TABLE DES MATIERES

LISTE DES ABREVIATIONS

Acronymes	Signification
2FA	Two Factor Authentication
ABAC	Attribute Based Access Control
ABAC	Attribute Based Access Control
AD	Active Directory
ADFS	Active Directory Federation Services
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
B2B	Business To Business
B2C	Business To Consumer
BAF	Bureau Administratif et Financier
BYOD	Bring Your Own Device
CAPEX	Capital Expenditure (dépenses d'investissement)
CIAM	Customer Identity & Access Management ou Consumer Identity & Access Management
DEPE	Division des Etudes et des Politiques Economiques
DGPPE	Direction Générale De La Planification et des Politiques Économiques
DPEE	Direction de la Prévision et des Etudes Economiques
DPMSP	Direction des Projections Macroéconomiques et du suivi des programmes
DSC	Division des synthèses conjoncturelles
eSSO	enterprise Single Sign-On
GGIA	Gestion et la Gouvernance des Identités et des Accès
GT	Groupe de Travail
IAG	Identity & Access Governance
IAI	Identity Analytics & Intelligence
IAM	Identity & Access Management ou GIA pour Gestion des Identités et des Accès
IAMaaS	Identity & Access Management as a Service
IDaaS	Identity as a Service
IRM	Identity Relationship Management
MFA	Multi-Factor Authentication
OOB	Out-Of-Band
RFID	Radio frequency identification
SSO	Single Sign-On

TABLE DES FIGURES

LISTE DES TABLEAUX

RESUME

Les services d'IAM (Identity and Access Management) vont bien au-delà de l'annuaire d'entreprise. Ils prennent en compte les comportements des utilisateurs du système d'information sur tous leurs terminaux, qu'il s'agisse d'employés, de clients ou même d'objets accédant légitimement aux ressources partagées. En plus des badges d'accès physiques et des codes nécessaires à la téléphonie et aux logiciels informatiques, l'IAM prend en considération l'habilitation aux services en fonction des métiers, des objectifs et des risques propres à chaque entreprise.

La Direction Générale, pour assurer la sécurité des personnels ainsi que les données doit avoir une procédure de contrôle d'accès physique ainsi qu'une mise en place d'une gestion et gouvernance des accès et identités. Le personnel de chaque structure doit pouvoir partager des données entre eux sans craindre de risque de les perdre ou de subir des attaques de tous types. La DSI doit comprendre en quoi la gestion et gouvernance des accès et identités peut aider l'entreprise. Ainsi, elle pourra fournir des solutions adéquates afin d'atteindre les objectifs sans l'exposer à des risques inutiles.

Pour une meilleur évolution et amélioration des outils, la Direction générale doit veiller à l'entretien et à la bonne utilisation des outils qui seront mis en place.

INTRODUCTION

Le passage au numérique impose à l'entreprise de rationaliser son système informatique. Dans ce contexte, plusieurs facteurs viennent booster l'organisation et la performance des systèmes d'information : intégration de nouvelles technologies de communication et d'information, modification de la structure et l'architecture des données, mise en interaction des supports téléphoniques et informatiques, extension du réseau informatique en interne et externe, etc.

Avec ces différents changements, les techniques d'échange et le traitement de l'information génèrent des flux à distance de plus en plus virtualisés et malheureusement, il devient de plus en plus facile pour les pirates de s'infiltrer dans les réseaux d'entreprises ainsi d'avoir tous les accès.

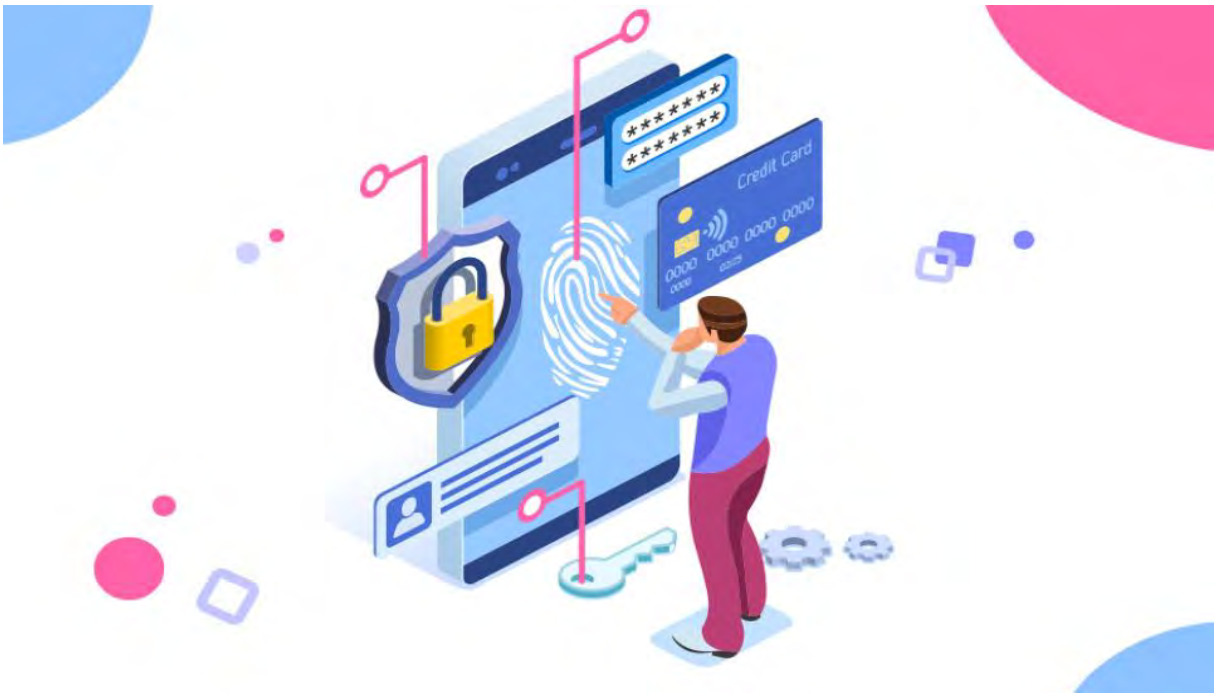


Figure 1: vue d'une mise en place de gestion d'accès et d'identité

De plus en plus d'entreprises et d'organismes appréhendent l'intérêt d'une mise en place du système d'information pour la gestion et gouvernance des accès et identités. Elle permet de renforcer le niveau de sécurité générale en garantissant la cohérence dans l'attribution des droits d'accès aux ressources hétérogènes du système d'information.

C'est la raison pour laquelle nous nous sommes proposés d'étudier les systèmes d'accès de la Direction générale afin de proposer une architecture pour la sécurité de leurs données.

L'étude ainsi réalisée a été découpée en trois (03) parties :

- ✓ Dans la première partie nous faisons une présentation générale
- ✓ Dans la deuxième partie dénommée généralité sur la gestion et gouvernance des accès et identités, nous présenterons les principes fondamentaux de la gestion des accès et des identités puis montrer les cas d'usages.
- ✓ Enfin dans la troisième partie, nous faisons la mise en œuvre, c'est-à-dire faire la pratique avec les outils présentés afin d'améliorer la sécurité de la structure.

1er partie :

Présentations générales

Dans le premier chapitre, nous présenterons la structure d'accueil. Ensuite nous expliciterons notre sujet pour plus de compréhension dans le deuxième chapitre.

CHAPITRE 1 : PRESENTATION DE LA STRUCTURE

1.1 Historique

La Direction générale de la Planification et des Politiques Economiques (DGPPE) a été instituée par le décret n° 2014-1171 du 16 septembre 2014, portant organisation du Ministère de l'Economie, des Finances et du Plan (MEFP) modifié par le décret n°2017-480 du 03 avril 2017. Sa création découle des résultats issus du diagnostic organisationnel et fonctionnel du Ministère de l'Economie et des Finances (MEF) réalisé en 2013. Elle regroupe les structures stratégiques du MEFP ayant en charge la formulation des politiques de développement et leur traduction en plans et programmes ainsi que la coordination, le suivi et l'évaluation des actions de développement mises en œuvre en vue d'une gestion pertinente de l'économie.

Elle répond ainsi à la nécessité de disposer d'une force de proposition et d'innovation devant permettre au MEFP de mieux prendre en charge les questions relatives à la conduite de la politique économique de manière cohérente, pertinente, efficace et efficiente au regard des nouveaux enjeux économiques, sociaux et environnementaux ainsi que des réformes de l'Etat.

La DGPPE, une des principales structures techniques du MEFP, donne corps aux orientations de la politique économique et financière du Gouvernement afin de mettre en place un cadre adéquat pour la mise en œuvre plus efficace et plus efficiente des politiques sectorielles. Sa vision et ses objectifs stratégiques s'inscrivent en droite ligne avec la Lettre de Politique sectorielle de développement (LPSD) du MEFP qui est en phase avec le Plan Sénégal Emergent (PSE).

1.2 Missions

La Direction générale de la Planification et des Politiques économiques, sous l'autorité du Directeur général de la Planification et des Politiques économiques est chargée de :

- Traduire les études exploratoires de long terme en orientations stratégiques ;
- Formuler, suivre et évaluer les politiques publiques ;
- Rechercher le meilleur système permettant de traduire les orientations stratégiques du Gouvernement en plans et programmes de développement ;
- Vérifier la cohérence des politiques sectorielles et thématiques avec les orientations stratégiques et priorités nationales en matière de développement économique et social ;
- Collecter et analyser toute information utile à la prise de décision des autorités publiques en matière économique et financière ;

- Proposer la politique de population/développement du pays ;
- Mener des études et recherches sur l'évolution des concepts et doctrines du développement ainsi qu'analyser leurs enjeux et opportunités pour le pays ;
- Participer à la préparation des lois de finances de l'Etat, notamment par la définition de cadre macroéconomique de la programmation budgétaire ainsi que la conception des rapports économiques et financiers ;
- S'assurer de l'efficacité, de l'équité sociale et de la durabilité des investissements publics ;
- Élaborer et suivre les instruments de pilotage stratégique de l'économie ;
- Suivre les processus d'intégration économique auxquels le Sénégal est partie prenante, en plus, coordonner les relations avec les organisations internationales à vocation économique.

Le Directeur général de la Planification et des Politiques économiques est assisté dans ses fonctions par un Coordonnateur nommé par décret, chargé également d'assurer son intérim en cas d'absence.

Le Directeur général de la Planification et des Politiques économiques peut, également, être assisté de Conseillers techniques nommés par arrêté du Ministre chargé des Finances.

1.3 ORGANISATION

La Direction générale de la Planification et des Politiques économiques comprend :

- les services propres ;
- les services rattachés ;
- les directions ;
- l'Unité de Coordination et de Suivi de la Politique économique ;
- la Cellule de Suivi de l'Intégration ;
- le Centre d'Etudes de Politiques pour le Développement.

➢ **Les Services propres**

Les services propres sont :

- le Bureau du courrier commun ;
- le Bureau des archives et de la documentation.

➢ **Les Services rattachés**

Les Services rattachés sont :

- l'Unité de suivi des Programmes d'investissements territoriaux de l'Etat ;
- la Cellule de la Thématique Multi-pôles ;
- le Secrétariat technique de la Commission nationale du Développement durable ;
- le Centre d'Information et de Documentation sur le Développement ;
- les Services régionaux de la Planification ;
- la Cellule de Communication ;
- la Cellule informatique ;
- le Bureau de Suivi stratégique et de Synthèse.

Outre ses services rattachés, la Direction générale de la Planification et des Politiques économiques comprend des services extérieurs qui sont constitués par les directions suivantes :

- la Direction du Contrôle interne ;
- la Direction de l'Administration et du Personnel ;
- la Direction de la Planification ;
- la Direction du Développement du Capital humain ;
- la Direction de la Prévision et des Etudes économiques.

➢ **La Direction du Contrôle interne**

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, la Direction du Contrôle interne est chargée de :

- veiller à l'application des directives issues des rapports de l'Inspection générale des Finances ainsi que de celles des autres corps de contrôle ;
- veiller à l'application des instructions et directives présidentielles ou primatorales ;
- assister le Directeur général dans le contrôle de la gestion du personnel, du matériel et des crédits de l'ensemble des services placés sous sa responsabilité ;
- donner un avis sur tous les projets de textes législatifs et réglementaires initiés au sein de la Direction générale ;
- effectuer toute mission d'enquête, de vérification et de contrôle qui lui est confiée par le Directeur général de la Planification et des Politiques économiques ;
- effectuer l'audit de performance des services, des plans, projets, programmes et réformes mis en œuvre par la DGPPE.

La Direction du Contrôle interne comprend :

- le Bureau de Contrôle ;
- le Bureau du Suivi ;
- le Bureau administratif et financier.

➢ La Direction de l'Administration et du Personnel

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, la Direction de l'Administration et du Personnel est chargée de la gestion du personnel, des moyens matériels et des ressources financières de la Direction générale de la Planification et des Politiques économiques.

A ce titre, elle est compétente, notamment, pour :

- suivre la mise en œuvre la politique de gestion des ressources humaines, en relation avec la Direction des Ressources Humaines du Département ;
- préparer les projets de budgets et autres programmes de la Direction générale de la Planification et des Politiques économiques et les défendre lors des réunions d'arbitrage budgétaire ;
- suivre, le cas échéant, la réalisation des programmes de construction et d'équipement de la Direction générale de la Planification et des Politiques économiques;
- gérer les moyens matériels, administrer les crédits et autres fonds alloués à la Direction générale de la Planification et des Politiques économiques ;
- assister les personnels de la Direction générale de la Planification et des Politiques économiques dans la préparation des missions à l'intérieur et à l'extérieur du pays.

La Direction de l'Administration et du Personnel comprend :

- la Division des Finances et de la Logistique ;
- la Division des Ressources humaines et de l'Action sociale.

➢ La Direction de la Planification

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, la Direction de la Planification est chargée de :

- coordonner les travaux d'élaboration des documents de planification pour le développement économique et social ainsi que de contribuer au suivi de leur mise en œuvre aux niveaux national, régional et sectoriel ;
- élaborer des études prospectives et d'en assurer l'actualisation ;
- élaborer des projections macro-économiques à moyen terme ;
- procéder à la modélisation à long terme ;
- veiller au renforcement des capacités des structures de planification de l'Administration ;
- élaborer les perspectives triennales devant servir de cadre de conception au Programme triennal d'Investissements et d'Actions publics ;
- appuyer l'élaboration des politiques sectorielles et territoriales ;

- procéder aux évaluations *ex ante*, à mi-parcours et finale des projets et programmes de développement ;
- de promouvoir la culture de l'évaluation en rapport avec les organisations et structures compétentes.

La Direction de la Planification comprend :

- la Division de la Planification générale ;
- la Division de la Planification sectorielle et de l'évaluation des projets ;
- la Division de la Planification régionale ;
- le Bureau de la Documentation ;
- le Bureau administratif et financier.

➢ **La Direction du Développement du capital humain**

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, la Direction du Développement du capital humain est chargée de la conception de la politique en matière de population/développement, de la coordination, du suivi et de l'évaluation de sa mise en œuvre. Elle prépare les Programmes d'Actions et d'Investissements prioritaires en matière de Population, suit l'impact social des politiques et élabore les instruments et les outils d'aide à la décision en matière de planification sociale.

A ce titre, elle :

- coordonne l'actualisation et le suivi de la mise en œuvre de la Déclaration de la Politique de Population et de tout autre document stratégique dans le domaine de la population/développement en vue de créer les conditions optimales pour la capture du dividende démographique ;
- prépare et met en œuvre les Programmes d'Actions et d'Investissements prioritaires en matière de Population ;
- coordonne l'élaboration et le suivi de la mise en œuvre des rapports nationaux sur le développement humain ;
- s'assure de la prise en compte des questions de population/développement dans les politiques, plans, programmes et stratégies de développement ;
- évalue l'impact social des politiques de développement ;
- publie régulièrement le Rapport national sur l'état de la population sénégalaise, le Rapport national de suivi de la mise en œuvre de la Politique nationale de Population et le Rapport national de suivi de la mise en œuvre de la politique nationale de migration ;
- suit la mise en œuvre du programme d'action de la Conférence internationale sur la population et le développement ;
- assure la réalisation d'études et de recherches en population/développement ;
- centralise et diffuse les résultats des études et recherches en population et développement ;
- assure la coordination des réseaux en population/développement ;

- réalise les projections des indicateurs démographiques sur la base de la politique de population à court, moyen et long termes.

➢ **La Direction du développement du capital humain comprend :**

- la Division de la Population ;
- la Division de la Planification sociale ;
- le Secrétariat permanent de la Commission nationale de la Population et des Ressources humaines et du Comité technique de Suivi des projets de Population ;
- le Centre d'Informations et de Documentation en Population ;
- le Bureau administratif et financier.

➢ **La Direction de la Prévision et des Études économiques**

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, la Direction de la Prévision et des Etudes économiques est chargée :

- de mener la collecte et la gestion de l'information conjoncturelle, intérieure et extérieure ;
- d'intégrer cette information dans un schéma global et prévisionnel et de procéder à des analyses conjoncturelles et à des travaux de prévision ;
- d'organiser la concertation entre les services concernés par les choix de politiques économique et financière à court terme ;
- de traduire les choix de la politique économique dans les relations entre le Ministère de l'Economie, des Finances et du Plan et les secteurs d'activités économiques et financières ;
- de présenter des synthèses macroéconomiques comme les tableaux de bords conjoncturels, les notes de conjoncture et des rapports sur les perspectives économiques et financières à court terme ;
- de réaliser des études sur les prix, les revenus et l'emploi, les finances publiques, la monnaie et le crédit, l'économie internationale et les échanges extérieurs ;
- de faire des simulations afin de mesurer les incidences des mesures de politique économique envisagées ;
- de préparer et de suivre les programmes économiques et financiers de court terme en relation avec d'autres services du Ministère de l'Economie, des Finances et du Plan, d'autres ministères et organisations sous-régionales ;
- d'élaborer la note d'orientation du budget de l'Etat et le rapport économique et financier annexé à la loi de finances.

➢ **La Direction de la Prévision et des Etudes économiques comprend :**

- la Division des Synthèses conjoncturelles ;
- la Division des Projections macroéconomiques et du Suivi des Programmes ;

- la Division des Etudes et des Politiques économiques ;
- le Bureau administratif et financier ;
- le Bureau de la Documentation ;
- le Bureau de l'Informatique et des Systèmes d'Information.

➢ L'Unité de Coordination et de Suivi de la Politique économique

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, l'Unité de Coordination et de Suivi de la Politique économique a pour mission d'appuyer la formulation et le suivi-évaluation de la politique économique et sociale en général et du document – cadre de référence de la politique économique, en particulier.

A ce titre, elle est chargée :

- de la coordination, au sein du Ministère, de la mise en œuvre de la politique économique et sociale ;
- de la coordination et de l'harmonisation des interventions des Partenaires techniques et financiers ;
- de la participation à la mobilisation des ressources extérieures pour le financement des projets prioritaires du Gouvernement ;
- du suivi de la mise en œuvre des politiques publiques à travers le document de référence pour l'atteinte des Objectifs du Millénaire pour le Développement ;
- de l'organisation de la revue annuelle conjointe servant de cadre de dialogue entre les différents instruments de politique économique ;
- du suivi de l'appui budgétaire dans le cadre de l'Arrangement Cadre des Appuis Budgétaires ;
- du suivi de la mise en œuvre de la Déclaration de Paris ;
- du suivi de l'articulation des politiques sectorielles au document – cadre ;
- de la conception et de la mise en œuvre des outils d'aide à la décision et/ou d'analyse de la politique économique en vue du renforcement des capacités des différents acteurs impliqués dans le processus ;
- de la promotion d'une bonne communication entre les différents acteurs impliqués dans la planification, la mise en œuvre et le suivi du document – cadre ;
- de la réalisation d'études et de recherche portant sur les questions relatives à la mission d'élaboration, de formulation, de suivi et d'évaluation des politiques publiques.

L'Unité de Coordination et de Suivi de la Politique économique comprend :

- la Division de la Croissance et Réduction de la Pauvreté ;
- la Division des Politiques sociales et Services sociaux de Base ;
- la Division de la Bonne Gouvernance ;
- le Bureau administratif et financier.

➢ La Cellule de suivi de l'Intégration

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, la Cellule de suivi de l'Intégration a pour mission d'assurer le traitement des questions relatives à l'intégration concernant le Ministère de l'Economie, des Finances et du Plan.

A ce titre, elle est chargée :

- d'assurer le Secrétariat du Comité des mandats pour les négociations au sein de l'Union Economique et Monétaire Ouest Africaine (UEMOA) ;
- d'animer un Comité national UEMOA chargé de l'étude préalable des dossiers inscrits à l'ordre du jour des réunions Comité des Experts statutaires, ainsi que de l'organisation de concertations autour de questions ponctuelles liées au fonctionnement du marché communautaire ;
- d'effectuer la coordination et le suivi au niveau national des dossiers de l'UEMOA ;
- de participer aux réunions du Comité des Experts statutaires de l'UEMOA ;
- de suivre les activités de la Communauté Economique des Etats de l'Afrique de l'Ouest concernant le Ministère de l'Economie, des Finances et du Plan ;
- de suivre en relation avec les services techniques concernés, les questions relatives à l'intégration économique et traitées dans d'autres instances régionales et internationales ;
- de contribuer à l'examen des questions de commerce régional et multilatéral ;
- de prendre part aux négociations commerciales et régionales et internationales impliquant le Ministère de l'Economie, des Finances et du Plan ;
- d'instruire, en collaboration avec les administrations concernées, les dossiers relatifs aux entraves dans les échanges intra-communautaires ;
- d'initier et de conduire des études sur les questions d'intégration.

➢ La Cellule de suivi de l'Intégration comprend :

- la Division du suivi de la surveillance multilatérale et des politiques macro-économiques ;
- la Division du suivi des réformes, des politiques et des programmes communautaires ;
- la Division du suivi des questions douanières et commerciales ;
- la Division du suivi des questions fiscales ;
- la Division du suivi des questions budgétaires et financières ;
- le Bureau administratif et financier.

➢ Le Centre d'Etudes de Politiques pour le Développement

Sous l'autorité du Directeur général de la Planification et des Politiques économiques, le Centre d'Etudes de Politiques pour le Développement a pour mission de contribuer :

- au renforcement des capacités nationales dans l'administration, le secteur privé et la société civile, en matière d'analyse et de formulation de politiques économique, financière et sociale et de promotion de la bonne gouvernance ;
- à la mise en œuvre d'activités de recherches et de formation sur les questions économiques, financières et sociales, notamment dans le cadre du programme de bonne gouvernance et de renforcement de la gestion économique et sociale, de la stratégie de développement du secteur privé, de la stratégie de réduction de la pauvreté et du Plan stratégique Sénégal Emergent ;
- au développement de mécanismes formels de discussions autour de résultats de recherches et de questions de politiques économiques et sociales entre représentants du secteur public, du secteur privé et de la société civile.

➢ **Le Centre d'Etudes de Politiques pour le Développement comprend :**

- le Bureau des Experts et des Assistants de Recherches ;
- le Bureau chargé de la Gestion des Finances, du Personnel et du Matériel.

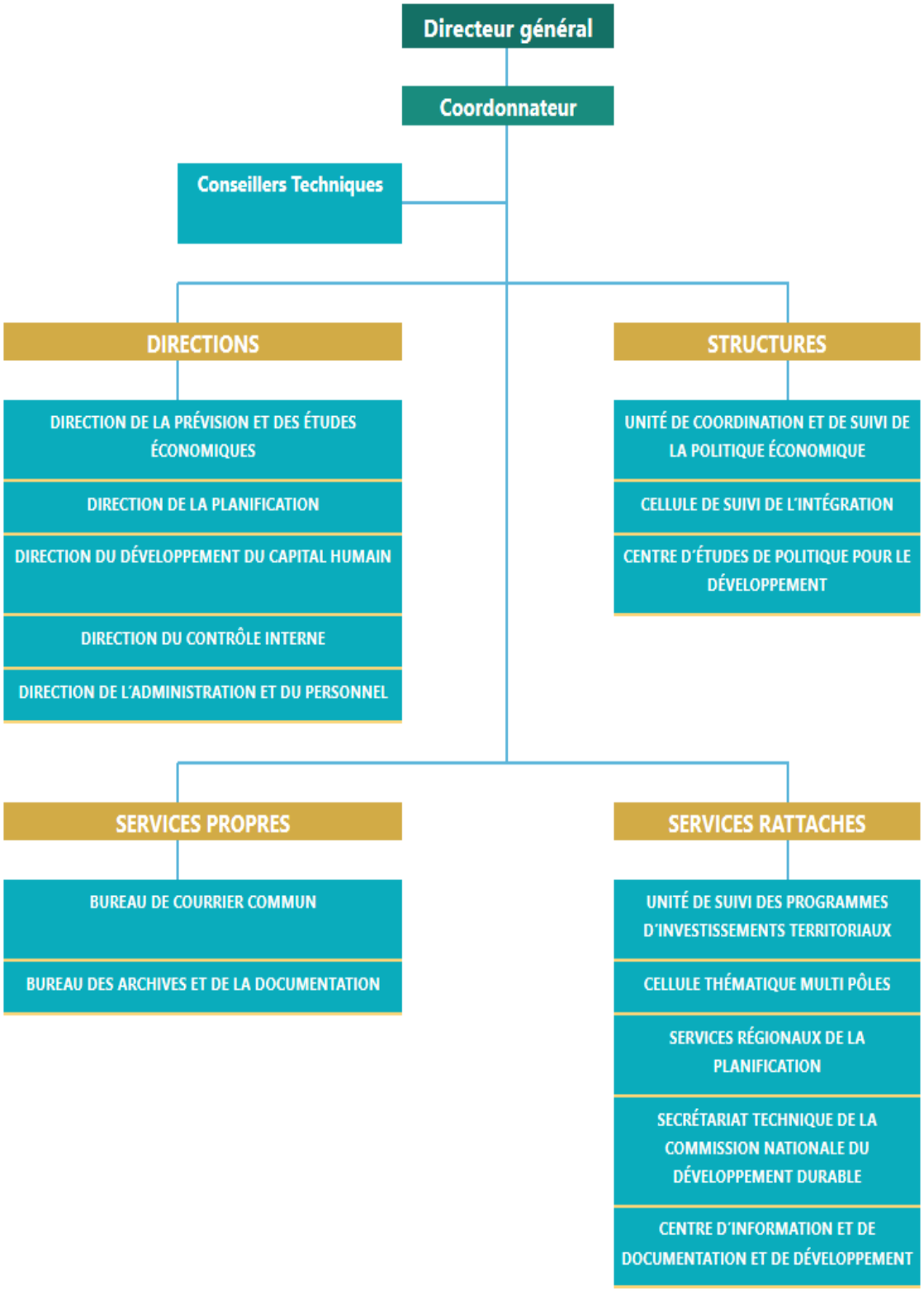


Figure 2: organigramme de la DGPPE

CHAPITRE 2 : Méthode de travail

2.1 Contexte du sujet

La gestion et gouvernance des identités est au centre des stratégies de sécurité et des opérations informatiques de la plupart des entreprises. Elles permettent aux entreprises d'offrir un accès automatisé à un nombre toujours croissant de ressources technologiques, tout en gérant les risques potentiels de sécurité et de conformité. La gouvernance des identités active et sécurise les identités numériques pour l'ensemble des utilisateurs, applications et données. Améliore

2.2 Etat des lieux

2.2.1 ORGANISATION DE LA DIVISION SI

L'informatique de la DGPPE est géré par une division des Systèmes d'Information placée sous l'autorité de la Direction de l'Administration et du Personnel. Cette division est composée de deux (2) pôles essentiels à savoir un pôle qui assure la gestion des ERP et un autre pôle réseau et sécurité.

Division	Pole	Rôles
Division SI	ERP (APPLICATIONS)	L'étude, la conception et le développement des applications, la formation des utilisateurs sur l'exploitation des différentes applications de la DGPPE, la veille technologie.
	Réseau et Sécurité	L'administration du réseau et de la sécurité et le support fonctionnel qui gère l'assistance aux utilisateurs.

Tableau 1 : organisation de la division du SI

2.2.2 LES APPLICATIONS MÉTIERS

2.2.2.1 INFRASTRUCTURE TECHNIQUE

a. LES SERVEURS

Nous pouvons noter l'absence de serveurs.

b. Les postes de travail et autres équipements

Les résultats du recensement du parc informatique de la DGPPE montrent que le matériel est composé de 400 actifs supports constitués essentiellement des micro-ordinateurs, des imprimantes, et des équipements connectés.

2.2.2.2 RÉSEAU ET SYSTÉME TÉLÉPHONIQUE

a. Réseau intranet et internet :

La DGPPE utilise le réseau intranet de l'ADIE exigé par l'Etat du Sénégal. Elle utilise aussi la fibre internet comme connexion alternative.

b. Câblage :

Le câblage réseau informatique a été réalisé. Cependant il ne respecte pas les normes de câblage usuels.
La Direction générale utilise des câbles UTP de catégorie 5E et 6 pour relier les Switches d'accès aux ordinateurs des utilisateurs. Les switch d'accès sont liés au Switch de distribution par des liaisons fibre.

c. Locaux ou salles informatiques et téléphoniques

Localisation	Observations (nbre switch, climatisation, sécurité d'accès, incendie, nbre de routeur ou modem wifi, cablage,...)
2eme Etage	6 switch linksys et HP 24 ports, fermé à clé, câblage catégorie 5E, 2 climatiseurs , 1 routeur, 1 modem wifi, les PABX pour la téléphonie
7eme Etage	3 switch Linksys 24 ports, fermé à clé, câblage catégorie 5E, 1 climatiseur , 2 routeurs
11eme Etage	1 switch Linksys de 24 ports, pas fermé à clé, câblage catégorie 5E, 1 routeur, 1 modem wifi

Tableau 2 : recensement matériels

2.2.2.3 LES ÉLÉMENTS TECHNIQUES DE LA SALLE DES SERVEURS

Dans les trois salles serveurs visitées, nous trouvons les éléments techniques suivants :

- Deux (2) armoires de brassage et des gaines techniques pour le câblage vertical, aménagées pour la circulation des câbles et la protection des équipements d'interconnexion. Ces armoires hébergent respectivement :

- ✓ Les équipements réseaux/télécom (des équipements réseaux et téléphonie de l'ADIE ...) ;

- Deux onduleurs équipés de batteries permettant d'avoir une autonomie d'au moins 20 minutes ;
- Un système de détection d'incendie basé sur du CO2.

2.2.2.2 Système d'exploitation:

Au niveau des systèmes d'exploitation, les postes de travail recensés utilisent Windows 7, Windows 8, Windows 10.

2.2.2.3 STRATÉGIE DE SÉCURITÉ

a. Stratégie anti-virus

La DGPPE dispose d'un système de l'anti-virus Kaspersky et Windows Defender pour tous les postes de travail. Il est directement sur le système d'exploitation des ordinateurs clients et fonctionne dans une architecture poste à poste.

b. Stratégie de Sauvegarde/Restauration

Les sauvegardes des données des applications critiques se font manuellement sur disque dur et peu fréquemment.

c. Système d'archivage

Nous pouvons noter l'absence de système d'archivage électronique.

d. Sécurité physique

L'accès au bâtiment est assuré par un poste de gendarme qui gère la sécurité du personnel mais aussi qui trace les entrées et sortie des visiteurs.
L'accès physique des agents est géré par un système d'accès et d'émargement électronique.

Le bâtiment dispose à certains endroits d'une sécurité anti-incendie (dans la salle des serveurs) et dans certains bureaux qui disposent aussi d'extincteurs CO2.

Pour la protection contre les pannes électriques, nous avons noté les éléments suivants :

- Un (01) groupe électrogène qui alimente exclusivement le 6ème et 11ème étage.

2.3 Schéma d'architecture

Le schéma de l'architecture réseau fournit une image complète du réseau établi avec une vue détaillée de toutes les ressources accessibles. Il comprend les composants matériels utilisés pour la communication, le câblage et les types de périphériques, la topologie et les topologies du réseau, les connexions physiques et sans fil, les zones mises en œuvre et les plans futurs.

