



COURS D'ADMINISTRATION DES RÉSEAUX INFORMATIQUES

Raphael Grevisse Yende

► To cite this version:

| Raphael Grevisse Yende. COURS D'ADMINISTRATION DES RÉSEAUX INFORMATIQUES. Licence. BENI (RDC), Congo-Kinshasa. 2019, pp.108. cel-01995184

HAL Id: cel-01995184

<https://hal.science/cel-01995184>

Submitted on 25 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

COURS D'ADMINISTRATION DES RESEAUX INFORMATIQUES



YENDE RAPHAEL Grevisse, Ph.D.

Docteur en Télécoms et Réseaux Inf.

A handwritten signature in blue ink that reads "Dr. Raphael Grevisse, Ph.D." The signature is fluid and cursive, with "Dr." and "Ph.D." written in a larger, more formal script.

**Cours dispensé à l'Institut Supérieur du Bassin du Nil
en troisième graduat RMI.**

©YENDE R.G., 2019

AVERTISSEMENTS

Le support de cours d'«*Administration des réseaux informatiques* », demande avant tout, un certain entendement de l'informatique et des connaissances de base des réseaux informatiques et principalement une prédisposition d'analyse inéluctable et cartésienne. Vu que l'apport de ce cours, met l'accent sur les concepts de base des systèmes d'administration réseau reposant sur une compréhension technique approfondie de la gestion des réseaux informatiques et leurs modes de communication modernes. Le cours d'administration se veut pour objectif primordial de donner aux étudiants de G3 Gestion Informatique, les facilités d'appréhender les modes de fonctionnement des réseaux de télégestions, aux concepts des réseaux informatiques, aux architectures et à l'utilisation de systèmes de transmission.

Ce support de cours est soumis aux droits d'auteur et n'appartient donc pas au domaine public. Sa reproduction est cependant autorisée à condition de respecter les conditions suivantes :

- * Si ce document est reproduit pour les besoins personnels du reproducteur, toute forme de reproduction (*totale ou partielle*) est autorisée à la condition de citer l'auteur.
- * Si ce document est reproduit dans le but d'être distribué à des tierces personnes, il devra être reproduit dans son intégralité sans aucune modification. Cette notice de copyright devra donc être présente. De plus, il ne devra pas être vendu.
- * Cependant, dans le seul cas d'un enseignement gratuit, une participation aux frais de reproduction pourra être demandée, mais elle ne pourra être supérieure au prix du papier et de l'encre composant le document.

Copyright © 2019 Dr. YENDE RAPHAEL; all rights reserved. Toute reproduction sortant du cadre précisé est prohibée.

A handwritten signature in blue ink, appearing to read "Dr. Raphaelyg. PhD".

TABLE DES MATIERES

AVERTISSEMENTS.....	1
TABLE DES MATIERES.....	2
BIBLIOGRAPHIE.....	4
INTRODUCTION.....	5
DEFINITION DES CONCEPTS CLES	6
OBJECTIFS DU COURS.....	7
PREMIER CHAPITRE - INTRODUCTION A L'ADMINISTRATION DES RESEAUX INFORMATIQUES	8
I.1. DEFINITION ET FINALITES	8
I.2. TYPOLOGIE DE L'ADMINISTRATION DES RESEAUX INFORMATIQUES.....	11
I.2.1. L'ADMINISTRATION DES UTILISATEURS (CONSOmmATEUR DE SERVICE).....	11
I.2.2. L'ADMINISTRATION DES SERVEURS (OU FOURNISSEUR DE SERVICE)	12
I.2.3. L'ADMINISTRATION DE LA MACHINE DE TRANSPORT	12
I.3. ATTENTES D'UNE ADMINISTRATION DES RESEAUX INFORMATIQUES	13
I.4. LES ROLES D'UN ADMINISTRATEUR DES RESEAUX INFORMATIQUES	15
I.5. NIVEAUX DE DECISIONS DE L'ADMINISTRATION DES RESEAUX	15
DEUXIEME CHAPITRE - LA SUPERVISION DES RESEAUX INFORMATIQUES	17
II.1. MODELES DE L'ADMINISTRATION DES RESEAUX SELON OSI	18
II.1.1. LE MODELE ORGANISATIONNEL	18
A. LA GESTION DU SYSTEME	18
B. LA GESTION DE COUCHE	20
C. OPERATIONS DE COUCHES	20
II.1.2. LE MODELE INFORMATIONNEL	20
II.1.3. LE MODELE FONCTIONNEL.....	21
II.2. MODELES DE L'ADMINISTRATION DES RESEAUX SELON TCP/IP	24
Les MIB (Management Information Base).....	25
II.3. LES LOGICIELS DE SUPERVISION RESEAUX INFORMATIQUES	27
II.3.1. LA GESTION DE RESEAU AVEC SNMP	27
II.2.2. LES LOGICIELS DE SUPERVISION « OPEN SOURCE »	30

