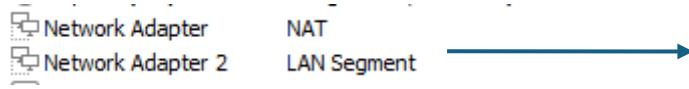


DOCUMENTATION SUR LA MISE EN PLACE DU PROJET

Afin de réaliser mon premier projet, je l'ai découpé en plusieurs étapes.

- Installation de pfSense
- Configuration de pfSense (réseau LAN et DHCP)
- Installation et Configuration de Windows Server 2022 (AD/DNS)
- Installation et Configuration d'un poste client
- Sécurisation du réseau avec pfSense

Étape 1 : Installation de pfSense

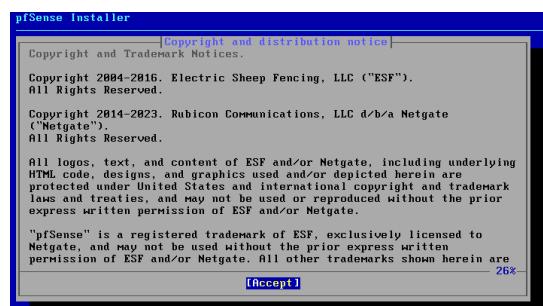


Configuration de la VM :

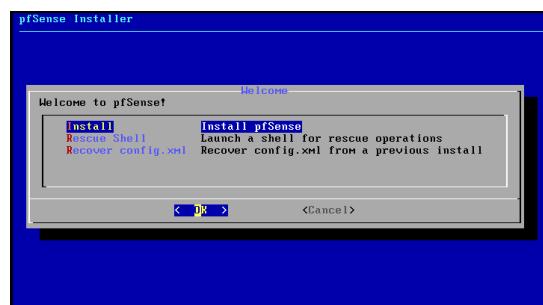
Une carte réseau en NAT qui permet de simuler le réseau internet

Une carte réseau en LAN

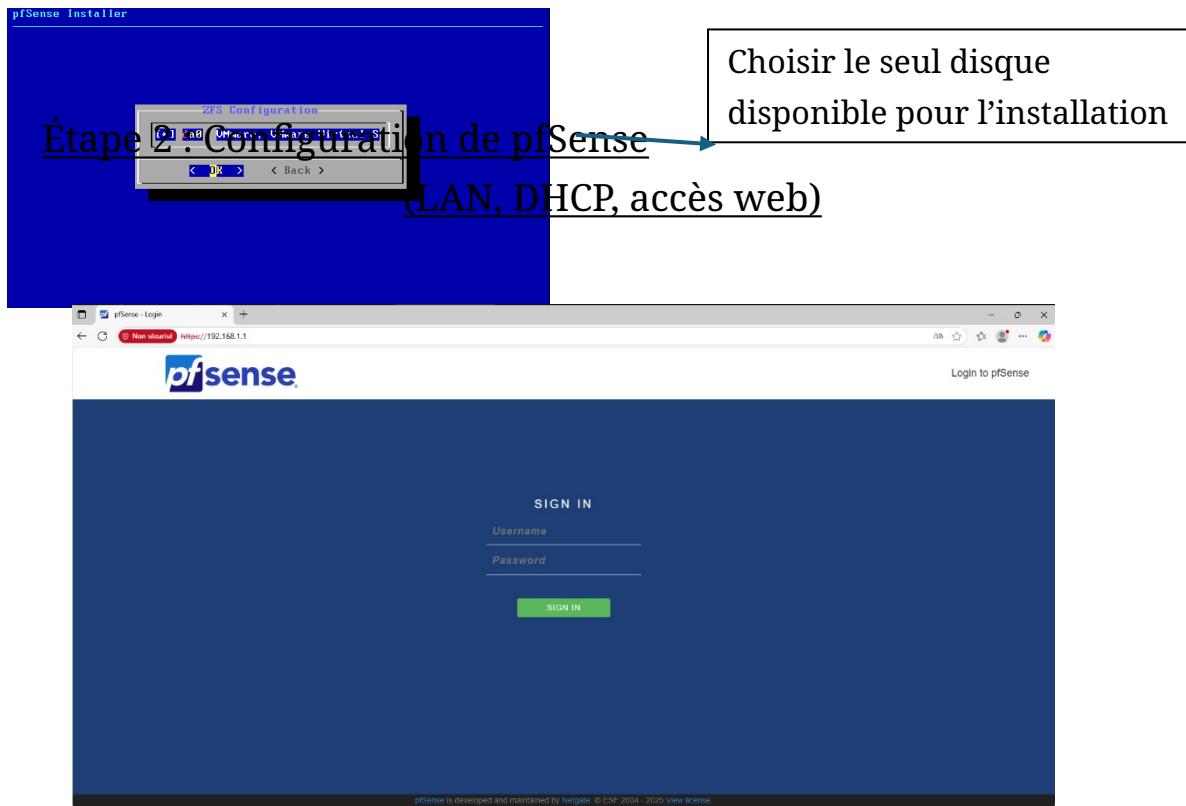
Servant afin d'avoir un



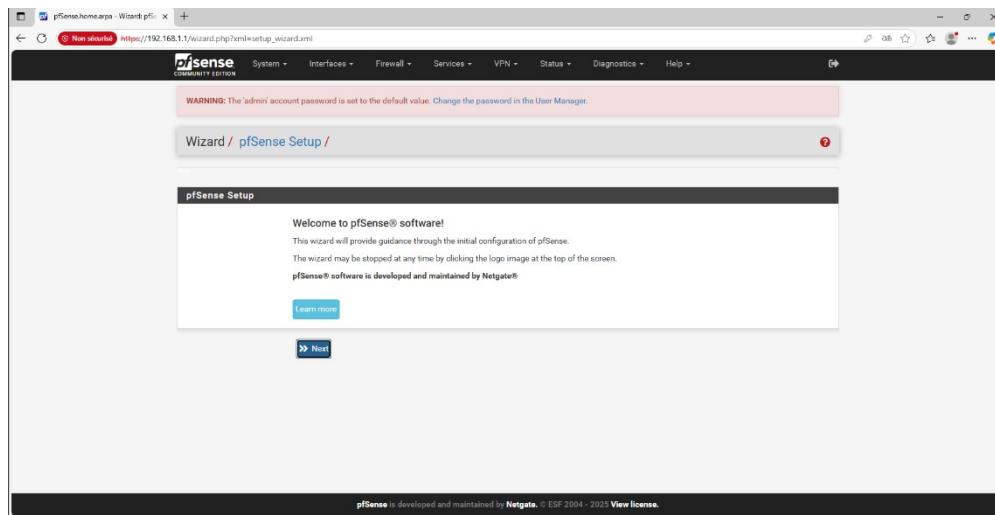
Au lancement, Accepter les conditions



Choisir Install



Une fois l'installation terminée, nous pouvons nous rendre à la page web du pfSense. Cela sera plus simple pour le configurer. Nous pouvons donc se connecter avec admin comme username et pfSense comme password.



Une fois connecté nous allons pouvoir suivre l'assistant de configuration.

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense-Router
Name of the firewall host, without domain part.
Examples: pfSense, firewall, edgewr

Domain: enterpriseBTlocal
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with 'local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server:

Secondary DNS Server:

Override DNS Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

Mise en place du nouveau nom du routeur

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Europe/Paris

>> Next

Mise en place de la Timezone Paris

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

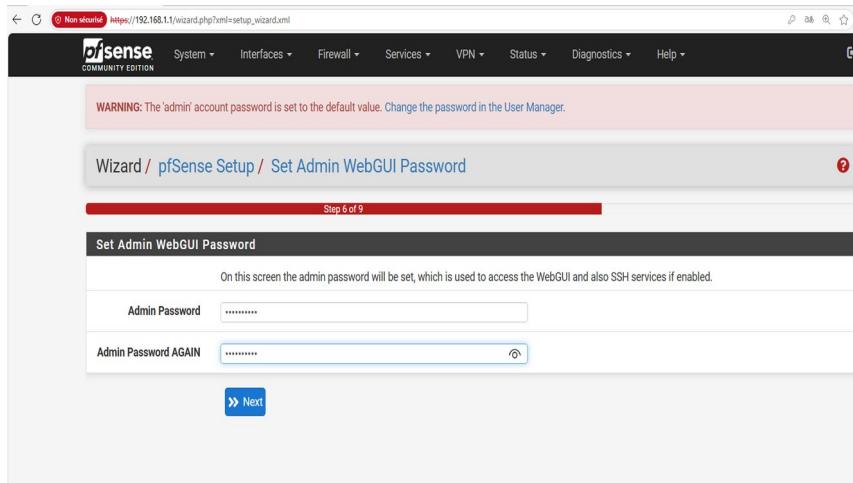
On this screen the Local Area Network information will be configured.

LAN IP Address: 10.0.0.1
Type dhcp if this interface uses DHCP to obtain its IP address.

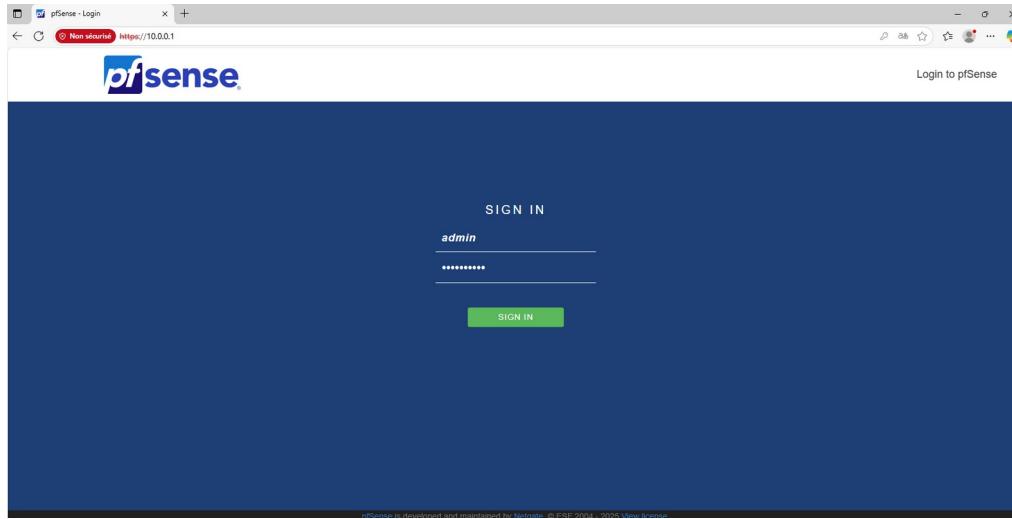
Subnet Mask: 24

>> Next

Mise en place d'une nouvelle adresse ip afin de personnaliser notre réseau



Changement du mot de passe en « adminadmin »



Nous voici sur la nouvelle page de connexion avec la nouvelle ip 10.0.0.1

General DHCP Options

- DHCP Backend: ISC DHCP
- Enable: Enable DHCP server on LAN interface
- BOOTP: Ignore BOOTP queries
- Deny Unknown Clients**: Allow all clients (selected)

When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
- Ignore Denied Clients**: Ignore denied clients rather than reject

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
- Ignore Client Identifiers**: Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet:	10.0.0.0/24
---------	-------------

Server Options

WINS Servers:	WINS Server 1
	WINS Server 2
DNS Servers:	10.0.0.10
	DNS Server 2
	DNS Server 3
	DNS Server 4

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

Activation du DHCP

Primary Address Pool

Subnet:	10.0.0.0/24
Subnet Range:	10.0.0.1 - 10.0.0.254
Address Pool Range:	From: 10.0.0.50 To: 10.0.0.60

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools: [+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers:	WINS Server 1
	WINS Server 2
DNS Servers:	10.0.0.10
	DNS Server 2
	DNS Server 3
	DNS Server 4

Mise en place de l'étendue pour la distribution d'adresses ip, puis on choisit le DNS qui sera notre Windows serveur

The screenshot shows the pfSense web interface at https://10.0.0.1/diag_ping.php. The navigation bar includes links for System, Interfaces, Firewall, Services, VPN, and Status. The main content area is titled "Diagnostics / Ping". The "Ping" configuration form has the following settings:

- Hostname: 8.8.8.8
- IP Protocol: IPv4
- Source address: Automatically selected (default)
- Maximum number of pings: 3
- Seconds between pings: 1

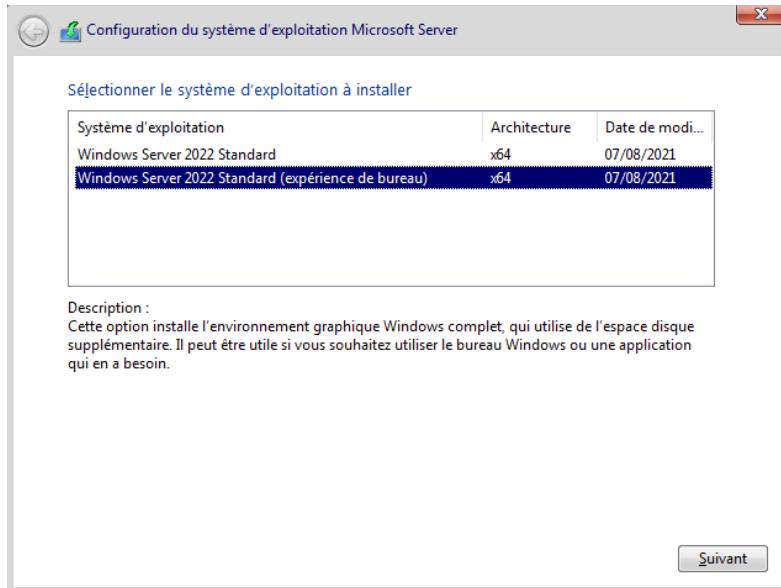
The "Results" section displays the output of the ping command:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=13.461 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=20.382 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=12.677 ms

