

Job 0	2
Introduction	2
Environnement	2
Fonctionnement et fonctionnalités	2
Avantages et inconvénients	3
Avantages :	3
Inconvénients :	3
Cas pratiques en milieu professionnel	3
Job 1	4
Installation Active Directory	4
Créer des Organisation Unite	10
Créer des groupe	11
Créer des utilisateur	12
Ajouter les utilisateur dans les groupes	13
JOB 2	16
Créer un dossier	16
Modifier les droits de partage	16
Modifier les droits ntfs	19
JOB 3	22
Entrer un poste client dans le domaine	22
Monter les lecteurs réseaux avec Sysvol	25
Mise en place d'un serveur dhcp :	28
Installation du rôle DHCP	28
Configuration du DHCP	35
Configurer le client avec dhcp	38
Pour aller plus loin scripting powershell	41
Script Déetecter les Utilisateurs inactifs.	41
Script alerte de connexion à l'active directory.	42
PingCastles	42
Conclusion :	43

Active Directory

Job 0

Introduction

Active Directory (AD) est un service d'annuaire développé par Microsoft, faisant partie intégrante de son système d'exploitation Windows Server. Il offre un ensemble de fonctionnalités permettant de gérer de manière centralisée les ressources informatiques d'une organisation, notamment les utilisateurs, les groupes, les ordinateurs et d'autres périphériques réseau.

Environnement

Active Directory repose sur une architecture distribuée, composée de plusieurs composants principaux :

1. **Domain Controller (Contrôleur de domaine)** : Les serveurs qui exécutent Active Directory et qui stockent la base de données d'annuaire, gérant ainsi les informations relatives aux objets et aux politiques de sécurité.
2. **Domain (Domaine)** : Un ensemble d'objets et de services administratifs partageant une base de données d'annuaire commune. Un domaine peut être étendu à plusieurs sites géographiques, connectés par des réseaux WAN.
3. **Forest (Forêt)** : Une collection de domaines qui partagent une structure hiérarchique commune, établissant ainsi des relations de confiance entre eux.

Fonctionnement et fonctionnalités

Les fonctionnalités clés d'Active Directory incluent :

1. **Gestion des utilisateurs et des groupes** : AD permet de créer, modifier et supprimer des comptes utilisateurs, ainsi que de gérer les droits d'accès via des groupes.
2. **Authentification et autorisation** : Il fournit des services d'authentification centralisée, permettant aux utilisateurs d'accéder à des ressources réseau en fonction de leurs permissions.
3. **Politiques de sécurité et de groupe** : Active Directory offre des outils pour définir et appliquer des politiques de sécurité et de groupe sur l'ensemble des ressources de l'organisation.
4. **RéPLICATION** : Les données d'annuaire sont répliquées entre les différents domain controllers pour assurer la disponibilité et la redondance.

5. **Intégration avec d'autres services Microsoft** : AD s'intègre étroitement avec d'autres services Microsoft tels que Exchange Server, SharePoint, et Office 365.

Avantages et inconvénients

Avantages :

- **Centralisation de la gestion des ressources** : Active Directory permet une gestion centralisée des utilisateurs, des ordinateurs et des autres ressources réseau, simplifiant ainsi l'administration.
- **Sécurité renforcée** : Avec des fonctionnalités telles que la gestion des stratégies de sécurité et de groupe, AD renforce la sécurité des systèmes d'information.
- **Intégration transparente** : Il s'intègre de manière transparente avec d'autres produits Microsoft, offrant ainsi une expérience utilisateur homogène.

Inconvénients :

- **Complexité de la mise en œuvre** : La configuration initiale et la maintenance d'Active Directory peuvent être complexes, nécessitant des compétences spécialisées.
- **Dépendance à l'égard des produits Microsoft** : Active Directory étant un produit Microsoft, il peut être difficile de l'intégrer avec des solutions non-Microsoft.
- **Coût de licence** : Il peut y avoir des coûts associés à l'acquisition de licences pour Windows Server et autres produits Microsoft nécessaires à l'utilisation d'Active Directory.

Cas pratiques en milieu professionnel

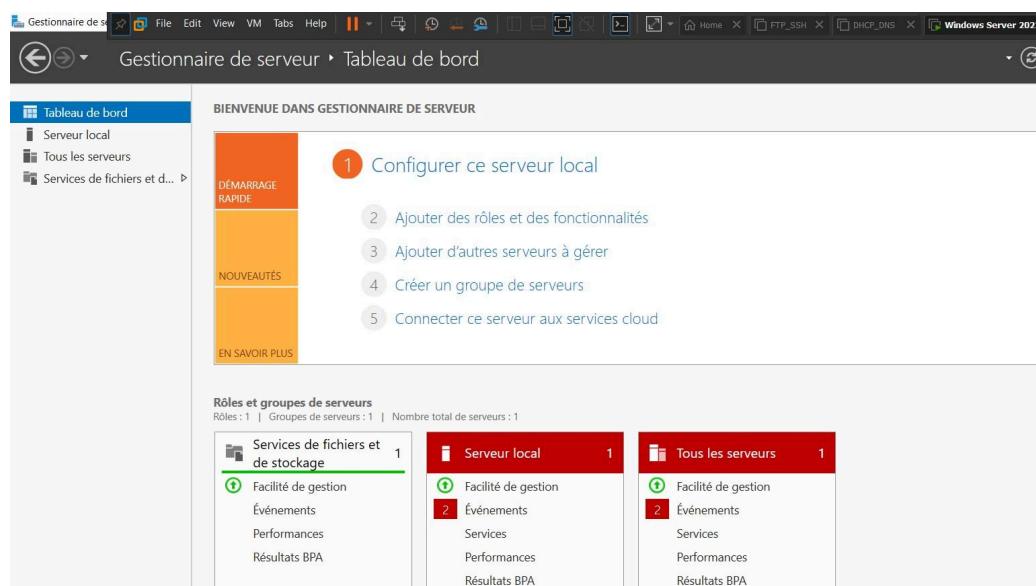
1. **Gestion des utilisateurs et des groupes** : Les administrateurs peuvent utiliser Active Directory pour créer et gérer des comptes utilisateurs, des groupes et des unités organisationnelles (OU), simplifiant ainsi la gestion des accès et des permissions.
2. **Authentification unique (SSO)** : Active Directory peut être utilisé pour mettre en place un système d'authentification unique, permettant aux utilisateurs de se connecter à différents services et applications avec un seul ensemble de identifiants.
3. **Déploiement d'applications** : Les entreprises peuvent déployer des applications via Active Directory, en utilisant les fonctionnalités de distribution de logiciels et de gestion des stratégies de groupe pour assurer une installation et une configuration uniformes.
4. **Synchronisation des annuaires** : Active Directory peut être synchronisé avec d'autres services d'annuaire tels que Azure AD ou LDAP, permettant ainsi une gestion centralisée des identités dans des environnements hybrides ou multi-cloud.
5. **Gestion des périphériques** : Active Directory peut être utilisé pour gérer et sécuriser l'accès aux périphériques réseau tels que les imprimantes, les routeurs et les commutateurs, en assignant des stratégies basées sur les utilisateurs et les groupes.

En conclusion, Active Directory est un outil puissant pour la gestion des identités et des ressources informatiques dans les environnements professionnels, offrant des fonctionnalités avancées de gestion, de sécurité et d'intégration avec d'autres services Microsoft. Cependant, sa mise en œuvre peut être complexe et nécessiter des ressources spécialisées pour une configuration et une maintenance efficaces.

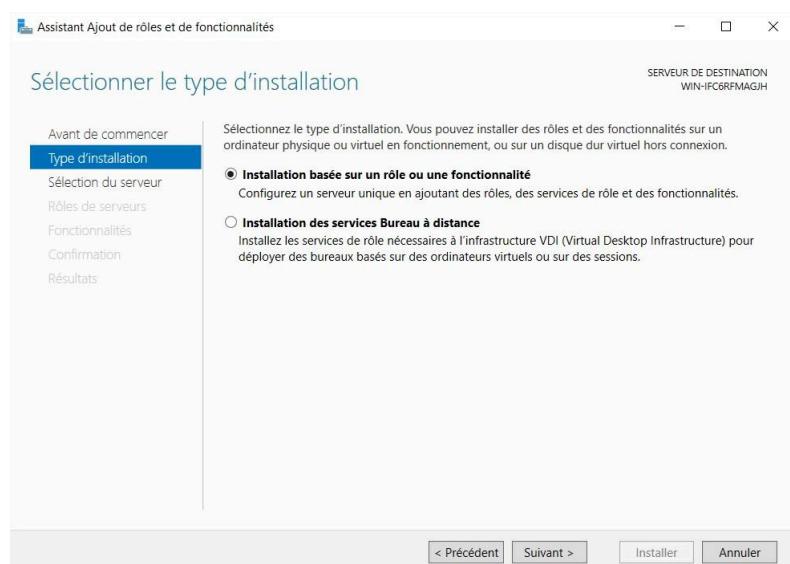
Job 1

Installation Active Directory

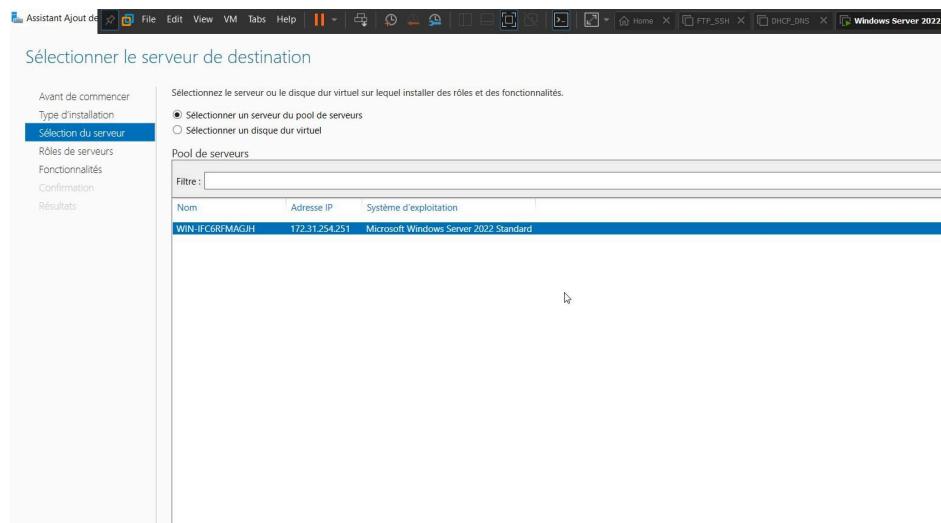
Tout d'abord ouvrir le gestionnaire de serveur.



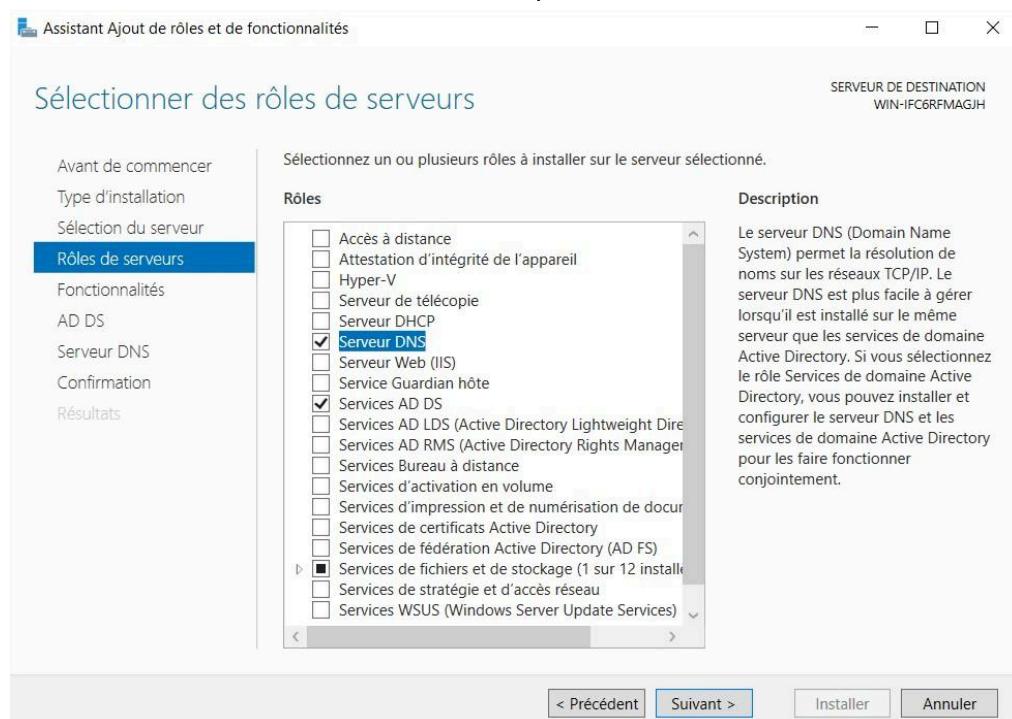
Sélectionner installation basée sur un rôle ou une fonctionnalité.



Sélectionner un serveur pool de serveurs cliquez sur suivant.

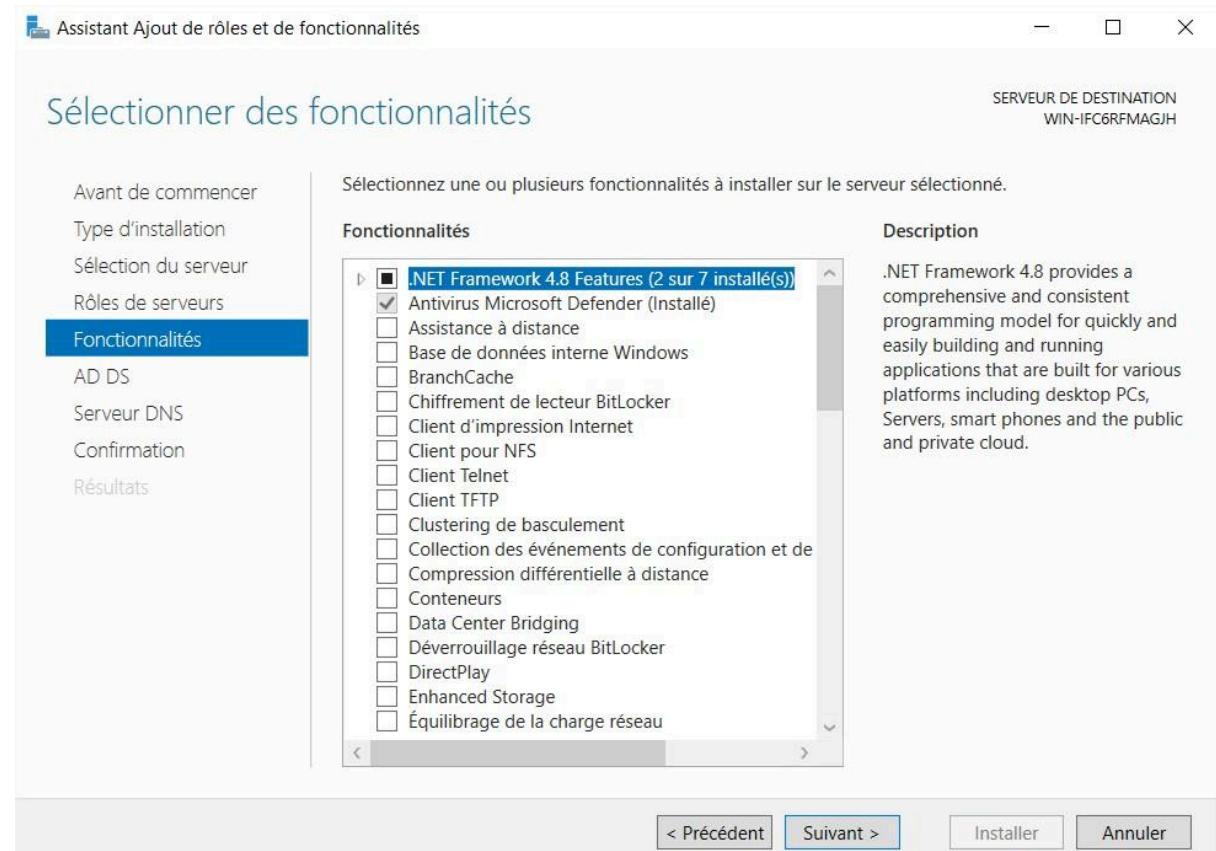


Sélectionner le rôle AD DS et DNS et cliquez sur suivant.



Allez à la page suivante pour voir la suite

Juste cliquez sur suivant.

