

Documentation
**“Gestion et administration d’Active
Directory”**



Active Directory

Smail Aries, Mithila Haque

Table des matières

I- Définitions

- Hyperviseur
- VMware
- Active Directory
- PingCastle

II- Prérequis

- Logiciels
- Machines virtuelles

III- Installation

1. Création d'utilisateurs et de groupes
2. Attribution de permissions
3. Configuration des stratégies de groupe
4. Gestion des ordinateurs clients
5. Surveillance et maintenance de l'Active Directory
6. Migration des utilisateurs et des groupes
7. Préparer des rapports sur l'état et la santé de l'infrastructure AD

1- Définitions :

Hyperviseur : L'hyperviseur, également connu sous le nom de moniteur de machine virtuelle (VMM), gère ces machines virtuelles qui fonctionnent côte à côte. Il sépare logiquement les machines virtuelles les unes des autres, en attribuant à chacune une part de la puissance de calcul, de la mémoire et du stockage de l'ordinateur.

VMware : VMware est une société informatique américaine fondée en 1998, filiale d'EMC Corporation depuis 2004, qui propose plusieurs produits propriétaires liés à la virtualisation d'architectures x86. C'est aussi par extension le nom d'une gamme de logiciels de virtualisation.

Active directory : Active Directory (AD) est une base de données et un ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour mener à bien leurs missions.

PingCastle : PingCastle est un outil d'audit de sécurité destiné à Active Directory. Il permet d'identifier les vulnérabilités, les mauvaises configurations et d'évaluer la sécurité globale de l'infrastructure Active Directory en fournissant des rapports détaillés et des recommandations.

2- Prérequis :

Logiciels :

- Logiciel de virtualisation (VMware)
- PingCastle

Machines virtuelles :

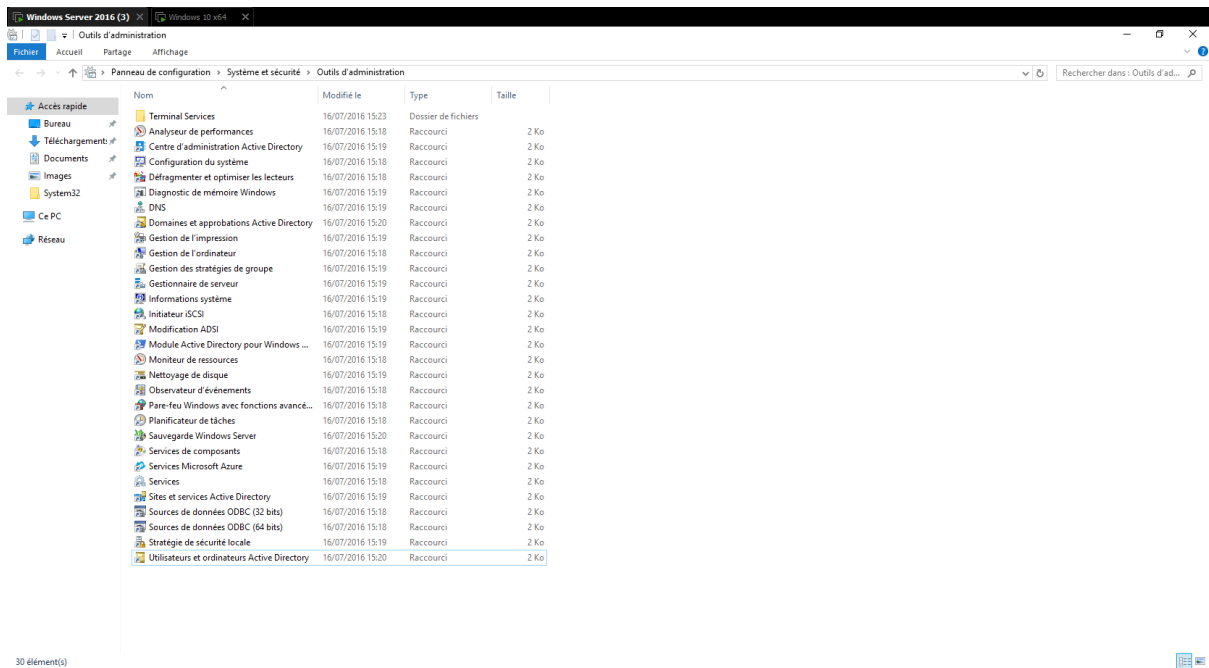
- Windows Server 2016 (pour le contrôleur de domaine)
- Windows 10 (pour le PC client)

3- Installation :

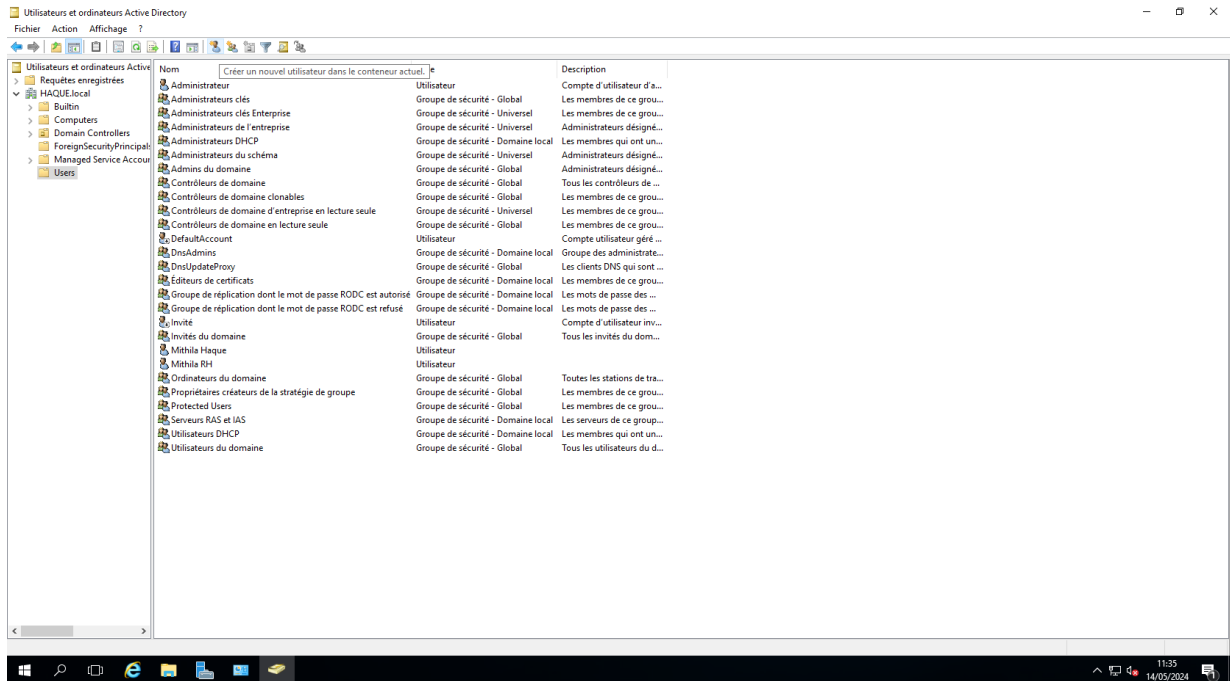
1. CRÉATION D'UTILISATEURS ET DE GROUPES

Création de comptes utilisateurs pour les membres du réseau

1. Sur Windows Server, aller dans Panneau de configuration, puis “Utilisateurs et ordinateurs Active Directory”.



2. Cliquer sur NOMDEFAMILLE.local > Users, puis en haut cliquer sur l'icône "Créer un nouvel utilisateur dans le conteneur actuel”.



3. Saisir les informations du nouvel utilisateur à créer (prénom, nom, nom d'utilisateur et mot de passe), puis cliquer sur "Suivant", et enfin "Terminer".

Nouvel objet - Utilisateur

Créer dans : HAQUE.local/Users

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @HAQUE.local

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

< Précédent **Suivant >** Annuler

Nouvel objet - Utilisateur

Créer dans : HAQUE.local/Users

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

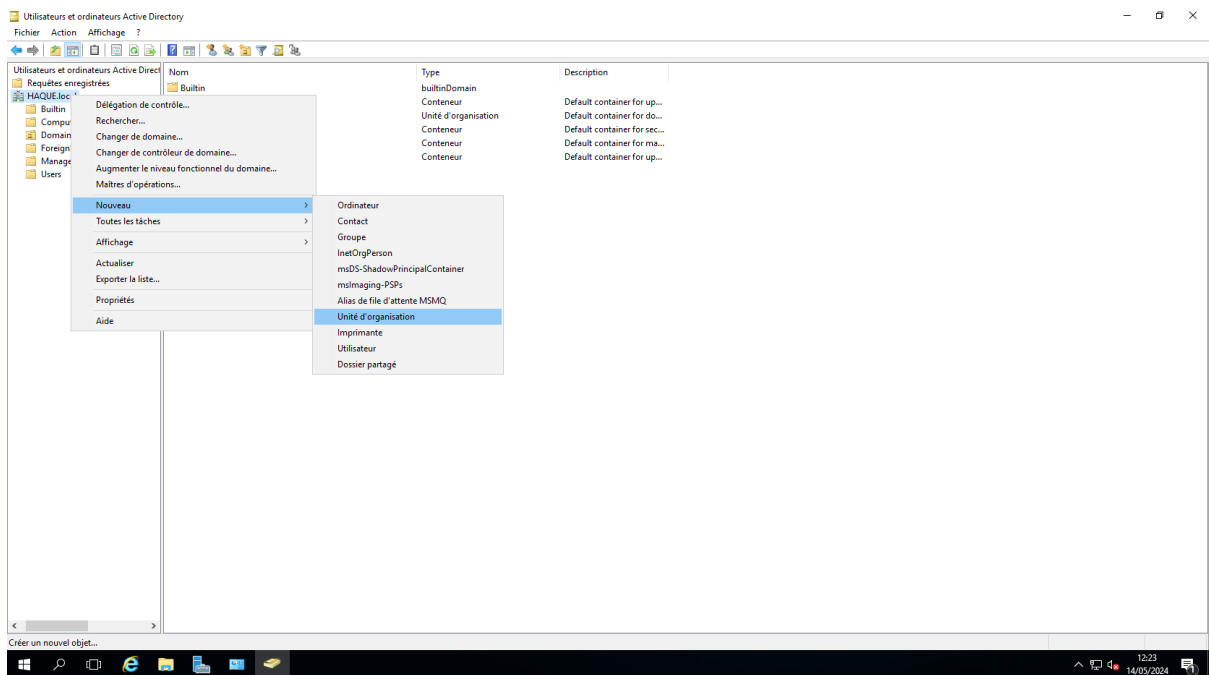
☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé

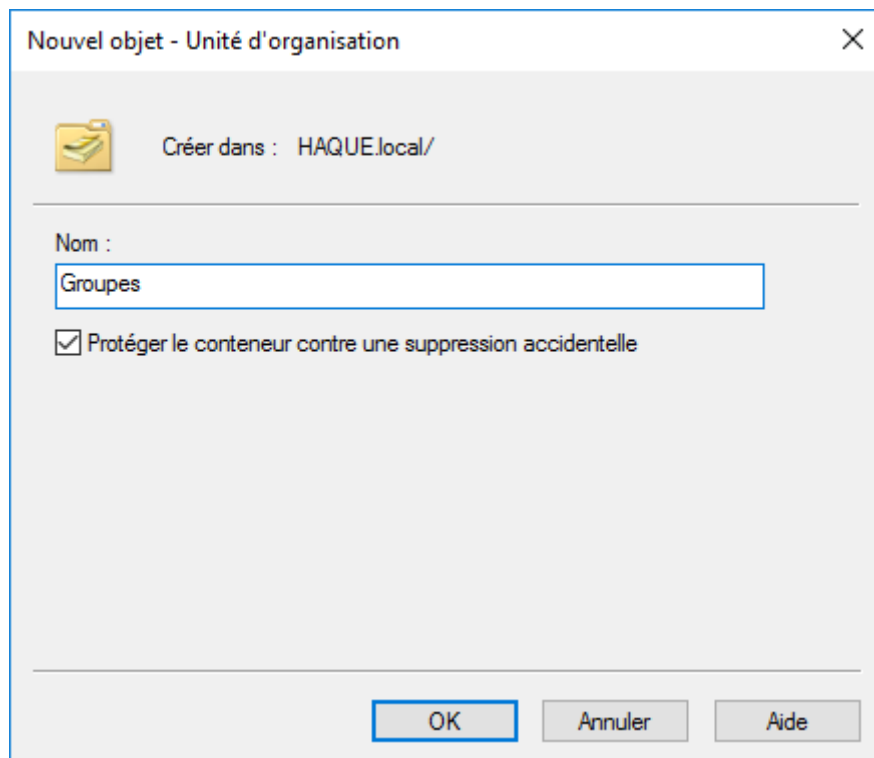
< Précédent Suivant > Annuler

Création de groupes pour organiser les utilisateurs selon leurs rôles ou leurs départements

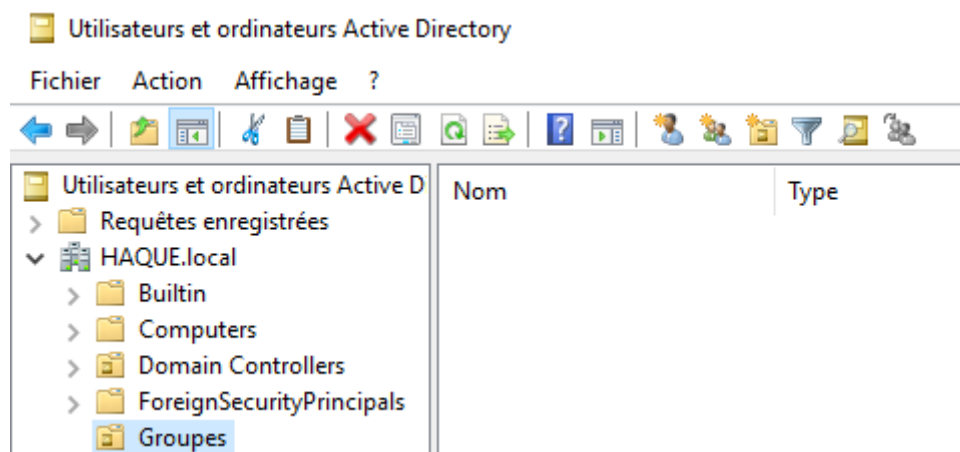
1. Clic-droit sur NOMDEFAMILLE.local, Nouveau > Unité d'Organisation.



2. Saisir le nom de l'UO et cliquer sur OK.




3. Dans le même outil "Utilisateurs et ordinateurs Active Directory", NOMDEFAMILLE.local > Groupes (le dossier que l'on vient de créer), cliquer sur l'icône "Créer un nouveau groupe dans le conteneur actuel".



4. Mettre le nom du groupe, puis choisir l'étendue du groupe ainsi que le type de groupe. OK.

Nouvel objet - Groupe X

 Créer dans : HAQUE.local/Groupes

Nom du groupe :

Nom de groupe (antérieur à Windows 2000) :

Étendue du groupe

☐ Domaine local

☐ Globale

☒ Universelle

Type de groupe


☒ Sécurité

☐ Distribution

Les groupes sont bien créés dans le dossier que nous avons choisi.

