International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 12, Issue 10 [October. 2023] PP: 147-161

Déploiement d'un serveur de filtrage des fichiers utilisant Windows Server 2012 R2 dans un système de communication interne d'entreprise.

[Deployment of a file filtering server using Windows Server 2012 R2 in an internal corporate communication system].

[1]Dr YENDE RAPHAEL Grevisse, [2]KAHAMBU KASAYI Merveille, [3]KABEYA ILUNGA Paulin, [4]BAKAJIKA NGANDU Léonard, [5]KABADA SESWA David-Jackson, [6]TSHIMANGA MUKADI Trésor.

[1,4]Département d'Informatique de l'Université Notre Dame du Kasayi (UKA), Kasaï Central, Kananga (RDC).
[2]Département d'Informatique de l'Institut Supérieur des Arts et Métiers de Butembo (ISAM/Butembo).
[3]Département d'Informatique de l'Université Saint Laurent de Kananga (USLK/Kananga).
[5]Département d'Informatique de l'Institut Supérieur de Commerce de Goma (ISC-Goma), Goma (RDC).
[6]Departement d'Informatique et Assistant de Recherche à l'Institut Supérieur de Développement Rural de DEMBA (ISDR-DEMBA), Kasaï Central (RDC).

Résumé : *La présente étude intitulée « Déploiement d'un serveur de filtrage des fichiers utilisant Windows Server 2012 R2 dans un système de communication interne d'entreprise » se veut de renforcer la sécurité des données échangées au sein de l'infrastructure. Cette solution offre des fonctionnalités avancées de filtrage, de surveillance et de protection contre les menaces potentielles liées aux fichiers. Elle permet également de garantir la conformité aux politiques de sécurité de l'entreprise et de prévenir les fuites de données sensibles. Grâce à une administration centralisée et à des rapports en temps réel, les administrateurs peuvent gérer efficacement le serveur de filtrage et détecter rapidement les anomalies ou les violations des politiques de sécurité. En intégrant cette solution avec les systèmes existants de communication interne, les entreprises bénéficieront d'une protection avancée des données et d'une meilleure surveillance de la sécurité… L'originalité cette recherche repose sur la capacité à intégrer le serveur de filtrage dans le système de communication interne existant de l'entreprise, en veillant à préserver la compatibilité et l'interopérabilité avec d'autres outils et plateformes utilisées. L'exploitation des fonctionnalités de Windows Server 2012 R2, telles que le filtrage avancé, l'administration centralisée et les rapports en temps réel, permettra d'améliorer la sécurité des données échangées au sein de l'infrastructure et de réduire les risques liés aux logiciels malveillants et aux fuites de données, mais aussi garantir la simplification d'une administration centralisée dans sa gestion.*

Mots-clés : *Déploiement, Serveur 2012 R2, Filtrage, Fichiers, Windows, Système, Entreprise, Interne, Communication, etc.*

Abstract: *This study, entitled "Deployment of a file filtering server using Windows Server 2012 R2 in a corporate internal communications system", aims to strengthen the security of data exchanged within the infrastructure. The solution offers advanced filtering, monitoring and protection against potential file-based threats. It also ensures compliance with corporate security policies and prevents the leakage of sensitive data. With centralized administration and real-time reporting, administrators can effectively manage the filtering server and quickly detect anomalies or breaches of security policies. By integrating this solution with existing internal communication systems, companies will benefit from advanced data protection and improved security monitoring... The originality of this research lies in the ability to integrate the filtering server into the company's existing internal communication system, while ensuring compatibility and interoperability with other tools and platforms used. Exploiting the features of Windows Server 2012 R2, such as advanced filtering, centralized administration and real-time reporting, will not only improve the security of data exchanged within the infrastructure and reduce the risks associated with malware and data leaks, but also ensure that centralized administration is simplified in its management.*

Keywords: *Deployment, Server 2012 R2, Filtering, Files, Windows, System, Communication, Enterprise, Internal, etc.*

Date of Submission: 09-10-2023 Date of acceptance: 23-10-2023

I. INTRODUCTION

La communication est un pilier fondamental dans les entreprises modernes. C'est un processus qui facilite la transmission d'informations, d'idées et d'objectifs entre les membres de l'organisation. Effectivement, elle facilite la collaboration, l'amélioration la prise de décisions, la gestion des crises, la motivation et le renforcement des relations entre les employés. Par conséquent, Les entreprises qui mettent en place une communication efficace sont mieux préparées pour réussir dans un environnement professionnel compétitif et en constante évolution.

Avec l'augmentation des moyens de communication comme les e-mails, les messages instantanés et les réseaux sociaux internes, les employés échangent dorénavant en ligne à partir de n'importe quel endroit sans se soucier des contraintes géographiques et financières qui prolongent nos conversations et augmente même la quantité des informations échangées. Ce qui peut rendre difficile la digestion des informations pertinentes, entrainant par la même occasion une communication inefficace.

De plus, Les NTIC (Nouvelles Technologies de l'Information et de la Communication), telles que les ordinateurs, les téléphones mobiles, les médias sociaux et Internet, ont profondément impacté la manière dont la communication est réalisée dans les entreprises actuelles. Les NTIC ont considérablement accéléré la vitesse de la communication. Les e-mails, les messages instantanés et les appels téléphoniques permettent des échanges rapides et instantanés, facilitant ainsi la prise de décisions et la résolution des problèmes quotidiens de gestion. Toutefois, La sécurité dans le partage des informations avec les NTIC (Nouvelles Technologies de l'Information et de la Communication) est une préoccupation majeure pour les entreprises. Alors que ces technologies permettent des échanges rapides et efficaces, elles présentent également des risques potentiels pour la confidentialité, l'intégrité et la disponibilité des informations (1). Cependant, la sécurité ne doit pas être une gêne au quotidien, elle ne doit pas aussi perturber le fonctionnement habituel de l'entreprise. Pour cela, il faut donc établir une politique de sécurité efficace qui identifie les besoins de la sécurité, en termes des risques et des conséquences que l'entreprise pourra faire face dans le cas échéant (1).

Par ailleurs, la mise en place de nombreux outils et de techniques d'attaques sont aujourd'hui une véritable bête noire pour les administrateurs système et des réseaux locaux d'entreprises. La sécurité informatique reste donc la seule solution pour garantir la confidentialité, l'intégrité et la disponibilité de la multitude d'informations échangées dans les entreprises contemporaines. La protection contre les cyberattaques est une preuve irréfutable de la responsabilité en matière de la sécurité des informations. Les entreprises sont appelées à mettre en place des mécanismes de protection plus efficaces tels que les pare-feu, les logiciels antivirus et les systèmes de détection des intrusions pour identifier et bloquer les attaques potentielles.

Il incombe subséquemment à chaque administrateur du système de choisir parmi les multitudes des solutions existantes de proposer celles qui semblent non seulement être efficaces mais aussi évolutives, en appliquant des règles strictes de gestion des accès et des droits pour contrôler qui peut accéder à quelles informations dans le système interne de l'entreprise. Parmi ces solutions, cette étude a opté de mettre en exergue la technique de filtrage des informations sous Windows Server 2012 R2 qui semble garantir la conformité aux politiques de sécurité de l'entreprise et de prévenir les fuites de données sensibles (10).

Le filtrage des informations dans les entreprises implique la surveillance et le contrôle des données qui entrent ou sortent du réseau de l'entreprise. Il s'agit d'une pratique courante visant à protéger les ressources internes et à garantir le respect des politiques de sécurité et de conformité. Le filtrage des informations est essentiel pour protéger les données confidentielles et sensibles de l'entreprise. Cela permet de prévenir les fuites de données, les attaques de phishing et autres menaces de sécurité. En filtrant les informations, les entreprises peuvent bloquer l'accès aux sites web malveillants, aux courriels de phishing et aux téléchargements non autorisés, renforçant ainsi la sécurité globale de l'entreprise.

