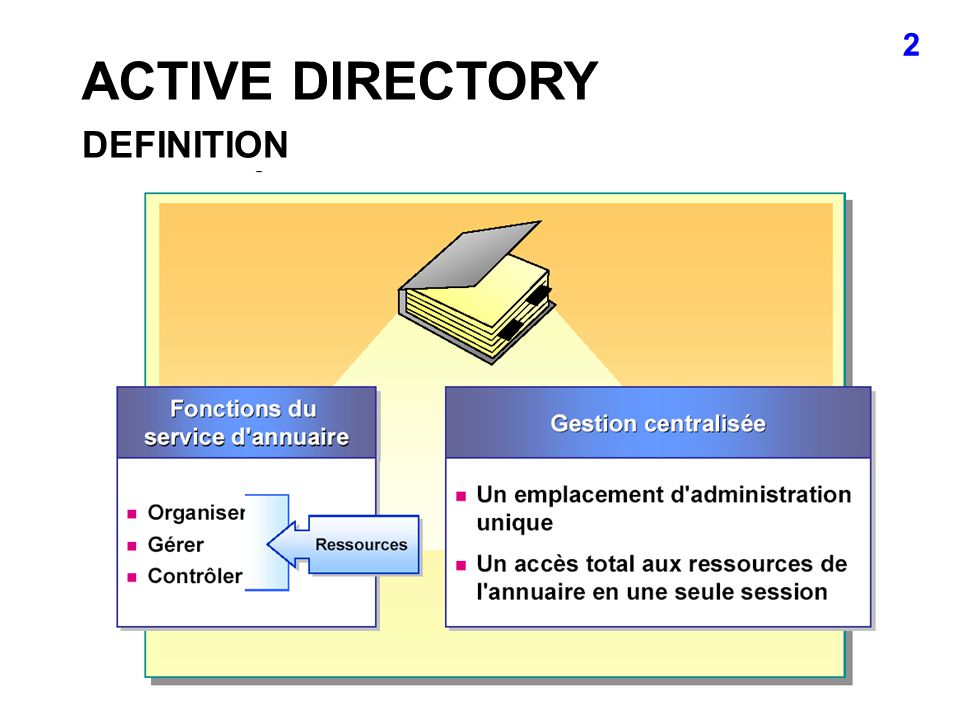
Active Directory

Qu’est-ce qu’Active directory AD

**Active Directory** est un **service complet de gestion d'identité** et de **système d'annuaire** qui fournit des fonctionnalités essentielles pour **la gestion centralisée et sécurisée** des utilisateurs, des groupes, des ordinateurs et des ressources du réseau dans les environnements informatiques basés sur Windows

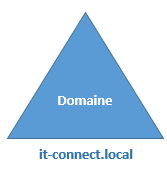


Voici une explication détaillée de ses composants et fonctionnalités :

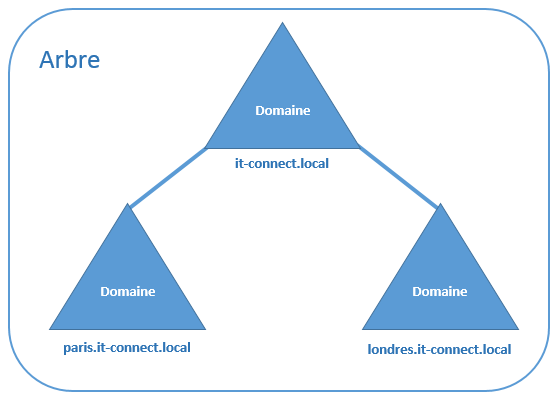
1. **Service d'annuaire** :
   * Au cœur d'Active Directory se trouve un service d'annuaire, qui agit comme une base de données centralisée pour stocker des informations sur les objets du réseau, tels que les utilisateurs, les groupes, les ordinateurs, les imprimantes, les serveurs, etc.
   * Cette base de données est organisée de manière hiérarchique en utilisant un modèle de données basé sur le schéma X.500, avec des objets organisés en classes et en attributs.
2. **Authentification et autorisation** :
   * Active Directory gère l'authentification des utilisateurs, permettant aux utilisateurs de se connecter au réseau en utilisant leurs identifiants (nom d'utilisateur et mot de passe).
   * Il gère également l'autorisation en contrôlant l'accès des utilisateurs aux ressources du réseau en fonction des autorisations définies pour chaque objet.
3. **Domaines et contrôleurs de domaine** :
   * Active Directory utilise une structure de domaine pour organiser les objets du réseau. Un domaine est une unité de gestion qui regroupe un ensemble d'objets (utilisateurs, ordinateurs, etc.) et définit des limites de sécurité.
   * Chaque domaine est contrôlé par un ou plusieurs contrôleurs de domaine, qui sont des serveurs exécutant le service Active Directory Domain Services (AD DS). Les contrôleurs de domaine stockent une copie de la base de données Active Directory pour leur domaine et fournissent des services d'authentification et de réplication.
4. **Unités d'organisation (OU)** :
   * Les unités d'organisation (OU) sont des conteneurs logiques qui permettent d'organiser les objets d'Active Directory de manière hiérarchique selon la structure de l'organisation. Les OU offrent une grande flexibilité pour définir des stratégies de gestion et des autorisations spécifiques.
5. **Politiques de groupe** :
   * Active Directory permet la mise en œuvre de politiques de groupe, qui sont des ensembles de paramètres de configuration appliqués aux utilisateurs et aux ordinateurs pour définir des paramètres de sécurité, des restrictions logicielles, des paramètres du bureau, etc.
   * Les politiques de groupe simplifient la gestion des systèmes en permettant une configuration centralisée et cohérente à travers le réseau.
6. **Services supplémentaires** :
   * Active Directory offre une gamme de services supplémentaires, tels que la gestion des certificats avec Active Directory Certificate Services (AD CS), la gestion de l'accès aux ressources avec Active Directory Federation Services (AD FS), la gestion de la synchronisation d'identité avec Azure Active Directory Connect, etc.

Voici les termes fondamentaux pour comprendre la structure d’active directory

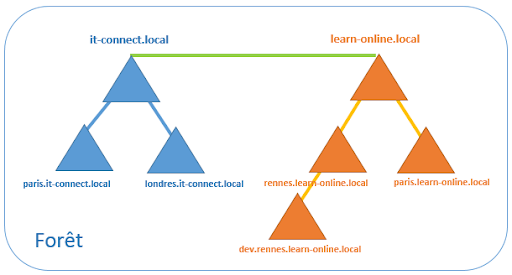
1. **Domaine** :
   * Un domaine est un regroupement logique d'objets, tels que des utilisateurs, des ordinateurs, des groupes et des ressources partageables, dans un réseau informatique. Il fournit un cadre pour l'organisation, la gestion et la sécurisation de ces objets. Par exemple, dans une entreprise, un domaine pourrait regrouper tous les utilisateurs et ordinateurs qui appartiennent à cette entreprise.



1. **Arborescence** (arbre):
   * Une arborescence est une structure hiérarchique composée de plusieurs domaines. Dans une arborescence Active Directory, un domaine parent peut avoir des domaines enfants, et ces domaines peuvent à leur tour avoir des sous-domaines, formant ainsi une structure en arbre. Cela permet d'organiser les ressources et les utilisateurs de manière hiérarchique et de déléguer l'administration de manière efficace.



1. **Forêt** :
   * Une forêt est un ensemble de domaines liés entre eux par des relations de confiance. Chaque domaine dans une forêt partage un schéma commun et une base de données Active Directory. Les forêts permettent aux entreprises de regrouper des domaines qui ont des relations entre eux et de partager des ressources tout en maintenant des niveaux de sécurité appropriés. Par exemple, une entreprise avec des succursales dans différentes villes peut les regrouper dans une forêt pour faciliter la gestion et le partage des ressources tout en maintenant des contrôles de sécurité appropriés.



Quels sont les avantages d’ACTIVE **DIRECTORY** :

Active Directory facilite la vie des administrateurs et des utilisateurs tout en renforçant la sécurité des organisations. Les administrateurs peuvent gérer facilement les utilisateurs et les accès, ainsi que configurer les ordinateurs et les utilisateurs à partir d'un seul endroit grâce aux Stratégies de groupe d'AD. Les utilisateurs n'ont besoin que de s'authentifier une fois pour accéder à toutes les ressources auxquelles ils ont accès (authentification unique). Les fichiers sont stockés dans un endroit centralisé, ce qui facilite le partage et la collaboration, tout en étant sauvegardés régulièrement pour assurer la continuité des activités.