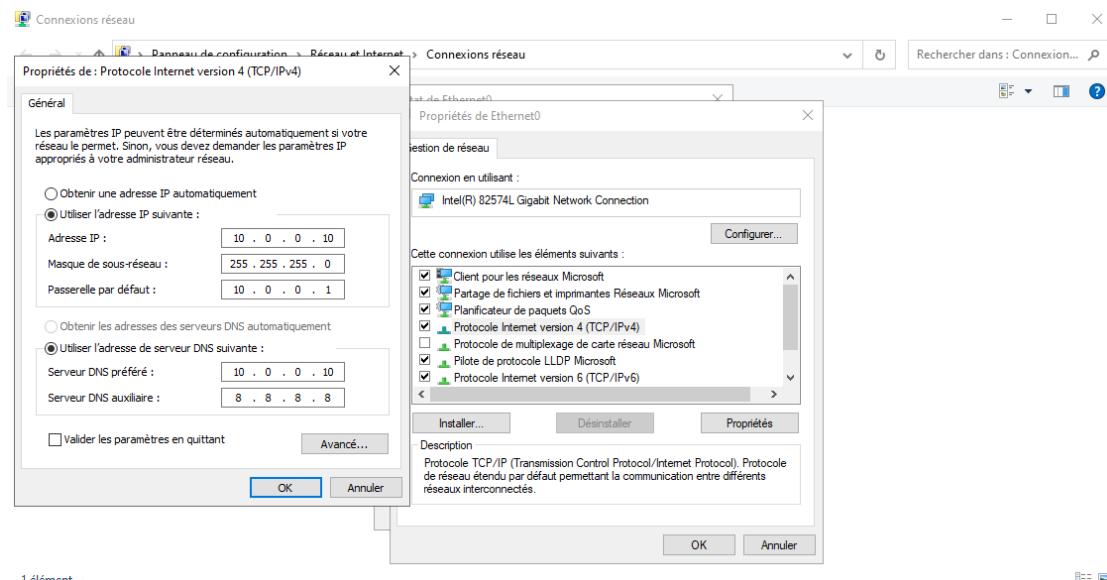
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 12.677/15.507/20.382/3.462 ms
```

Test de ping vers le DNS de google, ce qui confirme que pfSense a bien accès à internet depuis l'interface WAN

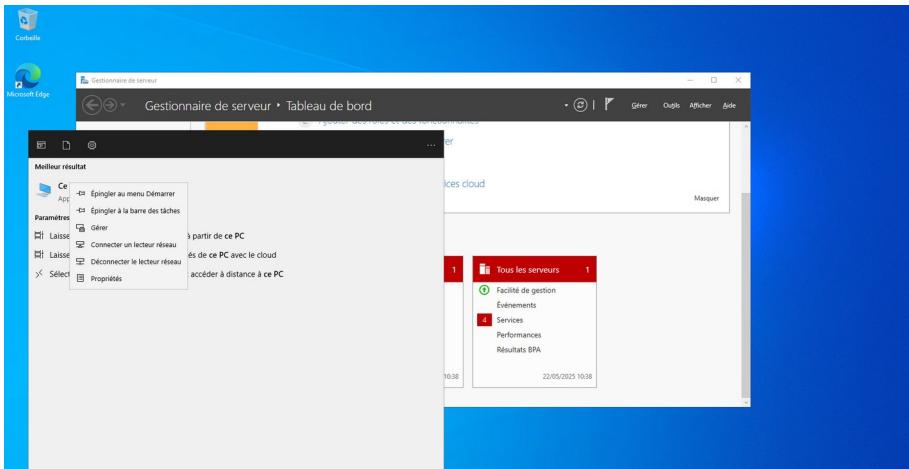
Étape 3 : Installation et Configuration de Windows Server 2022 (AD/DNS)



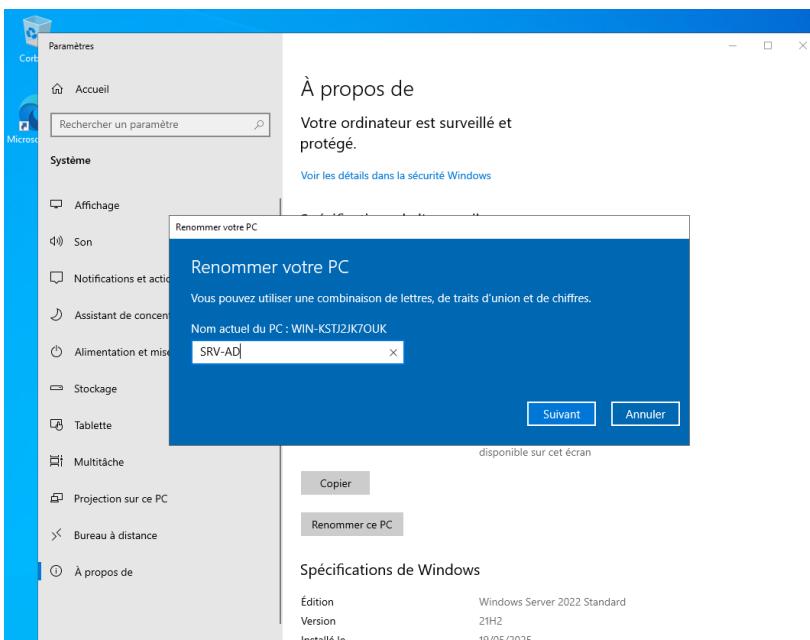
Sélection de l'expérience de bureau afin d'avoir un retour graphique



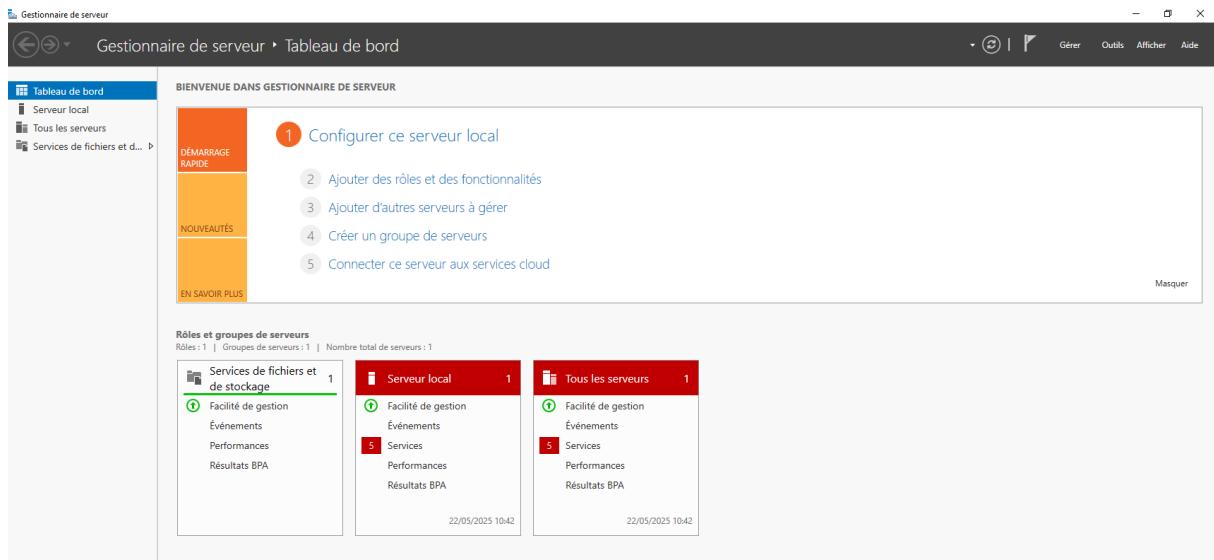
Une fois l'installation terminée, nous allons définir l'adresse ip du windows serveur en 10.0.0.10 et mettre le pfSense en passerelle par défaut.



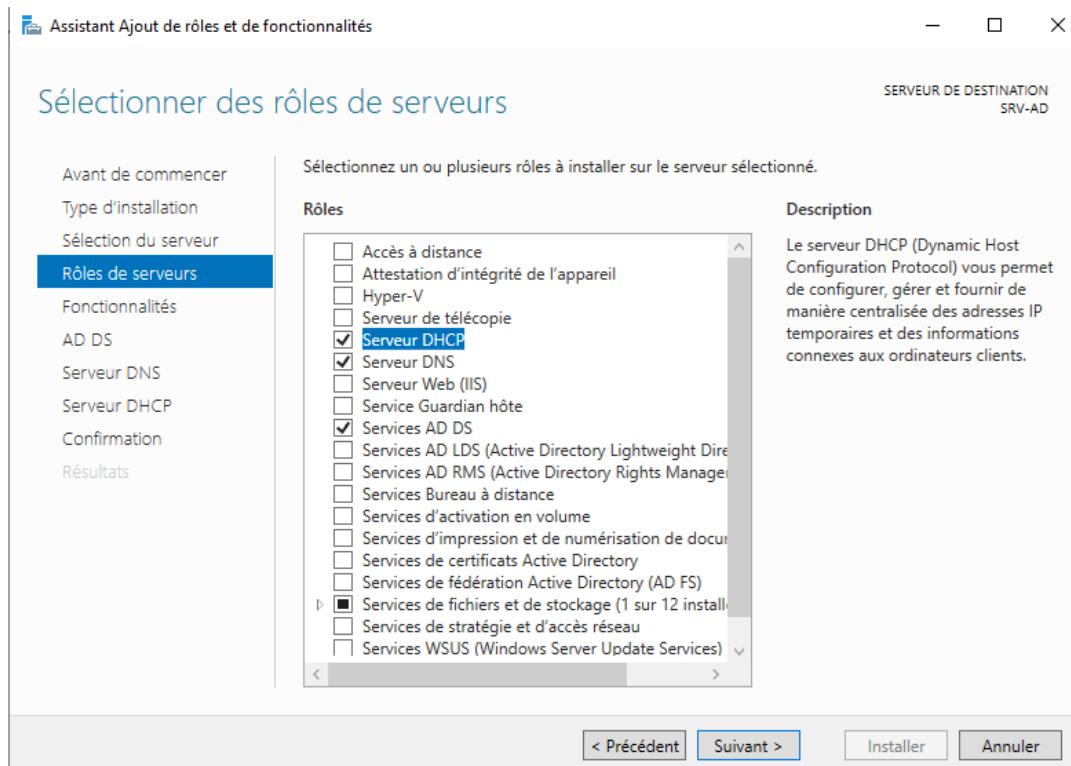
Puis nous allons aller dans les paramètres afin de renommer le pc



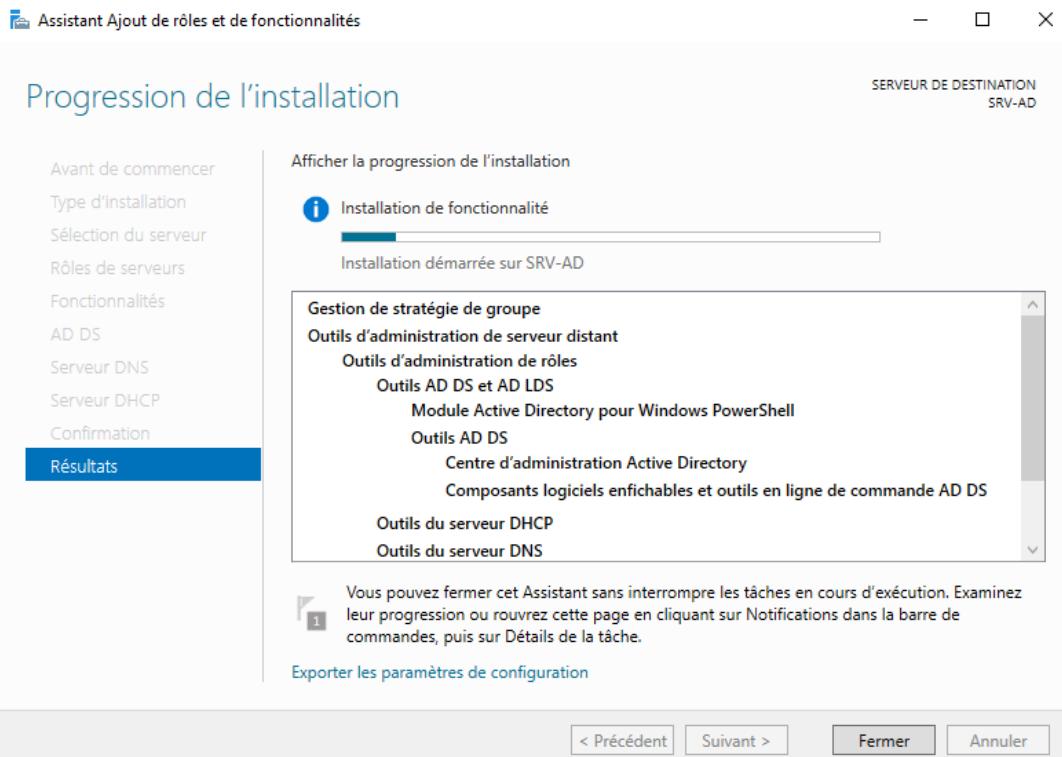
Nous renommons donc le pc en SRV-AD



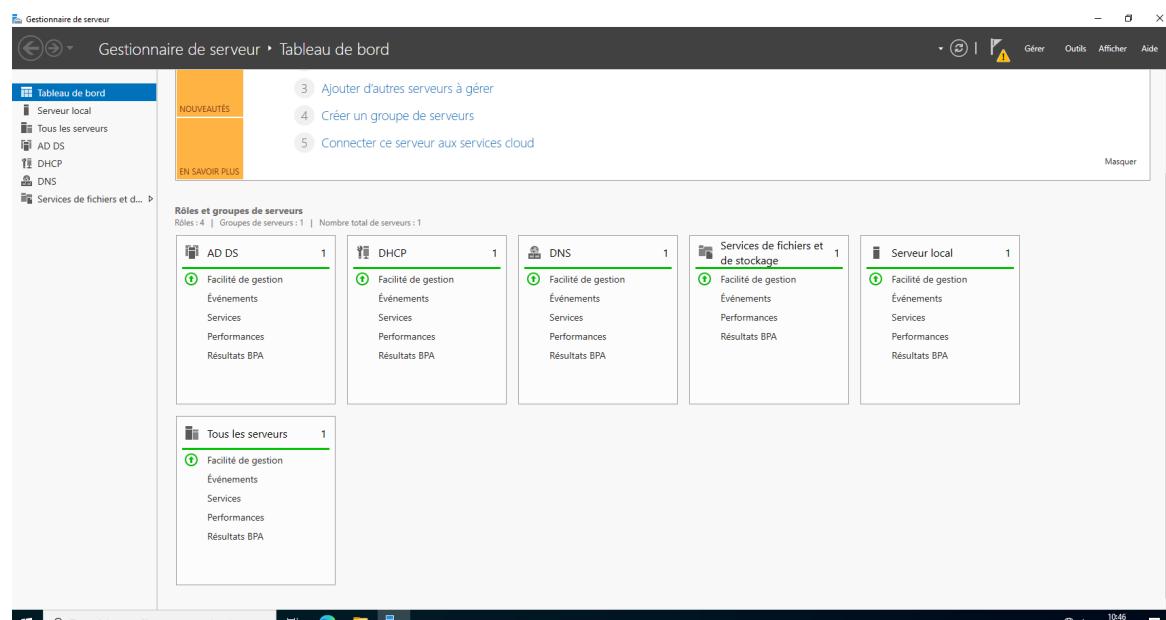
Nous voici sur le tableau de bord du gestionnaire de serveur afin d'y ajouter des rôles



Sélection des rôles DNS et AD DS. (ici le service DHCP ne devrait pas être coché c'est une erreur)



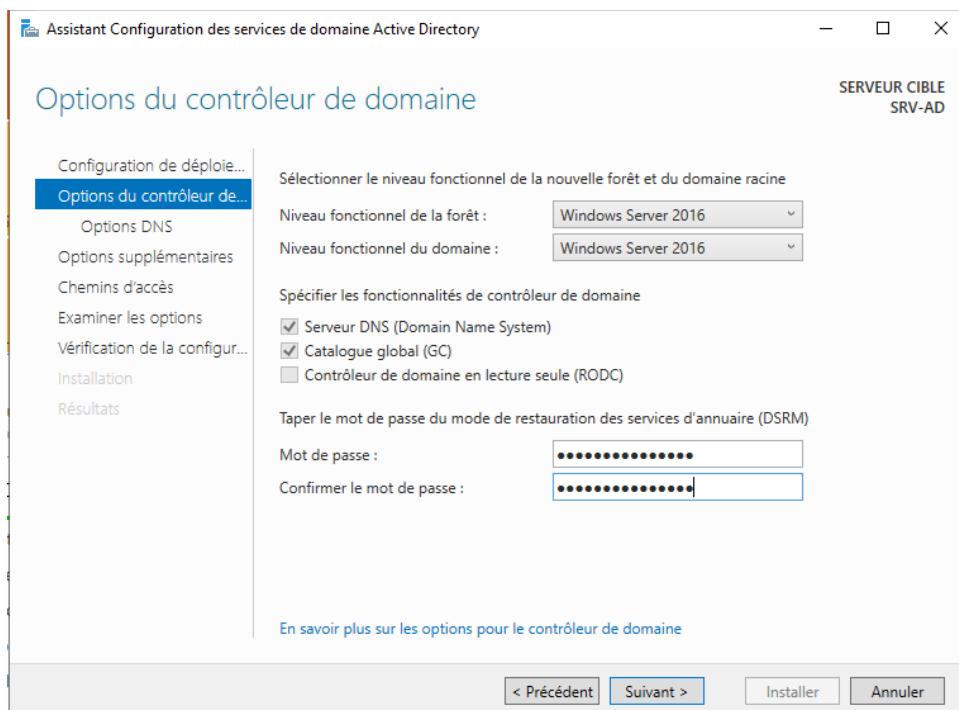
Installation des services (ici le service DHCP s'installe mais c'est aussi une erreur)



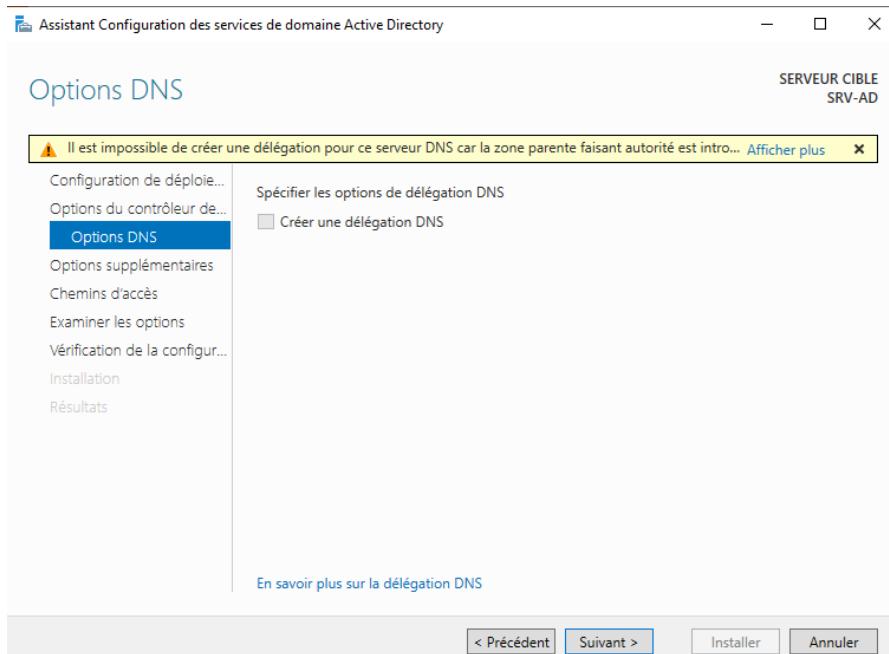
Voici les rôles installés (le rôle dhcp sera supprimé plus tard)

Nous allons maintenant promouvoir ce serveur en contrôleur de domaine

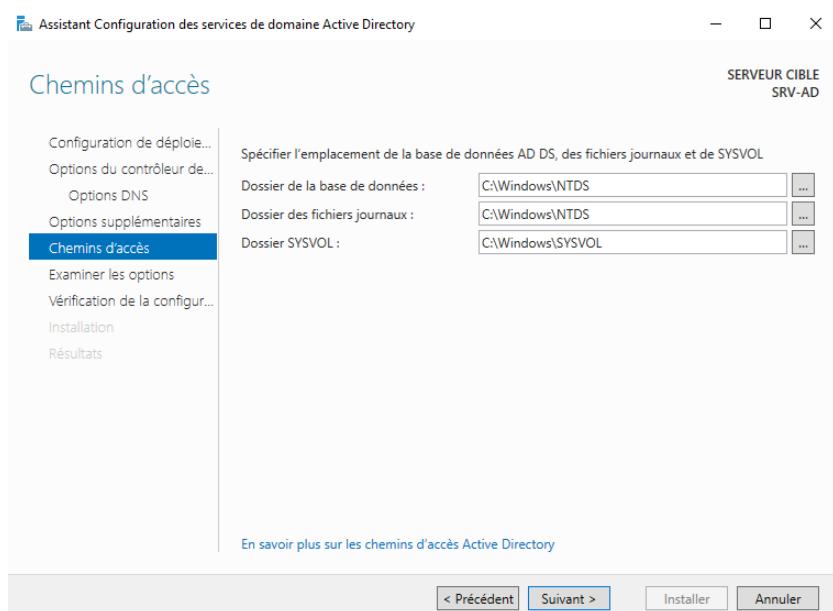
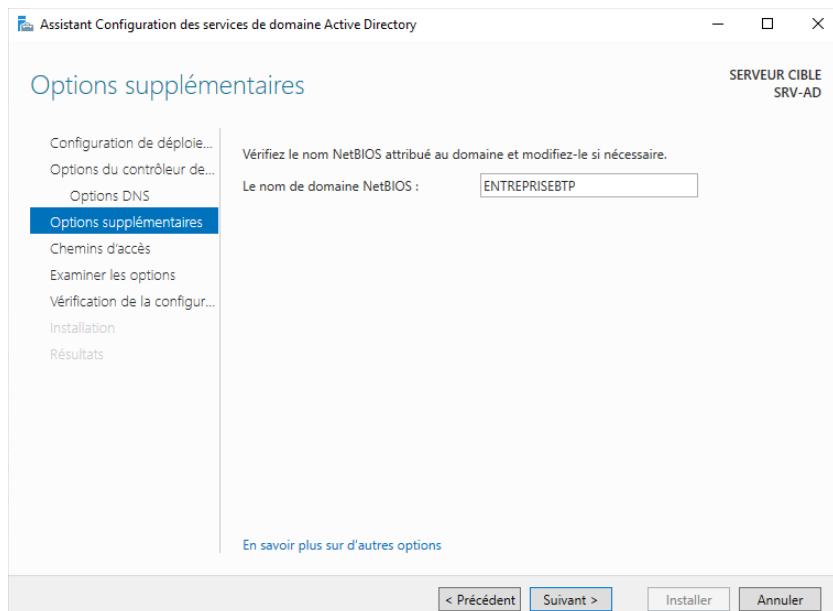
Nous choisissons « entreprisebtp.local » comme nom de domaine racine

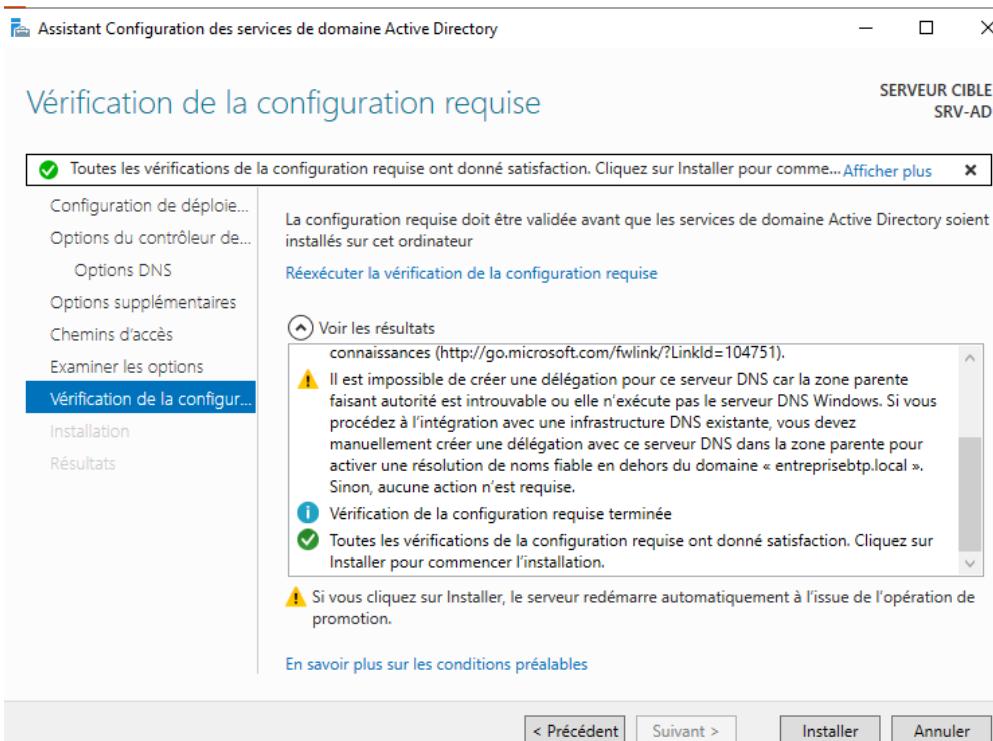
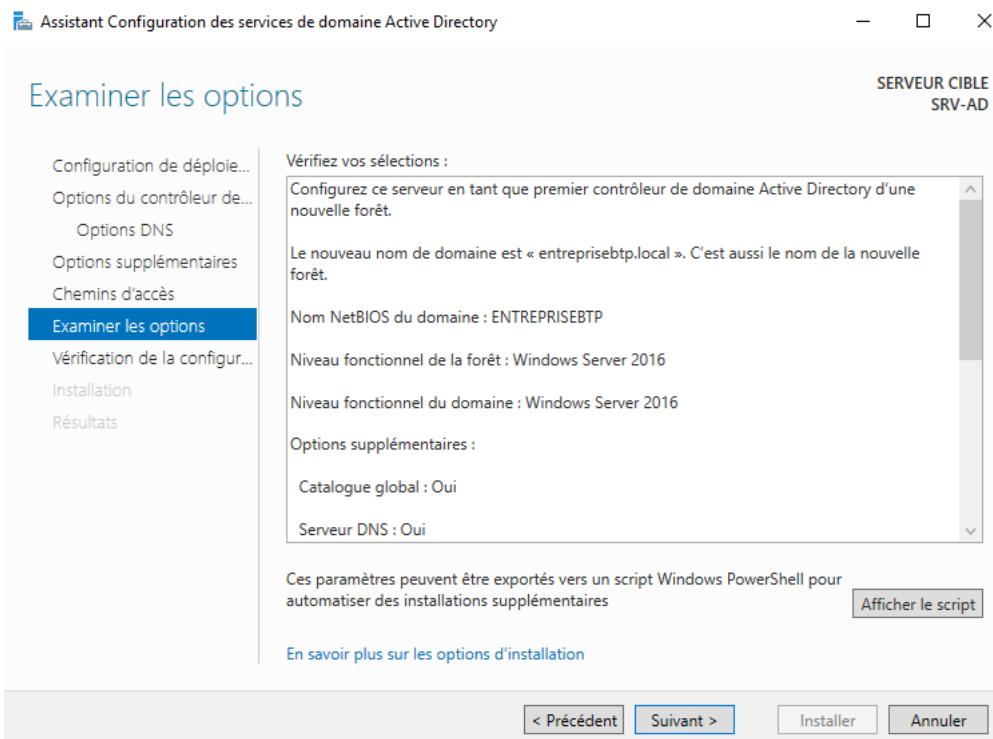


Mise en place d'un mot de passe DSRM

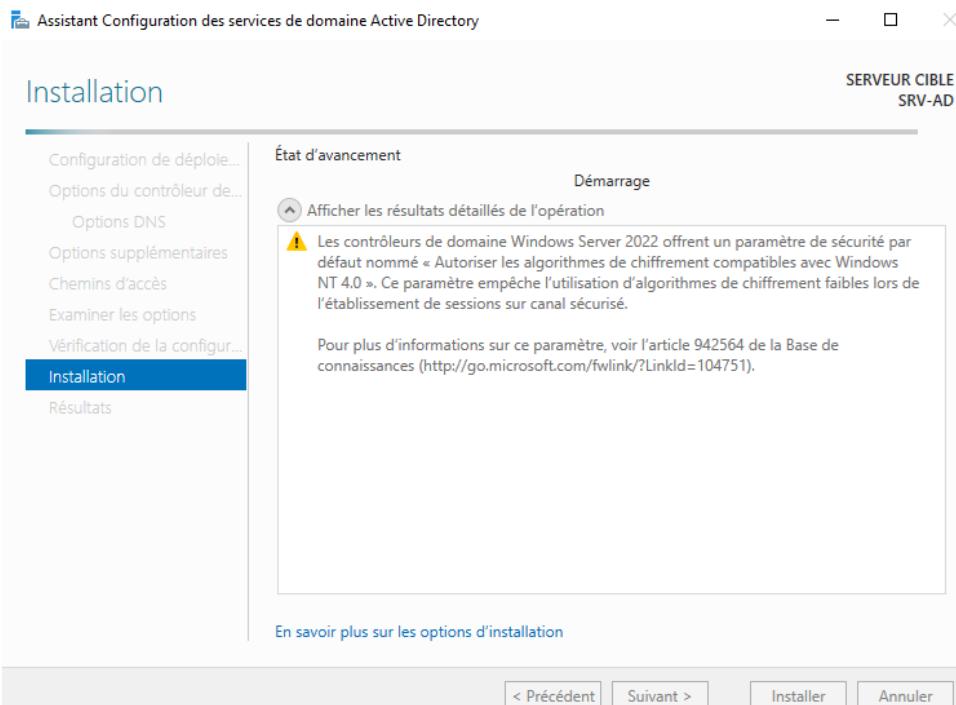


Nous allons suivre les étapes de l'installation

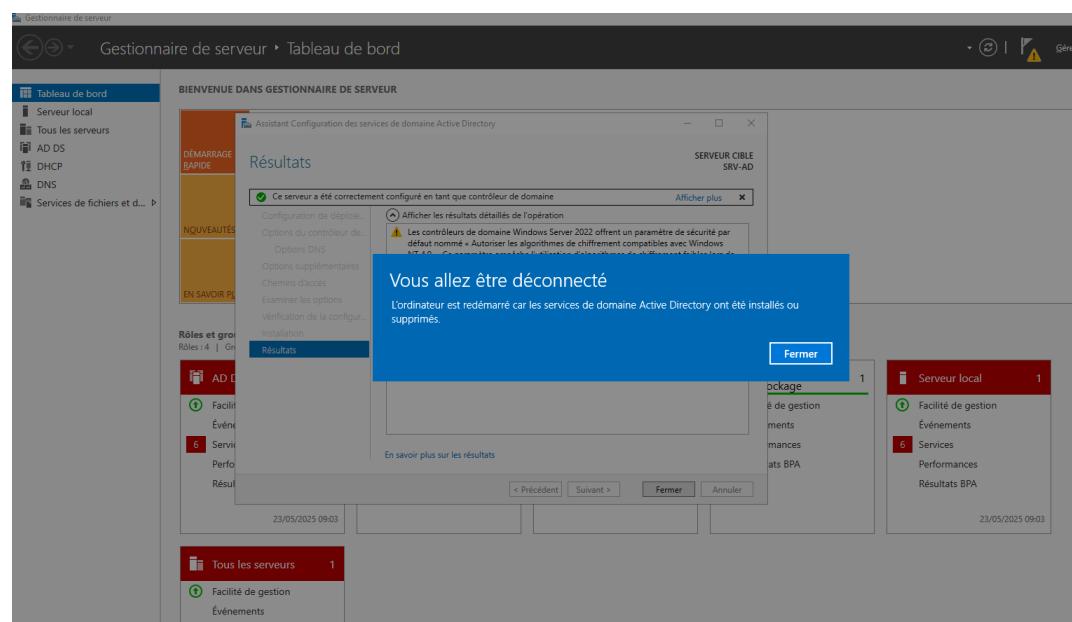




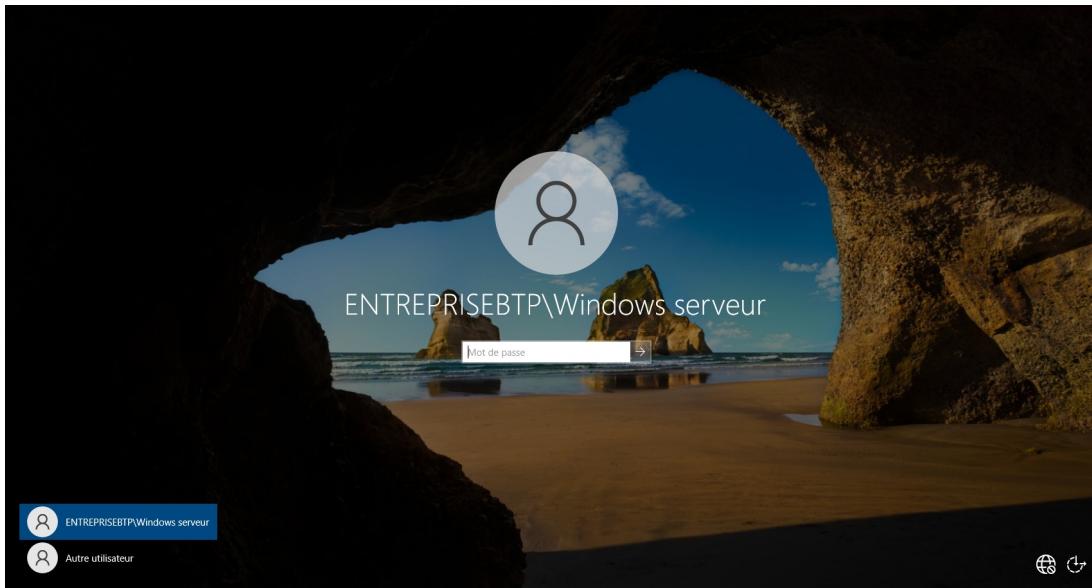
L'installation va pouvoir commencer



Installation en cours



L'ordinateur doit redémarrer afin de se mettre à jour

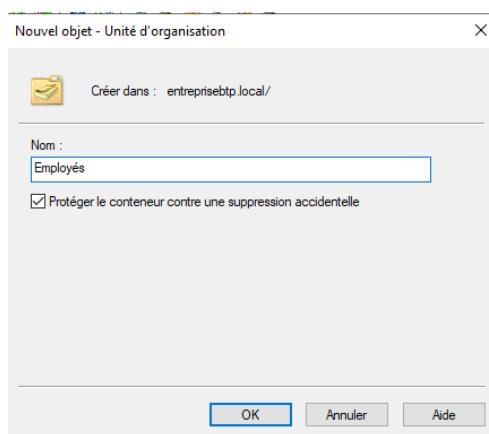
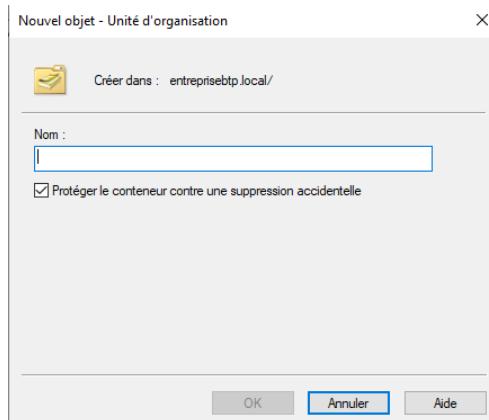


Le serveur est bien un contrôleur de domaine

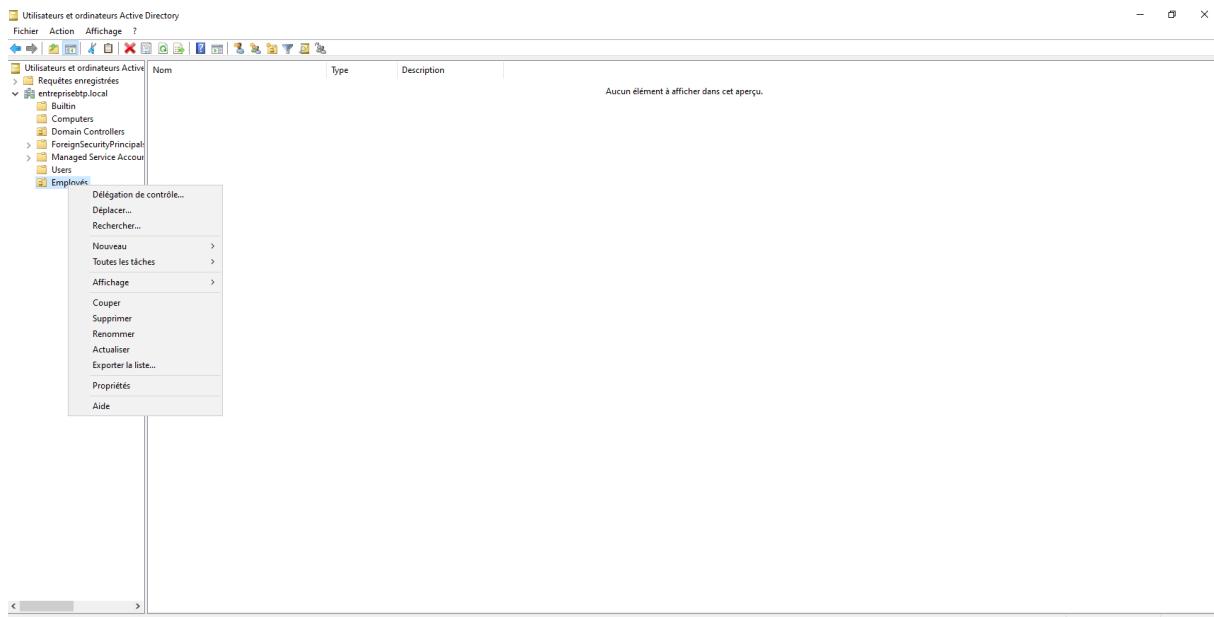
Le rôle DHCP a été supprimé car le DHCP est fait par Pfsense.