A. LE LOGICIEL NAGIOS	31
B. LE LOGICIEL CACTI	33
C. LE LOGICIEL CENTREON.....	35
II.3.2. LES LOGICIELS DE SUPERVISION « PROPRIETAIRES »	37
A. LE LOGICIEL HP –OPENVIEW	37
B. LE LOGICIEL PRTG NETWORK MONITOR	38
C. LE LOGICIEL MEMO GUARD	39
II.4. LES PLATES-FORMES D'ADMINISTRATION DES RESEAUX INFORMATIQUES	40
A. LES OUTILS D'ADMINISTRATION DES COUCHES BASSES	40
B. LES HYPERVISEURS	40
C. LES SYSTEMES INTEGRES AU SYSTEME D'EXPLOITATION	40
TROISIEME CHAPITRE – INSTALLATION ET CONFIGURATION D'UN SYSTEME WINDOWS SERVER « 2012 R₂ ».....	41
III.1. PREREQUIS TECHNIQUES	41
III.2. INSTALLATION DE WINDOWS SERVER 2012 R2	41
III.3. CONFIGURATION DE WINDOWS SERVER 2012 R2	46
III.3.1. CONFIGURATION ETAPE 1 : PARAMETRES DE BASE.....	46
III.3.2. CONFIGURATION ETAPE 2 : PARAMETRES AVANCES	50
A. CRÉATION D'UN COMPTE UTILISATEUR	50
B. SAUVEGARDE DU SERVEUR	54
C. CRÉATION DU PARTAGE RÉSEAU.....	59
D. CONFIGURATION DE L'ACCÈS DISTANT	61
QUATRIEME CHAPITRE – VUE D'ENSEMBLE DE L'ADMINISTRATION DE MICROSOFT WINDOWS SERVER 2012 R₂,.....	69
IV. 1. INSTALLATION DU « ACTIVE DIRECTORY ».....	69
IV. 2. INSTALLATION DU SERVEUR DNS.....	74
IV.3. INSTALLATION DU SERVEUR DHCP	84
IV.4. INSTALLATION DU SERVICE SNMP	93
IV.5. INSTALLATION DU SERVICE DFS	101
CONCLUSION	107

BIBLIOGRAPHIE

- **Alain WIARD, Jean-Marc LEDUC**, « *Les réseaux locaux faciles* », Marabout, novembre 1994, 235p,
- **Andrew S. TANENBAUM**, “*Computer Networks, 3rd edition*” (traduction française 1998) Prentice Hall, avril 1996, 813p
- **Danièle DROMARD, Fetah OUZZANI, Dominique SERET**, « *l'administration des Réseaux informatiques. Cours et exercices. De la transmission de données à l'accès au réseau. Tome 1*» Eyrolles, mars 1995, 329p,
- **Eric HARTMANN et Frederic HINGRAY**, “*Administration de réseaux locaux*”, Addison-Wesley, août 1994, 390p,
- **GALACSI**, « *Comprendre les systèmes d'information : exercices corrigés d'analyse et de conception* », Dunod, 1985
- **Gérard MOURIER**, « *L'indispensable pour l'administration des réseaux locaux, l'essentiel pour bien débuter* », Marabout, janvier 1996, 658p,
- **James F. KUROSE, et Keith W. ROSS**; “*Computer Networking: A Top-Down Approach*”, 5th Edition, Addison-Wesley, 2008, ISBN 013-607967-9
- **Jean-Luc MONTAGNIER**, « *Pratique des réseaux d'entreprise - Du câblage à l'administration - Du réseau local aux réseaux télécom* » Eyrolles, juillet 1996, 482p.
- **Laurent BLOCH et Christophe WOLFHUGEL**, *Sécurité informatique. Principes et méthode à l'usage des DSI, RSSI et administrateurs*, 2e édition, Eyrolles, Paris, 2009.
- **Nicolas Ochoa**, « *Le principe de libre-circulation de l'information - Recherche sur les fondements juridiques d'Internet* », HALSHS, 2016.
- **Pierre ROLIN, Gilbert MARTINEAU, Laurent TOUTAIN, Alain LEROY**, « *l'administration des réseaux : principes fondamentaux* », Hermès, décembre 1996, 574p.
- **William R. Stanek**, « *Microsoft® Windows Server 2012 : Guide de l'Administrateur* », 5th Edition, Addison-Wesley, 2008, ISBN 013-607967-9;

INTRODUCTION

L'administration réseau, de même que l'administration système d'ailleurs, est une discipline qui ne s'enseigne pas. Ceci peut paraître paradoxal puisque ce document est le support d'un cours d'administration réseau, justement. Relativisons les choses, si l'administration réseau ne s'enseigne pas, en revanche, elle s'apprend et le but de ce cours est de donner aux élèves un minimum d'éléments leur permettant par la suite d'orienter leur apprentissage dans la bonne direction.