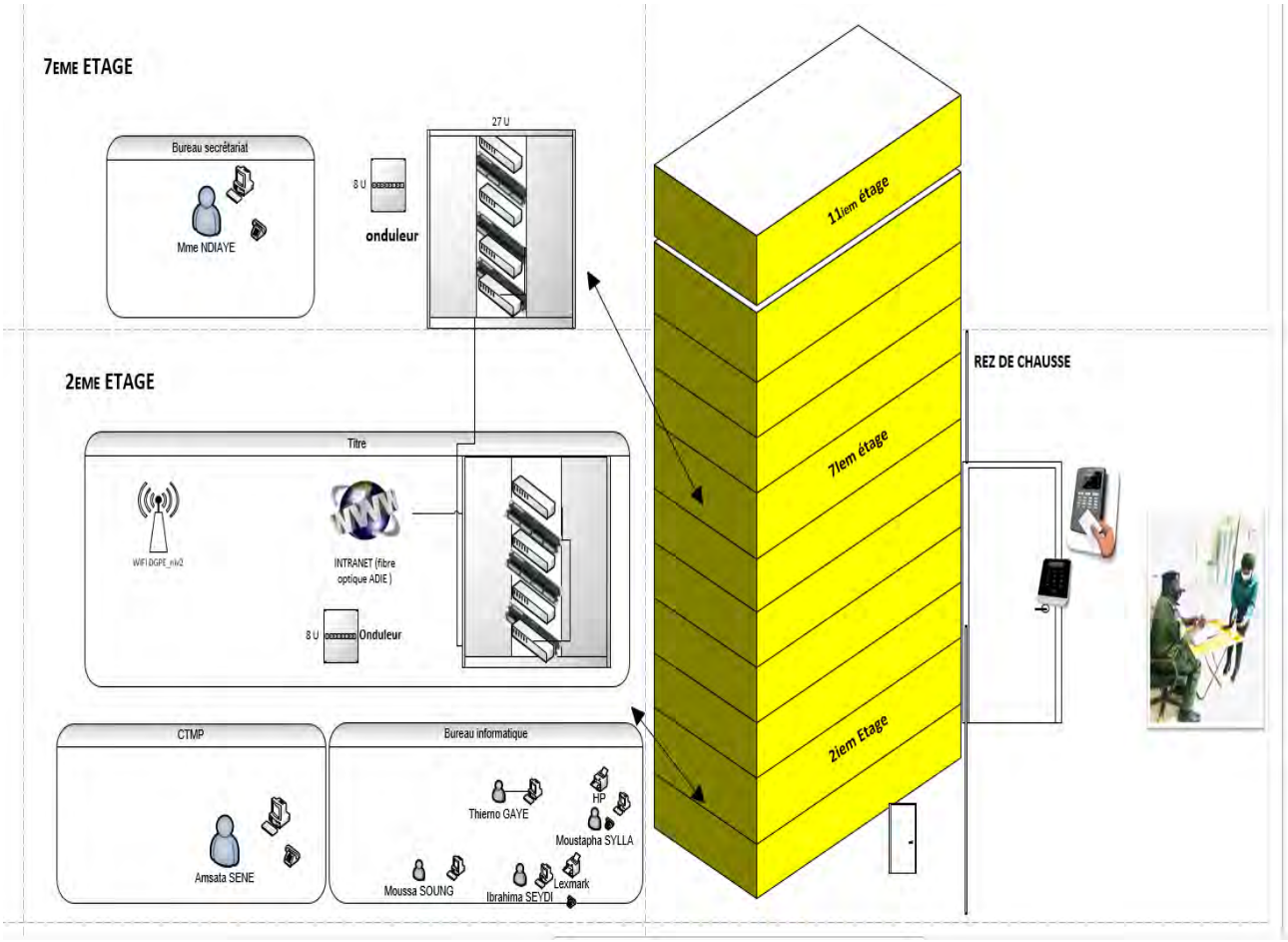


Figure 3: Schéma d'architecture de la DGPPE

2.4 Problématique

A l'heure de la multiplication des fichiers dans l'entreprise, du développement du travail collaboratif et de la mobilité, la gestion et l'accès des fichiers en entreprise est devenue problématique.

Les anciennes méthodes de stockage et d'organisation sont devenues obsolètes et ne permettent plus de répondre aux nouveaux besoins et aux modes de fonctionnement actuels des entreprises.

L'absence de gestion globale et gouvernance des accès et identités génère de nombreux problèmes au sein de la structure, parmi lesquels nous pouvons citer :

- La pertes de données : les utilisateurs se plaignent souvent des pertes de données qu'ils ont subies par vol de matériel ;
- la charge important d'administrations (multiplication des administrateurs, réinitialisation des mots de passe, etc.) ;
- la difficulté d'auditer les accès aux ressources ;
- l'impossibilité de tracer les actions d'administration des droits et d'en contrôler la cohérence et la pertinence ;
- l'erreur humaine est la cause la plus fréquente de perte de données. L'être humain n'est tout simplement pas infaillible et aucun utilisateur ne peut se prétendre à l'abri d'une erreur de manipulation.
- Baisse de vigilance, inattention ou négligence sont à l'origine de la plupart de ces erreurs :
- Suppression accidentelle de fichiers ou de dossiers
- Ecrasement involontaire de sauvegarde ou de données
- Erreurs de saisie entraînant une altération des données
- Formatage involontaire
- la plupart des virus et logiciels malveillants circulent de manière aveugle et ont pour but de corrompre un système informatique, supprimer des données… Des procédures informatiques rigoureuses et des dispositifs de sécurité (firewall, logiciels anti-virus…) peuvent suffire à les prévenir.

2.5 Objectifs à atteindre

L'objectif de ce projet est d'apporter une solution de gestion et gouvernance des accès et identités visant à la sécurité du système d'information de l'entreprise.
Après avoir énuméré tous les problèmes que rencontrent l'entreprise, je dois trouver la solution la plus adapté pour les résoudre.
La justification de ce projet de gestion et gouvernance des accès et identités reposera sur les améliorations suivantes :

2.5.1 Amélioration de la sécurité

Un système de gestion des identités et des droits d'accès permet de renforcer la sécurité. Une telle approche conduit à établir des liens entre toutes les applications, bases de données et annuaires en s'appuyant sur des notions de rôle et de profil. Cette solution offre un point unique

de gestion des règles de sécurité pour l'ensemble des systèmes concernés. Elle permet de créer simplement des règles d'accès et de sécurité, en cohérence avec la Politique de Sécurité des Systèmes d'Information et les besoins métier, puis de les propager automatiquement à tous les systèmes de l'entreprise.

La gestion centralisée des identités permet d'éliminer une source considérable d'erreurs d'administration pouvant causer des failles de sécurité d'accès au SI de l'entreprise. Elle permet également de résilier complètement et immédiatement les droits d'accès sur l'ensemble des systèmes lorsque des salariés ou personnels extérieurs quittent l'entreprise ou changent d'affectation et supprimer ainsi les comptes « fantômes ».

Cependant, la mise en place de solution d'accès et d'identité nécessite l'amélioration de la sécurité des équipements (acquisitions des onduleurs, back-up énergétiques et/ou groupe électrogène pouvant alimenter toutes la DGPPE, climatiseurs, sécurisation porte d'accès salles informatiques et armoires), logiciels (antivirus, licences offices et Windows, etc.)

En mettant en place des processus maîtrisés d'habilitation, le système permet d'impliquer les responsables métiers dans le circuit d'habilitation et de ne plus laisser au seul administrateur technique la maîtrise des droits d'accès.

2.5.2 Réduction des coûts d'administration

Un système de gestion des identités et des droits d'accès permet d'alléger la charge de travail de l'équipe du « support informatique » (administration, help desk). Cet allègement résulte d'une part de l'automatisation de tâches de gestion de comptes (réduction du nombre d'administrateurs) et d'autre part de la diminution du nombre d'appels d'utilisateurs (perte ou oubli de nombreux mots de passe, relance de demandes d'accès, etc.).

Le système de gestion des identités peut permettre aux utilisateurs la gestion directe de certains aspects de leur profil (par exemple le mot de passe, l'adresse, les numéros de téléphone, etc.).

2.5.3 Amélioration de l'efficacité et de la réactivité

Un système de gestion des identités et des droits d'accès permet de réduire le nombre d'interventions humaines par une automatisation de la propagation des droits sur les différents environnements concernés. La conséquence est à la fois une réduction des délais de mise à disposition des droits d'accès et une réduction des sources d'erreur (prise en compte systématique de tous les besoins liés à l'activité de l'utilisateur, garantie de cohérence dans les droits attribués).

Les gains générés concernent à la fois les utilisateurs internes (gain de productivité) et externes (amélioration de la qualité du service et de l'image de l'entreprise). Sur un autre plan, lors d'une fusion ou d'une acquisition, il faut fournir le plus rapidement possible un accès aisé aux ressources rassemblées d'entreprises auparavant autonomes. Là encore, une solution de gestion des identités et des droits d'accès aidera à relever ce défi au travers d'un service d'intégration des informations multi-plates-formes permettant de connecter les systèmes de chaque entreprise à la plupart des systèmes (nouveaux ou préexistants) de la nouvelle entité.

2ème partie :

Généralités sur gestion et gouvernance des identités et des accès

Cette partie vise à donner une définition simplifiée des principes fondamentaux couverts par la Gestion et la Gouvernance des Identités et des Accès (GGIA) mais aussi parer des cas d'usage de l'IAM/IAG.

Chapitre 3 : Principes fondamentaux IAM et IAG

3.1 Définition

En sécurité des systèmes d'information, la Gestion des Identités et des Accès (GIA) (en anglais Identity and Access Management : IAM) est l'ensemble des processus mis en œuvre par une entité pour la gestion des habilitations de ses utilisateurs à son système d'information ou à ses applications[1]. Il s'agit donc de gérer qui a accès à quelle information à travers le temps[2]. Cela implique ainsi d'administrer la création, la modification, et les droits d'accès de chaque identité numérique interagissant avec les ressources de l'entité.
La gestion des identités et des accès s'intéresse par exemple au contrôle de la façon dont les utilisateurs acquièrent une identité, la protection de cette identité et les technologies permettant cette protection.

Aussi, nous avons retenu de présenter une vision simple – et simplifiée – de l'IAM/IAG en regroupant les principes fondamentaux autour de 6 enjeux concrets :
1. améliorer et simplifier la gestion des identités, des droits et des comptes ;
2. piloter, auditer et contrôler les identités, les droits et les accès ;
3. authentifier les utilisateurs ;
4. contrôler et simplifier l'accès aux données ;
5. étendre les services IAM/IAG et IAI ;

Ce chapitre vise à donner une définition simplifiée des principes fondamentaux couverts par la Gestion et la Gouvernance des Identités et des Accès. En effet, les terminologies sont nombreuses (IAM, IAG, IGA, IRM, IAI, IDaaS…) et ne fournissent pas toutes une vision claire de ce qu'elles recouvrent.
Aussi, nous avons retenu de présenter une vision simple – et simplifiée – de l'IAM/IAG en regroupant les principes fondamentaux autour de 6 enjeux concrets :
1. améliorer et simplifier la gestion des identités, des droits et des comptes ;
2. piloter, auditer et contrôler les identités, les droits et les accès ;
3. authentifier les utilisateurs ;
4. contrôler et simplifier l'accès aux applications ;
5. étendre les services IAM/IAG et IAI ;
6. tirer parti du cloud.

3.2 Améliorer et simplifier la gestion des identités, des droits et des comptes

Il s'agit ici de simplifier et d'automatiser les actions du quotidien liées à la gestion des identités et de leurs droits.

3.2.1 Gestion du cycle de vie des identités

La gestion du cycle de vie des identités consiste à modéliser et outiller la gestion des événements de la vie d'une identité au sein de l'entreprise.
Elle couvre ainsi :

- toutes les populations devant se connecter au SI de l'entreprise : employés, prestataires in situ et ex situ, fournisseurs, partenaires, clients… voir demain des objets connectés, les machines, les robots, etc. ;
- tous les événements touchant à une identité au cours de son cycle de vie et pouvant varier selon les populations et selon les activités : arrivée, changement de poste, départ, arrivée/retour de saisonnier, détachement, absence longue durée, suspension, mission supplémentaire, etc.

3.2.2 Gestion des habilitations

Les identités étant gérées, il convient également de gérer leurs habilitations sur le SI, c'est-à-dire leur(s) compte(s) applicatif(s) et leurs droits dans les applications.

- La gestion des habilitations s'appuie généralement sur :
- un **modèle d'habilitation**, c'est-à-dire la modélisation homogène des droits sur le SI ;
- une **organisation « back office »** en charge de la définition et de l'évolution de cette modélisation ;
- des **processus d'approbation** en cas de demande, modification ou retrait d'un droit ;
- une **organisation « front office »** en charge d'approuver, de rejeter ou de compléter les demandes soumises.

- Enfin, pour simplifier l'expérience utilisateur et faire de l'IAM l'outil principal de la gestion des demandes, la gestion des habilitations peut être étendue à d'autres ressources comme :
- des badges d'accès logique ou physique : restauration, machine à café, etc. ;
- des équipements IT : téléphone portable, tablette, etc. ;
- des droits d'accès physiques : accès aux bâtiments, à certains locaux, etc.
- 15/106 Gestion & Gouvernance des Identités et des Accès © CLUSIF 2017

Pour cela, il est nécessaire de :

- prendre en compte les référentiels maîtres déjà présents dans l'entreprise (SI-RH pour les internes en général, bases spécifiques ou applications des achats pour les prestataires ou les partenaires, référentiels organisationnels, etc.) via des alimentations régulières ;
- offrir des IHM et des processus de gestion (workflows d'approbation) pour les populations ou les événements sans référentiel maître, comme par exemple les prestataires ;
- permettre de configurer des contraintes dans la gestion de certaines populations comme :
- la possibilité de limiter les personnes autorisées à créer des prestataires ;

3.2.2 Provisioning

Après avoir géré les demandes d'habilitations, il reste à créer les comptes et droits ad hoc sur le SI. C'est l'objectif du provisioning. Il cherche à maintenir à jour les référentiels majeurs comme l'annuaire Active Directory et les annuaires LDAP ainsi que les référentiels propres à chaque application.
Plusieurs niveaux d'intégration sont possibles.
Le provisioning automatique vise à créer automatiquement les comptes et droits nécessaires.
Le provisioning manuel ou guidé nécessite que les actions techniques soient réalisées manuellement par un administrateur. Pour le mettre en œuvre, il existe principalement deux approches :

- Interfacer l'outil IAM/IAG avec l'outil ITSM existant. Ainsi, l'IAM/IAG crée un ticket dans l'ITSM puis suit son traitement afin de pouvoir afficher un niveau d'avancement à l'utilisateur ;
- implémenter directement dans l'IAM les processus appropriés pour notifier les administrateurs des tâches en attente et leur permettre de rendre compte de leurs actions.
- Le provisioning mixte ou semi-automatique combine des tâches automatiques et des actions manuelles. Suivant le contexte, il permet de combiner plusieurs avantages tels que :
  - la gestion automatique des attributs sensibles comme le statut actif ou suspendu d'un compte ou le délai d'expiration des mots de passe afin de garantir un haut niveau de sécurité ;
  - la gestion manuelle des droits d'accès pour une implémentation simple.
- Le provisioning « à la volée », est apparu plus récemment avec les outils de fédération d'identités. Il consiste à fournir, dans le jeton d'identité échangé, l'ensemble des informations nécessaires à la création et à la mise à jour du compte. Charge alors à l'application consommant ce jeton de créer le compte à la première connexion de l'utilisateur puis de le mettre à jour lors des accès suivants. 18/106 Gestion & Gouvernance des Identités et des Accès © CLUSIF 2017

3.3 Piloter, auditer et contrôler les identités, les droits et les accès

L'objectif est ici de disposer de la capacité à piloter, auditer et contrôler les accès au SI. Historiquement ces fonctions étaient relativement peu développées dans les solutions d'IAM, jusqu'à l'apparition d'outils dédiés à cet enjeu, sous le nom d'IAG ou IAI (Identity & Access Governance, Identity Analytics & Intelligence). A noter qu'à ce jour les outils d'IAM cherchent

à étendre leur couverture fonctionnelle, menant parfois à un recouvrement entre solutions d'IAM, d'IAG et d'IAI.
Les solutions IAM, IAG et IAI se distinguent par:

- **la conception intrinsèque des outils** : les outils d'IAI sont le pendant « Business Intelligence » de l'IAM. Ils sont construits autour d'un puits de données ou cube de données et ont vocation à réagir a posteriori ;
- **la granularité des droits gérés** : les outils d'IAM et d'IAG se limitent en grande majorité aux droits dont ils doivent gérer l'attribution. Par exemple dans SAP, il s'agira des rôles composites. Allant plus loin, les outils d'IAI ont vocation à recréer la chaîne de liaison complète, jusqu'au droit le plus fin dans les applications. Par exemple dans SAP, il s'agira des transactions. L'objectif est de détecter les risques ou les non-conformités dues à la définition des rôles ou des profils.
- **Les sponsors et donneurs d'ordre visés** : les solutions d'IAI visent en premier lieu à maîtriser le niveau de risques liés aux droits d'accès. En ce sens, elles s'adressent prioritairement aux directions des risques et à l'audit interne.

- Ainsi, et de manière très schématique, l'IAI vise principalement 3 objectifs :
- **améliorer la qualité des données** par des contrôles de cohérence et une assistance à l'identification des sources d'incohérence ;
- **maîtriser les risques liés aux habilitations** avec un suivi de l'attribution des droits à risques, le pilotage de campagnes de revues et la gestion des exceptions ;
- **ajuster le modèle d'habilitation** ou « Role Management » grâce à l'analyse de l'usage des profils métiers et applicatifs définis et à la comparaison des droits attribués et transactions effectivement utilisées.

L'intérêt de l'IAI prend toute sa dimension lorsque les directions des risques et de l'audit interne sont fortement impliquées dans le projet.
La suite du chapitre donne un éclairage rapide sur les principales fonctionnalités d'un IAI. 19/106 Gestion & Gouvernance des Identités et des Accès © CLUSIF 2017

3.4 Authentifier les utilisateurs

Authentifier un utilisateur vise à garantir, avec un niveau de confiance adapté, son identité. L'objectif de ce chapitre est de donner un aperçu des moyens d'authentification autres que le simple couple « login/mot de passe » encore très répandu.

❖ **Authentification forte, authentification renforcée, MFA**

Sans qu'il existe de définition officielle et partagée, **l'authentification forte** peut se définir comme la combinaison de deux principes :

- la combinaison d'au moins deux facteurs différents parmi les suivants :
- ce que je sais et que je suis le seul à connaître : par exemple un mot de passe ou un code PIN ;
- ce que je possède : par exemple une carte à puce, un certificat, un token ou un smartphone ;
- ce que je suis : par exemple par une empreinte digitale, un réseau veineux, un visage.

- au moins un de ces facteurs n'est pas rejouable. C'est-à-dire que les données échangées entre l'utilisateur et le serveur ne peuvent pas être réutilisées. Ainsi, même si elles sont interceptées, elles restent inutilisables.

❖ Authentification OOB (Out-Of-Band)

L'authentification OOB consiste à recourir, pour un facteur d'authentification, à un canal différent de celui utilisé pour accéder à l'application.
• Exemple OOB : accès à une application Web à partir d'un PC + application sur un smartphone recevant une notification push dans laquelle il faut confirmer son identité.
• Exemple non OOB : accès à une application Web à partir d'un PC + envoi d'un SMS sur un smartphone, à ressaisir dans l'IHM de l'application Web.

❖ Biométrie comportementale

La biométrie comportementale consiste à comparer le comportement de l'utilisateur par rapport à son « empreinte comportementale ». Cette dernière peut être générée lors d'une phase d'enrôlement ou construite progressivement, à mesure que l'utilisateur utilise ses équipements. A titre d'exemples : la vitesse ou la dynamique de frappe, les mouvements de la souris, les habitudes dans l'utilisation d'un écran tactile.

3.5 Contrôler et simplifier l'accès aux applications

L'objectif ici est double :

- ✓ simplifier l'accès de l'utilisateur en limitant les demandes d'authentification : c'est le principe du SSO qui vise, après une première authentification, à ne plus authentifier l'utilisateur durant une période déterminée ;
- ✓ contrôler l'accès aux applications, c'est-à-dire vérifier que l'utilisateur est bien autorisé à réaliser l'accès demandé, et tracer cet accès.

3.6 Tirer parti du cloud

Les services d'IDaaS/IAMaaS visent à offrir les fonctionnalités d'IAM dans le Cloud, c'est-à-dire en mode SaaS.
Comme pour les autres services IT, nombreux sont les clients qui s'interrogent sur la pertinence de recourir au Cloud pour les services IAM. A la date de rédaction de ce document, le recours à ces services reste limité car toutes les briques IAM n'offrent pas le même niveau de maturité :

- ➢ les services Cloud associés à la gestion des accès, tels que l'authentification multi-facteurs, le SSO ou la Fédération d'Identités, offrent déjà un niveau de maturité intéressant ;
- ➢ les services Cloud associés à la gestion des identités restent en retrait par rapport à l'offre « on-premise ». A noter que la couverture fonctionnelle n'est pas nécessairement identique chez un même éditeur offrant sa solution en mode « on-premise » et en mode Cloud ;

- les services Cloud associés à l'IAI sont les moins bien représentés dans les offres Cloud.

Les approches les plus répandues actuellement sont au mieux « hydrides », combinant une infrastructure « on-premise » et certains services Cloud.
Enfin, pour pallier le manque d'offres Cloud, certains intégrateurs tendent à délivrer des implémentations de solutions « on-premise » sur des hébergements Cloud (PaaS). Ce mode de délivrance reste lui aussi assez récent et n'offre pas un niveau de service identique à une offre Cloud à part entière.

CHAPITRE 4 : CAS D'USAGES

Nous avons proposé de regrouper les principes de l'IAM/IAG autour de 6 enjeux concrets qui mettent en évidence un certain nombre de composants ou modules. Cela étant, nous n'avons volontairement pas abordé en détail l'ensemble des briques fonctionnelles de l'IAM/IAG, privilégiant les modules les plus fondamentaux, les plus répandus et les plus matures sur le marché actuel, rassemblés par « grandes familles ».

4.1 Pourquoi démarrer un projet IAM/IAG ?

Les motivations liées au démarrage de tout ou partie d'un projet de Gestion et Gouvernance des Identités et des Accès sont nombreuses. C'est pourquoi l'objet de ce chapitre n'est pas d'en dresser la liste exhaustive mais plutôt d'identifier de nombreux cas d'usages ou objectifs concrets qui sont autant d'arguments justifiant de lancer un projet d'IAM/IAG.
Le tableau ci-après présente un certain nombre de ces cas d'usages, organisés par domaines fonctionnels et problématiques, en face desquels nous avons positionné les briques de l'IAM/IAG les plus directement concernées.
La liste n'est pas exhaustive, d'autres cas d'usages sont fournis dans la suite du document, et notamment dans les fiches pratiques présentées au chapitre VI.

Domaines	Exemples de problématiques et de cas d'usages	Auth. forte	SSO	Fédération	Annuaire	Cycle de vie	Habilitations	Revues	Rôles
Sécurité	Savoir qui peut accéder à quoi				■	■	■	■	■
	Savoir qui accède à quoi	■	■	■	■				
	Supprimer l'utilisation de mots de passe triviaux et adapter le niveau d'authentification au contexte	■	■						
	Contrôler et tracer les accès aux applications depuis n'importe quel point d'entrée	■	■	■					
	Renforcer les mécanismes d'authentification sur les applications et/ou sur les postes de travail	■	■						
	Maîtriser l'ouverture de son SI et l'externalisation de services	■		■					
	Disposer d'un annuaire central pour gérer les identités et les accès				■	■	■		
	Maîtriser et tracer l'allocation, la modification et le retrait des droits des utilisateurs sur le SI				■	■	■		
	Supprimer les comptes orphelins, s'assurer du non-cumul de droits toxiques					■	■	■	
	S'assurer de la clôture effective des comptes pour les personnes ayant quitté l'entreprise					■	■	■	
Ergonomie & satisfaction utilisateurs	Disposer d'une authentification unique et ergonomique pour toutes les applications	■	■	■	■				
	Rendre les utilisateurs autonomes sur la réinitialisation de leurs mots de passe		■						
	Déléguer l'authentification à des fournisseurs d'identités tiers			■					
	Uniformiser les parcours utilisateurs quel que soit le support utilisé : interne, mobile, distant, etc.		■	■					
	Offrir un portail self-service de demandes d'accès à des applications du SI				■	■	■		■
	Simplifier les processus d'affectation et de retraits de droits					■	■		
	Simplifier les tâches opérationnelles de revues						■	■	■
Coûts / ROI	Alléger la gestion des mots de passe et leur renouvellement	■	■	■					
	Standardiser et mutualiser les infrastructures d'authentification et d'autorisation		■		■				
	Simplifier l'intégration et le raccordement des nouveaux services dans le SI		■	■	■				
	Réduire les tâches administratives					■			
	Améliorer l'efficacité et la fiabilité des processus d'entrée, mobilité, sortie et d'allocation de droits				■	■	■	■	■
	Automatiser le provisionnement des comptes et des droits dans les applications du SI				■	■	■		■
	Supprimer les processus utilisant des formulaires « papier »				■	■	■		

Source (Gestion et Gouvernance des Identités et des Accès (clusir-rha.fr))

Tableau 3 : cas d'usages l'IAM/IAG

4.2 Représentation graphique IAM/IAG

La représentation graphique de la Gestion et la Gouvernance des Identités et des Accès pouvant se présenter sous différentes formes, nous avons fait le choix d'une représentation classique correspondant à l'organisation du présent document.

Figure 4: briques fonctionnelles de l'IAM/IAG

Les fiches suivantes sont présentées en tableau :

	Composant
Gestion Accès	SSO – Single Sign-On
	Fédération des identités

	Authentification forte
Gestion Identités	Annuaire d'identités
	Cycle de vie des utilisateurs
	Gestion des habilitations
Gouvernance	Revue des habilitations / Recertification
	Gestion de rôles

Tableau 4 : briques fonctionnelles de l'IAM/IAG

4.3 Gestion des accès

La gestion des accès comprend divers procédés et techniques permettant de veiller à ce que les droits d'accès soient corrects en permanence. Elle se concentre sur l'élaboration et la gestion de la matrice des accès, des dérogations étant approuvées et visées par les responsables habilités, aux éléments d'audits, etc.

4.3.1 SSO – Single Sign-On

L'acception la plus courante de ce terme est informelle et désigne la possibilité pour un utilisateur de s'authentifier une seule fois pour avoir accès à plusieurs services.

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Sécurité** • supprimer l'effet « post-it » des mots de passe connus de tous ou l'utilisation de mots de passe triviaux ; • contrôler les accès aux applications depuis n'importe quel point d'entrée ; • homogénéiser les politiques de sécurité globales du SI ; • renforcer les stratégies de mots de passe sur les applications ; • mettre en place des mécanismes de délégation de comptes ; • tracer les accès aux applications : authentifications et autorisations ; • auditer la sécurité et disposer de statistiques des accès au SI, y compris sur les postes ou les applications partagées entre plusieurs utilisateurs.	RSSI
• **Ergonomie / Confort & satisfaction des utilisateurs** • simplifier la vie des utilisateurs en facilitant l'accès aux applications du SI ; • disposer d'une authentification unique pour toutes les applications ; • rendre les utilisateurs autonomes sur la réinitialisation de leurs mots de passe ou de leurs moyens d'authentification ; • accéder à des services de type « portail SSO » ou « délégation de comptes » ;	Utilisateurs
• **Coûts d'administration** • alléger la gestion des mots de passe et leur renouvellement ; • standardiser et mutualiser les infrastructures d'authentification et d'autorisation ; • simplifier l'intégration et le raccordement des nouveaux services dans le SI ; • contrôler l'adéquation entre les licences payées et celles réellement utilisées, cas du Saas par exemple, via des rapports d'utilisation des applications.	Direction Financière Contrôle de gestion

Tableau 3 : fonctionnement du SSO

4.2.2 Fédération des identités

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Business** • accompagner le mouvement de fond vers le cloud ; • accompagner l'ouverture de son SI vers des tiers : partenaires, clients, etc. ; • faciliter les accès aux applications dans des contextes de transformation de l'entreprise : réorganisation, joint-venture, fusion/acquisition, division, etc. ; • faciliter la gestion des accès aux services mutualisés au sein d'organisations complexes ou de cercles de partenaires.	Direction Générale DSI RSSI
• **Ergonomie, services aux utilisateurs** • faciliter et uniformiser les parcours d'inscription et d'authentification à des services proposés à des utilisateurs externes ; • déléguer l'authentification à des fournisseurs d'identités tiers : France Connect, Google, Facebook, etc. ; • simplifier l'accès à des applications externes : services SaaS ou Cloud, de type O365, GoogleApps, etc. ou à des services proposés par des partenaires B2B ; • uniformiser les parcours utilisateurs sur tous les supports, Web ou mobile.	Direction Générale Marketing Digital
• **Urbanisation, standardisation** • définir un socle d'authentification indépendant des implémentations spécifiques ; • simplifier l'intégration de nouvelles applications dans le SI ; • apporter de la flexibilité et de l'agilité dans le SI ; • bénéficier de standards de fédération garantissant la sécurité et la traçabilité des accès dans une relation de confiance entre partenaires.	DSI RSSI Urbanistes du SI Architectes
• **Sécurité** • éviter de dupliquer les annuaires dans les infrastructures SaaS ou de donner un accès depuis l'extérieur à ses annuaires d'identités ou d'authentification ; • ne pas avoir à gérer les « identités des autres » ; • maîtriser l'ouverture de son SI et l'externalisation de services.	RSSI

Tableau 4 : fonctionnement du Fédération des identités

4.2.3 Authentification forte

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Sécurité** • renforcer les mécanismes d'authentification sur les applications et/ou sur les postes de travail, notamment les plus sensibles ; • adapter le niveau d'authentification au contexte utilisateur, par exemple s'il est dans le réseau de l'entreprise ou hors de ce réseau ; • garantir un bon niveau d'authentification sur les périphériques mobiles ou pour les accès distants ; • identifier les utilisateurs qui accèdent à des postes partagés, ou « kiosque », démarrés sur une session Windows générique.	RSSI
• **Conformité** • pour un acteur du monde de la Santé, être en conformité avec le décret de confidentialité et déployer la carte « CPS » pour les professionnels de santé ; • pour un acteur du monde bancaire, répondre aux exigences de la norme PCI DSS, en intégrant l'authentification à deux facteurs pour les accès distants au réseau par les employés, les administrateurs et les tiers ainsi que pour l'accès local pour les administrateurs depuis la version 3.2 de 2016 ; • pour un OIV, respecter les règles de sécurité de la LPM, notamment celles relatives à la protection des systèmes : règles 11 à 19, dont l'authentification.	RSSI Responsable conformité
• **Coûts d'administration** • alléger la gestion des mots de passe et leur renouvellement ;	Direction financière

Tableau 5 : fonctionnement du Fédération de l'authentification forte

4.3 Gestion des identités

La gestion des identités s'intéresse par exemple au contrôle de la façon dont les utilisateurs acquièrent une identité, la protection de cette identité et les technologies permettant cette protection.

4.3.1 Annuaire d'identités

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Urbanisation du système d'information** • constituer un référentiel central, unique et fiable, pour tous les autres référentiels ou applications du SI ; • satisfaire aux prérequis à la mise en œuvre de services liés à la notion d'identité : gestion des identités, des habilitations – Cf. fiches suivantes.	DSI Urbanistes du SI Architectes
• **Sécurité** • disposer d'un annuaire central pour fédérer les identités ; • préparer sa gestion centralisée des accès et son annuaire d'authentification. Cf. fiche « Gestion des habilitations » et fiches « Access Management ».	RSSI DSI
• **Services utilisateurs** • mettre à disposition des services de pages blanches d'entreprise, organigrammes, et localisation géographique des collaborateurs.	Tous

Tableau 6 : fonctionnement de l'annuaire d'identité

4.3.2 Cycle de vie des utilisateurs

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Sécurité** • provisionner les identités : créer l'identité des nouveaux arrivants, prendre en compte les mouvements de personnes et les changements de situation, harmoniser les données dans les différents référentiels ; • conformité : prendre en compte les mutations et les départs ; • faciliter la réalisation d'audits et de contrôles.	DSI Risques et audit Métiers RSSI
• **Retour sur investissement** • diminuer la part des tâches administratives ; • remplacer les formulaires « papier ».	DRH, DAF DSI
• **Urbanisation** • disposer d'un annuaire utilisateur à jour et de référence.	DSI Métiers

Tableau 7 : fonctionnement du cycle de vie des utilisateurs

4.3.3 Gestion des habilitations

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Sécurité** • maîtriser et tracer l'allocation, la modification et le retrait des droits des utilisateurs sur le SI ; • produire des rapports sur les habilitations permettant de savoir qui a accès à quoi ; • contrôler le retrait des droits et désactiver automatiquement les comptes après la date de départ de l'utilisateur ; • sensibiliser les valideurs impliqués dans l'attribution de droits ; • réduire le risque opérationnel lié à l'utilisation de processus manuels ; • protéger le secret industriel grâce au contrôle des droits	RSSI Risque Conformité DSI
• **Audit / Conformité** • répondre aux contraintes du contrôle interne, des régulateurs, des commissaires aux comptes ou autres autorités de tutelles ; • faciliter les revues d'habilitations. Cf. fiche « revues d'habilitations » ; • permettre le contrôle du respect du principe de la SoD.	RSSI Risque Conformité Finance / DAF
• **Urbanisation** • disposer d'un annuaire et référentiel utilisateur à jour ; • disposer d'un référentiel central d'habilitations pour les applications.	DSI Urbanistes du SI Architectes
• **Confort / fonctionnalités / services** • fournir du confort aux utilisateurs via des procédures automatisées ; • gérer les habilitations sur les applications Cloud/externes ; • offrir un portail self-service de demande d'accès à des applications du SI.	DSI Utilisateurs

Tableau 8 : fonctionnement gestion des habilitations

4.4 Gouvernance des accès et identités

Il s'agit de superviser les comportements des utilisateurs du système d'information sur tous leurs terminaux, qu'il s'agisse d'employés, de clients ou même d'objets accédant légitimement aux ressources partagées.