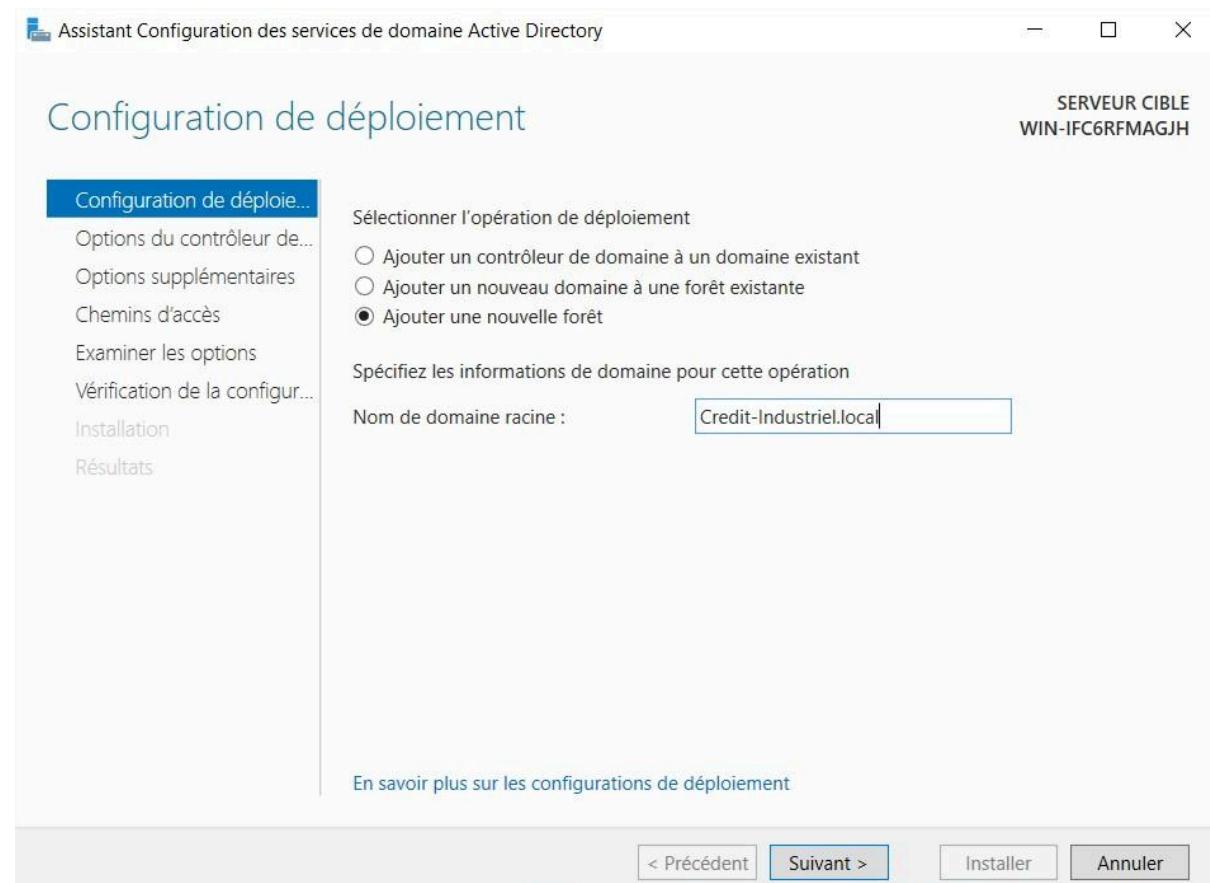


Ensuite promouvoir ce serveur en contrôleur de domaine

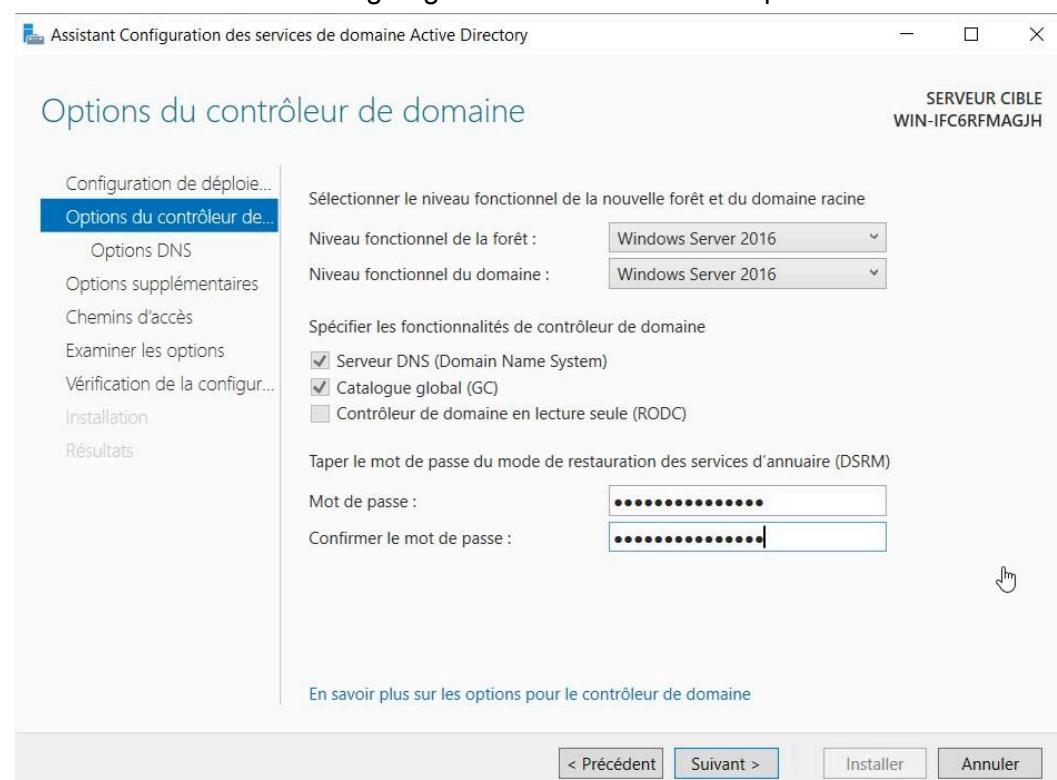


Allez à la page suivante pour voir la suite

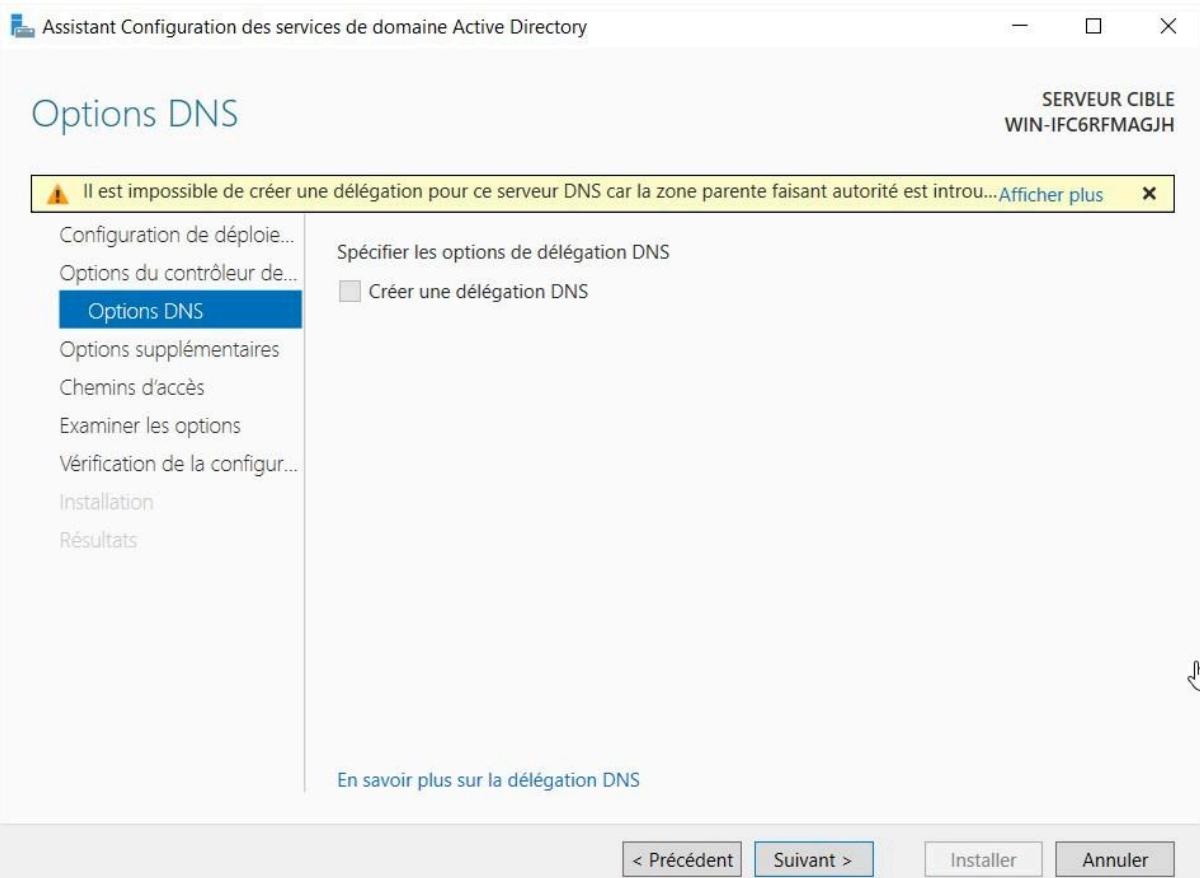
Ensuite créer une nouvelle forêt et nommer la puis cliquer sur suivant.



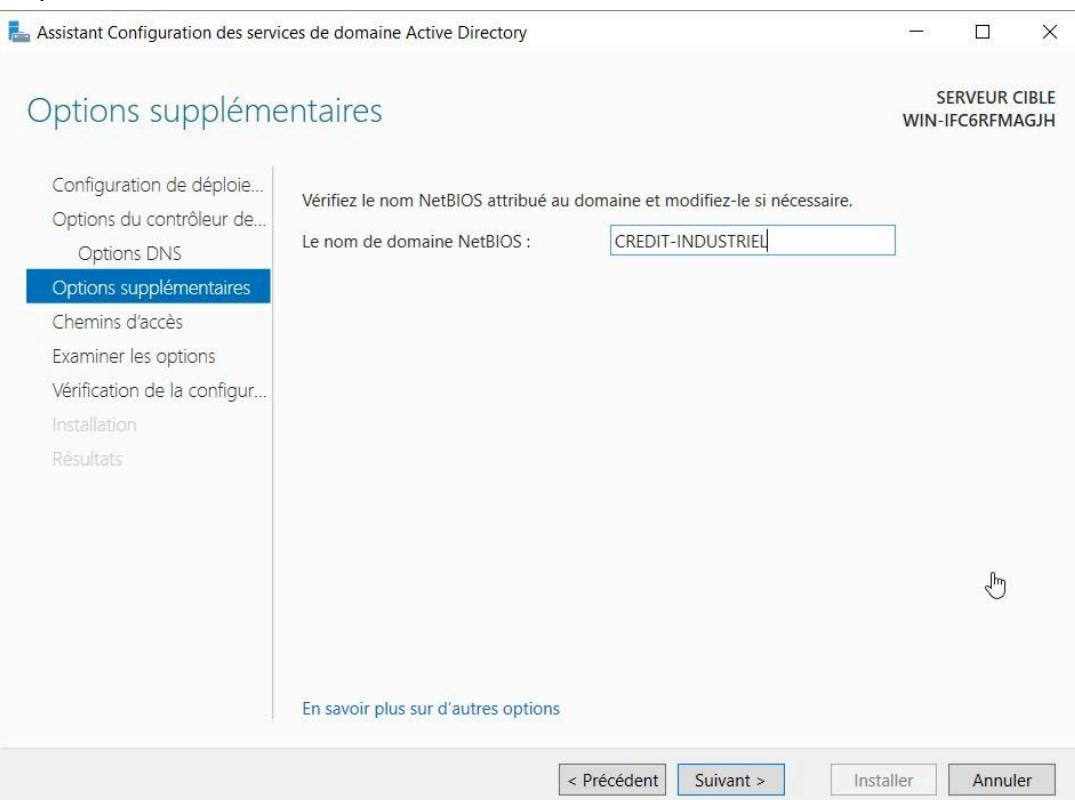
Sélectionner DNS (Domain Name System) Attribuer un mot de passe au domain controllers.
Ensuite Sélectionner catalogue global attribuer un mot de passe au domaine controller.



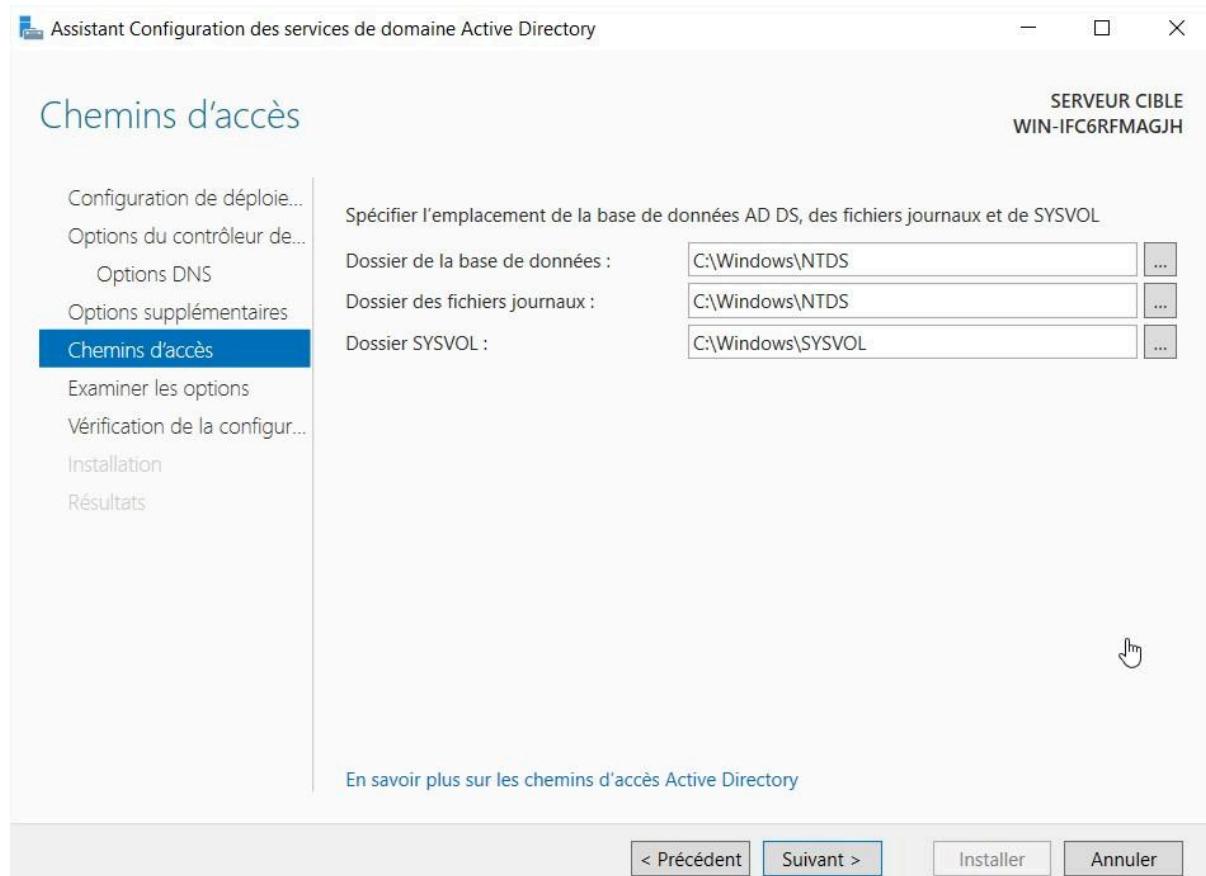
Ne pas créer de zone de délégation DNS.



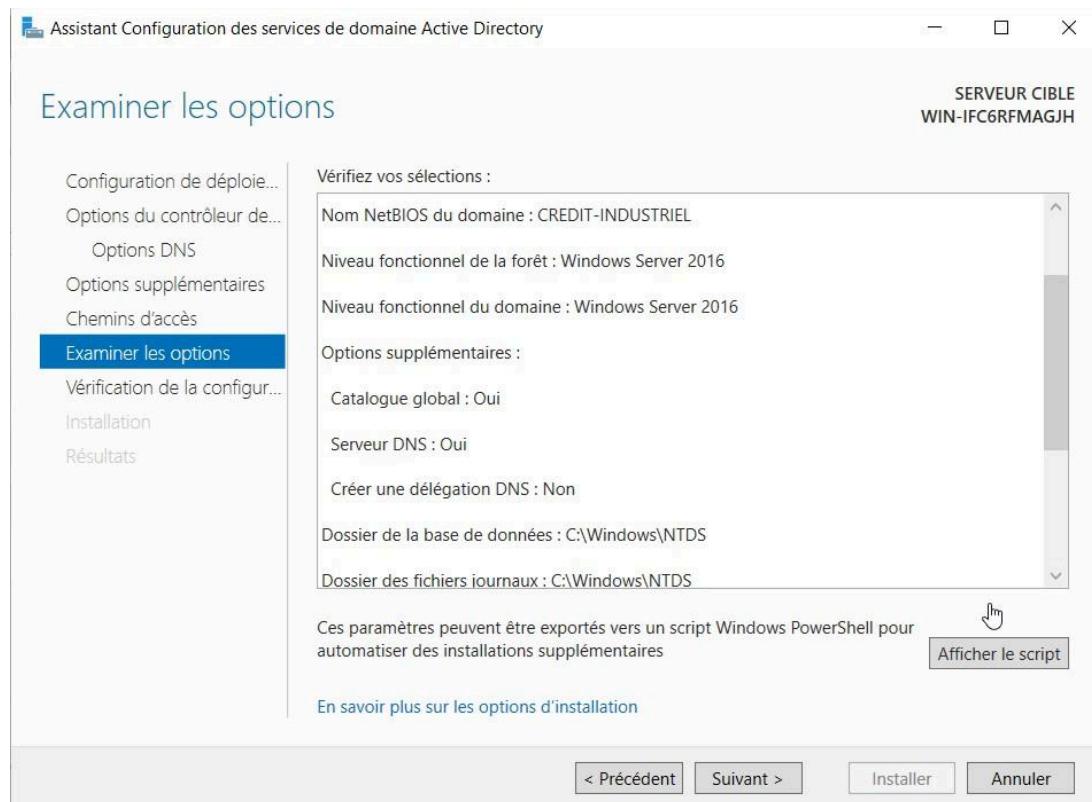
Cliquez sur suivant.



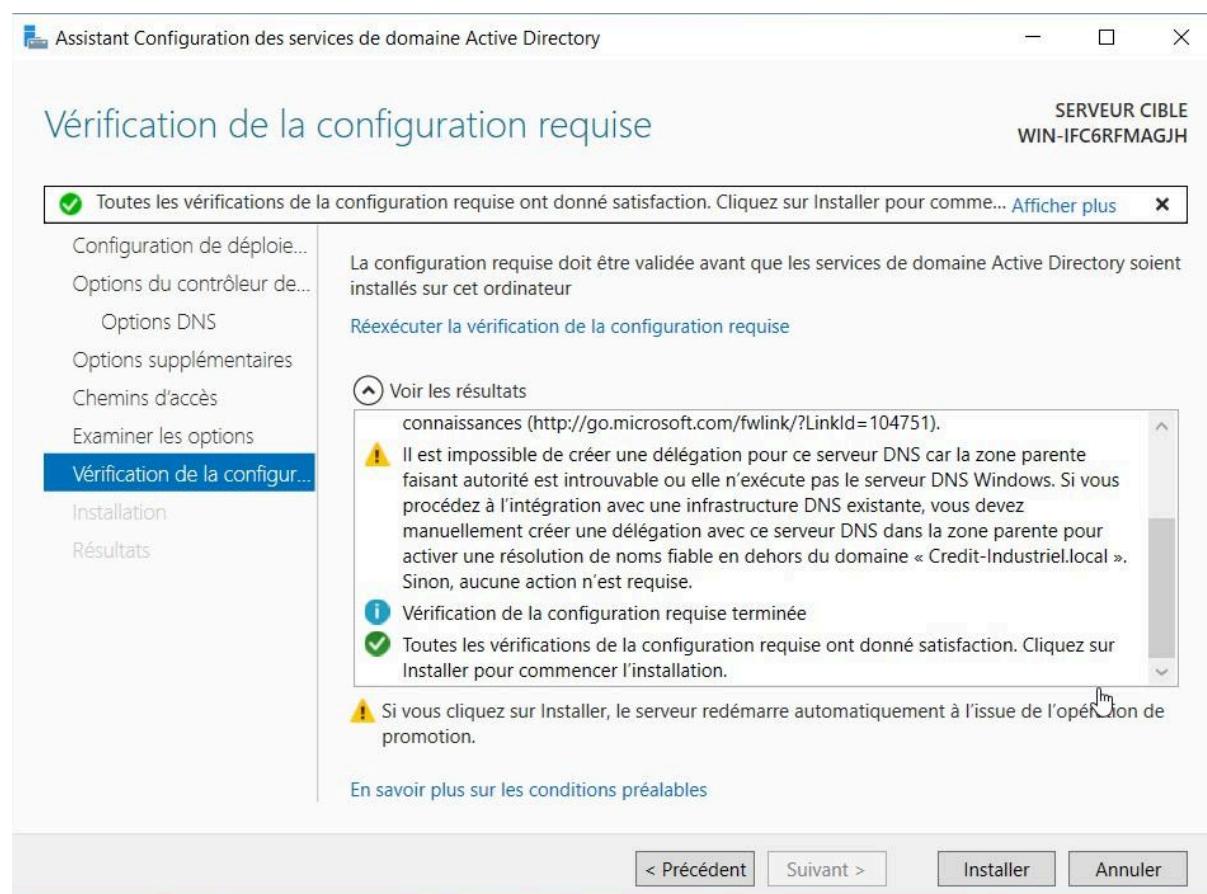
Cliquez sur suivant.