Grâce aux techniques de filtrages des informations, les entreprises deviennent désormais soumises à des réglementations strictes concernant la confidentialité des données, telles que le RGPD (Règlement Général sur la Protection des Données) dans l'Union européenne. Le filtrage des informations permet alors de se conformer à ces réglementations en contrôlant les données qui entrent et sortent du réseau de l'entreprise, ainsi qu'en évitant la propagation de données confidentielles. En filtrant les informations, les entreprises peuvent éviter les distractions en ligne et les utilisations abusives des ressources informatiques. Cela permet de réduire les pertes de temps et d'améliorer la productivité des employés en les concentrant sur les tâches professionnelles essentielles. En définitive, le filtrage des informations aide autant les entreprises à gérer efficacement leur bande

passante en limitant l'accès à des sites web ou à des contenus gourmands en bande passante. Cela permet d'optimiser les performances du réseau en évitant les ralentissements causés par une utilisation excessive des ressources.

En égard de ce qui précède, la préoccupation majeure de cette étude est d'évaluer l'efficacité la technique de filtrage des fichiers partagés sous Windows Server 2012 R2 au sein d'un système de communication interne d'Entreprise, en termes des accès et téléchargements non-autorisés, la protection contre les menaces potentielles liées aux fichiers partagés, la garantie de la conformité aux politiques de sécurité adoptées et la prévention contre les fuites de données sensibles de l'entreprise.

En définitive, rappelons que la présente étude se veut l'objectif principal de proposer un mécanisme efficace de sécurité des informations partagées au sein d'un système de communication interne de l'entreprise, en visant la protection, l'amélioration et la transformation des échanges de plus en plus diversifiées dans les entreprises modernes … Spécifiquement, cette étude tentera de développer les notions de l'utilisation des « File Server Ressource Manager sous Windows Server 2012 R2 » comme moyen de sécurité dans les systèmes de communication interne des Entreprises ; Contrôler les différents accès et téléchargements des informations en filtrant les permissions et les autorisations de chaque utilisateurs du systèmes et enfin Proposer un modèle schématique d'installation et de configuration d'un système de filtrage sécurisé au moyen File server Ressource Manager sous Windows serveur 2012 R2.

II. DEMARCHE METHODOLIQUE

La présente étude scientifique préconise l'utilisation des méthodes analytiques et PERT accompagné des techniques telles que l'interview et la documentation. La méthode analytique (10) nous a permis d'examiner les différents systèmes de communication interne existants dans nos entreprises modernes en vue d'en dégager une solution ajustée. Quant à la méthode PERT, elle nous a permis de faire un planning prévisionnel de notre projet en planifiant le risque et l'incertitude attachée à sa réalisation. La documentation nous a servi à la collecte des informations et l'interview nous a facilité l'interaction verbale pour appréhender quelques structures de communication interne qui ont constituées notre population d'étude.

III. PLANNING PREVISINEL DU PROJET

III.1. Identification des taches

Code	Taches	Durée en jour
A	Etude de faisabilité	10
B	Récolte des données	30
C	Spécification des besoins	15
D	conception du système	20
E	Configuration du nouveau système	30
F	Test du nouveau système	7
G	Déploiement du système	10
H	Evaluation du système	14
TOTAL		136

Tableau 1. Identification des tâches.

III.2. Détermination des antériorités et postériorités

1. Détermination des antériorités

A cette étape, il revient à déterminer les tâches antérieures à d'autres. La question qu'on se pose ici est de savoir quelle tâche doit être terminée pour que l'autre commence. La première tâche est appelée antécédente ou prédécesseur alors que la seconde est dite subséquente ou successeur (3).

Code	Durée en jour	antériorités
A	10	-
B	30	A
C	15	B
D	20	C

E	30	C, D
F	7	E
G	10	F
H	14	G

Tableau 2. Détermination des antériorités.

Commentaires : Dans le tableau ci-dessus, nous avons déterminé les taches antérieurs de notre projet. La tache A n'a pas d'antériorité car celle-ci est la tache initiale, elle ne demande pas qu'il y ait exécution d'une autre tâche avant elle. La tâche B a comme antériorité la tache A parce que ce deux tâches ne sont pas lié c'est-à-dire la récolte des données va débuter après l'étude des faisabilités qui est la tache A. La spécification des besoins qui est la taches C a comme antériorité B car on spécifie ou on analyse les besoins dur base des données récoltés. La conception du système (tache D) a comme taches antérieurs C parce que lors de la conception du système on part de la spécification des besoins (de l'analyse des besoins). La configuration du système (tâche E) a comme antériorité les tâches C et D parce qu'on configure un système grâce à l'analyse des besoins et la conception. La tâche F a comme antériorité E car on ne teste qu'un système qui a été configuré. G a comme tâche antérieur F car on déploie un système déjà configuré, le déploiement dépend du test. La tâche H a comme antériorité la tâche G parce qu'on évalue un système qui est déjà mise en place ou déployé.

2. Détermination des postériorités

Dans la phase de la détermination de tâches postérieures, on se demande si quelle tâche doit s'exécuter après l'autre ou succède l'autre. Dans le tableau ci-dessous nous allons établir la succession logique des tâches.

Code	Durée en jour	antériorités	Postériorités
A	10	-	B
B	30	A	C
C	15	B	D, E
D	20	C	E
E	30	C, D	F
F	7	E	G
G	10	F	H
H	14	G	-

Tableau 3. Détermination des postériorités.

Commentaires : la tache B est successeur de A car cette dernière débute tout juste après la fin de l'étude de la faisabilité (tâche A). La spécification des besoins est postérieur à la récolte des données du fait que cette dernière commence tout juste après la récolte des données c'est-à-dire la fin de la récolte des données déclenche le début de la spécification des besoins. La tache C a comme postériorités D, E car le déclenchement de ces deux tâches dépend de la réalisation la tache C. La conception du système (tache D) a comme tache postérieur E car après la conception du système on passe directement au paramétrage (configuration) de ce dernier. La tache F est postérieure à E car après le test est l'étape qui vient après la configuration du système. Le déploiement est la tache postérieure au test car après le test du système on passe directement à la mise en œuvre. Apres le déploiement d'un système (mise en œuvre) on passe à l'évaluation du système (tâche H)

III.3 Calculs des niveaux

La détermination des niveaux se fait selon les règles suivantes :

- Sont du niveau 1, les tâches qui n'ont pas d'antériorités;
- Celles du niveau 2 sont les tâches qui ont pour antériorité les tâches du niveau 1 ;
- Le niveau 3 est celui des tâches qui ont pour antériorité les tâches du niveau 2;

Ainsi on continue, jusqu'à ce que toutes les tâches du projet aient pu être positionnées. Voici le tableau qui montre le différent niveau des taches :

Code	Durée à jour	antériorités	Postériorités	niveaux
A	10	-	B	1
B	30	A	C	2
C	15	B	D, E	3
D	20	C	E	4
E	30	C, D	F	5
F	7	E	G	6
G	10	F	H	7
H	14	G	-	8

Tableau 4. Calculs des niveaux.

II.4. Construction du réseau PERT

Le réseau PERT, nous permet de voir sur un schéma la succession des différentes tâches du début jusqu'à la fin et leurs durée respectives.

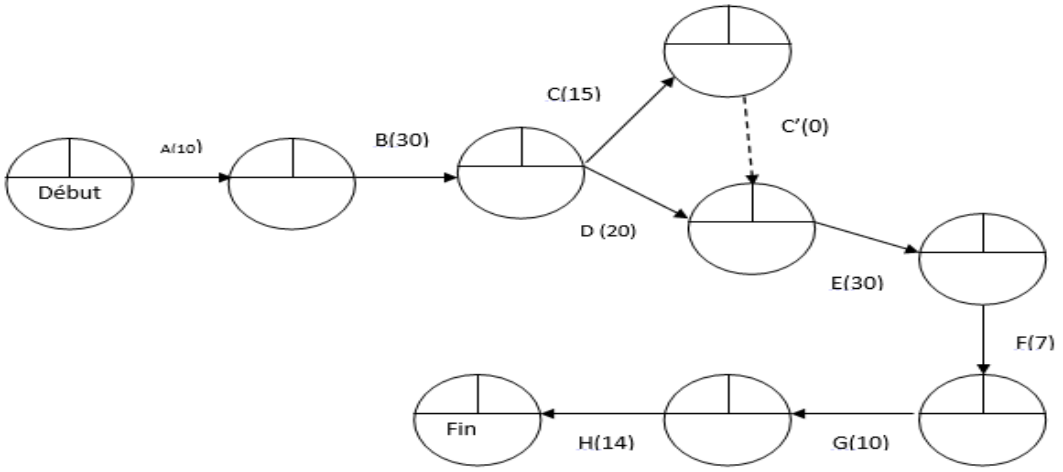

Figure 1. Construction du Réseau PERT.

