

Université Mohammed Premier Ecole Supérieure de Technologie -Oujda-

03/05/2020



المدرسة العليا للتكنولوجيا
École Supérieure de Technologie
+212 524 80 000 | +212 524 84 418

Département Génie informatique

Filière : Administrateur de Système et Réseaux

Stage de Fin D'études :

La Sécurisation d'un Système Informatique

Réalisé par :

TOR Mohcine

RAHAL Yousra

Encadré par :

Mr. Ahmed Chelkha

Année Universitaire :

2019/2020

Remerciements

Nous tenons à remercier dans un premier temps, toute l'équipe pédagogique de l'Ecole Supérieure de Technologie -Oujda- et les intervenants professionnels responsables de la formation génie informatique.

Avant d'entamer ce rapport, nous profitons de l'occasion pour remercier tout d'abord Monsieur Mohamed EL BOUKHARI le chef de département de filière administration de système et réseau.

Notre Encadrant Monsieur Ahmed CHELKHA qui n'a pas cessé de nous encourager pendant la durée du projet, ainsi pour sa générosité en matière de formation et d'encadrement. Nous le remercions également pour l'aide et les conseils concernant les missions évoquées dans ce rapport, qu'il nous a apporté lors des différents suivis, et la confiance qu'il nous a témoigné.

Nous tenons à remercier nos professeurs de nous avoir incités à travailler en mettant à notre disposition leurs expériences et leurs compétences.

Nous tenons à exprimer enfin notre gratitude à tous les professeurs et toute personne qui ont participé de près ou de loin à l'élaboration de ce travail.

TABLE DE MATIERES

Remerciements	1
Introduction générale	3
Chapitre 1 : Sécurisation d'un Système Informatique :	4
1. Système informatique :	4
I. Introduction :	4
II. Définition :	4
2. Sécurité du système informatique :	4
I. Introduction :	4
II. Le principe de la sécurité de système informatique :.....	5
III. Etablissement d'un politique de sécurité :.....	5
IV. Les principes faillent de sécurité du système :.....	6
3. Les attaques informatiques :	7
I. Introduction :	7
II. Différentes Type des hackers :	8
III. Différentes classes d'une attaque :	9
IV. Les outils de piratage informatique Plus connue :	11
V. Les principes attaquent informatique actuelle :	15
Chapitre 2 : Etude théorique pour la sécurisation de système informatique :.....	18
1. Système de la société :.....	18
I. Description de système de la société :	18
II. Les recommandations de la société :	18
2. L'étude du système est les solutions proposées :	19
Chapitre 3 : Application pratique pour la sécurisation de système informatique :.....	26
1. Installation de système :	26
2. Installation d'un Active Directory Domain Services + DNS intégré :	27
3. Création des dossiers et les utilisateurs :	28
4. Configuration du dossier partagé :	29
5. Protéger le serveur de fichiers contre les ransomwares :	32
6. La haute disponibilité de service :	33
7. Installation et Configuration de pfSense :.....	38
8. Filtrage de sécurité des stratégies de groupe :	44
9. Sauvegarder les données à l'aide de Synology Drive et Windows server :	48
CONCLUSION.....	53
BIBLIOGRAPHIE	54

Introduction générale

Dans le cadre de notre formation, nous avons effectué un stage de fin d'étude au linge avec un ingénieur d'administration réseau et sécurité.

Ce stage nous a permis de passer de la théorie à la pratique, et nous a permis aussi de mettre en application nos connaissances acquises pendant cette formation et de maîtriser les mécanismes susceptibles de nous faciliter l'intégration dans le monde du travail pour le contact avec la vie professionnelle.

Dans le premier chapitre , nous avons représenté un peu de théorie sur tout ce qui concerne la sécurité d'un système informatique, des définitions et des notions de base ont été envisagées aussi les attaques et analyse actuelle dans le monde.

Dans le deuxième chapitre, nous présentons une étude théorique qui concerne brièvement la description et solution trouver pour sécuriser le système informatique.

Dans le troisièmes chapitre est le dernier représente le travail pratique pour sécuriser un système informatique.

Enfin, la conclusion générale et les perspectives de ce travail sont présentées, en résumant les principales contributions et en présentant nos futurs travaux de recherche.

Chapitre 1 : Sécurisation d'un Système Informatique :

1. Système informatique :

I. Introduction :

Les systèmes informatiques jouent un rôle de plus en plus important dans notre vie quotidienne. En une septantaine d'années les ordinateurs se sont rapidement améliorés et démocratisés. Aujourd'hui, tous les entreprises sont de plus en plus dépendantes des systèmes informatiques. Il est une composante essentielle de la gestion des informations, appelée « système d'information ». Alors l'importance de l'efficacité du système informatique est donc devenue un atout majeur dans la réussite d'une entreprise. Les dysfonctionnements et les risques sont nombreux et peuvent donc entraver le développement des organisations.

II. Définition :

Un système informatique est un ensemble de moyens informatiques et de télécommunications, matériels et logiciels, ayant pour finalité de collecter, traiter, stocker, acheminer et présenter des données.

A l'heure actuelle, l'informatique a pris une place prépondérante dans la gestion des organisations. L'équipement informatique des entreprises assurant la gestion des informations, les deux systèmes précédemment cités sont à présent étroitement liés.

L'innovation du système informatique doit être quasi permanente. Elle doit à la fois exploiter au mieux les nouvelles technologies et les nouveaux médias. Cependant, il faut éviter d'apporter d'incessants changements dans les modes de procédures souvent en cours d'acquisition par le personnel.

2. Sécurité du système informatique :

I. Introduction :

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de

maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet. Il est donc nécessaire de savoir comment nous pouvons protéger nos informations confidentielles.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

II. Le principe de la sécurité de système informatique :

La sécurité informatique est une discipline qui se veut de protéger l'intégrité et la confidentialité des informations stockées dans un système informatique.

La gestion de la sécurité d'un réseau ou d'un système informatique implique :

1. la mise en place des mécanismes de sécurité préventifs pour protéger les données et ressources du système ou réseau contre tout accès non autorisé ou abusif.
2. le déploiement des outils de sécurité pour détecter les attaques qui réussiraient à porter atteinte à la sécurité du réseau ou système malgré les mesures préventives.
3. la mise en place des mécanismes de réponse aux attaques détectées.

En effet, il est pratiquement impossible d'avoir un réseau complètement sûr et de le protéger contre toutes les attaques possibles. Malgré la mise en place de politiques préventives de sécurité, les réseaux et systèmes restent sujets à des attaques potentielles entreprises par des personnes qui réussissent à contourner ces mesures préventives par des comportements frauduleux.

III. Etablissement d'un politique de sécurité :

Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Elle est matérialisée dans

un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- 1-Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- 2-Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
- 3-Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
- 4-Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

IV. Les principes faillett de sécurité du système :

Toutes les entreprises, même les plus sécurisées, redoutent toujours les attaques des hackers à travers des failles informatiques. De plus, les attaques se passent souvent de manière inaperçue. En effet, 8 entreprises sur 10 qui subissent des piratages informatiques ne le savent pas. Voici 5 failles informatiques les plus courantes qui peuvent compromettre le système informatique des entreprises.

1-Failles au niveau des protocoles d'administration :

Pour ce type de faille, les négligences en matière de sécurité se trouvent au niveau des éléments actifs comme les switchs, les routeurs ou encore les imprimantes. Souvent, les mots de passe d'administration par défaut pour accéder à ces types d'équipement restent inchangés. Ce type de faille est souvent exploité par les hackers pour porter atteinte à l'entreprise.

2- Failles au niveau des bases de données :

Les bases de données constituent une cible privilégiée des pirates informatiques. Ce type de faille s'explique souvent par l'utilisation de mots de passe qui sont en fonction du nom du serveur. Certains administrateurs de bases de données usent de cette technique lorsqu'ils gèrent un grand nombre de serveurs, afin de mémoriser plus facilement les mots de passe.

Les hackers exploitent cette faille pour accéder aux fichiers de la base de données pour pouvoir ensuite obtenir d'autres comptes utilisateurs avec des

mots de passe faibles. Ces mots de passe faibles peuvent être facilement décryptés par la technique de cassage. Ces comptes piratés seront par la suite utilisés par le hacker pour poursuivre son attaque sur l'ensemble du réseau.

3- Failles au niveau du partage de fichiers :

La plupart des entreprises, pour ne pas dire toutes les entreprises, utilisent le partage de fichiers. Le plus souvent, la restriction est rarement préconisée. Pourtant le partage de fichiers non sécurisés représente une porte sans serrure pour les hackers et leur permettant d'obtenir des informations sensibles, voire confidentielles, de l'entreprise.

Pour les imprimantes les plus récentes par exemple, des failles permettant aux pirates informatiques de récupérer des données numérisées ou photocopiées dans l'entreprise existent, si aucune mesure de sécurité informatique adaptée n'a été prise en amont.

4- Failles au niveau de la gestion des droits :

Dans beaucoup d'entreprises, les restrictions d'accès sont parfois trop laxistes, et parfois même inexistantes. Des études menées par les experts en sécurité informatique ont déduit que 50% des menaces proviennent directement des employés de l'entreprise.

Non pas parce qu'ils sont mal intentionnés, mais souvent ils ne sont conscients des risques que représente leur laxisme en matière de **sécurité informatique**. Bref, ils constituent le maillon faible de la chaîne de sécurité informatique.

Par exemple, en permettant à un stagiaire d'utiliser la session de son encadreur au sein de la boîte. L'entreprise s'expose à des risques comme **le vol d'informations stratégiques ou confidentielles**.

5- Les vulnérabilités web :

Les vulnérabilités web représentent des risques non négligeables en matière de sécurité informatique. Ces vulnérabilités permettent d'avoir un premier accès au système et obtenir des informations. Par ordre de fréquence.

3. Les attaques informatiques :

I. Introduction :

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant des systèmes et généralement préjudiciables. Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques. Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives. Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Rassembler des informations personnelles sur un utilisateur.
- Récupérer des données bancaires.
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.).
- Troubler le bon fonctionnement d'un service.
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

II. Différentes Type des hackers :

Le terme « hacker » est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatiques aiment à penser qu'ils ont été attaqués par des pirates chevronnés ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour en exploiter les failles.

En réalité il existe de nombreux types d'attaquants catégorisés selon leur expérience et selon leurs motivations :

1. **White hat** : Est un hacker éthique ou un expert en sécurité informatique c'est celui qui réalise des tests d'intrusion et les audits de sécurité afin d'assurer la sécurité des systèmes informatiques d'une organisation ou d'une entreprise.
2. **Black hat** : Est un hacker mal intentionné. En plus de rechercher les failles de sécurité des systèmes informatiques, le black hacker développe des outils

(Cheval de Troie, ransomWare, etc) pour pouvoir gagner de l'argent en exploitant ces systèmes informatiques.

3. Grey hat : Un grey hat dans la communauté de la sécurité de l'information, et généralement de l'informatique, est un hacker qui agit parfois avec éthique, et parfois non. Il se situe entre hacker white hat et hacker black hat. Un hacker éthique est un professionnel qui applique ses connaissances dans la légalité et la moralité.

III. Différentes classes d'une attaque :

Malgré la diversité des attaques de sécurité, nous retiendrons quatre classifications possibles.

Première classification :

Un système informatique peut être attaqué :

- Soit par des utilisateurs internes, dans le but d'abuser de leurs droits et priviléges, on parlera alors **d'attaques internes**.
- Soit par des utilisateurs externes qui essayent d'accéder à des informations ou ressources de manière illégitime et non autorisée et dans ce cas on parlera **d'attaques externes**.

Deuxième classification :

C'est la classification la plus classique, elle regroupe quatre types d'attaques.

Ainsi une attaque peut porter atteinte à :

- La **confidentialité** Concept permettant de s'assurer que l'information ne peut être lue que par les personnes autorisées.
- L'**intégrité** est un ensemble de moyens et techniques permettant de restreindre la modification des données aux personnes autorisées.
- L'**authenticité** consistant à assurer que seules les personnes autorisées aient accès aux ressources.
- La **disponibilité**, permettant de maintenir le bon fonctionnement du système d'informatique. ?
- La **non réputation**, permettant de garantir qu'une transaction ne peut être niée.

Troisième classification :

Elle correspond à la classification de Stallings [Stallings 1995], qui identifie deux types d'attaques :

- Les **attaques passives**.
- Les **attaques actives**.

Les **attaques passives** regroupent les attaques portant atteinte à la confidentialité.

Il en existe deux types :

- La **lecture de contenus de messages** confidentiels : courrier électronique, fichier transféré.
- L'**analyse de trafic** pour déterminer la nature d'une communication : identité des "hosts" communiquant, fréquence et longueur des messages échangés.

Les attaques passives ne sont pas facilement détectables car elles n'impliquent aucune altération des informations.

Les **attaques actives** concernent celles qui entraînent une modification des données ou création de données incorrectes. Autrement dit, celles qui portent atteinte à l'intégrité, l'authenticité et la disponibilité. On retrouve alors quatre types d'attaques actives :

- **L'usurcation** : c'est lorsqu'une entité se fait passer pour une autre.
- **Le rejeu** : retransmission de messages capturés lors d'une communication, et cela à des fins illégitimes.
- **La modification de messages**.
- **Le déni de service**.

Quatrième classification :

Les attaques de sécurité peuvent également être classées en termes :

- **D'attaques réseaux** : leur but principal est d'empêcher les utilisateurs d'utiliser une connexion réseau, de rendre indisponible une machine ou un

service et de surveiller le trafic réseau dans le but de l'analyser et d'en récupérer des informations pertinentes.

- **D'attaques systèmes** : ce sont des attaques qui portent atteinte au système, comme par exemple effacer des fichiers critiques (tel que le fichier "password") ou modifier la page web d'un site dans le but de le discréditer ou tout simplement le ridiculiser.

IV. Les outils de piratage informatique Plus connue :

Il existe des dizaines d'outils de piratage publiés chaque jour, donc organiser tous ces programmes et logiciels est vraiment un défi.

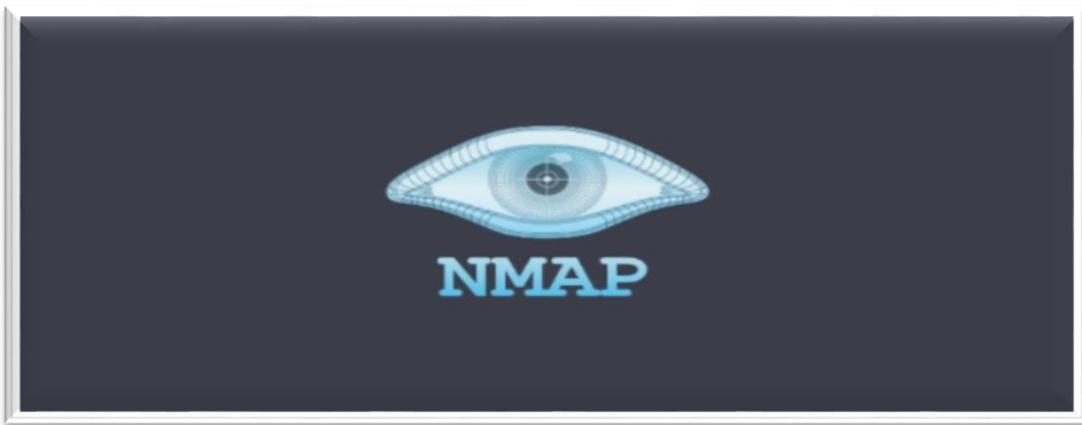
Nous avons regroupé certains des outils de test d'intrusion les plus populaires pour vous aider à comprendre le principe de piratage et de sécurité informatique. Vous trouverez certains des outils classiques qui semblent exister depuis toujours et de nouveaux outils qui ne sont peut-être pas connus.

1. Metasploit : Metasploit Framework est une plate-forme de test d'intrusion modulaire basée sur Ruby qui vous permet d'écrire, de tester et d'exécuter du code d'exploitation. Il contient une suite d'outils que vous pouvez utiliser pour tester les failles de sécurité, énumérer les réseaux, exécuter les attaques et échapper à la détection. À la base, Metasploit Framework est une collection d'outils couramment utilisés qui fournissent un environnement complet pour les tests de pénétration et le développement d'exploits. Il appartient à la société de sécurité **Rapid7** de Boston, dans le Massachusetts.

```
[*] Starting the Metasploit Framework console.../  
_____  
 \_o_ / \ M S F | \| *  
 \ \_ _WW|_|/  
 | | | | | |  
 =[ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0]]  
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post ]  
+ -- --=[ 356 payloads - 37 encoders - 8 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
msf >
```

Metasploit set disponible pour toutes les principales plates-formes, notamment Win, Linux et OS .Cet outil est l'un des outils de cybersécurité les plus populaires permettant d'identifier les vulnérabilités de différentes plates-formes.

2. Nmap : (Network Mapper) est un scanner de réseau gratuit et open source créé par Gordon Lyon (également connu sous son pseudonyme *Fyodor Vaskovich*). Il est utilisé pour découvrir des hôtes et des services sur un réseau_informatique en envoyant des paquets et en analysant les réponses. Il fournit un certain nombre de fonctionnalités pour sonder les réseaux informatiques, y compris la détection d'hôte et la détection de service et de système_d'exploitation . Ces fonctionnalités sont extensibles par des scripts qui fournissent une détection de service plus avancée, une détection de vulnérabilité, et d'autres fonctionnalités.



3. Wireshark : Autrefois connu sous le nom d'Ethereal, Wireshark est un "sniffer" ou analyseur de protocoles réseau et applicatif. C'est-à-dire qu'il va capturer des paquets IP transitant sur un réseau de manière transparente pour qu'ils soient ensuite analysés. Des filtres de capture peuvent être appliqués afin de recueillir des paquets correspondants à des besoins particuliers.



4. John the Ripper : John the Ripper, généralement appelé simplement, «John» est un outil de pentesting de piratage de mot de passe populaire qui est le plus couramment utilisé pour effectuer des attaques par dictionnaire. John the Ripper prend des échantillons de chaînes de texte à partir d'une liste contenant des mots populaires et complexes trouvés dans un dictionnaire ou de vrais mots de passe piratés auparavant, le chiffrant de la même manière que le mot de passe piraté, et comparer la sortie à la chaîne chiffrée.



5. Suite Burp : est une application Java, développée par *PortSwigger Ltd*, qui peut être utilisée pour la sécurisation ou effectuer des tests de pénétration sur les applications web. La suite est composée de différents outils comme un serveur proxy (Burp Proxy), robot d'indexation (Burp Spider), un outil d'intrusion (Burp Intruder), un scanner de vulnérabilités (Burp Scanner) et un répéteur HTTP (Burp Repeater).



6. Nessus : est un outil d'analyse de sécurité à distance, qui analyse un ordinateur et déclenche une alerte s'il découvre des vulnérabilités que des pirates malveillants pourraient utiliser pour accéder à n'importe quel ordinateur que vous avez connecté à un réseau. Il le fait en exécutant plus de 1200 vérifications sur un ordinateur donné, en testant pour voir si l'une de ces attaques pourrait être utilisée pour s'introduire dans l'ordinateur ou l'endommager.



