



# Rapport de projet

Mise en place d'une infrastructure réseau et de services pour l'entreprise SIO-Formations

NERON DE AZEVEDO Aloïs – SIO 2



# Table des matières

- Objectifs du projet
- Planning prévisionnel du projet
- Planning réel
- Description des étapes du projet
  - Étape 1 : pfSense
  - Étape 2 : AD DNS + portail captif
  - Étape 3 : Courrier électronique (hmailserver), partage Next cloud
  - Étape 4 : Supervision avec Zabbix
  - Étape 5 : Borne Wifi
  - Étape 6 : Hébergement cloud des serveurs (AD, Zabbix et NextCloud)
  - Étape 7 : Rédaction du rapport
- Références



# Objectifs du projet

Le projet consiste à mettre en place une infrastructure informatique pour SIO-Formations, une entreprise spécialisée dans les formations en informatique. L'objectif est de proposer des salles de cours connectées (filaire et Wi-Fi) où chaque participant utilise son propre ordinateur.

L'infrastructure inclura :

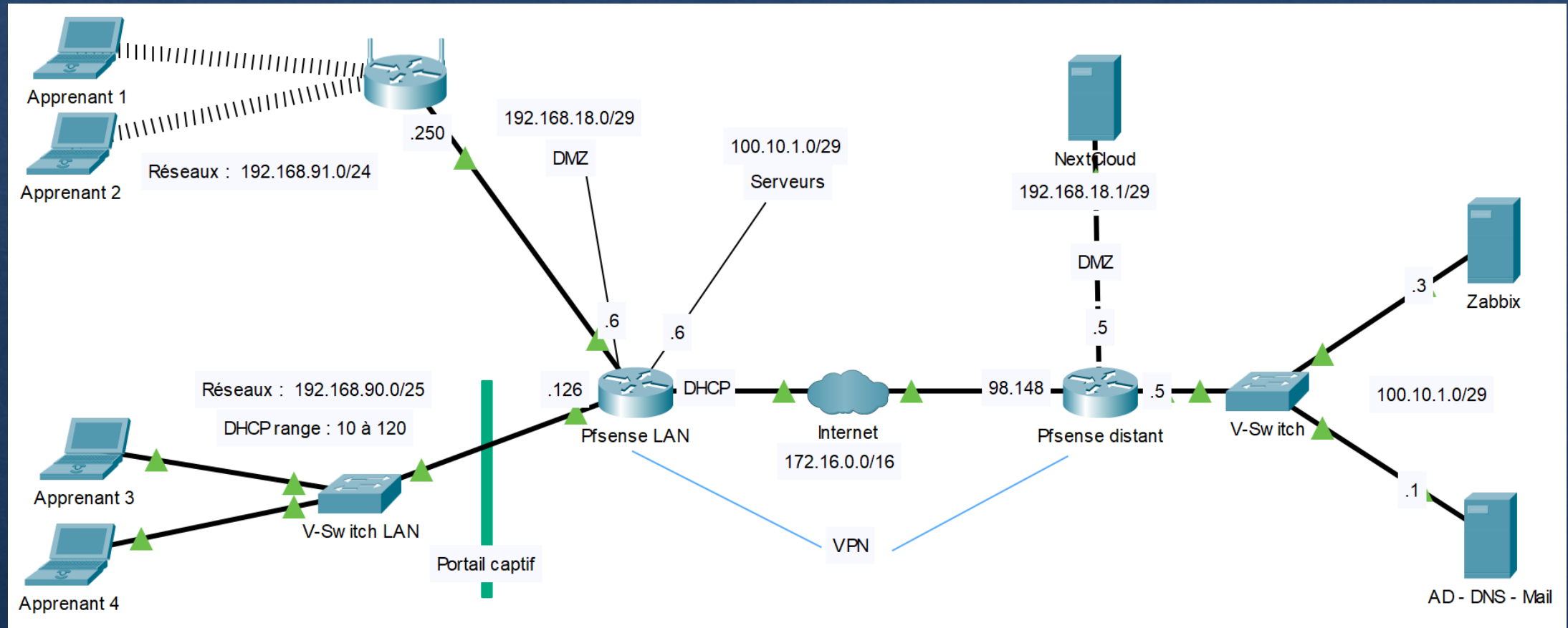
Un serveur web en DMZ pour afficher les formations à venir et recueillir les travaux des apprenants.

Un service de messagerie électronique pour les communications.

Un serveur Active Directory (AD) pour gérer l'authentification des utilisateurs.

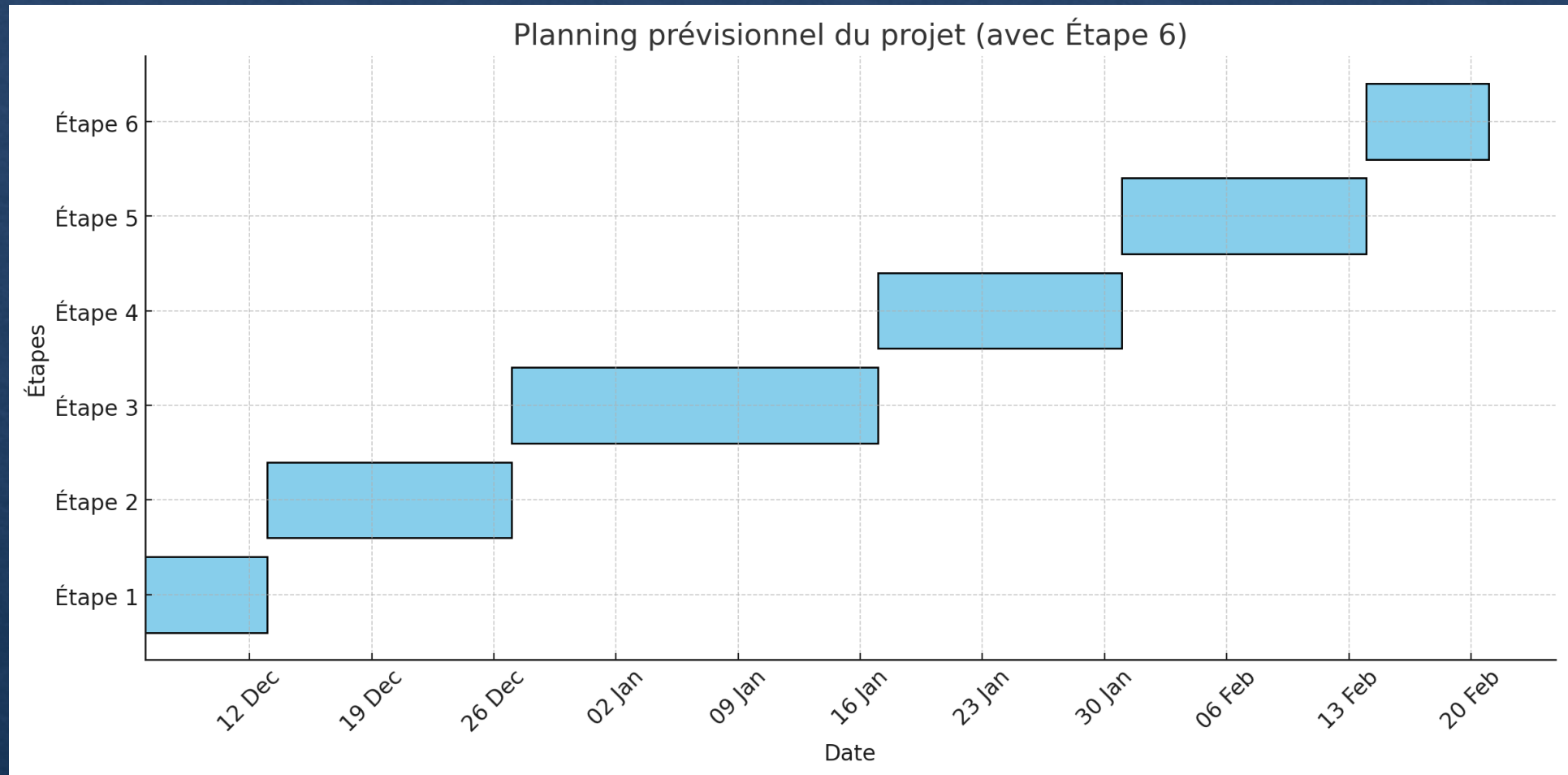
Un système de supervision Zabbix pour assurer le suivi et la maintenance de l'infrastructure.

# Objectif final





# Planning prévisionnel



# Planning réel

Etape 1 : 6 Décembre

Etape 2 : 6 Décembre – 15 Décembre

Etape 3 : 15 Décembre – 3 Janvier

Etape 4 : 9 - 10 Janvier

Etape 5 : 16 Janvier

Etape 6 : 30 janvier

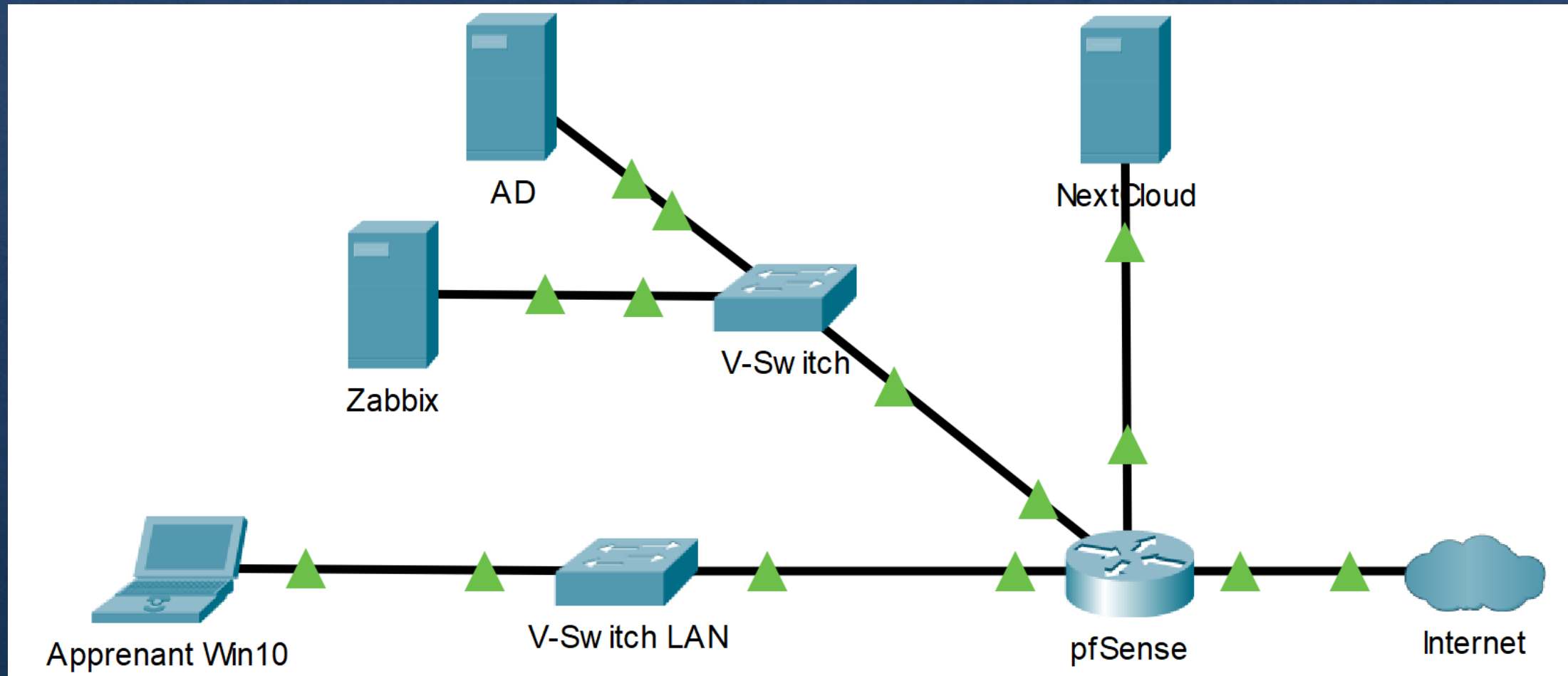
Etape 7 : 6 Décembre 2024 – 7 février 2025



# Etape 1 – pfSense







# Etape 1 – Architecture réseau



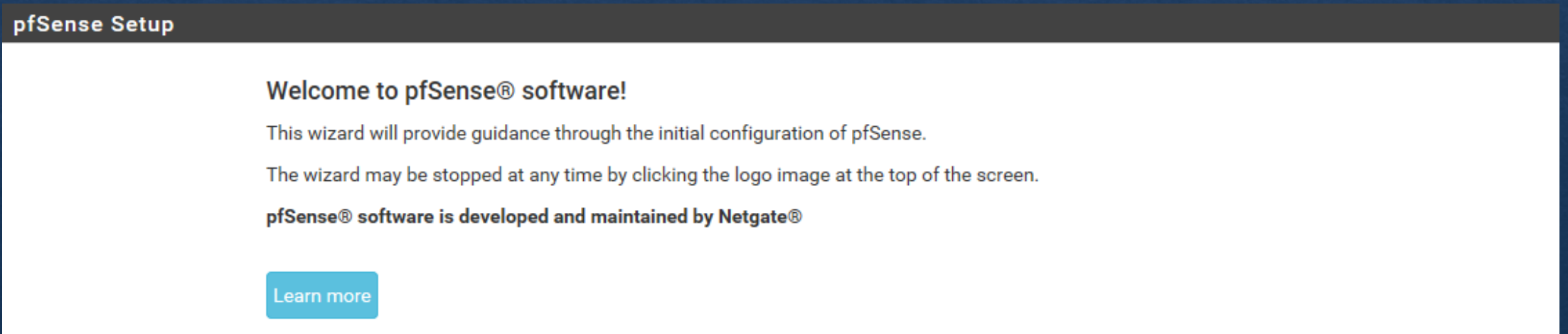


# Etape 1 – Mise en place

 Network Adapter	Bridged (Automatic)
 Network Adapter 2	LAN Segment SIO - LAN
 Network Adapter 3	LAN Segment SIO - DMZ
 Network Adapter 4	LAN Segment SIO - Serveurs

Au niveau de la configuration de la VM, je vais rajouter les différents LAN qui seront nécessaires pour la suite du projet.

Ensuite, direction l'interface Web pour continuer la configuration du routeur.



# Etape 1 – Mise en place

Il faut activer les nouvelles interfaces ainsi que leurs affecter une adresse IP.

Enfin il ne faut pas oublier de rajouter une règle par défaut dans le FW sur nos deux nouvelles interfaces afin de laisser passer le trafic.

```
WAN (wan)      -> em0      -> v4/DHCP4: 172.16.5.86/16
LAN (lan)      -> em1      -> v4: 192.168.98.126/25
DMZ (opt1)     -> em2      -> v4: 192.168.18.6/29
SERVEURS (opt2) -> em3      -> v4: 100.10.1.6/29
```

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓	0/0 B	IPv4 *	*	*	*	*	none		règle par défaut pour laisser passer le trafic



# Etape 1 – Tests

```
root@Zabbix-Server:~# ping 100.10.1.6
PING 100.10.1.6 (100.10.1.6) 56(84) bytes of data.
64 bytes from 100.10.1.6: icmp_seq=1 ttl=64 time=0.371 ms
64 bytes from 100.10.1.6: icmp_seq=2 ttl=64 time=0.371 ms
64 bytes from 100.10.1.6: icmp_seq=3 ttl=64 time=0.496 ms
```

Serveur Zabbix vers routeur

```
C:\Users\Administrateur>ping 100.10.1.6
```

```
Envoi d'une requête 'Ping' 100.10.1.6 avec 32 octets de données :
Réponse de 100.10.1.6 : octets=32 temps<1ms TTL=64
Réponse de 100.10.1.6 : octets=32 temps<1ms TTL=64
Réponse de 100.10.1.6 : octets=32 temps<1ms TTL=64
Réponse de 100.10.1.6 : octets=32 temps<1ms TTL=64
```

Serveur Windows2022 vers routeur

```
root@Nextcloud-Server:~# ping 192.168.18.6
PING 192.168.18.6 (192.168.18.6) 56(84) bytes of data.
64 bytes from 192.168.18.6: icmp_seq=1 ttl=64 time=0.741 ms
64 bytes from 192.168.18.6: icmp_seq=2 ttl=64 time=0.456 ms
64 bytes from 192.168.18.6: icmp_seq=3 ttl=64 time=0.299 ms
```

Serveur NextCloud vers routeur

Chacun ping sa passerelle sans soucis, l'apprenant n'est pas mentionné car il a fait la configuration sur l'interface web donc il ping forcément.

# Etape 2 – AD/DNS + portail captif pfSense

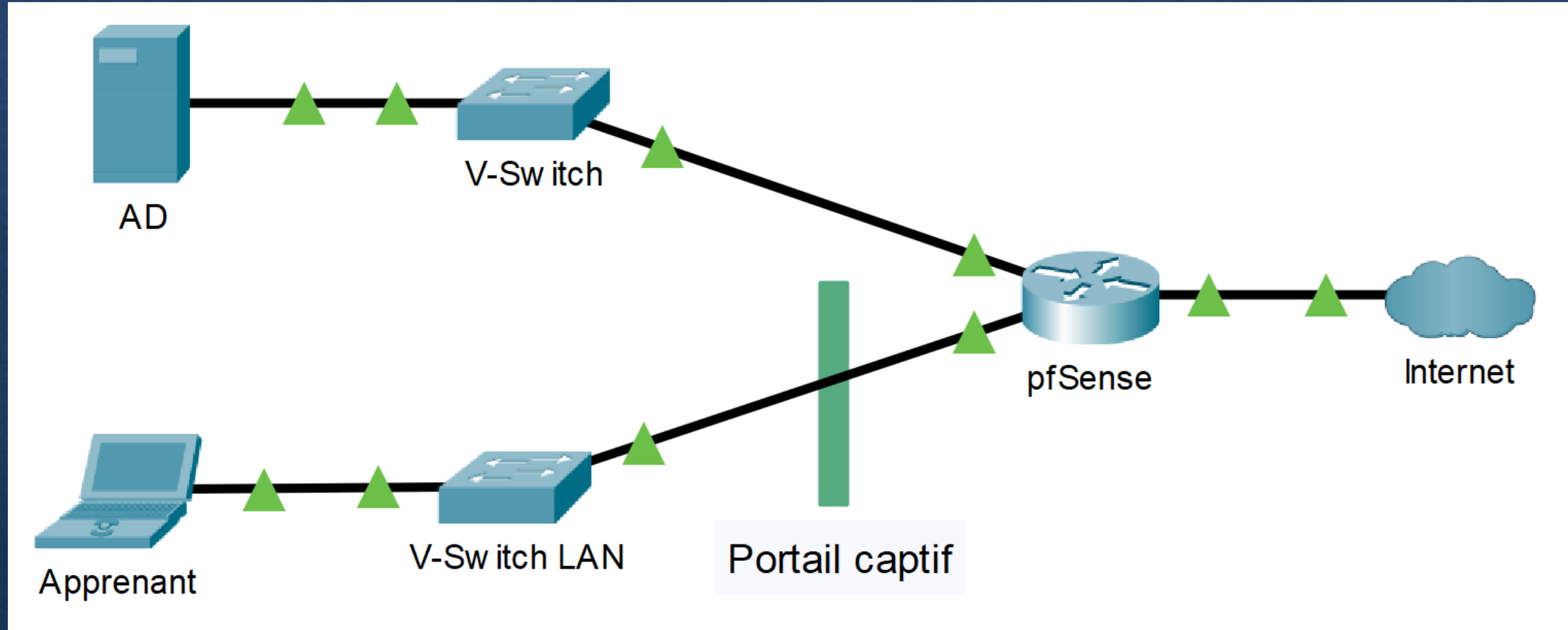


Windows Server





# Etape 2 – Architecture réseau



# Etape 2 – Mise en place

Sur le Windows serveur, on commence par changer son nom généré automatiquement par quelque chose d'identifiable.

Mettre une IP fixe est aussi nécessaire mais cela a déjà été fait pour la réalisation de l'étape 1.

