

-
BTS SIO 2025 Option SISR

Epreuve E6
-
Situation professionnelle 2 – Documentation Technique

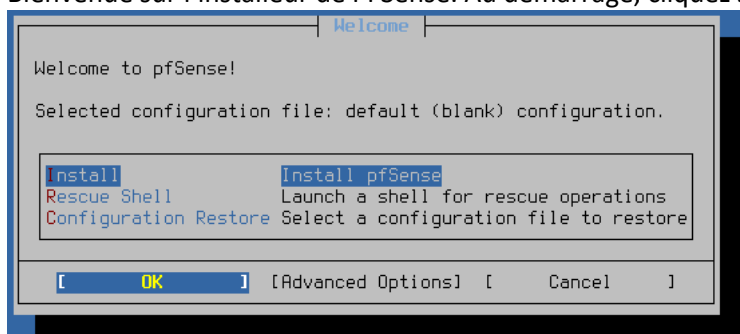
Table des matières

<i>Installation d'un routeur PfSense avec la mise en place d'un VPN Road Warrior.....</i>	3
<i>Installation d'un serveur Windows SERVER 2022 avec les services AD DNS DHCP (avec basculement)...</i>	4
<i>Installation du rôle sur le serveur</i>	5
<i>Configuration du rôle AD avec mise en place d'une forêt.....</i>	5
<i>Configuration du rôle DHCP avec création d'une étendue de test</i>	8
<i>Installation des rôles AD DS et DHCP sur le second serveur.</i>	14
<i>Configuration du basculement DHCP.....</i>	17
<i>Installation d'un serveur de téléphonie VOIP.....</i>	18
<i>Installation d'un serveur de messagerie sur Debian 12</i>	26
<i>Installation d'un serveur web Apache sur Ubuntu 22.04</i>	36
<i>Installation d'un serveur de supervision Centreon</i>	44
<i>Mise en place d'un VPN RoadWarrior OpenVPN.....</i>	46

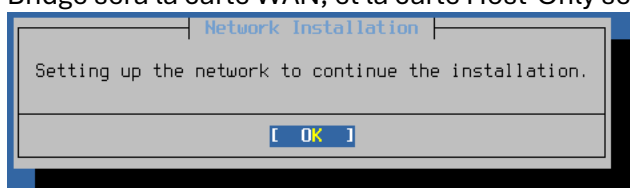
Documentation d'installation

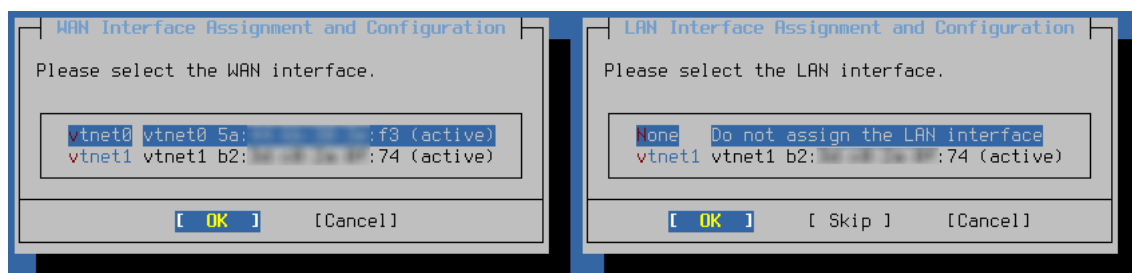
Installation d'un routeur PfSense avec la mise en place d'un VPN Road Warrior

Bienvenue sur l'installateur de PFSense. Au démarrage, cliquez sur Install.



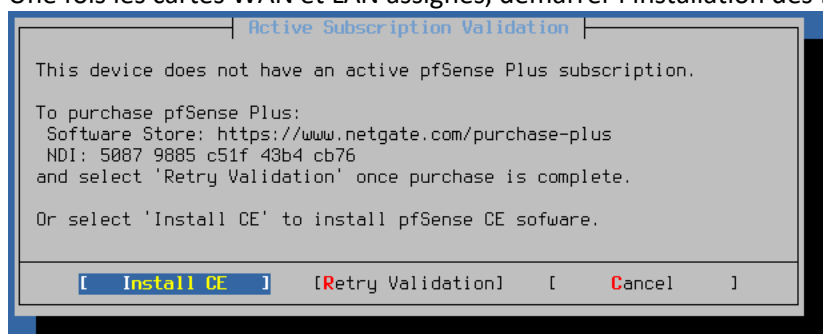
Après avoir démarré l'installation, assigner les interfaces WAN et LAN aux cartes réseaux, la carte Bridge sera la carte WAN, et la carte Host-Only sera la carte LAN.



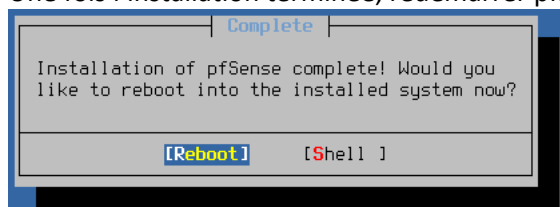


Il est recommandé d'attribuer une adresse IP fixe pour l'adresse LAN, pour éviter les problèmes d'accès à l'interface WEB de pfSense.

Une fois les cartes WAN et LAN assignés, démarrer l'installation des fichiers de pfSense.



Une fois l'installation terminée, redémarrer pfSense, et l'installations sera alors terminée.



Installation d'un serveur Windows SERVER 2022 avec les services AD DNS DHCP (avec basculement)

Prérequis :

- 1 Windows SERVER 2022 avec interface graphique (Carte réseau VMNet1)
- 1 Windows SERVER 2022 Core (Carte réseau VMNet1)
- 1 Routeur (Carte réseau VMNet1, et VMNet2) (optionnel, utilisé dans le cadre du projet M2i)

Description des cartes réseau dans ce cas :

- VMNet 1 : Carte Host-only (réseau LAN)
- VMNet2 : Carte NAT / Bridge (réseau WAN)

Cet exemple utilisera 2 serveurs mentionnés auparavant. Nous passerons par un routeur (PFSense) qui fera office de passerelle entre le réseau local et le réseau WAN. Nous allons voir comment installer les fonctionnalités AD DS, DNS (fonctionnalité obligatoire avec AD DS), ainsi que DHCP. Nous allons également voir comment répliquer tout cela sur le serveur Core pour assurer la disponibilité en cas de panne du serveur 1.

L'installation du rôle DNS ne sera pas mentionnée explicitement car elle est automatiquement installée avec l'Active Directory. Aucune configuration n'est alors requise pour que DNS fonctionne.

Étape 1 : Installation des rôles / fonctionnalités sur le serveur 1 :

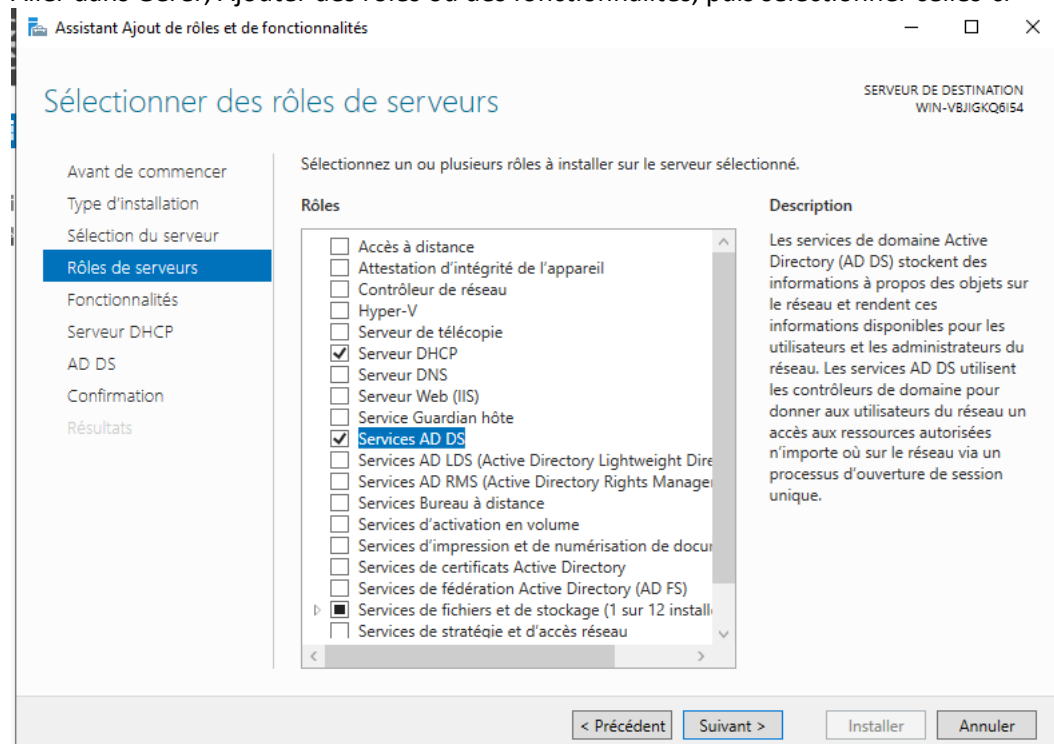
Installation du rôle sur le serveur

Pour commencer, nous allons définir une adresse IP fixe sur le serveur :

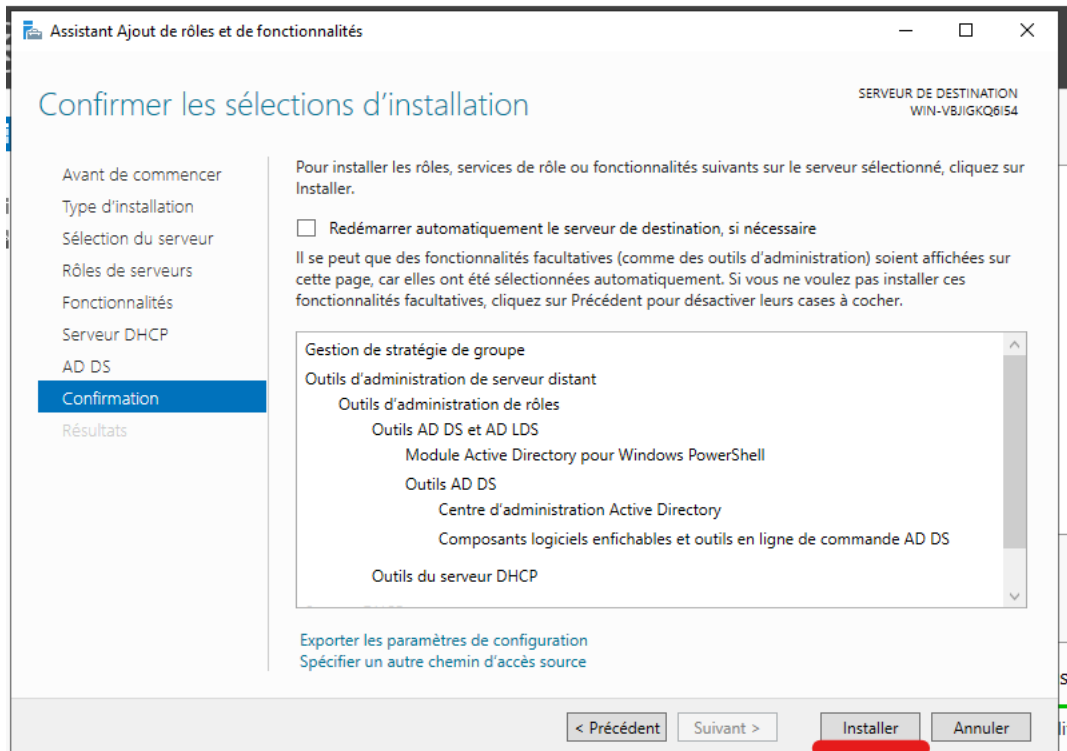
- Aller dans le gestionnaire de serveur sous Serveur Local
- Double cliquer sur Adresse IPv4 attribuée par DHCP
- Cliquer sur sa carte réseau *EthernetX*
- Aller dans les propriétés, puis Protocole Internet version 4
- Dans cette interface il sera alors possible de définir une adresse IP fixe.

Configuration du rôle AD avec mise en place d'une forêt

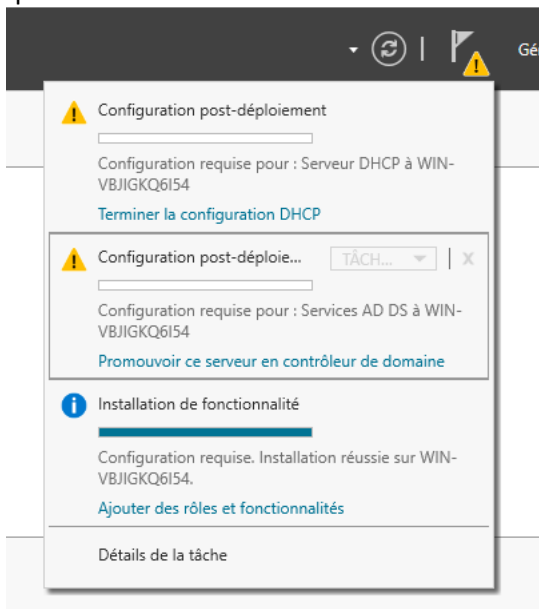
Aller dans Gérer, Ajouter des rôles ou des fonctionnalités, puis sélectionner celles-ci



Lancer l'installation des rôles :



Ensuite, nous allons lancer la création de la forêt Active Directory en cliquant sur Promouvoir ce serveur en tant que contrôleur de domaine :



Nous allons définir le nom du domaine que nous voulons créer.

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
WIN-VBJGKQ6I54

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 :

[En savoir plus sur les configurations de déploiement](#)

< Précédent Suivant > Installer Annuler

Nous allons également définir un mot de passe de restauration des services.