7. SQLmap : sqlmap est un outil de test de pénétration open source qui automatise le processus de détection et d'exploitation des failles d'injection SQL et la prise en charge des serveurs de base de données. Il est livré avec un puissant moteur de détection, de nombreuses fonctionnalités de niche pour le testeur de pénétration ultime et une large gamme de commutateurs allant des empreintes digitales de la base de données, à la récupération des données de la base de données, à l'accès au système de fichiers sous-jacent et à l'exécution de commandes sur le système d'exploitation via out-connexions hors bande.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
caused by this program

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
(possible DBMS: 'MySQL')
```

8. Shodan :est un moteur de recherche qui permet à l'utilisateur de trouver des types spécifiques d'ordinateurs (webcams , routeurs , serveurs , etc.) connectés à Internet à l aide d'une variété de filtres. Certains l'ont également décrit comme un moteur de recherche de bannières de service , qui sont des métadonnées que le serveur renvoie au client. Il peut s'agir d'informations sur le logiciel serveur, les options prises en charge par le service, un message de bienvenue ou tout autre élément que le client peuvent découvrir avant d'interagir avec le serveur.



V. Les principes attaquent informatique actuelle :

Dans un monde où le progrès technologique avance à grande vitesse, où les gens, les entreprises, les organismes, les pays et même les objets sont de plus en plus connectés, les attaques informatiques sont de plus en plus fréquentes. La question de la **cybersécurité** se pose à tous les niveaux et tend à devenir un enjeu essentiel ces prochaines années.

Pour mieux se protéger, il est primordial de savoir à quoi s'attendre, et donc de connaître à minima les attaques informatiques les plus courantes. En voici une liste non-exhaustive :

a. Les attaques DDoS ou attaques par déni de service :

Les attaques par déni de service sont faites pour submerger les ressources d'un système pour qu'il ne puisse plus répondre aux demandes. Contrairement aux autres attaques qui visent à obtenir ou à faciliter l'accès à un système, l'attaque DDoS ne vise qu'à l'empêcher de fonctionner correctement. Cela ne procure pas d'avantages en soi à un pirate, si ce n'est la pure satisfaction personnelle. L'attaque par déni de service peut aussi avoir pour but de lancer un autre type d'attaque.

b. Les Man-in-the-Middle attaques ou MitM :

Les MitM sont un type d'attaque dont le principe est de s'insérer dans les communications entre un serveur et un client. Il en existe plusieurs : comme Le détournement de session, L'usurpation d'IP, Le replay.

C. Les logiciels malveillants ou malwares :

Un malware est un logiciel indésirable installé dans votre système sans votre consentement. Il en existe tous types, mais en voici quelques-uns :

- **Les macro-virus** : ils infectent des applications comme Microsoft Word ou Excel en s'attachant à la séquence d'initialisation de l'application.
- **Les infecteurs de fichiers** : ils s'attachent à des fichiers exécutables comme les .exe.
- **Les infecteurs de systèmes** : ils infectent les disques durs.
- **Les chevaux de Troie** : ils se cachent dans un programme utile pour ensuite se déployer.
- **Les vers** : contrairement aux virus qui s'attachent à un fichier hôte, les vers sont des programmes autonomes qui se propagent sur les réseaux et les ordinateurs.
- **Les ransomwares** : c'est un type de logiciel malveillant qui crypte les données d'un ordinateur et exige une rançon à la victime contre son déchiffrement.

d. Les attaques par mot de passe :

Trouver un mot de passe est souvent bien plus facile qu'il n'y paraît, et les pirates s'en donnent à cœur joie. Pour trouver un mot de passe, il suffit parfois simplement de fouiller un bureau, en surveillant la connexion pour obtenir un mot de passe non chiffré, en ayant recours à **l'ingénierie sociale** ou en devinant :

- **Par force brute** : deviner un mot de passe en entrant ce que les gens entrent le plus souvent : nom, prénom, passe-temps favori, dates de naissance des enfants, etc.

e. Injection SQL :

C'est un problème affectant les sites web exploitant des bases de données : le pirate exécute une requête SQL sur la base de données via les données entrantes du client au serveur.

f. Les attaques de Phishing :

Le phishing, c'est cette fameuse fenêtre qui surgit en vous disant que vous avez gagné un million d'euros, ou cet étrange email que vous recevez de votre banque, vous demandant de saisir votre identifiant... cette technique combine ingénierie sociale et stratagème technique vous incitant à télécharger par vous-même des malwares qui voleront vos informations personnelles et confidentielles comme vos numéros de carte de crédit.

g. Zéro Day :

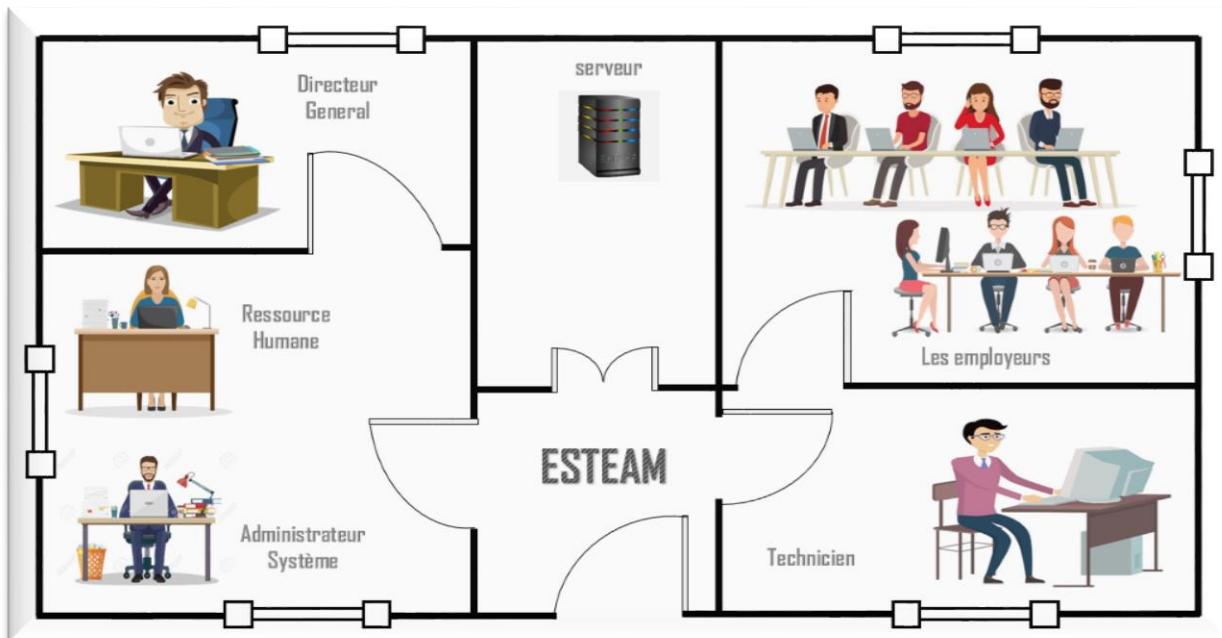
Une vulnérabilité zero-day fait référence à une faille de sécurité dans un logiciel inconnue du fabricant du logiciel ou des éditeurs d'antivirus. Ces failles de sécurité peuvent exister dans tout type de logiciel et sont particulièrement courantes dans les logiciels de navigation, les logiciels de système d'exploitation et les logiciels largement utilisés par des sociétés telles qu'Adobe, Oracle et Apple. Bien que la vulnérabilité ne soit pas connue du public, elle peut être découverte par des chercheurs ou des attaquants.

Chapitre 2 : Etude théorique pour la sécurisation de système informatique :

1. Système de la société :

I. Description de système de la société :

Une petite entreprise appelée ESTEM, nous recommandons de sécuriser leur système informatique, ce dernier peut être décrit comme une petite infrastructure informatique qui compte environ 20 d'ordinateurs de type Lenovo V520 Caractéristiques Processeur (Intel® Core™ i5-7400), Mémoire RAM (8 GA), Capacité disque dur (1TB), et aussi il y a un serveur dédié de type Lenovo ThinkSystem ST50, Processeur Intel Xeon E-2124G (Quad-Core 3.4 GHz / 4.5 GHz Turbo), et 8 Go de mémoire DDR4, sans oublier un système d'alarme qui compte environ de 12 camera IP de (G2EP) et un ADSL de débit moyen de 12 Mb/s.



Les systèmes d'exploitation installés sur les postes clients sont de la plate-forme Microsoft, plus précisément Windows 7.

II. Les recommandations de la société :

Parmi les recommandations qui nous aurons donné par la société sont listé comme suivante :

- A. La haute disponibilité (d'assurer et de garantir le bon fonctionnement de système et des services ou applications proposées et ce 24h/24 et 7j/7).
- B. Chaque poste ou bien équipement individuel dans ce système doit être sécurisé.
- C. Sécurisation des ressources.
- D. La sauvegarde informatique pour protéger les données détenues dans système d'informatique.
- E. Chaque accès distance doit être aussi sécuriser (audit).
- F. Besoin d'un firewall physique pour contrôler et sécuriser les accès interne et externe de l'entreprise.

2. L'étude du système est les solutions proposées :

La mise en place d'un système informatique de gestion de données et nécessite une étude détaillée. À partir de cette étude que nous avons réalisée parmi les solutions qui nous avons proposées sont :

1) La Haute disponibilité :

Pour garantir la haute disponibilité on va suivre la démarche suivante :

- On a choisi un onduleur (Eaton Ellipse ECO 650 USB) pour protéger vos équipements sensibles aux surtensions et aux coupures électriques de chaque poste. Et un stabilisateur de tension de 220 V est un appareil capable de répondre aux changements dans le niveau de tension.
- Besoin d'un autre serveur slave, une fois le serveur master tombe en panne le serveur slave prend sa place.
- A côté de performante on va faire une migration d'ADSL (12 Mb/s) vers une fibre optique de 100 Mb/s pour éviter le conflit et surcharge de la bande passante.
- Acheter d'une adresse IP fixe ou serveur.

2) Sécurisation de chaque poste de travail :

Pour rendre les postes de travail sécuriser, il y a des règles qu'on doit adoptées et respectées sont :

- L'installation de la dernière version 20.04 de Windows 10.
- Installation d'un antivirus (Kaspersky).
- Mise à jour des logiciels dans chaque poste.
- Désactivation des ports USB et Lecteur CD, parce que c'est l'un des moyens de transmission les plus courants du virus.

- Désactiver le protocole de partage de fichiers réseau SMB1 (Server Message Block) sur chaque poste a des raisons de sécurité. Il existe d'autre version : version 2 (SMB2) et version 3 (SMB3).

3) Sauvegarde les informations et les données :

L'objectif est de préserver toutes les données de l'entreprise, et garantir la pérennité des données en rendant possible la récupération des informations indispensables.

On a appliqué deux stratégies de sauvegarde online et offline :

La stratégie Online (planifié) :

- Le matériel choisie : NAS ds918+ (network attached storage)
- Les programmes choisie : synology drive et sauvegarde Windows Server
- Les méthodes choisies : complète (hebdomadaire), différentielle (journalière) et la synchronisation en temps réel.

Alors le serveur NAS est toujours connecté au système informatique.

La stratégie offline (manuelle) :

- Le matériel choisie : disque dur externe (SSD 2TB)
- Les programmes choisie : USBcopy et sauvegarde de windows server
- Les méthodes choisies : complète (hebdomadaire), différentielle (journalière).

Alors le disque dur Externe connecter au système informatique au temps de la sauvegarde seulement.

Pour la sauvegarde des informations, il existe deux types de sauvegarde, le hardware et le software :

- On a choisi comme hardware un Synology NAS en tant que serveur hôte et installer Synology Drive Server qui fournit la synchronisation de fichiers et le service de sauvegarde.
- Comme software on a choisi la Sauvegarde Windows, sauvegarde tous les dossiers sélectionnés uniquement lors de la première exécution (sauvegarde complète), puis sauvegarde uniquement les fichiers nouveaux ou modifiés depuis la dernière sauvegarde (sauvegarde incrémentielle) lors des sauvegardes suivantes.

4) Sécuriser l'entreprise avec le firewall pfSense :

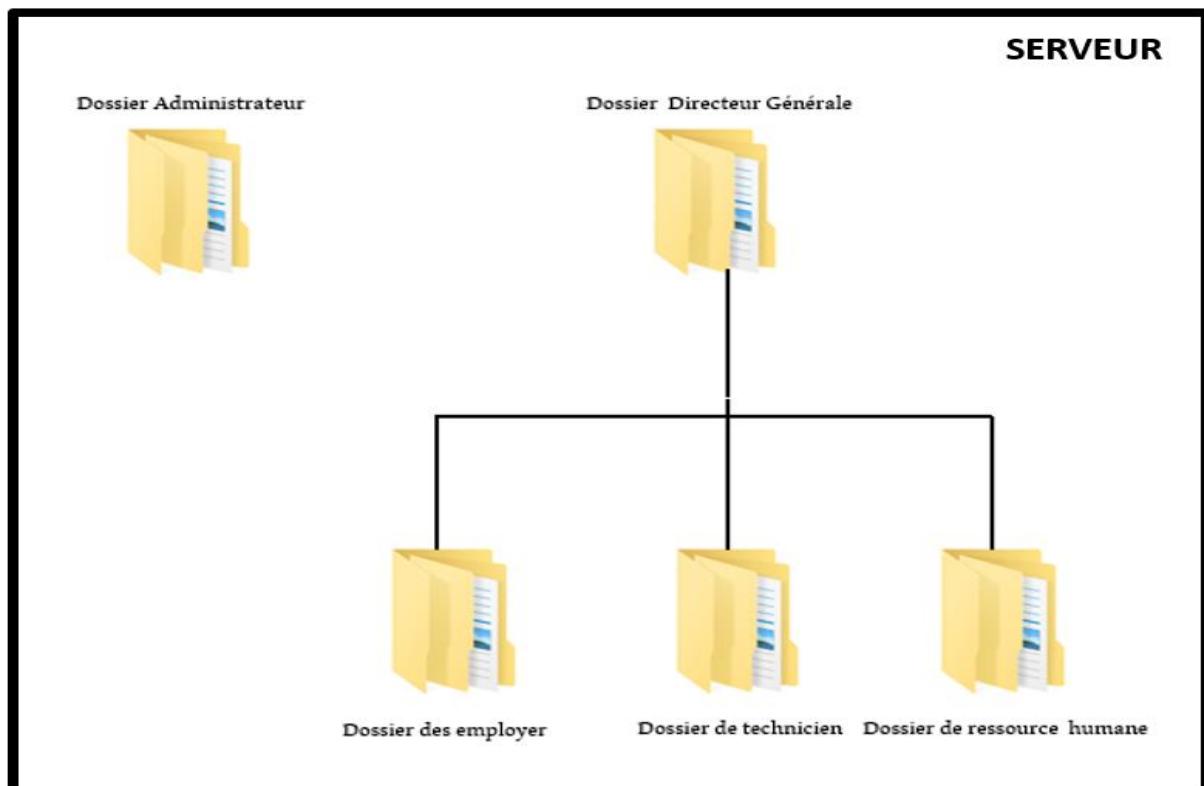
pfSense est un pare feu, puissant, et open source, alors on a choisi pfSense à cause de ses avantages et ses fonctionnalité :

- Il est très peu gourmand en termes de ressources.
- Plusieurs services/fonctionnalités, permettant de sécuriser au mieux notre réseau (Règles, Proxy...).
- pfSense peut être utilisé comme serveur DHCP ou relai DHCP.
- Dispose le filtrage par IP source et destination, port source et destination des protocoles TCP et UDP.
- Superviser son réseau (Monitoring), permet d'avoir de manière visuelle l'ensemble des activités du parc informatique.

5) Sécurisation des ressources :

Après l'analyse du système, on a trouvé que tous les utilisateurs ont même niveau du droits (contrôle total), alors ensuite nous avons créé des groupes avec leurs types, et pour chaque groupe nous avons spécifié leurs droits d'accès.

Voilà le Schéma des dossiers de la société :



GROUPES	TYPE	LES DROITS
G1	Niveau 1	- Lecture (dossier spécifié)
G2	Niveau 2	- Lecture - Ecriture (dossier spécifié)
G3	Niveau 3	- Lecture - Ecriture (tous les dossiers de travail)
G4	Niveau 4	- Lecture - Ecriture - exécution (dossier technique)
G5	Niveau 5	- Control total

- L'audit de fichiers peut fournir des détails sur les comptes utilisateurs ayant pris des mesures pour accéder aux données protégées, et définir le type d'autorisation et enregistrer les tentatives d'accès effectuées ou les échecs de connexion dans le journal de sécurité.

Pour effectuer cette procédure, nous devons être connecté en tant que membre du groupe d'administrateurs intégrés ou disposer des droits de gestion d'audit et de journal de sécurité, et aussi on peut utiliser d'autre utile comme :

- TCPView est un programme Windows qui vous montrera des listes détaillées de tous les points de terminaison TCP et UDP sur votre système, y compris les adresses locales et distantes et l'état des connexions TCP.

```

TCPView v3.01 - TCP/UDP endpoint viewer
Copyright (C) 1998-2010 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

