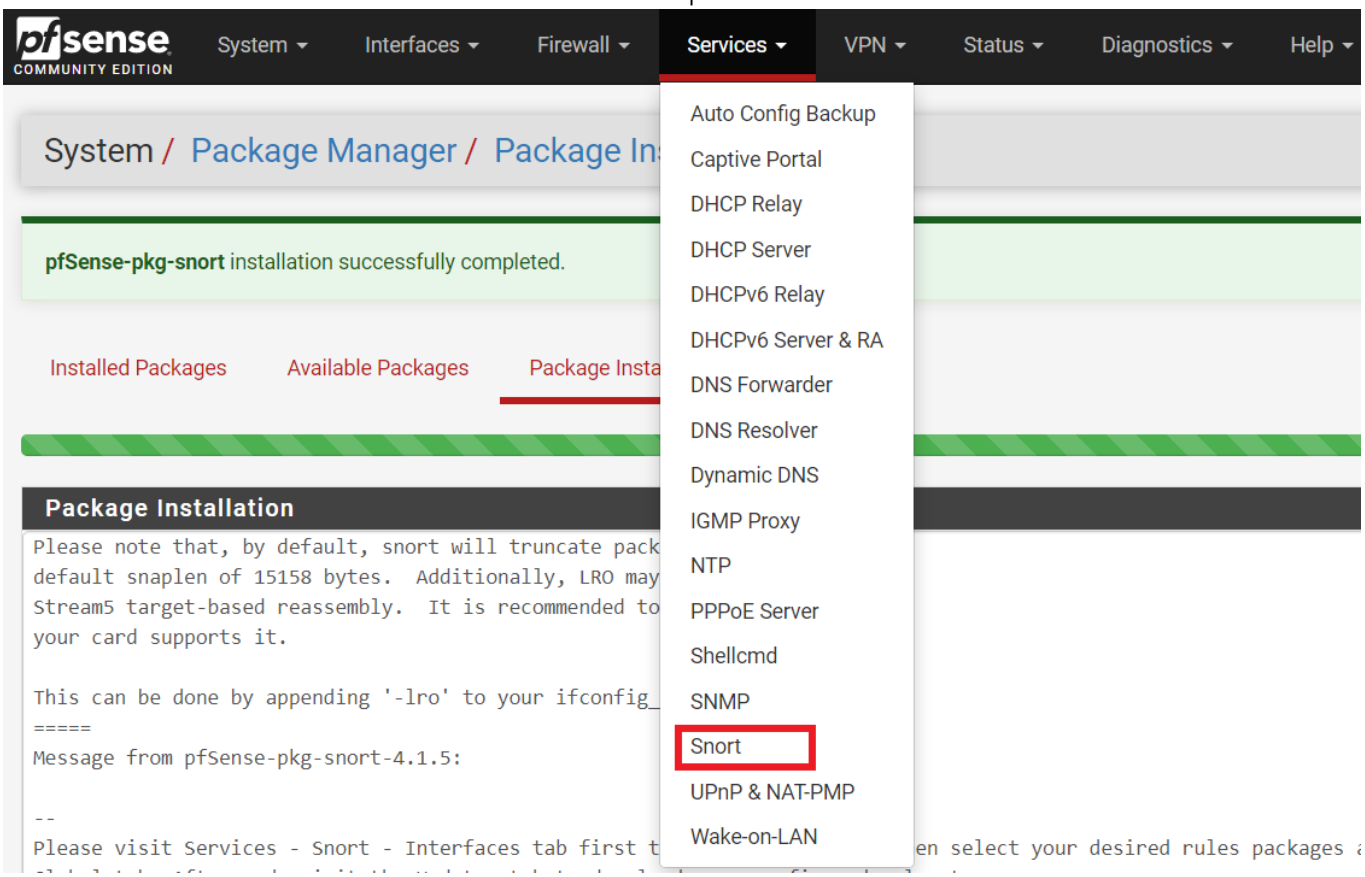
On accède au menu **System** et sélectionnez l'option de **Package Manager**.



Sur l'écran de **Package Manager**, accédez à l'onglet **Available Paquages**.
Sur le moteur de recherche, on cherche Snort et on installe le paquet Snort.



Accédez au menu Pfsense Services et sélectionnez l'option Snort.

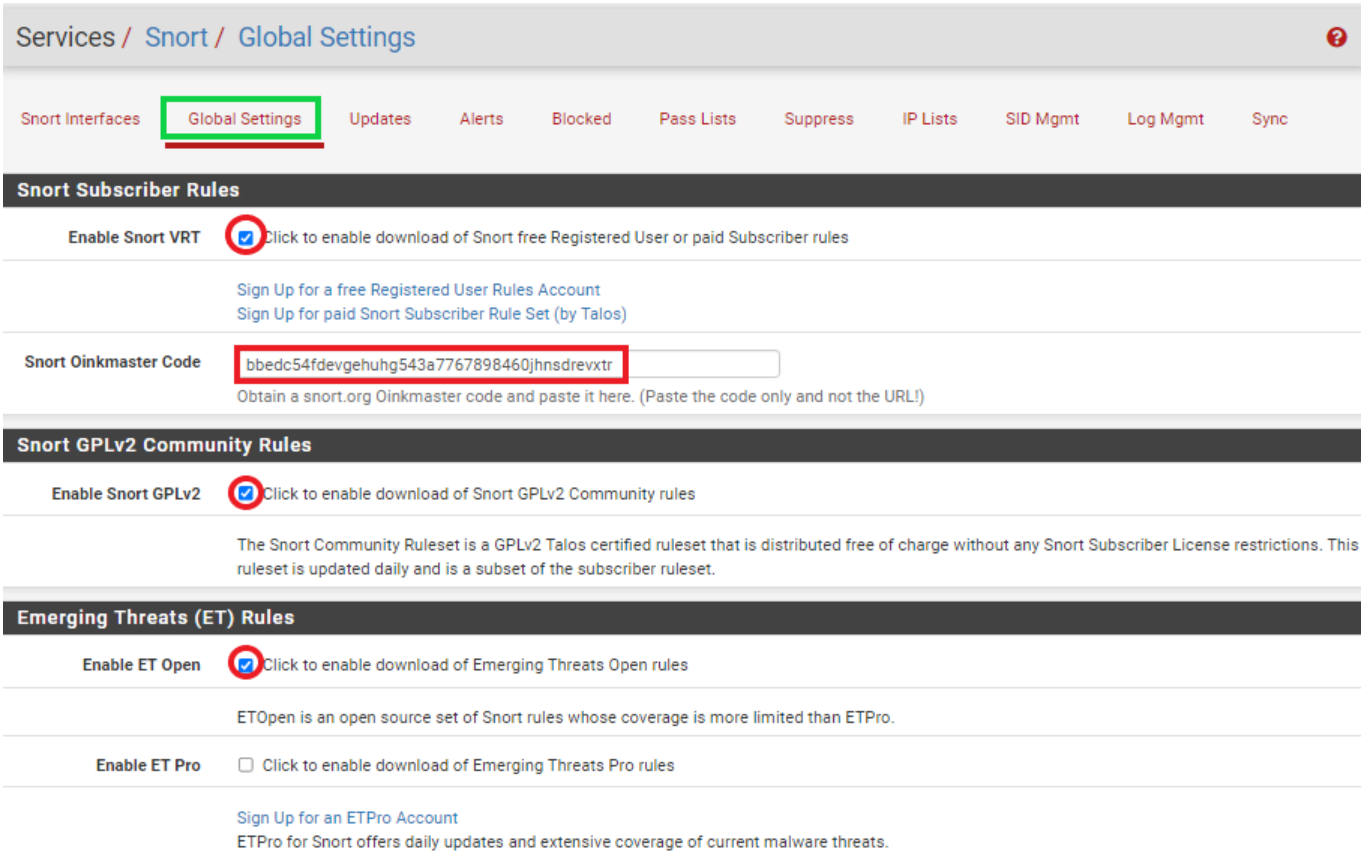


4. Configuration de Snort

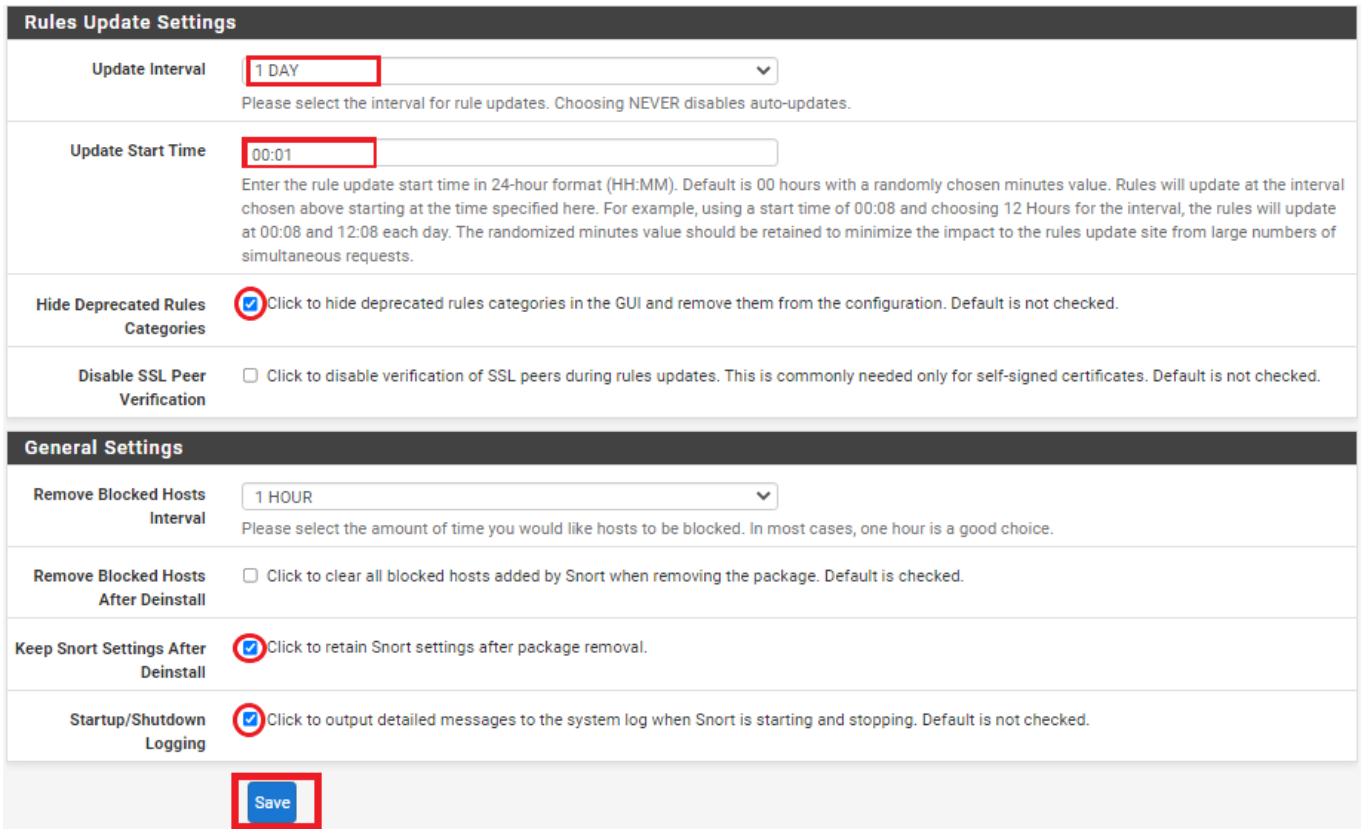
On va dans l'onglet **Global Settings**, dans cette étape on va activer le téléchargement de règles gratuites, en cochant la case **Enable Snort VRT**.

Et ensuite nous pouvons cocher les cases :

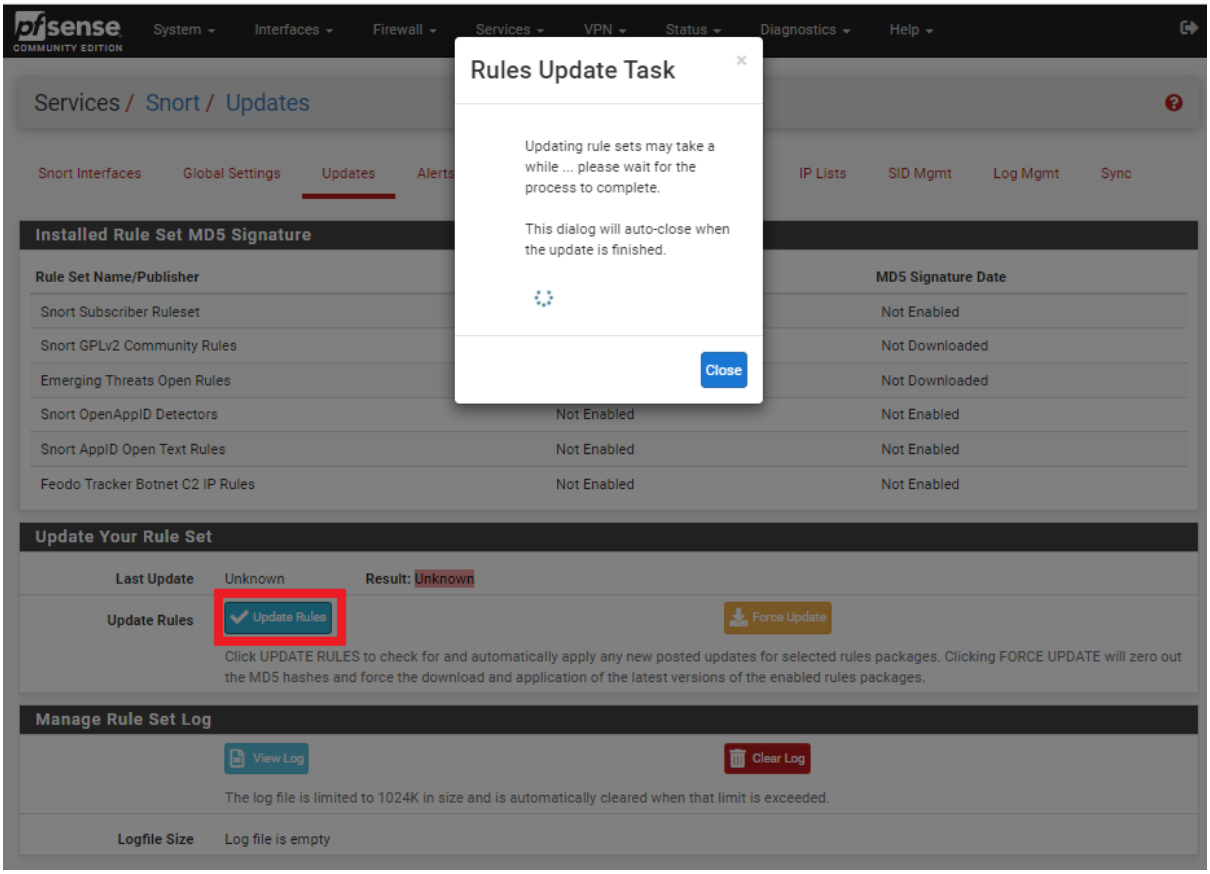
- **Enable Snort GPLv2**,
- **Enable ET Open**,
- **Enable OpenAppID**, On ne coche pas car il faut une licence



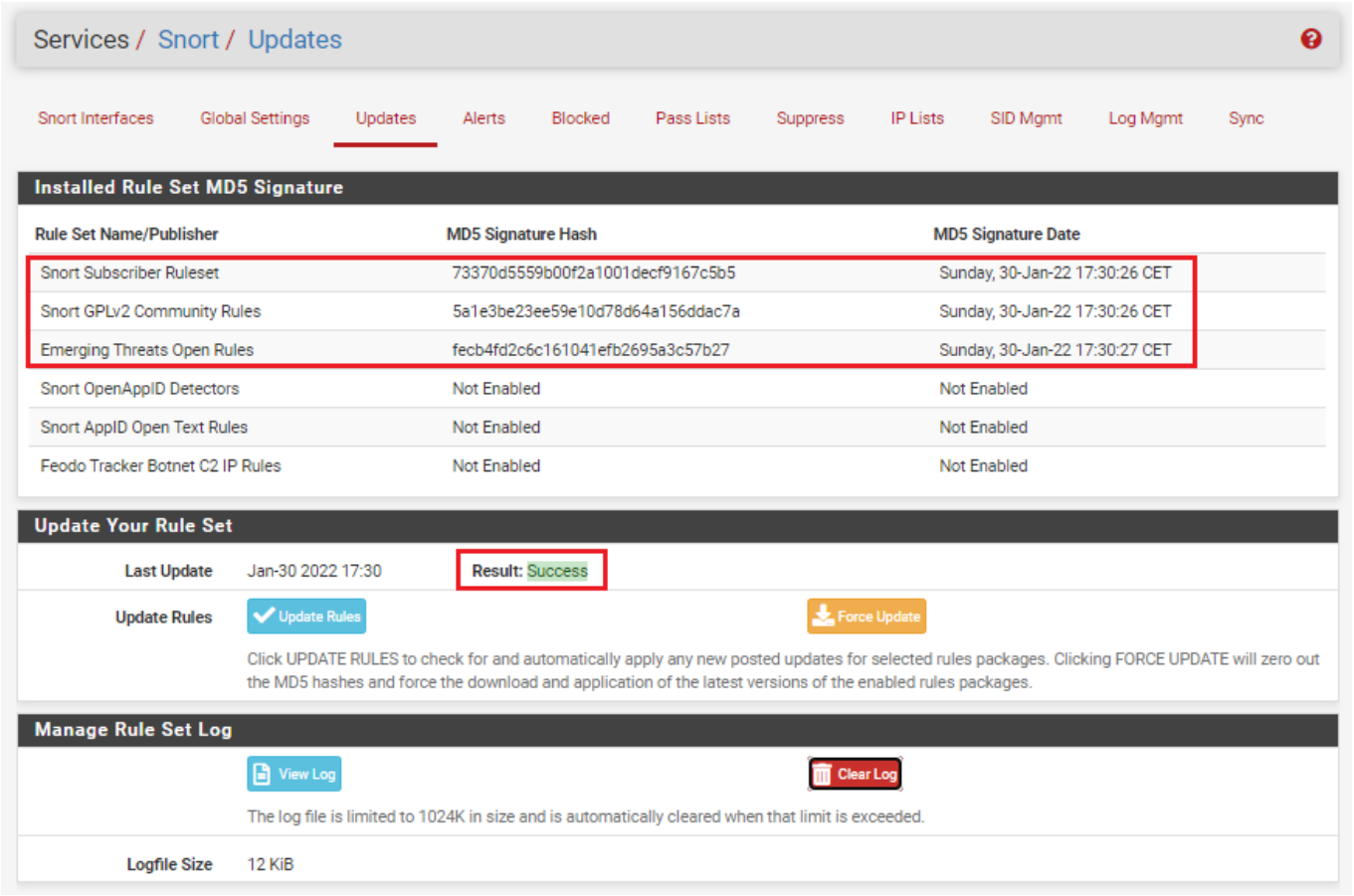
Dans la zone **Rules Update Settings** on effectue la configuration suivante :
Update Interval :1 DAY
Update Start Time : 00 :01
Hide Deprecated Rules Categories : On coche
Remove Blocked Hosts Interval : 1 HOUR
Keep Snort Settings After Deinstall : Si on désinstalle Snort on laisse les paramètres de configuration On coche
Startup/Shutdown Logging : pour avoir les log On coche



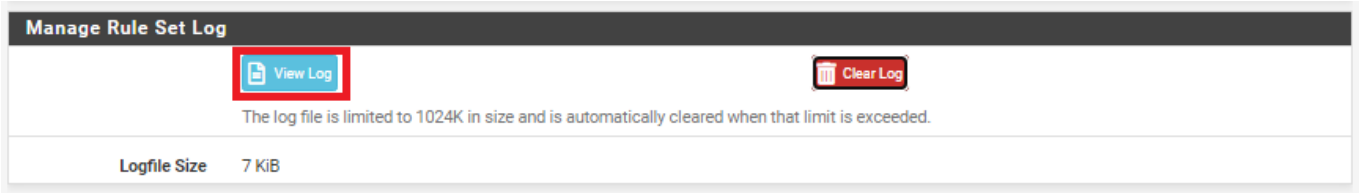
Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.

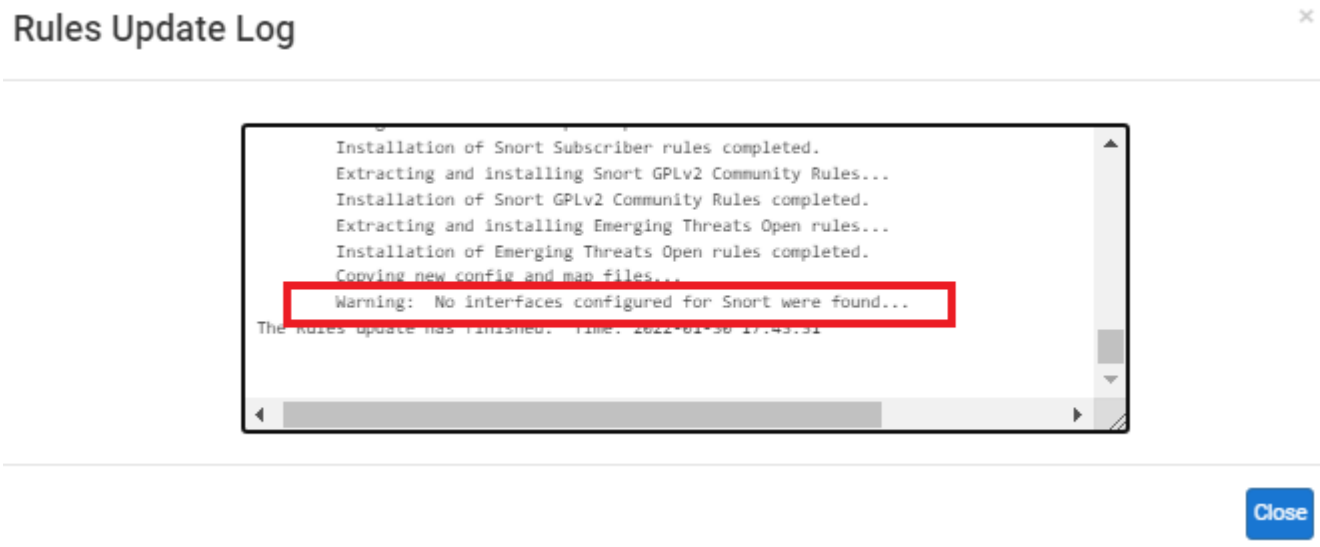


A la fin de la mise à jours on voit qu'on a le message **Result :Success**

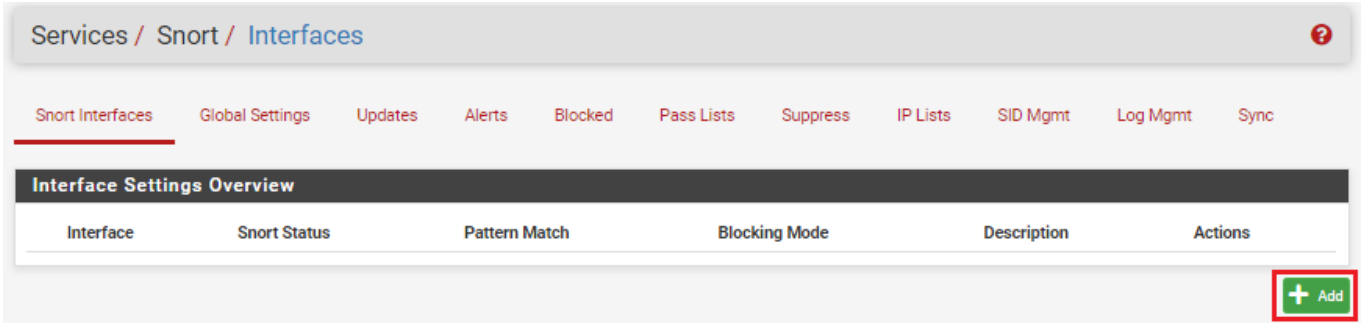


En affichant les log on un message qui précise que Snort n'est configuré sur aucune interface

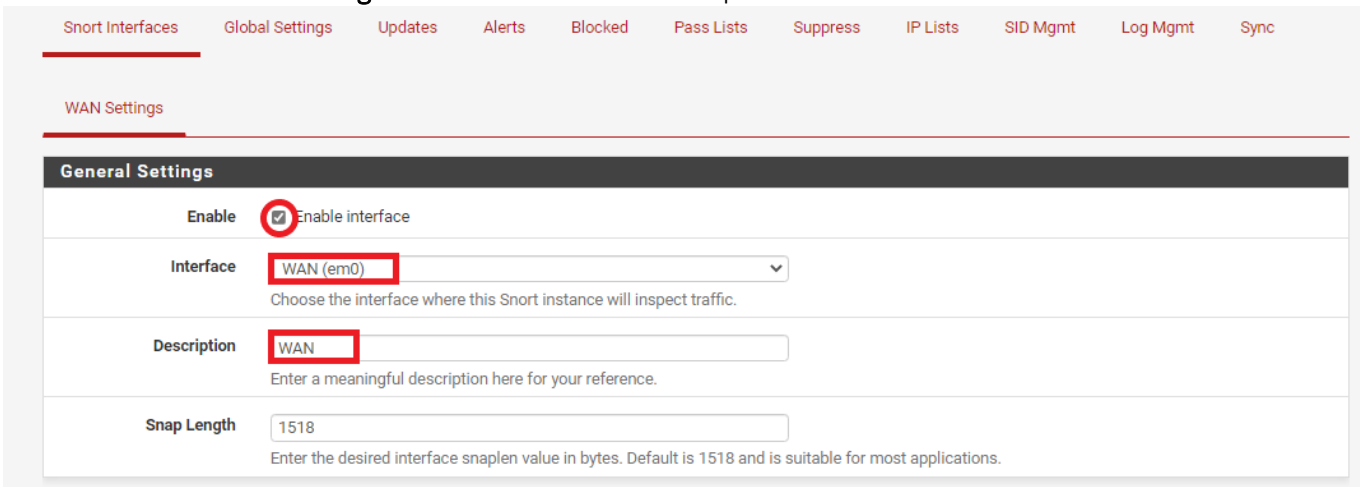




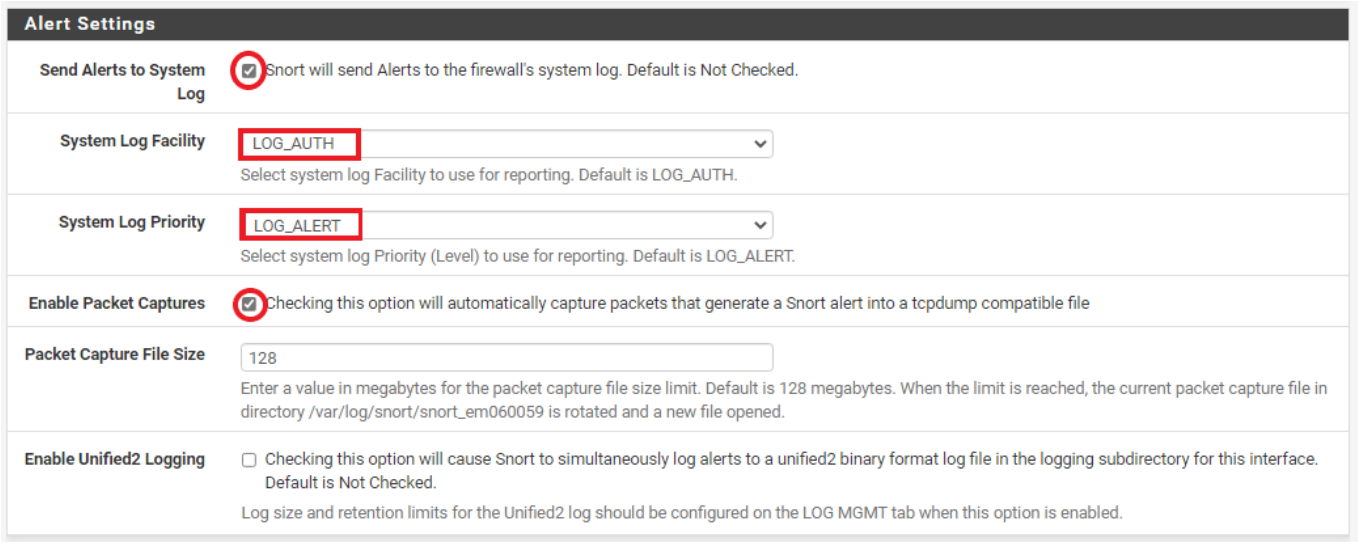
Maintenant on va sur **Snort interfaces** pour choisir l'interface ou les interfaces sur laquelle Snort va analyser et écouter le trafic réseau on clique sur add pour rajouter notre interface :



