

**Titre de l'activité N°11 :**  
**Gestion des utilisateurs Active Directory et droits NTFS**

Intitulé Activité Type de référence.		
Compétence(s) Evaluée(s).		
Durée effective de l'activité.		
Conditions de réalisation	En autonomie	En équipe
	X	

**Description de l'activité.**

**I. Contexte :**

Créer des utilisateurs Active Directory, les associer à des groupes de sécurité, gérer les droits d'accès sur un partage réseau et mettre en place une délégation de droits.

**II. Matériel mis en œuvre :**

MATERIEL	LOGICIELS ET DOCUMENTATIONS
Serveur Lenovo ThinkStation P320 (Windows Server 2016)	Windows Server 2016 PowerShell

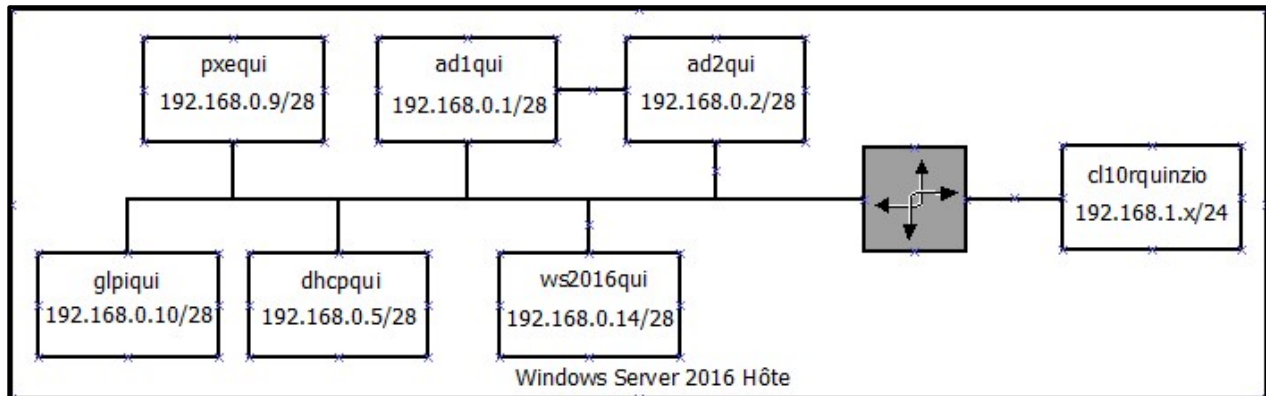
**III. Consignes de réalisation :**

Sur le domaine existant rquinzio.lan, créer des Unités d'Organisation (OU), des groupes de sécurité et y associer des utilisateurs à l'aide d'un script. Créer des délégations de contrôle sur les OU existantes seulement pour les groupes 'Manager'. Configurer les droits NTFS sur un partage réseau en restant cohérent avec les groupes et utilisateurs.

**IV. Résultats attendus :**

Les utilisateurs ciblés par la délégation de contrôle devront être en mesure de réinitialiser les mots de passe des utilisateurs de leur OU respective. Les utilisateurs doivent avoir les bons droits dans leurs répertoires respectifs sur le partage réseau.

## V. Plan de l'infrastructure réseau mise en œuvre :



## VI. Principales étapes de réalisation :

### 1 – Application du script PowerShell :

Afin de créer nos OU, Groupes de sécurité et Utilisateurs, nous allons utiliser un script PowerShell associé à des feuilles CSV. Le script va extraire les informations du fichier CSV sous formes de variables et va ensuite exécuter des commandes PowerShell avec ces variables. Le script, ainsi que les feuilles CSV seront en annexe.

Voici une brève description du script :

```

1  Import-Module ActiveDirectory
2
3  $userCsv = 'C:\ps\users.csv'
4  $ouCSV = 'C:\ps\ou.csv'
5  $groupsCSV = 'C:\ps\groups.csv'
6  $dcPath = 'DC=rquinzio,DC=lan'
7  $ouPath = 'OU=GROUPES,DC=rquinzio,DC=lan'
8  $groups = Import-Csv $groupsCSV
9  $ouNames = Import-Csv $ouCSV
10 $users = Import-Csv $userCsv

```

1. Importation des outils de gestion Active Directory dans le script
- 2.
3. Indique l'emplacement de la feuille CSV Utilisateurs
4. Indique l'emplacement de la feuille CSV OU
5. Indique l'emplacement de la feuille CSV Groupes
6. Indique le nom distingué (DN) du DC
7. Indique l'OU dans laquelle sont stockés les groupes
8. Importe la feuille CSV Groupes dans une nouvelle variable du script
9. Importe la feuille CSV OU dans une nouvelle variable du script
10. Importe le CSV Utilisateurs dans une nouvelle variable du script

```

11
12 foreach($ou in $ouNames){
13     New-ADOrganizationalUnit -Name $ou.name -Path $dcPath -ProtectedFromAccidentalDeletion $True
14 }
15