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
WIN-VBJGKQ6I54

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 :

Niveau fonctionnel du domaine :

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 :

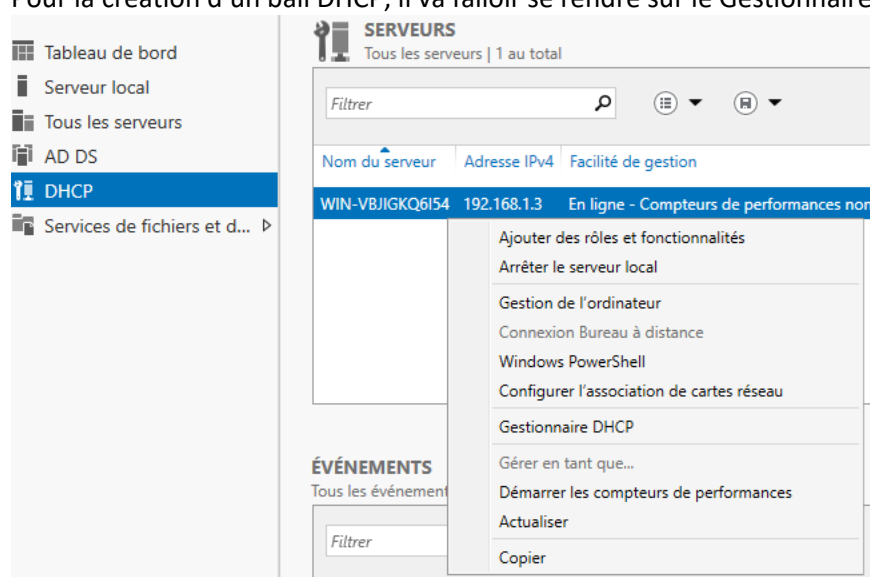
[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

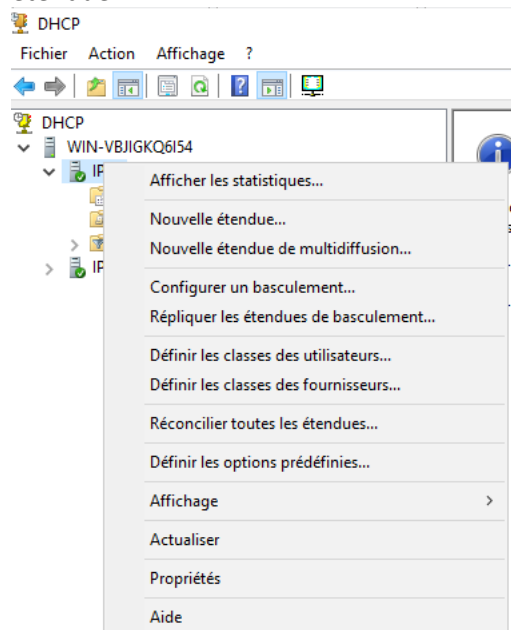
Une fois cela fait, l'AD sera complètement installé, prêt à l'usage.

Configuration du rôle DHCP avec création d'une étendue de test

Pour compléter l'installation de DHCP, il suffira de se rendre dans le drapeau en haut à droite, cliquer sur Terminer la configuration DHCP. Il y aura juste à cliquer sur Suivant pour terminer la configuration. Pour la création d'un bail DHCP, il va falloir se rendre sur le Gestionnaire DHCP :



Une fois dessus, il faudra aller dans : *ServerName/IPv4* puis faire clic droit sur IPv4 pour créer une nouvelle étendue.



Nous allons ensuite la nommer, puis définir une plage d'adresse que l'on souhaite allouer à la plage.

allation d'un serveur DHCP voir l'aide en ligne.

Assistant Nouvelle étendue

Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.



Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

< Précédent Suivant > Annuler

lation d'un serveur DHCP voir l'aide en ligne.

Assistant 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 :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent Suivant > Annuler

Il est également possible de modifier la durée du bail afin que les adresses utilisées puissent être reprises et ne restent pas bloqués pendant le temps par défaut (8 jours)

Installation d'un serveur DHCP - voir l'aide en ligne.

Assistant Nouvelle étendue

Durée du bail
La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

< Précédent **Suivant >** Annuler

A la fin, il faudra alors activer l'étendue, et tout sera prêt à la connexion d'un potentiel client.

Installation d'un serveur DHCP - voir l'aide en ligne.

Assistant Nouvelle étendue

Activer l'étendue
Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.

Voulez-vous activer cette étendue maintenant ?

☒ Oui, je veux activer cette étendue maintenant

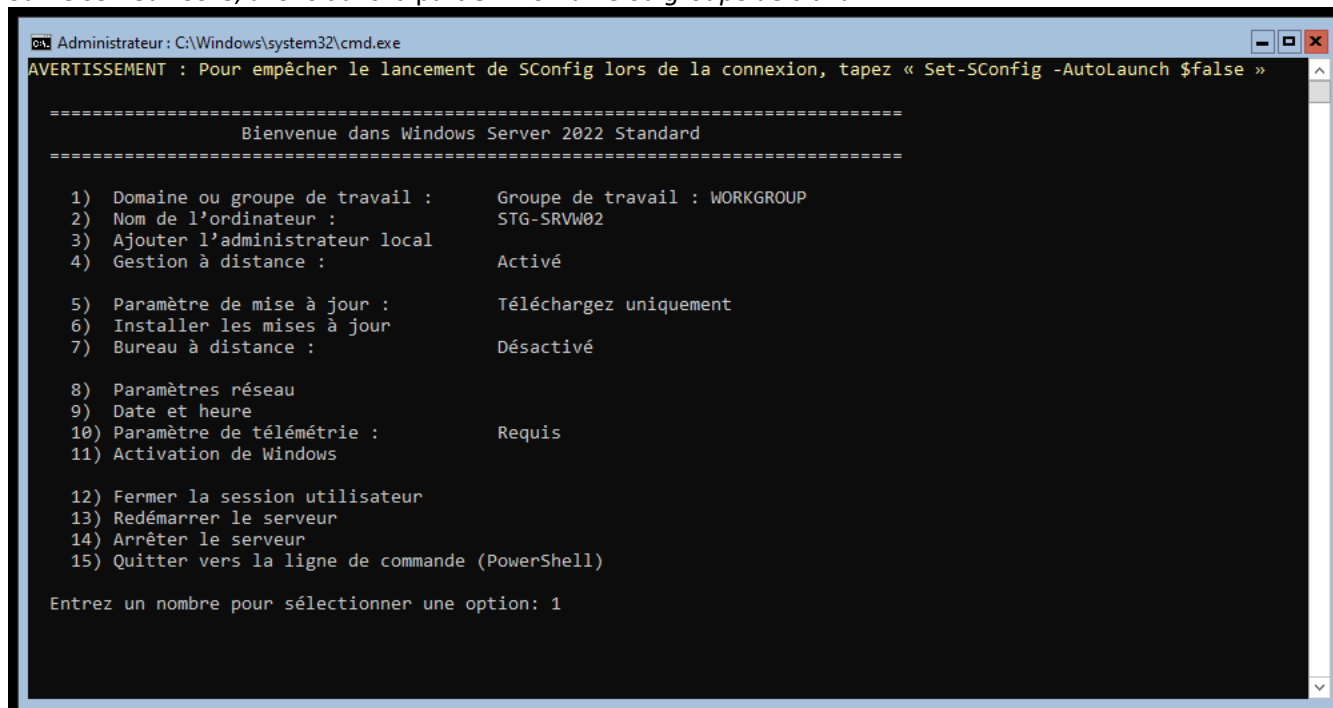
☐ Non, j'activerai cette étendue ultérieurement

< Précédent **Suivant >** Annuler

Contenu du serveur DHCP	État	Description	Relation de basculement
Étendue [192.168.1.0] test	** Actif **	test	
Options de serveur			
Stratégies			
Filtres			

Étape 2 : Installation des rôles / fonctionnalités sur le serveur 2 :

Sur le serveur Core, allons dans la partie 1 *Domaine ou groupe de travail*.



```

C:\Windows\system32\cmd.exe
AVERTISSEMENT : Pour empêcher le lancement de SConfig lors de la connexion, tapez « Set-SConfig -AutoLaunch $false »

=====
                    Bienvenue dans Windows Server 2022 Standard
=====

1) Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :              STG-SRVW02
3) Ajouter l'administrateur local
4) Gestion à distance :               Activé

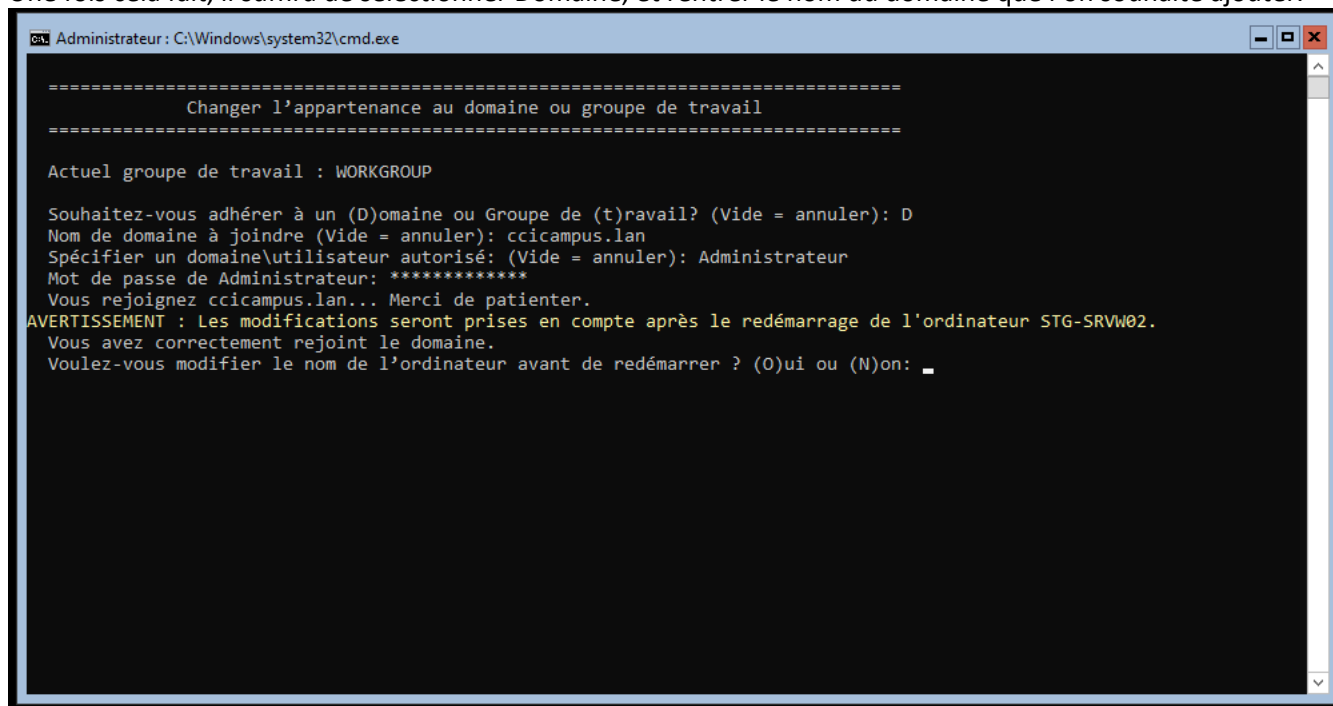
5) Paramètre de mise à jour :          Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :                Désactivé

8) Paramètres réseau
9) Date et heure
10) Paramètre de télémétrie :          Requis
11) Activation de Windows

12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 1
  
```

Une fois cela fait, il suffira de sélectionner *Domaine*, et rentrer le nom du domaine que l'on souhaite ajouter.



```

C:\Windows\system32\cmd.exe

=====
                    Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): ccicampus.lan
Spécifier un domaine\utilisateur autorisé: (Vide = annuler): Administrateur
Mot de passe de Administrateur: *****
Vous rejoignez ccicampus.lan... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur STG-SRVW02.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on: _
  
```

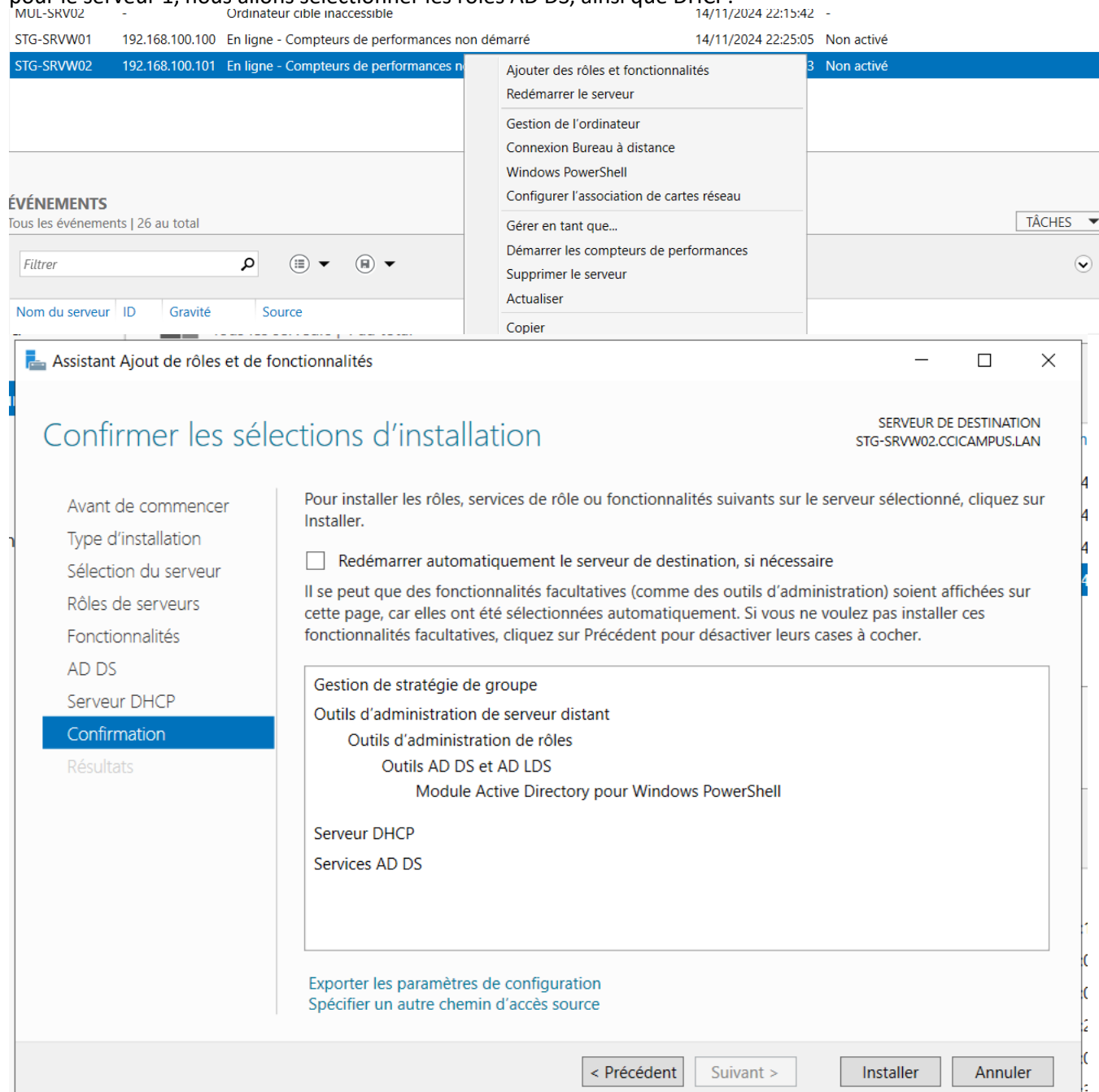
Une fois que le serveur sera dans le domaine, il sera possible de l'administrer depuis le serveur 1, pour cela, nous allons nous rendre dans la section Tous les serveurs du gestionnaire de serveur, puis faire Clic droit dessus, et Ajouter un serveur. Il suffira de rentrer son nom, le sélectionner et ce sera bon.

Nous pourrions alors apercevoir que le serveur apparaît En Ligne.

Filtrer				
Nom du serveur	Adresse IPv4	Facilité de gestion	Dernière mise à jour	Activation de Windows
MUL-SRV01	-	Ordinateur cible inaccessible	14/11/2024 22:15:42	-
MUL-SRV02	-	Ordinateur cible inaccessible	14/11/2024 22:15:42	-
STG-SRVW01	192.168.100.100	En ligne - Compteurs de performances non démarré	14/11/2024 22:15:04	Non activé
STG-SRVW02	192.168.100.101	En ligne - Compteurs de performances non démarré	14/11/2024 22:25:03	Non activé

Installation des rôles AD DS et DHCP sur le second serveur.