[TCP] TeamViewer_Service.exe
    PID:      5724
    State:   ESTABLISHED
    Local:   DESKTOP-404QC0I
    Remote:  localhost
[TCP] TeamViewer_Service.exe
    PID:      5724
    State:   ESTABLISHED
    Local:   DESKTOP-404QC0I
    Remote:  localhost
[TCP] TeamViewer_Service.exe
    PID:      5724
    State:   ESTABLISHED
    Local:   DESKTOP-404QC0I
    Remote:  localhost
[TCP] TeamViewer.exe
    PID:      2836
    State:   ESTABLISHED
    Local:   DESKTOP-404QC0I
    Remote:  localhost

```

- LastActivityView est un outil pour le système d'exploitation Windows qui collecte des informations à partir de diverses sources sur un système en cours d'exécution et affiche un journal des actions effectuées par l'utilisateur et des événements survenus sur cet ordinateur.

Action	Time	Description	Filename	Full Path	More Info
Run .EXE file	13/06/2020 23:2...	OSK.EXE	C:\WINDOWS\SYSTEM32\OSK.EXE	Microsof	
Run .EXE file	13/06/2020 23:2...	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSENT.EXE	Microsof	
Run .EXE file	13/06/2020 23:2...	sethc.exe	C:\Windows\System32\sethc.exe	Microsof	
Run .EXE file	13/06/2020 23:2...	AtBroker.exe	C:\Windows\System32\AtBroker.exe	Microsof	
Run .EXE file	13/06/2020 23:2...	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSENT.EXE	Microsof	
Run .EXE file	13/06/2020 23:2...	dllhost.exe	C:\Windows\SysWOW64\dllhost.exe	Microsof	
Run .EXE file	13/06/2020 23:2...	WinRAR.exe	C:\PROGRAM FILES (X86)\WinRAR\WinRAR...	Alexande	D:\
View Folder in Expl...	13/06/2020 23:2...				
Run .EXE file	13/06/2020 23:2...	chrome.exe	C:\PROGRAM FILES (X86)\Google\Chrome\...	Google L	
Run .EXE file	13/06/2020 23:2...	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsof	
Run .EXE file	13/06/2020 23:2...	SEARCHPROTOCOLHOS...	C:\Windows\System32\SEARCHPROTOCOL...	Microsof	
Run .EXE file	13/06/2020 23:2...	chrome.exe	C:\PROGRAM FILES (X86)\Google\Chrome\...	Google L	
Run .EXE file	13/06/2020 23:2...	AUDIODG.EXE	C:\WINDOWS\SYSTEM32\AUDIODG.EXE	Microsof	
Run .EXE file	13/06/2020 23:2...	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsof	
Run .EXE file	13/06/2020 23:2...	SEARCHPROTOCOLHOS...	C:\Windows\System32\SEARCHPROTOCOL...	Microsof	
Open file or folder	13/06/2020 23:2...	Stage WinServer	D:\Stage WinServer		
Open file or folder	13/06/2020 23:2...	tcp.PNG	D:\Stage WinServer\tcp.PNG		

4250 item(s) NirSoft Freeware. <http://www.nirsoft.net>

- FullEventLogView est un outil simple pour Windows 10/8/7 / Vista qui affiche dans un tableau les détails de tous les événements des journaux d'événements de Windows. Il vous permet également d'exporter la liste des événements vers un fichier texte / csv / délimité par des tabulations / html / xml à partir de l'interface graphique et de la ligne de commande.

The screenshot shows a software interface titled "FullEventLogView". The menu bar includes "File", "Edit", "View", "Options", and "Help". The main window displays a table of event logs with columns: "Event Time", "Record ID", "Event ID", "Level", "Channel", "Provider", and "Description". The log entries are numerous, mostly from June 13, 2020, at 18:32:00, showing various system and application events such as ClipSVC stopping, Cortana and ZuneVideo processes running, and Microsoft Office Hub activity.

Event Time	Record ID	Event ID	Level	Channel	Provider	Description
13/06/2020 ...	99299	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	31088	102	Information	Microsoft-Client-Licensi...	Microsoft-Client-Licensi...	Le service ClipSVC s'est arrêté.
13/06/2020 ...	99300	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.Windows.Cortana_cw5n1hz
13/06/2020 ...	99301	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.ZuneVideo_8wekyb3d8bbv
13/06/2020 ...	99302	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99303	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.People_8wekyb3d8bbwe e:
13/06/2020 ...	99304	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.Windows.Cortana_cw5n1hz
13/06/2020 ...	99305	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.ZuneVideo_8wekyb3d8bbv
13/06/2020 ...	99306	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99307	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.People_8wekyb3d8bbwe e:
13/06/2020 ...	31089	100	Information	Microsoft-Client-Licensi...	Microsoft-Client-Licensi...	Le service ClipSVC est en cours de dé
13/06/2020 ...	31090	101	Information	Microsoft-Client-Licensi...	Microsoft-Client-Licensi...	Le service ClipSVC est en cours d'exé
13/06/2020 ...	58745	16	Information	System	Microsoft-Windows-Ker...	L'historique des accès à la ruche \??
13/06/2020 ...	99308	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99309	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.MicrosoftOfficeHub_8weky
13/06/2020 ...	99310	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99311	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.MicrosoftOfficeHub_8weky
13/06/2020 ...	33296	210	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Création du conteneur Desktop App
13/06/2020 ...	33297	211	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Ajout du processus 11568 au contene
13/06/2020 ...	33298	201	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Création du processus 11568 pour l'a
13/06/2020 ...	33299	217	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Destruction du conteneur Desktop Ap
13/06/2020 ...	99312	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99313	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99314	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99315	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99316	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	microsoft.windowscommunicationsa