Cliquez sur suivant.



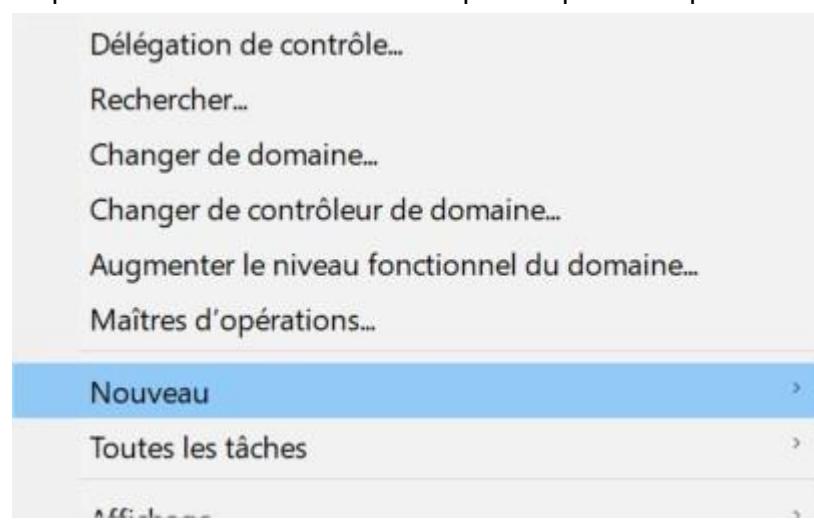
Cliquez sur installer.



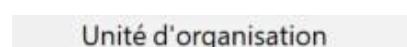
Redémarrer la machine virtuelle.

Créer des Organisation Unite

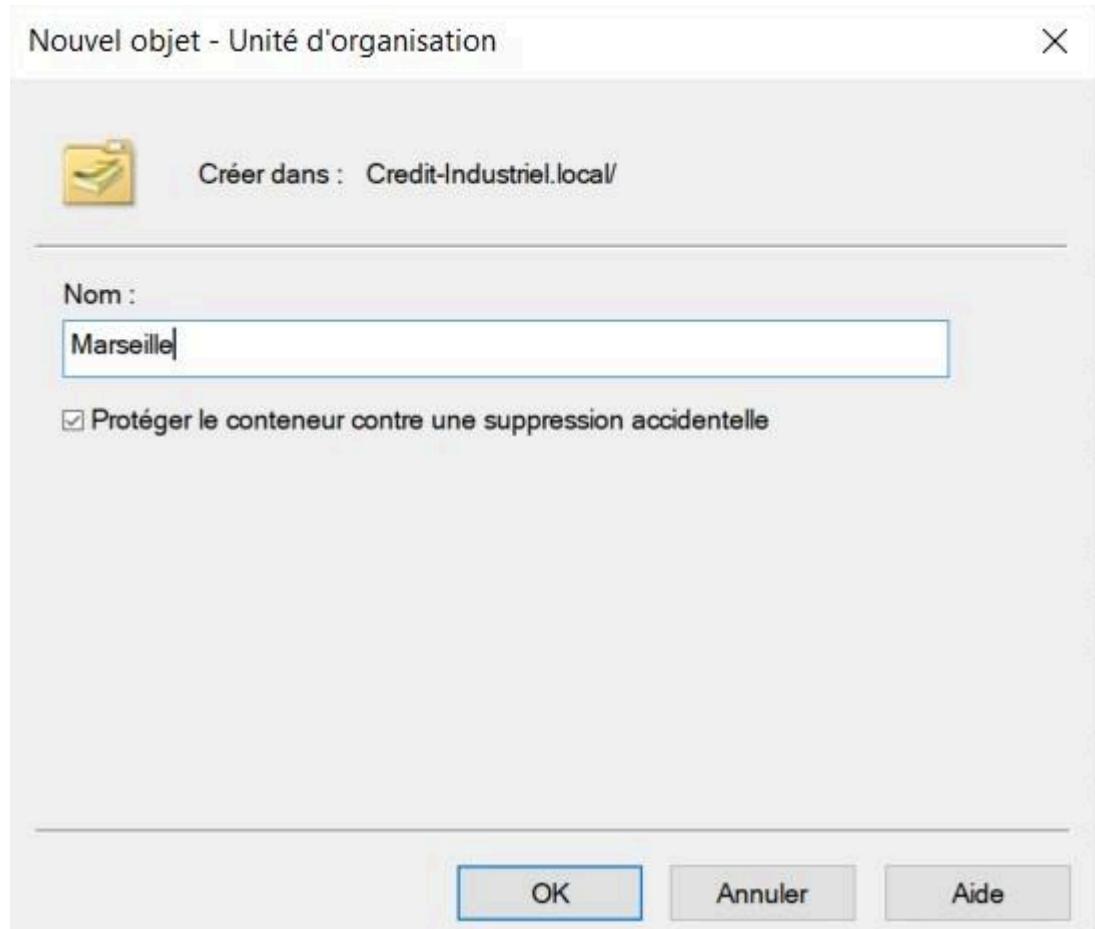
Cliquez sur votre nom de domaine puis cliquez droit puis allez dans l'onglet nouveau



puis sur cliquez sur unité d'organisation

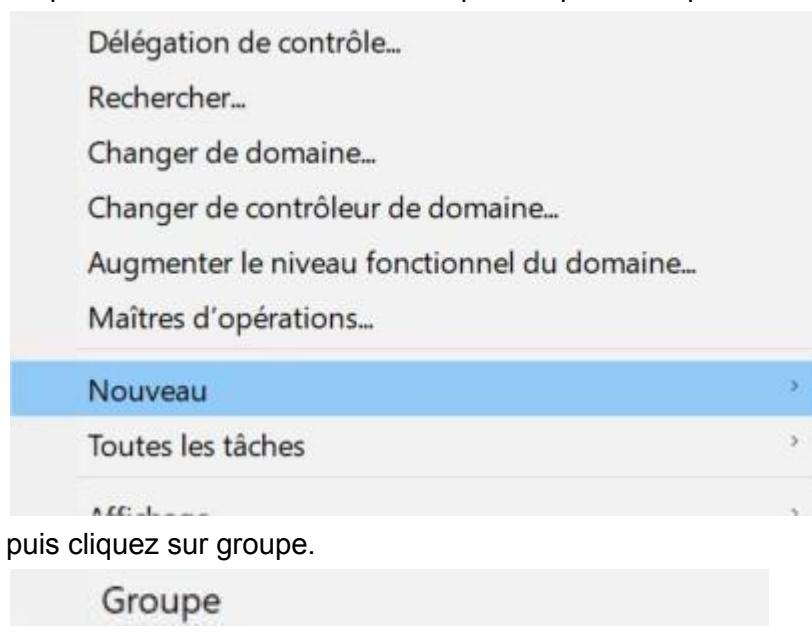


Définissez le nom de votre OU puis cliquez sur ok



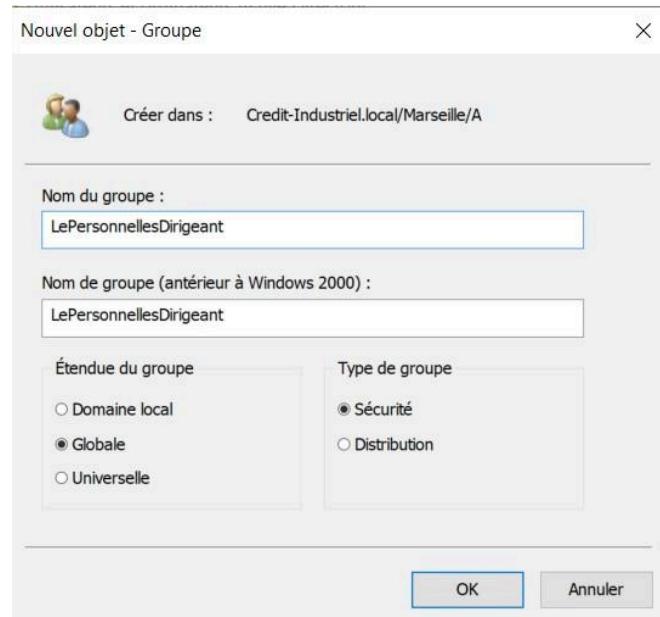
Créer des groupe

Cliquez sur votre nom de domaine puis cliquez droit puis allez dans l'onglet nouveau



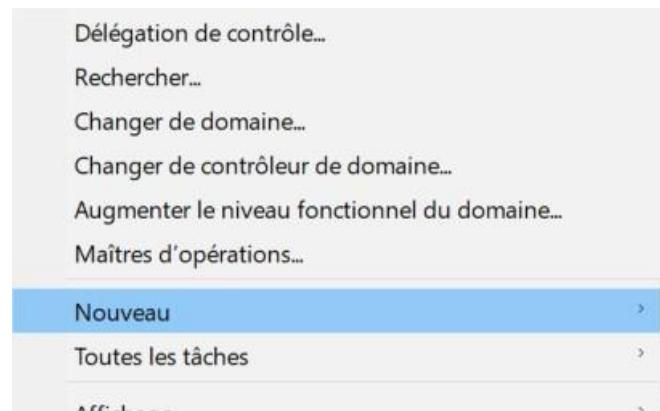
puis cliquez sur groupe.

Définissez le nom du groupe que vous souhaitez créer puis cliquez sur ok.



Créer des utilisateur

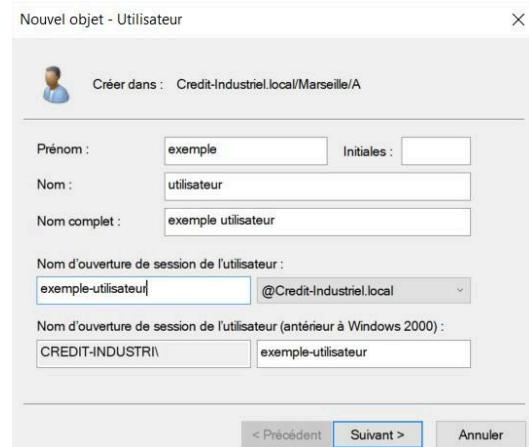
Cliquez sur votre nom de domaine puis cliquez droit puis allez dans l'onglet nouveau



Cliquez ensuite sur Utilisateurs



Définissez le nom, prenom et nom de session puis cliquez sur suivant.



Définissez en mot de passe en fonctionne des stratégie de group définies par votre organisation. sélectionnez l'utilisateur doit changer de mot de passe puis cliquez sur suivant

Nouvel objet - Utilisateur

Créer dans : Credit-Industriel.local/Marseille/A

Mot de passe : 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

Ajouter les utilisateur dans les groupes

Tout d'abord sélectionnez le groupe dans lequel vous voulez ajouter des utilisateurs, par exemple LesGuichetiers.

Nom	Type	Description
 LesGuichetiers	Groupe de sécurité	
 Arthur Neutron	Utilisateur	
 Amelie Lotte	Utilisateur	

Ensuite allez dans l'onglet membre.

Propriétés de : LesGuichetiers

Général Membres Membre de Géré par Objet Sécurité Éditeur d'attributs

 LesGuichetiers

Nom de groupe (antérieur à Windows 2000) :

Description :

Adresse de messagerie :

Étendue du groupe

Domaine local
 Globale
 Universelle

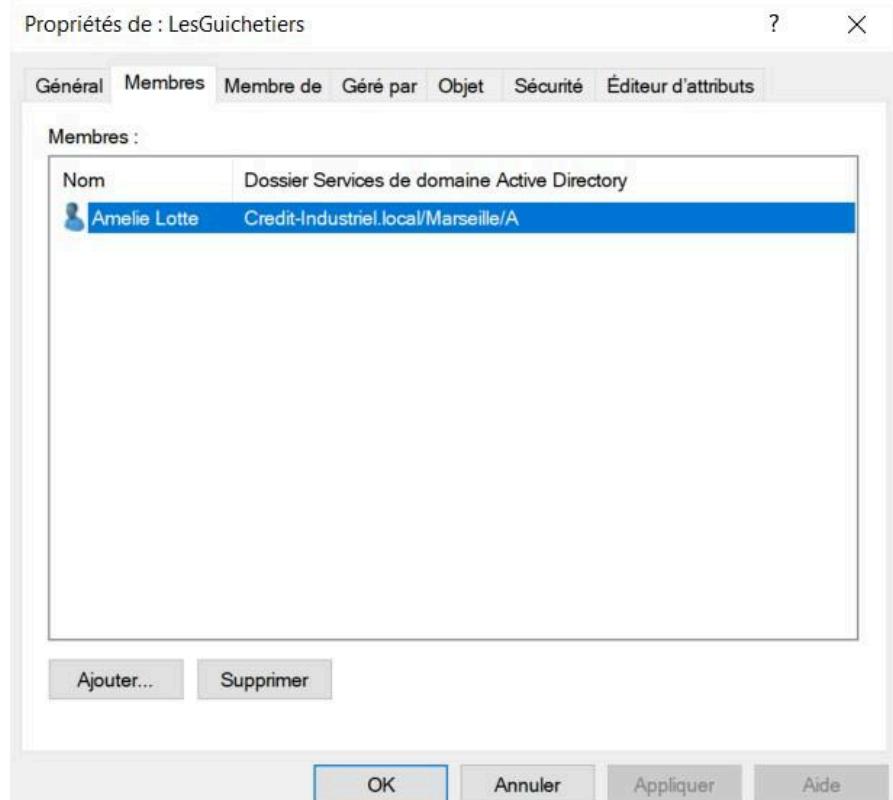
Type de groupe

Sécurité
 Distribution

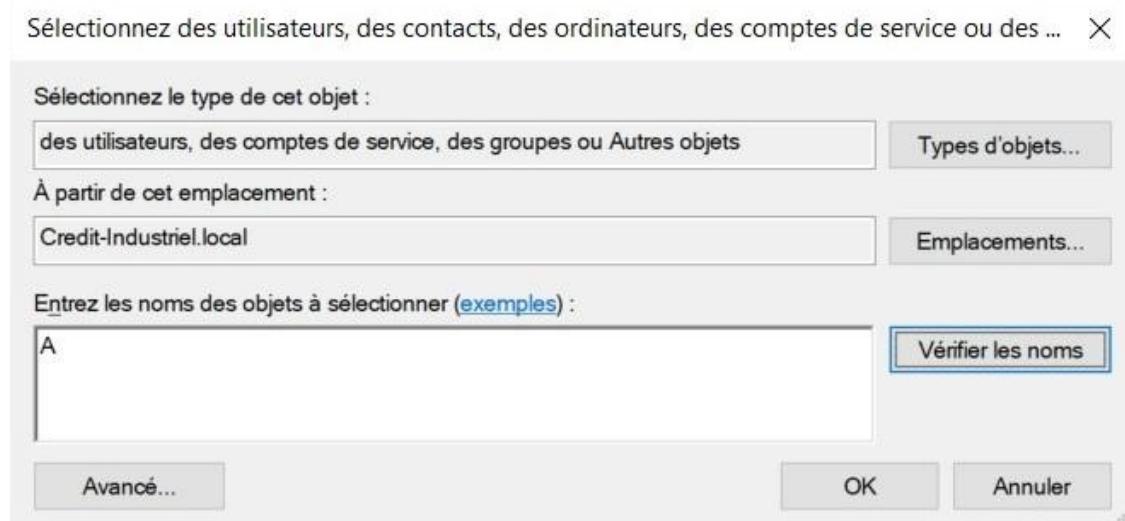
Remarques :

OK Annuler Appliquer Aide

Une fois dans l'onglet membre cliquez sur ajouter.

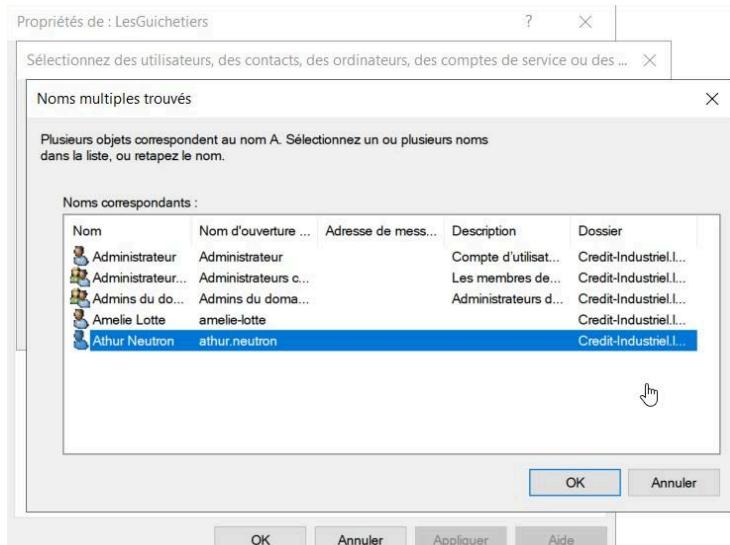


Tapez la première lettre du nom du groupe

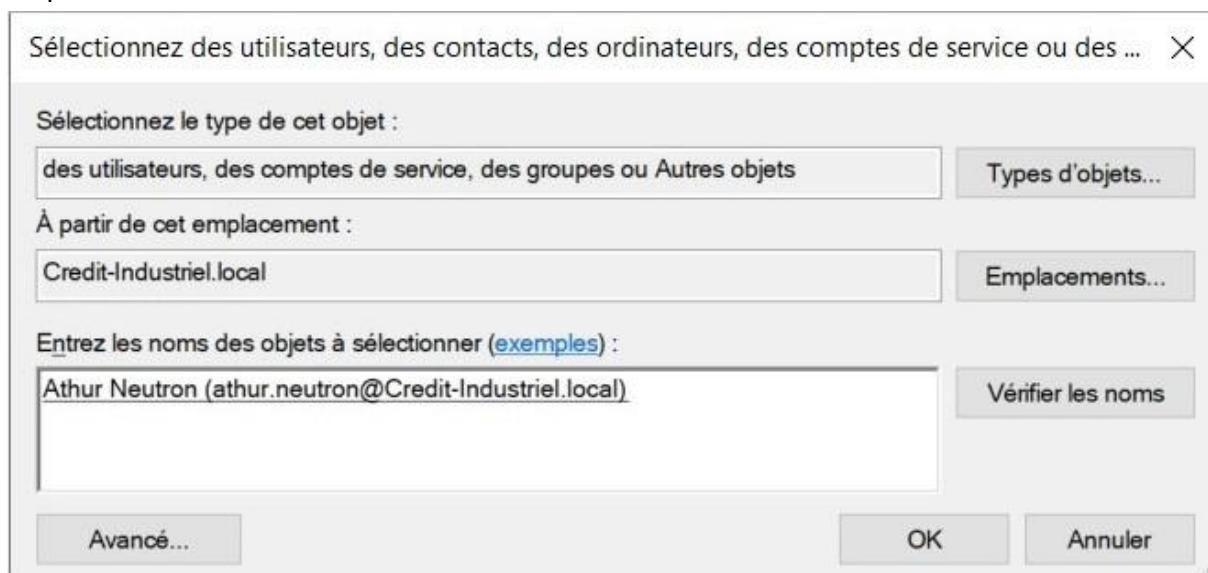


Allez à la page suivante pour voir la suite

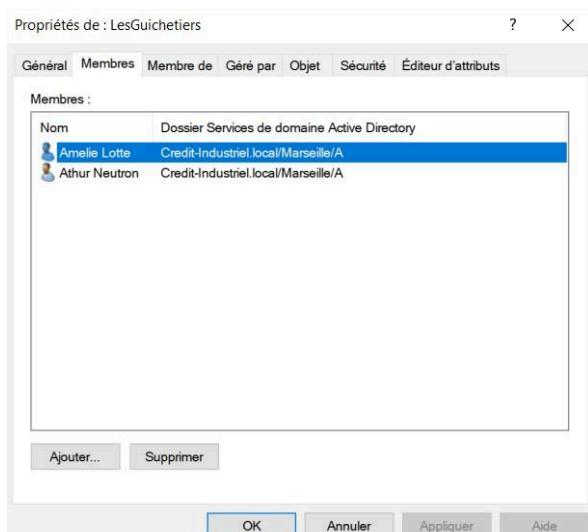
Sélectionnez l'utilisateur que vous voulez ajouter puis cliquez sur ok.