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?



	Nom	Type
Utilisateurs et ordinateurs Active Directory		
Requêtes enregistrées		
HAQUE.local		
Builtin		
Computers		
Domain Controllers		
ForeignSecurityPrincipals		
Groupes	Groupe_Commerciaux	Groupe de sécurité - Global
	Groupe_Managers	Groupe de sécurité - Global
	Groupe_RH	Groupe de sécurité - Global
Managed Service Accounts		
Users		

Ajout d'utilisateurs dans les groupes

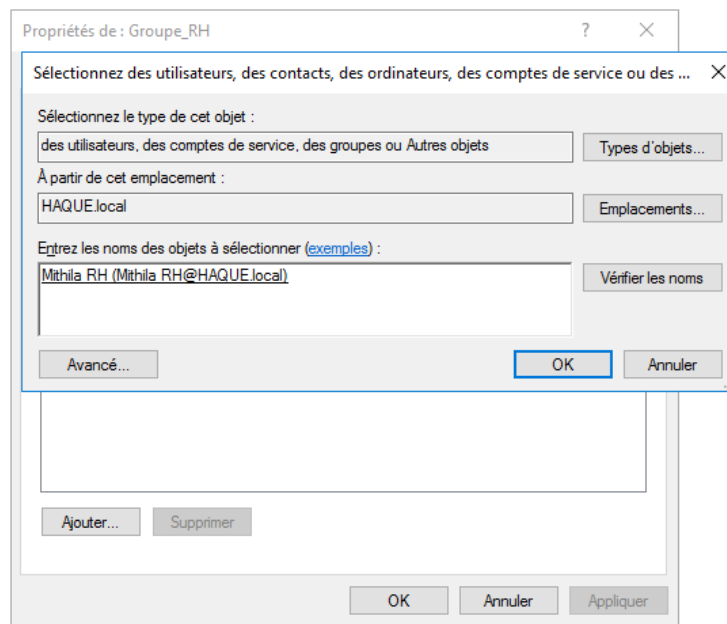
1. Double-cliquer sur votre groupe, puis cliquer sur “Membres”.

The screenshot shows the 'Propriétés de : Groupe_RH' dialog box with the 'Général' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are four tabs: 'Général', 'Membres', 'Membre de', and 'Géré par'. The 'Général' tab is active, showing a group icon and the name 'Groupe_RH'. Below this, there are three text input fields: 'Nom de groupe (antérieur à Windows 2000) :', 'Description :', and 'Adresse de messagerie :'. The first field contains the text 'Groupe_RH'. Below these fields are two sections: 'Étendue du groupe' with three radio buttons ('Domaine local', 'Globale', 'Universelle') and 'Type de groupe' with two radio buttons ('Sécurité', 'Distribution'). The 'Universelle' and 'Sécurité' options are selected. At the bottom is a 'Remarques' text area. The bottom of the dialog has three buttons: 'OK', 'Annuler', and 'Appliquer'.

2. Cliquer sur “Ajouter”.

The screenshot shows the 'Propriétés de : Groupe_RH' dialog box with the 'Membres' tab selected. The dialog has the same title bar and tabs as the previous screenshot. The 'Membres' tab is active, showing a list of members. The list has two columns: 'Nom' and 'Dossier Services de domaine Active Directory'. The first row contains the text 'Dossier Services de domaine Active Directory'. Below the list are two buttons: 'Ajouter...' and 'Supprimer'. The bottom of the dialog has three buttons: 'OK', 'Annuler', and 'Appliquer'.

3. Entrer les noms des utilisateurs à ajouter dans le groupe. Cliquer sur OK, et encore OK.

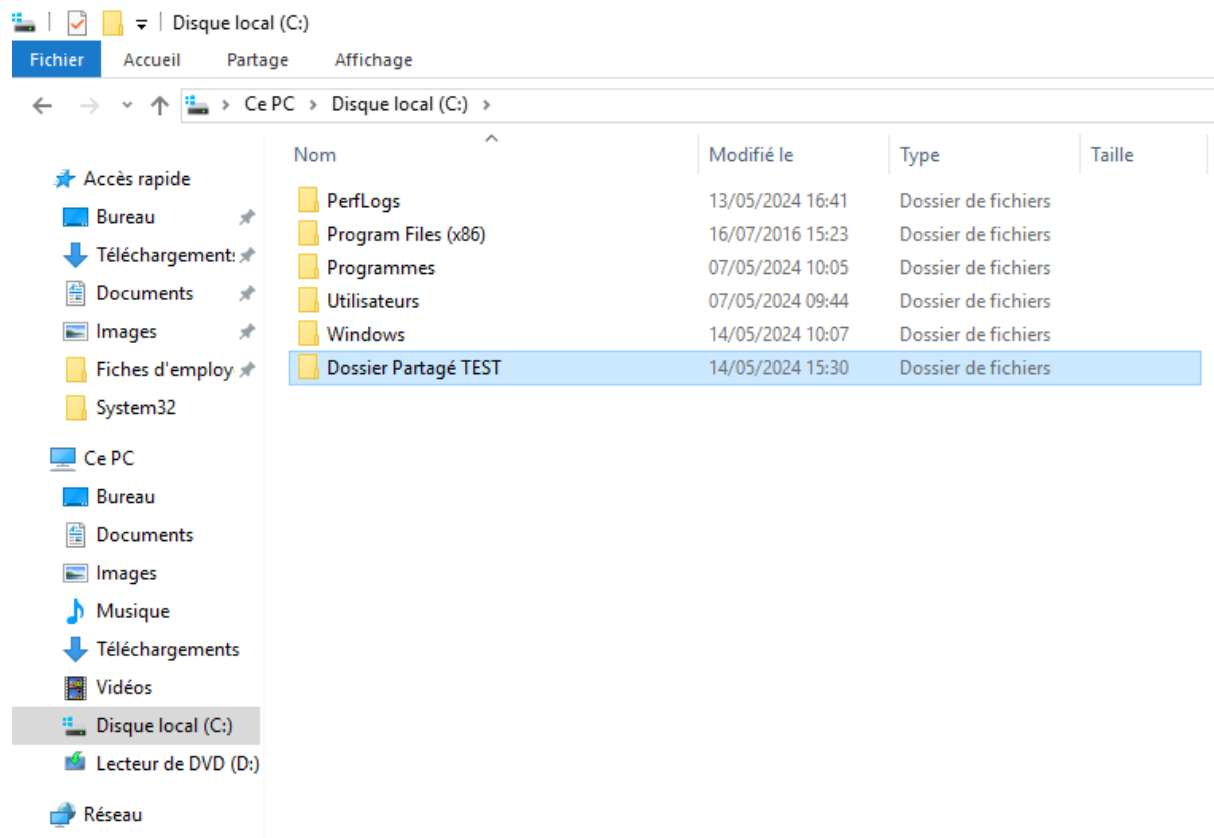


Les utilisateurs sont maintenant bien dans les groupes que vous avez choisis.

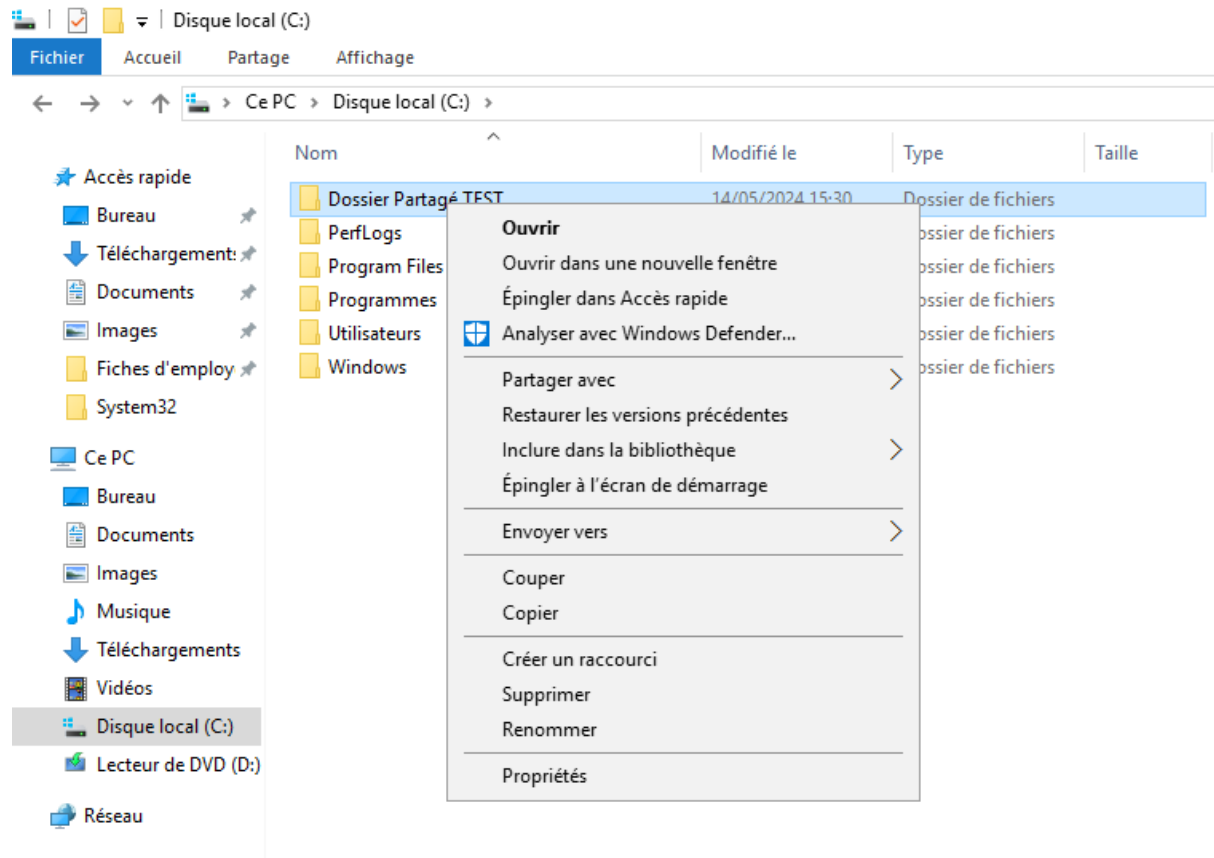
2. ATTRIBUTION DE PERMISSIONS

Accorder des autorisations spécifiques à certains utilisateurs ou groupes sur des ressources partagées telles que des dossiers ou des imprimantes :

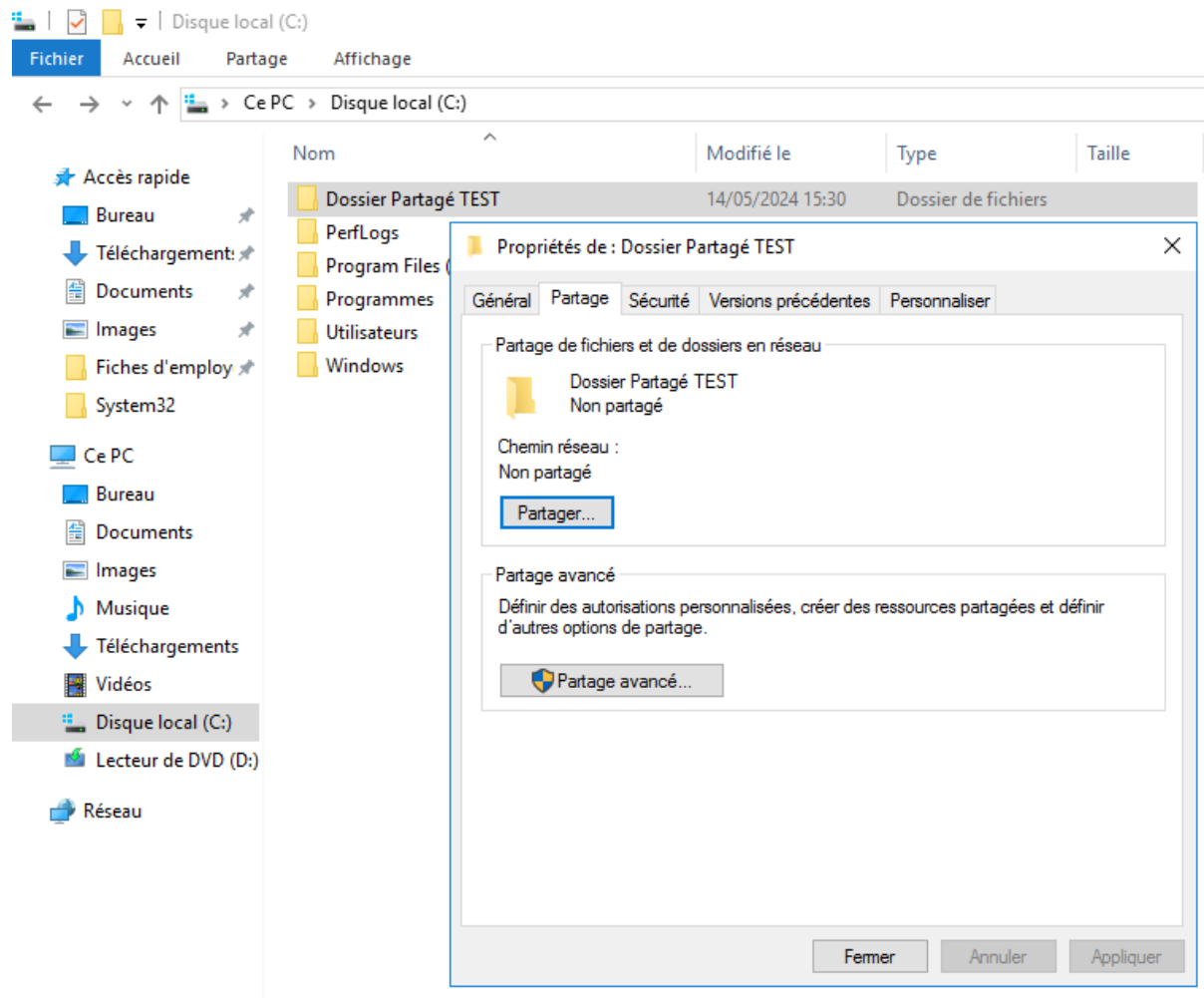
1. Créer un dossier partagé. Ici, nous créons un dossier directement dans le disque local.