13/06/2020 ...	99317	325	Information	Microsoft-Windows-Ap...	Microsoft-Windows-Ap...	Microsoft.Windows.Photos_8wekyb3c v

6) Sécurisation de l'accès distance :

Pour l'accès à distance, on a choisi le protocole RDP qui nécessite une adresse IP fixe, et on a baser sur un exemple réel d'un serveur qui est attaqué par une attaque brute force. Mais ils ont utilisé un anti-virus Kaspersky qui contient une option prévention des intrusions qui empêche l'exécution des actions dangereuses pour le système et il assure aussi le contrôle de l'accès aux ressources du système d'exploitation et aux données personnelles.

The screenshot shows the "Gestionnaire de serveur" (Server Manager) interface. The left sidebar shows "Tableau de bord" with links like "Serveur local", "Tous les serveurs", "AD DS", "DNS", and "Services de fichiers et d...". The main pane is titled "Rôles et groupes de rôles" and lists "AD DS" and "Services de stockage". A "Rapports détaillés" (Detailed Reports) window is open, showing a log of network attacks. The log entries are as follows:

- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:42
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.
- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:39
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.
- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:37
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.
- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:34
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.
- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:32
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.
- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:29
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.
- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:27
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.
- L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée. (Blocked) - 18:25
Tcp contre 45.141.84.28 sur le port 3389
L'ordinateur à l'origine de l'attaque a été bloqué.

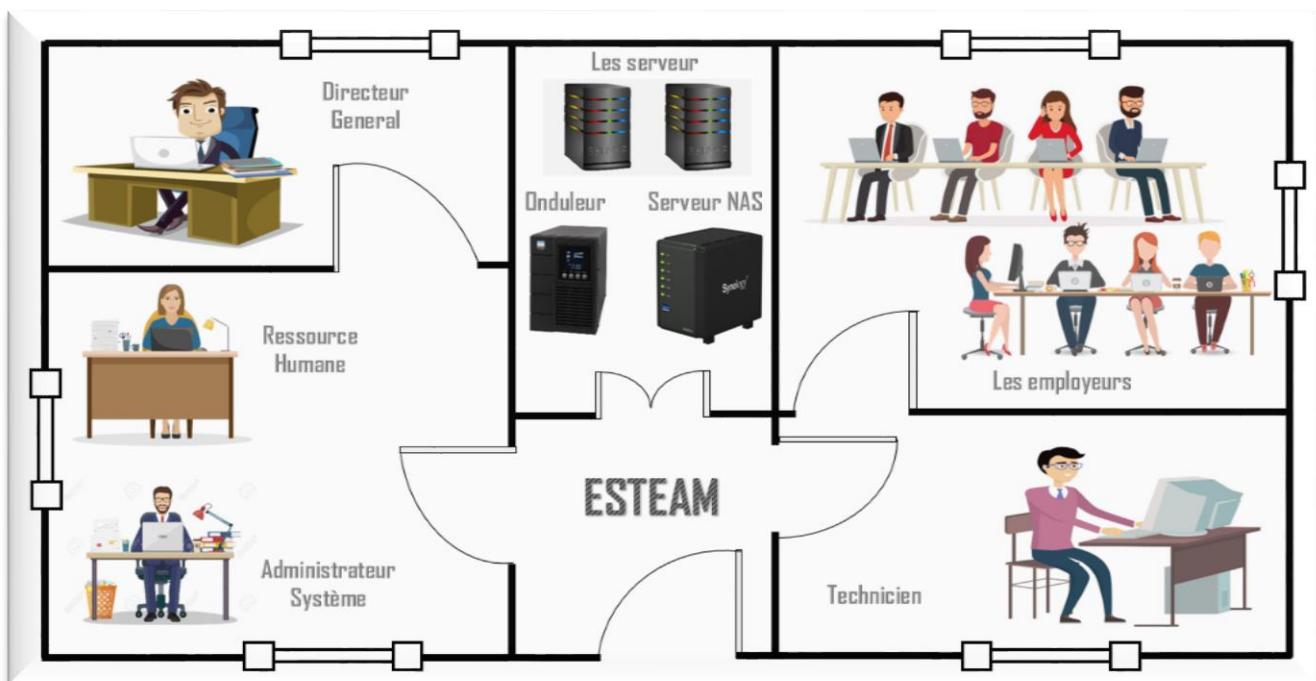
The right side of the window shows a summary of the last attack: "L'attaque réseau BruteForce.Generic.Rdp.d a été bloquée." (The network attack BruteForce.Generic.Rdp.d was blocked). It details the protocol (Tcp), the source IP (45.141.84.28), and the date and time (Aujourd'hui, 05/06/2020 18:42).

Exemple d'une attaque brute force sur un serveur d'entreprise ciblant le protocole RDP

Voilà les mesures préventives que l'on peut mettre en place, pour limiter les attaques par force brute.

- Le port d'écoute par défaut du RDP est le 3389. Il peut être dangereux de garder ce port, car il est connu et souvent scanné sur le web par des mains malveillantes voulant s'introduire dans votre système. Donc en droit Changez le port d'écoute par défaut en entrant un numéro au choix qui, de préférence.
- Changer le nom part défaut de serveur (Administrateur).
- Limiter les utilisateurs autorisés à se connecter via RDP : Si certains comptes utilisateurs sont nécessaires pour le bon fonctionnement du serveur sans jamais nécessiter de connexion Bureau à Distance (RDP) alors le réglage ci-dessous permettra de limiter aux seuls utilisateurs souhaités.
- Activer l'option de prévention d'instruction sur Antivirus Kaspersky.
- Un mot de passe fort pour réduire le risque de succès d'une attaque par force brute, il faut d'employer des mots de passe forts avec tous les types de caractères : majuscules, minuscules, les chiffres...
- Désactiver le port par défaut dans le pare-feu et activer le nouveau port choisir.
- Limiter le temps d'accès.
- Limiter le nombre de fois d'accès au serveur (On va spécifier que les utilisateurs a le droit d'autre leur mode de passe 3 fois).

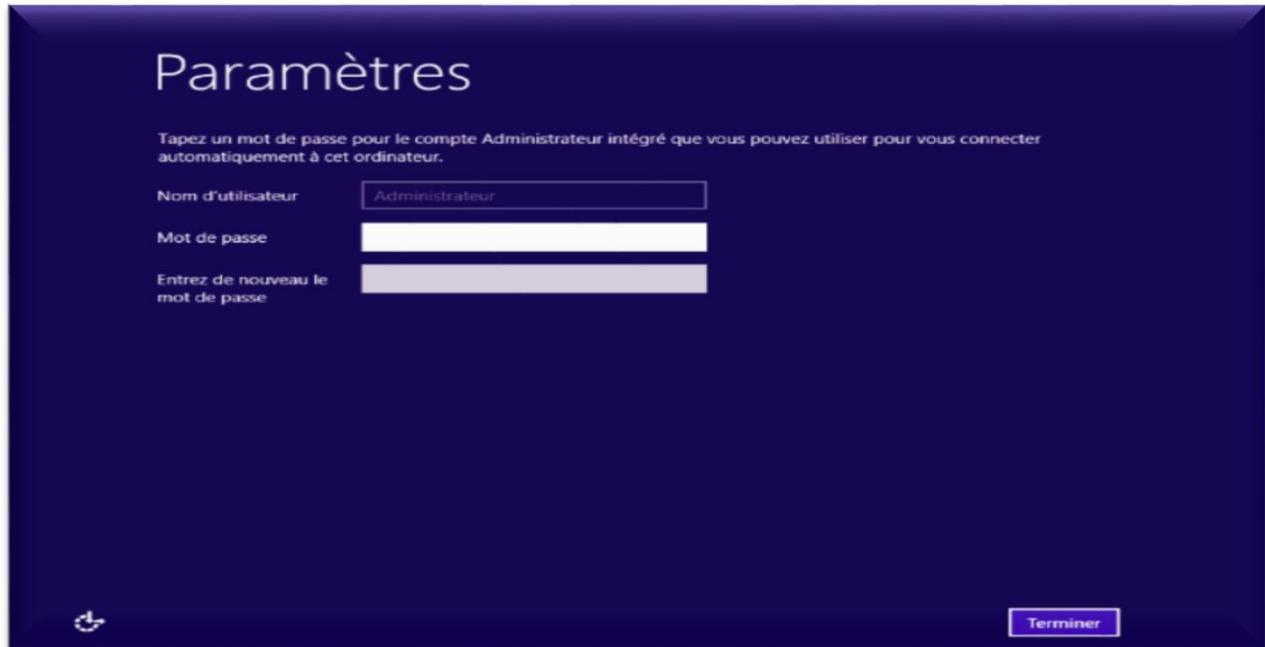
Voilà le schéma final de l'entreprise avec le critère de sécurité proposé :



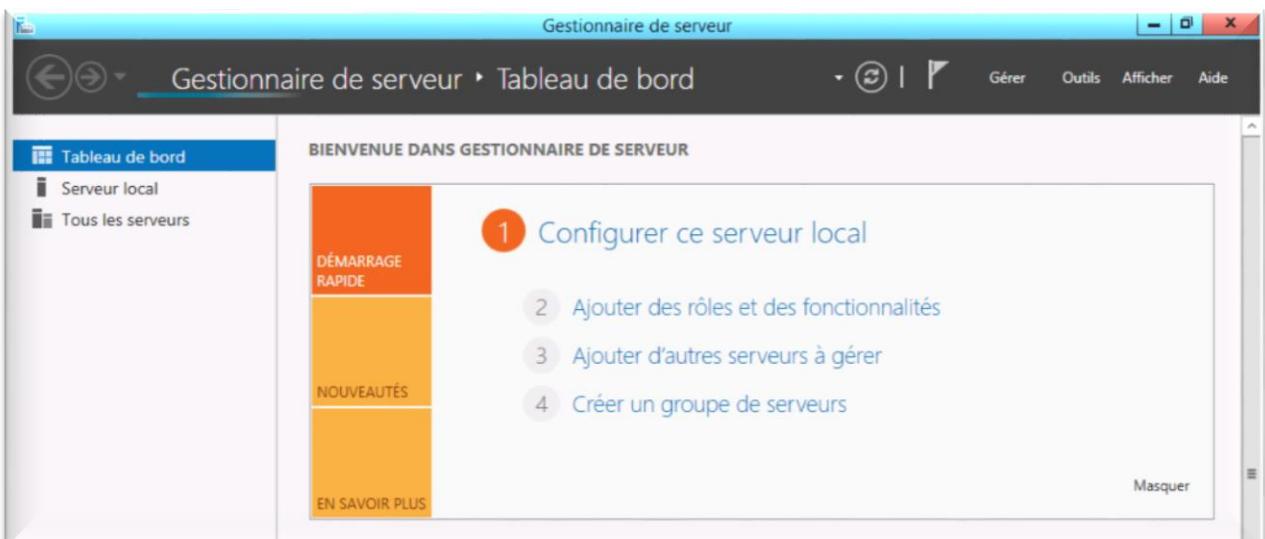
Chapitre 3 : Application pratique pour la sécurisation de système informatique :

1. Installation de système :

Après l'installation du système, nous devons configurer les paramètres du compte Administrateur. Nous avons à définir uniquement le mot de passe (le compte administrateur portera obligatoirement le nom « Administrateur »).

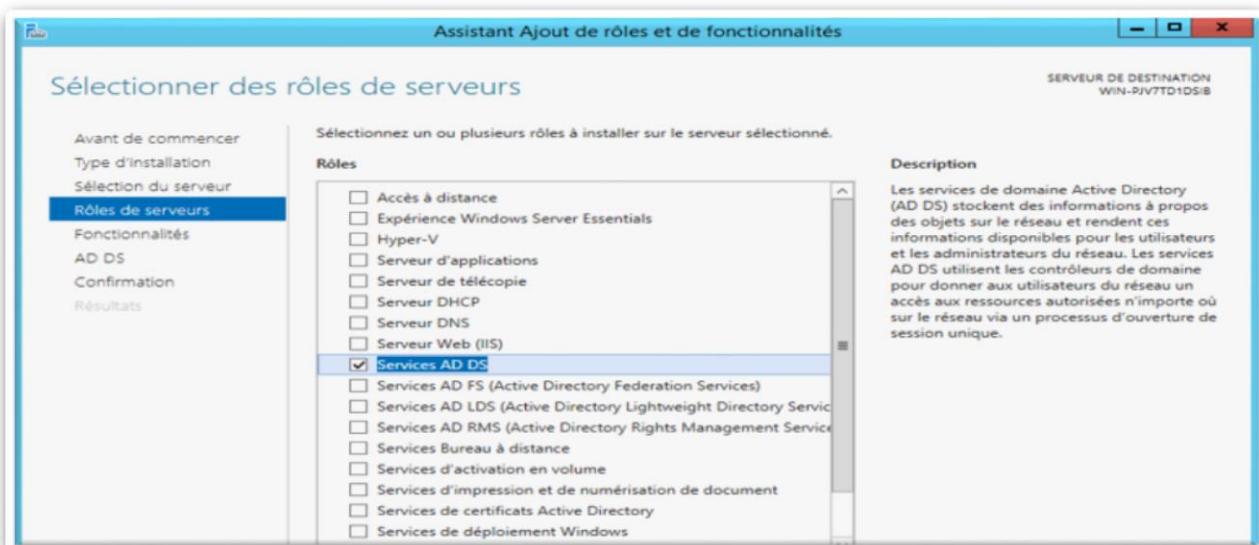


Une fois connecté, nous accédons au compte Administrateur du serveur sur lequel se trouve le « Gestionnaire de serveur ». C'est à partir de cette fenêtre que nous pourrons gérer tous les droits et les fonctionnalités du serveur.

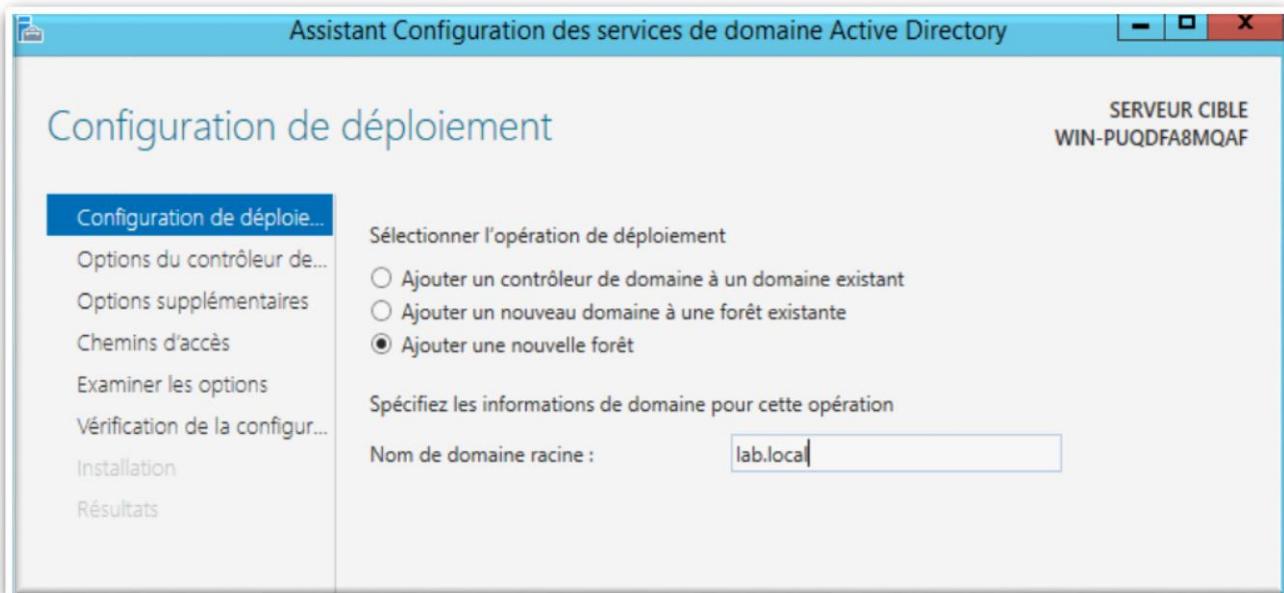


2. Installation d'un Active Directory Domain Services + DNS intégré :

Nous allons installer le rôle Active Directory en définissant ce serveur en tant que « Contrôleur de domaine ». Pour ce faire, il faudra cliquer sur « Gérer » puis sur « Ajouter des rôles et fonctionnalités », en suite une fenêtre va s'ouvrir « Assistant Ajout de rôles et de fonctionnalités », c'est à partir de cette fenêtre que nous allons effectuer toutes les modifications qui vont suivre.



Sélectionner le niveau fonctionnel de la forêt, ainsi que du domaine. On vient tout juste de créer un nouveau contrôleur de domaine et une nouvelle forêt.



Une vérification système est effectuée, il suffit de cliquer sur « Installer ». L'installation se lancera et le serveur redémarrera automatiquement.



Après, il suffit de rejoindre tous les utilisateurs au Domaine.

3. Création des dossiers et les utilisateurs :

En arrivant sur la console, on va développer l'arborescence de notre domaine et organisation notre travail on va cliquer sur le domaine lab.local, puis on va créer des unités d'organisation.