Cliquez sur ok.



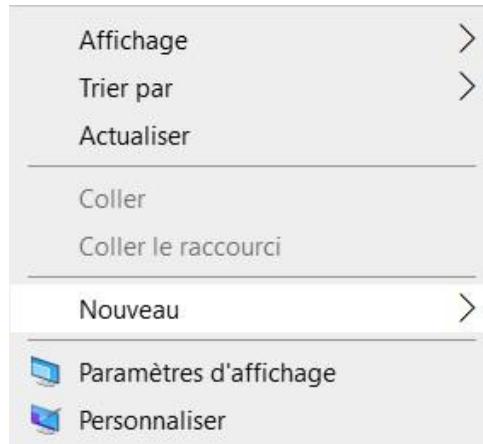
Ensuite cliquez sur appliquer puis ok



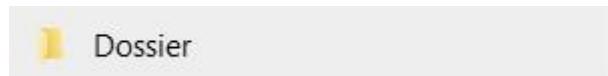
JOB 2

Créer un dossier

Clique droit nouveau



Cliquez sur dossier.

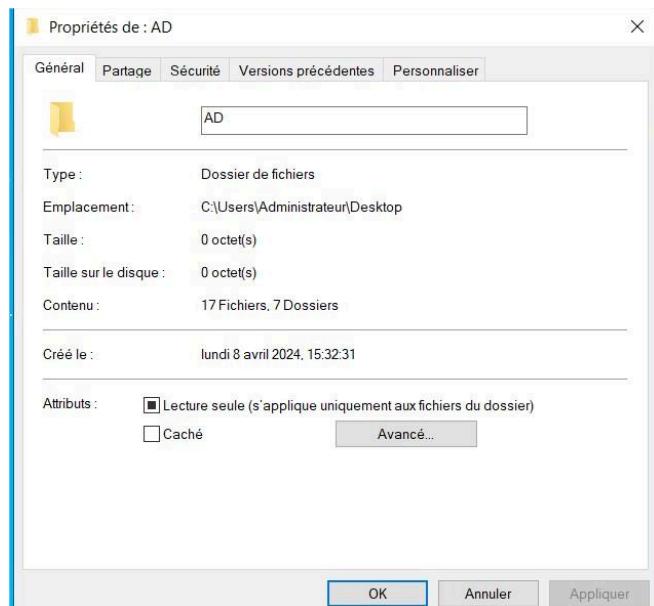


Modifier les droits de partage

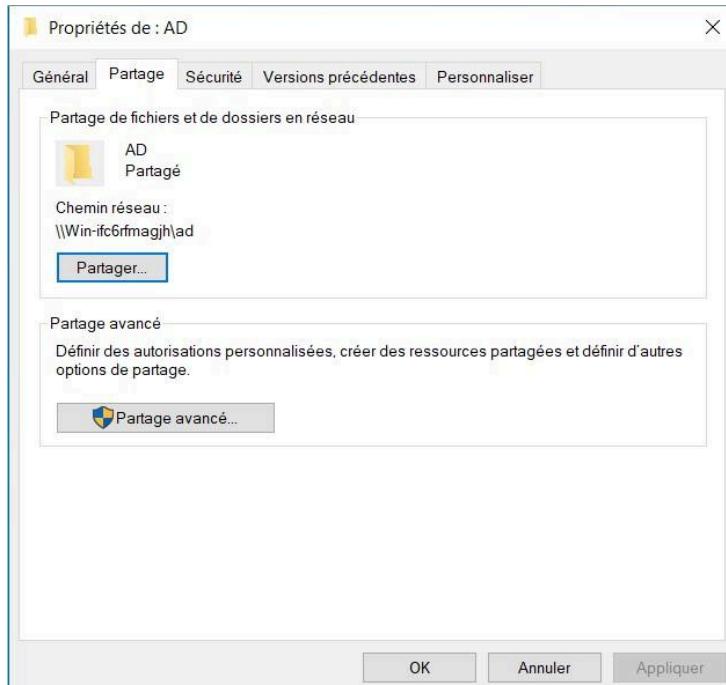
Faites clique droit sur le dossier que vous souhaitez partager puis cliquez sur propriétés

Propriétés

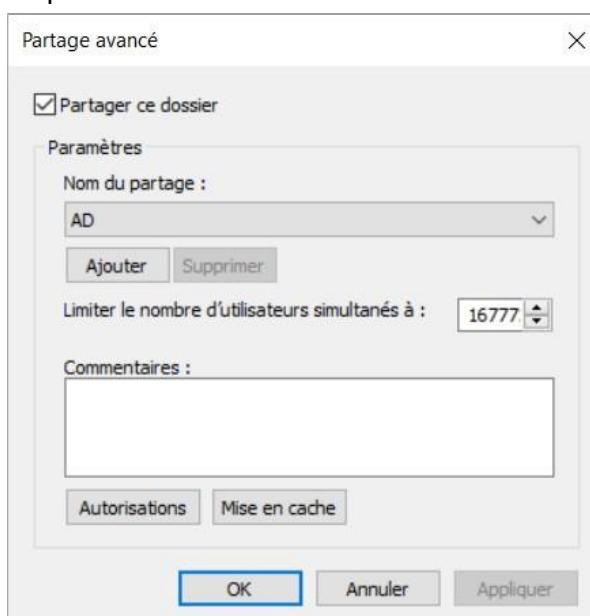
Allez dans l'onglet partage



Dans l'onglet partage cliquez sur partage avancé



Cliquez sur autorisation



Allez à la page suivante pour voir la suite

Tapez le début du nom du groupe auquel vous souhaitez attribuer des droits

Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes X

Sélectionnez le type de cet objet :
des utilisateurs, des groupes ou Principaux de sécurité intégrés Types d'objets...

À partir de cet emplacement :
Credit-Industriel.local Emplacements...

Entrez les noms des objets à sélectionner ([exemples](#)) :
Les Vérifier les noms

[Avancé...](#) OK Annuler

Cliquez sur le groupe que vous souhaitez ajouter par exemple les prestataires puis cliquez sur ok.

Noms multiples trouvés X

Plusieurs objets correspondent au nom Les. Sélectionnez un ou plusieurs noms dans la liste, ou retapez le nom.

Noms correspondants :

Nom	Nom d'ouverture ...	Adresse de mess...	Description	Dossier
LesChefDePro...	LesChefDeProjet			Credit-Industriel...
LesClients	LesClients			Credit-Industriel...
LesGestionnai...	LesGestionnaires			Credit-Industriel...
LesGuichetiers	LesGuichetiers			Credit-Industriel...
LesInformatici...	LesInformaticiens			Credit-Industriel...
LesPrestataires	LesPrestataires			Credit-Industriel...

OK Annuler

Cliquez sur ok.

Sélectionnez des utilisateurs, des ordinateurs, des comptes de service ou des groupes X

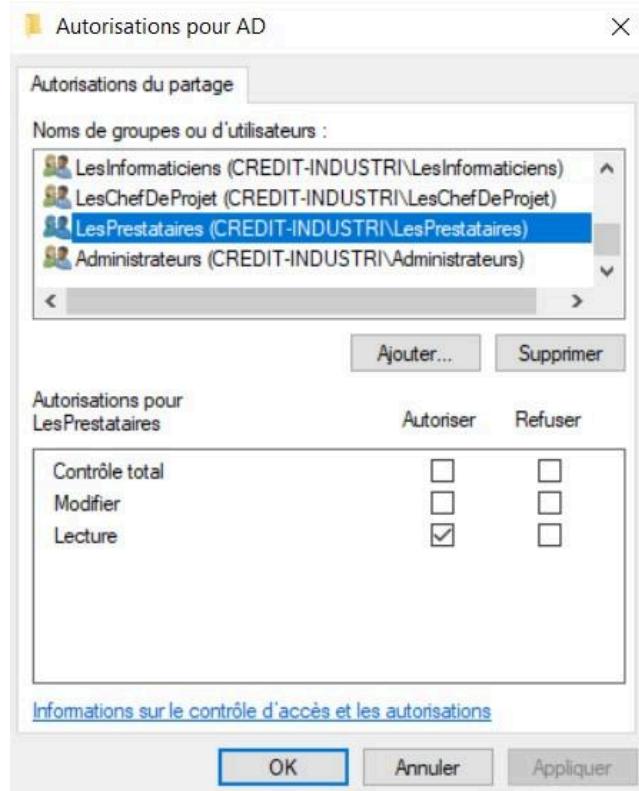
Sélectionnez le type de cet objet :
des utilisateurs, des groupes ou Principaux de sécurité intégrés Types d'objets...

À partir de cet emplacement :
Credit-Industriel.local Emplacements...

Entrez les noms des objets à sélectionner ([exemples](#)) :
LesPrestataires Vérifier les noms

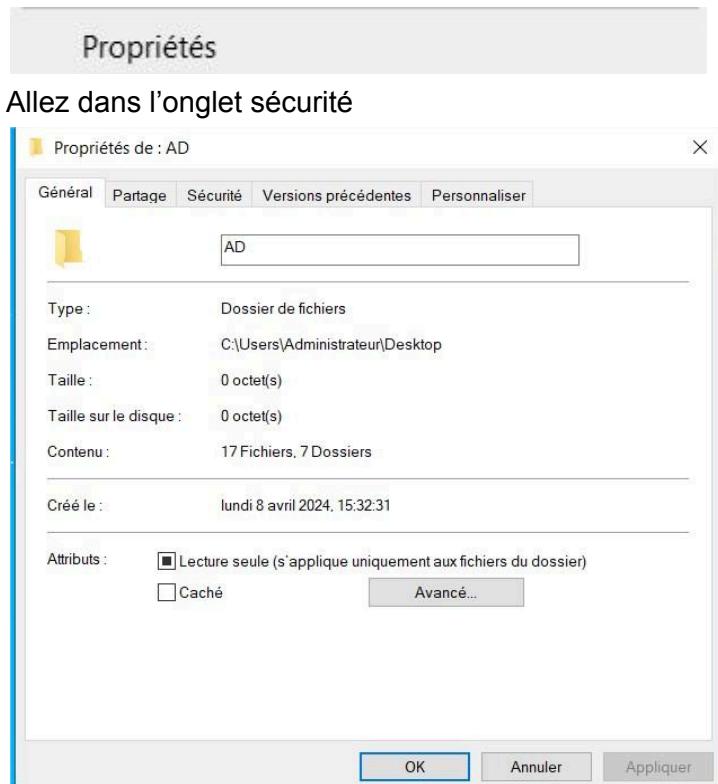
[Avancé...](#) OK Annuler

Définissez les droits puis appliquer et cliquez sur ok.

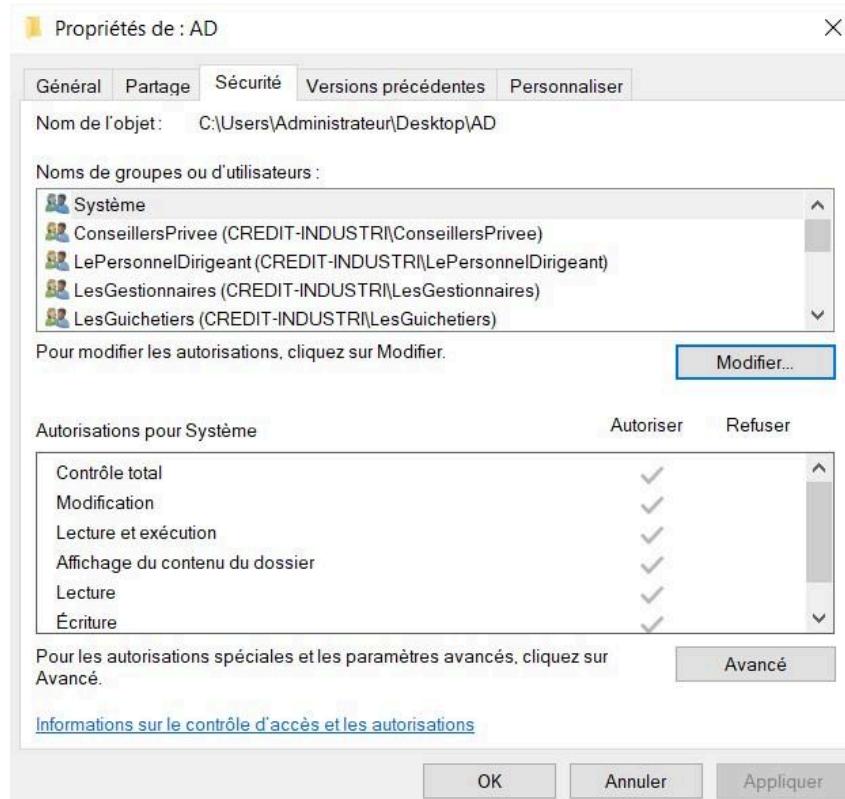


Modifier les droits ntfs

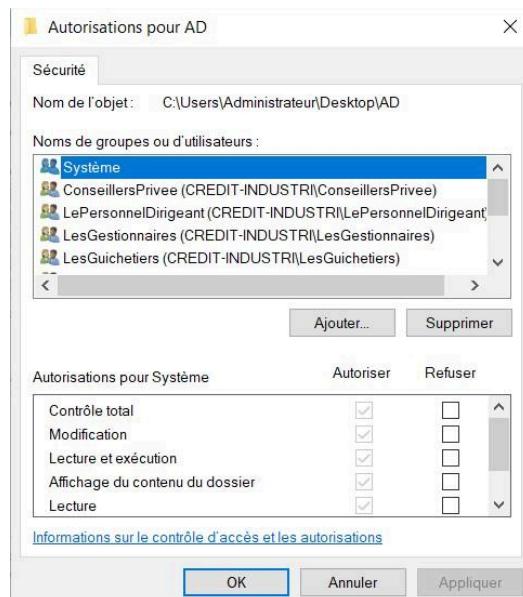
Clique droit sur le dossier dont vous souhaitez modifier les droits NTFS.



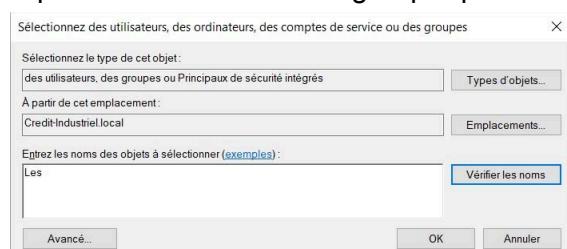
Cliquez ensuite sur modifier



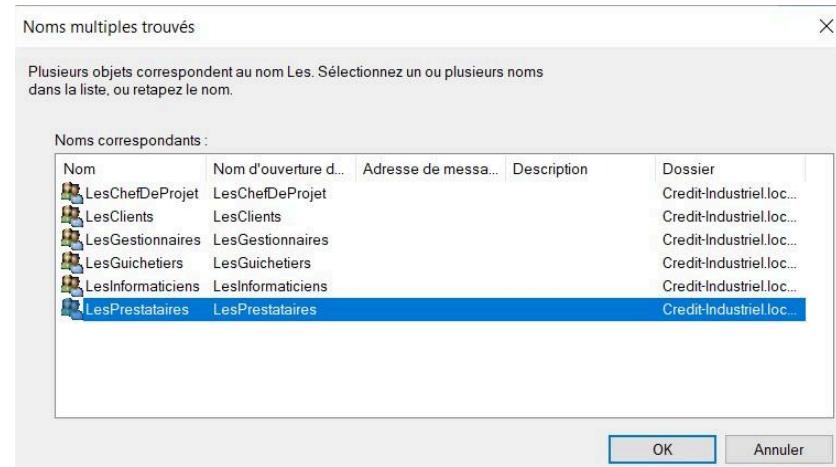
Cliquez sur ajouter.



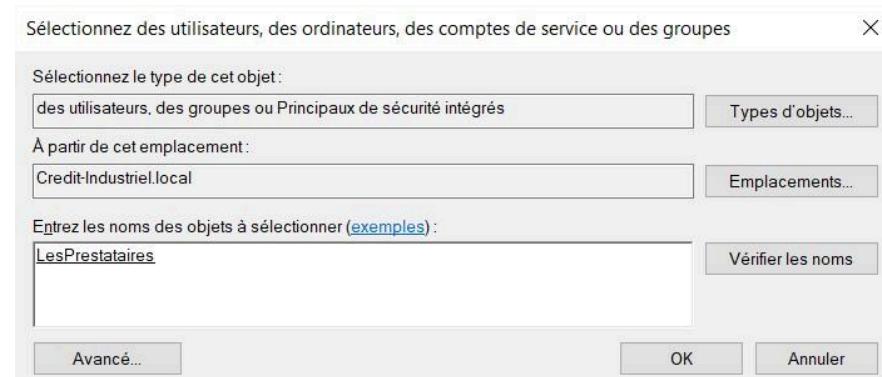
Tapez le début du nom du groupe que vous souhaitez ajouter et cliquez sur Vérifier les noms.