Pourquoi l'administration réseau ne s'enseigne-t-elle donc pas ? Tout d'abord, parce c'est un domaine bien trop vaste et qui évolue trop rapidement pour que quiconque puisse le dominer de la tête et des épaules. De plus, le nombre de matériels et de logiciels est trop important pour qu'on puisse en faire une étude sérieuse. De toute façon, chaque entreprise a fait ses choix dans ce domaine et les jeunes ingénieurs auront généralement à s'y plier. Ce cours ne se veut donc pas exhaustif. En particulier, nous n'aborderons pas du tout la configuration des équipements actifs (*routeurs, commutateurs, etc.*). Celle-ci nécessiterait un cours entier à elle seule et obligerait à faire un choix partial pour tel ou tel constructeur.

Le but d'un réseau informatique est d'assurer le transport des données de manière automatique. Il faut donc tendre vers les 100 % de disponibilité et arriver à minimiser l'impact des incidents et les interventions d'urgence par :

- Les protocoles palliant aux incidents (OSPF, RIP, VRRP) ;
- Les protocoles permettant une gestion centralisée (DHCP, LDAP) ;
- Les matériels redondants ;
- Les matériels de secours ;
- Le système de surveillance.

En revanche, dans ce cours, nous essaierons de dégager des principes généraux sur la bonne façon d'administrer un réseau. Le champ d'application étant plutôt étendu, nous nous limiterons à quelques technologies fondamentales, applicables aux réseaux IP dans l'environnement OSI et TCP/IP.

DEFINITION DES CONCEPTS CLES

- **Adresse mac** : Adresse physique d'une interface réseau fixée par le constructeur qui permet d'identifier de façon unique une machine sur un réseau local.
- **Agent** : Elément logiciel embarqué dans un élément actif du réseau permettant sa gestion par une station de supervision.
- **Alerte** : Signal qui prévient d'un incident.
- **Authentification** : Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel.
- **Evénement**: Signal qui permet, par ses différents états, d'indiquer la situation ou l'évolution d'une partie d'un système.
- **Interface** : Ensemble de moyens permettant la connexion et l'interrelation entre le matériel, le logiciel et l'utilisateur.
- **IP** : Protocole de télécommunications utilisé sur les réseaux qui servent de support à Internet, qui permet de découper l'information à transmettre en paquets, d'adresser les différents paquets, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée.
- **Manager** : Station de gestion de réseau.
- **Ping** : Commande issue du monde Unix qui permet de mesurer le temps de réponse d'une machine à une autre sur un réseau.
- **Port** : Dans une architecture client-serveur, connexion virtuelle permettant d'acheminer les informations directement dans le logiciel d'application approprié de l'ordinateur distant.
- **Requête**: Ensemble de commandes dont l'exécution permet d'obtenir un résultat.
- **Routage** : Détermination par des routeurs du chemin que doit emprunter une information sur un réseau afin de parvenir à sa destination dans les meilleures conditions possibles.
- **Supervision** : Surveillance de l'état d'un réseau et de ses composants.

OBJECTIFS DU COURS

L'objectif général de ce cours est d'initier les étudiants aux concepts communs d'administration réseaux en mettant en place les services réseaux associées afin de sa gestion active. Et d'une manière spécifique :

- Comprendre les différentes configurations et gestion d'un parc informatique ;
- Optimiser la gestion des services des systèmes informatiques ;
- Permettre le déploiement automatique des nouvelles machines connectées sur un réseau informatique ;
- Connaitre et comprendre le mode de fonctionnement des protocoles applicatifs du réseau et savoir mettre en place les services associés des réseaux informatiques ;
- Permettre d'acquérir les différentes compétences sur les éléments techniques indispensables permettant d'effectuer des choix éclairés d'architectures et protocoles en fonctions des besoins à satisfaire et des problèmes à résoudre.

YENDE RAPHAEL Grevisse, PhD.

Professeur associé

PREMIER CHAPITRE - INTRODUCTION A L'ADMINISTRATION DES RESEAUX INFORMATIQUES

I.1. DEFINITION ET FINALITES

L'administration de réseaux informatique (*ou Network management*) se réfère aux activités, méthodes, procédures comme la surveillance du réseau et aux outils de mise en œuvre par l'administrateur réseaux ayant trait à l'exploitation, l'administration, la maintenance et la fourniture des réseaux informatiques. La gestion des réseaux informatiques constitue un problème dont l'enjeu est de garantir au meilleur coût, non seulement la qualité du service rendu aux utilisateurs mais aussi la réactivité dû aux changements et à l'évolution rapide du secteur informatique.