III.5. Calculs de dates au plus tôt et les dates au plus tard

Le planning d'un projet, sous la méthode PERT, exige qu'à chaque tâche qu'on associe un délai ou une durée. Ce délai a une date de début qui peut être avancée (date au plus tôt) ou retardée (date au plus tard) et une date de fin pouvant être également avancée (date de fin au plus tôt) ou retardée (date de fin au plus tard). Ainsi, compte tenu des contraintes d'enchaînement des tâches, de leur durée et de la date de début de projet, la tâche Ti ne peut pas commencer avant la date au plus tôt (D+tôt) et ne peut se terminer avant la date de fin au plus tôt (F+tôt). Aussi, compte tenu des contraintes d'enchaînement des tâches, de leur durée et de la date de fin de projet, la tâche Ti ne doit pas se terminer après la date de fin au plus tard (F+tard) sans mettre le projet en retard ; de même, elle ne doit pas commencer après la date au plus tard (D+tard), sinon la date de fin du projet serait dépassée (3).

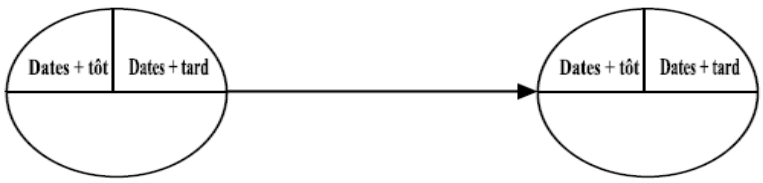

Figure 2. Illustration de date des taches sur le réseau PERT.

1. Calcul de dates au plus tôt(3)

On commence tout d'abord par calculer les **dates au plus tôt.** Pour une étape donnée, cette information détermine à quelle date minimum depuis le début du projet sera atteinte, au plus tôt. L'étape considérée. Pour ce faire, on se base sur l'estimation de la durée des tâches. On part de l'étape de début, pour laquelle la date au plus tôt est initialisée à 0. Et on parcourt le réseau en suivant l'agencement des tâches déterminé auparavant. Deux méthodes de calcul existent alors selon que l'étape considérée est atteinte par 1 ou par plusieurs tâches :

- 1 tâche : il n'y a qu'un seul chemin possible pour atteindre l'étape : La date au plus tôt vaut la date au plus tôt antérieure à laquelle on rajoute la durée de la tâche liant les 2 étapes :

$$To0 = to1 + durée\ 1$$

- Plusieurs tâches : il y a plusieurs chemins possibles pour atteindre l'étape. On applique le procédé décrit ci-dessus (pour 1 tâche) pour chacune des tâches antérieures : la date au plus tôtvaut alors le maximum parmi ces résultats :

$$To0 = \mathbf{Max}\ (\ (to1 + durée!)\ \mathbf{:}(to2 + durée!) : \ldots\ )$$

2. Calcul des dates au plus tard(6)

On poursuit avec le calcul des **dates au plus tard.** Pour une étape donnée, cette information détermine à quelle date maximum, depuis le début du projet, doit être atteinte, au plus tard, l'étape considérée, afin que le délai de l'ensemble du projet ne soit pas modifié. Pour ce faire, on se base sur l'estimation de la durée des tâches. On part de l'étape de fin. Pour laquelle la date au plus tard est initialisée à la même valeur que la date au plus tôt et on parcourt le réseau en suivant l'agencement inverse des tâches. Là encore, il existe deux méthodes de calcul selon que 1 ou plusieurs tâches partent de l'étape considérée : 1 tâche : il n'y a qu'un seul chemin possible pour partir de l'étape : La date au plus tard vaut la date an plus tard« précédente » (la postérieure dans l'agencement des tâches) à laquelle on retranche la durée de la tâche liant les 2 étapes :

$$taO = ta1 - durée\ 1$$

Le graphe ci-dessous reprend toutes les dates de notre projet :

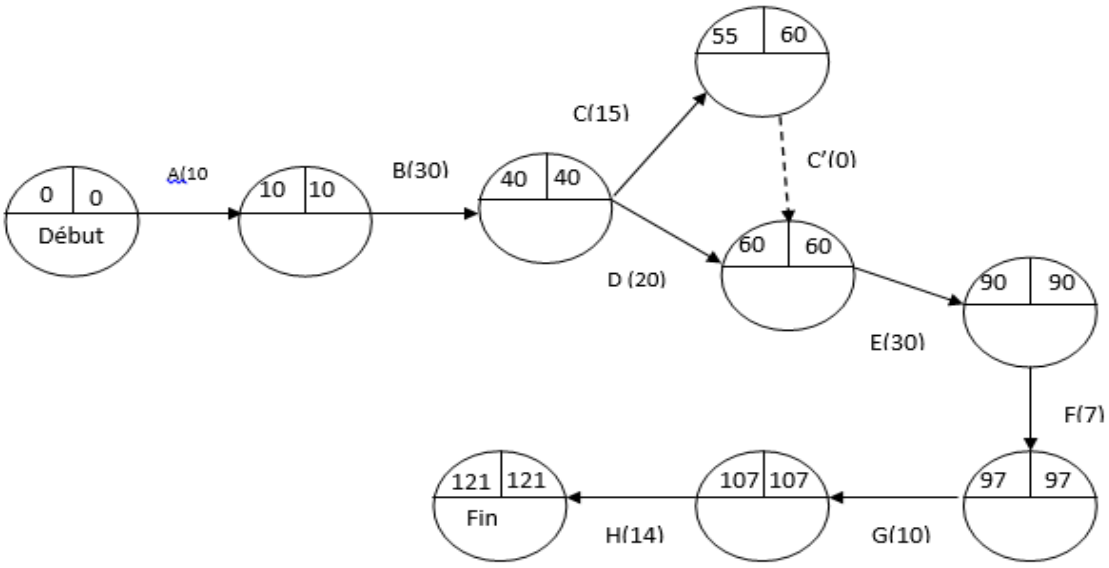

Figure 3. Réseau PERT avec les dates.

III.6. Calcul des marges

La **marge** attachée à chaque tâche est la différence entre date au plus tard (Tj,) et date au plus **tôt**(T_i). En l'absence de liens autres que des liens fin-début, elle peut être calculée indifféremment sur les dates de début ou sur les dates de fin. Sinon, on peut avoir deux marges différentes sur une tâche, l'une attachée au début de la tâche, l'autre attachée à la fin de la tâche. La marge représente la latitude dont on dispose quand on élabore le planning (3).

1. Calcul de marge libre

La marge libre d'une tâche indique le retard que l'on peut admettre dans la réalisation de cette tâche sans modifier les dates au plus tôt des tâches suivantes et sans allonger la durée optimale du projet. (3) Cette marge se calcule par la formule : ML = D+tot-dt-D+tot (9). Pour notre projet nous regroupons les marges libres dans le tableau ci- dessous

Tâches	Marges libres
A	=10-10-0=0
B	=40-30-10=0
C	=55-15-40=0
C’	=60-0-55=5
D	=60-20-40=0
E	=90-30-60=0
F	=97-7-90=0
G	=107-10-97=0
H	=121-14-107=0

Tableau 5. Calculs des marges libres.

2. Calcul de marge total

La marge totale d'une tâche indique le retard maximal que l'on peut admettre dans la réalisation de cette tâche sans allonger la durée optimale du projet. Cette marge se calcule par la formule : MT =D+tard-dt-D+tot (9)**.** Voici les différentes marges totales pour notre projet.

Tâches	Marges Total
A	=10-10-0=0
B	=40-30-10=0
C	=60-15-40=5
C’	=60-0-55=5
D	=60-20-40=0
E	=90-30-60=0
F	=97-7-90=0
G	=107-10-97=0
H	=121-14-107=0

Tableau 6. Calculs des marges totales.