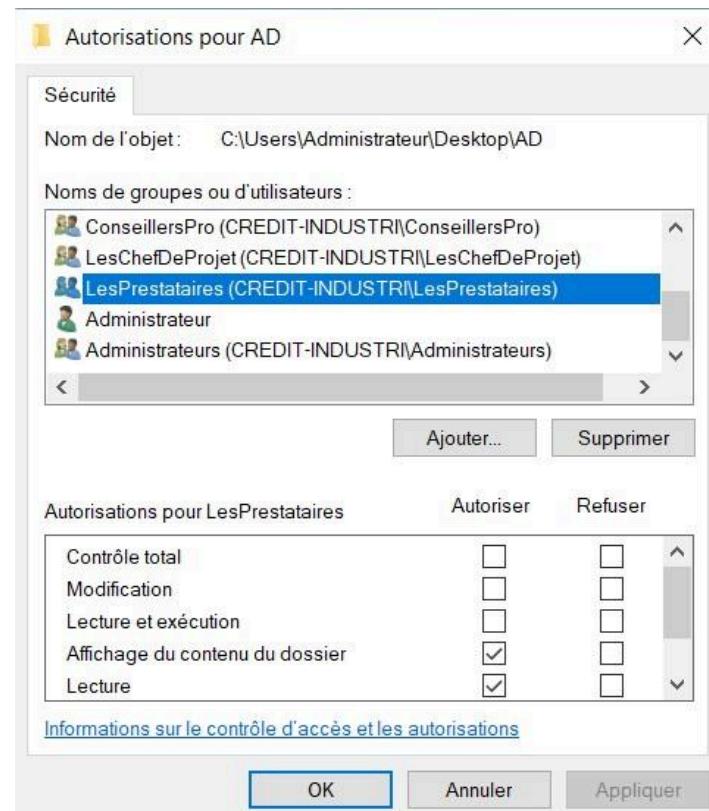
Double cliquez sur le groupe que vous voulez ajouter puis cliquez sur ok.



Cliquez encore sur ok



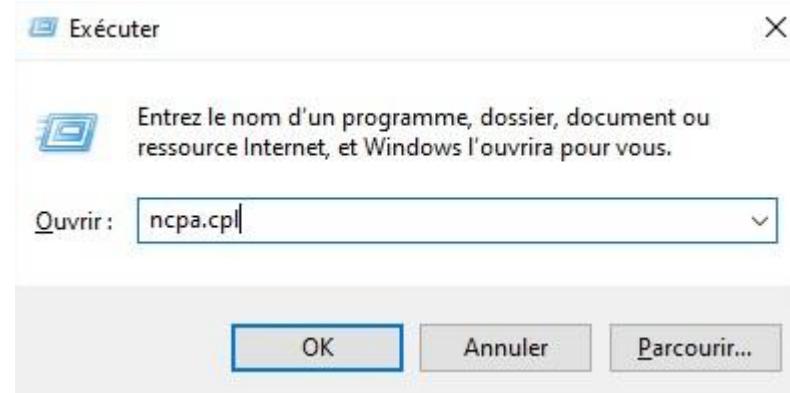
Puis attribuer les droit ntfs demandé puis cliquez sur appliquez et ok.



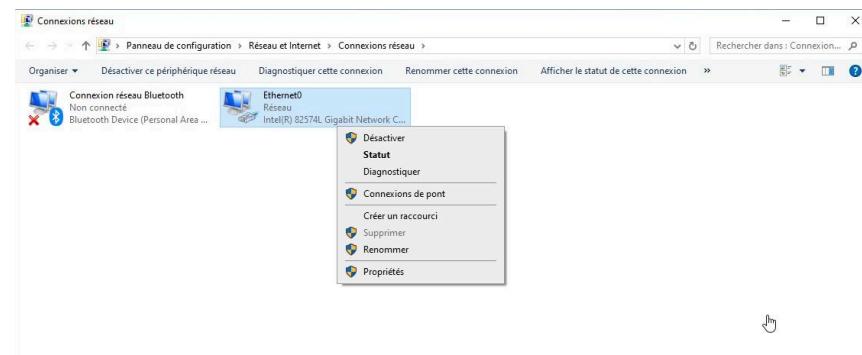
JOB 3

Entrer un poste client dans le domaine

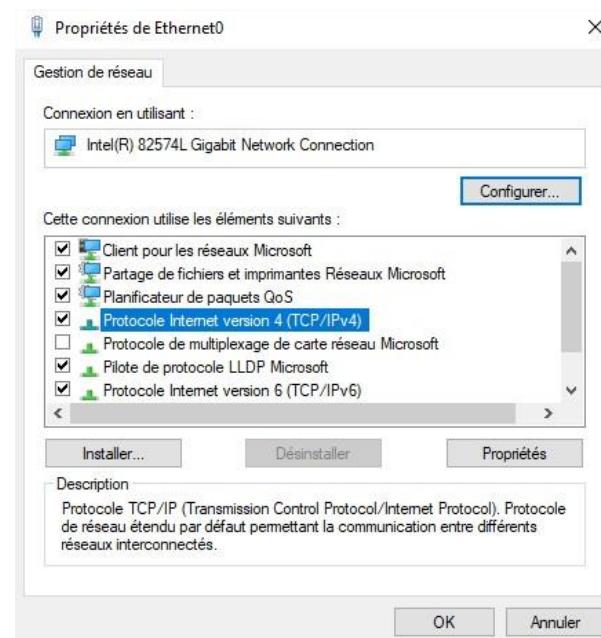
Tapez win+r sur votre machine cliente, puis tapez ncpa.cpl



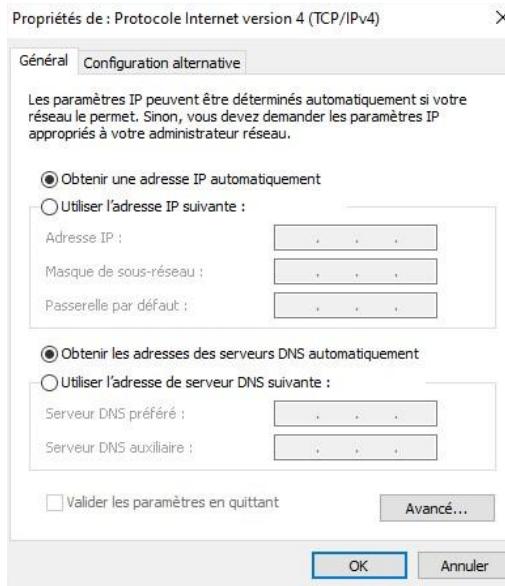
Sélectionnez votre carte réseau puis cliquez droit propriétés.



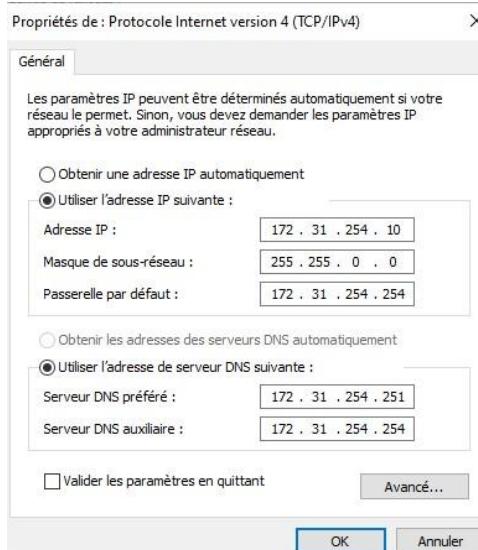
Sélectionnez le protocole IPv4.



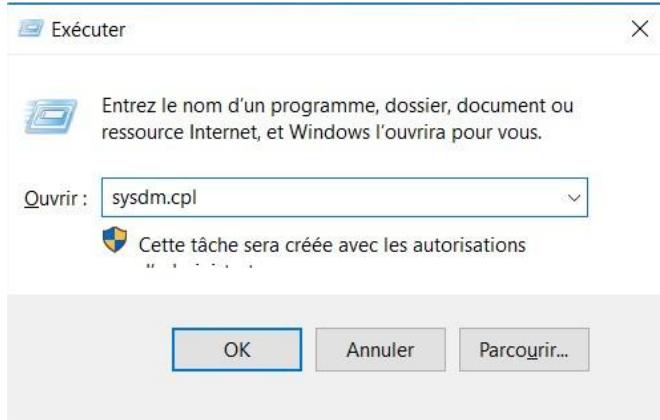
Cliquez sur utiliser l'adresse IP suivante et utilisez l'adresse de serveur DNS suivante.



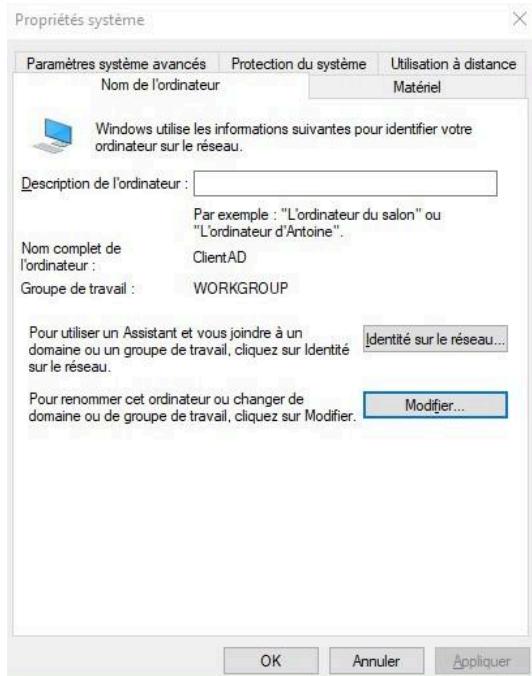
Rentrer les paramètres IP appropriés puis sélectionner Valider les paramètres en quittant puis cliquez sur ok.



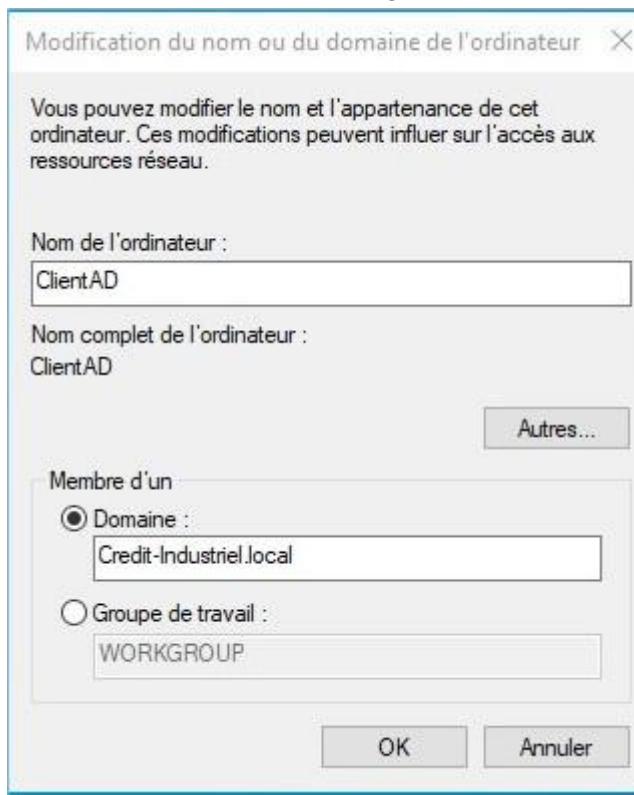
Tapez win+r puis tapez sysdm.cpl



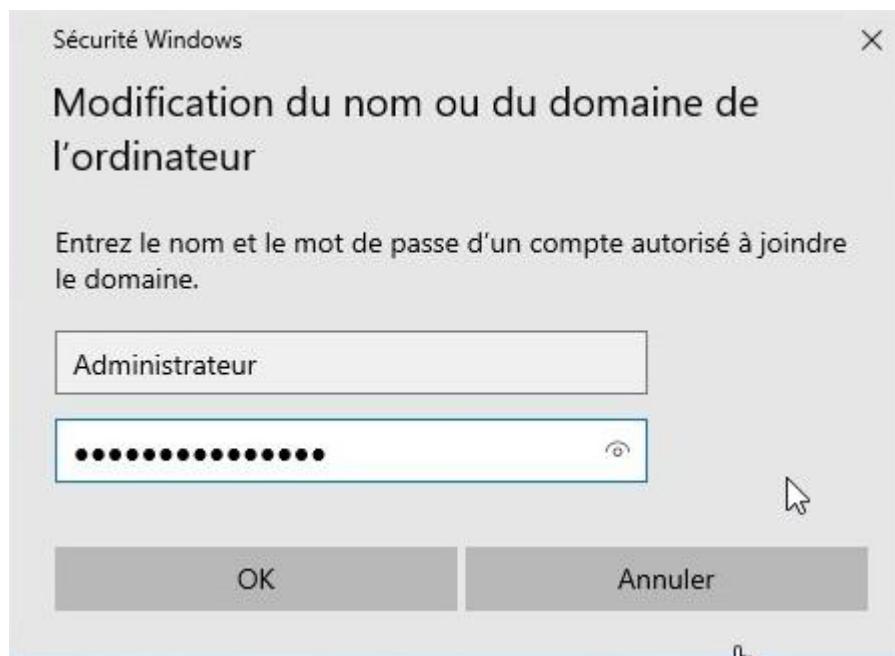
Cliquez ensuite sur modifier.



Penser à renommer votre machine avant de la rentré dans le domaine selon les convention de nom d'utilisateur définies par votre organisation exemple (ClientAD). puis ensuite indiquer le nom de domaine de votre organisation par exemple : (Credit-Industriel.local).



Ensuite logger vous avec le compte Administrateur du domaine



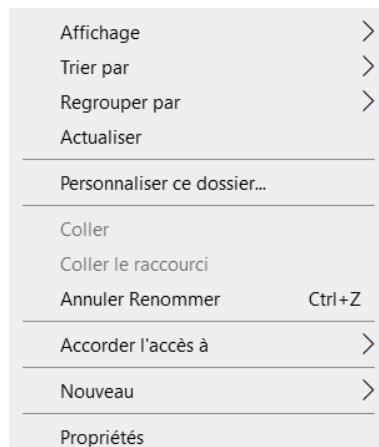
Ensuite cliquez sur ok et redémarrer le poste client.

Monter les lecteurs réseaux avec Sysvol

Allez dans le dossier

C:\Windows\SYSVOL\sysvol\Credit-Industriel.local\scripts

Faites clic droit et allez dans l'onglet nouveau



Ensuite cliquez sur Document texte.



Renommez votre script en fonction de ce qu'il fait et indiquez l'extension des script batch
exemple : (lecteur.bat)

Ensuite faites clic droit modifier. Puis tapez net use suivie du lecteur réseau suivi du chemin vers le partage suivi du nom du partage exemple :

net use x: "\172.31.254.251\Compte client"

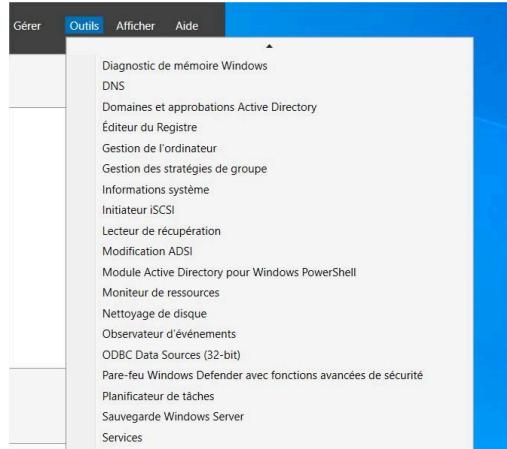
net use g: \172.31.254.251\AD

```
lecteur.bat - Bloc-notes
Fichier Edition Format Affichage Aide
net use x: "\\\\"172.31.254.251\\Compte client"
net use g: \\\\172.31.254.251\\AD
```

Ensuite allez dans le gestionnaire de serveur.



Cliquez ensuite sur outils



Cliquez ensuite sur Utilisateurs Active Directory

Nom	Type	Description
LesGuichetiers	Groupe de sécurité	
Arthur Neutron	Utilisateur	
Amelie Lotte	Utilisateur	

Sélectionnez l'utilisateur sur lequel vous voulez que le script s'exécute lors de sa connexion.

Propriétés de : Arthur Neutron

Membre de	RéPLICATION de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	COM+	Contrôle à distance	
Profil des services	Bureau à distance		Éditeur d'attributs	
Général	Adresse	Compte	Profil	Téléphones
				Organisation Certificats publiés

Arthur Neutron

Prénom : Arthur Initials :

Nom : Neutron

Nom complet : Arthur Neutron

Description :

Bureau :

Numéro de téléphone : Autre...

Adresse de messagerie :

Page Web : Autre...

OK Annuler Appliquer Aide

Allez dans l'onglet profil et indiquer le nom du script puis cliquez sur Appliquer et ensuite sur ok.

Propriétés de : Arthur Neutron

Membre de	RéPLICATION de mot de passe	Appel entrant	Objet	Sécurité
Environnement	Sessions	COM+	Contrôle à distance	
Profil des services	Bureau à distance		Éditeur d'attributs	
Général	Adresse	Compte	Profil	Téléphones Organisation Certificats publiés

Profil utilisateur

Chemin du profil :

Script d'ouverture de session : lecteur.bat

Dossier de base

Chemin d'accès local :

Connecter : à :

OK Annuler Appliquer Aide

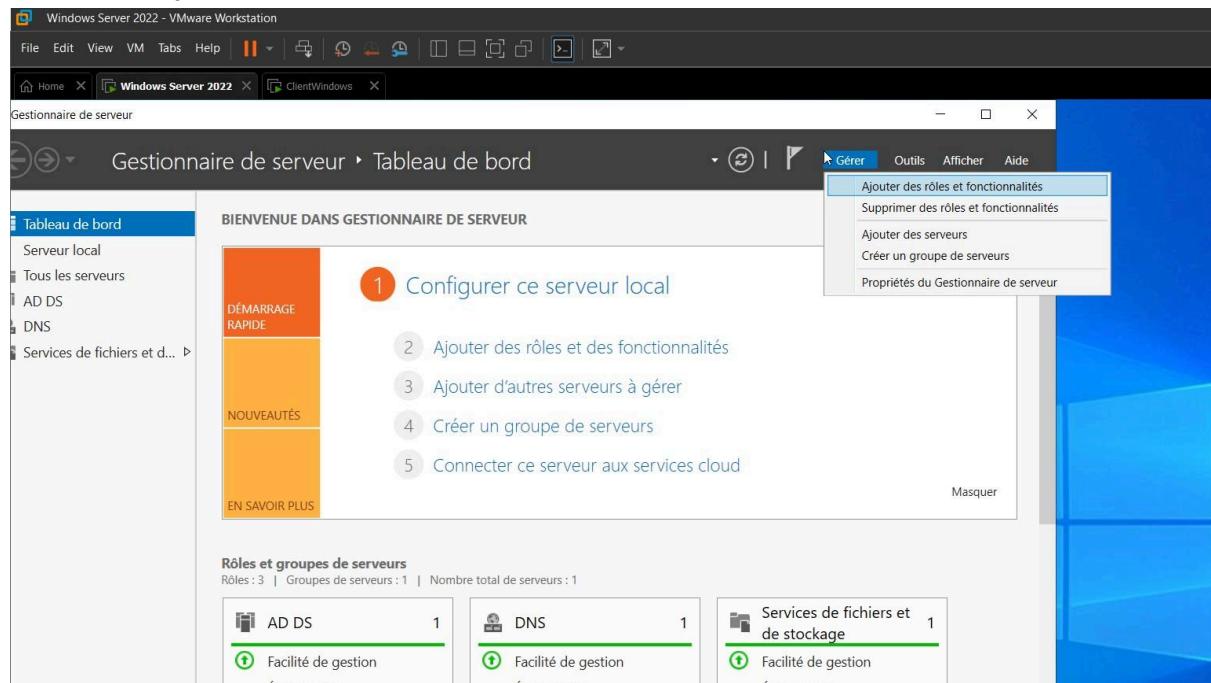
Répéter cette tâche sur tous les compte utilisateur du domaine qui doivent avoir accès au lecteur réseau.