Nom	Type	Description
Administrateur System	Unité d'organisme	
Builtin	builtinDomain	
Computers	Conteneur	Default container for up...
Directeur General	Unité d'organisme	
Domain Controllers	Unité d'organisme	Default container for do...
Employer	Unité d'organisme	
ForeignSecurityPrincipals	Conteneur	Default container for sec...
Managed Service Accounts	Conteneur	Default container for ma...
Ressources Humaines	Unité d'organisme	
Technicien	Unité d'organisme	
Users	Conteneur	Default container for up...

Après, sur chaque unité d'organisation on va créer des utilisateurs associé à ce dernier :

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a tree view lists organizational units: 'Utilisateurs et ordinateurs Active', 'Requêtes enregistrées', 'lab.local', 'Administrateur System', 'Builtin', 'Computers', 'Directeur General', 'Domain Controllers', 'Employer' (which is highlighted with a red box), 'ForeignSecurityPrincipal', 'Managed Service Account', 'Ressources Humaines' (highlighted with a red box), 'Technicien' (highlighted with a red box), and 'Users'. On the right, a table displays user information:

Nom	Type	Description
oussama ma...	Utilisateur	
wafae aissaoui	Utilisateur	
yassine mali	Utilisateur	
yousra belh...	Utilisateur	
youssef sma...	Utilisateur	

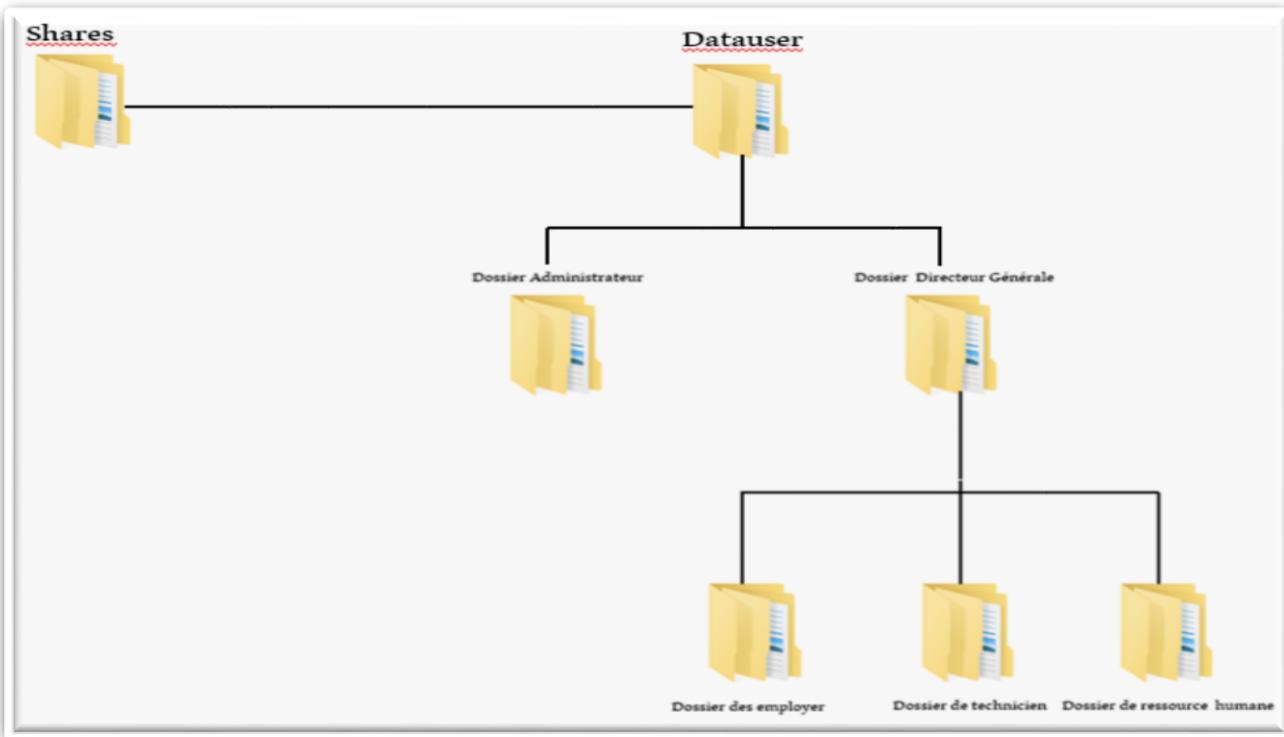
4. Configuration du dossier partagé :

Il existe différentes façons de partager un dossier dans Server 2012. Le moyen le plus efficace consiste à utiliser le Gestionnaire de serveur. Ici, je vais configurer un dossier partagé à partir du contrôleur de domaine nommé Serveur Master.

The screenshot shows the Windows Server Manager interface. The left sidebar has icons for Servers, Volumes, Disks, Storage Pools, **Partages** (which is selected and highlighted with a blue background), iSCSI, and Work Folders. The main pane is titled 'RESSOURCES PARTAGÉES' and shows 'Tous les partages | 16 au total'. It includes a search bar and filters for 'Partager', 'Chemin d'accès local', 'Protocole', and 'Type de disponibilité'. A table lists 16 shared resources, with the first two rows highlighted with a red box:

Partager	Chemin d'accès local	Protocole	Type de disponibilité
AS	C:\Shares\Datauser\AS	SMB	Non-cluster
DG	C:\Shares\Datauser\DG	SMB	Non-cluster

Nous souhaitons partager un dossier nommé Shares ce dernier contient d'autre dossier :



Nous sommes maintenant invités à indiquer l'emplacement de partage du dossier que nous souhaitons partager. Nous choisissons l'emplacement personnalisé C:\Shares.

Sélectionner un profil

Emplacement du partage

Nom de partage

Autres paramètres

Autorisations

Confirmation

Résultats

Serveur :

Nom du serveur	Statut	Rôle du cluster	Noeud propriétaire
ServeurMaster	En ligne	Non-cluster	

Emplacement du partage :

Sélectionner par volume :

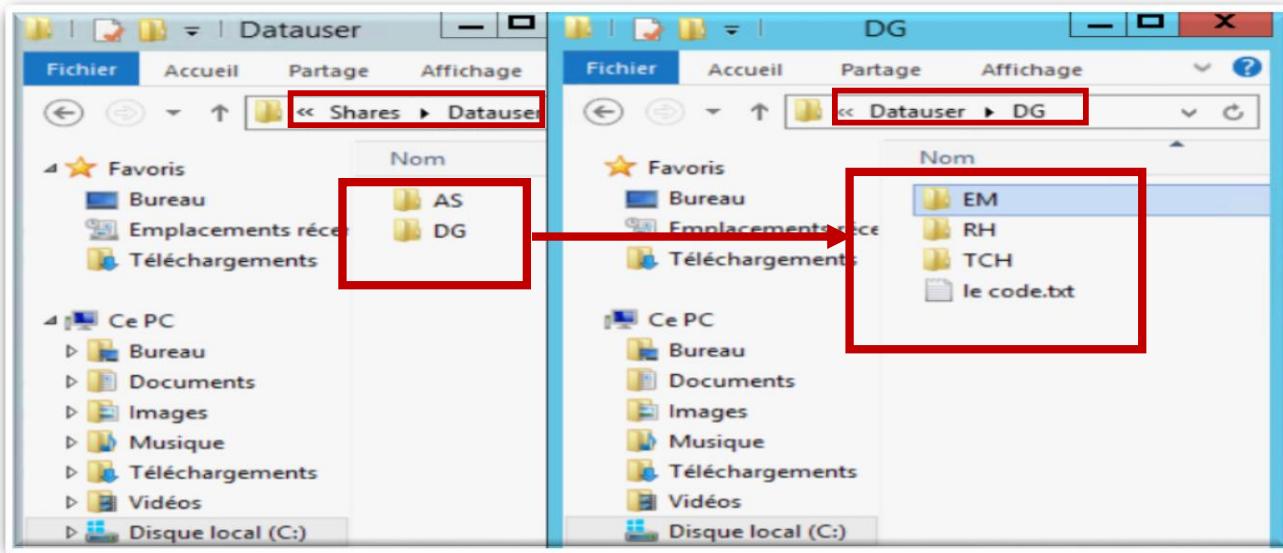
Volume	Espace libre	Capacité	Système de fichiers
C:	118 Go	127 Go	NTFS

L'emplacement du partage de fichiers sera un nouveau dossier du répertoire \Shares sur le volume sélectionné.

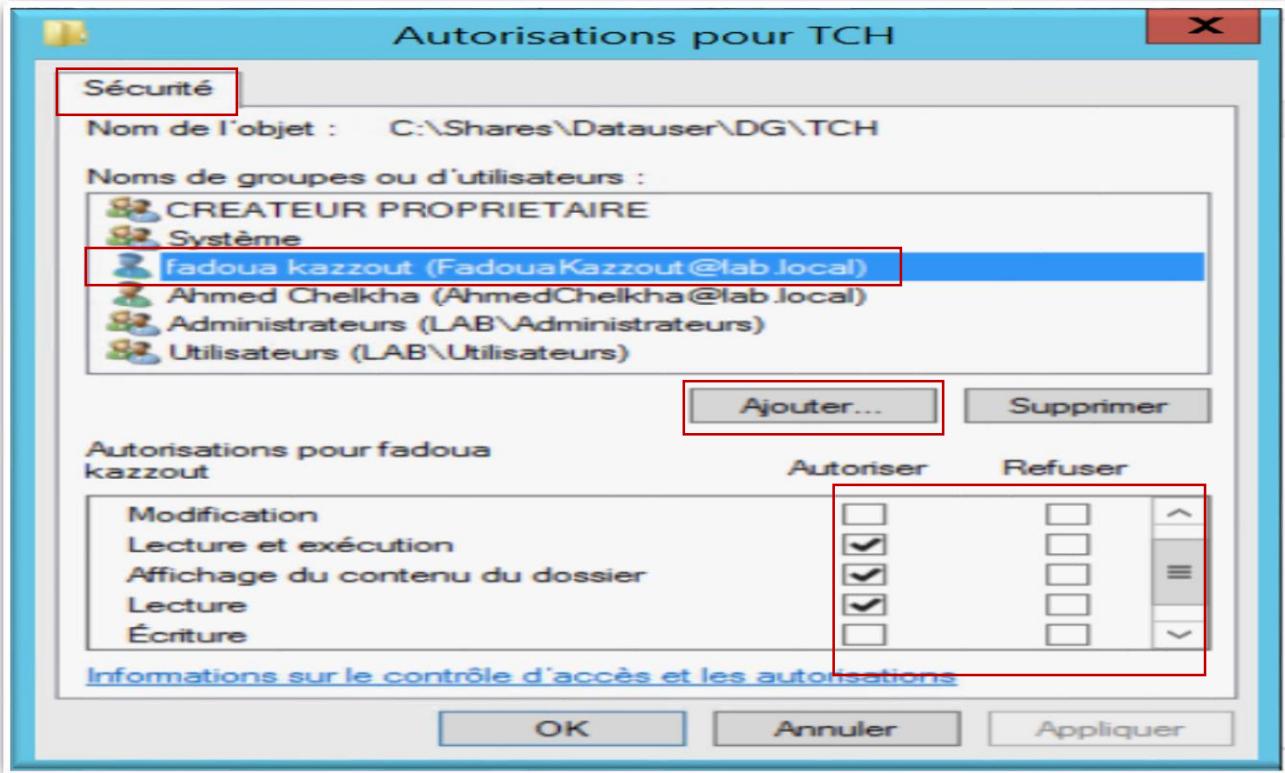
Tapez un chemin personnalisé :

Parcourir...

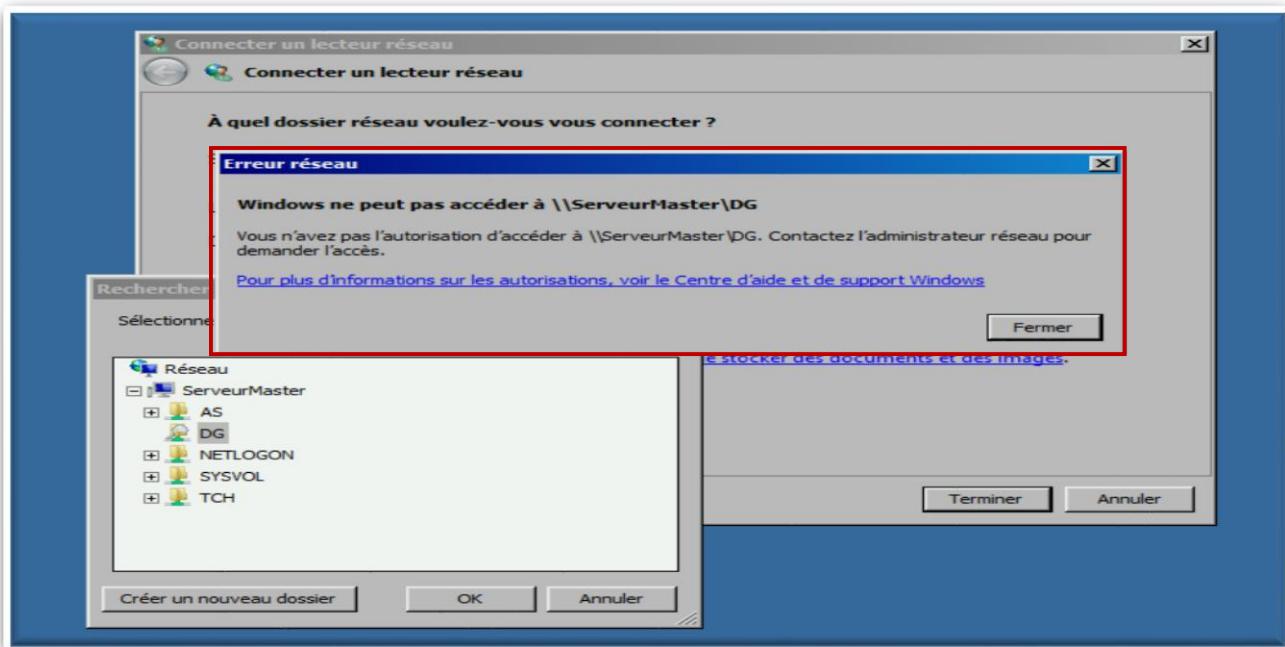
Nous pouvons afficher le dossier partagé dans la console du gestionnaire de serveur. Et on va créer un dossier (Datauser), à l'intérieur de ce dossier on va créer des sous dossier.



Pour sécuriser le partage des dossiers, on doit spécifier les droits d'accès de chaque utilisateur :



Puis on arrivera sur le poste de Fadoua et on essaye d'accéder au dossier de (DG), on voit qu'un message d'autorisateur s'affiche, Mais si on accède au dossier spécifié (TCH) on va voir qu'on a le droit d'accès.



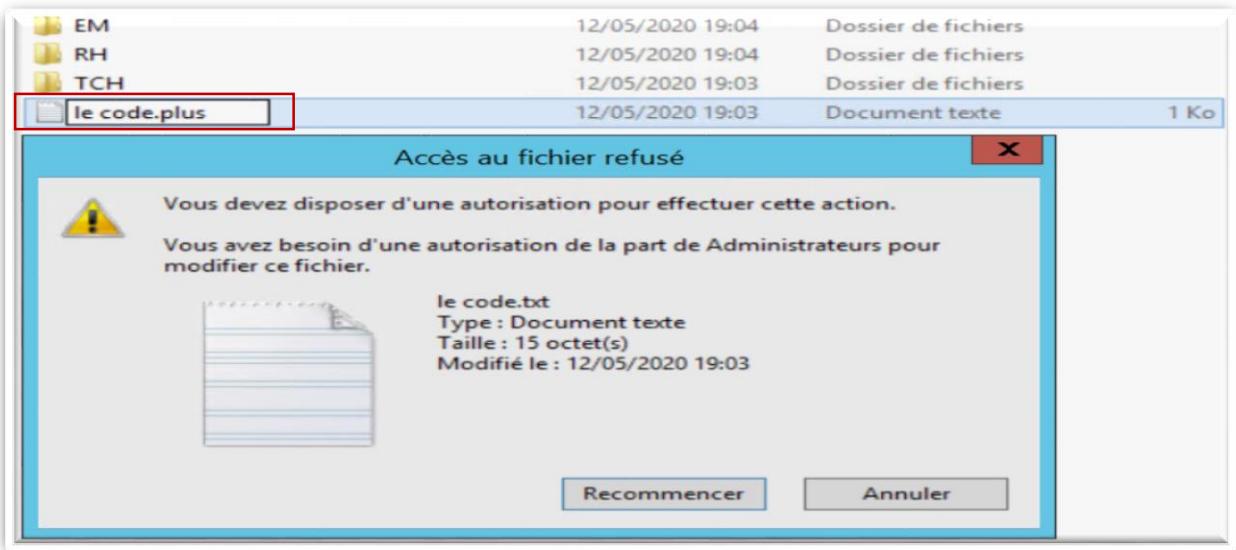
5. Protéger le serveur de fichiers contre les ransomwares :

Depuis plusieurs mois, le nombre de ransomwares qui circulent est particulièrement important. Handicapant pour les particuliers, ce type de logiciel malveillant peut avoir des conséquences parfois dramatiques pour les PME.

Pour protéger le serveur contre les ransomware, Nous avons Crée un modèle de filtre de fichier ou bien une base de données qui contient des extensions actuelle de ransomware.

Groupes de fichiers	Fichiers à inclure	Exclusion de fichiers
CryptoBlockerGroup1	! ПРОЧТИ МЕНЯ !.html, !! RETURN FILES !!.txt, !!! HOW TO DECRYPT FILES...	
CryptoBlockerGroup10	.*.SANTANA, *.SARS-CoV-2, *.SATANA, *.SAVEYOURDATA, *.SAVEfiles, *.S...	
CryptoBlockerGroup11	*+recover+*, *-DECRYPT.html, *-DECRYPT.txt, *-Lock.onion, *-PLIIKI.txt,...	
CryptoBlockerGroup12	.KARLOS, .KEY0004, .KRAB, .PLUT, .SARS-CoV-2, .arripiante, .bxtyunh, .co...	
CryptoBlockerGroup13	FILES ENCRYPTED.txt, FILES.TXT, FILESAREGONE.TXT, FILES_BACK.txt, File ...	
CryptoBlockerGroup14	--README---.TXT, NOTE:!!-ODZYSKAJ-PLIKI-!!!.TXT, OKSOWATHAPPEN...	
CryptoBlockerGroup15	Инструкция по расшифровке.TXT	
CryptoBlockerGroup2	*.+jabber-theone@safetyjabber.com, *.0000, *.010001, *.0402, *.08kJA, *...	
CryptoBlockerGroup3	*.ACTUM, *.ADHUBLKA, *.ADMIN@BADADMIN.XYZ, *.ADR, *.AES, *.AES...	
CryptoBlockerGroup4	*.C-VIR, *.CHIP, *.CHRISTMAS, *.CIFGKSAFFSFYGH, *.CIOP, *.CK, *.CNM...	
CryptoBlockerGroup5	*.DHDRA4, *.DIABLO6, *.DMA Locker*, *.DMR, *.DMR64, *.DOCM!Sample, *...	
CryptoBlockerGroup6	*.GSupport3, *.GX40, *.GrujaRS, *.GusCrypter, *.HAPP, *.HCY!!, *.HDDCrypt...	
CryptoBlockerGroup7	*.I WANT MONEY, *.ID-7ES642406.CRY, *.iEncrypt, *.IFN643, *.IElection20...	
CryptoBlockerGroup8	*.LOCKED.txt, *.LOCKED_BY_pablukl0cker, *.LOCKED_PAY, *.LOCKOUT, *.L...	
CryptoBlockerGroup9	*.PA-SIEM, *.PANDA, *.PAUSA, *.PAY, *.PAY_IN_MAXIM_24_HOURS_OR_A...	

Puis on arrivera sur les fichiers pour tester ce dernier, et on essaye de modifier l'extension de fichier :