The screenshot shows the Windows Server Active Directory management interface. The main pane displays the structure of the 'entrepreneurhs.local' domain. A single 'BuiltIn' object is visible under the 'entrepreneurhs.local' container. The left sidebar features a context menu with various administrative options. The top navigation bar includes standard Windows menu items like 'Fichier', 'Actions', and 'Affichage'.

Nous allons donc créer les différents postes de notre entreprise en créant une nouvelle Unité D'organisation



L'unité employés a été créée



Nous allons pouvoir créer des utilisateurs

Nouvel objet - Utilisateur

X



Créer dans : entreprisebtp.local/Employés

Prénom : Enzo Initiales :
Nom : ALCARAZ
Nom complet : Enzo ALCARAZ

Nom d'ouverture de session de l'utilisateur :

e.alcaraz@entreprisebtp.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

ENTREPRISEBTP\ e.alcaraz

< Précédent

Suivant >

Annuler

Nouvel objet - Utilisateur

X



Créer dans : entreprisebtp.local/Employés

Mot de passe : ······

Confirmer le mot de passe : ······|

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Le compte est désactivé

< Précédent

Suivant >

Annuler

L'utilisateur Enzo ALCARAZ a été créé

Nouvel objet - Utilisateur

X



Créer dans : entreprisebtp.local/Employés

Prénom :

Loris

Initiales :

Nom :

PAILHAS

Nom complet :

Loris PAILHAS

Nom d'ouverture de session de l'utilisateur :

I.pailhas

@entreprisebtp.local



Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

ENTREPRISEBTP\

I.pailhas

< Précédent

Suivant >

Annuler

Nouvel objet - Utilisateur

X



Créer dans : entreprisebtp.local/Employés

Mot de passe :

Confirmer le mot de passe :

*****|

- L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
- L'utilisateur ne peut pas changer de mot de passe
- Le mot de passe n'expire jamais
- Le compte est désactivé

< Précédent

Suivant >

Annuler

L'utilisateur Loris PAILHAS a été créé

Nouvel objet - Utilisateur X

 Créer dans : entreprisebtp.local/Employés

Prénom : Initiales :
Nom :
Nom complet :

Nom d'ouverture de session de l'utilisateur :
 ▼

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur X

 Créer dans : entreprisebtp.local/Employés

Mot de passe :

Confirmer le mot de passe :

