

Gestion accès sous Windows Server

La plupart des entreprises et des organisations ont investi dans des outils et des techniques de sécurité. Cependant, superposer des briques de défense est tout à fait différent de bâtir une sécurité intelligente. Qu'en est-il d'une approche proactive de la sécurité permettant d'intégrer la maîtrise du risque au cœur même de son environnement ? La gouvernance de la gestion des identités et des accès proposés par Windows server contribue à apporter une réponse à ces questions et à dépasser le simple contrôle du risque, en intégrant la responsabilité et la transparence dans la gestion des droits des utilisateurs tout au long de leur cycle de vie.

6.1 CHOIX DU SYSTÈME D'EXPLOITATION DE VOTRE/VOS SERVEURS

En fonction des logiciels, les éditeurs valident un certain nombre de système d'exploitation : Microsoft Windows Server, RedHat Enterprise, SUSE Linux Enterprise.

Le choix de l'OS sera fait en fonction de vos habitudes : Windows ou Linux, une version avec support commercial ou support communautaire

Tous les agents de la Direction générale ainsi que les RSSI travaillent et ne maîtrise que l'environnement Windows, donc le choix se fera sur Windows serveur.

6.2 Présentation et installation VMware

6.2.1 Présentation VMware

VMware Workstation Player est l'outil idéal pour exécuter une machine virtuelle unique sur un PC Windows ou Linux. Les organisations utilisent Workstation Player pour déployer des postes de travail professionnels gérés, tandis que les étudiants et les éducateurs l'utilisent pour l'apprentissage et la formation.

La version gratuite est disponible pour une utilisation non commerciale, personnelle et domestique. Nous encourageons également les étudiants et les organisations à but non lucratif à profiter de cette offre.

6.2.2 Installation VMware

- Configuration requise :

L'ordinateur physique sur lequel on installe VMware Workstation est appelé « système hôte » et son système d'exploitation est appelé le système d'exploitation hôte. Pour exécuter VMware

Workstation, le système hôte et le système d'exploitation hôte doivent satisfaire à des exigences matérielles et logicielles spécifiques

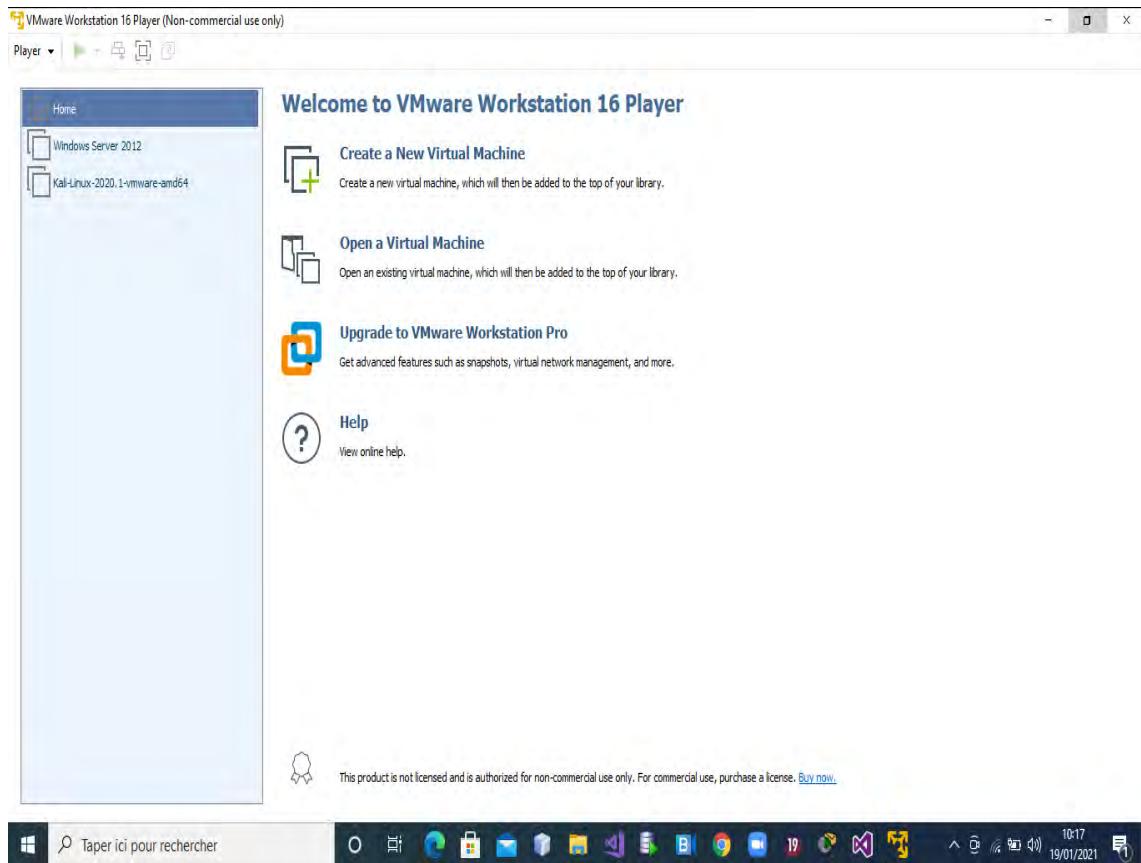


Figure 14 : interface d'accueil VMware

6.3 Présentation et configuration Windows server

Nous allons choisir Windows server 2012 R2 pour mieux exercer la pratique de nos cours.

6.2.1 Présentation Windows server 2012 R2

Microsoft Windows Server 2012, anciennement connu sous le nom de code Windows Server 8, est la seconde avant dernière version du système d'exploitation réseau Windows Server. La version suivante est Windows Server 2012 R2. Windows Server 2016 est sorti le 1^{er} octobre 2014 en phase de développement et est prévu pour le 3^e trimestre 2016 en version finale.

Il s'agit de la version serveur de Windows 8 et du successeur de Windows Server 2008 R2. Windows Server 2012 est la première version de Windows Server à ne pas supporter les systèmes Itanium depuis Windows NT 4.0.

Une pré-bêta a été publiée le 9 septembre 2011 pour les abonnés MSDN; puis Microsoft publie une bêta publique le 1^{er} mars 2012 (build 8250).

Le 17 avril 2012, Microsoft annonce que le nom du produit sera Windows Server 2012. Le 31 mai 2012, Microsoft annonce la version RC pour Windows Server 2012. La version finale (RTM) de Microsoft Windows Server 2012 est publiée le 1^{er} août 2012 et le lancement public a lieu le 4 septembre 2012.

Cette nouvelle version de Windows Server apporte de nombreuses nouveautés qui permettent de rendre les serveurs plus évolutifs, virtualisables (Hyper-V) et favorise les évolutions vers les clouds privés ou publics.

	
Famille	Microsoft Windows NT
Type de noyau	Noyau hybride
État du projet	Achevé
Plates-formes	AMD64
Entreprise / Développeur	Microsoft
Licence	Microsoft EULA
États des sources	Source fermée
Première version	Octobre 2012
Dernière version stable	6.2 (Build 9200)
Méthode de mise à jour	Windows Update
Site web	www.microsoft.com [archive]

Tableau 13 : description de Windows server 2012

Editions

Contrairement à Windows Server 2008 R2 qui offrait pléthore d'éditions, Windows Server 2012 se contente de quatre éditions : Foundation, Essential, Standard et Datacenter¹.

Le lancement de Windows Server 2012 annonce également la fin d'un produit phare de Microsoft à destination des PME : Windows Small Business Server. En effet, la version 2011 de ce produit n'aura pas de successeur.

Windows Server 2012 Foundation (Win12)

Cette édition n'est disponible qu'à l'achat d'un nouveau serveur. Destinée aux TPE, cette édition est limitée à 15 utilisateurs, ne prend pas en charge la virtualisation et ne supporte qu'un seul processeur. Il n'y a, par contre, pas besoin de CAL Windows pour se connecter à un serveur Foundation. Le serveur doit être hébergé sur une machine physique².

Windows Server 2012 Essential

Cette édition a pour objectif d'amener les PME vers les solutions cloud de Microsoft. Elle est limitée à 25 utilisateurs, ne prend pas en charge la virtualisation et supporte jusqu'à deux

processeurs. Elle est aussi conçue pour une intégration directe à Microsoft Office 365. Le serveur peut être hébergé sur une machine physique ou virtuelle².

Windows Server 2012 Standard

La principale édition de Windows Server 2012 offre toutes les fonctionnalités du produit, tout comme l'édition Datacenter. Elle se distingue de cette dernière par le nombre de machines virtuelles couvertes par la licence, à savoir deux.

Windows Server 2012 Standard supporte jusqu'à deux processeurs par licence. Tout comme l'édition Datacenter, elle prend en charge les machines disposant d'un maximum de 64 processeurs (sockets) et de 4 To de mémoire RAM.

Windows Server 2012 Datacenter

Cette édition est destinée à ceux qui ont un recours intensif aux machines virtuelles. Chaque licence couvre en effet jusqu'à deux processeurs et un nombre de machines virtuelles illimité. Il existe aussi une version déployable en tant qu'application matérielle: Windows Storage Server 2012³. Cette version destinée aux partenaires Microsoft existe en deux éditions, la version Workgroup et la version Standard (pas de limites de ressources, déduplication, mode grappe de serveurs).

6.2.2 Installation Windows server 2012 R2

Configuration du matériel (DD, SE, RAM,...)

Configuration minimum :

- Processeur : 1.4 GHz 64-bit
- RAM : 512 Mo
- Disque : 32 Go



Figure 15 : choix langue sous Windows server

A la fin de l'installation, vous devez définir le mot de passe du compte Administrateur avec un minimum de complexité.

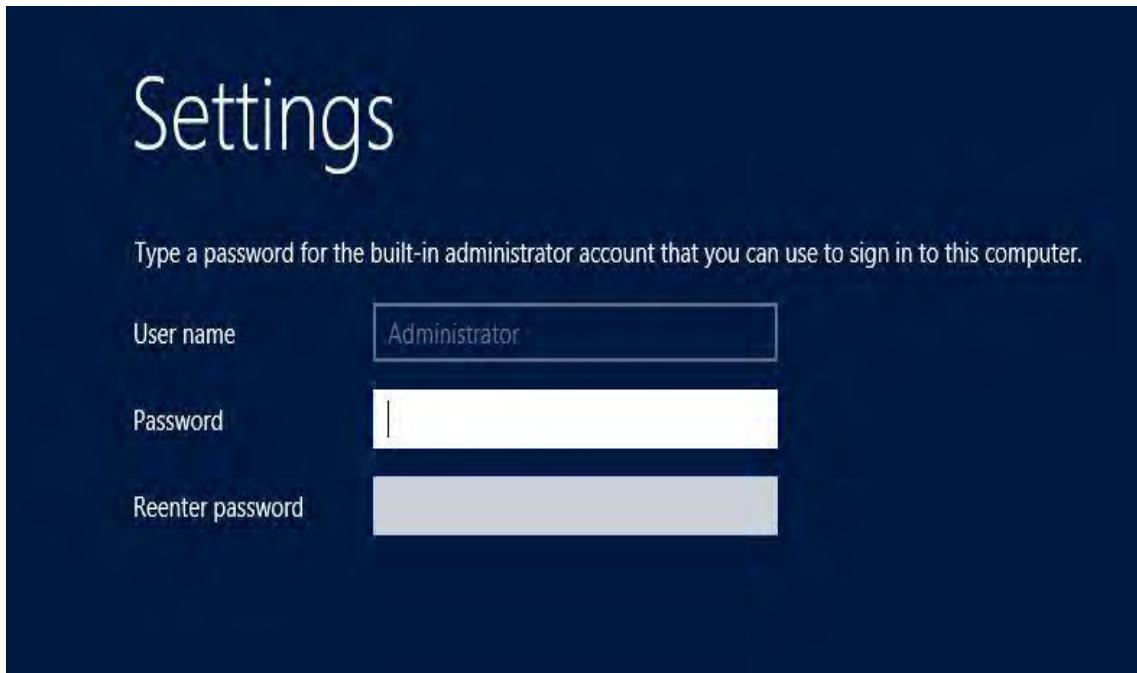


Figure 16 : interface connexion

L'installation est terminée avec succès, nous allons commencer notre configuration.

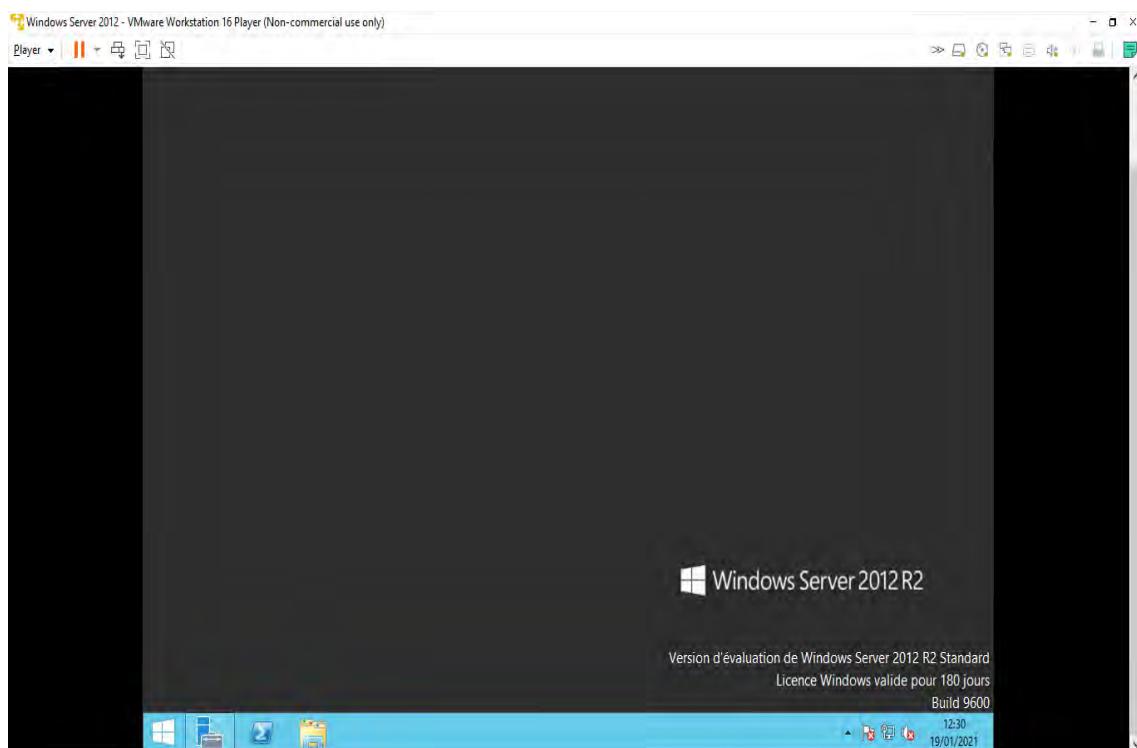


Figure 17 : interface d'accueil Windows server R2

6.4 Configuration des accès et identités sous Windows server

6.3.1 Présentation et installation d'Active Directory (AD)

6.3.1.1 Présentation AD

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, MacOs et encore Linux. Il permet également l'attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés (en), les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

Si les administrateurs ont indiqué les attributs convenables, il sera possible d'interroger l'annuaire pour obtenir, par exemple, « toutes les imprimantes couleur à cet étage du bâtiment ».

Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2012 (voire hors Microsoft par Samba) et Windows Server 2016, il résulte de l'évolution de la base de compte plane SAM. Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ».

Active Directory stocke ses informations et paramètres dans une base de données distribuée sur un ou plusieurs contrôleurs de domaine, la réplication étant prise en charge nativement¹. La taille d'une base Active Directory peut varier de quelques centaines d'objets, pour de petites installations, à plusieurs millions d'objets, pour des configurations volumineuses.

6.3.1.2 Installation Active Directory

Nous allons dans **Ajout de rôles et de fonctionnalités** avant de cocher **Service AD**

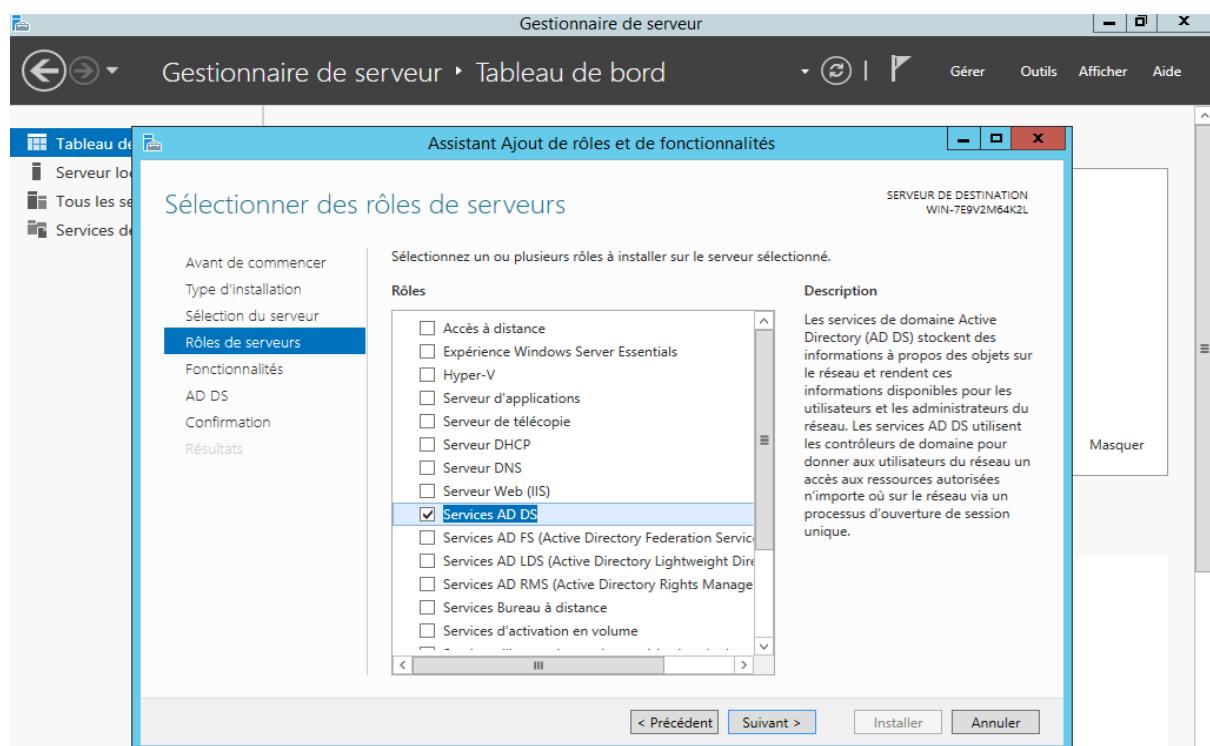


Figure 18: liste des fonctionnalités AD

Puis cliquer sur suivant pour poursuivre l'installation.

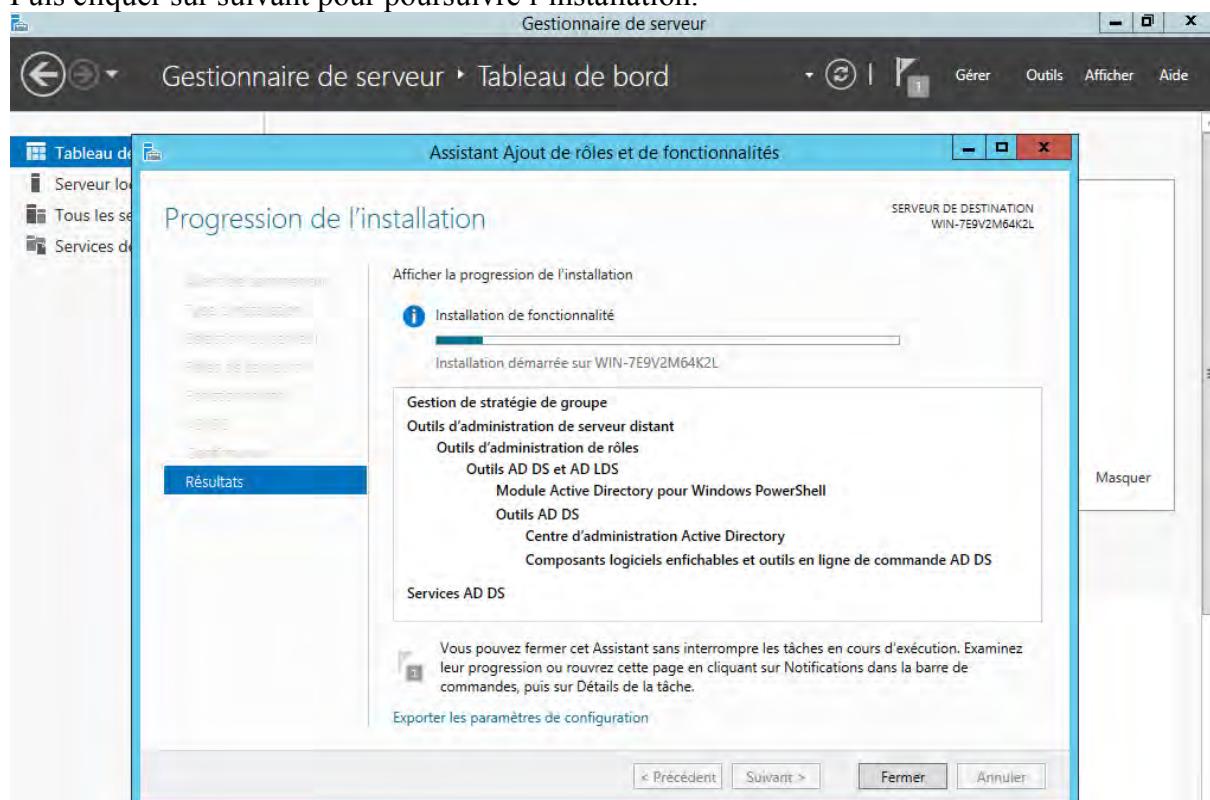


Figure 19 : progression d'installation Active Directory

➤ Ajout Forêt

Si vous êtes d'accord avec moi pour dire qu'une forêt c'est un ensemble d'arbres, alors vous avez déjà compris le principe de la notion de « forêt » dans un environnement Active Directory.