```

La boucle *foreach* indique au script de lancer la commande *New-ADOrganizationalUnit* en créant pour chaque colonne une variable *\$ou*. Le commutateur *-Name* indique le nom des OU à créer, en utilisant les valeurs de la colonne *name* dans la feuille CSV OU (représentée par *\$ou.name*), dans le DC attribué par la variable *\$dcPath*. Le dernier commutateur (booléen) sert à indiquer si les OU créés doivent être protégées contre les suppressions accidentelles.

```

16 foreach ($group in $groups){
17     New-ADGroup -Name $group.name -Path $ouPath -GroupScope $group.scope -GroupCategory $group.category
18 }

```

Cette boucle sert à la création des groupes depuis la feuille CSV Groupes. Le commutateur *-GroupScope* indique la portée de nos groupes (Globale dans notre cas). Le commutateur *-GroupCategory* indique la catégorie des groupes (Sécurité dans notre cas).

```

20 foreach ($user in $users) {
21     $firstName = $user.firstname
22     $lastName = $user.lastname
23     [boolean]$changePassword = [System.Convert]::ToBoolean($user.chpasswdlogon)
24     [boolean]$enabled = [System.Convert]::ToBoolean($user.enabled)
25
26     New-ADUser `
27     -Name "$firstName $lastName" `
28     -SamAccountName $user.username `
29     -GivenName $user.firstname `
30     -Surname $user.lastname `
31     -AccountPassword (ConvertTo-SecureString $user.password -AsPlainText -Force) `
32     -ChangePasswordAtLogon $changePassword `
33     -Enabled $enabled `
34     -Path $user.ou
35 }
36

```

Cette boucle sert à la création des utilisateurs. On remarquera l'utilisation du type *boolean* sur les variables lignes 23 et 24. En effet, dans la feuille CSV Utilisateurs, les entrées des colonnes *chpasswdlogon* et *enabled* sont soit 0 soit 1. Sachant que les commutateurs *-ChangePasswordAtLogon* et *-Enabled* n'acceptent que les valeurs *\$True* ou *\$False*, nous devons convertir les valeurs extraites des colonnes afin qu'elles soient valides.

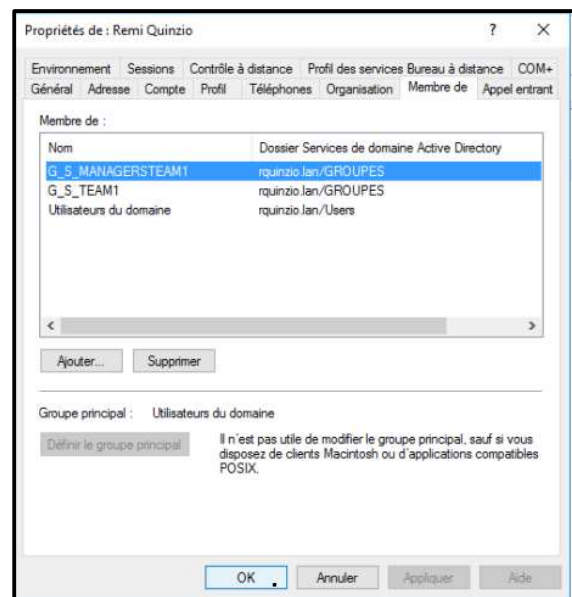
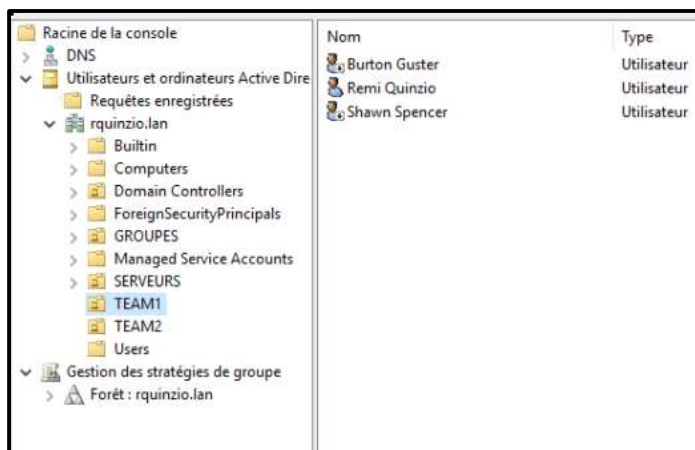
```

37
38 foreach ($user in $users) {
39     if ([string]($user.group2) -like "CN=") {
40         Add-ADGroupMember -Identity $user.group2 -Members $user.userPath}
41         Add-ADGroupMember -Identity $user.group1 -Members $user.userPath
42     }
43 }