4.5.1 Revue des habilitations

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Sécurité / diminution des risques opérationnels** • supprimer les comptes orphelins ; • s'assurer de la bonne fermeture des comptes pour les personnes parties ; • s'assurer que chaque personne possède bien le minimum de droits suffisants et nécessaires sur le SI ; • contrôler les droits sur les comptes génériques et leur association aux personnes physiques ; • s'assurer, pour chaque application et chaque ressource, que seules les personnes autorisées peuvent y accéder, et selon leur fonction.	RSSI Contrôle interne Risques
• **Audits réglementaires ou d'organes de tutelle** • fournir des preuves de revues ; • fournir des preuves de suivi de plan d'actions post-revues.	DAF DG
• **Lutte contre la fraude** • s'assurer du non-cumul de droits toxiques.	DAF Risques
• **Coûts** • réduire le coût des licences applicatives en s'assurant que les comptes inutiles sont supprimés.	DSI DAF

Tableau 9 : fonctionnement revue des habilitations

4.5.2 Gestion de rôles

Exemples d'arguments	*Interlocuteur(s) concerné(s)*
• **Sécurité et diminution des risques opérationnels** • s'assurer simplement que, pour une fonction donnée, seuls les droits nécessaires sont affectés : ajout d'un ou plusieurs rôles correspondant à la fonction ; • s'assurer du retrait des anciens droits lors d'une mutation.	RSSI Contrôle interne Risques
• **Audits réglementaires ou d'organes de tutelle** • disposer d'une documentation justifiée des rôles existants : valideurs, contenu ; • répondre à certains audits qui mentionnent simplement de « mettre en place une gestion par rôles », ce qui peut être discutable puisqu'il s'agit plus d'un moyen que d'un but.	DAF DG
• **Lutte contre la fraude** • une matrice de SoD basée sur les rôles est généralement plus facile à maintenir qu'une matrice basée sur des droits fins.	DAF Risques
• **Expérience utilisateur** • simplifier les processus d'affectation et de retrait de droits ; • simplifier les tâches opérationnelles de revue ; • éviter aux exploitants et aux utilisateurs d'avoir à connaître tous les rôles.	Utilisateurs

Tableau 10 : fonctionnement gestion de rôles

3ème partie :

MISE EN ŒUVRE

Dans cette partie, il s'agira de décrire le travail que nous avons eu à effectuer. Dans un premier temps nous aurons à décrire le processus d'utilisation de l'outil de pointage Safescan (que nous présenterons), ensuite nous allons procéder à l'installation et à la configuration de la gestion d'accès de données sous Windows server.

CHAPITRE 5 : Contrôle d'accès physique

5.1 Introduction

La sécurité en entreprise est un point primordial pour protéger les biens et le personnel d'une société. Pour assurer la sûreté d'un bâtiment rien de tel que de se munir d'un système de contrôle d'accès. Le contrôle d'accès désigne les différentes solutions techniques qui permettent de sécurité et gérer les points d'accès et de sortie d'un bâtiment. Nous allons vous démontrer l'importance du contrôle d'accès dans la sécurité d'une entreprise.
Deux (02) dispositifs sont mis en place pour l'accès au bâtiment da la direction :

- ✓ Un lecteur RFFI DAHUA pour l'accès de la porte
- ✓ Un outil Safescan qui enregistre les flux d'accès.

5.2 Lecteur RFID DAHUA

5.2.1 RFID :

La radio-identification, le plus souvent désignée par le sigle RFID (de l'anglais radio frequency identification), est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« RFID tag » ou « RFID transponder » en anglais).

5.2.2 Lecteur RFID DAHUA

Il permet de DOMEOO sécuriser vos locaux et gérez l'accès de vos bâtiments avec un système de contrôle d'accès soit par un badge personnel, soit via un dispositif biométrique.

Figure 5: lecteur RFID DAHUA

5.3 Présentation et utilisation de l'outil SAFESCAN

La Safescan TA-8010 est un appareil intelligent qui associe les dernières technologies en matière de proximité RFID à un logiciel de gestion complet qui permet à vos employés d'enregistrer facilement leurs heures d'arrivée et de départ tout en vous procurant d'excellents outils pour gérer de manière efficace le temps de travail de vos employés. Le logiciel de pointage TA met à votre disposition une gamme complète d'outils de présentation et de gestion. Vous aurez toujours - même en temps réel - le plein contrôle sur les heures travaillées de vos employés. Avec ses nombreuses fonctions pratiques et pratiques, le logiciel Safescan TA est tout ce que vous avez besoin pour une gestion efficace de vos employées.

Figure 6: dispositif Safescan

5.3.1 Types identification

Identifiant + Mot de passe	*Avantages*	• Facile à mettre en œuvre
	Inconvénients	• Nécessite une politique de mot de passe complexe • Les mots de passe peuvent être craqués, par force brute par exemple • Gestion des oublis des mots de passe
	Ergonomie	• Gestion de mots de passe multiples • Notation des identifiants sur post-it • « Irritant » pour l'utilisateur
	Sécurité	• Faible
	Coût	• Moyen
RFID	*Avantages*	• Facile à déployer • Pas de mot de passe à retenir • Supports RFID variés
	Inconvénients	• Nécessite des lecteurs RFID • Sécurité de la transaction carte-lecteur faible • Risque de perte/vol/casse du support
	Ergonomie	• Pas de code PIN pour sécuriser l'accès au support • Support multi-services : couplage avec le contrôle d'accès physique par exemple
	Sécurité	• Faible
	Coût	• Faible

Tableau 11 : type d'identification pour émargement sur le dispositif Safescan

5.3.2 Liste des agents

Ci-dessous la liste de tous les utilisateurs qui ont été créé dans l'application du TA.

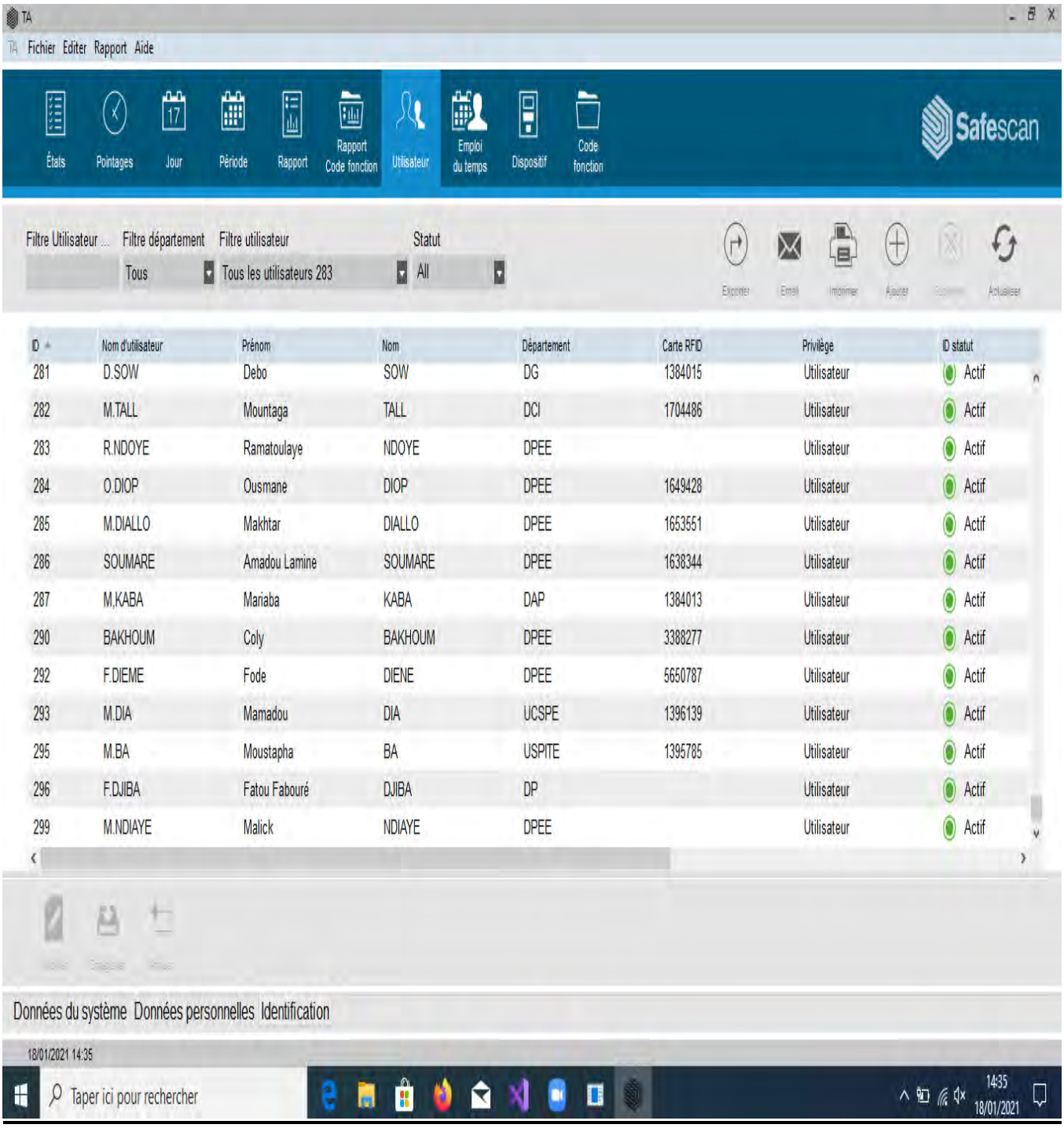


Figure 7 : liste de tous les agents

5.3.3 Synchronisation des données ajoutées avec le dispositif TA

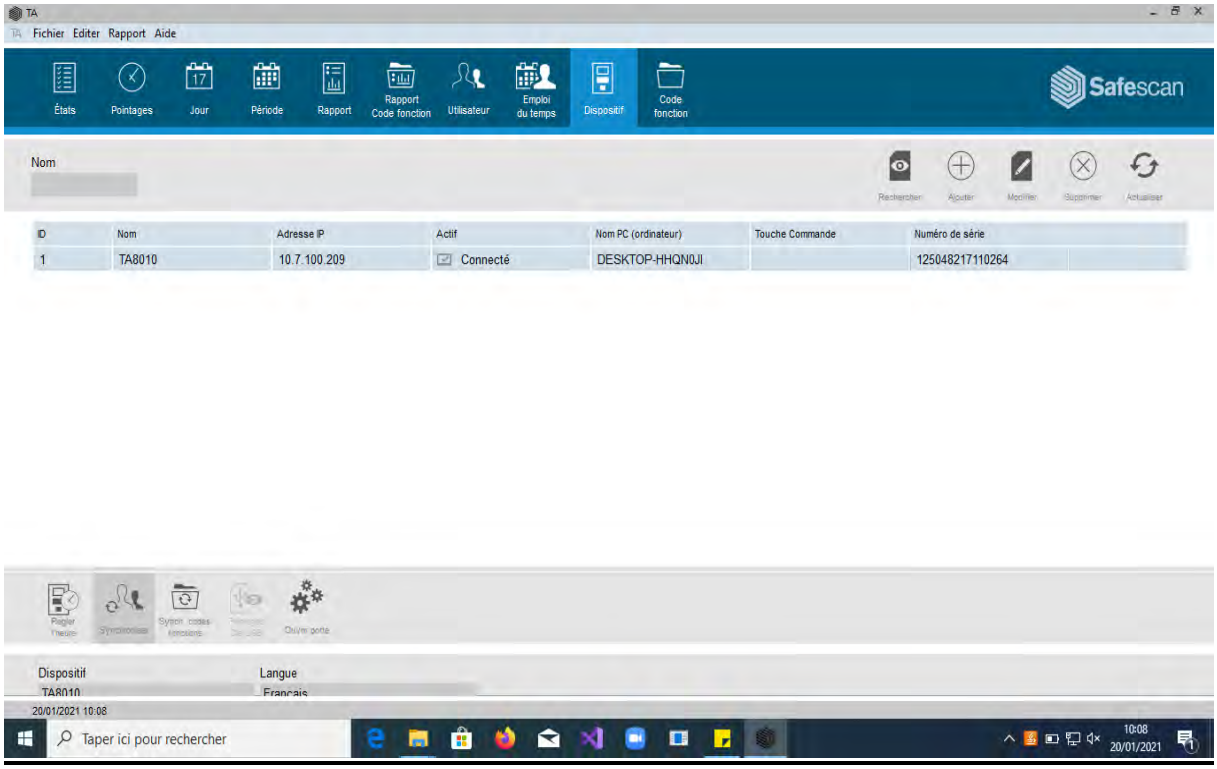


Figure 8 : récupération code RFID pour le nouvel utilisateur ajouté

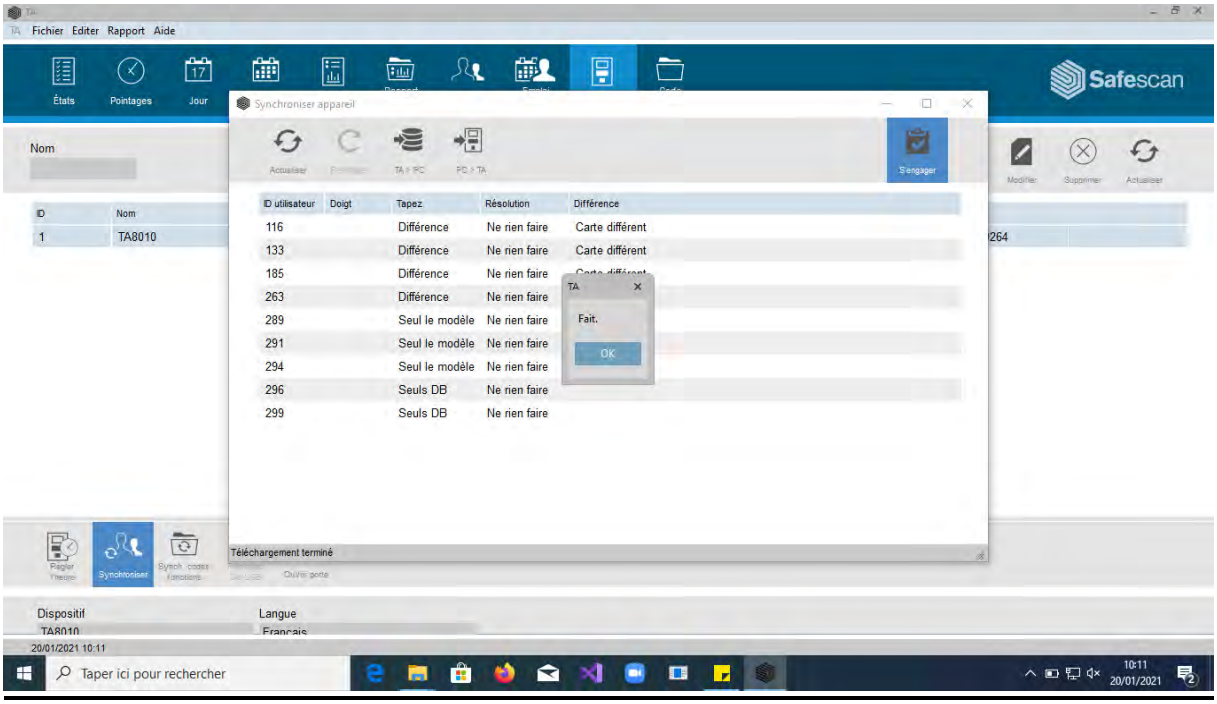


Figure 9 : synchronisation réussie

5.3.4 Interface de pointage des utilisateurs

Ci-dessous la liste des agents qui ont émargé selon une date demandée ainsi que leurs détails (heure de pointage, type …).

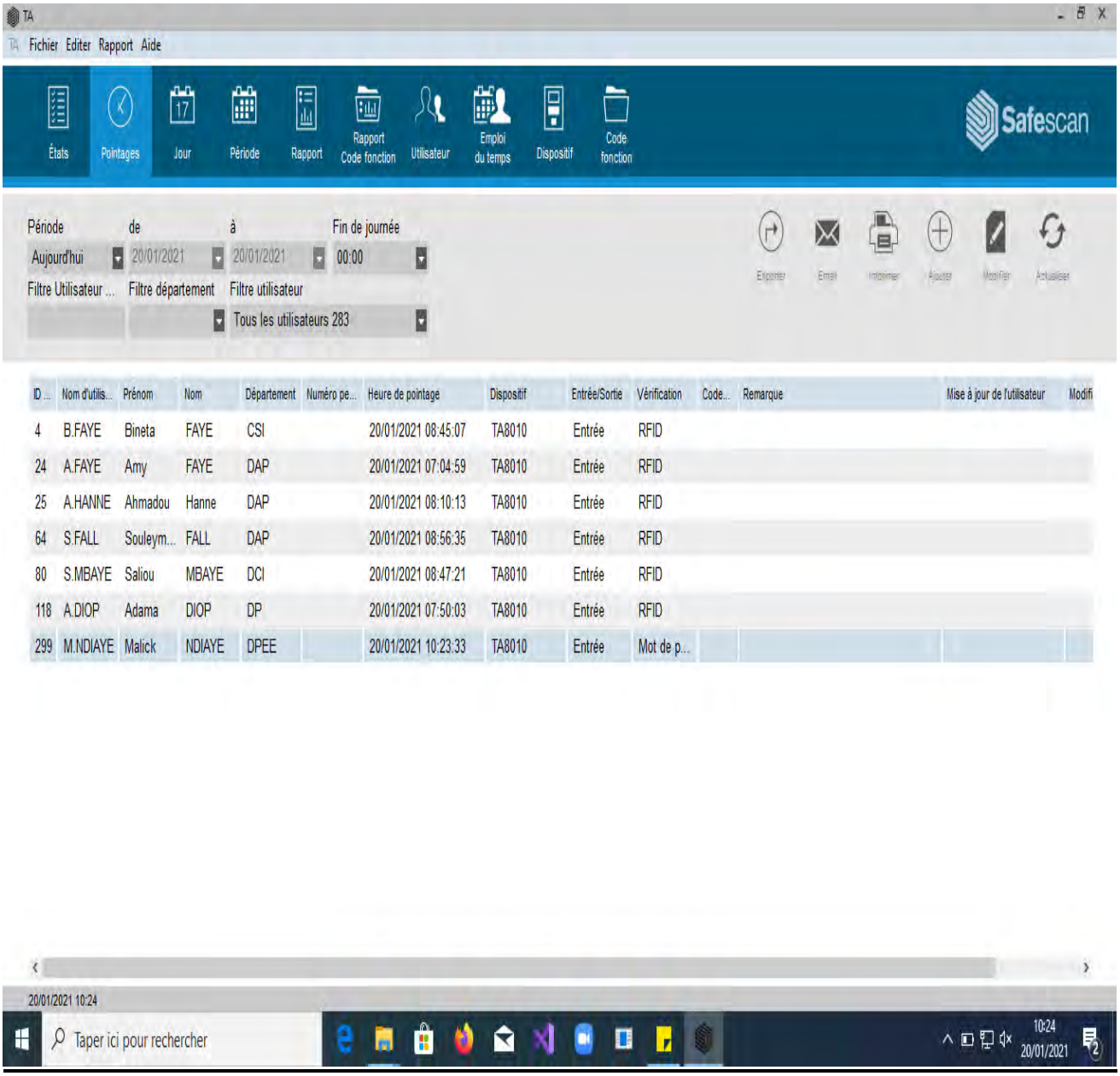


Figure 10 : Pointages des agents

5.3.5 Interface Code fonction

Permet d'enregistrer les évènements exceptionnels et jours fériés.

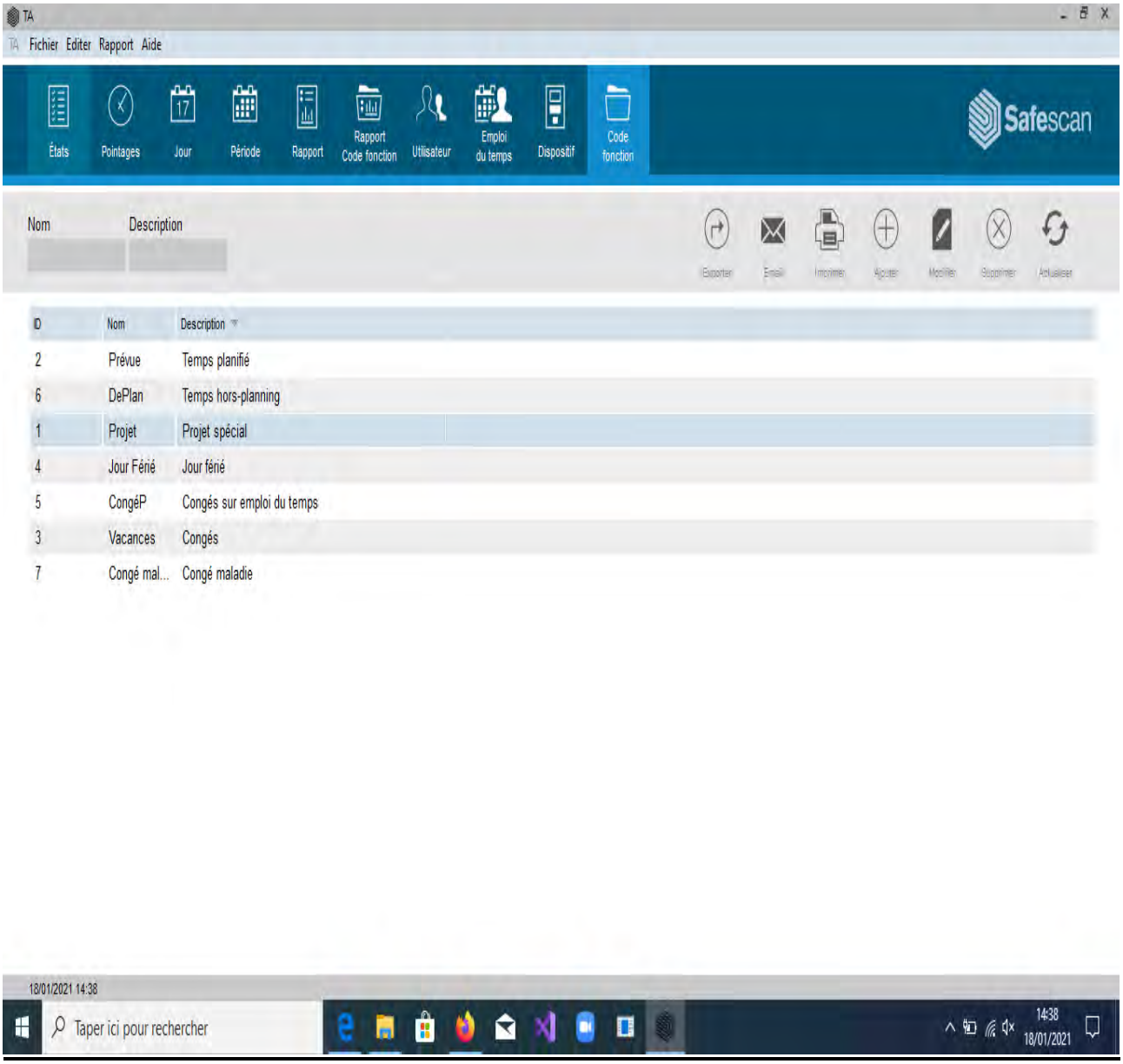


Figure 11 : code fonction

5.3.6 Rapports d'émargement

Date: 29/01/2021
Temps: 11:53

Rapport mensuel

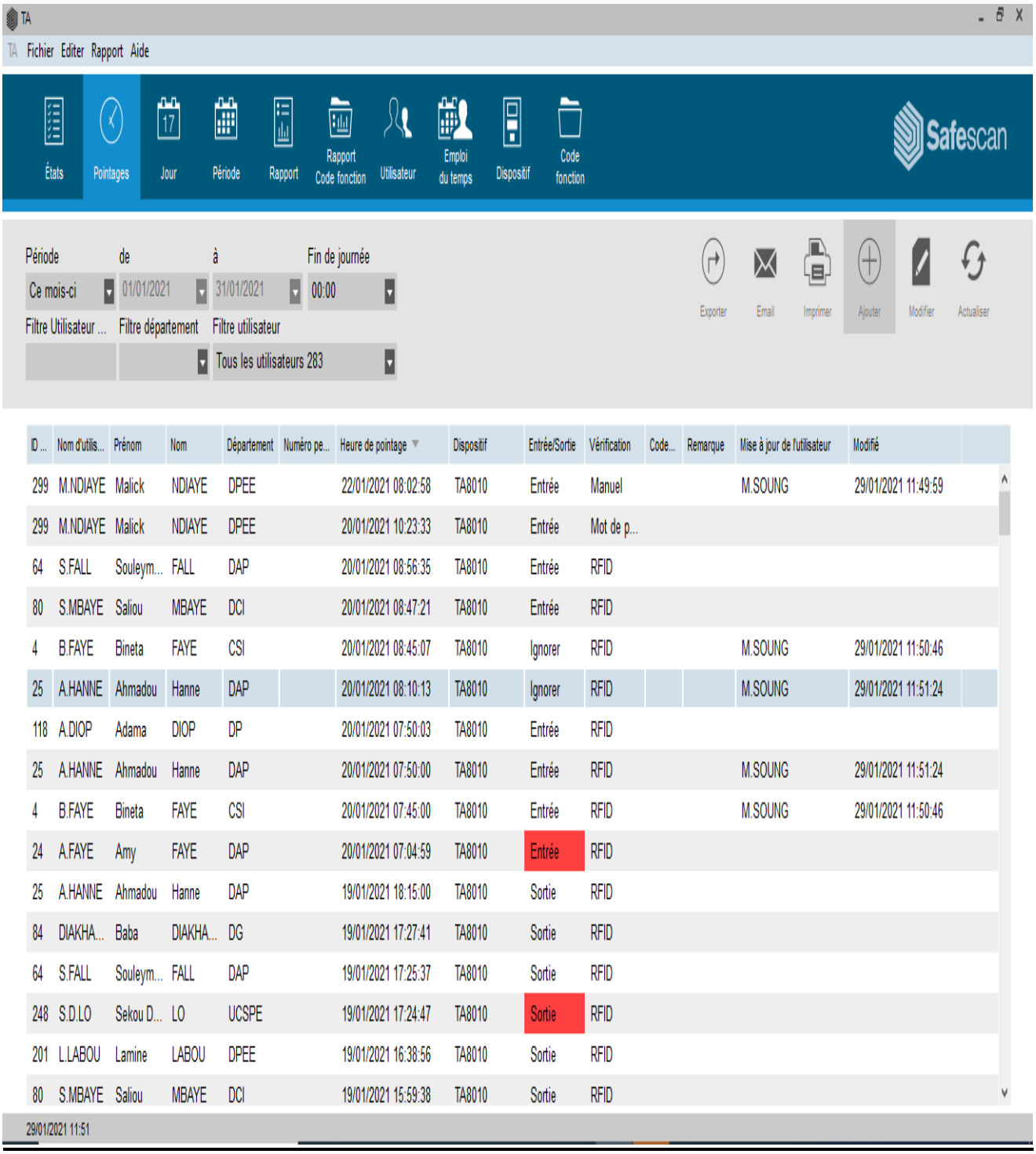
01/01/2021 - 31/01/2021

Nom: **Bineta FAYE** ID: **4** Groupe calendrier: Standard
Département: CSI Numéro personnel:

Date	Jour	Entrée	Sortie	Emploi du temps	Heures	Saldo	Cumm.	Absent	Remarques / Codes de fonction
01/01	Ve	-	-	8:00	-	-	-8:00	8:00	Absent
02/01	Sa	-	-	-	-	-	-8:00	-	
03/01	Di	-	-	-	-	-	-8:00	-	
Semaine	1			8:00	-	-8:00			
04/01	Lu	-	-	8:00	-	-	-16:00	8:00	Absent
05/01	Ma	-	-	8:00	-	-	-24:00	8:00	Absent
06/01	Me	08:34	16:30	8:00	7:56	-0:04	-24:04	-	Dépointé par le système
07/01	Jeu	-	-	8:00	-	-	-32:04	8:00	Absent
08/01	Ve	08:35	16:30	8:00	7:55	-0:05	-32:09	-	Dépointé par le système
09/01	Sa	-	-	-	-	-	-32:09	-	
10/01	Di	-	-	-	-	-	-32:09	-	
Semaine	2			40:00	15:51	-24:09			
11/01	Lu	08:36	16:30	8:00	7:54	-0:06	-32:15	-	Dépointé par le système
12/01	Ma	-	-	8:00	-	-	-40:15	8:00	Absent
13/01	Me	-	-	8:00	-	-	-48:15	8:00	Absent
14/01	Jeu	08:39	16:30	8:00	7:51	-0:09	-48:24	-	Dépointé par le système
15/01	Ve	08:40	16:30	8:00	7:50	-0:10	-48:34	-	Dépointé par le système
16/01	Sa	-	-	-	-	-	-48:34	-	
17/01	Di	-	-	-	-	-	-48:34	-	
Semaine	3			40:00	23:35	-16:25			
18/01	Lu	-	-	8:00	-	-	-56:34	8:00	Absent
19/01	Ma	-	-	8:00	-	-	-64:34	8:00	Absent
20/01	Me	07:45	16:30	8:00	8:45	0:45	-63:49	-	Dépointé par le système
21/01	Jeu	-	-	8:00	-	-	-71:49	8:00	Absent
22/01	Ve	-	-	8:00	-	-	-79:49	8:00	Absent
23/01	Sa	-	-	-	-	-	-79:49	-	
24/01	Di	-	-	-	-	-	-79:49	-	
Semaine	4			40:00	8:45	-31:15			
25/01	Lu	-	-	8:00	-	-	-87:49	8:00	Absent
26/01	Ma	-	-	8:00	-	-	-95:49	8:00	Absent
27/01	Me	-	-	8:00	-	-	-103:49	8:00	Absent
28/01	Jeu	-	-	8:00	-	-	-111:49	8:00	Absent
29/01	Ve	-	-	8:00	-	-	-119:49	8:00	Absent
30/01	Sa	-	-	-	-	-	-119:49	-	
31/01	Di	-	-	-	-	-	-119:49	-	
Semaine	5			40:00	-	-40:00			
Total				**168:00**	**48:11**	**-119:49**			

Figure 12 : rapport d'émargement mensuel d'un agent

5.4 Audit des tentatives de manipulation de données



ID ...	Nom d'utilis...	Prénom	Nom	Département	Numéro pe...	Heure de pointage	Dispositif	Entrée/Sortie	Vérification	Code...	Remarque	Mise à jour de l'utilisateur	Modifié
299	M.NDIAYE	Malick	NDIAYE	DPEE		22/01/2021 08:02:58	TA8010	Entrée	Manuel			M.SOUNG	29/01/2021 11:49:59
299	M.NDIAYE	Malick	NDIAYE	DPEE		20/01/2021 10:23:33	TA8010	Entrée	Mot de p...				
64	S.FALL	Souleym...	FALL	DAP		20/01/2021 08:56:35	TA8010	Entrée	RFID				
80	S.MBAYE	Saliou	MBAYE	DCI		20/01/2021 08:47:21	TA8010	Entrée	RFID				
4	B.FAYE	Bineta	FAYE	CSI		20/01/2021 08:45:07	TA8010	Ignorer	RFID			M.SOUNG	29/01/2021 11:50:46
25	A.HANNE	Ahmadou	Hanne	DAP		20/01/2021 08:10:13	TA8010	Ignorer	RFID			M.SOUNG	29/01/2021 11:51:24
118	A.DIOP	Adama	DIOP	DP		20/01/2021 07:50:03	TA8010	Entrée	RFID				
25	A.HANNE	Ahmadou	Hanne	DAP		20/01/2021 07:50:00	TA8010	Entrée	RFID			M.SOUNG	29/01/2021 11:51:24
4	B.FAYE	Bineta	FAYE	CSI		20/01/2021 07:45:00	TA8010	Entrée	RFID			M.SOUNG	29/01/2021 11:50:46
24	A.FAYE	Amy	FAYE	DAP		20/01/2021 07:04:59	TA8010	Entrée	RFID				
25	A.HANNE	Ahmadou	Hanne	DAP		19/01/2021 18:15:00	TA8010	Sortie	RFID				
84	DIAKHA...	Baba	DIAKHA...	DG		19/01/2021 17:27:41	TA8010	Sortie	RFID				
64	S.FALL	Souleym...	FALL	DAP		19/01/2021 17:25:37	TA8010	Sortie	RFID				
248	S.D.LO	Sekou D...	LO	UCSPE		19/01/2021 17:24:47	TA8010	Sortie	RFID				
201	L.LABOU	Lamine	LABOU	DPEE		19/01/2021 16:38:56	TA8010	Sortie	RFID				
80	S.MBAYE	Saliou	MBAYE	DCI		19/01/2021 15:59:38	TA8010	Sortie	RFID				

Figure 13 : audit manipulation données

5.5 Propositions d'amélioration du système de pointage

L'étude du système d'émargement électronique existant au sein de la Direction générale nous conduit à faire des propositions techniques sous la forme d'un tableau classé par ordre de priorité pour améliorer les outils pour une meilleure sécurité d'accès.