En effet, une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt.

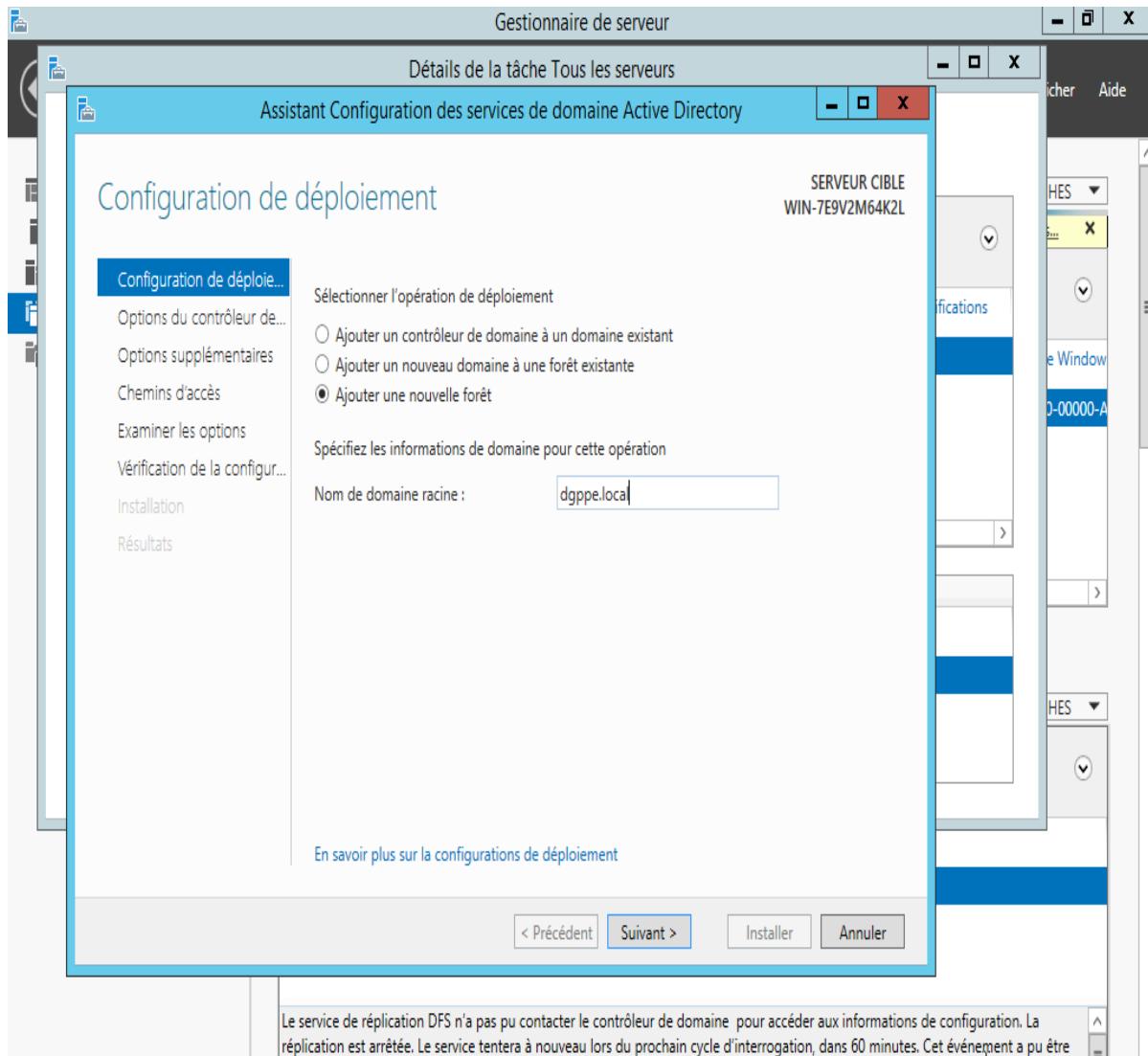


Figure 20 : ajout d'un forêt dgppe.local

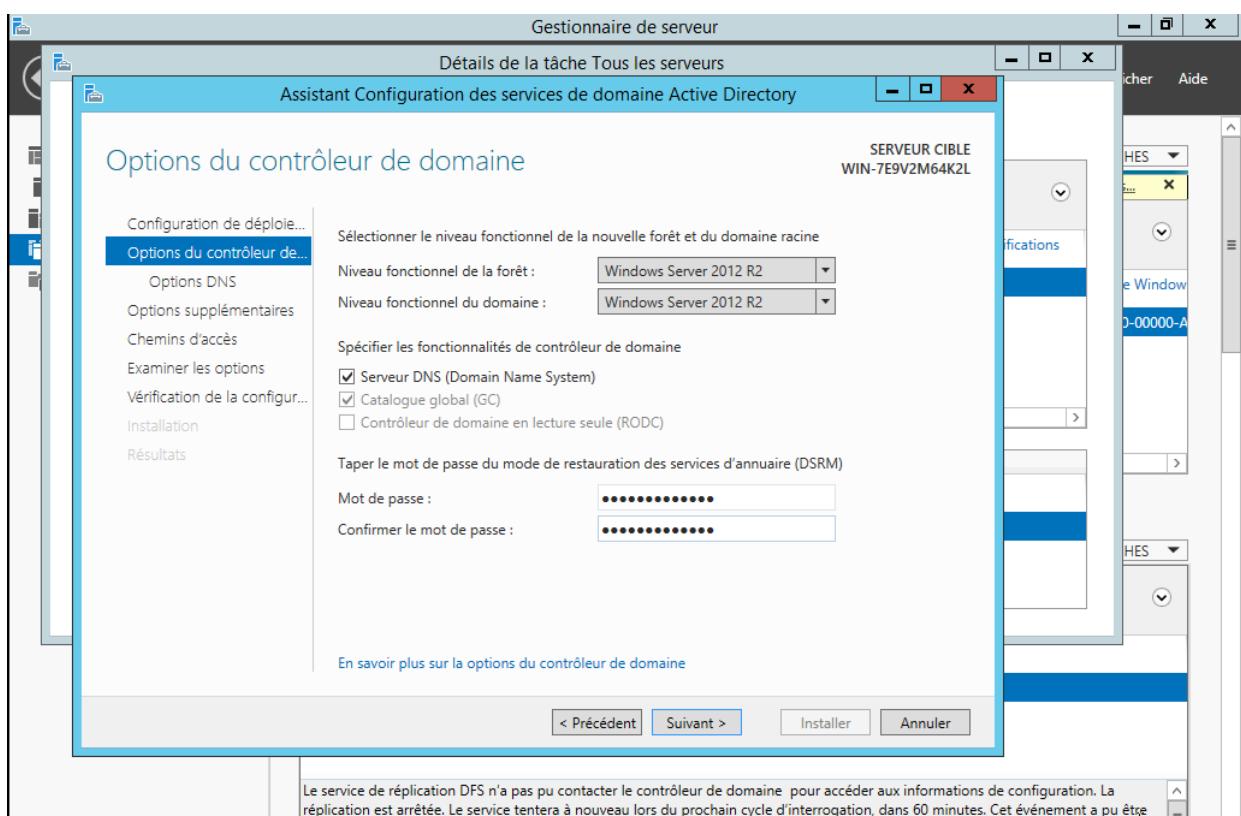


Figure 21 : option du contrôleur de domaine

Apres l'installation d'AD

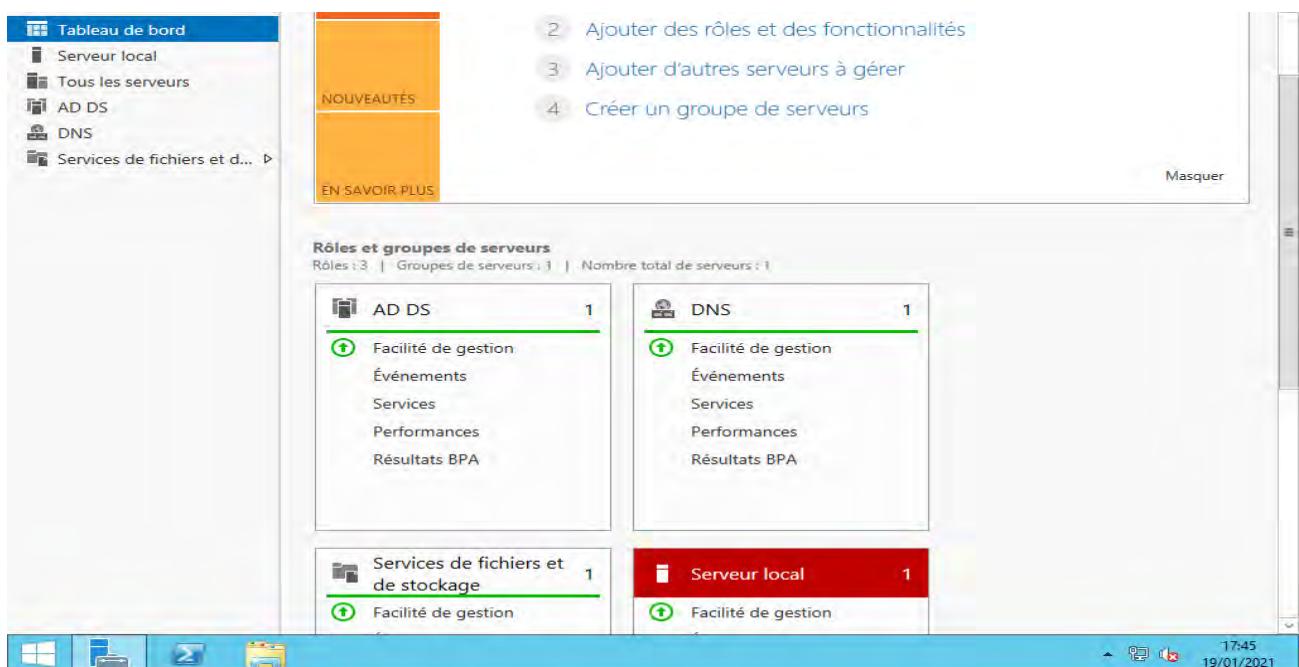


Figure 22 : vérification de l'installation AD

6.3.2 Crédation des utilisateurs et groupes Active directory

Pour notre pratique, nous allons cibler une direction (la DPEE par exemple), ainsi que le Cabinet de la Direction générale vue la charge de toute la structure.

Tous d'abord, nous allons ajouter les groupes ainsi que les utilisateurs de cette direction. Ensuite, nous allons partager leurs documents de travail et restreindre les accès aux groupes d'utilisateurs selon l'appartenance par divisions et bureaux.

Pour ajouter un nouveau groupe, **cliquons sur Utilisateurs et ordinateurs d'AD**, clique droite puis **Ajouter nouvel utilisateur ou groupe**

■ Ajout groupe :

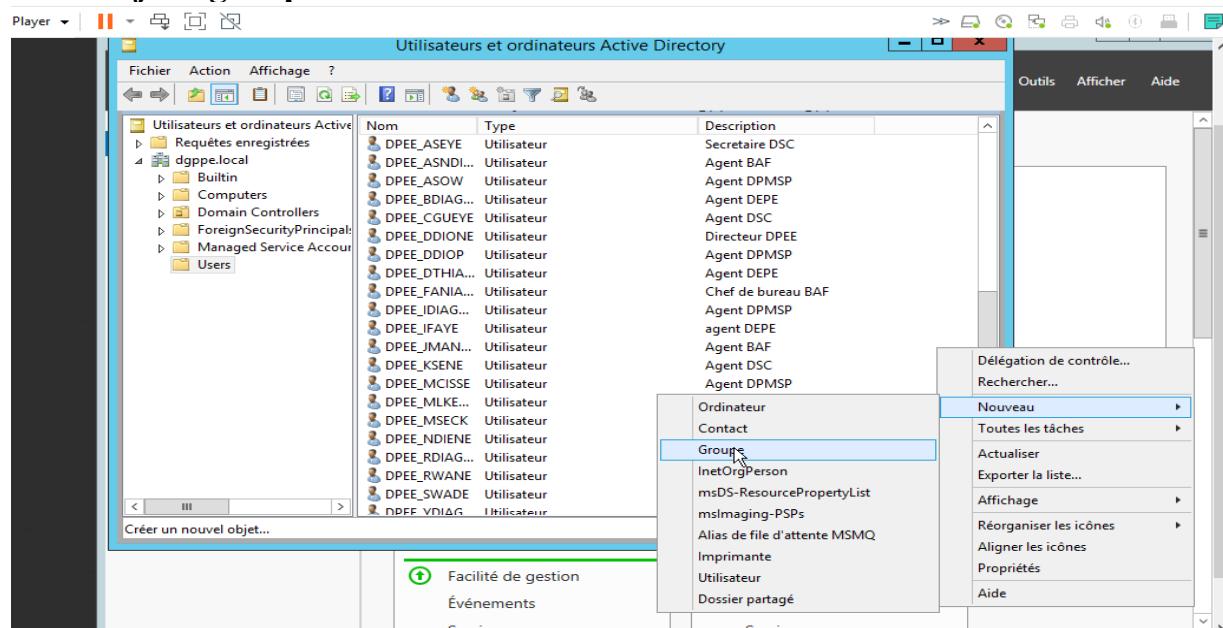


Figure 23 : ajout nouveau groupe

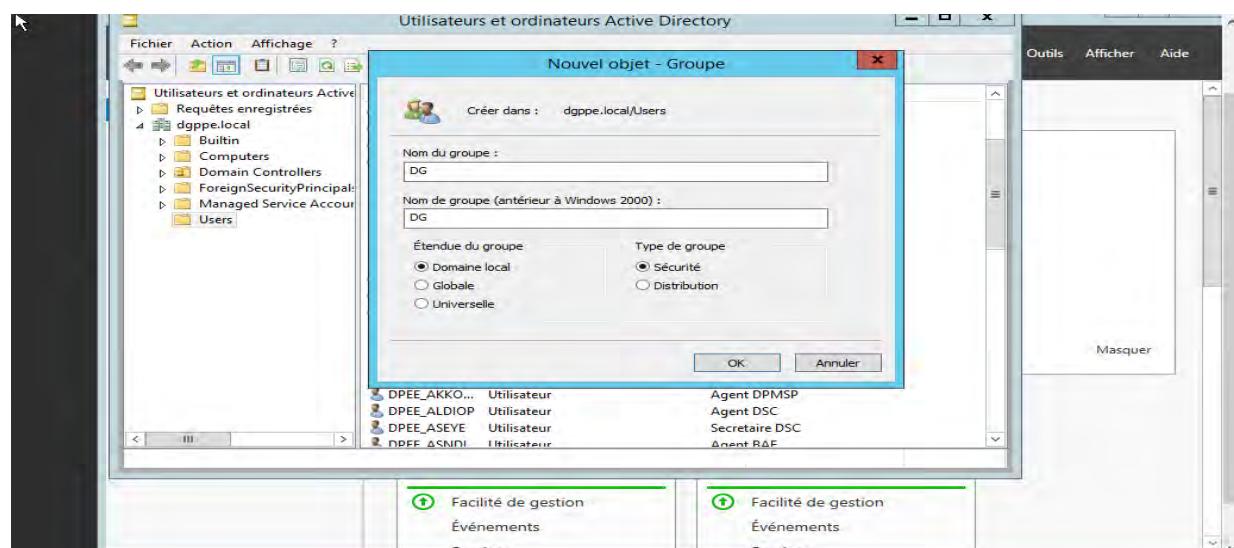


Figure 24 : interface pour création groupe

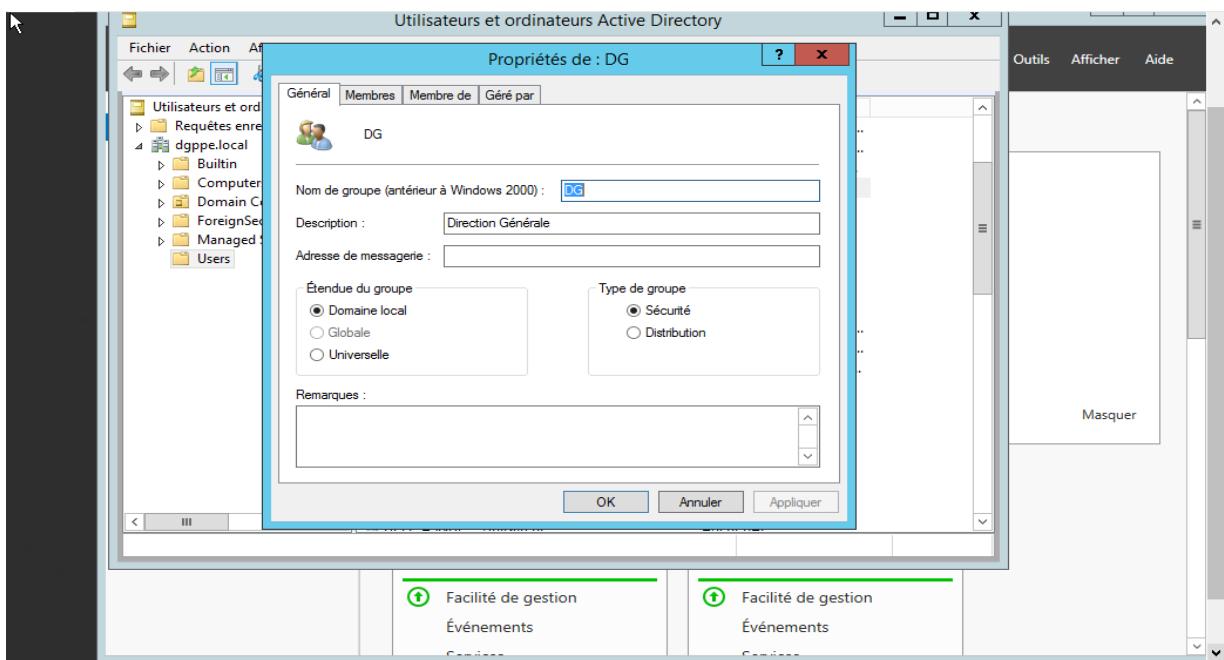


Figure 25 : interface ajout groupes sur AD

Ajout utilisateurs

Quand vous ajoutez un compte d'utilisateur, l'utilisateur affecté peut se connecter au réseau. En outre, nous pouvons donner à cet utilisateur l'autorisation d'accéder à des ressources réseau telles que les dossiers partagés et le site d'accès web à distance.

Pour ajouter un compte d'utilisateur :

1. Ouvrez le tableau de bord Windows Server Essentials.
2. Dans la barre de navigation, cliquez sur **Utilisateurs**.
3. Dans le volet **Tâches utilisateur**, cliquez sur **Ajouter un compte d'utilisateur**. L'Assistant Ajout d'un compte d'utilisateur s'affiche.

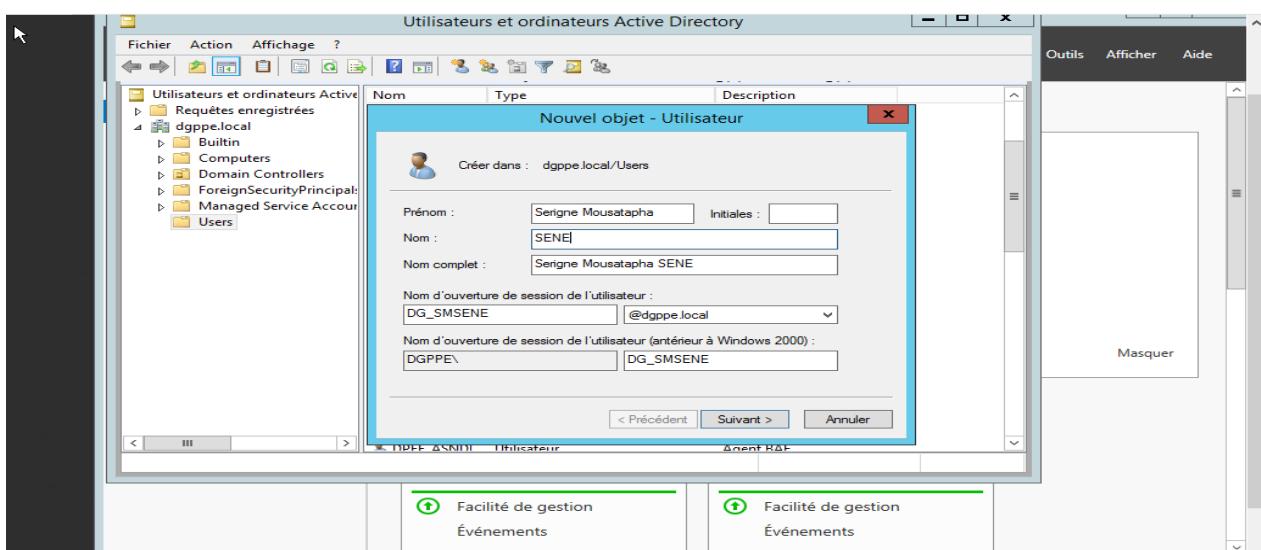


Figure 26 : interface ajout utilisateurs

▪ Stratégie de mot de passe

La stratégie de mot de passe est un ensemble de règles qui définissent la façon dont les utilisateurs créent et utilisent des mots de passe.