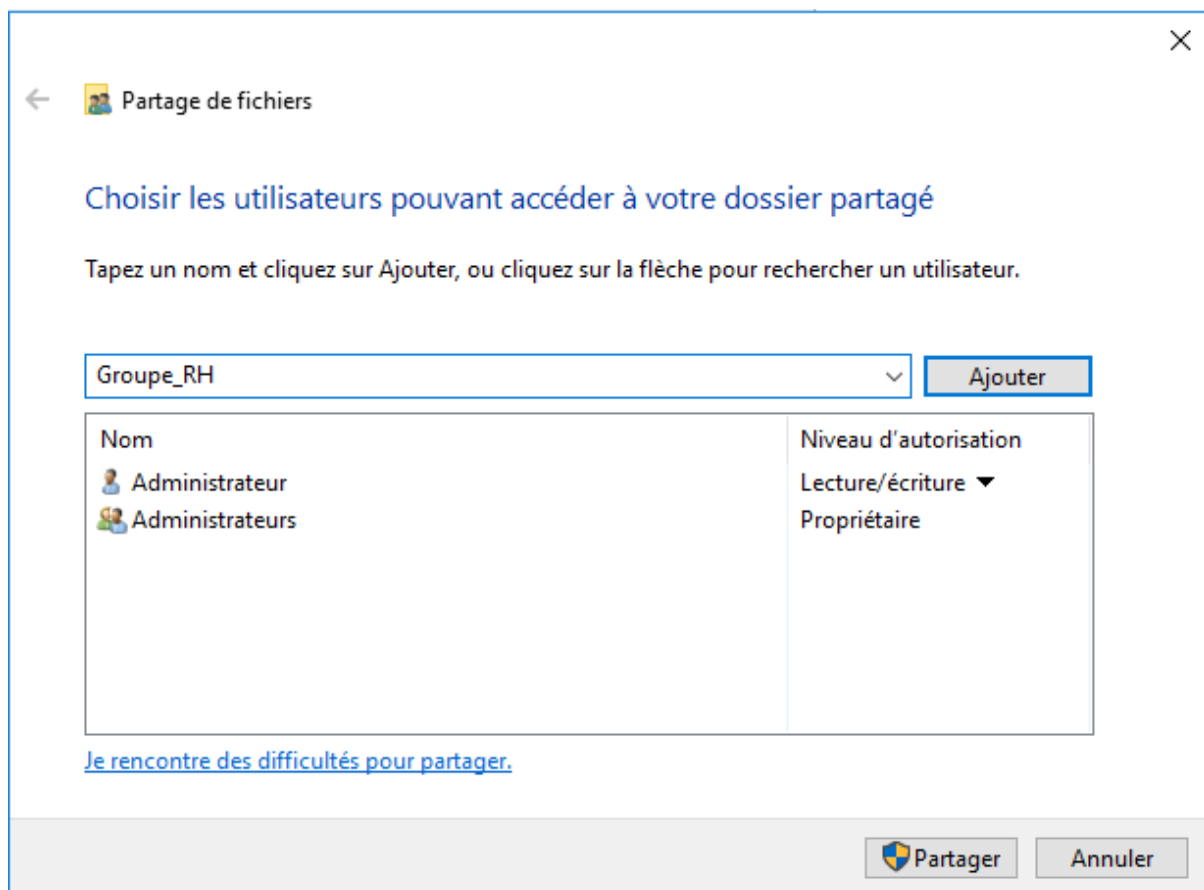
2. Pour partager le dossier, faire un clic-droit sur le dossier et sélectionner “Propriétés”.



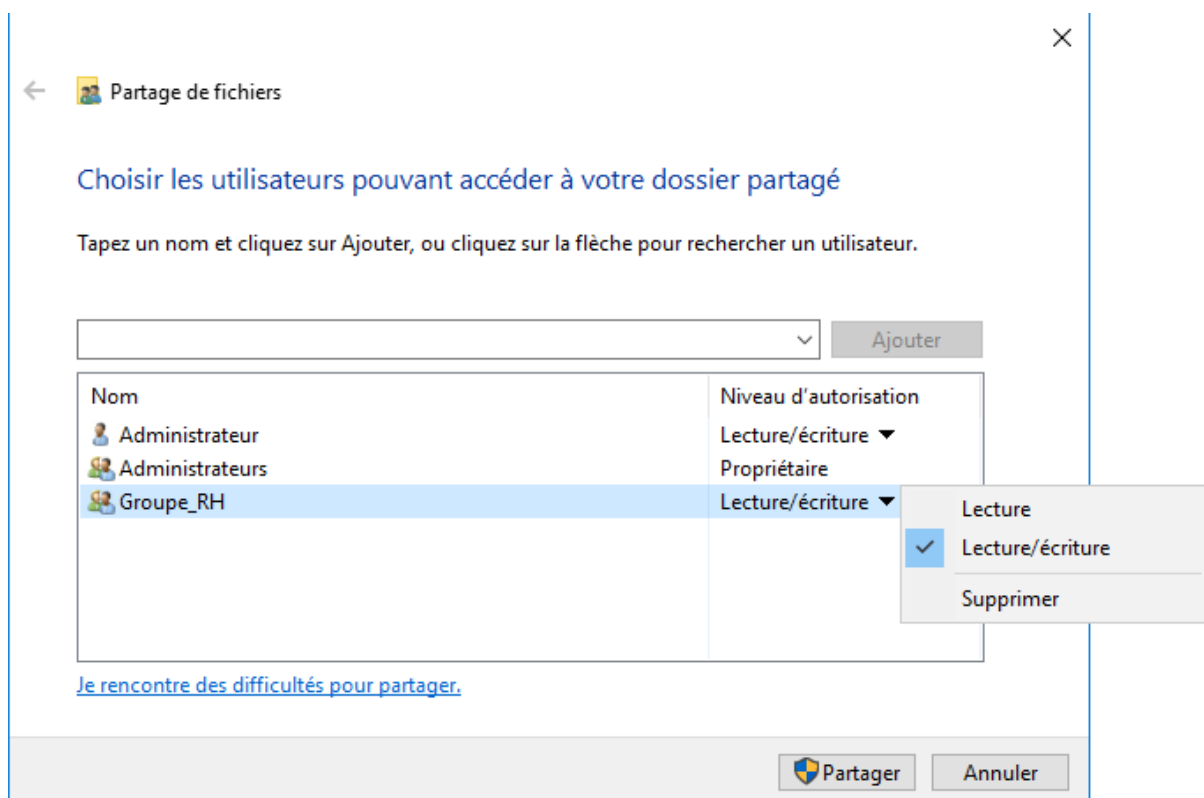
3. Cliquer sur l'onglet "Partage", puis le bouton "Partager..."



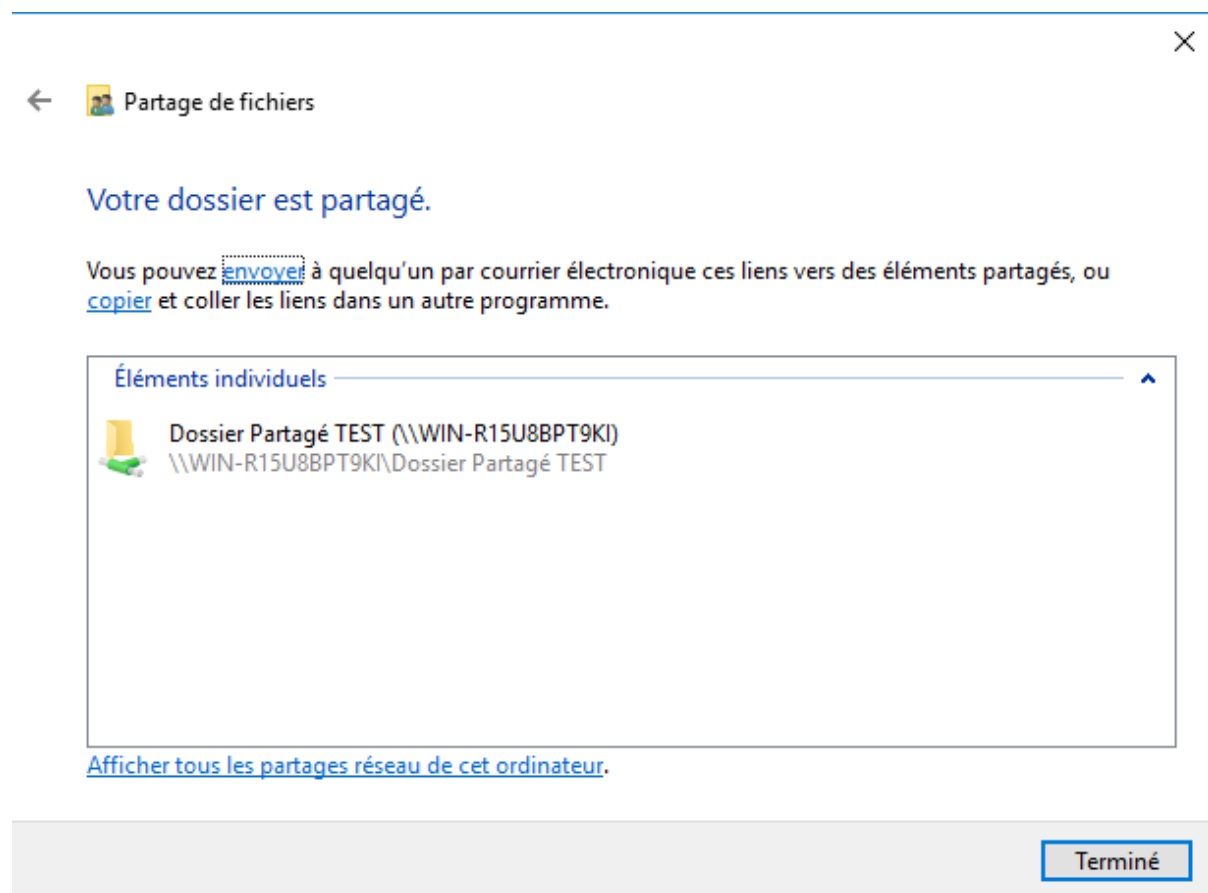
4.



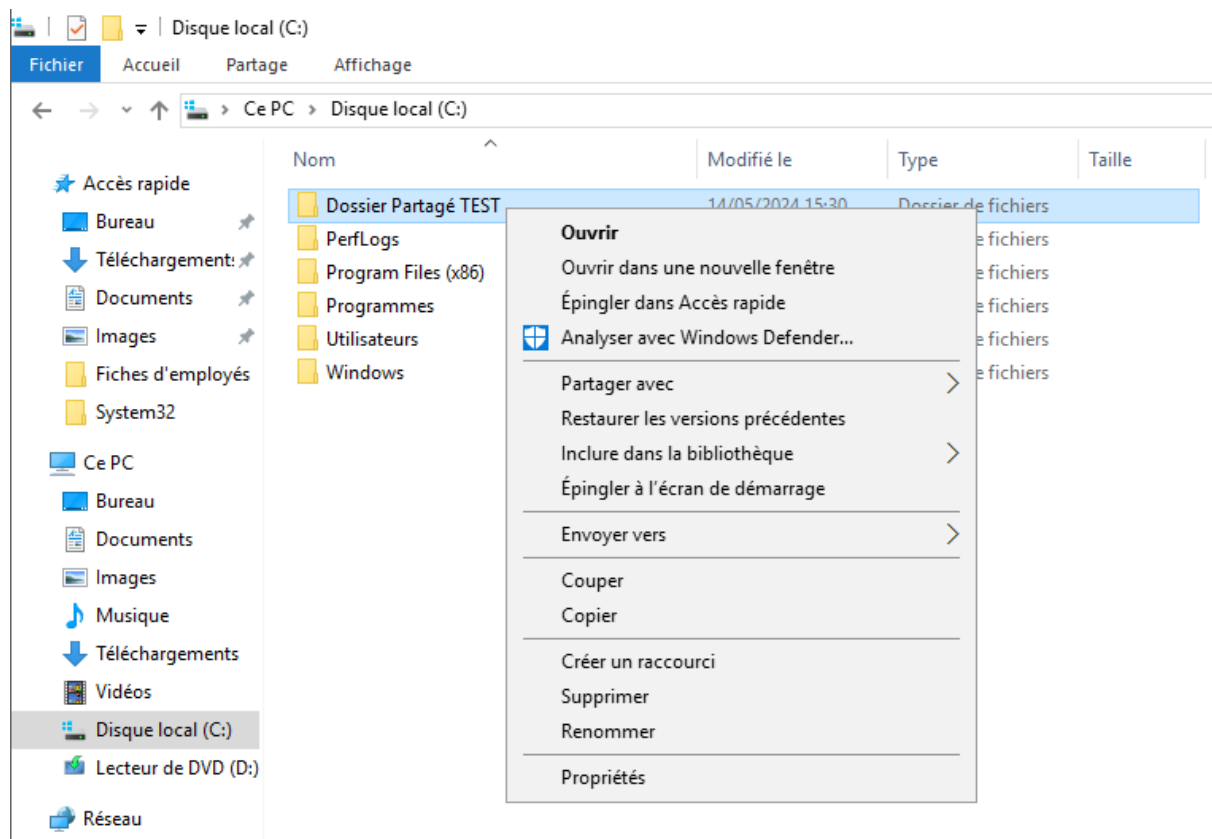
5.



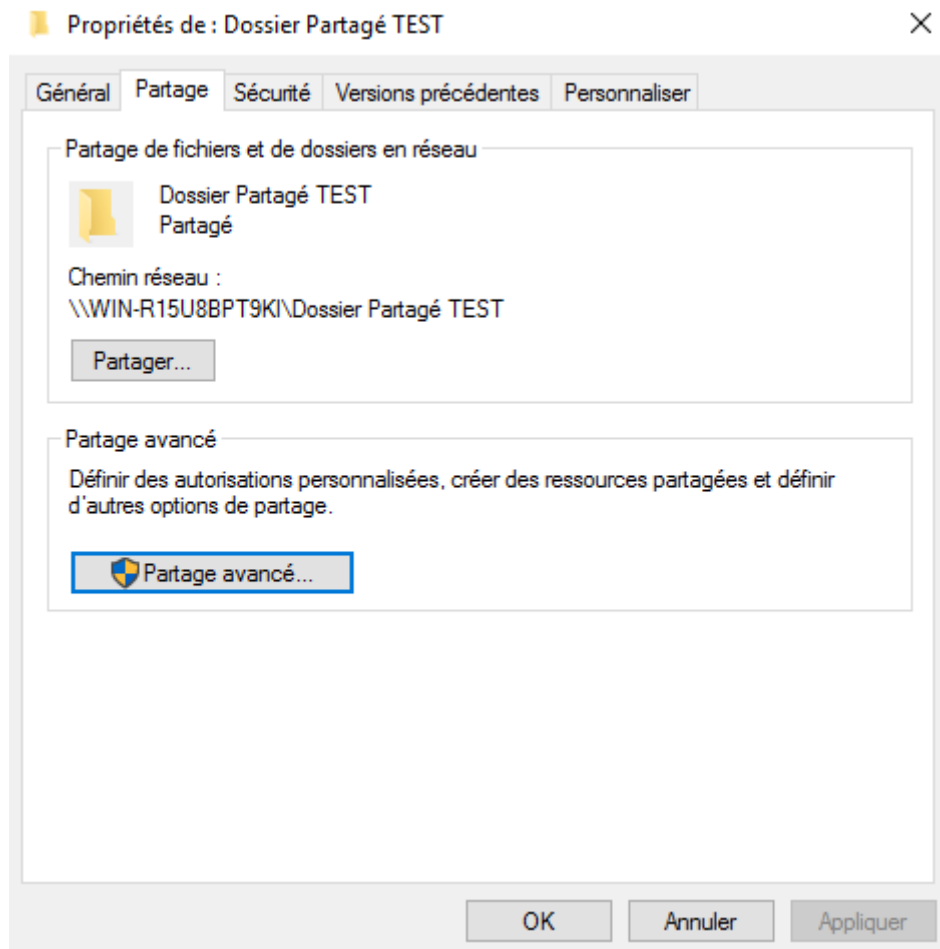
6.