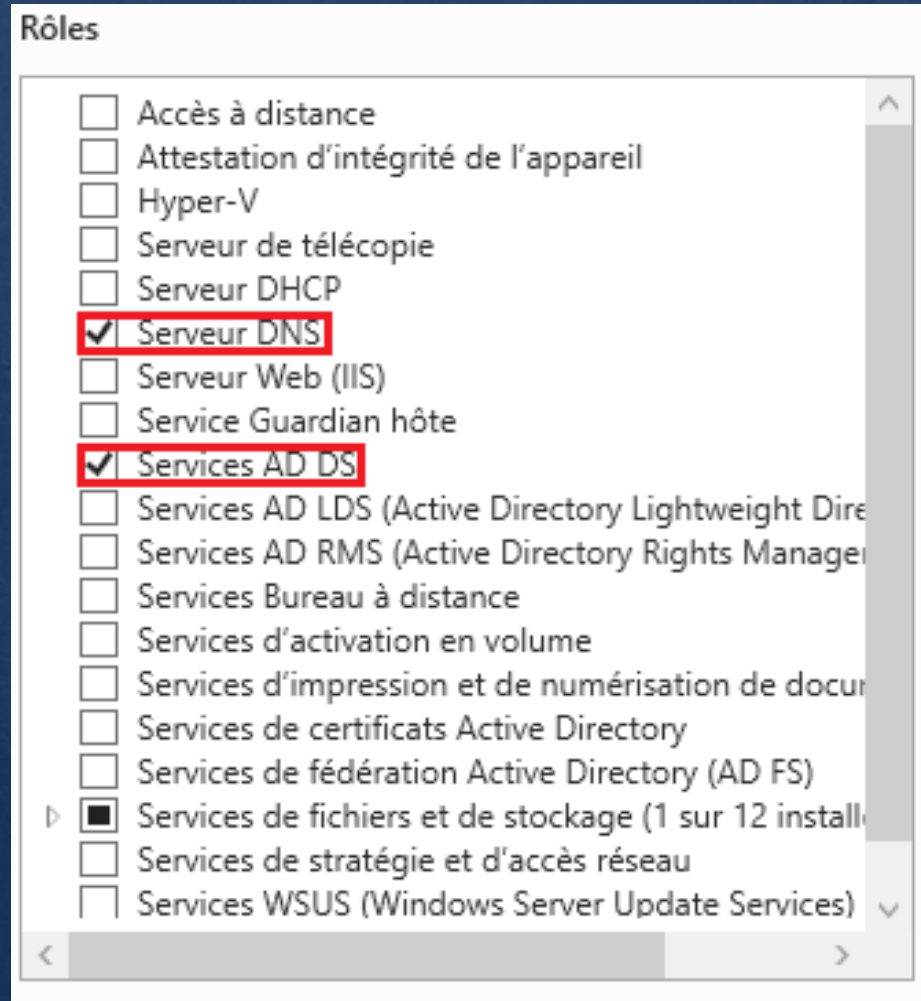
100 . 10 . 1 . 2
255 . 255 . 255 . 248
100 . 10 . 1 . 6

Nom complet de  
l'ordinateur :

AD-SIO-A



# Etape 2 – Mise en place



On commence par installer les services AD et DNS pour transformer ce serveur en contrôleur de domaine.

# Etape 2 – Mise en place

Configuration de déploiement

SERVEUR CIBLE  
AD-SIO-A

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

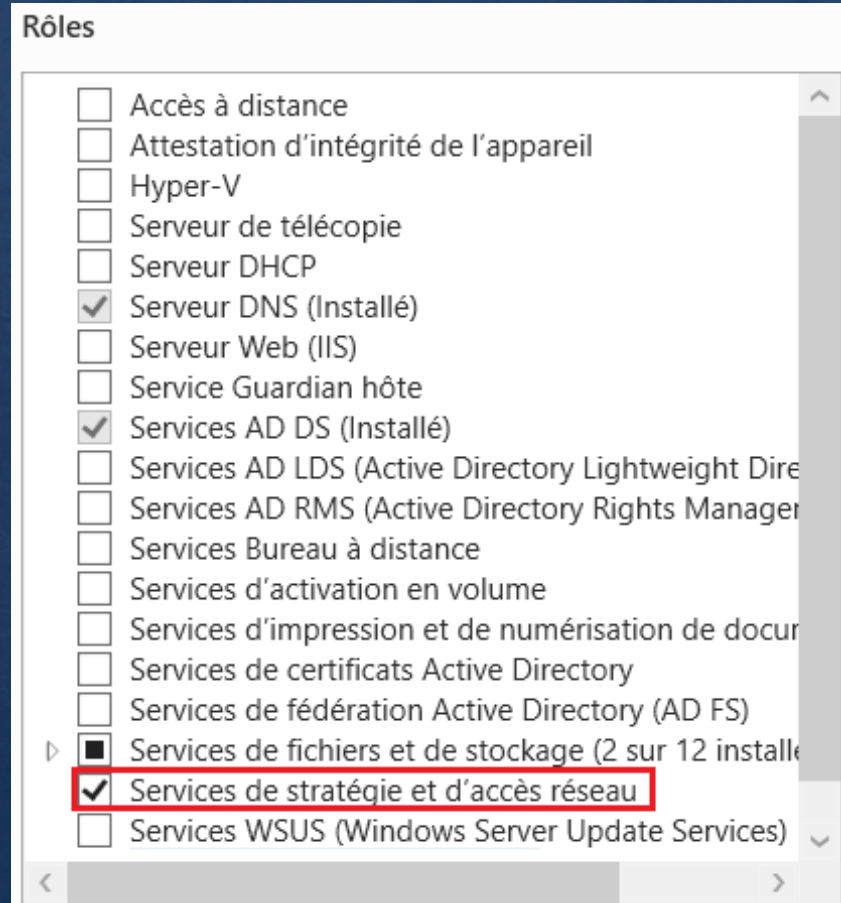
Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

On ajoute une nouvelle forêt ainsi qu'un nom de domaine.



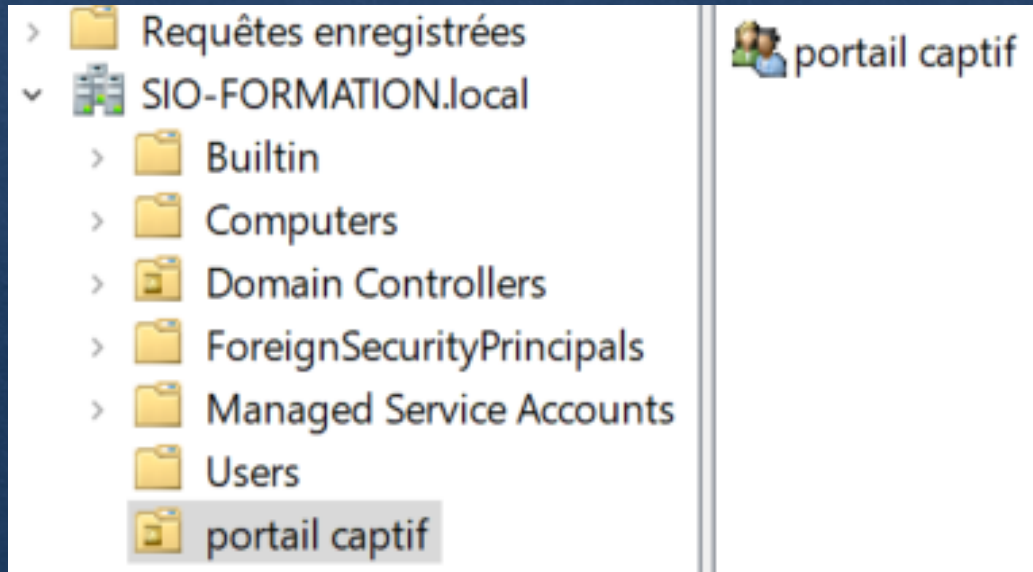
# Etape 2 – Mise en place






Pour mettre en place le portail captif sur pfSense et permettre aux utilisateurs de Windows de s'authentifier avec leurs propres comptes, il faut mettre en place RADIUS sur le serveur.

Pour se faire, on installe le service de stratégie et d'accès réseau.

# Etape 2 – Mise en place

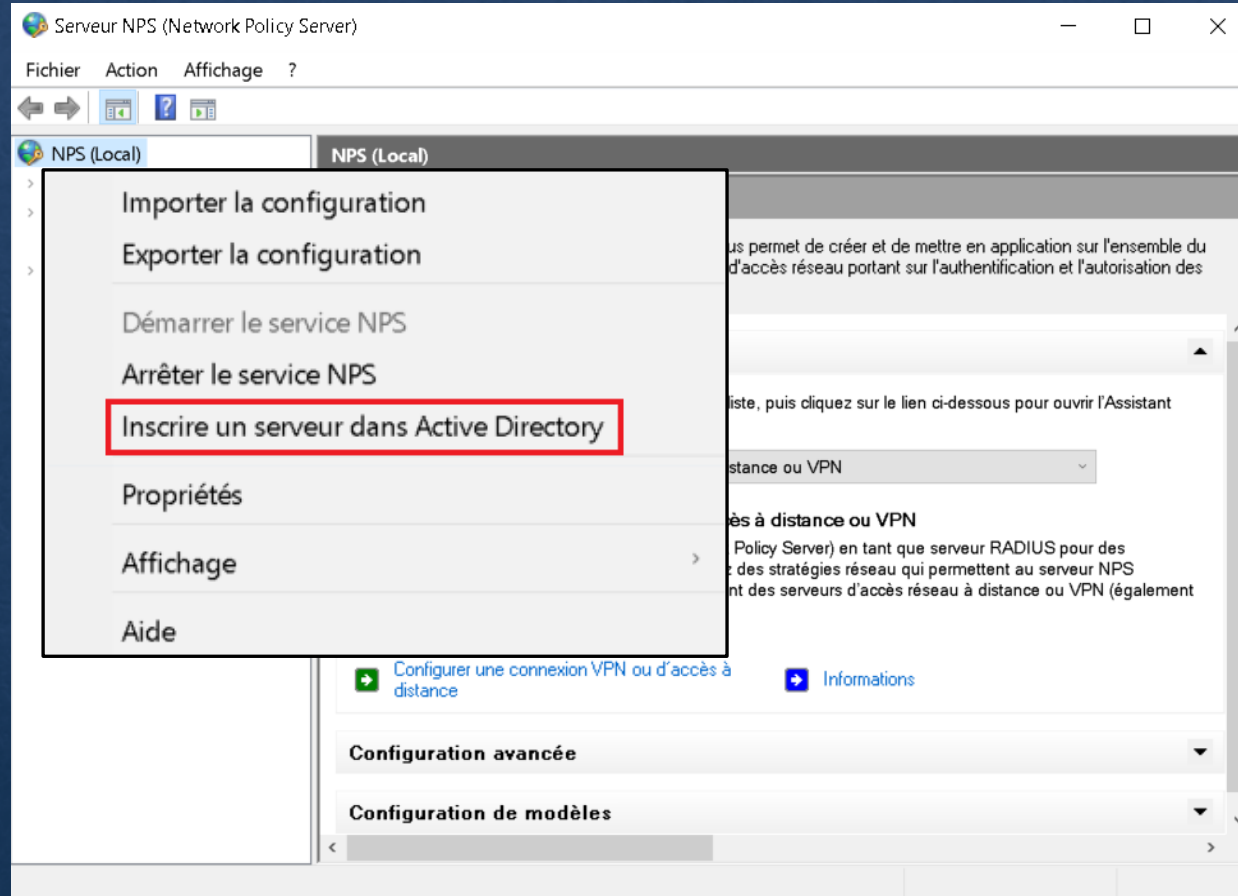


Pour réaliser les tests qui suivront, j'ai besoin de créer des utilisateurs. Pour une question d'organisation, j'ai créé une OU dédiée avec un groupe qui contient tous les utilisateurs du LAN et donc du portail captif.

Nom	Dossier Services de domaine Active Directory
 apprenant 001	SIO-FORMATION.local/Users
 Jean Loup	SIO-FORMATION.local/Users
 user1	SIO-FORMATION.local/Users



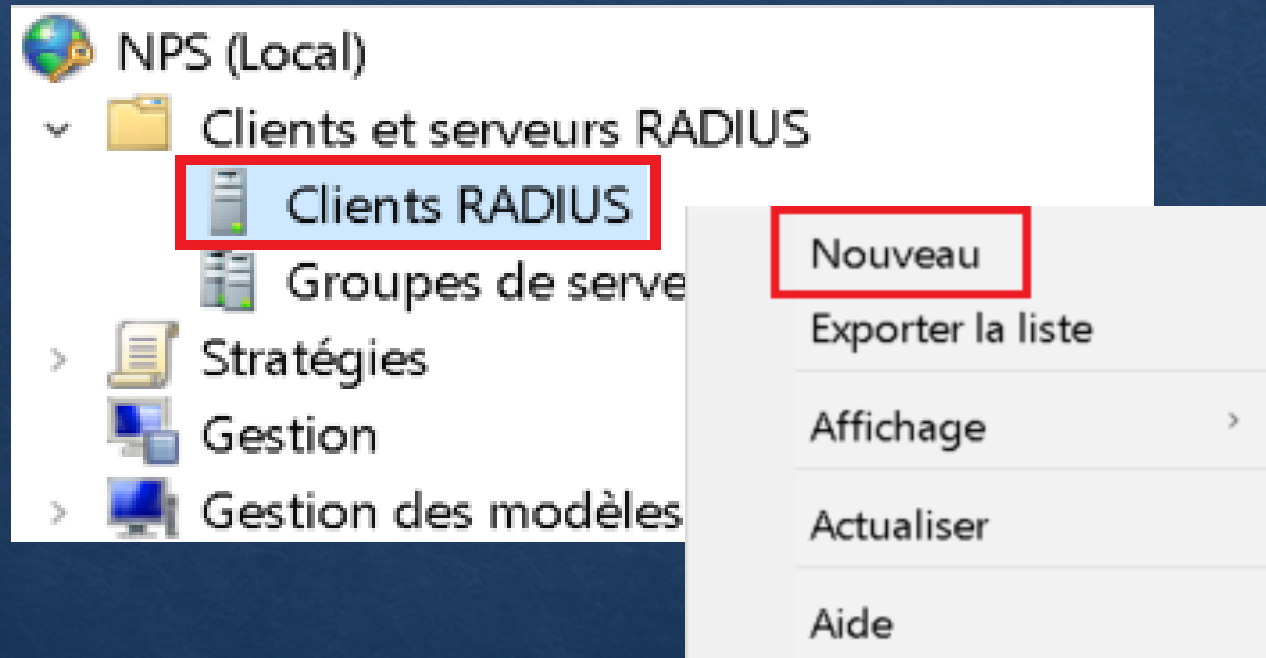
# Etape 2 – Mise en place



Dans l'outil d'administration « **serveur NPS** », clic droit sur « **NPS (local)** » puis « **inscrire un serveur dans Active directory** ».

Cela permet de créer un serveur RADIUS dans notre Windows serveur.

# Etape 2 – Mise en place



Maintenant que le serveur est créé, nous allons pouvoir configurer nos différents clients.

Clic droit sur « clients RADIUS » puis « nouveau ».



# Etape 2 – Mise en place

Propriétés de pfsense portail captif

Paramètres Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :  
pfsense portail captif

Adresse (IP ou DNS) :  
100.10.1.6 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :  
Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

☒ Manuel ☐ Générer

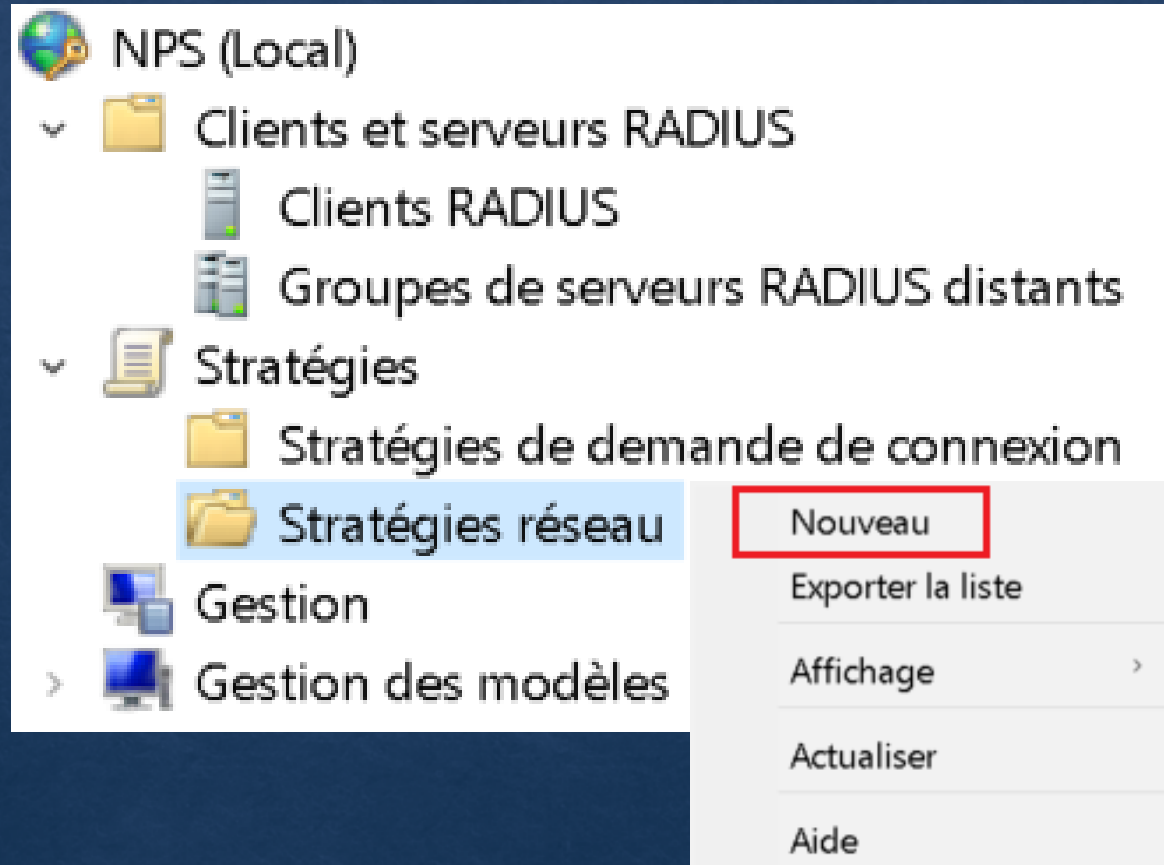
Secret partagé :  
••••

Confirmez le secret partagé :  
••••

OK Annuler Appliquer

On lui donne un nom identifiable avec l'IP du pfSense sur l'interface ou le serveur est relié.

# Etape 2 – Mise en place




On peut maintenant créer notre stratégie réseau.



# Etape 2 – Mise en place

Nouvelle stratégie réseau

 **Spécifier le nom de la stratégie réseau et le type de connexion**

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.


**Nom de la stratégie :**

pfsense portail captif

**Méthode de connexion réseau**


Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

Nouvelle stratégie réseau

 **Spécifier les conditions**

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

**Conditions :**

Condition	Valeur
 Groupes d'utilisateurs	SIO-FORMATION\portail captif

On y ajoute le groupe dédié au portail captif crée précédemment en lui accordant les droits d'accès.

## ☒ Accès accordé

Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

# Etape 2 – Mise en place

Nouvelle stratégie réseau

## Configurer des contraintes

Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.

Configurez les contraintes de cette stratégie réseau.  
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

- Contraintes
- Délai d'inactivité**
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion

☒ Déconnecter au-delà de la durée d'inactivité maximale

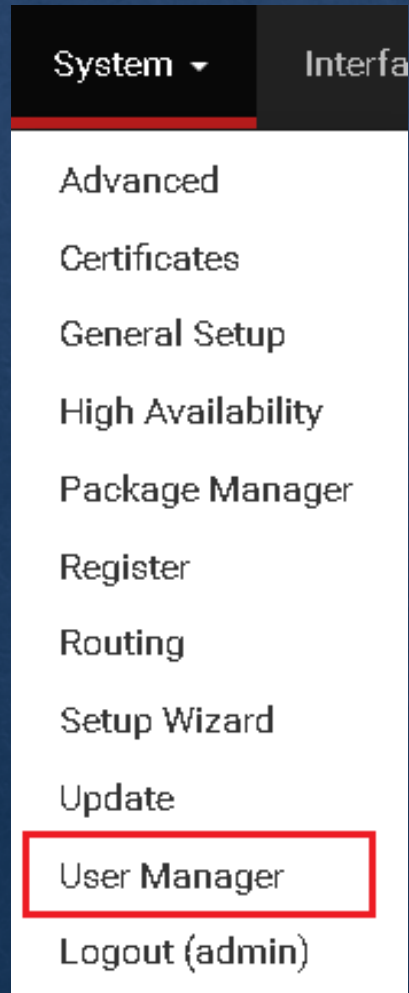
5

Précédent Suivant Terminer Annuler

Pas obligatoire mais pour des raisons pratiques je vais mettre en place une déconnexion automatique au bout de 5 minutes d'inactivités.