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
 L'utilisateur ne peut pas changer de mot de passe
 Le mot de passe n'expire jamais
 Le compte est désactivé

< Précédent Suivant > Annuler

L'utilisateur Antoine MOREAUX a été créé

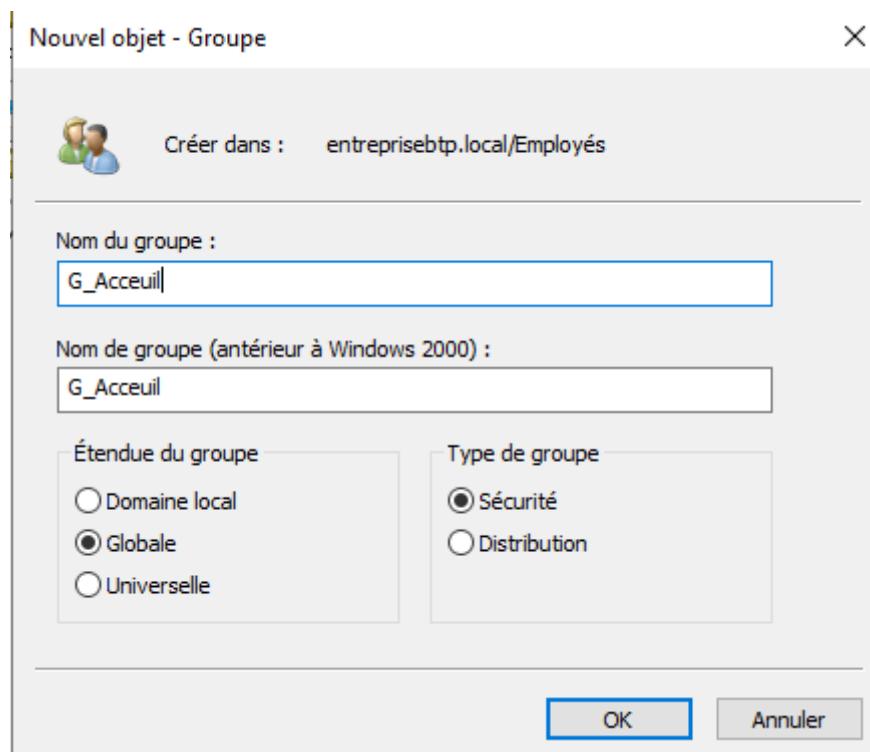
Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a navigation pane displays the tree structure of the domain: Utilisateurs et ordinateurs Active, Requêtes enregistrées, entreprisebtp.local (with subfolders Builtin, Computers, Domain Controllers, ForeignSecurityPrincipal, Managed Service Account, and Users), and Employés. On the right, a list of users is shown in a table with columns Nom, Type, and Description. Three users are listed: Antoine MOREAUX (Utilisateur), Enzo ALCARAZ (Utilisateur), and Loris PAILHAS (Utilisateur). The 'Employés' folder in the navigation pane is highlighted.

Nom	Type	Description
Antoine MOREAUX	Utilisateur	
Enzo ALCARAZ	Utilisateur	
Loris PAILHAS	Utilisateur	

Voici nos différents utilisateurs



Création d'un groupe Accueil

Nouvel objet - Groupe

X



Créer dans : entreprisebtp.local/Employés

Nom du groupe :

G_Responsable|

Nom de groupe (antérieur à Windows 2000) :

G_Responsable

Étendue du groupe

- Domaine local
- Globale
- Universelle

Type de groupe

- Sécurité
- Distribution

OK

Annuler

Création d'un groupe Responsable

Nouvel objet - Groupe

X



Créer dans : entreprisebtp.local/Employés

Nom du groupe :

G_Direction

Nom de groupe (antérieur à Windows 2000) :

G_Direction

Étendue du groupe

- Domaine local
- Globale
- Universelle

Type de groupe

- Sécurité
- Distribution

OK

Annuler

Création du groupe Direction

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Back Forward Refresh Stop Filter Help

Utilisateurs et ordinateurs Active Directory

Requêtes enregistrées

entreprisebtp.local

Builtin Computers Domain Controllers

ForeignSecurityPrincipal Managed Service Account

Users Employés

Nom	Type	Description
Antoine MOREAUX	Utilisateur	
Enzo ALCARAZ	Utilisateur	
G_Acceuil	Groupe de sécurité	
G_Direction	Groupe de sécurité	
G_Responsable	Groupe de sécurité	
Loris PAILHAS	Utilisateur	

Voici les utilisateurs ainsi que des groupes vides

Propriétés de : G_Direction