ALLEZ À LA PAGE SUIVANTE POUR VOIR LA SUITE

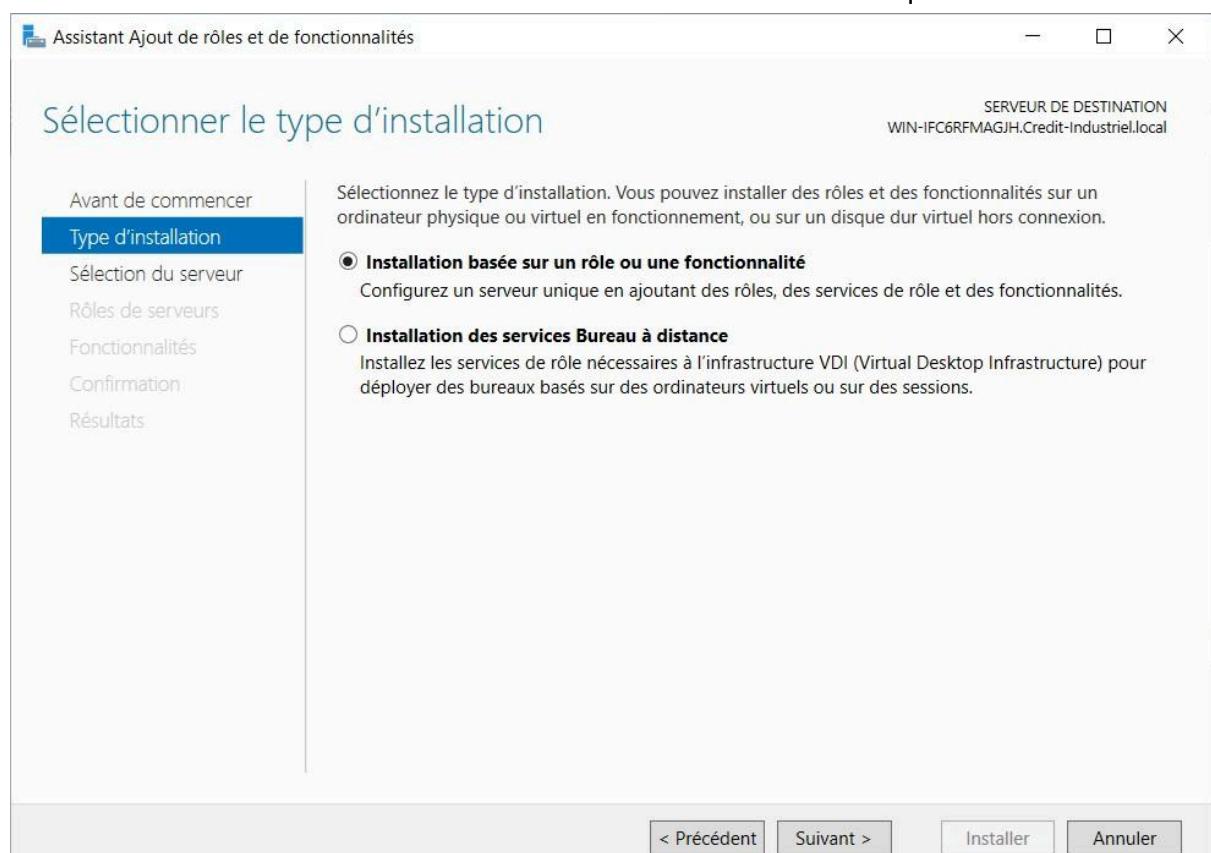
Mise en place d'un serveur dhcp :

Installation du rôle DHCP

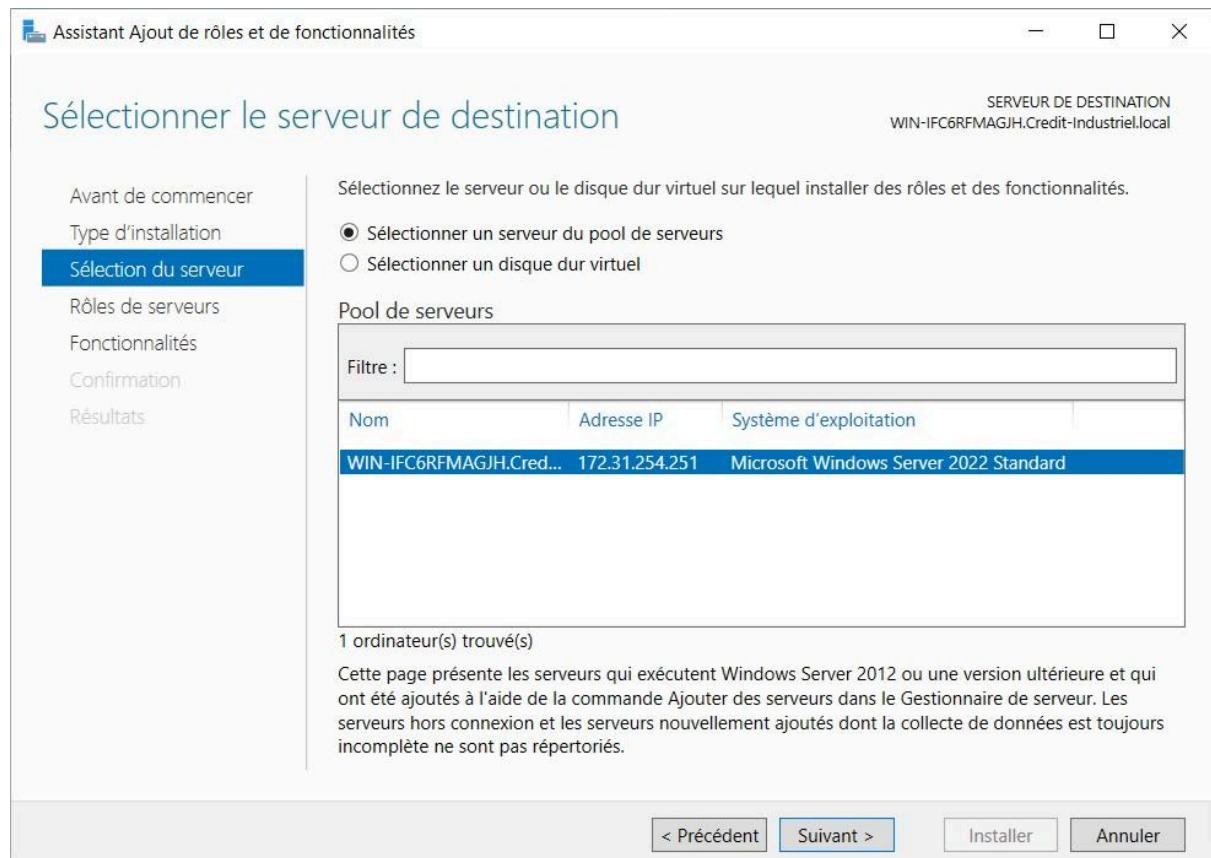
Cliquez sur ajouter rôle ou fonctionnalité



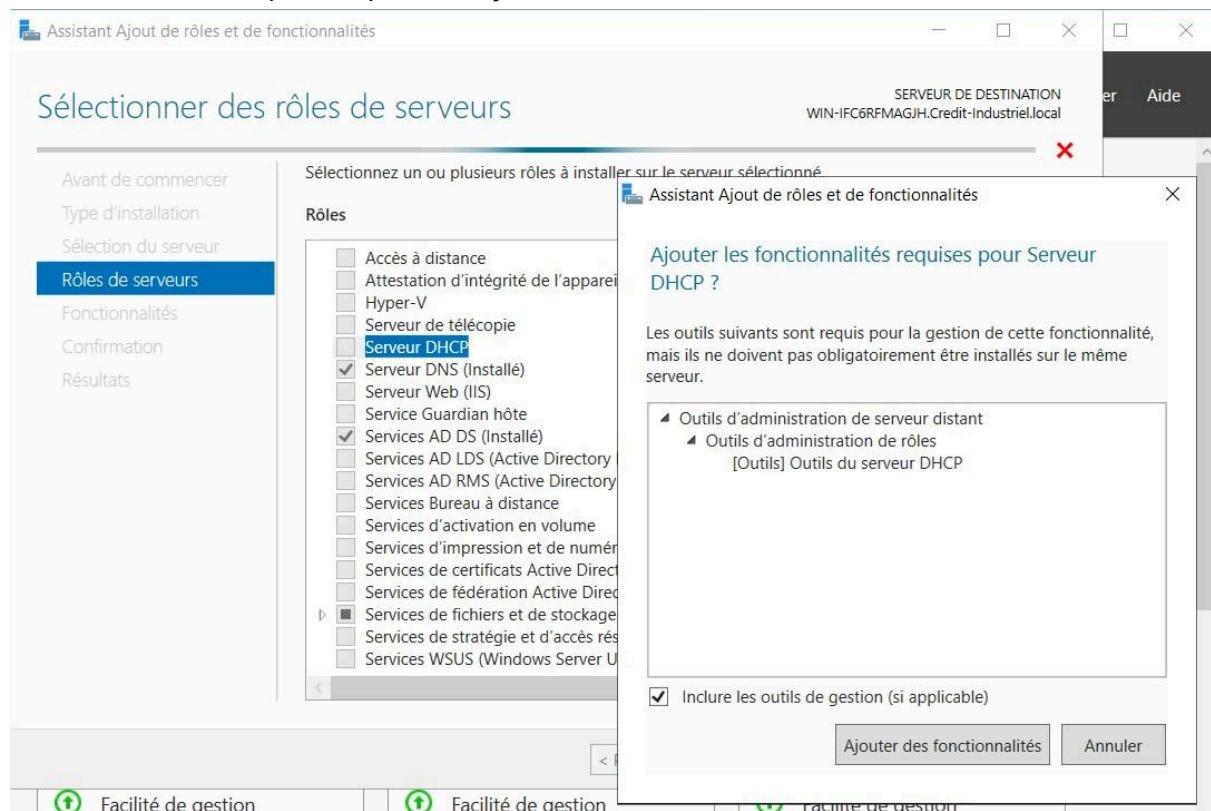
Sélectionner installation basée sur un rôle ou une fonctionnalité et cliquez sur suivant.



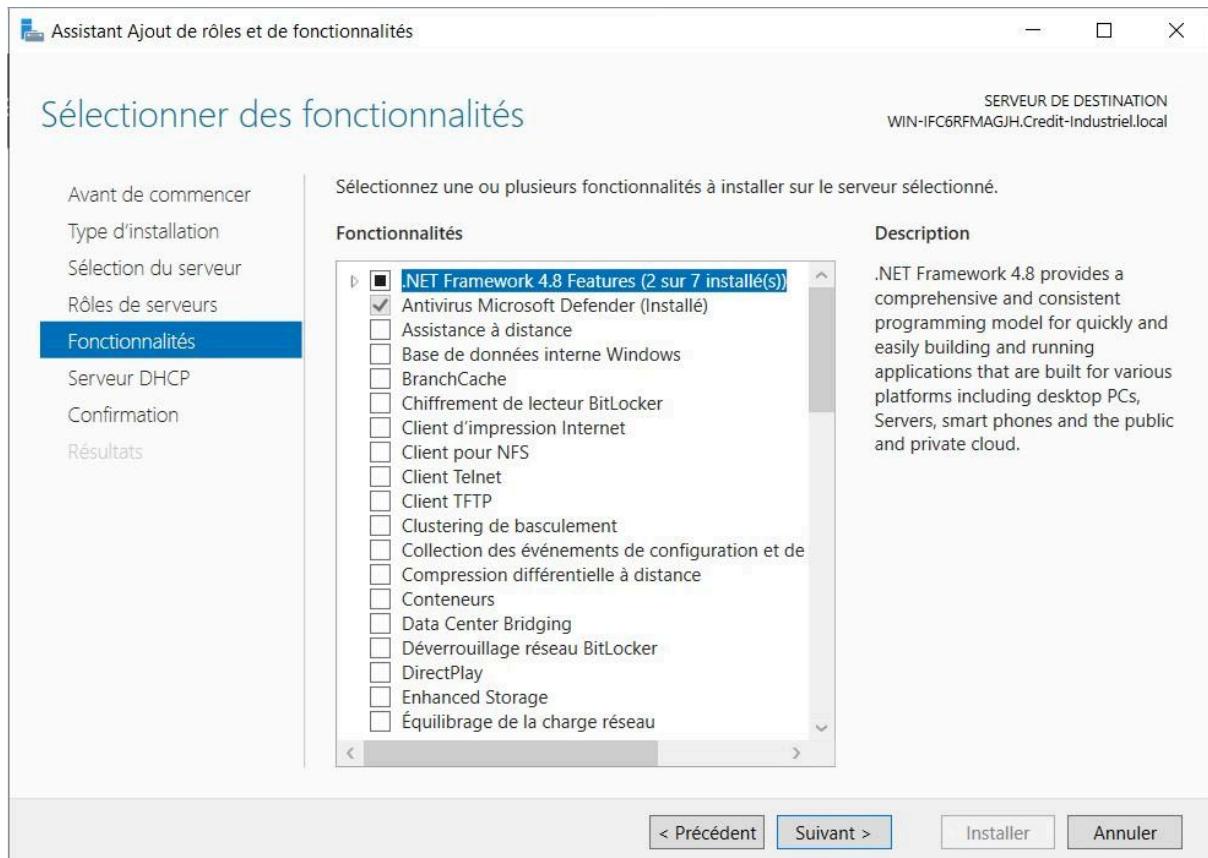
Sélectionner un serveur du pool de serveur et cliquez sur suivant.



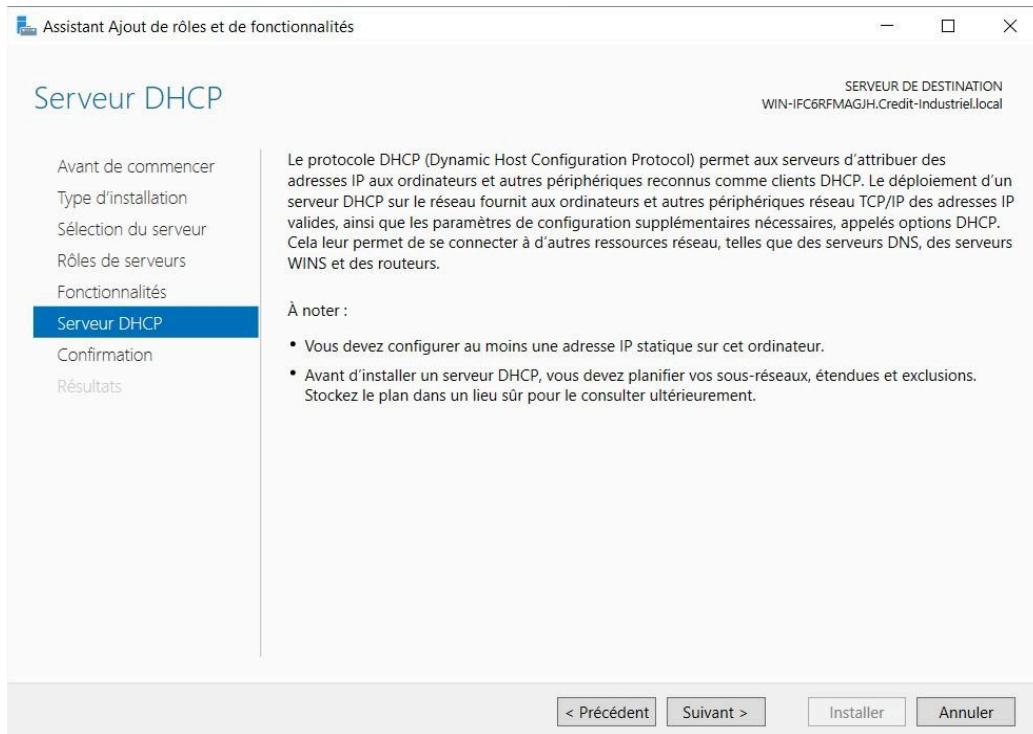
Sélectionner DHCP puis cliquez sur ajouter une nouvelle fonctionnalité.



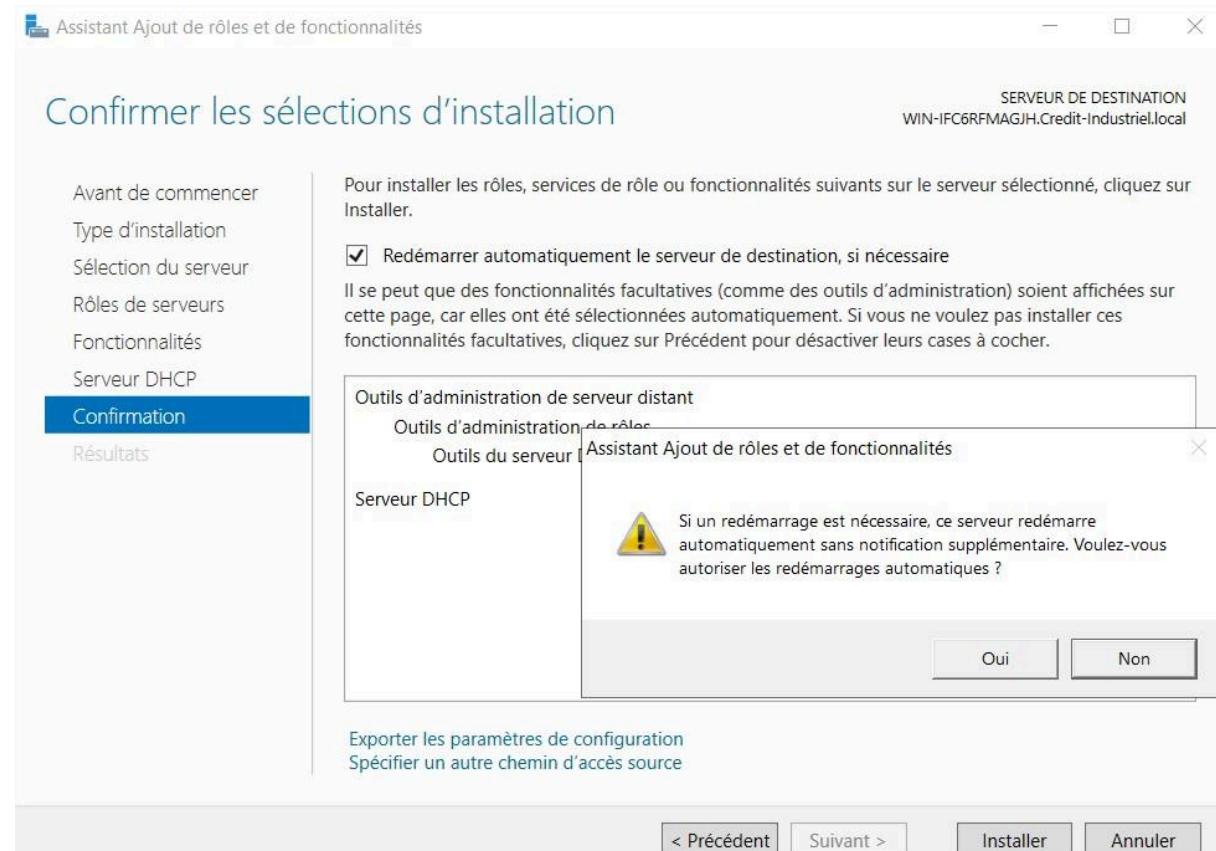
Cliquez sur suivant.