# Etape 2 – Mise en place



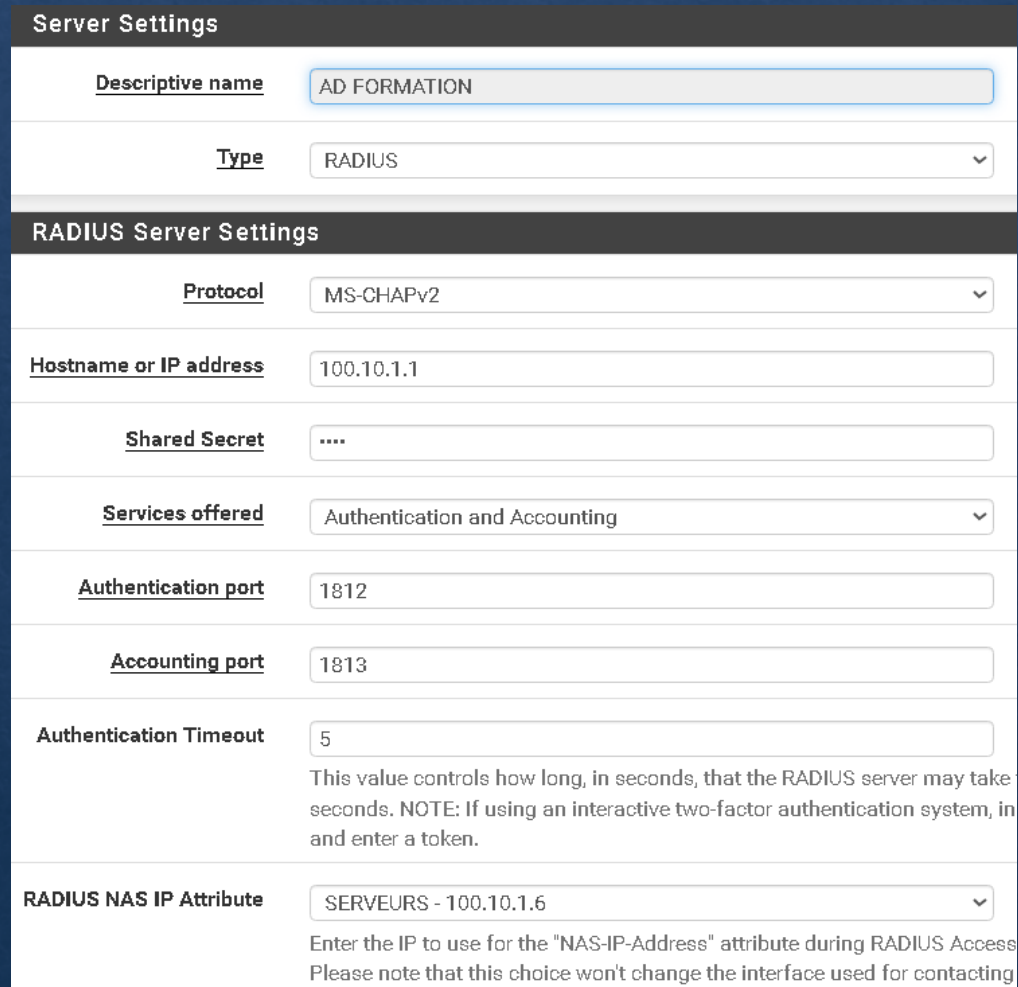
Une fois la configuration RADIUS sur le Windows serveur, nous passons à la configuration du routeur.

On commence par ajouter le serveur d'authentification (AD) dans la liste des serveurs de pfSense. Pour se faire, nous allons dans « system » puis « user manager ». Une fois dedans, il faut changer d'onglet et aller dans « authentication servers » et cliquer sur « +add ».

A screenshot of the 'Authentication Servers' configuration page in pfSense. The 'Authentication Servers' tab is selected and highlighted with a red box. Below the tab is a table listing the configured authentication servers.

Authentication Servers			
Server Name	Type	Host Name	Actions
AD FORMATION	RADIUS	100.10.1.1	  
Local Database		pfSense	

# Etape 2 – Mise en place



The screenshot shows the 'Server Settings' section of the pfSense configuration interface. It includes a 'Descriptive name' field set to 'AD FORMATION' and a 'Type' dropdown menu set to 'RADIUS'. Below this is the 'RADIUS Server Settings' section, which contains several fields: 'Protocol' (MS-CHAPv2), 'Hostname or IP address' (100.10.1.1), 'Shared Secret' (masked with four dots), 'Services offered' (Authentication and Accounting), 'Authentication port' (1812), 'Accounting port' (1813), 'Authentication Timeout' (5), and 'RADIUS NAS IP Attribute' (SERVEURS - 100.10.1.6). A note at the bottom explains that the NAS IP attribute is used for RADIUS Access and that this choice won't change the interface used for contacting the server.

Server Settings	
<b>Descriptive name</b>	AD FORMATION
<b>Type</b>	RADIUS
RADIUS Server Settings	
<b>Protocol</b>	MS-CHAPv2
<b>Hostname or IP address</b>	100.10.1.1
<b>Shared Secret</b>	....
<b>Services offered</b>	Authentication and Accounting
<b>Authentication port</b>	1812
<b>Accounting port</b>	1813
<b>Authentication Timeout</b>	5 <small>This value controls how long, in seconds, that the RADIUS server may take seconds. NOTE: If using an interactive two-factor authentication system, in and enter a token.</small>
<b>RADIUS NAS IP Attribute</b>	SERVEURS - 100.10.1.6 <small>Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access. Please note that this choice won't change the interface used for contacting</small>

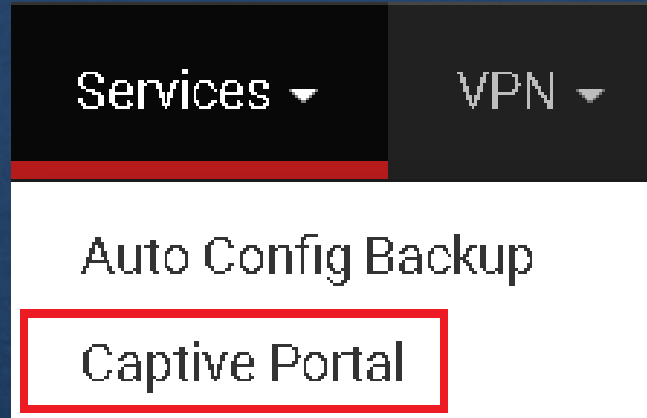
La configuration à mettre est assez simple, on y met le type de lien soit « RADIUS » dans notre cas.

On y met l'IP de l'AD avec un secret partager « shared secret » crée dans le client RADIUS précédemment.

Dans « RADIUS NAS IP Attribute », il faut mettre l'interface qui relie le pfSense à l'AD donc le segment SERVEURS.



# Etape 2 – Mise en place

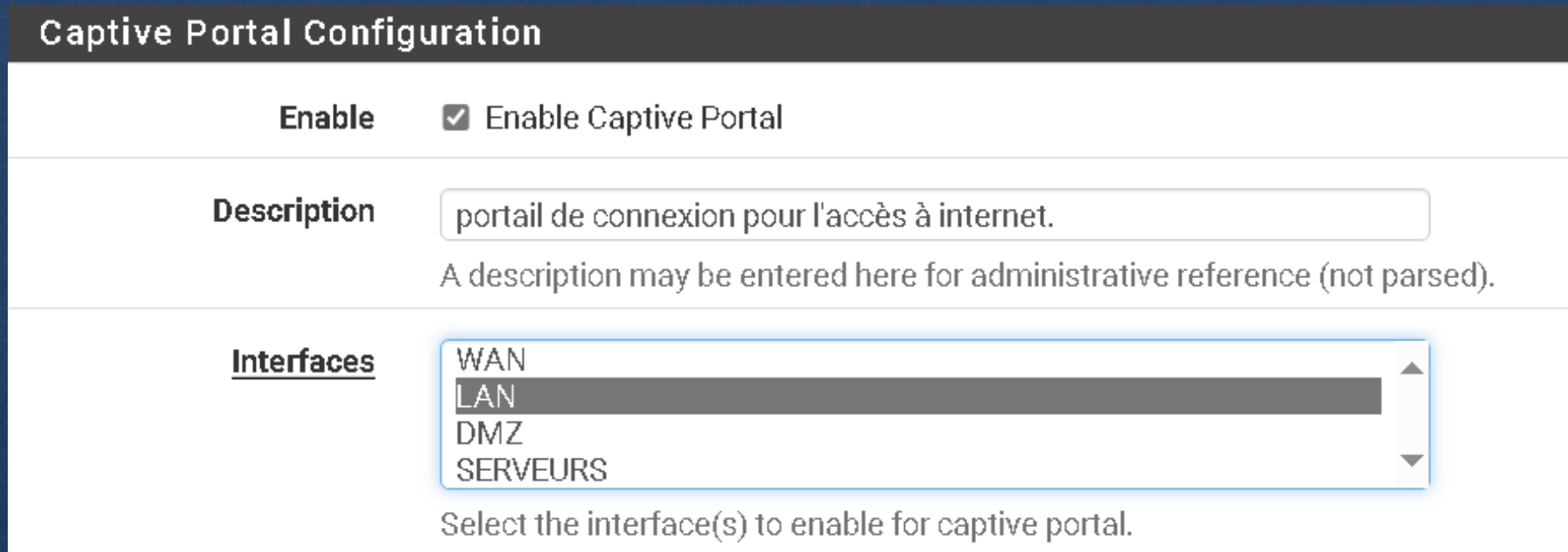


Notre serveur a été ajouté à notre pfSense, nous allons pouvoir passer à la mise en place du portail captif.

« **Services** » puis « **captive portal** » et « add »

Add Captive Portal Zone	
<u>Zone name</u>	<input type="text" value="portail_captif"/> <small>Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.</small>
<b>Zone description</b>	<input type="text" value="portail de connexion pour l'accès à internet."/> <small>A description may be entered here for administrative reference (not parsed).</small>

# Etape 2 – Mise en place



**Captive Portal Configuration**

**Enable** ☒ Enable Captive Portal

**Description**   
A description may be entered here for administrative reference (not parsed).

**Interfaces** WAN  
LAN  
DMZ  
SERVEURS

Select the interface(s) to enable for captive portal.

On active le portail captif et on définit l'interface sur laquelle le portail va intervenir. Dans notre cas, ce sera le LAN.



# Etape 2 – Mise en place

**Authentication**

Authentication Method

Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server

AD FORMATION

Local Database

You can add a remote authentication server in the [User Manager](#).  
Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

On définit la méthode d'authentification et on sélectionne le serveur concerné.

# Etape 2 – Tests

Pour savoir si la liaison entre le client et le serveur RADIUS fonctionne, nous allons dans l'onglet « diagnostics » puis « authentication ».

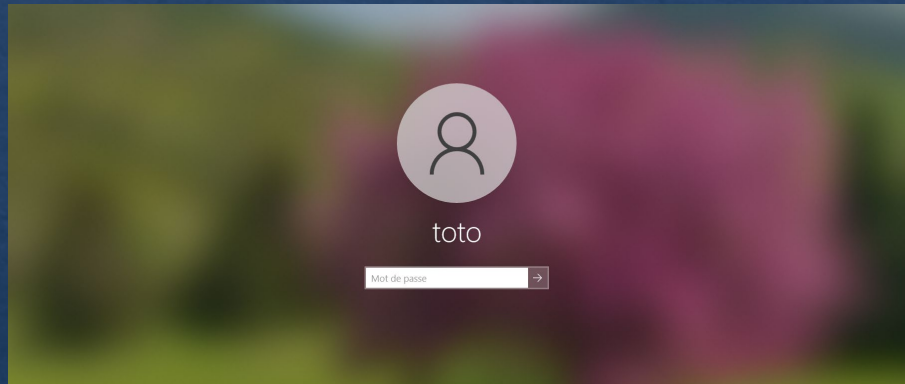
On sélectionne le serveur d'authentification correspondant, on se connecte avec un utilisateur crée dans l'AD et dans le groupe autorisé dans les règles RADIUS et on test.

The screenshot shows the Mikrotik WinBox interface. At the top, the breadcrumb is 'Diagnostics / Authentication'. A dropdown menu on the right shows 'Diagnostics' expanded with 'Authentication' selected and highlighted with a red box. Below this, a green message box states: 'User Jean Loup authenticated successfully. This user is a member of groups:'. The main section is titled 'Authentication Test'. It contains three input fields: 'Authentication Server' with a dropdown menu showing 'AD FORMATION' and a note 'Select the authentication server to test against.', 'Username' with the text 'Jean Loup', and 'Password' with masked characters '.....'.



# Etape 2 – Tests

Ensuite il suffit simplement de tester du côté apprenant. On ouvre une machine sans configurations particulière et en dehors du domaine. L'apprenant est en DHCP.



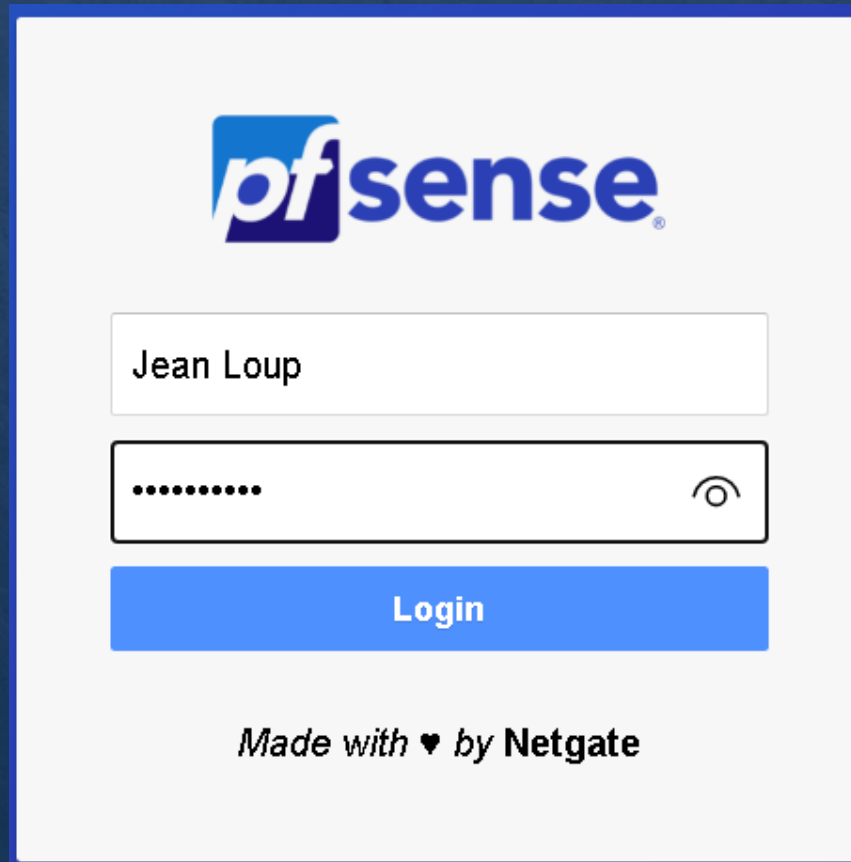
```
C:\Users\toto>hostname
DESKTOP-4GASCTQ

C:\Users\toto>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : home.arpa
    Adresse IPv4. . . . . : 192.168.90.10
    Masque de sous-réseau. . . . . : 255.255.255.128
    Passerelle par défaut. . . . . : 192.168.90.126
```



# Etape 2 – Tests

```
C:\Users\toto>ping google.fr

Envoi d'une requête 'ping' sur google.fr [172.217.20.195] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 172.217.20.195:
    Paquets : envoyés = 2, reçus = 0, perdus = 2 (perte 100%),
Ctrl+C
^C
C:\Users\toto>ping google.fr


Envoi d'une requête 'ping' sur google.fr [172.217.20.195] avec 32 octets de données :
Réponse de 172.217.20.195 : octets=32 temps=21 ms TTL=114
Réponse de 172.217.20.195 : octets=32 temps=22 ms TTL=114
Réponse de 172.217.20.195 : octets=32 temps=19 ms TTL=114
Réponse de 172.217.20.195 : octets=32 temps=19 ms TTL=114

Statistiques Ping pour 172.217.20.195:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 19ms, Maximum = 22ms, Moyenne = 20ms
```

Avant connexion

Après connexion

Notre client apparaît bien dans la liste des utilisateurs authentifié auprès du portail captif.

Status / Captive Portal / portail_captif					
Users Logged In (1)					
IP address	MAC address	Username	Session start	Last activity	Actions
192.168.90.10	00:0c:29:20:d4:74	Jean Loup	12/19/2024 15:30:19	12/19/2024 15:38:38	