Cette gestion des réseaux se définit comme étant l'ensemble des moyens mis en œuvre (*connaissances, techniques, méthodes, outils, ...*) pour superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût, de qualité et de matériel. La qualité de service se décline sur plusieurs critères pour le futur utilisateur, notamment la disponibilité, la performance (temps de réponse), la fiabilité, la sécurité... L'administration des réseaux est couramment classée en trois activités :

1. La Supervision

La supervision consiste à surveiller les systèmes et à récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes. Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état des réseaux afin d'éviter un arrêt prolongé de celui-ci. La supervision doit permettre d'anticiper les problèmes et de faire remonter les informations sur l'état des équipements et des logiciels.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils adéquats. Une grande majorité des logiciels de supervision sont basés sur *le protocole SNMP* qui existe depuis de nombreuses années. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information ;
- Visualiser l'architecture du système ;
- Analyser les problèmes ;
- Déclencher des alertes en cas de problèmes ;
- Effectuer des actions en fonction des alertes ;
- Réduire les attaques entrantes.

La tâche de *l'administrateur* est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée.

2. l'Administration

L'administration désigne plus spécifiquement les opérations de contrôle du réseau avec la gestion des configurations et de sécurité. De façon générale, une administration de réseaux a pour objectif d'englober un ensemble de techniques de gestion mises en œuvre pour :

- Offrir aux utilisateurs une certaine qualité de service;
- Permettre l'évolution du système en incluant de nouvelles fonctionnalités;
- Rendre opérationnel un système ;

3. l'Exploitation

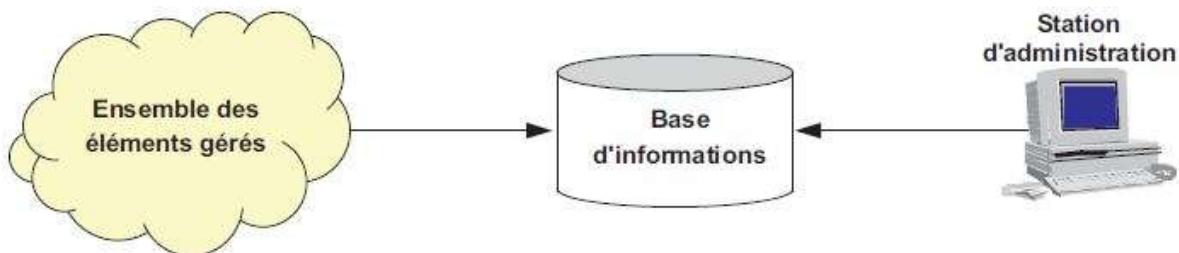
De nos jours, les systèmes d'exploitation à savoir les systèmes UNIX, MacOs et Windows gèrent tous l'aspect de l'exploitation des réseaux, les procédures, et les fonctions associés. Un système d'administration réseau est une collection d'outils pour la supervision et le contrôle du réseau qui sont intégrés dans le sens qu'ils impliquent :

- *Une interface opérateur unique avec un puissant, mais convivial ensemble de commandes* pour exécuter toutes les tâches d'administration réseau ;
- *Un nombre minimal d'équipements séparés* qui sont le plus souvent des composants matériels et logiciels requis pour l'administration réseau, et incorporés dans les équipements utilisateurs existants.

Les objectifs (*les finalités*) de l'administration des réseaux pour un administrateur :

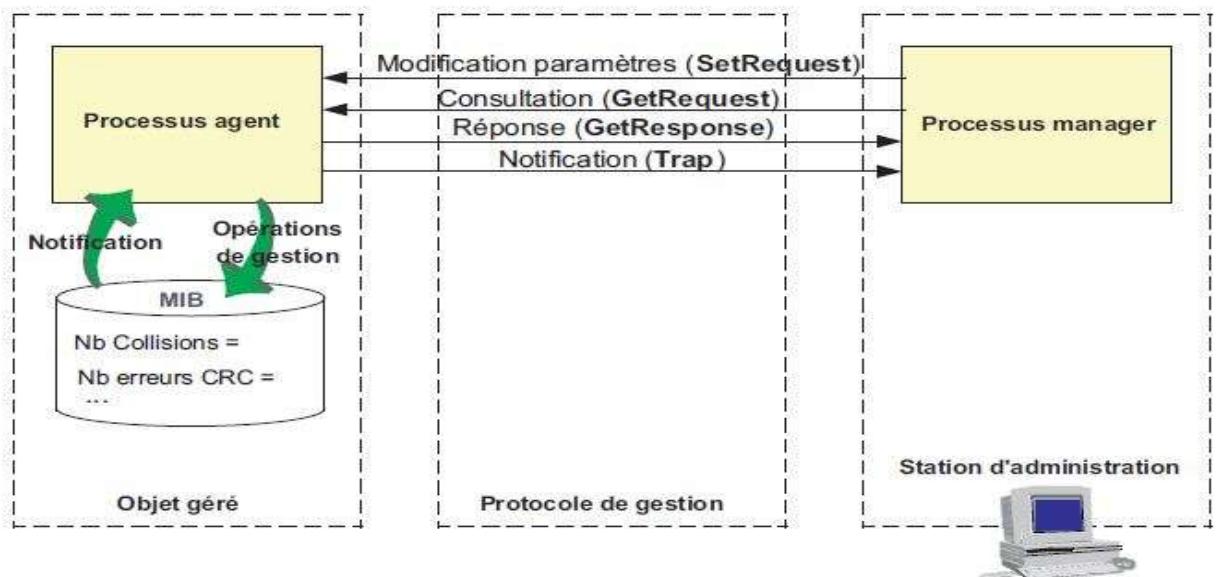
- Supervision du fonctionnement des réseaux ;
- Optimisation pour l'utilisation des ressources ;
- Détection et prévision des erreurs ;
- Signalisation des pannes ;
- Calculs de facturations à l'utilisation des ressources ;
- Le support technique pour utilisateurs.