```

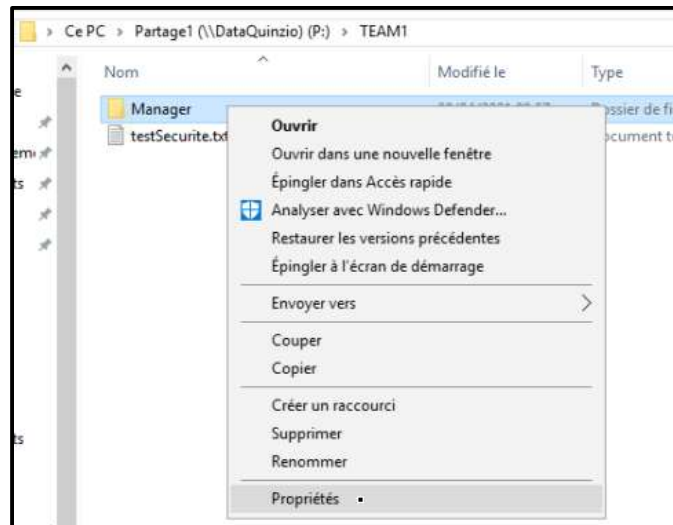
Enfin, cette dernière boucle sert à attribuer les utilisateurs à leurs groupes respectifs avec *Add-ADGroupMember*. On notera l'utilisation de l'instruction *if* afin de filtrer les utilisateurs qui appartiennent à deux groupes.

Une fois le script exécuté, on remarque son bon fonctionnement :

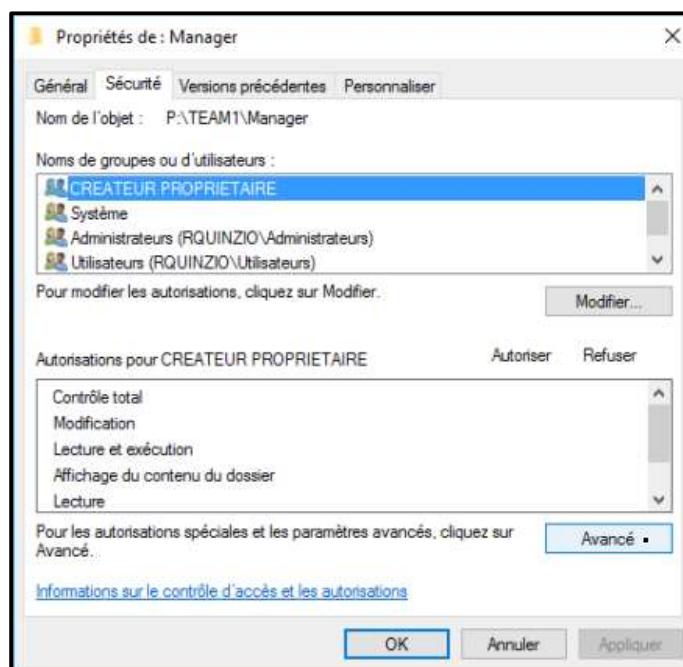


## 2 – Gestion des droits NTFS :

Afin de configurer les droits d'accès de nos utilisateurs aux fichiers partagés, se rendre dans le partage réseau disponible sur le cluster *DataQuinzio* (cf. FA 5 – *Création d'un cluster à basculement*), y créer des dossiers et fichiers, puis **Clic-droit > Propriétés** sur l'un d'eux.

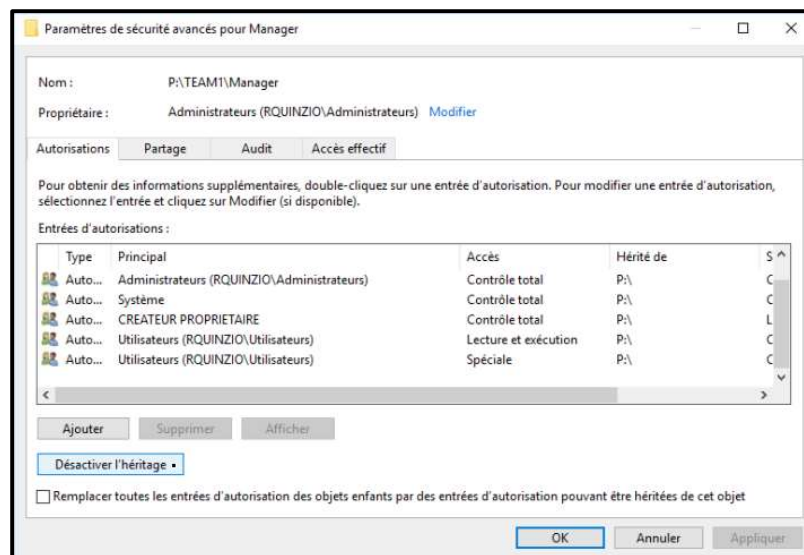


Se rendre dans l'onglet **Sécurité**, puis cliquer sur **Avancé** :