Voici quelques-uns des principaux avantages :

1. **Centralisation de l'authentification et de l'autorisation** :
   * AD centralise l'authentification des utilisateurs, ce qui permet à ces derniers d'utiliser les mêmes identifiants (nom d'utilisateur et mot de passe) pour accéder à diverses ressources du réseau.
   * Il centralise également l'autorisation en permettant aux administrateurs de définir des autorisations granulaires pour chaque objet du réseau, contrôlant ainsi l'accès des utilisateurs aux ressources.
2. **Simplicité de gestion** :
   * AD simplifie la gestion des utilisateurs, des groupes et des ressources en offrant une interface unifiée pour gérer tous ces éléments.
   * Les politiques de groupe permettent de configurer et de gérer les paramètres de sécurité et autres paramètres système de manière centralisée, ce qui simplifie la maintenance et la conformité.
3. **Sécurité renforcée** :
   * Active Directory propose des fonctionnalités de sécurité avancées telles que la gestion des stratégies de mot de passe, le contrôle d'accès basé sur les rôles (RBAC), la surveillance des comptes et des activités, etc.
   * La gestion centralisée des comptes d'utilisateur et des autorisations permet de mieux contrôler les accès et de réduire les risques liés à la sécurité.
4. **Réplication et redondance** :
   * AD utilise un modèle de réplication multi-maître qui permet de distribuer les données d'annuaire sur plusieurs contrôleurs de domaine.
   * Cela garantit une disponibilité élevée des services d'annuaire, ainsi qu'une redondance des données pour éviter les pertes en cas de panne matérielle ou logicielle.
5. **Extensibilité et intégration** :
   * Active Directory est conçu pour être extensible et s'intégrer avec d'autres services et applications. Il peut être utilisé comme base pour la mise en place de services complémentaires tels que la gestion des certificats, la fédération d'identité, la synchronisation avec des services cloud, etc.
   * Il offre également des API et des interfaces de programmation pour permettre aux développeurs de créer des applications qui tirent parti des fonctionnalités d'AD.
6. **Interopérabilité avec d'autres systèmes** :
   * Bien qu'Active Directory soit principalement utilisé dans les environnements Windows, il prend en charge les protocoles standard tels que LDAP (Lightweight Directory Access Protocol) et Kerberos, ce qui lui permet d'interagir avec d'autres systèmes d'annuaire et applications qui prennent en charge ces protocoles.

Ses inconvénients :

1. **Complexité initiale** : La configuration initiale et la mise en place d'Active Directory peuvent être complexes, en particulier pour les organisations qui n'ont pas d'expertise interne en matière de gestion des réseaux Windows. Cela peut nécessiter du temps, des ressources et une formation adéquate.
2. **Coût** : Active Directory est souvent associé à des coûts de licence, notamment pour les licences Windows Server et les éventuels services complémentaires tels que les certificats numériques ou les solutions de sauvegarde.
3. **Maintenance requise** : Comme tout système complexe, Active Directory nécessite une maintenance régulière pour assurer son bon fonctionnement. Cela peut inclure la surveillance de la santé du système, la gestion des mises à jour et des correctifs de sécurité, la sauvegarde et la récupération des données, etc.
4. **Risques de sécurité** : Bien qu'Active Directory offre des fonctionnalités de sécurité avancées, il peut également être une cible pour les attaquants. Les vulnérabilités dans la configuration ou les failles de sécurité dans le logiciel peuvent être exploitées pour compromettre le système.
5. **Dépendance aux services Windows** : Active Directory est étroitement intégré aux services et aux technologies Windows. Cela signifie que les organisations qui utilisent des systèmes d'exploitation ou des applications non-Windows peuvent rencontrer des difficultés d'interopérabilité ou de compatibilité.
6. **Évolutivité limitée** : Bien qu'Active Directory soit conçu pour être scalable, les grandes organisations avec des infrastructures très complexes peuvent rencontrer des limitations en termes de performances et d'évolutivité, nécessitant parfois des solutions supplémentaires ou des configurations spécifiques.

Son fonctionnement et ses fonctionnalités

**Fonctionnement :**

1. **Stockage des données** :
   * Active Directory stocke les informations sur les objets du réseau, tels que les utilisateurs, les groupes, les ordinateurs et les ressources, dans une base de données centralisée appelée annuaire. Cette base de données est répliquée sur plusieurs serveurs pour garantir la disponibilité et la redondance des données.
2. **Authentification** :
   * Lorsqu'un utilisateur tente de se connecter au réseau ou d'accéder à une ressource, Active Directory vérifie son identité en utilisant des informations d'identification telles que le nom d'utilisateur et le mot de passe. Si les informations sont correctes, l'utilisateur est authentifié et autorisé à accéder aux ressources autorisées.
3. **Autorisation** :
   * Une fois qu'un utilisateur est authentifié, Active Directory vérifie les autorisations de cet utilisateur pour accéder aux différentes ressources du réseau. Il s'assure que l'utilisateur a les droits appropriés pour effectuer les actions demandées.
4. **Gestion des politiques** :
   * Active Directory permet de définir et de gérer des politiques de groupe qui spécifient les paramètres de configuration des ordinateurs et des utilisateurs. Ces politiques sont appliquées de manière centralisée et permettent de définir des règles de sécurité, des restrictions d'accès, des paramètres de stratégie de mot de passe, etc.

**Fonctionnalités principales :**

1. **Gestion des identités** :
   * Active Directory offre une gestion centralisée des identités des utilisateurs, des groupes et des ordinateurs. Les administrateurs peuvent créer, modifier et supprimer des comptes utilisateur, des groupes et des comptes d'ordinateurs à partir d'une console d'administration centralisée.
2. **Authentification unique** :
   * Les utilisateurs peuvent s'authentifier une seule fois pour accéder à plusieurs ressources et services du réseau, ce qui simplifie leur expérience de connexion.
3. **Politiques de groupe** :
   * Les politiques de groupe permettent de définir et de gérer les paramètres de configuration des ordinateurs et des utilisateurs de manière centralisée. Cela inclut les paramètres de sécurité, les paramètres de bureau, les restrictions logicielles, etc.
4. **Réplication** :
   * Active Directory utilise un mécanisme de réplication pour synchroniser les données entre les différents serveurs de domaine. Cela garantit que toutes les informations d'annuaire sont cohérentes et à jour sur l'ensemble du réseau.
5. **Services supplémentaires** :
   * Active Directory propose une gamme de services supplémentaires tels que la gestion des certificats avec Active Directory Certificate Services (AD CS), la gestion des droits d'accès avec Active Directory Rights Management Services (AD RMS), etc.

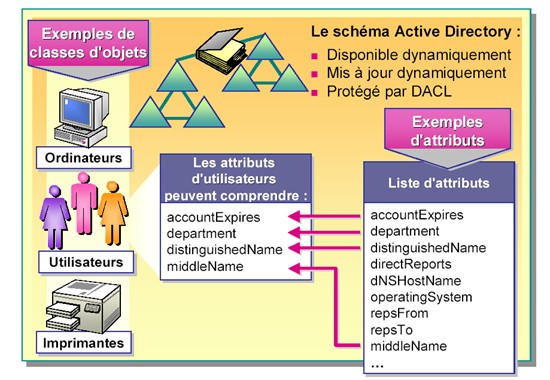
Les attributs et les classes

Dans Active Directory, il y a différents types d'objets comme les utilisateurs, les ordinateurs, les serveurs, les groupes, etc. Chaque type d'objet correspond à une classe, ce qui signifie qu'ils partagent les mêmes caractéristiques appelées attributs.

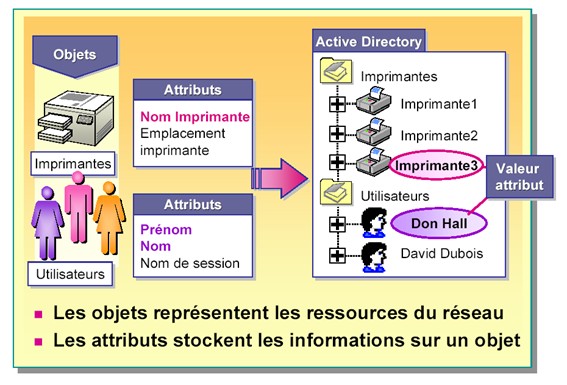
Par exemple, un objet représentant un ordinateur appartient à la classe "Ordinateur" et possède des valeurs spécifiques comme le nom de l'ordinateur, son adresse IP, etc.

Certains objets peuvent agir comme des contenants pour d'autres objets. Par exemple, les groupes peuvent contenir plusieurs utilisateurs pour simplifier leur gestion. De même, les unités d'organisation servent à organiser les objets dans une structure hiérarchique.

Imaginez les unités d'organisation comme des dossiers dans lesquels vous rangez des fichiers. Cela aide à garder les objets bien organisés dans l'annuaire et facilite l'administration du réseau.



Le Schéma

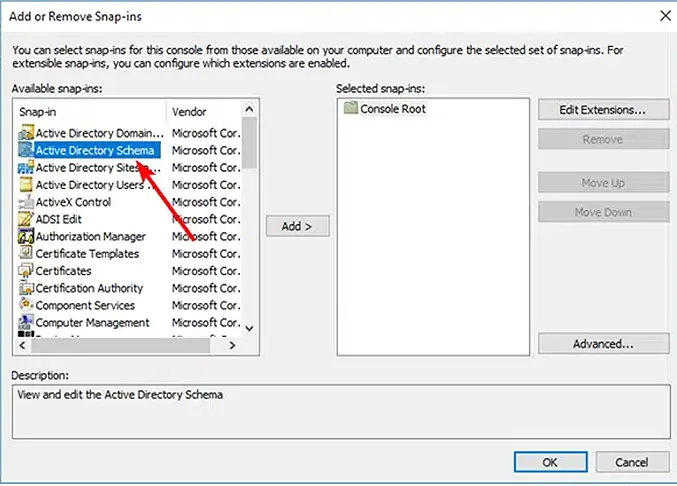


Le schéma dans Active Directory est comme un **ensemble de règles qui définissent quelles sont les différentes catégories d'objets** (comme les utilisateurs, les ordinateurs, etc.) et quels types d'informations peuvent être stockés sur ces objets (comme leur nom, leur adresse email, etc.).