Général Membres Membre de Géré par

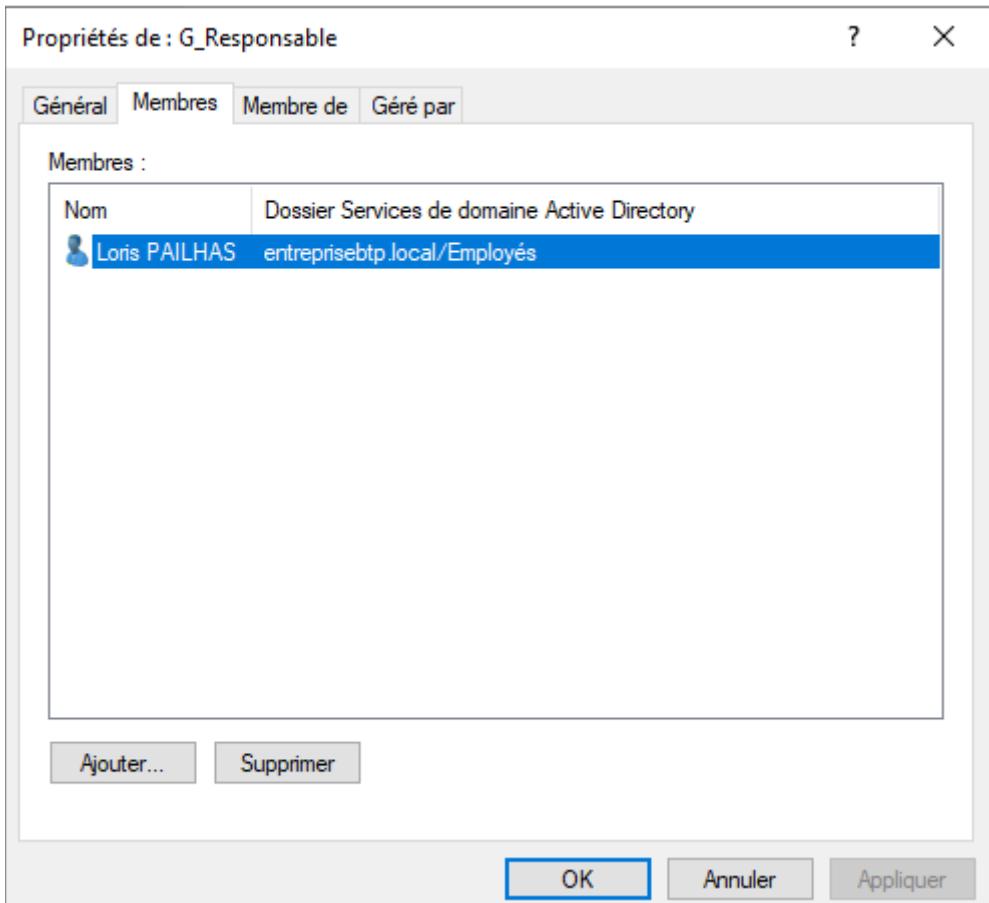
Membres :

Nom	Dossier Services de domaine Active Directory
Enzo ALCARAZ	entreprisebtp.local/Employés

Ajouter... Supprimer

OK Annuler Appliquer

Ajout de Enzo dans le groupe Direction



Ajout de Loris dans le groupe Responsable

Propriétés de : G_Accueil

?

X

Général Membres Membre de Géré par

Membres :

Nom Dossier Services de domaine Active Directory

 Antoine MOR... entreprisebtp.local/Employés

Ajouter...

Supprimer

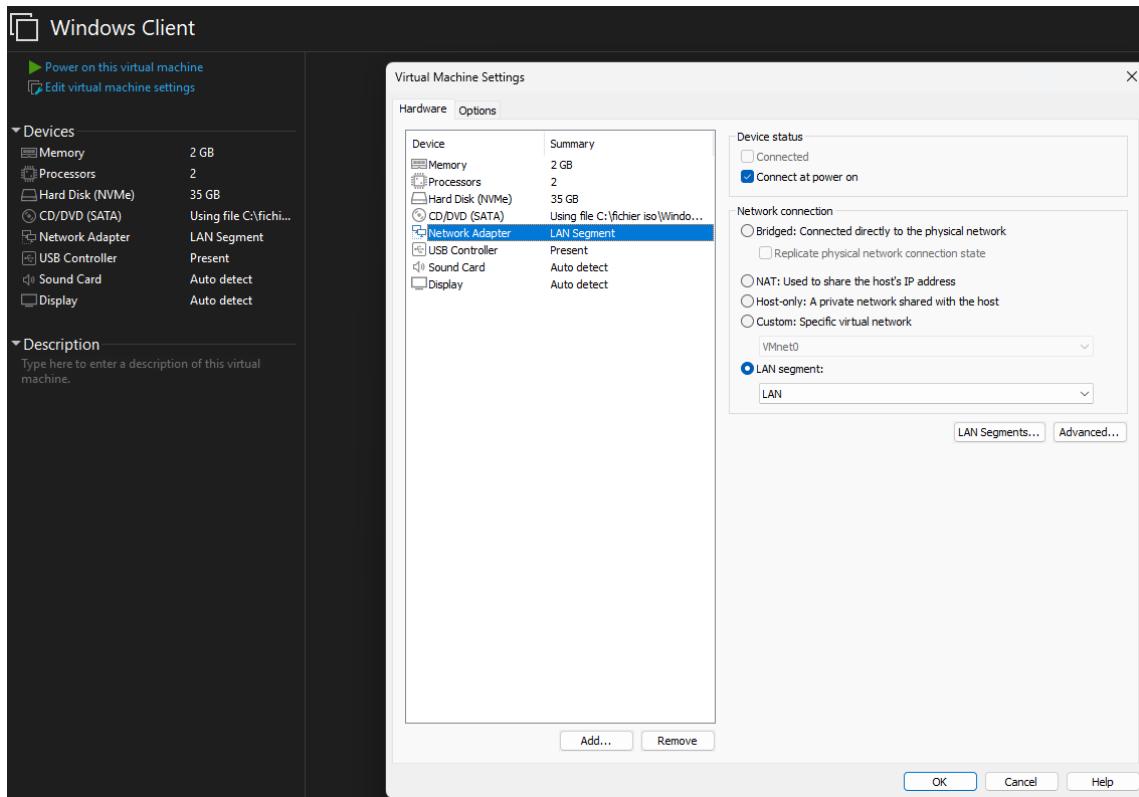
OK

Annuler

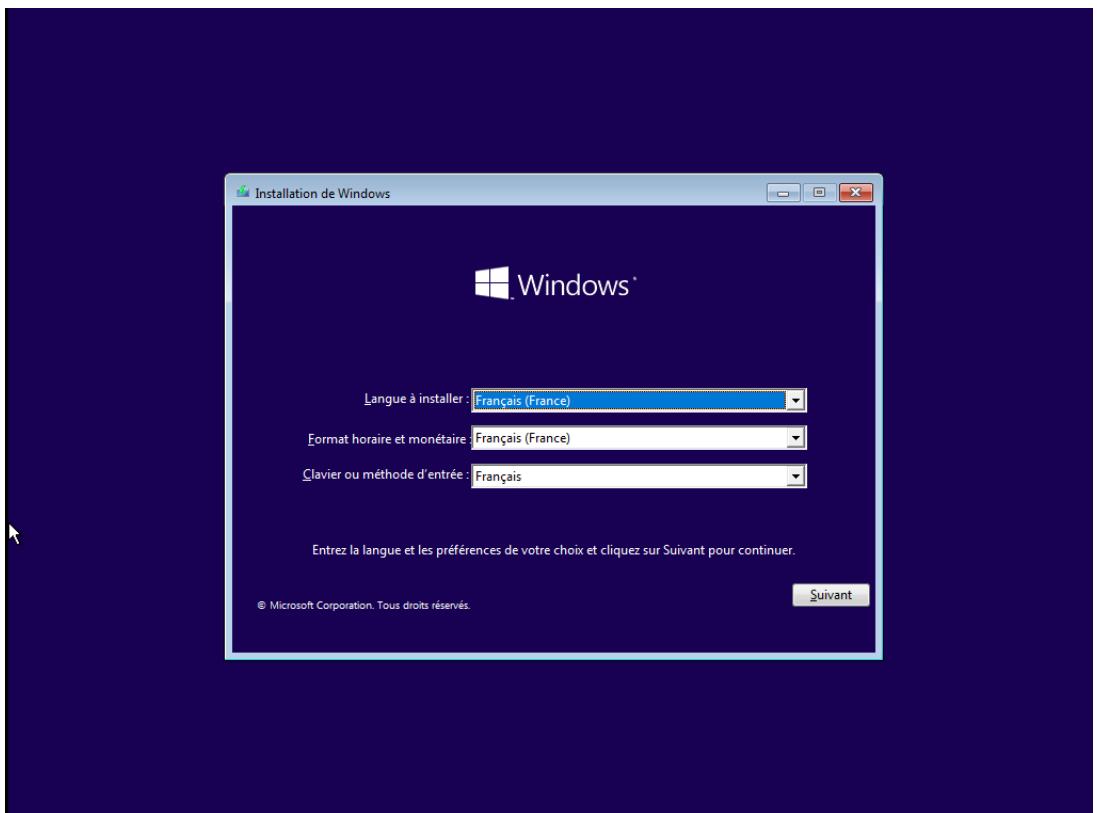
Appliquer

Ajout de Antoine dans le groupe Accueil

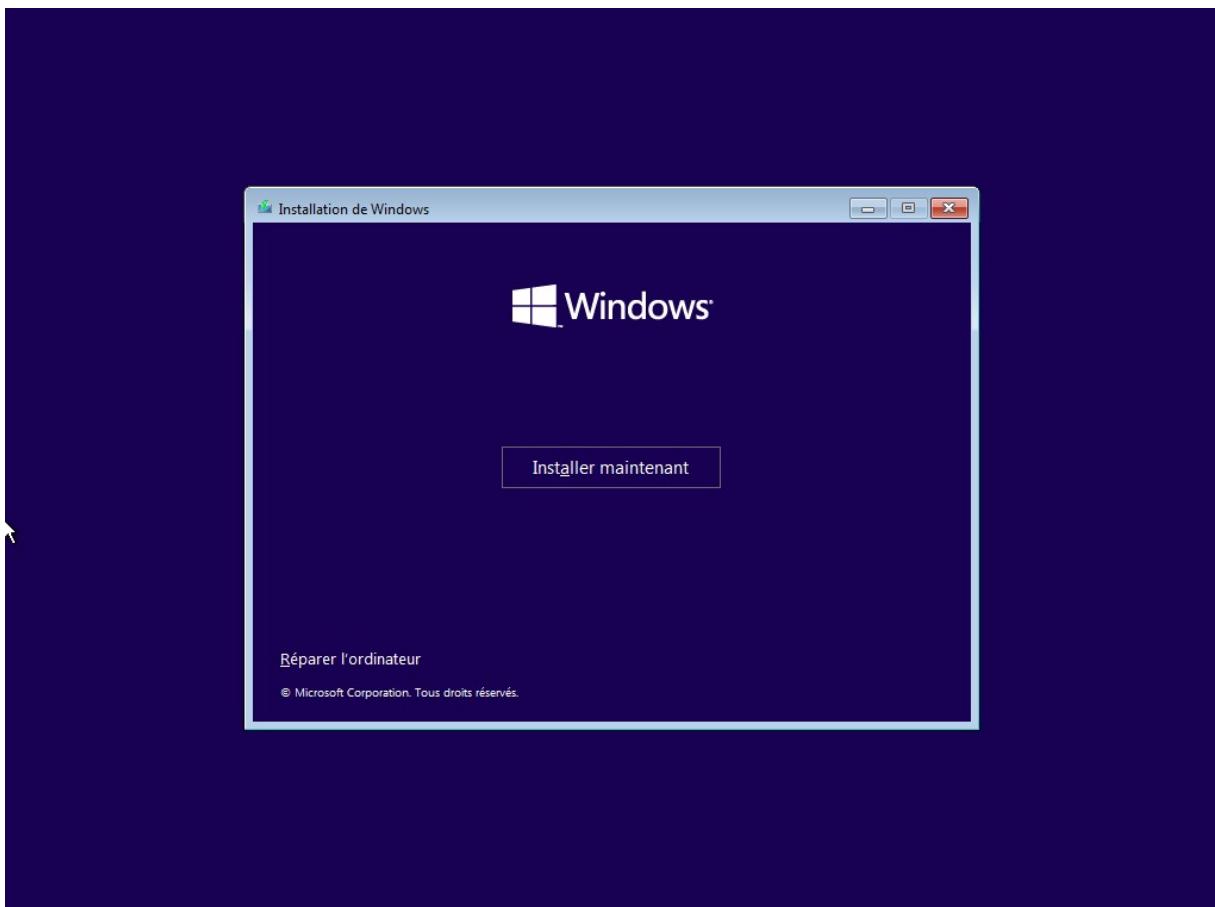
Étape 4 : Installation et Configuration d'un poste Client

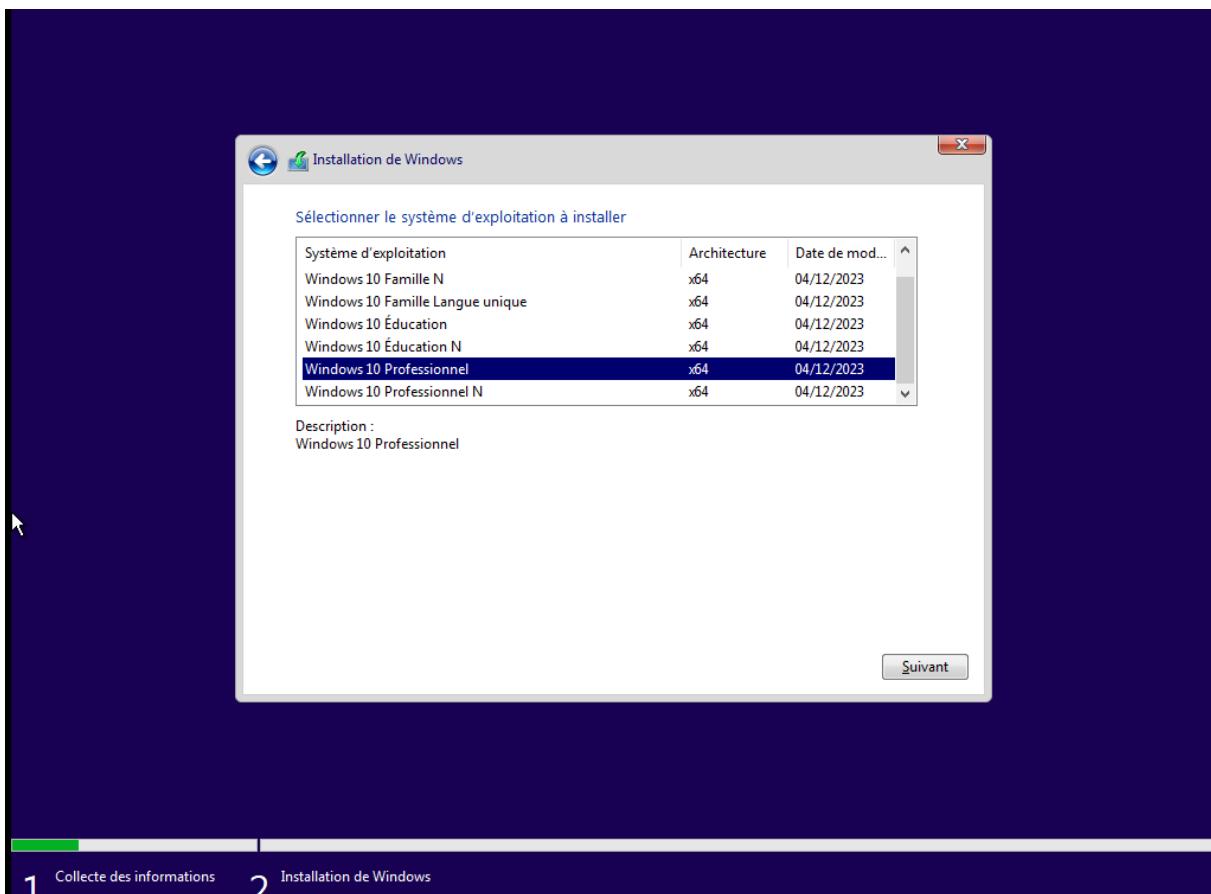


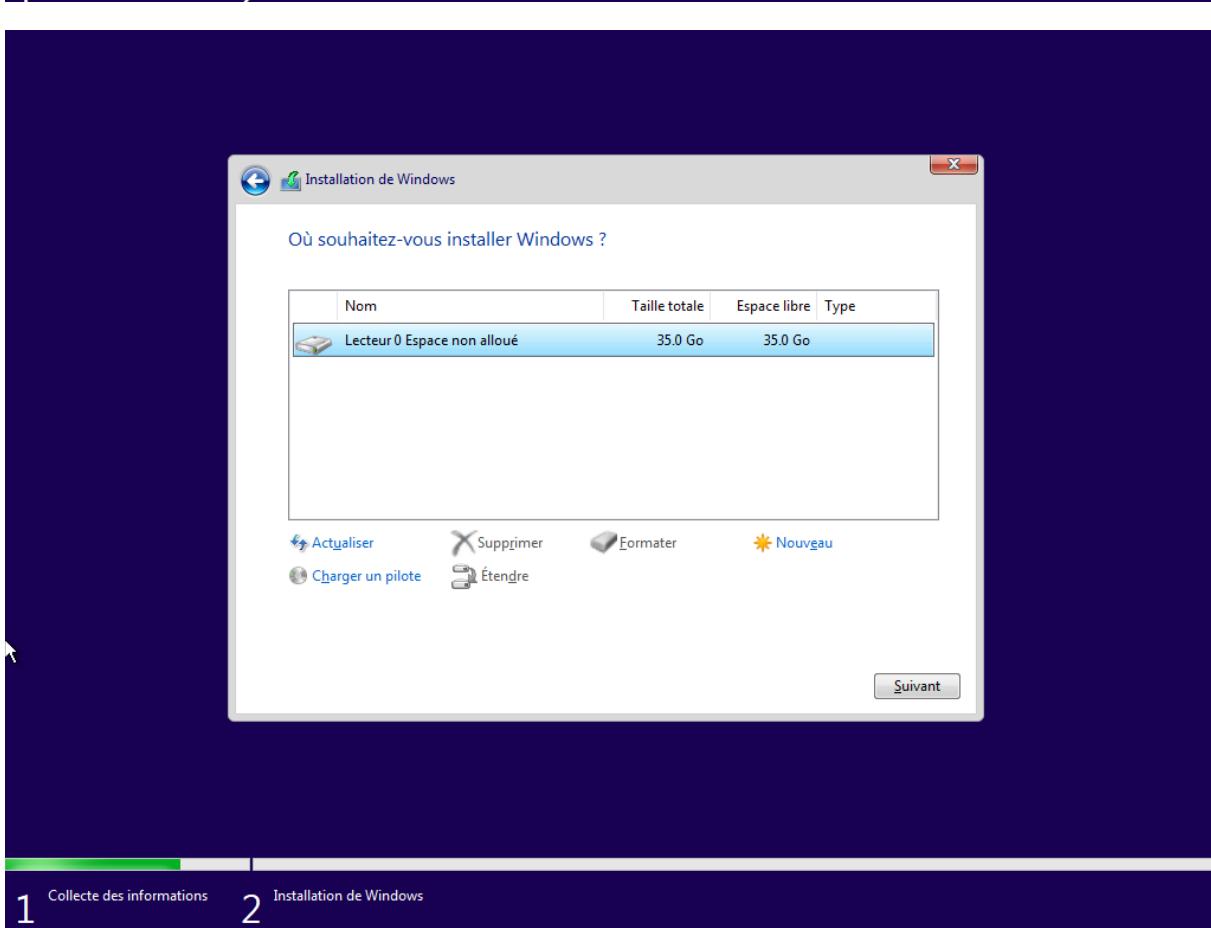
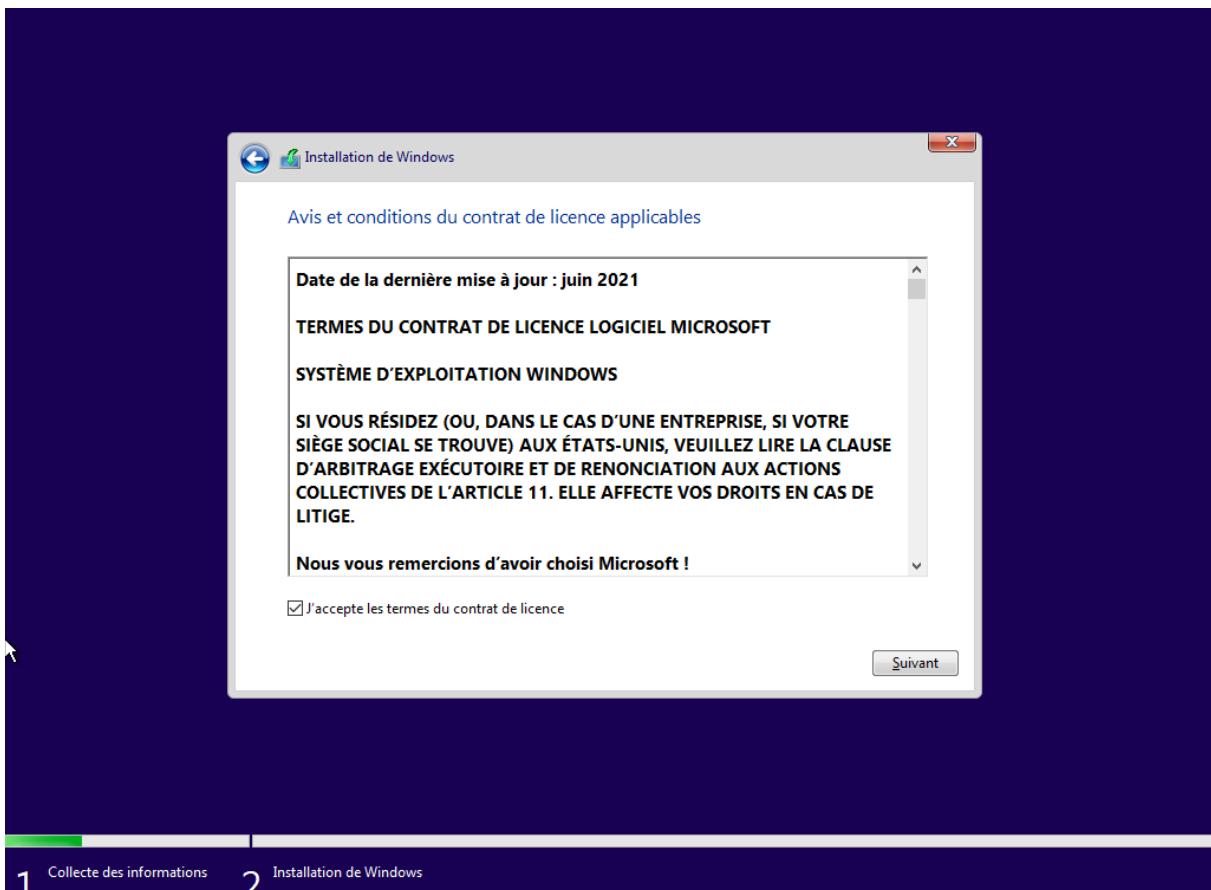
Dans les paramètres de la VM, mise en place du Network adaptator en LAN afin qu'il puisse accéder au réseau

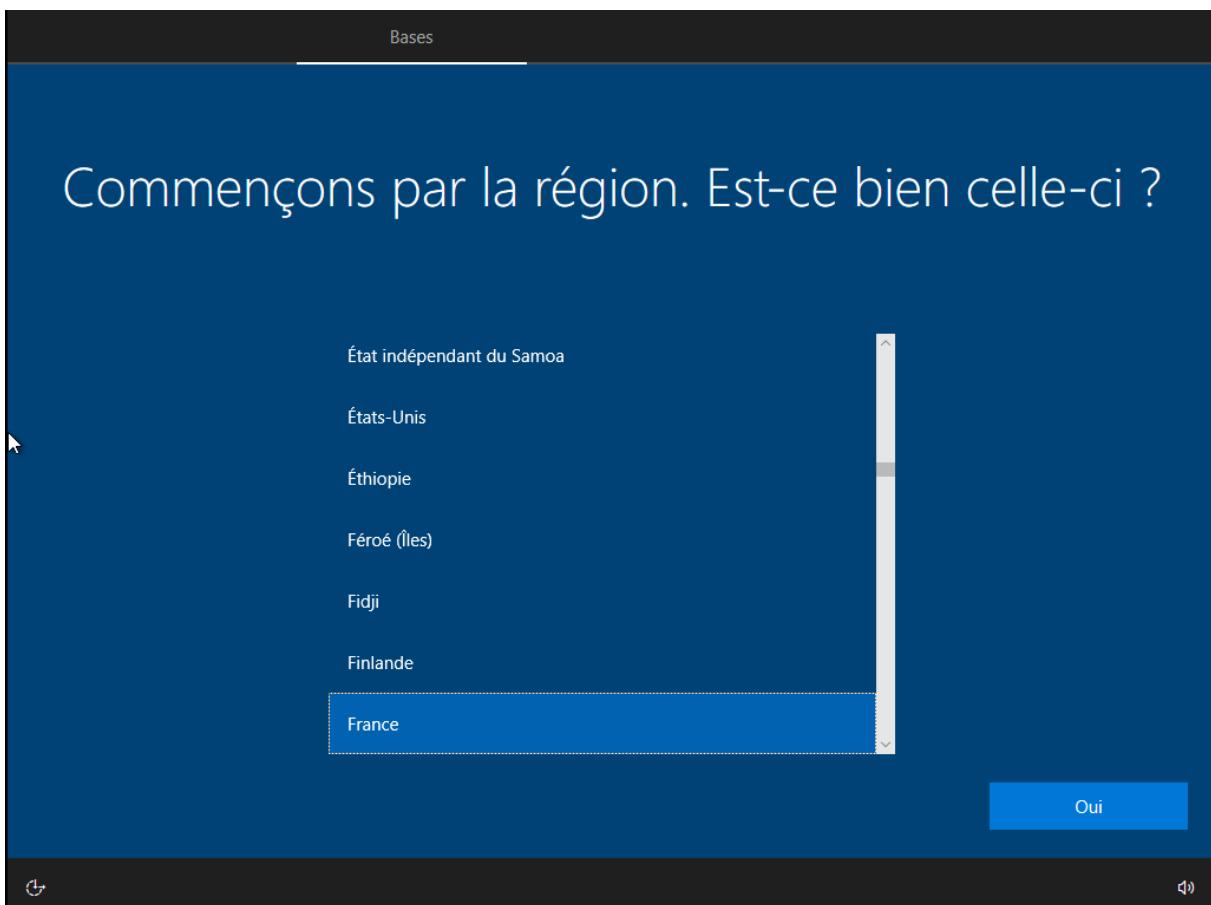
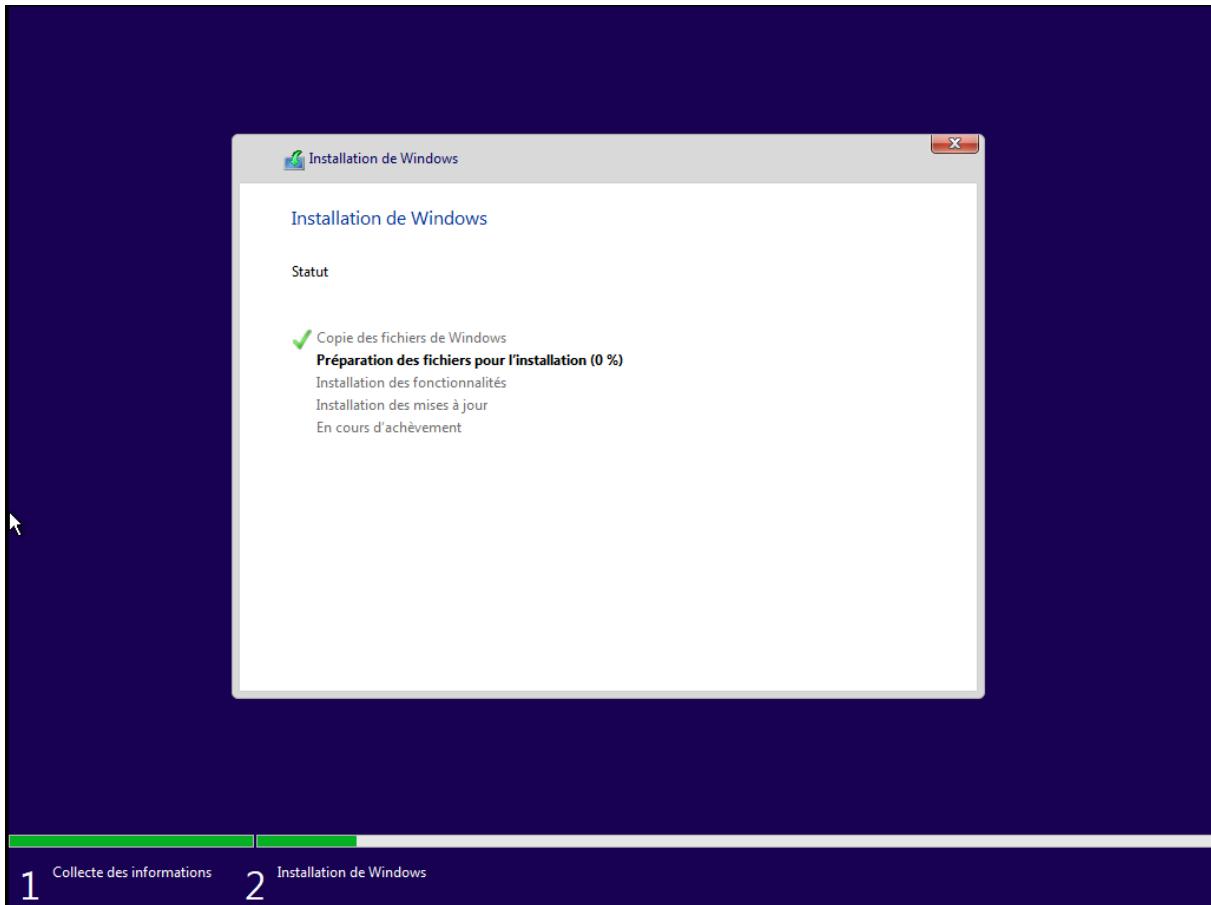


Installation de Windows 10









Bases

Est-ce la bonne disposition de clavier ?

Si vous utilisez également une autre disposition de clavier, vous pouvez l'ajouter après.

Français

Belge (virgule)

Français (Belgique)

Français (Suisse)

Français traditionnel (Canada)

Albanais

Allemand

Oui

Compte

Qui sera amené à utiliser ce PC ?

Quel nom voulez-vous utiliser ?



test

X

Suivant

Autoriser Microsoft et les applications à utiliser votre emplacement

Choisissez vos paramètres, puis sélectionnez « Accepter » pour les enregistrer. Consultez le lien « En savoir plus » pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.



Oui

Obtenez des expériences basées sur les emplacements comme des itinéraires et des prévisions météo. Laissez Windows et les applications vous demander votre emplacement. Microsoft utilisera les données d'emplacement pour améliorer les services de localisation.



Non

Vous ne pourrez pas obtenir d'expériences basées sur les emplacements, comme des itinéraires et des prévisions météo, ni profiter d'autres services nécessitant votre emplacement pour fonctionner.

[En savoir plus](#)

[Accepter](#)