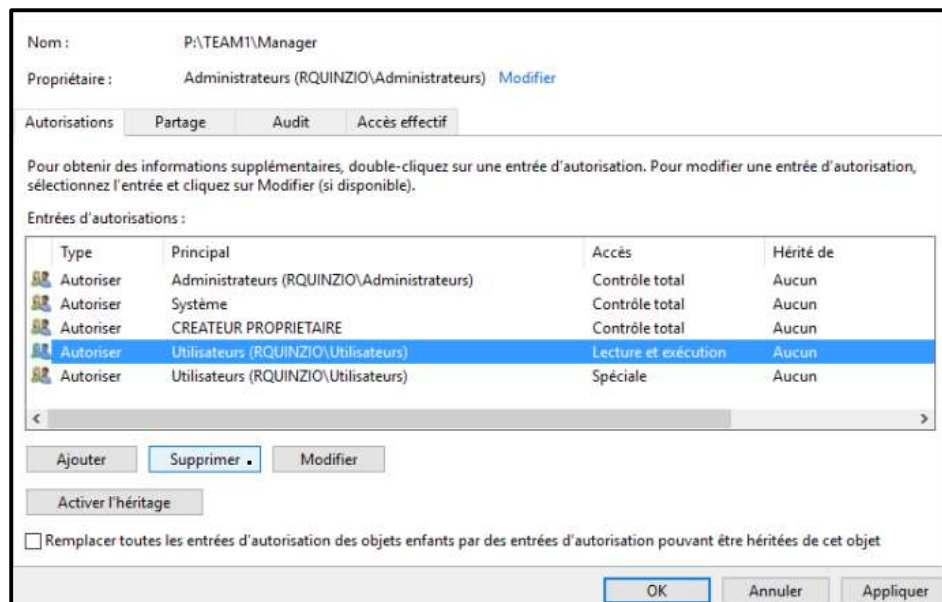




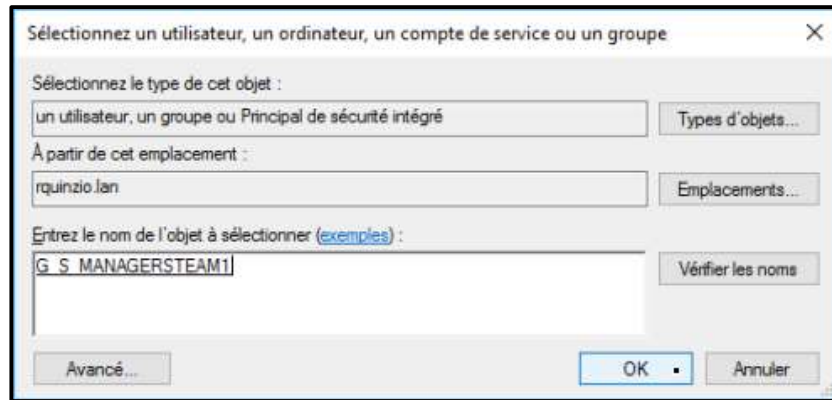
Cliquer ensuite sur **Désactiver l'héritage**, puis **Convertir les autorisations...** :



**Supprimer les Entrées d'autorisations Utilisateurs :**



Cliquer ensuite sur **Ajouter**. Dans la nouvelle fenêtre Autorisations pour ..., cliquer sur **Sélectionner un principal**, puis choisir l'un des Groupes de sécurité créés précédemment :



Sélectionnez un utilisateur, un ordinateur, un compte de service ou un groupe

Sélectionnez le type de cet objet :

un utilisateur, un groupe ou Principal de sécurité intégré

À partir de cet emplacement :

rquinzio.lan

Entrez le nom de l'objet à sélectionner (exemples) :

G S MANAGERSTEAM1

Types d'objets...

Emplacements...