# Etape 3 – Courrier électronique et NextCloud

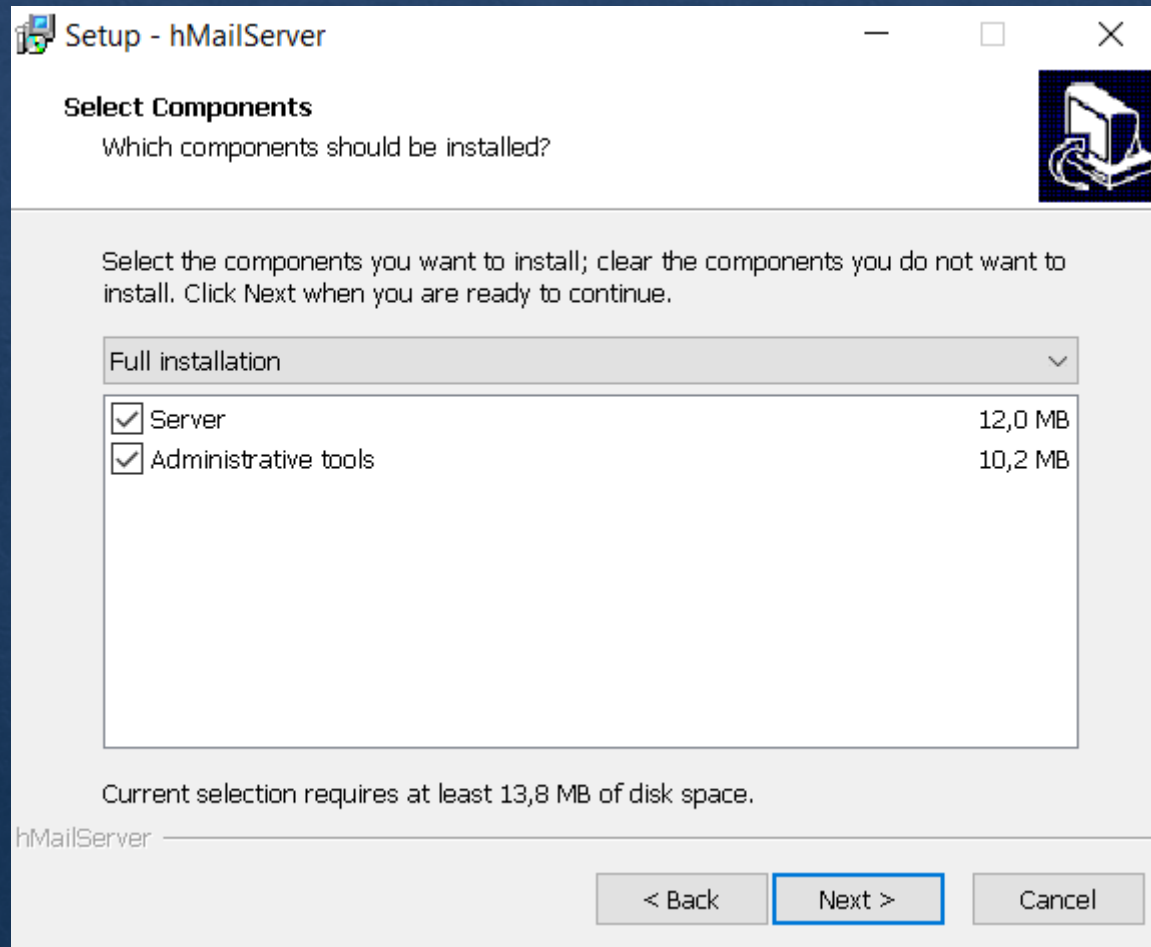


**hMailServer**



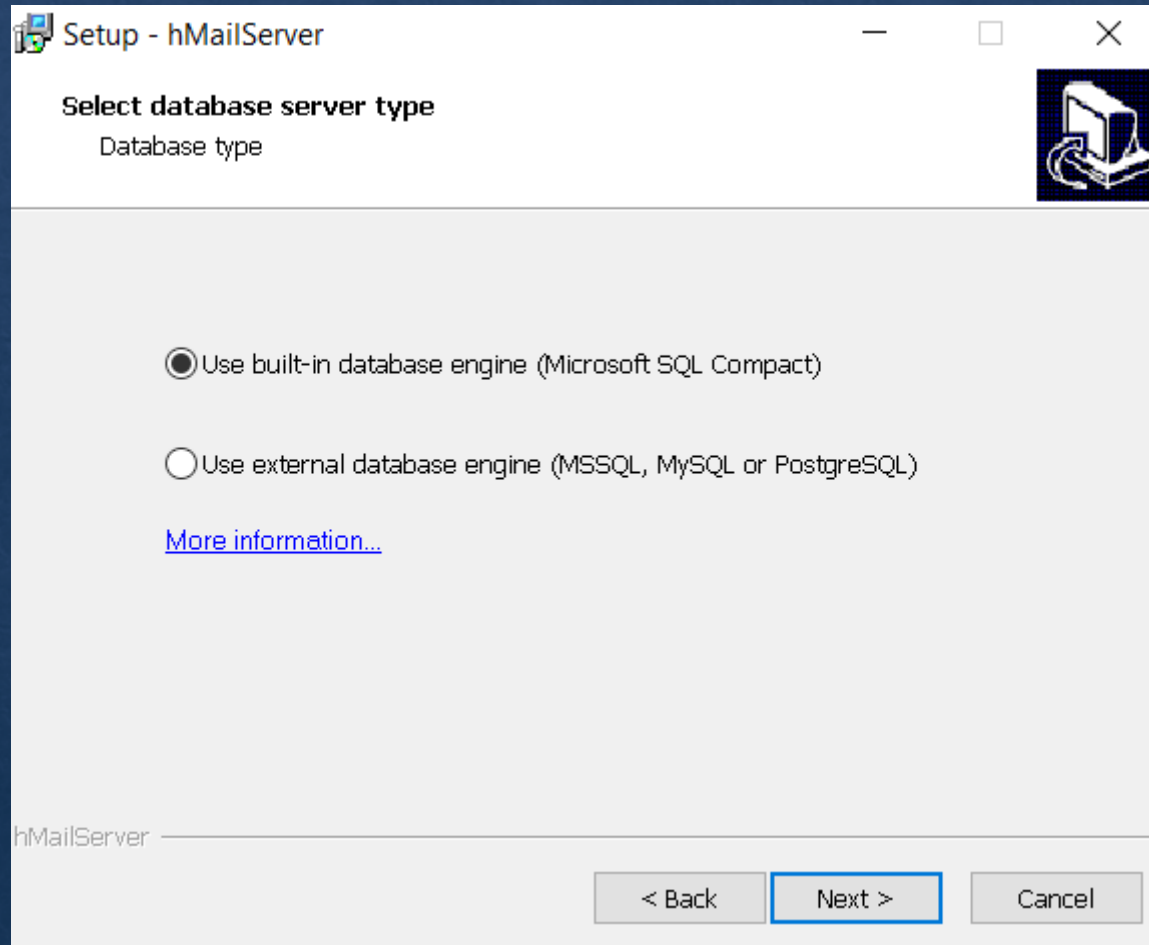
nextcloud

# Etape 3 – Mise en place - hMail

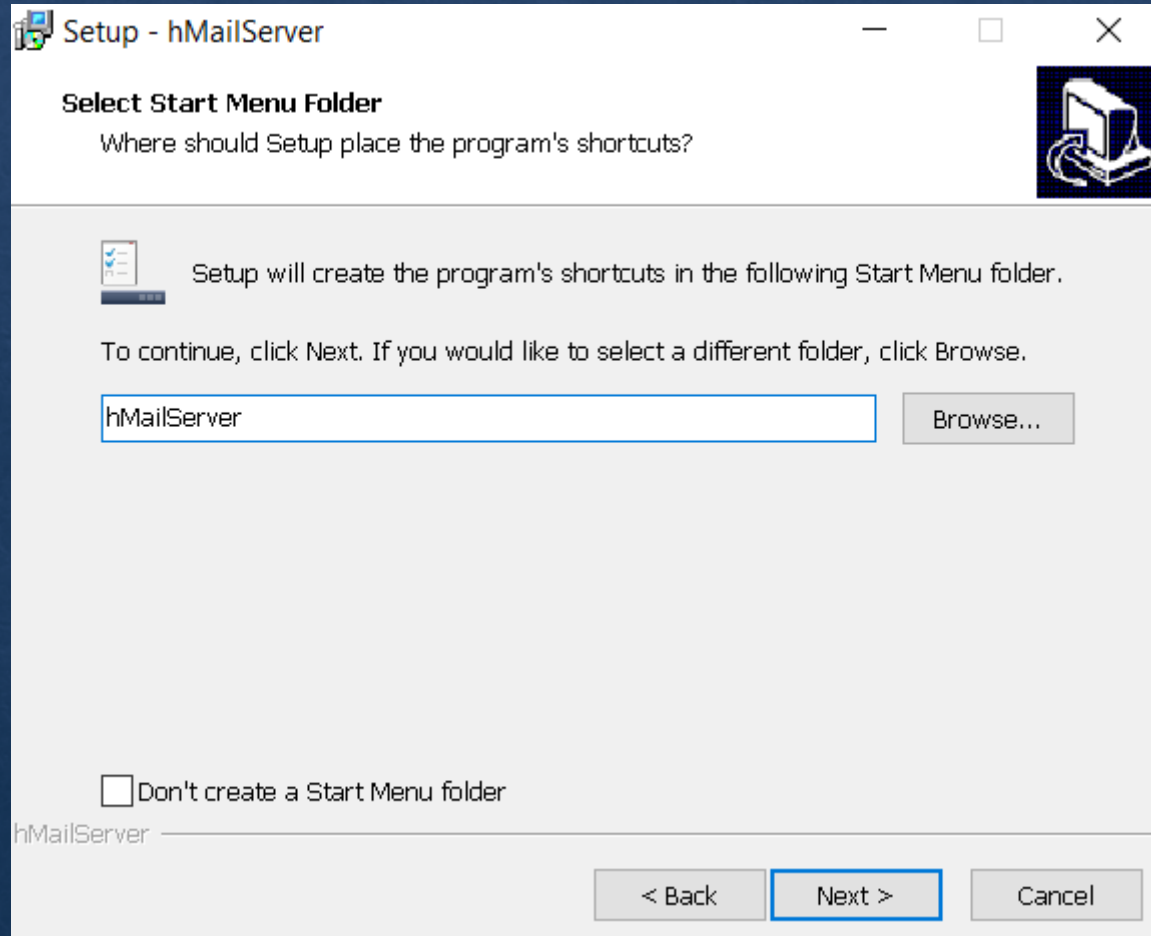




# Etape 3 – Mise en place - hMail

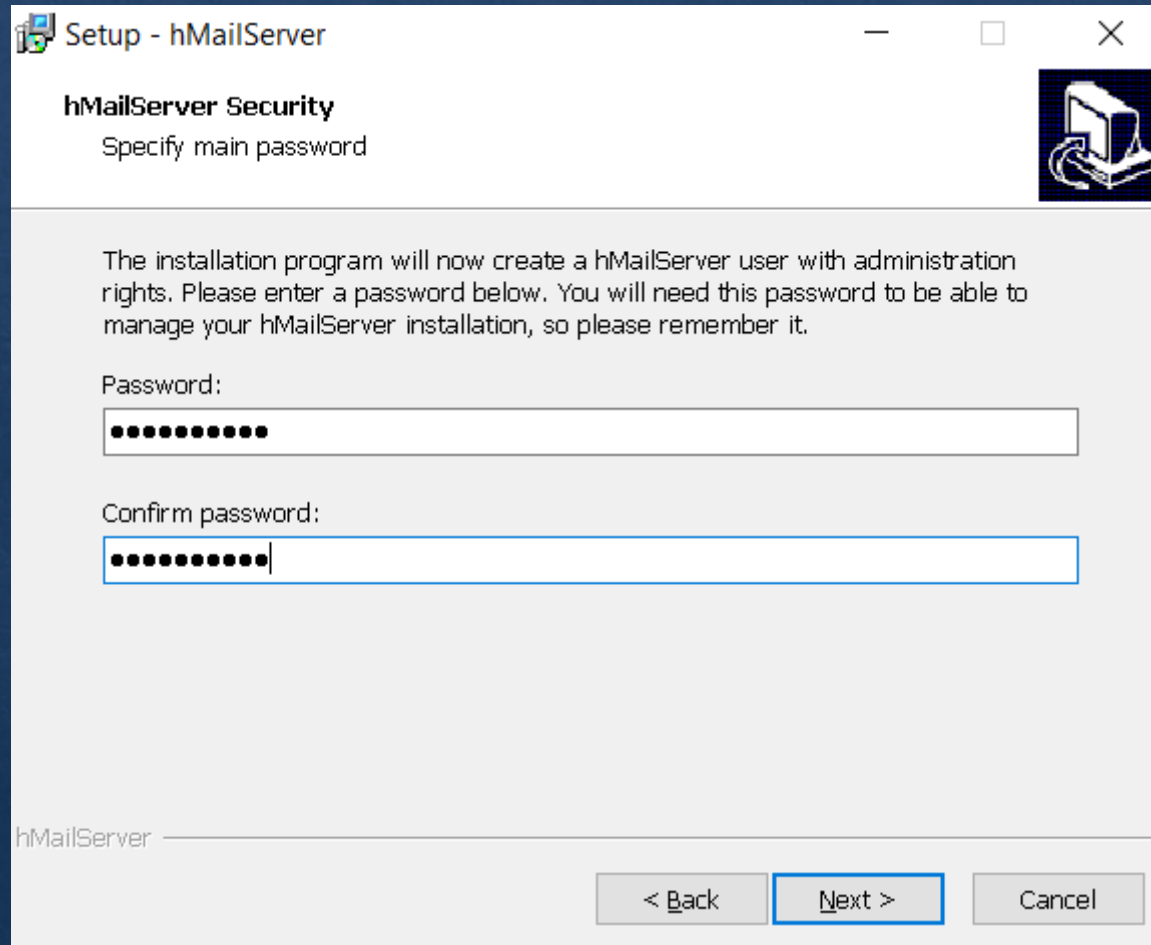


# Etape 3 – Mise en place - hMail





# Etape 3 – Mise en place - hMail



The screenshot shows the 'Setup - hMailServer' window with the 'hMailServer Security' tab selected. The window title bar includes standard Windows window controls (minimize, maximize, close). The main content area has a header 'hMailServer Security' with the subtitle 'Specify main password'. Below this, a text block explains that the installation will create an administrator user and asks for a password. There are two password input fields: 'Password:' and 'Confirm password:', both containing masked characters. At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'. The hMailServer logo is visible in the bottom left corner of the window.

Setup - hMailServer

**hMailServer Security**  
Specify main password

The installation program will now create a hMailServer user with administration rights. Please enter a password below. You will need this password to be able to manage your hMailServer installation, so please remember it.

Password:  
[Masked Password]

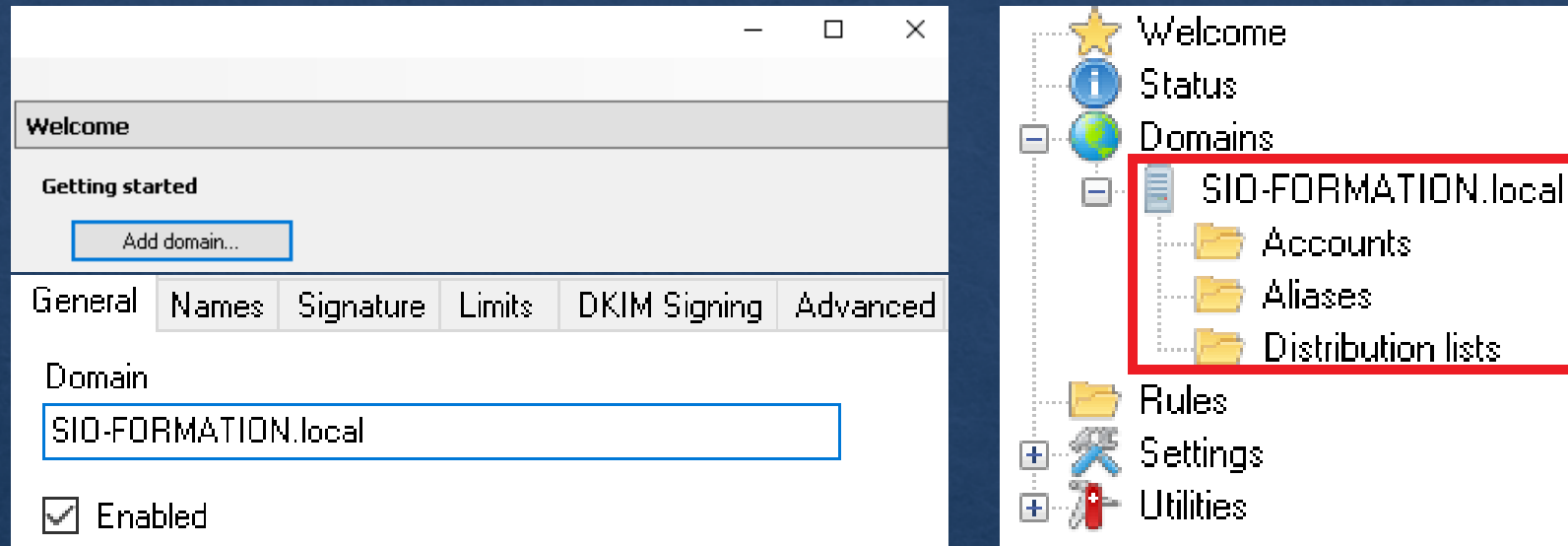
Confirm password:  
[Masked Password]

hMailServer

< Back   Next >   Cancel

On crée notre mdp administrateur de l'application hmail server puis « Next ».

# Etape 3 – Mise en place - hMail



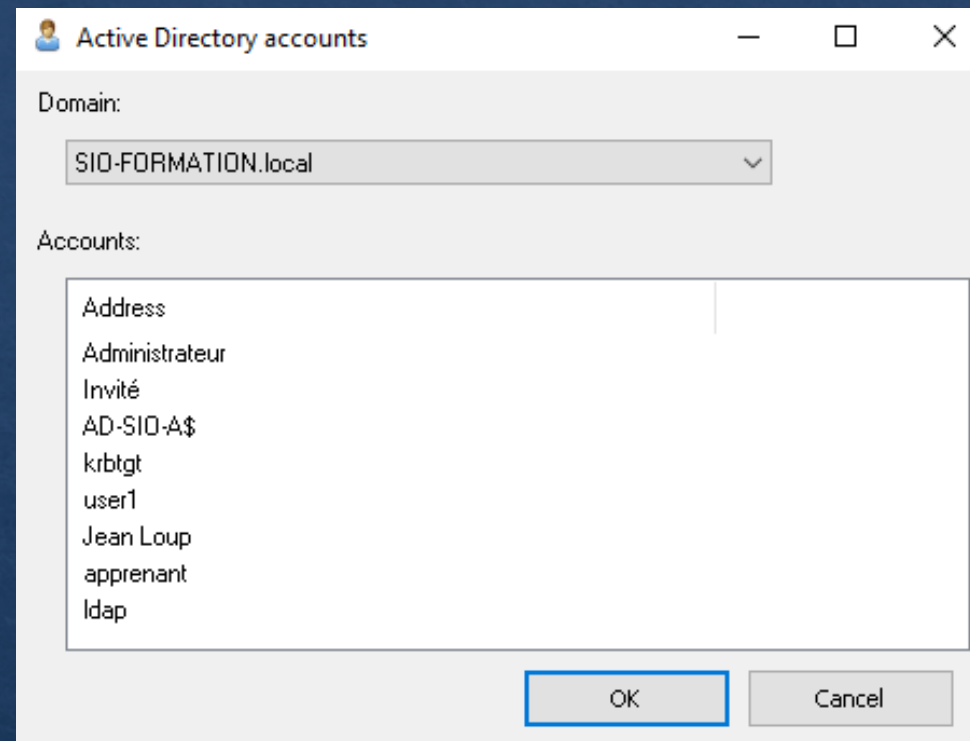
Une fois l'installation terminée, nous allons commencer par ajouter notre domaine. Une fois celui-ci créé de nouveaux dossiers apparaissent.



# Etape 3 – Mise en place - hMail



Name	Enabled
apprenant001@SIO-FORMATION.local	Yes
Jean-Loup@SIO-FORMATION.local	Yes
user1@SIO-FORMATION.local	Yes



Nous allons donc pouvoir créer nos adresses mail dans le dossier « Accounts ».

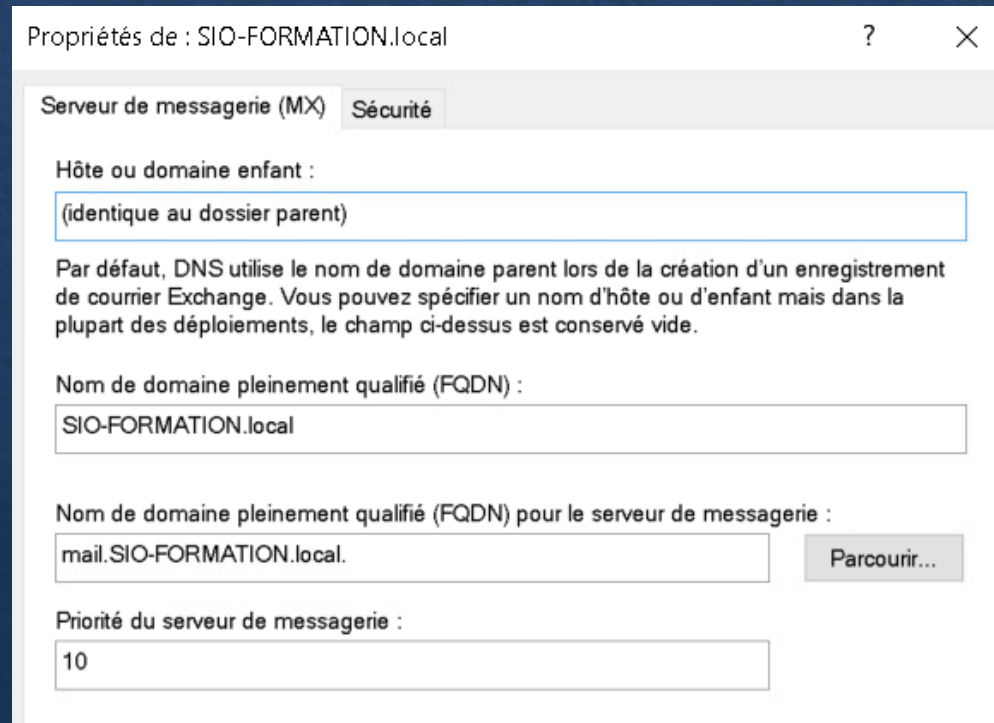
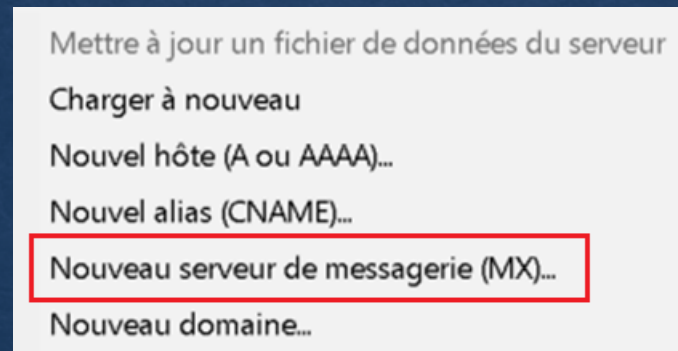
Pour cela nous pouvons le faire manuellement ou bien les importer de notre AD directement.

Pour ce faire, clic droit sur « Accounts » puis « Add AD account » et choisir les utilisateurs souhaités.

# Etape 3 – Mise en place - hmail

Il va falloir créer un enregistrement MX dans le DNS du serveur Windows afin d'indiquer où se trouve le serveur de messagerie.