▪ Modifier la stratégie de mot de passe

Pour changer la stratégie de mot de passe

1. Ouvrez le tableau de bord Windows Server Essentials, puis cliquez sur **Utilisateurs**.
2. Dans le volet **Tâches**, cliquez sur **Définir la stratégie de mot de passe**.
3. Dans l'écran **Modifier la stratégie de mot de passe**, définissez le niveau de sécurité du mot de passe en déplaçant le curseur.

Sécurité des mots de passe avec Windows Server 2012 / R2 Windows Server 2008 / R2 nécessite de se rendre dans les **Outils d'administration**, **Gestion des stratégies de groupe** (ou **GPMC.msc**). Les GPO peuvent s'appliquer au domaine, aux unités d'organisation (OU), aux groupes, etc.

1. Dérouler **Gestion de stratégie de groupe**, **Forêt**, **Domaines**, *nom du domaine*.
2. **Clic droit et Modifier** sur **Default Domain Policy**, cela ouvre l'**Editeur de gestion des stratégies de groupe**.
3. Dérouler **Configuration ordinateur**, **Configuration ordinateur**, **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité**, **Stratégies de comptes**, **Stratégie de mot de passe**.

Paramètres de sécurité, **Stratégies de comptes**, **Stratégie de mot de passe**.

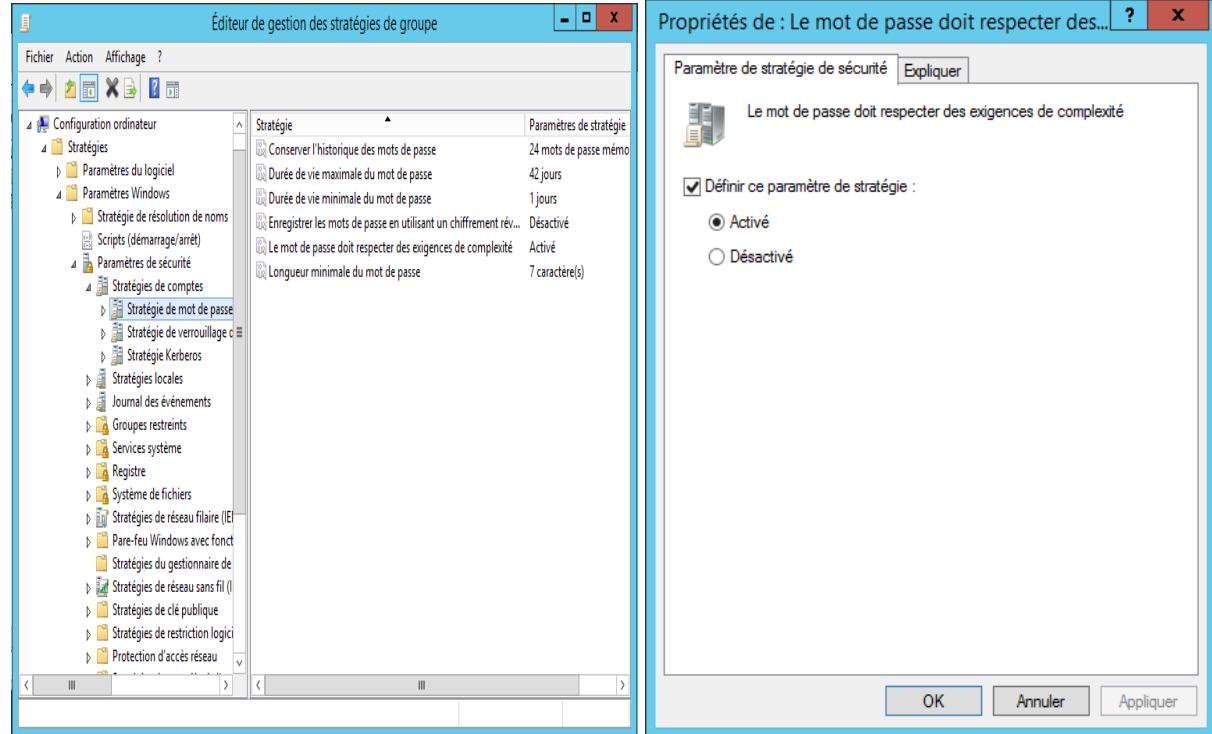


Figure 27 : interfaces *Editeur de gestion des stratégies de groupe*

■ Liste des agents créés

Il s'agit de la liste de tous les agents de la Direction générale ainsi que les agents de la DPEE. Les noms des utilisateurs sont créés comme suite :

Structure_1^{er} lettre prénom et le nom de l'agent pour faciliter l'identification de l'utilisateur sur le réseau ainsi que l'appartenance à un groupe.

The screenshot shows a Windows application window titled 'Utilisateurs et ordinateurs Active Directory'. The left pane displays a tree view of the Active Directory structure under 'dgppe.local'. The right pane is a table with three columns: 'Nom', 'Type', and 'Description'. The 'Nom' column lists user names, the 'Type' column shows they are all 'Utilisateur', and the 'Description' column provides a brief description of their role. The user 'DG_SMSENE' is selected and highlighted in blue. A VMware Tools status bar at the bottom indicates 'Press Ctrl+Alt to release the mouse cursor' and offers options to 'Install Tools', 'Remind Me Later', and 'Never Remind Me'.

Nom	Type	Description
Administrat...	Utilisateur	Compte d'utilisateur d'a...
DG_BDIOP	Utilisateur	Directeur Général
DG_DSOW	Utilisateur	Conseillère technique
DG_HDIANDY	Utilisateur	Secrétaire cordonnateur
DG_IDIENG	Utilisateur	Conseiller Technique
DG_NKA	Utilisateur	Secrétaire DG
DG_SMSENE	Utilisateur	Coordonnateur
DPEE_ABA	Utilisateur	Agent DEPE
DPEE_ADIAL...	Utilisateur	Chef de division DPMSP
DPEE_ADIOP	Utilisateur	Secrétaire DPEE
DPEE_AFall	Utilisateur	Agent DSC
DPEE_AKKO...	Utilisateur	Agent DPMSP
DPEE_ALDIOP	Utilisateur	Agent DSC
DPEE_ASEYE	Utilisateur	Secrétaire DSC
DPEE_ASNDI...	Utilisateur	Agent BAF
DPEE_ASOW	Utilisateur	Agent DPMSP
DPEE_BDIAG...	Utilisateur	Agent DEPE
DPEE_CGUEYE	Utilisateur	Agent DSC
DPEE_DDIONE	Utilisateur	Directeur DPEE
DPEE_DDIOP	Utilisateur	Agent DPMSP
DPEE_DTHIA...	Utilisateur	Agent DEPE
DPEE_FANIA...	Utilisateur	Chef de bureau BAF
DPEE_IDIAG...	Utilisateur	Agent DPMSP
DPEE_IFAYE	Utilisateur	agent DEPE
DPEE_JMAN...	Utilisateur	Agent BAF
DPEE_KSENE	Utilisateur	Aaent DSC

Figure 28 : liste des utilisateurs

▪ Horaire d'accès d'un utilisateur

Pour accéder à la configuration des horaires d'accès d'un utilisateur, faites clic droit dessus et allez dans « **Propriétés** » et dans l'onglet « **Compte** » cliquez sur « **Horaire d'accès** ».

Avant l'exécution, la configuration des horaires d'accès était sur « **Ouverture de session autorisée** » tous le temps.

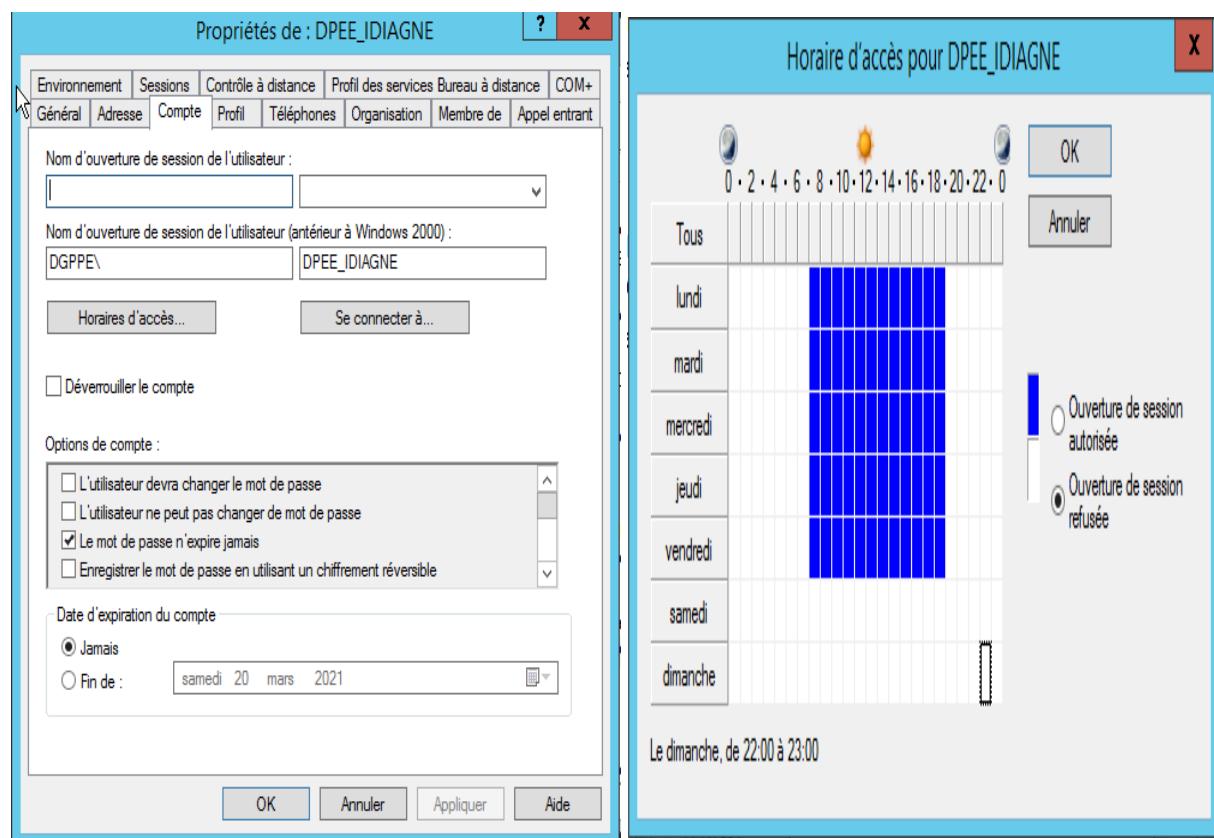


Figure 29 : horaire d'accès d'un utilisateur

■ Liste des groupes :

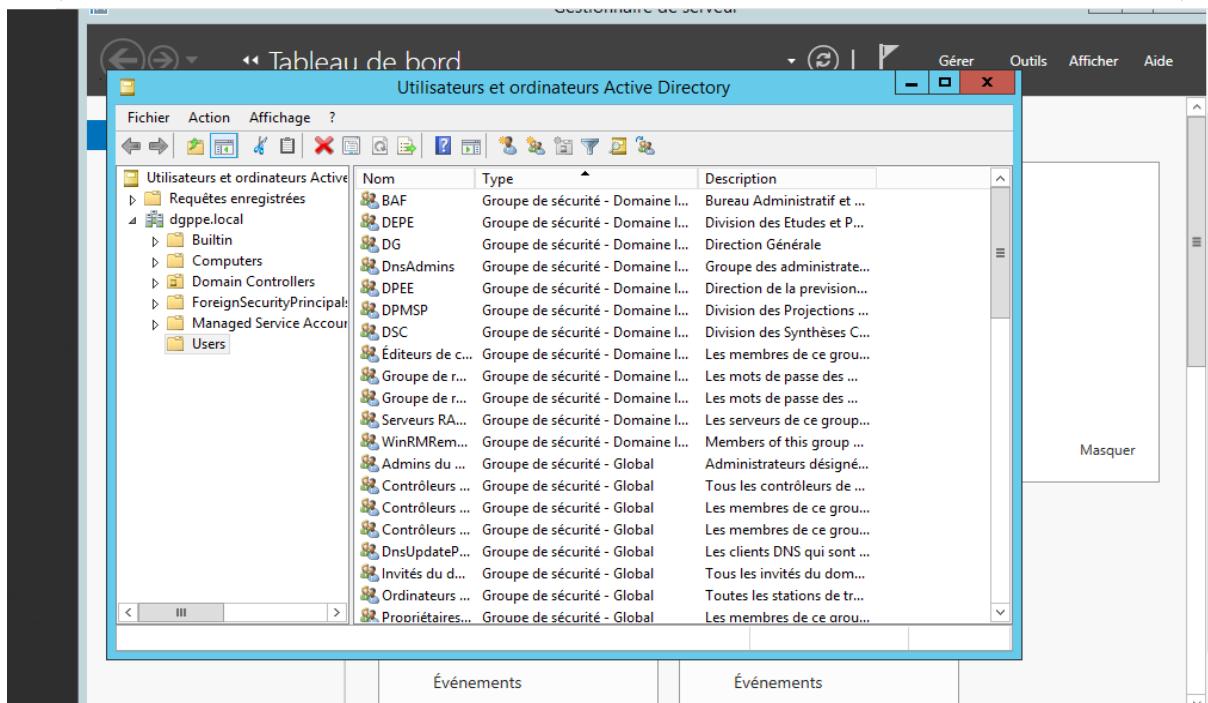


Figure 30 : liste des groupes

6.3.3 Appartenance utilisateurs aux groupes

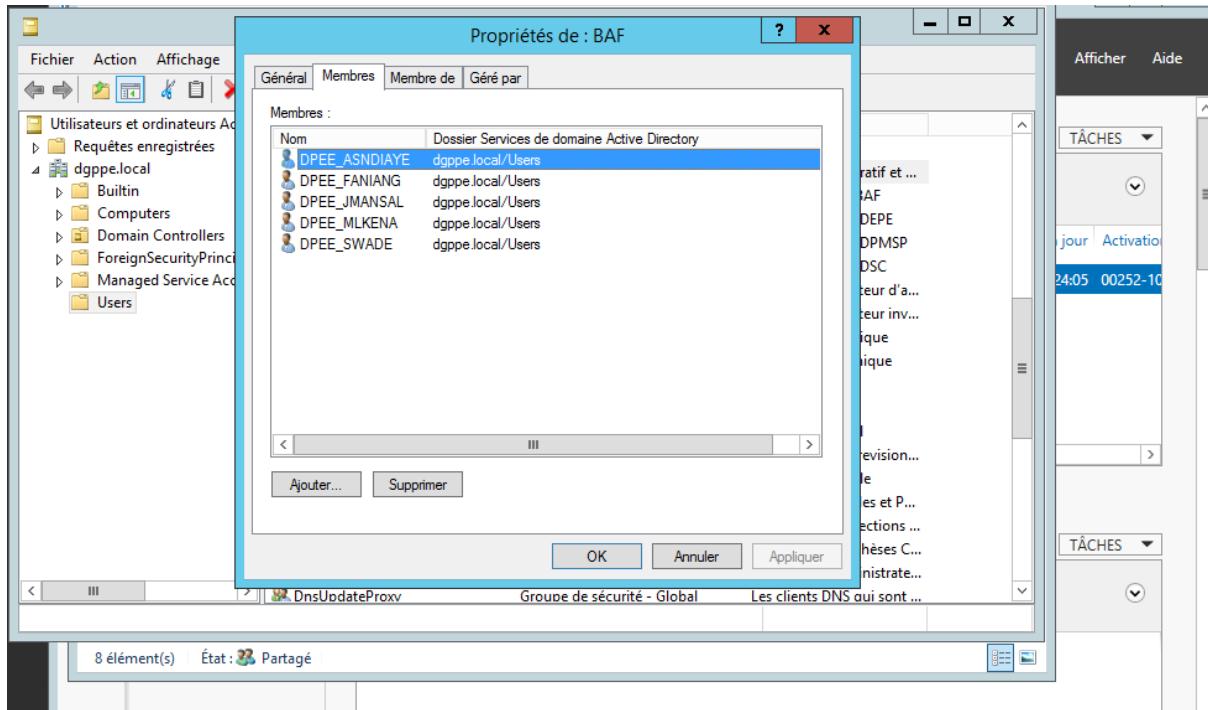


Figure 31 : détail d'un groupe (BAF)

Hiérarchie et droit accès

Groupes	Données DG	Données des Directions	Données de sa Direction	Données des Divisions	Données de sa Division
DG & Coordonnateur	<input checked="" type="checkbox"/>				
Directeur Direction	<input checked="" type="checkbox"/>				
Agent	<input checked="" type="checkbox"/>				

Tableau 14 : accès des utilisateurs selon leur hiérarchie

■ Exemple :

- ✓ Mr Bamba DIOP, le DG va avoir accès à tous les documents qui seront partagés dans toute la Direction générale, ce qui légitime conformément aux normes de l'administration.
- ✓ Mr Djibril DIONE, Directeur de la DPEE, peut lui aussi avoir accès à tous les données qui seront partagés au sein de sa Direction. Cependant, il ne pourra pas accès aux données de sa direction mère qui est la DGPPE.
- ✓ Mr Idrissa DIAGNE, agent d'une division, lui ne pourra accéder qu'aux données de sa division et aux données publiques de sa direction. Par contre il ne pourra pas accéder aux données des autres divisions.

■ Appartenance des utilisateurs

Le Directeur général appartient au groupe Direction générale

Figure 32 : profil DG

Le Directeur de la DPEE est membre du groupe DPEE.

Figure 33 : profil Directeur

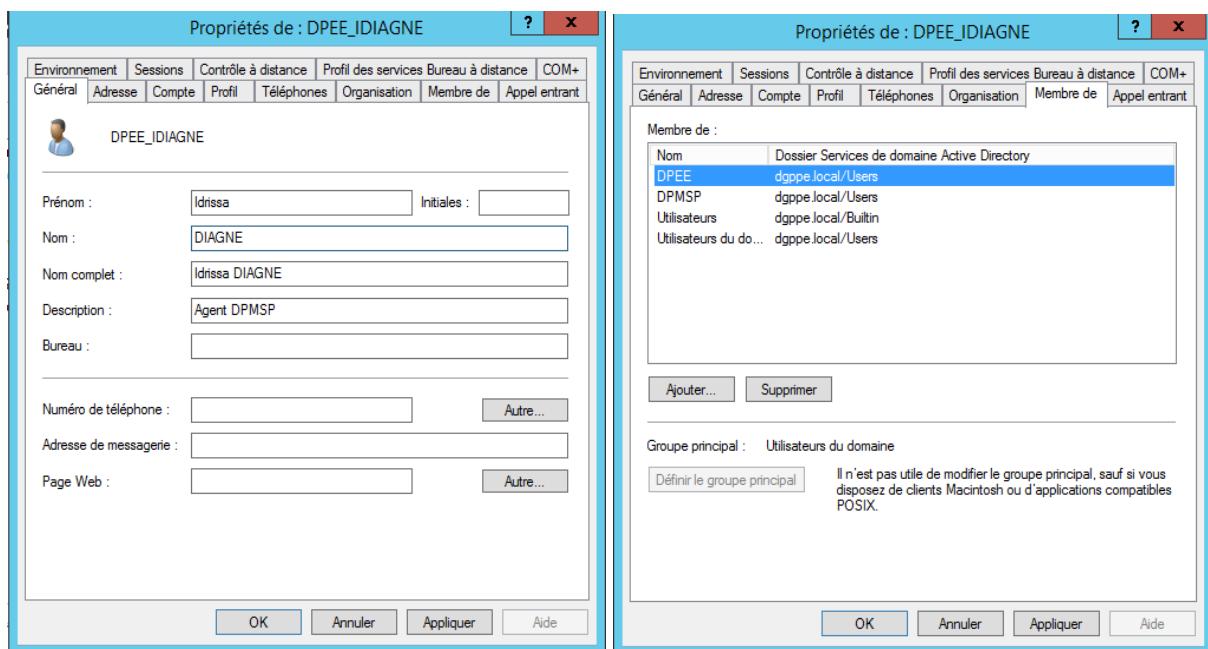


Figure 34 : profil Agent simple

6.3.4 Partage et Restriction de dossiers

6.3.4.1 Partage de dossiers

Création des dossiers

Créer ici les dossiers de chaque structure. Ces dossiers vont permettre aux utilisateurs de se partager des fichiers.