Ces règles sont importantes car elles déterminent la façon dont vous pouvez organiser et gérer votre annuaire. Par exemple, elles définissent quelles informations vous pouvez ajouter à un utilisateur et comment vous pouvez les utiliser.

Le schéma peut évoluer au fil du temps pour s'adapter à vos besoins ou aux besoins de certaines applications. Par exemple, si vous installez un logiciel comme Microsoft Exchange pour la messagerie, il peut modifier le schéma pour prendre en charge ses propres fonctionnalités.

Cependant, la modification du schéma doit être faite avec précaution car elle peut avoir un impact sur toute votre infrastructure. C'est pourquoi seuls les administrateurs spéciaux, appelés "Administrateurs du schéma", sont autorisés à apporter des modifications au schéma par défaut. Cela garantit que les changements sont bien réfléchis et contrôlés.



Les partitions d’annuaires

L'annuaire Active Directory est divisé en trois parties principales appelées partitions de répertoire, ou "Naming Contexts" :

1. **Partition de schéma** :
   * Contient les définitions des différentes catégories d'objets (comme les utilisateurs, les ordinateurs, etc.) et de leurs attributs (comme le nom, l'adresse email, etc.). C'est comme un guide qui indique ce que chaque objet peut contenir et faire. Cette partition est unique pour toute la forêt Active Directory.
2. **Partition de configuration** :
   * Contient des informations sur la structure et la configuration de l'environnement Active Directory, comme les domaines, les contrôleurs de domaine, les sites réseau, etc. C'est comme une carte qui montre comment tous ces éléments sont connectés les uns aux autres. Cette partition est unique pour toute la forêt Active Directory.
3. **Partition de domaine** :
   * Contient les informations spécifiques à chaque domaine, comme les objets utilisateurs, les groupes, les ordinateurs, etc. C'est comme un dossier qui contient toutes les informations locales à un domaine particulier. Chaque domaine a sa propre partition de domaine.

Contrôleurs de domaine

Les contrôleurs de domaine sont des serveurs Windows qui stockent la base de données Active Directory et exécutent les fonctions essentielles telles que l'authentification et l'autorisation des utilisateurs.

Chaque contrôleur de domaine contient une copie de la base de données Active Directory pour son domaine spécifique, ce qui comprend toutes les informations sur les objets (utilisateurs, groupes, ordinateurs, etc.) appartenant à ce domaine. De plus, chaque contrôleur de domaine sauvegarde également des informations sur le schéma de la forêt et sur la structure de cette dernière.

Les contrôleurs de domaine ne sauvegardent pas de copies des schémas ou des forêts d'autres domaines, même s'ils sont sur le même réseau.

Certains contrôleurs de domaine peuvent également être spécialisés pour remplir des fonctions spécifiques qui ne sont pas disponibles sur les contrôleurs de domaine standard. Ces rôles spécialisés, appelés **les rôles de maîtres**, sont initialement attribués au premier contrôleur de domaine créé dans chaque forêt ou domaine. Cependant, l'administrateur a la possibilité de redistribuer manuellement ces rôles si nécessaire.

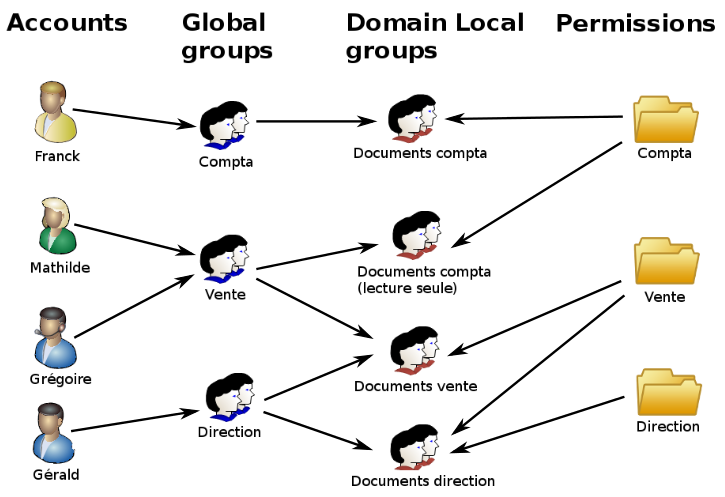
Dans une forêt Active Directory, il y a plusieurs rôles de maître qui assurent des fonctions critiques pour le bon fonctionnement de l'infrastructure. Voici quelques-uns de ces rôles :

1. **Maître de schéma** :
   * Il y a un seul maître de schéma par forêt. Ce maître contient la copie principale du schéma utilisé par tous les autres contrôleurs de domaine dans la forêt. Cela garantit que la définition des objets est cohérente dans toute la forêt.
2. **Maître d’attribution des noms de domaine** :
   * Chaque forêt a un seul maître d’attribution des noms de domaine. Ce maître s'assure que tous les noms d'objets sont uniques dans la forêt et peut effectuer des vérifications croisées avec d'autres annuaires si nécessaire.
3. **Maître d’infrastructure** :
   * Chaque domaine a un seul maître d’infrastructure. Ce maître garde une trace des objets supprimés et maintient les références d'objets entre différents domaines.
4. **Maître des ID relatifs (RID Master)** :
   * Chaque domaine a un seul maître des ID relatifs. Ce maître est responsable de la génération et de l'attribution des identifiants uniques de sécurité (SID) pour les objets dans le domaine.

La méthode AGDLP

La méthode AGDLP est une façon organisée de gérer qui peut accéder à quoi dans un réseau informatique. Elle se base sur l'idée de mettre les utilisateurs dans des groupes, puis d'associer ces groupes à d'autres groupes qui représentent le type d'accès nécessaire, et enfin de donner des autorisations à ces groupes pour accéder à des fichiers, des dossiers ou des imprimantes.

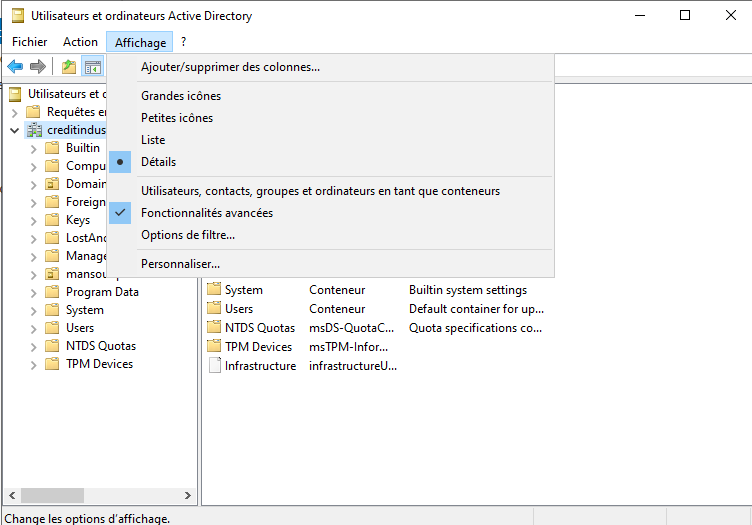
Cela rend la gestion des autorisations plus facile et moins sujette aux erreurs. Mais pour que ça marche bien, il faut que les administrateurs soient disciplinés et suivent toujours cette méthode. Sinon, ça peut devenir compliqué à gérer, surtout quand il y a des changements d'équipe.