DESIGNATION	Justificatif(s)	Qté
Badgeuse par empreinte TA-8025 Safescan 	✓ Pointer facilement et rapidement : les employés n'ont qu'à passer le badge, le porte clé RFID ou leur doigt puisque le terminal permet le pointage par empreinte digitale. ✓ Un logiciel complet et efficace inclus : le logiciel de pointage TA permet de créer des rapports de données, de créer des emplois du temps et même d'exporter des données sur des fichers excel. ✓ Une installation murale rapide : fourni avec un kit d'installation murale, cette pointeuse est simple à installer. Il suffit de disposer d'une connexion internet. ✓ Une pointeuse pour se connecter même en wifi : pas besoin d'avoir un câble Ethernet là où vous souhaitez installer la pointeuse, vous pouvez l'installer là où vous voulez.	**2**
Barrière de sécurité (tourniquets de sécurité) 	Puisque certains sites ont besoin d'une haute sécurité grâce à des obstacles toute hauteur. Nous suggérons les tourniquets de sécurité, dispositifs de contrôle d'accès utilisés en extérieur qui verrouillent le périmètre de sites sensibles.	**1**

SYSTÈME DE CONTRÔLE D'ACCÈS 	MA300: système de Contrôle d'accès étanche avec empreintes + Badges RFID	**2**
SYSTÈME DE VIDÉOSURVEILLANCE 	Ce système permet de disposer d'une vidéosurveillance d'une structure de haute qualité et pouvant être associée à votre système de détection. Il permet : - Surveillance extérieure en couplant la vidéo surveillance avec des détecteurs de mouvement - Possibilité de disposer de caméras orientables, de caméras dôme ou de caméras bullets - Vision nocturne infrarouge et caméras thermiques	**1**

Tableau 12 : récapitulatif des besoins de matériels pour l'accès physique par ordre de priorité

CHAPITRE 6 : 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 maitrise 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

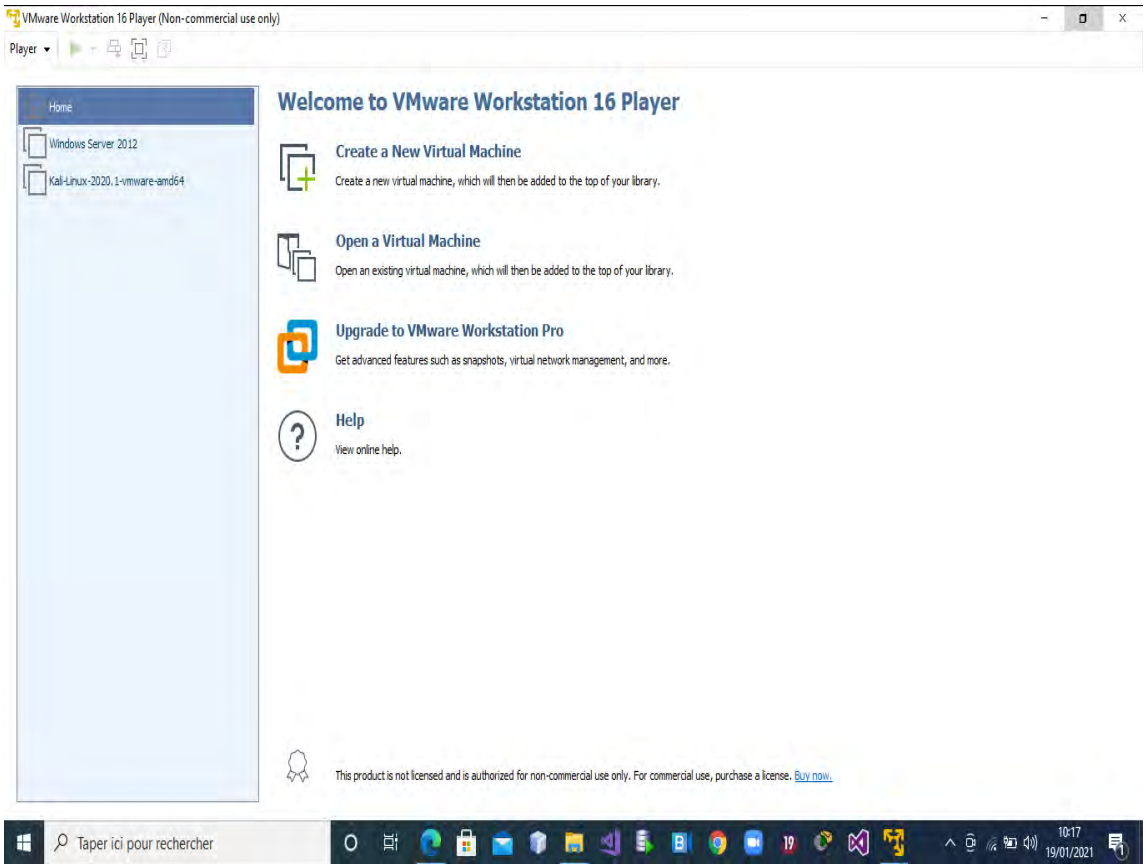


Figure 14 : interface d'accueil VMware

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 1er octobre 2014 en phase de développement et est prévu pour le 3e 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 1er 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 1er 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.

Windows Server 2012	
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 Datacenter[1].

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 physique[2].

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 virtuelle[2].

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 2012[3]. 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.

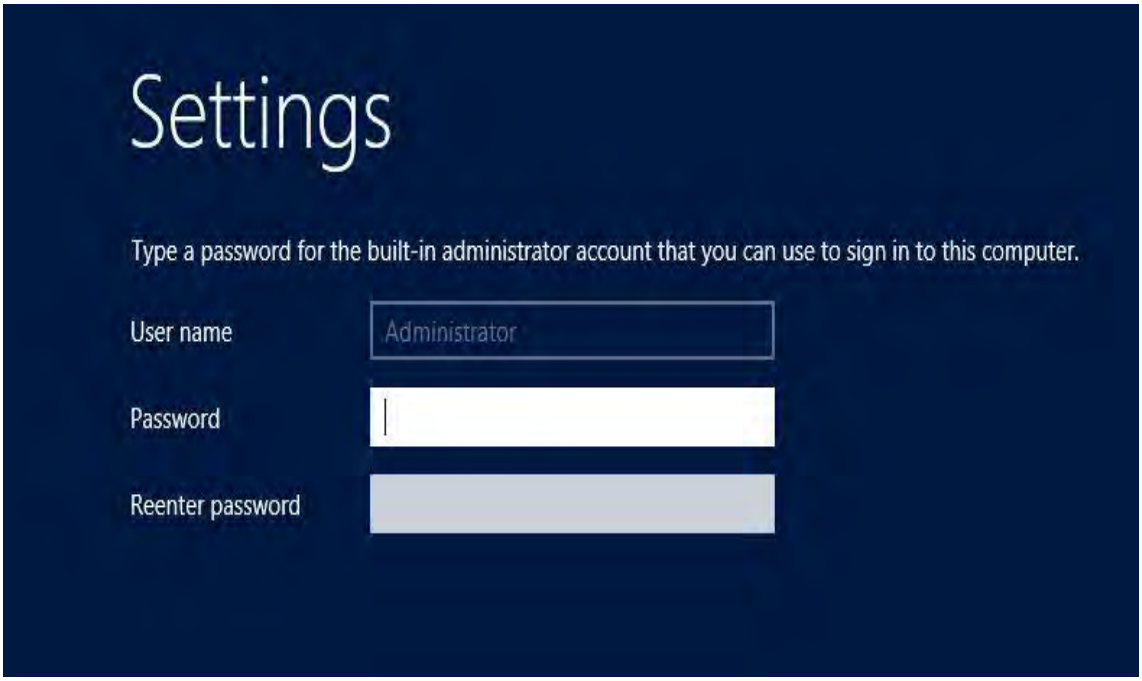


Figure 16 : interface connexion

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

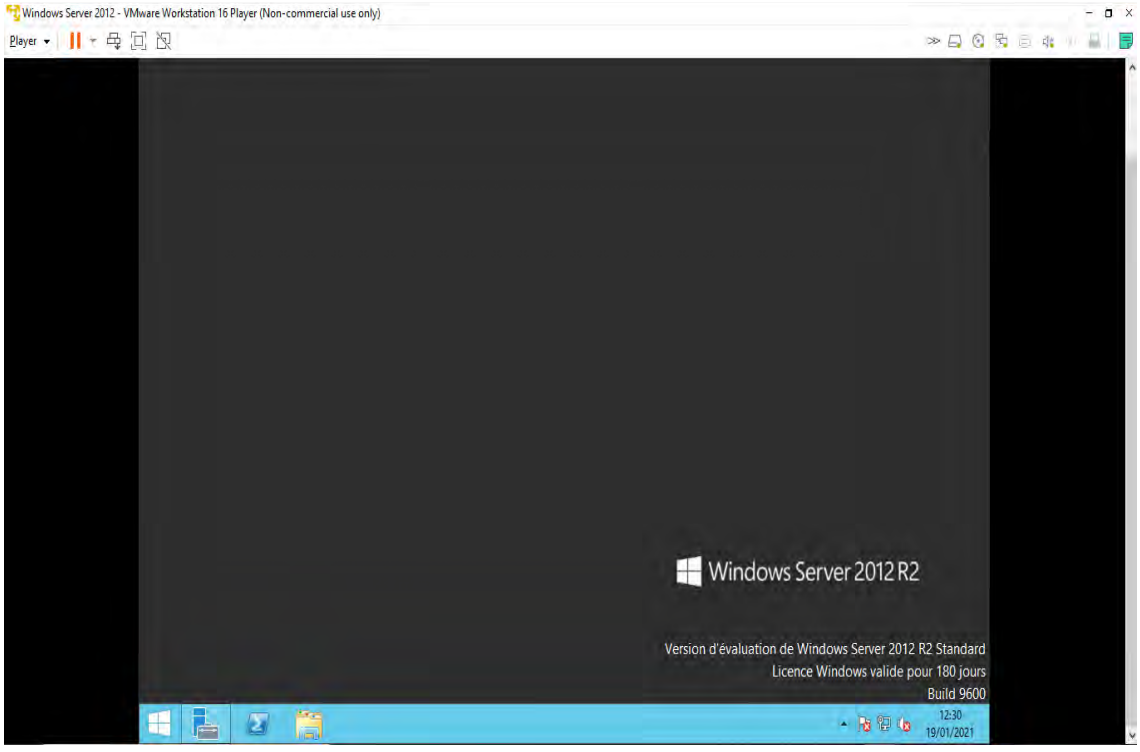


Figure 17 : interface d'accueil Windows server R2

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 nativement[1]. 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**

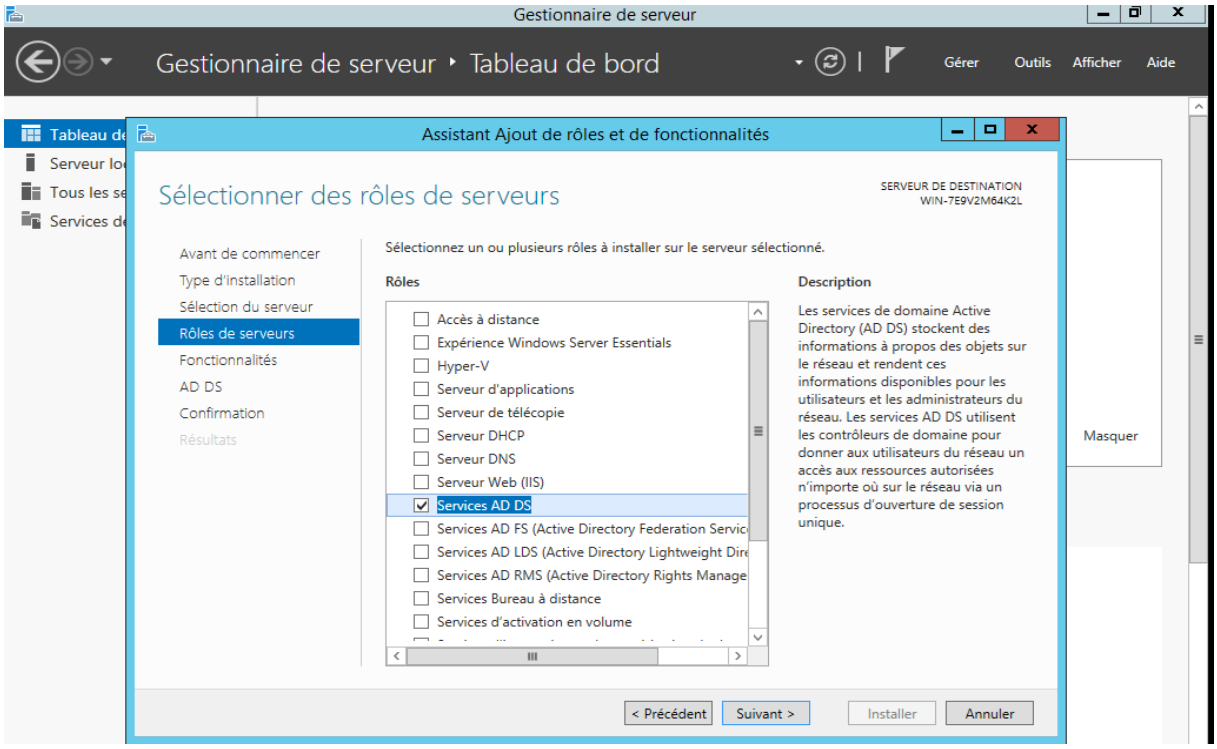


Figure 18: liste des fonctionnalités AD

Puis cliquer sur suivant pour poursuivre l'installation.

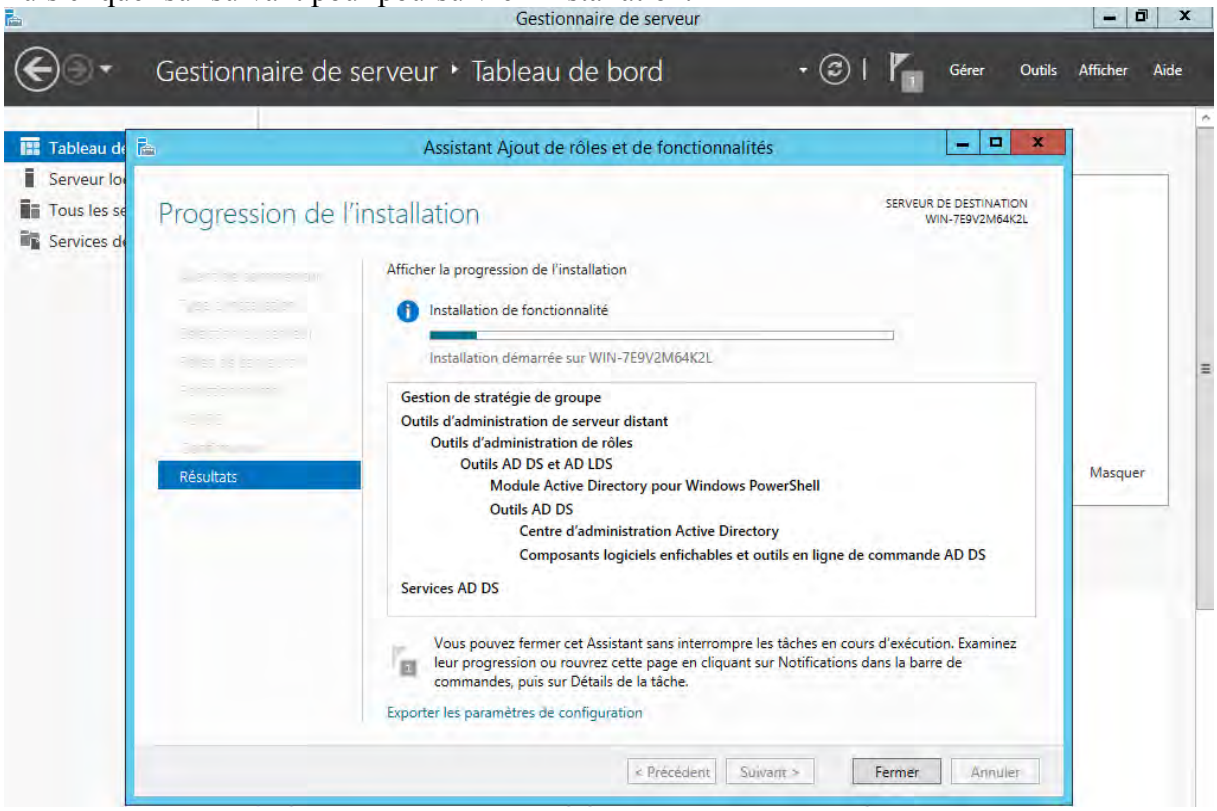


Figure 19 : progression d'installation Active Directory

➢ Ajout Foret

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.

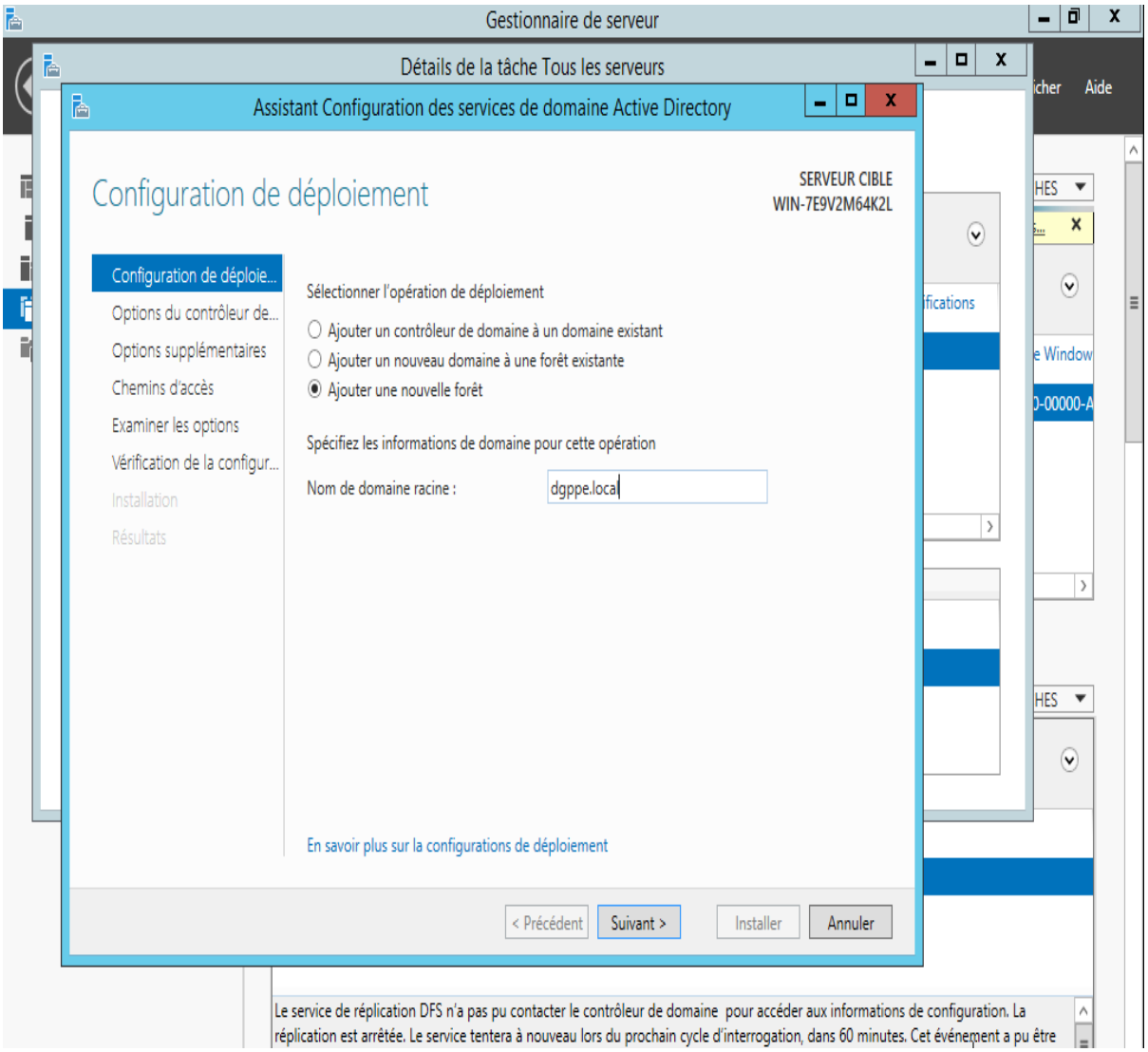


Figure 20 : ajout d'un foret dgppe.local

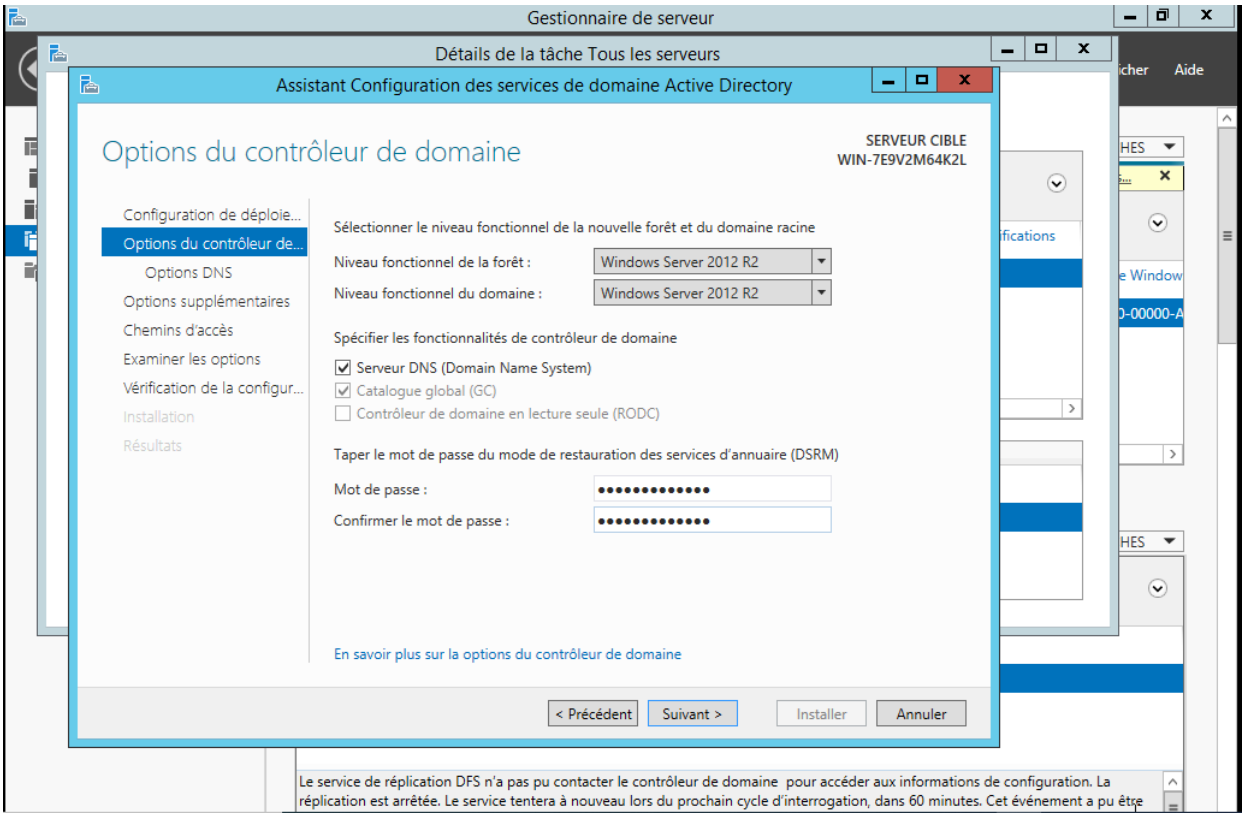


Figure 21 : option du contrôleur de domaine

Apres l'installation d'AD

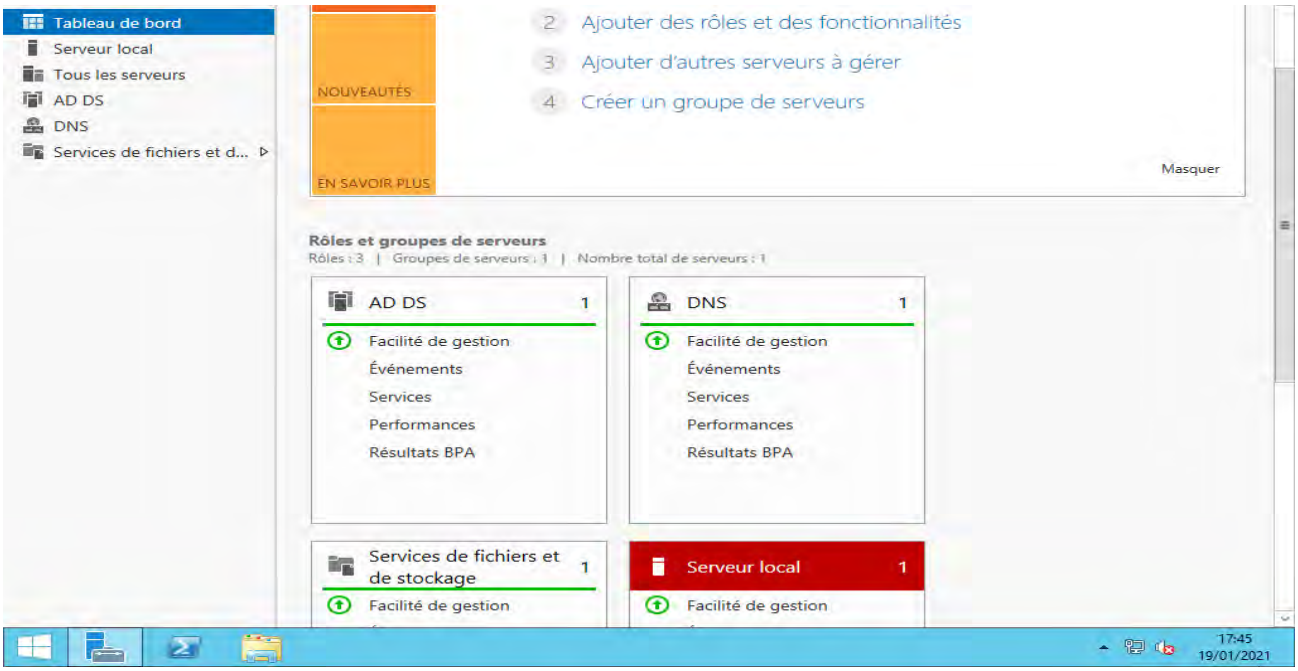


Figure 22 : vérification de l'installation AD

6.3.2 Création 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 :**

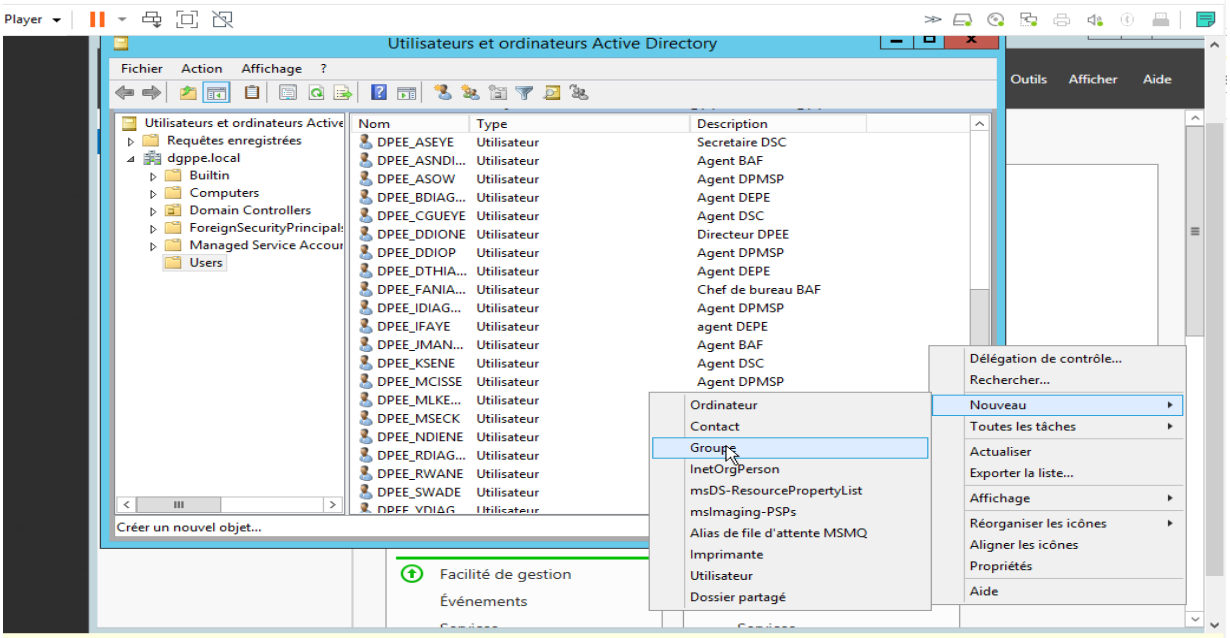


Figure 23 : ajout nouveau groupe

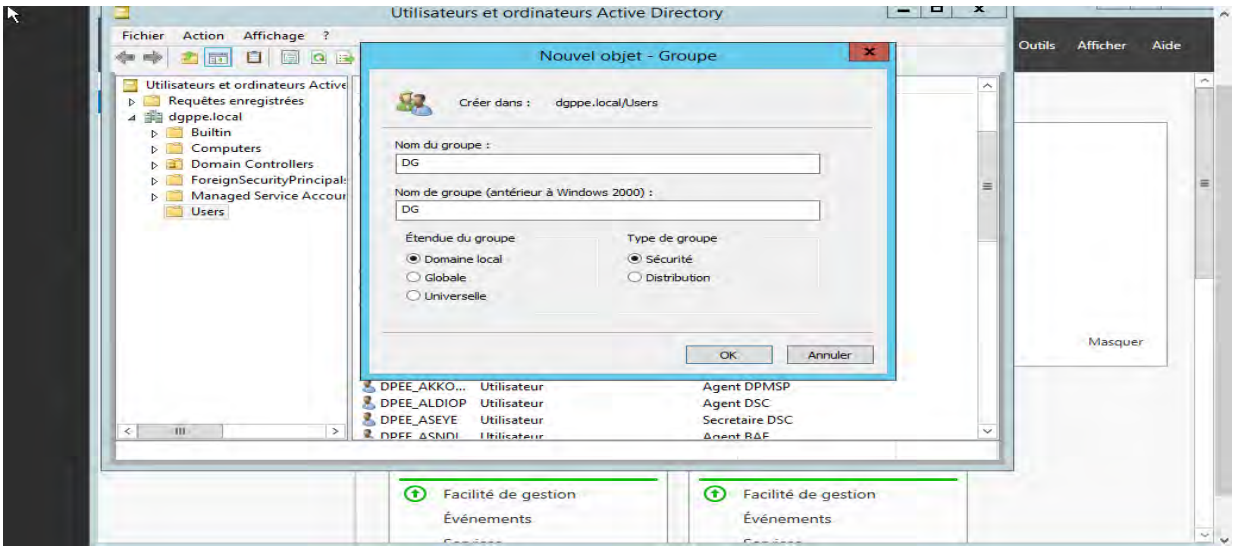


Figure 24 : interface pour création groupe

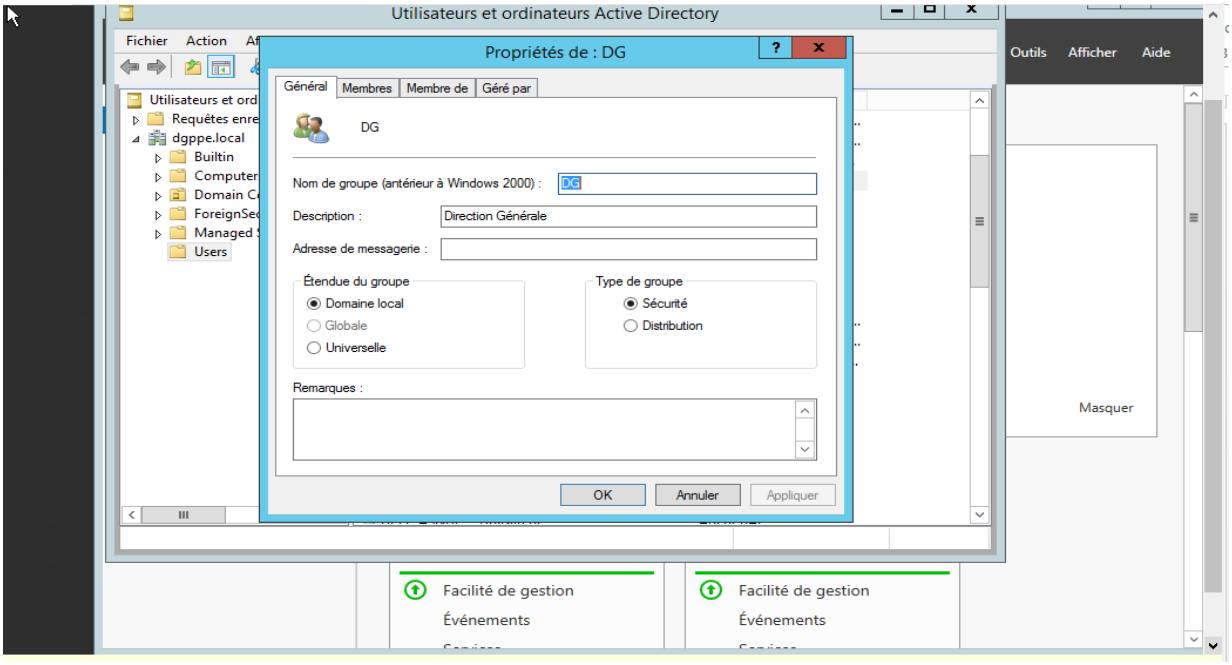


Figure 25 : interface ajout groupes sur AD

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.