6. La haute disponibilité de service :

A côté de la haute disponibilité on va appliquer deux types :

- La haute disponibilité de l'Active Directory.

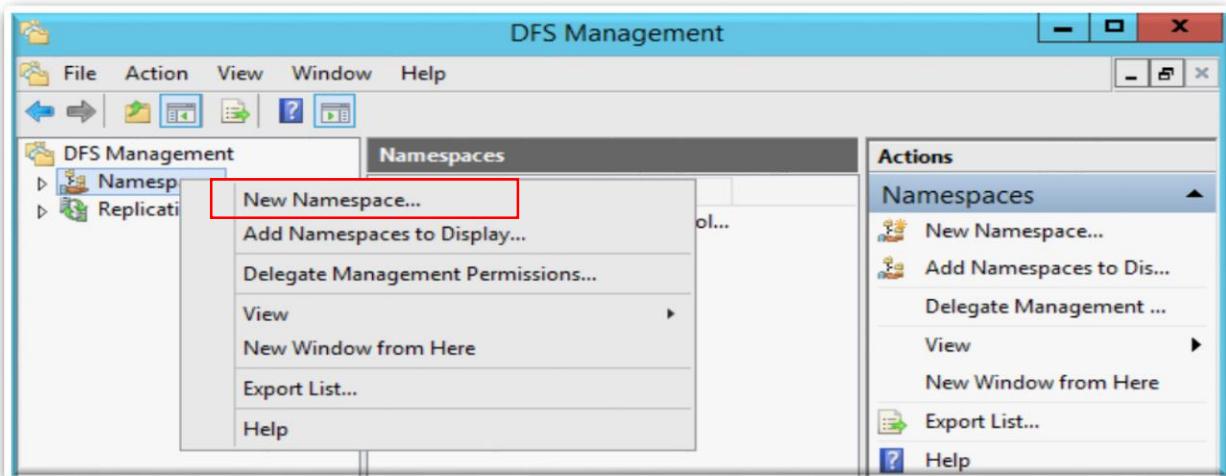
La différence se fait à la configuration du déploiement où nous devrons sélectionner "ajouter un contrôleur de domaine à un domaine existant", ensuite renseignez le nom de domaine, puis suivez les étapes jusqu'à l'installation, afin de terminer on va tester la fonctionnalité de ce dernier.

ServeurMaster sur DESKTOP-4O4QC01 - Connexion à un ordinateur virtuel			ServeurSlave sur DESKTOP-4O4QC01 - Connexion à un ordinateur virtuel		
Fichier	Action	Média	Fichier	Action	Média
Utilisateurs et ordinateurs Active Directory			Utilisateurs et ordinateurs Active Directory		
Fichier Action Affichage ? 			Fichier Action Affichage ? 		
Nom Type Description			Nom Type Description		
admin1 asr Utilisateur Admin2 asr Utilisateur mohamed asr Utilisateur najim asr Utilisateur oussama maziane Utilisateur wafae aissaoui Utilisateur Yassine Mali Utilisateur yousra belhoussine Utilisateur youssef smali Utilisateur			admin1 asr Utilisateur Admin2 asr Utilisateur mohamed asr Utilisateur najim asr Utilisateur oussama ma... Utilisateur wafae aissaoui Utilisateur Yassine Mali Utilisateur yousra bel... Utilisateur youssef sma... Utilisateur		
Utilisateurs et ordinateurs Active Directory [ServeurM] <ul style="list-style-type: none"> > Utilisateurs et ordinateurs Active Directory > Requêtes enregistrées & lab.local <ul style="list-style-type: none"> > Administrateur System > Builtin > Computers > Directeur General > Domain Controllers Employer > ForeignSecurityPrincipals > Managed Service Accounts > Ressources Humaines > Technicien > Users 			Utilisateurs et ordinateurs Active Directory [ServeurS] <ul style="list-style-type: none"> > Utilisateurs et ordinateurs Active Directory > Requêtes enregistrées & lab.local <ul style="list-style-type: none"> > Administrateur System > Builtin > Computers > Directeur General > Domain Controllers Employer > ForeignSecurityPrincipals > Managed Service Accounts > Ressources Humaines > Technicien > Users 		

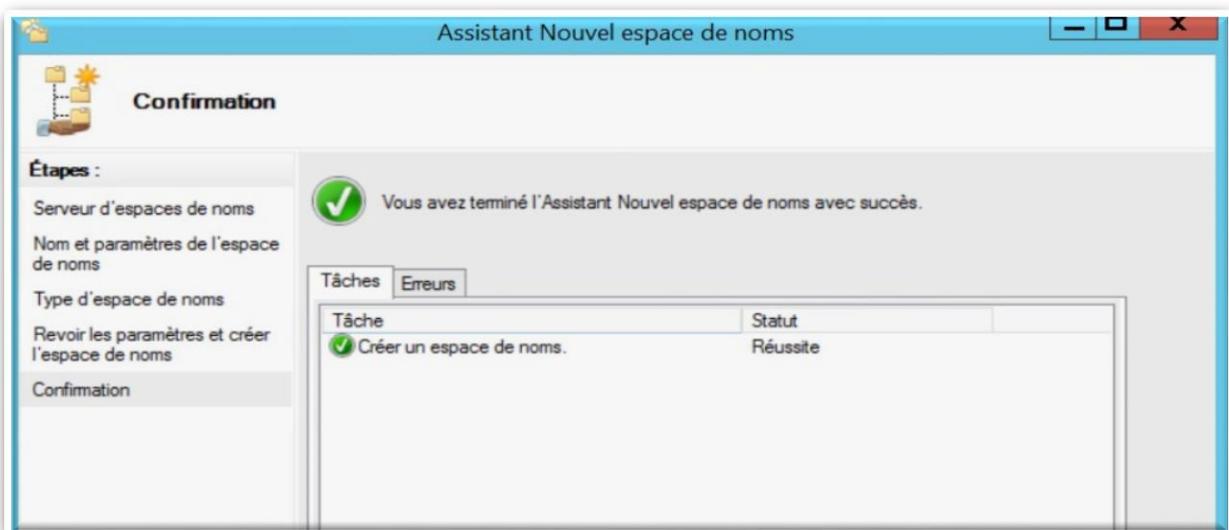
- La haute disponibilité des fichiers avec le protocole DFS :

Après l'installation de la fonctionnalité DFS, nous allons le configurer uniquement sur le serveur DFS maître qui sera le serveur -Master, alors nous observons que nous avons bien « DFS Management » et ses sous rubrique « Namespaces » et « Replication ».

Pour cela, nous allons faire un clic droit sur « Namespaces » et cliqué sur « New Namespaces ».

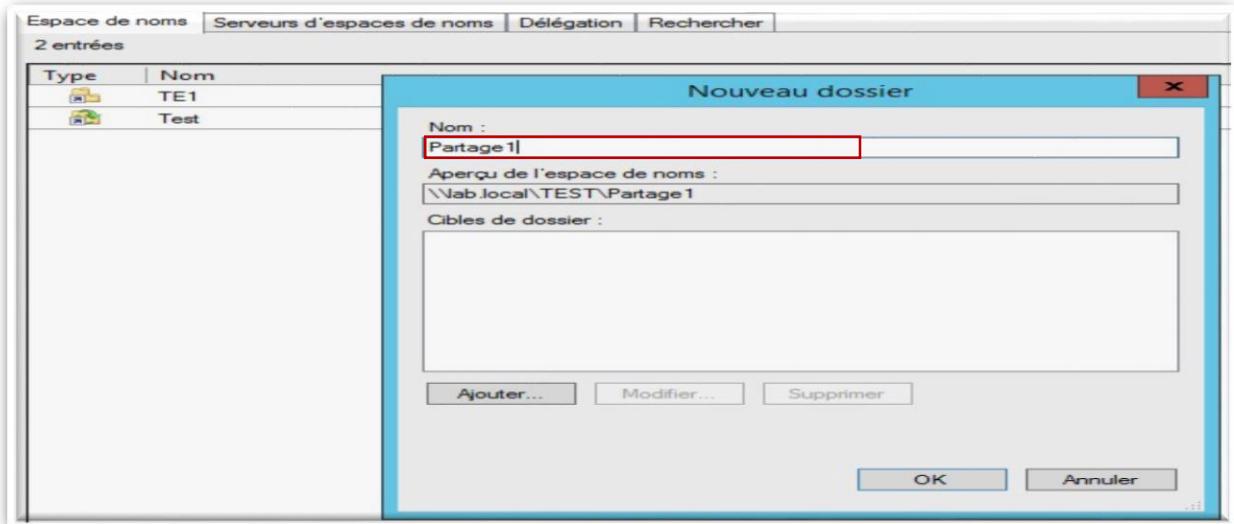


Puis nous allons donner un nom à notre dossier de partage « shares », et l'utilisateur pourra entrer l'url « \\ServeurMaster\shares » pour directement accéder aux dossiers partagés en réseau. On clique sur Suivant, nous avons un résumé global et on valide sur « Créer », puis nous avons une confirmation de la création Réussite.

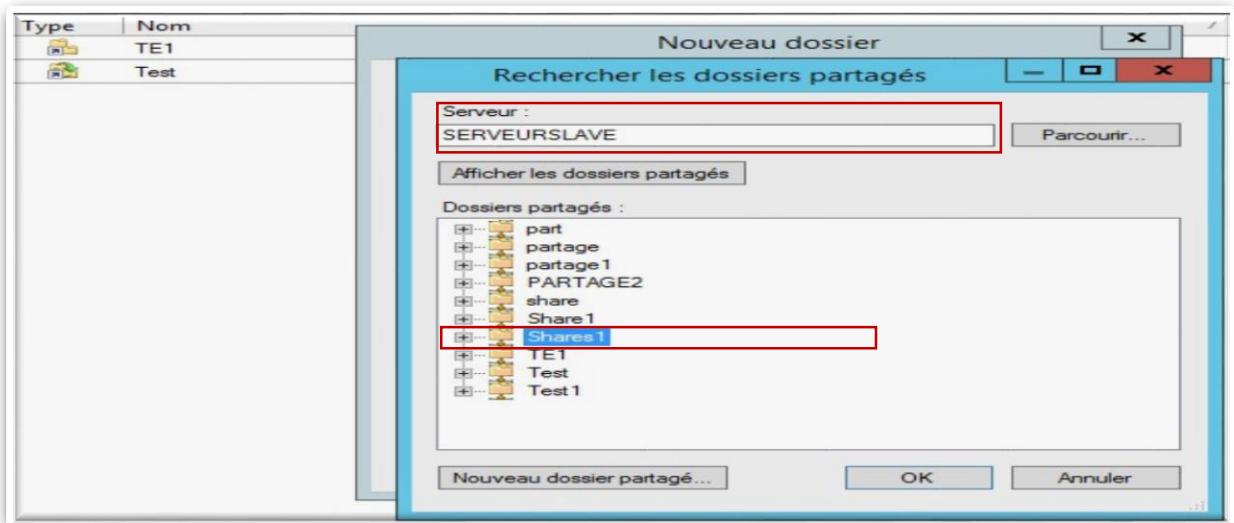


Maintenant que l'espace de noms est opérationnel, nous devons créer un dossier dans celui-ci, alors on clique droit sur notre nouvel espace de noms puis clique sur « Nouveau dossier ».

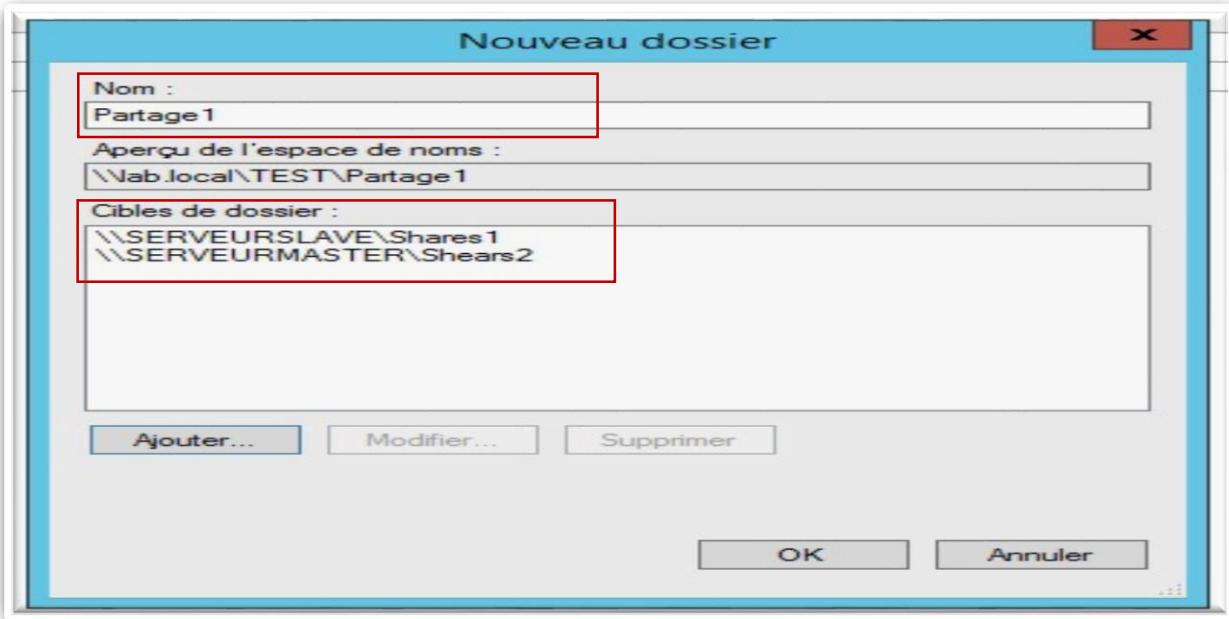
Tous les fichiers qui seront alors mis dans le dossier d'espace de noms seront répliqués sur nos deux serveurs de stockage.



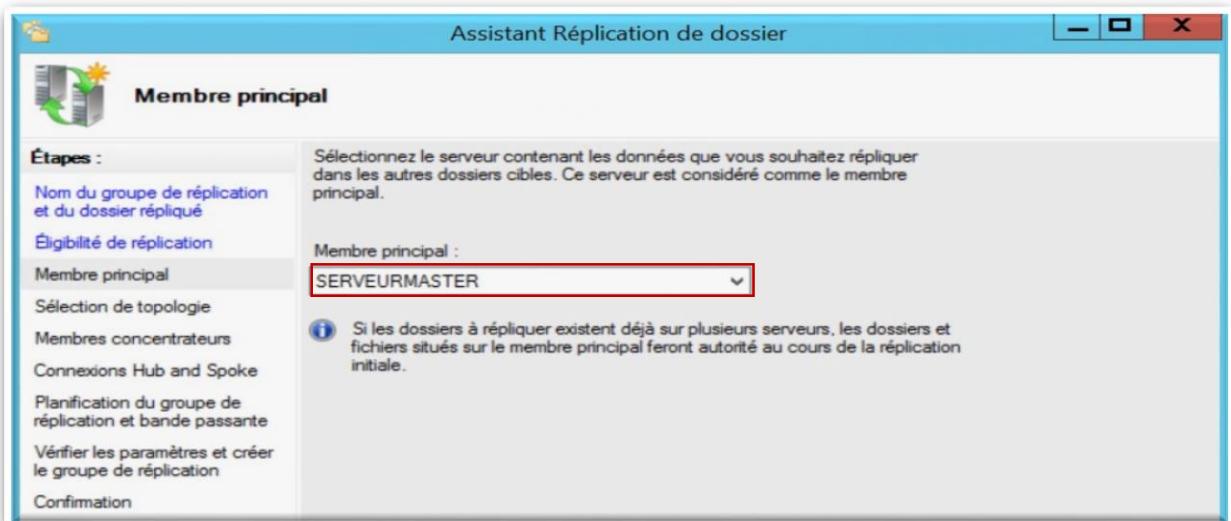
Ensuite on a sélectionné un des serveurs de stockage (Server Slave), et on a choisi le dossier partagé où seront stockées nos données.



Nous recommençons pour le dossier partagé de notre second serveur Server Master. Une fois la cible des dossiers sélectionnée, on clique sur « OK » pour continuer.

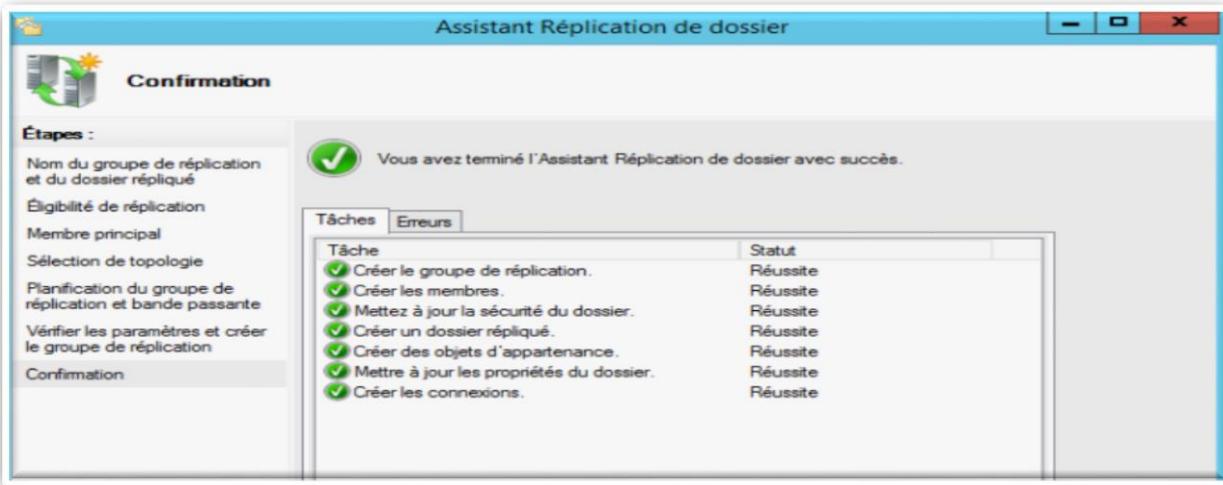


Comme notre dossier d'espace de noms comporte deux cibles une nouvelle fenêtre nous demande si l'on veut créer un groupe de réPLICATION. Puis nous choisissons le membre principal du groupe de réPLICATION.



Nous avons besoin de configurer la bande passante ou la planification de notre réPLICATION. On a choisi de laisser la totalité de la bande passante pour la réPLICATION.

Alors la réPLICATION est bien fonctionnée.



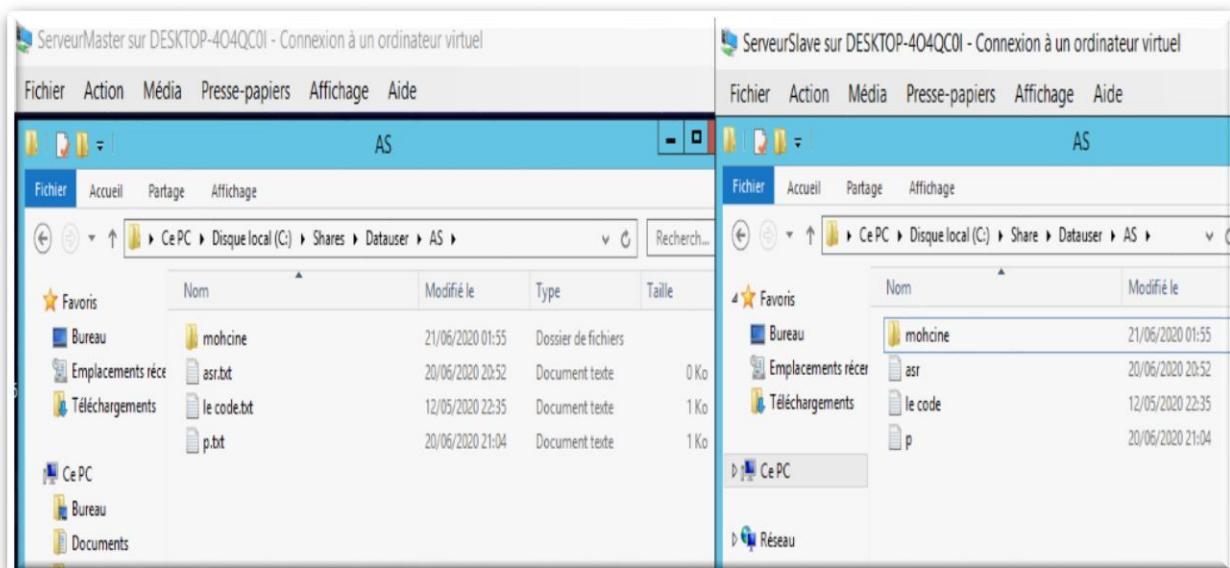
TEST :

Nous pouvons à présent accéder à notre espace de noms via « \\lab.local\REP\Share\Share\Datauser\AS ». Si nous copions un fichier dans notre dossier d'espace de noms il sera automatiquement répliqué entre les deux serveurs cibles (Server Master et Server Slave).

Si un des serveurs cibles venait à planter, les données seront toujours accessibles et cela sera totalement transparent pour l'utilisateur.

Pour tester notre réPLICATION, nous pouvons créer un nouveau dossier ou déplacer un fichier dans notre dossier d'espace de noms « \\lab.local\REP\Share\Share\Datauser\AS ».

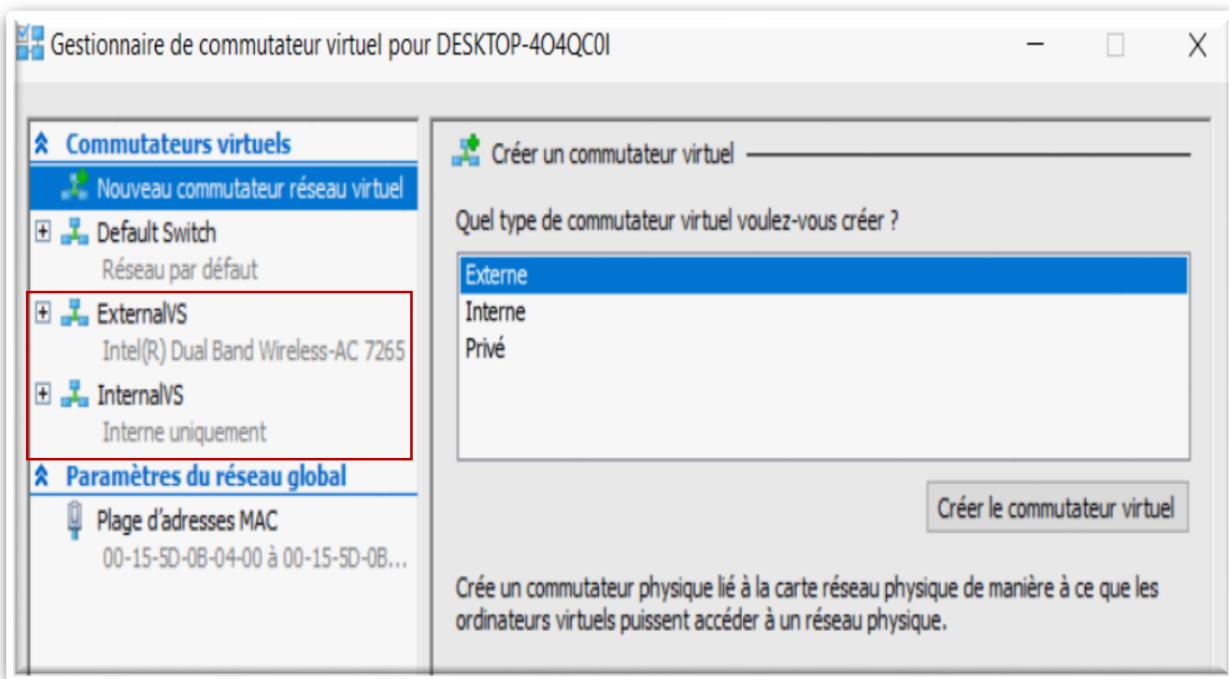
En nous rendant dans les dossiers partagés de nos serveurs Server Master et Server Slave, nous constatons que ce dossier a été répliqué sur ces deux serveurs. La réPLICATION peut prendre quelques minutes.



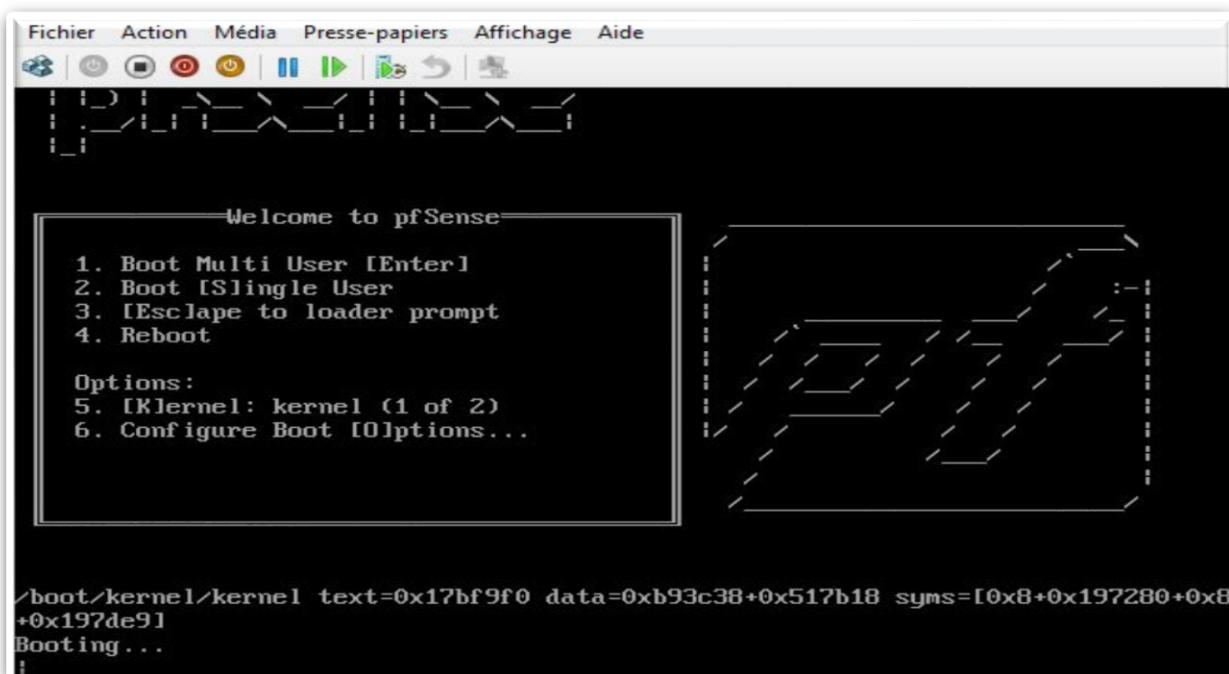
7. Installation et Configuration de pfSense :

Configuration de la VM Hyper-V :

Il s'agit d'une machine virtuelle sous Hyper-V. La configuration est la suivante : On va créer 2 Cartes réseaux interne et externe.



Démarrer la VM :



On va accepter la licence, puis on installe pfSense,

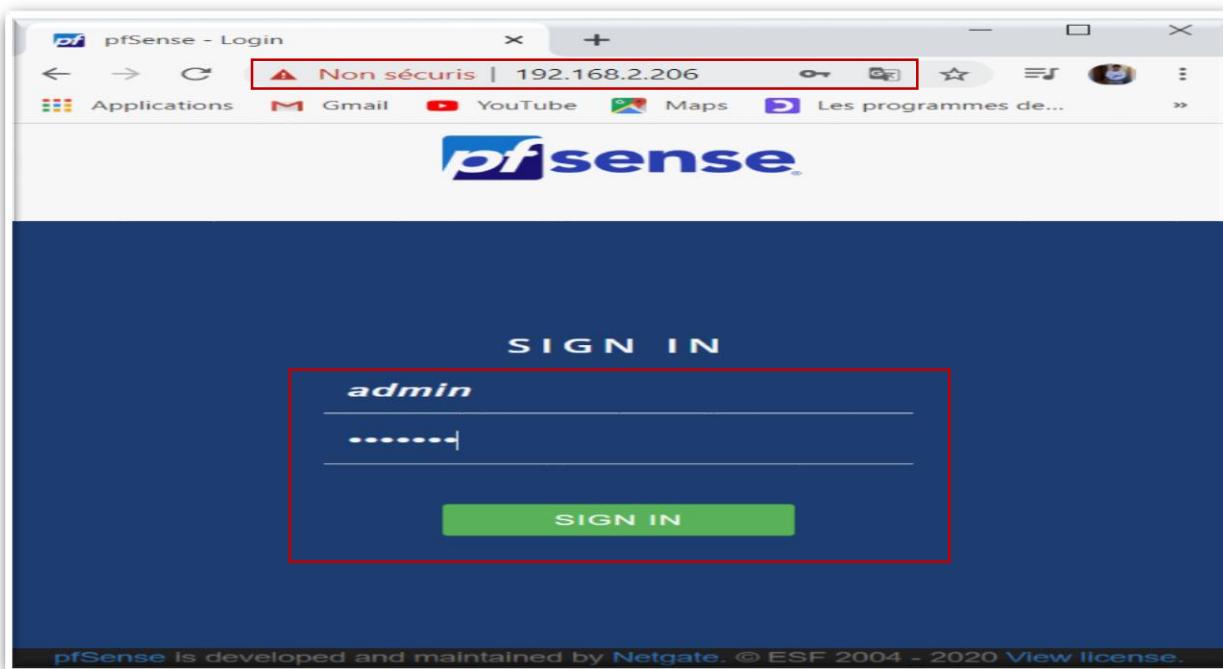
Une fois l'installation terminée, sélectionnez redémarre et éjecter l'ISO. On sélectionne N pour ne pas configurer le VLAN, après on affecte les interfaces WAN et LAN aux adaptateurs réseau appropriés.