III.7. Détermination du chemin critique

C’est le chemin dont la succession des tâches donne la durée d’exécution la plus longue et fournit le délai de fabrication de l’ensemble (10). Il s’agit donc d’un chemin qui reprend les tâches pour lesquelles la date au plus tôt est égale à la date au plus tard. C’est le chemin le plus long du projet(3).

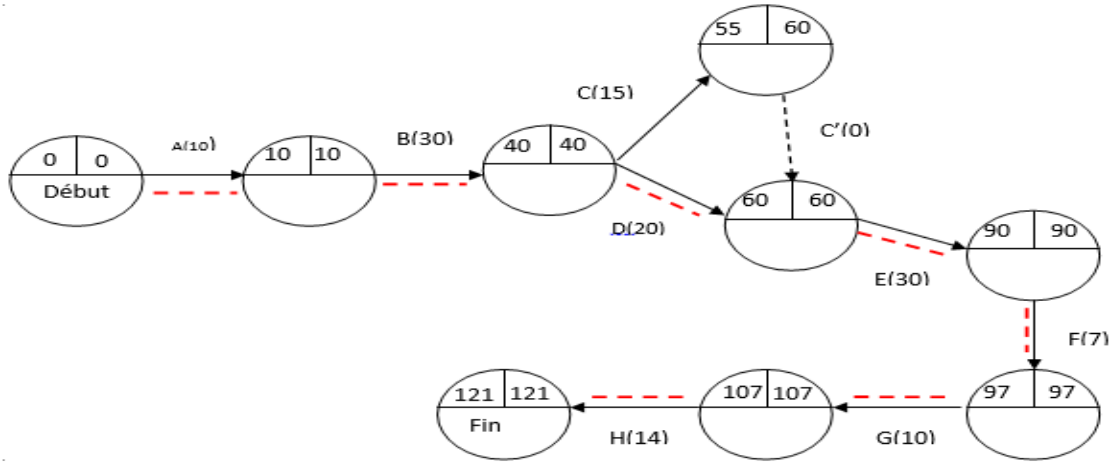

Figure 4. Détermination du chemin critique.

III.8. EVALUATION DU COUT DU PROJET

Quelle que soit le type et la nature d'un projet, l'évaluation du cout du projet s'avère quasi importante. En effet, la « gestion des coûts correspond à la définition, au contrôle et à l'ajustement éventuel du budget du projet » (2). Ainsi, cette partie repose essentiellement à l'évaluation du cout du projet pour la mise en place de notre système. Elle permet d'estimer les coûts d'investissement et de fonctionnement du projet.

Matériels	**P.U**	**Nombre**	**PT**
Licence de Windows serveur	800$	1	800$
Ordinateur	500$	1	500$
Logiciels	15$	2	30$
FAI	50$	12	600$
Courant	20$	12	240$
Autres (mise en jour, maintenance, imprévues)	90$	12	1080$
TOTAL			3250$

Tableau 7. Evaluation du cout du projet.

IV. CONCEPTION ET CONFIGURATION DU SYSTEME PROPOSE

Ici, le système proposé est basé sur le filtrage des fichiers. Pour ce faire nous avons utilisé le système d'exploitation Windows Server 2012R2 pour la mise en place de la solution. Le système mise en place, une fois intégrer au sein du cyber permettra à ce dernier de contrôler les utilisateurs en filtrant leurs fichiers ; la mise en place de la fonctionnalité de filtrage a nécessité l'installation de Windows serveur.

IV.1. Installation de Windows serveur

Windows serveur est un système d'exploitation comme tous les autres systèmes bien qu'il soit un système d'exploitation serveur ; ce dernier se fait comme celle d'autres systèmes d'exploitation hors ligne. A la fin de l'installation de Windows serveur il vous présente à son bureau une fenêtre appeler tableau de bord qui permettra de faire la configuration du serveur et d'afficher les différents rôles et fonctionnalités installes sur le serveur; il se présente comme suit :

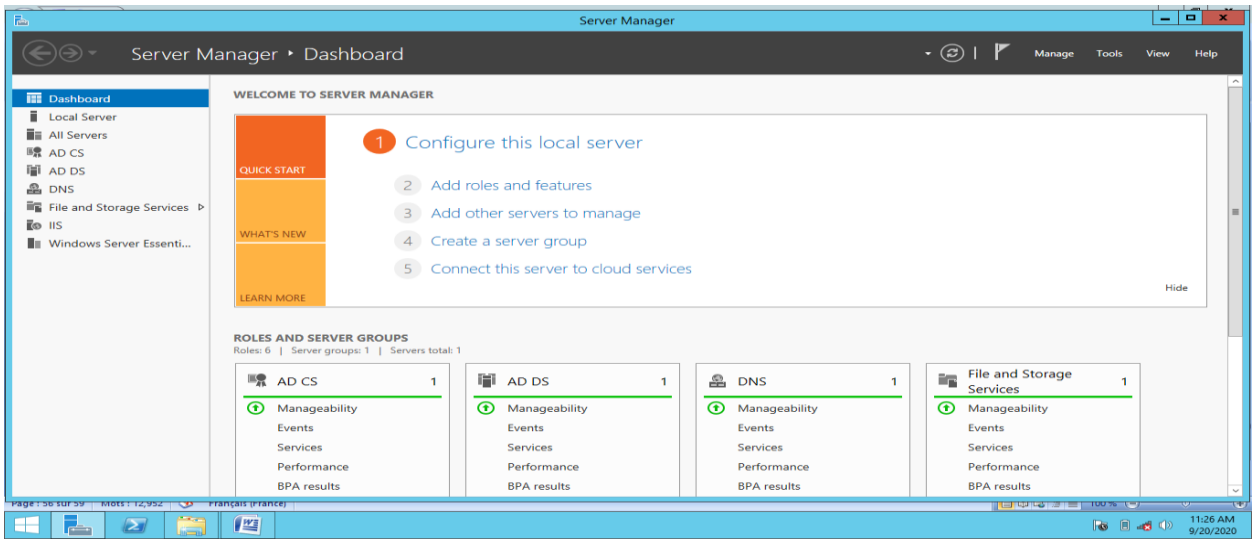

Figure 5. Tableau de Bord de Windows Serveur 2012 R2.

IV.2. Configuration du serveur

1. La création des utilisateurs

Après l'installation de Windows serveur ; nous procédons à la création des utilisateurs avec possibilité de créer les utilisateurs de deux manière : soit à partir du tableau de bord ou soit à partir de la fonctionnalité de Windows appeler Windows essentials tableau de bord (dashbord). Pour notre part, nous avons pris la procédure avec Windows essential. La figure Ci-dessous montre l'interface de Windows essential :

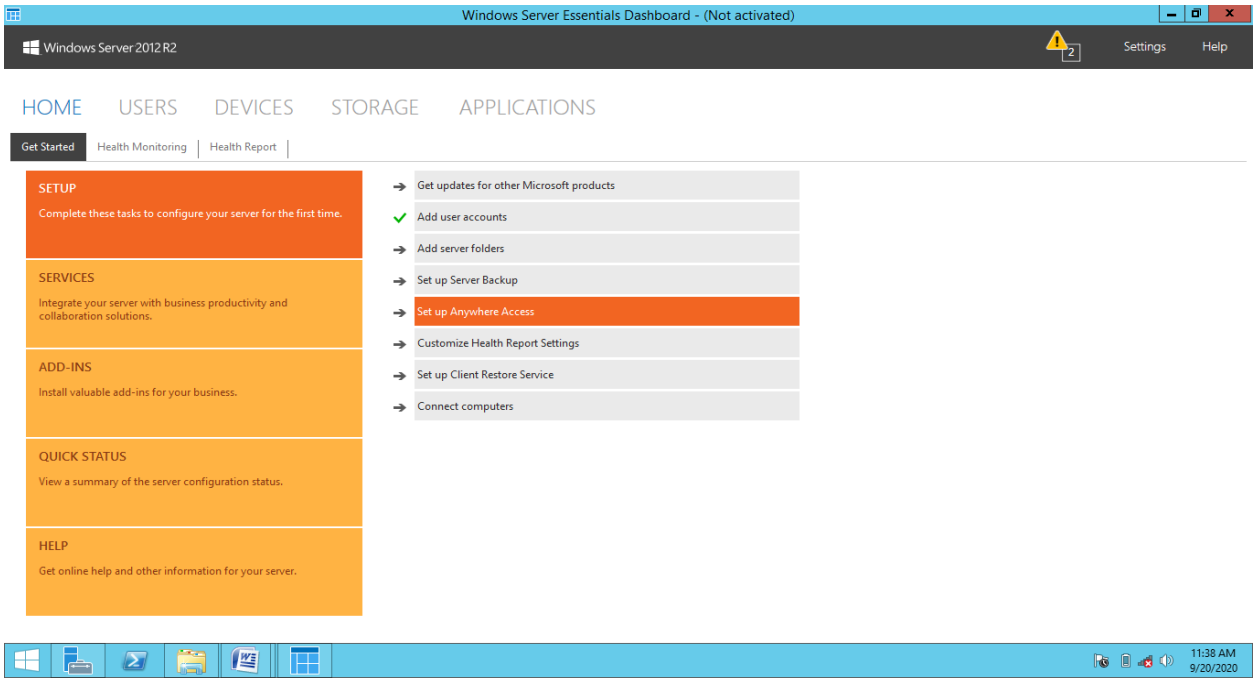

Figure 6. Windows Essential Tableau de Bord.