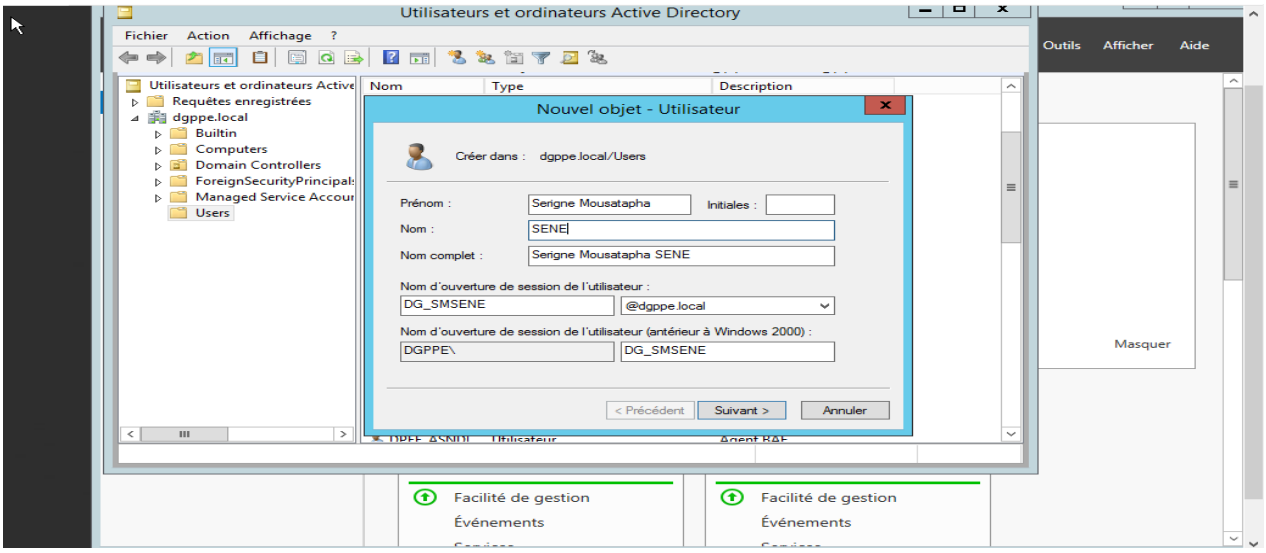


Figure 26 : interface ajout utilisateurs

▪ 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**.

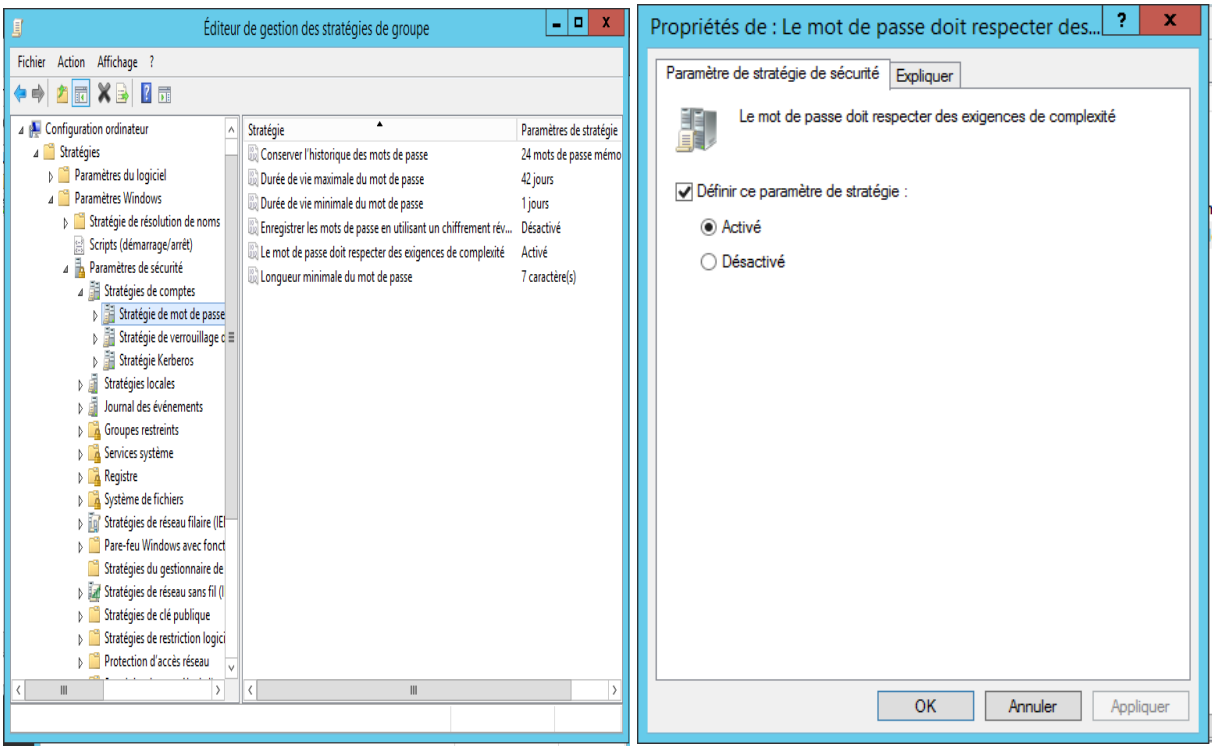


Figure 27 : interfaces Editeur de gestion des stratégies de groupe

- **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 :
Structrure_1er 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.

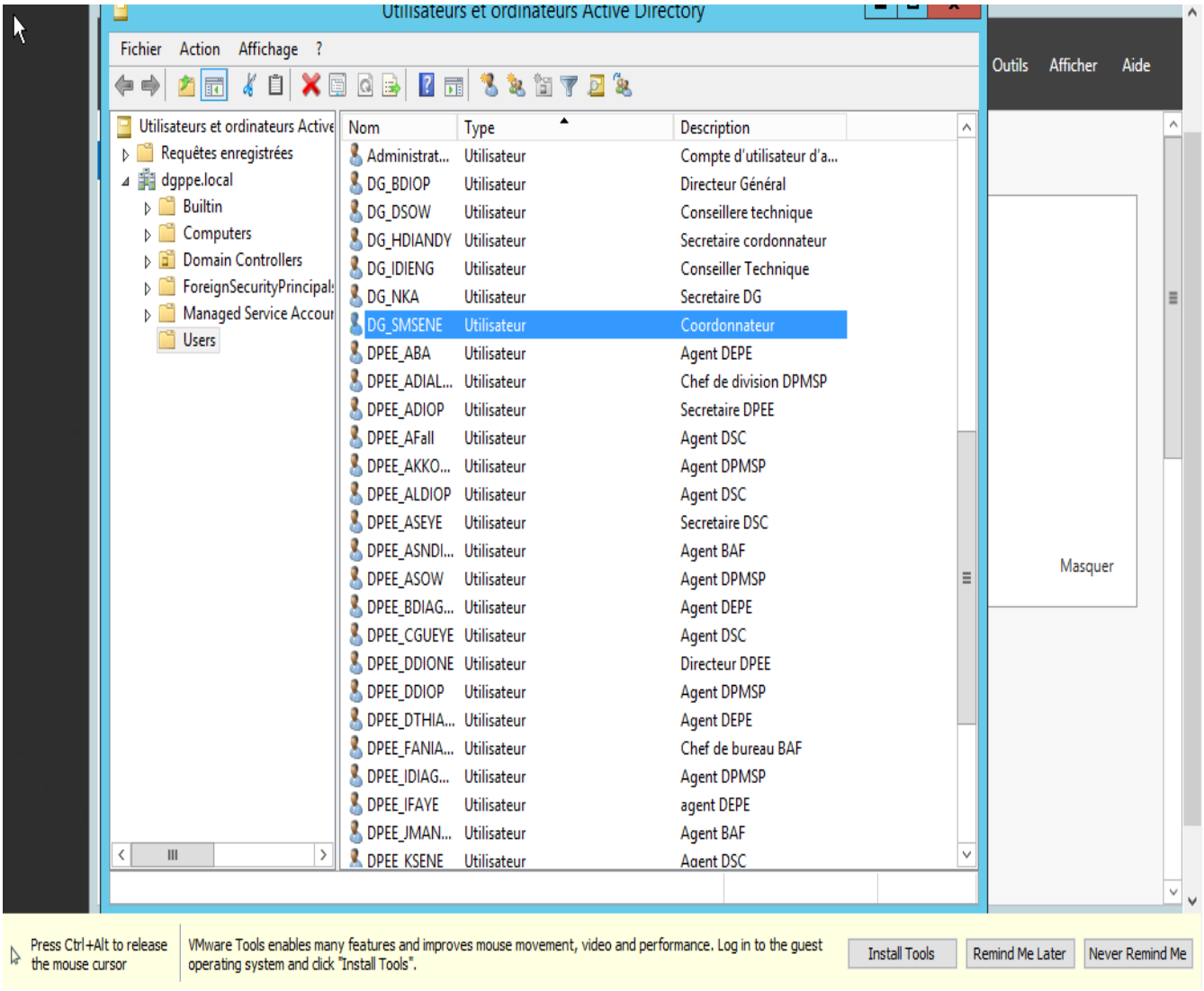


Figure 28 : liste des utilisateurs

- **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.

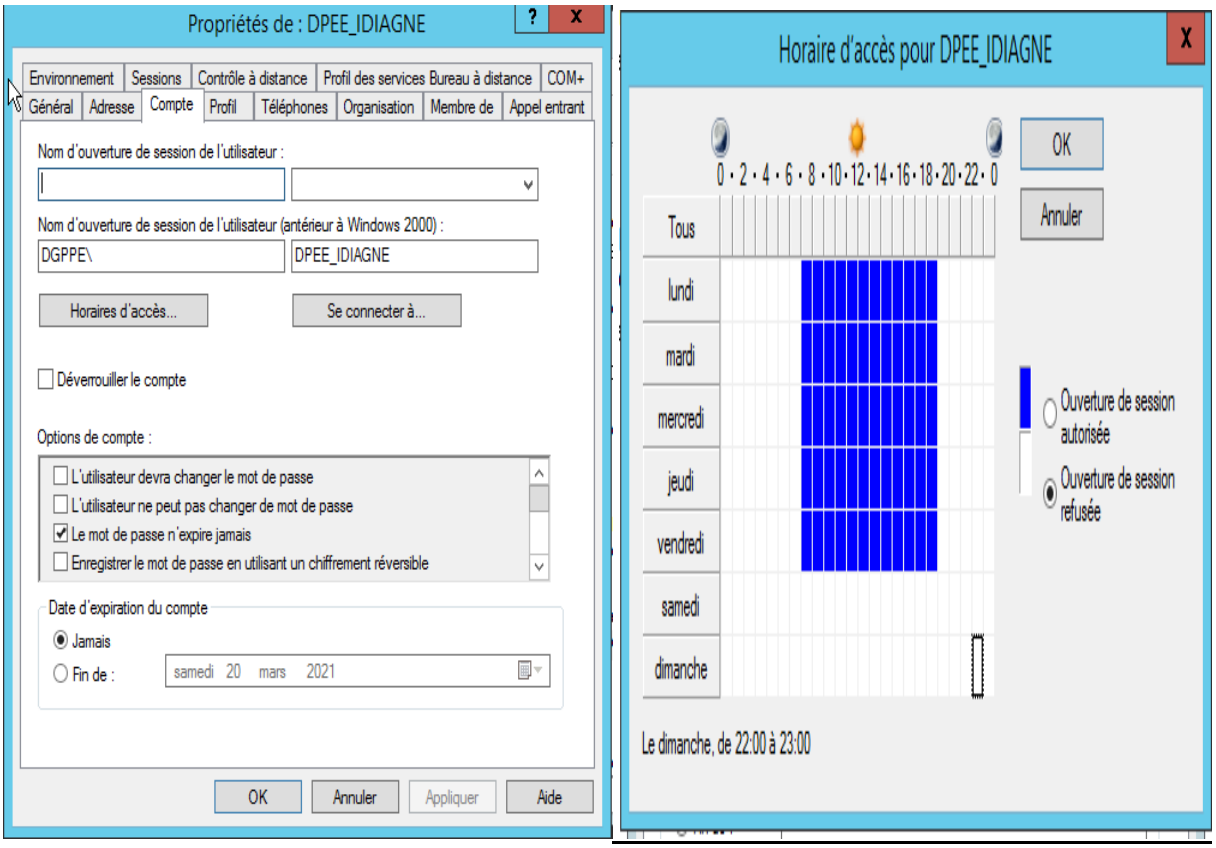


Figure 29 : horaire d'accès d'un utilisateur

- **Liste des groupes :**

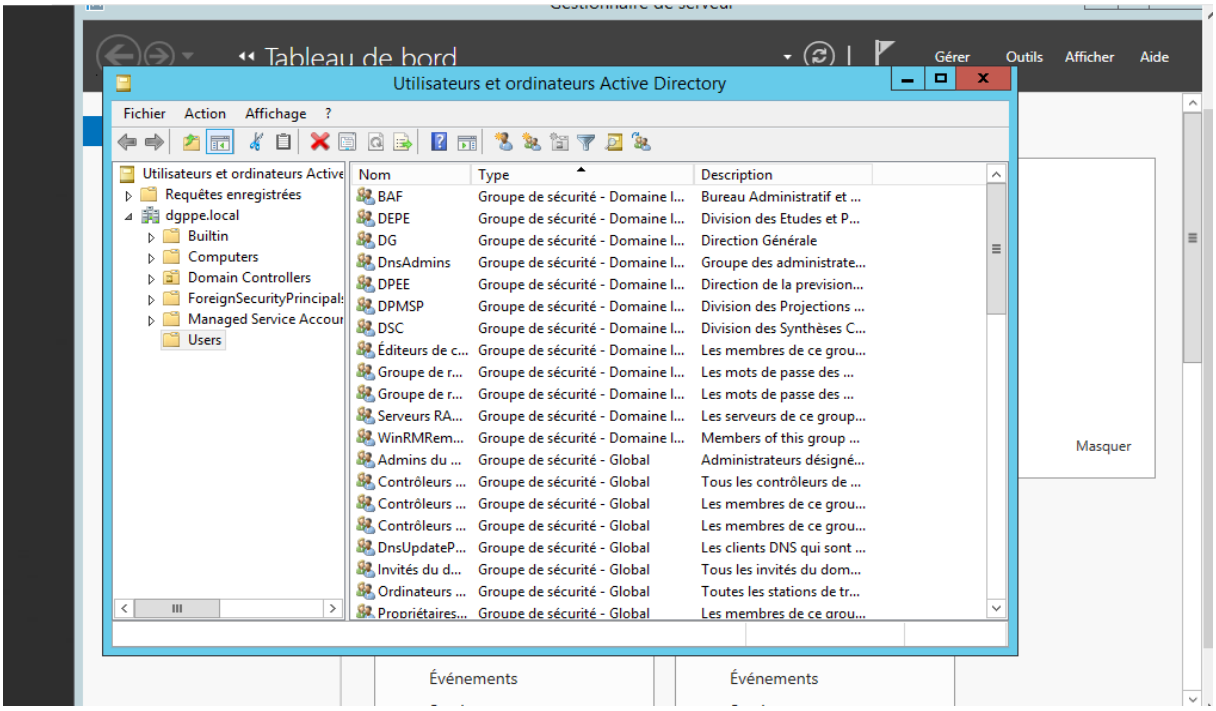


Figure 30 : liste des groupes

6.3.3 Appartenance utilisateurs aux groupes

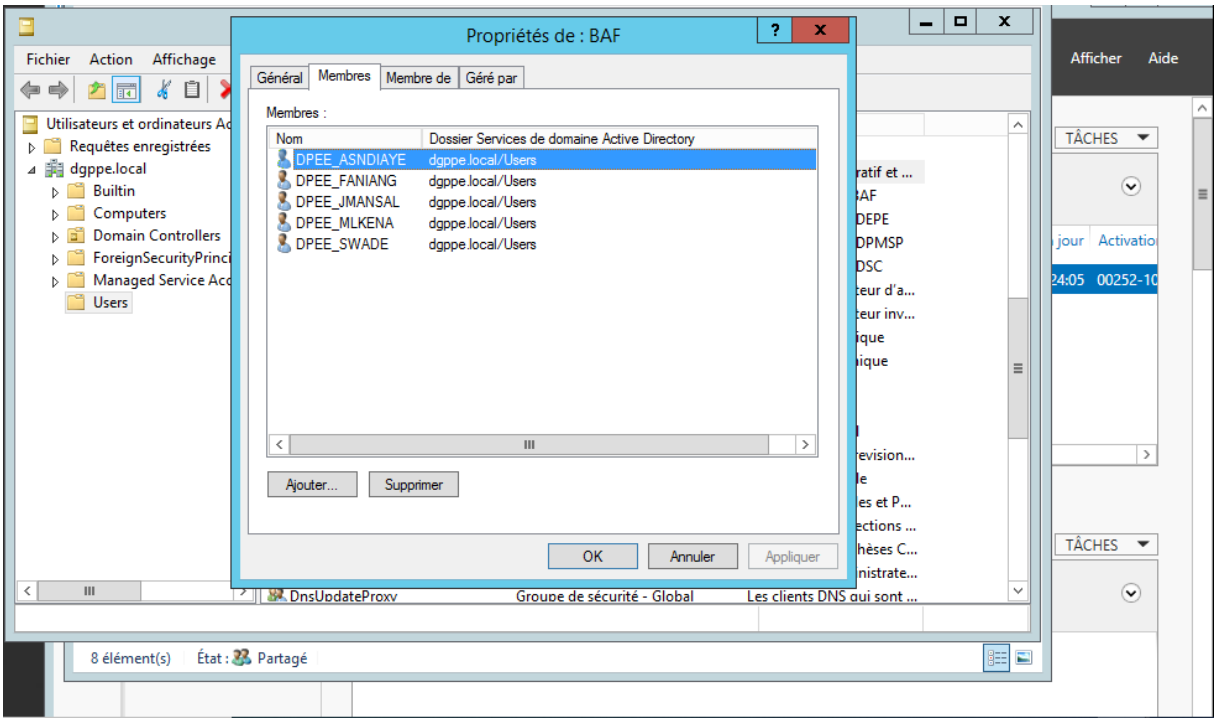


Figure 31 : détail d'un groupe (BAF)

Hiérarchie et droit accès

Groupes	Données DG	Données des Directions	Données de sa Direction	Données des Divisions	Données de sa Division
DG & Coordonnateur	✓	✓	✓	✓	✓
Directeur Direction	✗	✗	✓	✓	✓
Agent	✗	✗	✗	✗	✓

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 générale appartient au groupe Direction générale

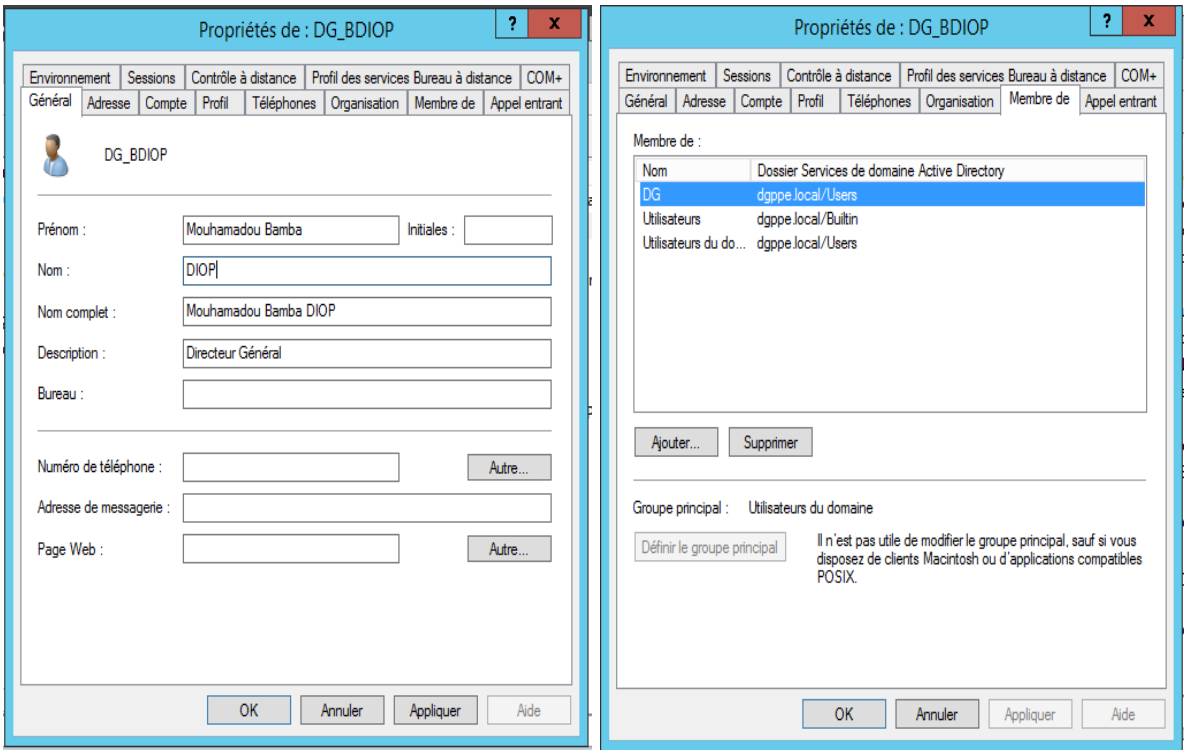


Figure 32 : profil DG

Le Directeur de la DPEE est membre du groupe DPEE.

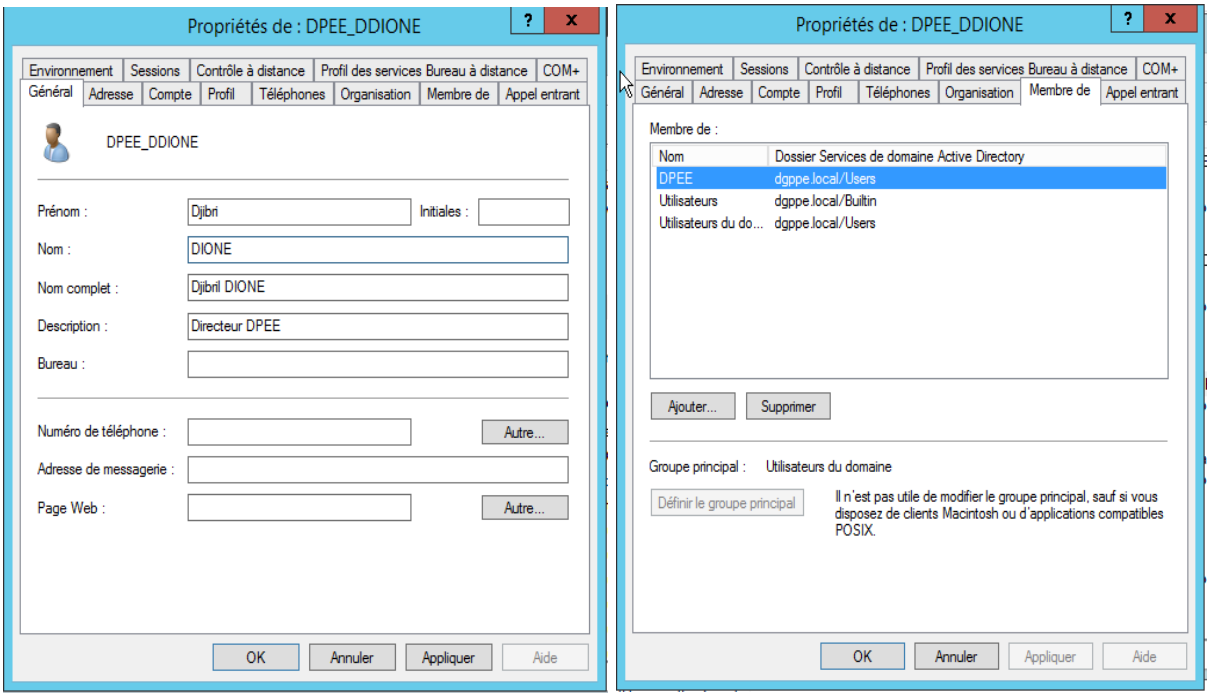


Figure 33 : profil Directeur

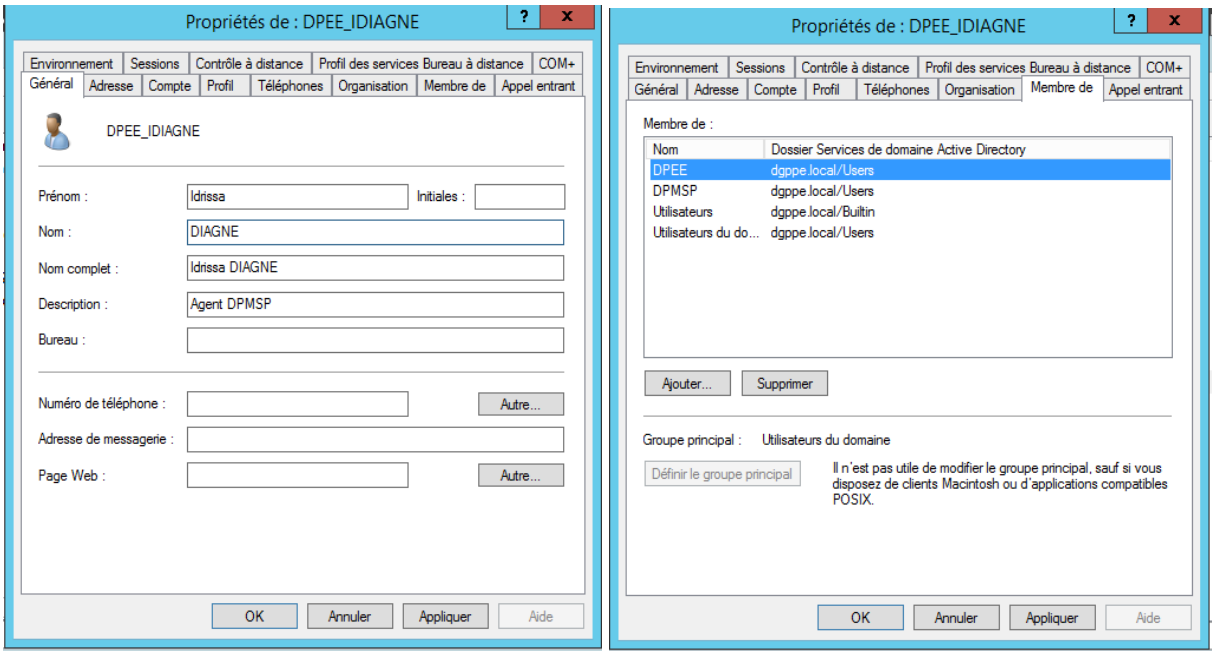


Figure 34 : profil Agent simple

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.

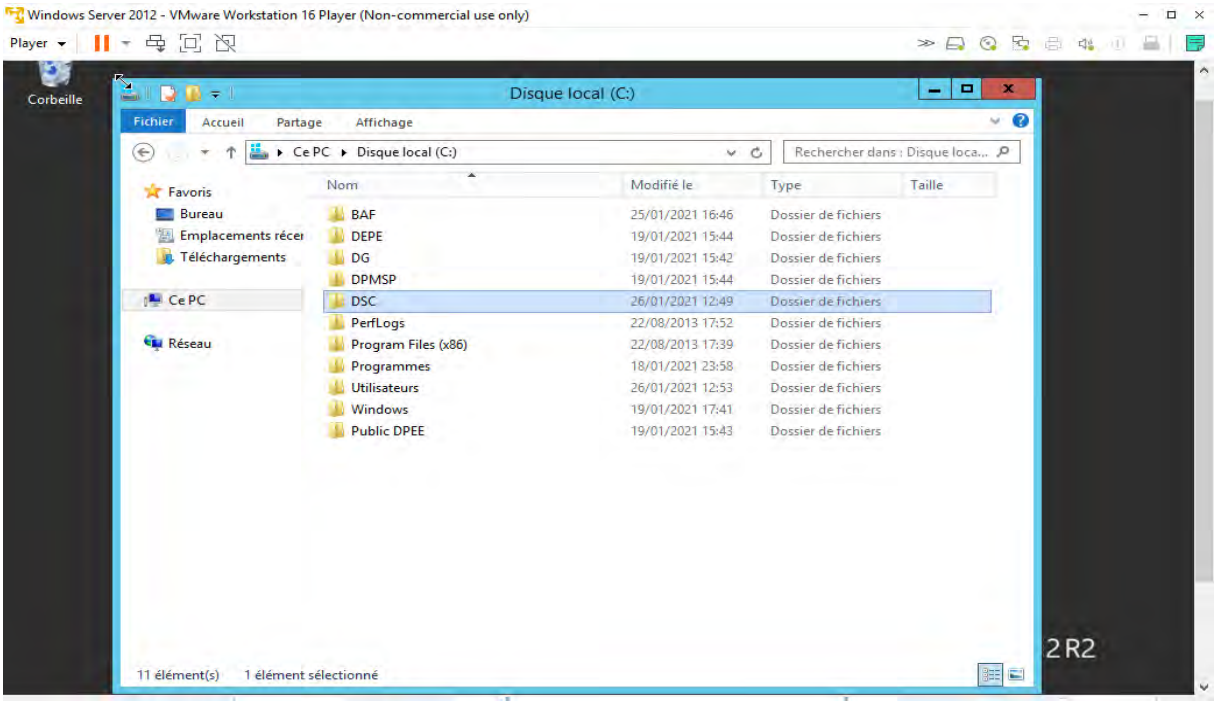


Figure 35 : création des dossiers à partager

Les dossiers ont été créé, 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.

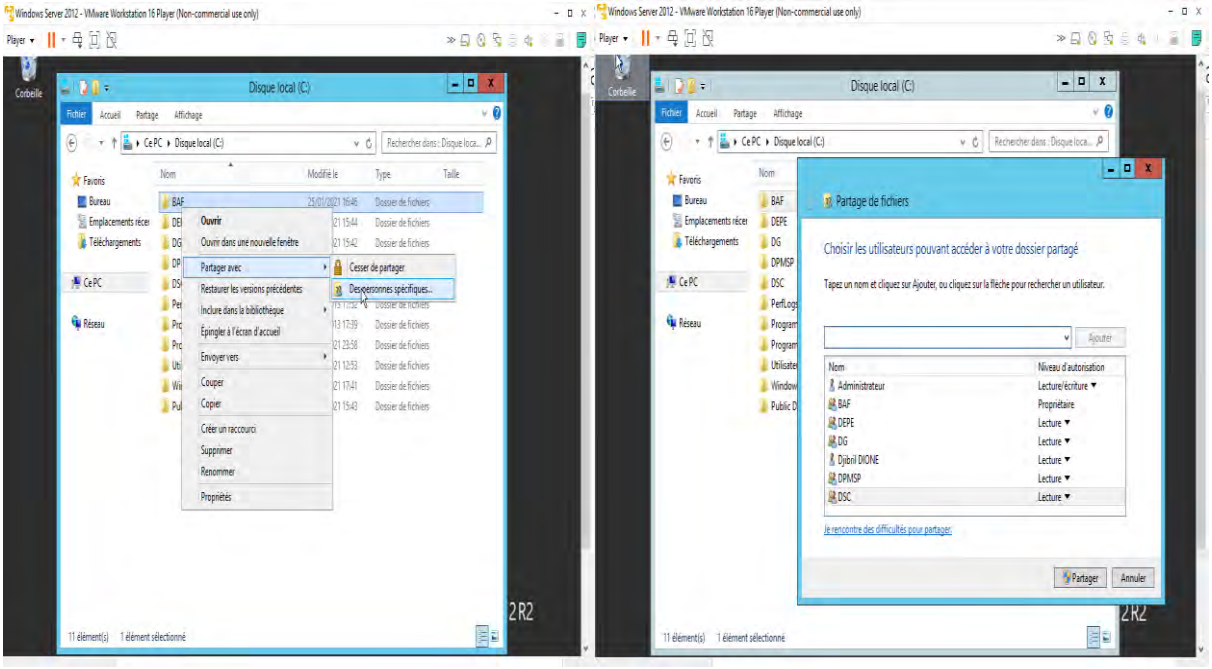


Figure 36 : partage de dossiers aux utilisateurs

- **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.