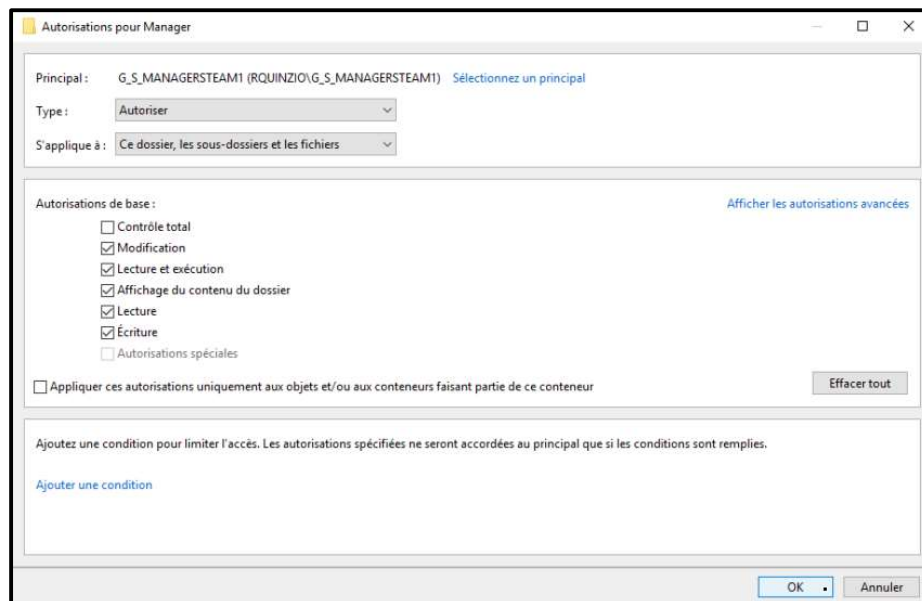
Vérifier les noms

Avancé...

OK

Annuler

Dans notre cas, nous lui donnerons les droits en Modification, afin qu'il puisse supprimer les dossiers et fichiers dont il est propriétaire, sans pouvoir effacer les autres (ceux créés par les administrateurs notamment). Faire ensuite de même pour les autres dossiers/fichiers créés :



Autorisations pour Manager

Principal : G\_S\_MANAGERSTEAM1 (RQUINZIO\G\_S\_MANAGERSTEAM1) Sélectionnez un principal

Type : Autoriser

S'applique à : Ce dossier, les sous-dossiers et les fichiers

Autorisations de base :

☐ Contrôle total

☒ Modification

☒ Lecture et exécution

☒ Affichage du contenu du dossier

☒ Lecture

☒ Écriture

☐ Autorisations spéciales

☐ Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

Ajouter une condition pour limiter l'accès. Les autorisations spécifiées ne seront accordées au principal que si les conditions sont remplies.

Ajouter une condition

Afficher les autorisations avancées

Effacer tout

OK

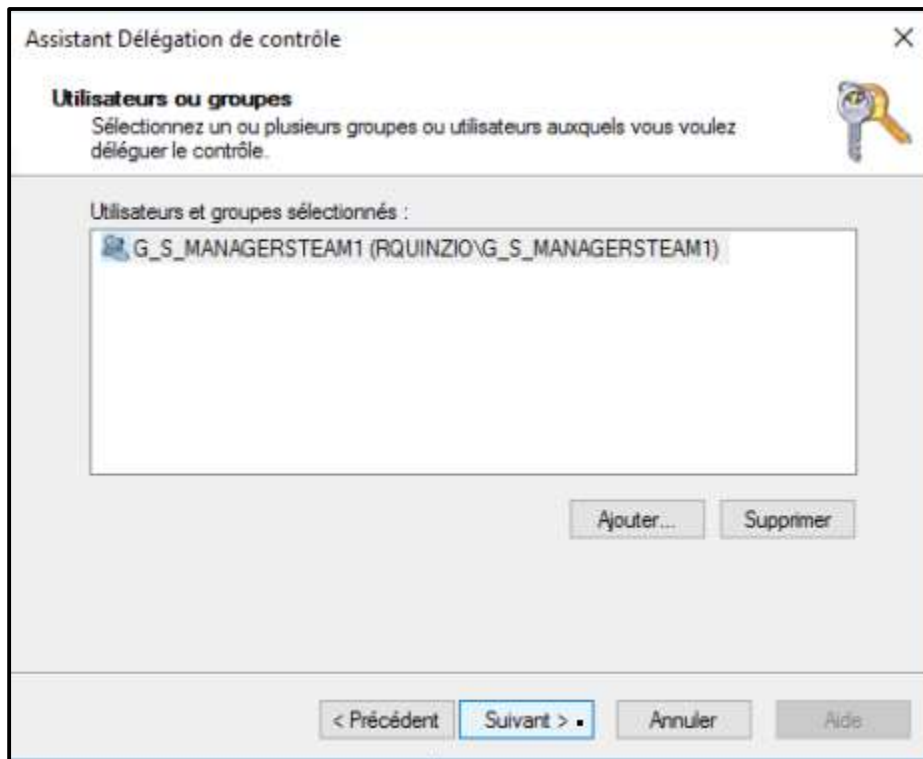
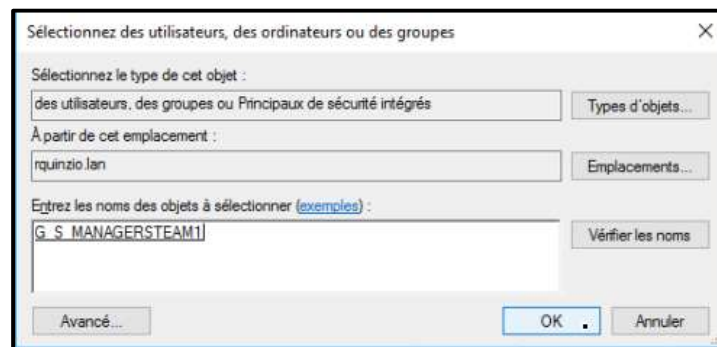
Annuler