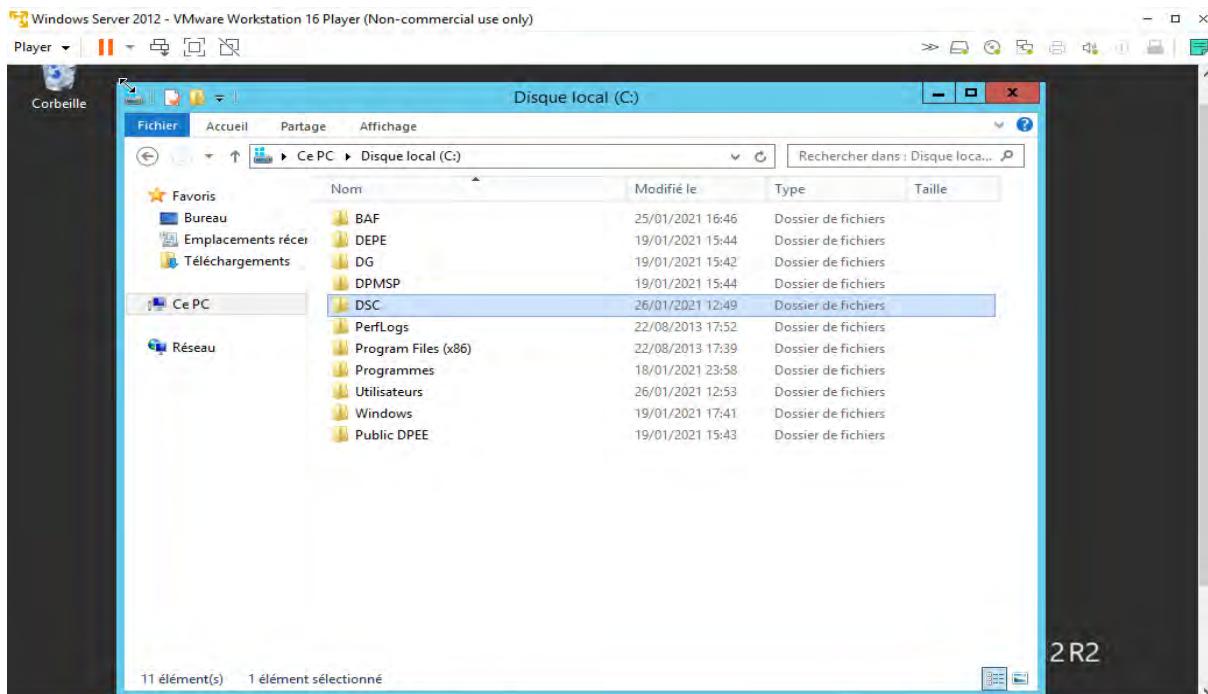


Figure 35 : création des dossiers à partager

Les dossiers ont été créés, puis seront partagés aux utilisateurs.

Pour le dossier BAF, nous allons faire le partage spécifique, et on va partager avec les groupes d'utilisateurs spécifiques ou avec tout le monde, puis on va activer la découverte réseaux pour permettre aux utilisateurs d'accéder à ce dossier via le réseau.

Pour les autres dossiers, c'est pareil, on va faire la même configuration.

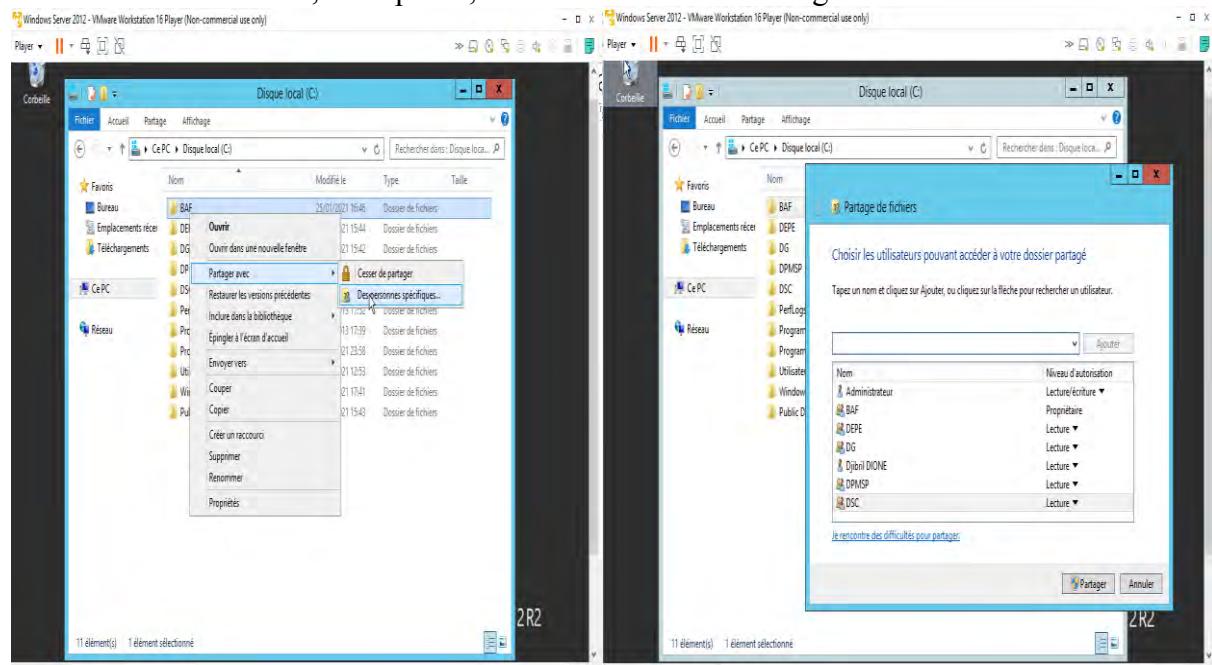


Figure 36 : partage de dossiers aux utilisateurs

■ Niveau d'accès aux dossiers partagés

Il est recommandé d'affecter aux utilisateurs les autorisations les plus restrictives tout en leur permettant d'effectuer les tâches dont ils ont besoin.

Il existe trois paramètres d'accès pour les dossiers partagés sur le serveur :

Nous allons restreindre ici l'accès des dossiers aux utilisateurs. Ceux qui auront l'accès, pourront manipuler les données de la structure concernant. Par exemple, les utilisateurs appartenant à un groupe spécifique auront le droit de **lire uniquement, lecture et écriture** ou bien de **modifier** aux données d'un groupe, est ce qu'il y a des restrictions spécifiques ou pas. Ce qu'on va voir via les permissions NTFS.

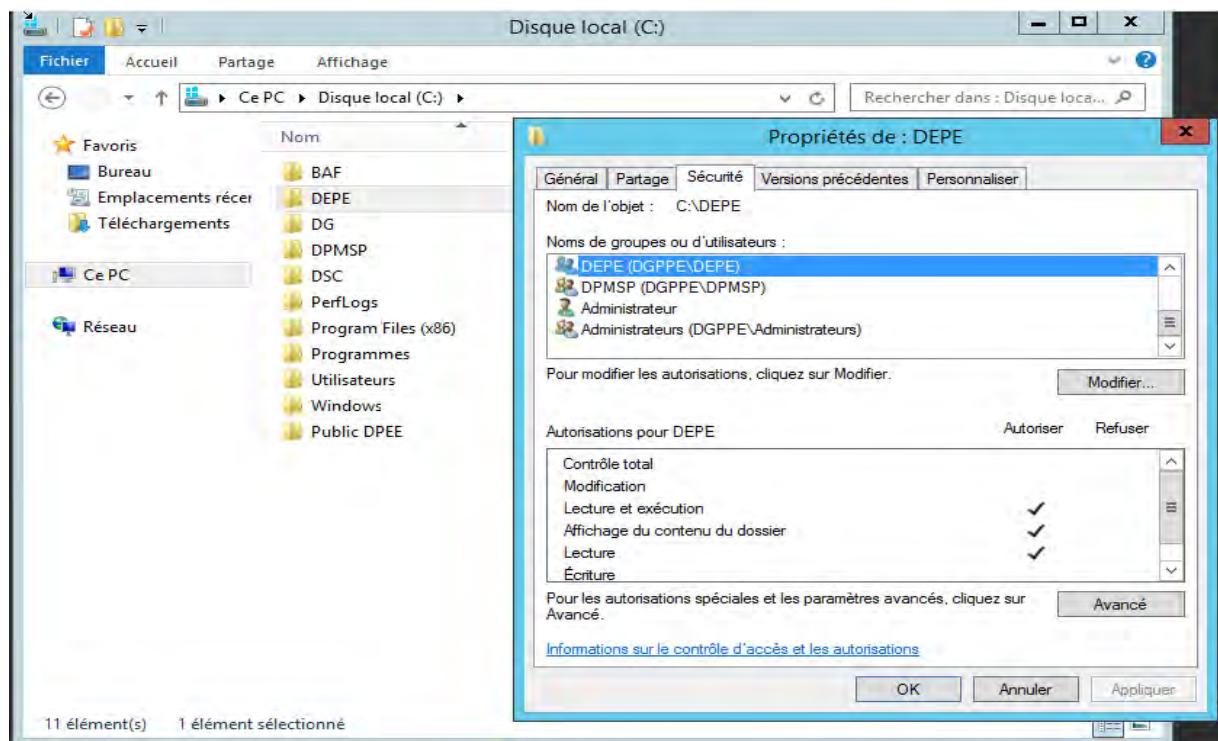


Figure 37 : vérification des restrictions du BAF

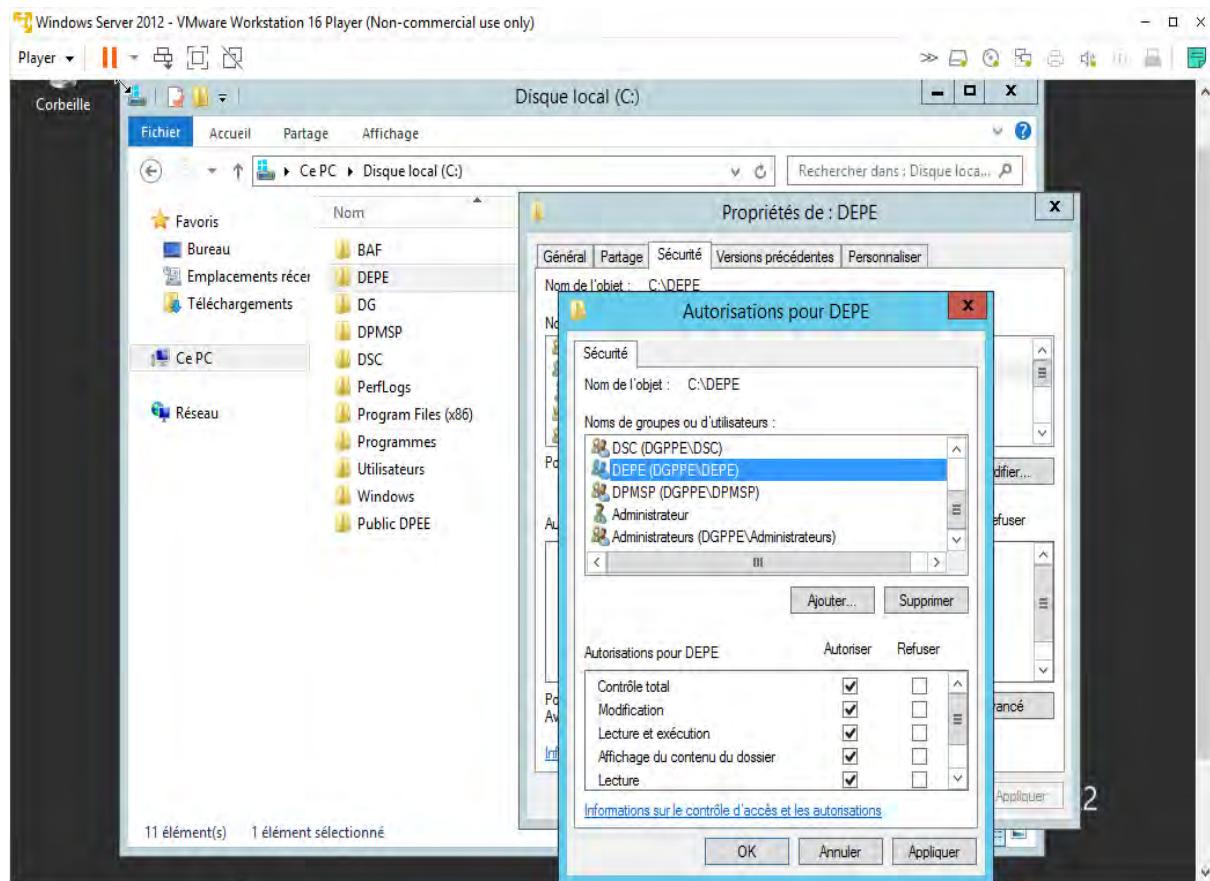


Figure 38 : allouer contrôle total à DPEE

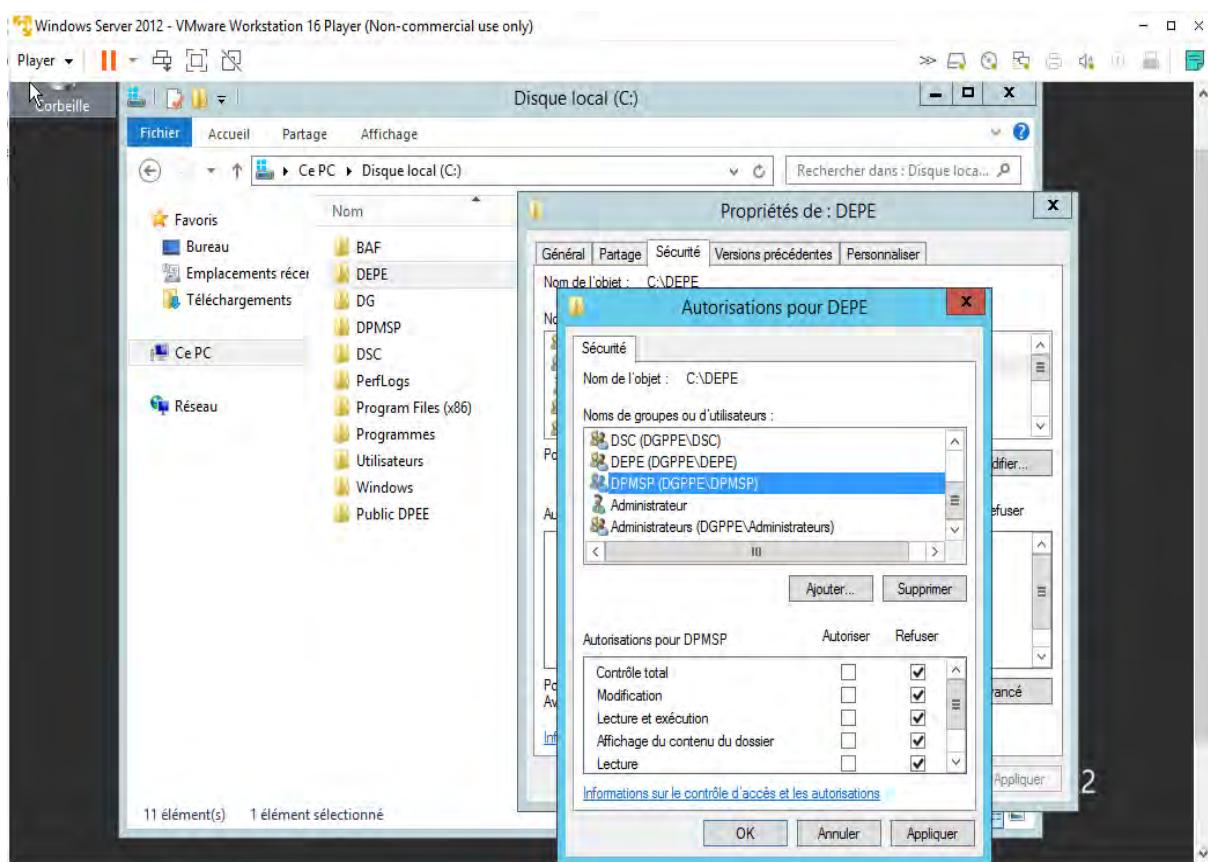


Figure 39 : refus du contrôle total des autorisations de la DPMP

On va installer le système d'exploitation Windows 10 sur VMware pour accéder au serveur via le réseau.

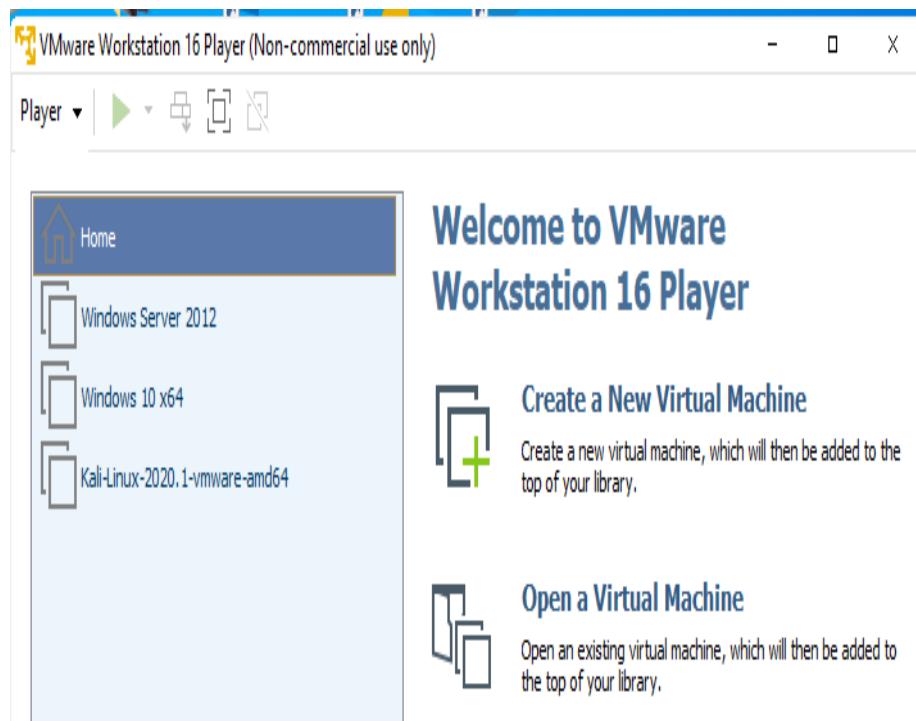


Figure 40 : installation Windows 10 sur VMware

Maintenant, à partir de notre machine Windows 10, nous allons accéder au domaine DGPPE pour se connecter en tant qu'agent de la direction.