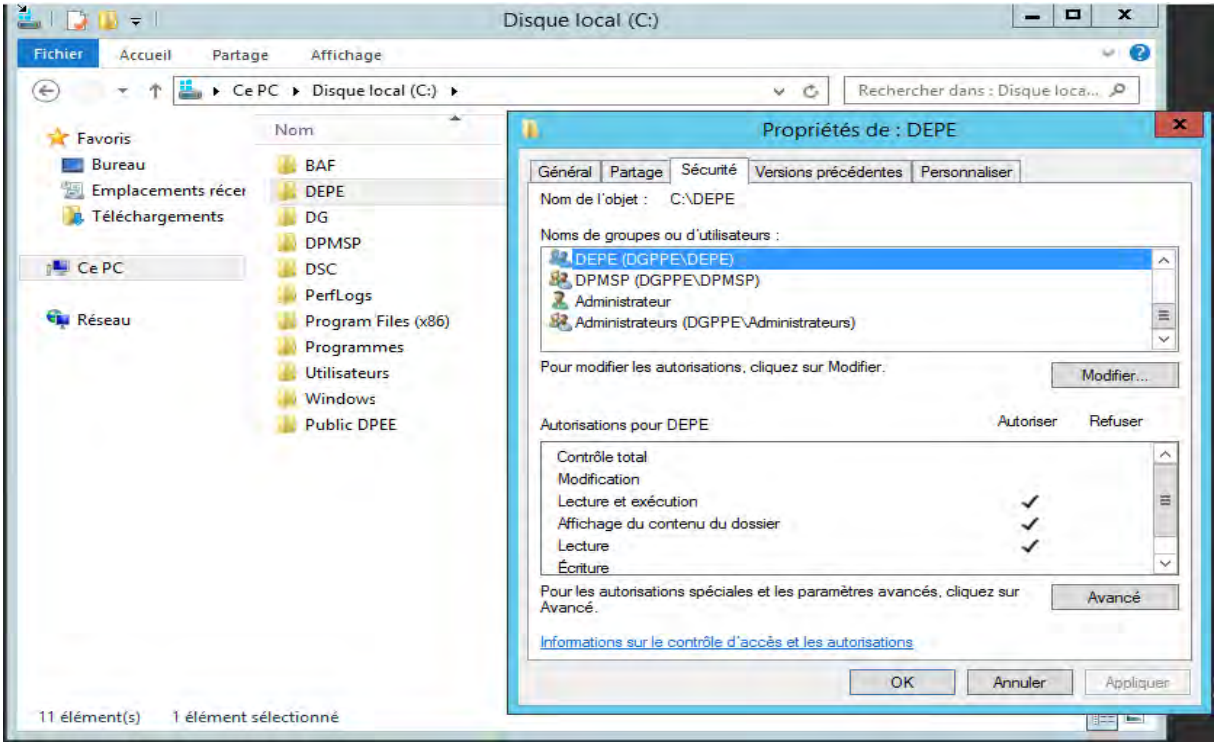


Figure 37 : vérification des restrictions du BAF

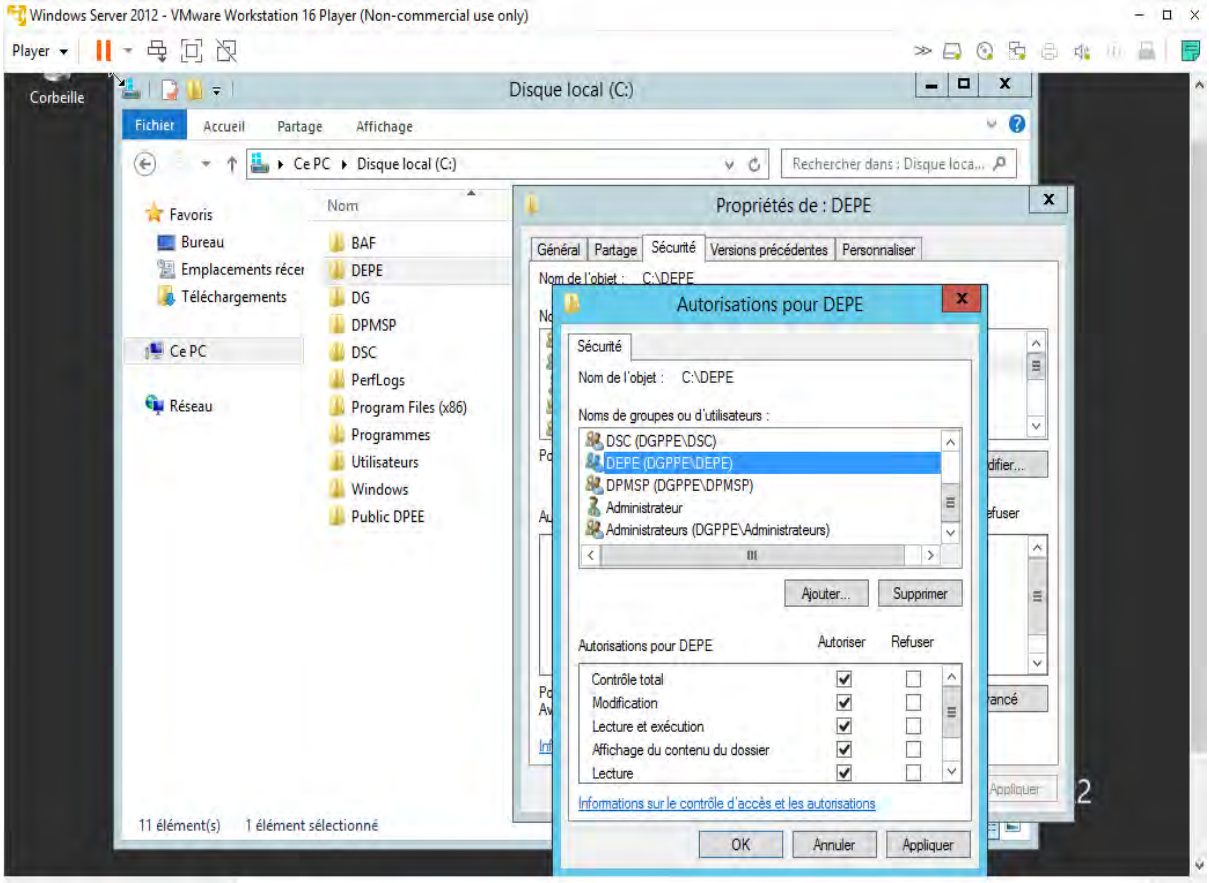


Figure 38 : allouer contrôle total à DPEE

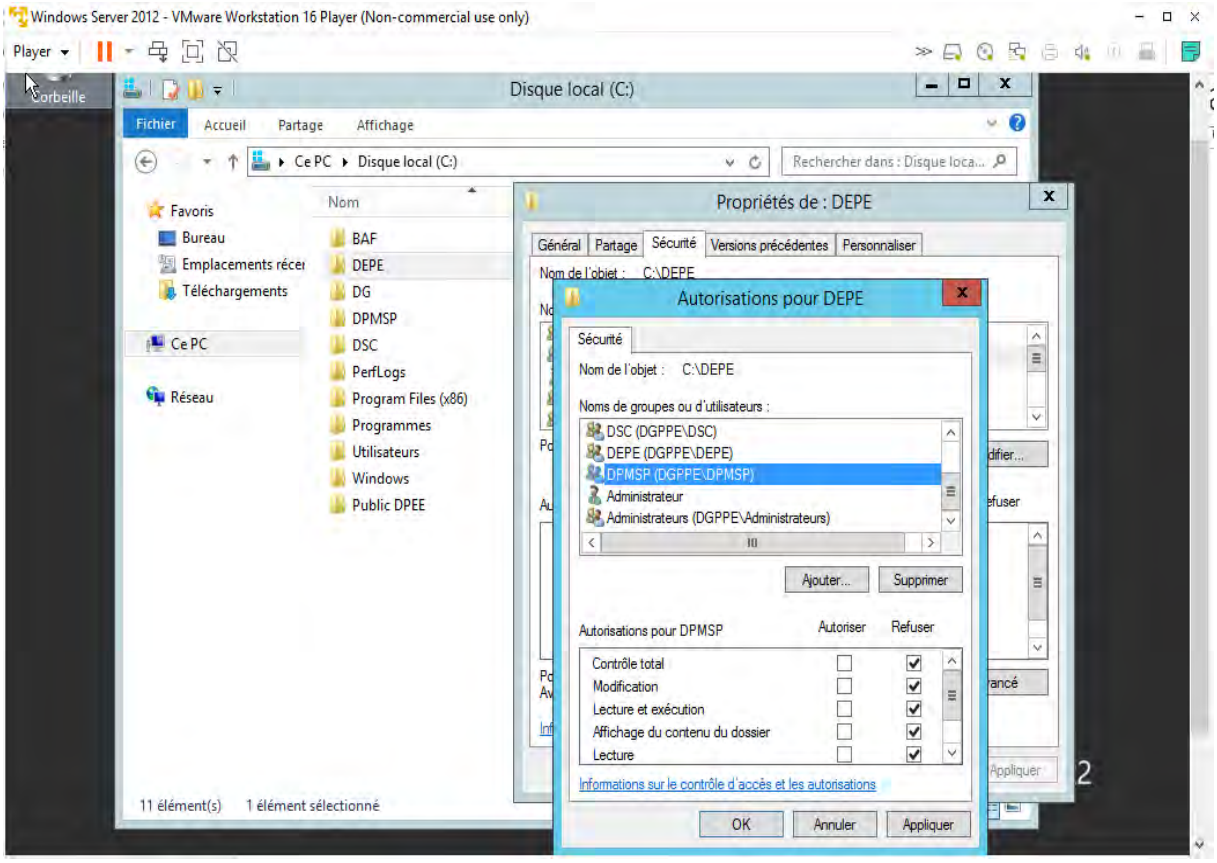


Figure 39 : refus du contrôle total des autorisations de la DPMSP

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

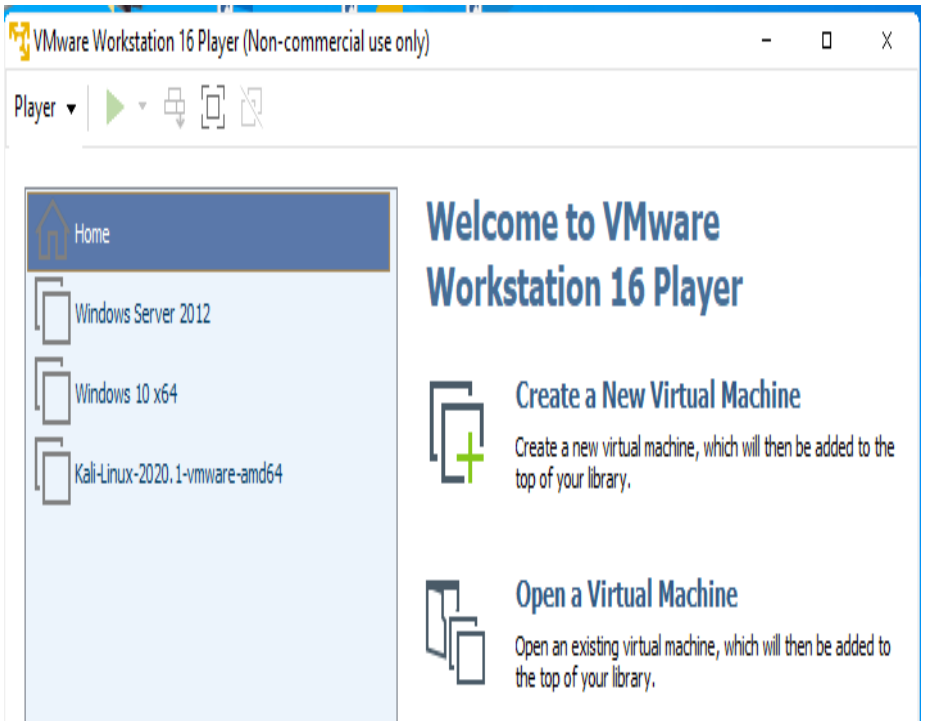


Figure 40 : installation Windows 10 sur VMware

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

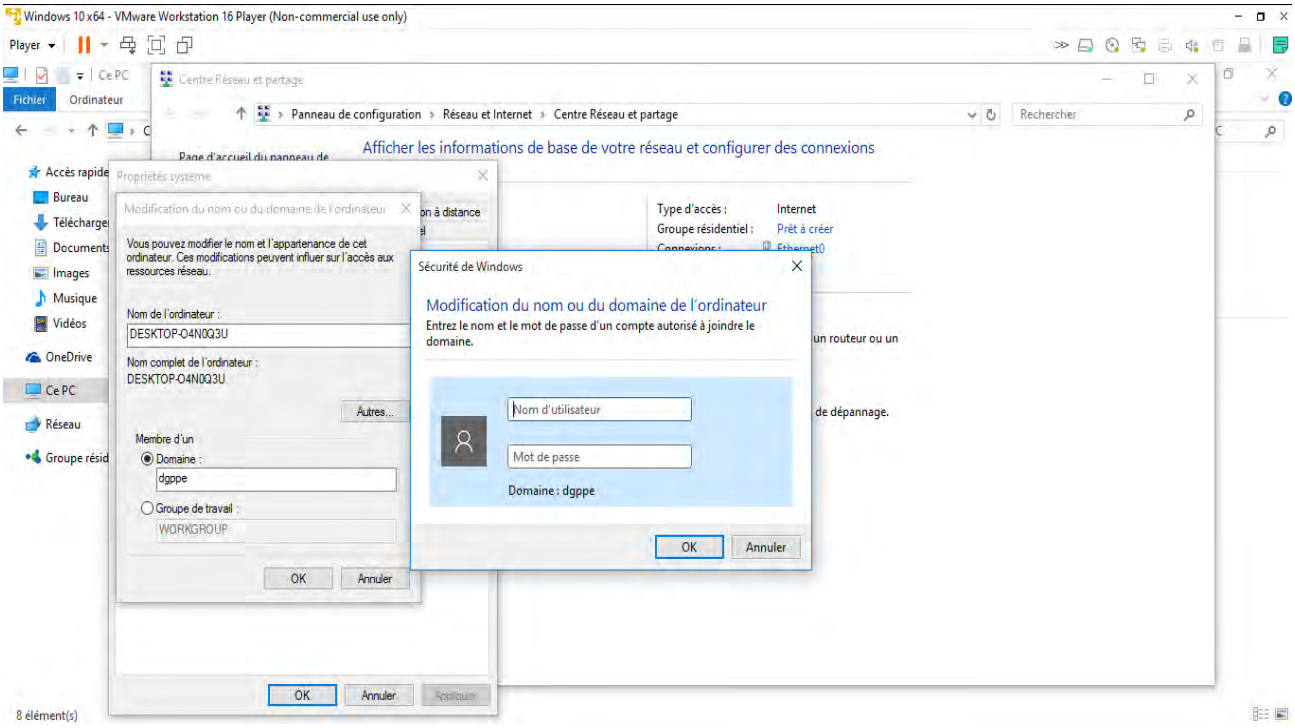


Figure 41 : interface connexion

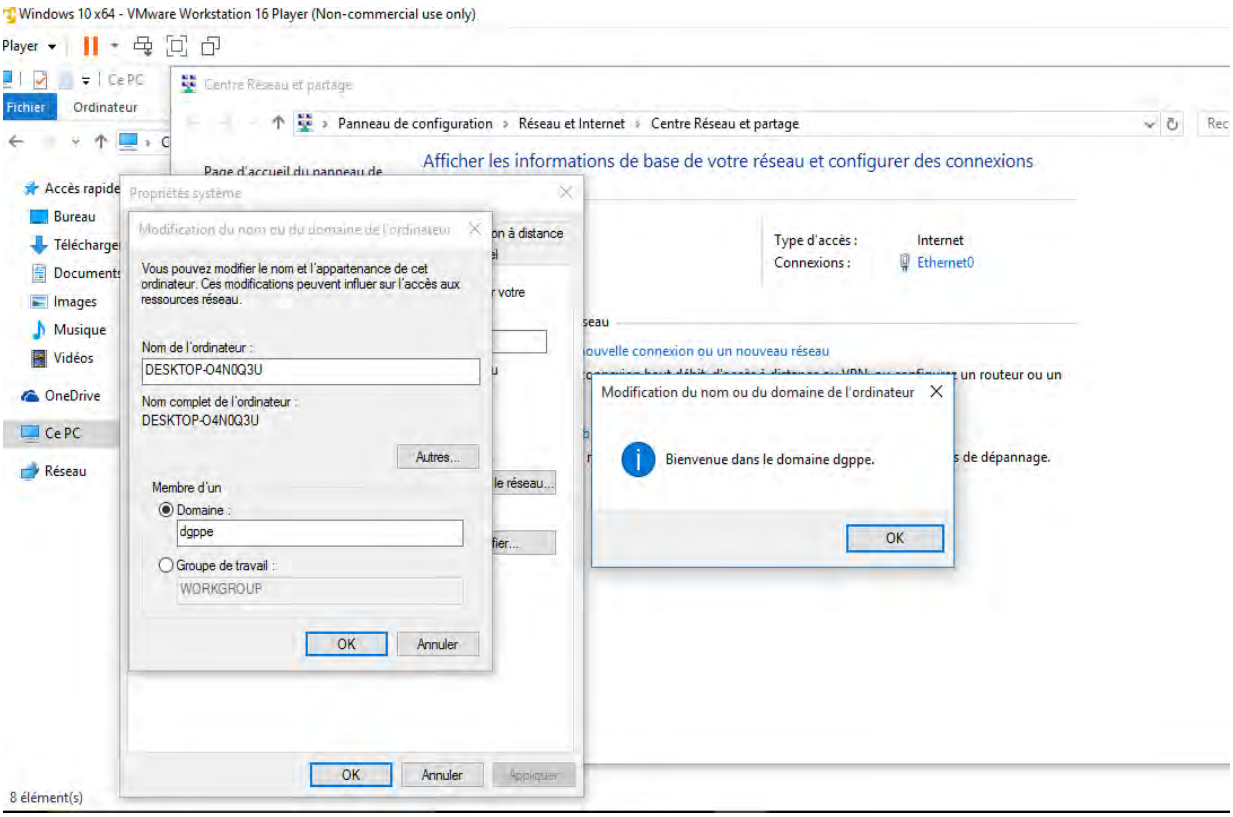


Figure 42 : connexion dans le domaine DGPPE

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).

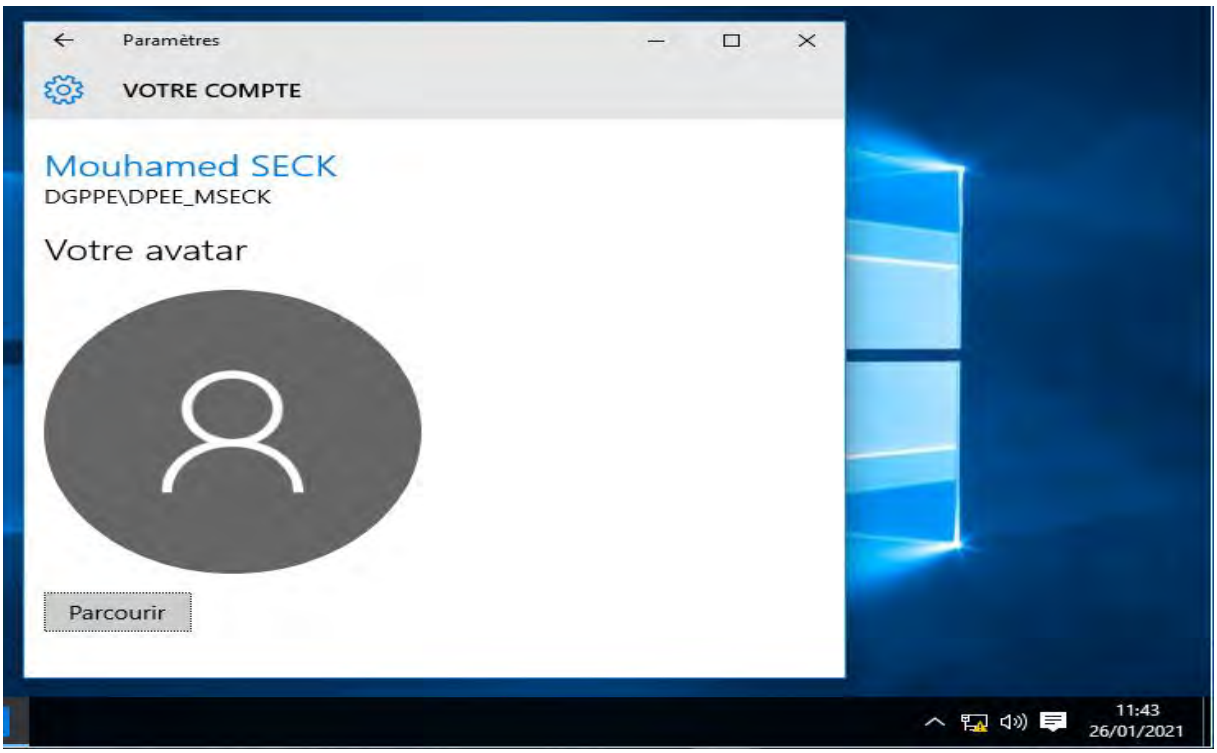


Figure 43 : profil Agent DSC

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

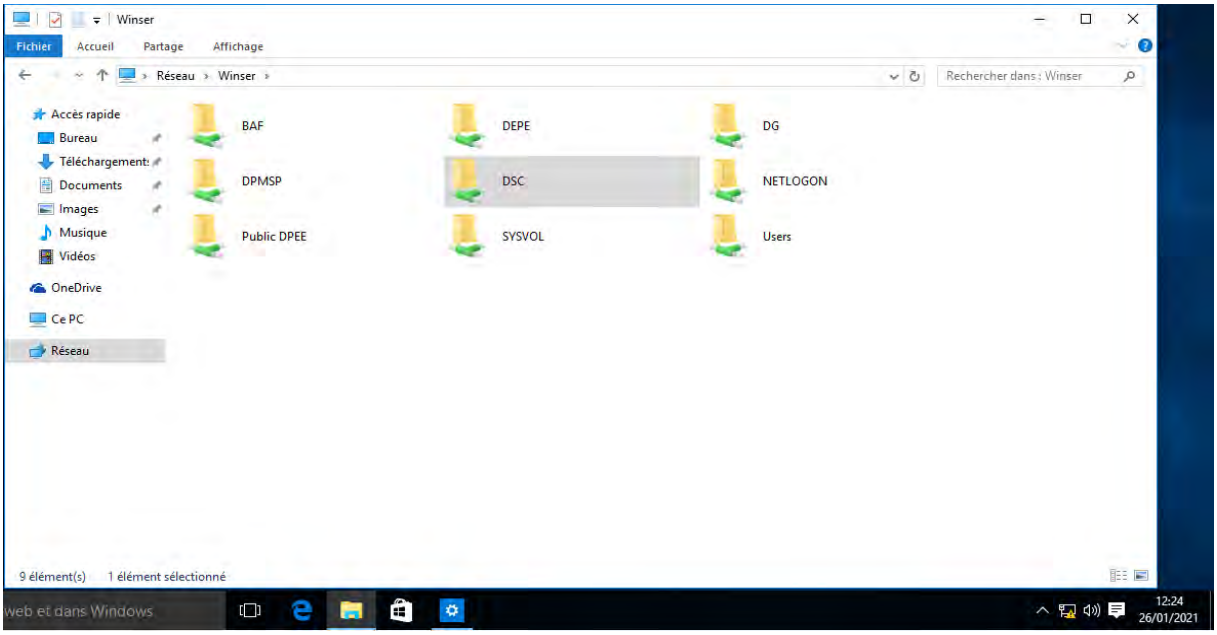


Figure 44 : aperçu des dossiers partagés

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.

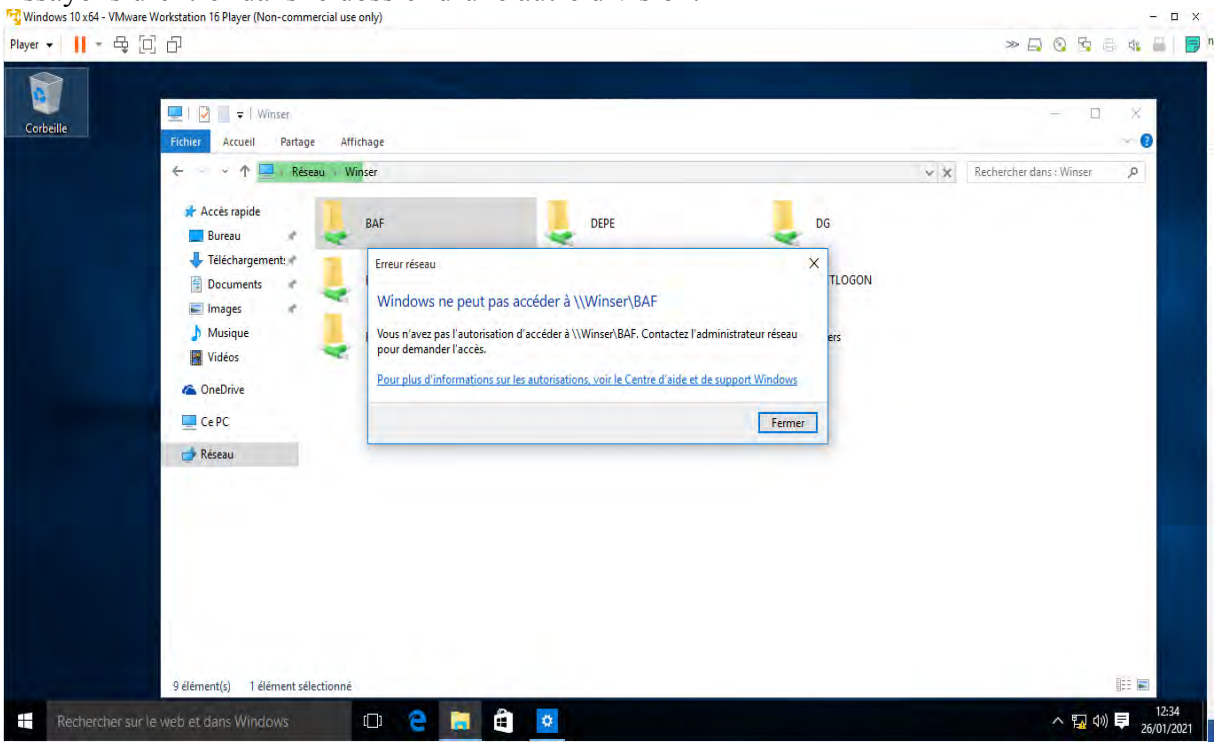


Figure 45 : refus d'accès dossier

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

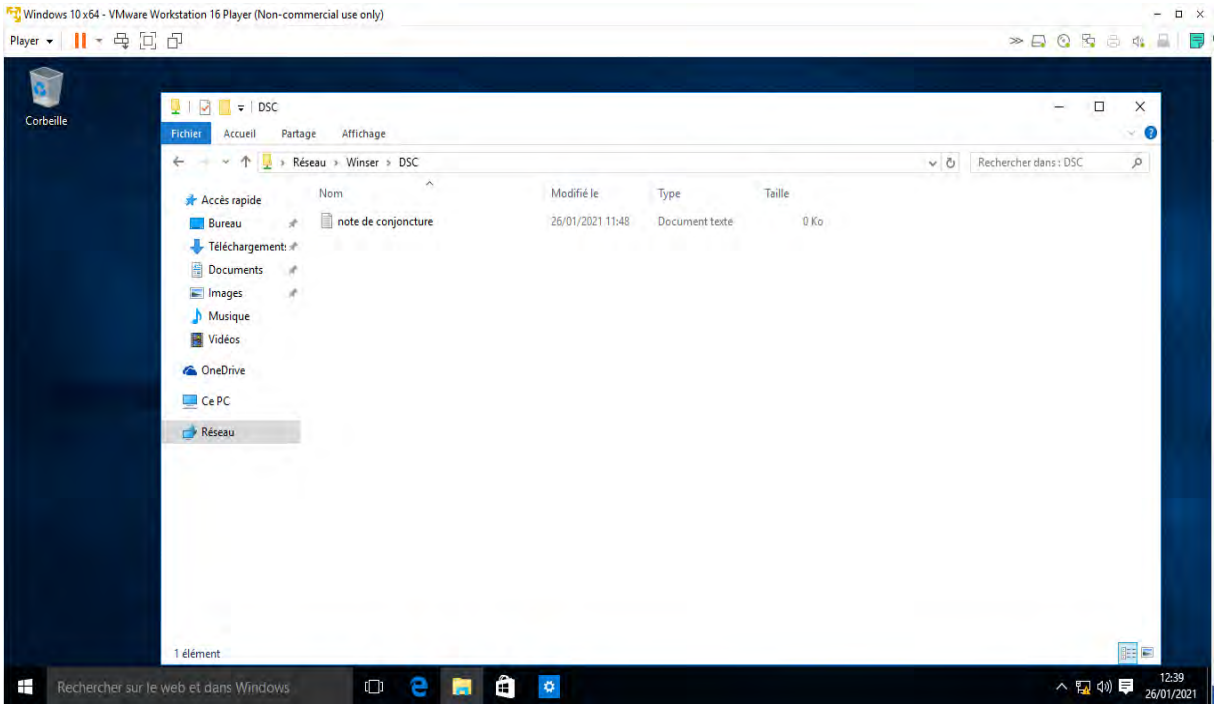


Figure 46 : accès réussi

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

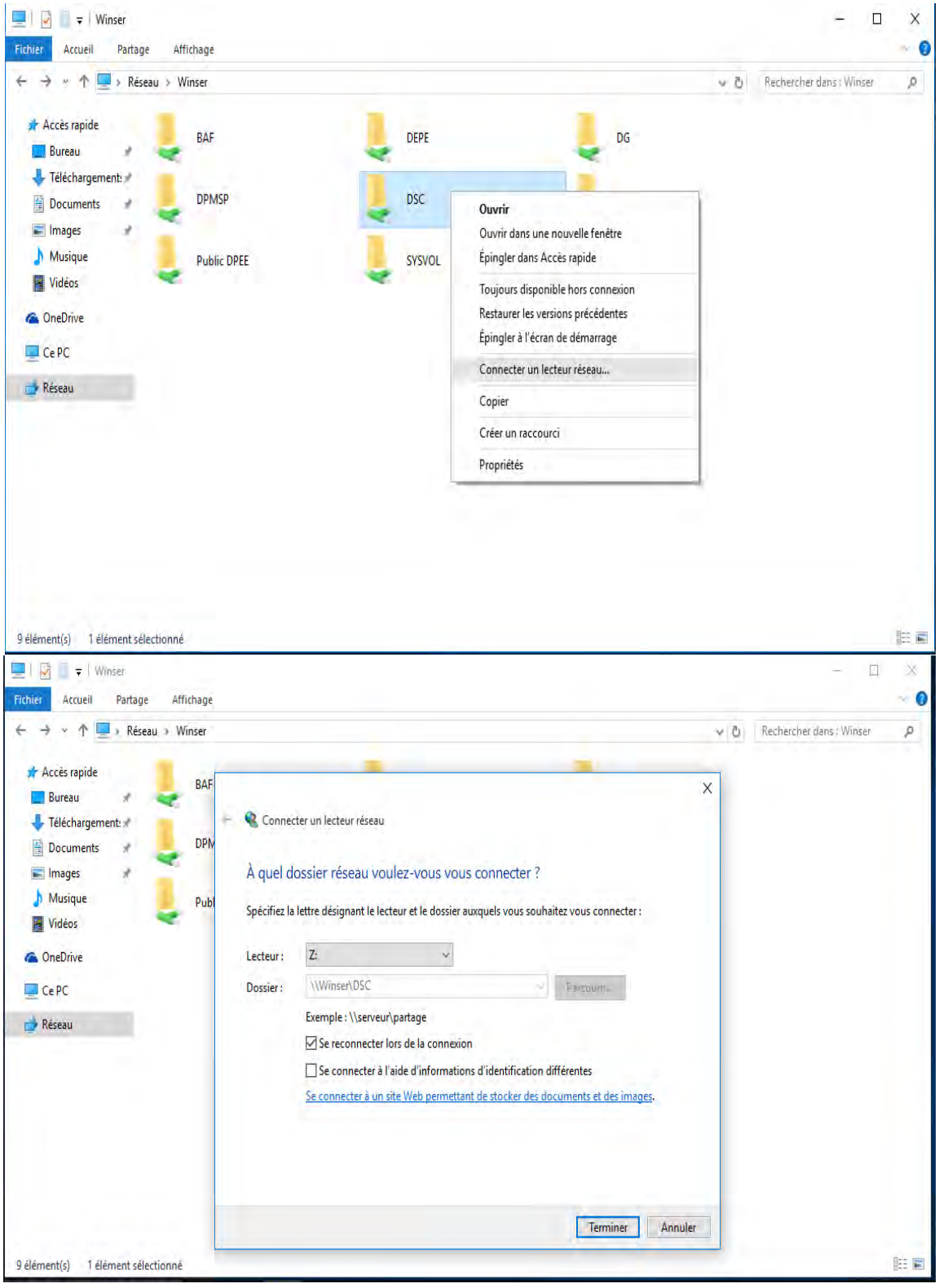


Figure 47 : connexion dossier partager via un lecteur

Le dossier est bien ajouté.