Pour créer un utilisateur pour Windows essential premièrement sur l'interface de ce dernier nous allons vers ajouter des comptes d'utilisateurs et cette commande nous présente l'interface ci-dessous afin de compléter les informations à rapport avec l'utilisateur.

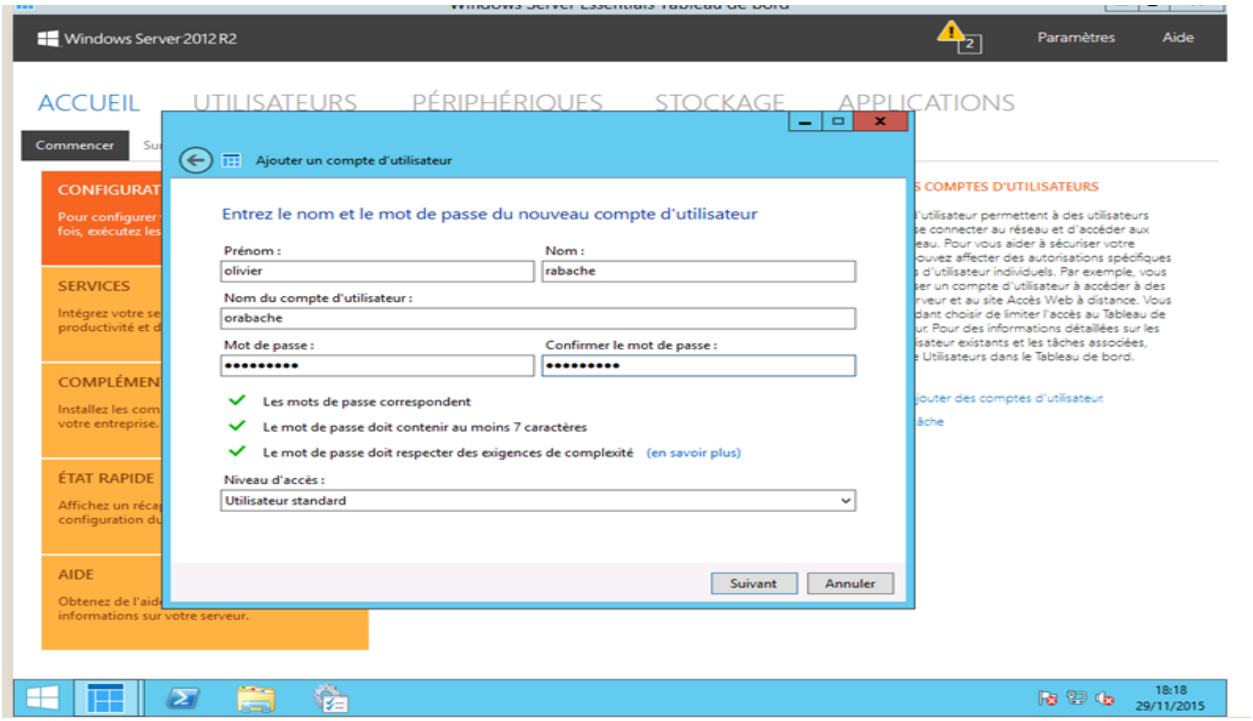

Figure 7. Interface pour la création des Utilisateurs.

Après avoir compléter les informations de l'utilisateur on clique sur suivant et par après la fenêtre suivante s'affiche pour confirmer que l'utilisateur a été ajouté correctement.

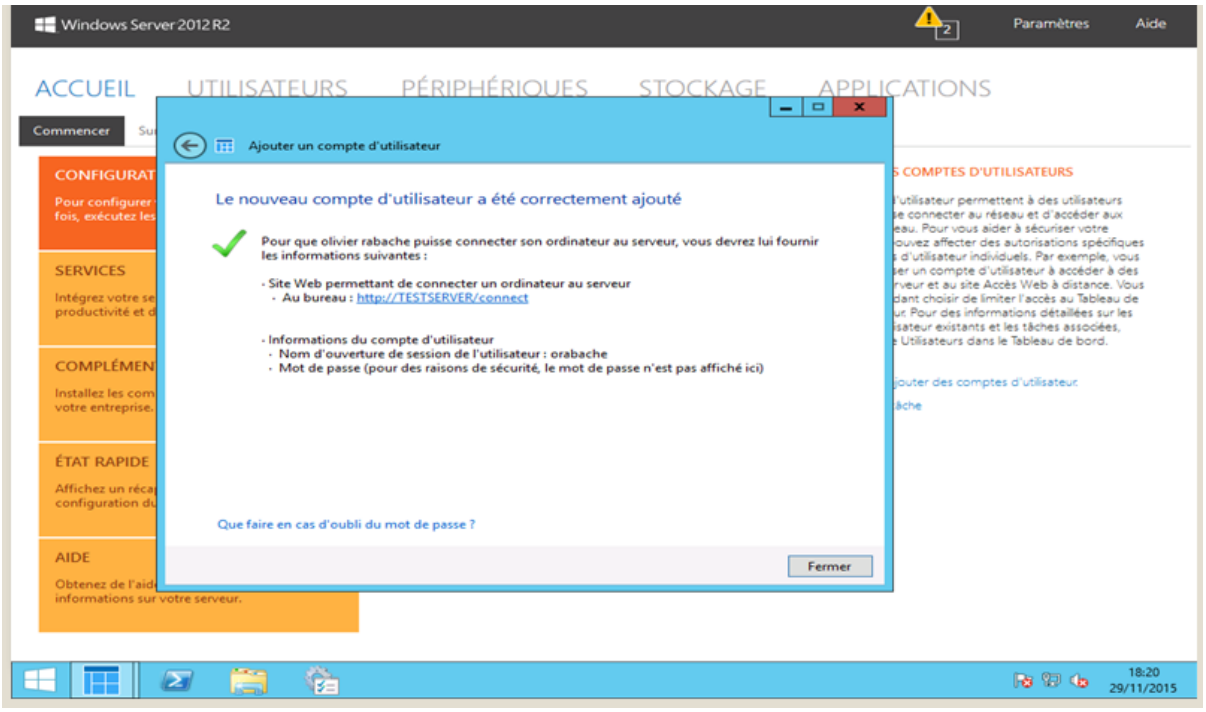

Figure 8. Ajout de l'utilisateur avec Succès.