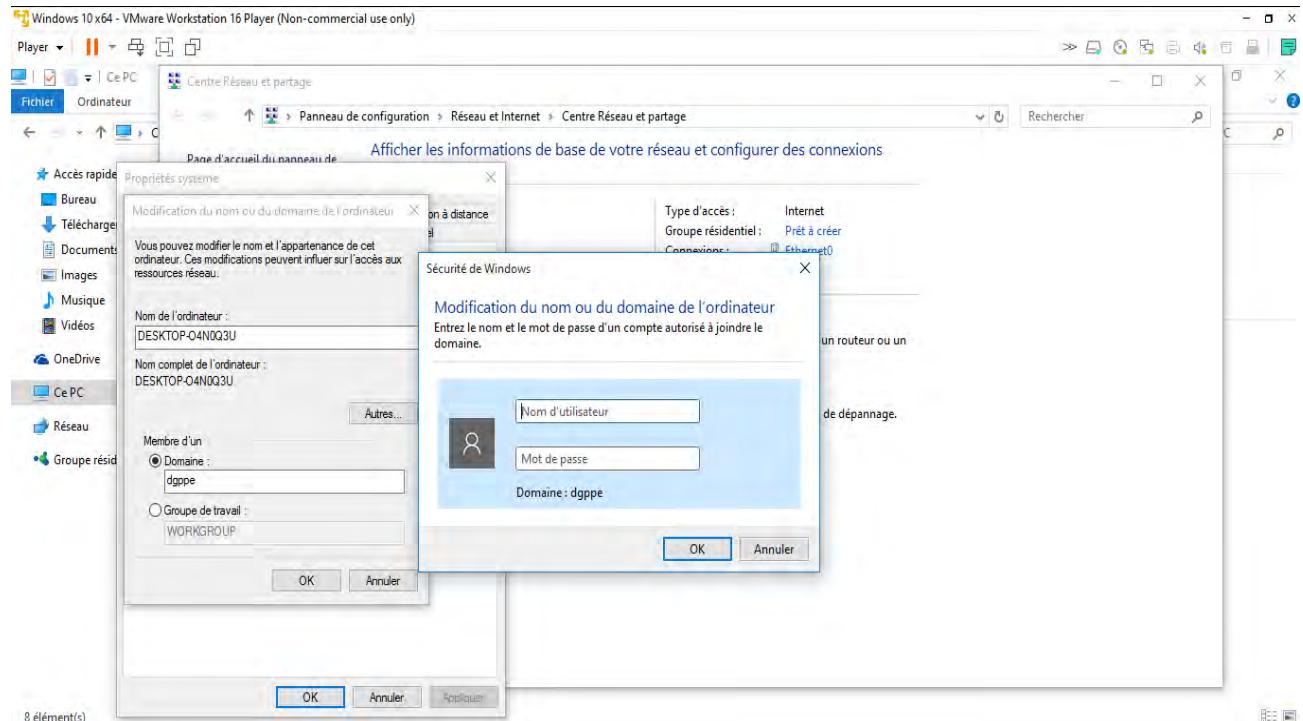


Figure 41 : interface connexion

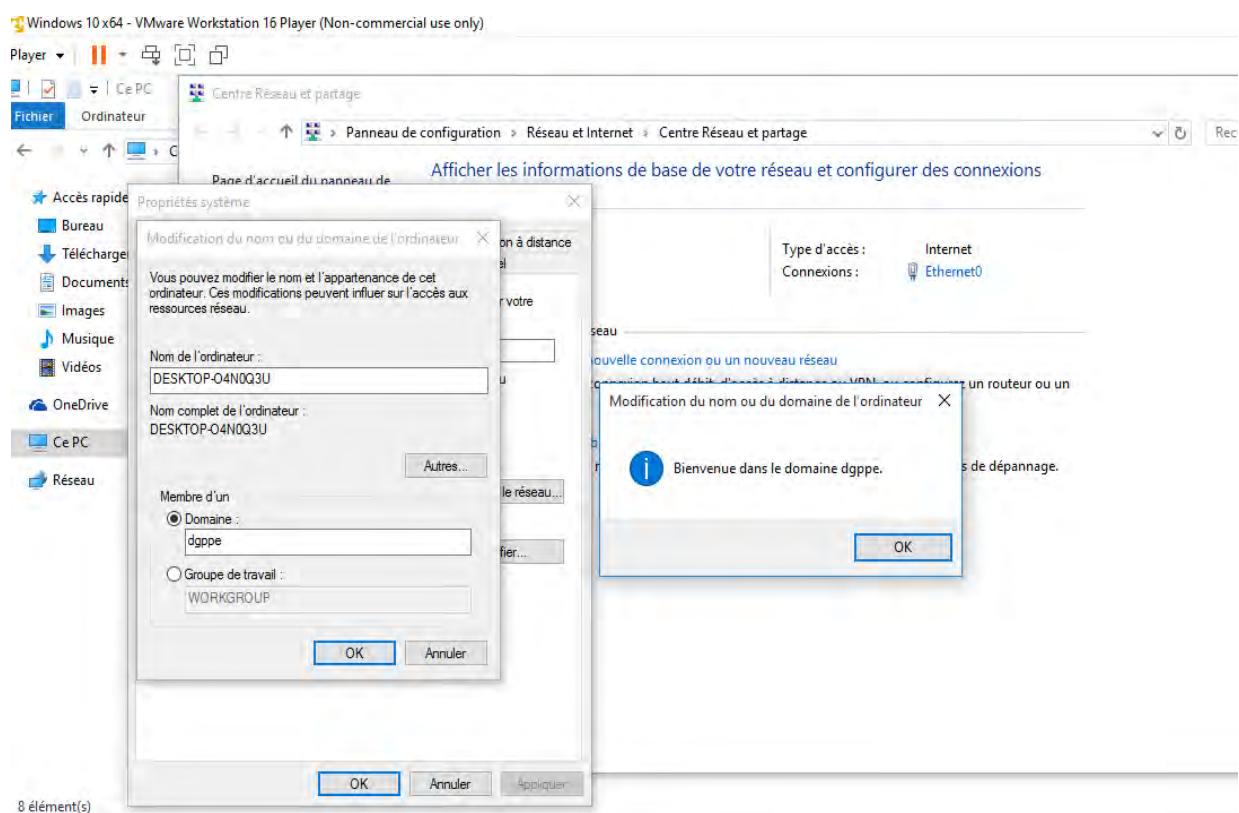


Figure 42 : connexion dans le domaine DGPPE

Maintenant nous allons nous connecter en tant qu'agent simple, en utilisant le profil de l'utilisateur Mouhamed SECK qui est un agent de division (DSC).

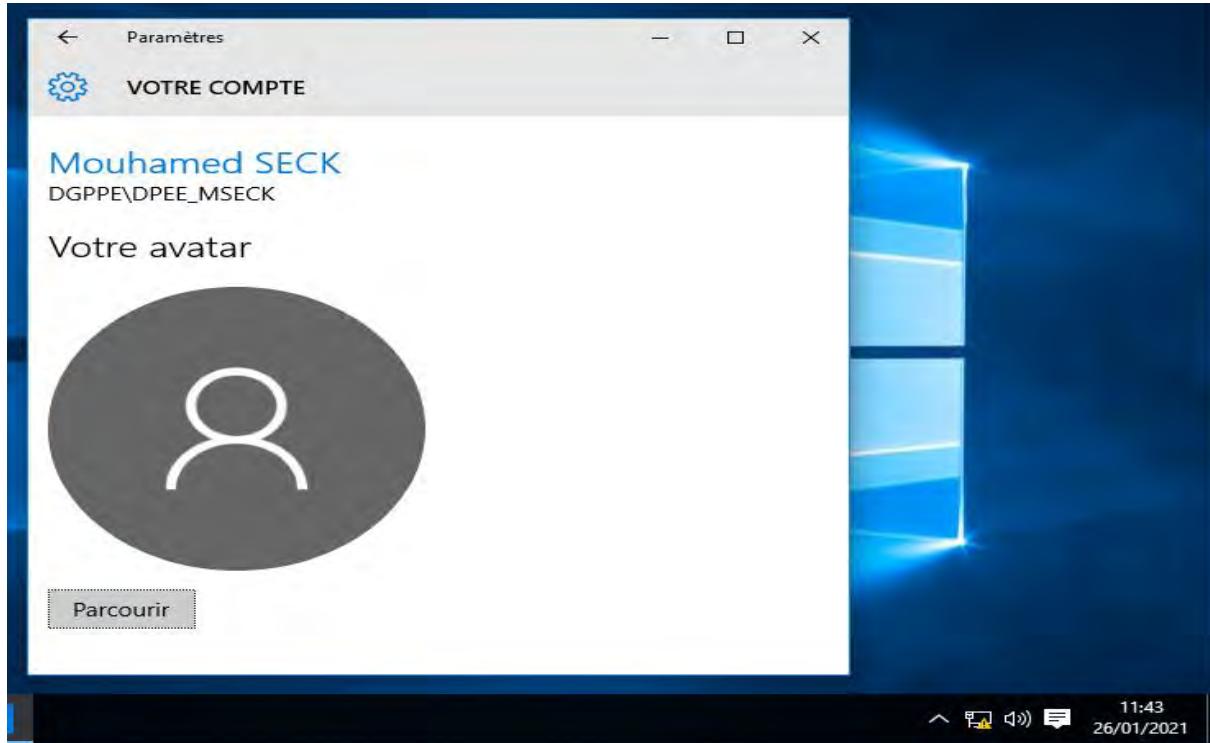


Figure 43 : profil Agent DSC

Pour accéder aux réseaux, il faut aller dans **Explorateur de fichier** avant de taper <\\WinSer> (nom du server)

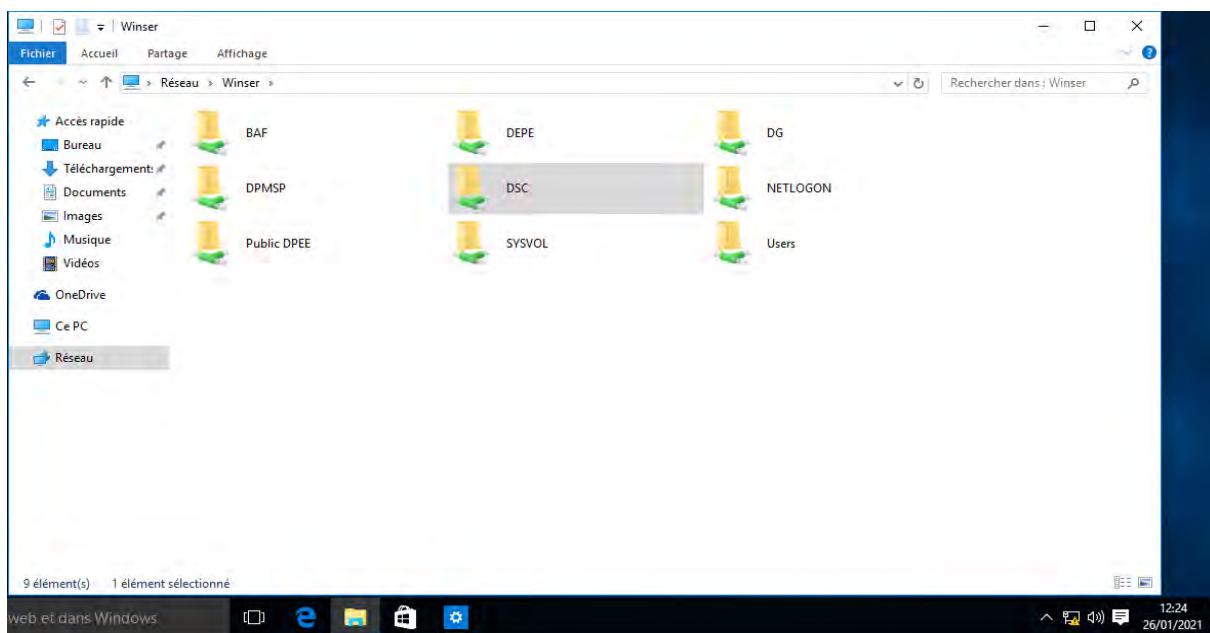


Figure 44 : aperçu des dossiers partagés

Avec le profil agent DSC, l'utilisateur n'aura accès qu'aux dossiers de sa propre division. Essayons d'entrer dans le dossier d'une autre division.

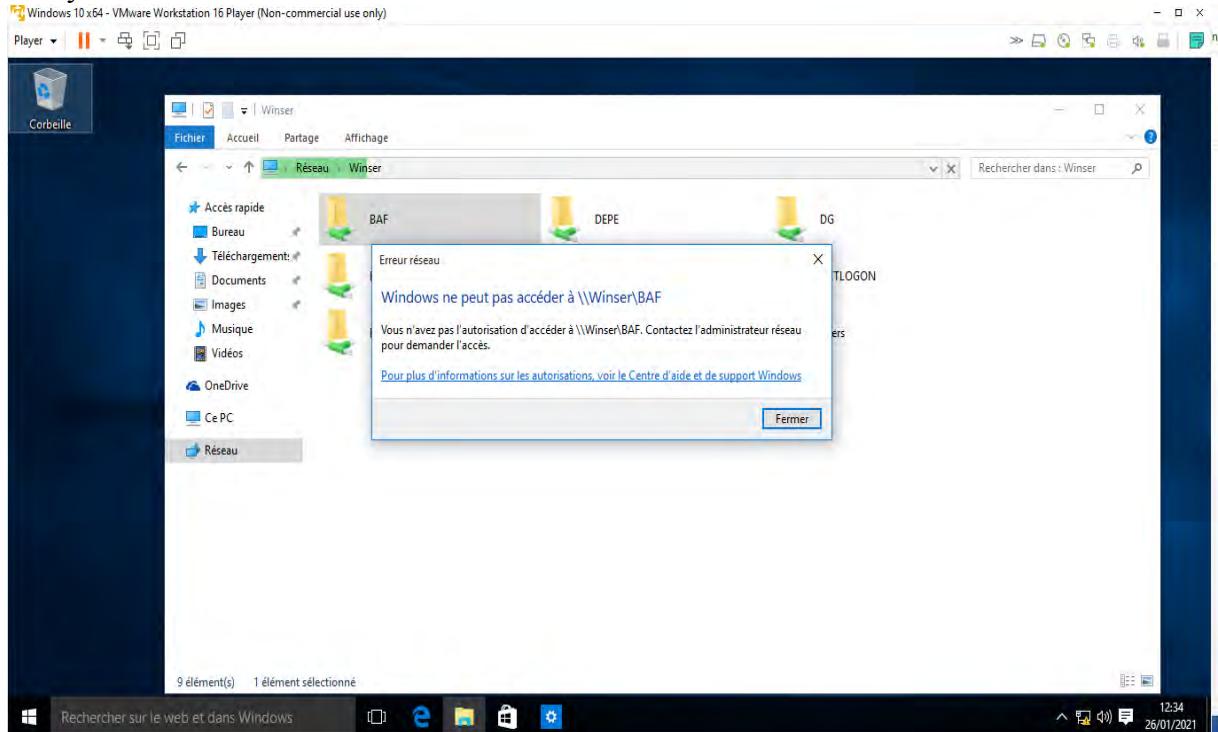


Figure 45 : refus d'accès dossier

Puis l'utilisateur va essayer d'accéder au dossier de sa propre division.

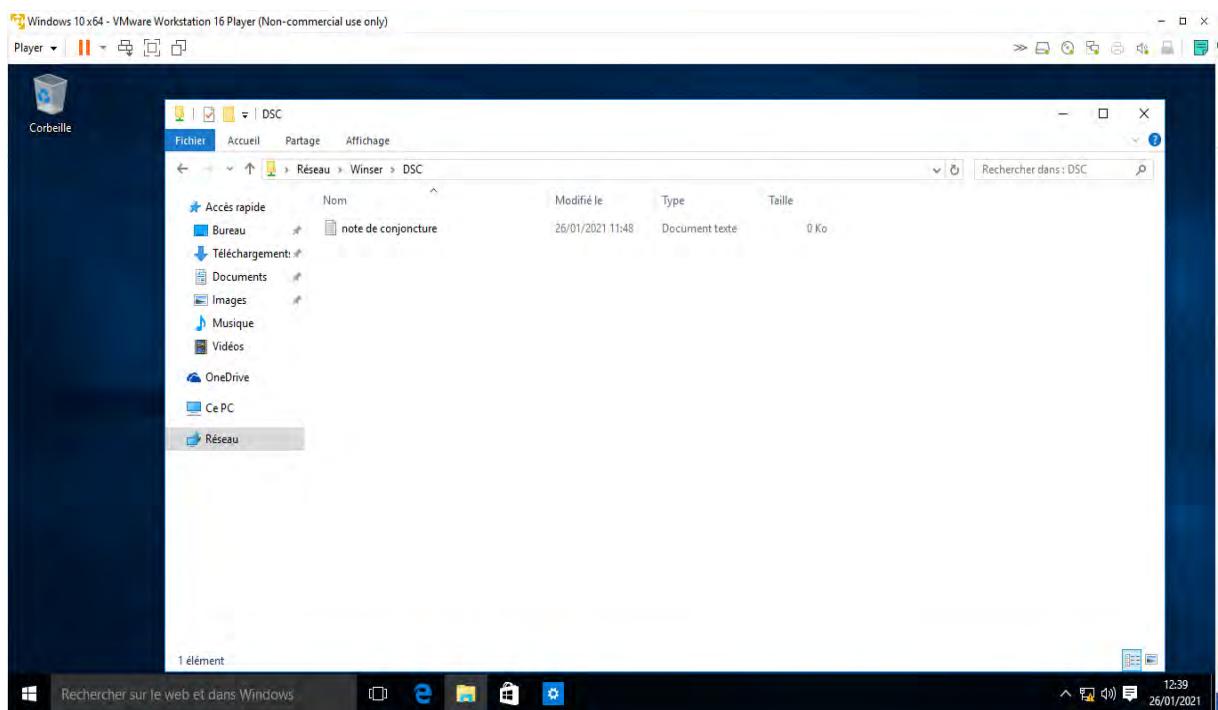


Figure 46 : accès réussi

On va connecter le dossier partagé via un lecteur pour faciliter l'accès à l'utilisateur.

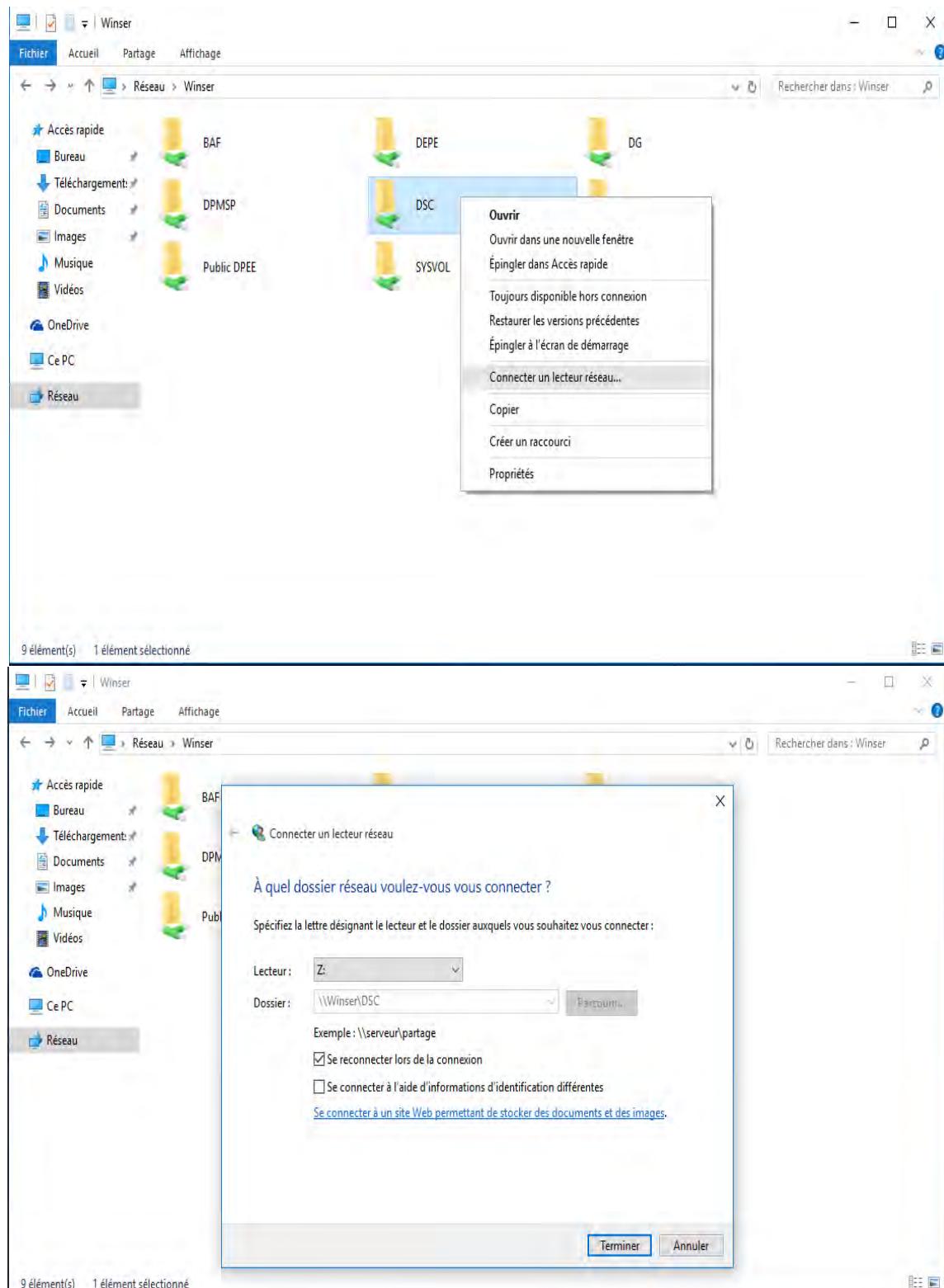


Figure 47 : connexion dossier partagé via un lecteur

Le dossier est bien ajouté.