```
C:\> Invite de commandes
Microsoft Windows [version 10.0.19045.3803]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\test>ipconfig

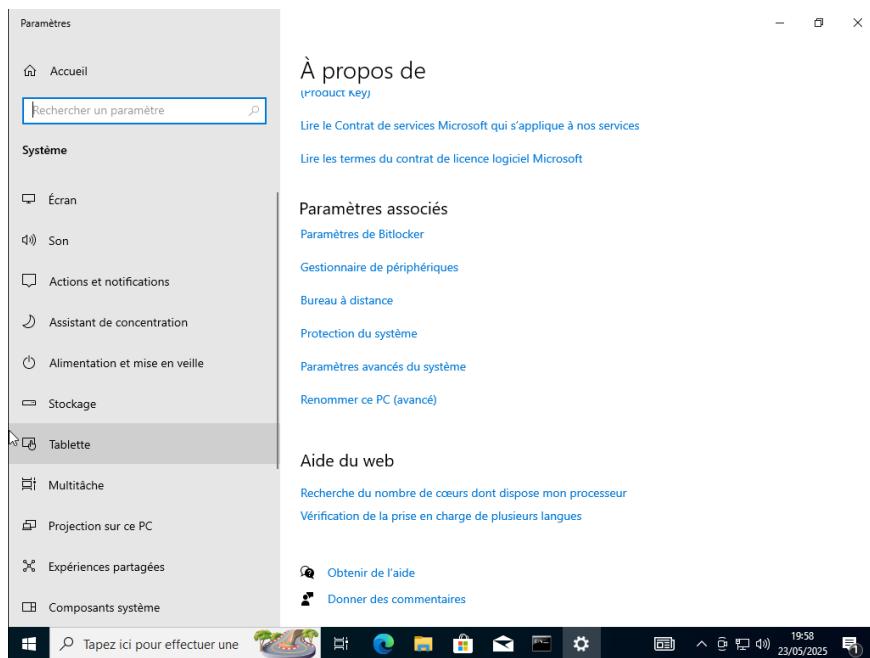
Configuration IP de Windows

Carte Ethernet Ethernet0 :

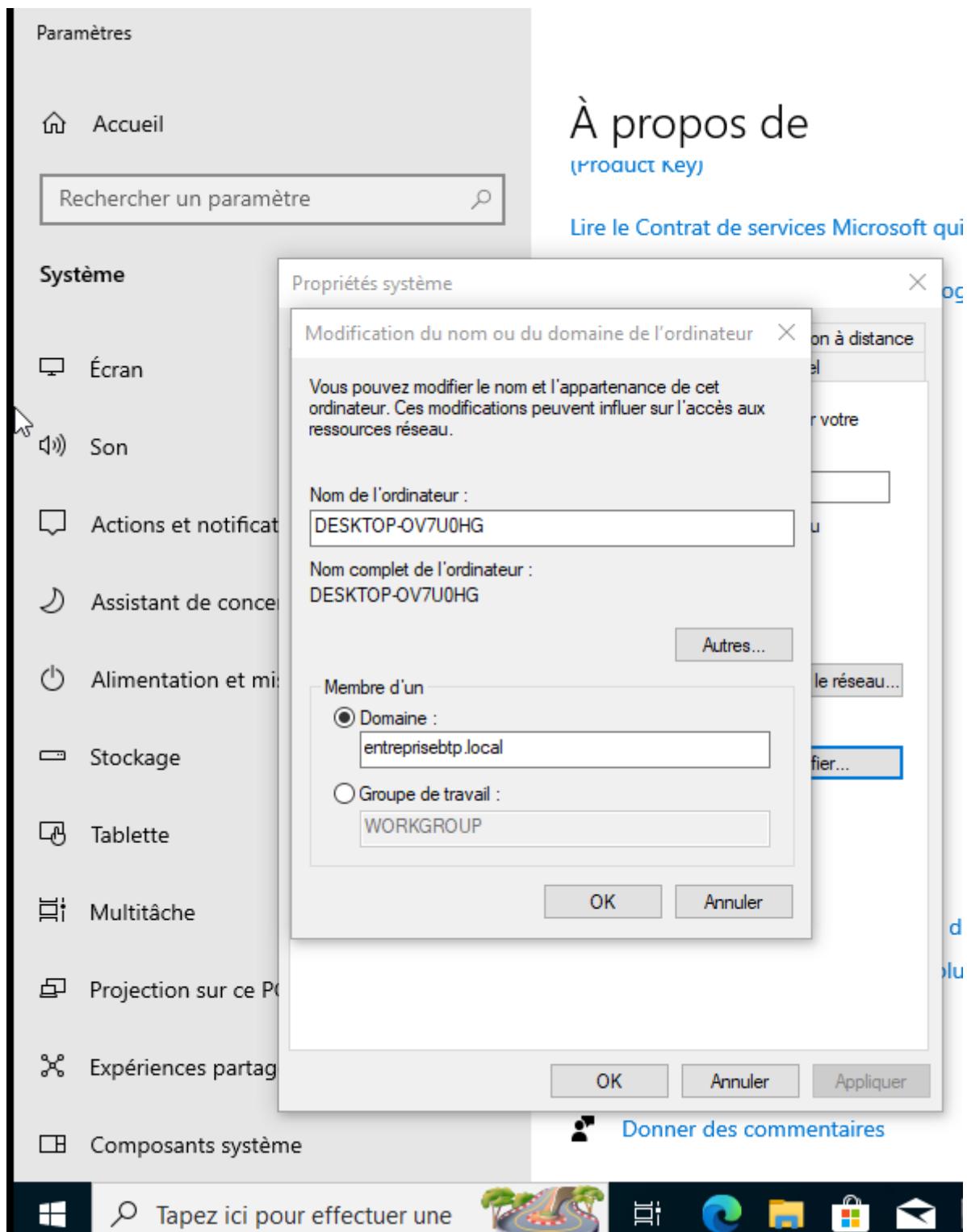
    Suffrage DNS propre à la connexion. . . . . : entrepriseBTP.local
    Adresse IPv6 de liaison locale. . . . . : fe80::fcd3:ff97:35ba:cc08%12
    Adresse IPv4. . . . . : 10.0.0.50
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : fe80::20c:29ff:fee7:df3a%12
                                         10.0.0.1