Apres avoir créé l'utilisateur on doit lui attribuer les différentes autorisations ou accès c'est-à-dire qu'on lui donne l'autorisation à accéder par exemple aux dossiers ; à la page d'accueil ; à l'ordinateur, etc. c'est ce qui illustre la figure ci-dessous :

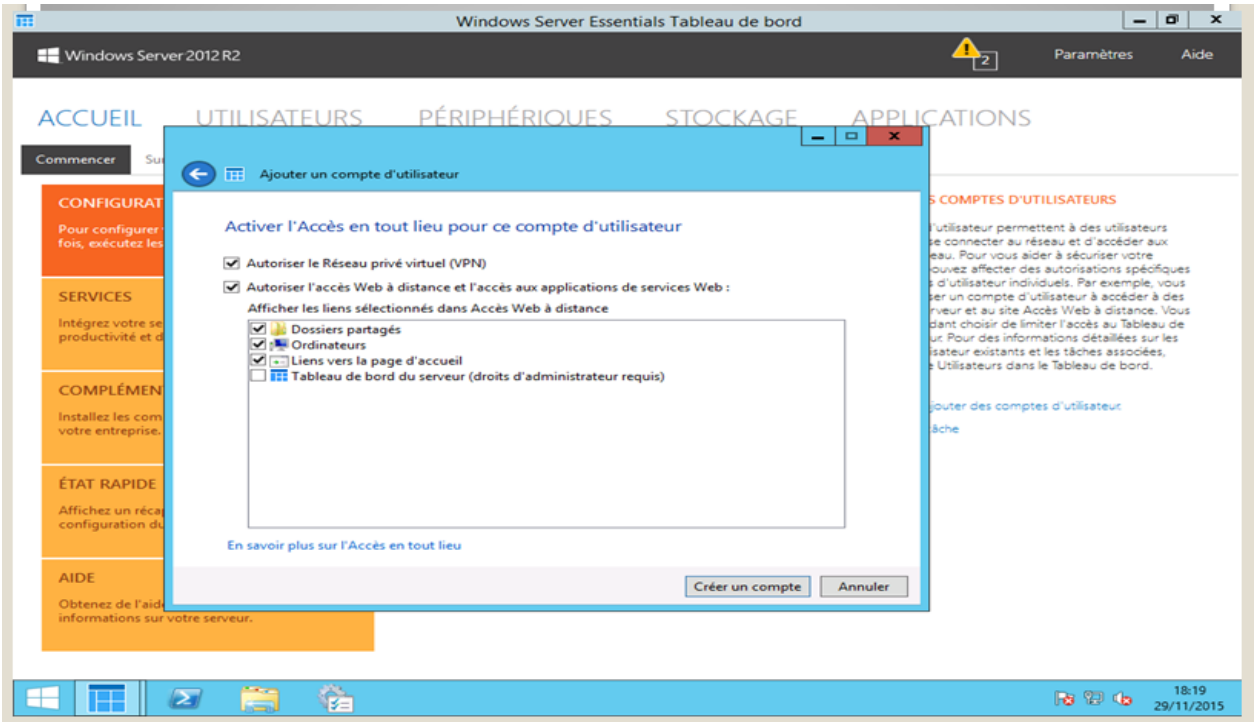

Figure 9. Interface de l'octroi d'accès aux Utilisateurs.

IV.3. Installation de file server ressource manager pour le filtrage des fichiers.

L'installation de la fonction file server ressource management se résume à quelque étapes. Initialement, on clique sur « *add roles and features* », ensuite, on clique sur la fonction « *file server ressource* manager », enfin, on clique sur le bouton « *installer* ».Sous la nouvelle fenêtre, cliquez sur « *add features* », Patienter pour que l'installation prenne fin. En définitive, cliquez sur fermer (close). Cela est succinctement illustré dans les figures ci-dessous :

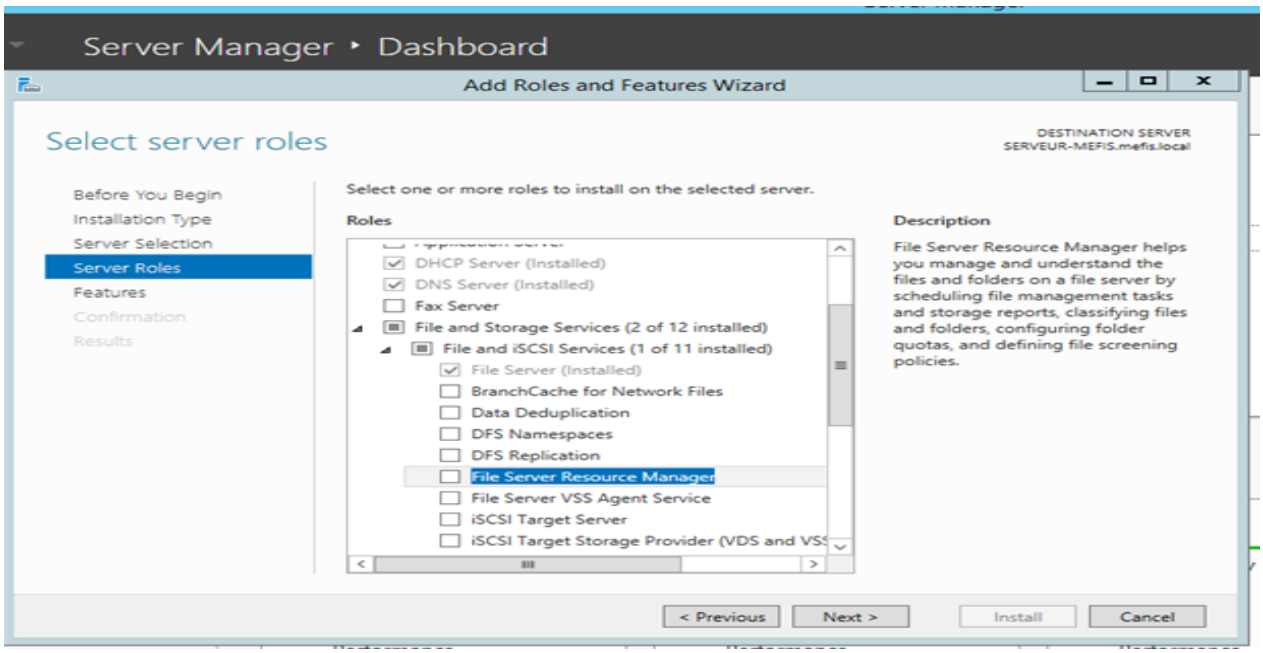

Figure 10. Interface de sélection du Rôle ou Fonctionnalités.

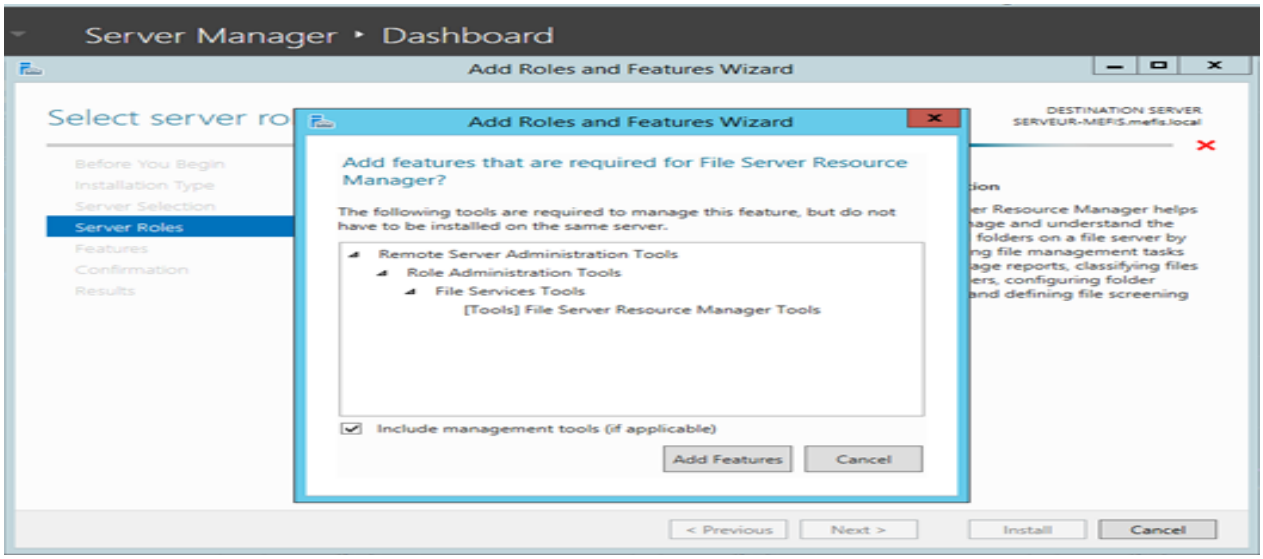

Figure 11. Interface de l'ajout de la Fonctionnalités.