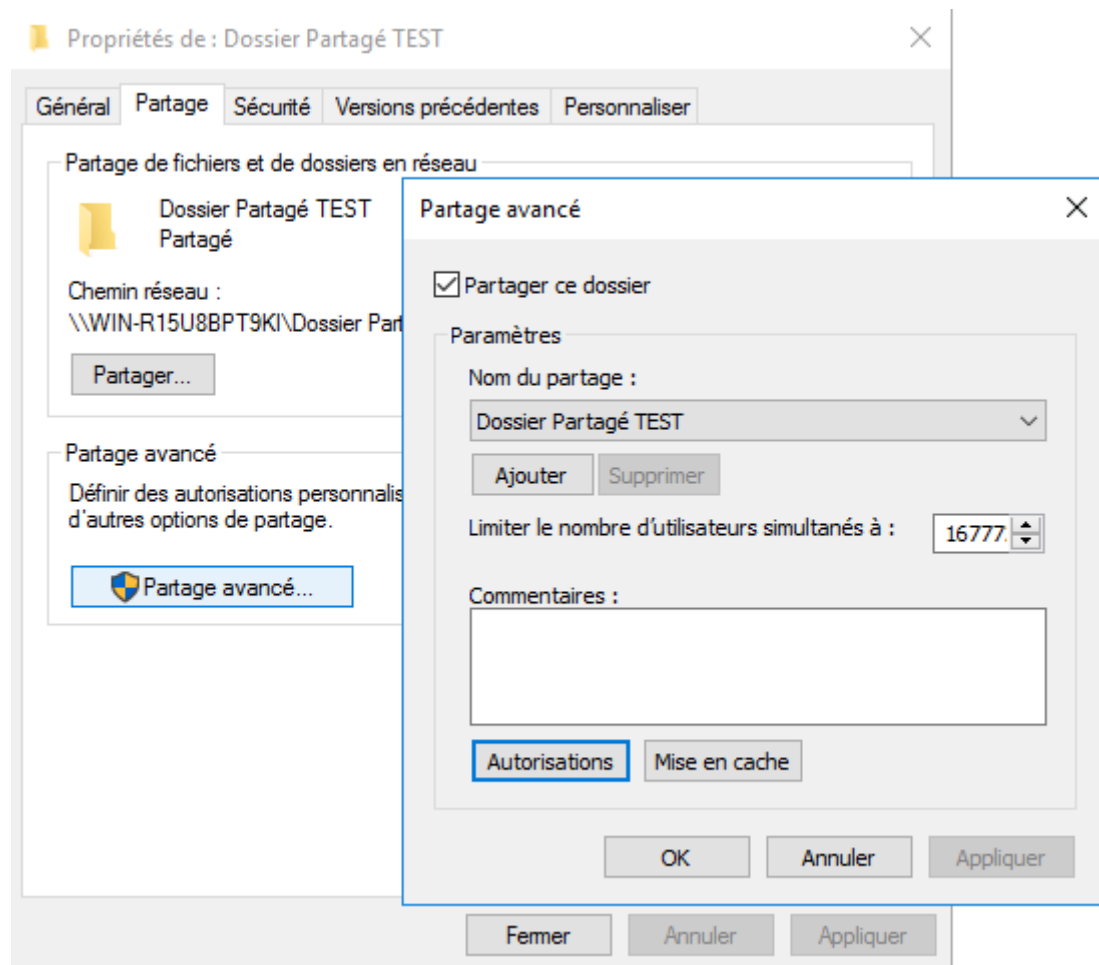
7. Faire un clic-droit sur le dossier à partager, et cliquer sur "Propriétés".



2. Cliquer sur l'onglet "Partage", puis sur le bouton "Partage avancé"

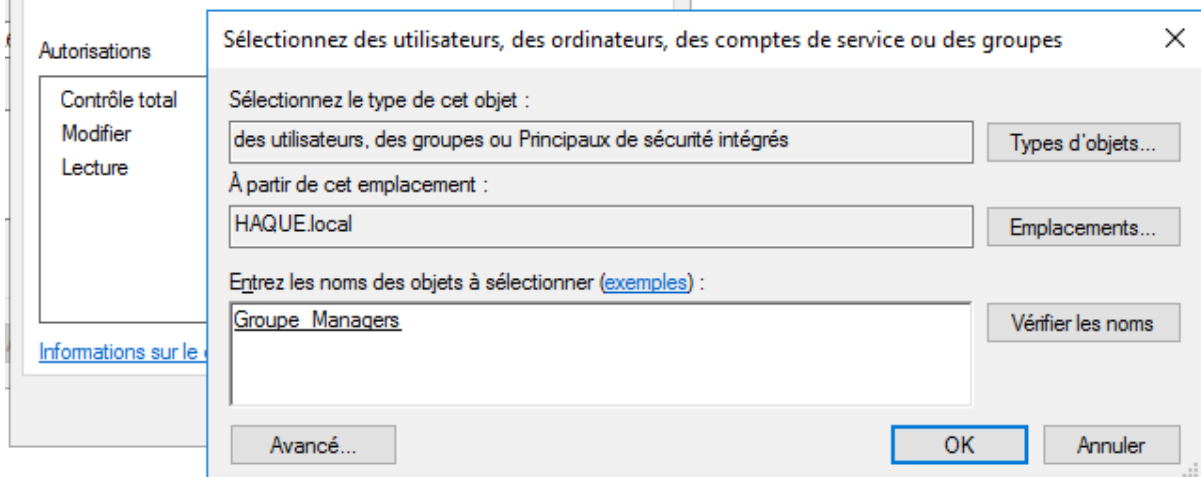
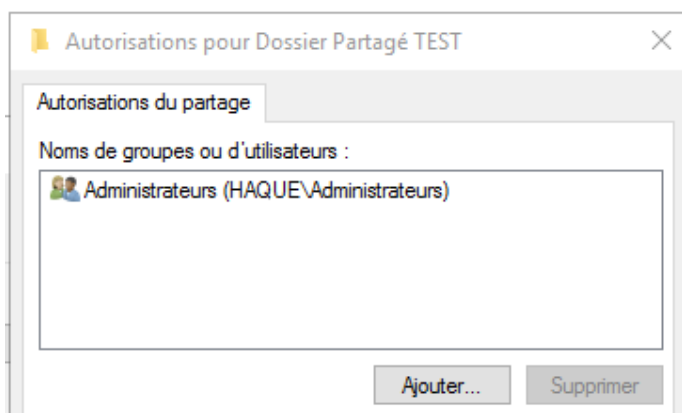
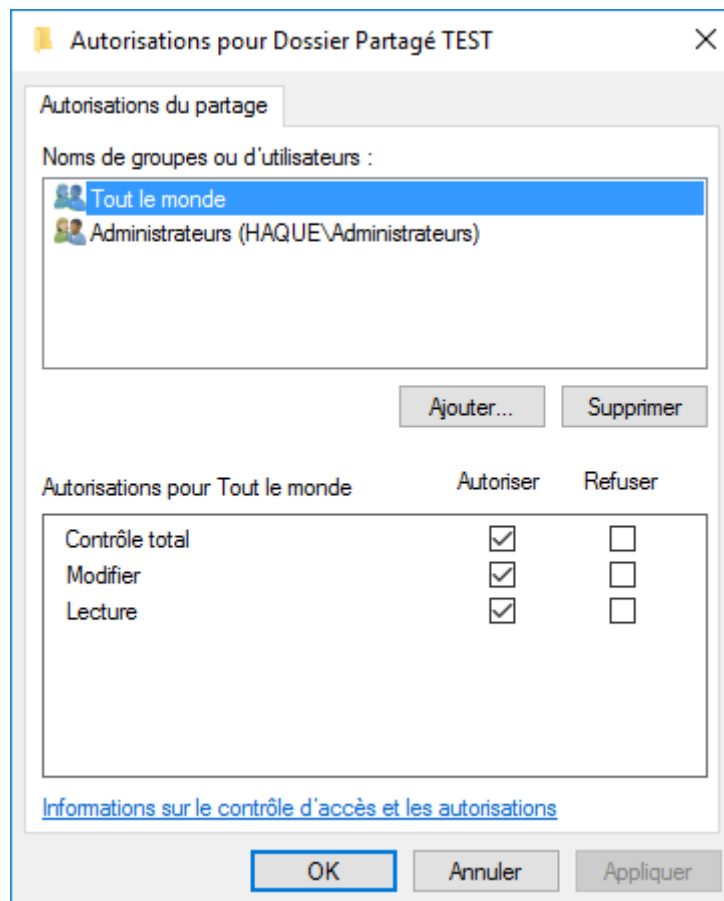


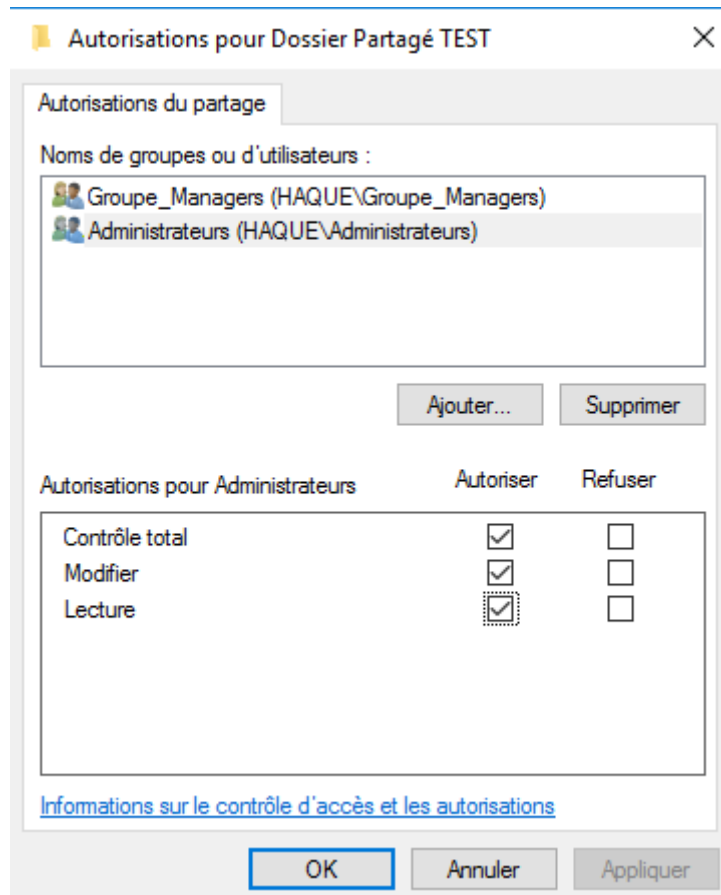
3. Cliquer sur “Autorisations” pour afficher les groupes et utilisateurs ayant des droits, avec le niveau de droits associés.



4. Cliquer sur “Tout le monde”, puis sur “Supprimer” pour supprimer les droits.

Cliquer sur “Ajouter” et choisir le groupe pour lui donner l’autorisation “**Contrôle total**”, “**Lecture**”, ou “**Lecture** et “**Modifier**”.



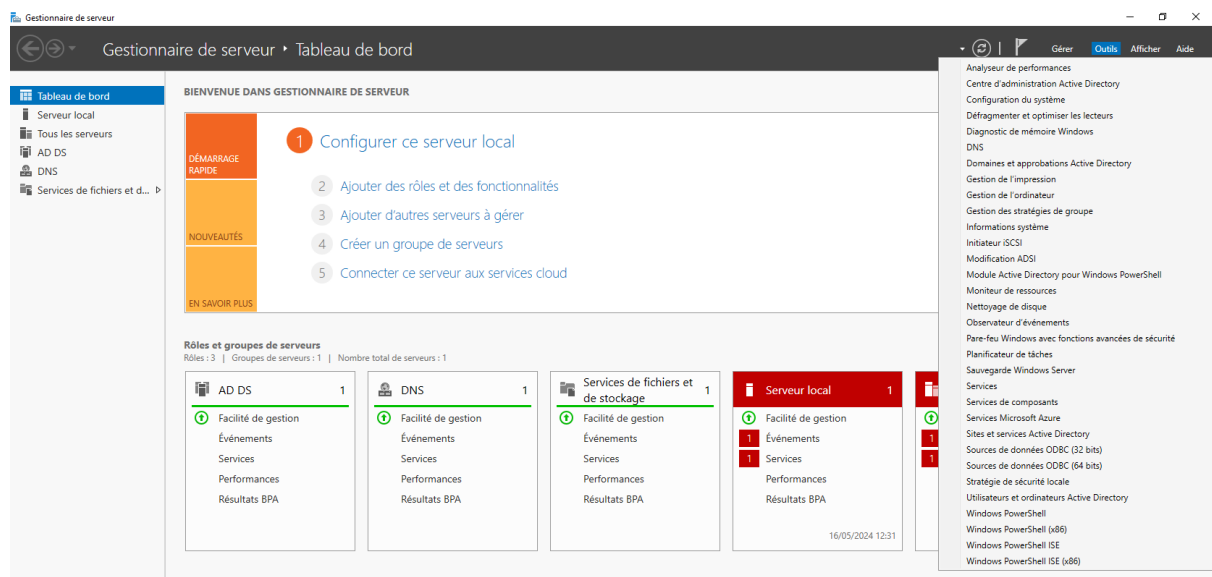


5. Cliquer sur OK, OK. Le dossier devrait maintenant être visible et pouvoir être modifié par le groupe “Groupe_Managers”.