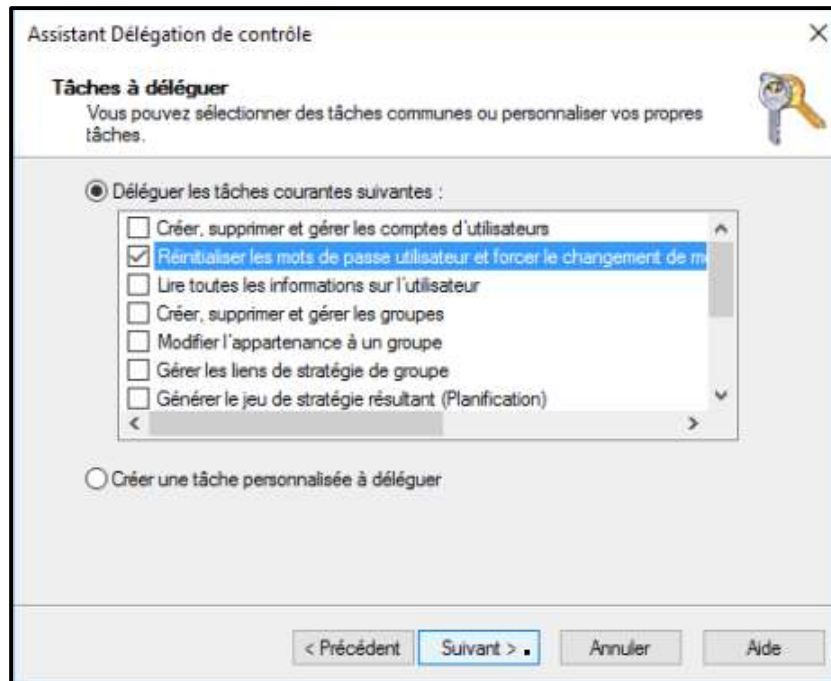
### 3 – Délégation de contrôle :

Afin de limiter les demandes au support informatique de la part d'utilisateurs qui oublieraient leur mot de passe, nous allons créer une Délégation de contrôle qui autorisera les membres des groupes **G\_S\_MANAGERSTXXX** à réinitialiser les mots de passe des utilisateurs de leurs OU respectives.

Pour ce faire, se rendre dans la console Utilisateurs et ordinateurs Active Directory, puis **Clic-droit sur l'OU à gérer > Délégation de contrôle**. L'Assistant Délégation de contrôle s'ouvre alors. Cliquer sur **Ajouter**, puis sélectionner le Groupe de sécurité qui recevra la délégation. Enfin, cliquer sur **Suivant**.



Sélectionner les tâches à déléguer, puis **Suivant**. La création de la délégation est terminée.



Assistant Délégation de contrôle

**Tâches à déléguer**  
Vous pouvez sélectionner des tâches communes ou personnaliser vos propres tâches.

☒ Déléguer les tâches courantes suivantes :

- ☐ Créer, supprimer et gérer les comptes d'utilisateurs
- ☒ Réinitialiser les mots de passe utilisateur et forcer le changement de m...
- ☐ Lire toutes les informations sur l'utilisateur
- ☐ Créer, supprimer et gérer les groupes
- ☐ Modifier l'appartenance à un groupe
- ☐ Gérer les liens de stratégie de groupe
- ☐ Générer le jeu de stratégie résultant (Planification)