C:\Users\test>
```

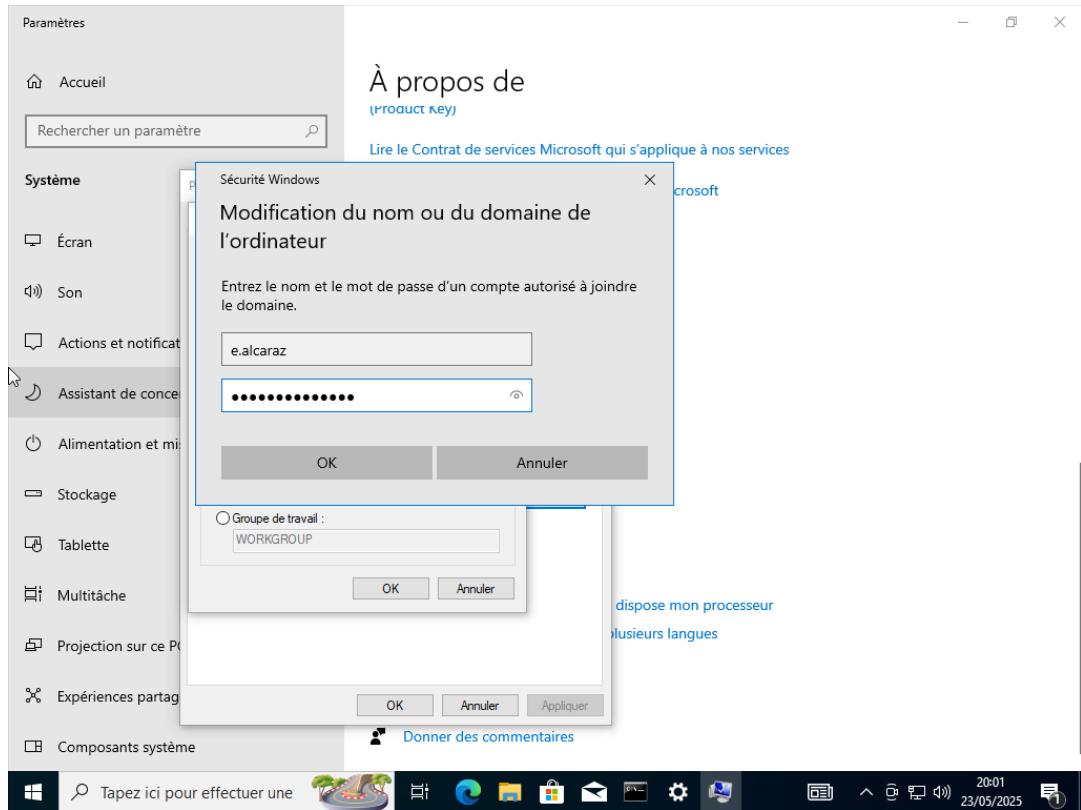
Une fois l'installation terminé, nous pouvons voir que le pc a bien pris la bonne adresse ip venant du DHCP



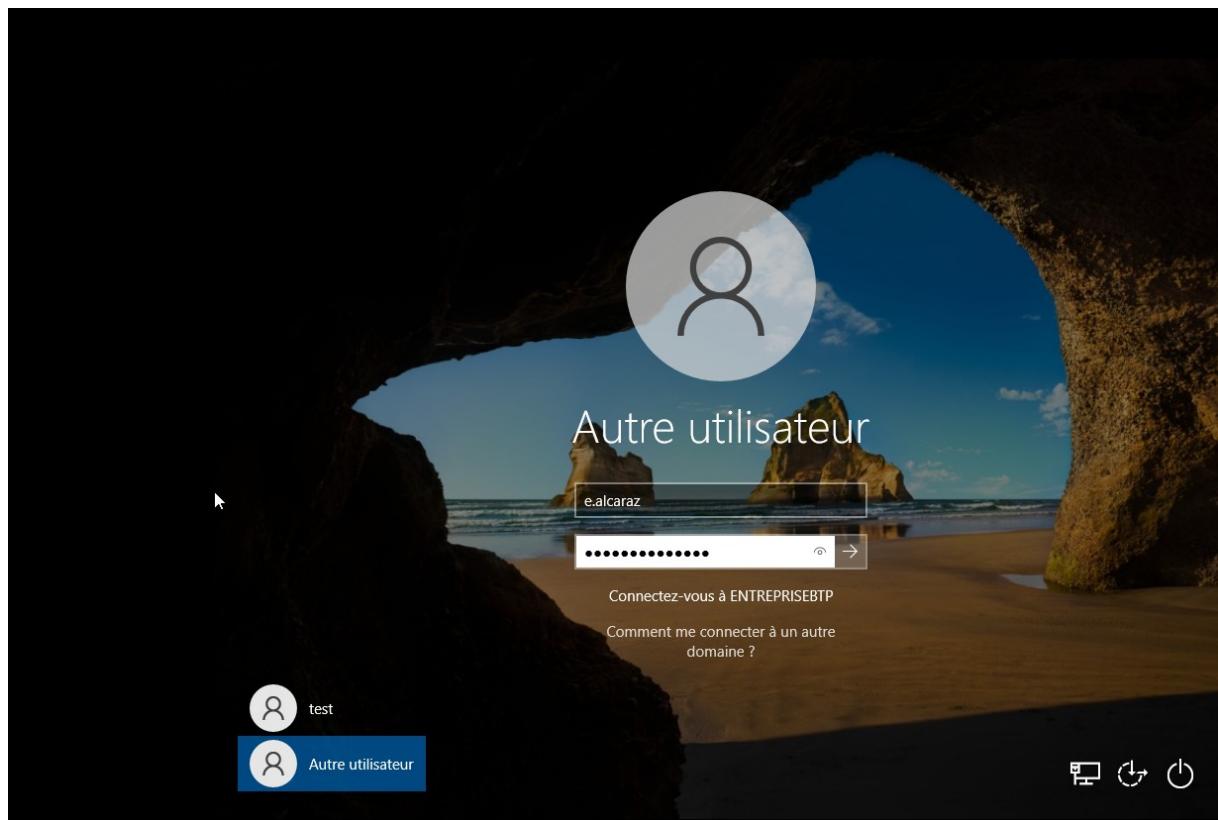
Dans les paramètres nous allons joindre le pc au domaine

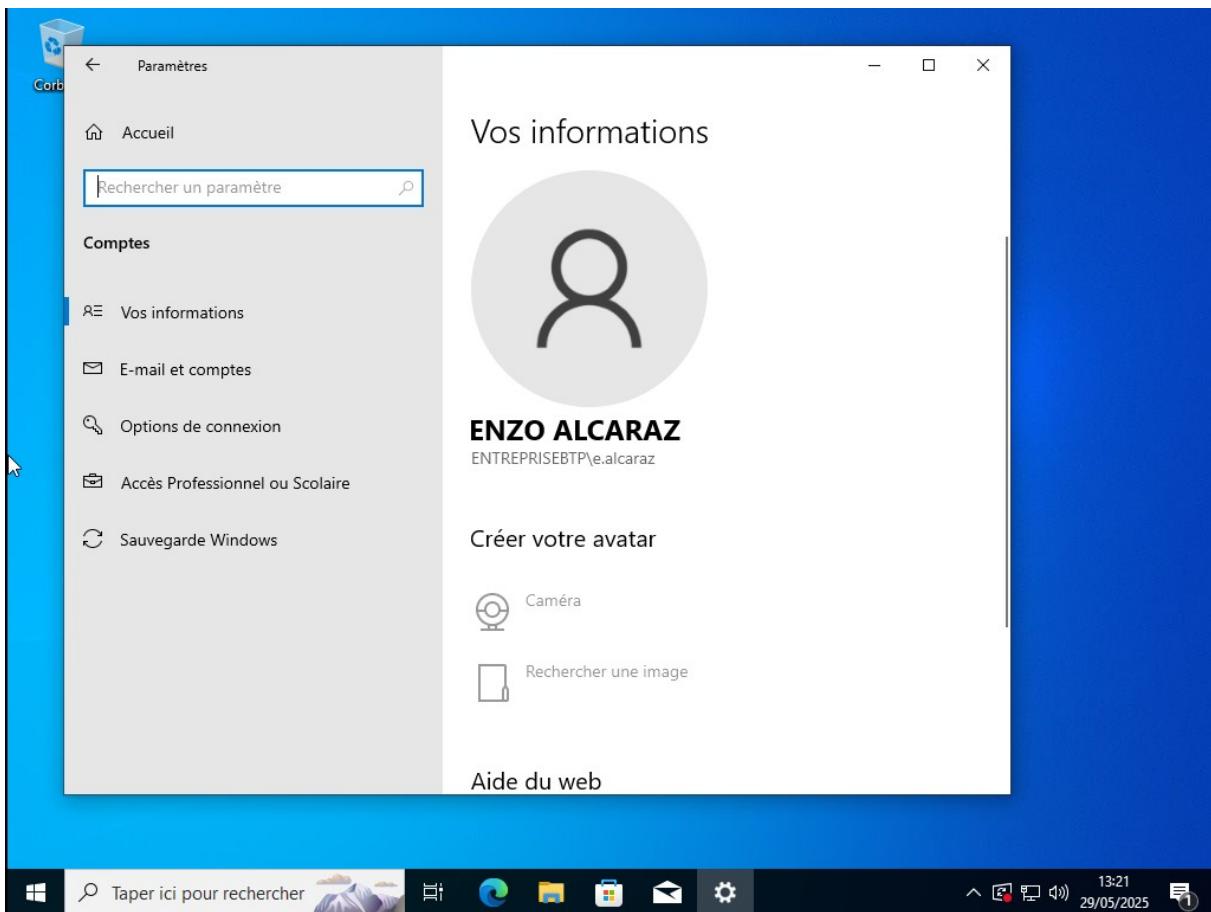


On rentre les coordonnées du domaines



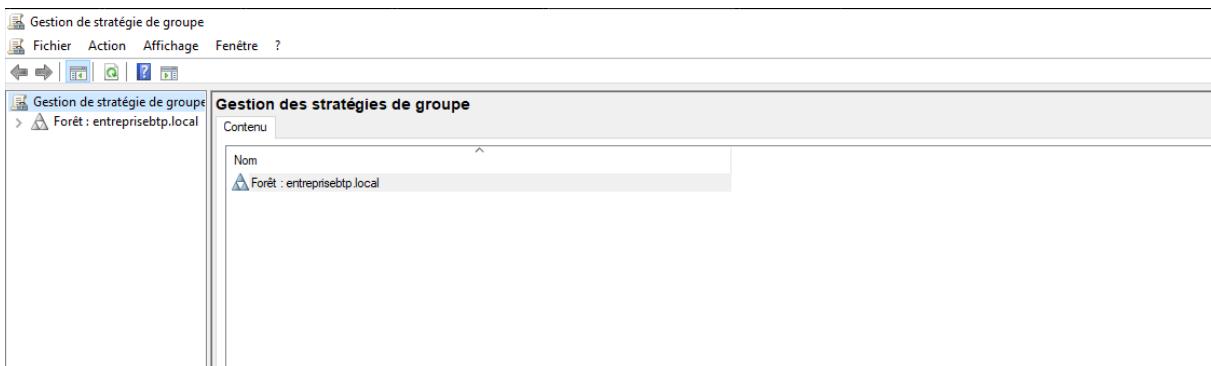
Nous allons nous connecter avec l'utilisateur Enzo Alcaraz

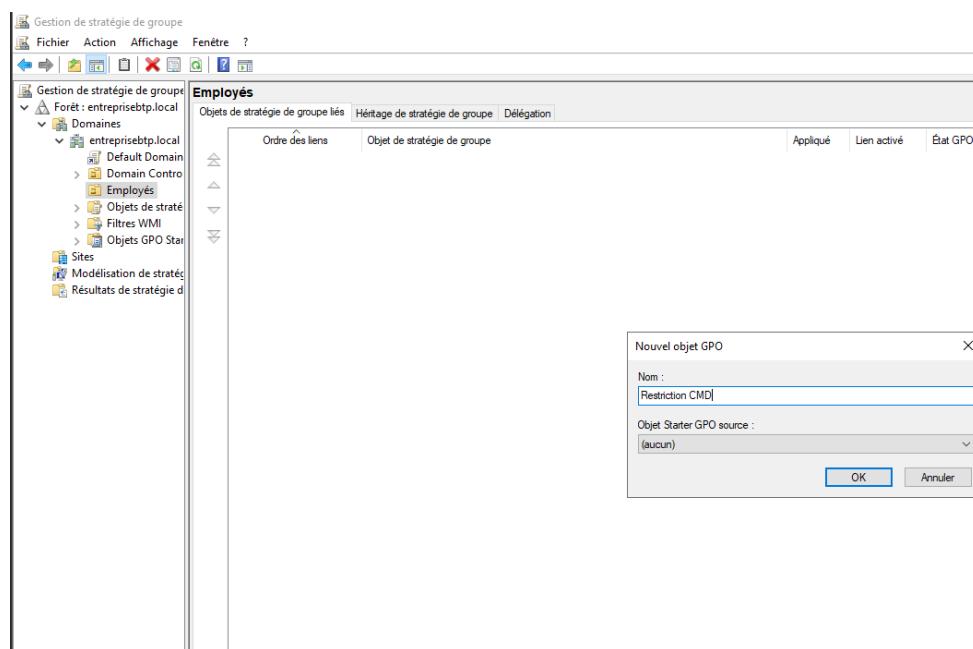
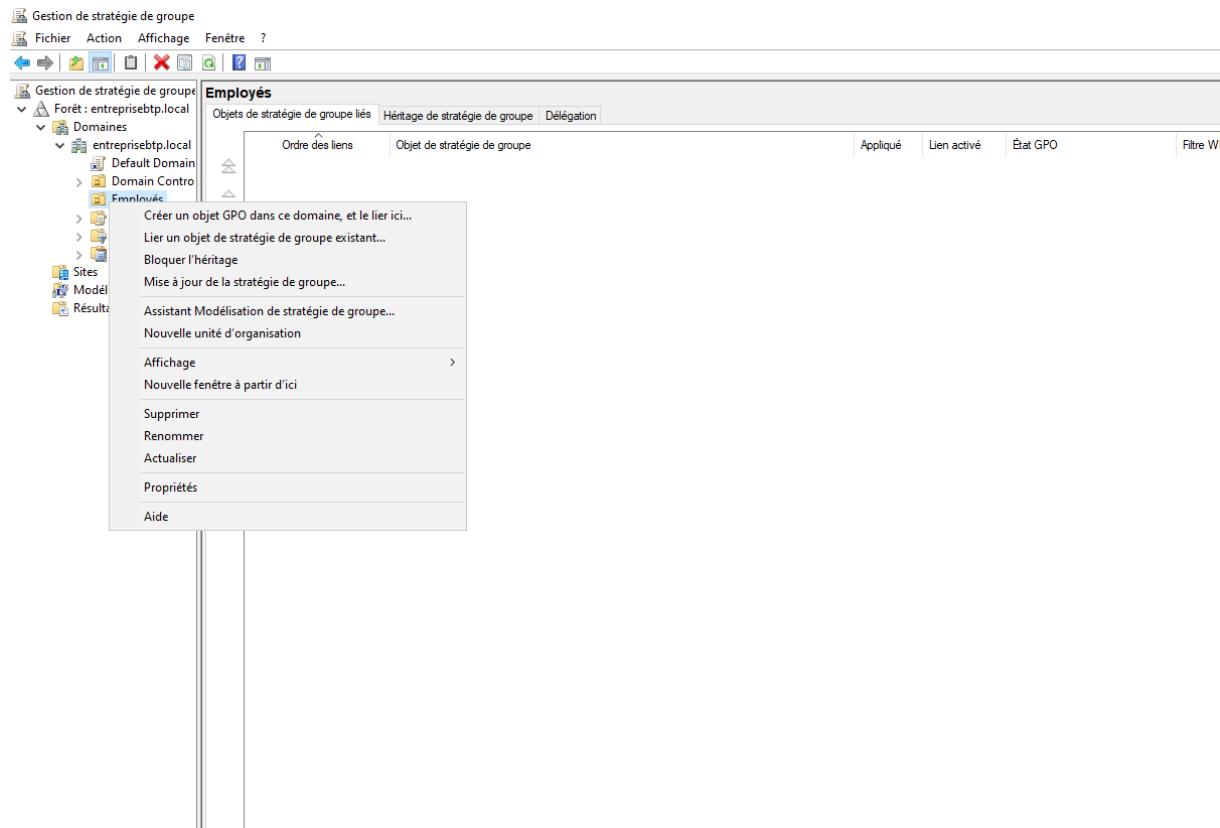




Une fois sur la session de l'utilisateur nous pouvons voir que l'utilisateur est bien dans le domaine

Création de GPO





Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

Forêt : entreprisebtp.local

Domaines

- entreprisebtp.local
 - Default Domain Policy
 - Domain Controllers
 - Employés
 - Restriction CMD
 - Objets de stratégie de groupe
 - Filtres WMI
 - Objets GPO Starter
- Sites
- Modélisation de stratégie de groupe
- Résultats de stratégie de groupe

Employés

Objets de stratégie de groupe liés Héritage de stratégie de groupe Délégation

Ordre des liens	Objet de stratégie de groupe	Appliqué	Lien activé	État GPO
1	Restriction CMD	Non	Oui	Activé

Modifier
Appliquée
Lien activé
Enregistrer le rapport...
Supprimer
Renommer
Actualiser

Stratégie Restriction CMD (SRV-AD.ENTREPRISEBTP.LOCAL)

Configuration ordinateur

- Stratégies
- Préférences
- Configuration utilisateur
 - Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Modèles d'administration : définitions de stratégies
 - Bureau
 - Composants Windows
 - Dossiers partagés
 - Menu Démarrer et barre des tâches
 - Panneau de configuration
 - Réseau
 - Système
 - Accès au stockage amovible
 - Affichage
 - Gestion de l'alimentation
 - Gestion de la communication Internet
 - Installation de pilotes
 - Options Ctrl+Alt+Suppr
 - Options d'atténuation
 - Ouverture de session
 - Profils utilisateur
 - Redirection de dossiers
 - Scripts
 - Services Paramètres régionaux
 - Stratégie de groupe
- Tous les paramètres
- Préférences

Système

Désactiver l'accès à l'invite de commandes

Modifier [le paramètre de stratégie](#)

Configuration requise : Au minimum Windows 2000

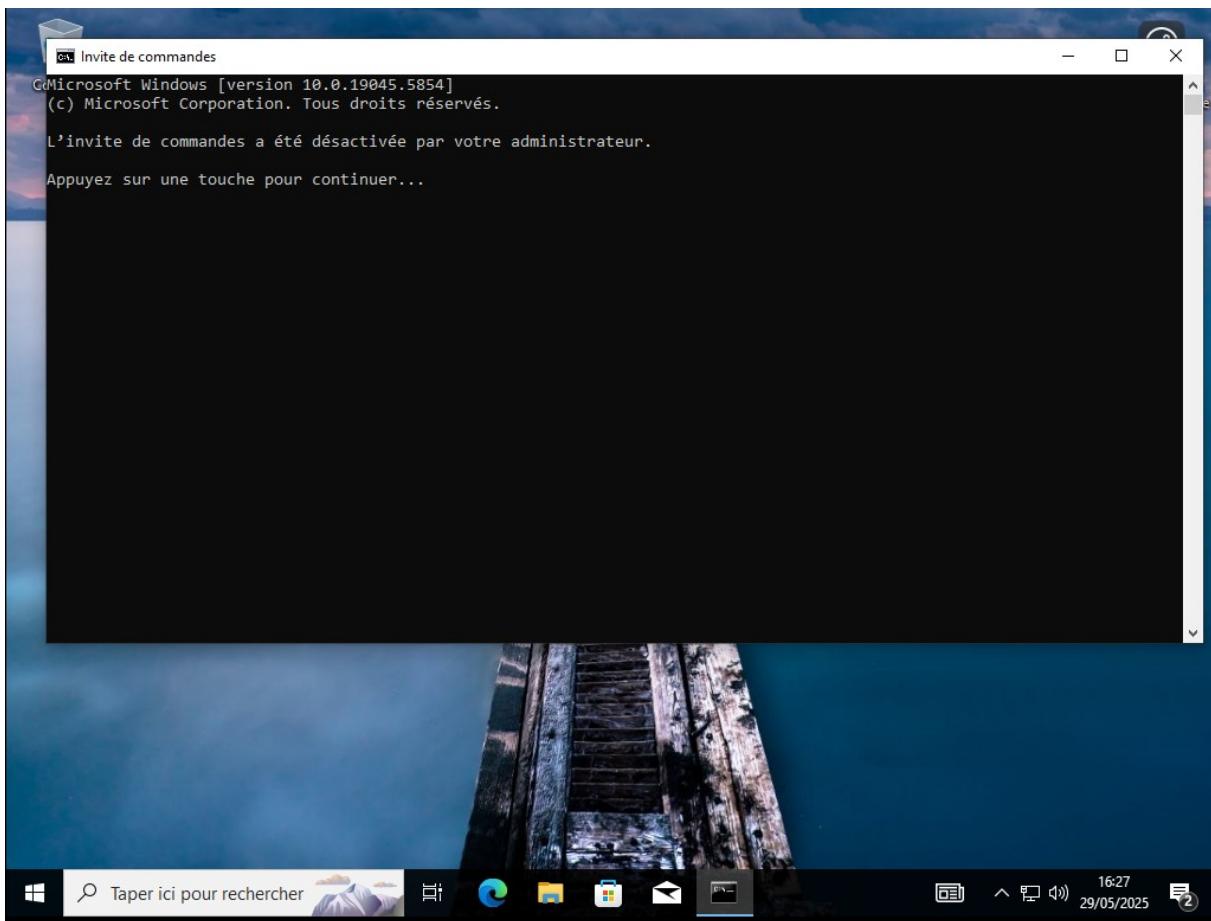
Description : Ce paramètre de stratégie empêche les utilisateurs d'exécuter l'invite de commande interactive, Cmd.exe. Ce paramètre de stratégie indique également s'il est permis d'exécuter ou non les fichiers de commandes (.cmd et .bat) sur l'ordinateur.

Si vous activez ce paramètre de stratégie et que l'utilisateur essaie d'ouvrir une fenêtre de commande, le système affiche un message signalant qu'un paramètre bloque l'action.

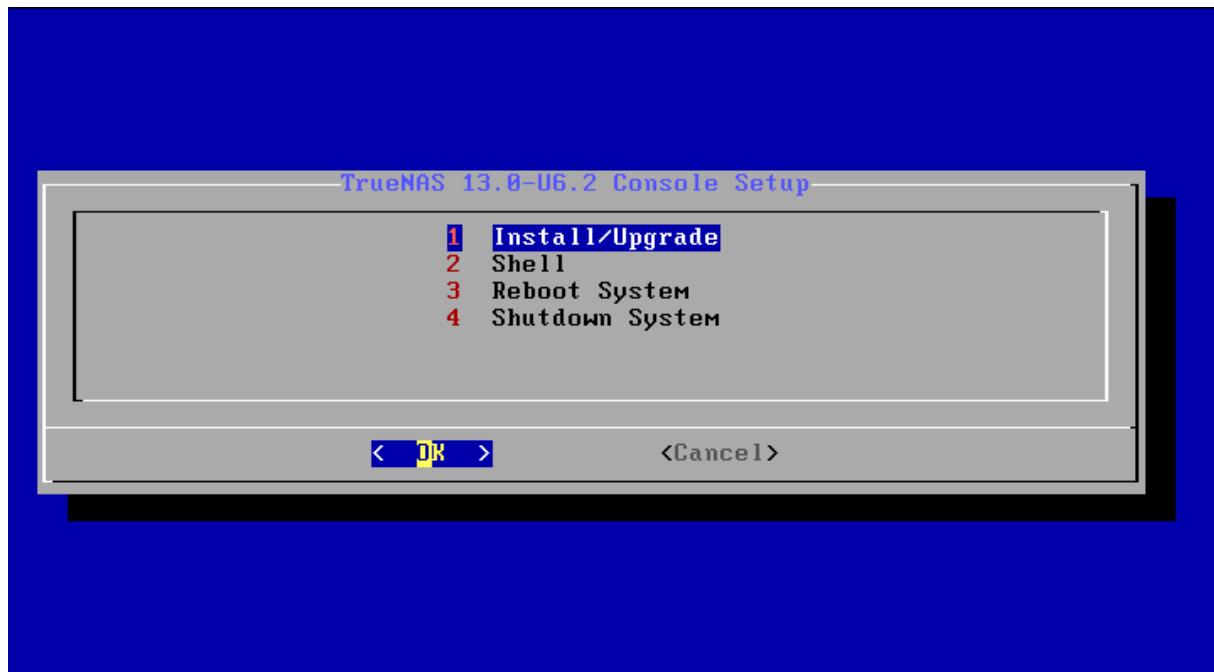
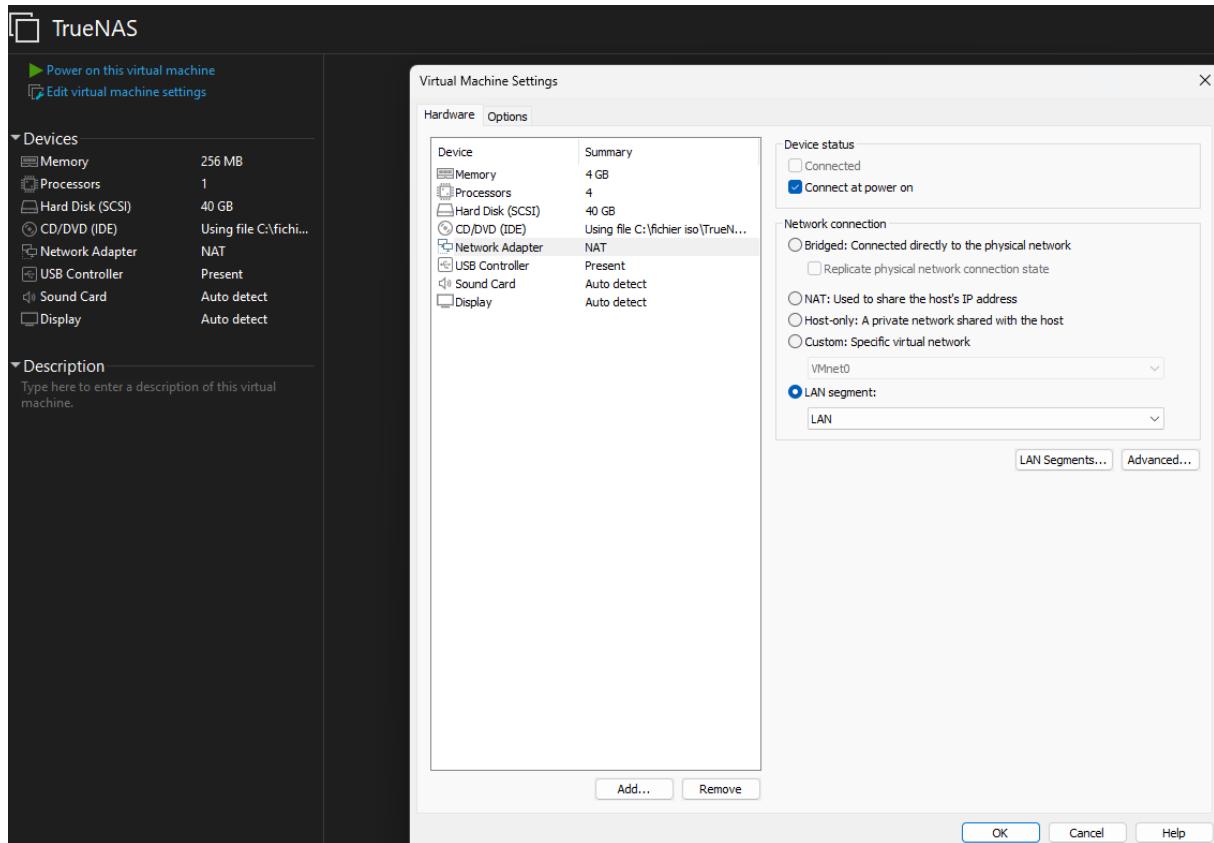
Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter normalement Cmd.exe et des fichiers de commandes.

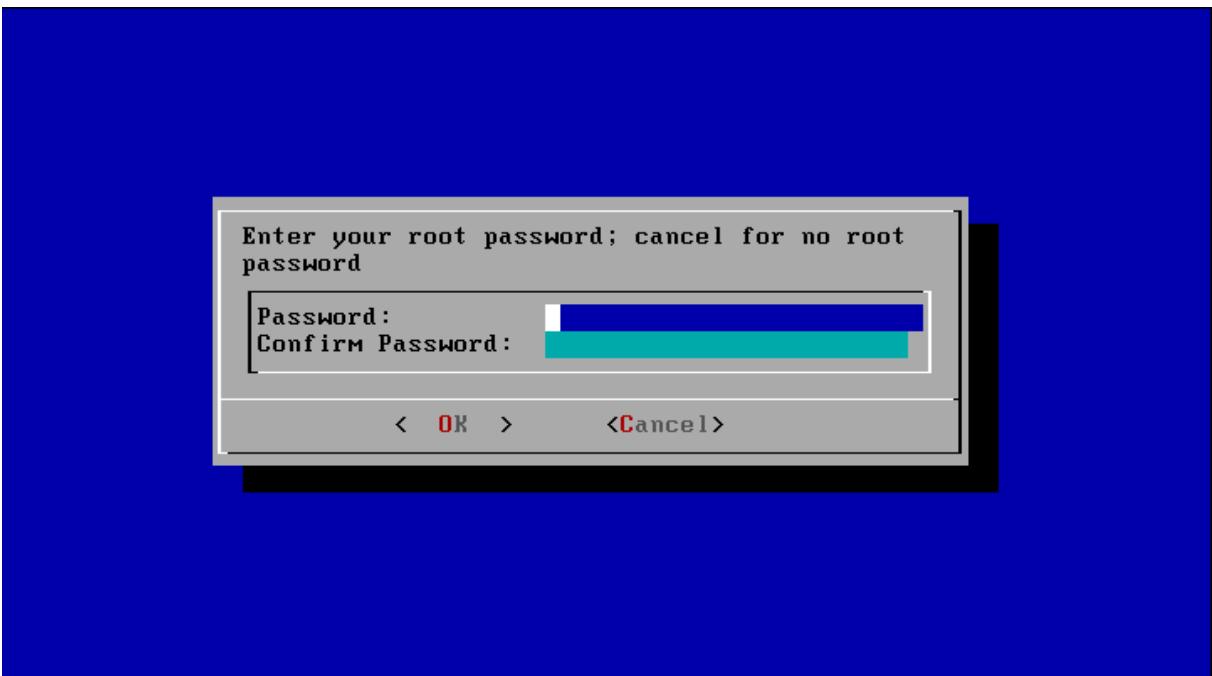
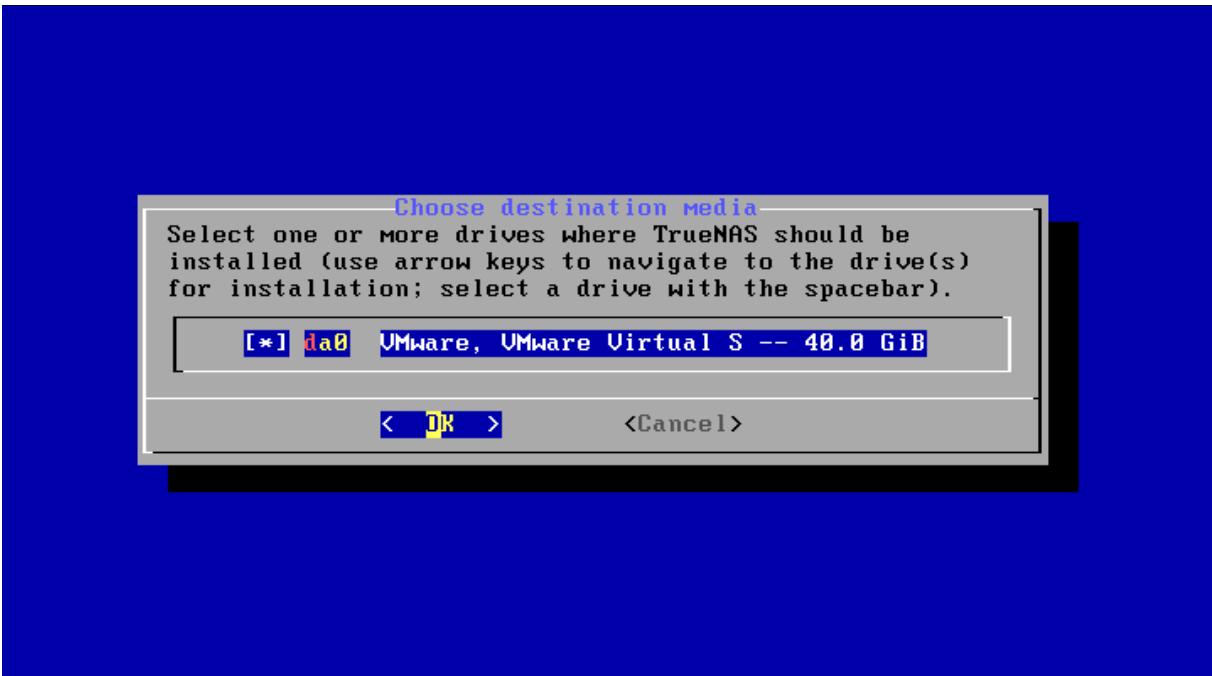
Remarque : n'empêche pas l'exécution des fichiers de commandes sur l'ordinateur si celui-ci utilise des scripts de fichiers de commandes pour la connexion, la déconnexion, le démarrage ou l'arrêt, ou pour les utilisateurs ayant recours aux services Bureau à distance.

Paramètre	État	Commentaire
Accès au stockage amovible	Non configuré	Non
Affichage	Non configuré	Non
Gestion de l'alimentation	Non configuré	Non
Gestion de la communication Internet	Non configuré	Non
Installation de pilotes	Non configuré	Non
Options Ctrl+Alt+Suppr	Non configuré	Non
Options d'atténuation	Non configuré	Non
Ouverture de session	Non configuré	Non
Profils utilisateur	Non configuré	Non
Redirection de dossiers	Non configuré	Non
Scripts	Non configuré	Non
Services Paramètres régionaux	Non configuré	Non
Stratégie de groupe	Non configuré	Non
Télécharger les composants manquants	Non configuré	Non
Interprétation du siècle pour l'an 2000	Non configuré	Non
Restreindre l'exécution de ces programmes à partir de l'aide	Non configuré	Non
Ne pas afficher l'écran de démarrage Mise en route à l'ouvert...	Non configuré	Non
Interface utilisateur personnalisée	Non configuré	Non
Désactiver l'accès à l'invite de commandes	Non configuré	Non
Empêche l'accès aux outils de modifications du Registry	Non configuré	Non
Ne pas exécuter les applications Windows spécifiées	Non configuré	Non
Exécuter uniquement les applications Windows spécifiées	Non configuré	Non
Mises à jour automatiques Windows	Non configuré	Non



Mise en place d'un TrueNAS