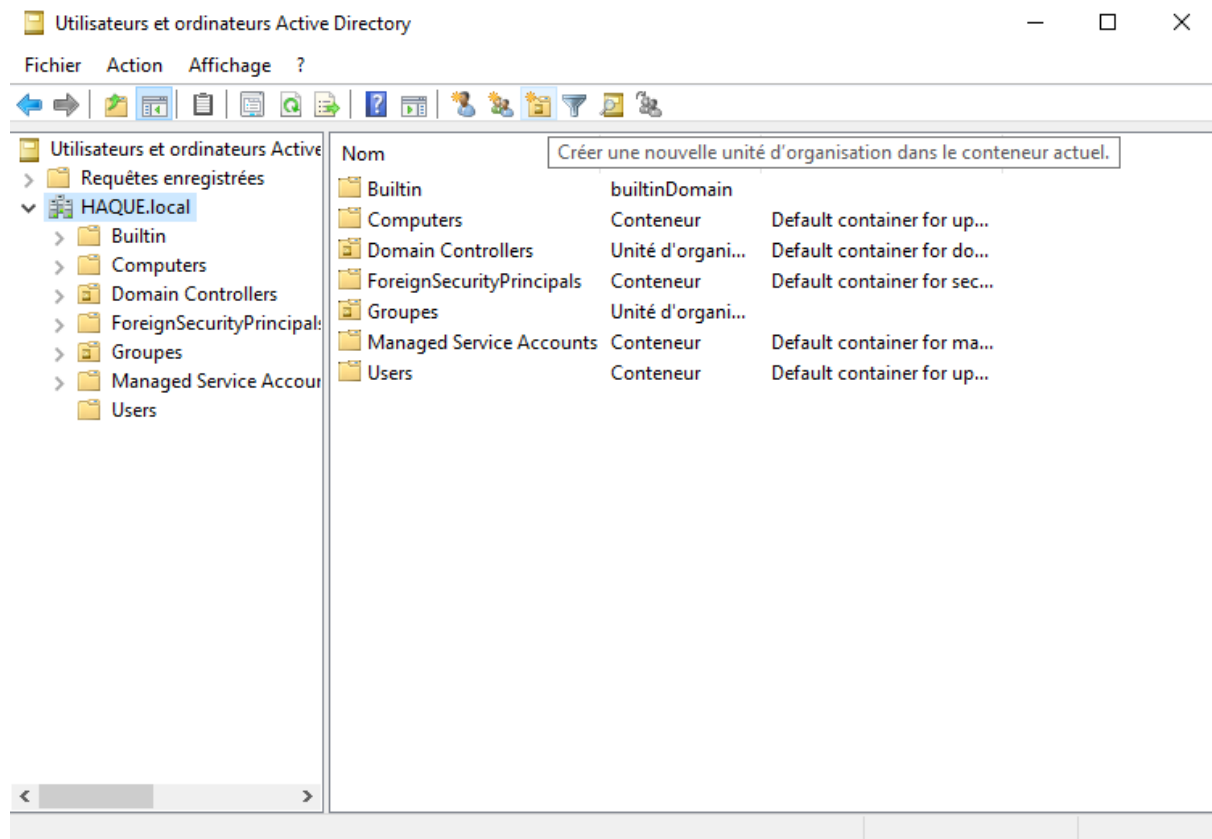
3. CONFIGURATION DES STRATEGIES DE GROUPE (Group Policy Object)

Définir des politiques de sécurité pour restreindre ou permettre certaines actions aux utilisateurs du réseau.

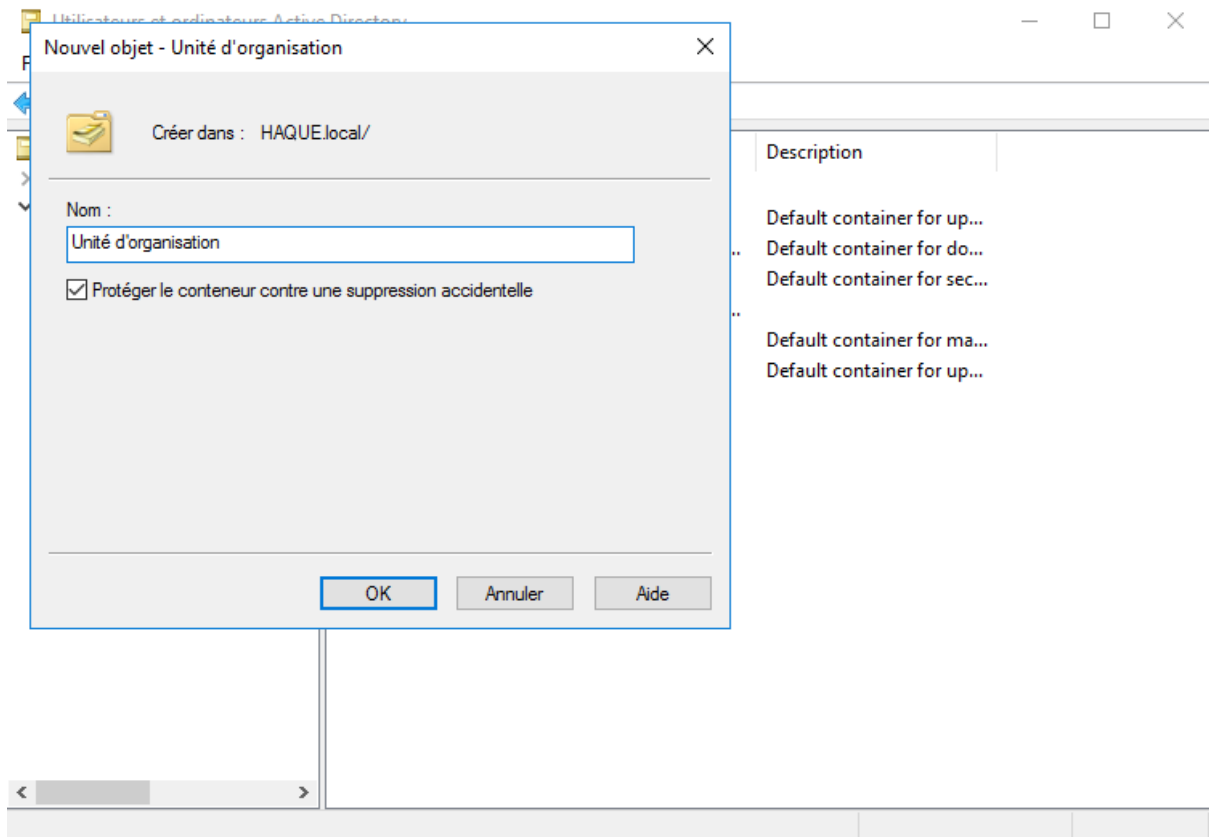
1. Cliquer sur Outils > Utilisateurs et ordinateurs Active Directory.



2. Cliquer sur le domaine (ici “NOMDEFAMILLE.local”), puis cliquer sur le bouton “Créer une nouvelle unité d’organisation dans le conteneur actuel”.

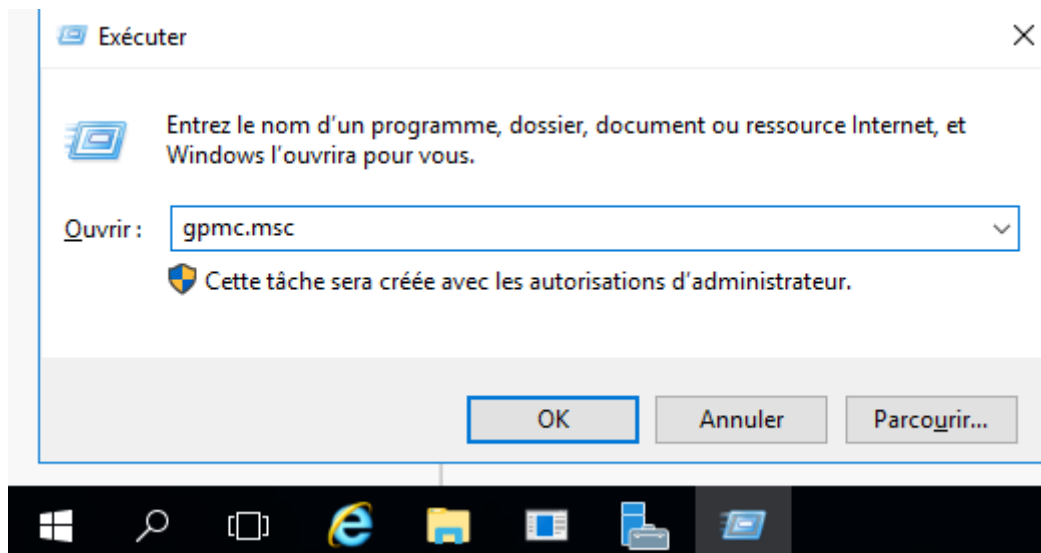


3. Saisir le nom de l’UO.

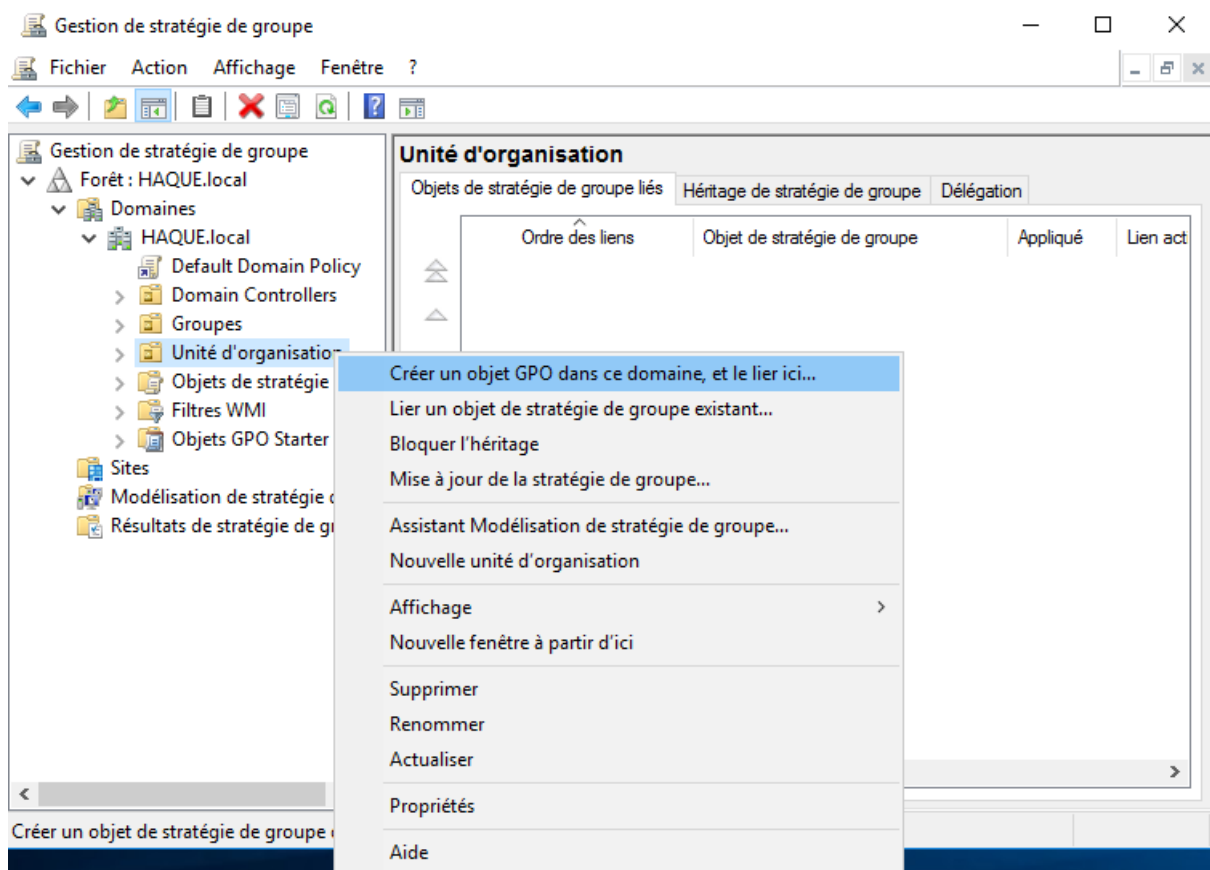


Création GPO (Objet de Stratégie de Groupe) :

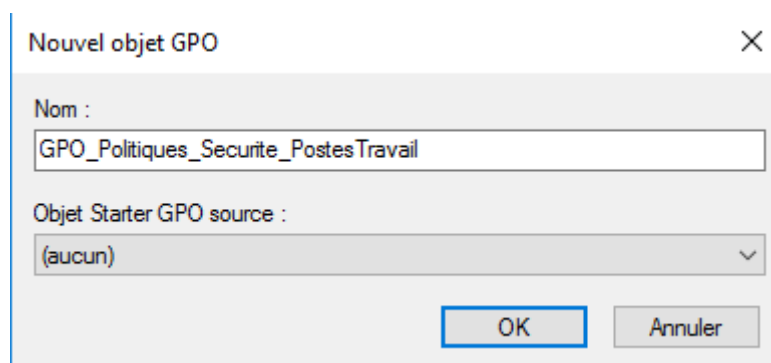
1. Faire Windows + R, puis taper "gpmc.msc", et cliquer sur le bouton OK.



2. Faire un clic-droit sur l'Unité d'Organisation où on veut lier la nouvelle GPO, puis cliquer sur "Créer un objet GPO dans ce domaine, et le lier ici..."



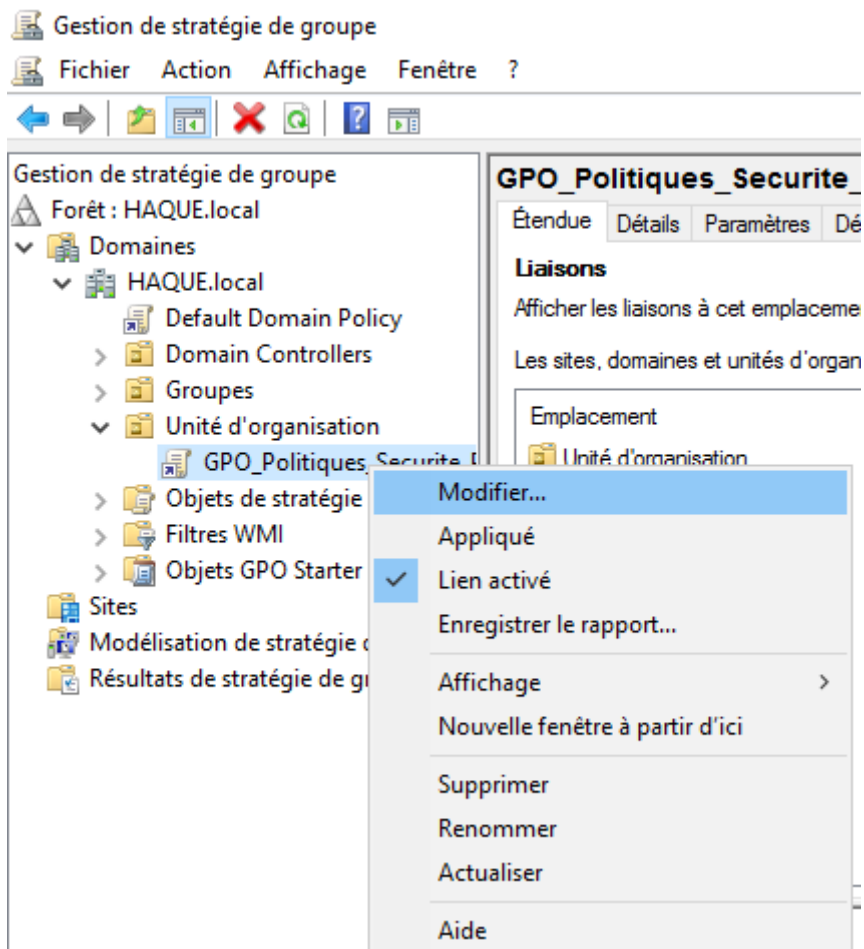
3. Rentrer le nom pour le nouvel objet GPO et cliquer sur OK.



Le nouvel objet GPO a bien été créé.