Pour ce faire nous allons dans les enregistrements DNS, clic droit et « nouveau serveur de messagerie (MX) »

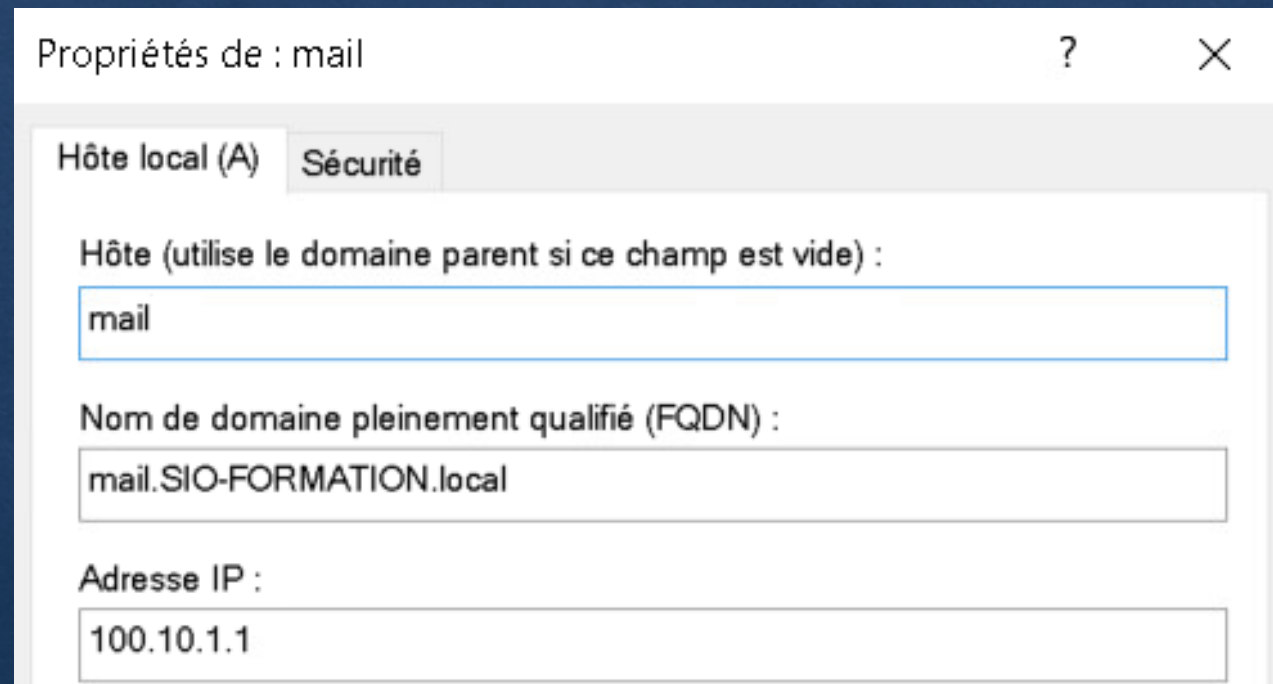
A screenshot of the 'Propriétés de : SIO-FORMATION.local' dialog box, specifically the 'Serveur de messagerie (MX)' tab. The dialog has a title bar with a question mark and a close button. It contains the following fields and controls:

- 'Hôte ou domaine enfant :' with a text box containing '(identique au dossier parent)'.
- A paragraph of text: 'Par défaut, DNS utilise le nom de domaine parent lors de la création d'un enregistrement de courrier Exchange. Vous pouvez spécifier un nom d'hôte ou d'enfant mais dans la plupart des déploiements, le champ ci-dessus est conservé vide.'
- 'Nom de domaine pleinement qualifié (FQDN) :' with a text box containing 'SIO-FORMATION.local'.
- 'Nom de domaine pleinement qualifié (FQDN) pour le serveur de messagerie :' with a text box containing 'mail.SIO-FORMATION.local.' and a 'Parcourir...' button to its right.
- 'Priorité du serveur de messagerie :' with a text box containing '10'.



# Etape 3 – Mise en place - hmail

Pour associer notre enregistrement MX à une IP, il suffit de créer un enregistrement A avec le nom de notre enregistrement MX et de l'associer à l'IP souhaiter.



Propriétés de : mail

Hôte local (A) Sécurité

Hôte (utilise le domaine parent si ce champ est vide) :

mail

Nom de domaine pleinement qualifié (FQDN) :

mail.SIO-FORMATION.local

Adresse IP :

100.10.1.1

# Etape 3 – Mise en place - hmail

Il va aussi falloir gérer le firewall du serveur pour autoriser le trafic des protocoles SMTP et IMAP soit les ports 25, 587 et 143. Je ne vais pas utiliser POP3 ici. On retrouve les ports utilisés par hmail dans les paramètres avancés.

Name

0.0.0.0 / 25 / SMTP

0.0.0.0 / 110 / POP3

0.0.0.0 / 143 / IMAP

0.0.0.0 / 587 / SMTP

✓ IMAP Port	Tout	Oui	Autoriser	Non	Tout	Tout	Tout	TCP	143	Tout	Tout	Tout	Tout	Tout	Aucun	Tout
✓ SMTP Port 25	Tout	Oui	Autoriser	Non	Tout	Tout	Tout	TCP	25	Tout	Tout	Tout	Tout	Tout	Aucun	Tout
✓ SMTP Port 587	Tout	Oui	Autoriser	Non	Tout	Tout	Tout	TCP	587	Tout	Tout	Tout	Tout	Tout	Aucun	Tout



# Etape 3 – Mise en place - hmail

The screenshot shows the hmail configuration window. At the top, there are three input fields: 'Your full name' with the value 'user1', 'Email address' with the value 'user1@sio-formation.local', and 'Password' with masked characters. Below these is a checked checkbox for 'Remember password'. A green status bar indicates 'Configuration found by trying common server names.' The 'Available configuration' section shows 'IMAP' selected with the description 'Keep your folders and emails synced on your server'. It lists 'Incoming IMAP NO ENCRYPTION sio-formation.local' and 'Outgoing SMTP NO ENCRYPTION sio-formation.local'. The 'Username' is listed as 'user1'. At the bottom, there are three buttons: 'Configure manually' (blue text), 'Cancel' (grey), and 'Done' (blue).

Your full name  
user1

Email address  
user1@sio-formation.local

Password  
••••••••

☒ Remember password

✓ Configuration found by trying common server names.

**Available configuration**

☒ **IMAP**  
Keep your folders and emails synced on your server

**Incoming IMAP** NO ENCRYPTION  
sio-formation.local

**Outgoing SMTP** NO ENCRYPTION  
sio-formation.local

**Username**  
user1

[Configure manually](#) Cancel Done

Si la configuration à bien été mise en place, nous devrions pouvoir nous connecter de façon automatique à notre serveur de messagerie.

# Etape 3 – Mise en place - hmail

**SERVEUR ENTRANT**

Protocole :

IMAP

Nom d'hôte :

hmail.sio-formation.local

Port :

143

Sécurité de la connexion :

Aucun

Méthode d'authentification :

Mot de passe normal

Nom d'utilisateur :

apprenant001@SIO-FORMATION.local

**SERVEUR SORTANT**

Nom d'hôte :

hmail.sio-formation.local

Port :

25

Sécurité de la connexion :

Aucun

Méthode d'authentification :

Mot de passe normal

Nom d'utilisateur :

apprenant001@SIO-FORMATION.local

Dans le cas où la connexion automatique ne fonctionne pas, il est possible de le faire manuellement.

Le serveur entrant et sortant est le même serveur dans notre cas ce qui facilite la configuration. Les ports sont ceux par défaut mais modifiable dans hmail server si besoins.



# Etape 3 – Mise en place - hmail

 **Avertissement !**

**Paramètres du courrier entrant :**  
**100.10.1.1** n'utilise pas de chiffrement.  
Les serveurs de courrier non sécurisés n'utilisent pas de connexions chiffrées pour protéger vos mots de passe et vos informations privées. En vous connectant à ce serveur, vous pourriez exposer votre mot de passe et vos informations privées.

**Paramètres du courrier sortant :**  
**100.10.1.1** n'utilise pas de chiffrement.  
Les serveurs de courrier non sécurisés n'utilisent pas de connexions chiffrées pour protéger vos mots de passe et vos informations privées. En vous connectant à ce serveur, vous pourriez exposer votre mot de passe et vos informations privées.

Thunderbird peut vous permettre d'accéder à vos e-mails en utilisant les configurations fournies. Cependant, vous devriez contacter votre administrateur ou votre fournisseur de messagerie au sujet de ces connexions incorrectes. Consultez la [FAQ de Thunderbird](#) pour plus d'informations.

☒ Je comprends les risques

Modifier les paramètres

Confirmer

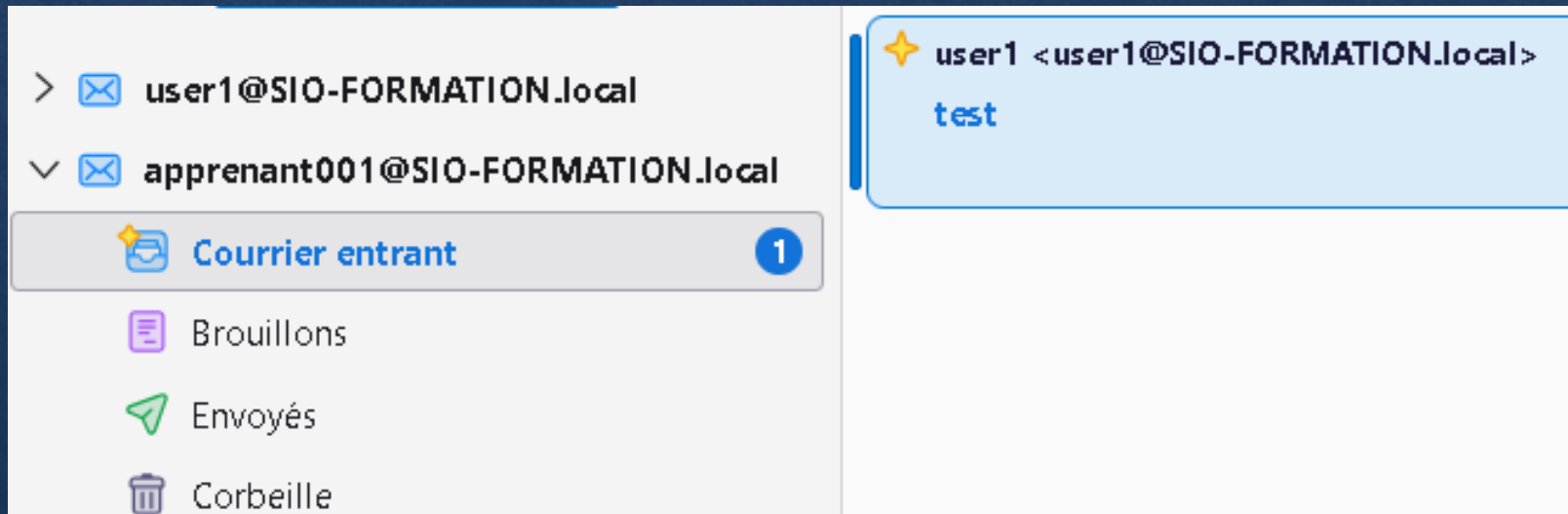
Dans les deux cas, si la connexion fonctionne, on doit tomber sur cet avertissement. On valide et on accepte le risque.

# Etape 3 – Tests - hMail

J'ai connecté deux boîtes mail sur la même application pour effectuer les tests.

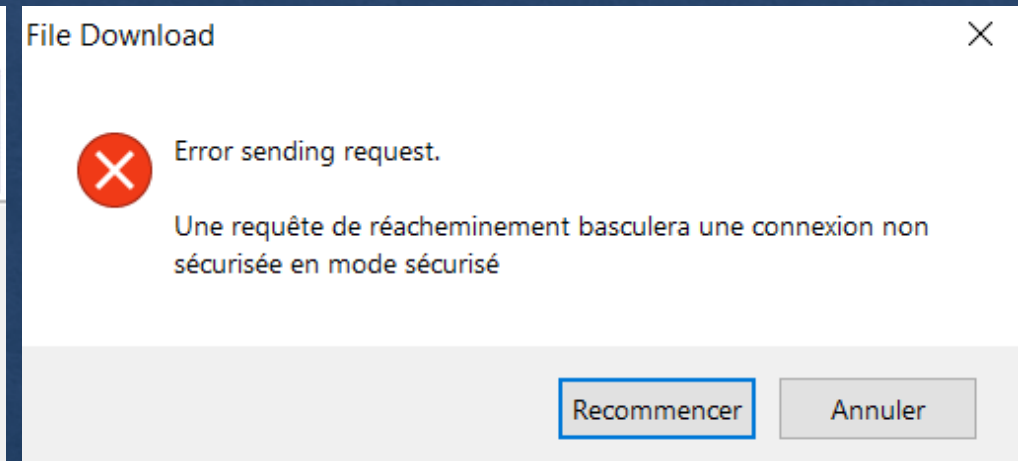
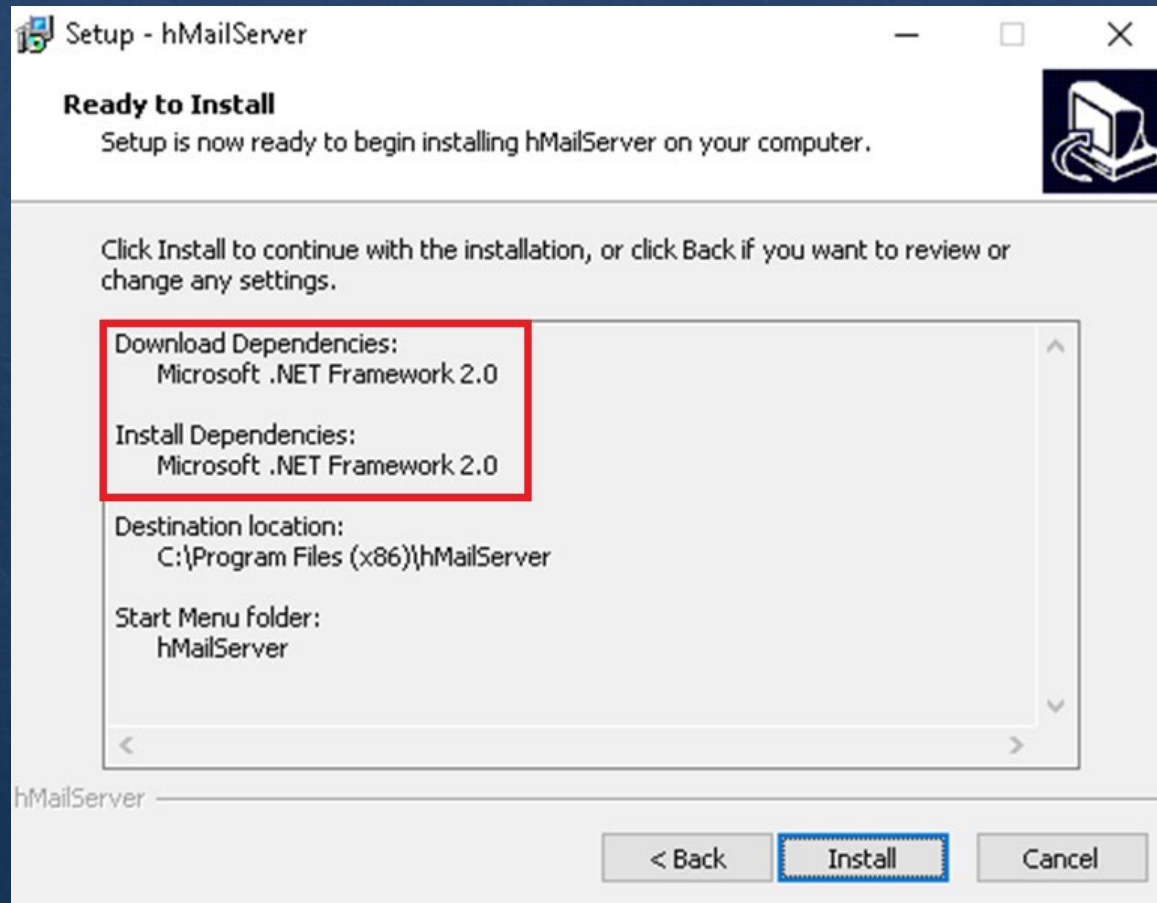
J'ai bien reçu le mail de user1 dans la boîte de l'apprenant.

✉ user1@SIO-FORMATION.local  
✉ apprenant001@SIO-FORMATION.local



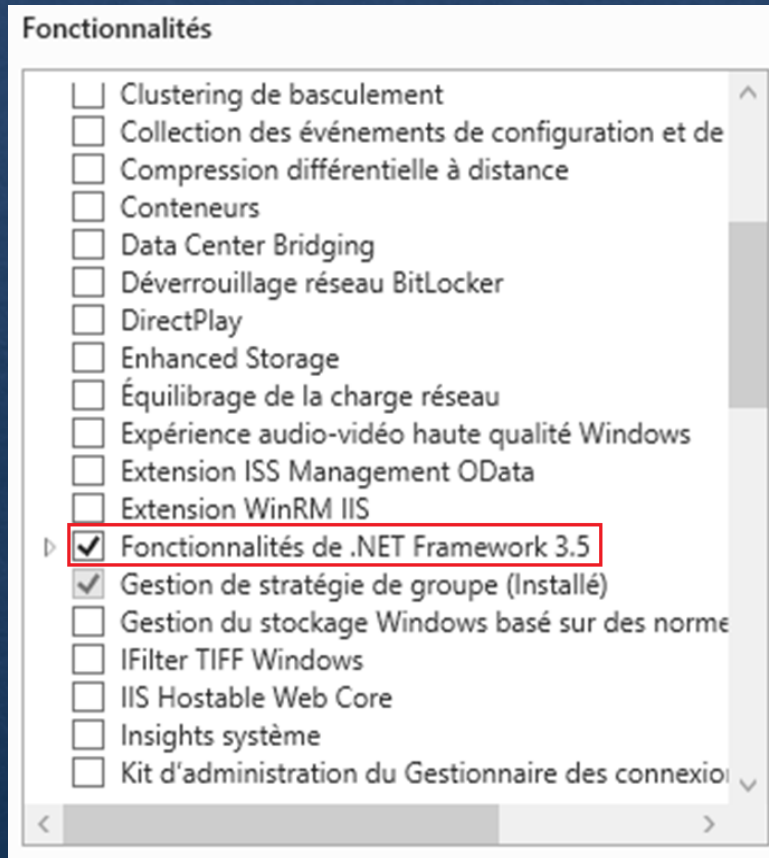


# Etape 3 – Problème rencontré - hmail



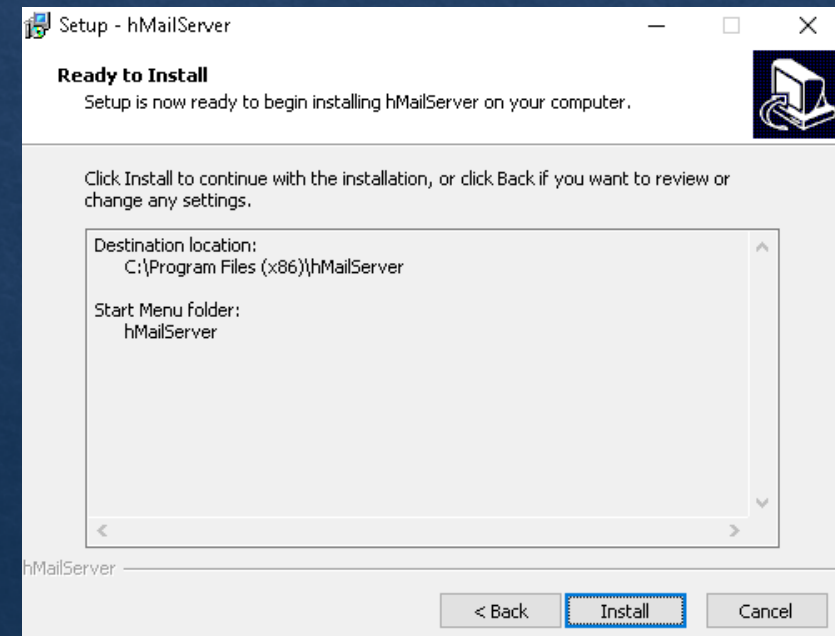
L'installation ne se finalise pas car elle doit installer des dépendances supplémentaires mais une erreur survient lors de l'installation.

# Etape 3 – Solution trouvé - hmail



Fonctionnalités de .NET Framework 3.5  
.NET Framework 3.5 (inclut .NET 2.0 et 3.0)

Pour résoudre ce souci j'ai commencé par chercher les dépendances directement sur internet mais l'installation ne fonctionne pas non plus, une erreur me conseille de le faire par le gestionnaire de serveur. Je me rends donc dans la liste des fonctionnalités du Windows serveur et j'ai trouvé ce qu'il fallait.





# Etape 3 – Mise en place - NextCloud

On installe nextCloud puis on crée la BDD nextCloud.

```
apt update && apt upgrade -y
```

```
wget https://download.nextcloud.com/server/releases/latest.zip
```

```
unzip latest.zip
```

```
mv nextcloud /var/www/html/
```

```
chown -R www-data:www-data /var/www/html/nextcloud/
```

```
systemctl restart apache2
```

```
MariaDB [(none)]> CREATE DATABASE nextcloud_db;
```

```
Query OK, 1 row affected (0,000 sec)
```

```
MariaDB [(none)]> CREATE USER 'nextcloud_user'@'localhost' IDENTIFIED BY '/Admintoto';
```

```
Query OK, 0 rows affected (0,001 sec)
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nextcloud_user'@'localhost';
```

```
Query OK, 0 rows affected (0,001 sec)
```

```
MariaDB [(none)]> FLUSH PRIVILEGES;
```

```
Query OK, 0 rows affected (0,000 sec)
```

# Etape 3 – Mise en place - NextCloud

```
root@Nextcloud-Server:~# cd /var/www/html/nextcloud/core/skeleton/  
root@Nextcloud-Server:/var/www/html/nextcloud/core/skeleton# ls  
Documents          'Nextcloud Manual.pdf'  Photos      'Reasons to use Nextcloud.pdf'  'Templates credits.md'  
'Nextcloud intro.mp4'  Nextcloud.png           Readme.md   Templates  
root@Nextcloud-Server:/var/www/html/nextcloud/core/skeleton# rm -rf *  
root@Nextcloud-Server:/var/www/html/nextcloud/core/skeleton# ls  
root@Nextcloud-Server:/var/www/html/nextcloud/core/skeleton#
```

Le dossier `/var/www/html/nextcloud/core/skeleton` contient les dossiers créés par défauts lors de la connexion d'un nouvel utilisateur. Supprimer son contenu permet d'éviter que tous ces documents inutiles polluent l'espace de partage des apprenants.