```
Pfsense sur DESKTOP-4O4QC0I - Connexion à un ordinateur virt...
Fichier Action Média Presse-papiers Affichage Aide
Warning: Configuration references interfaces that do not exist: em0 em1
Network interface mismatch -- Running interface assignment option.
Valid interfaces are:
hn0      00:15:5d:0b:04:0a (down) Hyper-V Network Interface
hn1      00:15:5d:0b:04:0b (down) Hyper-V Network Interface
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y/n]? n
If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.
Enter the WAN interface name or 'a' for auto-detection (hn0 hn1 or a): hn0
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn1 a or nothing if finished): hn1
```

Après on tape L'adresse IP dans le navigateur : 192.168.2.206 :

Username : **admin**

Password : **pfsense**



Configuration de l'installation de Base de pfSense :

Après le message de bienvenue, on clique sur next deux fois pour continuer sans souscrire à un contrat de maintenance. On saisit le nom de notre Serveur et du domaine d'appartenance.

Les deux écrans suivants sont des résumés des options que nous avons déjà mis en œuvre sur le réseau. Enfin, pour terminer, il faut modifier le mot de passe du compte **admin**.

The screenshot shows the pfSense Community Edition dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area has two tabs: "Status / Dashboard" (selected) and "ESTEAM". The "Status / Dashboard" tab displays "System Information" with details like Name (ServeurMaster.lab.local), User (admin@192.168.2.205), System (Microsoft Azure), BIOS (Vendor: American Megatrends Inc., Version: 090007, Release Date: Fri May 18 2018), and Version (2.4.5-RELEASE-p1). It also shows a message: "The system is on the latest version." and "Version information updated at Sat Jun 27 13:44:53 UTC 2020". The "ESTEAM" tab shows a logo and the word "ESTEAM". The "Interfaces" tab lists two interfaces: "WAN" (10Gbase-T <full-duplex>, IP: 192.168.1.118) and "LAN" (10Gbase-T <full-duplex>, IP: 192.168.2.206).

Configuration du serveur DHCP :

Pour activer le service DHCP sur PfSense, il se fait de rendre dans le menu « Services » puis « DHCP Server », et on choisit l'interface sur laquelle nous souhaitons activer le serveur DHCP. Dans notre cas, ce sera « LAN ». Et nous cochons évidemment la case « Enable DHCP server on LAN interface », puis nous configurons pfSense avec une première plage (champ Range) allant de 192.168.2.10 à 192.168.2.40, nous avons spécifié le serveur DNS, Gateway et aussi le Domain et on filtrer les accès au serveur DHCP par adresse MAC.

The changes have been applied successfully.

LAN

General Options

Enable Enable DHCP server on LAN interface

BOOTP Ignore BOOTP queries

Deny unknown clients Only the clients defined below will receive an IP address.

Ignore denied clients Denied clients will be ignored rather than assigned an IP address.

This option is not compatible with failover.

Ignore client identifiers If a client includes a unique identifier, it will be recorded in its lease.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet	192.168.2.0
Subnet mask	255.255.255.0
Available range	192.168.2.1 - 192.168.2.254
Range	From: 192.168.2.10 To: 192.168.2.40

Servers

WINS servers

WINS Server 1:

WINS Server 2:

DNS servers

192.168.2.200 DNS servers

DNS Server 2:

DNS Server 3:

DNS Server 4:

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder is disabled or the IP of the DNS server in the System / General Setup page.

Other Options

Gateway: 192.168.2.206 Gateway

The default is to use the IP on this interface of the firewall as the gateway. Specify another IP if you want to use a different network. Type "none" for no gateway assignment.

Domain name: lab.local Domain name

The default is to use the domain name of this system as the default domain name.

Et pour tester nous avons rendu sur la machine win7, et on essaye d'activer le service DHCP :

The screenshot shows a Windows 7 desktop with several windows open:

- A File Explorer window titled "Corbeille".
- An "État de Connexion au réseau local" (Network Connection Status) window for "Réseau 2 Carte réseau". It shows general connectivity information like IPv4 and IPv6 status, and a detailed "Détails de connexion réseau" (Network Connection Details) window. The "Détails de connexion réseau" window is highlighted with a red box and displays the following properties:

Propriété	Valeur
Suffixe DNS propre à l'interface	lab.local
Description	Carte réseau de bus Microsoft Hyper-V
Adresse physique	00:15:5D:0B:04:05
DHCP activé	Oui
Adresse IPv4	192.168.2.10
Masque de sous-réseau	255.255.255.0
Bail obtenu	vendredi 26 juin 2020 15:33:27
Bail expirant	vendredi 26 juin 2020 17:33:27
Passerelle par défaut IPv4	192.168.2.206
Serveur DHCP IPv4	192.168.2.206
Serveur DNS IPv4	192.168.2.200
Serveur WINS IPv4	
NetBIOS sur TCP/IP activé	Oui
Adresse IPv6 locale de l'interface	fe80:f43e:cdf:4c2e:5d75%11
Passerelle par défaut IPv6	
Serveur DNS IPv6	
- A "cmd.exe" window showing the command "ping 8.8.8.8" and its output, which is also highlighted with a red box.

Bloquer l'accès aux sites Web sur Pfsense :

Commençons par création d'un nouvel alias et nous mettrons toutes les adresses IP et les noms d'hôte pleinement qualifiés des sites Web auxquels nous souhaitons autoriser ou bloquer l'accès.

The screenshot shows the 'Aliases' configuration page. A new alias is being created with the following details:

- Name:** allowed_websites
- Description:** Gmail and Google drive
- Type:** Host(s)

In the 'Host(s)' section, three hosts are listed:

- IP or FQDN: mail.google.com
- IP or FQDN: drive.google.com
- IP or FQDN: google.com

Each host entry includes an 'Entry added' timestamp and a delete button.

Nous devons maintenant utiliser cette alias pour configurer la règle réelle qui autorisera ou empêchera l'accès.

Autoriser l'accès à un site Web on définisse l'action à passer, car nous voulons autoriser l'accès justement au Gmail et Google Drive. Puis l'interface doit être LAN net, car cela s'applique aux utilisateurs LAN.

The screenshot shows the 'Edit Firewall Rule' configuration page. A new rule is being created with the following settings:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP

Below these settings, the 'Source' and 'Destination' sections are shown:

- Source:** Source: Invert match, LAN net, Source Address: /
- Destination:** Destination: Invert match, Single host or alias: allowed_websites, Destination Port Range: any / any, From: Custom, To: Custom

A note at the bottom of the destination section states: "Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port."

Pour Bloquer l'accès d'un site Web on définit l'action à block, car nous voulons bloquer l'accès à tous d'autre site web. Puis l'interface doit être LAN, car cela s'applique aux tous les utilisateurs LAN.

Edit Firewall Rule

Action	Block
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any

Source

Source	<input type="checkbox"/> Invert match	any	Source Address	/
--------	---------------------------------------	-----	----------------	---

Destination

Destination	<input type="checkbox"/> Invert match	any	Destination Address	/
-------------	---------------------------------------	-----	---------------------	---

Une fois ajouter tous les rôles on va déplacer le rôle « allow » avant « deny » pour autoriser l'accès au site spécifier puis refuser.

Rules (Drag to Change Order)

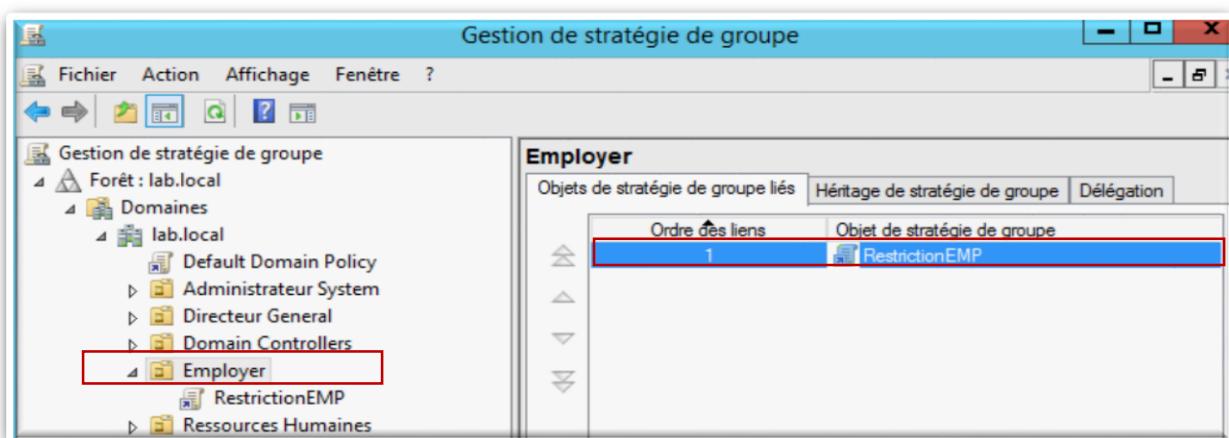
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 /237 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	LAN net	*	allowed_websites	*	*	none		allowed Gmail and Google Drive	
<input type="checkbox"/>	✗ 0 /3 KiB	IPv4*	*	*	*	*	*	none		deny All Web site	
<input type="checkbox"/>	✓ 0 /0 B	IPv4*	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 /0 B	IPv6*	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

8. Filtrage de sécurité des stratégies de groupe :

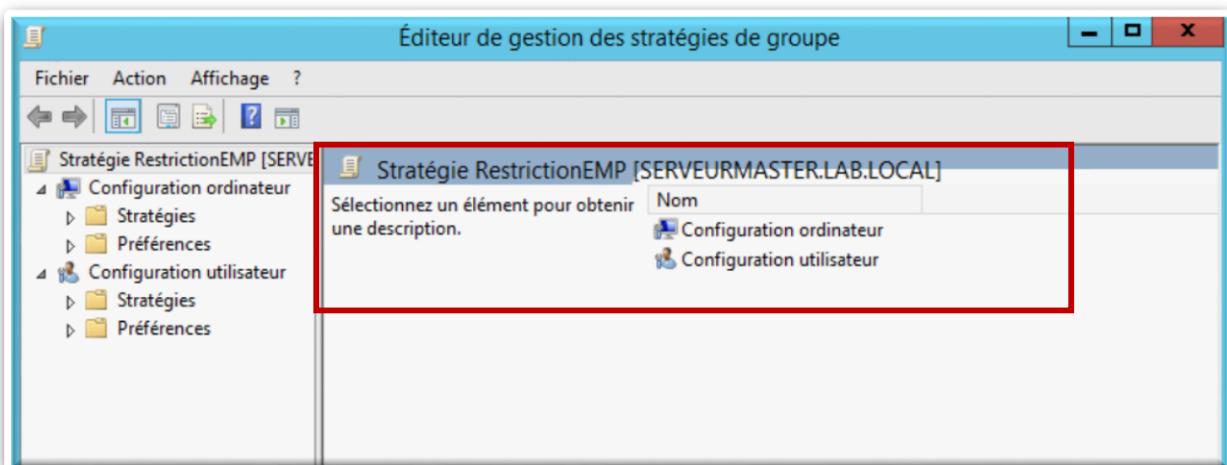
Cette dernière partie décrit comment l'administrateur d'un domaine peut déployer des logiciels automatiquement aux membres de son domaine. Cela permet d'automatiser une tâche autrefois fastidieuse qui consistait à installer un logiciel manuellement sur plusieurs machines. Cette application s'installera automatiquement au démarrage de leur session utilisateur.

Configuration de GPO :

Après l'installation de stratégie de groupe, puis on clique droit sur l'unité d'organisation « Employer » qui contient des utilisateurs et puis on crée un objet GPO « RestrictionEMP » dans ce domaine.

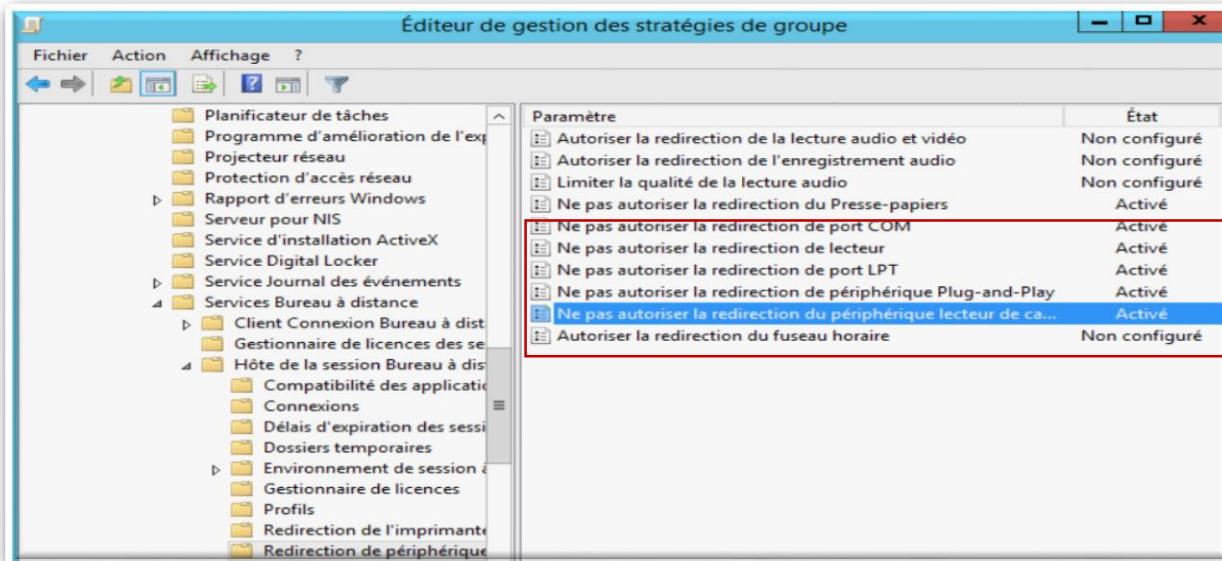


Une fois créée, la GPO apparaît dans notre liste déroulante. Clic droit sur notre GPO → Modifier. Ainsi nous accédons aux paramètres configurables de notre GPO.

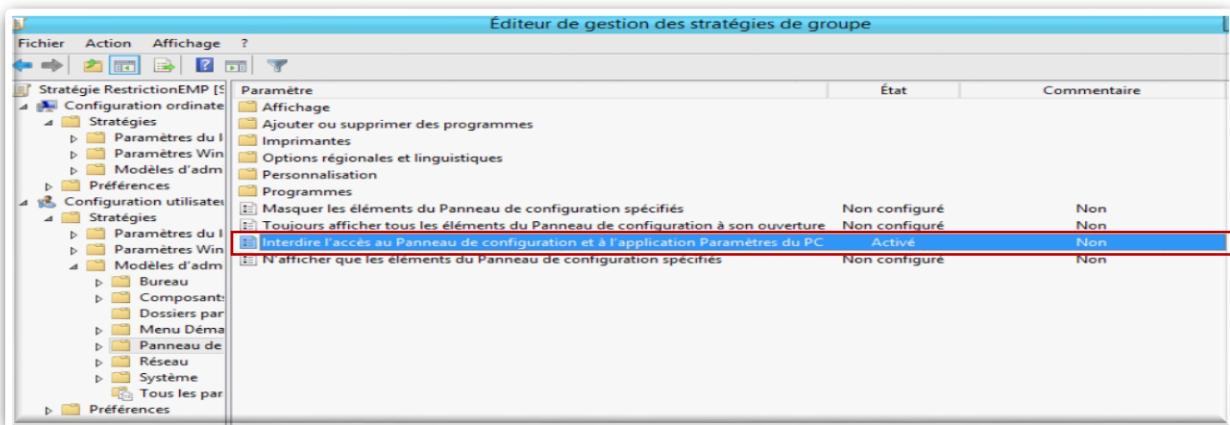


On se déplace vers la partie qu'on veut configurer :

- Configuration ordinateur\ Stratégies \Modèles\ d'administration définitions\Composants Windows \Services Bureau à distance\Hôte de la session Bureau à distance\Redirection de périphérique.

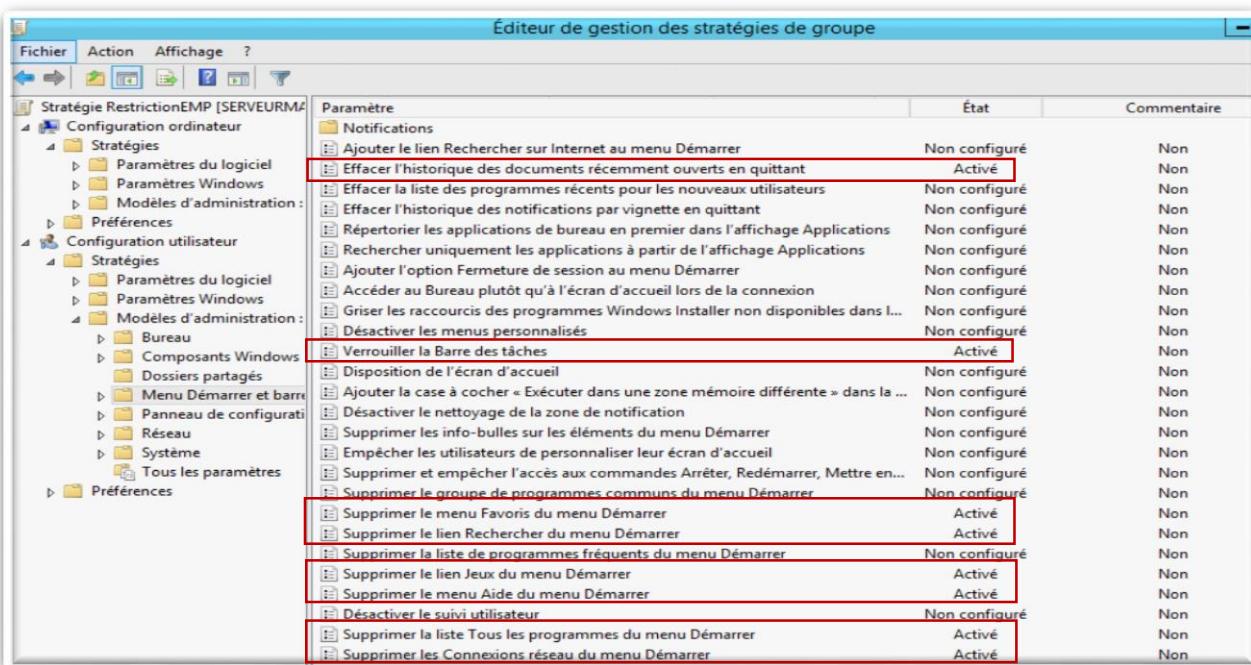


- Configuration utilisateur \Stratégies \Modèles\d'administration définitions\ Panneau de configuration.



On arrivera sur :

Configuration utilisateur\Stratégies\Modèles\d'administration définitions\ Menu Démarrer et barre...



▷	Paramètres du logiciel	Supprimer et empêcher l'accès aux commandes Arrêter, Redémarrer, Mettre en...	Non configuré	Non
▷	Paramètres Windows	Supprimer le groupe de programmes communs du menu Démarrer	Non configuré	Non
▷	Modèles d'administration :	Supprimer le menu Favoris du menu Démarrer	Activé	Non
▷	Préférences	Supprimer le lien Rechercher du menu Démarrer	Activé	Non
Configuration utilisateur		Supprimer la liste de programmes fréquents du menu Démarrer	Non configuré	Non
Stratégies		Supprimer le lien Jeux du menu Démarrer	Activé	Non
▷	Paramètres du logiciel	Supprimer le menu Aide du menu Démarrer	Activé	Non
▷	Paramètres Windows	Désactiver le suivi utilisateur	Non configuré	Non
▷	Modèles d'administration :	Supprimer la liste Tous les programmes du menu Démarrer	Activé	Non
▷	Bureau	Supprimer les Connexions réseau du menu Démarrer	Activé	Non
▷	Composants Windows	Supprimer la liste de programmes en attente du menu Démarrer	Non configuré	Non
▷	Dossiers partagés	Ne pas conserver d'historique des documents récemment ouverts	Non configuré	Non
▷	Menu Démarrer et barre	Supprimer le menu Documents récents du menu Démarrer	Non configuré	Non
▷	Panneau de configura	Ne pas utiliser la méthode basée sur la recherche pour déterminer les raccourci...	Non configuré	Non
▷	Réseau	Ne pas utiliser la méthode basée sur le suivi pour déterminer les raccourcis de l'...	Non configuré	Non
▷	Système	Supprimer le menu Exécuter du menu Démarrer	Activé	Non
▷	Tous les paramètres	Supprimer le lien Programmes par défaut du menu Démarrer.	Activé	Non
▷	Préférences	Supprimer l'icône Documents du menu Démarrer	Activé	Non
		Supprimer l'icône Musique du menu Démarrer	Non configuré	Non
		Supprimer l'icône Réseau du menu Démarrer	Activé	Non
		Supprimer l'icône Images du menu Démarrer	Activé	Non

Enfin on déplace vers :

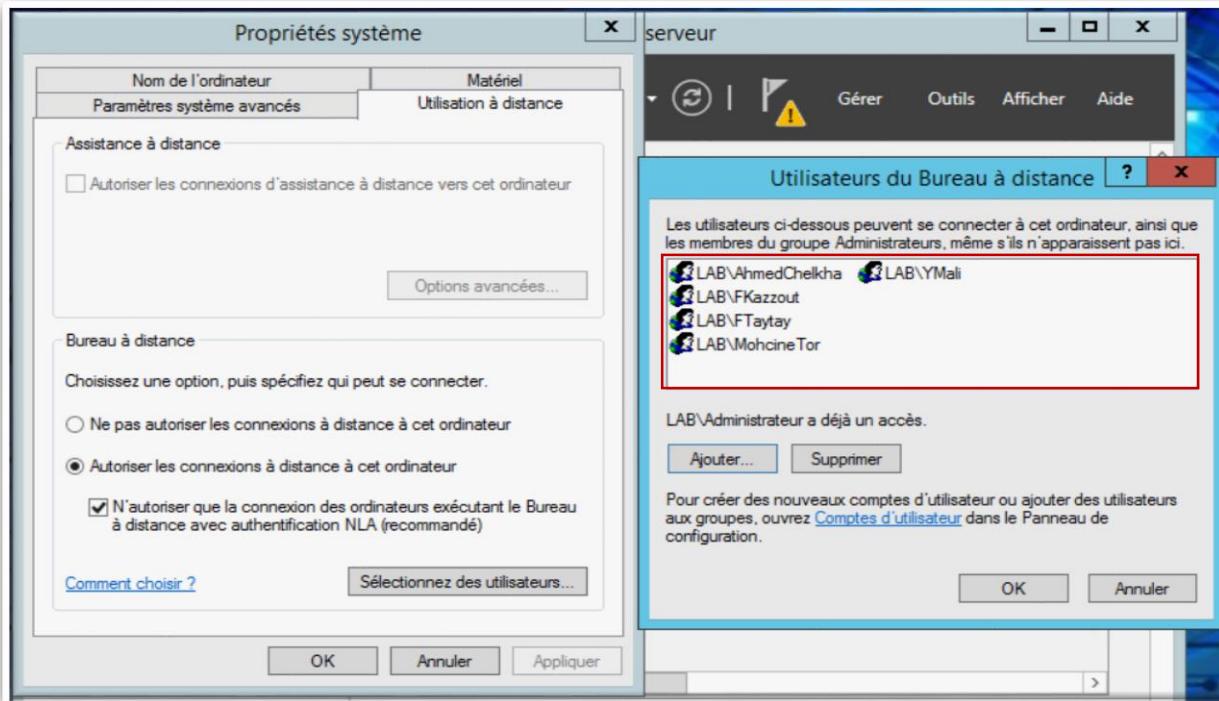
Configuration utilisateur\Stratégie\Modèles\d'administration définitions\Système

▷	Paramètres Win	Scripts		
▷	Modèles d'adm	Services Paramètres régionaux		
▷	Bureau	Stratégie de groupe		
▷	Composant	Télécharger les composants manquants	Non configuré	Non
▷	Dossiers par	Interprétation du siècle pour l'an 2000	Non configuré	Non
▷	Menu Déma	Restreindre l'exécution de ces programmes à partir de l'aide	Non configuré	Non
▷	Panneau de	Ne pas afficher l'écran d'accueil Mise en route à l'ouverture de session	Non configuré	Non
▷	Réseau	Interface utilisateur personnalisée	Non configuré	Non
▷	Système	Désactiver l'accès à l'invite de commandes	Activé	Non
▷	Tous les par	Empêche l'accès aux outils de modifications du Registre	Activé	Non
▷	Préférences	Ne pas exécuter les applications Windows spécifiées	Non configuré	Non
		Exécuter uniquement les applications Windows spécifiées	Non configuré	Non
		Mises à jour automatiques Windows	Activé	Non

Sur PowerShell on va taper la commande gpupdate /force pour la mettre à jour des stratégies de groupe.