Pour commencer, nous allons faire clic droit sur le serveur 2, puis ajouter des rôles ou des fonctionnalités. Comme pour le serveur 1, nous allons sélectionner les rôles AD DS, ainsi que DHCP.



Concernant la configuration du DHCP, elle est identique à celle réalisée auparavant sur le premier serveur.

Pour la configuration de la réplication de l'AD, il faudra se rendre dans le petit drapeau d'information, puis cliquer sur Promouvoir ce serveur en tant que contrôleur de domaine.

Configuration post-déploiement

Configuration requise pour : Services AD DS à STG-SRVW02

[Promouvoir ce serveur en contrôleur de domaine](#)

Configuration post-déploiement

Configuration requise pour : Serveur DHCP à STG-SRVW02

[Terminer la configuration DHCP](#)

Installation de fonctionnalité

Configuration requise. Installation réussie sur STG-SRVW02.CCICAMPUS.LAN.

[Ajouter des rôles et fonctionnalités](#)

Une fois cela fait, nous allons rentrer le domaine déjà existant ici, il faudra également rentrer les informations de connexion du compte Administrateur du domaine.

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVER CIBLE
STG-SRVW02.CCICAMPUS.LAN

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

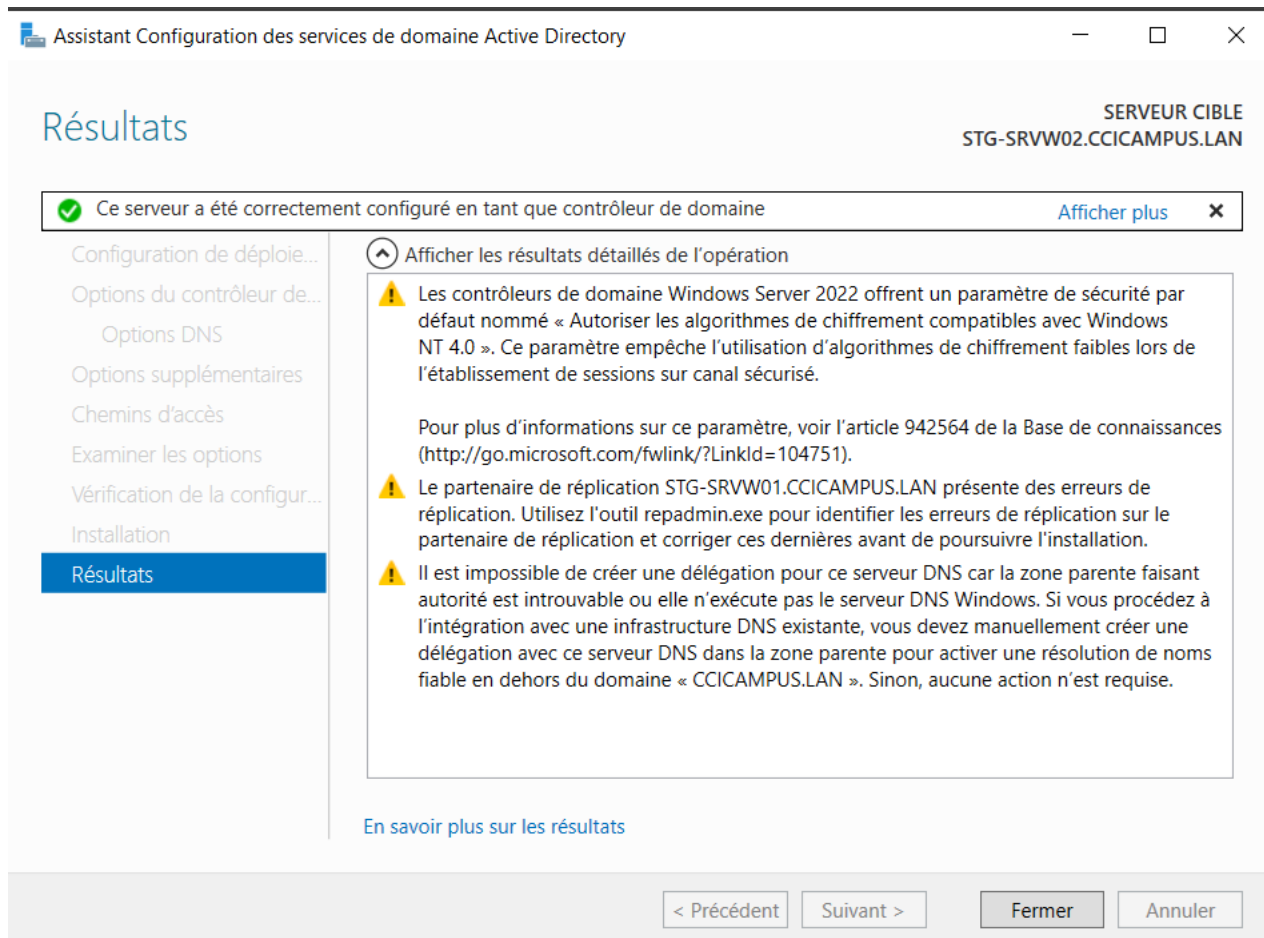
Domaine : [Sélectionner...](#)

Fournir les informations d'identification pour effectuer cette opération

CCICAMPUS\Administrateur [Modifier...](#)

[En savoir plus sur les configurations de déploiement](#)

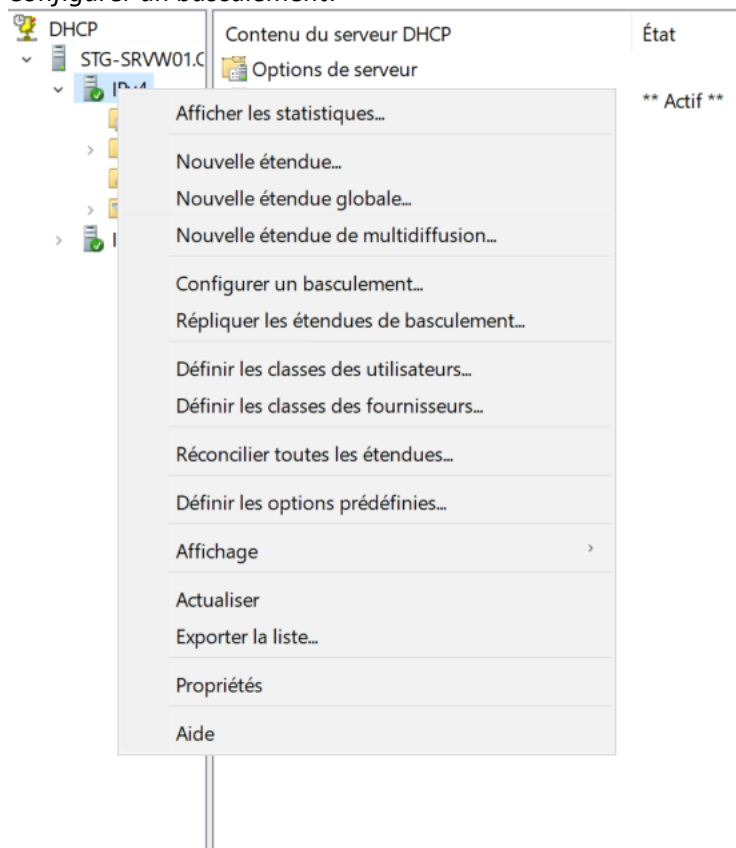
< Précédent Suivant > Installer Annuler



Cette étape nous montre que le serveur est désormais bien contrôleur de domaine secondaire du domaine CCICAMPUS.LAN.

Configuration du basculement DHCP

Nous allons nous rendre sur le gestionnaire DHCP du premier serveur, puis clic droit sur IPv4 pour afficher l'option *Configurer un basculement*.



Une fois dans l'interface, nous allons rentrer les informations du serveur 2 pour définir qui va gérer le basculement, et comment.

Configurer un basculement

Créer une relation de basculement 

Créer une relation de basculement avec le partenaire stg-srvw2

Nom de la relation :

Délai de transition maximal du client (MCLT) : heures minutes

Mode :

Configuration du serveur de secours

Rôle du serveur partenaire :

Adresses réservées pour le serveur de secours : %

☐ Intervalle de basculement d'état : minutes

☒ Activer l'authentification du message

Secret partagé :

< Précédent Suivant > Annuler

Installation d'un serveur de téléphonie VOIP

1. Installation d'Asterisk

Cette section détaille la procédure d'installation d'Asterisk 22.3.0 par **compilation des sources** sur Debian 11. Cette méthode offre une flexibilité optimale pour sélectionner les modules nécessaires à notre environnement VOIP.

Préparation du système

Avant de commencer l'installation, assurez-vous que tous les paquets système sont à jour :

```
root@E-SRV-VOIP:~# sudo apt update && sudo apt upgrade -y
```

Installez ensuite les dépendances requises pour la compilation :

```
root@E-SRV-VOIP:~# sudo apt install -y build-essential wget git curl subversion \
libjansson-dev libxml2-dev libsqlite3-dev uuid-dev
```

Récupérez les sources d'Asterisk depuis le site officiel. Et sur le bouton pour télécharger la dernière version faite cliquer puis « Copier l'adresse du lien ».



Téléchargement de Asterisk

Créez un dossier que vous allez nommer « VOIP »

```
root@E-SRV-VOIP:~/test# mkdir VOIP
```

Puis allez dans le dossier VOIP et collez l'adresse du lien de Asterisk pour le télécharger

```
root@E-SRV-VOIP:~# cd VOIP
root@E-SRV-VOIP:~/VOIP# wget https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-22-current.tar.gz
```

Maintenant il faudra unzip l'archive.

```
root@E-SRV-VOIP:~/VOIP# tar -xvzf asterisk-22-current.tar.gz
```

Configuration de la compilation

Exécutez le script de configuration pour vérifier les dépendances manquantes :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# ./configure
```

Attention : Notez toute dépendance manquante signalée à cette étape et installez-la avant de continuer.

Pour sélectionner les modules à compiler, utilisez l'outil de configuration interactif :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# make menuconfig
```

Dans l'interface qui s'affiche, assurez-vous d'activer les modules suivants, essentiels pour notre configuration VOIP :

- **chan_pjsip** (Canal SIP basé sur PJSIP)
- **res_rtp_asterisk** (Gestion des flux RTP)
- Autres modules de base pour la téléphonie IP

Compilation et installation

Lancez la compilation avec les commandes suivantes :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# make
make install
make samples
make config
```

Cette étape peut prendre plusieurs minutes selon les performances de votre machine.

Vérification de l'installation

Vérifiez que le service Asterisk fonctionne correctement :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# systemctl status asterisk
● asterisk.service - LSB: Asterisk PBX
   Loaded: loaded (/etc/init.d/asterisk; generated)
   Active: active (running) since Thu 2025-04-10 10:59:16 CEST; 43min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 814 ExecStart=/etc/init.d/asterisk start (code=exited, status=0)
    Tasks: 65 (limit: 2264)
   Memory: 122.0M
      CPU: 20.803s
   CGroup: /system.slice/asterisk.service
           └─866 /usr/sbin/asterisk

avril 10 10:59:16 E-SRV-VOIP systemd[1]: Starting LSB: Asterisk PBX...
avril 10 10:59:16 E-SRV-VOIP asterisk[814]: Starting Asterisk PBX: asterisk.
avril 10 10:59:16 E-SRV-VOIP systemd[1]: Started LSB: Asterisk PBX.
lines 1-14/14 (END)
```

Vous devriez voir une sortie indiquant que le service est actif (running).

Paramétrage initial du service

Assurez-vous que le service Asterisk démarre automatiquement au démarrage du système sinon faites les commandes ci-dessous.

```

root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# systemctl enable asterisk

root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# systemctl start asterisk

```

2. Configuration de base

Cette section décrit la configuration initiale d'Asterisk après l'installation pour établir une plateforme VOIP opérationnelle. Nous nous concentrons sur les deux fichiers de configuration essentiels qui nécessitent des modifications pour une première mise en service fonctionnelle.

Emplacement des fichiers de configuration

Les fichiers de configuration d'Asterisk se trouvent dans le répertoire **/etc/asterisk**. Dans notre configuration de base, seuls deux fichiers nécessitent des modifications :

Fichier	Fonction
pjsip.conf	Configuration des comptes SIP et transports
extensions.conf	Plan de numérotation et logique d'appel

Configuration du transport SIP

La première étape consiste à configurer le transport SIP dans le fichier **pjsip.conf**. Cette configuration permet à Asterisk d'écouter les requêtes SIP entrantes.

Ouvrez le fichier avec votre éditeur :

```

root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# nano /etc/asterisk/pjsip.conf

```

Ajoutez la section de transport UDP suivante :

```

[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0:5060

```

L'utilisation de 0.0.0.0 permet d'écouter sur toutes les interfaces réseau. Dans un environnement de production, limitez cette écoute à des interfaces spécifiques pour des raisons de sécurité.

Création des comptes PJSIP

Notre configuration minimale comprend deux comptes SIP (1001 et 1002) pour permettre des tests d'appels entre deux postes téléphoniques. Toujours dans le fichier **pjsip.conf**, ajoutez les sections suivantes :

```
[1001]
type=endpoint
transport=transport-udp
context=internal
disallow=all
allow=ulaw,alaw,g722
auth=auth1001
aors=1001
max_contacts=1

[1001]
type=auth
auth_type=userpass
password=P@ssword10
username=admin1

[1001]
type=aor
max_contacts=1
;contact=sip:1001@192.168.100.30:5060
```

Cette configuration définit pour chaque utilisateur :

- Un **endpoint** : point de terminaison SIP
- Une **authentification** : identifiants de connexion
- Un **AoR** (Address of Record) : gestion de l'enregistrement

Configuration du plan de numérotation

Le plan de numérotation définit le comportement d'Asterisk lorsqu'un numéro est composé. Ouvrez le fichier `extensions.conf` :

```
root@E-SRV-V0IP:/etc/asterisk# nano /etc/asterisk/extensions.conf
root@E-SRV-V0IP:/etc/asterisk# |
```

Ajoutez la configuration suivante pour permettre aux comptes de s'appeler mutuellement :

```
[default]
exten => 1001,1,Answer()
exten => 1001,n,Dial(PJSIP/1001,20)
exten => 1001,n,Hangup()

exten => 1002,1,Answer()
exten => 1002,n,Dial(PJSIP/1002,20)
exten => 1002,n,Hangup()
```

Explication du plan de numérotation

Chaque ligne du plan de numérotation suit la syntaxe :

Exten => numéro,priorité,Application(paramètres)

Application des modifications

Après avoir modifié les fichiers de configuration, rechargez-les dans Asterisk sans redémarrer le service :

```
root@E-SRV-V0IP:~/VOIP/asterisk-22.3.0# asterisk -rx "core reload"
root@E-SRV-V0IP:~/VOIP/asterisk-22.3.0# |
```

Pour vérifier que les configurations sont correctement chargées :


```

root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# asterisk -rx "pjsip show endpoints"

Endpoint: <Endpoint/CID.....> <State.....>
> <Channels.>
  I/OAuth: <AuthId/UserName.....>
.....>
  Aor: <Aor.....> <MaxContact
>
  Contact: <Aor/ContactUri.....> <Hash.....> <Statu
s> <RTT(ms) ..>
  Transport: <TransportId.....> <Type> <cos> <tos> <BindAddress.....>
.....>
  Identify: <Identify/Endpoint.....>
.....>
  Match: <criteria.....>
  Channel: <ChannelId.....> <State.....>
> <Time.....>
  Exten: <DialedExten.....> CLCID: <ConnectedLineCID.....>
=====
=====

Endpoint: 1001                               Unavailable
  0 of inf
    InAuth: 1001/1001
      Aor: 1001                               1

Endpoint: 1002                               Unavailable
  0 of inf
    InAuth: 1002/1002
      Aor: 1002                               1

Objects found: 2

root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#

```

Vous devriez voir les endpoints 1001 et 1002 listés dans la sortie.