Je vais juste créer un dossier Documents et Cours par défauts pour chaque utilisateur. Le dossier « Document » fera office de dossier personnel même si celui-ci n'est pas affiché avec le nom du user connecté.

```
root@Serveur-Zabbix:/var/www/html/nextcloud/core/skeleton# mkdir Documents Cours
```



# Etape 3 – Mise en place - NextCloud

<http://192.168.18.1/nextcloud>

On saisit le lien du serveur dans la barre de recherche, on crée notre user admin pour se connecter à l'interface web et on renseigne l'utilisateur admin de la BDD créée précédemment pour permettre à Next cloud d'y accéder.

Créer un **compte administrateur**

S'identifier

admin

Mot de passe

.....

Stockage & base de données ▼

Répertoire des données

/var/www/html/nextcloud/data

Configurer la base de données

Seul(e) MySQL/MariaDB est disponible. Installez et activez les modules PHP additionnels adéquats pour choisir d'autres types de base de données. Consultez la documentation pour plus de détails. ☒

Compte de base de données

nextcloud\_user

Mot de passe de la base de données

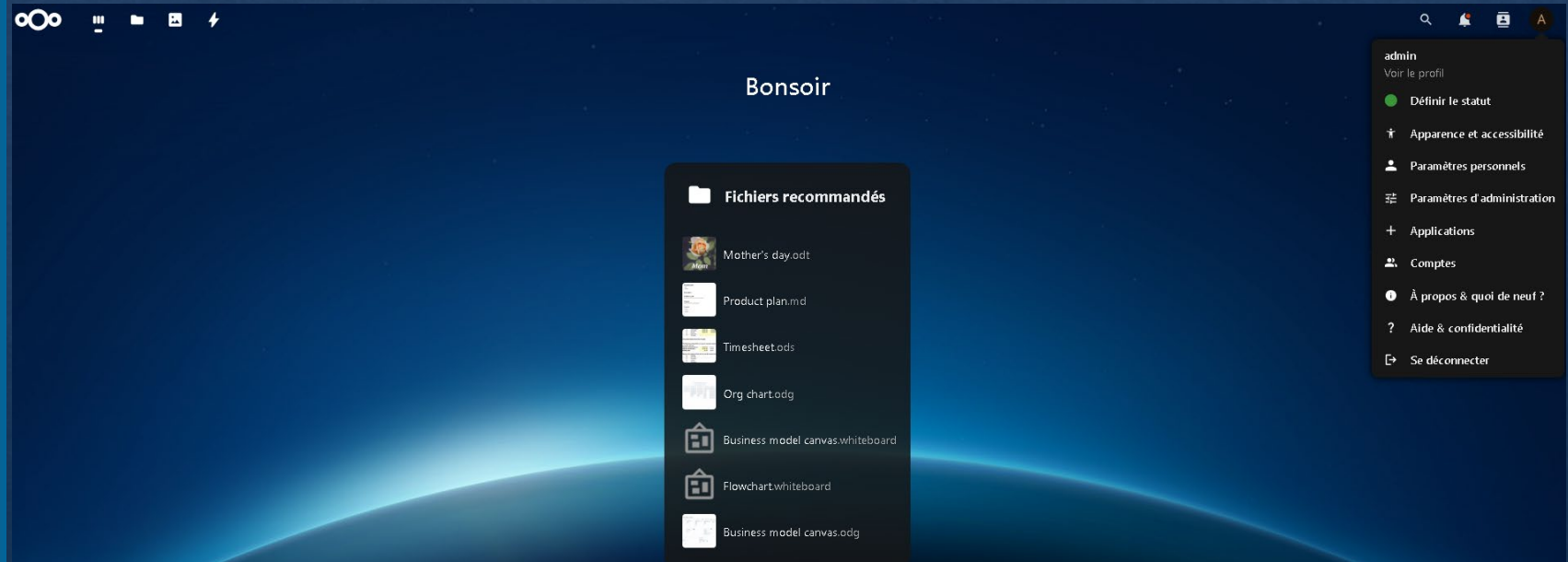
.....

Nom de la base de données

nextcloud\_db

Hôte de la base de données

localhost



# Etape 3 – Mise en place - NextCloud

admin  
Voir le profil

- Définir le statut
- ✎ Apparence et accessibilité
- 👤 Paramètres personnels
- ⚙️ Paramètres d'administration
- + Applications**
- 👥 Comptes

Dans l'onglet « application » puis « applications désactivées », on active le protocole LDAP.

Applications désactivées

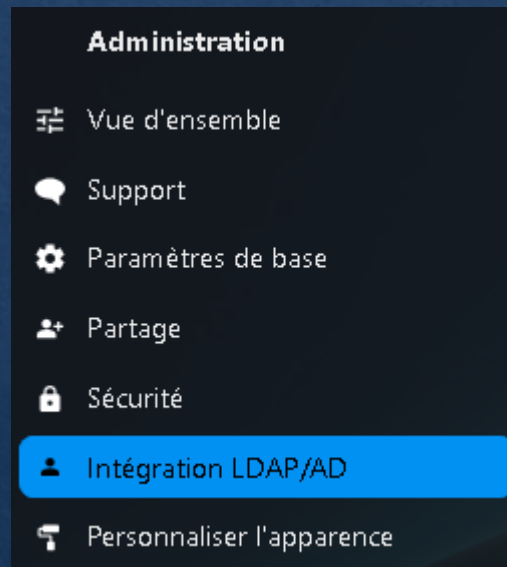
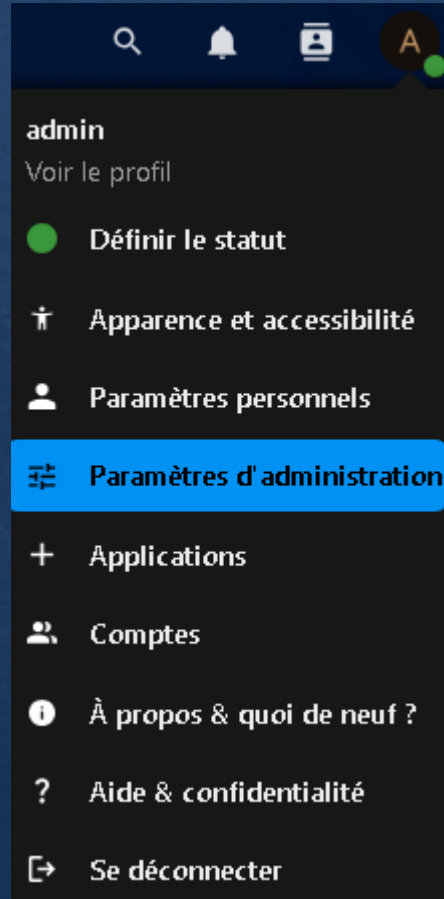
Toutes les applications sont à jour.

⚙️ Auditing / Logging	1.20.0	✓ En vedette	Activer
🛡️ Default encryption module	2.18.0	✓ En vedette	Activer
📁 External storage support	1.22.0	✓ En vedette	Activer
👤 LDAP user and group backend	1.21.0	✓ En vedette	Activer
🔍 Suspicious Login	8.0.0	✓ En vedette	Activer
🔊 Two-Factor Authentication via Nextcloud notification	4.0.0	✓ En vedette	Activer
🔑 Two-Factor TOTP Provider	12.0.0-dev	✓ En vedette	Activer



# Etape 3 – Mise en place - NextCloud

L'application est installée, place à la configuration de celui-ci.



### Intégration LDAP/AD

Serveur Utilisateurs Attributs de connexion Groupes

1. Serveur : 100.10.1.1 +

100.10.1.1 389 Détecter le port

CN=ldap,CN=Users,DC=SIO-FORMATION,DC=local

..... Sauvegarder les informations d'identification

DC=SIO-FORMATION,DC=local Détecter le DN de base Tester le DN de base

☐ Saisir les filtres LDAP manuellement (recommandé pour les annuaires de grande ampleur)

Configuration OK ● Continuer Aide

# Etape 3 – Mise en place - NextCloud

Pour pouvoir récupérer automatiquement les utilisateurs de l'AD nous devons faire une intégration LDAP avec les paramètres suivants :

L'ip du serveur AD suivi du DN de l'utilisateur qui va permettre la connexion LDAP, dans notre cas ce sera l'utilisateur « ldap » créé spécifiquement pour l'occasion. On y met le MDP associé au compte.

Enfin on clic sur « détecter le DN de base », si la configuration est bien faite, celui-ci s'affiche automatiquement.

Le DN permet de localiser un endroit spécifique dans l'AD. Le DN de base trouvée englobe tout, il est donc possible de le paramétrer pour juste récupérer les utilisateurs de l'OU créée au début.



# Etape 3 – Mise en place - NextCloud

Serveur **Utilisateurs** Attributs de connexion Groupes

Rechercher et lister les utilisateurs qui respectent ces critères :

Seulement ces classes d'objets :

Les classes d'objets fréquentes pour les utilisateurs sont : organizationalPerson, person, user et inetOrgPerson. Si vous n'êtes pas sûr de la classe à utiliser, demandez à l'administrateur de l'annuaire.

Seulement dans ces groupes :

- Serveurs RAS et IAS
- Serveurs RDS Endpoint
- Serveurs de licences de Storage Replica Adminis
- Utilisateurs
- Utilisateurs de gestion à
- Utilisateurs de l'Analyse
- Utilisateurs du Bureau à

>

Utilisateurs du dom

<

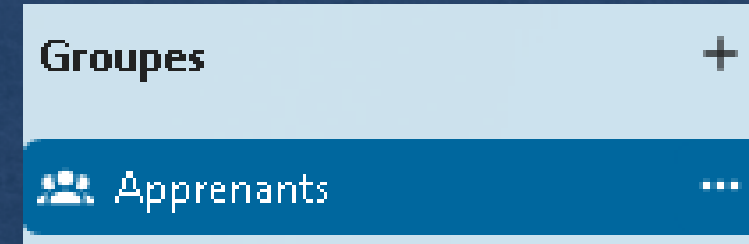
[Modifier la requête LDAP](#)

Filtre LDAP : (&((objectclass=user))((memberof=CN=Utilisateurs du domaine,CN=Users,DC=SIO-FORMATION,DC=local)(primaryGroupID=513))))

J'ai quand même eu la possibilité de simplement récupérer les utilisateurs du domaine par la suite.

# Etape 3 – Mise en place - NextCloud

☰	Nom d'affichage	Nom du compte	Mot de passe
U	user1	27E10A88-B75F-49FF-9DB...	
AO	apprenant 001	56774D2D-3395-4755-B43...	
L	ldap	5E7167B5-B2CC-4657-BF...	
JL	Jean Loup	A8D2D138-89BA-4FBF-B...	
A	admin	admin	

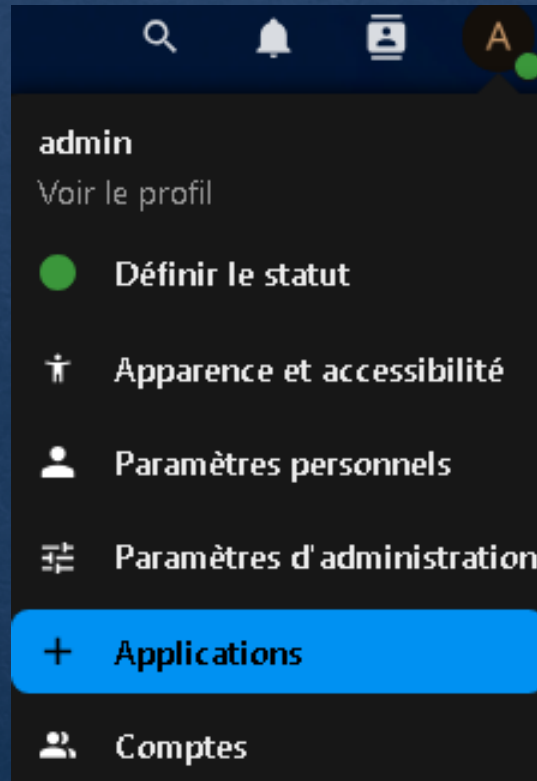


J'en profite pour mettre utilisateurs dans un groupe afin de faciliter les choses par la suite.

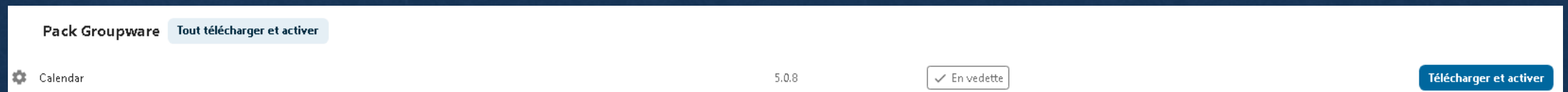
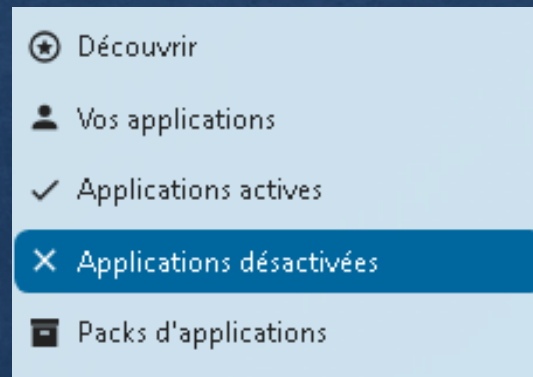
Le seul compte qui n'a pas été récupéré est le compte « administrateur » du domaine car le compte « admin » ici présent est celui que j'ai créé pour l'interface web de NextCloud.



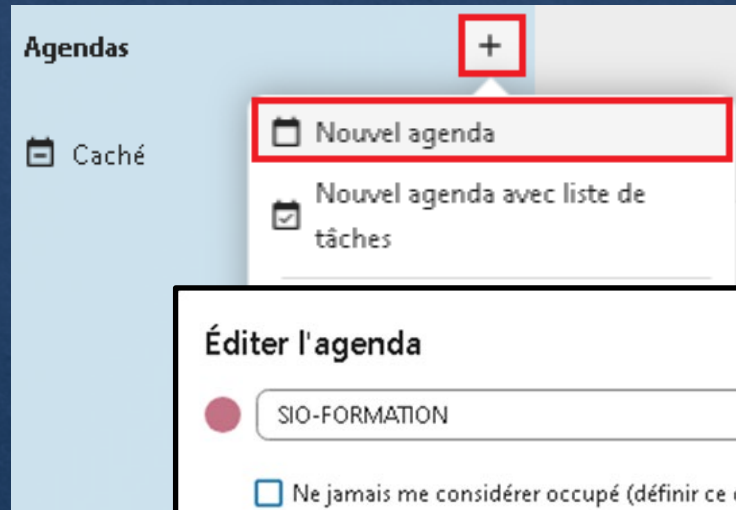
# Etape 3 – Mise en place - NextCloud



Pour installer le calendrier, on dirige dans l'onglet « application » puis « applications désactivées » et on recherche « calendar » puis « Télécharger et activer »



# Etape 3 – Mise en place - NextCloud



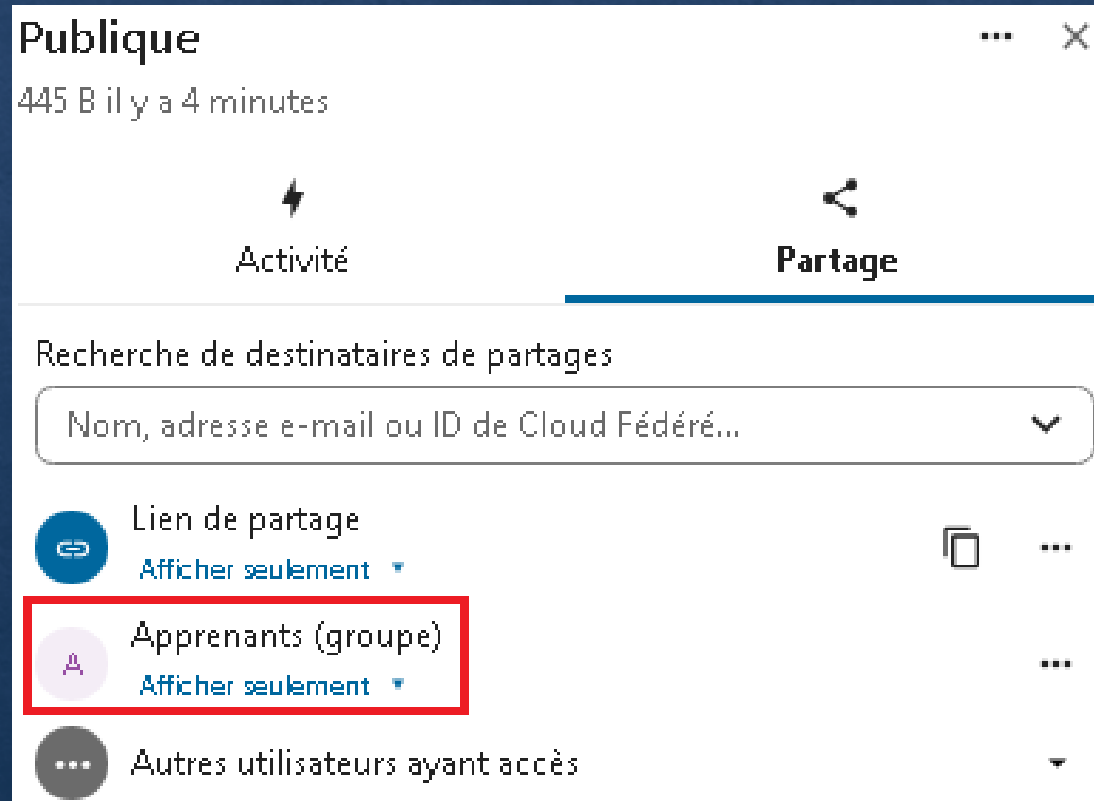
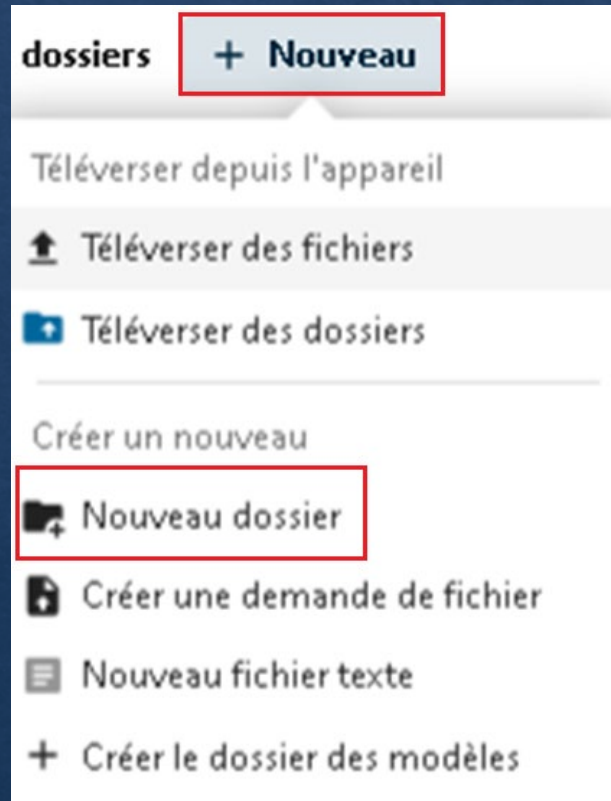
Dans l'application agenda on crée un nouvel agenda et on y ajoute le groupe avec tout nos apprenants afin qu'il puisse être ajouter à leurs comptes automatiquement.

The image shows the 'Éditer l'agenda' dialog box. It has a title bar with a close button (X). Below the title, there is a red circular icon and a text input field containing 'SIO-FORMATION'. Below this, there is a checkbox labeled 'Ne jamais me considérer occupé (définir ce calendrier comme transparent)'. The next section is titled 'Partager l'agenda' and contains a dropdown menu with the text 'Partager avec des utilisateurs ou des groupes'. Below the dropdown, there are three options: 'Lien de partage' (Link sharing), 'Lien interne' (Internal link), and 'Apprenants' (Learners). The 'Apprenants' option is highlighted with a red box. To the right of the 'Apprenants' option, there is a checkbox labeled 'peut modifier' (can modify) and a trash icon. At the bottom of the dialog, there are three buttons: 'Supprimer' (Delete), 'Exporter' (Export), and 'Enregistrer' (Save).



# Etape 3 – Mise en place - NextCloud

Pour la création d'un dossier partager c'est la même manipulation que pour le calendrier mais dans l'onglet « tous les fichiers ». On crée un nouveau dossier et on modifie les droits sur le partage.



# Etape 3 – Mise en place - NextCloud

Pour faciliter l'accès au serveur, il est possible de modifier le DNS de Windows pour ajouter un enregistrement A (« nextcloud » dans mon cas) qui pointe vers l'IP du serveur. Il faudra aussi aller dans les fichiers de configuration de NextCloud pour ajouter le nom « nextcloud » dans la liste des domaines autorisés.