```
FreeBSD/amd64 (truenas.local) (ttyv0)
```

```
Console setup
```

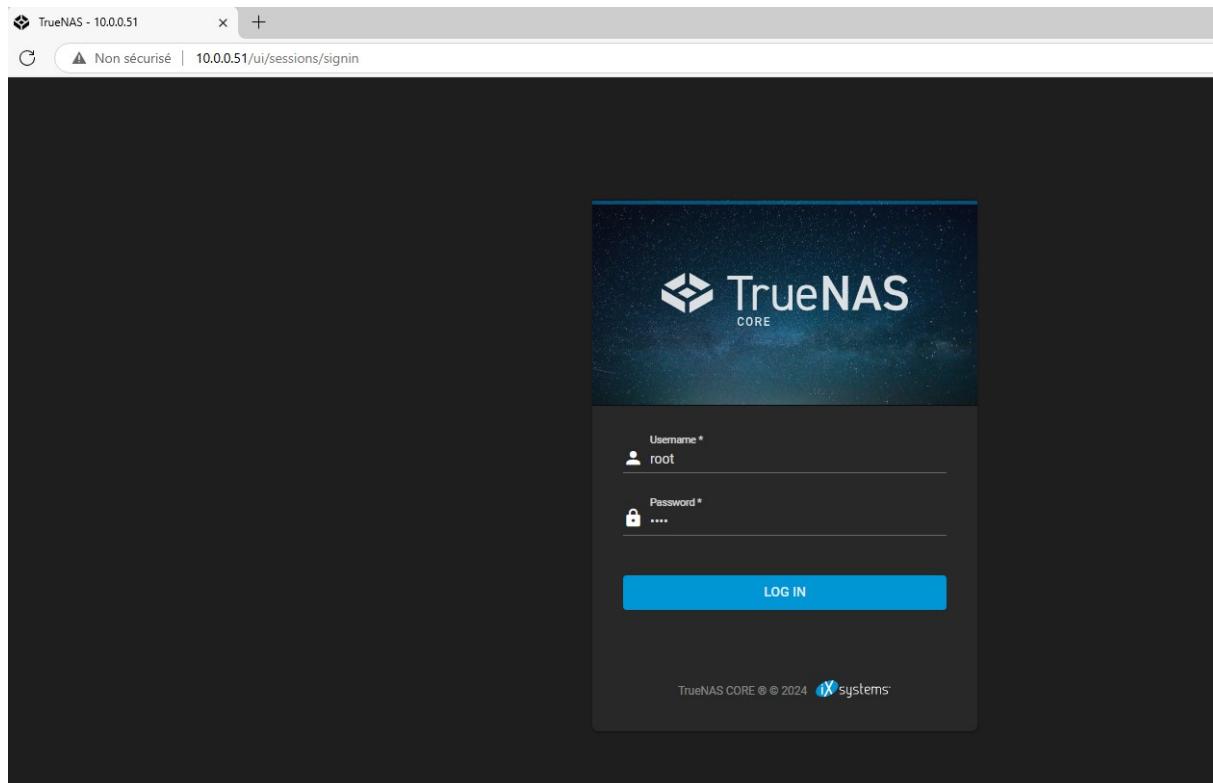
- ```

1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down
```

```
The web user interface is at:
```

```
http://10.0.0.51
https://10.0.0.51
```

```
Enter an option from 1-11: █
```



Storage / Pools

TrueNAS CORE® © 2024 - IXsystems, Inc.

| Pools                                    |            |                                                |           |             |                   |          |       |          |
|------------------------------------------|------------|------------------------------------------------|-----------|-------------|-------------------|----------|-------|----------|
| Partage entreprise (System Dataset Pool) |            | ONLINE ✓   6.96 MiB (0%) Used   16.95 GiB Free |           |             |                   |          |       |          |
| Name                                     | Type       | Used                                           | Available | Compression | Compression Ratio | Readonly | Dedup | Comments |
| Partage entreprise                       | FILESYSTEM | 6.96 MiB                                       | 16.95 GiB | Iz4         | 18.88             | false    | OFF   | ⋮        |

Samba

Filter Samba

COLUMNS ADD ⚙️

| Name      | Path                              | Description | Enabled | ⋮ |
|-----------|-----------------------------------|-------------|---------|---|
| direction | /mnt/Partage entreprise/direction |             | yes     | ⋮ |

1 - 1 of 1

Users

Filter Users

COLUMNS ADD ⚙️

| Username  | UID  | Builtin | Full Name         | ⋮ |
|-----------|------|---------|-------------------|---|
| direction | 1000 | no      | Chef d'entreprise | ⋮ |
| root      | 0    | yes     | root              | ⋮ |

1 - 2 of 2

←  Connecter un lecteur réseau

## À quel dossier réseau voulez-vous vous connecter ?

Spécifiez la lettre désignant le lecteur et le dossier auxquels vous souhaitez vous connecter :

|           |                      |                              |
|-----------|----------------------|------------------------------|
| Lecteur : | Z:                   | ▼                            |
| Dossier : | <input type="text"/> | <a href="#">Parcourir...</a> |

Exemple : \\serveur\partage

Se reconnecter lors de la connexion

Se connecter à l'aide d'informations d'identification différentes

[Se connecter à un site Web permettant de stocker des documents et des images.](#)

[Terminer](#)

[Annuler](#)