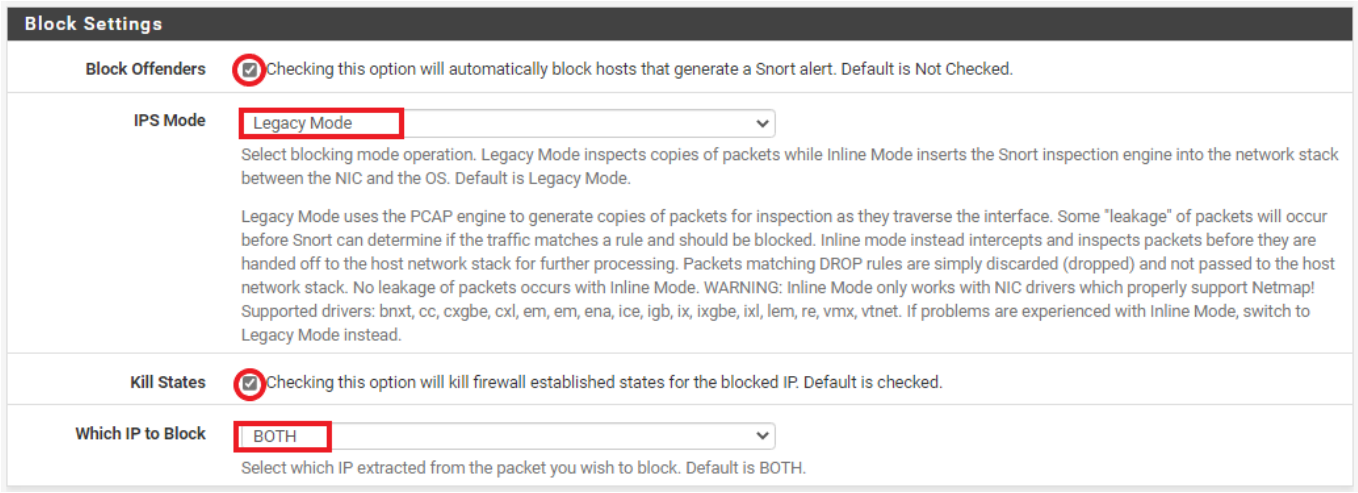
Dans la zone **General Setting** on activer l'interface wan qui est l'interface à surveiller



Localiser la zone **Alerts Settings** et effectuer la configuration suivante :
Send Alerts to System Log on active cette option pour avoir les alertes de snort



Dans la zone Block Settings on active le mode IPS en appliquant la configuration ci-dessous
Ceci permettra de bloquer les hôtes qui génère l'alerte

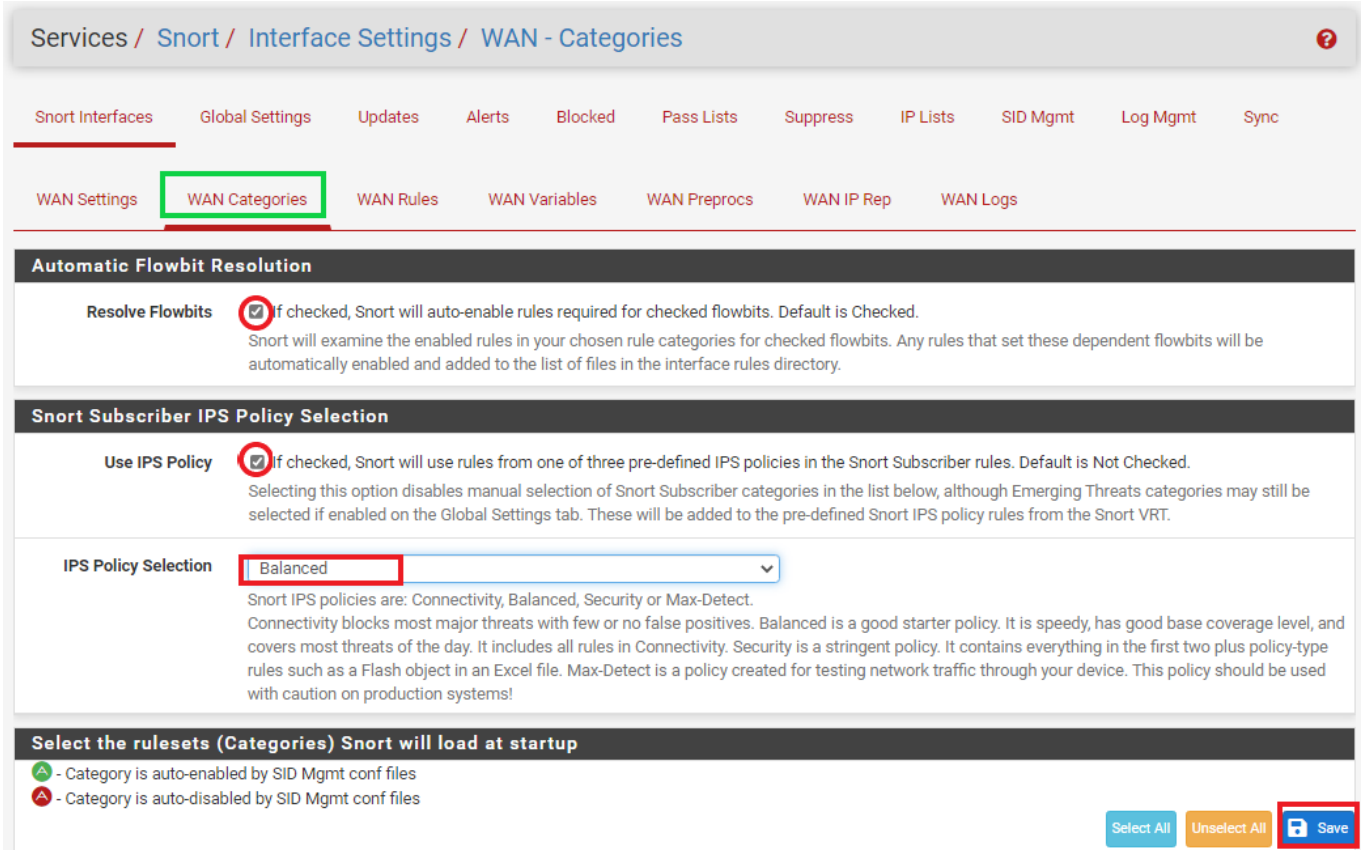


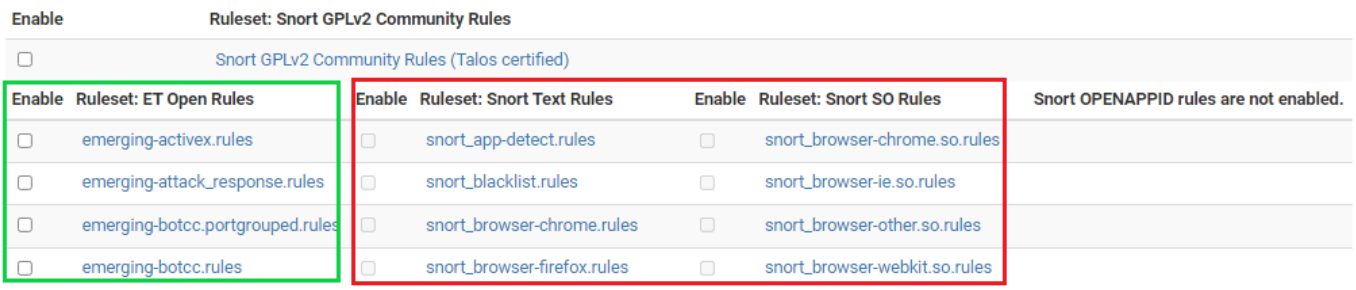
Après on laisse tout par défaut et clique sur le bouton **Save**.

Maintenant on accède à l'onglet **Wan Catégories** et on effectue la configuration suivante :
Resolve Flowbits : On active cette option Snort activera automatiquement les règles requises pour les flowbits et il examinera les règles activées dans les catégories de règles qu'on a choisies pour les **Resolve Flowbits**. Toutes les règles qui définissent ces flowbits dépendants seront automatiquement activées et ajoutées à la liste des fichiers dans le répertoire des règles de l'interface.
- **IPS Policy Selection** : On active cette option et on sélectionne comme politique IPS **Balanced.**
L'activation de cette option désactive le choix manuel des règles Snort **Snort Text Rules**, **Snort SO Rules** par-contre les règles **ET Open Rules reste manuelle**

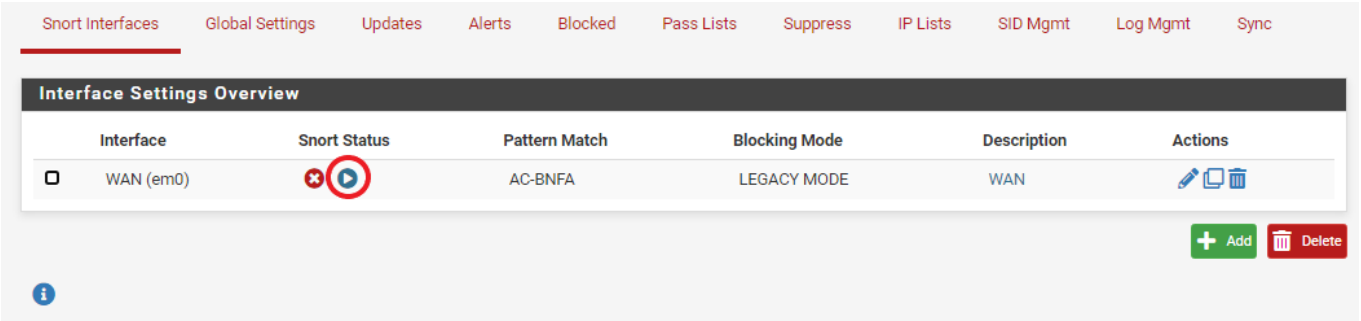
Les politiques Snort IPS sont **Connectivity**, **Balanced**, **Sécurity** et **Max-Detect**:
Connectivity bloque la plupart des menaces majeures avec peu ou pas de faux positifs.
Balanced est une bonne politique de départ. Il est rapide, a un bon niveau de couverture de base et couvre la plupart des menaces. Il inclut toutes les règles de Connectivité.
Sécurity est une politique stricte. Il contient tout ce qui se trouve dans les deux premiers plus les règles de type politique telles qu'un objet Flash dans un fichier Excel.
Max-Detect est une stratégie créée pour tester le trafic réseau via votre appareil. Cette politique doit être utilisée avec prudence sur les systèmes de production !

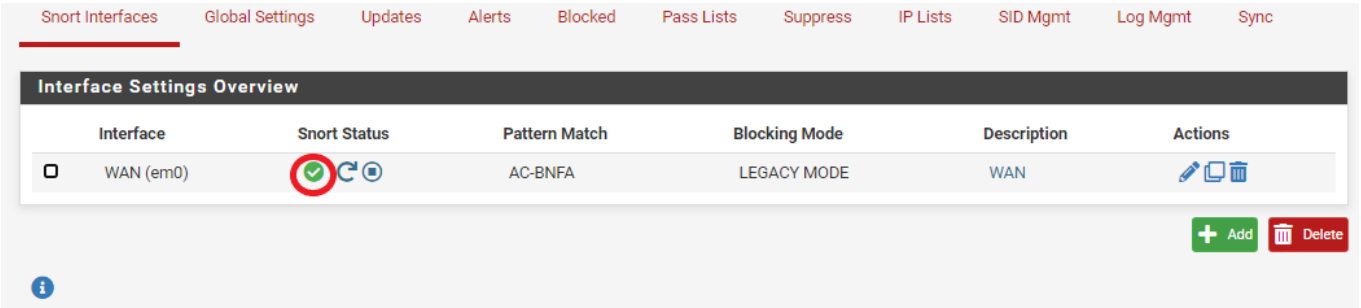
Après avoir terminé la configuration, cliquez sur le bouton Enregistrer et démarrez le service Snort





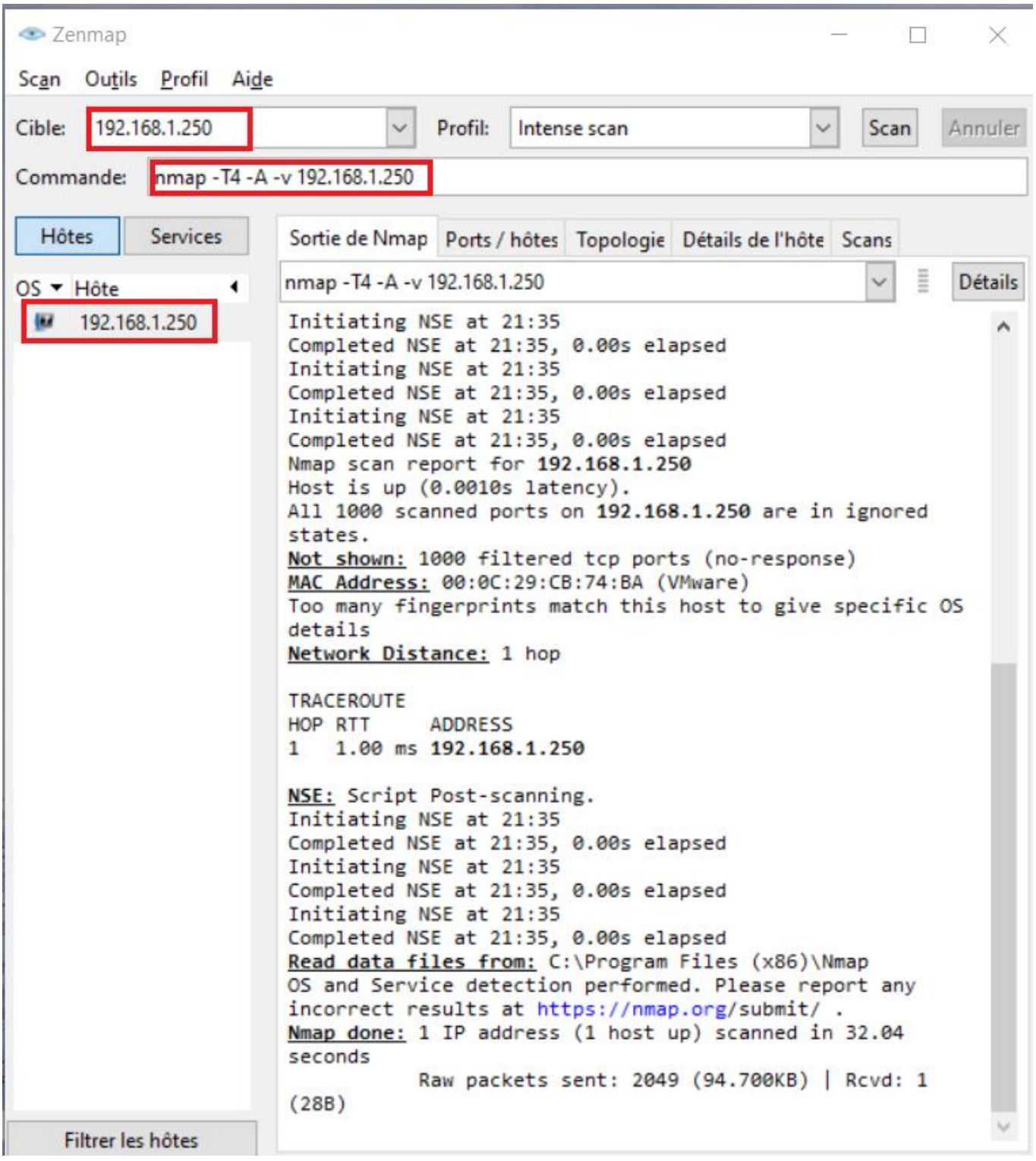
Maintenant on va démarrer notre Interface Snort



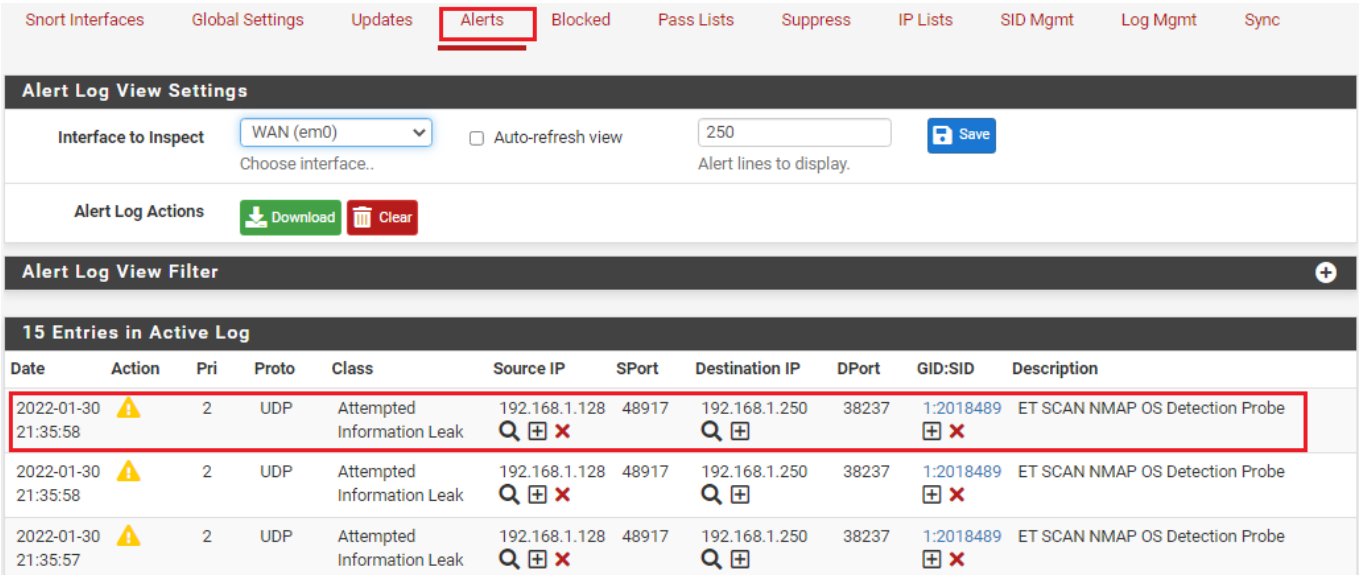


Test d'intrusion

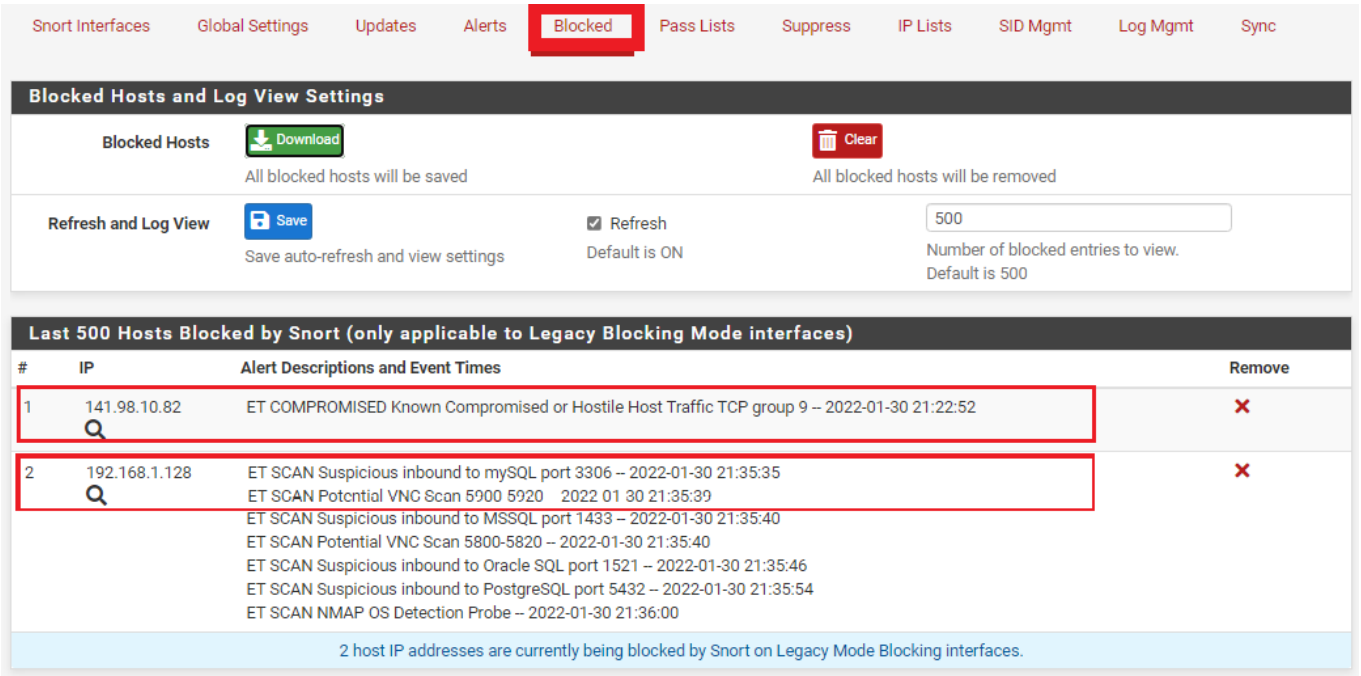
Sur Notre machine physique on installe un utilitaire nmap qui servira de scanner les ports de pfsense



Sur Pfsense dans l'onglet Alerte on relève des notifications d'attaques d'une machine dont l'adresse IP est 192.168.1.128 c'est l'adresse de notre machine physique, l'attaque détectée n'est que la requête nmap



Dans l'onglet Bloked on voit que la machine dont l'adresse IP est 192.168.1.128 est bloqué car elle est identifié comme hoste hostile



Mission 4 : Redondance et haute disponibilité

Paragraphe 1 : Test et comparaison des solutions de la mission 4

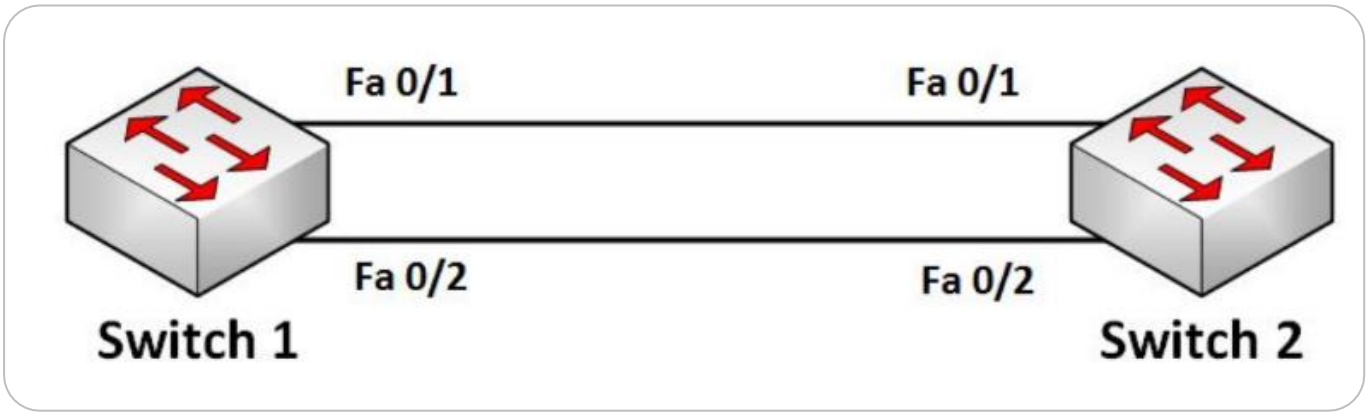
A) La couche 2

1) L'Etherchannel

L'Etherchannel est une technique permettant l'agrégation de lien. Il est utilisé **pour augmenter la bande passante entre deux switchs**. Voyons ensemble comment ce protocole fonctionne, puis comment le mettre en place.

Comme nous venons de le dire, l'Etherchannel consiste en une agrégation de lien.
Le principe est simple : Il s'agit de **combiner plusieurs liens** pour obtenir un lien virtuel de meilleure capacité.

Par exemple : Sur des switchs avec des ports à 100 Mb/s, ces derniers pourront communiquer à une vitesse de 100 Mb/s. Pour bénéficier d'une meilleure bande passante, nous devons faire une agrégation de lien. En voici le schéma ci-dessous :



En plus de l'agrégation de lien, la redondance est un avantage. Ainsi, si l'un des liens tombe, les autres seront toujours là pour assurer la connectivité. La bande passante sera simplement réduite.

2) Link Aggregation avec EtherChannel

Un EtherChannel peut agréger de **1 à 8 ports physiques**. On peut modifier la méthode de load-balancing sur les ports.

Un EtherChannel peut être **de niveau 2 ou niveau 3**, de protocole standard LACP *(Link Aggregation Control Protocol)* IEEE 802.3ad, propriétaire de Cisco PAgP *(Port Aggregation Protocol)* ou forcé.

Les ports doivent avoir le même duplex, speed, et VLAN information.

Attention, en fonction des modèles de switchs/IOS/protocole, un Etherchannel sur des ports des switchs différents.

3) Port Agregation Protocol

PAgP est un protocole propriétaire Cisco. Contrairement à LACP, PagP ne fonctionne que sur des équipements CISCO. Son fonctionnement est assez similaire à celui de LACP.