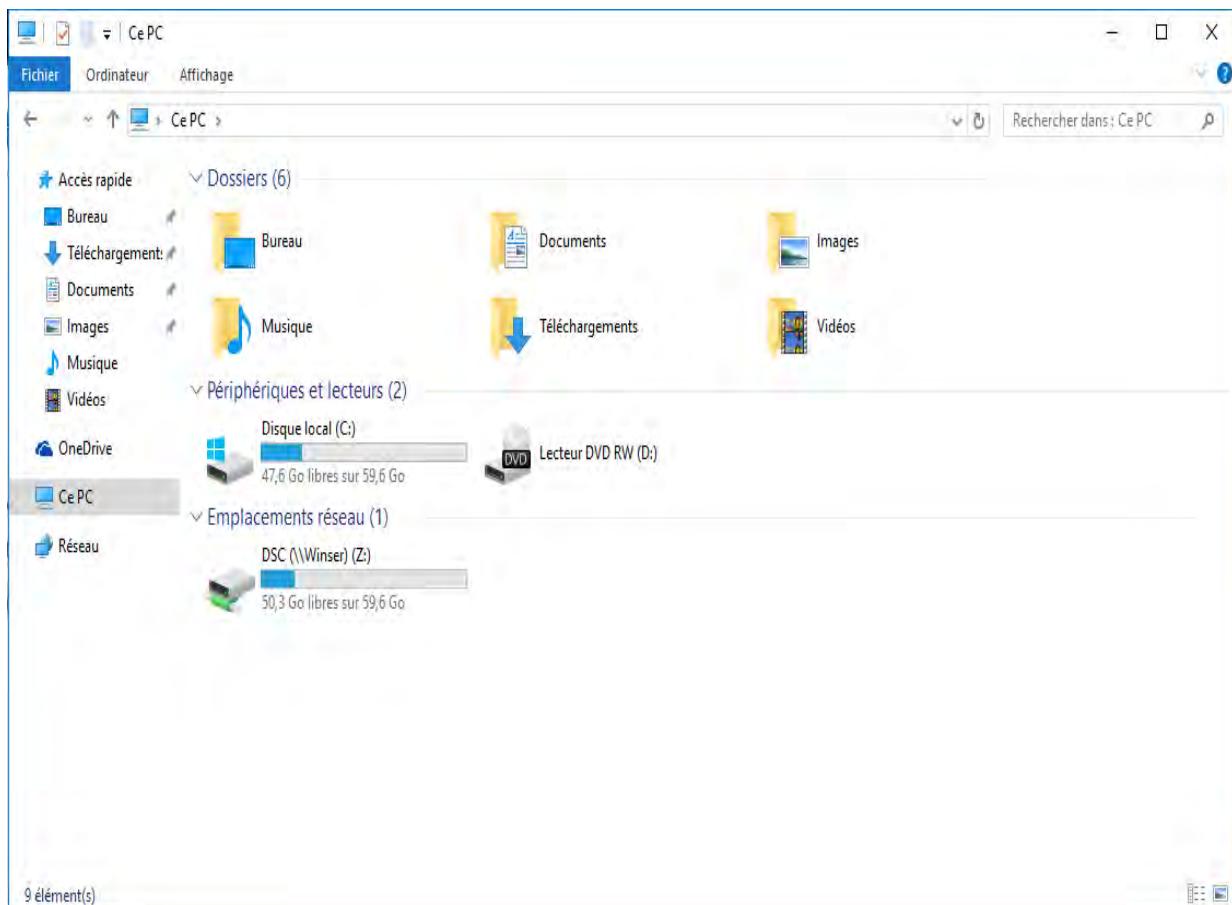


Figure 48 : aperçu d'un dossier partagé dans un lecteur

6.5 Audit des tentatives d'accès

L'audit : permet l'enregistrement d'une entrée dans le journal d'événements lorsqu'un utilisateur effectue une action (accès à une ressource, etc.).

Une entrée dans le journal de sécurité est ajoutée, indiquant l'action effectuée, le compte utilisateur associé ainsi que la date et l'heure de l'action.

6.4.1 Configuration de la politique d'audit

Il faut aller dans **Gestionnaire du server** puis dans **outils** puis **Gestion de stratégie et groupe**

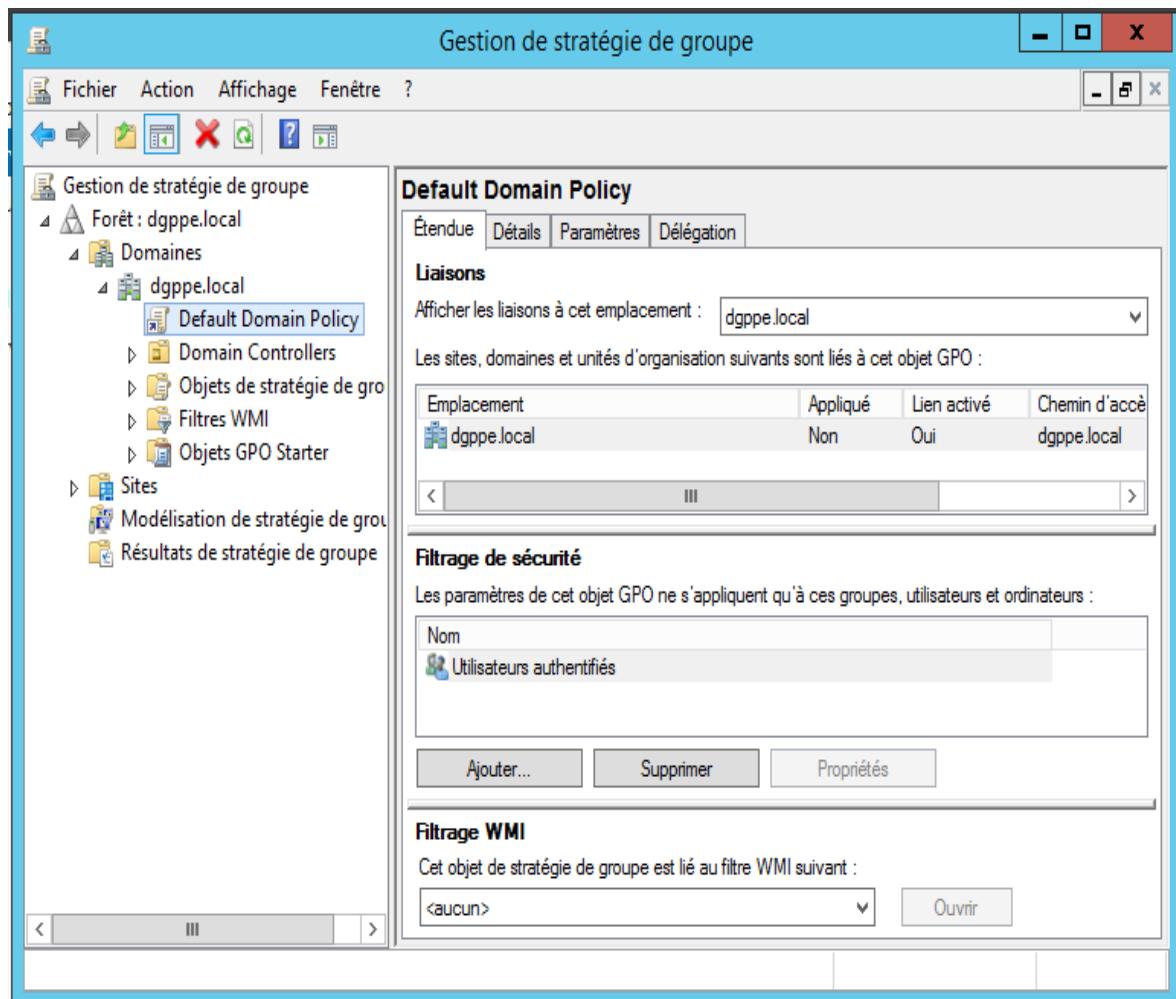


Figure 49 : gestion des stratégies de groupe

Cliquons dans **nouvel object GPO** qu'on va nommer **Audit_DGPPE**.

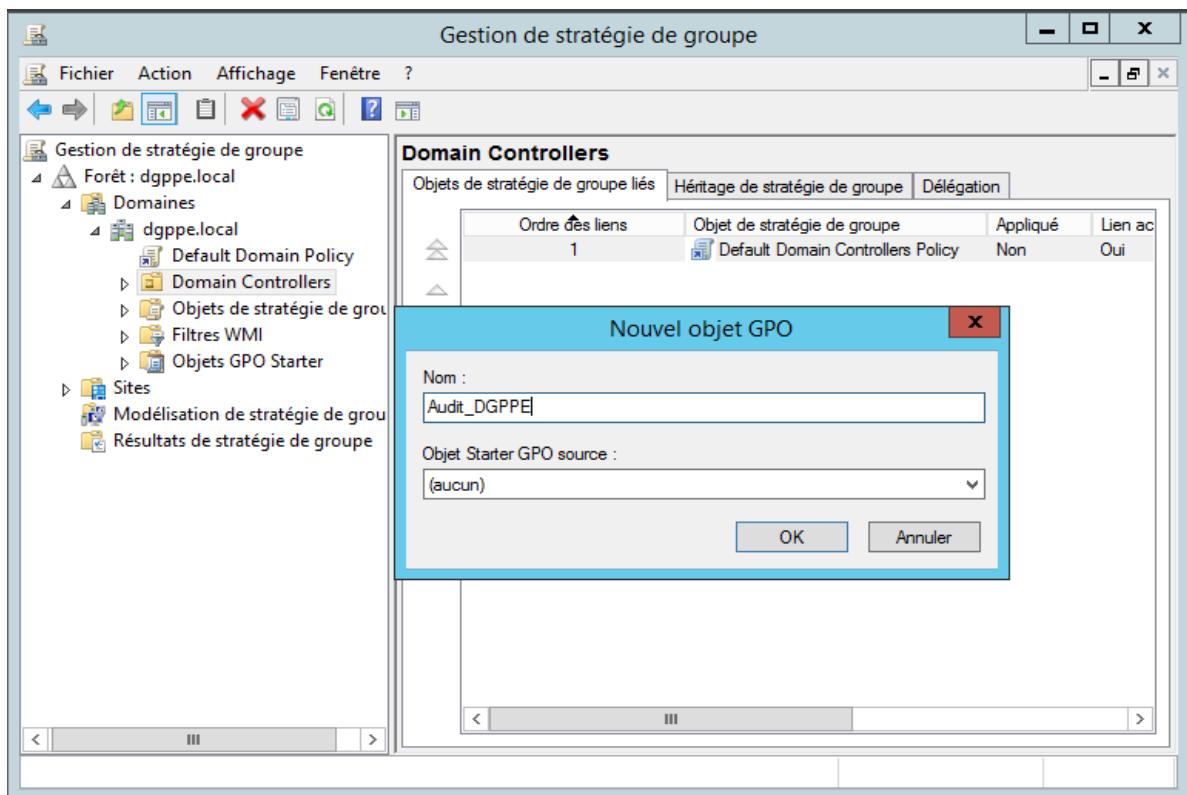


Figure 50 : création d'un nouvel objet GPO

Maintenant on peut modifier notre stratégie qu'on vient de créer :

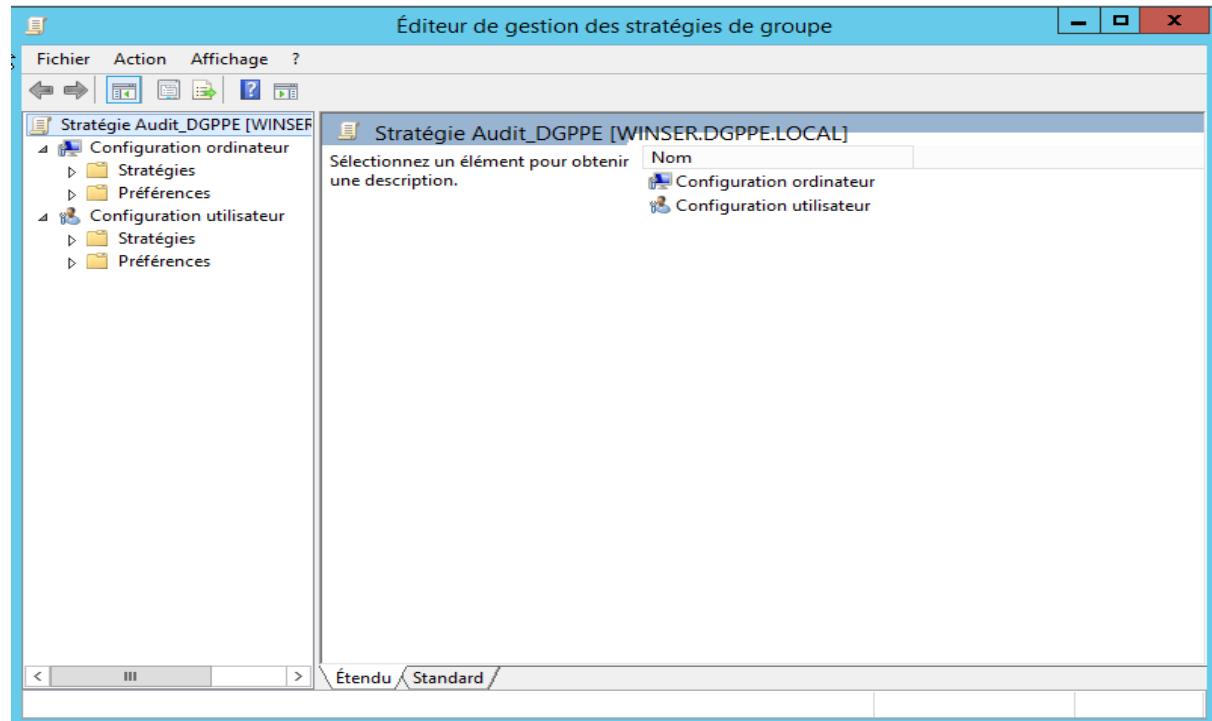


Figure 51 : éditeur de gestion des stratégies de groupe

On va dans Stratégies > paramètres Windows > Stratégie de résolution de noms puis dans paramètre de sécurité

Après dans configuration avancée de la stratégie d'audit Puis dans stratégie d'audit et là on a une liste de quelque stratégie d'audit avancé qui nous permet de faire un audit basique.

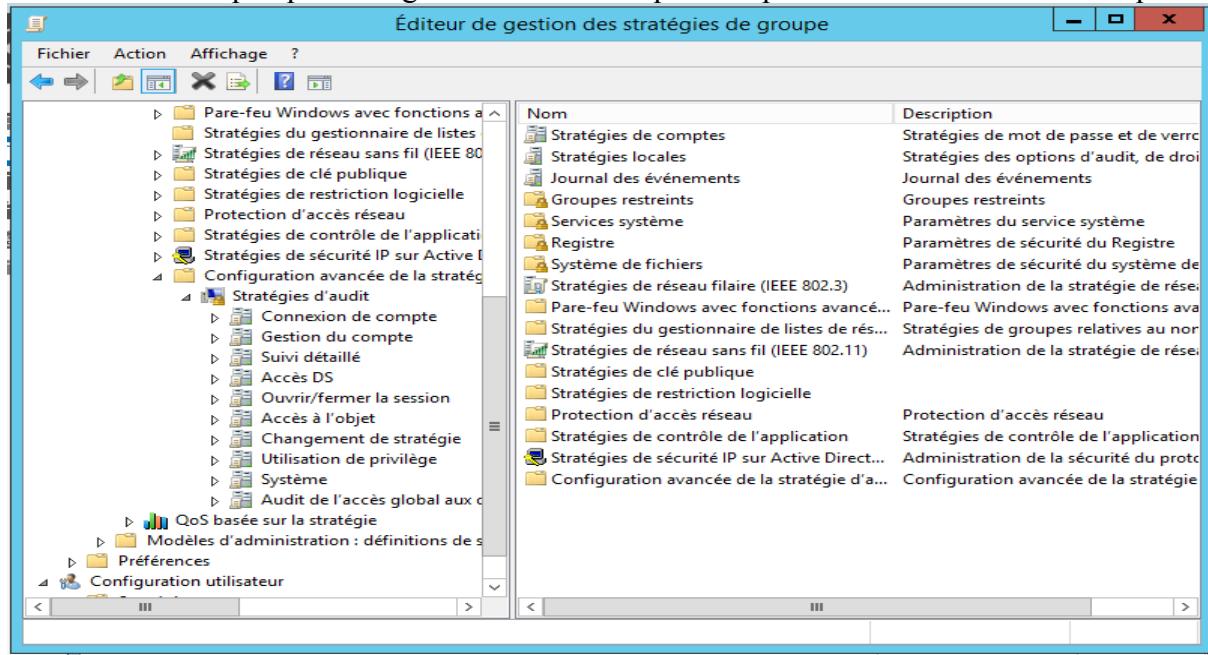


Figure 52 : éditeur de gestion de stratégies de groupe

Cliquer dans Accès à l'objet et ici sur auditer le partage de fichier détaillé, on va double-cliquer déçu :

On va auditer le partage de fichier.

Réussi veut dire auditer les tentatives d'accès réussi

Echec veut dire auditer les tentatives d'accès qui ont échoué.

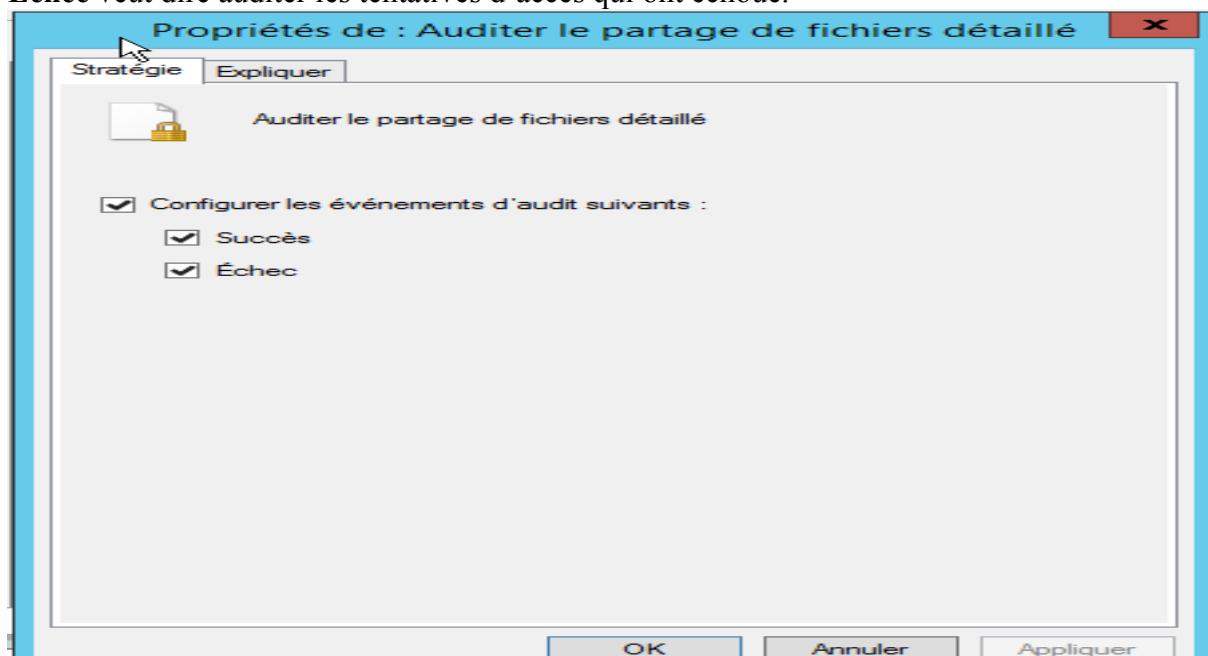


Figure 53 : propriété d'audit du partage de fichier

Donc on va mettre à jour la stratégie.

```

Gestionnaire de serveur
Administrator : Invite de commandes
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

C:\Users\Administrateur>

```

Figure 54 : aperçu invite de commande

6.4.2 Observateur d'évènements

Maintenant on va essayer d'accéder à des dossiers partagés dans le réseau.

Puis on vérifie le journal d'évènement en allant dans **journaux de Windows, puis sécurité**, avant de cliquer sur **sécurité** pour voir les évènements.

Echec :

Mots clés	Date et heure	Source	ID de l'événement	Catégorie
Échec de l'audit	24/01/2021 22:26:21	Micros...	4625	Ouvrir l...
Échec de l'audit	24/01/2021 22:25:28	Micros...	4625	Ouvrir l...
Échec de l'audit	19/01/2021 11:06:23	Micros...	4625	Ouvrir l...
Échec de l'audit	24/01/2021 22:26:28	Micros...	4625	Ouvrir l...