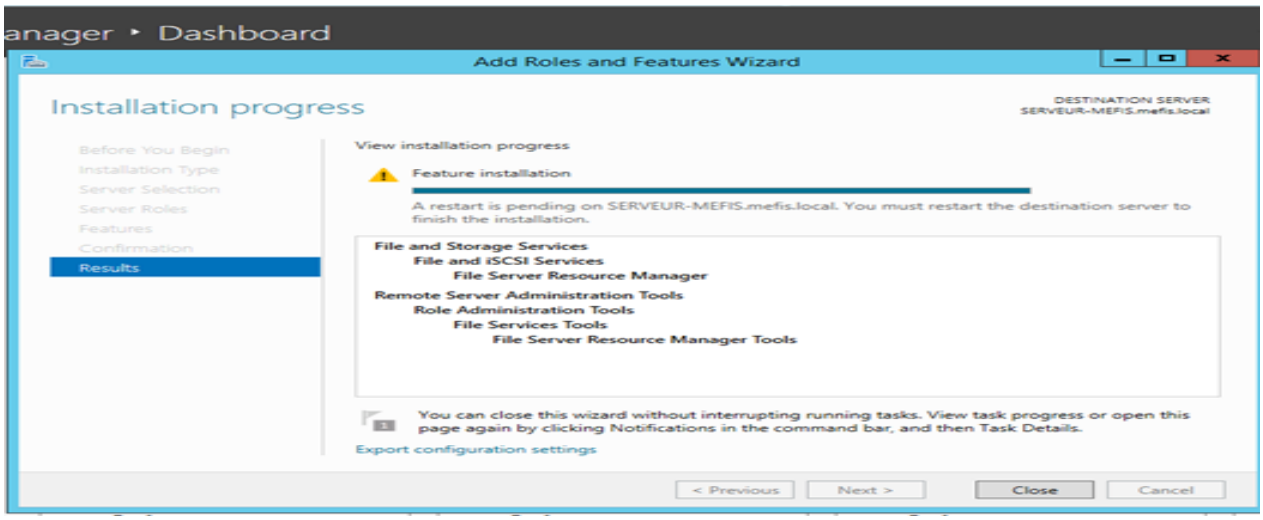

Figure 12. Interface de la fin de l'installation de la Fonctionnalité.

IV.3.1. Configuration de L'accès des utilisateurs aux fichiers

La configuration des utilisateurs permet de donner aux utilisateurs créés par l'administrateur le moyen d'accéder aux ressources du serveur quand il est connecté à un réseau à n'importe quel moment. Avant que l'utilisateur accède au serveur il doit se connecter à un réseau câblé si la machine cliente et les serveurs n'ont pas des pilotes wifi ou à un point d'accès si les deux machines ont les pilotes wifi ; pour notre cas nous avons utilisé un point d'accès. Après la connexion des machines à un réseau, nous avons donné à la machine cliente une adresse IP fixe pour que celle-ci accède au domaine du serveur, l'adresse IP qui est donné à la machine cliente est celle même du domaine :

1. Connexion de l'utilisateur au domaine

Au cours de notre configuration, nous avons créé le domaine appelé « *test.local* ». La machine étant connecté et ayant un IP fixe, Allez vers propriété du système, changer le paramètre du système, sur la boite dialogue qui s'affiche cliquer sur modifier, puis choisissez domaine et entrer le nom du domaine de votre serveur, en fin valider. Ce qui illustre la figure ci-dessous :

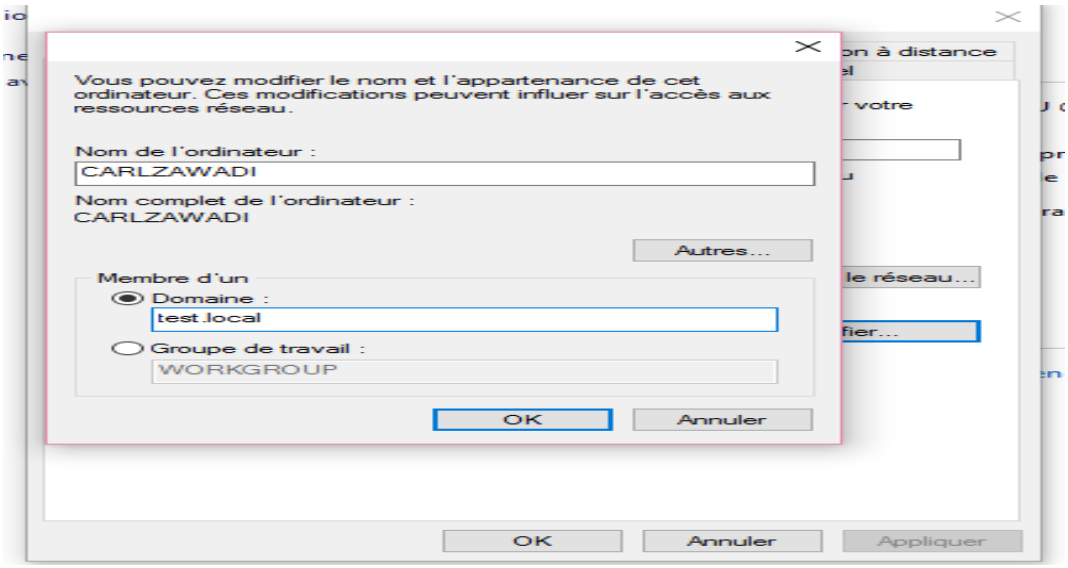

Figure 13. Connexion au Domaine.

La procédure de connexion continue, après avoir cliqué sur ok une fenêtre s'ouvre qui vous demande de taper le nom d'utilisateur et le mot de passe de l'administrateur du serveur.si les identités des d'administrateur sont validé un message de bienvenue s'affiche. Les figures ci-dessous nous l'expliquent davantage :

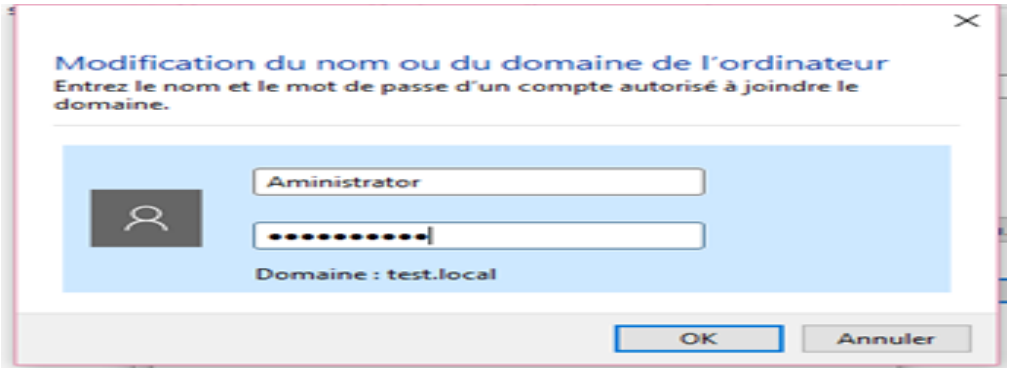

Figure 14. Interface d'administrateur.