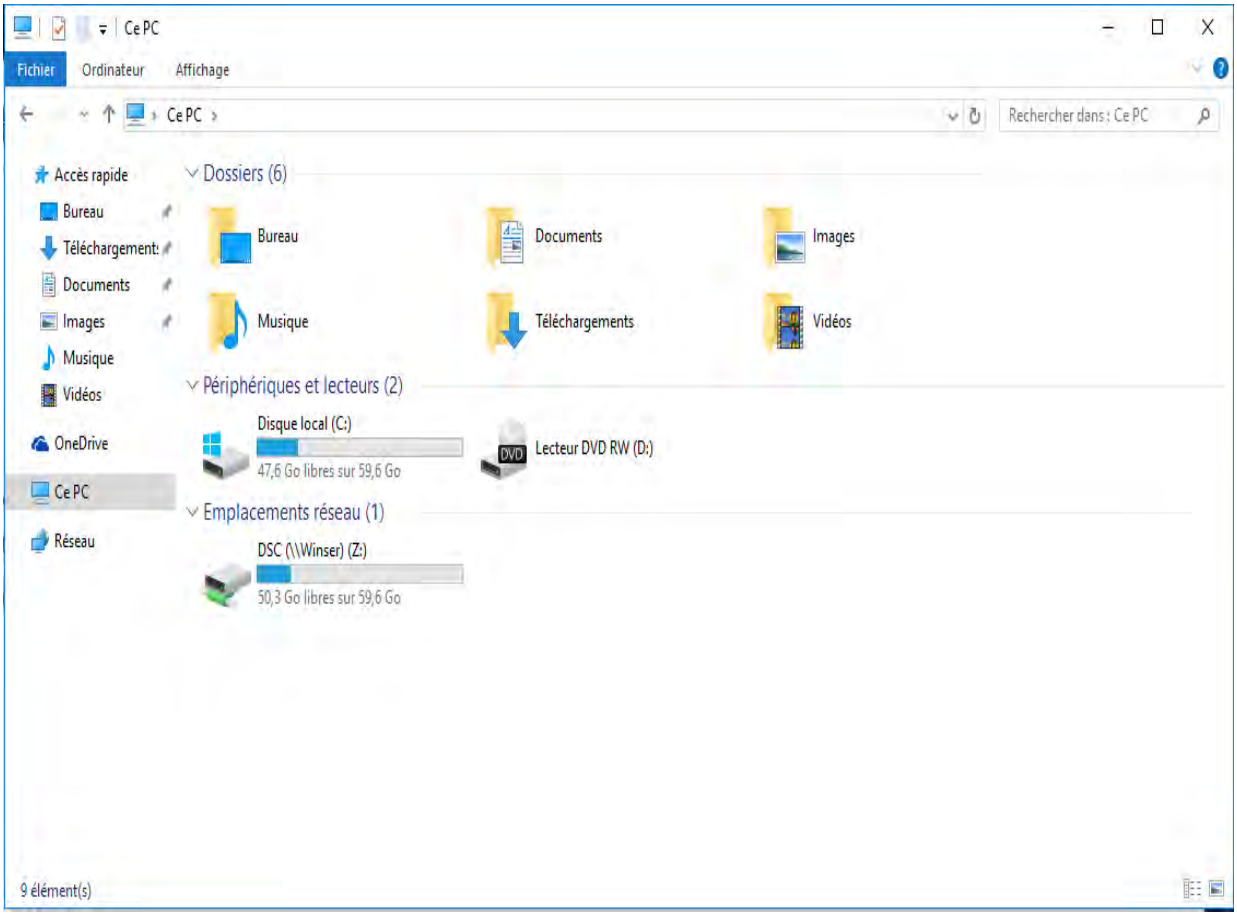


Figure 48 : aperçu d'un dossier partager dans un lecteur

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**

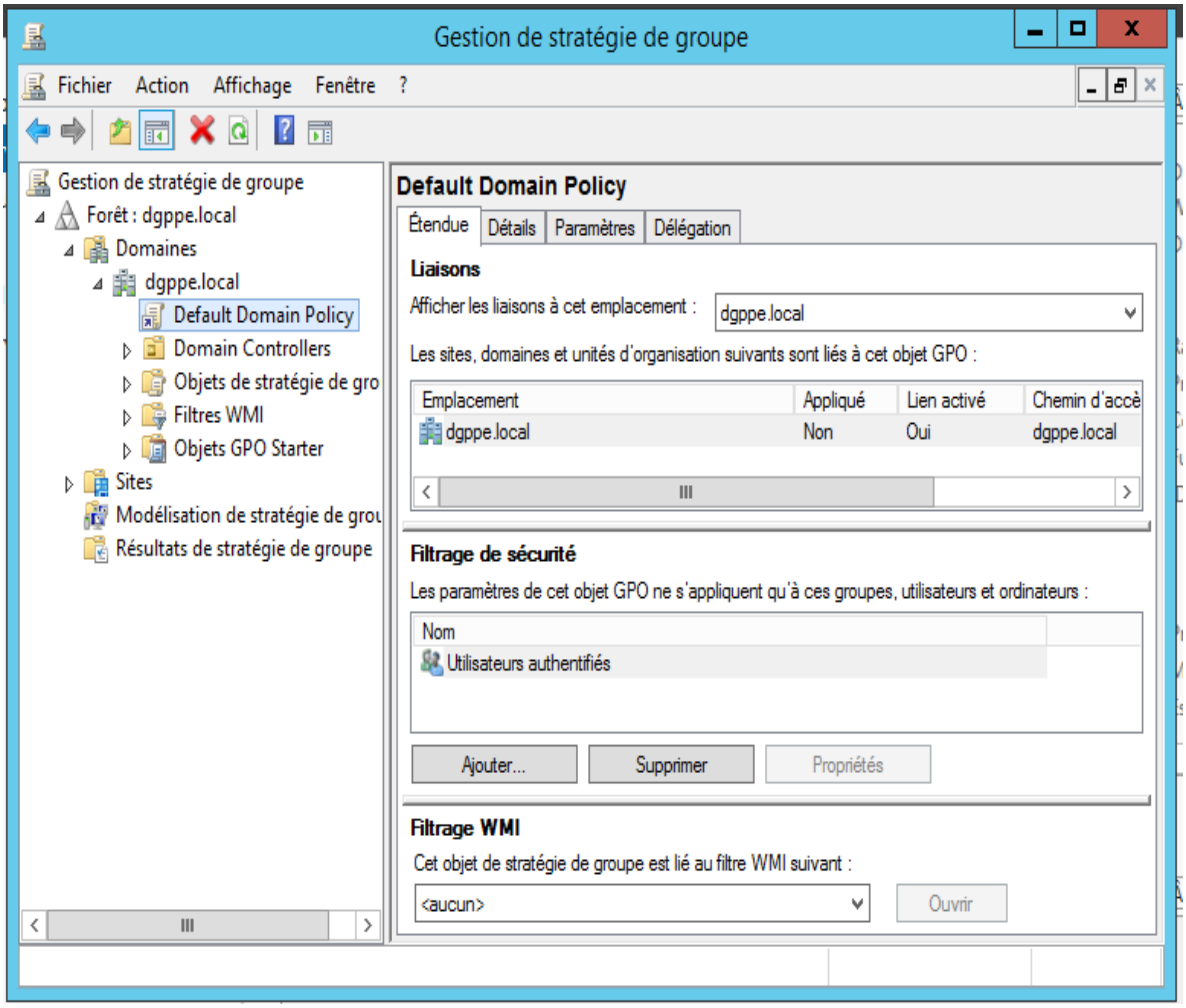


Figure 49 : gestion des stratégies de groupe

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

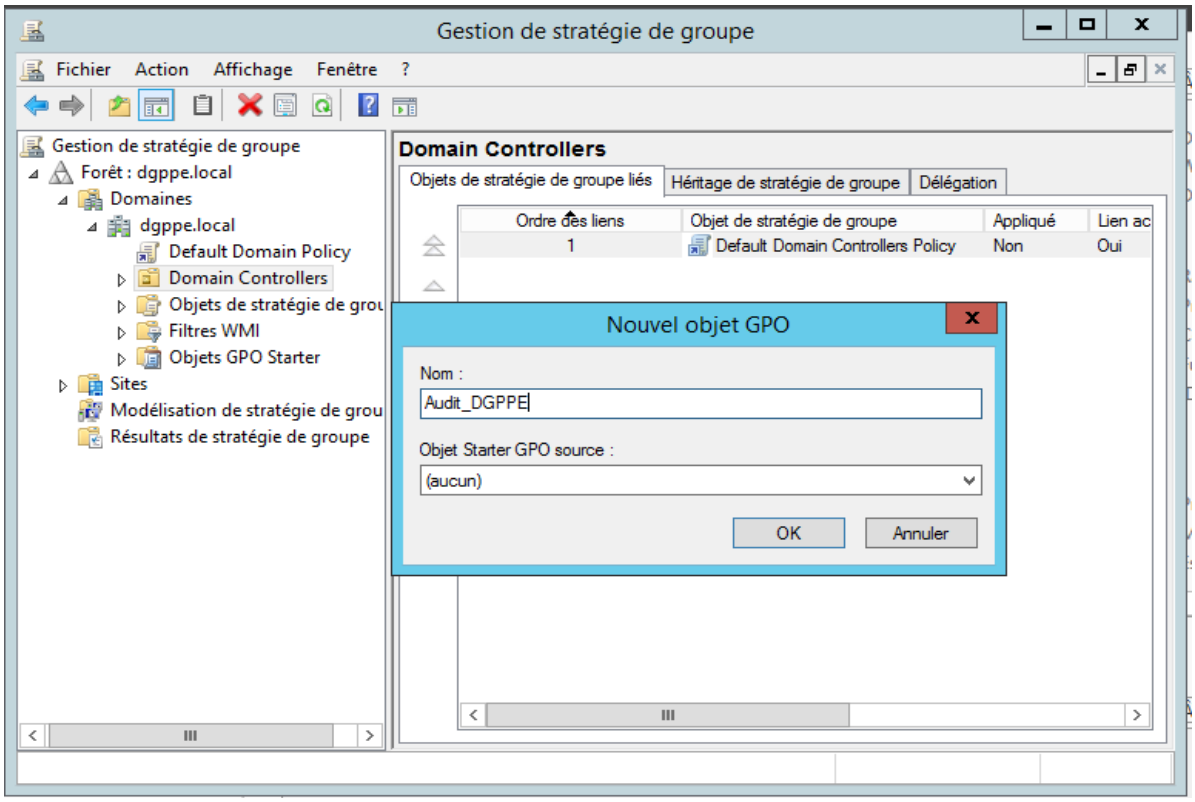


Figure 50 : création d'un nouvel objet GPO

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

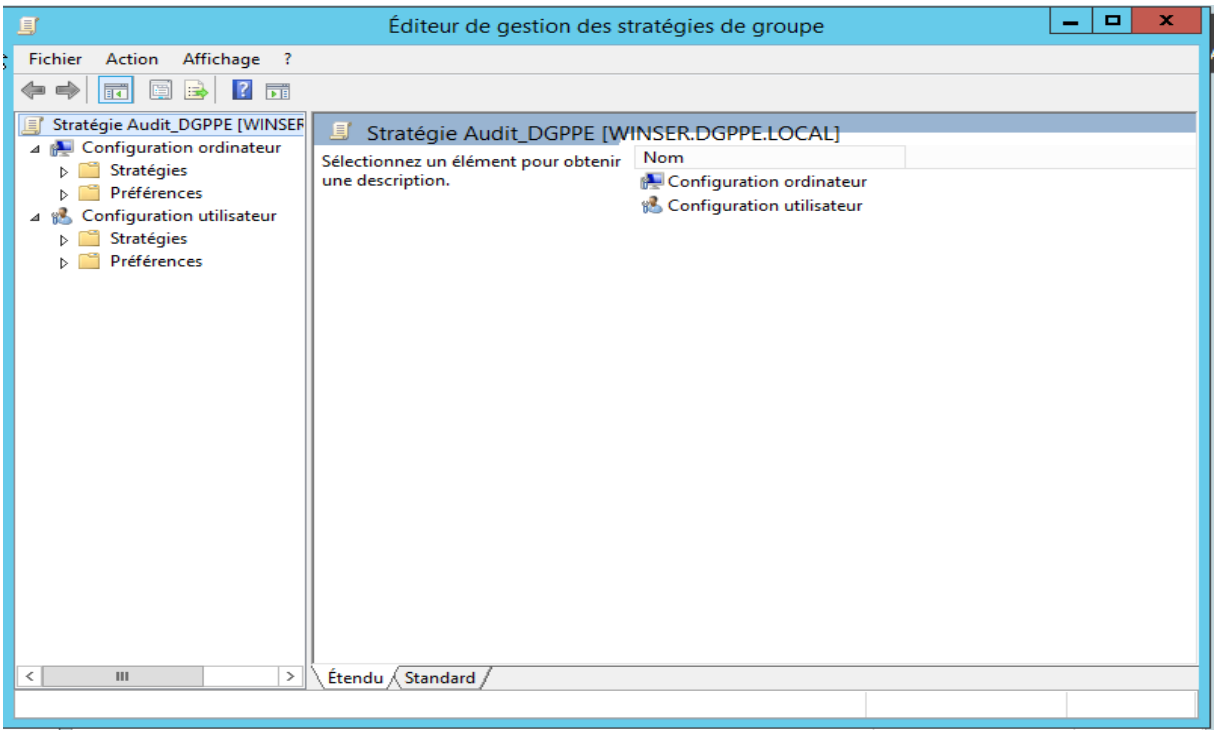


Figure 51 : éditeur de gestion des stratégies de groupe

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.

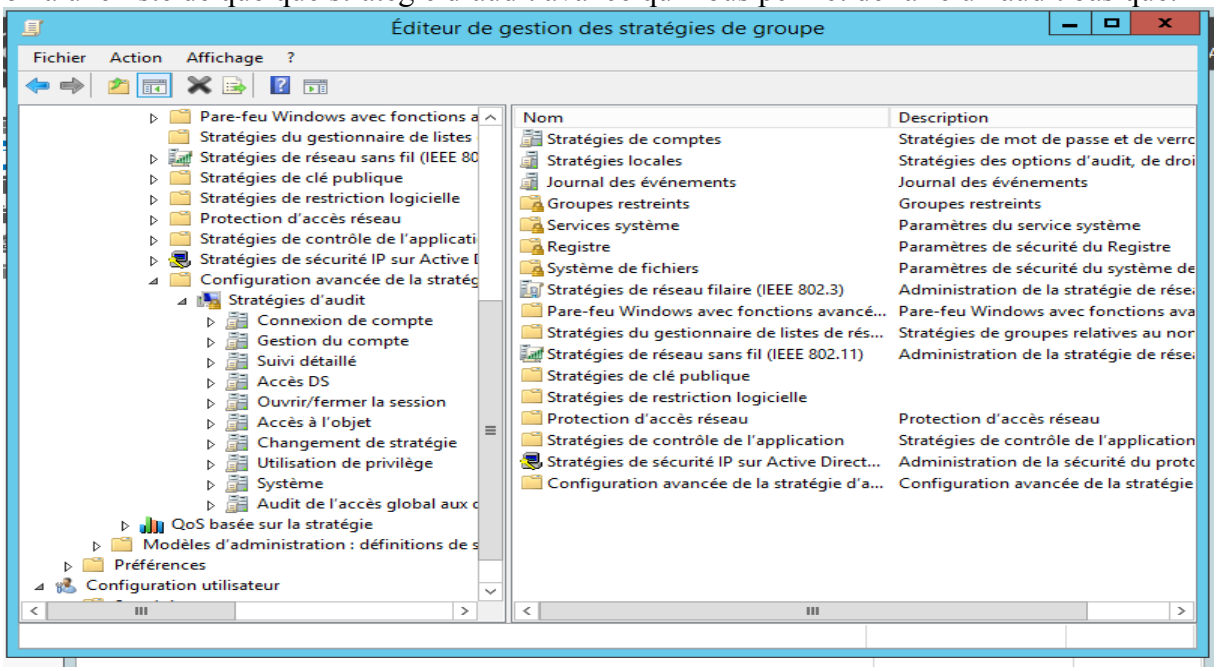


Figure 52 : éditeur de gestion de stratégies de groupe

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.

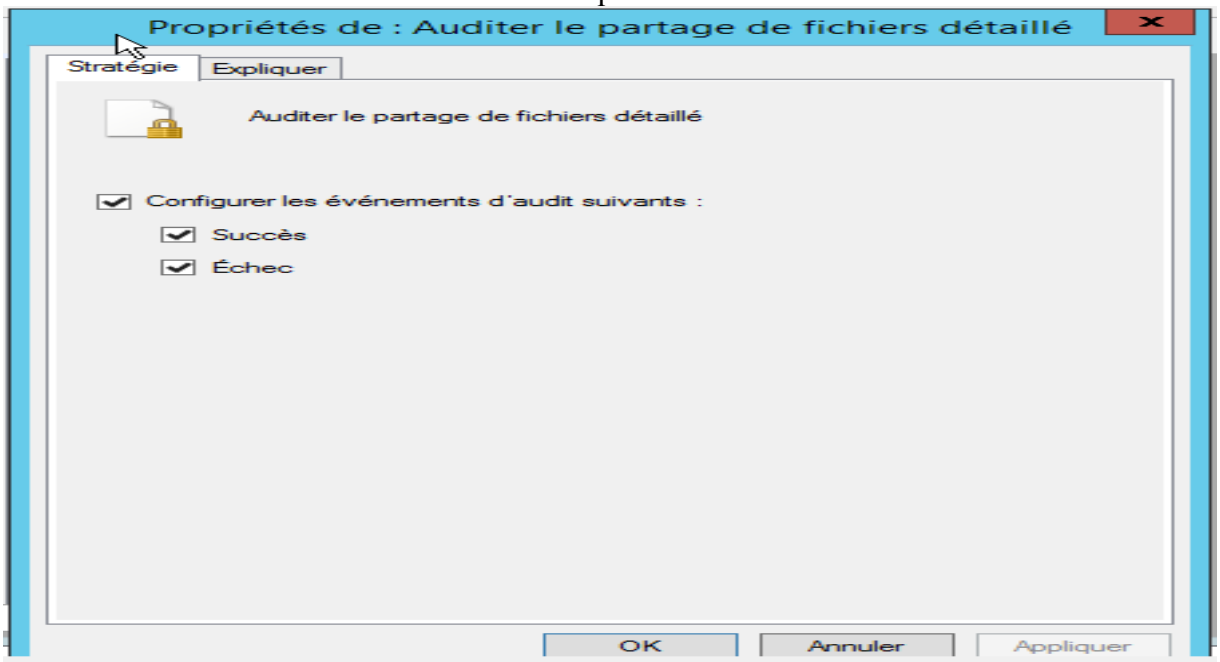


Figure 53 : propriété d'audit du partage de fichier

Donc on va mettre à jour la stratégie.

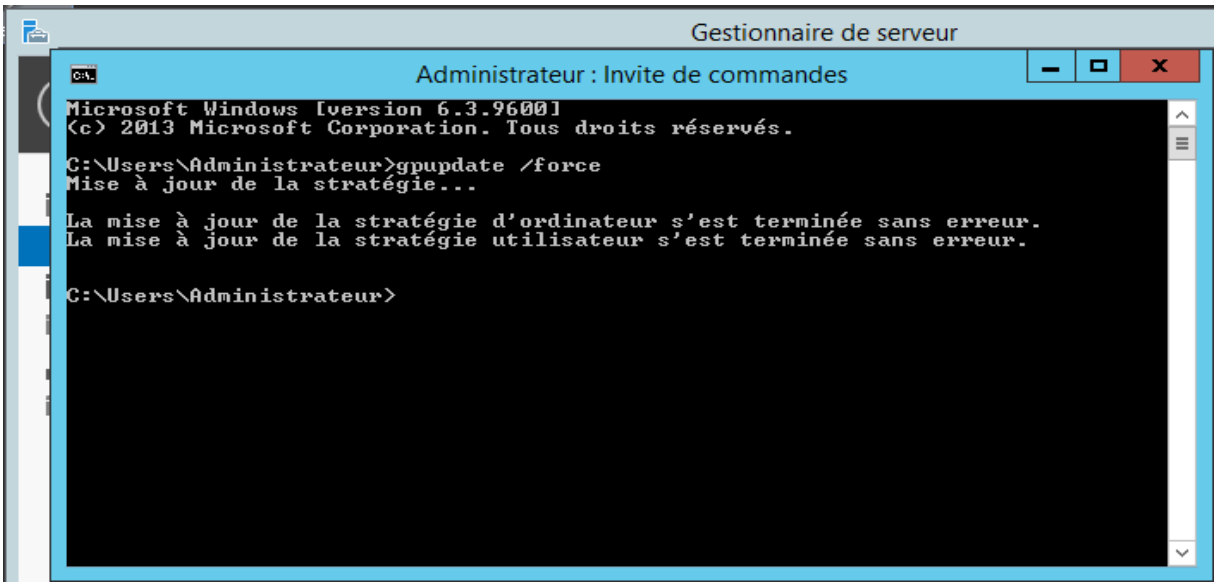


Figure 54 : aperçu invite de commande

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 :

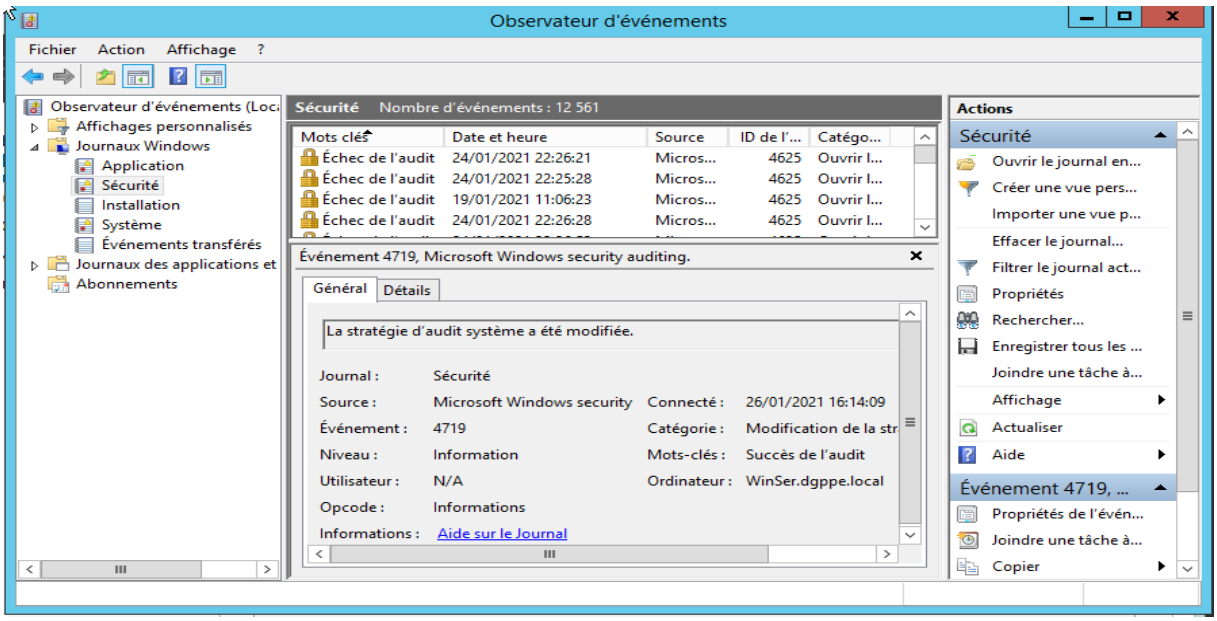


Figure 55 : évènement des audits échoués

Succès

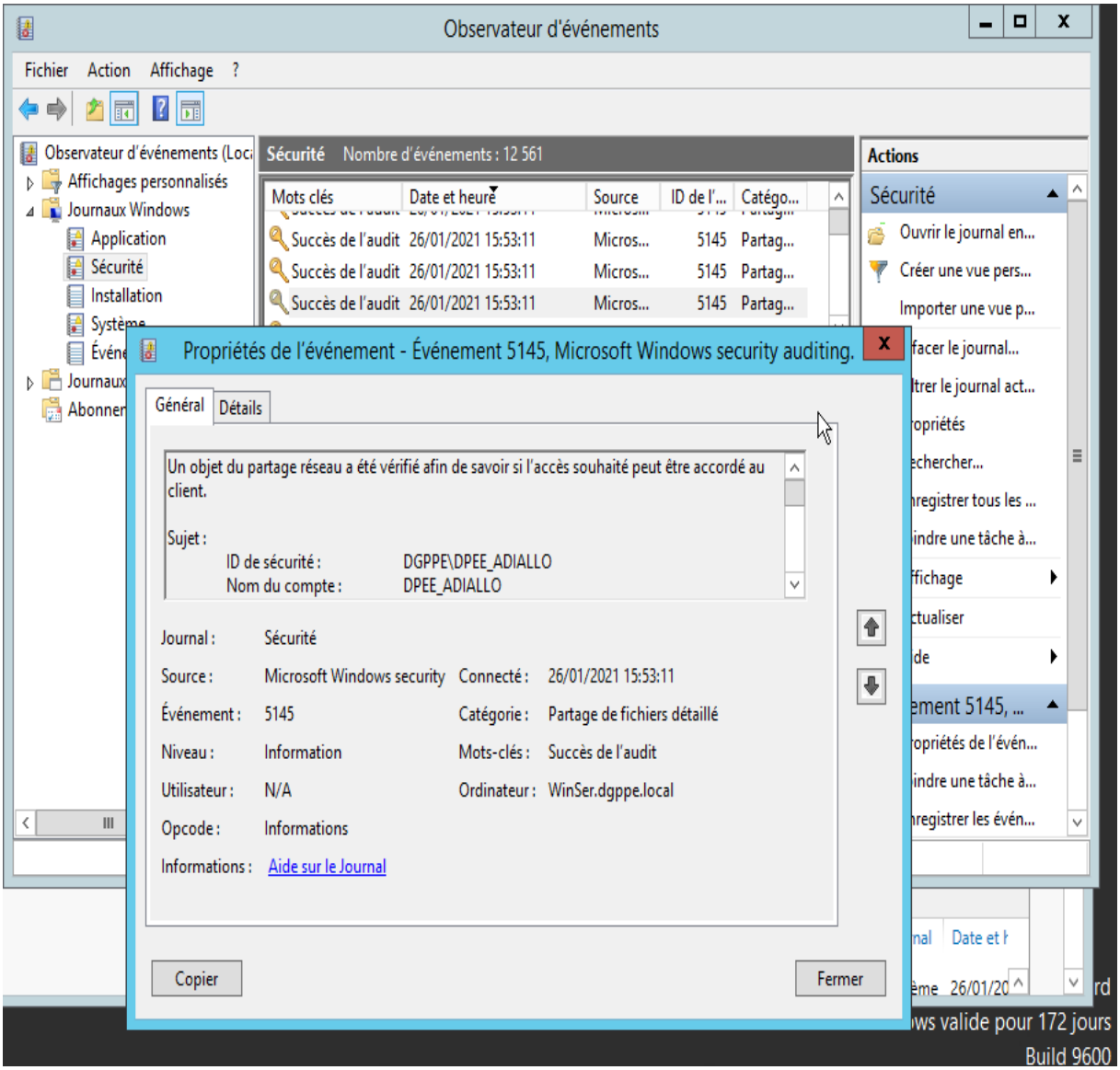


Figure 56: propriétés de l'évènement de l'utilisateur Alassane DIALLO

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 accidentelles 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. Elle nécessite moins d'espace de stockage. Elle requiert moins de supports à gérer. Un utilisateur peut sauvegarder des données.	Les utilisateurs doivent copier leurs fichiers importants sur les serveurs. Elle ne peut pas sauvegarder le Registre sur les ordinateurs distants. Elle augmente le trafic réseau. 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 :**

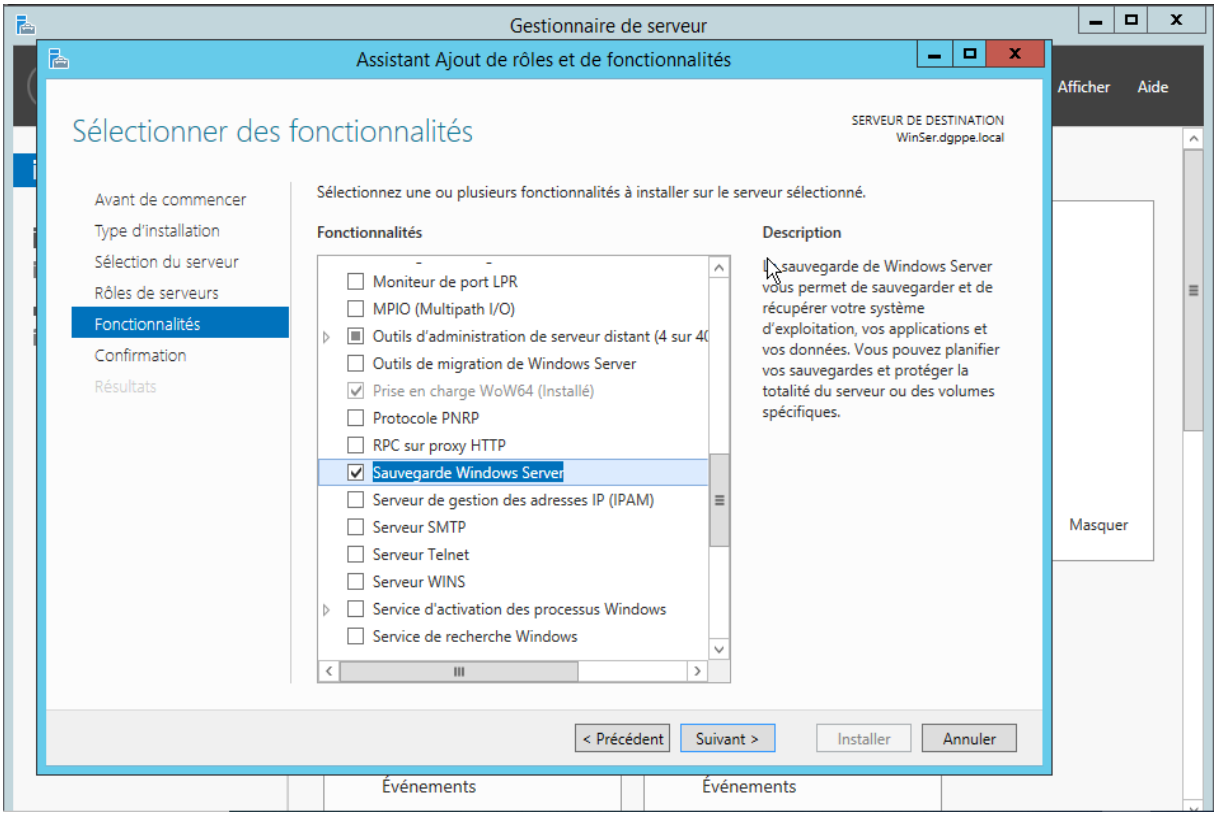


Figure 57 : ajout fonctionnalité Sauvegarde Windows Server

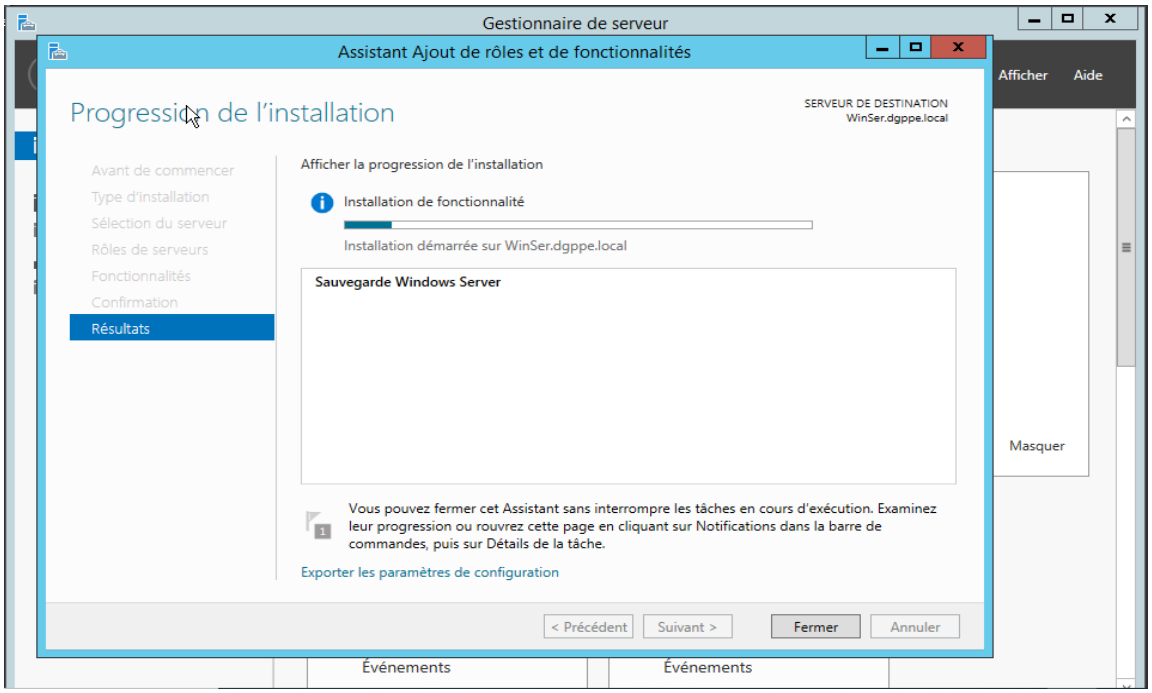


Figure 58 : installation en cours de la fonctionnalité Sauvegarde Windows Server

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.