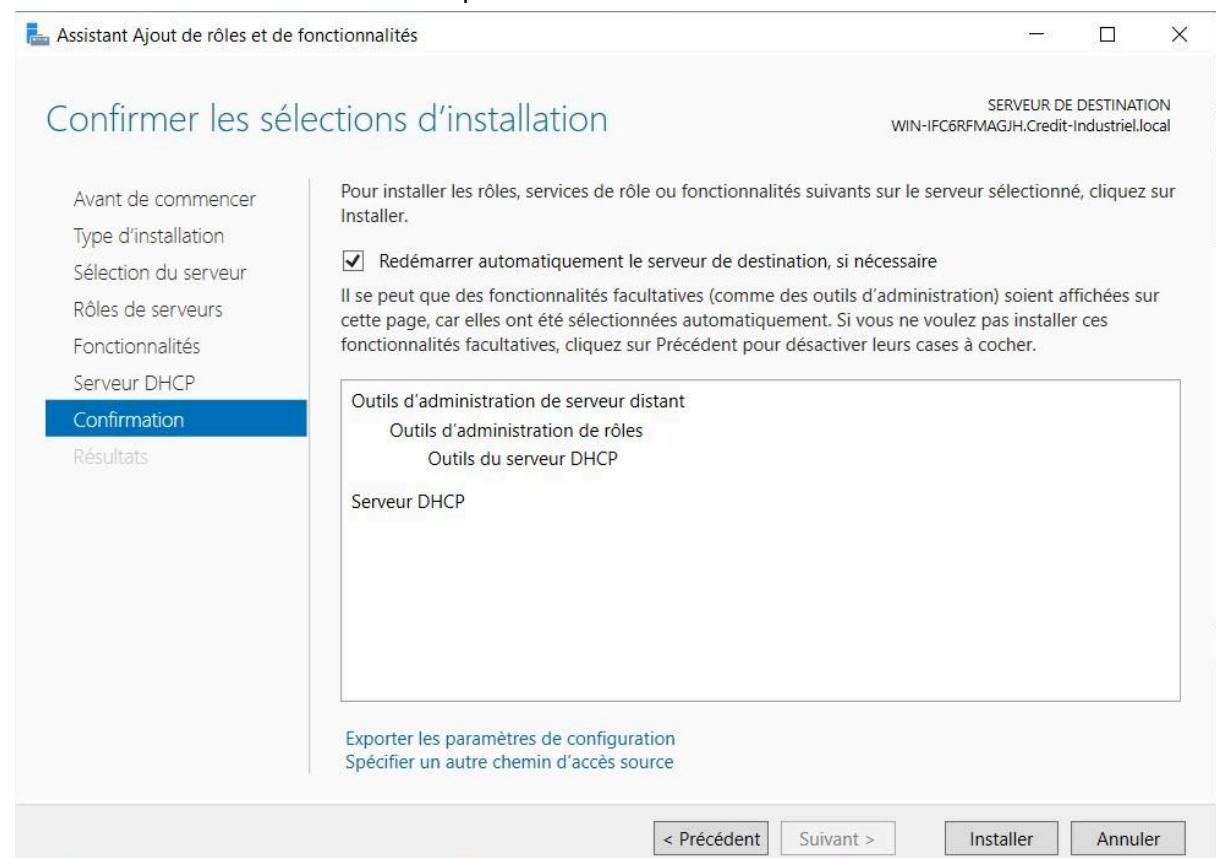
Cliquez sur suivant.



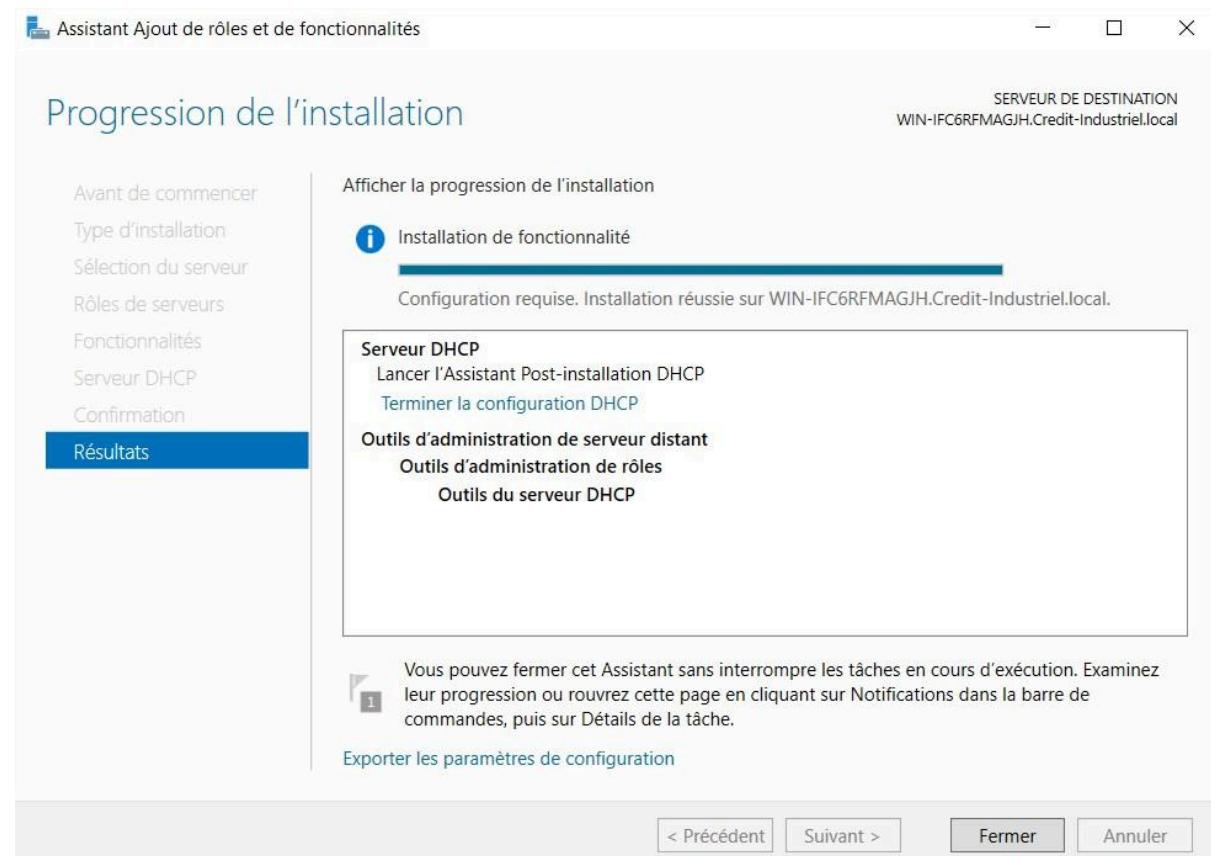
Cliquez sur oui pour redémarrer.



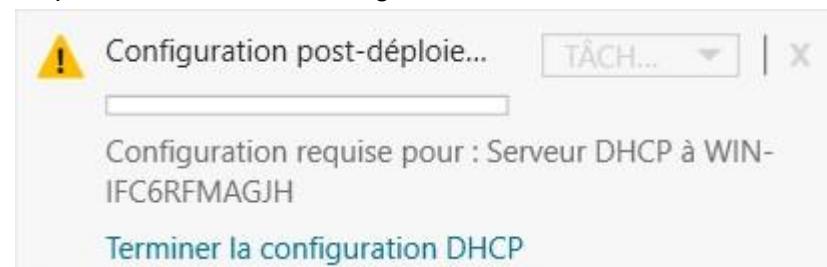
Sélectionnez redémarrer automatiquement le serveur.



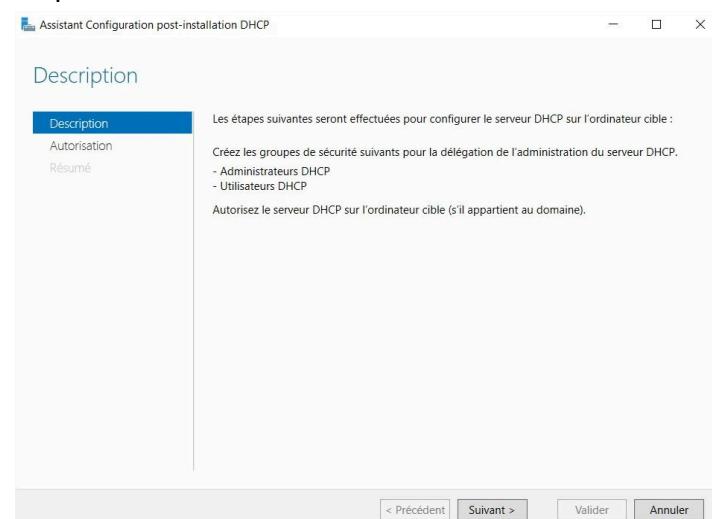
Ensuite cliquez sur fermer.



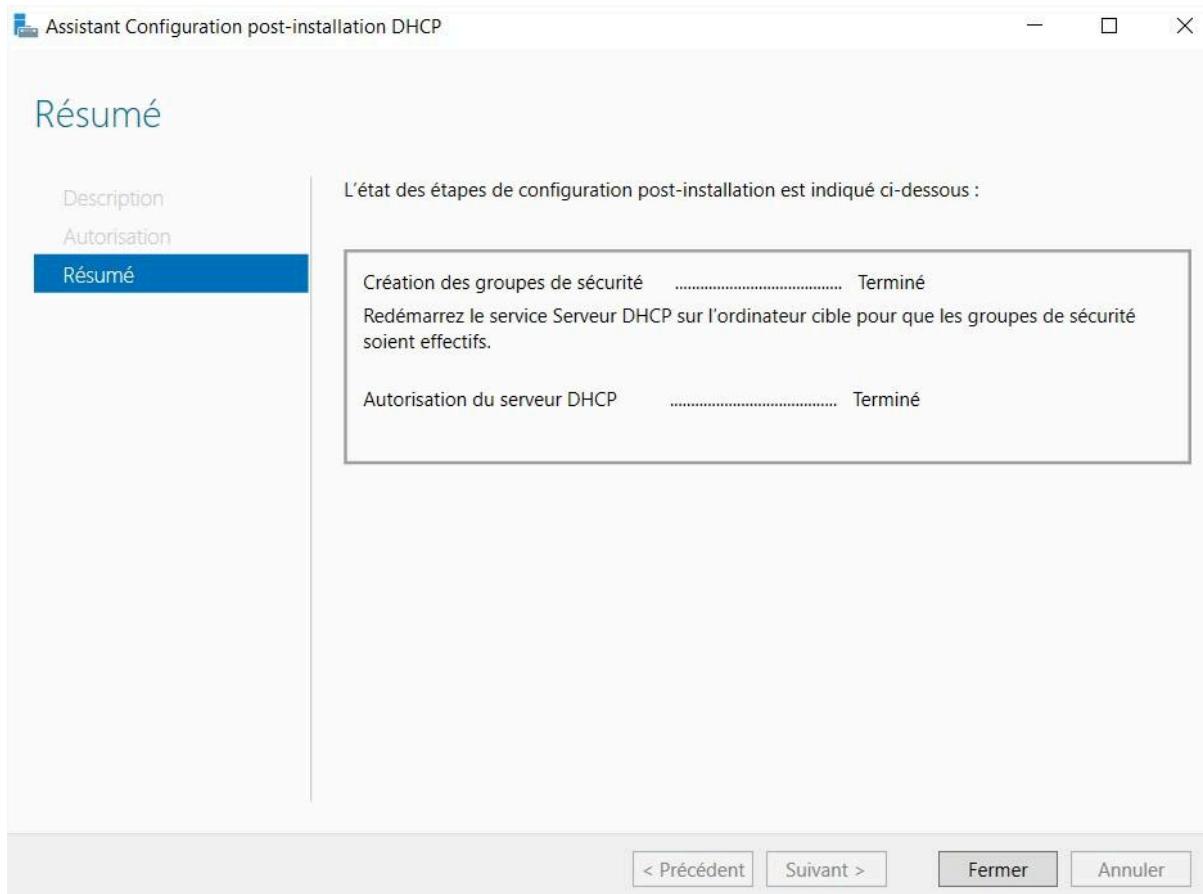
Cliquez sur terminer la configuration DHCP.



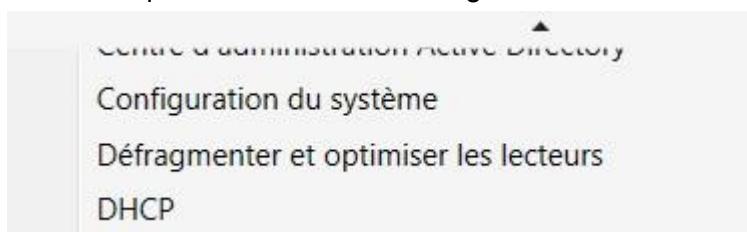
Cliquez sur suivant



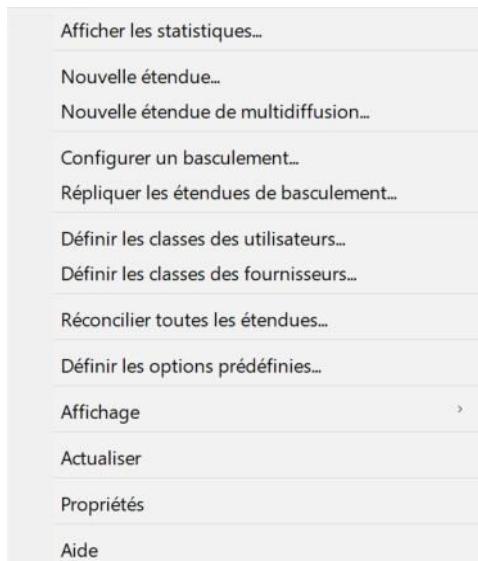
Cliquez sur fermer



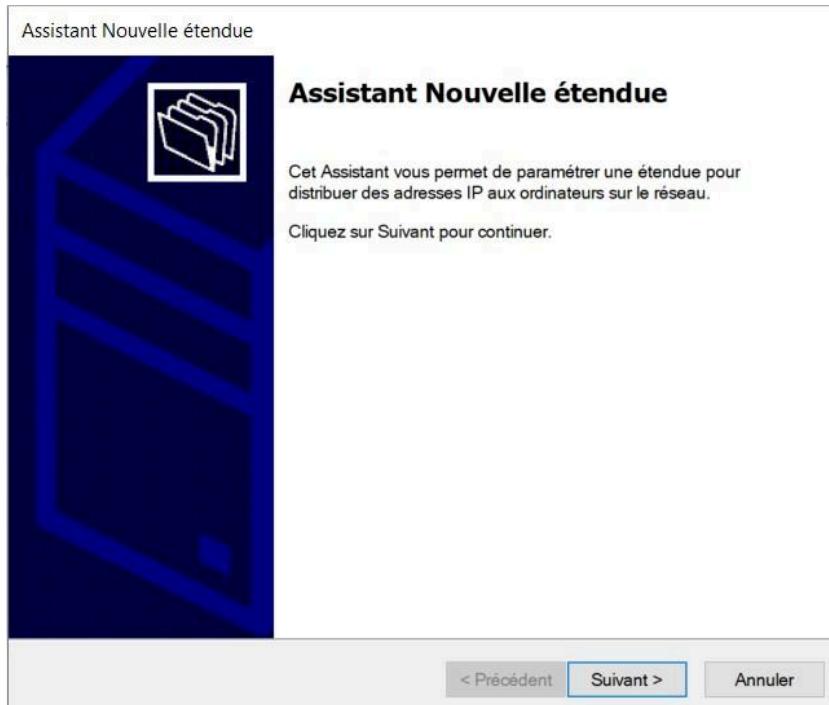
Ensuite cliquez sur DHCP dans l'onglet outils.



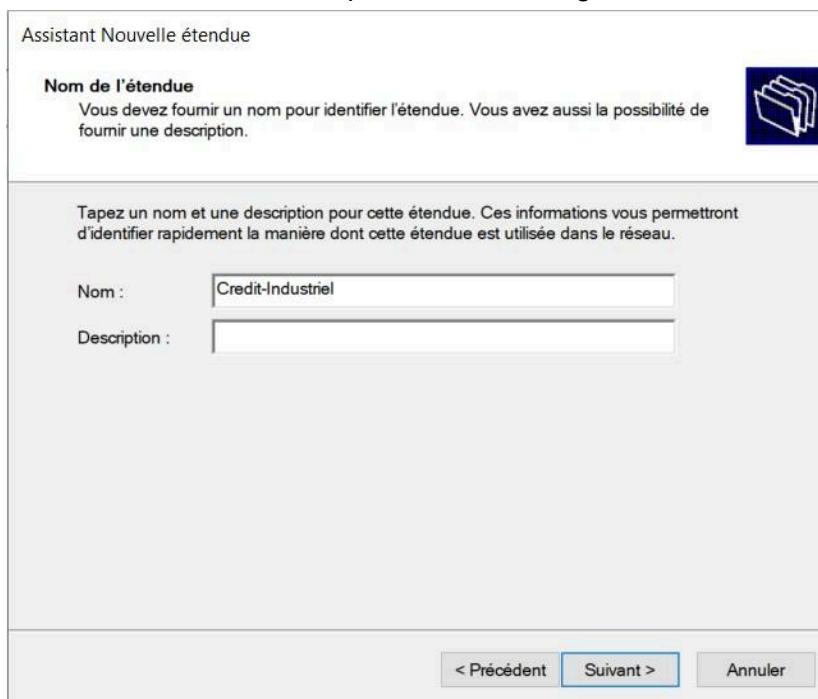
Cliquez sur nouvelle étendue



Cliquez sur suivant



Nommé votre étendue dhcp comme votre organisation le souhaite puis cliquez sur suivant.



ALLEZ À LA PAGE SUIVANTE POUR VOIR LA SUITE

Configuration du DHCP

Définissez votre pool DHCP.

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 : 172 . 31 . 0 . 10
Adresse IP de fin : 172 . 31 . 0 . 254

Paramètres de configuration qui se propagent au client DHCP.

Longueur : 16
Masque de sous-réseau : 255 . 255 . 0 . 0

< Précédent Suivant > Annuler

Définissez un pool DHCP à exclure sinon juste cliquez sur suivant.

Assistant Nouvelle étendue

Ajout d'exclusions et de retard
Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCPOFFER.

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : Adresse IP de fin : Ajouter

Plage d'adresses exclue : Supprimer

Retard du sous-réseau en millisecondes : 0

< Précédent Suivant > Annuler

PS : ALLEZ A LA PAGE SUIVANTE

Définissez la durée du bail DHCP.