Figure 55 : évènement des audits échoués

Succès

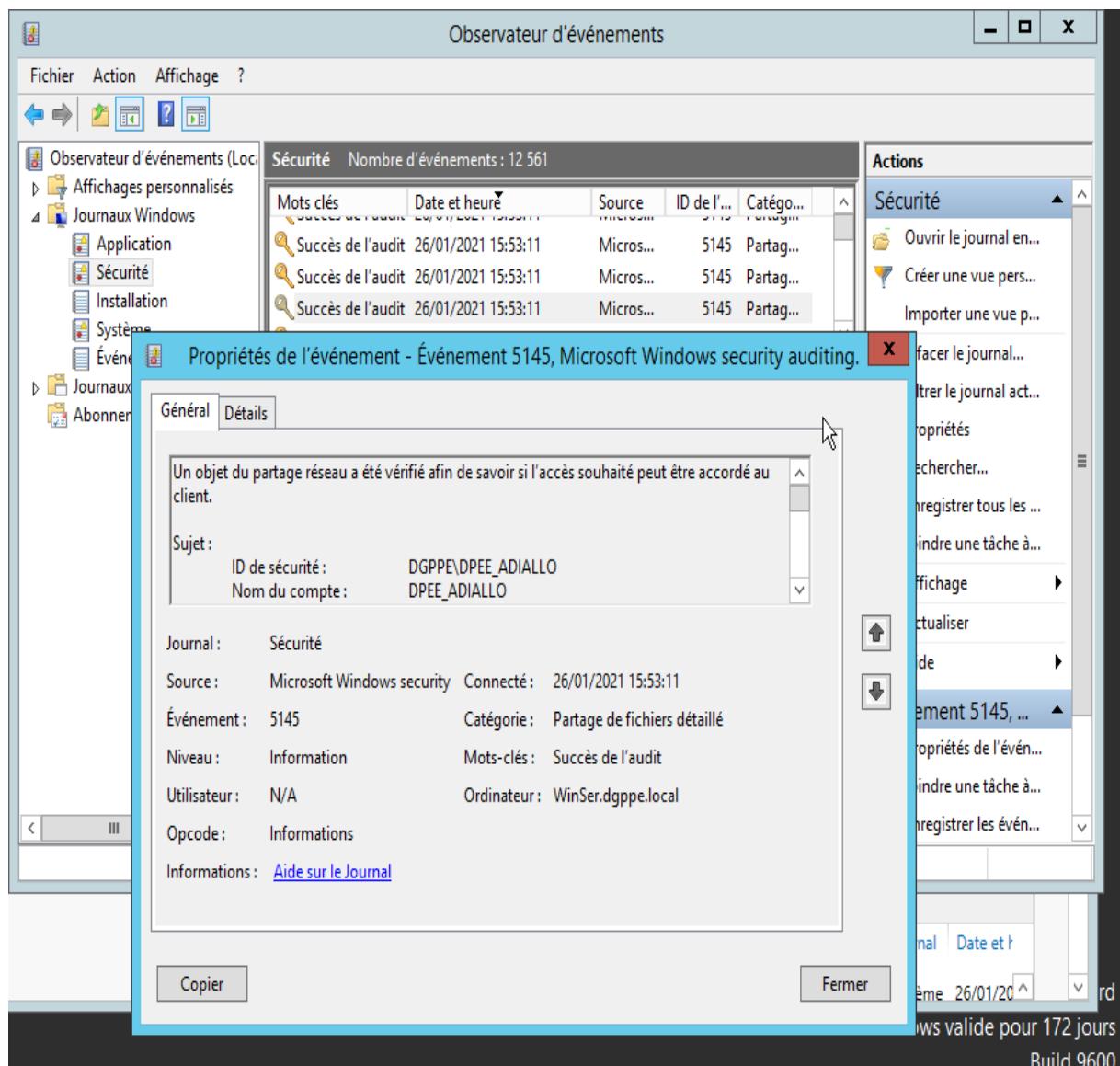


Figure 56: propriétés de l'événement de l'utilisateur Alassane DIALLO

6.6 Sauvegarde et restauration

Peu importe que vous perdiez vos données en raison d'une défaillance mécanique, d'une catastrophe naturelle ou d'une attaque criminelle, le résultat est le même. Toutefois, les données ne sont pas vouées à être perdues. Vous pouvez les sauvegarder et restaurer.

6.5.1 Sauvegarde

La sauvegarde est un processus unique qui consiste à copier des fichiers et des dossiers d'un emplacement vers un autre. La sauvegarde régulière des données sur les disques durs des ordinateurs serveurs et clients évite les pertes de données dues aux défaillances des disques durs, aux coupures de courant, aux infections par les virus et aux autres incidents de ce type. En cas de perte de données, si vous avez effectué des sauvegardes régulières selon un planning scrupuleux, vous pouvez restaurer les données perdues, que cette perte concerne un seul fichier ou tout un disque dur.

❖ Types de données à sauvegarder

En matière de sauvegarde, la règle générale est la suivante : si vous ne pouvez pas vous en passer, faites-en une sauvegarde.

Les données critiques sont les informations dont votre organisation a besoin pour suivre. Si des fichiers sont accidentellement perdus ou endommagés, vous pouvez utiliser la sauvegarde la plus récente pour restaurer ces données.

Les données sur l'état du système définissent la configuration du système d'exploitation du serveur. Si des modifications accidentnelles se produisent ou si des données sur l'état du système sont perdues, vous pouvez les restaurer à partir d'une sauvegarde.

❖ Fréquence des sauvegardes

Les facteurs suivants déterminent la fréquence des sauvegardes :

- Quelle est l'importance des données pour l'organisation ? Vous devez sauvegarder les données critiques plus souvent que les données de moindre importance.
- Quelle est la fréquence de modification des données ? Par exemple, si les utilisateurs créent ou modifient des rapports uniquement les vendredis, une sauvegarde hebdomadaire de ces fichiers est suffisante.

❖ Conditions d'utilisation d'une sauvegarde réseau

Exécutez une sauvegarde réseau lorsque les données critiques sont stockées sur plusieurs serveurs. Le tableau suivant décrit les avantages et les inconvénients d'une sauvegarde réseau.

Avantages	Inconvénients
Elle sauvegarde le réseau entier.	Les utilisateurs doivent copier leurs fichiers importants sur les serveurs.
Elle nécessite moins d'espace de stockage.	Elle ne peut pas sauvegarder le Registre sur les ordinateurs distants.
Elle requiert moins de supports à gérer.	Elle augmente le trafic réseau.
Un utilisateur peut sauvegarder des données.	Elle requiert plus de planification et de préparation.

Tableau 15 : avantages et inconvénients d'une sauvegarde réseau

• Configuration sauvegarde

Installation utilitaire de sauvegarde sur Active Directory. On clique dans Ajouter **rôles et fonctionnalités**, suivant, on sélectionne notre serveur puis on sélectionne la fonctionnalité **sauvegarde Windows server** :

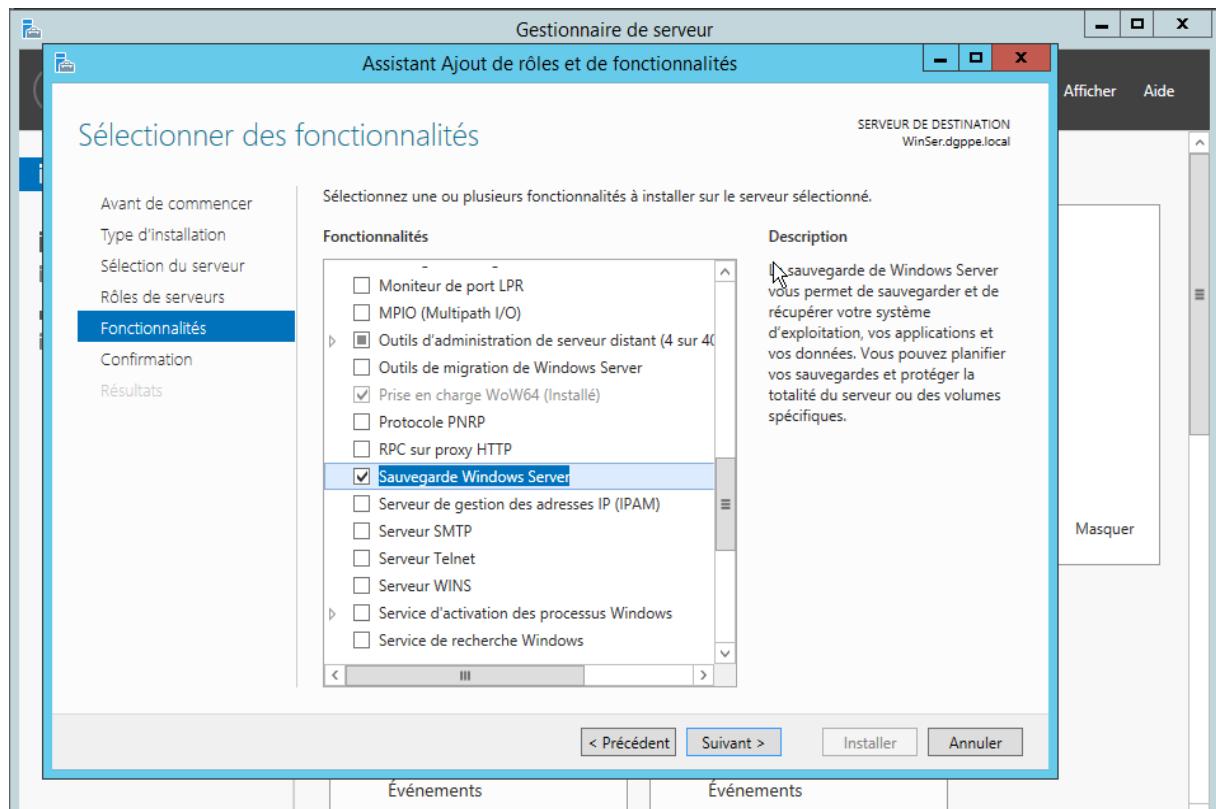


Figure 57 : ajout fonctionnalité Sauvegarde Windows Server

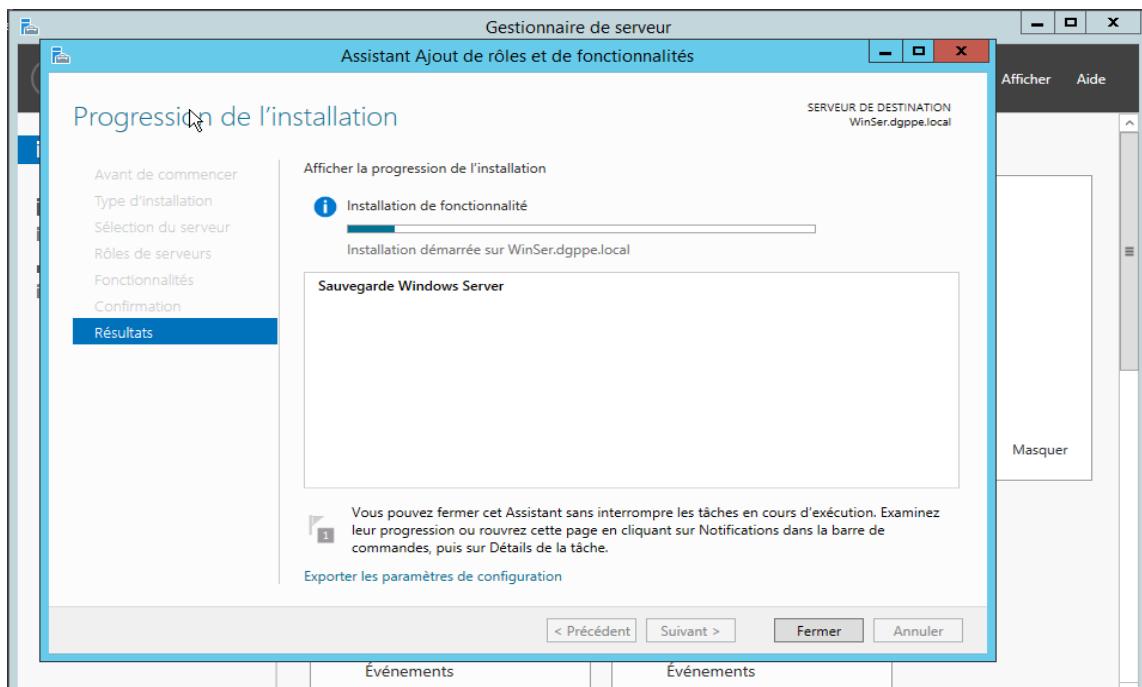


Figure 58 : installation en cours de la fonctionnalité Sauvegarde Windows Server

Donc l'installation de cette fonctionnalité, on va accéder à la console de gestion, à savoir la console sauvegarde Windows Server.

Ci-dessous l'interface sur laquelle on va configurer la sauvegarde.

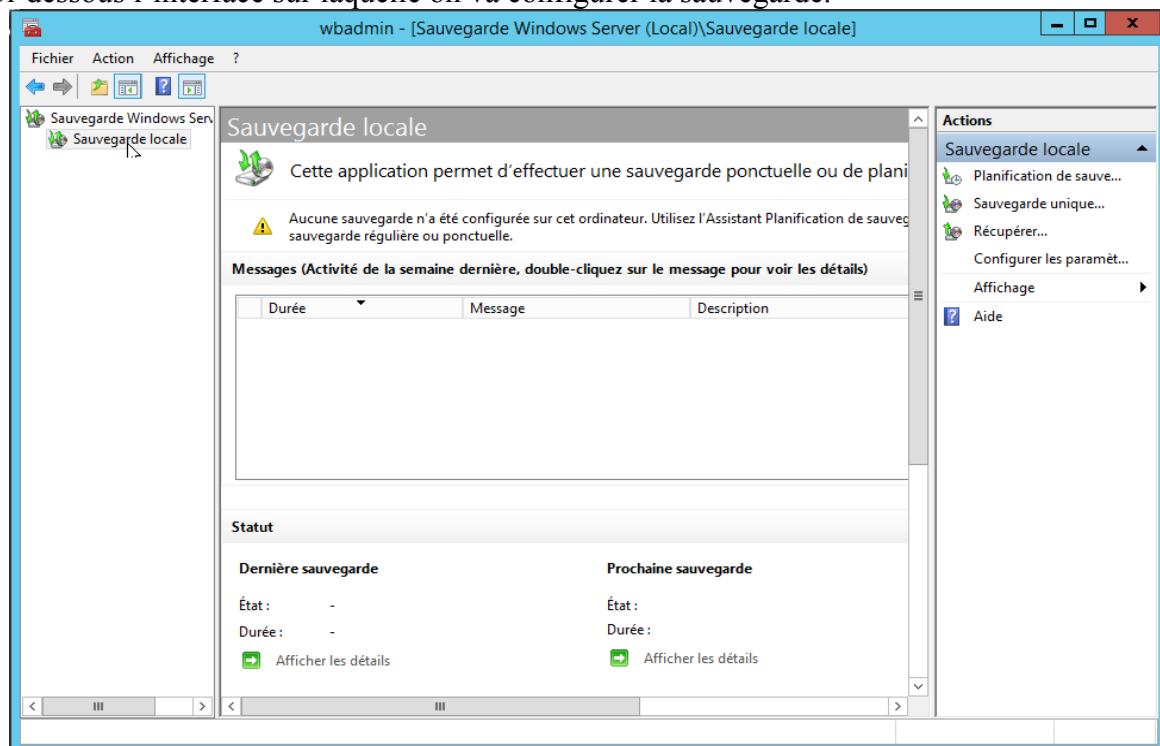


Figure 59 : interface sauvegarde et restauration Windows Server

Maintenant on va sauvegarder les dossiers partagés.

Il y'a 2 façons de faire la sauvegarde : soit la sauvegarde planifiée, soit la sauvegarde manuelle. Nous, on va planifier notre sauvegarde.

La planification de sauvegarde veut juste dire qu'on va choisir une journée sur laquelle on va procéder notre sauvegarde de notre système, fichiers, données ou de notre Active Directory.

On clique sur Planification de sauvegarde, puis personnalisé la sauvegarde pour spécifier les dossiers qu'on souhaite sauvegarder.

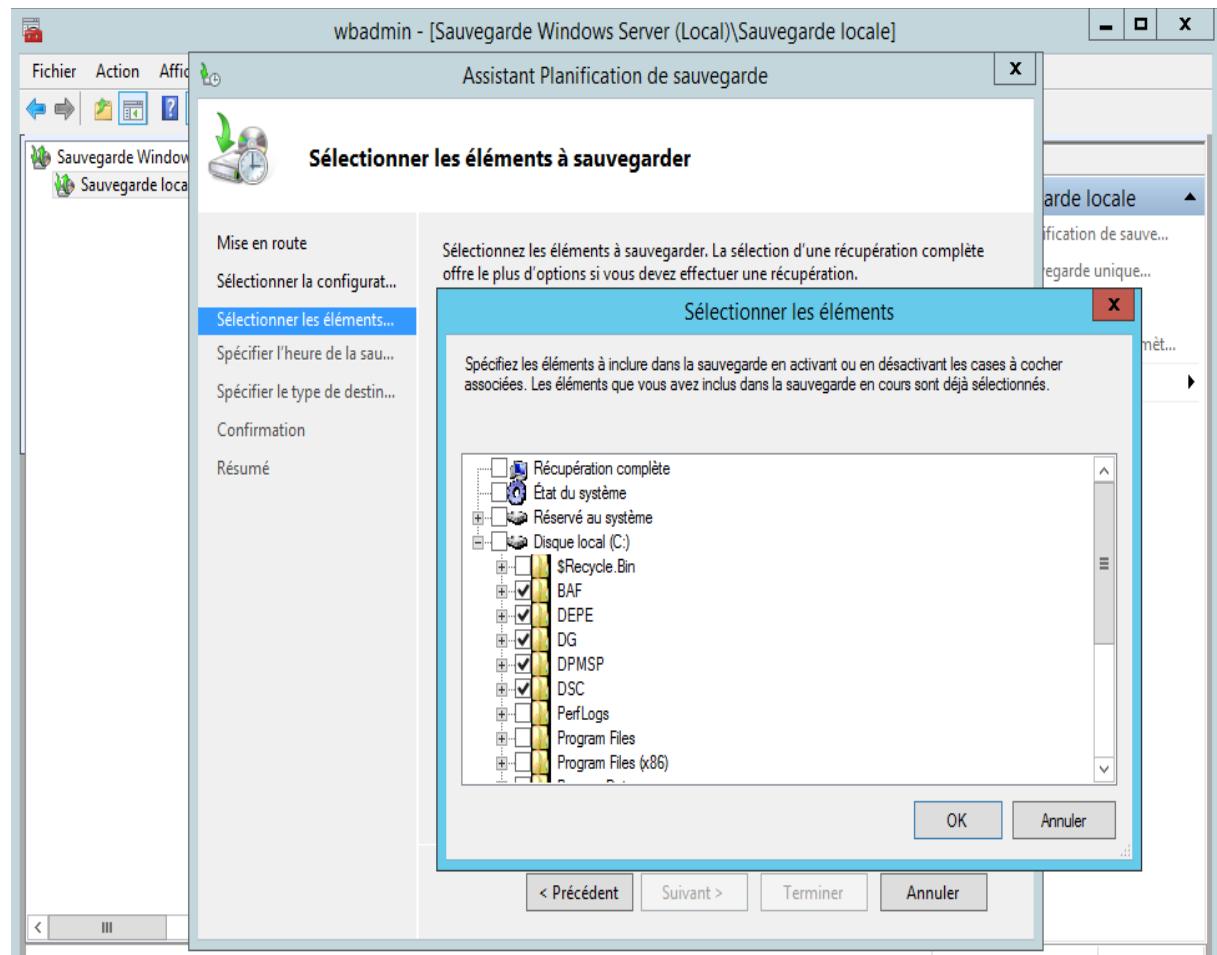


Figure 60 : aperçu des dossiers sélectionnés pour la sauvegarde

Et puisque c'est une planification de sauvegarde, on va choisir 23h comme heure, pour tous les jours :

Sauvegarde Windows Server utilise le Service VSS (Volume Shadow Copy Service) de trois façons différentes.

- Lorsque qu'on lance une sauvegarde complète.
- Sauvegarde Windows Server lance des sauvegardes incrémentielles au niveau des blocs qui consistent uniquement à lire les blocs modifiés du volume source.
- Si vous sauvegardez un volume particulièrement on utilise donc custom

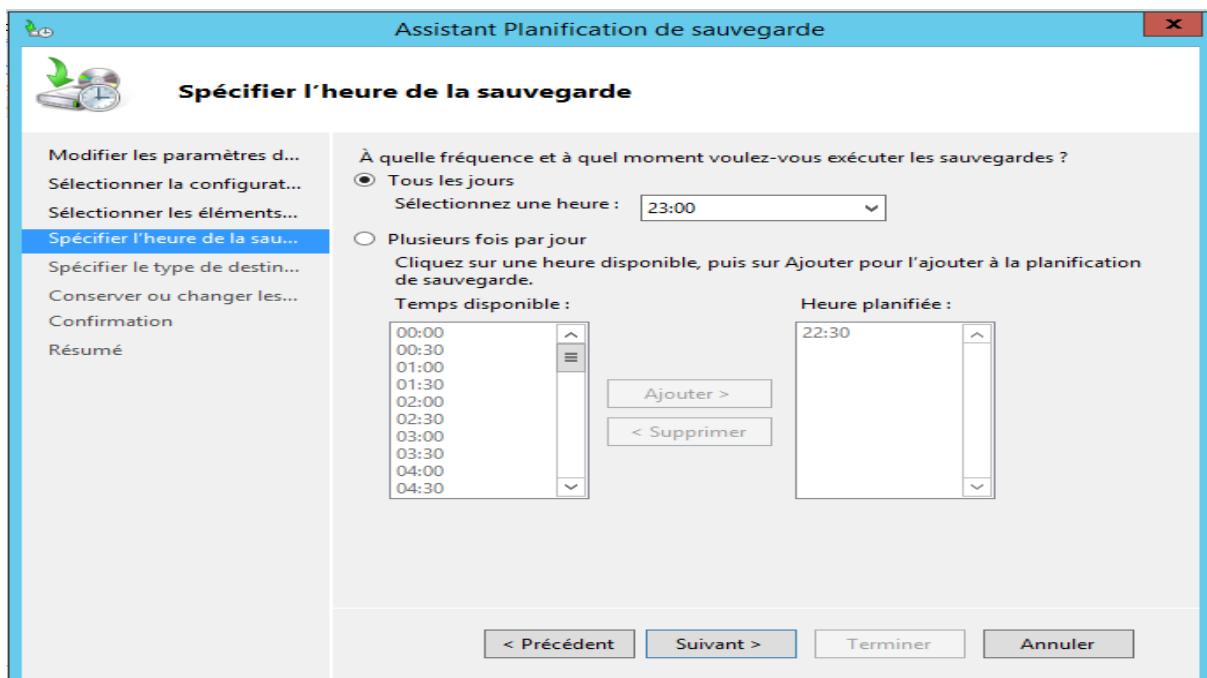


Figure 61 : aperçu du choix de l'heure de sauvegarde

Puis pour le type de destination, on choisit la sauvegarde vers un **disque dur dédié** (recommandé).