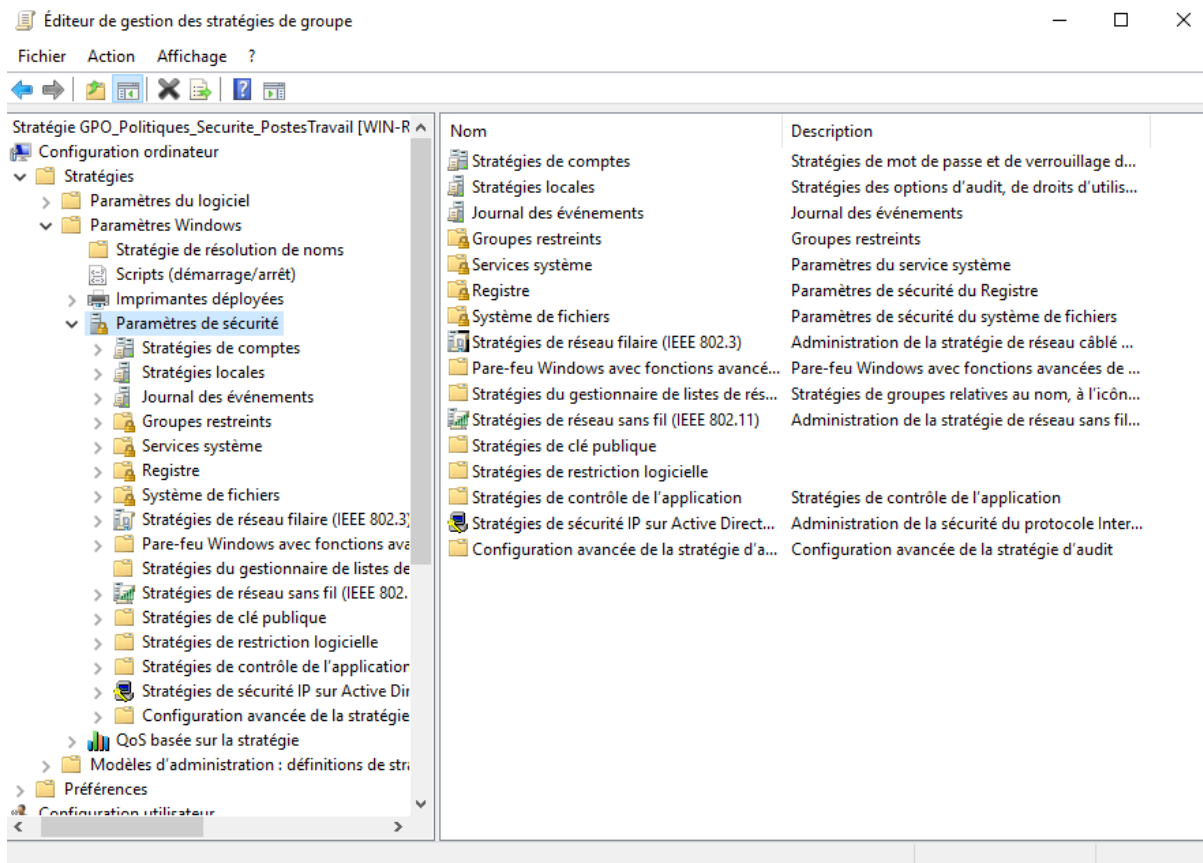
Définir les politiques de sécurité à l'intérieur de la GPO :

1. Faire un clic droit sur la GPO qui vient d'être créée, cliquer sur Modifier. Maintenant vous pouvez configurer les politiques de sécurité.



2. Dans l'éditeur de GPO, cliquer sur :

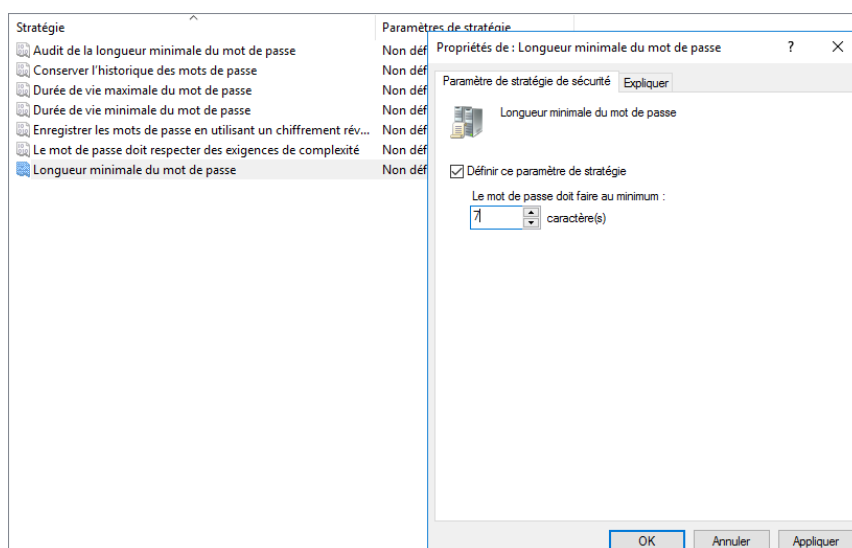
Configuration de l'ordinateur / Configuration utilisateur > Stratégies > Paramètres Windows
> Paramètres de Sécurité.

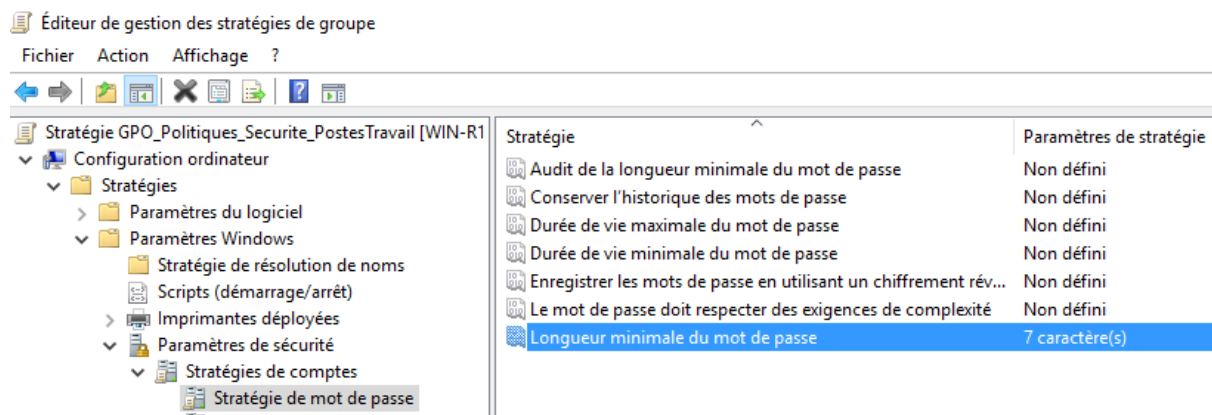


Vous pouvez ici configurer différentes politiques pour renforcer la sécurité de votre environnement informatique.

3. Aller dans Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégie de comptes > Stratégie de mot de passe.

Vous pouvez donc modifier les caractéristiques des mots de passe, telles que le nombre minimum de caractères par exemple.



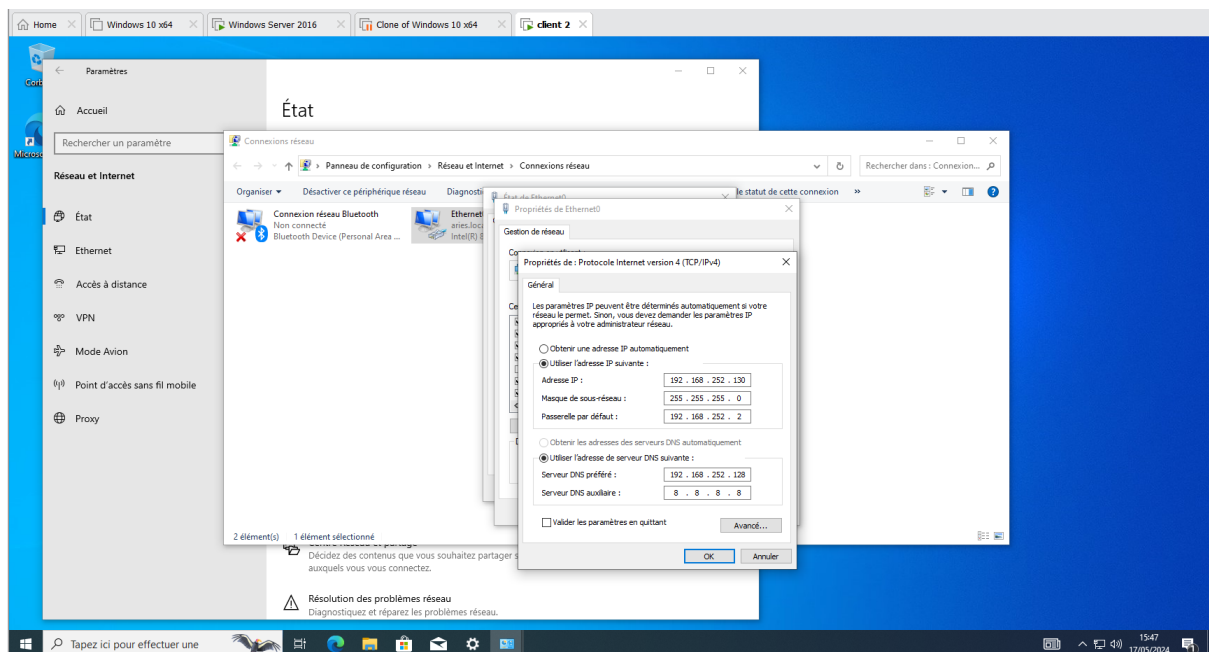


Vous savez maintenant comment configurer les stratégies de groupe.

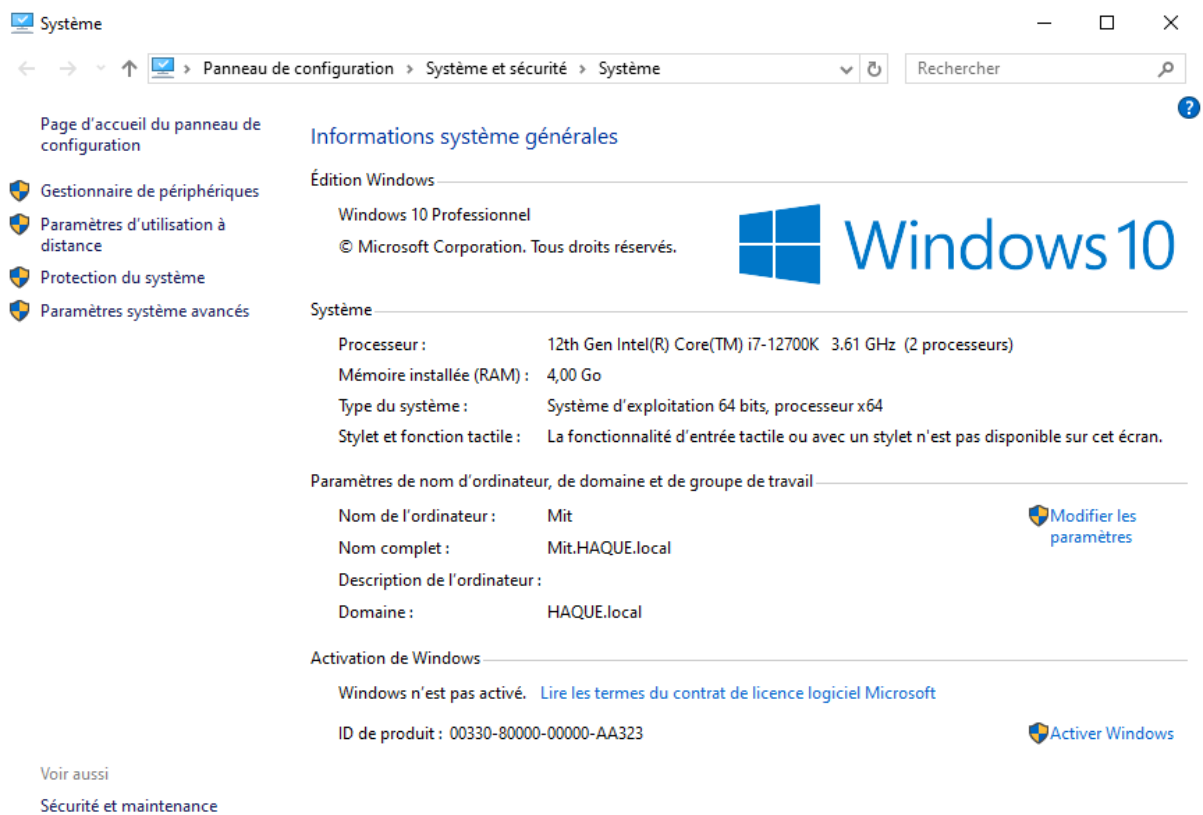
4. GESTION DES ORDINATEURS CLIENTS

Ajouter des ordinateurs au domaine :

1. Après avoir créé votre nouvelle machine, la joindre au domaine Active Directory en remplaçant l'adresse IP automatique par une adresse IP statique qui correspond à l'adresse IP du serveur.