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

Sélectionnez oui je configure ces options maintenant.

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.



Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

- Oui, je veux configurer ces options maintenant
 Non, je configurerais ces options ultérieurement

< Précédent Suivant > Annuler

Indiquez la passerelle par défaut puis cliquez sur ajouter puis suivant.

Assistant Nouvelle étendue

Routeur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



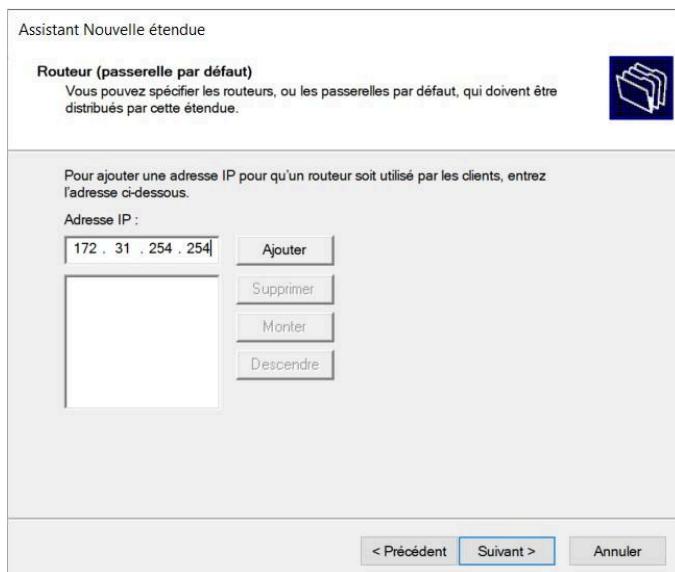
Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

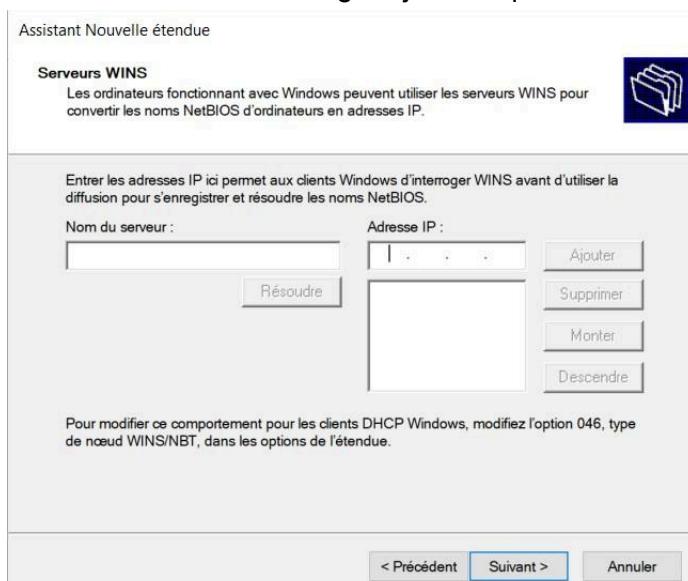
Ajouter
Supprimer
Monter
Descendre

< Précédent Suivant > Annuler

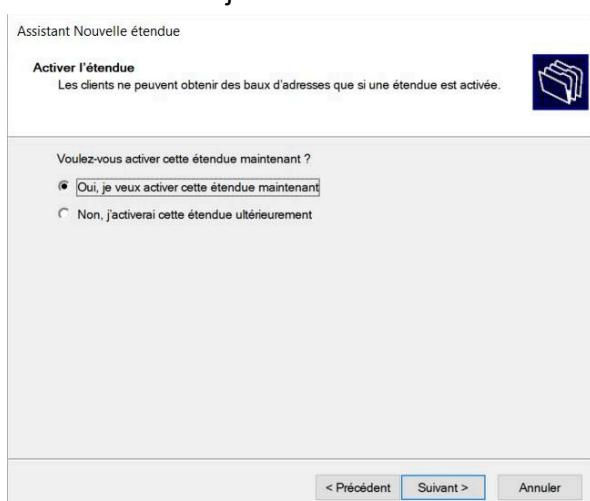
Indiquez le nom de domaine puis l'adresse IP du serveur dns que vous voulez attribuer au poste client, puis cliquez sur suivant.



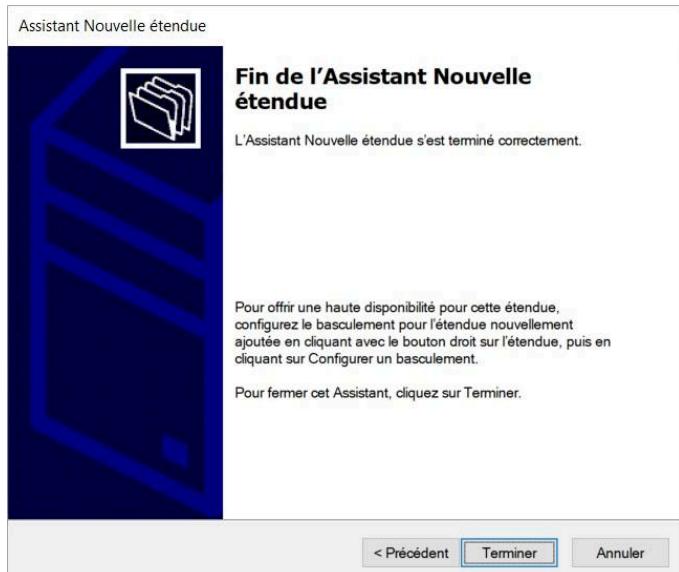
Nom netbios rien à renseigner juste cliquez sur suivant.



Sélectionnez oui je veux activer cette étendue maintenant puis cliquez sur suivant.



Cliquez sur terminer.



L'installation et la configuration et fini voici le pool d'adresse

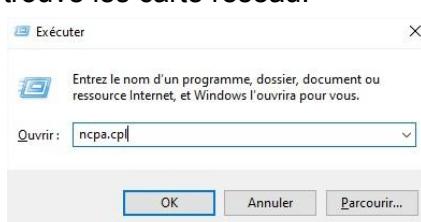
Adresse IP de début	Adresse IP de fin	Description
172.31.0.10	172.31.0.254	Plage d'adresses pour la distribution

Voici les options d'étendue

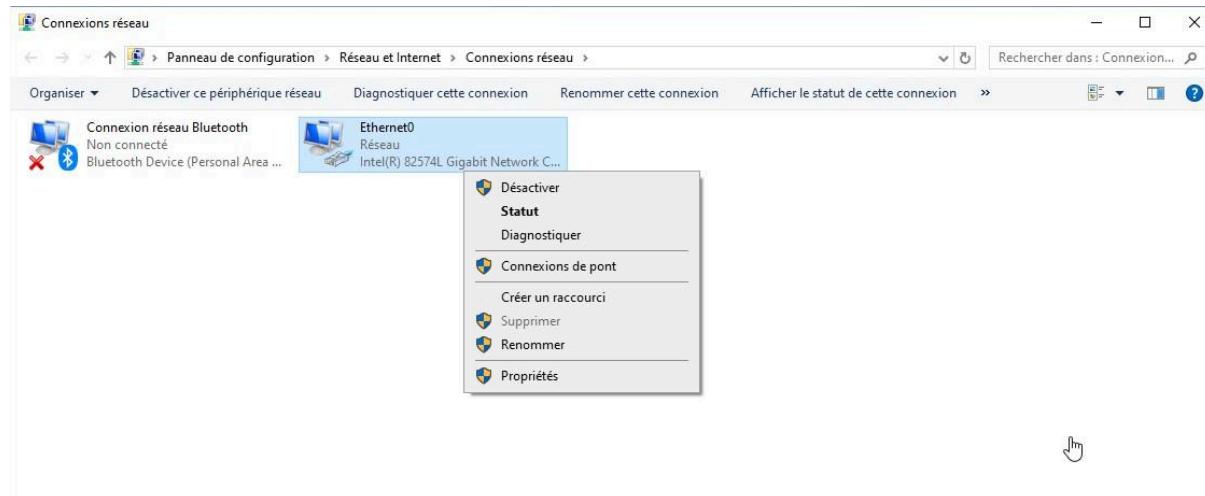
Nom d'option	Fournisseur	Valeur	Nom de la stratégie
003 Routeur	Standard	172.31.254.254	Aucun
006 Serveurs DNS	Standard	172.31.254.251	Aucun
015 Nom de domaine DNS	Standard	Credit-Industriel.local	Aucun

Configurer le client avec dhcp

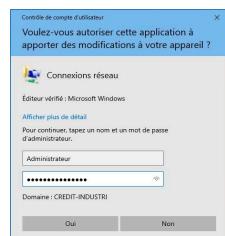
Appuyer sur la touche win+r puis tapez ncpa.cpl pour ouvrir la page du contrôle panel ou ce trouve les carte réseau.



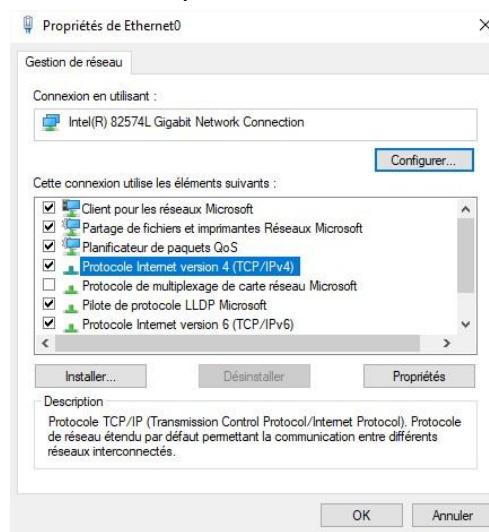
Sélectionnez votre carte réseau wifi ou ethernet en fonction de votre connexion puis cliquer sur propriétés.



Connectez vous avec le compte Administrateur du domaine.

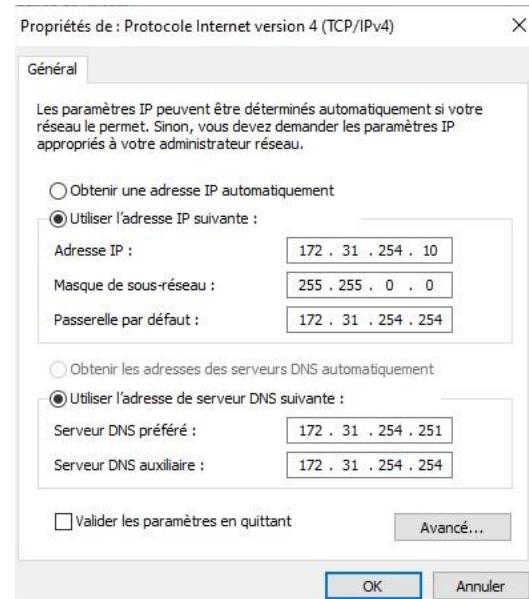


Sélectionnez protocole IPv4



ALLEZ À LA PAGE SUIVANTE POUR VOIR LA SUITE

Cliquez sur obtenir une adresse automatiquement.



Si vous faites des modifications sur votre DHCP et que vous voulez les appliquer sans redémarrer votre machine il vous suffit de faire win+r puis tapez cmd.exe et appuyez sur entrer puis ensuite tapez ipconfig /release.

```
C:\Users\dorian-mathias>ipconfig /release

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Connexion réseau Bluetooth lorsque
son média est déconnecté.

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . .
    Adresse IPv6 de liaison locale. . . . . : fe80::e8f9:e6a9:251a:9f8d%3
    Passerelle par défaut. . . . . : . . . . .

Carte Ethernet Connexion réseau Bluetooth :

    Statut du média. . . . . . . . . . . . . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . :
```

ALLEZ À LA PAGE SUIVANTE POUR VOIR LA SUITE

Puis tapez ipconfig /renew

pour finir tester la configuration réseau en pigan un nom de domaine qui n'est pas sur le réseau local.

```
C:\Users\dorian-mathias>ping google.com

Envoi d'une requête 'ping' sur google.com [142.250.201.174] avec 32 octets de données :
Réponse de 142.250.201.174 : octets=32 temps=57 ms TTL=128
Réponse de 142.250.201.174 : octets=32 temps=45 ms TTL=128
Réponse de 142.250.201.174 : octets=32 temps=55 ms TTL=128
Réponse de 142.250.201.174 : octets=32 temps=222 ms TTL=128

Statistiques Ping pour 142.250.201.174:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 45ms, Maximum = 222ms, Moyenne = 94ms
```

Pour aller plus loin scripting powershell

Script Déetecter les Utilisateurs inactifs.

```
PS C:\Users\Administrateur.WIN-IFC6RFMAGJH> Search-ADAccount -UsersOnly -AccountInactive -Timespan 180

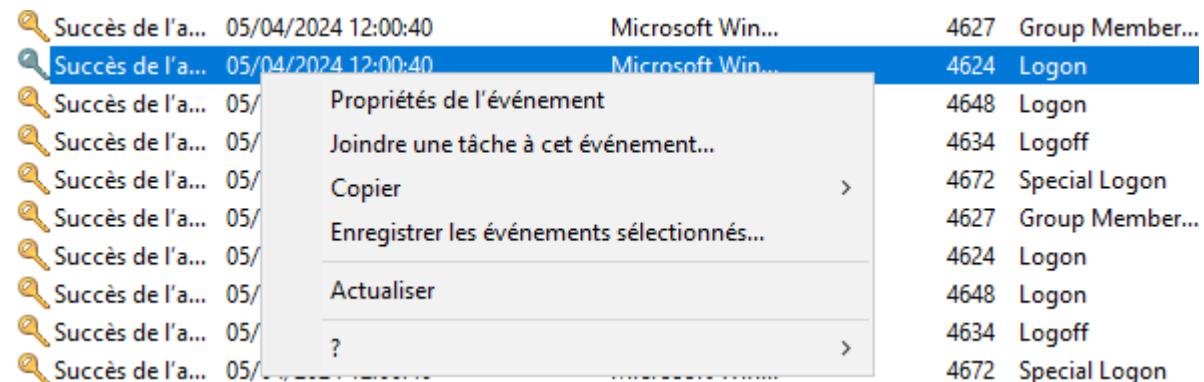
AccountExpirationDate :
DistinguishedName      : CN=Invité,CN=Users,DC=credit-industriel,DC=com
Enabled                 : False
LastLogonDate          :
LockedOut               : False
Name                   : Invité
ObjectClass            : user
ObjectGUID              : 4311b989-e6bf-4876-bb0d-3a17b34008ee
PasswordExpired         : False
PasswordNeverExpires   : True
SamAccountName          : Invité
SID                     : S-1-5-21-3467446566-492738626-1163352156-501
UserPrincipalName       :

AccountExpirationDate :
DistinguishedName      : CN=krbtgt,CN=Users,DC=credit-industriel,DC=com
Enabled                 : False
LastLogonDate          :
LockedOut               : False
Name                   : krbtgt
ObjectClass            : user
ObjectGUID              : 19235356-310b-4c71-aba3-f41bb31a8aff
PasswordExpired         : False
PasswordNeverExpires   : False
SamAccountName          : krbtgt
```

Search-ADaccount : permet de rechercher un utilisateur -UserOnly : seulement les utilisateurs -AccountInactive : compte inactif seulement -Timespan 180 durée d'inactivité.

Script alerte de connexion à l'active directory.

```
log_alert_connexion.ps1 X
1 $Time = Get-Date
2 $Hour = Get-Date -Format HH
3 $text = "Alert connexion at time : " + $Time
4
5 If(($Hour -gt 20) -or ($Hour -lt 7)){
6     Out-File -FilePath C:\Users\Administrateur\Desktop\alert.log -InputObject $text
7 }
```



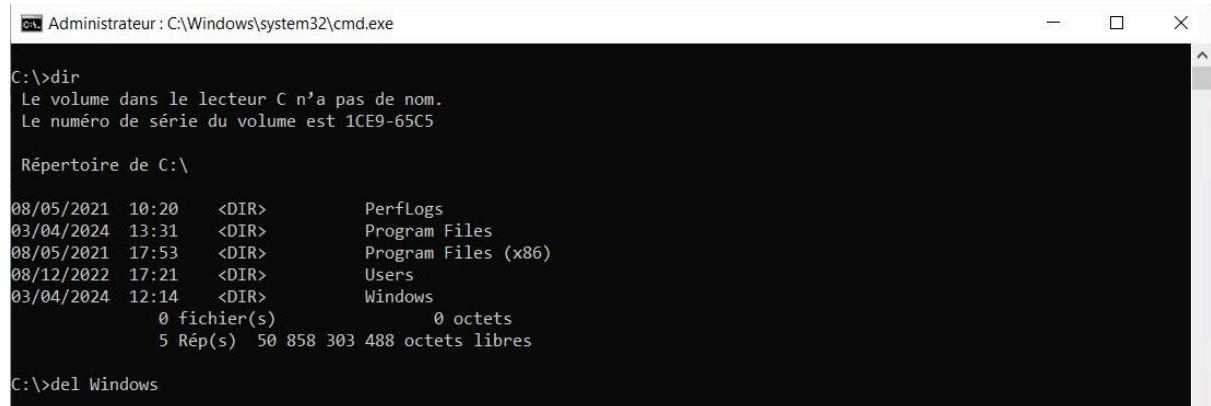
PingCastles

Pour vérifier les failles de sécurité au niveau de l'active directory nous pouvons utiliser un petit logiciel nommé PingCastles pour se faire tapez PingCastles dans la barre de recherche google.com puis ensuite cliquez sur le lien du site puis cliquez sur free download puis download puis ensuite décompresser le fichier PingCastle_3.2.0.1.zip et ensuite rentrer à l'intérieur puis lancer l'exécutable PingCastle.exe.

```
C:\Users\Administrateur\Downloads\PingCastle_3.2.0.1\PingCastle.exe
\---0---> PingCastle (Version 3.2.0.1    13/02/2024 22:23:43)
 \ / \ ``-> Get Active Directory Security at 80% in 20% of the time
  \ \ , ' End of support: 2025-07-31
   0---0
    \ , ' Vincent LE TOUX (contact@pingcastle.com)
     v      twitter: @mysmartlogon      https://www.pingcastle.com
What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
1-healthcheck-Score the risk of a domain
2-azuread  -Score the risk of AzureAD
3-conso    -Aggregate multiple reports into a single one
4-carto   -Build a map of all interconnected domains
5-scanner -Perform specific security checks on workstations
6-export   -Export users or computers
7-advanced -Open the advanced menu
0-Exit
=====
This is the main functionality of PingCastle. In a matter of minutes, it produces a report which will give you an overview of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```

Conclusion :

Windows c'est nul !!!!!! Linux c'est mieux ;)



```
C:\>dir
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est 1CE9-65C5

Répertoire de C:\

08/05/2021 10:20    <DIR>        PerfLogs
03/04/2024 13:31    <DIR>        Program Files
08/05/2021 17:53    <DIR>        Program Files (x86)
08/12/2022 17:21    <DIR>        Users
03/04/2024 12:14    <DIR>        Windows
              0 fichier(s)          0 octets
              5 Rép(s)   50 858 303 488 octets libres

C:\>del Windows
```