L'administration d'un réseau suppose l'existence d'un système d'information décrivant le réseau de l'entreprise et recensant toutes les données et événements relatifs à chaque constituant du réseau administré.



Principe générale d'un système d'administration des réseaux

Un réseau comporte un grand nombre de composants (*objets*) que le système d'administration surveille. Dans chaque objet, un programme en tâche de fond (*Daemon*) transmet régulièrement, ou sur sollicitation, les informations relatives à son état.



Structure fonctionnelle d'un système d'administration.

I.2. TYPOLOGIE DE L'ADMINISTRATION DES RESEAUX INFORMATIQUES

L'administration des réseaux informatiques peut se décomposer en trois types d'administration :



I.2.1. L'ADMINISTRATION DES UTILISATEURS (CONSOMMATEUR DE SERVICE)

L'administration des utilisateurs fournit l'ensemble des mécanismes nécessaires pour une personne afin d'utiliser le réseau, à savoir :

- *Accessibilité et Connectivité aux applications* : l'utilisateur doit pouvoir se connecter aux différentes applications fournies par le réseau et doit disposer d'un ensemble d'outils lui assurant une certaine transparence au niveau des méthodes d'accès et connexions aux applications;
- *L'accès aux serveurs de noms* : afin de permettre la localisation des ressources et d'assurer à l'utilisateur l'existence et l'utilisation de ces ressources.
- *La Confidentialité et la Sécurité* : Le système doit fournir l'ensemble des mécanismes qui permettent de garantir la confidentialité des informations de l'utilisateur, de sécuriser son environnement et de prévenir toute perte ou altération des échanges effectués par l'utilisateur.
- *La Qualité de service fournit à l'utilisateur* : Il s'agit principalement de la disponibilité et des performances du système et sa capacité à assurer le service attendu.

I.2.2. L'ADMINISTRATION DES SERVEURS (OU FOURNISSEUR DE SERVICE)

L'administration des serveurs fournit tous les mécanismes suivant :

- *La Connexion et la Distribution des applications sur tout le réseau* : afin de permettre la relation entre les différents services;
- *La Gestion et la Distribution des données* : comme pour les utilisateurs, doivent garantir la fiabilité de transmission des informations et offrir des outils permettant le transfert de ces informations. C'est le rôle des outils de transfert de fichiers, qui permettent le partage des capacités de stockage entre plusieurs systèmes;
- *la Gestion des applications* : est essentiellement lié au contrôle et à la protection des accès de ces applications par la distribution de droits, et de différents protocoles de contrôle d'utilisation de ressources concernant les applications utilisées.

I.2.3. L'ADMINISTRATION DE LA MACHINE DE TRANSPORT

L'administration de la machine de transport consiste à fournir :

- *les opérations de réseau*, dont le rôle est de permettre l'intervention sur le fonctionnement et la modification du réseau;
- *la liste des incidents réseaux par la mise en place de protocoles de détection et de correction* : Lorsqu'une alerte est déclenchée, des actions vont être prises pour résoudre l'incident et de ce fait, réduire son influence et ses perturbations sur l'ensemble du réseau;
- *les performances fournies par le réseau*, le but est d'afficher et d'évaluer le système par un ensemble de paramètres comme le temps de réponse ou la charge du système;
- *les coûts*, afin de pouvoir les mesurer (*dans un réseau, les coûts d'utilisation sont complexes à évaluer puisqu'ils concernent un ensemble de composants distribués*);

- *la configuration*, le but est de déterminer la meilleure configuration du réseau afin d'améliorer les performances du système et la qualité du service;
- *l'inventaire*, qui a pour rôle de tenir à jour en temps réel la liste des éléments logiciels et matériels qui constituent un réseau;
- *l'évolution et les changements*, l'objectif est de fournir les informations permettant de déterminer les nouveaux besoins et les parties du système concernées par ces besoins de changement.