Avec LACP, il est possible de configurer les ports dans 2 modes différents :

On : **sert à déclarer une agrégation active. Aucun protocole de négociation ne sera utilisé. Il faut donc mettre les ports d'en face en mode On**

- **Désirable** : **fait la demande avec le switch d'en face pour créer l'agrégation si le port d'en face est soit en mode Auto ou en mode Desirable**
- **Auto** : **attend la négociation pour devenir une agrégation lorsque le port d'en face est en mode Desirable**

Attention, il n'est pas possible d'avoir un port en mode ON d'un côté, et d'utiliser un protocole de négociation de l'autre côté d'une agrégation.

4) LACP – Link Agregation Control Protocol

LACP est un protocole standardisé par l'IEEE : le protocole est supporté par un grand nombre de constructeurs. Il permet le contrôle de l'agrégation de **plusieurs liens physiques en un lien logique**. Le protocole échange des paquets LACP pour s'assurer que l'équipement connecté est configuré pour utiliser LACP, et qu'il soit bien configuré de la même manière.

La seule différence est le nom des modes de port.

Nous retrouvons donc deux modes de ports :

- **Passive : correspond au mode Auto de PAGP : création d'une agrégation si le port en face est en Active.**
- **Active : correspond au mode Desirable de PAGP : création d'une agrégation si le port d'en face est en Passive ou Active.**

Il faut donc choisir un protocole de négociation puis choisir le mode des ports.

Pour des raisons de sécurité, **le mieux est d'utiliser le mode Desirable (ou Active) des deux côtés**.

Il est également possible d'utiliser le mode ON. Néanmoins cela peut parfois mener à des boucles réseau, que le STP ne pourra empêcher. Le mode ON est donc à utiliser avec précaution.

5) STP et RSTP

a) Le Spanning Tree Protocol (STP)

L'algorithme original de **Spanning Tree** a été décrit par Radia Perlman alors employée par Digital Equipment Corporation, il est nommé DEC STP. En 1990, l'IEEE publie le premier standard 802.1D basé sur le travail de Perlman.

Les ports des commutateurs où STP est actif sont dans l'un des états suivants :

- **Listening** : **le commutateur « écoute » les BPDU et détermine la topologie réseau**

- **Learning** : **le switch construit une table matchant les adresses MAC aux numéros des ports**
- **Forwarding** : **un port reçoit et envoie des données**

Blocking : **un port provoquant une boucle, aucune donnée n'est envoyée ou reçue mais le port peut passer en mode forwarding si un autre lien tombe**

Disabled : **désactivé.**

Forward delay : **c'est le délai de transition entre les modes Listening vers Learning et Learning vers forwarding. Il est fixé par le root bridge et vaut 15 secondes par défaut**

b) Rapid Spanning Tree Protocol (RSTP)

En 1998, l'IEEE publie le document 802.1w qui accélère la convergence du protocole STP après un changement de topologie. Il est inclus dans le standard IEEE 802.1D-2004. Tandis que le STP classique peut prendre de 30 à 50 secondes pour converger après un changement de topologie, **RSTP** est capable de converger en 3 fois la valeur du délai Hello *(6 secondes par défaut)*.

États des ports RSTP :

- **Root** : **le port vers le root bridge**
- **Designated** : **le port qui transmet les trames sur un segment**
- **Alternate** : **un port distinct du root port vers le root bridge**
- **Backup** : **un autre port vers un segment connecté au pont**

Le fonctionnement de RSTP est semblable à celui du STP classique. Les différences sont les suivantes :

- **défaillance du root bridge détectée en 3 délais hello**

- **les portes qui ne sont pas connectées à d'autres commutateurs peuvent basculer dans l'état forwarding**

- **RSTP continue à observer l'arrivée de BPDU sur ces ports pour s'assurer qu'aucune boucle n'est possible**

- **si un BPDU est observé, la porte bascule dans le statut non edge**

- **RSTP réagit aux annonces BPDU qui proviennent du root bridge**

- **un bridge RSTP diffuse son information RSTP sur ses designated ports**

- **si un bridge reçoit un BPDU indiquant un meilleur root bridge, il place tous les autres ports dans l'état Discarding en informant le meilleur chemin vers le root**

- **en recevant cette information, celui-ci peut faire transiter le port vers ce bridge immédiatement dans l'état Forwarding sans passer par les états Listening et Learning, car aucune boucle n'est possible. C'est une amélioration majeure en termes de vitesse de convergence**

- **RSTP conserve des informations au sujet d'un chemin alternatif vers le root bridge et un chemin de sauvegarde vers les segments, permettant une transition rapide en cas de problème sur une liaison**

B) La couche 3

1) Protocole HSRP

Le protocole HSRP *(Hot Standby Routing Protocol)* est un protocole dont le propriétaire est Cisco pour la gestion des routeurs dits de « secours ». Le protocole normalisé est présent chez d'autres constructeurs est le protocole VRRP. Ce protocole permet **à partir de deux routeurs physiques (en actif/passif) de mettre en place un routeur virtuel afin d'augmenter la tolérance à la panne**.

Le principe de fonctionnement de HSRP est que tous les routeurs **émulent une IP virtuelle** qui sera utilisée comme passerelle par défaut par les clients du parc informatique. Chacun des routeurs configurera son protocole HSRP avec un niveau de priorité. Celui ayant le plus grand niveau est actif.

La communication liée au protocole HSRP entre les routeurs se fait par l'envoi de paquets multicast à l'adresse IP 224.0.0.2 vers le port UDP 1985. Cela permet d'élire le routeur actif.

La technologie HSRP permet aux routeurs situés dans un même groupe qu'on appelle ''standby group'' de **former un routeur virtuel qui sera l'unique passerelle** des clients du LAN. Un routeur dans ce groupe est élu comme « actif » et ce sera lui qui fera transiter les requêtes du LAN. Pendant que le routeur actif travaille, il envoie également des messages aux autres routeurs indiquant qu'il est actif. L'élection se faisant en prenant en compte de la priorité. Cette priorité comprise entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface (par défaut la priorité est à 100).

Le routeur virtuel aura toujours la même adresse IP et adresse MAC sur les hôtes du LAN même lors d'un changement de gateway lors de la chute d'un routeur principal.

Tout ceci car : le routeur que voient les hôtes est un routeur virtuel composé de plusieurs routeurs qui se relaient via le protocole HSRP.

Pour résumer, le HSRP :

- **assure la redondance donc la continuité de service**
- **s'attribue une adresse IP virtuelle**
- **compatible sur les équipements Cisco**

Or, on peut y trouver les points négatifs suivant :

- **l'authentification des requêtes n'est pas chiffrée sur le réseau**
- **ne gère pas l'équilibrage des charges**
- **les messages hello sont envoyés aux routeurs en multicast**

2) Protocole VRRP

Virtual Router Redundancy Protocol est un protocole standard dont le but est **d'augmenter la disponibilité de la passerelle** par défaut des hôtes d'un même réseau.

Le principe est de définir la gateway pour les hôtes du réseau en utilisant une adresse IP virtuelle référençant un groupe de routeurs. VRRP est **l'équivalent de HSRP chez Cisco**.

A ce groupe on associe une adresse IP virtuelle.

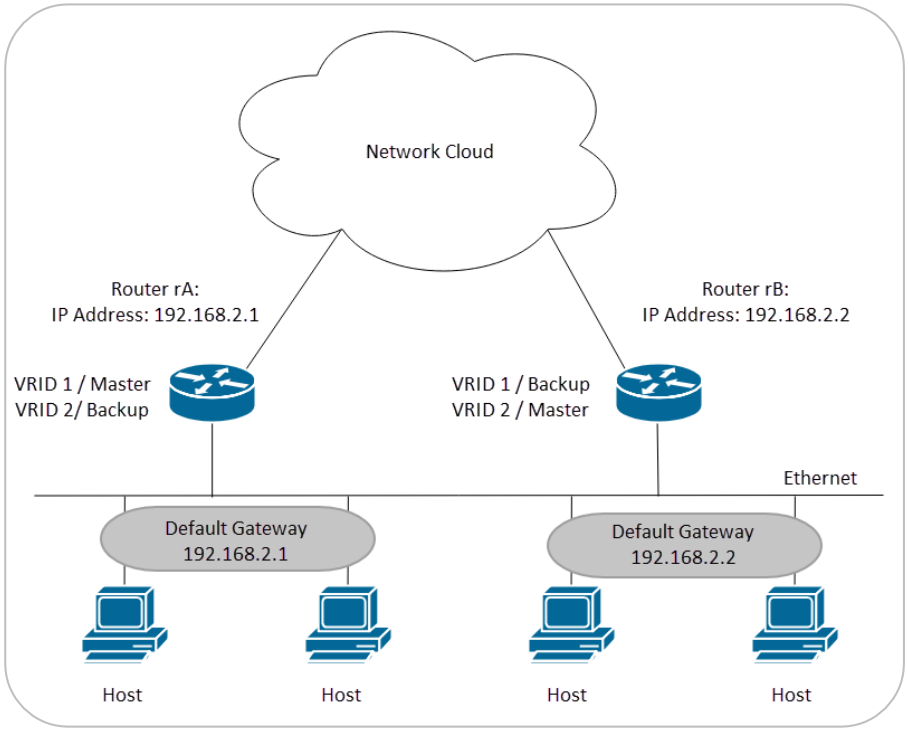
La redondance est mise en place par le biais du protocole ARP. Lorsque l'hôte doit envoyer une trame à sa passerelle, il émet une requête ARP et celle-ci répond en fournissant son adresse MAC.

Dans le cas de VRRP, les routeurs vont associer une adresse MAC particulière à l'adresse IP virtuelle sous la forme 00:00:5E:00:01:XX (où XX est le n° du groupe VRRP).

Pour l'hôte, ce sera cette adresse MAC qui identifiera sa passerelle.

Les routeurs dialoguent par multicast à l'adresse (224.0.0.18) afin d'élire le routeur qui devra se charger de traiter la trame destinée à l'adresse MAC VRRP. Cette adresse MAC virtuelle est associée à un des routeurs du groupe grâce à un système d'élection basé sur la priorité d'un routeur avec la priorité la plus forte ce qui voit élire routeur maitre et les autres routeurs comme routeur « backup ».

Schéma d'un réseau VRRP :



On peut citer les avantages suivants :

- **assure la redondance et la continuité de service**
- **standardisé**
- **rapidité de réactivité du routeur backup inférieur à 4 secondes**
- **adresses IP et MAC virtuelle**

Or, on peut citer les inconvénients suivants :

- **authentification par mot de passe non chiffrée**
- **adresse MAC virtuelle unique**

3) Protocole GLBP

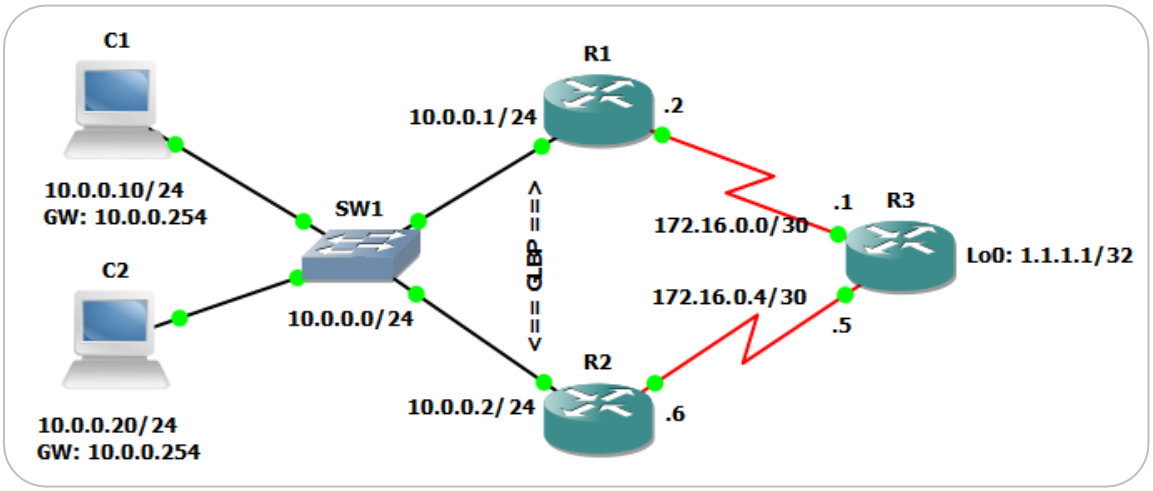
Gateway Load Balancing Protocol est un protocole propriétaire Cisco permettant de mettre en place de **la redondance et de la répartition de charge sur plusieurs routeurs en utilisant une seule adresse IP virtuelle**, associée à plusieurs adresses MAC virtuelles.

GLBP utilise l'adresse IP multicast 224.0.0.102 pour l'envoi des paquets Hello et le numéro de port UDP 3222.

Le protocole HSRP ne permet pas la mise en place de Load-Balancing entre les routeurs membres du groupe HSRP. Si un routeur est choisi comme routeur principal vers lequel tous les paquets transiteront tant qu'il sera opérationnel, **les autres routeurs de secours sont totalement inutiles** tant qu'il n'y a pas de panne sur le routeur principal.

Avec le protocole GLBP qui reprend **le principe de continuité de service** (tolérance aux pannes), il y a également **une notion de répartition de charge** : les routeurs membres du groupe virtuel se répartissent le traitement des paquets et leur routage afin d'alléger la charge de chacun. Tout ceci en assurant une continuité du service sur la même IP, **si un des routeurs tombe, sa charge sera répartie sur les autres routeurs disponibles**. Cela permet d'utiliser la totalité des ressources disponibles plutôt que d'en laisser une partie en mode passif.

Schéma d'un réseau GLBP :



On peut citer les avantages du GLBP :

- **redondance et la continuité de service**
- **répartition des charges (load balancing)**
- **adresse IP virtuelle**
- **jusqu'à 4 adresses MAC virtuelles possible par groupe GLBP**
- **requête d'authentification cryptée**

Or, on y trouve l'inconvénient suivant :

- **protocole propriétaire Cisco**

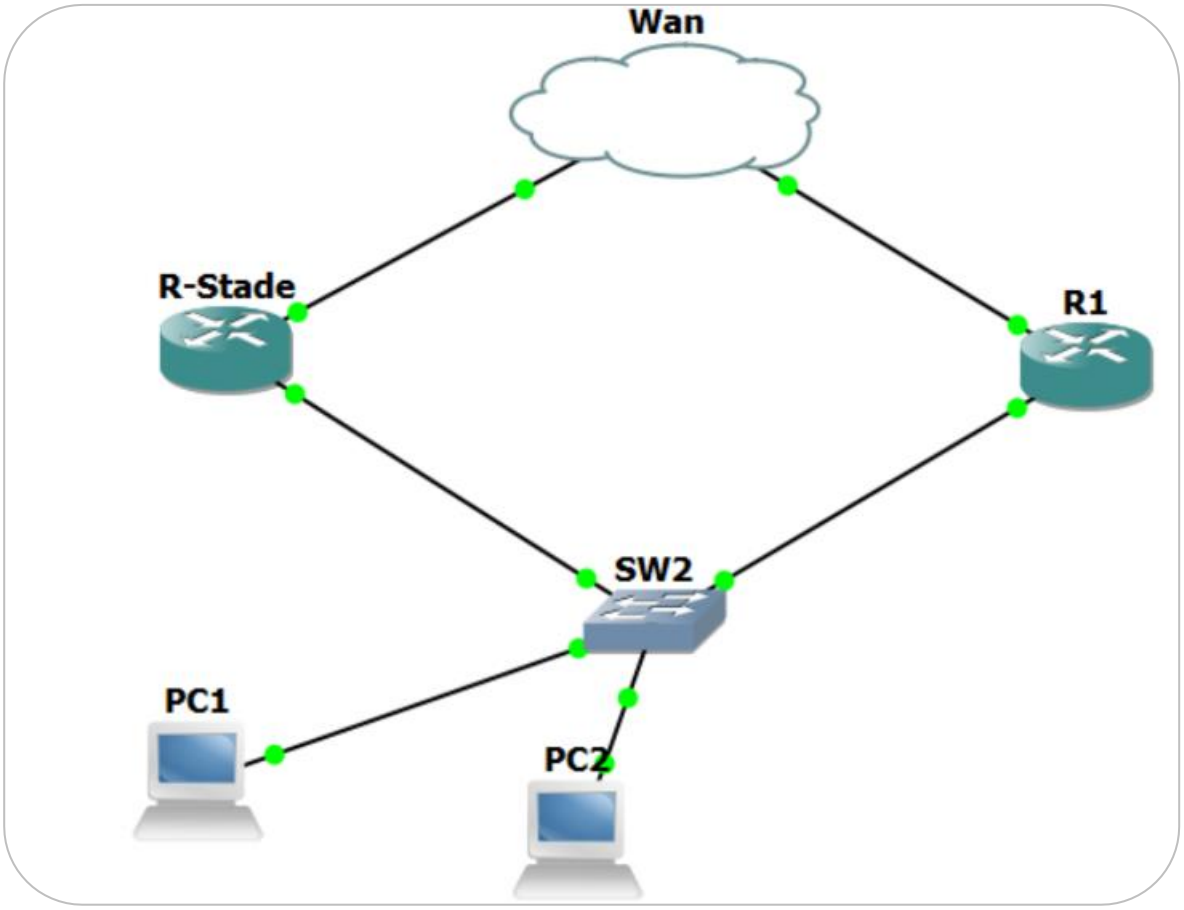
Paragraphe 2: Notre choix de solutions

Concernant **la couche 2**, nous déploierons **le protocole STP** ainsi que **le PAGP.**

Concernant **la couche 3**, nous mettrons en place **HSRP**.

Schéma de la Mise en place de la redondance des services, la tolérance de panne et l'équilibrage

des charges des éléments d'interconnexions de niveau 2 et 3



A) Configuration du STP

Nous activons le spanning-tree sur l'ensemble des VLAN :

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spa
Switch(config)#spanning-tree vlan 10 root primary
Switch(config)#spanning-tree vlan 20 root primary
Switch(config)#spanning-tree vlan 30 root primary
Switch(config)#spanning-tree vlan 40 root primary
Switch(config)#spanning-tree vlan 50 root primary
Switch(config)#spanning-tree vlan 100 root primary
Switch(config)#spanning-tree vlan 200 root primary
Switch(config)#
```

Nous vérifions le spanning-tree sur le switch :

```
witch#sh sp
Switch#sh spanning-tree
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     00D0.BA2D.DE46
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24586  (priority 24576 sys-id-ext 10)
              Address     00D0.BA2D.DE46
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

witch#
```


B) Configuration Etherchannel

Le but final de la mise en place du protocole Etherchannel est d'arriver à avoir toutes les interfaces actives afin d'activer l'agrégation de lien comme ceci :

Mais avant l'activation du protocole Etherchannel, seul le mode STP est activé et l'agrégation de lien n'est pas mise en place comme on peut le constater ci-dessous :

1) Implémentation du protocole Etherchannel sur le Switch COMM1

Nous mettons en place un groupe Etherchannel pour chaque VLAN :

```
witch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#channel-group 1 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up
```

```
Switch(config)#interface range fastEthernet 0/6-8
Switch(config-if-range)#channel-group 2 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 2

Switch(config-if-range)#interface range fastEthernet 0/9-10
Switch(config-if-range)#channel-group 3 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 3
```


```
Switch(config)#interface range fastEthernet 0/11-12
Switch(config-if-range)#channel-group 4 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 4

Switch(config-if-range)#interface range fastEthernet 0/13-14
Switch(config-if-range)#channel-group 5 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 5

Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/15-16
Switch(config-if-range)#channel-group 6 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 6

Switch(config-if-range)#interface range fastEthernet 0/17-18
Switch(config-if-range)#channel-group 7 mode auto
```

Nous vérifions la création des différents groupes Etherchannel :

```
itch#sh etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 7 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 2
----------
Group state = L2
Ports: 3 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 3
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 4
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 5
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 6
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP
itch#
```


2) Implémentation du protocole Etherchannel sur le Switch COMM2

Nous mettons en place d'un groupe Etherchannel pour chaque VLAN :

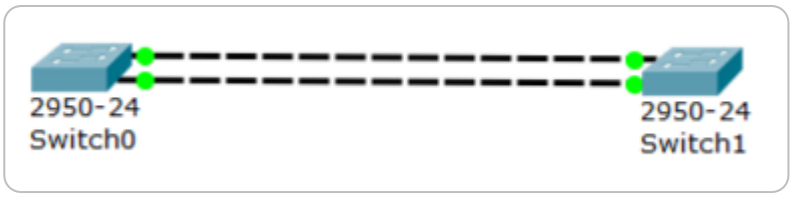
```
witch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#channel-group 1 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up
```

```
Switch(config)#interface range fastEthernet 0/6-8
Switch(config-if-range)#channel-group 2 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 2

Switch(config-if-range)#interface range fastEthernet 0/9-10
Switch(config-if-range)#channel-group 3 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 3
Switch(config)#interface range fastEthernet 0/11-12
Switch(config-if-range)#channel-group 4 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 4

Switch(config-if-range)#interface range fastEthernet 0/13-14
Switch(config-if-range)#channel-group 5 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 5

Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/15-16
Switch(config-if-range)#channel-group 6 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 6

Switch(config-if-range)#interface range fastEthernet 0/17-18
witch(config-if-range)#channel-group 7 mode auto
```


Nos vérifions la création des différents groupes Etherchannel :

```
witch#sh etherchannel
                Channel-group listing:
                ----------------------

Group: 1
----------
Group state = L2
Ports: 7 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 2
----------
Group state = L2
Ports: 3 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 3
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 4
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 5
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP

Group: 6
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAGP
witch#
```


Une fois le protocole Etherchannel activé sur les deux switchs, on peut constater que l'agrégation de lien a bien eu lieu en observant les voyants lumineux sur les switchs qui indiquent que tous les liens sont bien UP et qu'il n'y a aucun blocage de port :



C) Configuration GLBP

1) Configuration des VLANS

Configuration de la sous-interface du vlan 10 :

```
R-Stade(config)#interface fa0/0.10
R-Stade(config-subif)#glbp 10 ip 172.20.0.2
R-Stade(config-subif)#glbp 10 priority 110
R-Stade(config-subif)#glbp 10 preempt
R-Stade(config-subif)#
```

```
R-Stade(config)#interface fastEthernet0/0.10
R-Stade(config-subif)#ip nat inside
R-Stade(config-subif)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R-Stade(config-subif)#exit
R-Stade(config)#
```

Configuration de la sous-interface du vlan 20 :

```
R-Stade(config)#interface fastEthernet0/0.20
R-Stade(config-subif)#glbp 20 ip 172.20.1.2
R-Stade(config-subif)#glbp 20 priority 110
R-Stade(config-subif)#glbp 20 pre
R-Stade(config-subif)#glbp 20 preempt
R-Stade(config-subif)#
```

```
R-Stade(config)#interface fastEthernet0/0.20
R-Stade(config-subif)#ip nat inside
R-Stade(config-subif)#
R-Stade(config-subif)#exit
R-Stade(config)#
```

Configuration de la sous-interface du vlan 30 :

```
R-Stade(config)#interface fastEthernet0/0.30
R-Stade(config-subif)#glbp 30 ip 172.20.3.2
R-Stade(config-subif)#glbp 30 priority 110
R-Stade(config-subif)#glbp 30 preempt
R-Stade(config-subif)#
```

```
R-Stade(config)#interface fastEthernet0/0.30
R-Stade(config-subif)#ip nat inside
R-Stade(config-subif)#exit
R-Stade(config)#
R-Stade(config)#
R-Stade(config)#
```

Configuration de la sous-interface du vlan 40 :

```
R-Stade(config)#interface fastEthernet0/0.40
R-Stade(config-subif)#glbp 40 ip 172.20.3.130
R-Stade(config-subif)#glbp 40 priority 110
R-Stade(config-subif)#glbp 40 preempt
R-Stade(config-subif)#exit
R-Stade(config)#
R-Stade(config)#
```

```
R-Stade(config)#interface fastEthernet0/0.40
R-Stade(config-subif)#ip nat in
R-Stade(config-subif)#ip nat inside
R-Stade(config-subif)#exit
R-Stade(config)#
```

Configuration de la sous-interface du vlan 50 :

```
R-Stade(config)#interface fastEthernet0/0.50
R-Stade(config-subif)#glbp 50 ip 172.20.3.194
R-Stade(config-subif)#glbp 50 priority 110
R-Stade(config-subif)#glbp 50 preempt
R-Stade(config-subif)#
```

```
R-Stade(config)#interface fastEthernet0/0.50
R-Stade(config-subif)#ip nat in
R-Stade(config-subif)#ip nat inside
R-Stade(config-subif)#exit
R-Stade(config)#
```


Configuration de la sous-interface du vlan 100 :

```
R-Stade(config)#interface fastEthernet0/0.100
R-Stade(config-subif)#glbp 100 ip 172.20.2.2
R-Stade(config-subif)#glbp 100 priority 110
R-Stade(config-subif)#glbp 100 preempt
R-Stade(config-subif)#exit
R-Stade(config)#
R-Stade(config)#
R-Stade(config)#
```

```
R-Stade(config)#interface fastEthernet0/0.100
R-Stade(config-subif)#ip na
R-Stade(config-subif)#ip nat in
R-Stade(config-subif)#ip nat inside
R-Stade(config-subif)#exit
R-Stade(config)#
```

Configuration de la sous-interface du vlan 200 :

```
R-Stade(config)#interface fastEthernet0/0.200
R-Stade(config-subif)#glbp 200 ip 172.20.2.130
R-Stade(config-subif)#glbp 200 priority 110
R-Stade(config-subif)#glbp 200 preempt
R-Stade(config-subif)#
R-Stade(config-subif)#
R-Stade(config-subif)#
R-Stade(config-subif)#
```

```
R-Stade(config)#interface fastEthernet0/0.200
R-Stade(config-subif)#ip nat inside
R-Stade(config-subif)#exit
R-Stade(config)#
R-Stade(config)#
R-Stade(config)#
```


Nous mettons en place des access-list :

```
R-Stade(config)#access-list 10 permit 172.20.0.0 0.0.0.255
R-Stade(config)#access-list 20 permit 172.20.1.0 0.0.0.255
R-Stade(config)#access-list 30 permit 172.20.3.0 0.0.0.127
R-Stade(config)#access-list 40 permit 172.20.3.128 0.0.0.63
R-Stade(config)#access-list 50 permit 172.20.3.192 0.0.0.63
R-Stade(config)#access-list 98 permit 172.20.2.0 0.0.0.127
R-Stade(config)#access-list 99 permit 172.20.2.128 0.0.0.127
```

```
R-Stade(config)#$de source list 10 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 20 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 30 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 40 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 50 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 98 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 99 interface fastEthernet0/1 overload
R-Stade(config)#
```

2) Configuration du R-1

Nous implémentons le protocole GLBP :

```
-1(config)#int fa0/0.10
R-1(config-subif)#glbp 10 ip 172.20.0.3
R-1(config-subif)#glbp 10 priority 90
R-1(config-subif)#int fa0/0.20
R-1(config-subif)#glbp 20 ip 172.20.1.3
R-1(config-subif)#glbp 20 priority 90
R-1(config-subif)#exit
R-1(config)#int fa0/0.30
R-1(config-subif)#glbp 30 ip 172.20.3.3
R-1(config-subif)#glbp 30 priority 90
R-1(config-subif)#exit
R-1(config)#int fa0/0.40
R-1(config-subif)#glbp 40 ip 172.20.3.130
R-1(config-subif)#glbp 40 priority 90
R-1(config-subif)#exit
R-1(config)#int fa0/0.50
R-1(config-subif)#glbp 50 ip 172.20.3.195
R-1(config-subif)#glbp 50 priority 90
R-1(config-subif)#exit
R-1(config)#int fa0/0.100
R-1(config-subif)#glbp 100 ip 172.20.2.3
R-1(config-subif)#glbp 100 priority 90
R-1(config-subif)#exit
R-1(config)#int fa0/0.200
R-1(config-subif)#glbp 100 ip 172.20.2.131
% Must use unique GLBP group number for each logical interface
   that is a member of the same physical interface.
R-1(config-subif)#glbp 200 ip 172.20.2.131
R-1(config-subif)#glbp 200 priority 90
R-1(config-subif)#exit
-1(config)#
```


Nous mettons en place les access-list :

```
R-Stade(config)#access-list 10 permit 172.20.0.0 0.0.0.255
R-Stade(config)#access-list 20 permit 172.20.1.0 0.0.0.255
R-Stade(config)#access-list 30 permit 172.20.3.0 0.0.0.127
R-Stade(config)#access-list 40 permit 172.20.3.128 0.0.0.63
R-Stade(config)#access-list 50 permit 172.20.3.192 0.0.0.63
R-Stade(config)#access-list 98 permit 172.20.2.0 0.0.0.127
R-Stade(config)#access-list 99 permit 172.20.2.128 0.0.0.127
```

```
R-Stade(config)#$de source list 10 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 20 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 30 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 40 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 50 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 98 interface fastEthernet0/1 overload
R-Stade(config)#ip nat inside source list 99 interface fastEthernet0/1 overload
R-Stade(config)#
```

<u>Test avec un client Windows :</u>

```
C:\WINDOWS\system32\cmd.exe
(c) 2015 Microsoft Corporation. Tous droits réservés.