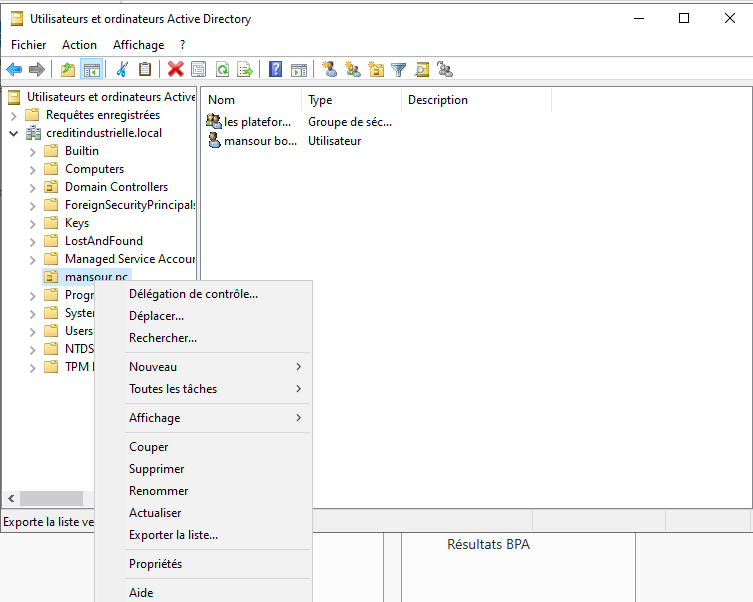
Haut du formulaire

Comment supprimer une unité d’organisation sur active directory :

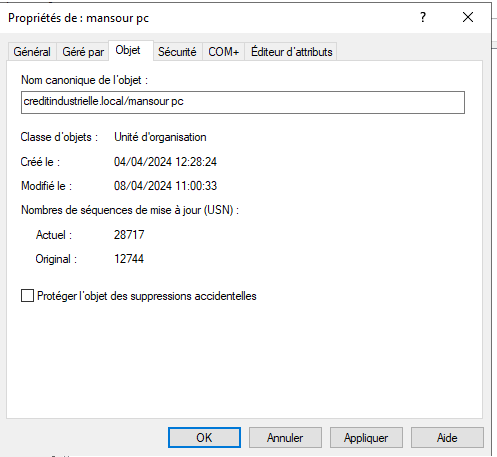
Il suffit de se rendre dans la console « **utilisateurs et ordinateurs Active Directory**», clic sur **« affichage**» et clique sur l’option **« Fonctionnalités avancées »**



Après clic droit sur l’unité d’organisation que l’on souhaite supprimer, sélectionne « propriétés »

\*

Allé dans l’onglet « **Objet** » et décoche la case « **Protéger l’objet des suppressions accidentelles »** et clic sur **« Appliquer »** pour enregistrer le changement



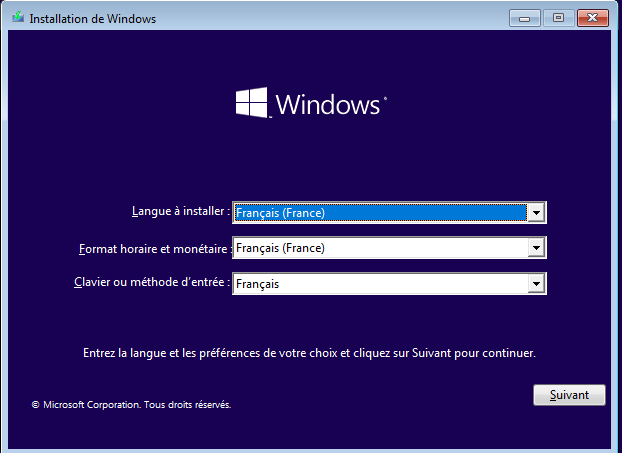
Sortir et supprimer l’OU.

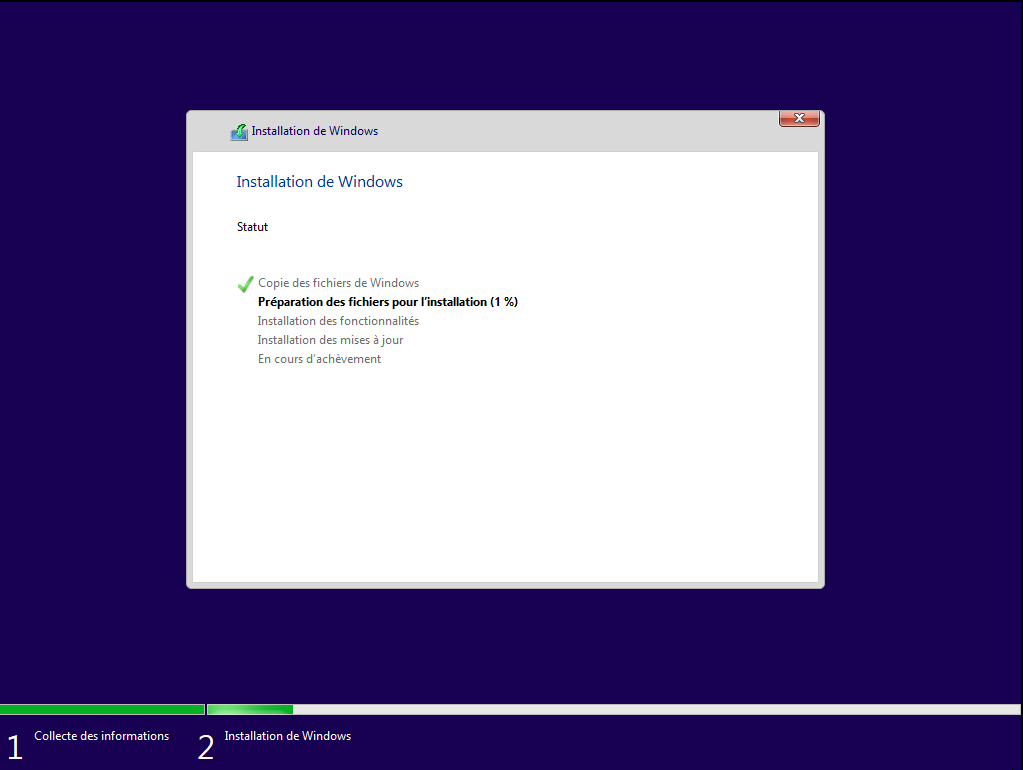
Job 1

Installation d’une vm windows

Suivons les étapes comme nous avons l’habitude de faire création d’une vm ajouter fichier iso correspondant au système d’exploitation que l’on souhaite, nous ça sera Windows

Puis a suit les intrcutions suivante :





Une fois Active directory installé et configuré.

Pour notre structure nous avons choisi la configurations suivante

Voici la matrice des droits acces :

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Groupe de service | | | | | | | | | |
| DOSSIERS | | Cat. A | Cat. B | Cat. C | Cat. D | Client | Informaticiens  Prestataires | Chefs de Projet |  |
| Opération |  | R | RW | RW | RW |  | RE |  |  |
|  | Versement > 10K | R | RW | RW | RW |  | RE |  |  |
|  | Versement max. 100K | R |  | RPW | RW |  | RE |  |  |
| Guichet |  | R |  |  | RW |  | RE |  |  |
| Accueil |  | R |  |  | RW |  | RE |  |  |
| Compte clients |  | R | R | R | RW | R | RE |  |  |
| App. |  |  |  |  | RW |  | RE | RW |  |

Haut du formulaire

LEGENDE :