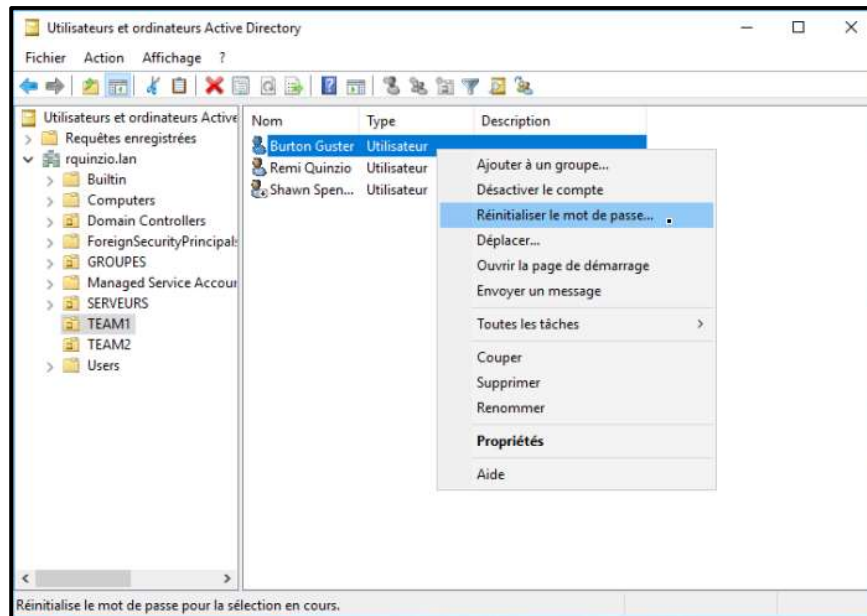
☐ Créer une tâche personnalisée à déléguer

< Précédent   Suivant > .   Annuler   Aide

## VII. Phase de validation :

### 1 – Délégation de contrôle :

Connexion avec l'utilisateur *rquinzio@rquinzio.lan* (membre du groupe *G\_S\_MANAGERSTEAM1*) et réinitialisation des mots de passe :



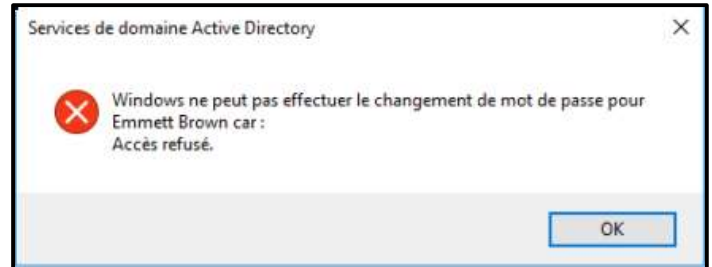
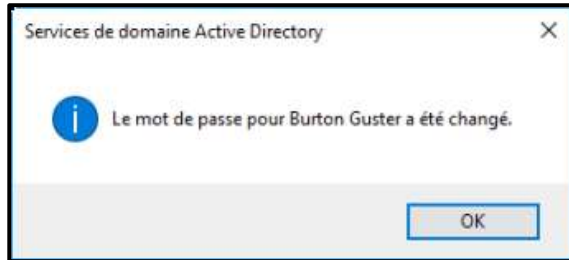
### 2 – Droits NTFS :

Manipulation des dossiers et fichiers dans le partage réseau avec les utilisateurs *rquinzio* et *bguster* sur *rquinzio.lan*.

## VIII. Bilan :

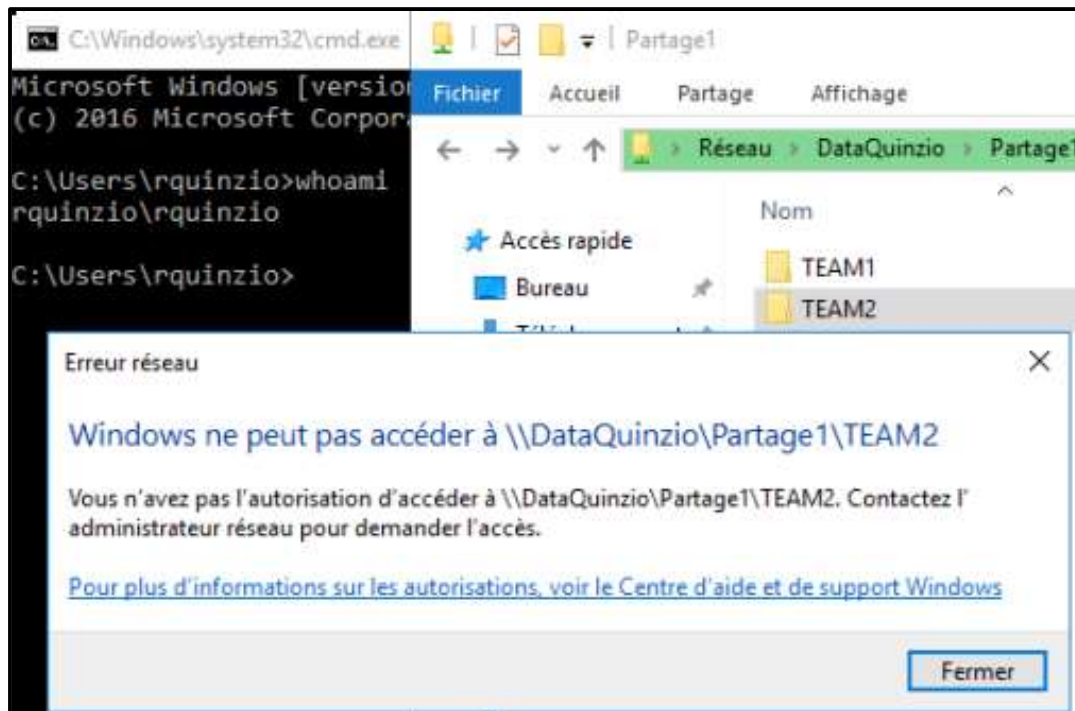
### 1 – Délégation de contrôle :