C:\Users\Iris>tracert 172.20.95.253

Détermination de l'itinéraire vers 172.20.95.253 avec un maximum de 30 sauts.

  1    <1 ms    <1 ms    <1 ms  172.20.0.1
  2    <1 ms    <1 ms    <1 ms  172.20.95.253

Itinéraire déterminé.

C:\Users\Iris>tracert 172.20.95.253

Détermination de l'itinéraire vers 172.20.95.253 avec un maximum de 30 sauts.

  1    <1 ms    <1 ms    <1 ms  172.20.0.1
  2  172.20.0.1  rapports : Impossible de joindre l'hôte de destination.

Itinéraire déterminé.

C:\Users\Iris>tracert 172.20.95.253

Détermination de l'itinéraire vers 172.20.95.253 avec un maximum de 30 sauts.

  1     *       <1 ms    <1 ms  172.20.0.2
  2    <1 ms    <1 ms    <1 ms  172.20.95.253

Itinéraire déterminé.

C:\Users\Iris>
```

Mission 5 : Déploiement d'une solution d'accès sans fil des utilisateurs mobiles de StadiumCompany (WIFI)

Paragraphe 1 : Solution d'accès Wifi pour le VLAN WIFI (stade-wifi)

1. Configurez le SSID "stade-wifi" sur les points d'accès Cisco, en utilisant la norme WPA2 Enterprise pour l'authentification des salariés du stade.

2. Créez un VLAN 30 avec l'adresse IP 172.20.2.0/25 pour le VLAN WIFI.

3. Configurez les interfaces VLAN sur les switchs PoE pour permettre la communication du VLAN WIFI.

4. Configurez les ports des switchs PoE connectés aux points d'accès en tant que ports access dans le VLAN WIFI.

Paragraphe 2 : Solution d'accès Wifi pour les visiteurs

1. Configurez le SSID "visiteurs" sur les points d'accès Cisco pour permettre aux visiteurs de se connecter

2. Créez un VLAN spécifique pour les visiteurs (par exemple, VLAN 40) avec une plage d'adresses IP distincte, différente du VLAN WIFI.

3. Configurez les interfaces VLAN sur les switchs PoE pour permettre la communication du VLAN visiteurs.

4. Configurez les ports des switchs PoE connectés aux points d'accès en tant que ports access dans le VLAN visiteurs.

Mission 6 : Solution de gestion du Parc informatique

Paragraphe 1 : Test et comparaison des solutions

A) GLPI

GLPI *(Gestion Libre de Parc Informatique)* est un gestionnaire de parc informatique libre. Il permet de **centraliser des outils liés à l'administration** d'une structure informatique d'une entreprise. La fonctionnalité qui est en majeur partie utilisée par les services informatique est **la gestion de tickets d'incidents.**

GLPI offre :

- **la gestion du parc matériel de la société avec leurs contrats associés** : ordinateurs (avec remontée automatique avec Fusion Inventory), périphériques, imprimantes, éléments réseau, consommables, téléphones, gestion des licences (acquises, à acquérir, sites, et des dates d'expiration), gestion des informations commerciales et financières (achat, garantie et extension, amortissement).

- **des fonctions d'assistance** : accès utilisateur ou non, gestion fine des droits, notifications automatiques avec modèles personnalisables, alertes automatiques (contrats, consommables, réservations de matériels), gestion des réservations de matériel

- **une grande extensibilité grâce à ses plugins** : intégration à des logiciels de supervision comme Centreon, interconnexion à des web services, gestion de projets, nouveaux éléments d'inventaire, etc.

- **une gestion des demandes d'intervention** pour tous les types de matériel de l'inventaire (helpdesk)

B) OCS Inventory

OCS Inventory NG *(Open Computer and Software Inventory Next Generation)* est une application permettant de **réaliser un inventaire de la configuration matérielle** du réseau et des logiciels installés.

OCS est simple d'utilisation grâce à son interface Web.

1) Fonctionnalités générales

OCS Inventory NG est un outil d'inventaire de parc informatique. Il permet de connaitre précisément la configuration matérielle des machines du réseau et les logiciels qui y sont installés. Grâce à des agents logiciels installés sur chaque PC du parc, on peut ainsi **collecter les caractéristiques matérielles et logicielles de chaque PC** et les transmettre au serveur où elles seront stockées et affichées sur une interface Web.

L'utilisation d'OCS Inventory NG se fait **à travers une console Web** avec 2 niveaux de droits : administrateur et utilisateur.

En définitive OCS est une application destinée à aider les administrateurs système pour connaitre précisément **la configuration des machines du réseau et les logiciels** qui y sont installés. Autrement dit, à mieux gérer leur parc.

Les informations fournies par OCS sur les PC du parc sont **extrêmement précises et complètes** :

- adresse IP
- processeur
- taille et type de la RAM
- taille du disque
- espace occupé du disque
- le système d'exploitation
- le numéro de série du constructeur
- les lecteurs logiques,

- les caractéristiques des cartes vidéo (avec chipset) et des cartes réseau (avec adresse MAC),
- les imprimantes et leur pilote
- les logiciels installés
- les utilisateurs avec la date et heure à laquelle ils se sont connectés à la machine

2) Fonctionnalités secondaires

OCS Inventory fournit également :

- **un télé déploiement de paquets logiciels** : OCS Inventory NG fournit une fonctionnalité de télédiffusion et d'installation de logiciels depuis le serveur, sur les ordinateurs clients. Cela se fait depuis le serveur central d'administration qui exécute le téléchargement par HTTPS, relayé par les agents sur les postes clients
- **la possibilité de scanner le réseau** pour détecter le matériel non inventorié et le classifie
- **la synchronisation des données avec GLPI** (en utilisant le plugin OCS INENTORY NG)
- **Interopérabilité**

L'association de OCS avec le logiciel GLPI est une force du projet car il permet de communiquer **l'inventaire du parc de PC à GLPI**, exploitable dans un contexte global.

3) Avantages d'OCS

- **Faible utilisation de la bande passante** : 5 KB pour un inventaire complet
- **Haute performance** : environ 1 000 000 d'ordinateurs inventoriés par jour sur un serveur bi-Xeon 3 GHz avec 4 GB de RAM
- **Basée sur des produits reconnus** : serveur web Apache, serveur de base de données MySQL, langages de programmation PHP et PERL
- **Solution modulable constituée de nombreux plugins** et d'un interfaçage avec d'autres solutions de gestion de parc informatique (GLPI)

C) Pulse

Pulse 2 est un logiciel d'inventaire de parc informatique, d'Imaging de poste et de télé déploiement créé par Mandriva.

Grâce à un agent installé sur les postes, Pulse 2 permet **la remontée des caractéristiques matérielles et logiciels des postes**.

L'agent permet également **la prise en main à distance sur les postes** par les administrateurs au travers du protocole VNC sur un canal sécurisé (SSH). Le télédéploiement se fait par packages sur les plateformes Windows, Mac et Linu.

L'imaging de poste permet de **créer des masters et de les installer rapidement** et à distance sur des postes sans aucune intervention des administrateurs.

Pulse 2 est distribué sous la licence GPL, **construit sur plusieurs technologies** (Python, MySQL et C++) et est en mesure de **créer et de restaurer des images des disques durs** des ordinateurs d'un parc informatique.

Ce logiciel sous licence *open source* prend en charge la plupart des fonctions classiques dans ce domaine :

- **inventaire** (matériel et logiciel)
- **administration** (déploiements et mises à jour)
- **maintenance** (supervision réseau et lancement de diagnostics)

La nouvelle version introduit **une fonctionnalité de clonage**, permettant de créer une image de secours du disque dur d'un ordinateur (sur toutes les versions *desktop* et serveur de Windows et Linux).

De là, l'image pourra être restaurée par la suite (faisant ainsi gagner un temps précieux aux équipes de maintenance informatique) ou déployée sur plusieurs ordinateurs.

De plus, il est possible de **lancer des scripts de personnalisation** après la phase de restauration.

D) FusionInventory

Fusion Inventory est né du projet OCS Inventory en changeant son architecture de fonctionnement : ce n'est plus le serveur central qui récupère les remontées d'inventaire des agents déployés sur les postes mais GLPI lui-même.

Ainsi, Fusion Inventory se décompose donc en 2 éléments :

- **le plugin qui s'intègre à GLPI**
- **les agents à déployer sur les postes**

Fusion Inventory dispose de ce fait **d'avantages importants** par rapport à OCS :

- **tout est centralisé dans GLPI** : il ne peut y avoir de latence ou de problème de synchronisation avec le serveur d'inventaire
- **la possibilité de forcer la remontée immédiate d'un inventaire d'un poste**

Fusion Inventory est cependant un projet plus récent et **ne dispose pas de fonctions aussi avancées qu'OCS Inventory** en ce qui concerne les télédéploiements.

FusionInventory propose une solution multiplateforme et évolutive permettant de **réaliser un inventaire automatique, instantané, dynamique et historisé** de votre parc informatique.

Ses modules sont les suivants :

- **Multi-OS**
- **Multi-Serveurs**
- **Multi-Connexions**
- **Multi-Capacité : Inventaire matériel et logiciel**
- **Module de requête SNMP : Permet l'inventaire complet d'imprimantes, routeurs, ou encore switchs**

Paragraphe 2 : Choix de solutions

L'objectif de notre projet est de mettre en place d'outils permettant la gestion du patrimoine informatique au sein de l'architecture informatique de Stadiumcompany.

Pour faire suite à notre comparaison précédente, notre choix de solution se repose vers **le couple GLPI/OCS**.

En effet, il s'agit **d'outils gratuits** qui disposent d'une importante communauté d'utilisateurs très actifs, en plus d'être l'un des couples les plus reconnus dans le domaine de gestion de patrimoine informatique.

Ces outils de gestion du parc informatique vont nous permettre d'assurer :

- **la remontée des inventaires du parc**
- **le déploiement de logiciels sur l'ensemble du parc de façon automatisée**
- **la possibilité pour les salariés de Stadiumcompany de générer un ticket d'incident et aux administrateurs de les résoudre**

À noter que nous serons dotés d'une interface graphique et nous possèderons une base de connaissance conséquente pour les utilisateurs de l'helpdesk.

A) Installation d'OCS NG

Nous utiliserons une machine virtuelle **pour le serveur** :

- **de 512 Mo de mémoire RAM** minimum
- **de 20 Go de disque dur**
- **équipé de deux interfaces réseaux** :
    - eth0 : DHCP (carte réseau sur VMWARE en : bridge ou NAT)
    - eth1 : LAN segment

Nous utiliserons une seconde machine virtuelle **pour le client Windows** :

- **de 512Mo de mémoire RAM minimum**
- **de 15 Go de disque dur**
- **équipé d'une interface en LAN Segment**

Le serveur devra avoir une adresse IP statique sur l'une de ses interfaces (172.20.1.100/24 pour eth1).

1) La configuration des cartes réseau

- **Nous mettons à jour le serveur debian :**

```
root@glppi:/home/shado# apt-get update && apt-get upgrade_
```

- **Nous configurons les cartes réseau :**

```
root@glppi:/home/shado# vi /etc/network/interfaces_
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
address 172.20.1.100
mask 255.255.255.0
network 172.20.1.0
broadcast 172.20.1.255
```

- **Nous redémarrons le service networking :**

```
root@glppi:/home/shado# service networking_restart
```


- **Avant de vérifier que les interfaces sont correctes :**

```
root@ocsng:/home/shado# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:6b:a0:d0
          inet adr:192.168.243.133  Bcast:192.168.243.255  Masque:255.255.255.0
          adr inet6: fe80::20c:29ff:fe6b:a0d0/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:462 (462.0 B)  TX bytes:2466 (2.4 KiB)

root@ocsng:/home/shado# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0c:29:6b:a0:da
          inet adr:172.20.1.100  Bcast:172.20.1.255  Masque:255.255.0.0
          adr inet6: fe80::20c:29ff:fe6b:a0da/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:0 (0.0 B)  TX bytes:798 (798.0 B)
```

Nous pouvons procéder à l'installation du serveur Apache2.

2) L'installation du serveur Apache2

- **Nous installons le paquet Apache2 :**

```
root@ocsng:/home/shado# apt-get install apache2_
```

- **Nous éditons le fichier *//etc/apache2/apache2.conf*** **pour ajouter la ligne ServerName 172.20.1.100 :**

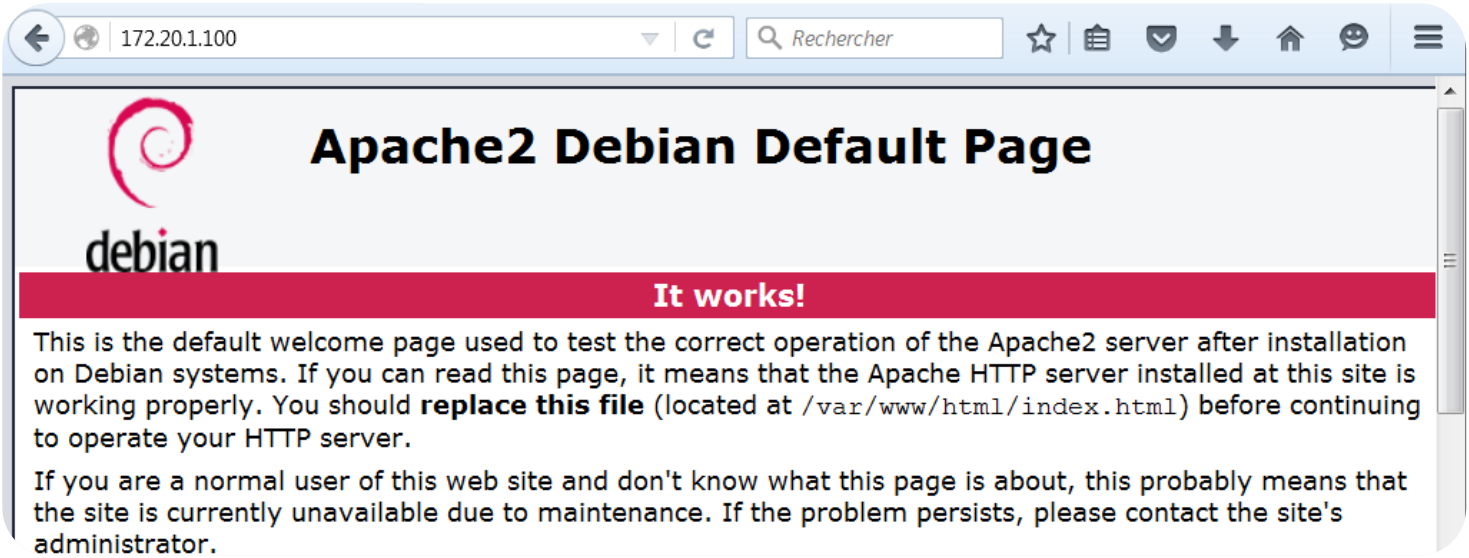
```
root@ocsng:/home/shado# vi /etc/apache2/apache2.conf _


# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
ServerName 172.20.1.100
"/etc/apache2/apache2.conf" 222L, 7139C écrit(s)
root@ocsng:/home/shado# _
```

- **Puis nous redémarrons le serveur Apache2 pour qu'il prenne en compte nos modifications :**

```
root@ocsng:/home/shado# service apache2 restart_
```


À présent, nous allons tester le fonctionnement de votre serveur depuis un navigateur web.

- **Sur un autre poste client appartenant au même réseau, nous inscrivons l'adresse IP de notre machine http://172.20.1.100 :**



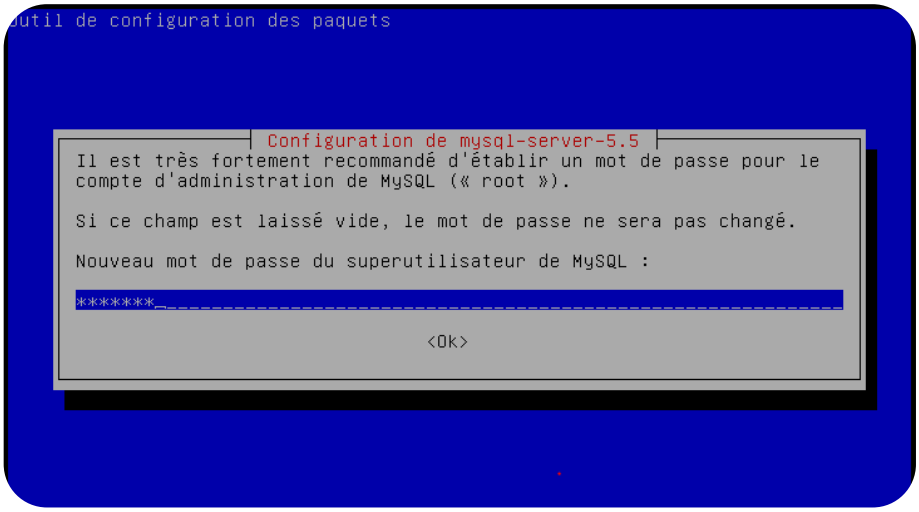
La page Apache2 s'affiche : le serveur est fonctionnel !

3) L'installation de PHP5 et SGBD MySQL

- **Nous installons le paquet php5 mysql-server :**

```
root@ocsng:/home/shado# apt-get install php5 mysql-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libaio1 libapache2-mod-php5 libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libmysqlclient18 libonig2 libqdbm14
  libterm-readkey-perl mysql-client-5.5 mysql-common mysql-server-5.5
  mysql-server-core-5.5 php5-cli php5-common php5-json php5-readline
Paquets suggérés :
  php-pear libclone-perl libmldbm-perl libnet-daemon-perl
  libsql-statement-perl libipc-sharedcache-perl tinyca php5-user-cache
Les NOUVEAUX paquets suivants seront installés :
  libaio1 libapache2-mod-php5 libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libmysqlclient18 libonig2 libqdbm14
  libterm-readkey-perl mysql-client-5.5 mysql-common mysql-server
  mysql-server-5.5 mysql-server-core-5.5 php5 php5-cli php5-common php5-json
  php5-readline
0 mis à jour, 19 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 14,0 Mo dans les archives.
Après cette opération, 117 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] _
```

- **Nous renseignons un mot de passe :**



- **Depuis le terminal, nous testons le bon fonctionnement du serveur MYSQL :**

```
root@ocsng:/home/shado# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 43
Server version: 5.5.46-0+deb8u1 (Debian)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

4) L'installation des librairies Perl et du module php5-mysql

- **Nous installons le paquet libapache2 Perl :**

```
root@ocsng:/home/shado# apt-get install libapache2-mod-perl2 libxml-simple-perl
libapache-dbi-perl libnet-ip-perl libsoap-lite-perl php5-mysql make
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libapache2-reload-perl libbsd-resource-perl libclass-inspector-perl
  libconvert-binhex-perl libcrypt-ssleay-perl libdevel-symdump-perl
  libio-sessiondata-perl libio-stringy-perl libmime-tools-perl
  libossp-uuid-perl libossp-uuid16 libperl5.20 libtask-weaken-perl
  libxmlrpc-lite-perl
Paquets suggérés :
  uuid libmime-lite-perl libnet-jabber-perl make-doc
Les NOUVEAUX paquets suivants seront installés :
  libapache-dbi-perl libapache2-mod-perl2 libapache2-reload-perl
  libbsd-resource-perl libclass-inspector-perl libconvert-binhex-perl
  libcrypt-ssleay-perl libdevel-symdump-perl libio-sessiondata-perl
  libio-stringy-perl libmime-tools-perl libnet-ip-perl libossp-uuid-perl
  libossp-uuid16 libperl5.20 libsoap-lite-perl libtask-weaken-perl
  libxml-simple-perl libxmlrpc-lite-perl make php5-mysql
0 mis à jour, 21 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 2 349 ko dans les archives.
Après cette opération, 8 143 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] _
```

- **Ensuite, nous installons les modules PERL :**

```
root@ocsng:/home/shado# perl -MCPAN -e 'install XML::ENtities'_
```

```
root@ocsng:/home/shado# apt-get install libapache2-mod-perl2-dev_

root@ocsng:/home/shado# cpan apache2::SOAP_
```


- **Puis nous procédons au téléchargement de OCS Server :**

```
root@ocsng:/home/shado# wget https://launchpad.net/ocsinventory-server/stable-2.
1/2.1.2/+download/OCSNG_UNIX_SERVER-2.1.2.tar.gz
--2015-12-16 22:04:45--  https://launchpad.net/ocsinventory-server/stable-2.1/2.
1.2/+download/OCSNG_UNIX_SERVER-2.1.2.tar.gz
Résolution de launchpad.net (launchpad.net)… 91.189.89.222
Connexion à launchpad.net (launchpad.net)|91.189.89.222|:443… connecté.
requête HTTP transmise, en attente de la réponse… 302 Moved Temporarily
Emplacement : https://launchpadlibrarian.net/179739296/OCSNG_UNIX_SERVER-2.1.2.t
ar.gz [suivant]
--2015-12-16 22:04:45--  https://launchpadlibrarian.net/179739296/OCSNG_UNIX_SER
VER-2.1.2.tar.gz
Résolution de launchpadlibrarian.net (launchpadlibrarian.net)… 91.189.89.229, 91
.189.89.228
Connexion à launchpadlibrarian.net (launchpadlibrarian.net)|91.189.89.229|:443…
connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 2890912 (2,8M) [application/x-tar]
Sauvegarde en : « OCSNG_UNIX_SERVER-2.1.2.tar.gz »

G_UNIX_SERVER-2.1.2  37%[=======>             ]   1,04M   172KB/s    eta 11s    _
```

- **Nous extrayons l'archive :**

```
root@ocsng:/home/shado# tar -xzvf OCSNG_UNIX_SERVER-2.1.2.tar.gz _
```

- **Nous lançons l'exécution du script d'installation d'OCS-NG :**

```
root@ocsng:/home/shado# cd OCSNG_UNIX_SERVER-2.1.2
root@ocsng:/home/shado/OCSNG_UNIX_SERVER-2.1.2# ./setup.sh _
```

- **Nous renseignons l'emplacement du fichier de configuration d'apache2 :**

```
AH00526: Syntax error on line 74 of /etc/apache2/apache2.conf:
Invalid Mutex directory in argument file:${APACHE_LOCK_DIR}
Where is Apache main configuration file [] ?/etc/apache2/apache2.conf_
```

- **Puis l'emplacement des fichiers d'inclusion d'apache2 :**

```
Setup will put OCS Inventory NG Apache configuration in this directory.
Where is Apache Include configuration directory [] ?/etc/apache2/conf-enabled_
```

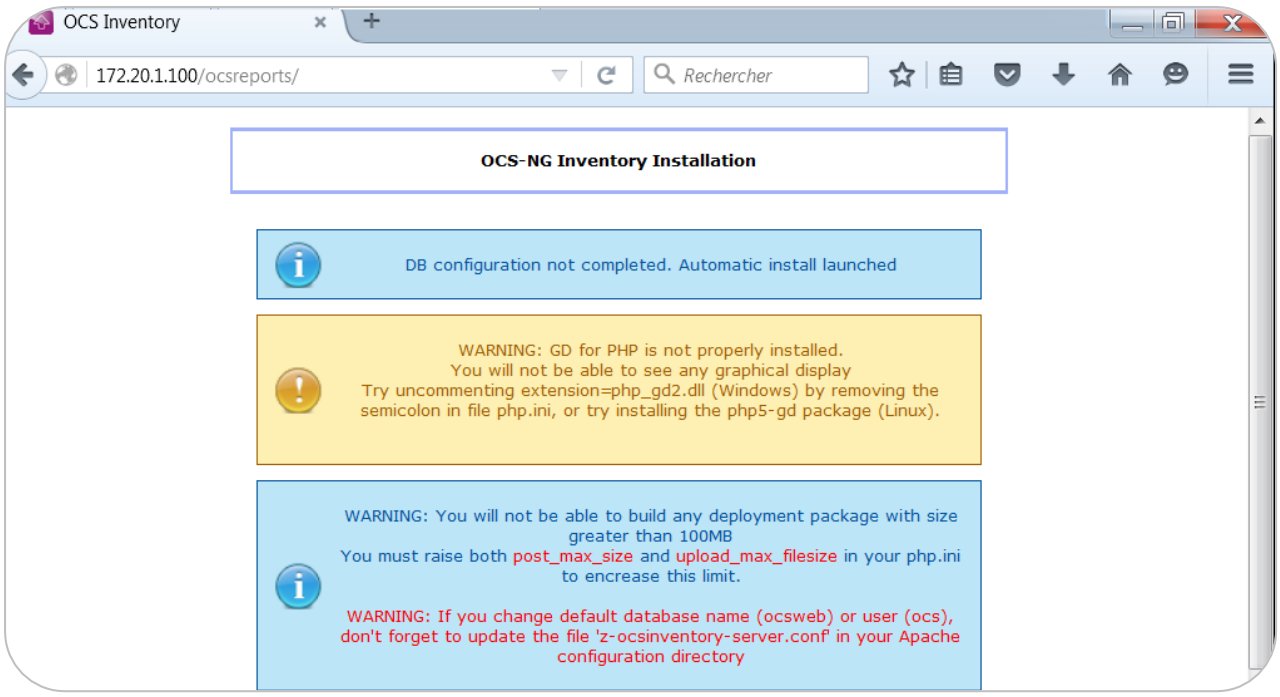
- **Et nous ouvrons le fichier/etc/apache2/conf-enabled/z-ocsinventory-server.conf, et nous modifions les lignes 315 et 316 :**

```
r
        Order deny,allow
        Allow from all
        AuthType Basic
        AuthName "OCS Inventory SOAP Area"
        # Use htpasswd to create/update soap-user (or another granted user)
        #AuthUserFile "APACHE_AUTH_USER_FILE"
        #require "SOAP_USER"
    </location>
-- INSERTION --                                          315,3-10      99%
```

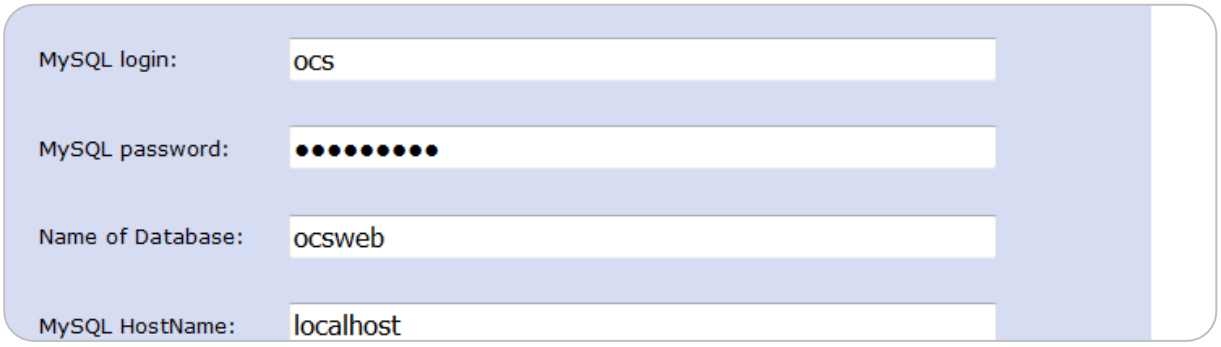
Enfin, nous redémarrons le service apache2 pour que les modifications soient prises en compte.