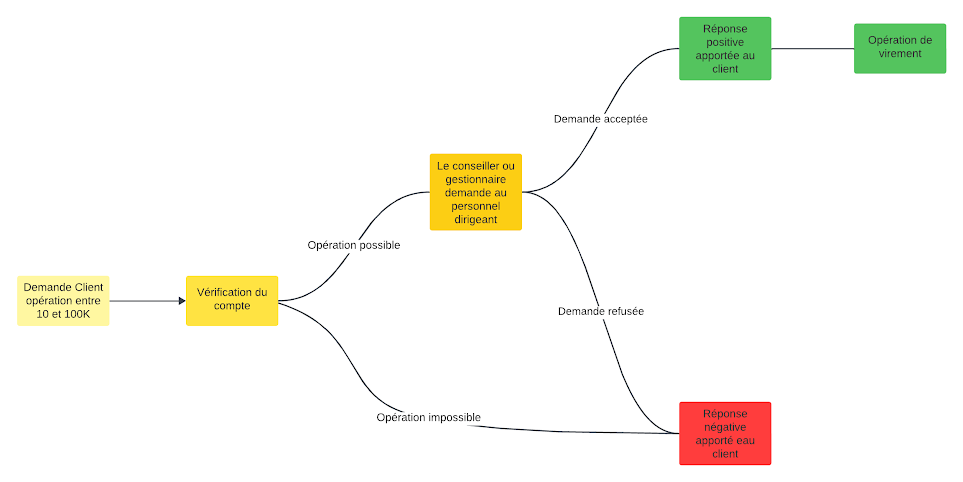
R = read

W = write

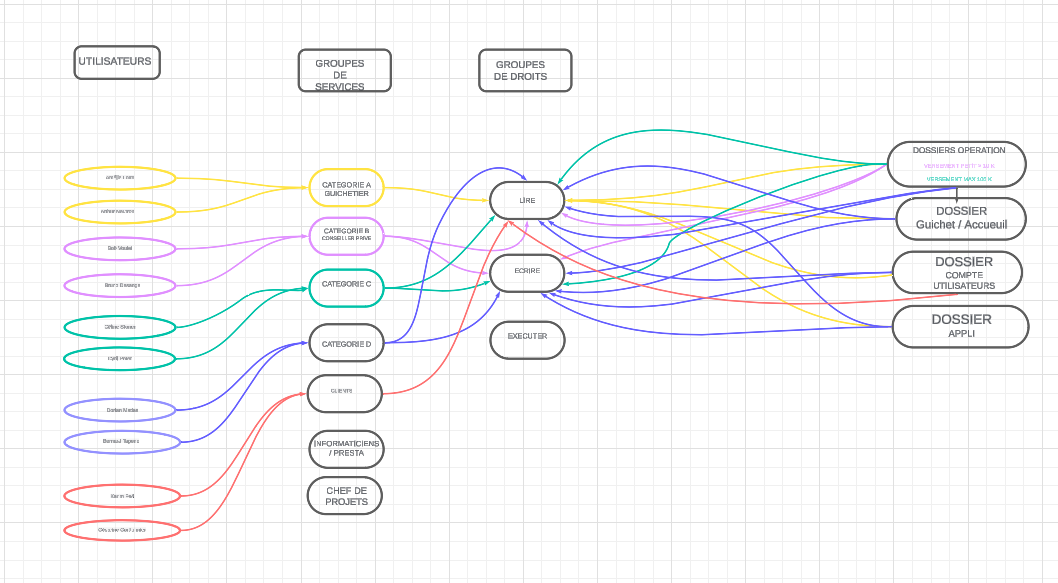
RP = read permission

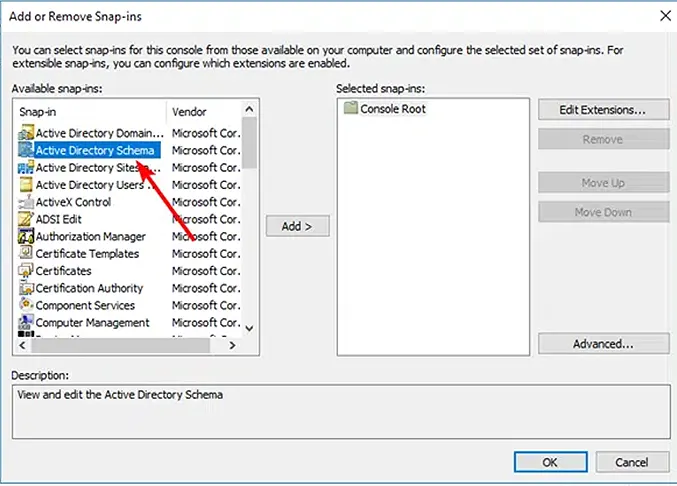
E= excute

Matrice de flux :

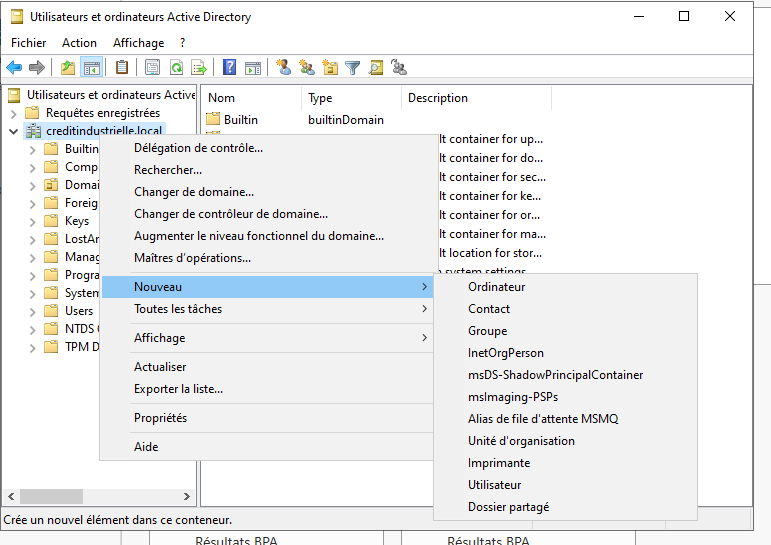


Diagrammes de droit détaillés



Pour créer une unité d’organisation dans notre domaine « creditIndustrielle.local » 

Il suffit de clic droit sur le nom domaine concerné. Puis nouveau et unité d’organisation



Que l’on appelle comme ci-dessous, voici notre OU crée



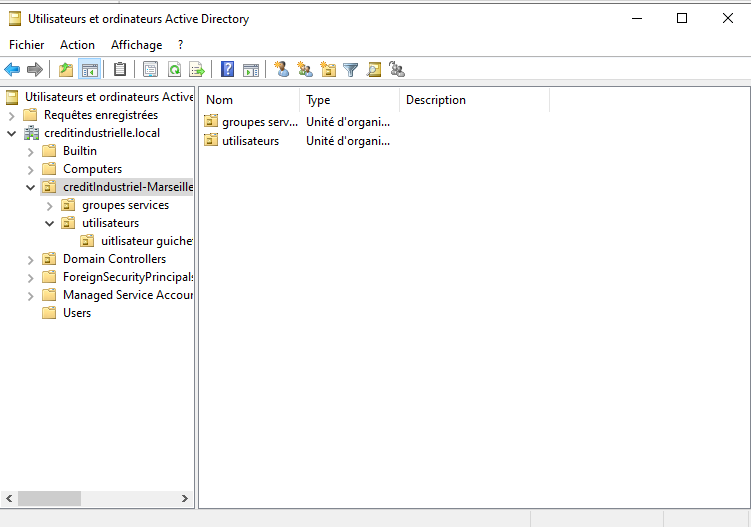
Une fois le « OU » crée on va créer des sous « OU »

Les sous-unités d'organisation (OU) dans Active Directory permettent de :

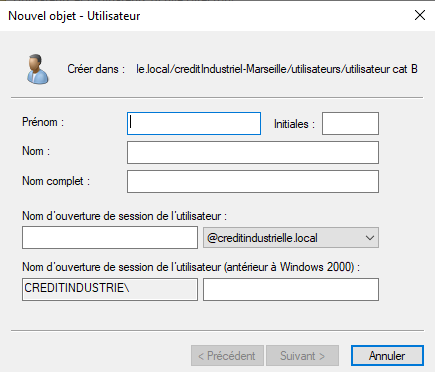
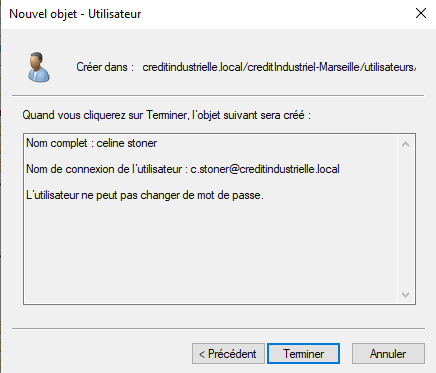
1. Organiser hiérarchiquement vos ressources, utilisateurs, groupes et ordinateurs.
2. Gérer les autorisations de manière spécifique pour chaque sous-OU.
3. Appliquer des stratégies de groupe (GPO) selon des besoins particuliers.
4. Segmenter votre environnement pour faciliter la gestion, en fonction de services, départements ou sites géographiques.
5. Définir des politiques de mot de passe adaptées à chaque sous-OU.
6. Déléguer certaines tâches d'administration à des utilisateurs ou groupes spécifiques, offrant ainsi une administration plus efficace et sécurisée.

On crée donc de sous O.U« GROUPES SERVICES qui contiendra tous nos groupes de services

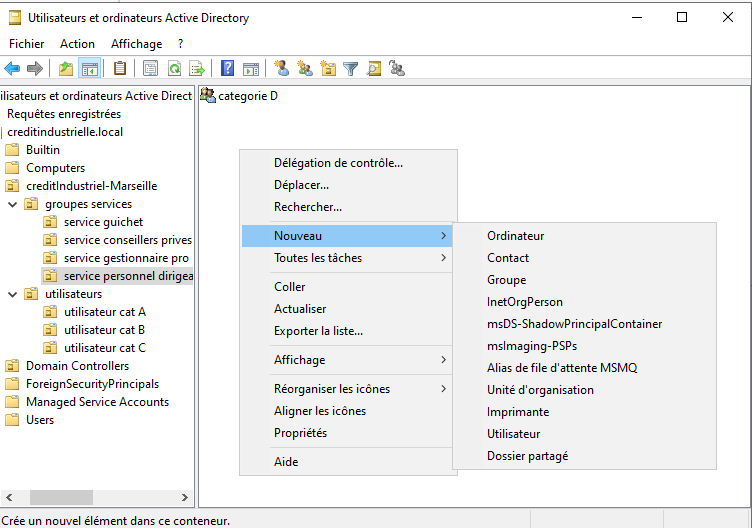
Et utilisateur pour nos groupes utilisateur par service pour une question d’organisation et de lisibilité

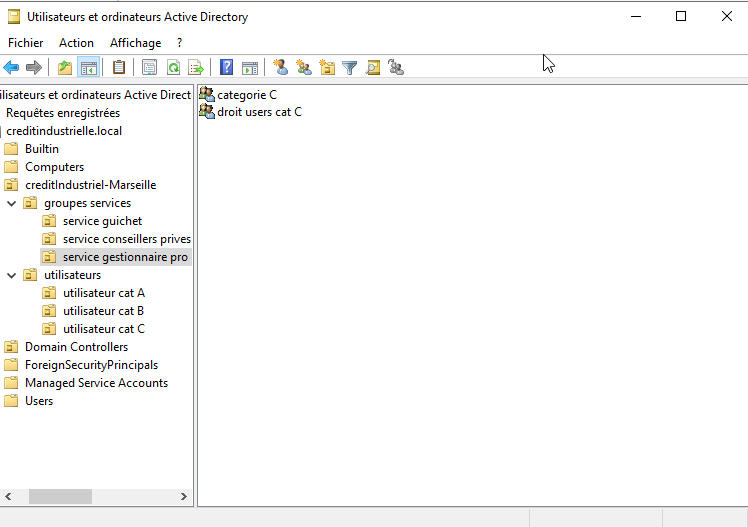


On crée nos user dans l’onglet dédié

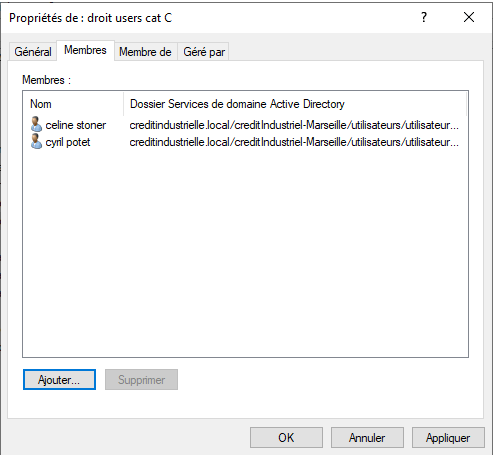
 

On crée 2 groupes l’un correspondant aux groupes de la catégorie du service et le groupes utilisateurs pour attribuer les droits en fonction du service ils appartiennent