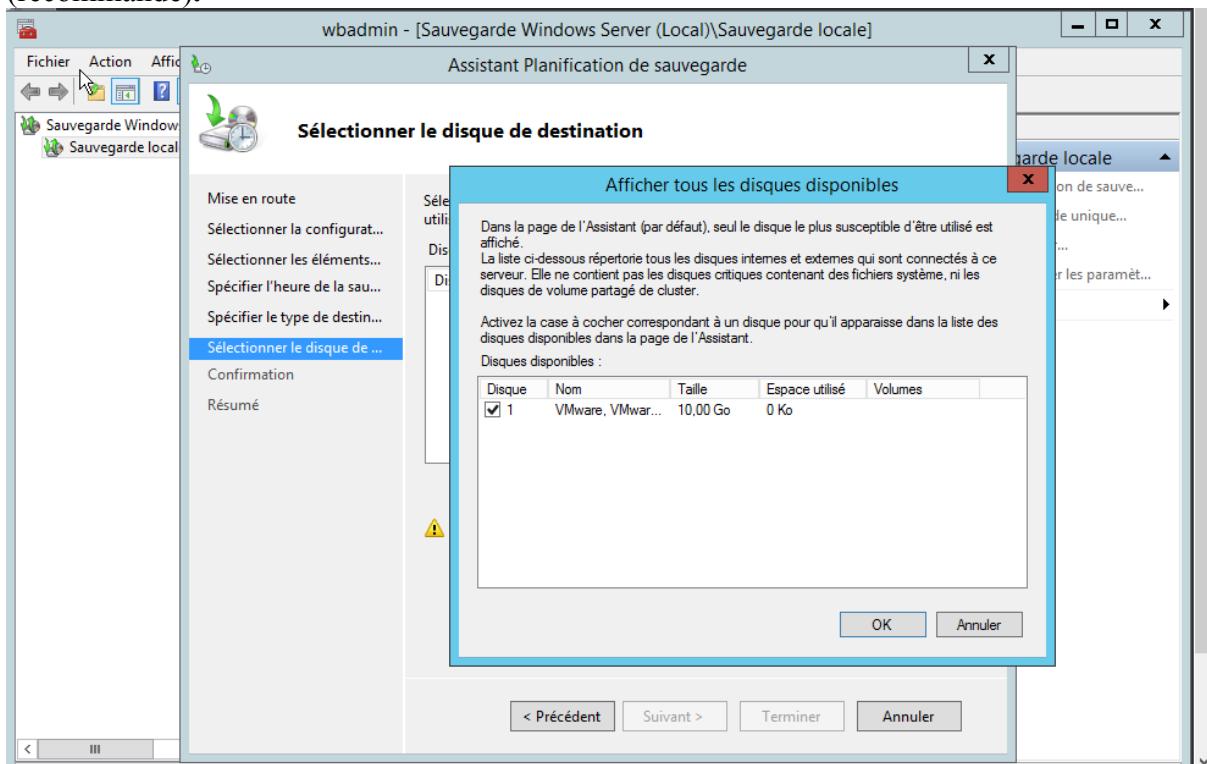


Figure 62 : sélection disque comme support de sauvegarde

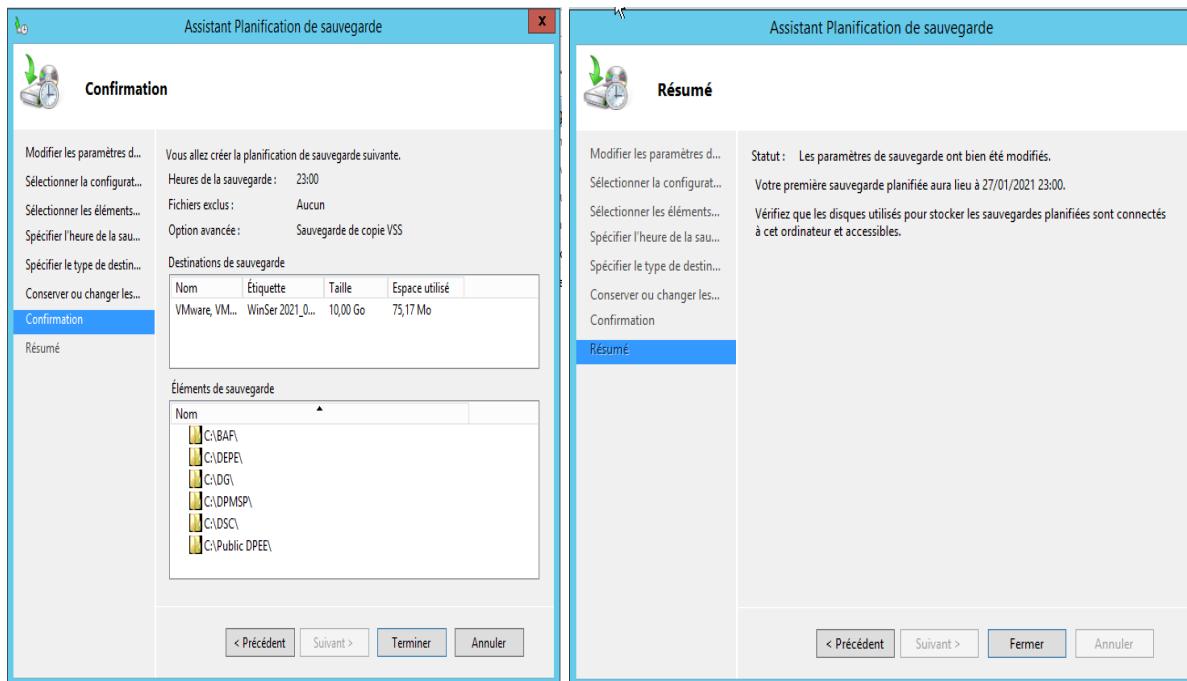


Figure 63 : aperçu de la configuration de notre sauvegarde

La sauvegarde a été effectuée à 23h comme demandé. On peut voir le message ci-dessous avec la description.

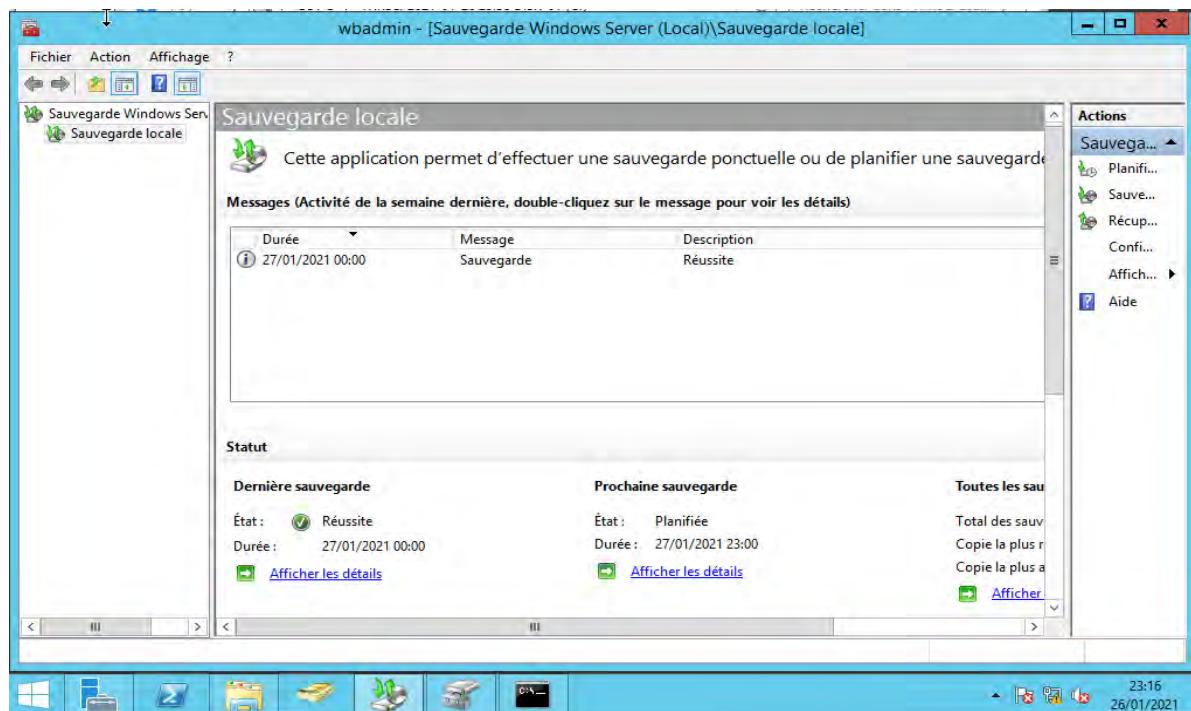


Figure 64 : aperçu de la sauvegarde réussite

6.5.2 Restauration

C'est une opération informatique qui consiste à retrouver les données perdues à la suite d'une erreur humaine, une défaillance matérielle, un accident ou au moment opportun d'un test de récupération de données défini dans une procédure de stratégie de sauvegarde et d'archive (également appelé plan de sauvegarde).

Comme la sauvegarde, on va accéder à la console de gestion, puis récupérer ...
On choisit le serveur, ainsi que la date de notre dernière sauvegarde.

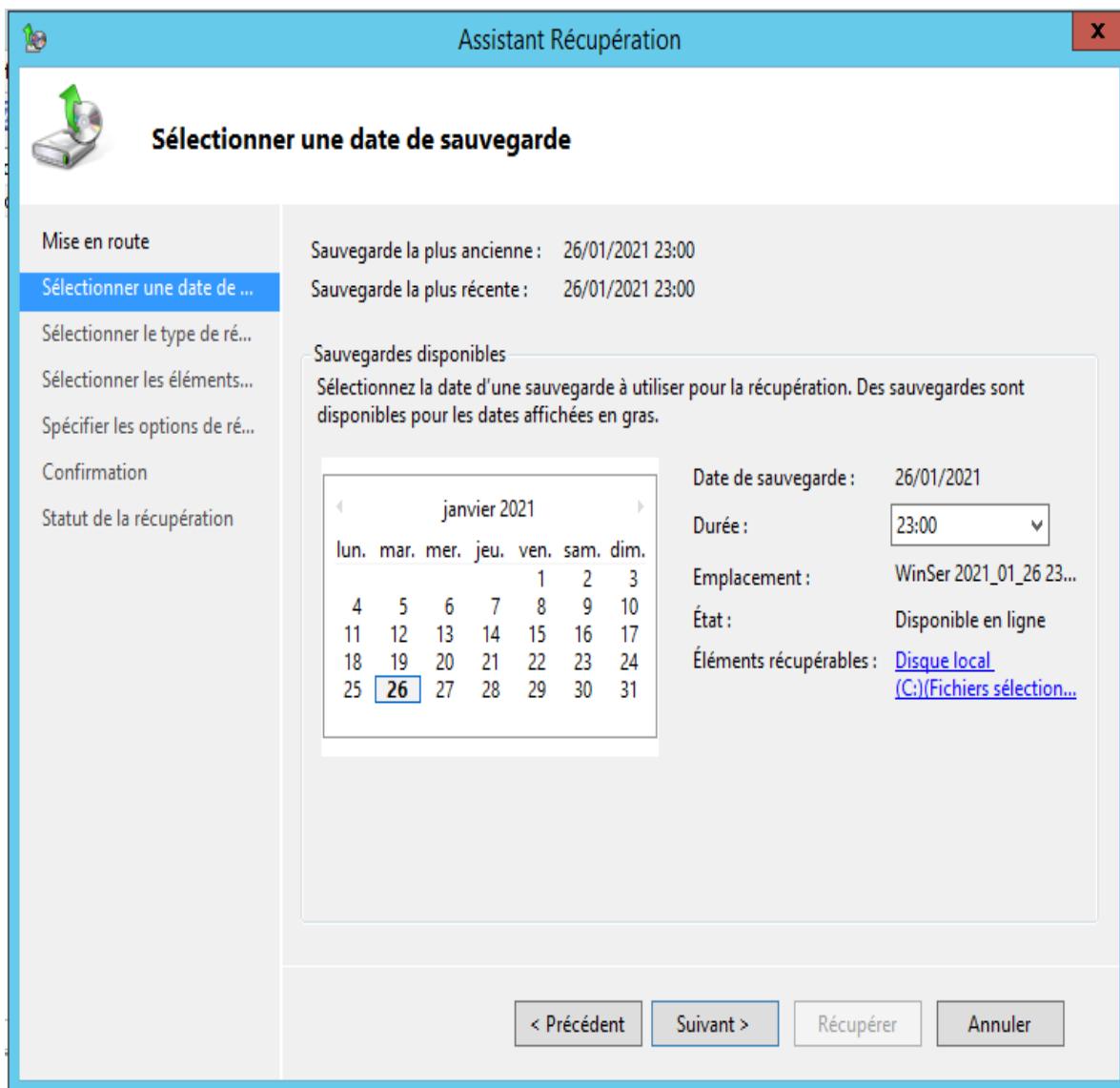


Figure 65 : assistant de récupération

Puis suivant, et on va sélectionner les dossiers ou fichiers qu'on souhaite récupérer.
Puis terminer par lancer notre récupération.

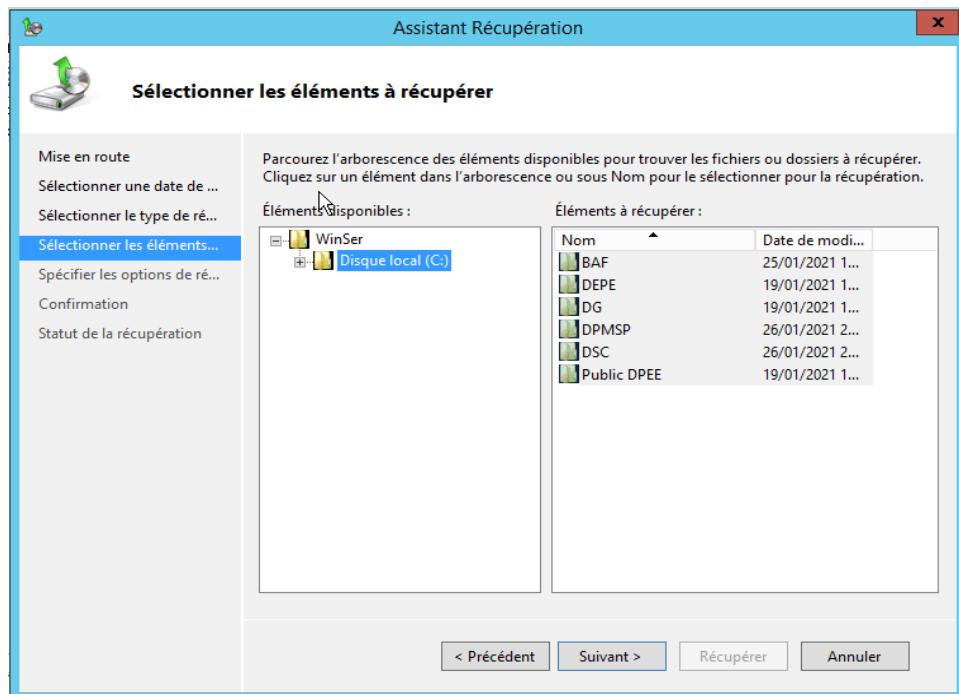


Figure 66 : sélection des dossiers à récupérer

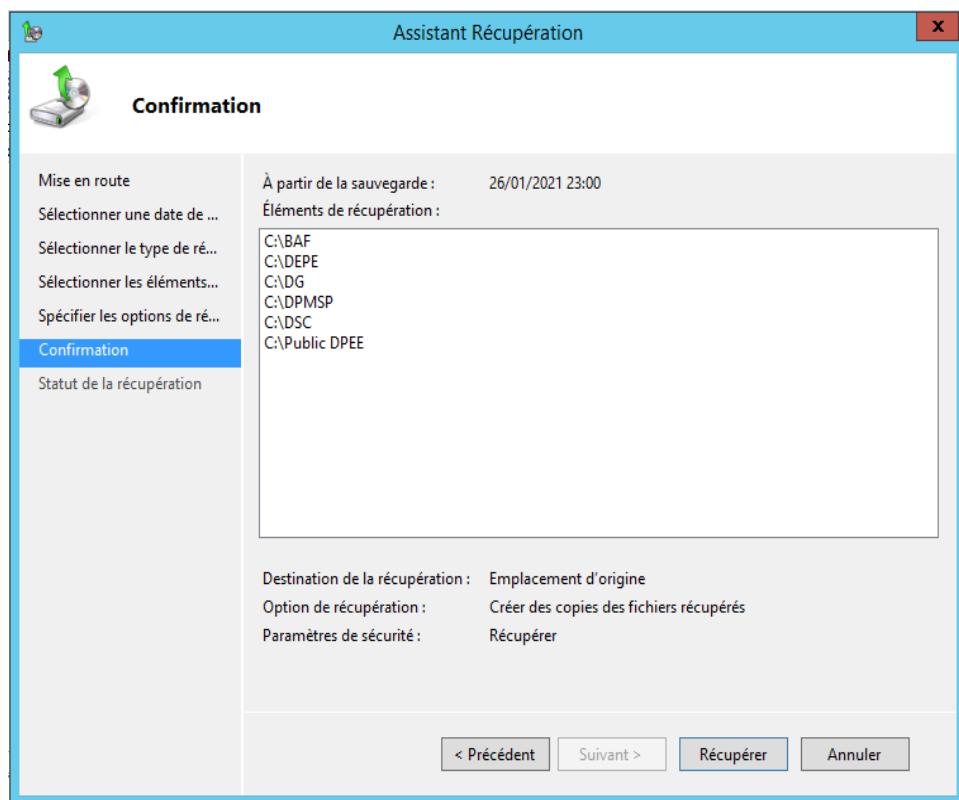


Figure 67 : liste des dossiers ou fichiers à récupérer

6.7 RECOMMANDATIONS

Notre solution a été configuré sur une machine virtuelle mais son déploiement au sein de la Direction Générale pour l'assurance de la sécurité nécessite un investissement.

Nous allons faire une proposition sous forme de table pour récapituler les besoins par ordre de priorité.

DESIGNATION	JUSTIFICATIF(S)	QTE
Serveur NAS	<p>NAS pour Network Attached Storage est un serveur de stockage en réseau.</p> <p>En installant ce serveur, les structures peuvent améliorer la productivité des employés. Un serveur central de fichiers et de bases de données permet en effet de partager des documents avec l'ensemble de l'entreprise. Les données sont au centre de toutes les attentions, car elles constituent le bien le plus précieux, à protéger (sécuriser), mais aussi à enrichir et à actualiser en permanence si l'on ne veut pas voir se perdre la valeur de l'entreprise. Un serveur permet d'effectuer un archivage et des copies de sauvegarde sur le réseau.</p>	1
Disques durs adaptés aux serveurs	<p>Le principal avantage est la redondance des disques durs et données.</p> <p>En effet, un NAS possède plusieurs disques durs qui fonctionnent en RAID. Le but est d'éviter les pertes de données.</p> <p>Par exemple, si un disque dur tombe en panne, les données restent accessibles sur un autre.</p> <p>Il faudra alors remplacer le disque dur défaillant.</p> <p>La plupart des NAS supportent le remplacement de disque à chaud, c'est à dire sans coupure électrique.</p> <p>Aucune opération n'est à faire par l'utilisateur car les données vont alors être synchronisées automatiquement.</p> <p>Il existe plusieurs types de RAID avec des fonctionnements différents.</p> <p>Ces derniers sont numérotés : RAID 0, RAID 1, etc.</p> <p>Capacité :</p> <p>D'après nos études, la DGPPE stocke à peu près 5 go de données mensuel (données à sauvegarder concernent plutôt les documents Word, Excel et PowerPoint (données critiques de l'entreprise) et Les données sur l'état du système). On a 18 entités d'après l'organigramme de la DG. Chaque entité va disposer 1To comme espace sur le disque.</p> <p>Donc la capacité prévue pour l'achat est 18 TO (18 000 go) pour chaque disque.</p>	4

Onduleur 	Les serveurs étant par nature destinés à être sous tension en permanence, ils sont très dépendants de la bonne qualité de leur alimentation électrique. En effet une surtension ou une coupure de courant pourrait être catastrophique pour les données qui y sont stockées. Pour éviter qu'un incident se produise et que votre matériel soit endommagé, vous pouvez recourir à un onduleur pour serveur. Un onduleur aura pour rôle de s'assurer que la tension destinée à votre serveur soit continue et sans parasite. Il pourra jouer sur l'intensité de celle-ci pour qu'elle reste stable.	2
Logiciel et Licence Windows server 2012 ou 2016 	Pour l'installation et l'activation du logiciel Windows Server.	1

Tableau 16 : récapitulatif des besoins de matériels pour la sécurité de données par ordre de priorité

- Fiche intervention

Lors des interventions effectuées par les différents prestataires de service, il est recommandé de disposer de fiche d'intervention.

Modèle :

FICHE D'INTERVENTION

Détails des travaux

Intervenant(s) Adresse, Téléphone ...	
Commentaire sur les travaux	
Date	

Equipement(s)

Ref.	
Etat	

Signature intervenant

Signature RSI

Figure 68 : Fiche d'intervention matériels de la DGPPE