5) Finalisation de l'installation de OCS depuis l'interface web

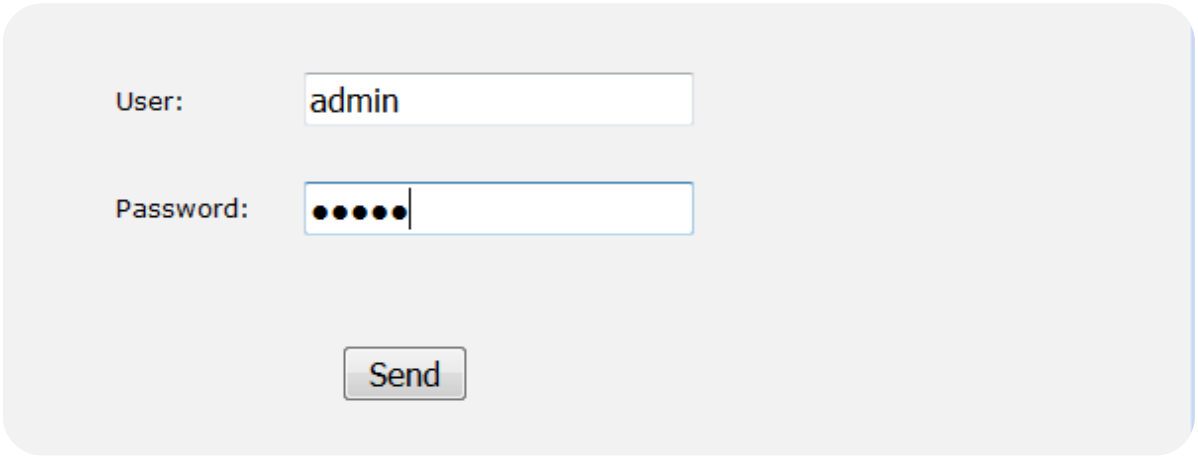
- **Nous lançons le navigateur sur le PC client http://172.20.1.100/ocsreports :**



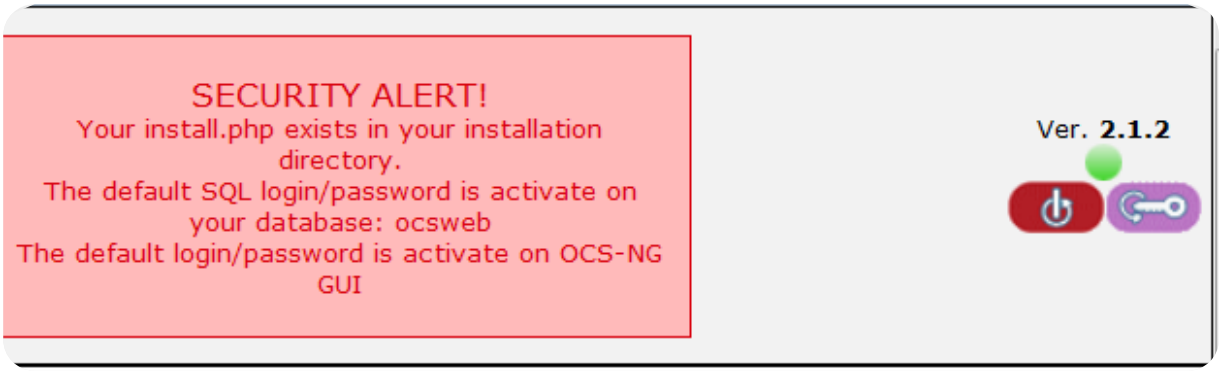
- **Ensuite, nous nous authentifions sur MYSQL-server :**



- **Puis sur l'interface d'OCS avec l'user : admin et le mot de passe : admin, et nous changeons le mot de passe admin :**



6) Applications des correctifs



- **Pour la première alerte de sécurité, nous renommons le fichier install.php :**

```
root@ocsng:/home/shado/OCSNG_UNIX_SERVER-2.1.2# mv /usr/share/ocsinventory-repor
ts/ocsreports/install.php /usr/share/ocsinventory-reports/ocsreports/install.php
.old_
```

- **Pour la seconde alerte de sécurité, nous éditons le fichier z-ocsinventory-server.conf**

```
  # User allowed to connect to database
  PerlSetEnv OCS_DB_USER ocs
  # Password for user
  PerlSetVar OCS_DB_PWD ocsscret_

  # Slave Database settings
  # Replace localhost by hostname or ip of MySQL server for READ
-- INSERTION --                                          31,33         3%
```

- **Nous remplaçons le mot de passe (ocs) au niveau de la ligne 31 par le mot de passe renseigné dans la requête SQL (UPDATE), puis nous enregistrons le fichier :**

```
define("DB_NAME", "ocsweb");
define("SERVER_READ","localhost");
define("SERVER_WRITE","localhost");
define("COMPTE_BASE","ocs");
define("PSWD_BASE","ocssecret");
?>
```


B) Installation de GLPI (Gestionnaire Libre de Parc Informatique)

1) Création de la base de données et de l'utilisateur, et installation de la version de GLPI

- **Nous créons d'une part la base de données « glpidb » qui sera utilisée par GLPI :**

```
shado@ocsng:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 71
Server version: 5.5.46-0+deb8u1 (Debian)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE glpidb;
Query OK, 1 row affected (0.05 sec)
```

- **Et d'autre part l'utilisateur « glpiuser » (avec son mot de passe) et lui accordons les privilèges maximums :**

```
mysql> grant all privileges on glpidb.*to glpiuser@localhost identified by 'glpi
secret';
Query OK, 0 rows affected (0.00 sec)
```

2) Téléchargement de la version de GLPI

- **Nous récupérons la version 0.90 de GLPI sur le site forge.indepnet.net :**

```
shado@ocsng:/var/www$ cd /var/www/html_
```


- **Puis nous décompressons l'archive dans le répertoire"/var/www/" ou "/var/www/html" si le dossier html existe :**

```
root@ocsng:/var/www# wget http://github.com/glpi-project/glpi/releases/download/
0.90/glpi-0.90.tar.gz
--2015-12-17 22:01:31--  http://github.com/glpi-project/glpi/releases/download/0
.90/glpi-0.90.tar.gz
Résolution de github.com (github.com)… _

root@ocsng:/var/www# tar -xzvf glpi-0.90.tar.gz _
```

7) Changement du propriétaire du dossier GLPI en « www-data » sur le serveur apache

```
root@ocsng:/var/www/html/glpi# chown -R www-data /var/www/html/glpi_
```

8) Installation du paquet « php5-gd »

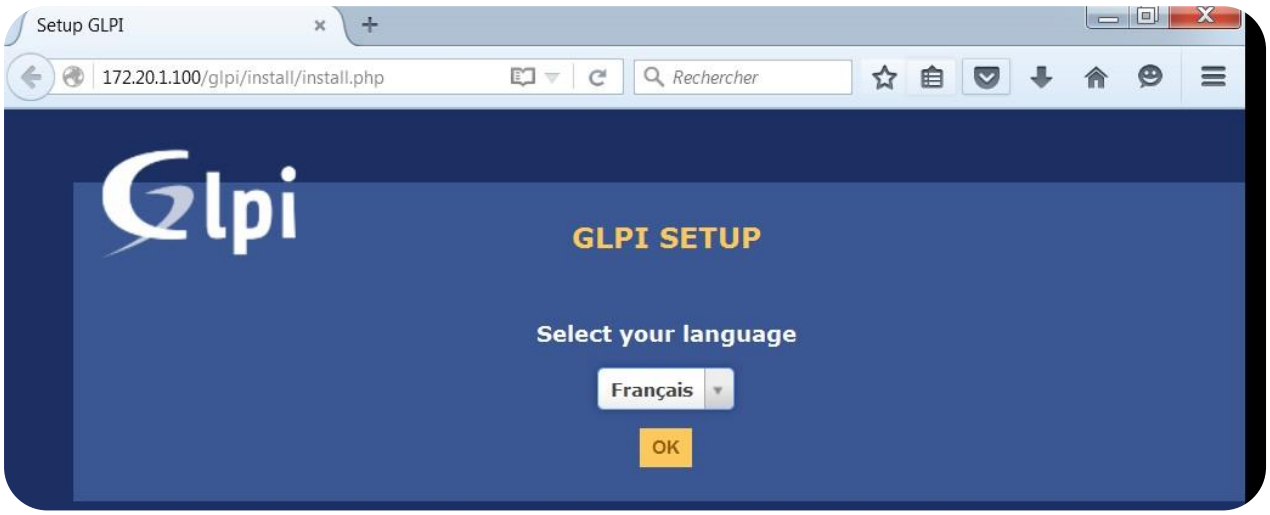
```
root@ocsng:/var/www/html/glpi# apt-get install php5-gd_
```

Il nous reste à redémarrer le serveur apache2 afin que les modifications soient prises en compte :

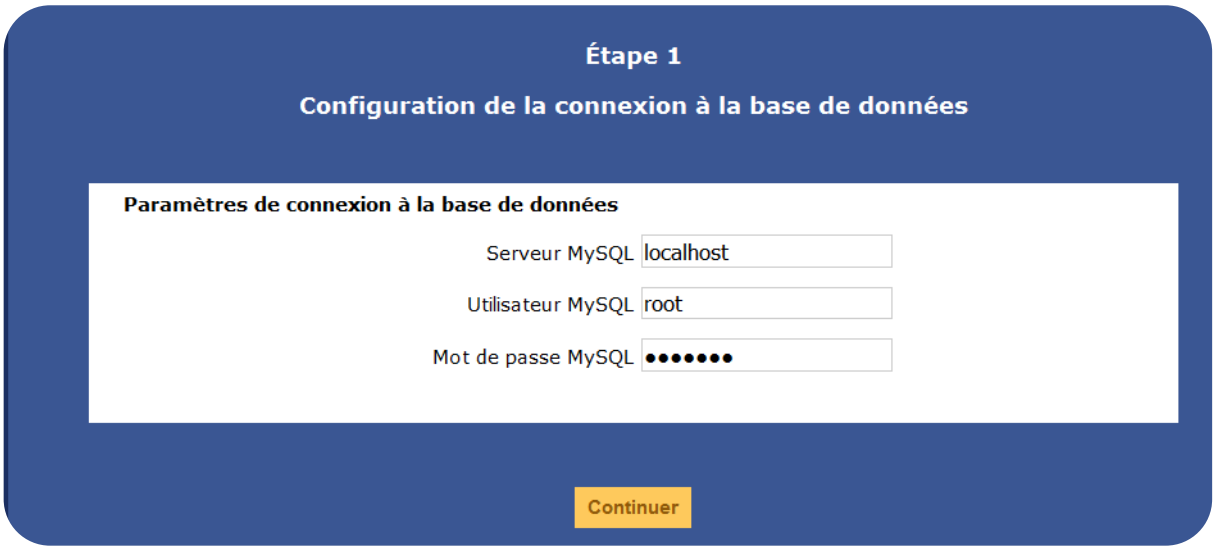
```
root@ocsng:/var/www/html/glpi# service apache2 restart
```


9) Finalisation de l'installation de GLPI depuis l'interface web

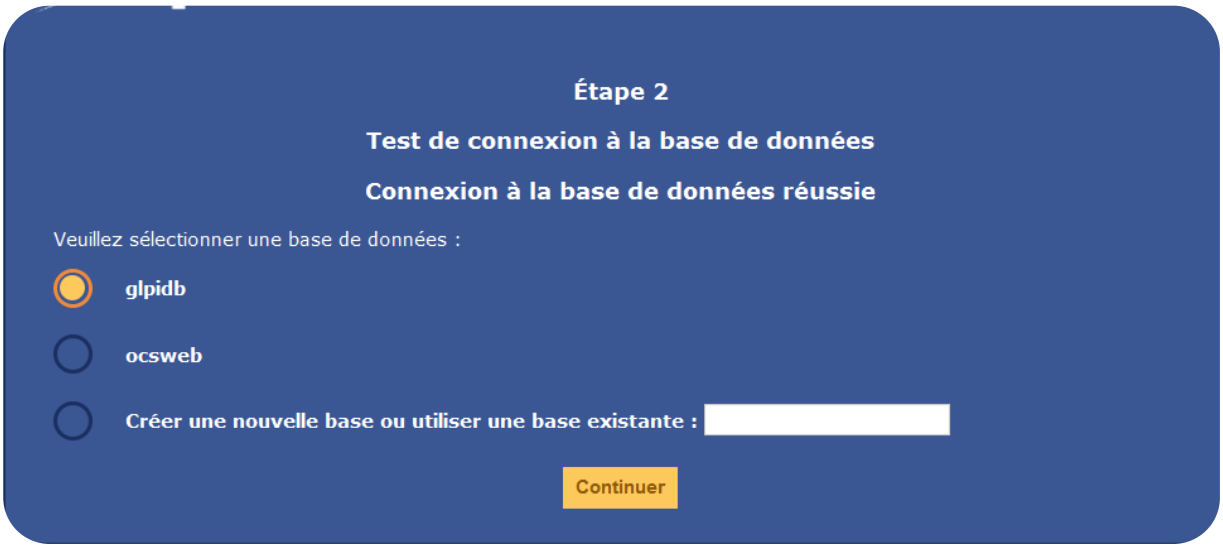
- **Nous nous connectons à l'interface Web de GLPI :**



- **Nous remplissons le formulaire avec les éléments précédemment configurés :**



- **Nous sélectionnons une base de données pour GLPI :**

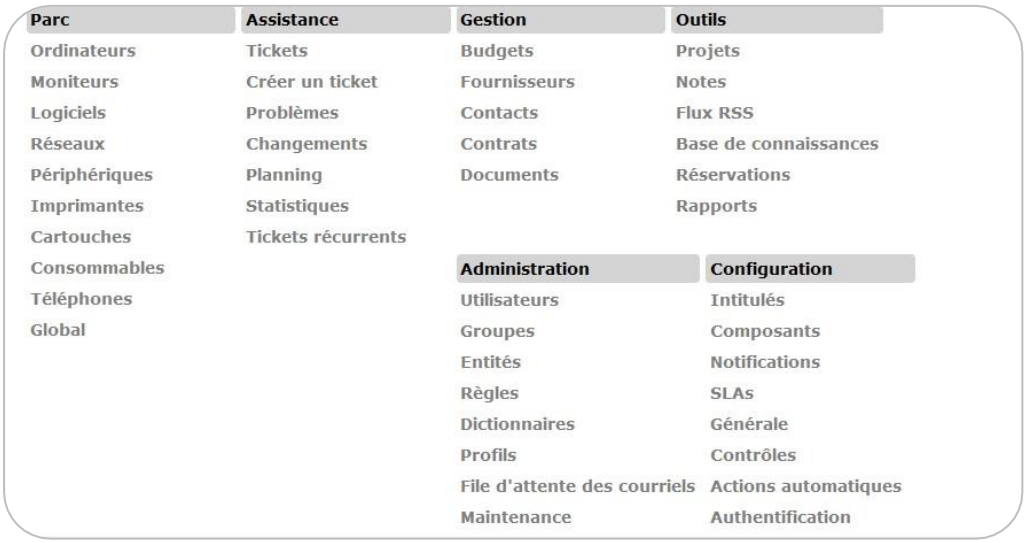


- **Enfin, nous terminons l'installation de GLPI :**

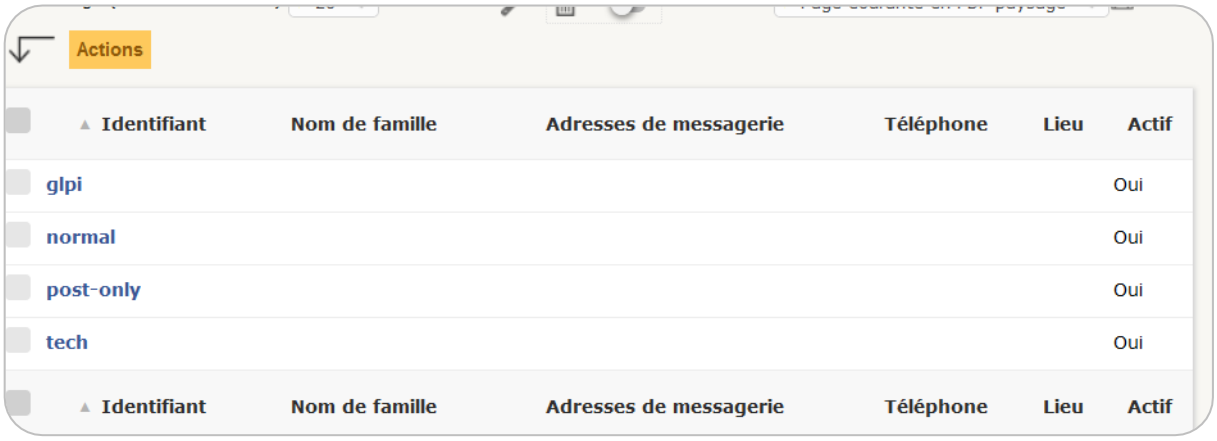
10) Applications des correctifs

- **Nous nous connectons à la session de l'utilisateur administrateur de GLPI :**

- **Nous entrons dans le menu Administrateur/Utilisateurs :**



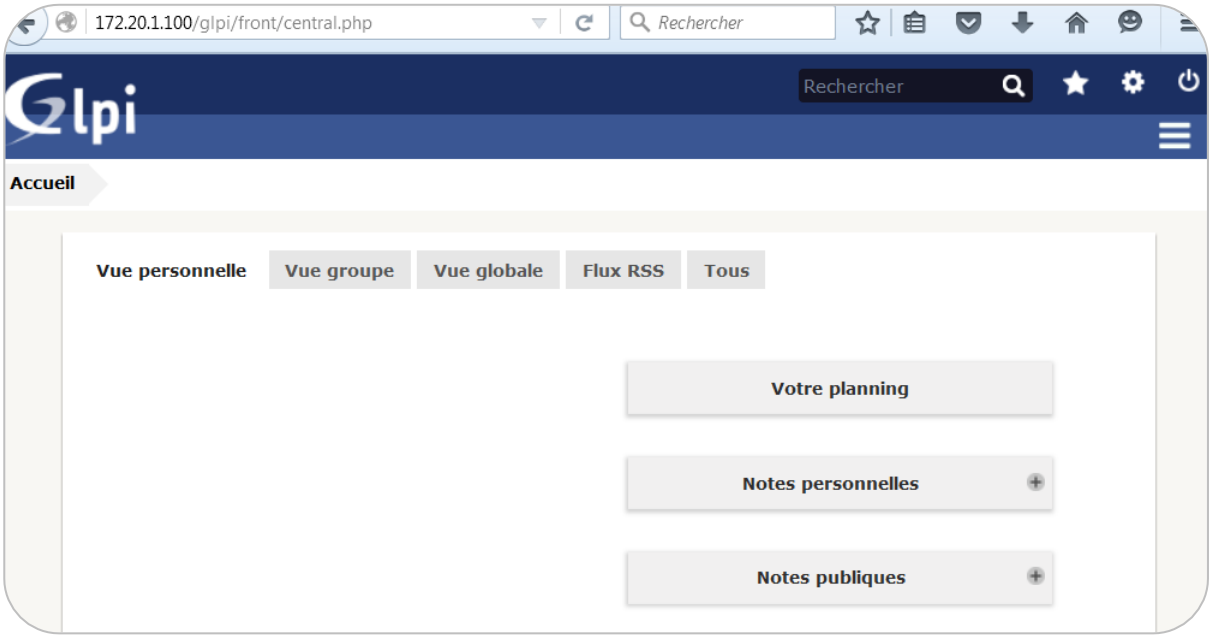
- **Nous cliquons sur un utilisateur pour modifier son profil et son mot de passe :**



- **Sur la machine Debiann nous changeons le nom du script « install.php » :**

```
root@ocsng:/var/www/html/glpi# mv /var/www/html/glpi/install/install.php /var/ww
w/html/glpi/install/install.php.old
```

- **Enfin, sur le poste du client, nous rafraichissons la page et constatons que les erreurs ont disparu :**



C) Installation du plugin GLPI/OCS

Le plugin GLPI/OCS permet de synchroniser GLPI avec la solution d'inventaire OCS Inventory NG.

- **Sur la machine Debian, nous nous dirigeons vers le dossier « plugin » de GLPI :**

```
root@ocsng:~# cd /var/www/html/glpi/plugins/_
```

- **Nous téléchargeons le plugin GLPI/OCS :**

```
root@ocsng:/var/www/html/glpi/plugins# wget https://forge.glpi-project.org/attac
hements/download/2016/glpi-ocsinventoryng-1.2.0.tar.gz
--2015-12-20 07:33:55--  https://forge.glpi-project.org/attachements/download/20
16/glpi-ocsinventoryng-1.2.0.tar.gz
Résolution de forge.glpi-project.org (forge.glpi-project.org)… _
```

- **Ensuite, nous décompressons l'archive téléchargée :**

```
root@ocsng:/var/www/html/glpi/plugins# tar -xzvf glpi-ocsinventoryng-1.2.1.tar.g
z _
```

- **Enfin, sur l'interface Web de GLPI, nous activons le plugin GLPI/OCS :**

Mission 7 : Solution de supervision de l'infrastructure réseau et système permettant d'assurer l'anticipation des pannes

Paragraphe 1 : Qu'est-ce que la supervision ?

- La supervision permet de surveiller l'ensemble du parc informatique d'une organisation. Les outils de supervisions s'appellent des superviseurs qui permettent de surveiller les traitements informatiques. Dès qu'un traitement ne s'est pas exécuté correctement, l'outil de supervision déclenche une alerte ; l'alerte est ensuite traitée par l'équipe en charge du monitoring
- L'équipe de pilotage ont pour mission de surveiller les alertes remontées par le logiciel et d'exécuter des consignes pour résoudre ces alertes. Aussi, les logiciels de supervision permettent de remonter des informations techniques et fonctionnelles du système d'information, en fonction du type d'équipement supervisé.
- Il est primordial que le système d'information puisse fonctionner pleinement et en permanence pour garantir l'efficacité de l'entreprise. En effet, les équipements réseaux, les PC des utilisateurs, les serveurs d'applications et les données constituent des éléments sensibles dont la disponibilité et la qualité de service conditionnent le bon fonctionnement de l'entreprise.
- Les problèmes liés à l'informatique doivent donc être réduits au minimum, car une indisponibilité du système d'information a des impacts très préjudiciables sur l'activité et sur la notoriété d'une entreprise.
- Une DSI fait face à deux enjeux : garantir la disponibilité du SI aux utilisateurs et tenter de prévenir en cas de problème et, le cas échéant, garantir une remontée d'information rapide et une durée d'intervention minimale. C'est le rôle de la supervision.

Paragraphe 2 : Comment superviser notre système d'information ?

Il existe plusieurs méthodes pour superviser le système d'information :

- Analyser les fichiers de log
- Récupérer des résultats de commandes et de scripts locaux ou distants
- SNMP : Simple Network Management Protocol

Paragraphe 3 : Nagios

La solution que nous proposons est la suivante : Nagios. En effet, Nagios est une solution de supervision très populaire, ce logiciel permet de nous informer de problèmes éventuels dans notre système d'informations avant que vos clients, utilisateurs ou managers ne le fassent. Nagios est un logiciel multiplateforme, qui peut être exécuté sur différents systèmes d'exploitation tels que Linux, Unix et Windows. Nous pouvons donc choisir le système d'exploitation qui convient le mieux à nos besoins en matière de performance, de fiabilité et de compatibilité avec leurs autres applications et systèmes. Il est important de noter que Nagios nécessite une installation et une configuration minimales pour fonctionner, et que les administrateurs doivent disposer des compétences nécessaires pour effectuer ces tâches. Le logiciel effectue des contrôles intermittents sur les hôtes et services que l'on spécifie en utilisant des plugins externes qui retournent un statut d'état à Nagios. Quand des problèmes surviennent, il peut envoyer des notifications à des contacts administratifs de façons différentes (email, SMS, messagerie instantanée, etc...). Les informations d'états courants, les historiques et les rapports peuvent être consultés à partir d'une simple interface web.

Nous pouvons citer les avantages suivants de notre solution de supervision :

- Vérification des services réseau (SMTP, http, etc…)
- Surveillance des ressources des hôtes (CPU, RAM, etc...)
- Contrôle des équipements réseau (CPU, ventilateurs, etc...)
- Service de notification fonction de l'état d'un service
- Gestion des escalades (par acquittement d'hôte ou de service par le superviseur en charge)
- Possibilité de paramétrer des réactions automatisées (masquer la supervision durant une plage de temps donnée qu'elle soit ponctuelle ou récurrente)
- Panoplie de plugins de vérification compatibles
- Possibilité de définir une hiérarchie des hôtes avec le système parents/enfants
- Une interface Web avec gestion des droits pour la consultation et/ou la modification de paramétrage de la supervision
- Génération de rapports de surveillance (automatisé ou non, communiqué ou non)

A) Architecture de Nagios

On peut découper Nagios en 3 parties techniques :

- Les tâches de supervision (requêtes SNMP) sont effectuées par un collecteur (ou ordonnanceur, voire poller chez Centreon)
- Une interface web, permettant l'affichage de la page de supervision (contenant le statut des hôtes)
- Les plugins, permettant d'être exploités en fonction du besoin de l'entreprise (par exemple : le plugin One Access ne sera pas sollicité si a totalité des équipements supervisés sont de la marque CISCO)

B) Les statuts

Chaque test renvoi un état particulier :

1. **OK** (aucune alerte n'est à déplorer, l'équipement fonctionne correctement)

2. **WARNING** (le seuil d'alerte paramétré, ou laissé par défaut est dépassé, ce seuil permet d'attirer l'attention et laisser place ou non à une action avant le seuil CRTICAL)

3. **CRITICAL** (le seuil d'alerte critique a été dépassé, le service est en état d'alerte)

4. **UNKNOWN** (l'hôte ou le service reste tout bonnement injoignable, impossible donc de savoir si le service est OK ou en alerte)

Nagios est un noyau, un logiciel Open Source. Il existe plusieurs dérivés destinés à être des versions améliorées voire personnalisées de Nagios. Parmi ces dérivés on peut citer le plus connu : Centreon.