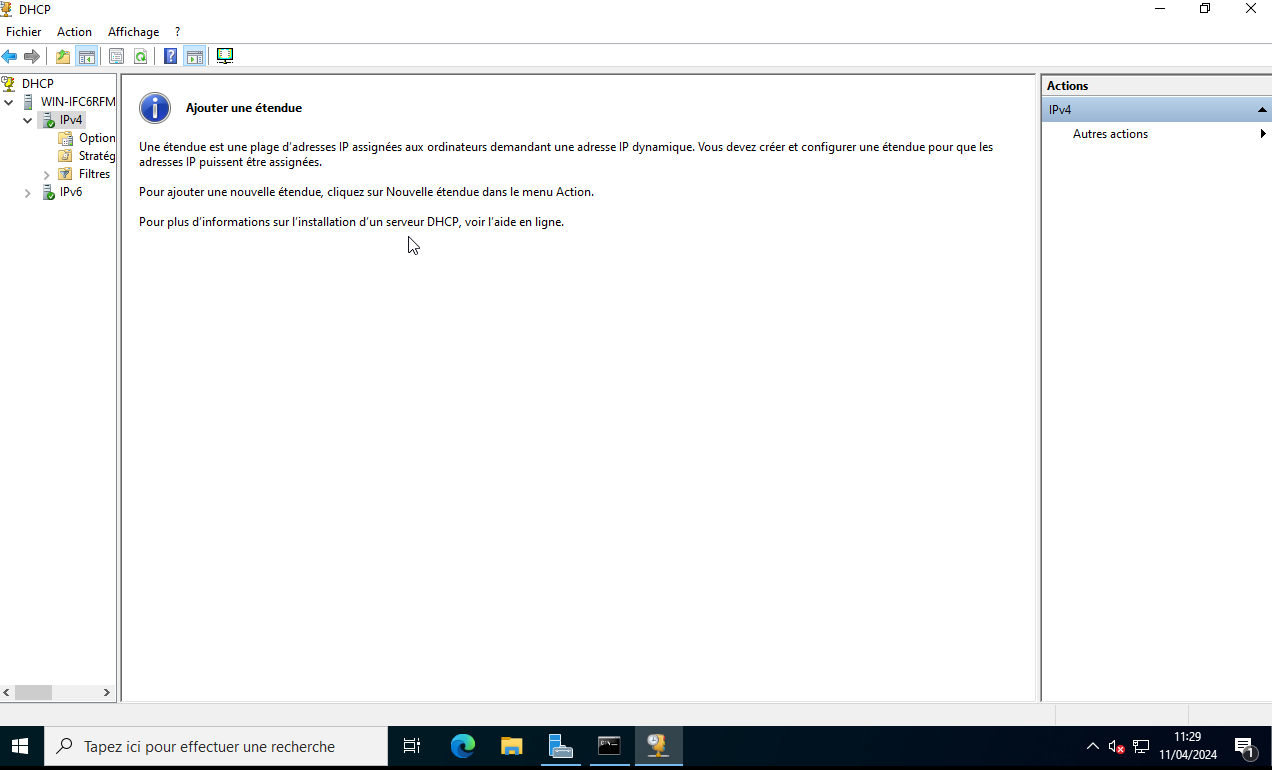
Dans le groupes droit users cat C, on a joute les utilisateurs correspondant à la catégorie du service correspondant



Apres on va dans « Gestion d’ordinateur », on crée des dossiers partager et par le dossier et on attribut les droits par dossier et on ajoute les droit correspondant dans dossier partager et / ou sécurité

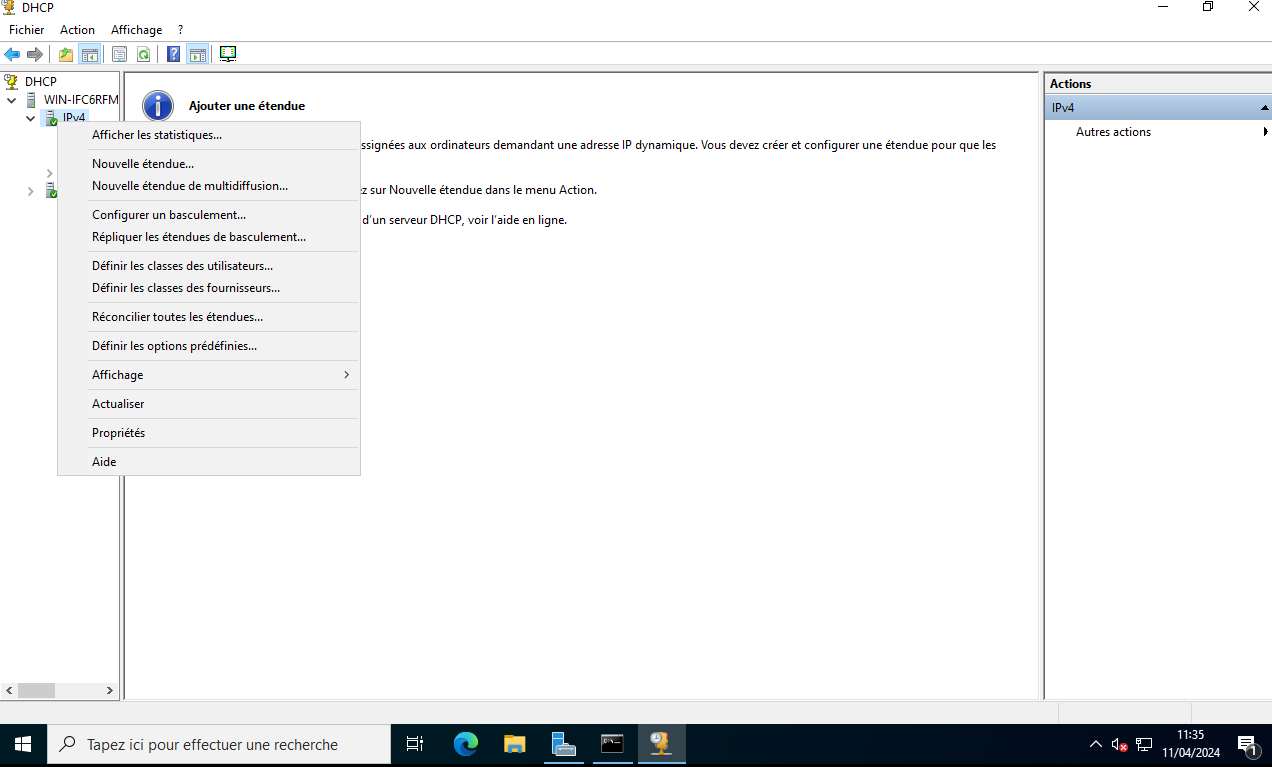
Pour relier notre domaine a notre autre vm correspondant au pc01, il faut aller dans le gestionnaire du dhcp du serveur et ajouter une etendue a notre dhcp

Après avoir installé et démarré le service DHCP, vous devez créer une étendue. L’étendue est une plage d’adresses IP valides disponibles à bail pour les ordinateurs clients DHCP sur le réseau. Microsoft recommande que chaque serveur DHCP de votre environnement ait au moins une étendue qui ne chevauche aucune autre étendue de serveur DHCP dans votre environnement. Dans Windows Server 2003, les serveurs DHCP d’un domaine Active Directory doivent être autorisés pour empêcher la mise en ligne de serveurs DHCP non autorisés.