Vérification des transports

Vérifiez que le transport SIP est correctement configuré :

```
root@E-SRV-V0IP:~/V0IP/asterisk-22.3.0# asterisk -rx "pjsip show transports"

Transport:  <TransportId.....>  <Type>  <cos>  <tos>  <BindAddress.....>
.....>
=====
=====

Transport:  transport-udp              udp          0          0  0.0.0.0:5060

Objects found: 1

root@E-SRV-V0IP:~/V0IP/asterisk-22.3.0# |
```

Le transport UDP doit apparaître comme actif et en écoute sur l'adresse spécifiée.

3. Tests et validation du système

Configuration du softphone Linphone

Configurez Linphone sur les postes de test avec les paramètres suivants :

UTILISER UN COMPTE SIP

Nom d'utilisateur	Nom d'affichage (optionnel)
1002	
Domaine SIP	
192.168.100.30	
Mot de passe	
.....	
Transport	
UDP ▼	

Une fois cliqué sur enregistrer vous devriez voir l'adresse IP du poste client et le port utilisé. Faites la même manipulation sur un ordinateur différents du même réseau avec le 2^{ème} compte SIP.

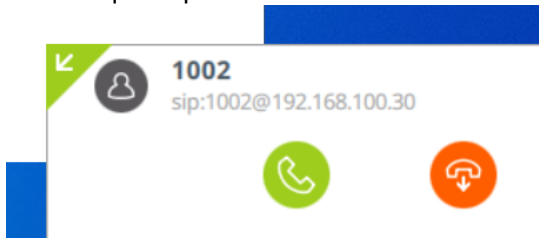
Test d'appel basique

Pour valider la configuration complète, effectuez un appel entre les extensions :

Depuis le poste 1002, composez le 1001



Vérifiez que le poste 1002 sonne

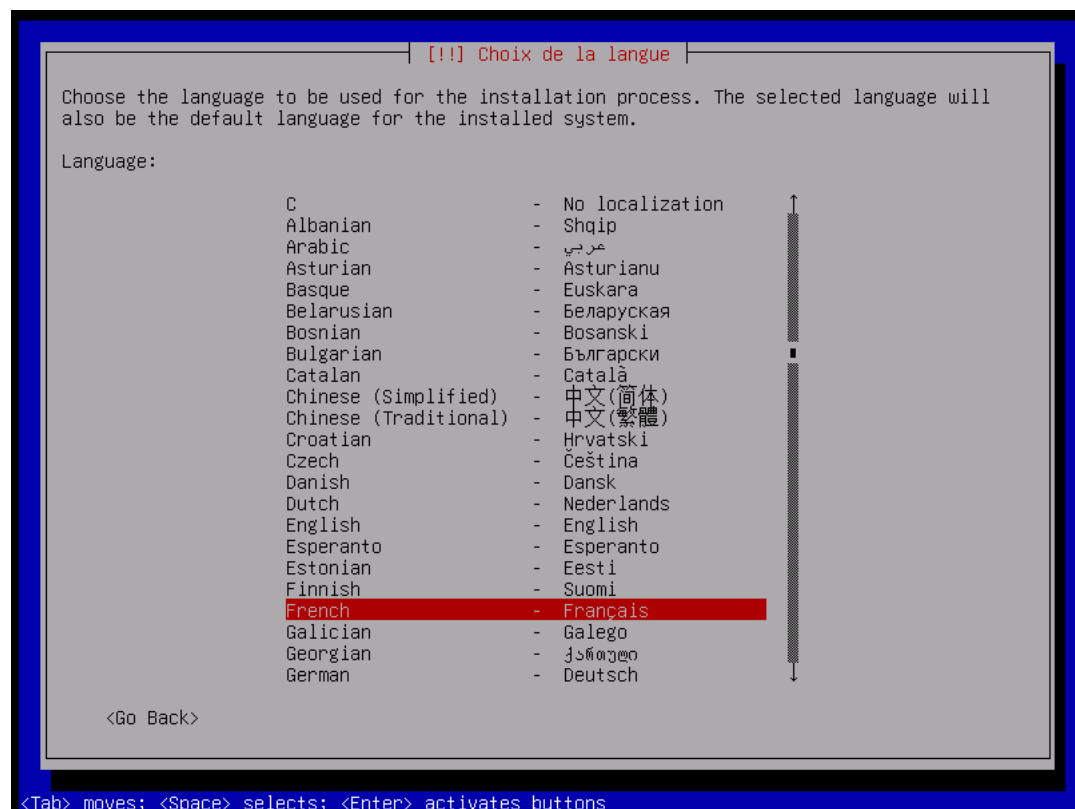


Comme vous pouvez l'apercevoir ci-dessus, je reçois bien l'appelle de 1002. Et en décrochant j'ai bien un retour audio du compte sans latence et bug.

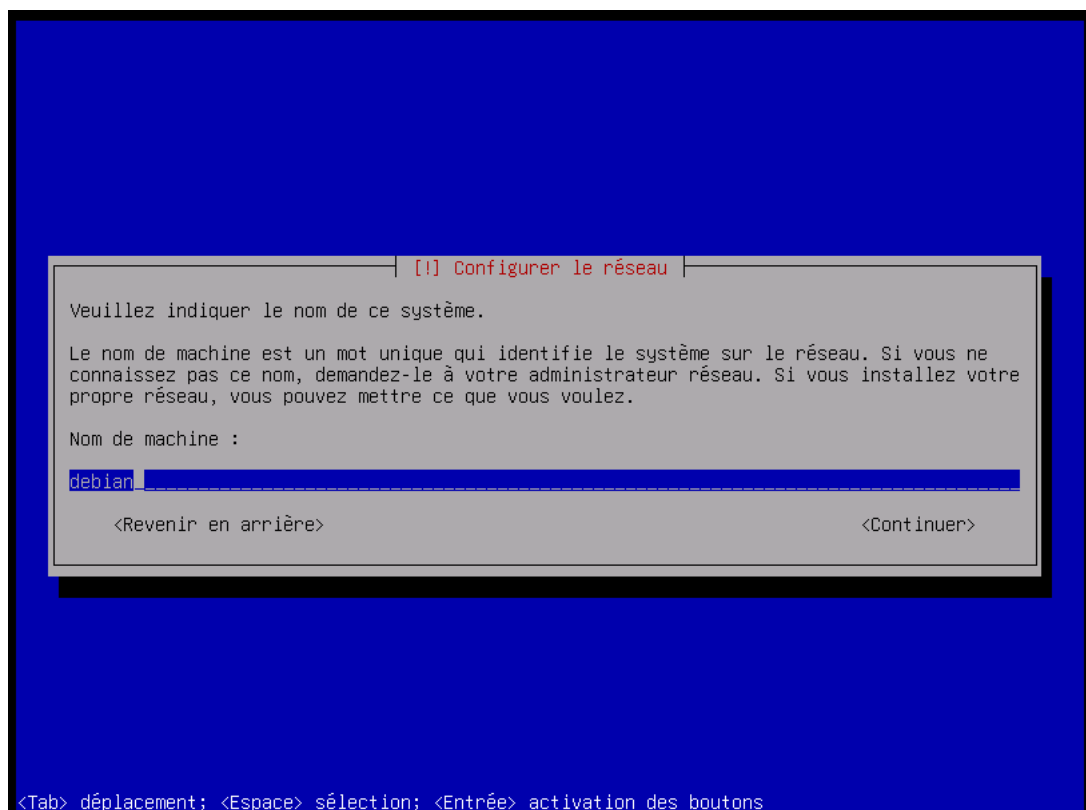
Installation d'un serveur de messagerie sur Debian 12

Partie 1 : Installation de Debian

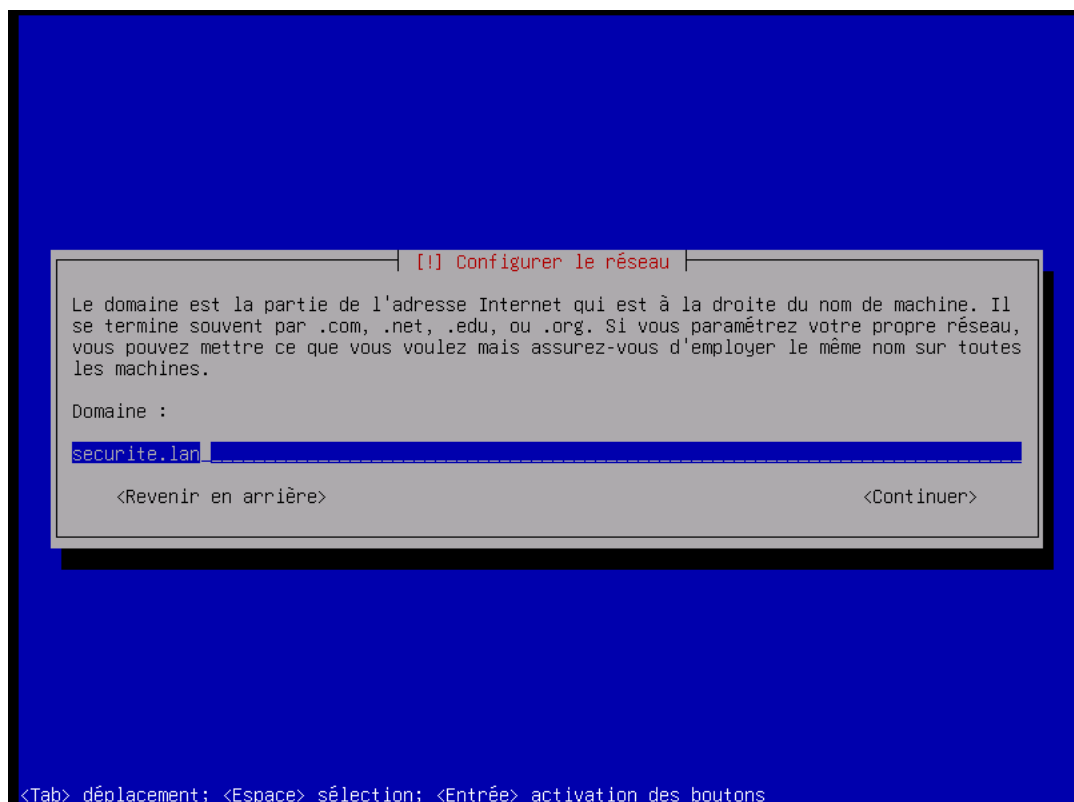
Bienvenue sur l'installateur de Debian 12, pour commencer, choisissez la langue de votre choix :



Ensuite, définissez un nom de machine pour votre serveur Debian.



Vous pouvez, si vous le souhaitez déjà rentrer le nom du domaine à cette étape



Maintenant, nous allons définir un nom d'utilisateur et un mot de passe pour l'utilisateur que l'on va utiliser avec le serveur :

[!!] Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veuillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

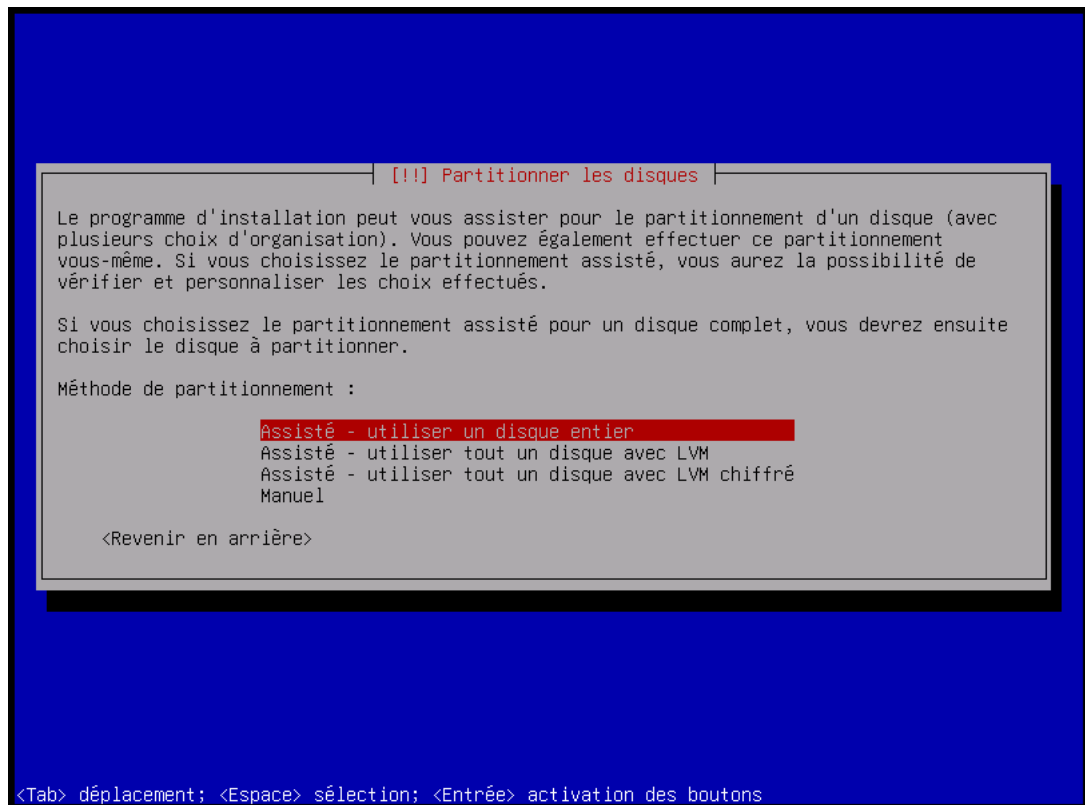
Nom complet du nouvel utilisateur :

admin-mess

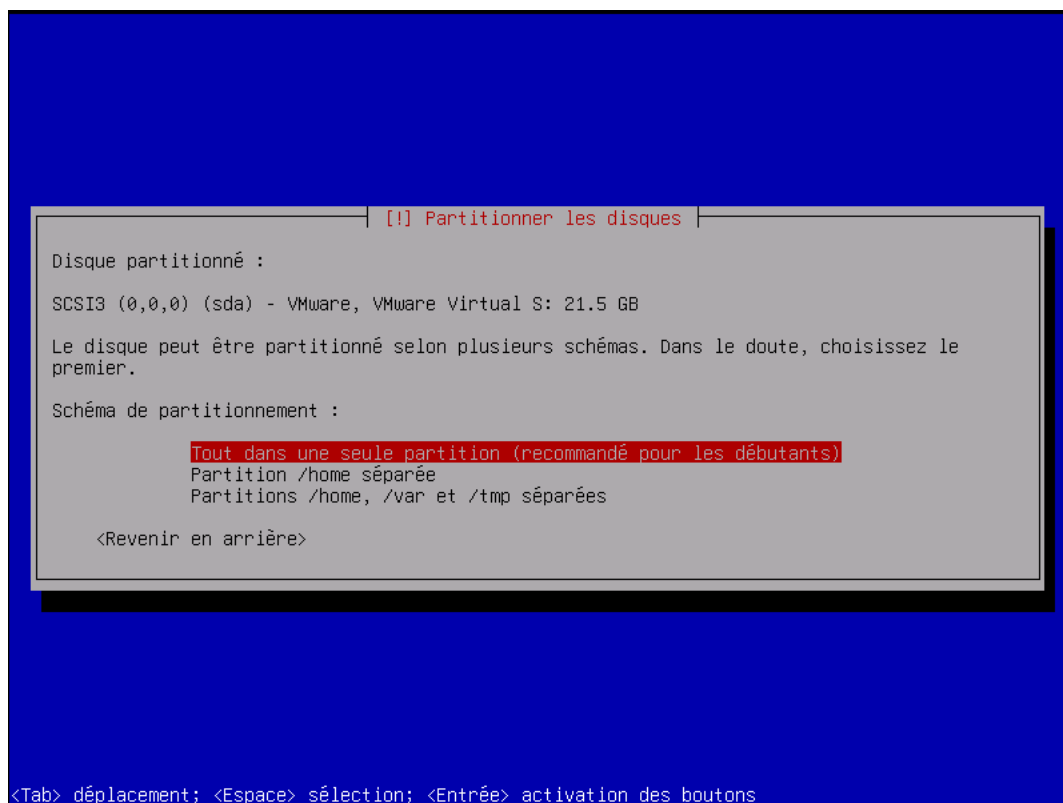
<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