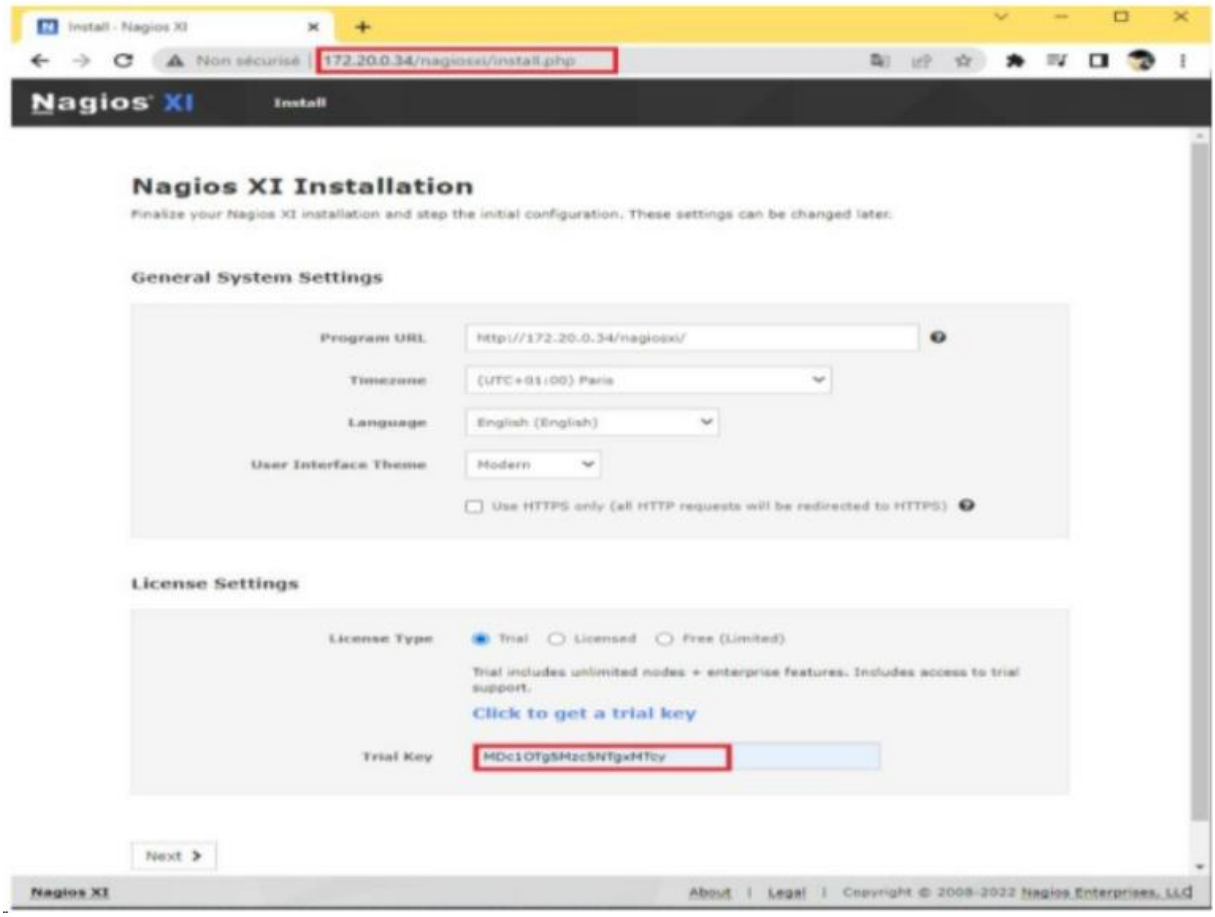
Centreon propose une interface Web très esthétique et facile d'utilisation afin de pouvoir superviser et configurer ses hôtes et ses services. De plus, Centreon propose un vaste choix de plugins packs afin de superviser de nombreux équipements de différentes marques.

Paragraphe 4 : Installation de Nagios

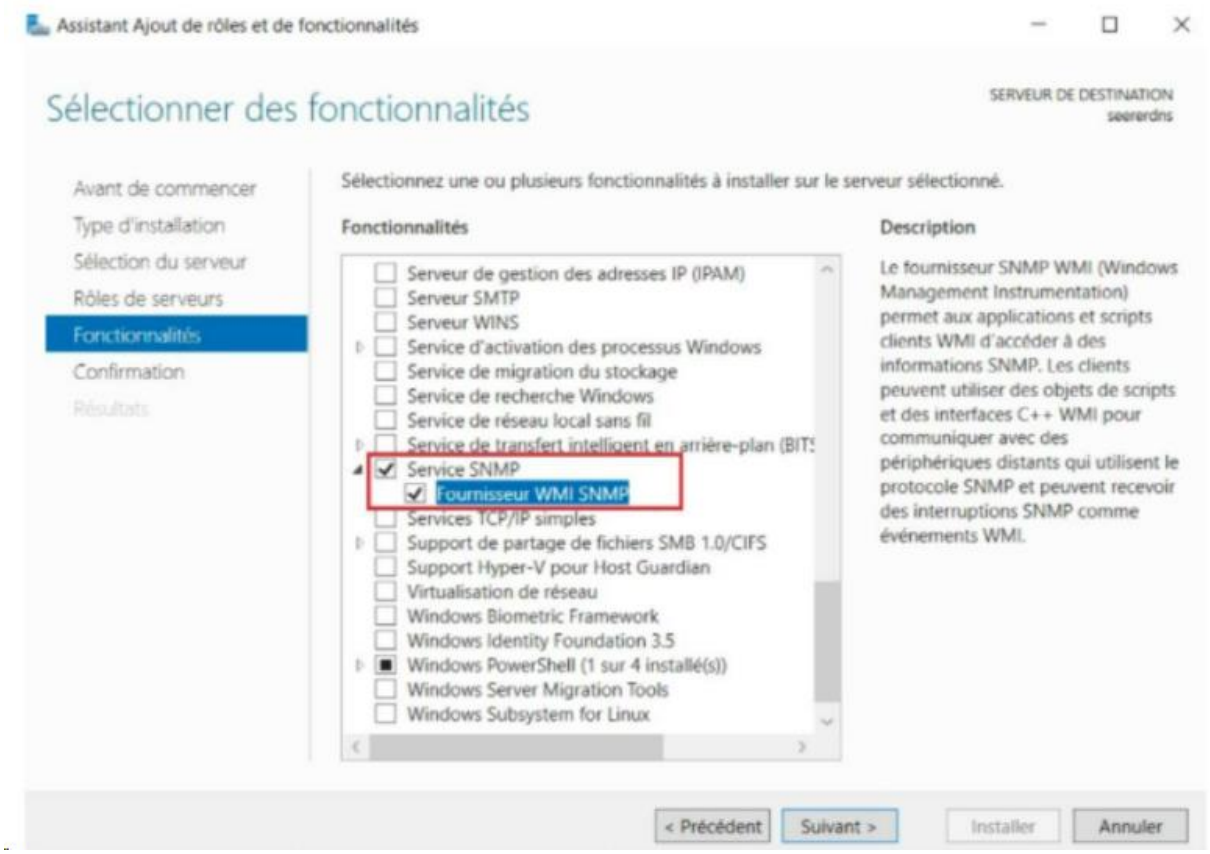
Passons maintenant à l'installation de Nagios :

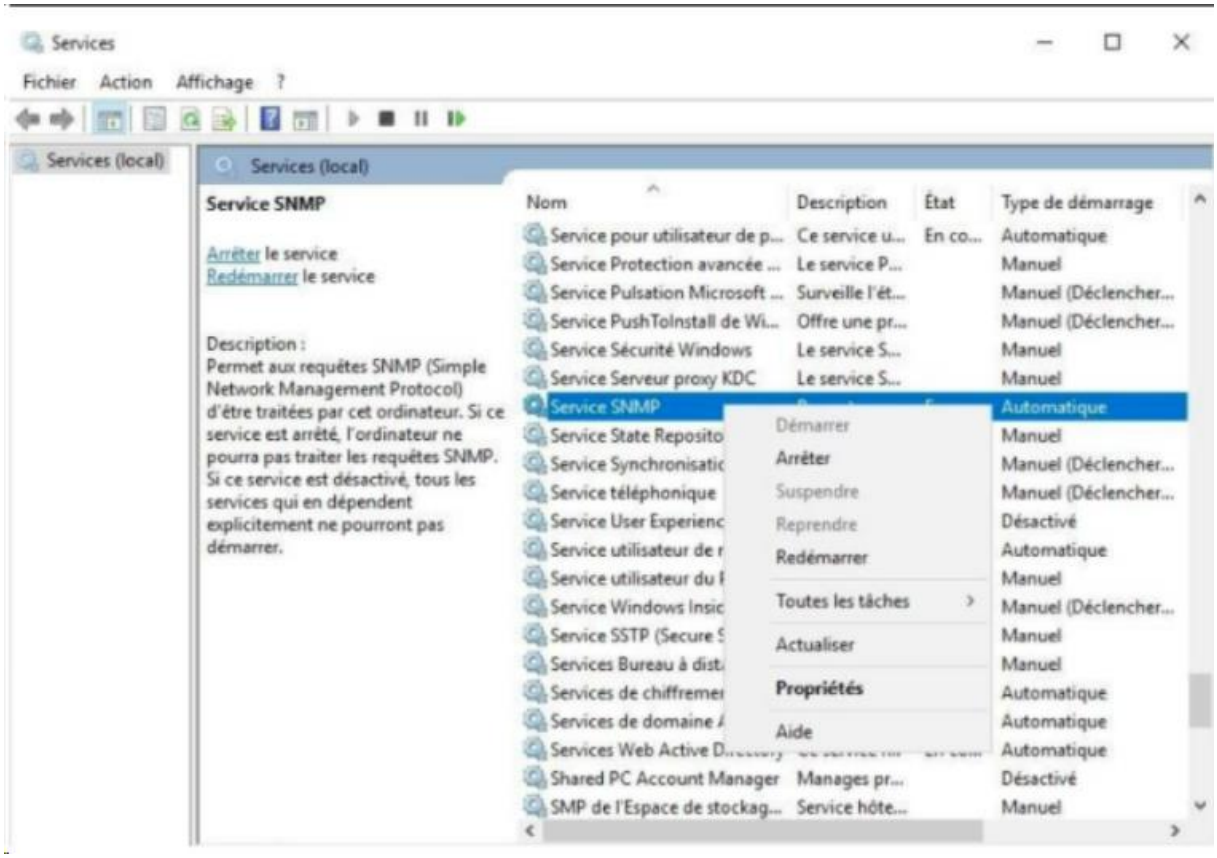
- Dans un premier temps on installe et on met à jour une machine Debian puis on installe les paquets nécessaires au fonctionnement de Nagios dans la machine :

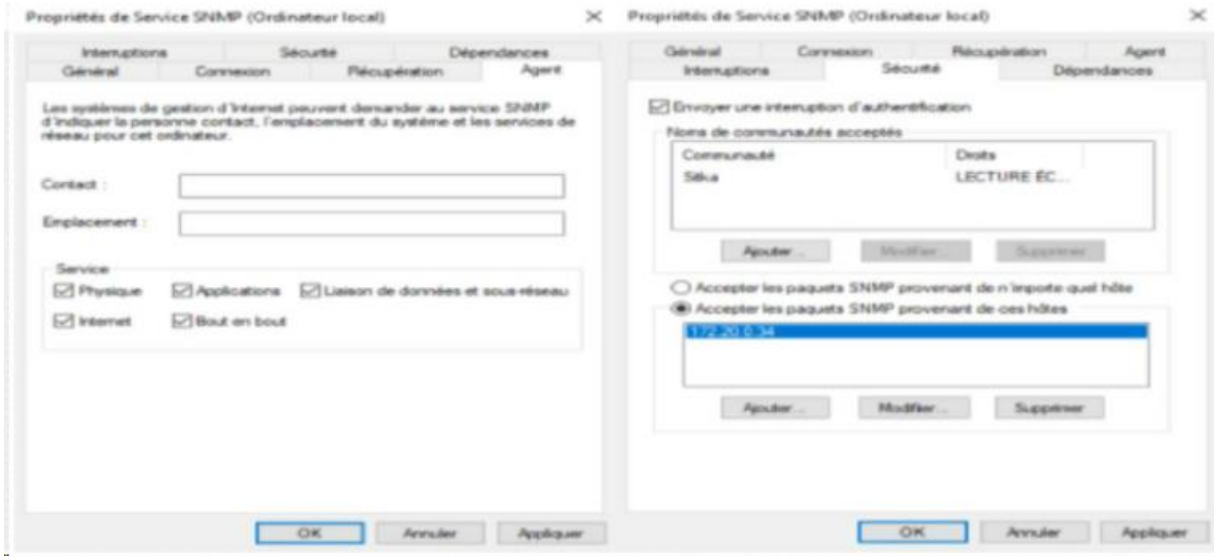
- On se charge ensuite d'utiliser la clé d'activation afin d'activer Nagios, on entre alors dans la période d'essai de 60 jours



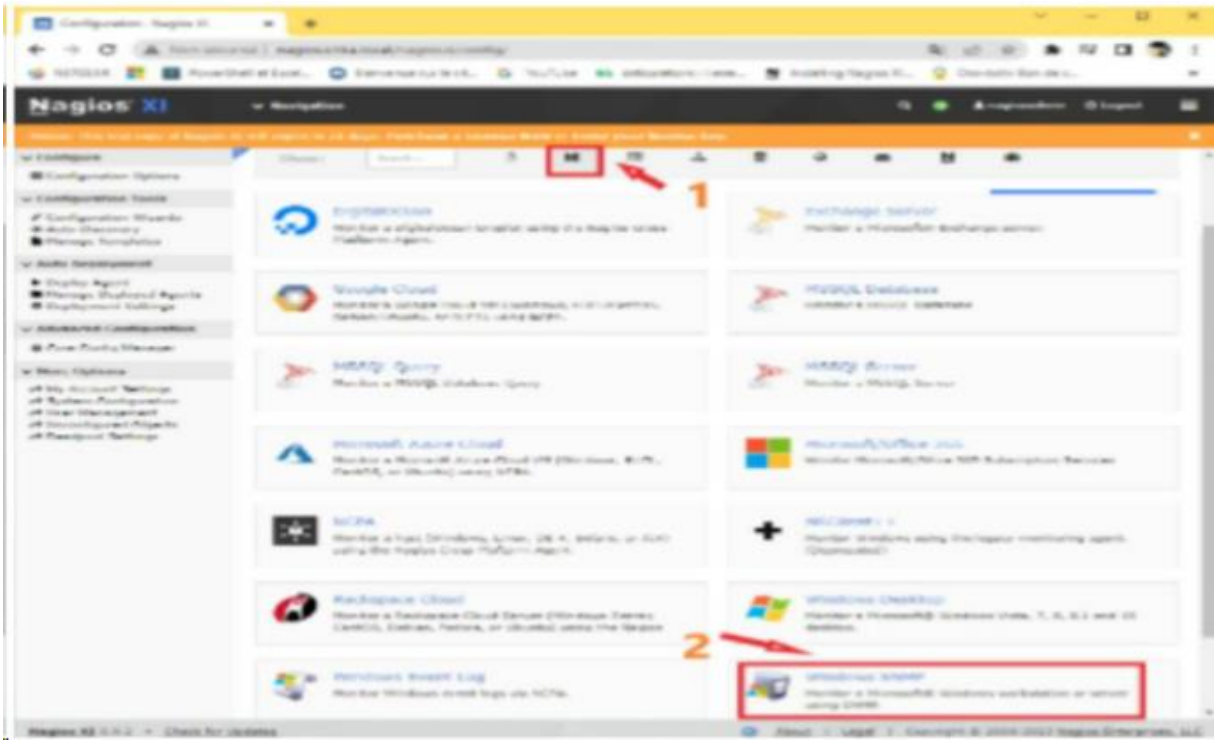
- Installons maintenant le protocole SNMP dans notre Active Directory :

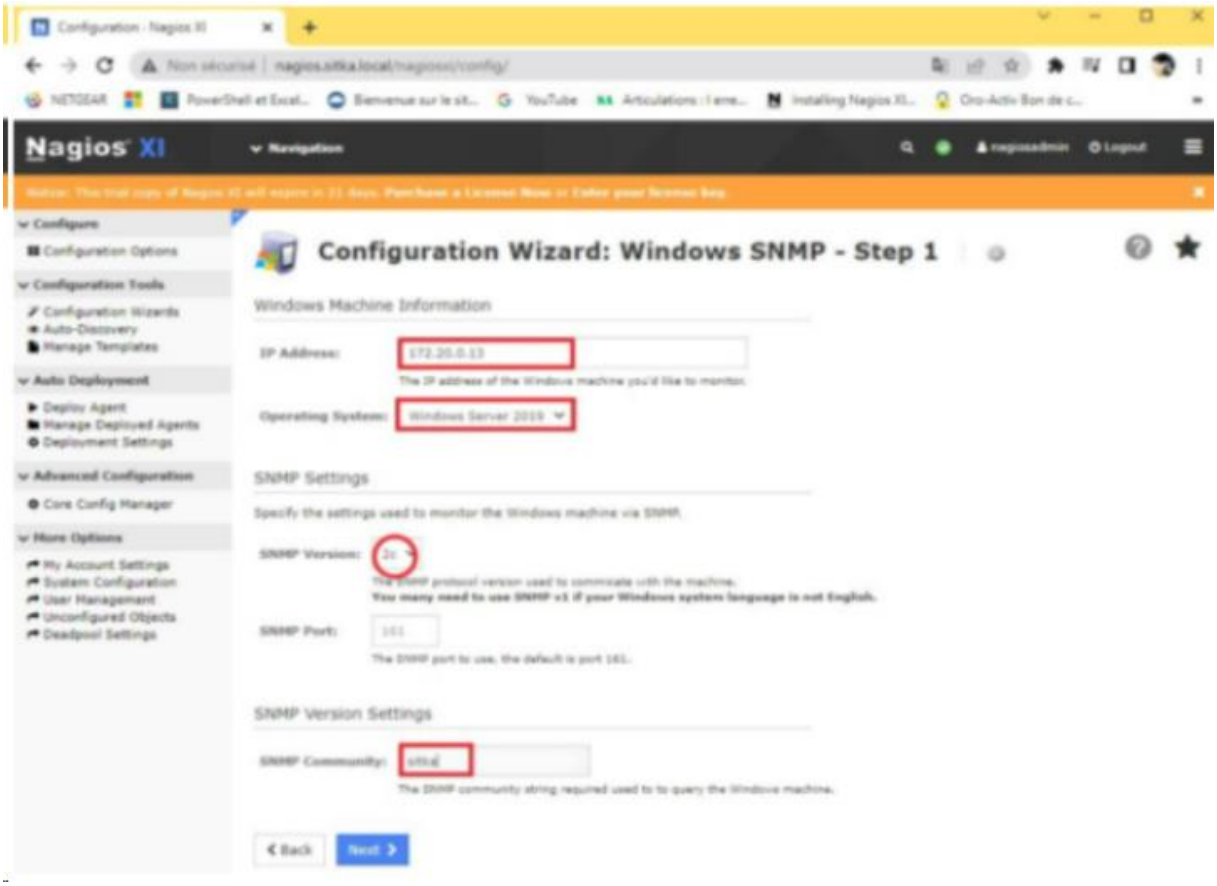

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des fonctionnalités
SERVEUR DE DESTINATION
seererdns
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.
Fonctionnalités
Description
Serveur de gestion des adresses IP (IPAM)
Serveur SMTP
Serveur WINS
Service d'activation des processus Windows
Service de migration du stockage
Service de recherche Windows
Service de réseau local sans fil
Service de transfert intelligent en arrière-plan (BITS
Service SNMP
Fournisseur WMI SNMP
Services TCP/IP simples
Support de partage de fichiers SMB 1.0/CIFS
Support Hyper-V pour Host Guardian
Virtualisation de réseau
Windows Biometric Framework
Windows Identity Foundation 3.5
Windows PowerShell (1 sur 4 installé(s))
Windows Server Migration Tools
Windows Subsystem for Linux
Le fournisseur SNMP WMI (Windows Management Instrumentation) permet aux applications et scripts clients WMI d'accéder à des informations SNMP. Les clients peuvent utiliser des objets de scripts et des interfaces C++ WMI pour communiquer avec des périphériques distants qui utilisent le protocole SNMP et peuvent recevoir des interruptions SNMP comme événements WMI.
< Précédent
Suivant >
Installer
Annuler

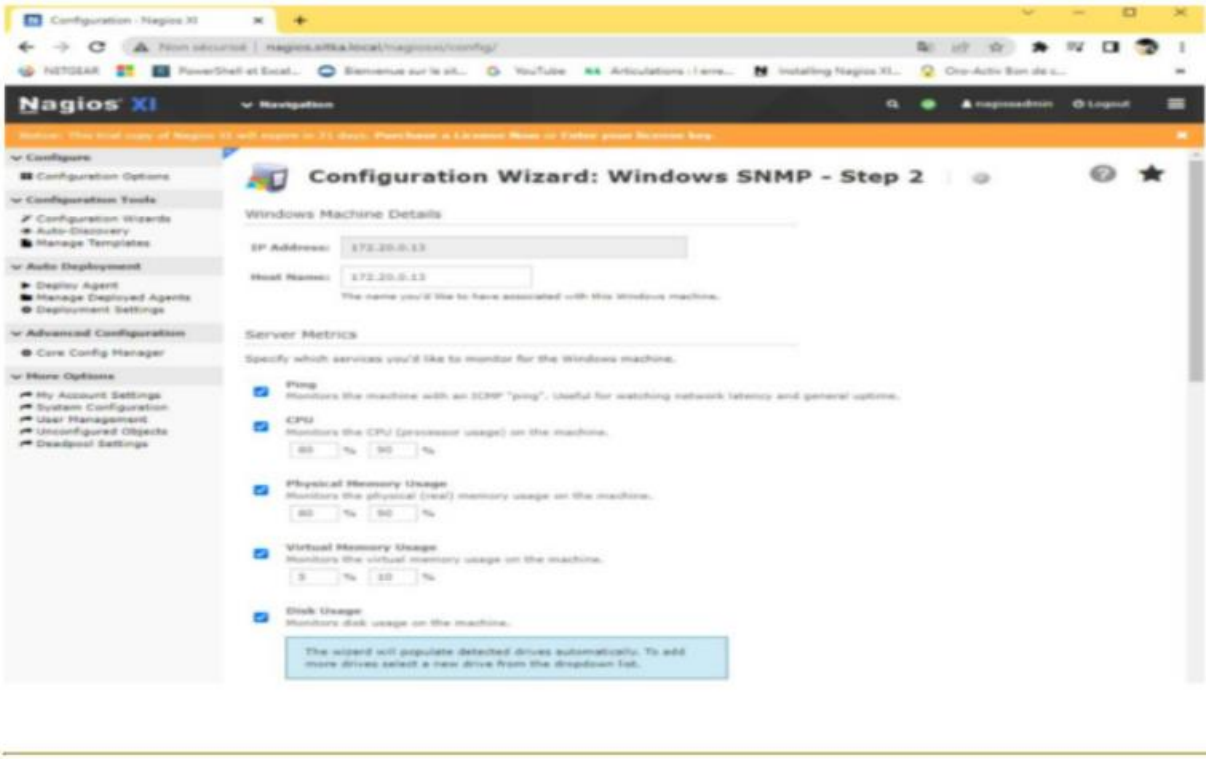

Services
Fichier
Action
Affichage
?
Services (local)
Services (local)
Service SNMP
Arrêter le service
Redémarrer le service
Description :
Permet aux requêtes SNMP (Simple Network Management Protocol) d'être traitées par cet ordinateur. Si ce service est arrêté, l'ordinateur ne pourra pas traiter les requêtes SNMP. Si ce service est désactivé, tous les services qui en dépendent explicitement ne pourront pas démarrer.
Nom
Description
État
Type de démarrage
Service pour utilisateur de p...
Ce service u...
En co...
Automatique
Service Protection avancée ...
Le service P...
Manuel
Service Pulsation Microsoft ...
Surveille l'ét...
Manuel (Déclencher...
Service PushToInstall de Wi...
Offre une pr...
Manuel (Déclencher...
Service Sécurité Windows
Le service S...
Manuel
Service Serveur proxy KDC
Le service S...
Manuel
Service SNMP
Automatique
Service State Reposito
Manuel
Service Synchronisatic
Manuel (Déclencher...
Service téléphonique
Manuel (Déclencher...
Service User Experienc
Désactivé
Service utilisateur de r
Automatique
Service utilisateur du I
Manuel
Service Windows Insic
Manuel (Déclencher...
Service SSTP (Secure S
Manuel
Services Bureau à dist
Manuel
Services de chiffremer
Automatique
Services de domaine A
Automatique
Services Web Active D
Automatique
Shared PC Account Manager
Manages pr...
Désactivé
SMP de l'Espace de stockag...
Service hôte...
Manuel
Démarrer
Arrêter
Suspendre
Reprendre
Redémarrer
Toutes les tâches
Actualiser
Propriétés
Aide