I.3. ATTENTES D'UNE ADMINISTRATION DES RESEAUX INFORMATIQUES

Une attente de l'administration des réseaux informatiques peut être considérée comme les débouchés auxquels s'attendent les utilisateurs des réseaux informatiques. D'une façon générale, les attentes d'une administration réseau doivent permettre :

- l'extraction des informations des éléments du réseau au moyen d'outils d'un grand nombre d'informations ;
- la réduction du volume d'informations au moyen de filtres afin de sélectionner les informations significatives ;
- le stockage des informations retenues dans une base de données d'administration ;
- des traitements sur ces informations ;
- offrir des interfaces (*utilisateur d'administration administration, opérateur réseau*).

Avec l'apparition des nouvelles technologies et la diversification des types de réseaux comme la multiplication des mobiles connectés et le développement des solutions de *Cloud computing*, la gestion des solutions de sécurité réseau est devenue une tâche complexe. L'efficacité des réseaux dépend de la manière dont se font les échanges d'informations. Ces échanges sont effectués grâce à des mécanismes qui président comme les protocoles, ceux-ci représentent l'ensemble des règles décrivant la manière de faire transiter les informations sur un réseau. L'évaluation de la performance d'un réseau peut être effectuée de plusieurs façons et revient à mesurer la rapidité et la fiabilité d'une transmission de données.

L'évaluation de la performance d'un réseau grâce à la modélisation mathématique repose sur des calculs complexes et se déroule en plusieurs étapes. Il est cependant à noter que cet outil de mesure n'est valable que pour les réseaux d'une taille relativement réduite (*moins de trois liens*) car les calculs gagnent fortement en complexité au-delà de ce seuil :

- *Représentation du modèle* : Cette représentation graphique permettra de mettre en place les différentes équations nécessaires aux calculs suivants.
- *Calcul du taux de blocage* : Ce taux représente le pourcentage de clients qui n'ont pas pu accéder au réseau par manque de ressources. Plus ce taux est faible, meilleure est la performance du réseau.
- *Calcul du taux de congestion¹* : Ce taux représente la perte de paquets engendrée quand les demandes d'utilisation des ressources sont plus grandes que les capacités effectives de ces ressources. Plus ce taux est faible, meilleure est la performance du réseau.
- *Calcul du taux d'insatisfaction* : Ce taux représente le pourcentage de clients n'obtenant pas les ressources demandées. Une fois de plus, plus ce taux est faible, meilleure est la performance du réseau.
- *Calcul du débit moyen* : Le débit moyen représente la vitesse de transition des paquets sur le réseau en moyenne pour une durée donnée. Plus le débit moyen est élevé, meilleure est la performance du réseau.
- *Calcul du taux de perte* : Ce taux représente le pourcentage de paquets perdus lors de leur transition le réseau. Encore une fois, plus ce taux est faible, meilleure est la performance du réseau.
- *Comparaison des métriques* : Cette étape finale sert à représenter les différentes mesures sous forme de courbe sur un même graphique pour évaluer les différents critères sur lesquels agir en priorité pour améliorer la performance du réseau.

¹ La congestion d'un réseau, c'est quand un réseau a des ressources insuffisantes pour faire face à toutes les demandes de toutes les demandes de transfert qui lui sont adressées.

I.4. LES ROLES D'UN ADMINISTRATEUR DES RESEAUX INFORMATIQUES

L'administrateur réseau est responsable de ce qui peut se passer dans un réseau administré ; ainsi les rôles d'un administrateur réseau consiste à :

- Mettre en place et maintenir l'infrastructure du réseau (*organisation, ...*) ;
- Installer et maintenir les services nécessaires au fonctionnement du réseau ;
- Assurer la sécurité des données internes au réseau (*particulièrement face aux attaques extérieures*) ;
- S'assurer que les utilisateurs n'outrepassent pas leurs droits ;
- Gérer les « *logins* » (*i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...*) ;
- Gérer les systèmes de fichiers partagés et les maintenir.

I.5. NIVEAUX DE DECISIONS DE L'ADMINISTRATION DES RESEAUX INFORMATIQUES

Pour une bonne administration d'un réseau, un bon administrateur a besoin différents niveaux de la prise des décisions d'administration :

- **les décisions opérationnelles** : sont des décisions à court terme, concernant l'administration du réseau au jour le jour et, la tenue de l'opération se fait à temps réel sur le système ;
- **les décisions tactiques** : sont des décisions à moyen terme et concernent l'évolution du réseau et l'application du politique à long terme ;
- **les décisions stratégiques** : sont des décisions à long terme concernant les stratégies pour le futur en exprimant les nouveaux besoins et les désirs des utilisateurs.