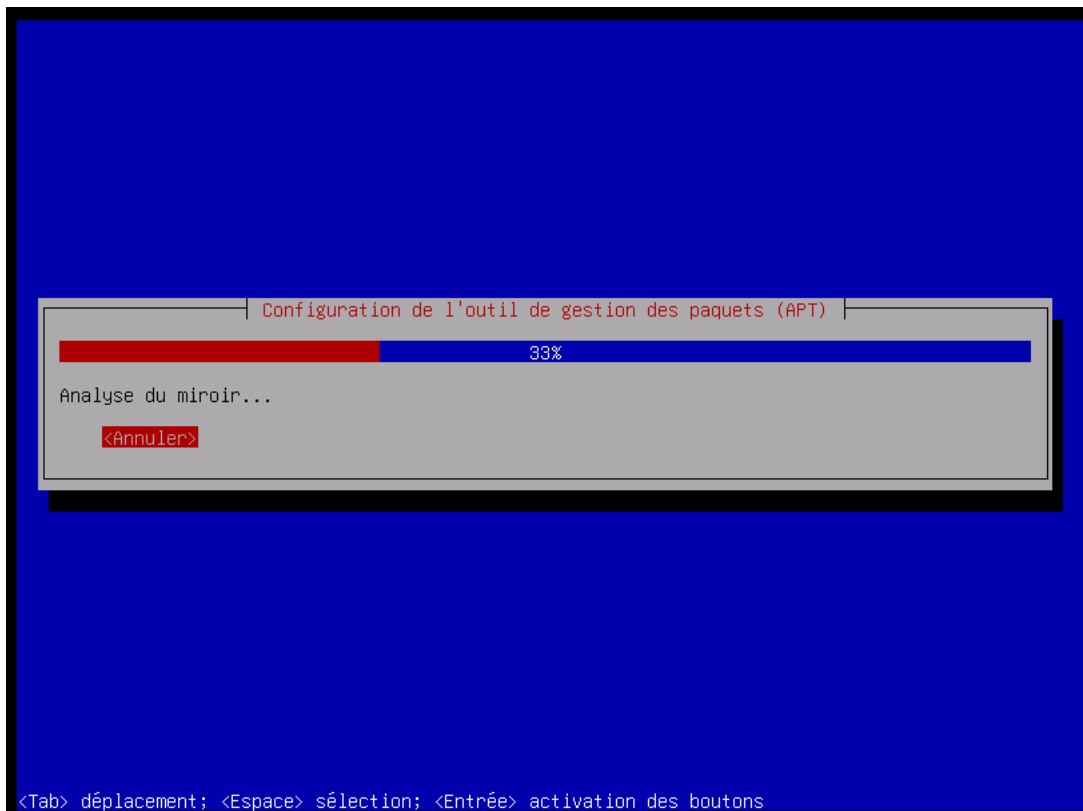
Nous allons continuer avec un disque entier, le partitionnement du disque n'est pas forcément nécessaire pour cet usage.



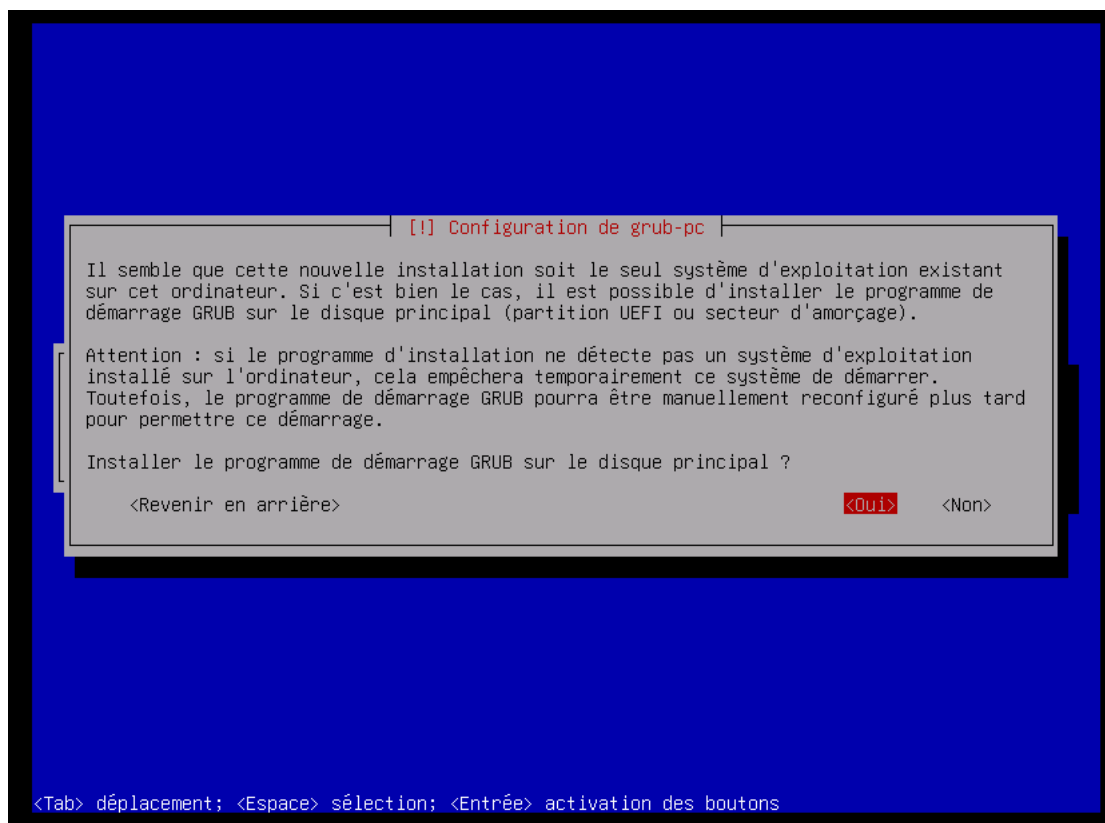
En conséquent, nous allons tout mettre dans la même partition



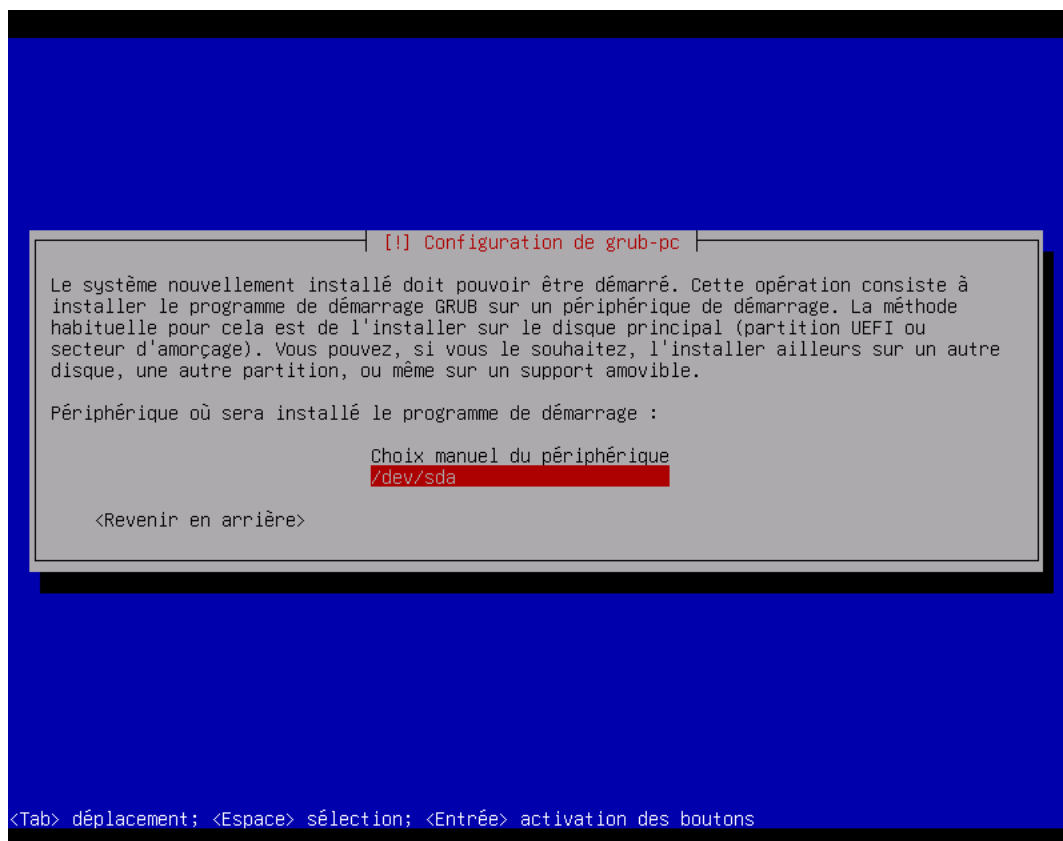
Après avoir appliqué les changements et terminé le partitionnement, comme sur Ubuntu, un test de connexion via un miroir Debian s'effectuera. Après cela, l'installateur va installer les utilitaires de base.



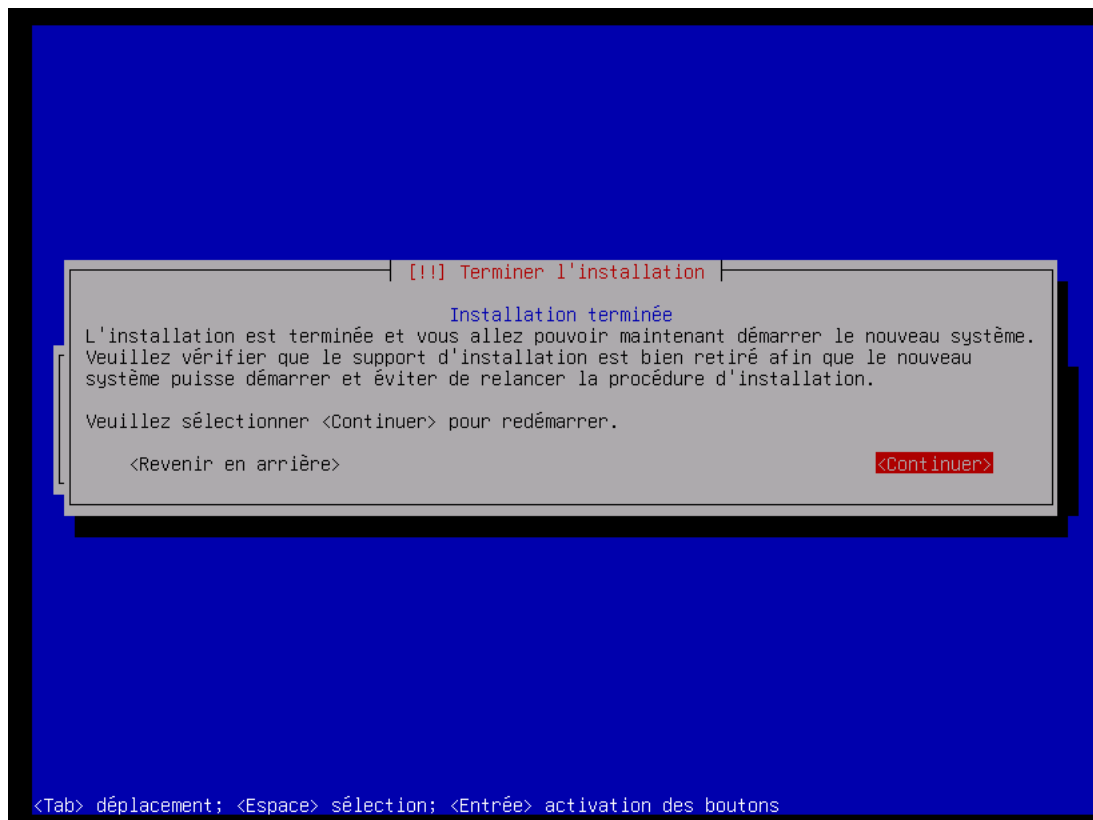
Maintenant, nous allons installer GRUB, ce qui permet d'arriver sur Debian au démarrage de la machine :



Nous allons également lui indiquer ou doit-il démarrer. Le chemin de base ci-dessous :



Debian est désormais installé !