**Path :** `/var/www/html/nextcloud/config/config.php`



nextcloud

Hôte (A)

192.168.18.1

```
'trusted_domains' =>
array (
    0 => '192.168.18.1',
    1 => 'nextcloud.sio-formation.local',
    2 => 'nextcloud',
),
```



# Etape 3 – Tests – NextCloud Calendar



**SIO-FORMATION** [X]

Formation disponible !

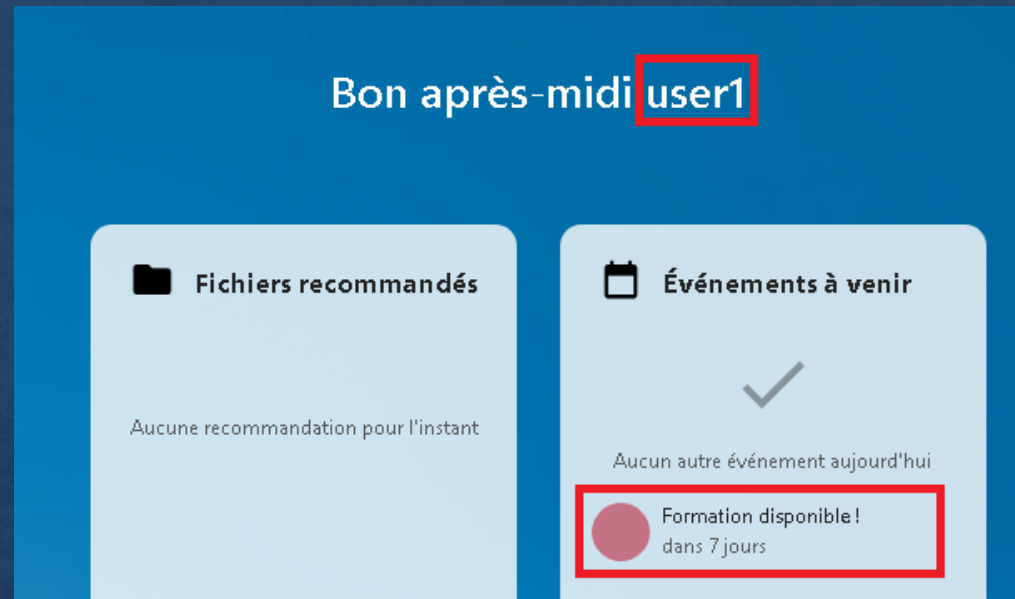
du 16/01/2025 à 09:00 [Globe icon] au 16/01/2025 à 15:30 [Globe icon]

☐ Journée entière

📍 Paris

📄 Sujet : Linux

[Plus de détails](#) [✓ Enregistrer](#)



Bon après-midi **user1**

**Fichiers recommandés**

Aucune recommandation pour l'instant

**Événements à venir**




✓

Aucun autre événement aujourd'hui


Formation disponible !  
dans 7 jours


Pour tester la configuration du calendrier je vais mettre une nouvelle date de formation et vérifié qu'elle s'affiche chez les utilisateurs.

# Etape 3 – Tests – NextCloud

<input type="checkbox"/>	Nom ▲
<input type="checkbox"/>	 Chapitre 1
<input type="checkbox"/>	 Chapitre 2
<input type="checkbox"/>	 Présentation de l'entreprise SIO-FORMATION.md

Présentation de l'entreprise SIO-FORMATION.md

 **Afficher le plan**

✓ 

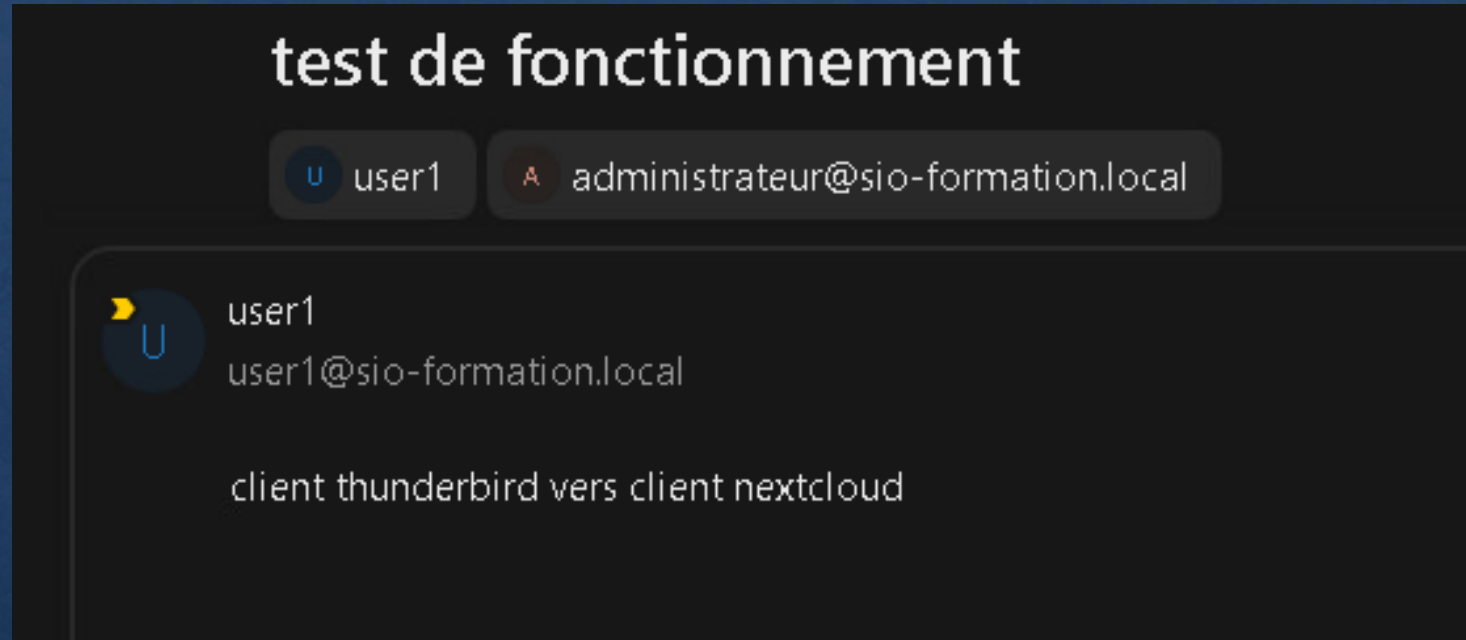
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Pour tester le dossier partager j'ai créé un fichier de test, il suffit de l'ouvrir avec un utilisateur du groupe « apprenant ». Je suis capable d'ouvrir le fichier sans soucis et sans la possibilité de le modifier.



# Etape 3 – Tests – NextCloud mail

Test d'envoi de mail de user1 vers administrateur.



# Etape 3 – Problème rencontré

Un des soucis rencontrés durant cette étape se trouve au moment de la création d'un enregistrement DNS pour faciliter l'accès au serveur. En effet, les utilisateurs arrivent à résoudre le nom de domaine « nextcloud » mais n'y accède pas contrairement au serveur qui y accède sans soucis.

```
C:\Users\Administrateur>nslookup nextcloud
Serveur : localhost
Address: 127.0.0.1

Nom : nextcloud.SIO-FORMATION.local
Address: 192.168.18.1

C:\Users\Administrateur>ping nextcloud

Envoi d'une requête 'ping' sur nextcloud.SIO-FORMATION.local [192.168.18.1] avec 32 octets de données :
Réponse de 192.168.18.1 : octets=32 temps=3 ms TTL=63
Réponse de 192.168.18.1 : octets=32 temps=3 ms TTL=63
Réponse de 192.168.18.1 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.18.1 : octets=32 temps=3 ms TTL=63
```



# Etape 3 – Solution trouvée

Je n'ai pas trouvé la solution. Cependant je soupçonne le fait que mes clients n'aient pas de « **suffixe DNS principal** » de défini comme le Serveur AD qui lui le possède et qui n'a pas de soucis à résoudre le nom depuis le navigateur. J'ai tenté de modifier le DHCP sur pfsense mais appart rajouter une « Liste de recherche de suffixe DNS » je n'ai pas su le faire de façon automatique. Mes clients peuvent quand même y accéder avec le nom complet : nextcloud.sio-formation.local même si cela n'est pas très pratique.

## Clients

```
Nom de l'hôte . . . . . : DESKTOP-4GASCTQ
Suffixe DNS principal . . . . . : ???
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: sio-formation.local
```

## Serveur

```
Nom de l'hôte . . . . . : AD-SIO-A
Suffixe DNS principal . . . . . : SIO-FORMATION.local
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: SIO-FORMATION.local
```

# Etape 4 – Zabbix

The Zabbix logo, featuring the word "ZABBIX" in white, uppercase, sans-serif font, centered within a solid red rectangular background.



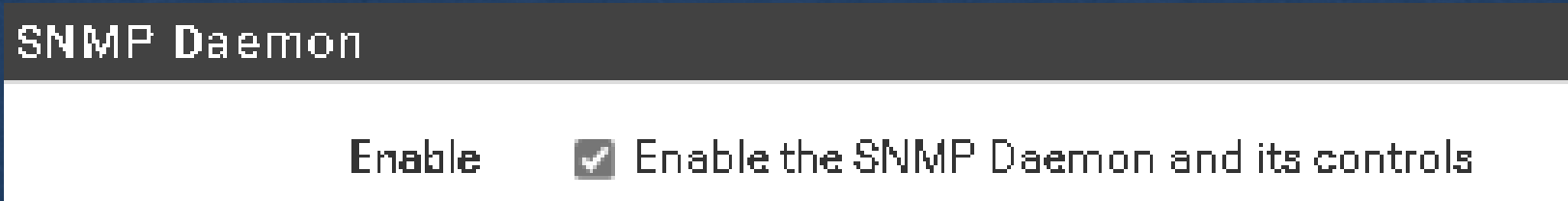
# Etape 4 – Mise en place

## Surveillance du routeur pfSense



Pour commencer la configuration de la supervision du pfSense avec SNMP on clic sur l'onglet « services » puis « SNMP ».

On active le Daemon SNMP, le reste des options restent par défaut.



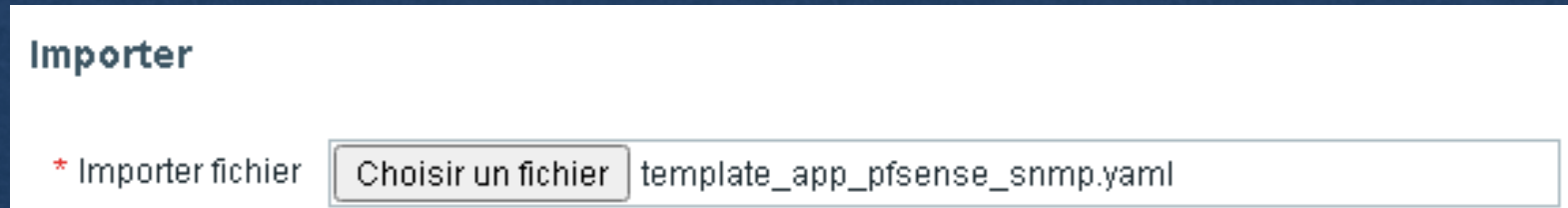
# Etape 4 – Mise en place

Direction Zabbix pour la fin de la configuration.

Nous aurons besoins des enregistrements SNMP de pfSense dans zabbix. Pour cela, nous allons sur le site officiel de zabbix et on copie colle dans un fichier .txt les informations avec l'extension .yaml .

<https://www.zabbix.com/integrations/pfsense>

Nom du fichier : template\_app\_pfsense\_snmp.yaml



Il ne reste plus qu'à l'importer dans les modèles.



# Etape 4 – Mise en place

Collecte de données ^

Groupes de modèles

Groupes d'hôtes

Modèles

Hôtes

Maintenance

Corrélation d'événement

Hôte

Hôte

IPMI

Tags

Macros

Inventaire

Chiffrement

Table de correspondance

\* Nom de l'hôte

pfsense

Nom visible

pfsense

Modèles

Nom

PFSense by SNMP

taper ici pour rechercher

Sélectionner

Action

[Supprimer lien](#)

[Supprimer lien et nettoyer](#)

\* Groupes d'hôtes

pfsense x

taper ici pour rechercher

Sélectionner

Interfaces

Type

adresse IP

Nom DNS

Connexion à

Port

SNMP

100.10.1.6

IP

DNS

161

On peut maintenant créer notre nouvel hôte. On lui renseigne le modèle que l'on vient d'importer ainsi qu'un groupe et enfin son IP/port .

# Etape 4 – Mise en place

## Surveillance du service apache sous debian12

```
apt update && apt upgrade -y  
apt install zabbix-agent
```

Mise à jour de la machine puis installation de l'agent zabbix.

```
nano /etc/zabbix/zabbix_agentd.conf  
Server= 100.10.1.3  
ServerActive=100.10.1.3  
Hostname=nextcloud
```

Fichier de configuration de l'agent.

```
systemctl restart zabbix-agent  
systemctl status zabbix-agent  
systemctl enable zabbix-agent
```

Redémarrage/Activations des services



# Etape 4 – Mise en place

**Hôte** ? x

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

\* Nom de l'hôte

Nom visible

Modèles

Nom	Action
Apache by Zabbix agent	<a href="#">Supprimer lien</a> <a href="#">Supprimer lien et nettoyer</a>

\* Groupes d'hôtes

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	<input type="text" value="192.168.18.1"/>	<input type="text"/>	<input type="button" value="IP"/> <input type="button" value="DNS"/>	<input type="text" value="10050"/>	<input checked="" type="radio"/> Supprimer

[Ajouter](#)

Description

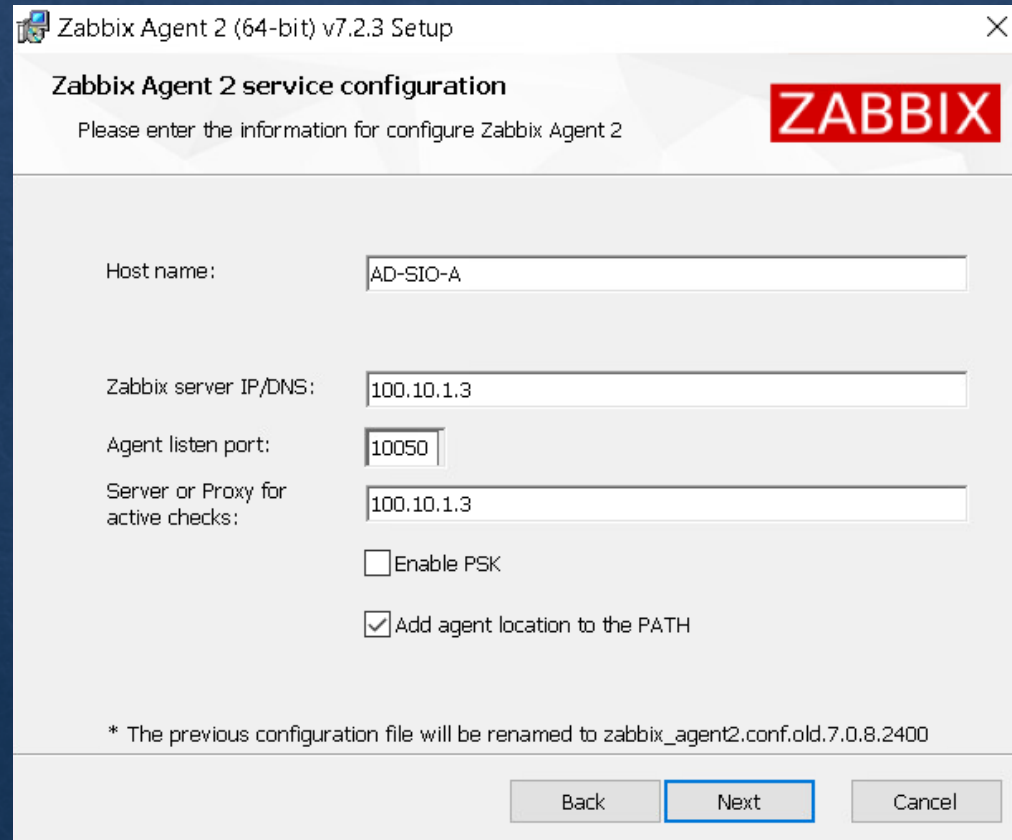
Surveillé par

Activé ☒

Une fois sur l'interface web, on crée un nouvel hôte identifiable, on lui met un groupe sinon zabbix chouine puis l'IP du serveur nextcloud.

# Etape 4 – Mise en place

## Surveillance de l'AD



Zabbix Agent 2 (64-bit) v7.2.3 Setup

**Zabbix Agent 2 service configuration**

Please enter the information for configure Zabbix Agent 2

Host name: AD-SIO-A

Zabbix server IP/DNS: 100.10.1.3

Agent listen port: 10050

Server or Proxy for active checks: 100.10.1.3

☐ Enable PSK

☒ Add agent location to the PATH

\* The previous configuration file will be renamed to zabbix\_agent2.conf.old.7.0.8.2400

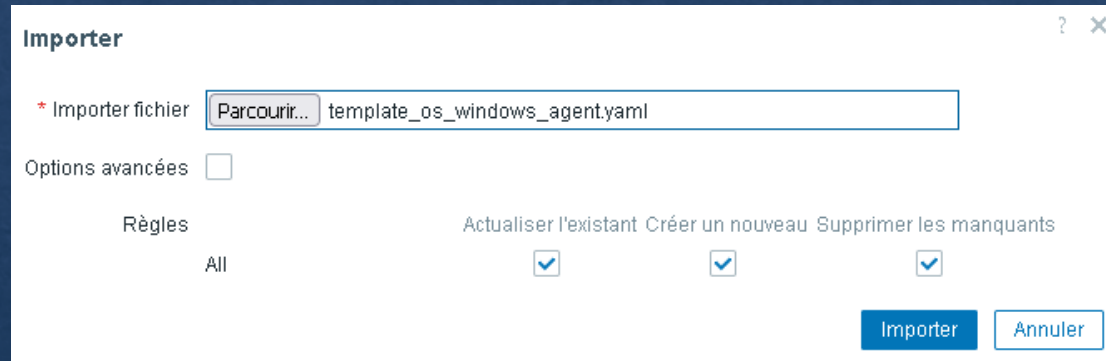
Back Next Cancel

On installe le client Zabbix sur notre AD.  
Il faut y renseigner l'IP du serveur Zabbix ainsi que le port d'écoute.



# Etape 4 – Mise en place

Comme pour pfSense, j'ai directement importé un Template depuis le site officiel Zabbix.



Importer

\* Importer fichier

Options avancées ☐

Règles

All ☒ Actualiser l'existant ☒ Créer un nouveau ☒ Supprimer les manquants ☒

```
templates:
- uuid: 13b06904a6bf41cbb795e3193d896340
  template: 'Windows by Zabbix agent'
  name: 'Windows by Zabbix agent'
  description: |
    This is an official Windows template. It requires Zabbix agent 7.0 or newer.
```

On peut éditer le fichier pour voir comment se nomme le Template afin de le retrouver par la suite.

# Etape 4 – Mise en place

## Hôte

[Hôte](#) [IPMI](#) [Tags](#) [Macros](#) [Inventaire](#) [Chiffrement](#) [Table de correspondance](#)

\* Nom de l'hôte

Active Directory

Nom visible

AD

Modèles

Windows by Zabbix agent x  
taper ici pour rechercher

Sélectionner

\* Groupes d'hôtes

Windows Serveurs x  
taper ici pour rechercher

Sélectionner

Interfaces	Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent		100.10.1.1		<div>IP DNS</div>	10050	<div><input checked="" type="radio"/> Supprimer</div>

Ajouter

Description

Surveillé par

Serveur

Proxy

Groupe de proxy

Activé

☒

Actualiser

Clone

Supprimer

Annuler

Comme pour les autres : Un nom identifiable, le modèles importer ainsi que le groupe et enfin le mode « agent » et l'IP du serveur windows.



# Etape 4 – Tests

<input type="checkbox"/> Nom ▲	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modèles	État	Disponibilité
<input type="checkbox"/> AD	Éléments 116	Déclencheurs 82	Graphiques 12	Découverte 4	Web	100.10.1.1:10050		Windows by Zabbix agent	Activé	ZBX
<input type="checkbox"/> nextcloud	Éléments 23	Déclencheurs 2	Graphiques 3	Découverte 2	Web	192.168.18.1:10050		Apache by Zabbix agent	Activé	ZBX
<input type="checkbox"/> pfsense	Éléments 252	Déclencheurs 61	Graphiques 28	Découverte 1	Web	100.10.1.6:161		PFSense by SNMP	Activé	SNMP
<input type="checkbox"/> Zabbix server	Éléments 161	Déclencheurs 92	Graphiques 20	Découverte 6	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Activé	ZBX

Tout le serveur supervisé fonctionne.