Ces trois principaux niveaux déterminent alors différents degrés de l'administration des réseaux informatiques :

- la **prévoyance** : anticiper l'avenir et préparer l'organisation à s'adapter aux changements ;
- **l'organisation** : construire une structure, définir les responsabilités ou charges, sélectionner, entraîner les managers ;
- les **commandements** : qui administre quoi?;
- la **coordination** : mettre de l'harmonie, concilier les activités afin que les fonctions travaillent dans le même sens, à la réalisation de mêmes objectifs ;
- le **contrôle** : vérifier si les objectifs sont réalisés conformément aux ordres et aux principes.

Notons que dans le cas d'un système d'exploitation multiutilisateurs, comme Unix, la gestion du système et des utilisateurs est confié à un super-utilisateur² nommé « *root* » ou racine. Le rôle de l'administrateur (*root*) est :

- configurer le noyau du système d'exploitation ;
- sauvegarder les données et réparer les systèmes de fichiers ;
- gérer les utilisateurs ;
- installer de nouveaux logiciels ;
- intégrer des nouveaux disques et de nouvelles partitions ;
- configurer le processus de démarrage de Linux ou autre ;
- configurer le réseau.

²Du fait que les super utilisateurs possèdent tous les droits, il doit posséder des connaissances concernant le fonctionnement du système.

DEUXIEME CHAPITRE - LA SUPERVISION DES RESEAUX INFORMATIQUES

La supervision consiste à surveiller les systèmes et à récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes.

Le plus grand souci d'un administrateur est la panne. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état des réseaux afin d'éviter un arrêt prolongé de celui-ci. La supervision doit permettre d'anticiper les problèmes et de faire remonter les informations sur l'état des équipements et des logiciels.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils adéquats. Une grande majorité des logiciels de supervision sont basés sur *le protocole SNMP* qui existe depuis de nombreuses années. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales :

- Surveiller le système d'information ;
- Visualiser l'architecture du système ;
- Analyser les problèmes ;
- Déclencher des alertes en cas de problèmes ;
- Effectuer des actions en fonction des alertes ;
- Réduire les attaques entrantes.

La tâche de *l'administrateur* est alors simplifiée. Il n'a plus qu'à faire une vérification ou réaliser une action en fonction d'une alerte déclenchée.

II.1. MODELES DE L'ADMINISTRATION DES RESEAUX INFORMATIQUES SELON OSI

L'ISO ne spécifie aucun système d'administration des réseaux informatiques mais définit plutôt un cadre général avec le document ISO 7498-4 dénommé « *OSI Framework* » ou « *Cadre Architectural OSI* » et un aperçu général des opérations d'administration des systèmes avec le document ISO 1004 dénommé « *OSI System Management* » ou « *Système d'administration OSI* ». Ces documents de base décrivent trois modèles :

- Le Modèle organisationnel ;
- Le Modèle informationnel ;
- Le Modèle fonctionnel.

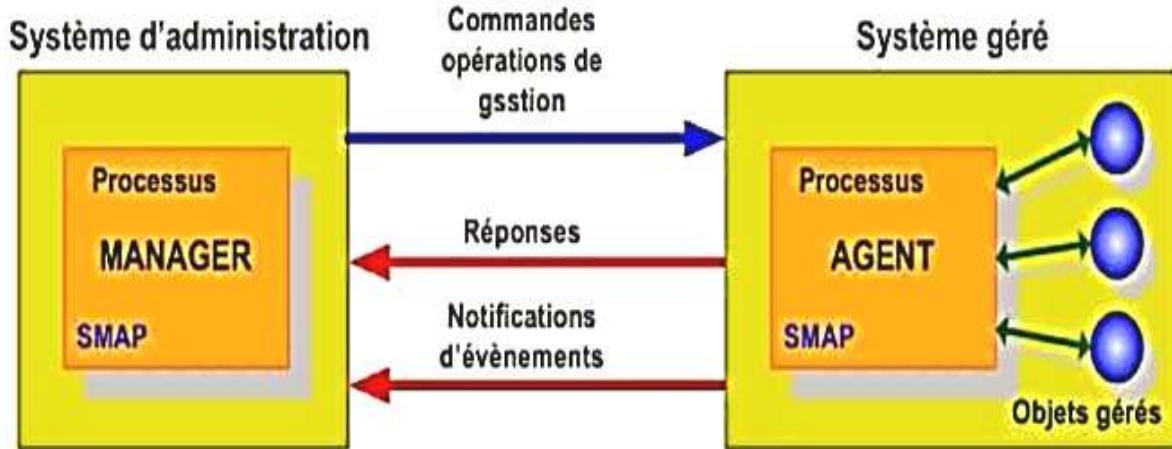
II.1.1. LE MODELE ORGANISATIONNEL

Le modèle organisationnel, aussi appelé ***modèle architectural*** (*Managed System and Agents (MSA)* ou *Système Administré et Agent*) : c'est un modèle qui organise l'administration OSI, définit la notion de systèmes administrés (Agents) et définit la notion du système Administrant (*DMAP* : *Distributed Management Application Processus*). Le modèle architectural définit trois types d'activité :

- La gestion du système (*System Management*) ;
- La gestion de couche (*Layer Management*) ;
- Les opérations de couche (*Layer Operations*).