Partie 2 : Installation de Modoboa

Pour commencer, connectons-nous et mettons à jour le système :

```
root@srv-mess:~# apt update
Réception de :1 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Réception de :2 http://deb.debian.org/debian bookworm InRelease [151 kB]
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Réception de :4 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [254 kB]
Réception de :5 http://security.debian.org/debian-security bookworm-security/main Translation-en [150 kB]
Réception de :6 http://security.debian.org/debian-security bookworm-security/contrib amd64 Packages [896 B]
Réception de :7 http://security.debian.org/debian-security bookworm-security/contrib Translation-en [652 B]
Réception de :8 http://security.debian.org/debian-security bookworm-security/non-free-firmware amd64 Packages [688 B]
Réception de :9 http://security.debian.org/debian-security bookworm-security/non-free-firmware Translation-en [472 B]
Réception de :10 http://deb.debian.org/debian bookworm/main amd64 Packages [8 792 kB]
40% [10 Packages 4 699 kB/8 792 kB 53%]
```

Une fois cela fait, nous allons commencer par lier notre serveur Debian au domaine Securite.lan, dans ce cas. Nous allons le définir dans le fichier hosts qui se trouve dans /etc/hosts

```
GNU nano 7.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    srv-mess.securite.lan  srv-mess
```

Maintenant, nous allons installer les paquets nécessaires pour joindre le serveur au domaine :

```
root@srv-mess:~# apt install -y realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin oddjob oddjob-mkhomedir packagekit krb5-user
```

Une fois l'installation terminée, nous allons vérifier si le serveur Debian peut voir le domaine avec la commande suivante :

```
root@srv-mess:~# realm discover securite.lan
securite.lan
  type: kerberos
  realm-name: SECURITE.LAN
  domain-name: securite.lan
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@securite.lan
  login-policy: allow-realm-logins
root@srv-mess:~# _
```

Si cela fonctionne, nous allons alors lier au domaine le serveur avec la commande suivante :

Sudo realm join --user=Administrateur securite.lan

Nous allons maintenant passer à l'installation de modoboa, pour cela, nous allons cloner le dépôt en ligne.

```
admin-mess@srv-mess:~$ git clone https://github.com/modoboa/modoboa-installer
Clonage dans 'modoboa-installer'...
remote: Enumerating objects: 3434, done.
remote: Counting objects: 100% (961/961), done.
remote: Compressing objects: 100% (251/251), done.
remote: Total 3434 (delta 810), reused 790 (delta 703), pack-reused 2473 (from 3)
Réception d'objets: 100% (3434/3434), 695.96 Kio | 3.48 Mio/s, fait.
Résolution des deltas: 100% (2387/2387), fait.
admin-mess@srv-mess:~$
```

Nous allons maintenant rentrer dans le dossier « Modoboa-installer » et nous allons exécuter le script run.py

```
admin-mess@srv-mess:~/modoboa-installer$ sudo ./run.py mail.securite.lan
Welcome to Modoboa installer!

Checking the installer...
Installer seems up to date!
Checks complete

Configuration file installer.cfg not found, creating new one.
Notice:
It is recommended to run this installer on a FRESHLY installed server.
(ie. with nothing special already installed on it)

Warning:
Before you start the installation, please make sure the following DNS records exist for domain 'mail.securite.lan':
  mail IN A    <IP ADDRESS OF YOUR SERVER>
  @ IN MX     mail.mail.securite.lan.

Your mail server will be installed with the following components:
fail2ban modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radicale opendkim
Do you confirm? (Y/n)
```

```
Your mail server will be installed with the following components:
fail2ban modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radicale opendkim
Do you confirm? (Y/n) y
The process can be long, feel free to take a coffee and come back later ;)
Starting...
Generating new certificate using letsencrypt
Installing amavis
Installing spamassassin
Installing razor
Installing clamav
Installing fail2ban
Installing modoboa
Installing automx
Installing radicale
Installing uwsgi
Installing nginx
Installing opendkim
Installing postfix
Installing postwhite
Installing dovecot
User dovecot already exists, skipping creation but please make sure the /srv/vmail directory exists.
Congratulations! You can enjoy Modoboa at https://mail.henrybroadway.com (admin:password)

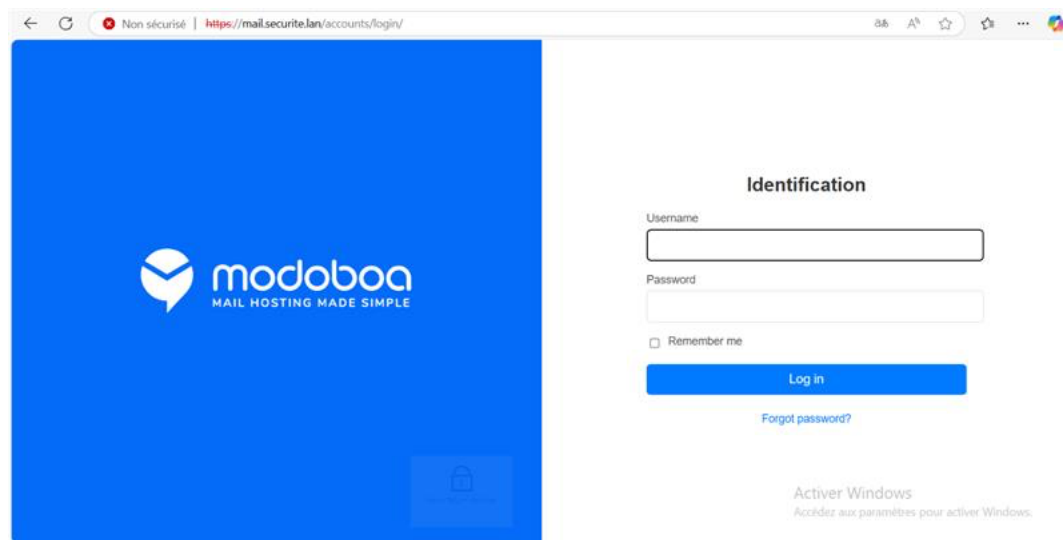
Modoboa is a free software maintained by volunteers.
You like the project and want it to be sustainable?
Then don't wait anymore and go sponsor it here:

https://github.com/sponsors/modoboa

Thank you for your help :-)
```

Une fois l'installation terminée, vous voilà fin prêt pour utiliser votre serveur de messagerie !

Nous allons alors nous rendre sur l'interface web depuis le lien qui nous ait donné ; en l'occurrence mail.securite.lan dans ce cas.



Nous allons rentrer les identifiants de base, donné à la fin de l'installation : admin / password. Il est très important de les modifier juste après ; et de créer un second compte d'administration avec uniquement les droits nécessaires pour éviter toute mauvaise manipulation.

Une fois connecté, vous allez pouvoir ajouter un domaine, en l'occurrence sécurité.lan dans mon cas, veuillez bien faire attention à avoir créé toutes les entrées DNS afin que le lien puisse se faire.

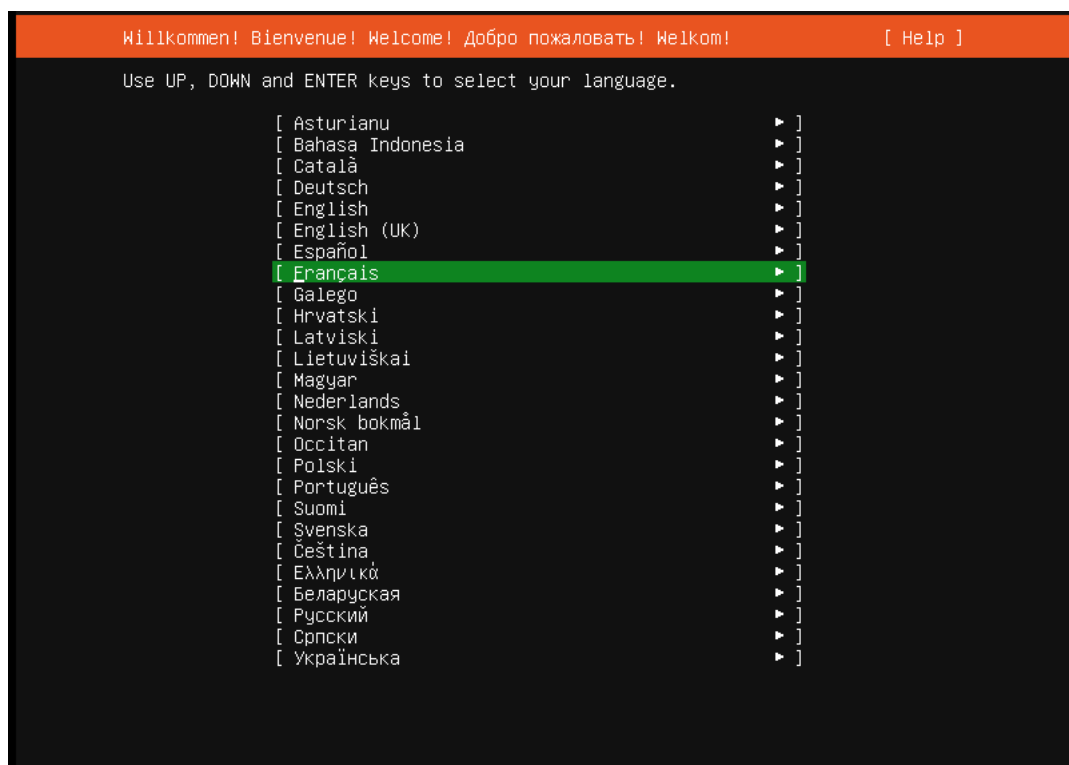
Il est également possible de créer des comptes utilisateurs, pour les différents utilisateurs du domaine. Nous pouvons aussi leur définir des quotas d'envoi de mail.

Une fois un compte créé, nous pouvons alors faire un test en essayant d'envoyer un mail au compte administrateur depuis notre compte test depuis un MUA, Thunderbird est un bon outil.

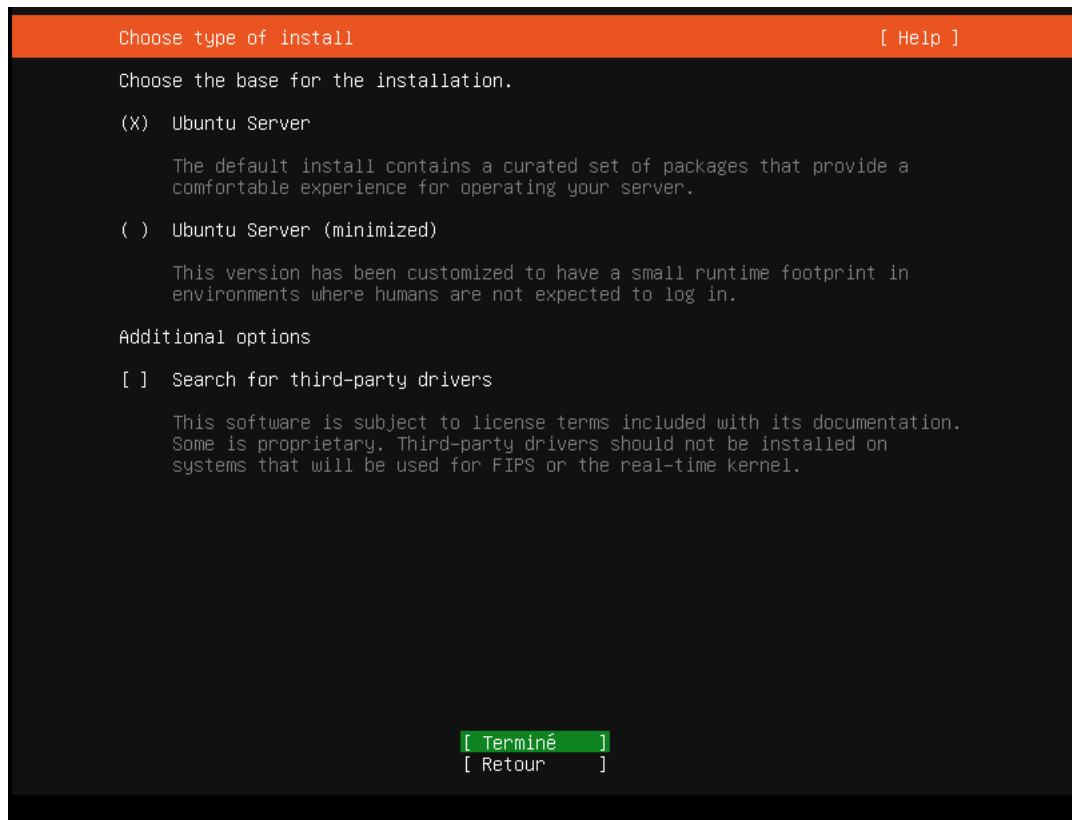
Installation d'un serveur web Apache sur Ubuntu 22.04

Partie 1 : Installation d'Ubuntu 22.04

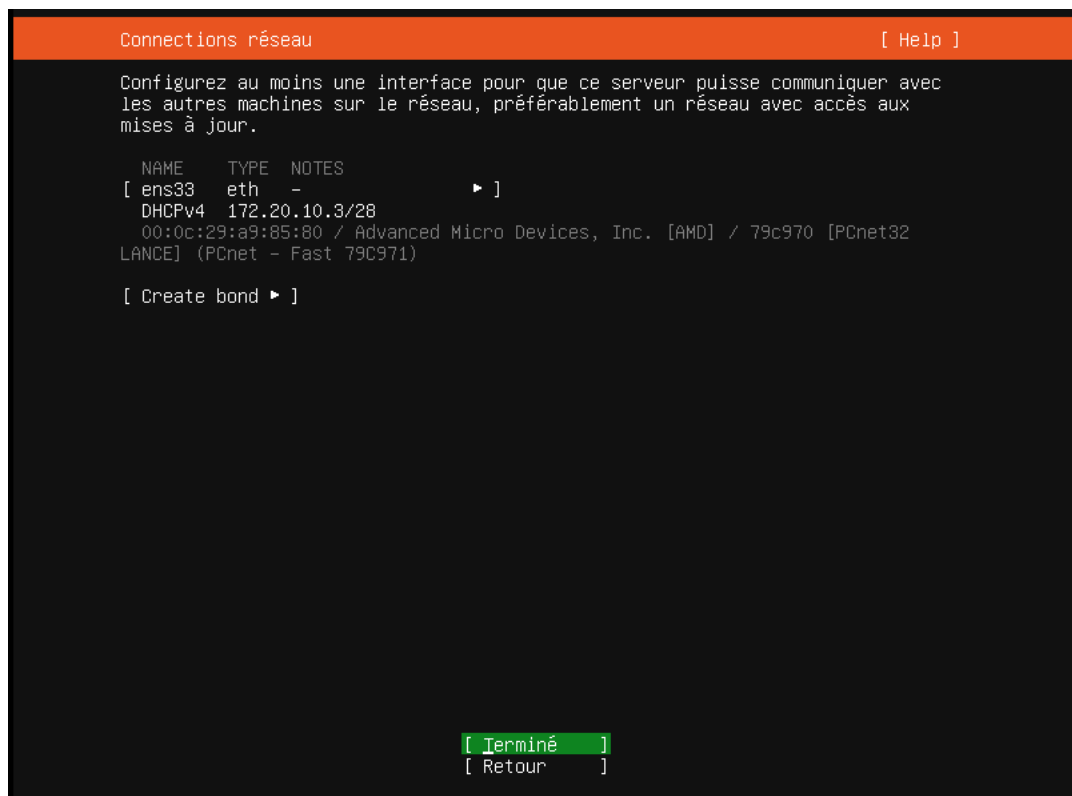
Bienvenue sur l'installateur d'Ubuntu 22.04 ; pour commencer, choisissez la langue du système d'exploitation.