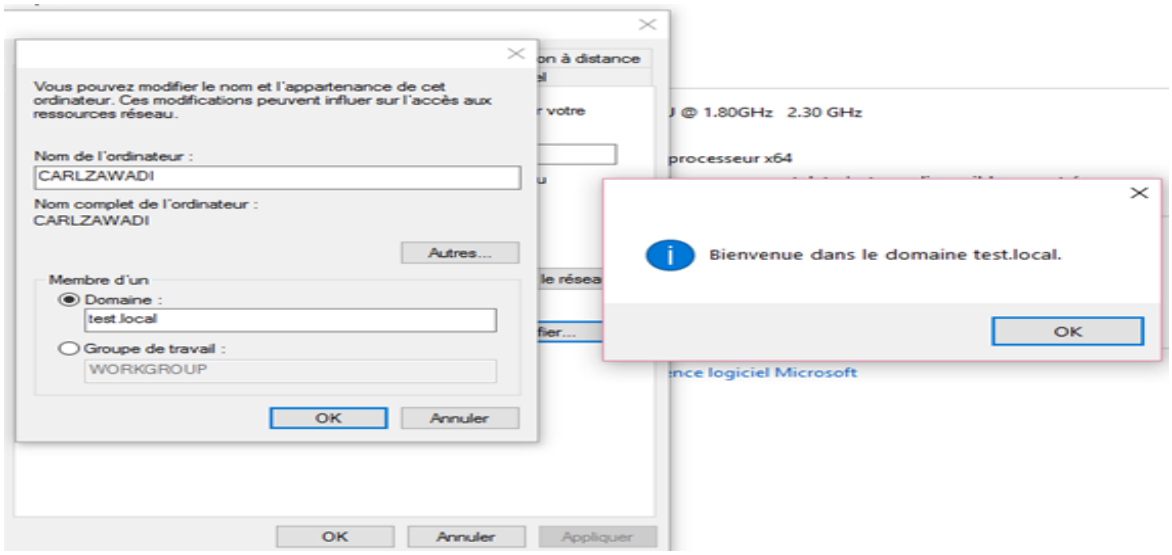

Figure 15. Message de bienvenue dans le Domaine.

Après le message de bienvenue le système vous demande de redémarrer la machine pour qu'il puisse prendre en charge l'utilisateur qui va se connecter. Grâce à son nom et son mot de passe. L'illustration ci-dessous :

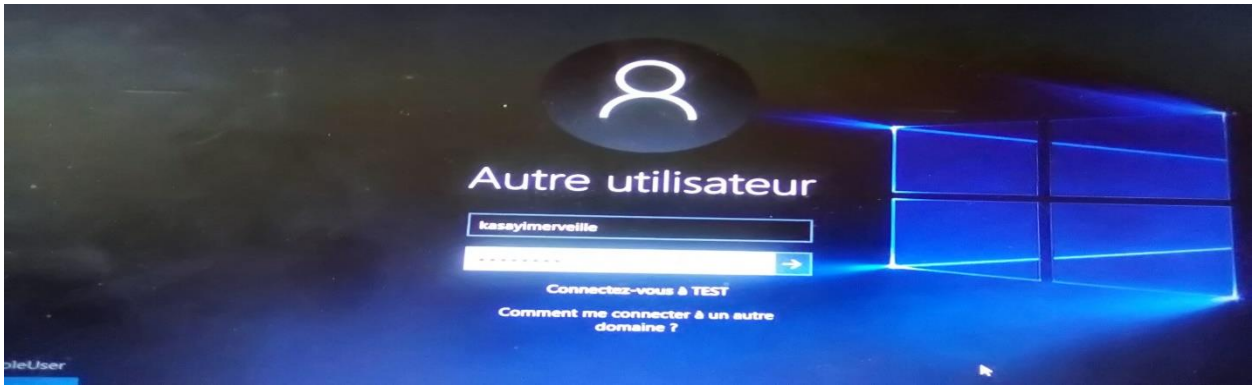

Figure 16. Interface Utilisateur.

2. Filtrage des fichiers

Dans notre réseau nous allons faire le filtrage par extensions qui consiste à bloquer certains fichiers qui ne sont pas autorisé dans ce dernier. Pour tester notre système nous avons connecté une machine sur notre serveur et nous avons interdit l'accès aux fichiers images et quand la machine cliente veut télécharger ce fichier (fichier image) le message suivant s'affiche :

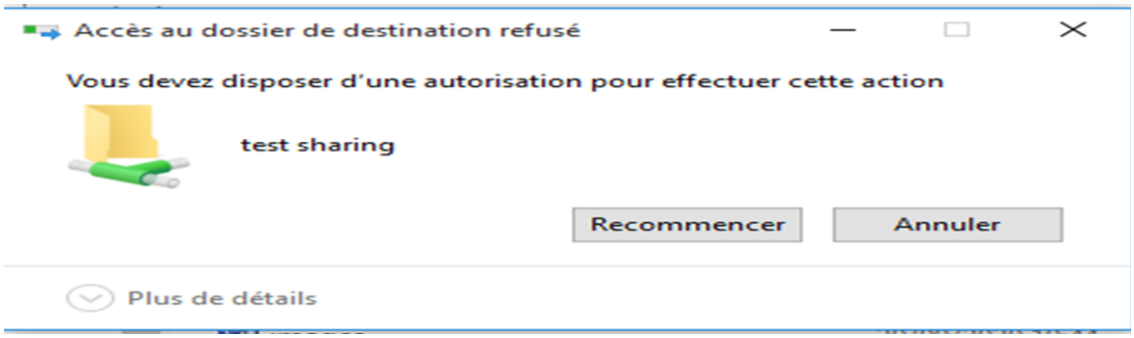

Figure 17. Message de Filtrage.

CONCLUSION

La communication électronique dans les entreprises modernes peut rencontrer plusieurs difficultés. Ces défis peuvent entraver l'efficacité de la communication et nuire à la collaboration et à la productivité des employés. C'est pour cela que la présente étude s'est fixé l'objectif primordial de déployer une solution de filtrage des fichiers sous Windows Server 2012 R2 pour offrir de nombreux avantages en termes de sécurité et de contrôle des données dans les systèmes de communication interne des entreprises contemporaines. En amont, Le déploiement d'un serveur de filtrage des fichiers permet de renforcer la sécurité du système de communication interne de l'entreprise en élucidant et en bloquant les fichiers malveillants ou non autorisés. Cela réduit le risque d'infection par des logiciels malveillants et protège les données sensibles. Une fois, déployez, cette solution offre un meilleur contrôle sur les types de fichiers qui peuvent être partagés et échangés à l'intérieur de l'entreprise. Ce qui permet aux administrateurs de définir des règles de filtrage spécifiques pour limiter les types de fichiers autorisés, les extensions potentiellement dangereuses et les tailles de fichiers.

Le déploiement d'un serveur de filtrage des fichiers est un outil essentiel pour lutter contre les fuites de données sensibles dans les systèmes de communication interne des entreprises. Elle permet de détecter et de prévenir les tentatives de transfert de fichiers confidentiels à l'extérieur de l'entreprise, en appliquant des règles de filtrage basées sur des critères tels que les étiquettes de classification des données ou les mots-clés spécifiques. En mettant en place cette solution, les entreprises peuvent présentement mieux se conformer aux réglementations en matière de protection des données, telles que le RGPD. Cela permet de garantir la confidentialité et l'intégrité des données, réduisant les risques de non-conformité et les sanctions associées. De

plus, elle offre des fonctionnalités de surveillance et de génération de rapports détaillés sur les activités de partage de fichiers. Cela permet aux administrateurs de suivre les activités des utilisateurs, de détecter les comportements suspects et de générer des rapports pour des audits de sécurité.

REFERENCES

[1]. ACISSI, « Sécurité informatique ethicalhaking, apprendre l'attaque pour mieux se défendre », Eni 2009,
[2]. ANIKAR M. Haseloff, « Les cybercafés et leur potentiel en tant qu'outils pour le développement de la communauté indienne », Université d'Ausbourg, 2010
[3]. Chantal MORELEY, « Management d'un projet système d'informations. Principes, techniques, mise en œuvre et outils », 6ème édition, Dunod, Paris, 2008.
[4]. EMMANUEL Chimi, « Administration des réseaux informatiques », Université virtuelle africaine, 2012
[5]. LABSHADOPI, « Livre vert sur les techniques des filtrages », Lab. Réseaux et Techniques, déc, 2011
[6]. PILIPPE latu, « Introduction à l'analyse avec wiresask », septembre 2014
[7]. SAADELI Nouria, OUARET Kahina, « Installation et configuration des services de Windows server 2012 R2Cas d'étude : Candia (Tchin-Lait) », mémoire inédit, Algérie 2017.
[8]. STEPHANE L, DOMINIQUE « Réseau, protocoles, Infrastructures et Services », Dunod 2013
[9]. YENDE R. Grevisse, « Administration des réseaux informatiques », Congo-Kinshasa. 2019.
[10]. YENDE R. Grevisse et al, "Operational approach to kernl system protection under Windows Server 2019 : Optimization, QoS and Performance", EJCSIT, Vol.11, No.2, pp.70-99, 2023.