L'utilisateur *rquinzio* peut réinitialiser le mot de passe de *bguster* qui se trouve dans l'OU qui lui est déléguée. En revanche, il ne peut pas le faire sur l'utilisateur *ebrown* qui se trouve dans l'OU *TEAM2* :

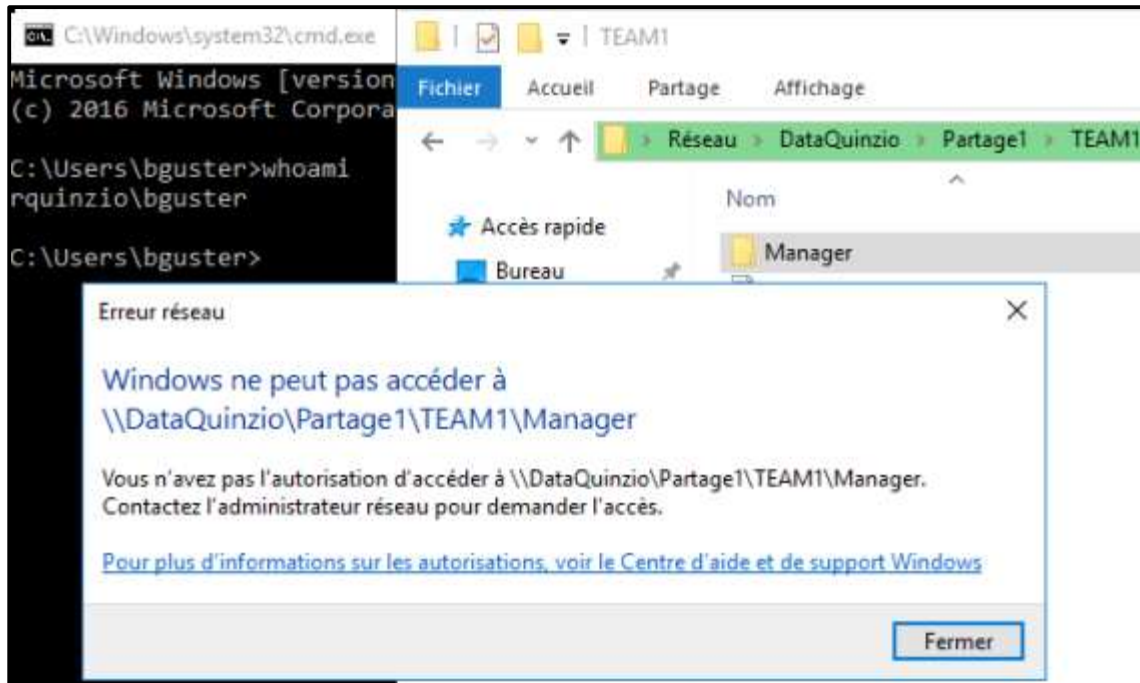


### 2 – Droits NTFS :

L'utilisateur *rquinzio* ne peut pas accéder au dossier *TEAM2* car il n'appartient pas aux groupes autorisés dans la liste de contrôle d'accès du dossier *TEAM2* :



L'utilisateur *bguster* ne peut pas accéder au dossier *Manager* pour les mêmes raisons :





AFPA LORIENT



Nom : QUINZIO REMI

Dates de réalisation : 07/04/2021

**Fiche d'évaluation.**

Nom du tuteur	Fonction

**CCP : N° .....**

**Evaluation de la compétence:...**

Critères d'appréciation généraux	Validation	Critères d'évaluation spécifiques	Validation

***V : validé. NV : Non validé. NE : Non évalué.***

**Observations du tuteur**

--

**Validation**

<u>Entreprise</u>	<u>Centre de Formation AFPA</u>
Date : Signature du tuteur	Nom : Michel CHARRA Pris connaissance le : Signature du responsable pédagogique :

**Observations du responsable pédagogique**

--