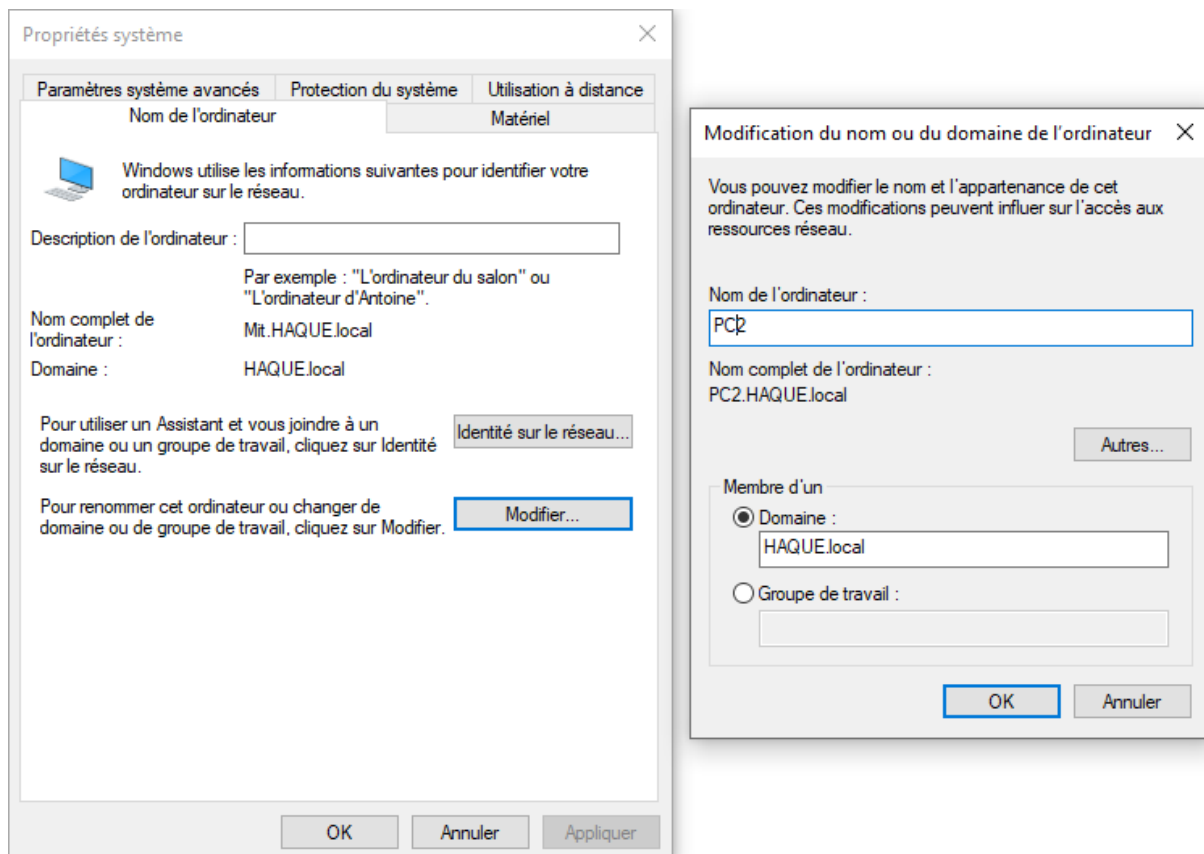


2. Accéder aux paramètres système : Ce PC > Propriétés > Paramètres système avancés.

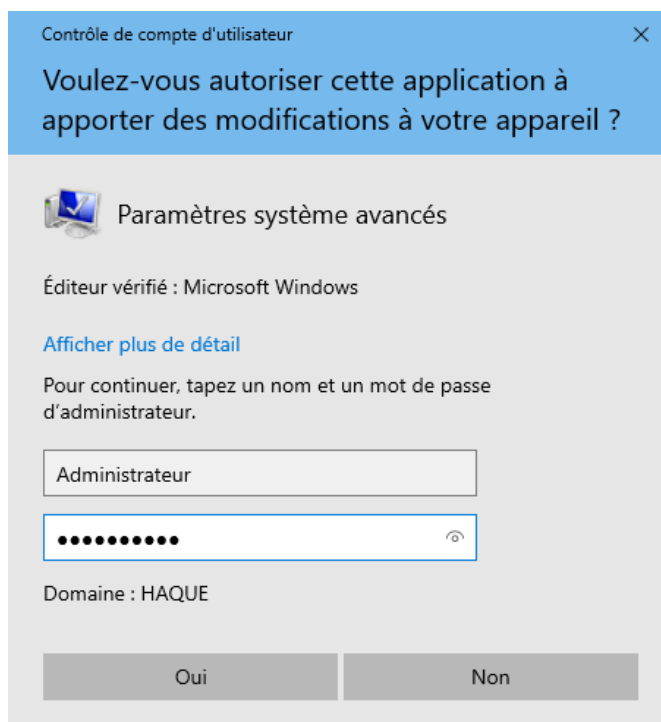


3. Dans l'onglet "Nom de l'ordinateur", cliquer sur "Modifier" puis sur "Domaine".

Saisir le nom du domaine AD auquel vous voulez joindre l'ordinateur, puis cliquer sur "OK".



4. Pour y avoir accès, mettre le nom d'utilisateur de l'Administrateur et le mot de passe.



5. Redémarrer l'ordinateur pour appliquer l'ajout de domaine.

Vous devez redémarrer votre ordinateur pour appliquer ces modifications

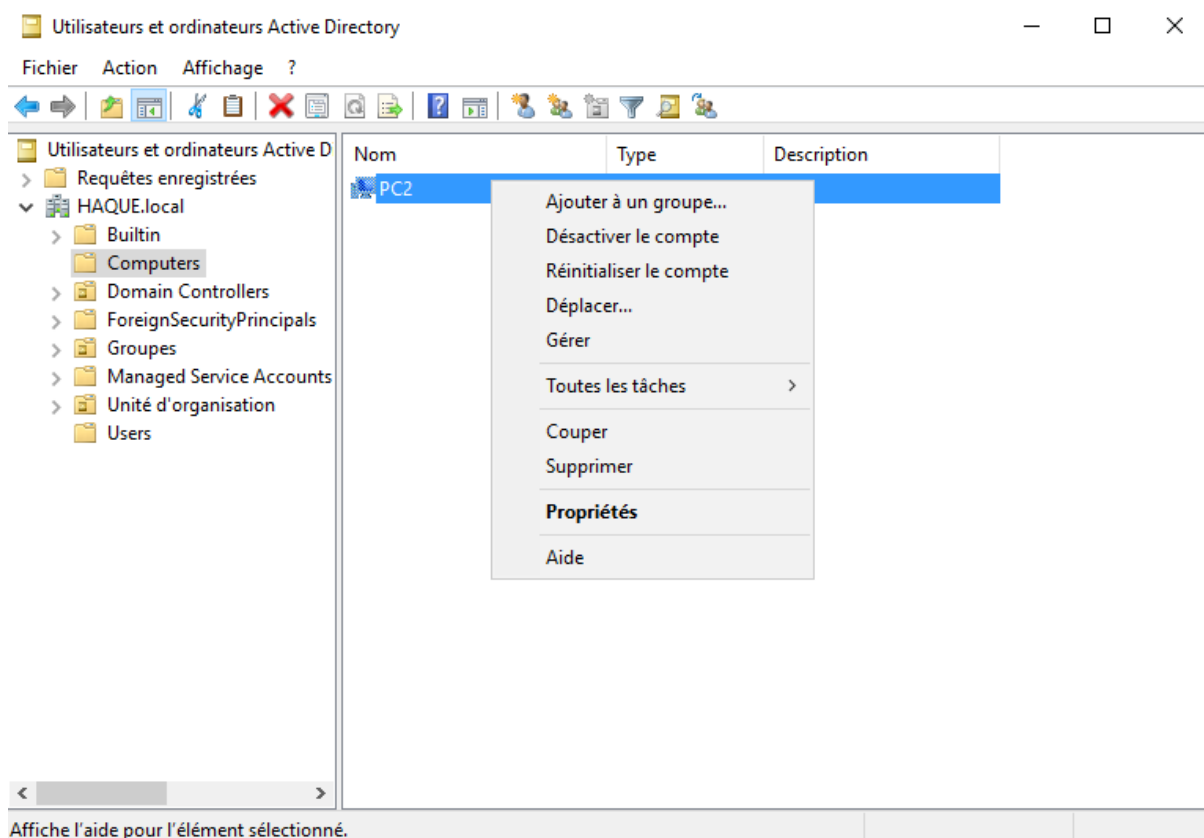
Avant de redémarrer, enregistrez les fichiers ouverts et fermez tous les programmes.

Redémarrer maintenant

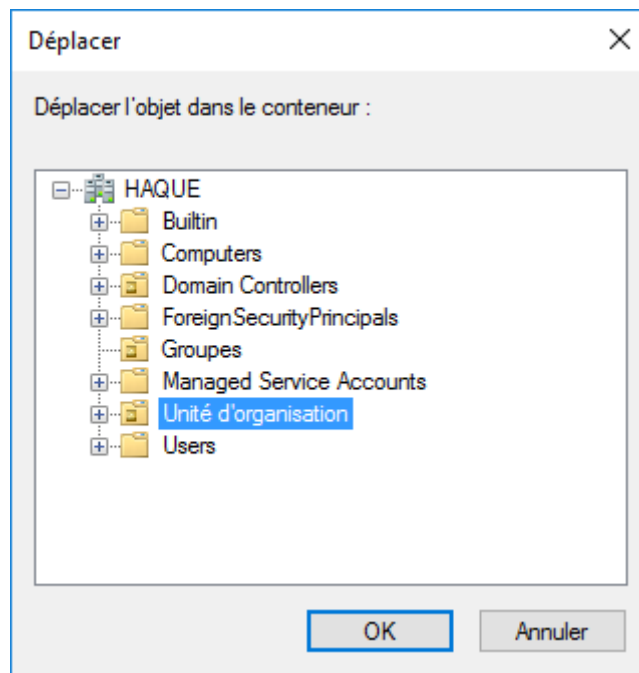
Redémarrer ultérieurement

Appliquer des paramètres de configuration spécifiques à ces ordinateurs à l'aide des objets de stratégie de groupe (GPO) :

1. Sur Windows Server, aller dans "Utilisateurs et ordinateurs AD", cliquer sur "Computers", faire clic-droit sur le nouvel ordinateur, et cliquer sur "Déplacer..." .



2. Choisir l'unité d'organisation dans laquelle vous désirez déplacer votre ordinateur, et cliquer sur "OK".

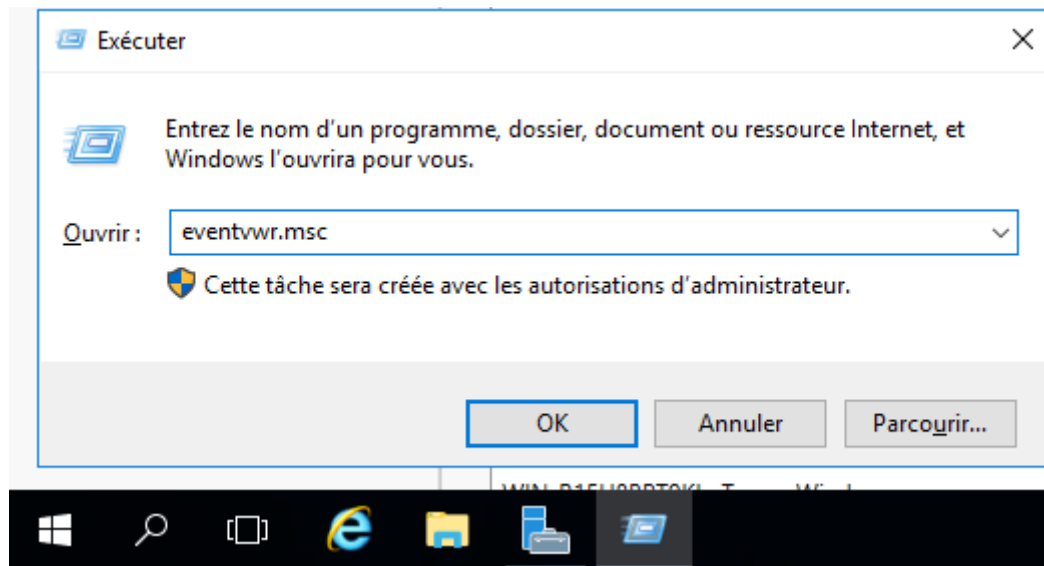


L'ordinateur a bien été déplacé vers l'UO choisie.

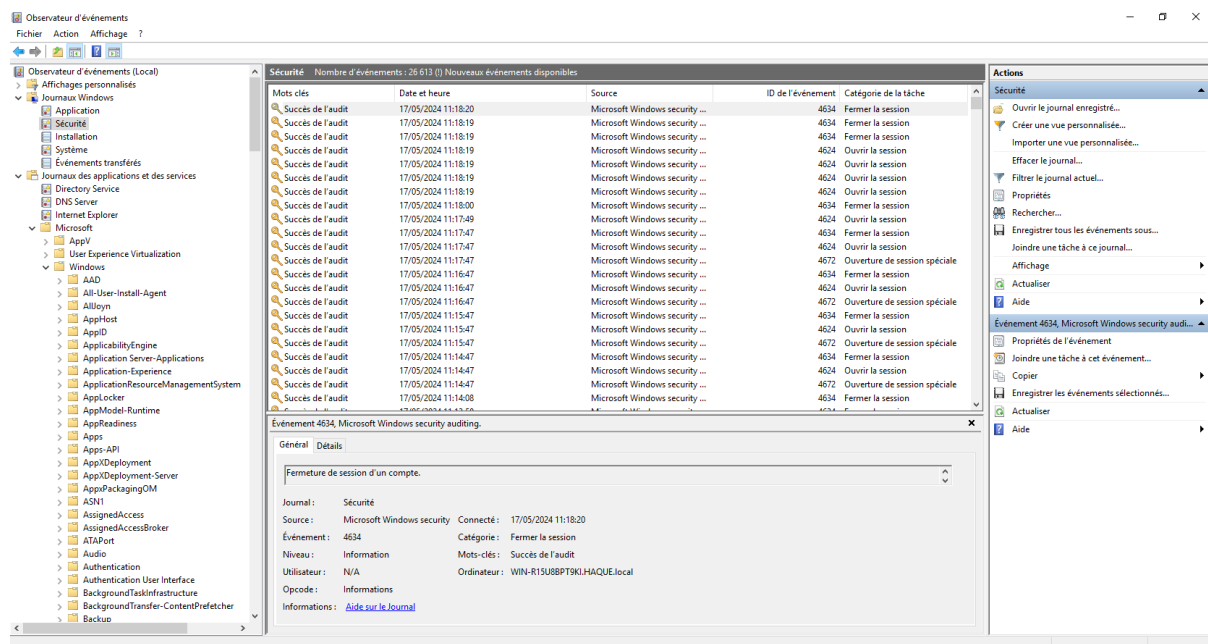
5. SURVEILLANCE ET MAINTENANCE DE L'ACTIVE DIRECTORY

Vérifier les journaux d'événements pour identifier les problèmes potentiels ou les activités suspectes.

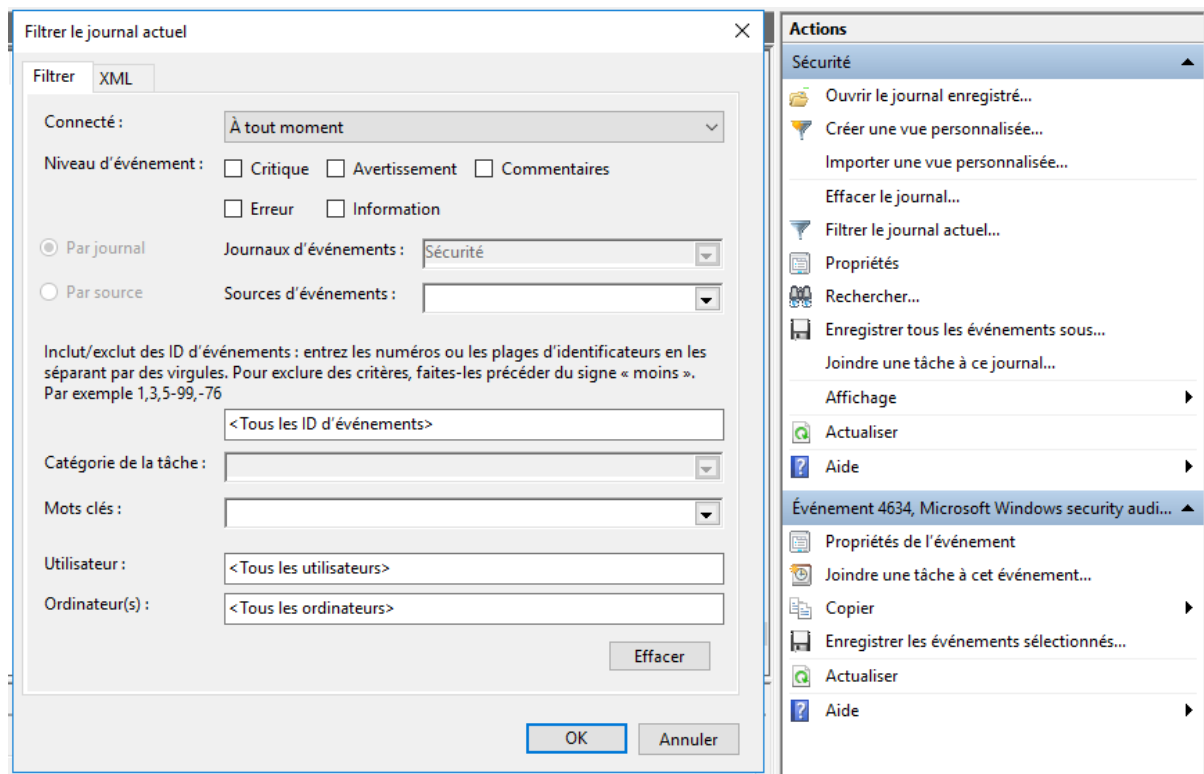
1. Faire Windows + R, écrire "eventvwr.msc" et appuyer sur Entrée.