```
Un accès est correct et reessayez.
Au caractère Ligne:1 : 1
+ gpupdate/force
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (gpupdate/force:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Users\Administrateur> gpupdate /force
Mise à jour de la stratégie...
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
PS C:\Users\Administrateur>
```

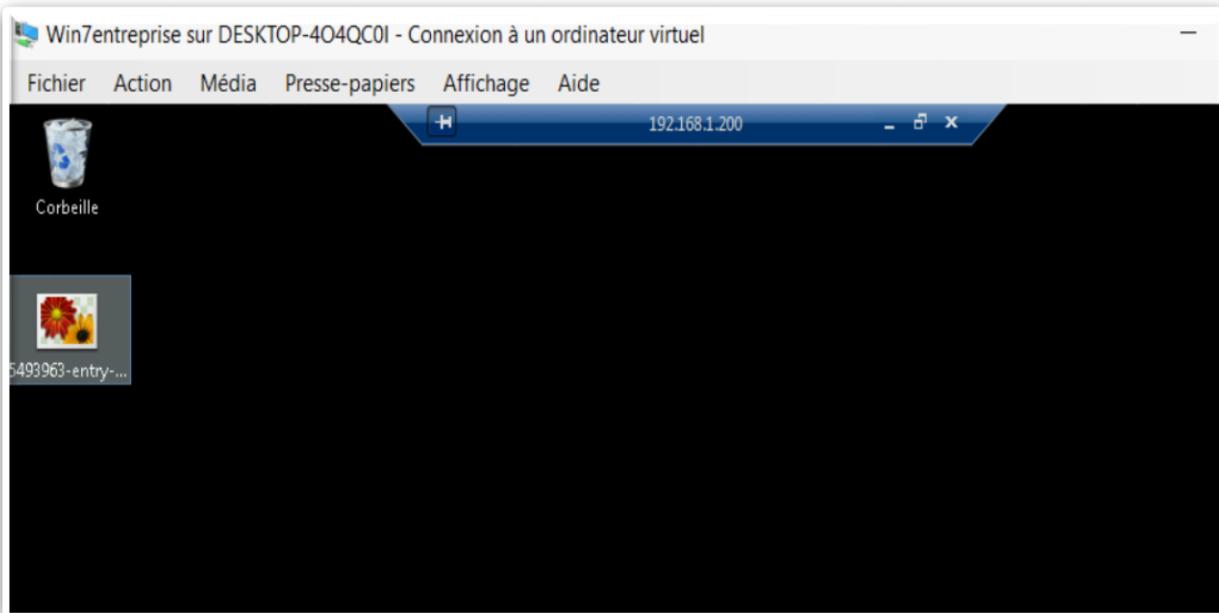
Puis on arrivera sur « Propriétés système » et on sélectionne les utilisateurs autoriser à l'accès distance :



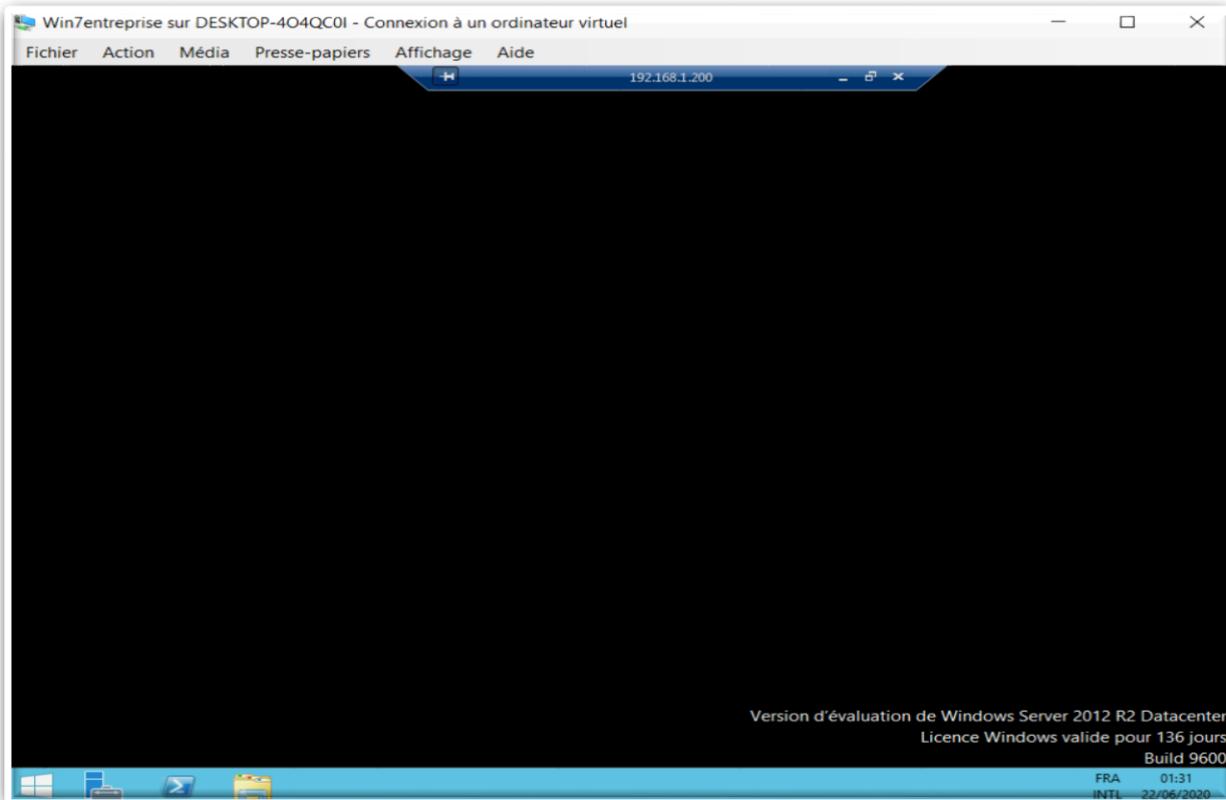
TEST :

Tester notre GPO en ouvrant la session de l'utilisateur « YMali ». Au démarrage, l'application devrait s'installer toute seule. Dans notre cas tous les éléments doivent être masqué et désactiver du bureau.

❖ Avant la configuration :



❖ Après la configuration :



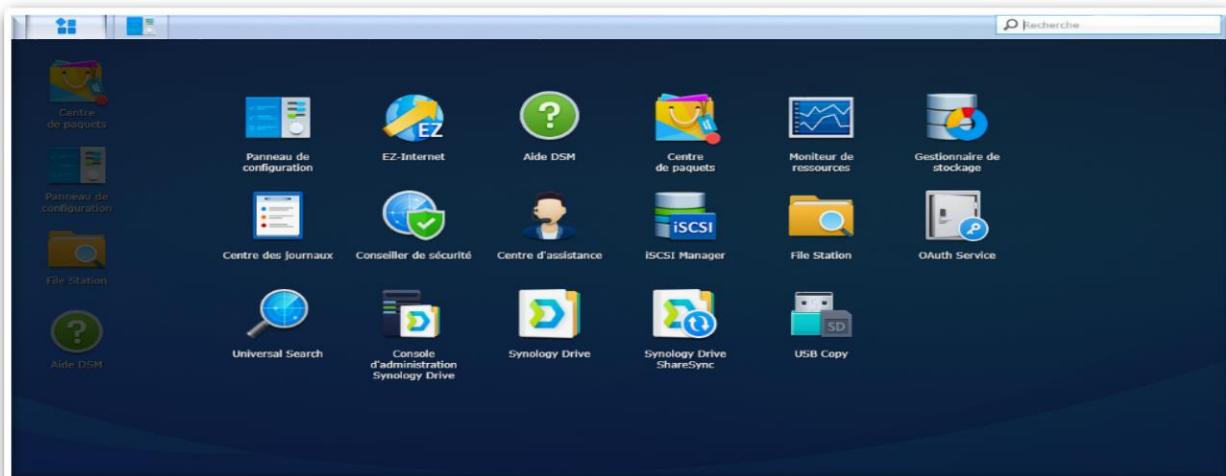
Si on essaye d'accéder au « cmd » ou bien « panneau de configuration » il affiche ce message :



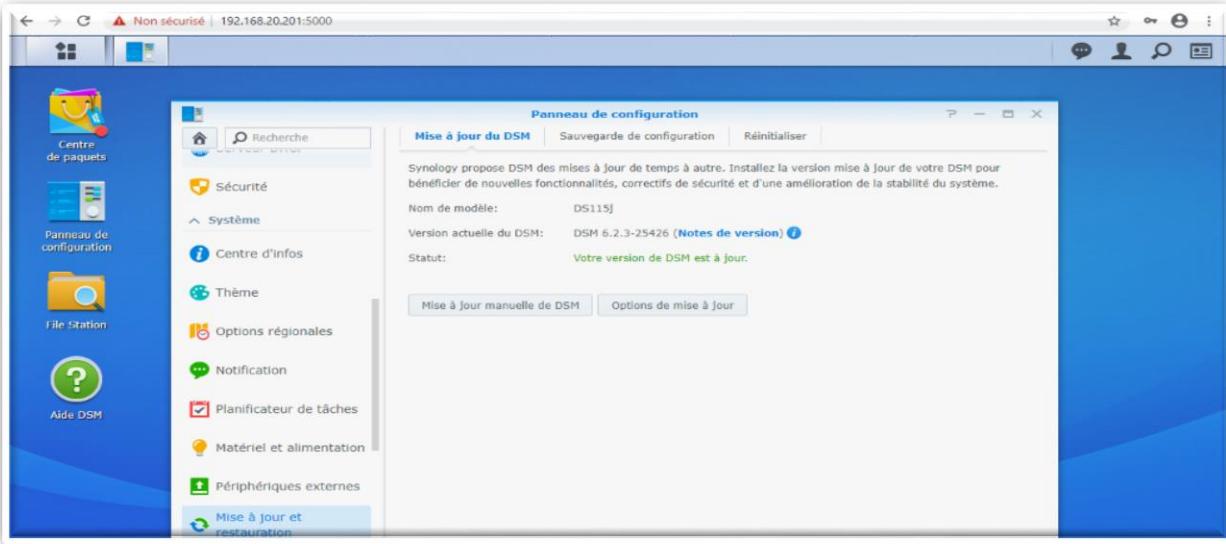
9. Application de Sauvegarder les données :

La stratégie Online « Planifie »

Après d'installation et configuration de base de Synology NAS, on arrivera sur l'interface suivante :



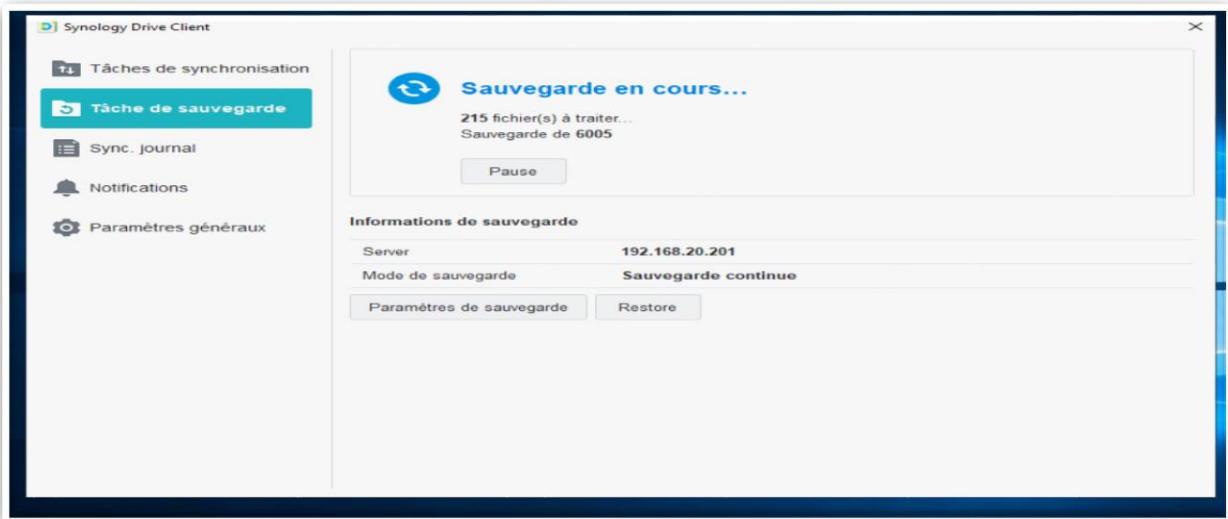
Et on a choisi la dernière version de DSM « sages d'un système complète de NAS », à cause de problème de sécurité et on a planifié de faire maître à jour de sécurité DSM chaque mercredi et samedi.



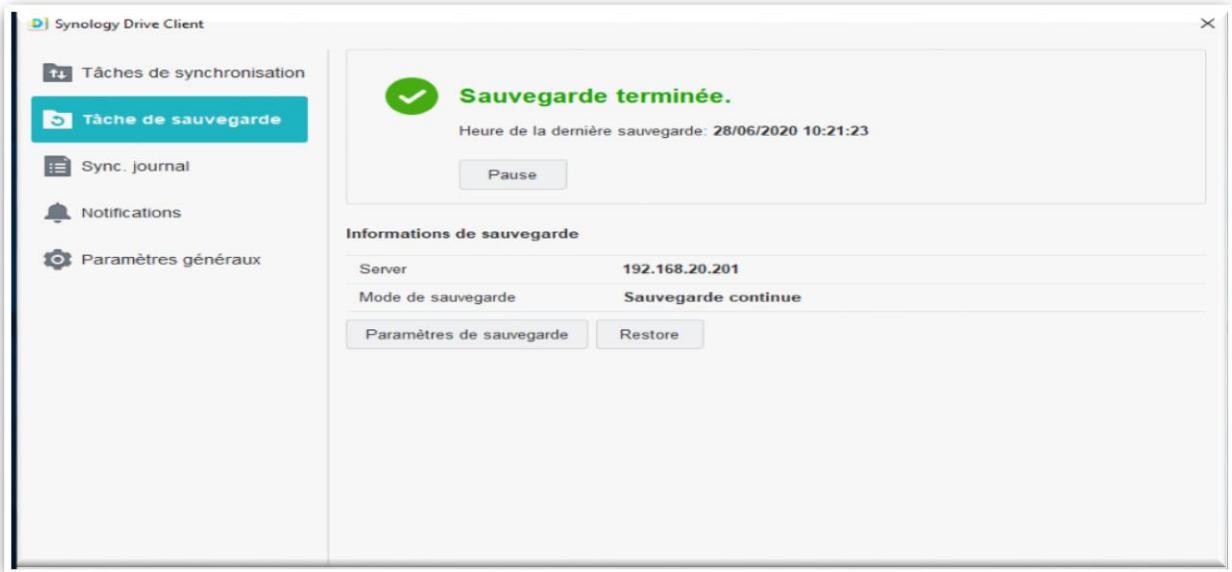
Après on a installé et configuré le Synology Drive Server, et on planifie une sauvegarde différentielle des données chaque jour en temps réel. On sélectionne la source de sauvegarde, et on décoche tous les sous-dossiers que nous ne souhaitons pas synchroniser.

Puis on arrivera sur le résumé de nos paramètres de sauvegarde. Et on clique sur « Précédent » pour apporter des modifications ou sur « Terminé » pour terminer la configuration.

Donc la sauvegarde et en cours :



Enfin nous pouvons consulter la progression de notre sauvegarde dans la fenêtre principale.

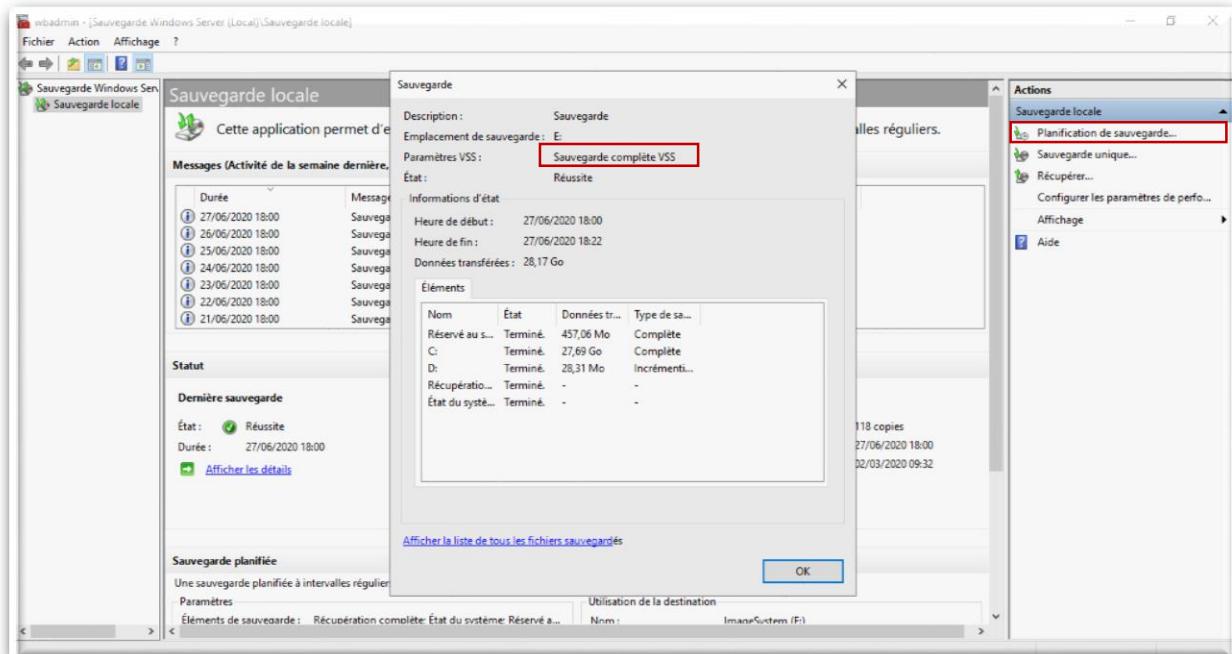


Maintenant on a fait une sauvegarde des données modifiable (sauvegarde différentielle), alors il ne reste une sauvegarde complète du l'état de système.

Une fois l'installation de la fonctionnalité « Sauvegarde Windows Server » réussie, nous pouvons lancer l'utilitaire de gestion des sauvegardes Windows à partir du menu « Outils » du « Gestionnaire de Serveur ».

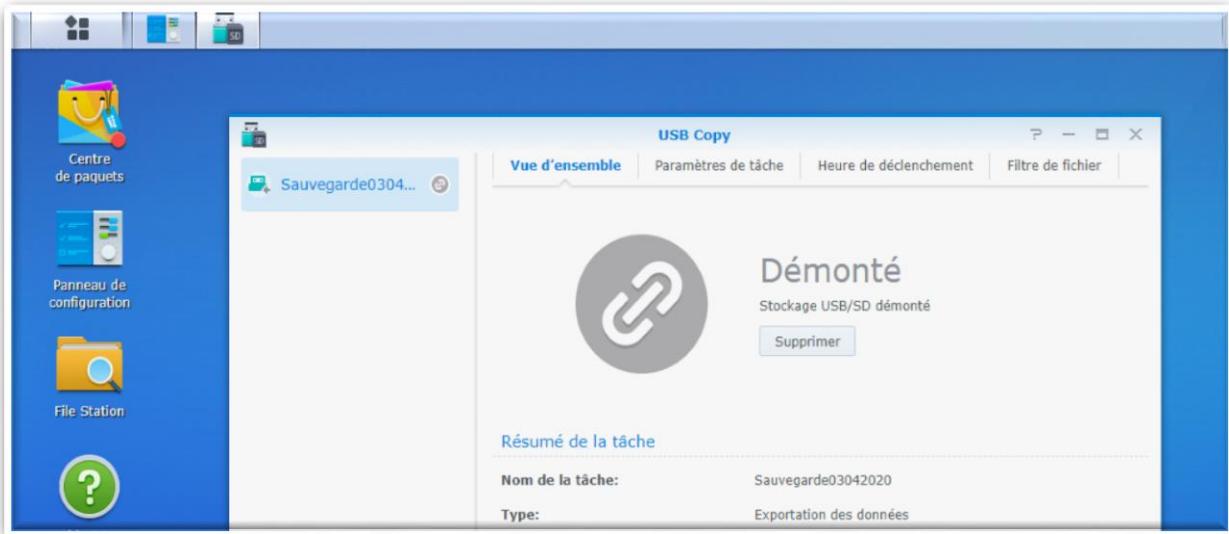
L'utilitaire de « Sauvegarde Windows Server », nous permet de créer des sauvegarde, les gérer, et récupérer des fichiers ou l'état du système.

Il nous permet aussi de planifier des sauvegardes complètes du serveur, ou en choisissant l'options serveur complète (Sauvegarde toutes les données et applications présentes sur le serveur ainsi que l'état du système).



La stratégie offline « manuelle »

On a utilisé USB copy, il s'agit d'un programme de NAS, qui effectuera une sauvegarde différentielle, elle nous aide à copier des fichiers entre Synology NAS et le disque dur Externe qui connecte au système informatique au temps de la sauvegarde seulement.



Puis, il ne reste une sauvegarde unique, qui permet de faire une sauvegarde à l'instant T. Elle s'effectue donc dès que nous l'avons paramétrée.



Enfin nous aurons un historique des sauvegardes dans la partie centrale de l'application. Nous saurons alors si la sauvegarde s'est correctement déroulée ou non. Si nous double-cliquons sur une sauvegarde, nous aurons plus d'informations et une description sur tous les sauvegarde qui nous avons planifié.

Fichier Action Affichage ?

Sauvegarde Windows Server Sauvegarde locale

Sauvegarde locale

Cette application permet d'effectuer une sauvegarde ponctuelle ou de planifier une sauvegarde à intervalles réguliers.

Messages (Activité de la semaine dernière, double-cliquez sur le message pour voir les détails)

Durée	Message	Description
27/06/2020 18:00	Sauvegarde	Réussite
26/06/2020 18:00	Sauvegarde	Réussite
25/06/2020 18:00	Sauvegarde	Réussite
24/06/2020 18:00	Sauvegarde	Réussite
23/06/2020 18:00	Sauvegarde	Réussite
22/06/2020 18:00	Sauvegarde	Réussite
21/06/2020 18:00	Sauvegarde	Réussite

Statut

Dernière sauvegarde	Prochaine sauvegarde	Toutes les sauvegardes
État : ✓ Réussite Durée : 27/06/2020 18:00 Afficher les détails	État : Planifiée Durée : 28/06/2020 18:00 Afficher les détails	Total des sauvegardes : 118 copies Copie la plus récente : 27/06/2020 18:00 Copie la plus ancienne : 02/03/2020 09:32 Afficher les détails

Sauvegarde planifiée

Une sauvegarde planifiée à intervalles réguliers est configurée pour ce serveur.

-Paramètres Utilisation de la destination

Actions

- Sauvegarde locale
 - Planification de sauvegarde...
 - Sauvegarde unique...
 - Récupérer...
- Configurer les paramètres de performance
- Affichage
- Aide

CONCLUSION

Nous avons tout au long de notre travail mis en place un système sécurisé avec authentification tout en restant compatible avec les différentes technologies existantes.

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau filaire ou non filaire, aucune entreprise ne peut prétendre vouloir mettre en place une infrastructure réseau, quel que soit sa taille, sans envisager une politique de sécurité.

Nous avons enfin structuré notre travail en trois chapitres :

Vue globale sur la sécurité réseau qui a parlé sur la sécurité réseau en générale, les mécanismes de protection et quelques protocoles de sécurité.

Une étude théorique qui concerne brièvement la description de la société et solution trouvé pour sécuriser le système informatique.

Dans ce chapitre nous avons eu une vue d'ensemble claire sur l'intégralité d'active directory qui offre des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels.

Pour terminer, nous tenons à souligner que nous n'avons nullement pas la prétention d'avoir présenté un travail parfait, car aucun travail scientifique ne peut l'être, ainsi nous laissons le soin à tous ceux qui nous liront et qui sont du domaine de nous parvenir leurs remarques et suggestions pour l'enrichir et l'améliorer.

BIBLIOGRAPHIE

- [https://www.erickscottjohnson.com/blog/pfsense-part-3-allowing-and-blocking-individual-websites.](https://www.erickscottjohnson.com/blog/pfsense-part-3-allowing-and-blocking-individual-websites)
- https://www.synology.com/fr/knowledgebase/DSM/help/DSM/Tutorial/backup_from_computer@ps
- <https://www.supinfo.com/articles/single/2629-architecture-configuration-dfs>
- <https://www.pandasecurity.com/france/mediacenter/malware/attaques-informatiques-courantes/>
- <https://www.supinfo.com/articles/single/2744-gpo-strategie-mot-passe-avec-active-directory>