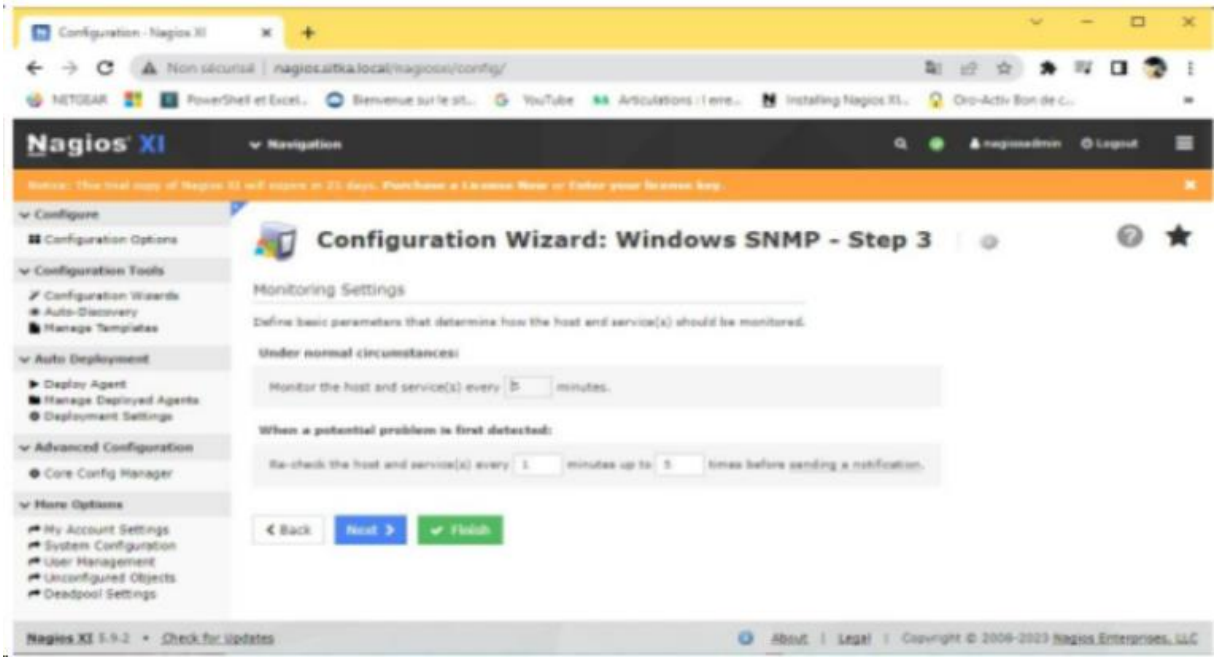


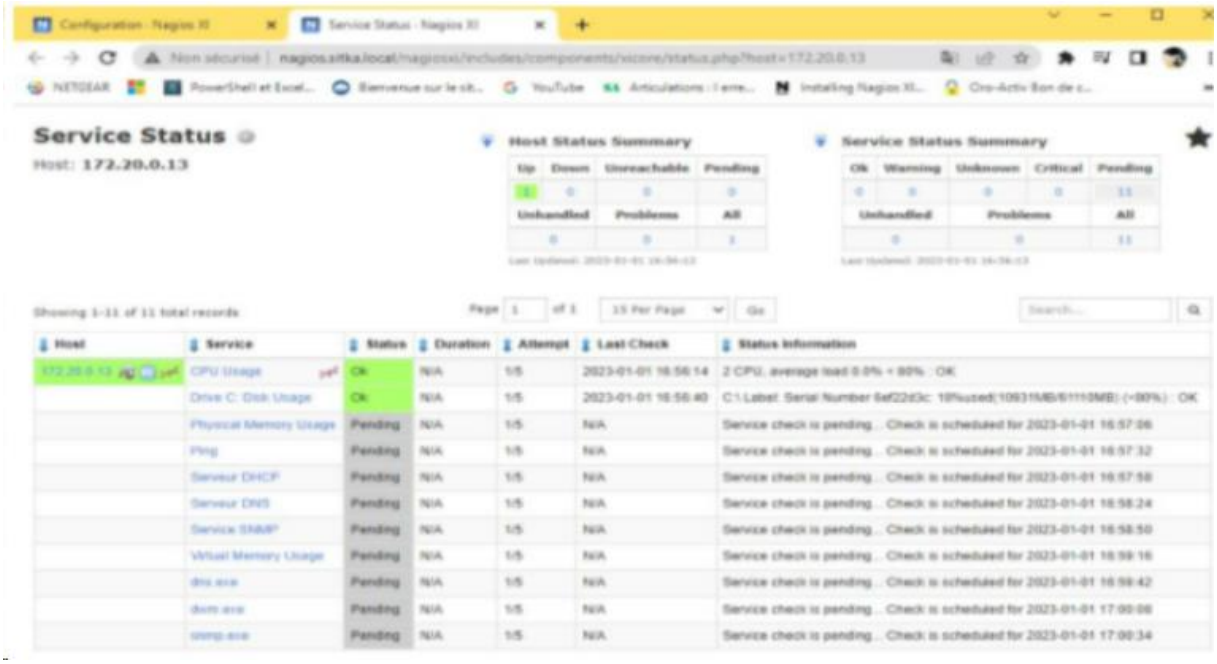
- Une fois le SNMP installé, on ajoute nos hôtes à superviser dans Nagios :




Nagios XI
Configuration Wizard: Windows SNMP - Step 1
Windows Machine Information
IP Address:
Operating System:
SNMP Settings
SNMP Version:
SNMP Port:
SNMP Version Settings
SNMP Community:
Back
Next


Nagios XI
Configuration Wizard: Windows SNMP - Step 2
Windows Machine Details
Server Metrics
Ping
CPU
Physical Memory Usage
Virtual Memory Usage
Disk Usage





- On retrouve maintenant la supervision dont nous avons parlé plus haut avec les statuts de chaque service, à noter que le statut *Pending* signifie que le poller va requêter pour la première fois le service (ou l'hôte) supervisé et qu'il est en attente de sa réponse.

Mission 8 : Systèmes de gestion des événements et des informations de sécurité

Introduction

Zimbra Collaboration Suite (ZCS) est une suite de logiciels de collaboration, qui comprend un serveur de messagerie et un client Web, actuellement détenue et développée par Zimbra, Inc. (anciennement Telligent Systems).
Zimbra a été initialement développé par Zimbra, Inc., et publié en 2005. La société a ensuite été achetée par Yahoo! en septembre 2007, et plus tard vendue à VMware, le 12 janvier 2010. En juillet 2013, elle a été vendue par VMware à Telligent Systems qui a changé son propre nom pour « Zimbra, Inc. » en septembre 2013.
En août 2015, Verint rachète Zimbra, Inc., cède ZCS à Synacor, et réintroduit le nom de Telligent pour les actifs restants.
Selon l'ancien président et directeur de la technologie de Zimbra Scott Dietzen, le nom de Zimbra est dérivé de la chanson I Zimbra des Talking Heads.
Historique et chiffres
Le 17 septembre 2007, Yahoo! rachète Zimbra pour 350 millions de dollars3.
Le 12 janvier 2010, VMware a conclu un accord définitif avec Yahoo! pour acquérir Zimbra4 pour un montant estimé à 100 millions de dollars5.
Le 15 juillet 2013, Telligent annonce qu'elle acquiert la totalité des actifs de Zimbra et que les deux entités fusionnent sous la bannière de Zimbra, Inc6. L'entreprise texane entend ainsi compléter les outils de messagerie avancés de Zimbra en y intégrant ses propres outils collaboratifs : messagerie et communication instantanée, fonctions de réseau social, stockage et communautés en ligne.
En janvier 2015, Zimbra comptabilise plus de 100 millions d'utilisateurs pour la version payante et plus de 500 millions de téléchargements pour sa version Open-Source [réf. nécessaire].
Le 18 août 2015, Synacor, entreprise cotée au NASDAQ, annonce l'acquisition de la suite logicielle Zimbra sur la base d'une valorisation de 24,5 millions de dollars7.
Installer Zimbra Ubuntu 20.04INSTALLATIONZIMBRAInstaller Zimbra Ubuntu 20.04Fanny Komala Sari21 Octobre 20217 Commentaires12.1k
Installez Zimbra Ubuntu 20.04. Dans ce tutoriel, nous discutons de l'installation de Zimbra sur Ubuntu 20.04. Zimbra est un logiciel de serveur de messagerie open source qui fournit des services de messagerie à ses utilisateurs, à la fois pour l'envoi et la réception d'e-mails. En outre, zimbra fournit également d'autres fonctionnalités telles que le partage d'e-mails et peut également être synchronisé avec Nextcloud. Il existe de nombreuses plates-formes de serveur de messagerie disponibles, mais à notre avis, Zimbra
Avant de commencer Installez Zimbra Ubuntu 20.04. Ce Zimbra, il y a quelques explications ci-dessous que vous devriez connaître sur Zimbra, telles que :
Installer Zimbra Ubuntu 20.04
Histoire De Zimbra
Zimbra Collaboration Suite (ZCS) est un produit collaboratif de Zimbra, Inc., situé à San Mateo, Californie, États-Unis. Cette société a été rachetée par Yahoo! en septembre 2007 [1]. Ce

logiciel comprend des composants client et serveur. Zimbra est disponible en deux versions : une version open source et une version prise en charge commercialement (« Zimbra Network ») avec des composants source commerciaux. Des versions de ce logiciel sont disponibles auprès de Zimbra pour un téléchargement et une utilisation gratuite, ainsi qu'auprès des partenaires agréés de Zimbra.

Le client Web ZCS est une suite de collaboration complète qui prend en charge la messagerie électronique et le calendrier de groupe à l'aide d'un outil d'interface Web Ajax qui active les conseils, les éléments déplaçables et les menus contextuels dans l'interface utilisateur. Comprend également des capacités de recherche avancées et des dates de relation. La création de documents en ligne, le mashup "Zimlet" et l'administration complète de l'interface utilisateur sont également inclus. Il est écrit à l'aide de la boîte à outils 'Zimbra Ajax.

Le serveur ZCS utilise plusieurs projets open source. Cela fera apparaître une interface de programmation d'application SOAP pour toutes les fonctions ainsi qu'un serveur IMAP et POP3. Le serveur fonctionne sur de nombreuses distributions Linux ainsi que sur Mac OS X.

Prérequis Pour L'installation De Zimbra Ubuntu
Serveur Ubuntu 20.04
Intel/AMD avec PassMark CPU Mark > 7 000 (par exemple, Dual Intel Xeon E5-2407 @ 2,2 GHz = 7 303)
RAM 8 Go minimale
Disque dur de 50 Go
DNS du serveur

TP
Renommer et mettre à jour la distribution
Je renomme ma machine xmail.sitka.local

```
root💀ubuntu:~# hostnamectl set-hostname xmail
```

Je mets à jour ma distribution

```
root💀xmail:~# apt update && apt upgrade
```

[Saut de retour à la ligne]Je modifie le fichier host

```
root💀xmail:~# vim /etc/hosts
```

Je rajoute le nom complet et le nom du serveur zimbra dans mon fichier hosts

```
172.20.0.70 xmail.sitka.local xmail
```

On supprime le fichier resolv.com car c'est un lien symbolique et en créé un autre du même nom

```
root💀xmail:/etc# vim resolv.conf
```

On remplit notre fichier resolv.conf comme indiqué ci-dessous

```
nameserver 172.20.0.14
nameserver 8.8.8.8
search sitka.local
~
```

Sur notre Dns on crée deux enregistrements :

Un enregistrement hôte (A) et un enregistrement MX

xmail	Hôte (A)	172.20.0.52	statique
xmail	Serveur de messagerie (MX)	[10] xmail.sitka.local.	statique

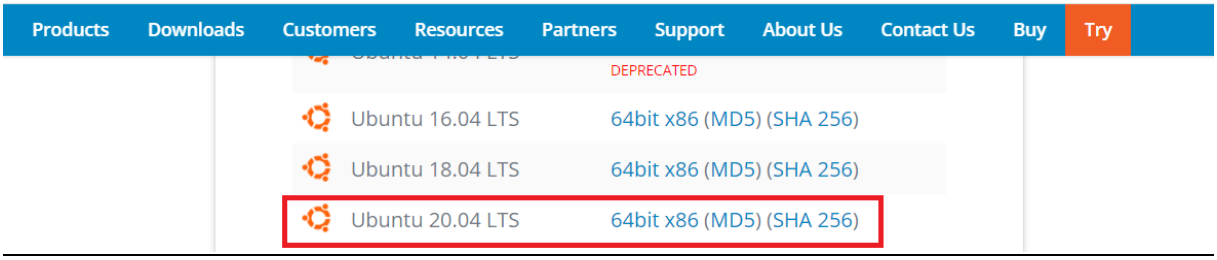
On fait un test de résolution dns

```
root@xmail:/etc# nslookup xmail.sitka.com
Server:         172.20.0.14
Address:        172.20.0.14#53

Name:   xmail.sitka.com
Address: 172.20.0.52
```

Je fais aussi un nslookup sur www.google.fr car dans le cas ou la résolution Dns ne fonctionne pas on ne peut pas télécharger zimbra avec la commande wget

```
root@xmail:~# nslookup www.google.com
Server:         172.20.0.14
Address:        172.20.0.14#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.75.228
Name:   www.google.com
Address: 2a00:1450:4007:808::2004
```

On se rend sur cette adresse pour télécharger zimbra
https://www.zimbra.com/downloads/zimbra-collaboration-open-source/
https://www.zimbra.com/downloads/zimbra-collaboration-open-source/



On utilise la commande wget et le lien qu'on récupérer sur le site de zimbra pour télécharger zimbra

```
#wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
root@xmail:~# wget https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
--2022-03-03 20:19:29--  https://files.zimbra.com/downloads/8.8.15_GA/zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
Resolving files.zimbra.com (files.zimbra.com)... 13.225.21.10
Connecting to files.zimbra.com (files.zimbra.com)|13.225.21.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 246927695 (235M) [application/x-tar]
Saving to: 'zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz'

zcs-8.8.15_GA_4179.UBUNTU20_64. 100%[=================================================>] 235,49M  3,35MB/s    in 58s

2022-03-03 20:20:28 (4,04 MB/s) - 'zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz' saved [246927695/246927695]
```

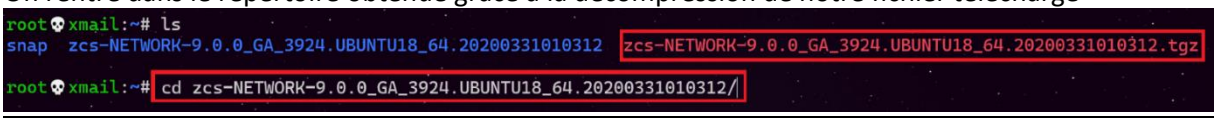
On vérifie que le fichier pour installer zimbra est téléchargé
y

```
root@xmail:~# ls
snap  zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
```

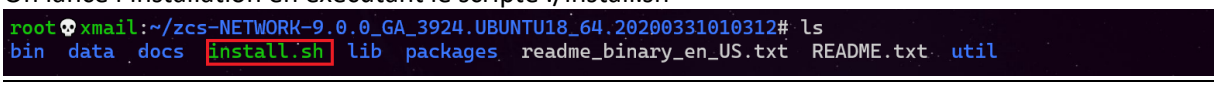
On décompresse notre fichier avec la commande tar

```
root@xmail:~# tar xzfv zcs-8.8.15_GA_4179.UBUNTU20_64.20211118033954.tgz
```


On rentre dans le répertoire obtenue grâce à la décompression de notre fichier téléchargé



On lance l'installation en exécutant le scripte ./install.sh



Une fois l'installantion lancée je fais les choix ci-dessous marquées en rouge
Do you agree with the terms of the software license agreement? [N] **Y**
Use Zimbra's package repository [Y] **Y**
Select the packages to install
Install zimbra-ldap [Y] **Y**
Install zimbra-logger [Y] **Y**
Install zimbra-mta [Y] **Y**
Install zimbra-dnscache [Y] **N**
Install zimbra-snmp [Y] **Y**
Install zimbra-store [Y] **Y**
Install zimbra-apache [Y] **Y**
Install zimbra-spell [Y] **Y**
Install zimbra-memcached [Y] **Y**
Install zimbra-proxy [Y] **Y**
Install zimbra-drive [Y] **Y**
Install zimbra-imapd (BETA - for evaluation only) [N] **N**
Install zimbra-chat [Y] **Y**
Checking required space for zimbra-core
Checking space for zimbra-store
Checking required packages for zimbra-store
zimbra-store package check complete.

Installing:
- zimbra-core
- zimbra-ldap
- zimbra-logger
- zimbra-mta
- zimbra-snmp
- zimbra-store
- zimbra-apache
- zimbra-spell
- zimbra-memcached
- zimbra-proxy
- zimbra-drive
- zimbra-patch
- zimbra-mta-patch
- zimbra-proxy-patch
- zimbra-chat

The system will be modified. Continue? [N] **Y**

Address unconfigured (**) items (? - help) **6**

Select, or 'r' for previous menu [r] **4**
Password for admin@xmail.sitka.local (min 6 characters): [PXu6A0HJH] zimbra
Select, or 'r' for previous menu [r] **r**
*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) **a**
Save configuration data to a file? [Yes] **Y**
Save config in file: [/opt/zimbra/config.17047] je clique sur la touche *entrée*
Saving config in /opt/zimbra/config.17047...done.
The system will be modified - continue? [No] **Y**

Notify Zimbra of your installation? [Yes] **N**
Configuration complete - press return to exit On appuyer sur **entree**

Une fois l'installation finie je vérifie l'état de mes services s'ils sont tous démarrées donc je me connecte tout d'abord avec le compte zimbra

```
root💀xmail:~# su zimbra
```

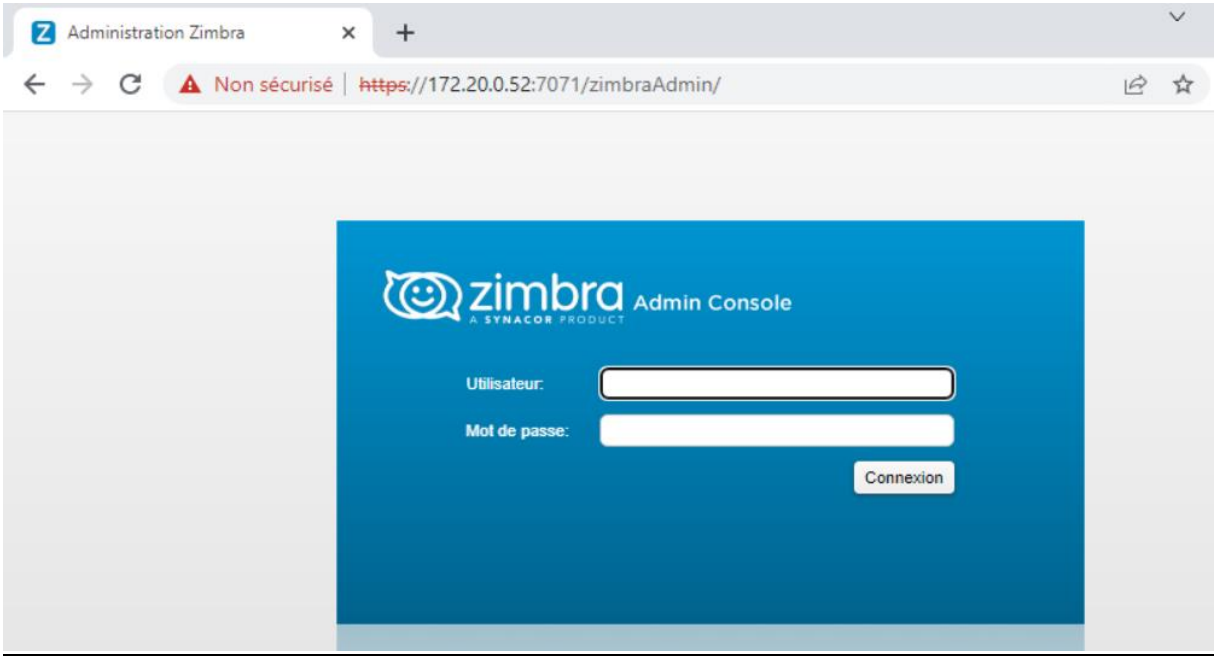
Après on tape la commande ci-dessus

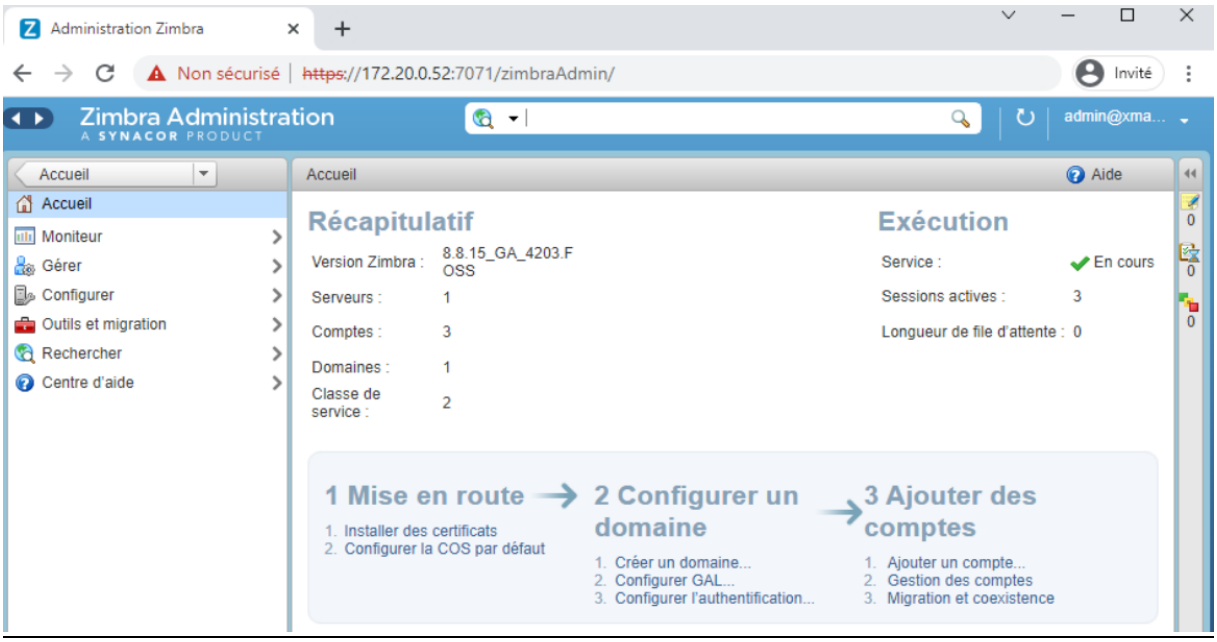
```
zimbra@xmail:/root$ zmcontrol status
Host xmail.sitka.local
        amavis                  Running
        antispam                Running
        antivirus               Running
        ldap                    Running
        logger                  Running
        mailbox                 Running
        memcached               Running
        mta                     Running
        opendkim                Running
        proxy                   Running
        service webapp          Running
        snmp                    Running
        spell                   Running
        stats                   Running
        zimbra webapp           Running
        zimbraAdmin webapp      Running
        zimlet webapp           Running
        zmconfigd               Running
```

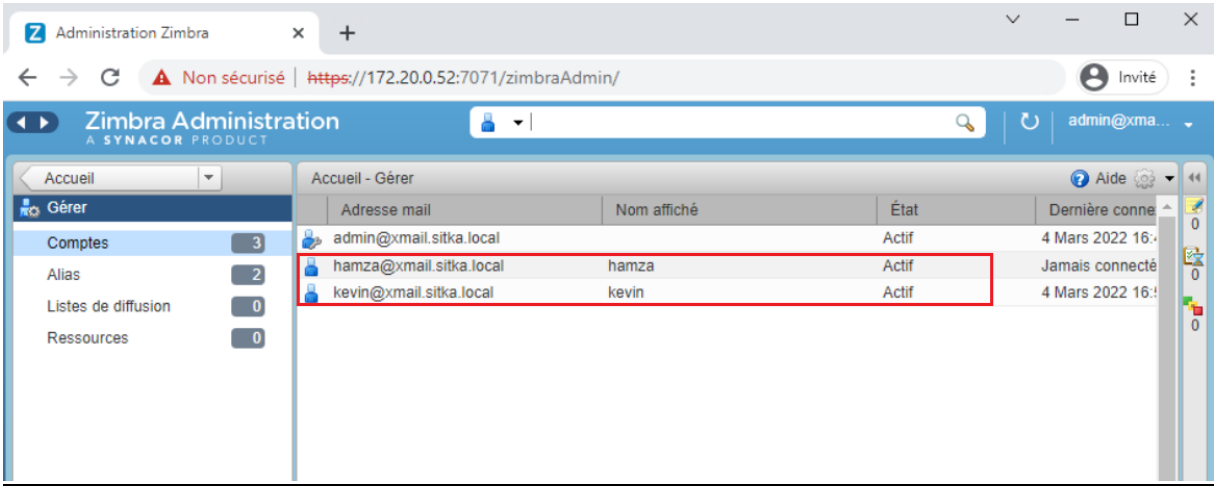
Dans le cas ou un service n'est pas redémarré on tape la commande ci-dessus

```
zimbra@xmail:/root$ zmcontrol restart
```

Maintenant on va accéder à l'interface d'administration de notre serveur de messagerie zimbra
En tapant :
https://172.20.0.52:7071
login :admin
Mot de passe zimbra

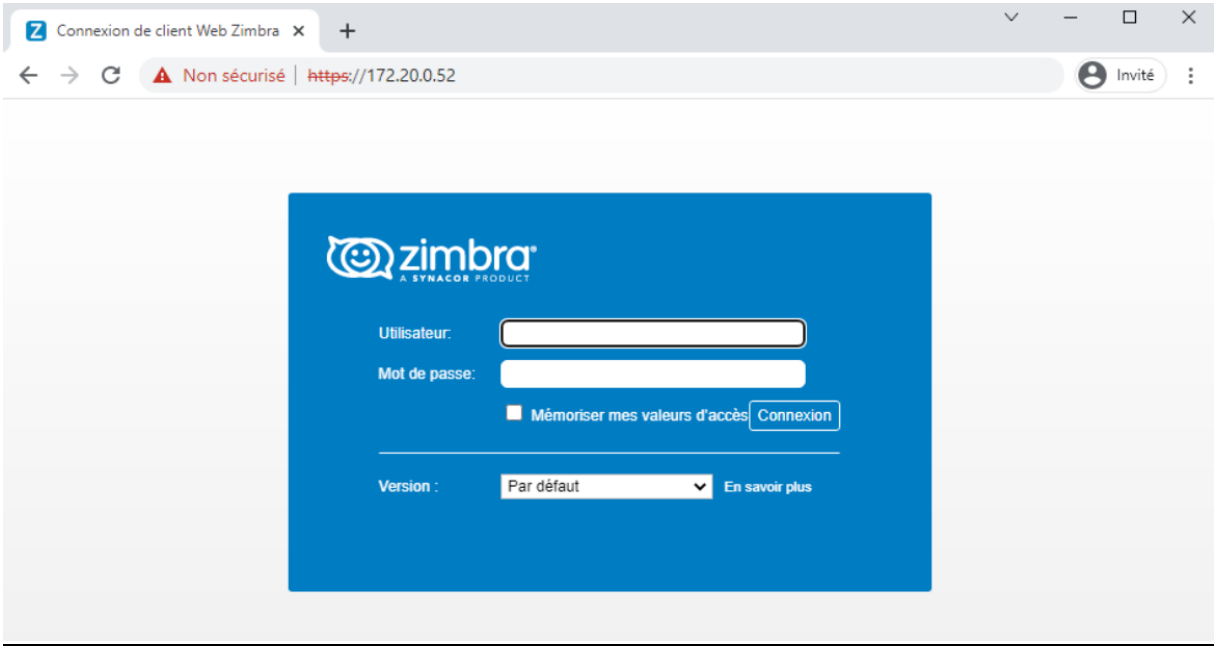

Administration Zimbra
Non sécurisé | https://172.20.0.52:7071/zimbraAdmin/
zimbra Admin Console
A SYNACOR PRODUCT
Utilisateur:
Mot de passe:
Connexion