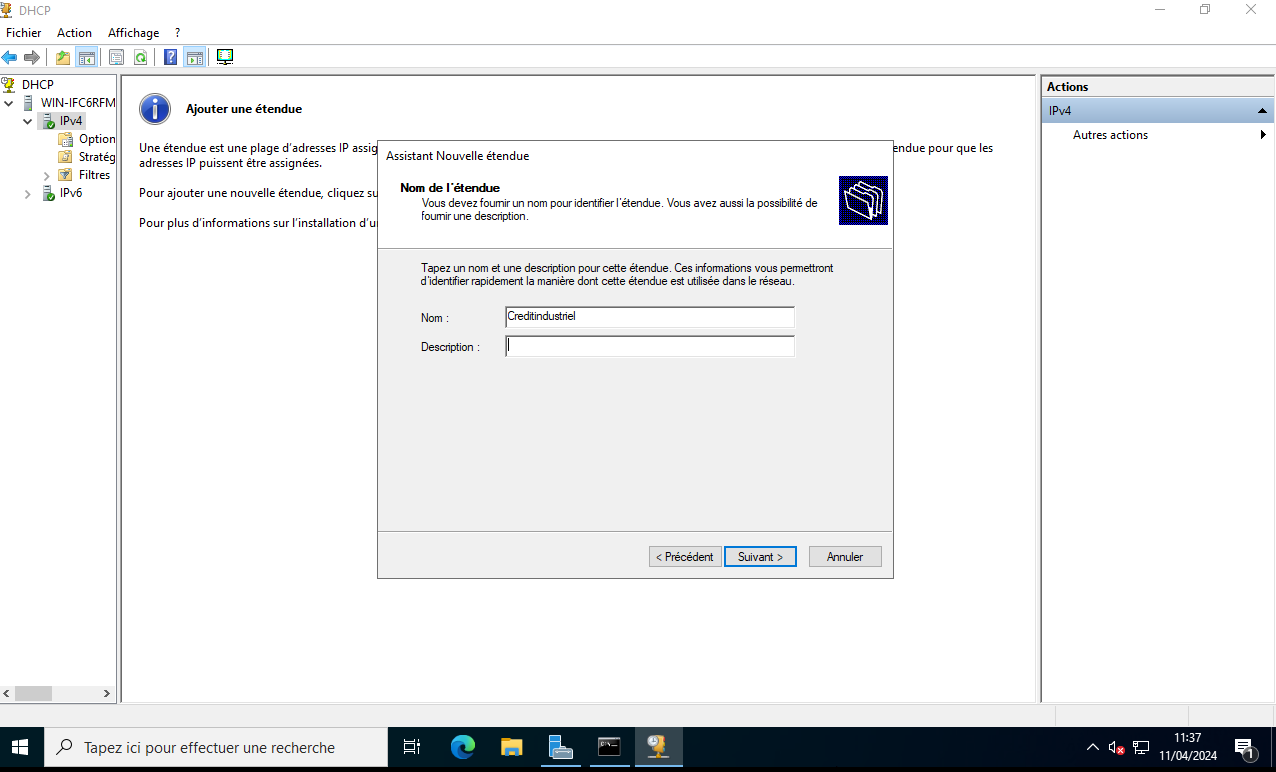


N'oubliez pas d'autoriser le serveur DHCP dans l'arborescence de la console en cliquant sur "Autoriser" dans le menu Action après avoir terminé la configuration.

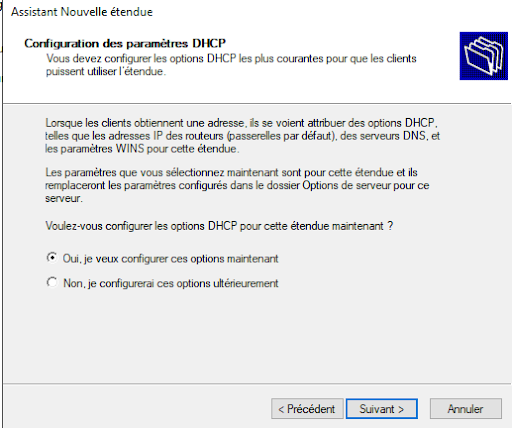
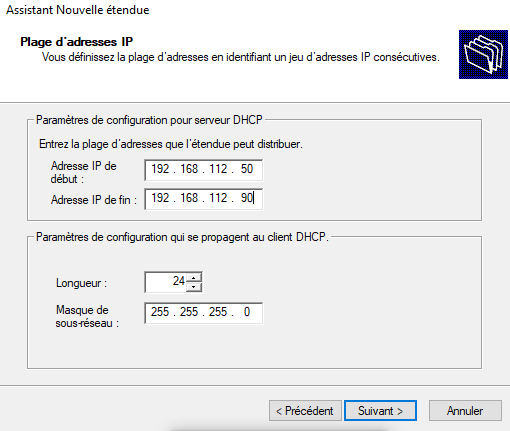
Sélectionnez le serveur DHCP approprié dans l'arborescence de la console et cliquez avec le bouton droit pour choisir "Nouvelle étendue".



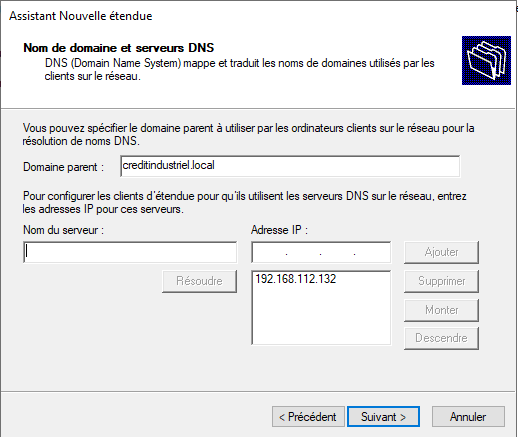
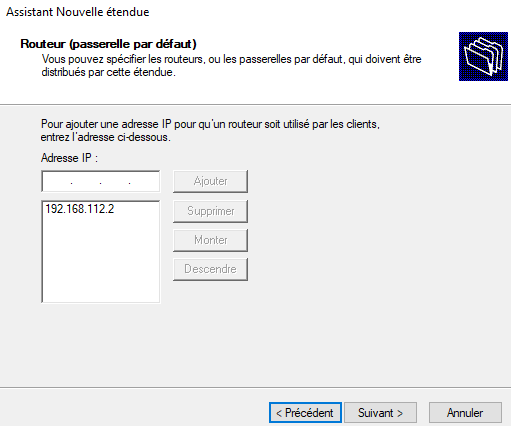
Nommez et décrivez l'étendue de manière descriptive



Définissez la plage d'adresses IP disponibles pour le bail DHCP, excluant les adresses déjà attribuées statiquement. Spécifiez la durée du bail DHCP.

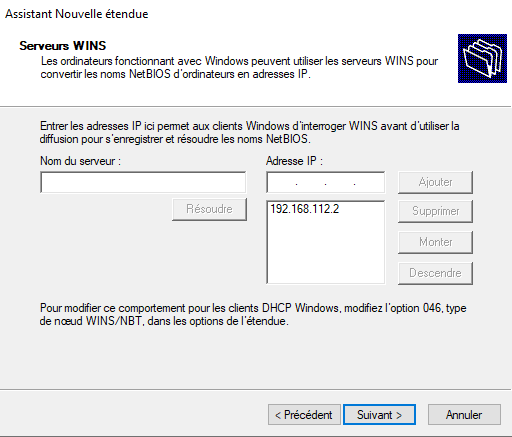


Configurez l'adresse IP de la passerelle par défaut et les serveurs DNS.

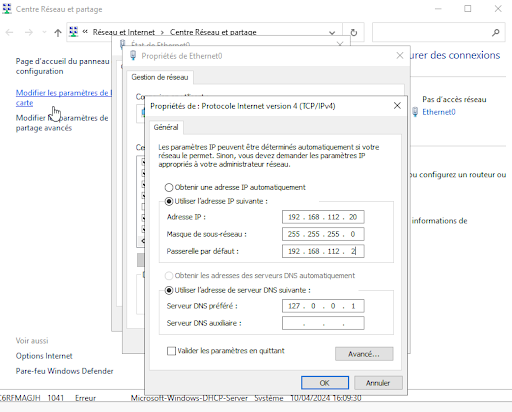


Le cas échéant, ajoutez un serveur WINS.

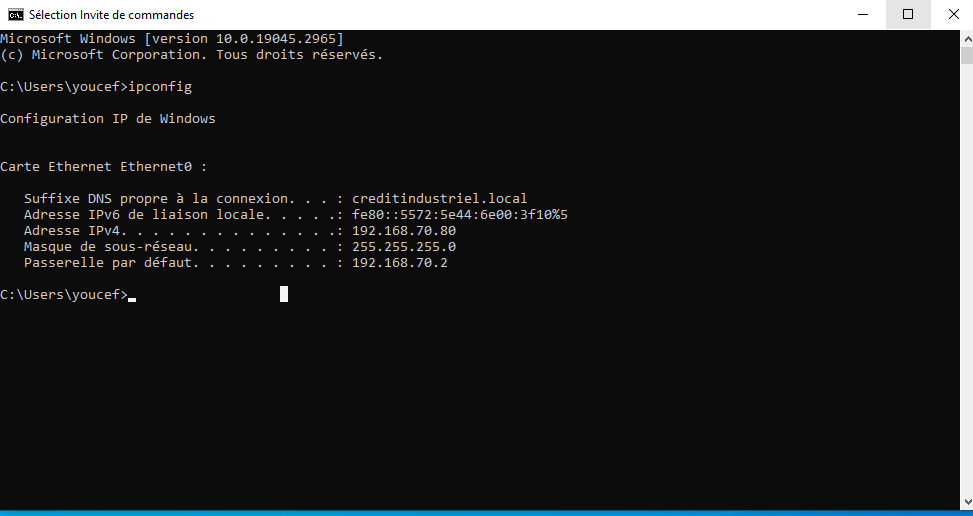
Activez l'étendue et autorisez les clients à obtenir des baux.