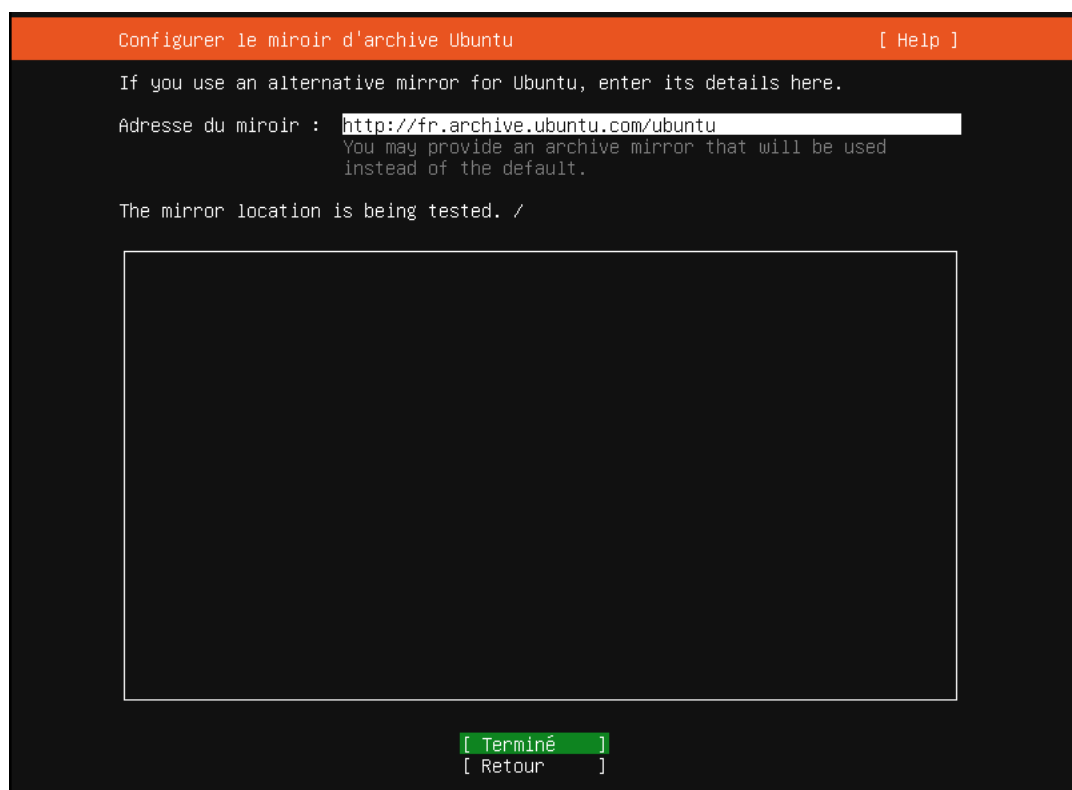
Nous allons choisir la version Ubuntu Server complète, un environnement en ligne de commande un peu plus gourmand que la version (minimized) mais adaptée au besoin.



Nous allons désormais définir les paramètres réseaux du serveur pour lui permettre de récupérer les mises à jour sur les dépôts en ligne



Après les paramètres réseaux définis, un test va être réalisé ce qui va permettre de voir si le serveur a bien un accès vers internet pour récupérer des paquets :



Concernant la taille du disque, un disque de 20Go peut être amplement suffisant, Ubuntu étant basé sur Linux, le système d'exploitation est très léger.

Configuration de stockage guidée

[Help]

Configure a guided storage layout, or create a custom one:

(X) Utiliser un disque entier

[/dev/sda local disk 20.000G ▼]

[X] Set up this disk as an LVM group

[] Encrypt the LVM group with LUKS

Phrase de passe :

Confirmez la phrase de passe :

() Custom storage layout

[Terminé]

[Retour]

Désormais, nous allons définir un utilisateur de base qui va nous servir à nous connecter après la configuration et l'installation de l'OS. Un nom de machine va également être demandé.

Configuration du profil

[Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.

Votre nom : test

Le nom de cette machine: test
The name it uses when it talks to other computers.

Choisir un nom d'utilisateur : test

Choisir un mot de passe : ****

Confirmer votre mot de passe: ****

[Terminé]

Pour une question de pratique, nous pouvons cocher l'option d'installation d'un serveur SSH, le service SSH sera alors installé, et configuré pour faire en sorte que seul l'utilisateur créé auparavant puisse se connecter. Il est également possible d'importer une clé SSH depuis GitHub.

Configuration SSH

[Help]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

[X]

Installer le serveur OpenSSH

Importer une identité SSH:

[Non ▼]

You can import your SSH keys from GitHub or Launchpad.

Importer le nom d'utilisateur :

[X]

Autoriser l'authentification par mot de passe via SSH

[Terminé]

[Retour]

Pour finir, nous allons pouvoir choisir des packages à installer en supplément, suivant l'utilisation du serveur. En l'occurrence, nous n'allons pas en choisir pour installer Apache.


```

Featured Server Snaps [ Help ]

These are popular snaps in server environments. Select or deselect with SPACE,
press ENTER to see more details of the package, publisher and versions
available.

[ ] microk8s      Kubernetes for workstations and appliances ▶
[ ] nextcloud     Nextcloud Server - A safe home for all your data ▶
[ ] wekan         Open-Source kanban ▶
[ ] kata-containers Build lightweight VMs that seamlessly plug into the c ▶
[ ] docker        Docker container runtime ▶
[ ] canonical-livepatch Canonical Livepatch Client ▶
[ ] rocketchat-server Rocket.Chat server ▶
[ ] mosquitto     Eclipse Mosquitto MQTT broker ▶
[ ] etcd          Resilient key-value store by CoreOS ▶
[ ] powershell   PowerShell for every system! ▶
[ ] sabnzbd       SABnzbd ▶
[ ] wormhole      get things from one computer to another, safely ▶
[ ] aws-cli       Universal Command Line Interface for Amazon Web Servi ▶
[ ] google-cloud-sdk Google Cloud SDK ▶
[ ] slcli         Python based SoftLayer API Tool. ▶
[ ] doctl         The official DigitalOcean command line interface ▶
[ ] postgresql10 PostgreSQL is a powerful, open source object-relation ▶
[ ] heroku        CLI client for Heroku ▶
[ ] keepalived    High availability VRRP/BFD and load-balancing for Lin ▶
[ ] prometheus    The Prometheus monitoring system and time series data ▶

[ Terminé ]
[ Retour ]

```

Nous y sommes, le serveur Ubuntu est désormais en train de s'installer. Après l'installation, il suffira de le redémarrer pour arriver à l'interface de connexion.

```

Installation du système [ Help ]

subiquity/Early/apply_autoinstall_config
subiquity/Reporting/apply_autoinstall_config
subiquity/Error/apply_autoinstall_config
subiquity/Userdata/apply_autoinstall_config
subiquity/Package/apply_autoinstall_config
subiquity/Debconf/apply_autoinstall_config
subiquity/Kernel/apply_autoinstall_config
subiquity/2dev/apply_autoinstall_config
subiquity/Ad/apply_autoinstall_config
subiquity/Late/apply_autoinstall_config
configuring apt
  curtin command in-target
installing system
  executing curtin install initial step
  executing curtin install partitioning step -

[ View full log ]

```

Partie 2 : Installation d'Apache sur le serveur Ubuntu 22.04

Pour commencer, connectons-nous avec l'utilisateur que nous avons défini auparavant

```

Ubuntu 22.04.3 LTS test tty1

test login: test
Password: _

```

Avant n'importe quelle installation, il est important de vérifier que le système soit à jour. Il faut donc exécuter la commande suivante qui va rechercher les mises à jour, les télécharger et les appliquer.

```
admin-apache@srv-apache:~$ sudo apt upgrade && sudo apt upgrade
```

Cette opération peut être longue, en fonction du nombre de mises à jour que Ubuntu doit récupérer. Après cette mise à jour, nous allons pouvoir installer Apache2 avec la commande suivante

```

test@test:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 226 not upgraded.
Need to get 2142 kB of archives.
After this operation, 8528 kB of additional disk space will be used.
Do you want to continue? [Y/n] _

```

Après l'installation, nous allons vérifier que l'installation s'est bien déroulée, et que apache est bien démarré :

```

admin-apache@ebrigade:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-04-14 08:01:51 UTC; 17min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 815 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 913 (apache2)
    Tasks: 6 (limit: 4519)
   Memory: 26.0M
      CPU: 387ms
   CGroup: /system.slice/apache2.service
           └─913 /usr/sbin/apache2 -k start
             └─954 /usr/sbin/apache2 -k start
               └─955 /usr/sbin/apache2 -k start
                 └─956 /usr/sbin/apache2 -k start
                   └─957 /usr/sbin/apache2 -k start
                     └─958 /usr/sbin/apache2 -k start

avril 14 08:01:50 ebrigade systemd[1]: Starting The Apache HTTP Server...
avril 14 08:01:51 ebrigade apachectl[877]: AH00558: apache2: Could not reliably determine the serve
avril 14 08:01:51 ebrigade systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)

```

Dans ce cas, apache a le statut 'active', il est donc fonctionnel. Pour afficher ce qui est partagé avec apache, il suffira d'aller sur un navigateur comme Edge, et rentrer <http://AdresseIP/>

Partie 3 : Faire marcher e-brigade sur apache

Pour faire fonctionner e-brigade, nous allons d'abord transférer les fichiers sources via sftp avec FileZilla par exemple.

Une fois cela fait, nous allons définir dans le fichier de configuration d'apache le chemin de la source d'E-brigade :

```
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/ebrigade

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
~
~
~
~
<c:/apache2/sites-available/000-default.conf" [lecture-seule] 31L, 1336B 1,1 Tout
```

Désormais, Apache affichera la page de configuration d'E-brigade sur l'interface web. **ATTENTION, EBRIGADE nécessite une version de php 7.4 ou plus.**

Nous allons maintenant installer mysql, ce qui va permettre d'ajouter une base de données pour ebrigade avec les commandes suivantes :

```
``sudo apt install mysql-server
```

Une fois mysql installé, nous allons nous y connecter avec l'utilisateur root, puis nous allons créer une base de données, un utilisateur spécifique à la base, et nous allons lui mettre les droits sur la base.

CREATE DATABASE database;

CREATE USER 'nom_utilisateur'@'localhost' IDENTIFIED BY 'mot_de_passe';

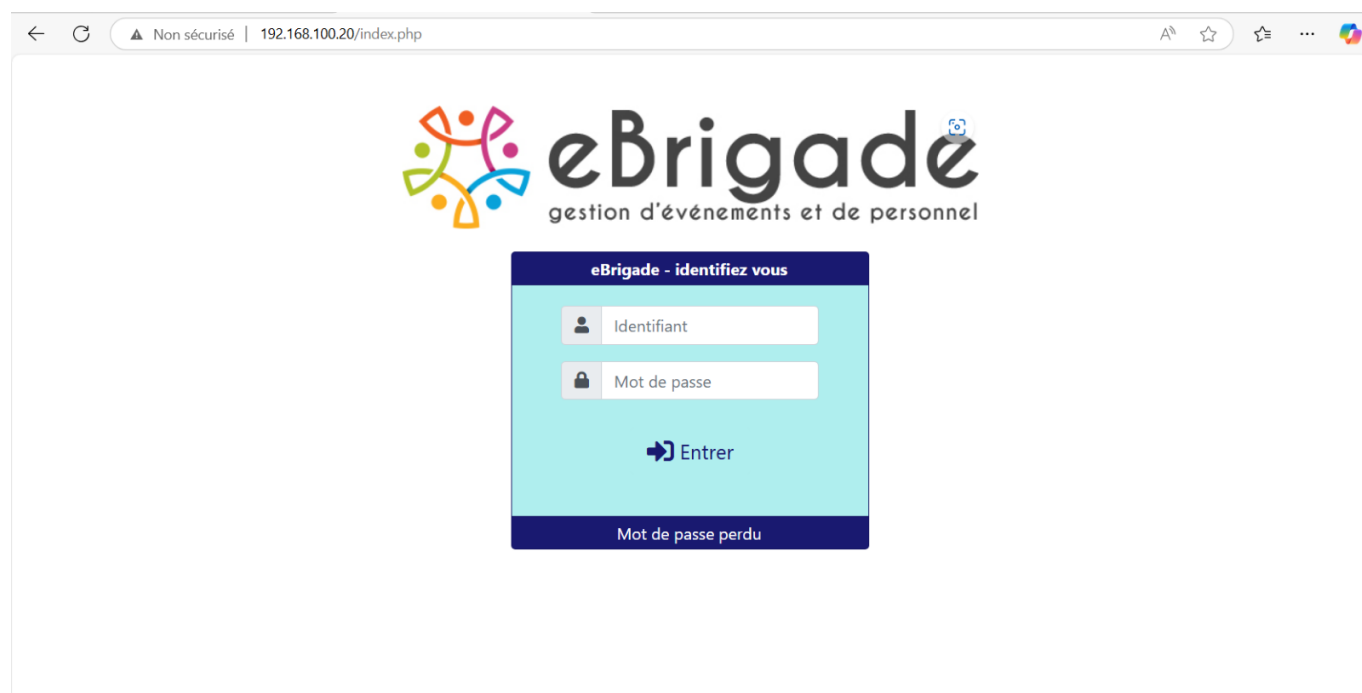
GRANT ALL PRIVILEGES ON database* TO 'nom_utilisateur'@'localhost';

FLUSH PRIVILEGES;

Une fois la création de la base de données faite, nous allons désormais pouvoir finaliser la configuration d'e-brigade :

Sur l'interface WEB, rentrez simplement 'localhost' comme hôte, le nom de la base, l'utilisateur et le mot de passe, puis cliquez sur continuer.

Nous y sommes, bienvenue sur e-brigade !



Installation d'un serveur de supervision Centreon

L'installation de Centreon passe par l'installation d'une machine virtuelle directement sur le site officiel de Centreon. C'est un fichier OVA qui va s'installer, qu'il va falloir importer sur le logiciel utilisé (VMWare ou VirtualBOX).

Une fois l'installation de la machine virtuelle et l'import fait, nous allons pouvoir démarrer notre machine :

```
Debian GNU/Linux 12 ip-10-1-154-78 tty1
ip-10-1-154-78 login: _
```

Une fois ici, nous allons rentrer les identifiants fournis par Centreon, l'utilisateur est root, et le mot de passe *centreon*.

A l'arrivée sur le serveur, une liste de choses à faire avant l'utilisation nous ai donné, nous allons alors la suivre.

```
Linux ip-10-1-154-78 6.1.0-32-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) x86_64
```

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 104

```
Last login: Fri Apr 4 14:45:52 CEST 2025 on tty1
"Based on "Debian GNU/Linux 12 (bookworm)"
```

Please execute following instruction:

1. Define the timezone of the server (ex. Europe/London):

```
# timedatectl set-timezone Europe/London
```

2. Define the PHP timezone (ex. Europe/London) in file `/etc/php.d/50-centreon.ini`

```
# systemctl restart php8.2-fpm
```

3. Change the hostname of the server (ex. centreon-central):

```
# hostnamectl set-hostname centreon-central
```

4. Update the Centreon database partitioning (mandatory):

```
# su - centreon
```

```
$ /bin/php /usr/share/centreon/cron/centreon-partitioning.php
```

```
$ exit
```

5. Restart Centreon services (mandatory):

```
# systemctl restart cbd centengine gorgoned
```

You can disable the CEIP program using Centreon official documentation.