# Etape 5 – Borne wifi



# Etape 5 – Mise en place

Pour débiter la mise en place de la borne wifi, nous allons commencer par la relier au réseaux LAN. Pour ma part j'ai créé un réseaux LAN WIFI distinct du réseaux LAN mais combiner les deux en un fonctionnent très bien.

J'ai rajouté une interface en bridge, fait la configuration de base sur pfsense comme pour le LAN, ajout d'une plage DHCP, règles de filtrages de base etc...

WAN (wan)	-> em0	-> v4/DHCP4: 172.16.5.111/16
LAN (lan)	-> em1	-> v4: 192.168.90.126/25
DMZ (opt1)	-> em2	-> v4: 192.168.18.6/29
SERVEURS (opt2)	-> em3	-> v4: 100.10.1.6/29
WIFI (opt3)	-> em4	-> v4: 192.168.91.254/24

# Etape 5 – Mise en place

Sur l'interface graphique, j'ai mis la borne en IP fixe avec l'AD comme DNS afin qu'il puisse contacter le server pour l'authentification radius.

The screenshot shows the 'Management' tab selected in the top navigation bar. Under the 'Management' tab, the 'Network' sub-tab is active. The 'IP Settings' section is displayed, showing options for 'Dynamic' and 'Static' IP configuration. The 'Static' option is selected. The following fields are filled in:

Field	Value
IP Address:	192.168.91.250
IP Mask:	255.255.255.0
Gateway:	192.168.91.254
Primary DNS:	100.10.1.1
Secondary DNS:	100.10.1.1 (Optional)

A 'Save' button is located at the bottom left of the form.



# Etape 5 – Mise en place

Du côté configuration de base j'ai donné un nom à la bonne puis j'ai retiré le mode de sécurité pour ne laisser que le portail captif.

The screenshot displays the 'Wireless' configuration page. At the top, there are tabs for 'Status', 'Wireless' (selected), 'Management', and 'System'. Below these, a sub-menu includes 'Wireless Settings' (selected), 'Portal', 'VLAN', 'MAC Filtering', 'Scheduler', 'QoS', and 'Rogue AP Detection'. The main section is titled '2.4GHz SSIDs' and features a '+ Add' button. A table lists the configured SSIDs:

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
1	Projet SIO-Formation (NDA)	0	Enable	None	Disable	

Below the table, a configuration modal is open for the first SSID. It contains the following fields:

- SSID:** A text field containing 'Projet SIO-Formation (ND/
- SSID Broadcast:** A checkbox labeled 'Enable' which is checked.
- Security Mode:** A dropdown menu currently set to 'None'.
- Guest Network:** A checkbox labeled 'Enable' which is unchecked, accompanied by an information icon.
- Rate Limit:** A checkbox labeled 'Enable' which is unchecked.

At the bottom of the modal are 'OK' and 'Cancel' buttons.

# Etape 5 – Mise en place

Enfin, la mise en place du portail captif.

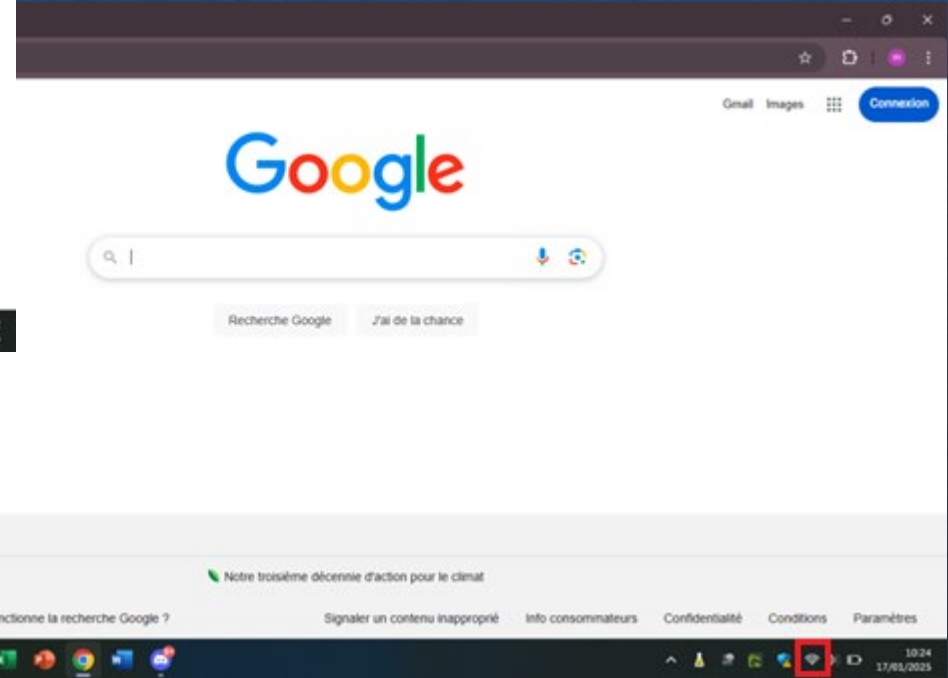
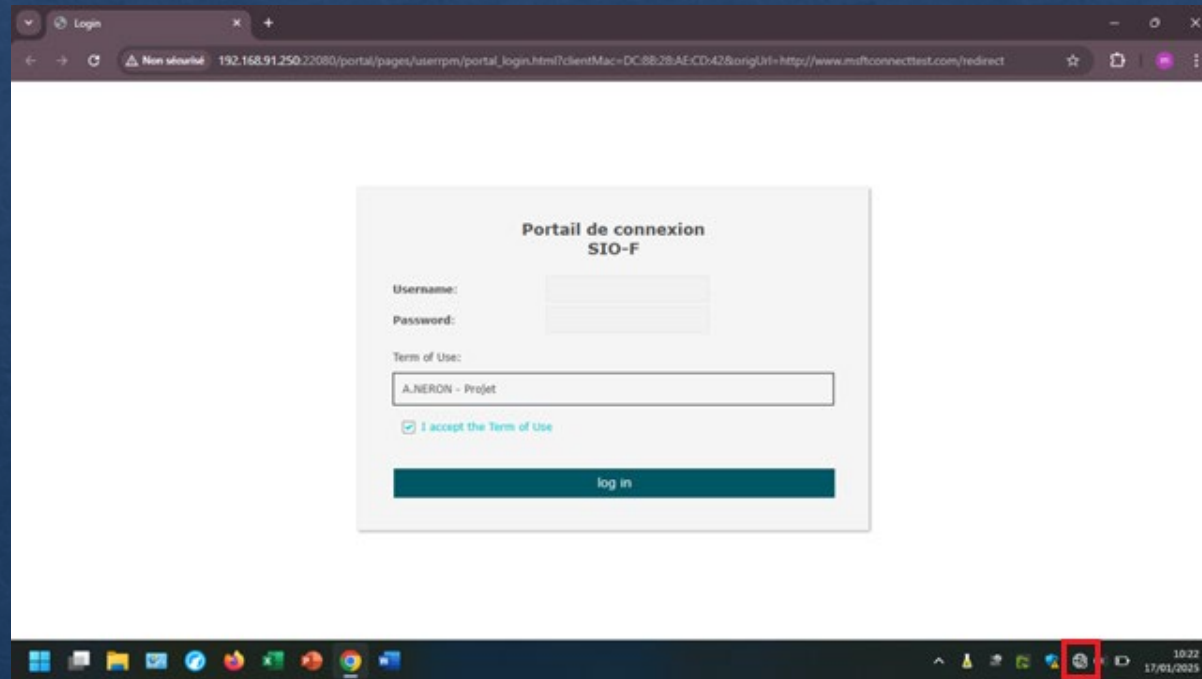
Status	Wireless	Management
Wireless Settings	<b>Portal</b>	VLAN
	MAC Filtering	Scheduler

### Portal Configuration

SSID:	Projet SIO-Formation (NDA) ▼
Authentication Type:	External RADIUS Server ▼
RADIUS Server IP:	100.10.1.1
RADIUS Port:	1812 (1-65535)
RADIUS Password:	toto



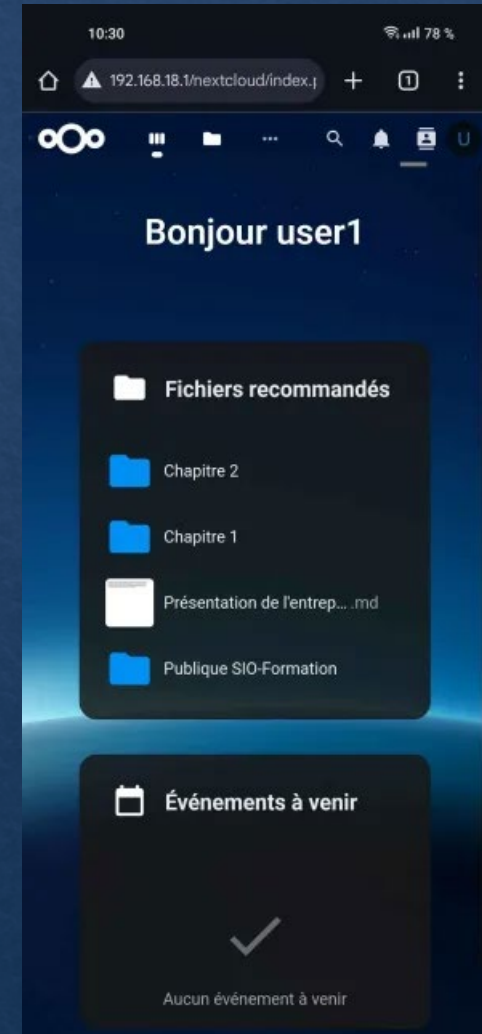
# Etape 5 – Test – pc portable



# Etape 5 – Tests - smartphone



Sur téléphone on est redirigé directement sur la page de connexion du portail captif. L'accès aux ressources du cloud sont accessible sans soucis !



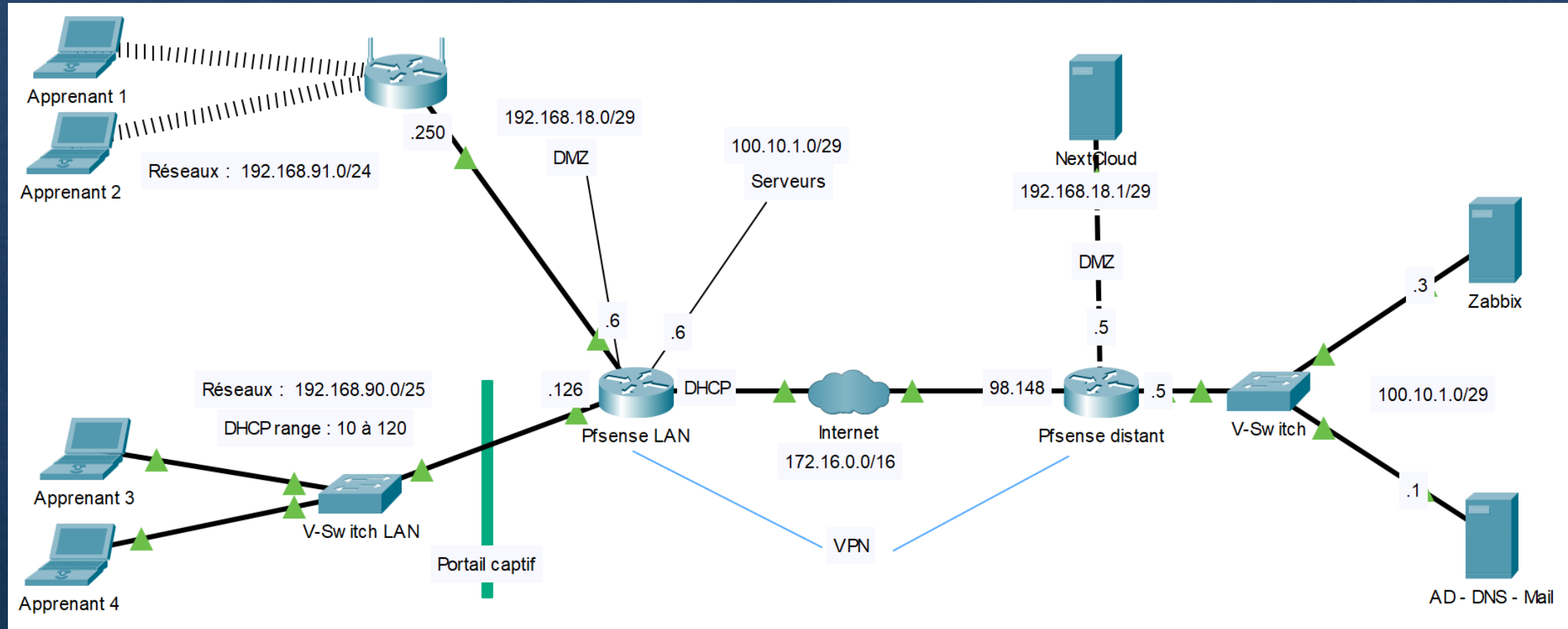


# Etape 6 – VPN

The logo for OpenVPN, featuring the word "OPEN" in orange and "VPN" in blue, with a registered trademark symbol (®) to the upper right of the "N".

OPENVPN®







# Etape 6 – Schéma réseaux











# Etape 6 – Mise en place

## PfSense Distant (Serveur VPN)

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TAP)	10.10.10.0/24	<b>Mode:</b> Peer to Peer ( Shared Key ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256	VPN DMZ	  
WAN	UDP4 / 1195 (TAP)	10.9.9.0/24	<b>Mode:</b> Peer to Peer ( Shared Key ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256	VPN SERVEUR	  

## PfSense Local (Client VPN)

OpenVPN Clients					
Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	UDP4 (TAP)	172.16.98.148:1194	<b>Mode:</b> Peer to Peer ( Shared Key ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256	VPN DMZ	  
WAN	UDP4 (TAP)	172.16.98.148:1195	<b>Mode:</b> Peer to Peer ( Shared Key ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256	VPN SERVEUR	  

# Etape 6 – Mise en place

## Configuration VPN Serveur

Mode Configuration	
<b><u>Server mode</u></b>	Peer to Peer ( Shared Key ) ▼
<b>WARNING:</b> OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.	
<b><u>Device mode</u></b>	tap - Layer 2 Tap Mode ▼
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)	
Endpoint Configuration	
<b><u>Protocol</u></b>	UDP on IPv4 only ▼
<b><u>Interface</u></b>	WAN ▼
The interface or Virtual IP address where OpenVPN will receive client connections.	
<b><u>Local port</u></b>	1194
The port used by OpenVPN to receive client connections.	



# Etape 6 – Mise en place

**Cryptographic Settings**

**Shared Key**

#  
-----BEGIN OpenVPN Static key V1-----  
35bc69e41b7d2c8304c3875f55ac6582  
ccdff11f684eb4305ac18e8124216991  
8dd4ac8a66b2c258cfd8aaff54013be4

Paste the shared key here

La clé à copier coller dans le client associé.

L'IP virtuelle doit être différente sur les deux tunnels.

**Tunnel Settings**

**IPv4 Tunnel Network**

10.10.10.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

# Etape 6 – Mise en place

## Configuration VPN Client

Endpoint Configuration	
<u>Protocol</u>	UDP on IPv4 only
<u>Interface</u>	WAN
	The interface used by the firewall to originate this OpenVPN client connection
<u>Local port</u>	
	Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
<u>Server host or address</u>	172.16.98.148
	The IP address or hostname of the OpenVPN server.
<u>Server port</u>	1194
	The port used by the server to receive client connections.



# Etape 6 – Mise en place

**Cryptographic Settings**

Peer Certificate Authority No Certificate Authorities defined. One may be created here: [System > Cert. Manager](#)

**Auto generate** ☐ Automatically generate a shared key

Shared Key

```
-----BEGIN OpenVPN Static key V1-----  
35bc69e41b7d2c8304c3875f55ac6582  
ccdff11f684eb4305ac18e8124216991  
8dd4ac8a66b2c258cfd8aaff54013be4  
793150ecfde29ac46756c0914524b509
```

**Coller la clé ici**

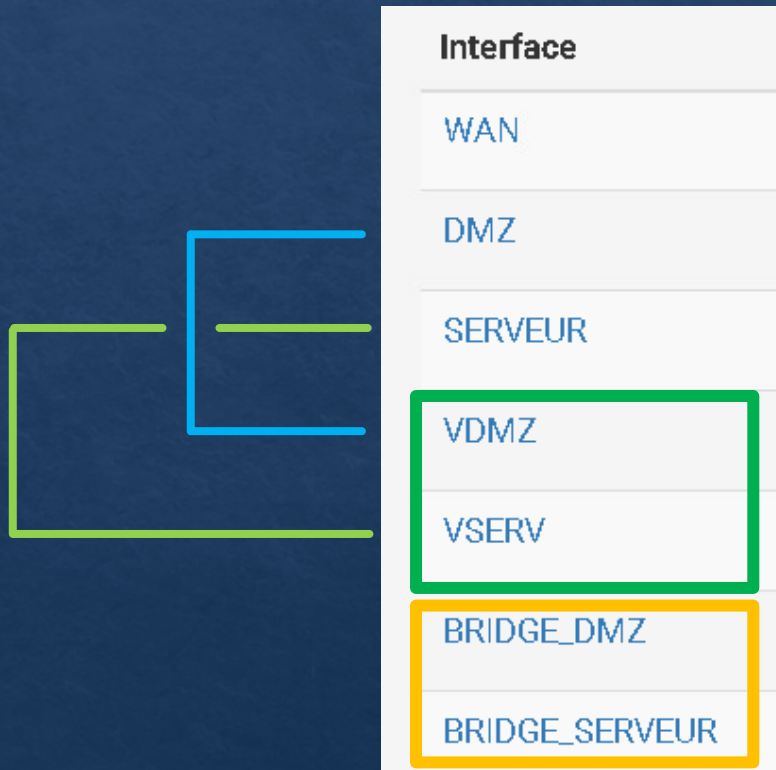
Paste the shared key here

Le reste des paramètres sont identiques à celui du serveur.

# Etape 6 – Mise en place

Une fois le VPN créé, il faut activer toutes les nouvelles interfaces ainsi que modifier les règles du pare-feu.

A réaliser sur les deux routeurs.



$\text{Bridge\_DMZ} = \text{DMZ} + \text{vDMZ}$

$\text{Bridge\_SERVEUR} = \text{SERVEUR} + \text{vSERV}$







Les deux nouvelles interfaces à activer.

Les deux bridges à créer et à activer par la suite.



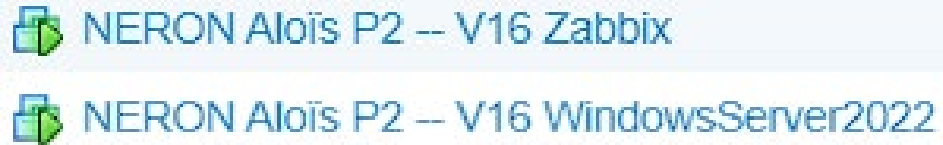
# Etape 6 – Mise en place

Pour le firewall, il faut au minimum mettre la règle par défaut sur toutes les interface/bridges.  
A réaliser sur les deux routeurs.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/114 KiB	IPv4 *	*	*	*	*	none			     

# Etape 6 – Mise en place







On peut maintenant déplacer tout nos serveurs concernés par le VPN sur le serveur ESXi.











# Etape 6 – Tests

Le VPN est en état de fonctionnement, la migration des serveurs s'est déroulée sans soucis et les clients accèdent toujours aux différents services mis en place.

Peer to Peer Server Instance Statistics							
Name	Status	Last Change	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
ovpns1 VPN DMZ UDP4:1194	Connected (Success)	Fri Jan 31 8:20:38 2025	10.10.10.1	172.16.5.100	228 KiB	322 KiB	  
ovpns2 VPN SERVEUR UDP4:1195	Connected (Success)	Fri Jan 31 8:20:39 2025	10.9.9.1	172.16.5.100	8.89 MiB	47.68 MiB	  

Client Instance Statistics								
Name	Status	Last Change	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
ovpnc1 VPN DMZ UDP4	Connected (Success)	Fri Jan 31 8:20:41 2025	172.16.5.100:51091		172.16.98.148:1194	322 KiB	229 KiB	  
ovpnc2 VPN SERVEUR UDP4	Connected (Success)	Fri Jan 31 8:20:42 2025	172.16.5.100:65315		172.16.98.148:1195	47.73 MiB	8.90 MiB	  

# Références

Etape 2 :

<https://www.youtube.com/watch?v=tFUsGjp1mR8&t=45s>

Etape 3 :

<https://www.youtube.com/watch?v=7loCVnLKmws> – hmail

<https://www.youtube.com/watch?v=u9JeH7lCs9g> – nextcloud

<https://www.youtube.com/watch?v=CXmaO19A4Gk> – nextcloud LDAP

Etape 4 :

<https://www.youtube.com/watch?v=GQX7Aszu9Io>

[https://www.zabbix.com/download\\_agents](https://www.zabbix.com/download_agents)