2. Dans l'Observateur d'événements, cliquer sur "Journaux Windows", puis vous pouvez choisir "Sécurité" pour afficher les tentatives de connexion échouées, des modifications de politique de sécurité, ou des activités suspectes, ou bien choisir "Système" pour afficher les problèmes de matériel, de service système, ou de contrôleurs de domaine.



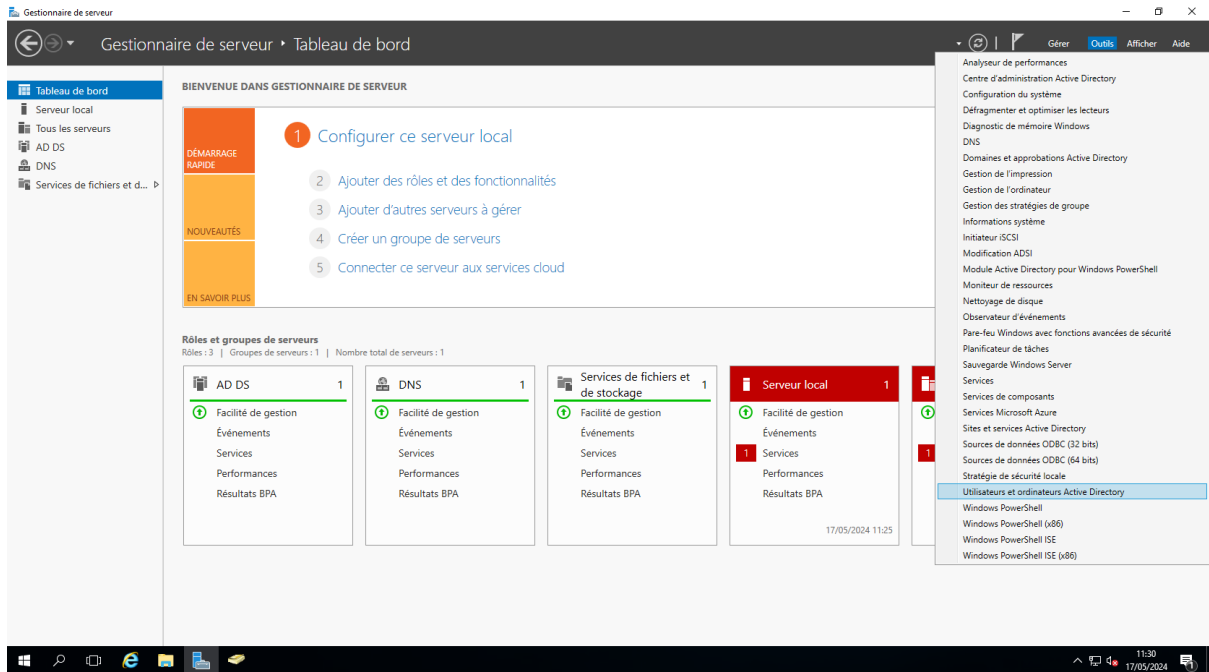
3. Cliquer à droite sur "Filtrer le journal actuel..." pour filtrer les événements par lesquels vous êtes intéressé.



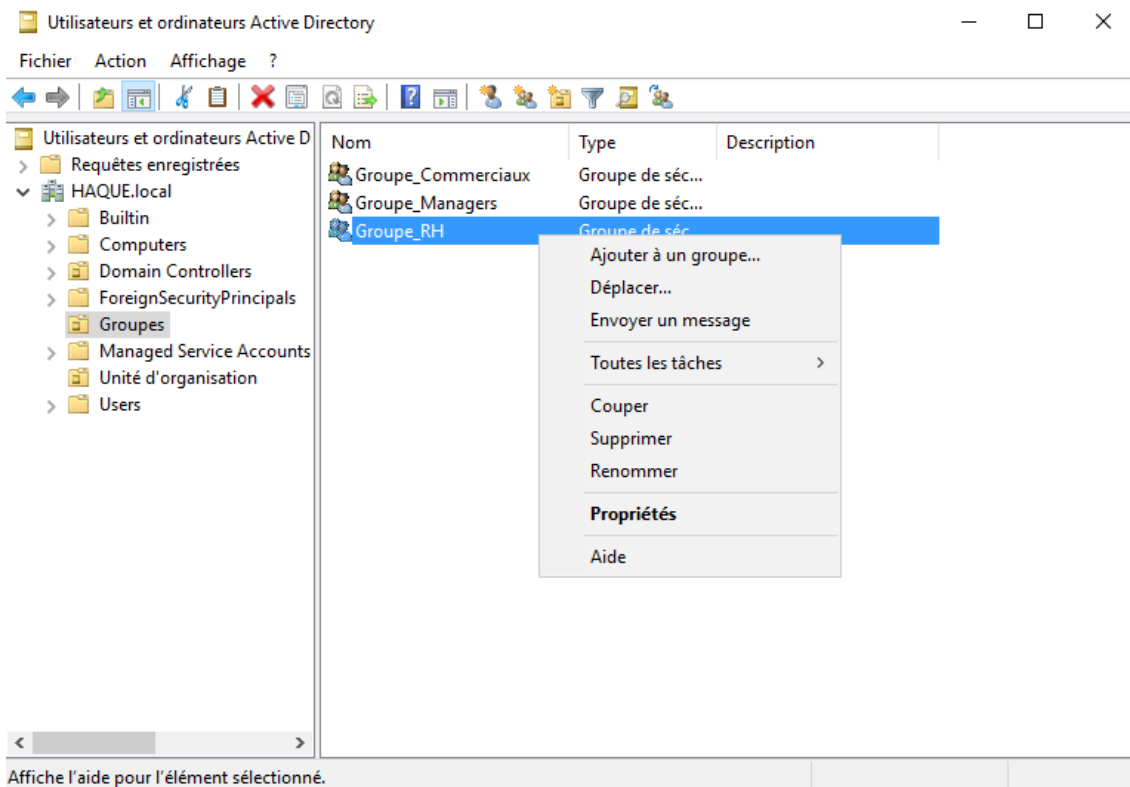
6. MIGRATION DES UTILISATEURS ET DES GROUPES

Déplacer des utilisateurs et des groupes entre différentes unités organisationnelles (OU) ou domaines.

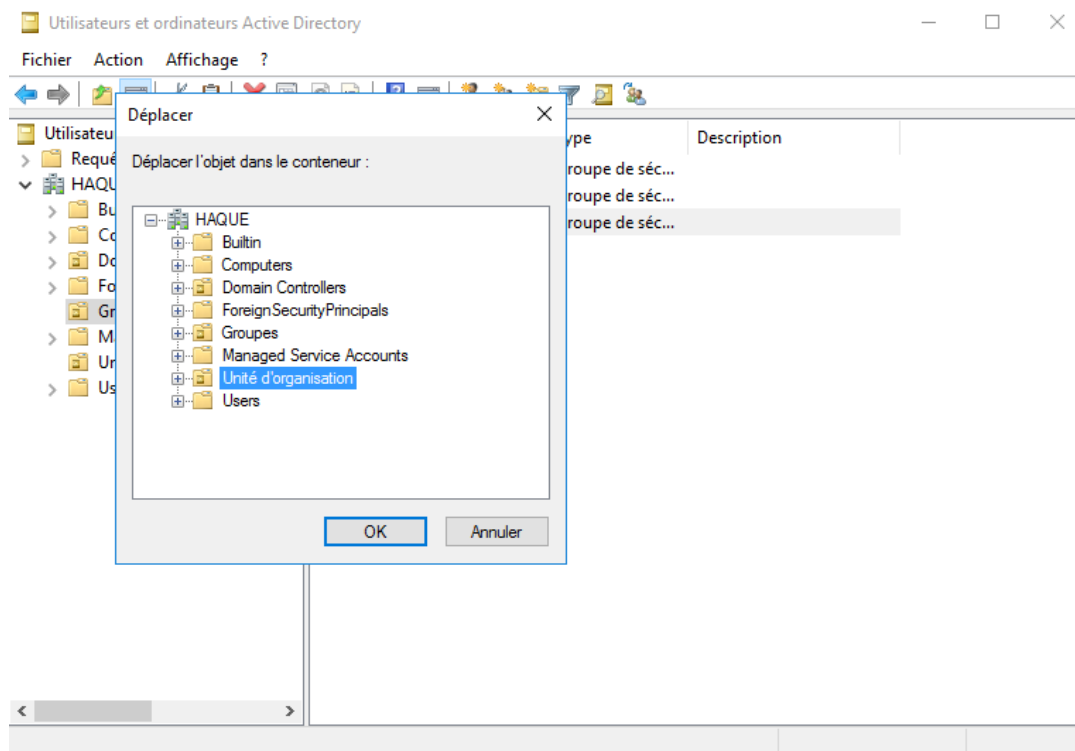
1. Dans le Tableau de bord, aller sur Outils, puis cliquer sur "Utilisateurs et ordinateurs Active Directory".



2. Cliquer sur l'Unité d'Organisation, puis faire un clic-droit sur le groupe que vous voulez déplacer, et cliquer sur "Déplacer..."



3. Cliquer sur l'UO où vous voulez mettre le groupe. Et cliquer sur OK pour valider le déplacement.



Le groupe a bien été déplacé vers l'Unité d'Organisation que vous vouliez.

7. PRÉPARER DES RAPPORTS SUR L'ÉTAT ET LA SANTÉ DE L'INFRASTRUCTURE AD

Utiliser PingCastle.

1. Lancer PingCastle.

```
C:\Users\Administrateur\Downloads\PingCastle_3.1.0.1\PingCastle.exe

\==--0      PingCastle (Version 3.1.0.1      28/08/2023 19:10:30)
 \ / \  ---> Get Active Directory Security at 80% in 20% of the time
  \ / \  , '  End of support: 2025-01-31
   0'---0
    \ , '
     v      Vincent LE TOUX (contact@pingcastle.com)
           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.
```

2. Pour faire un audit de votre Active Directory, utilisez le programme 5 de l’outil PingCastle “5-scanner –Perform specific security checks on workstation”. Allez dessus et appuyez la touche Entrée.

```
C:\Users\Administrateur\Downloads\PingCastle_3.1.0.1\PingCastle.exe

\==--0      PingCastle (Version 3.1.0.1      28/08/2023 19:10:30)
 \ / \  ---> Get Active Directory Security at 80% in 20% of the time
  \ / \  , '  End of support: 2025-01-31
   0'---0
    \ , '
     v      Vincent LE TOUX (contact@pingcastle.com)
           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
=====
You can know your local admins, if Bitlocker is properly configured, discover unprotect shares, ... A menu will be shown to
select the right scanner.
```

3. Ici, choisir ce que vous voulez scanner. Localadmin par exemple.

```
C:\Users\Administrateur\Downloads\PingCastle_3.1.0.1\PingCastle.exe

\==--0      PingCastle (Version 3.1.0.1    28/08/2023 19:10:30)
 \ / \-->    Get Active Directory Security at 80% in 20% of the time
  \ / \,'    End of support: 2025-01-31
 0'---0
  \,'
  v          Vincent LE TOUX (contact@pingcastle.com)
              twitter: @mysmartlogon      https://www.pingcastle.com

Select a scanner
=====
What scanner would you like to run ?
WARNING: Checking a lot of workstations may raise security alerts.
1-aclcheck          9-oxidbindings
2-antivirus         a-remote
3-computerversion   b-share
4-foreignusers      c-smb
5-laps bitlocker    d-smb3querynetwork
6-localadmin        e-spooler
7-nullsession       f-startup
8-nullsession-trust g-zeroologon
0-Exit

Enumerate the local administrators of a computer.
```

```
C:\Users\Administrateur\Downloads\PingCastle_3.1.0.1\PingCastle.exe

\==--0      PingCastle (Version 3.1.0.1    28/08/2023 19:10:30)
 \ / \-->    Get Active Directory Security at 80% in 20% of the time
  \ / \,'    End of support: 2025-01-31
 0'---0
  \,'
  v          Vincent LE TOUX (contact@pingcastle.com)
              twitter: @mysmartlogon      https://www.pingcastle.com

Select the scanning mode
=====
This scanner can collect all the active computers from a domain and scan them one by one automatically. Or scan only one co
mputer
1-all              -This is a domain. Scan all computers.
2-one              -This is a computer. Scan only this computer.
3-workstation      -Scan all computers except servers.
4-server           -Scan all servers.
5-domaincontrollers-Scan all domain controllers.
6-file             -Import items from a file (one computer per line).
0-Exit
```

```
C:\Users\Administrateur\Downloads\PingCastle_3.1.0.1\PingCastle.exe

\==--0_ PingCastle (Version 3.1.0.1 28/08/2023 19:10:30)
 \ / \--> Get Active Directory Security at 80% in 20% of the time
  \ / \,' End of support: 2025-01-31
   0'---0
    \,' Vincent LE TOUX (contact@pingcastle.com)
     \,' twitter: @mysmartlogon https://www.pingcastle.com
      v
Select a domain or server
=====
Please specify the domain or server to investigate (default:HAQUE.local)
HAQUE.local
```

```
C:\Users\Administrateur\Downloads\PingCastle_3.1.0.1\PingCastle.exe

\==--0_ PingCastle (Version 3.1.0.1 28/08/2023 19:10:30)
 \ / \--> Get Active Directory Security at 80% in 20% of the time
  \ / \,' End of support: 2025-01-31
   0'---0
    \,' Vincent LE TOUX (contact@pingcastle.com)
     \,' twitter: @mysmartlogon https://www.pingcastle.com
      v
Select a domain or server
=====
Please specify the domain or server to investigate (default:HAQUE.local)
HAQUE.local
[12:21:21] Getting computer list
[12:21:23] 2 computers to explore
[12:21:44] Done
[12:21:44] Results saved to C:\Users\Administrateur\Downloads\PingCastle_3.1.0.1\ad_scanner_localadmin_HAQUE.local.txt
Task Scanner completed
=====
Program launched in interactive mode - press any key to terminate the program
=====
```

4. Une fois le scan terminé, vous pouvez aller voir les résultats enregistrés dans le fichier mentionné sur PingCastle.

ad_scanner_localadmin_HAQUE.local - Bloc-notes

Fichier	Edition	Format	Affichage	?
Computer	SID	Account		
WIN-R15U8BPT9KI.HAQUE.local	S-1-5-21-3568470425-562583214-1169620312-500	HAQUE\Administrateur		
WIN-R15U8BPT9KI.HAQUE.local	S-1-5-21-3568470425-562583214-1169620312-519	HAQUE\Administrateurs de l'entreprise		
WIN-R15U8BPT9KI.HAQUE.local	S-1-5-21-3568470425-562583214-1169620312-512	HAQUE\Admins du domaine		

Voilà, vous savez maintenant comment préparer des rapports sur l'état et la santé de l'infrastructure Active Directory.