To delete this message, delete the `/etc/profile.d/centreon.sh` file."

```
root@ip-10-1-154-78:~#
```

Dans un premier temps, nous allons devoir se synchroniser sur des serveurs de temps afin d'éviter les incohérences entre les autres machines. Le serveur PHP lui aussi aura besoin de synchronisation du temps.

Nous allons ensuite renommer le serveur avec la commande `hostnamectl`, Centreon nous donne directement les arguments à rentrer pour les différentes commandes à exécuter.

Pour finir, nous allons mettre à jour la base de données de Centreon avec les commandes données à l'étape 4, puis nous allons redémarrer les services, il peut également être conseillé de redémarrer le serveur complètement afin qu'il se mette à jour au niveau des fuseaux horaires.

Après toutes ces étapes, Centreon est désormais prêt à l'utilisation et a la supervision des équipements !

Mise en place d'un VPN RoadWarrior OpenVPN

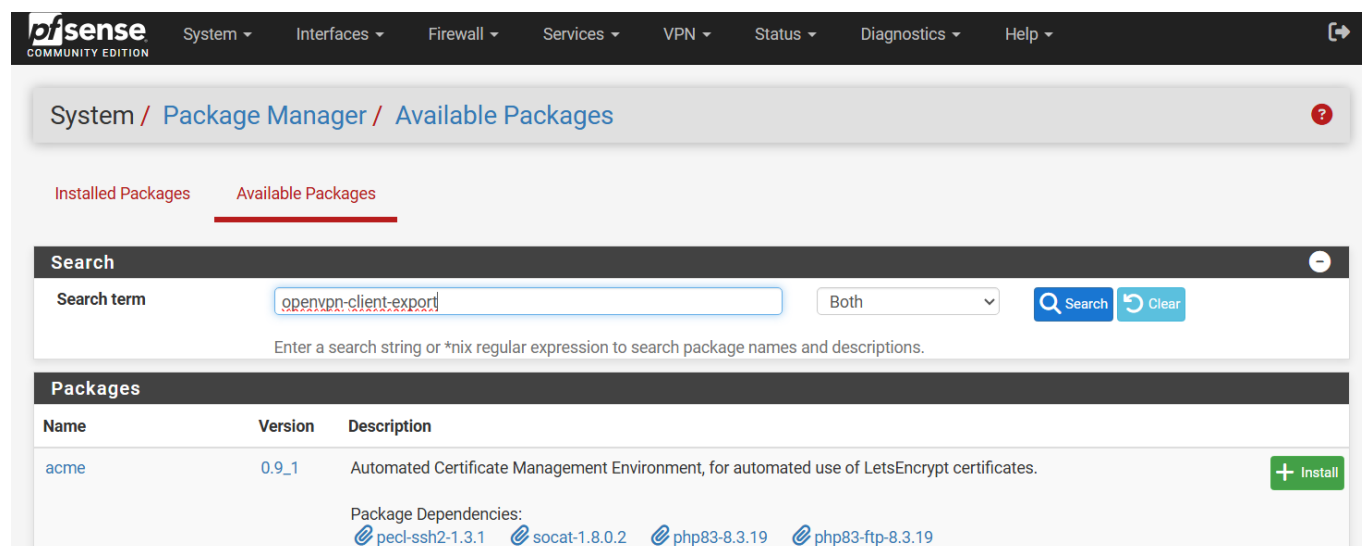
Configuration du VPN

La mise en place d'un VPN (RW) sur pfSense constitue une étape cruciale dans notre architecture sécurisée. Cette configuration permettra aux utilisateurs distants d'accéder de manière sécurisée aux ressources du réseau interne en s'authentifiant via leurs comptes Active Directory existants.

Installation du package OpenVPN

L'installation du service OpenVPN a été réalisée via l'interface d'administration de pfSense :

1. Navigation vers **System > Package Manager**
2. Sélection de l'onglet **Available Packages**
3. Recherche et installation du package **openvpn-client-export**



Ce package additionnel simplifie la génération des configurations clients et permet l'exportation des paramètres nécessaires à la connexion.

Création de l'autorité de certification

Avant de configurer le serveur VPN, nous avons généré une infrastructure de clés publiques (PKI) via le gestionnaire de certificats intégré à pfSense :

1. Navigation vers **System > Certificates**
2. Création d'une nouvelle autorité de certification. Cliqué sur Add et compléter avec les paramètres suivants :

System / Certificates / Authorities / Edit

Authorities

Certificates

Revocation

Create / Edit CA

Descriptive name

VPN-CA

The name of this entry as displayed in the GUI for reference.

This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method

Create an internal Certificate Authority

Trust Store☐ Add this Certificate Authority to the Operating System Trust Store

When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the

Randomize Serial☐ Use random serial numbers when signing certificates

When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority	
Key type	RSA
	2048
	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificat
Digest Algorithm	sha256
	The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI , algorithms invalid.
Lifetime (days)	3650
Common Name	vpn-ca
	The following certificate authority subject components are optional and may be left blank.
Country Code	FR
State or Province	Alsace
City	Strasbourg
Organization	Securite
Organizational Unit	e.g. My Department Name (optional)
Save	

Génération du certificat serveur

Après la création de l'autorité de certification, nous avons généré un certificat spécifique pour le serveur VPN :

1. Toujours dans **System > Certificates**, sélection de l'onglet **Certificates**
2. Création d'un nouveau certificat avec les paramètres suivants :

System / Certificates / Certificates / Edit

[Authorities](#)
[Certificates](#)
[Revocation](#)

Add/Sign a New Certificate

Method
Create an internal Certificate

Descriptive name
Openvpn-Cert

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following character

Internal Certificate

Certificate authority
VPN-CA

Key type
RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm
sha256

The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, may consider some algorithms invalid.

Lifetime (days)
3650

The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name
openvpn-cert

The following certificate subject components are optional and may be left blank.

Country Code
FR

Certificate Attributes					
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.				
Certificate Type	User Certificate Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or g				
Alternative Names	<table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>IP address</td> <td>172.20.10.9</td> </tr> </tbody> </table> Enter additional identifiers for the certificate in this list. The Common Name field is automatically added. signing CA may ignore or change these values.	Type	Value	IP address	172.20.10.9
Type	Value				
IP address	172.20.10.9				
Add SAN Row	+ Add SAN Row				
Save					

Et cliqué sur Save

Configuration du serveur OpenVPN

La configuration du serveur OpenVPN a été réalisée via l'interface graphique de pfSense :

1. Navigation vers **VPN > OpenVPN**, onglet **Servers**
2. Création d'un nouveau serveur avec les paramètres suivants :

Servers	Clients	Client Specific Overrides	Wizards	Client Export
General Information				
Description	Securite-VPN A description of this VPN for administrative reference.			
Disabled	☐ Disable this server Set this option to disable this server without removing it from the list.			
Mode Configuration				
Server mode	Remote Access (User Auth)			
Backend for authentication	Certificat-VPN Local Database			
Device mode	tun - Layer 3 Tunnel Mode "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible "tap" mode is capable of carrying 802.3 (OSI Layer 2.)			
Endpoint Configuration				
Protocol	UDP on IPv4 only			
Interface	WAN The interface or Virtual IP address where OpenVPN will receive client connections.			
Local port	1194 The port used by OpenVPN to receive client connections.			
Cryptographic Settings				
TLS Configuration	☒ Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common secret key. This layer of HMAC authentication allows control channel packets without the proper key to be rejected, thus preventing unauthorized connections. The TLS Key does not have any effect on tunnel data.			
	☒ Automatically generate a TLS Key.			
Peer Certificate Authority	VPN-CA			
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager			
OCSP Check	☐ Check client certificates with OCSP			
Server certificate	Openvpn-Cert (Server: Yes, CA: VPN-CA, In Use) Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using weak digest algorithms.			
DH Parameter Length	2048 bit Diffie-Hellman (DH) parameter set used for key exchange. i			

Tunnel Settings	
IPv4 Tunnel Network	192.168.1.0/24 This is the IPv4 virtual network or network type alias with a single entry used for p expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the n usable addresses will be assigned to connecting cli A tunnel network of /30 or smaller puts OpenVPN in to-peer mode with several options, including Exit Notify, and Inacti
IPv6 Tunnel Network	This is the IPv6 virtual network or network type alias with a single entry used for p expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will will be assigned to connecting clients.
Redirect IPv4 Gateway	☐ Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	☐ Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	192.168.100.0/24 IPv4 networks that will be accessible from the remote endpoint. Expressed as a cc type aliases. This may be left blank if not adding a route to the local network throu LAN network.
IPv6 Local network(s)	IPv6 networks that will be accessible from the remote endpoint. Expressed as a cc aliases. This may be left blank if not adding a route to the local network through th network.
Concurrent connections	10 Specify the maximum number of clients allowed to concurrently connect to this se
Allow Compression	Refuse any non-stub compression (Most secure) Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to ext

Advanced Client Settings	
DNS Default Domain	☒ Provide a default domain name to clients
DNS Default Domain	securite.lan
DNS Server enable	☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	192.168.100.15
DNS Server 2	
DNS Server 3	
DNS Server 4	
Block Outside DNS	☐ Make Windows 10 Clients Block access to DNS servers except across Open Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to not affected.

Advanced Configuration	
Custom options	Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"
Username as Common Name	☒ Use the authenticated client username instead of the certificate common name (CN). When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate such as determining Client Specific Overrides.
UDP Fast I/O	☐ Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and no bandwidth limiting.
Exit Notify	Reconnect to this server / Retry once Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately connect for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
Send/Receive Buffer	Default Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512K values.
Gateway creation	☐ Both ☒ IPv4 only ☐ IPv6 only If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default is IPv4 only.

Et cliqué sur Save.

Intégration avec l'Active Directory

Configuration du serveur OpenVPN

La configuration du serveur OpenVPN a été réalisée via l'interface graphique de pfSense :

1. Navigation vers **System > User Manager**, onglet **Authentication Servers**
2. Création de l'autorisation pour la communication entre le serveur pfsense et le serveur AD

System / User Manager / Authentication Servers / Edit

[Users](#)
[Groups](#)
[Settings](#)
[Change Password](#)
[Authentication Servers](#)

Server Settings

Descriptive name Certificat-VPN

Type LDAP

LDAP Server Settings

Hostname or IP address 192.168.100.15
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject server SSL/TLS Certificate.

Port value 389

Transport Standard TCP

Peer Certificate Authority VPN-CA
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encryption' is enabled. The CA used by the LDAP server.

Protocol version 3

Server Timeout 25
Timeout for LDAP operations (seconds)

Search scope Level
 Entire Subtree

Search scope Level
 Entire Subtree

Base DN
 DC=securite.lan,DC=local

Authentication containers OU=Users LDAP,DC=securite,DC=lan
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
 Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers

Extended query ☐ Enable extended query

Bind anonymous ☐ Use anonymous binds to resolve distinguished names

Bind credentials CN=vpn-bing,OU=Users LDAP,DC=securite,DC=lan

User naming attribute samAccountName

Group naming attribute cn

Group member attribute memberOf

Configuration des règles de pare-feu

Pour permettre l'accès au serveur VPN depuis Internet, les règles de pare-feu suivantes ont été ajoutées :

1. Navigation vers **Firewall > Rules**, onglet **WAN**
2. Création d'une règle permettant le trafic UDP entrant sur le port 1194 :

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP
whereas with block the packet is dropped silently. In either case, the original p

Disabled

☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must ren
its default value, any.

Destination

Destination

☐ Invert match

Any

Destination Address

/

Destination Port Range

OpenVPN (1194)

From

Custom

To

OpenVPN (1194)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Et cliqué sur Save.

Export du client

Pour permettre l'accès au serveur VPN depuis Internet, Il faut exporter un « client » pour pouvoir l'importer dans OpenVPN pour qu'il puisse récupérer toutes les infos de connexions.

1. Navigation vers **VPN > OpenVPN**, onglet **Client Export**
2. Exportation du client avec les paramètres suivants :

OpenVPN / Client Export Utility

Server
Client
Client Specific Overrides
Wizards
Client Export

OpenVPN Server

Remote Access Server
Securite-VPN UDP4:1194

Client Connection Behavior

Host Name Resolution
Interface IP Address

Verify Server CN
Automatic - Use verify-x509-name where possible

Optionally verify the server certificate Common Name (CN) when the client connects.

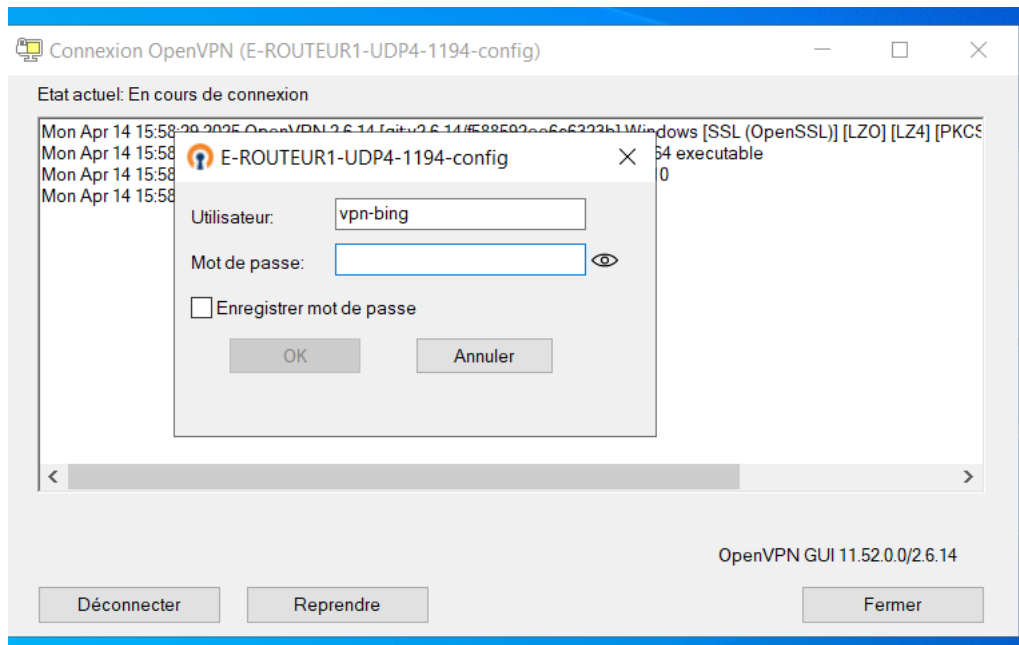
OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.6.7-1x001):

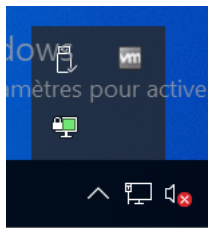
Cliquer sur « Most Clients » pour l'exportation

Tests et validation du VPN

1. Télécharger et installer OpenVPN GUI
2. Lancez OpenVPN et importe le .ovpn télécharger précédemment.



Il va donc vous demander de vous connecter avec un de vos utilisateurs de l'AD qui est autorisée de se connecter en VPN.



Si l'icône affiche vert vous êtes bien connecté en VPN.