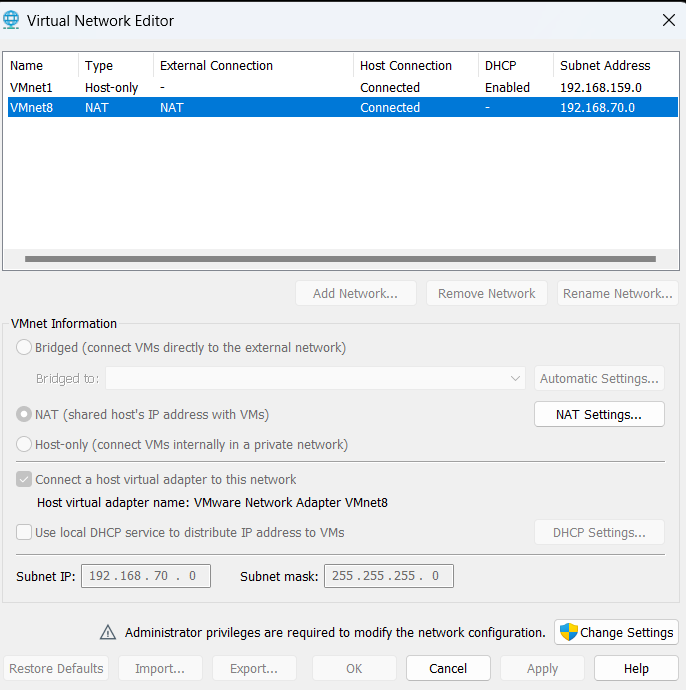
On va ensuite dans **centre de réseau et partage**, **propriété de Ethernet** et on configure une **adresse static** pour notre machine **Active Directory** qui comprend **DHCP** et **DNS**



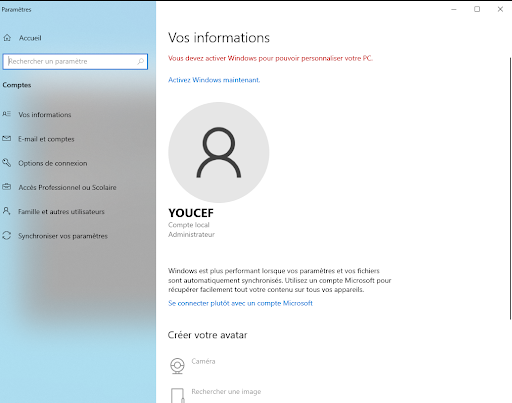
On se rend dans le terminal,avec la commande ipconfig pour s’assurer que l’adresse IP soit bien conforme à celle du DHCP configuré sur le serveur .



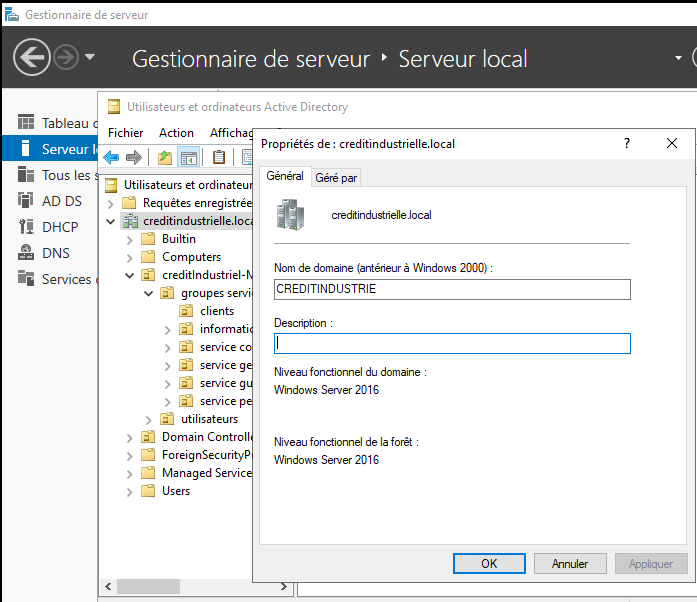
ATTENTION regarder dans VIRTUAL NETWORK EDITOR et bien décoché le DHCP du NAT



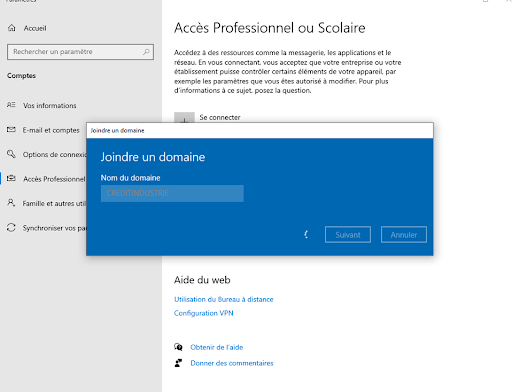
Ensuite on va dans la VM client et on va relier le domaine a ce pc, allé dans la barre démarrer🡺utilisateur et cliqué sur Modifier les paramètres du compte et on va sur accès professionnel ou scolaire.



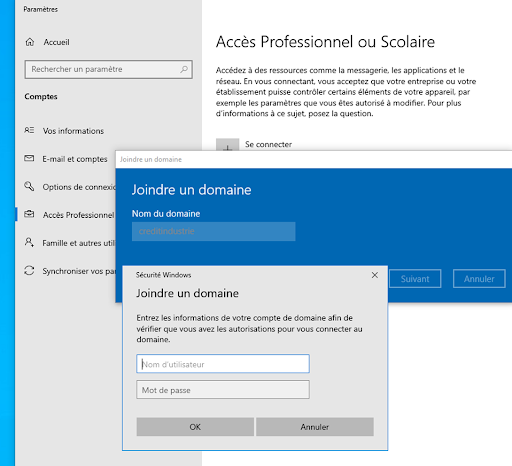
Pour trouver le nom du domaine il suffit d’aller dans propriétés de notre domaine



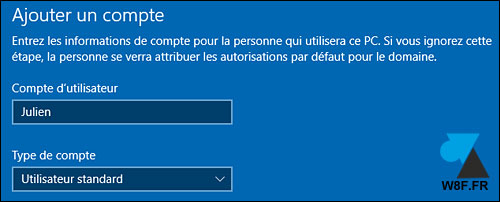
on rentre le nom de notre domaine



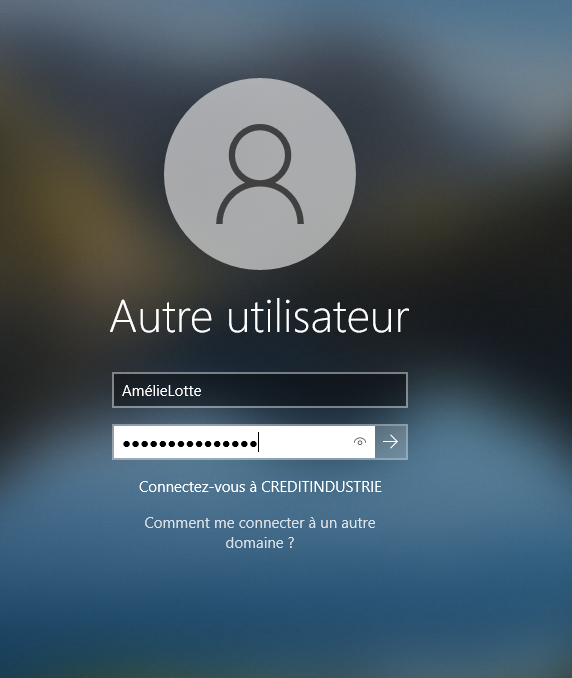
Puis on entre Administrateur du serveur avec son mdp pour relier au domaine



La on met le nom de l’utilisateur que l’on veut pour la machine



On redémarre la machine et on rentre le nom de l’utilisateur et son mdp



SCRIPT SUR POWERSHELL

Pour éditer des scripts PowerShell directement dans l'interface de PowerShell, vous pouvez utiliser l'éditeur intégré **ISE** (Integrated Scripting Environment). Voici comment ouvrir l'ISE PowerShell :

1. Ouvrez PowerShell en tant qu'administrateur en cliquant avec le bouton droit sur l'icône de PowerShell et en sélectionnant "Exécuter en tant qu'administrateur" dans le menu contextuel.
2. Une fois PowerShell ouvert, tapez simplement **powershell\_ise** et appuyez sur Entrée.

Cela ouvrira l'éditeur de scripts PowerShell. À partir de là, vous pouvez écrire, éditer et exécuter des scripts PowerShell. L'ISE PowerShell offre des fonctionnalités pratiques telles que la coloration syntaxique, l'auto-complétion et le débogage de scripts.

Si vous préférez utiliser un éditeur de texte externe comme Visual Studio Code pour écrire des scripts PowerShell, vous pouvez le faire également. Il existe également des extensions pour Visual Studio Code qui améliorent la prise en charge de PowerShell, telles que "PowerShell" par Microsoft.