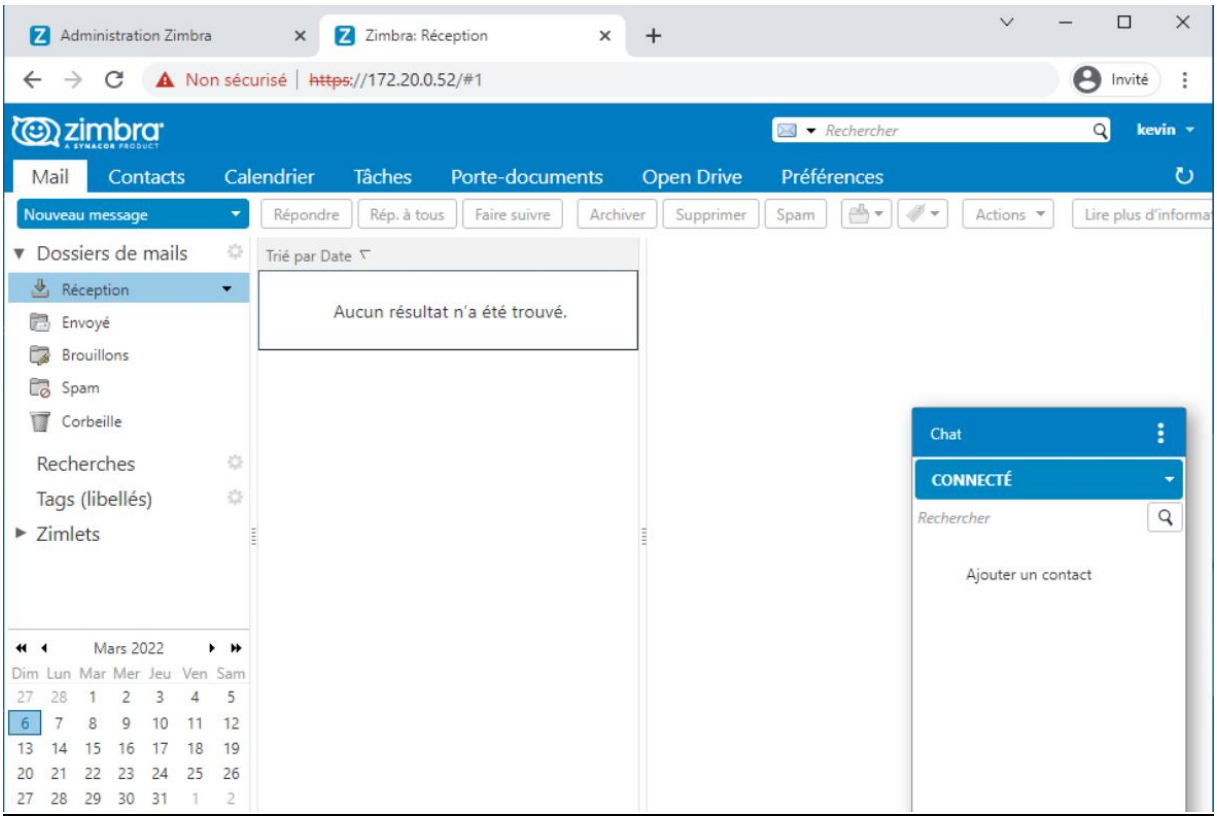

Administration Zimbra
Non sécurisé | https://172.20.0.52:7071/zimbraAdmin/
Invité
Zimbra Administration
A SYNACOR PRODUCT
admin@xma...
Accueil
Aide
Accueil
Moniteur
Gérer
Configurer
Outils et migration
Rechercher
Centre d'aide
Récapitulatif
Version Zimbra : 8.8.15_GA_4203.F OSS
Serveurs : 1
Comptes : 3
Domaines : 1
Classe de service : 2
Exécution
Service : En cours
Sessions actives : 3
Longueur de file d'attente : 0
1 Mise en route
1. Installer des certificats
2. Configurer la COS par défaut
2 Configurer un domaine
1. Créer un domaine...
2. Configurer GAL...
3. Configurer l'authentification...
3 Ajouter des comptes
1. Ajouter un compte...
2. Gestion des comptes
3. Migration et coexistence

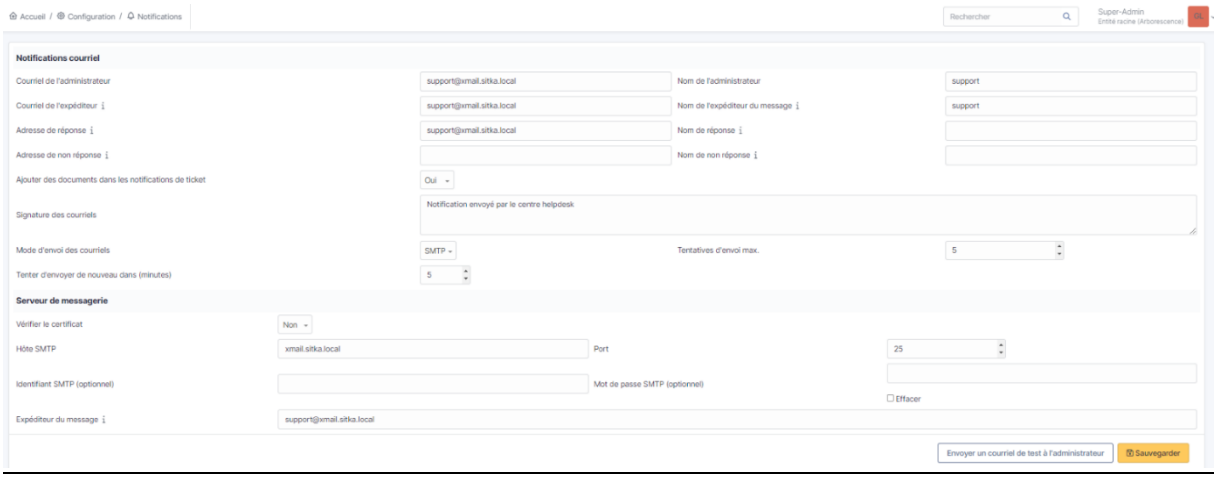


On peut créer deux utilisateur à partir du menu gérer et se connecter avec ces deux comptes et s'envoyer des mail entre eux pour tester le bon fonctionnement de zimbra
Pour se connectert sur le client zimbra il faut taper :

https://172.20.0.52:8443
Login : nom d'utilisateur crée
Mot de passe : mot de passe choisit à la création de l'utilisateur



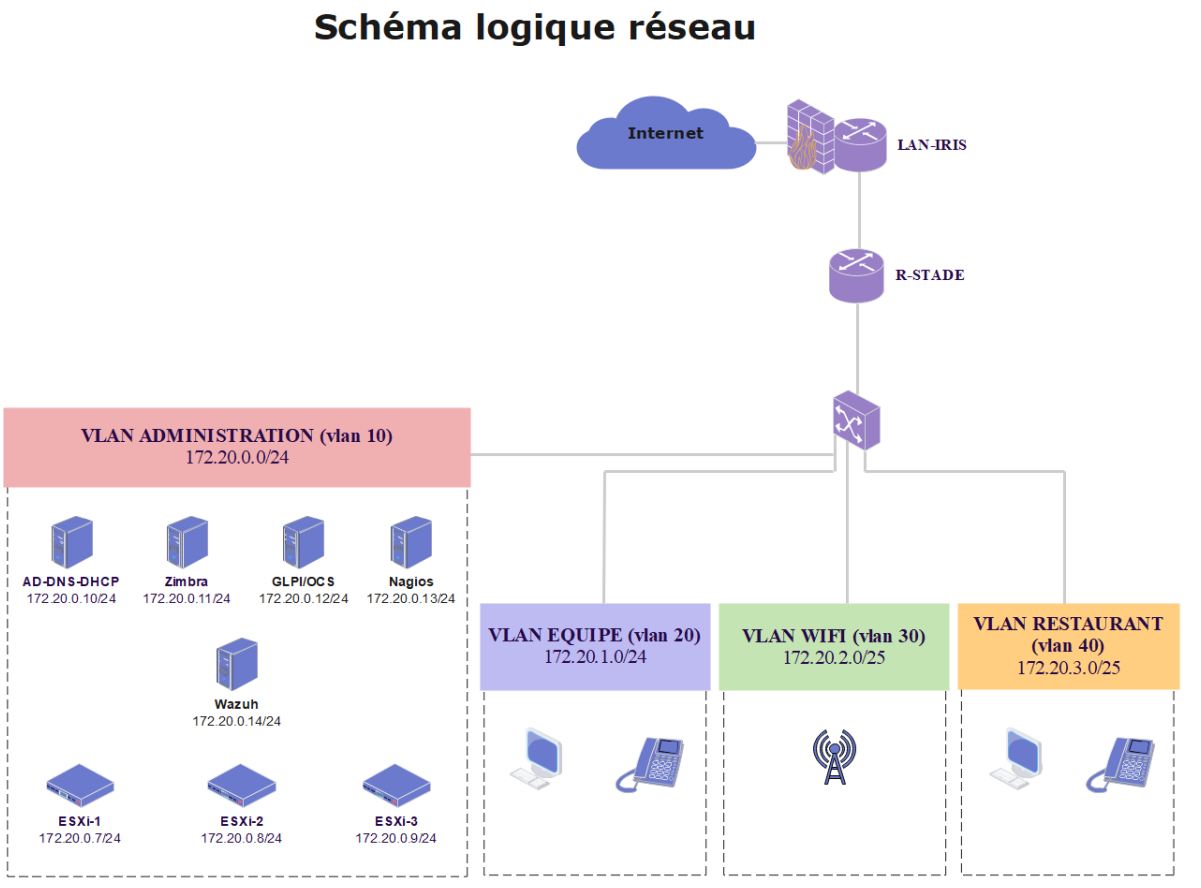

Administration Zimbra
Zimbra: Réception
Non sécurisé | https://172.20.0.52/#1
Invité
zimbra
Rechercher
kevin
Mail
Contacts
Calendrier
Tâches
Porte-documents
Open Drive
Préférences
Nouveau message
Répondre
Rép. à tous
Faire suivre
Archiver
Supprimer
Spam
Actions
Dossiers de mails
Réception
Envoyé
Brouillons
Spam
Corbeille
Recherches
Tags (libellés)
Zimlets
Trié par Date
Aucun résultat n'a été trouvé.
Mars 2022
Dim Lun Mar Mer Jeu Ven Sam
Chat
CONNECTÉ
Rechercher
Ajouter un contact

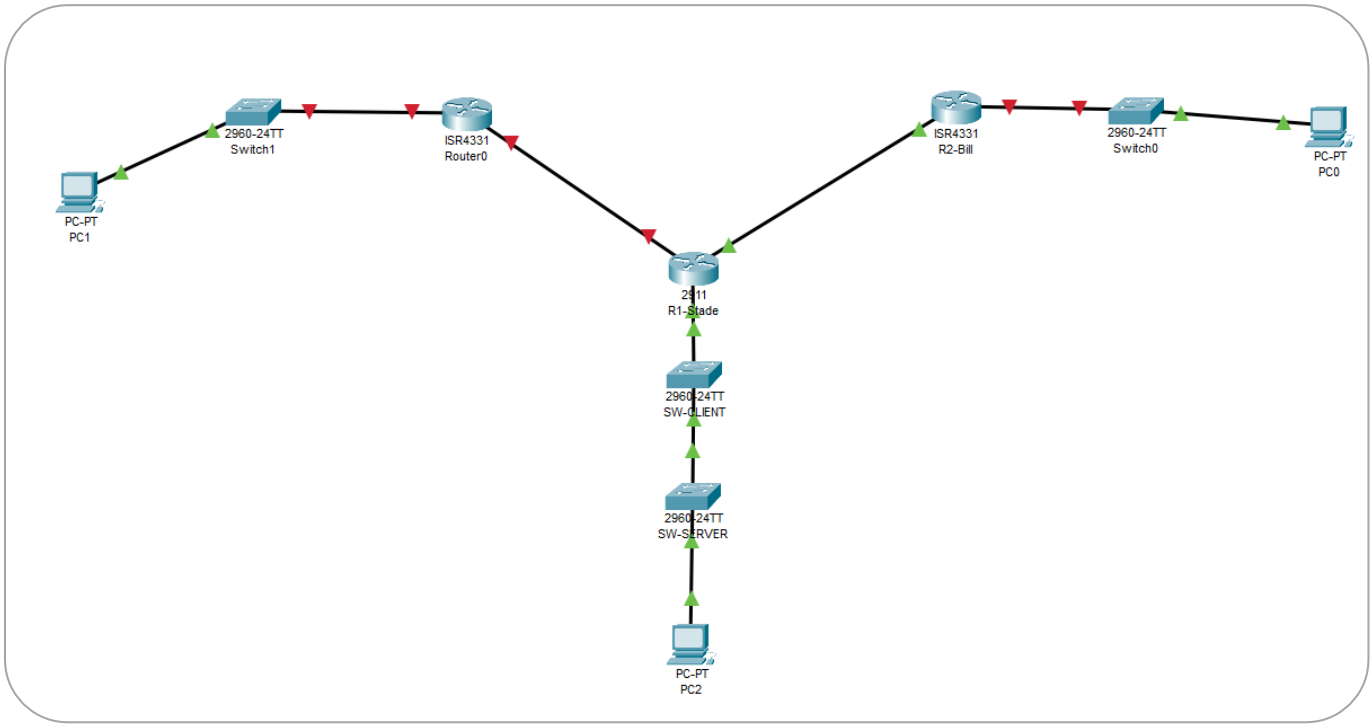

Notifications courriel
Courriel de l'administrateur
support@xmail.sitka.local
Nom de l'administrateur
support
Courriel de l'expéditeur
Nom de l'expéditeur du message
Adresse de réponse
Nom de réponse
Adresse de non réponse
Nom de non réponse
Ajouter des documents dans les notifications de ticket
Oui
Signature des courriels
Notification envoyé par le centre helpdesk
Mode d'envoi des courriels
SMTP
Tentatives d'envoi max.
Tenter d'envoyer de nouveau dans (minutes)
Serveur de messagerie
Vérifier le certificat
Non
Hôte SMTP
xmail.sitka.local
Port
25
Identifiant SMTP (optionnel)
Mot de passe SMTP (optionnel)
Effacer
Expéditeur du message
Envoyer un courriel de test à l'administrateur
Sauvegarder


(root💀xmail)-[~]
telnet xmail.sitka.local 25
Trying 172.20.0.70...
Connected to xmail.sitka.local.
Escape character is '^]'.
220 xmail.sitka.local ESMTP Postfix
helo xmail.sitka.local
250 xmail.sitka.local
mail from:<support@xmail.sitka.local>
250 2.1.0 Ok
rcpt to:<admin@xmail.sitka.local>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject : test envoi mail par telnet
Ceci est une test
.
250 2.0.0 Ok: queued as AA7051213EC
quit
221 2.0.0 Bye
Connection closed by foreign host.

Annexe

1) Schéma logique réseau






```
Device Name: SW-SERVER
Custom Device Model: 2960 IOS15
Hostname: SW-SERVER

Port                 Link   VLAN   IP Address         MAC Address
FastEthernet0/1      Down   10     --                 00D0.BAAC.1D01
FastEthernet0/2      Down   10     --                 00D0.BAAC.1D02
FastEthernet0/3      Down   10     --                 00D0.BAAC.1D03
FastEthernet0/4      Down   10     --                 00D0.BAAC.1D04
FastEthernet0/5      Down   10     --                 00D0.BAAC.1D05
FastEthernet0/6      Down   10     --                 00D0.BAAC.1D06
FastEthernet0/7      Down   20     --                 00D0.BAAC.1D07
FastEthernet0/8      Down   20     --                 00D0.BAAC.1D08
FastEthernet0/9      Down   20     --                 00D0.BAAC.1D09
FastEthernet0/10     Down   20     --                 00D0.BAAC.1D0A
FastEthernet0/11     Down   20     --                 00D0.BAAC.1D0B
FastEthernet0/12     Down   20     --                 00D0.BAAC.1D0C
FastEthernet0/13     Down   30     --                 00D0.BAAC.1D0D
FastEthernet0/14     Down   30     --                 00D0.BAAC.1D0E
FastEthernet0/15     Down   1      --                 00D0.BAAC.1D0F
FastEthernet0/16     Down   1      --                 00D0.BAAC.1D10
FastEthernet0/17     Down   1      --                 00D0.BAAC.1D11
FastEthernet0/18     Down   1      --                 00D0.BAAC.1D12
FastEthernet0/19     Down   1      --                 00D0.BAAC.1D13
FastEthernet0/20     Down   1      --                 00D0.BAAC.1D14
FastEthernet0/21     Down   1      --                 00D0.BAAC.1D15
FastEthernet0/22     Down   --     --                 00D0.BAAC.1D16
FastEthernet0/23     Down   --     --                 00D0.BAAC.1D17
FastEthernet0/24     Up     --     --                 00D0.BAAC.1D18
GigabitEthernet0/1   Up     1      --                 00D0.BAAC.1D19
GigabitEthernet0/2   Down   1      --                 00D0.BAAC.1D1A
Vlan1                Down   1      <not set>          0030.F2A0.A573

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > SW-SERVER
```


```
Device Name: SW-CLIENT
Custom Device Model: 2960 IOS15
Hostname: SW-CLIENT

Port                 Link   VLAN   IP Address          MAC Address
FastEthernet0/1      Down   10     --                  000A.F359.0401
FastEthernet0/2      Down   10     --                  000A.F359.0402
FastEthernet0/3      Down   10     --                  000A.F359.0403
FastEthernet0/4      Down   10     --                  000A.F359.0404
FastEthernet0/5      Down   10     --                  000A.F359.0405
FastEthernet0/6      Down   10     --                  000A.F359.0406
FastEthernet0/7      Down   20     --                  000A.F359.0407
FastEthernet0/8      Down   20     --                  000A.F359.0408
FastEthernet0/9      Down   20     --                  000A.F359.0409
FastEthernet0/10     Down   20     --                  000A.F359.040A
FastEthernet0/11     Down   20     --                  000A.F359.040B
FastEthernet0/12     Down   20     --                  000A.F359.040C
FastEthernet0/13     Down   30     --                  000A.F359.040D
FastEthernet0/14     Down   30     --                  000A.F359.040E
FastEthernet0/15     Down   1      --                  000A.F359.040F
FastEthernet0/16     Down   1      --                  000A.F359.0410
FastEthernet0/17     Down   1      --                  000A.F359.0411
FastEthernet0/18     Down   1      --                  000A.F359.0412
FastEthernet0/19     Down   1      --                  000A.F359.0413
FastEthernet0/20     Down   1      --                  000A.F359.0414
FastEthernet0/21     Down   1      --                  000A.F359.0415
FastEthernet0/22     Down   --     --                  000A.F359.0416
FastEthernet0/23     Down   --     --                  000A.F359.0417
FastEthernet0/24     Up     --     --                  000A.F359.0418
GigabitEthernet0/1   Up     1      --                  000A.F359.0419
GigabitEthernet0/2   Down   1      --                  000A.F359.041A
Vlan1                Down   1      <not set>           00E0.B0BC.E0CC

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > SW-CLIENT
```

```
Device Name: R1-Stade
Device Model: 2911
Hostname: R1-Stade

Port                 Link   VLAN   IP Address          IPv6 Address                              MAC Address
GigabitEthernet0/0   Up     --     <not set>           <not set>                                 0001.97A0.ED01
GigabitEthernet0/0.10 Up    --     172.20.0.1/24       <not set>                                 0001.97A0.ED01
GigabitEthernet0/0.20 Up    --     172.20.1.1/24       <not set>                                 0001.97A0.ED01
GigabitEthernet0/0.30 Up    --     172.20.2.1/25       <not set>                                 0001.97A0.ED01
GigabitEthernet0/1   Up     --     200.200.200.1/30    <not set>                                 0001.97A0.ED02
GigabitEthernet0/2   Down   --     <not set>           <not set>                                 0001.97A0.ED03
Vlan1                Down   1      <not set>           <not set>                                 0090.2120.0559

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > R1-Stade
```

```
Device Name: R2-Bill
Device Model: ISR4331
Hostname: R2-Bill

Port                 Link   VLAN   IP Address          IPv6 Address                              MAC Address
GigabitEthernet0/0/0 Down   --     <not set>           <not set>                                 000B.BEB1.4C01
GigabitEthernet0/0/1 Up     --     200.200.200.2/30    <not set>                                 000B.BEB1.4C02
GigabitEthernet0/0/2 Down   --     <not set>           <not set>                                 000B.BEB1.4C03
Vlan1                Down   1      <not set>           <not set>                                 0060.70B5.AC76

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > R2-Bill
```


2) Running-configuration du routeur R-Stade

```
de#sh run
ilding configuration...

Current configuration : 3115 bytes
!
version 12.4
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption
!
hostname R-Stade
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
```

```
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.20.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 glbp 10 ip 172.20.0.2
 glbp 10 priority 110
 glbp 10 preempt
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.20.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 glbp 20 ip 172.20.1.2
 glbp 20 priority 110
 glbp 20 preempt
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.20.3.1 255.255.255.128
 ip nat inside
 ip virtual-reassembly
lbp 30 ip 172.20.3.2
p 30 priority 110
```


rface FastEthernet0/0.40
ncapsulation dot1Q 40
ip address 172.20.3.129 255.255.255.192
ip nat inside
ip virtual-reassembly
glbp 40 ip 172.20.3.130
glbp 40 priority 110
glbp 40 preempt
!
interface FastEthernet0/0.50
encapsulation dot1Q 50
ip address 172.20.3.193 255.255.255.224
ip nat inside
ip virtual-reassembly
glbp 50 ip 172.20.3.194
glbp 50 priority 110
glbp 50 preempt
!
interface FastEthernet0/0.100
encapsulation dot1Q 100
ip address 172.20.2.1 255.255.255.128
ip nat inside
ip virtual-reassembly
glbp 100 ip 172.20.2.2
glbp 100 priority 110
glbp 100 preempt
!
interface FastEthernet0/0.200
encapsulation dot1Q 200
ip address 172.20.2.129 255.255.255.128
ip nat inside
ip virtual-reassembly
--More--
ip virtual-reassembly
glbp 100 ip 172.20.2.2
glbp 100 priority 110
glbp 100 preempt
!
interface FastEthernet0/0.200
encapsulation dot1Q 200
ip address 172.20.2.129 255.255.255.128
ip nat inside
ip virtual-reassembly
glbp 200 ip 172.20.2.130
glbp 200 priority 110
glbp 200 preempt
!
interface FastEthernet0/1
ip address dhcp
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
!
ip forward-protocol nd
!
ip flow-export version 9
!
ip http server
ip http secure-server

```
 duplex auto
 speed auto
!
!
ip forward-protocol nd
!
ip flow-export version 9
!
no ip http server
no ip http secure-server
ip nat inside source list 10 interface FastEthernet0/1 overload
ip nat inside source list 20 interface FastEthernet0/1 overload
ip nat inside source list 30 interface FastEthernet0/1 overload
ip nat inside source list 40 interface FastEthernet0/1 overload
ip nat inside source list 50 interface FastEthernet0/1 overload
ip nat inside source list 98 interface FastEthernet0/1 overload
ip nat inside source list 99 interface FastEthernet0/1 overload
!
access-list 10 permit 172.20.0.0 0.0.0.255
access-list 20 permit 172.20.1.0 0.0.0.255
access-list 30 permit 172.20.3.0 0.0.0.127
access-list 40 permit 172.20.3.128 0.0.0.63
access-list 50 permit 172.20.3.192 0.0.0.63
access-list 98 permit 172.20.2.0 0.0.0.127
access-list 99 permit 172.20.2.128 0.0.0.127
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
--More--
```

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.20.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 glbp 10 ip 172.20.0.3
 glbp 10 priority 90
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.20.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 glbp 20 ip 172.20.1.3
 glbp 20 priority 90
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.20.3.1 255.255.255.128
 ip nat inside
 ip virtual-reassembly
 glbp 30 ip 172.20.3.3
 glbp 30 priority 90
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.20.3.129 255.255.255.192
 ip nat inside
 ip virtual-reassembly
 glbp 40 ip 172.20.3.130
 glbp 40 priority 90
```


```
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 10 interface FastEthernet0/1 overload
ip nat inside source list 20 interface FastEthernet0/1 overload
ip nat inside source list 30 interface FastEthernet0/1 overload
ip nat inside source list 40 interface FastEthernet0/1 overload
ip nat inside source list 50 interface FastEthernet0/1 overload
ip nat inside source list 98 interface FastEthernet0/1 overload
ip nat inside source list 99 interface FastEthernet0/1 overload
!
access-list 10 permit 172.20.0.0 0.0.0.255
access-list 20 permit 172.20.1.0 0.0.0.255
access-list 30 permit 172.20.3.0 0.0.0.127
access-list 40 permit 172.20.3.128 0.0.0.63
access-list 50 permit 172.20.3.192 0.0.0.63
access-list 98 permit 172.20.2.0 0.0.0.127
access-list 99 permit 172.20.2.128 0.0.0.127
no cdp log mismatch duplex
!
!
!
control-plane
```

```
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 172.20.3.193 255.255.255.224
 ip nat inside
 ip virtual-reassembly
 glbp 50 ip 172.20.3.195
 glbp 50 priority 90
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.20.2.1 255.255.255.128
 ip nat inside
 ip virtual-reassembly
 glbp 100 ip 172.20.2.3
 glbp 100 priority 90
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 ip address 172.20.2.129 255.255.255.128
 ip nat inside
 ip virtual-reassembly
 glbp 200 ip 172.20.2.131
 glbp 200 priority 90
!
interface FastEthernet0/0.1000
!
interface FastEthernet0/1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
```


3) Running-configuration du Switch

```
Switch#sh run
Building configuration...

Current configuration : 2002 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
spanning-tree mode pvst
spanning-tree vlan 10,20,30,40,50,100,200 priority 24576
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 --More-- |
```

```
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
```


```
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/14
```

```
!
interface FastEthernet0/14
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet0/19
 switchport mode trunk
!
interface FastEthernet0/20
```


4) Running-configuration des switchs

```
Switch#
Switch#sh run
Building configuration...

Current configuration : 2593 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 10
 channel-group 1 mode auto
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 channel-group 1 mode auto
 switchport mode access
```

```
interface FastEthernet0/3
 switchport access vlan 10
 channel-group 1 mode auto
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 channel-group 1 mode auto
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 channel-group 1 mode auto
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 channel-group 2 mode auto
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 channel-group 2 mode auto
 switchport mode access
```


```
interface FastEthernet0/8
 switchport access vlan 20
 channel-group 2 mode auto
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 channel-group 3 mode auto
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 30
 channel-group 3 mode auto
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 40
 channel-group 4 mode auto
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 40
 channel-group 4 mode auto
 switchport mode access
```

```
interface FastEthernet0/13
 switchport access vlan 50
 channel-group 5 mode auto
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 50
 channel-group 5 mode auto
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 100
 channel-group 6 mode auto
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 100
 channel-group 6 mode auto
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 200
 channel-group 1 mode auto
 switchport mode access
```