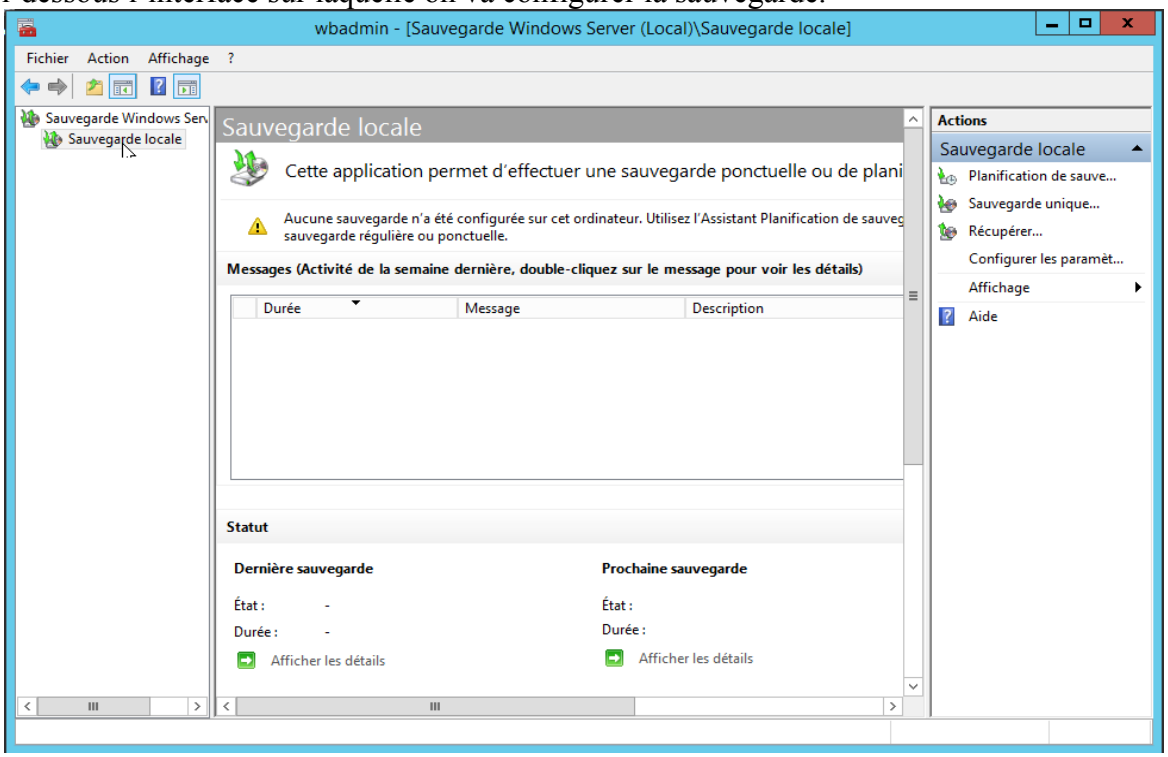


Figure 59 : interface sauvegarde et restauration Windows Server

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.

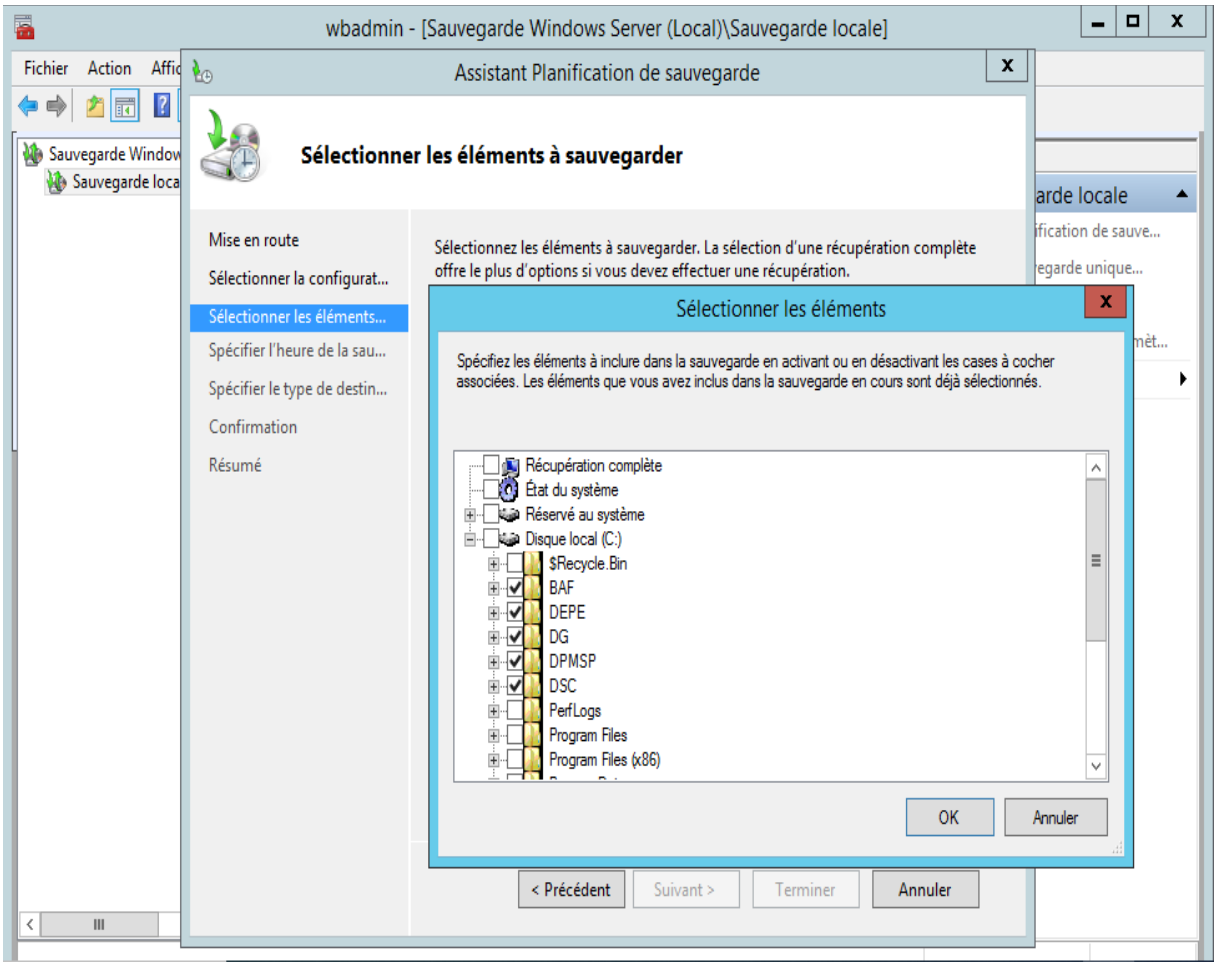


Figure 60 : aperçu des dossiers sélectionnés pour la sauvegarde

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

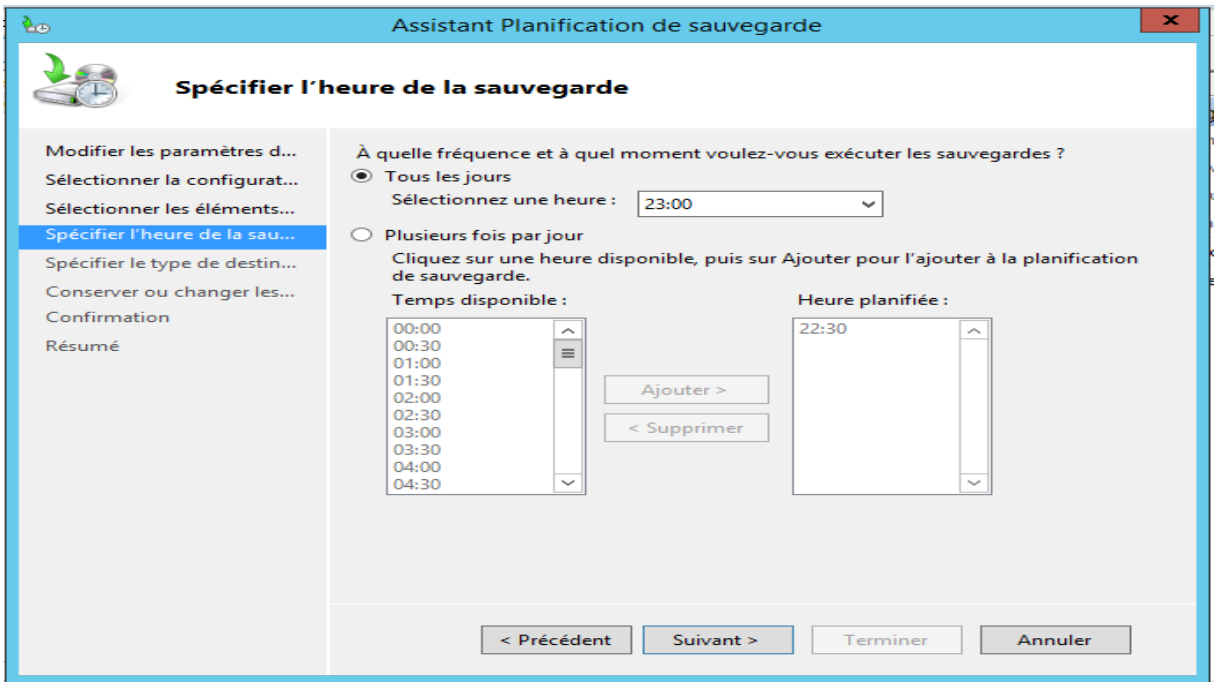


Figure 61 : aperçu du choix de l'heure de sauvegarde

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

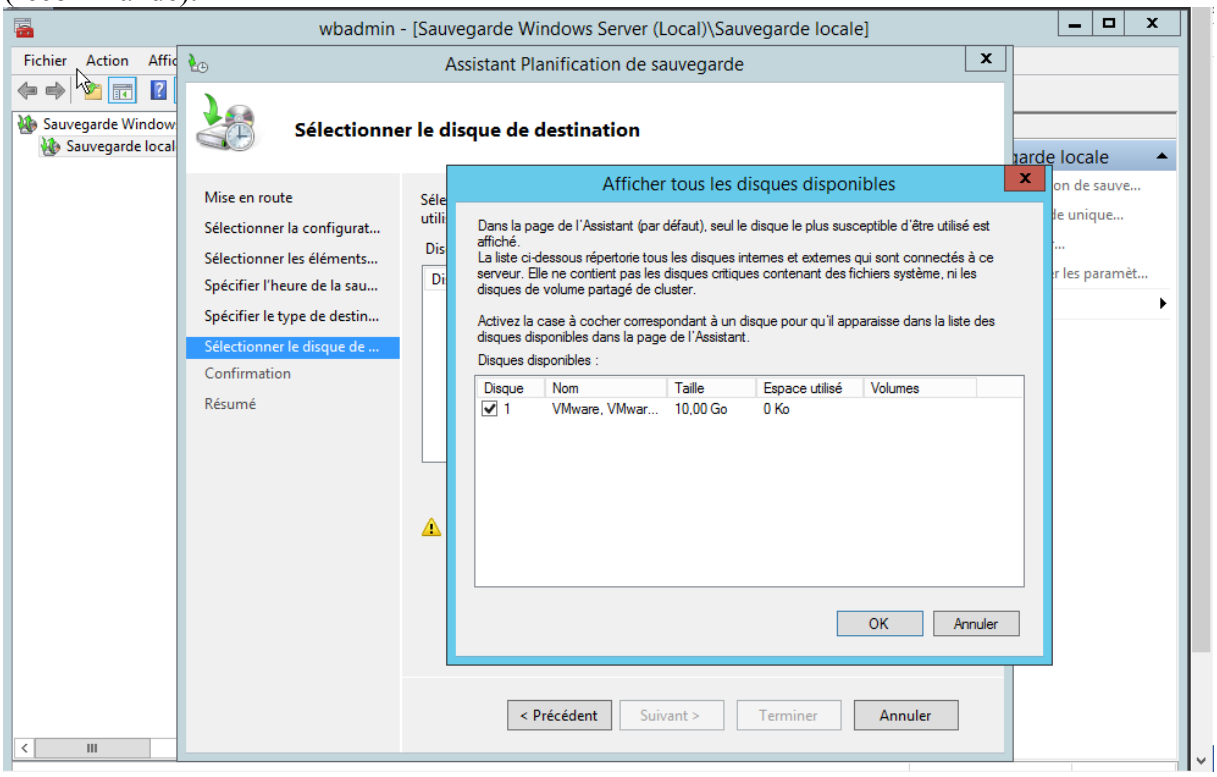


Figure 62 : sélection disque comme support de sauvegarde

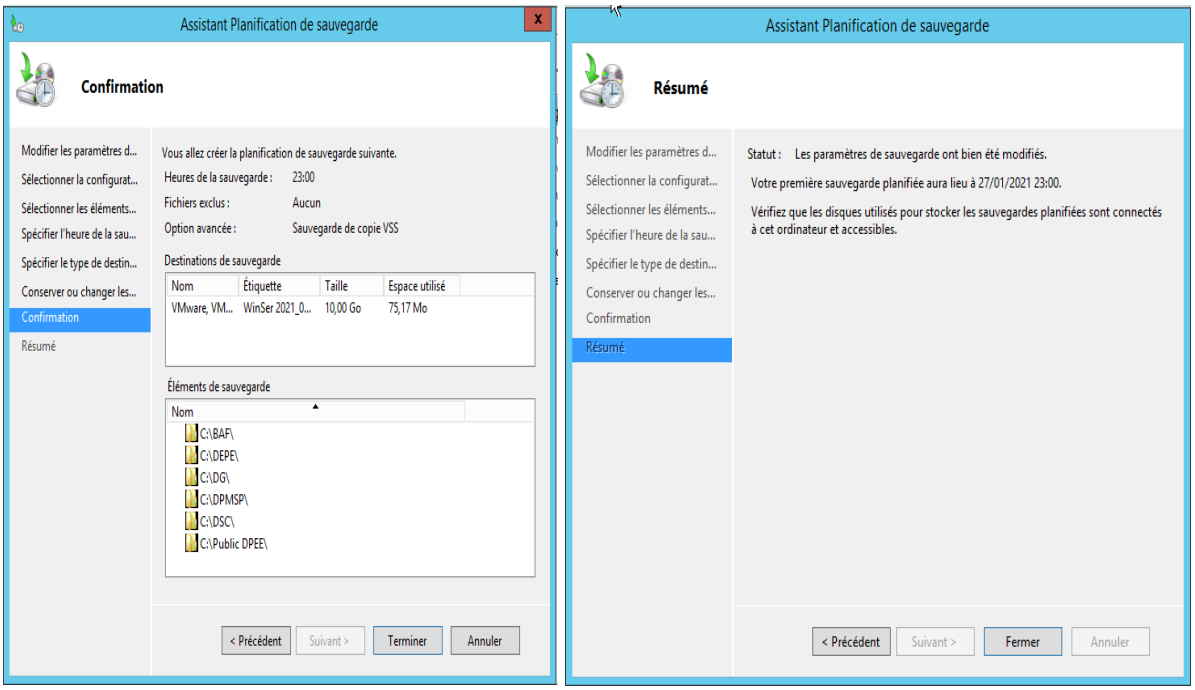


Figure 63 : aperçu de la configuration de notre sauvegarde

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

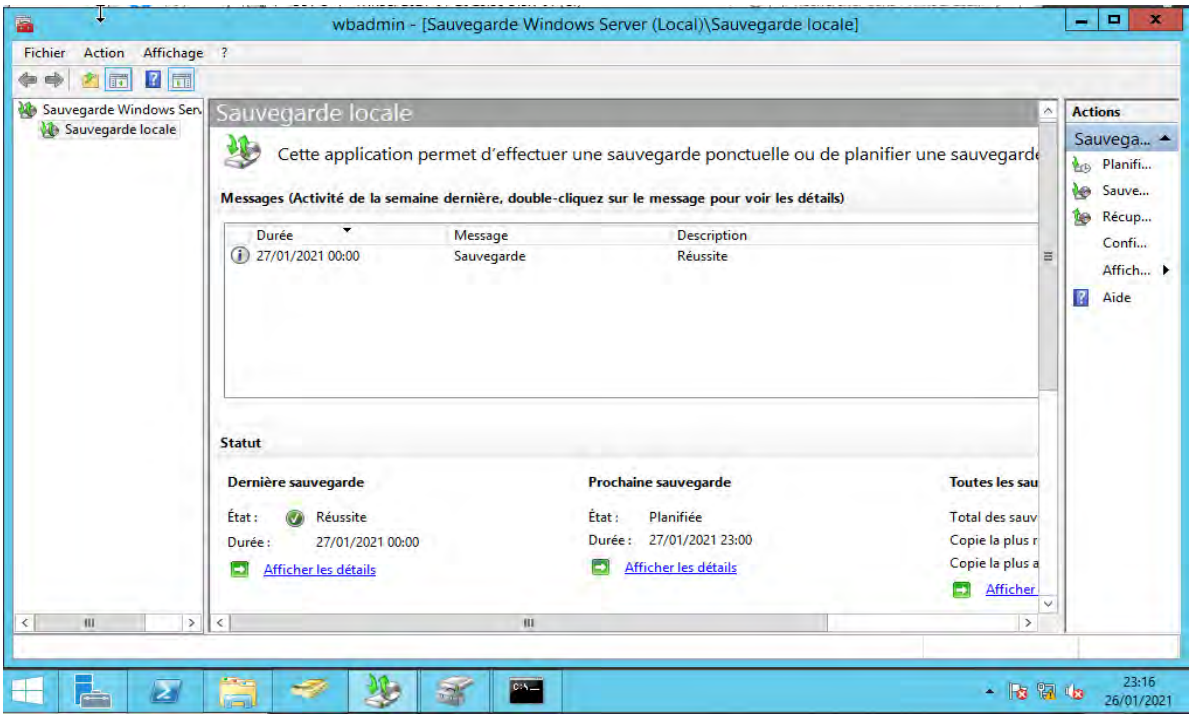


Figure 64 : aperçu de la sauvegarde réussite

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.

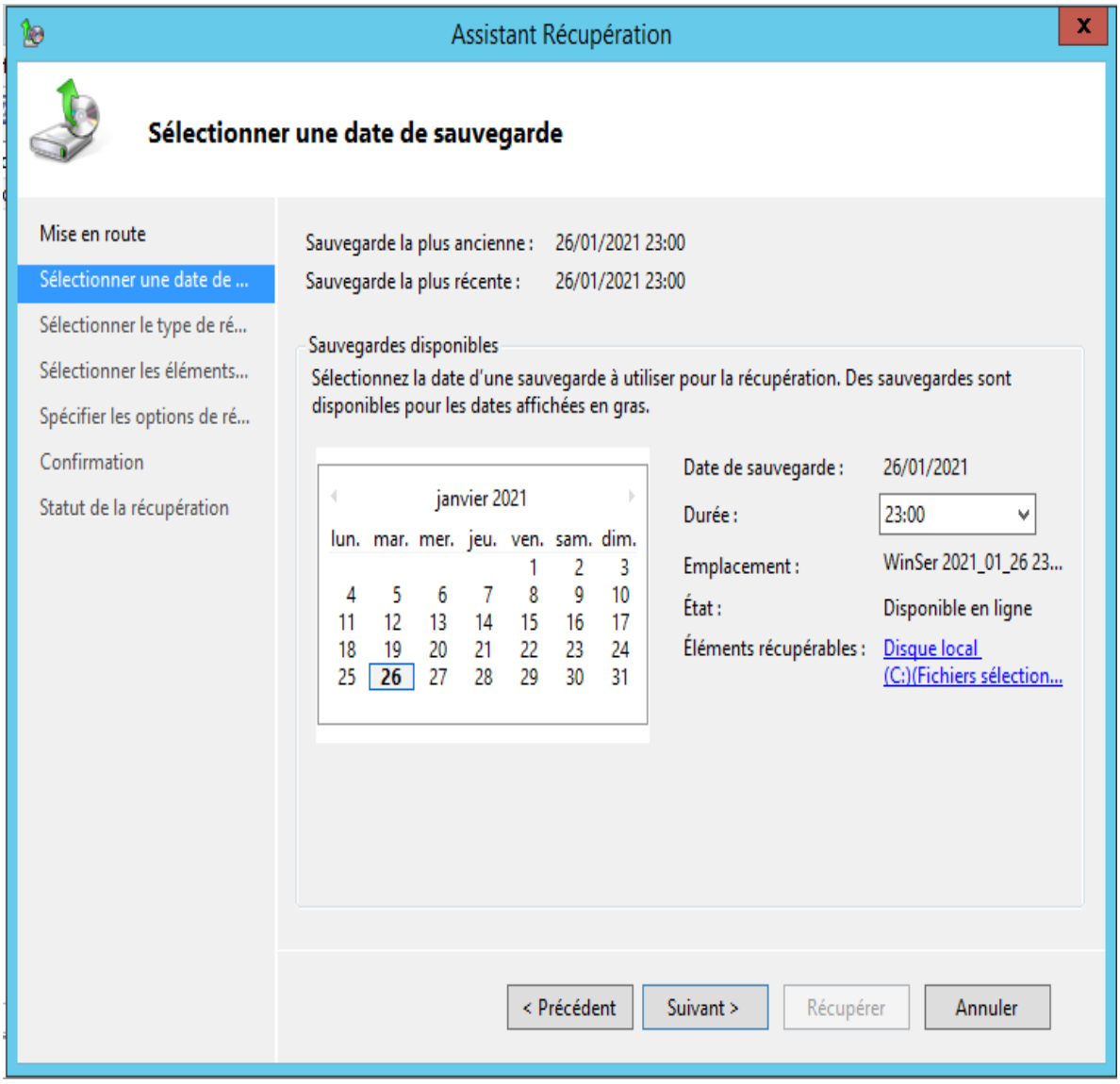


Figure 65 : assistant de récupération

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

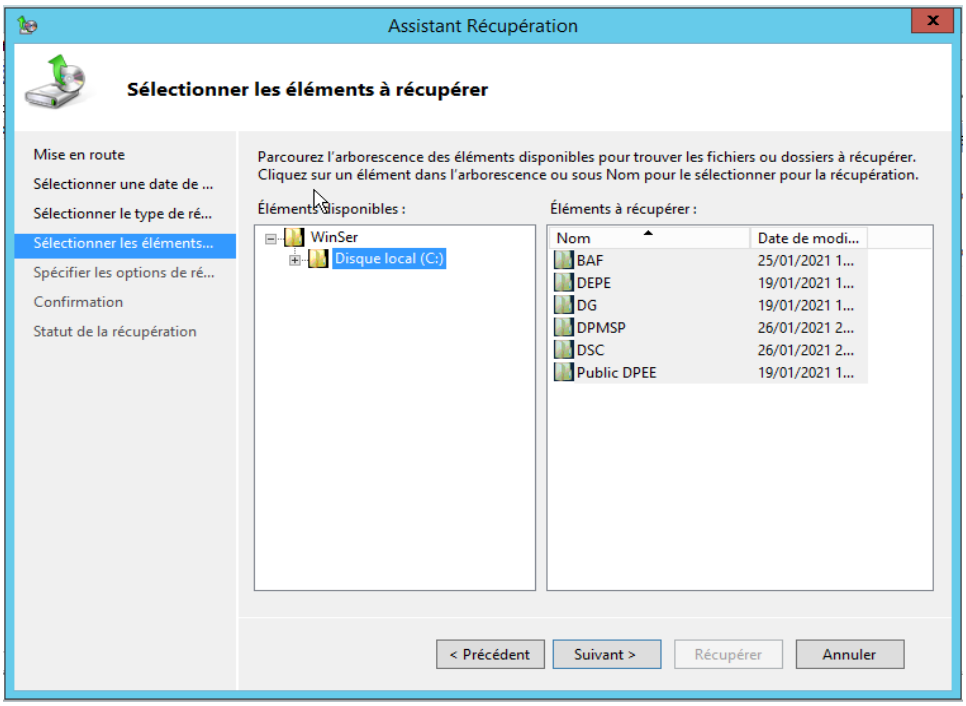


Figure 66 : sélection des dossiers à récupérer

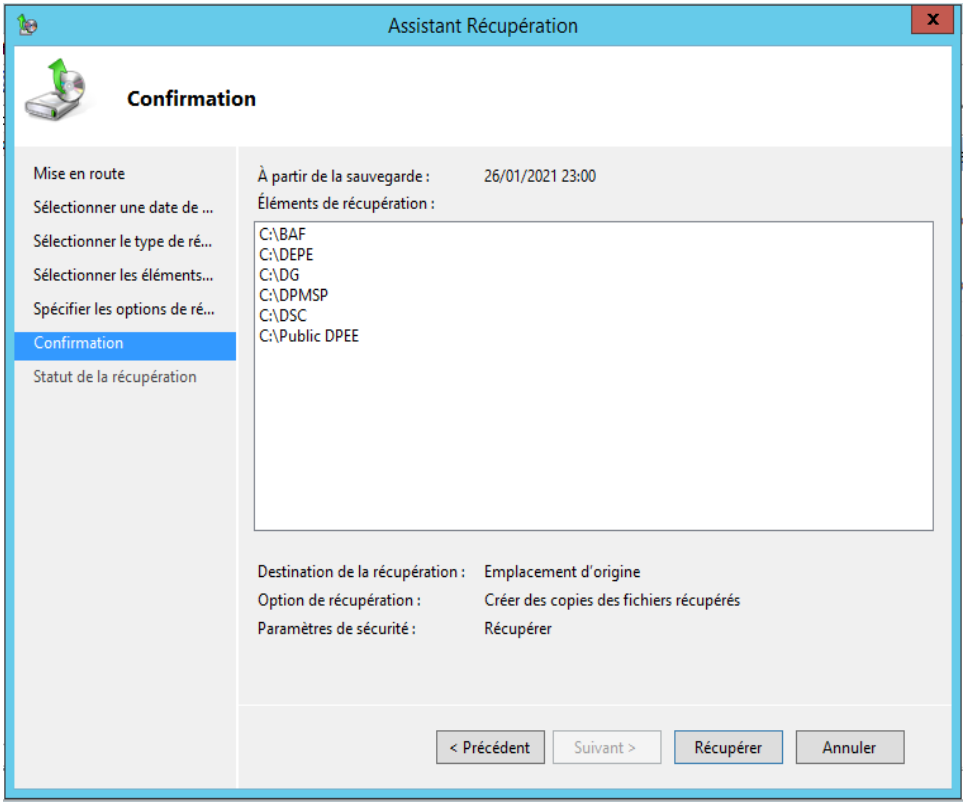


Figure 67 : liste des dossiers ou fichiers à récupérer

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  Un NAS QNAP avec quatre disque du	NAS pour Network Attached Storage est un serveur de stockage en réseau. 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.	1
Disques durs adaptés aux **serveurs** 	Le principal avantage est la redondance des disques dur et données. En effet, un NAS possède plusieurs disques durs qui fonctionnent en RAID. Le but est d'éviter les pertes de données. Par exemple, si un disque dur tombe en panne, les données restent accessibles sur un autre. Il faudra alors remplacer le disque dur défaillant. La plupart des NAS supportent le remplacement de disque à chaud, c'est à dire sans coupure électrique. Aucune opération n'est à faire par l'utilisateur car les données vont alors être synchronisées automatiquement. Il existe plusieurs types de RAID avec des fonctionnements différents. Ces derniers sont numérotés : RAID 0, RAID 1, etc. Capacité : 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 (donnés critiques de l'entreprise) et Les données sur l'état du système). On à 18 entités d'après l'organigramme de la DG. Chaque entité va disposer 1To comme espace sur le disque. Donc la capacité prévue pour l'achat est 18 TO (18 000 go) pour chaque disque.	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

CONCLUSION

L'étude suivante aurait pu porter, du fait de la pandémie de Covid 19, sur la configuration du système avec accès distant (du fait du télétravail qui est la tendance actuelle) et la sauvegarde sur le cloud…. Cependant les outils et moyens mis à notre disposition ne nous ont pas permis de la réalisée.

Un système de gestion et surveillance des accès et identités dans une structure est une solution de qualité pour l'assurance de la sécurité. Sa mise en place est certes couteuses, mais le retour sur investissement est très visible car facilitant l'accès et le partages de données aux utilisateurs et administrateurs, accroit aussi fortement la productivité au sein de la structure.

Ce projet nous a permis de connaitre comment mettre en place une politique d'accès et d'identités pour assurer la sécurité.

Comme perspective de ce travail, nous souhaitons que le déploiement de cette solution prenne une autre tournure : celle d'une réalisation future (qui est prévue même par le Responsable des systèmes d'information) à savoir la possibilité d'acheter les équipements physiques nécessaires et de mettre en place l'ensemble des configurations qui ont été fait.

BIBLIOGRAPHIE

SAFESCAN « *Safescan-TA-8000-Series-Manual-FR* » (18-03-2015)

SAFESCAN « *Safescan-TA-8010-Productsheet-FR*» (18-03-2015)

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS
« *Gestion et Gouvernance des Identités et des Accès* » Guide pratique – Mise en œuvre
Publié par CLUSIF (Février 2017)

IBM Software & IBM Security Systems
« Gestion des identités et des accès pour garantir la conformité et réduire les risques » ©
Copyright IBM Corporation 2012

WEBOGRAPHIE

https://fr.wikipedia.org/wiki/Windows_Server_2012 (vue le 12/01/2021)

https://www.toutwindows.com/windows-server-2012-installation/ (vue le 12/01/2021)

https://www.safescan.com/fr-be (vue le 28/12/2020)

https://www.safescan.com/fr-be/store/pointeuses-badgeuses (vue le 28/12/2020)

https://fr.wikipedia.org/wiki/Gestion_des_identit%C3%A9s_et_des_acc%C3%A8s (vue le 28/01/2021)

https://hal.archives-ouvertes.fr/hal-00879556/document (vue le 03/01/2021)

https://dantilatech.com/controle-dacces/ (vue le 28/12/2020)

https://fr.wikipedia.org/wiki/Microsoft_Azure (vue le 05/03/2021)

https://clusir-rha.fr/public/fichiers/presentation/2016-2017/20170225-gestion-et-gouvernance-des-identites-et-des-acces-guide-pratique-mise-en-%C5%93uvre.pdf (vue le 002/01/2021)