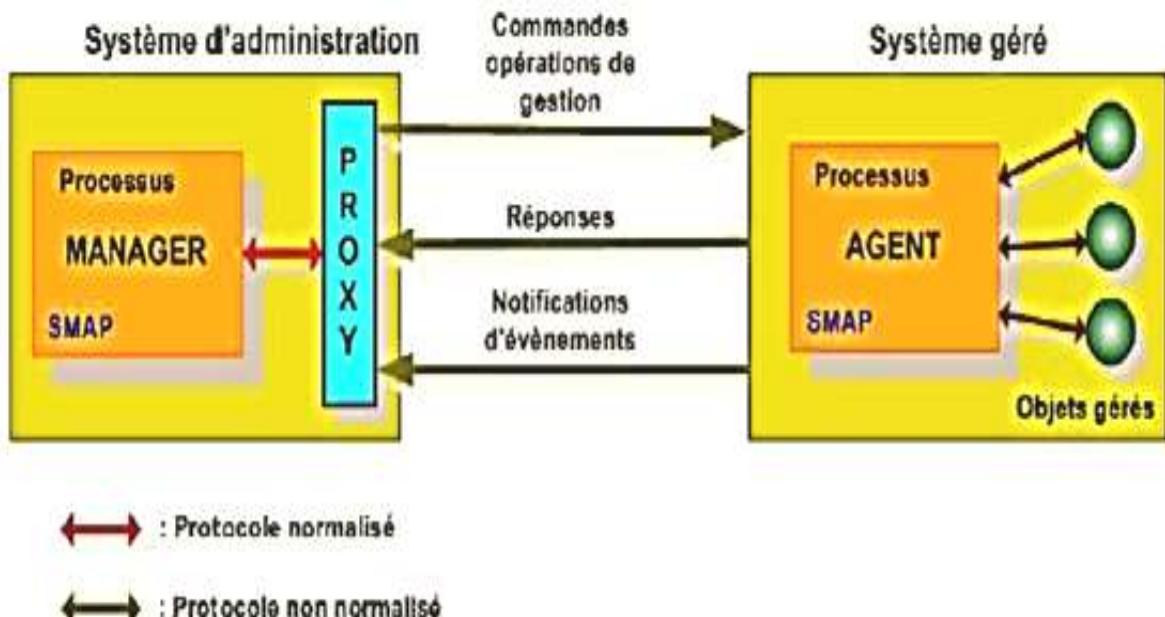
A. LA GESTION DU SYSTEME

La gestion du système (*SMAE* : *System Management Application Entity*) met en relation deux processus Manager et Agent. Le protocole standardisé de niveau application CMIP « *Common Management Information Protocol* » est utilisé. Le **Manager** envoie des messages de commandes à ses **Agents**; ceux-ci lui retournent les résultats des opérations effectuées dans des messages de réponses.



Modèle de Gestion Manager –Agent

Dans ce modèle, l'Agent n'utilise pas les mêmes normes ou la même syntaxe de communication que le Manager, une entité tierce appelée « **Proxy-Agent** » permet d'adapter le protocole de l'Agent et de convertir ses données au format du Manager. Le Proxy-Agent est situé soit au niveau de l'Agent, soit au niveau du Manager.



Modèle de Gestion Manager –Agent avec l'agent Proxy

B. LA GESTION DE COUCHE

La gestion de couche (ou *protocole de couche*), fournit les moyens de transfert des informations de gestion entre les sites administrés. C'est un dialogue horizontal (*CMIP*, *Common Management Information Protocol*, ISO 9596). Les opérations de couche (N), ou protocole de couche (N) supervisent une connexion de niveau N. Ces opérations utilisent les protocoles OSI classiques pour le transfert d'information. C'est par exemple : Le CMIP utilise les primitives de service suivantes (*CMISE* : *Common Management Information Service Element*) :

- ***Get*** : il est utilisé par le gérant pour lire la valeur d'un attribut ;
- ***Set*** : fixe la valeur d'un attribut ;
- ***Event*** : permet à un agent de signaler un événement ;
- ***Create*** : génère un nouvel objet ;
- ***Delete*** : permet à l'agent de supprimer un objet.

C. OPERATIONS DE COUCHES

Elles concernent les mécanismes mis en œuvre pour administrer l'unique instance d'une communication entre 2 entités homologues. Les opérations de couche N (*protocole de Couche N*) supervisent une connexion de niveau N en utilisant un certain nombre de primitive de service. Il s'agit d'un dialogue Vertical assuré par le **CMIS** (*Common Management Information Service*).

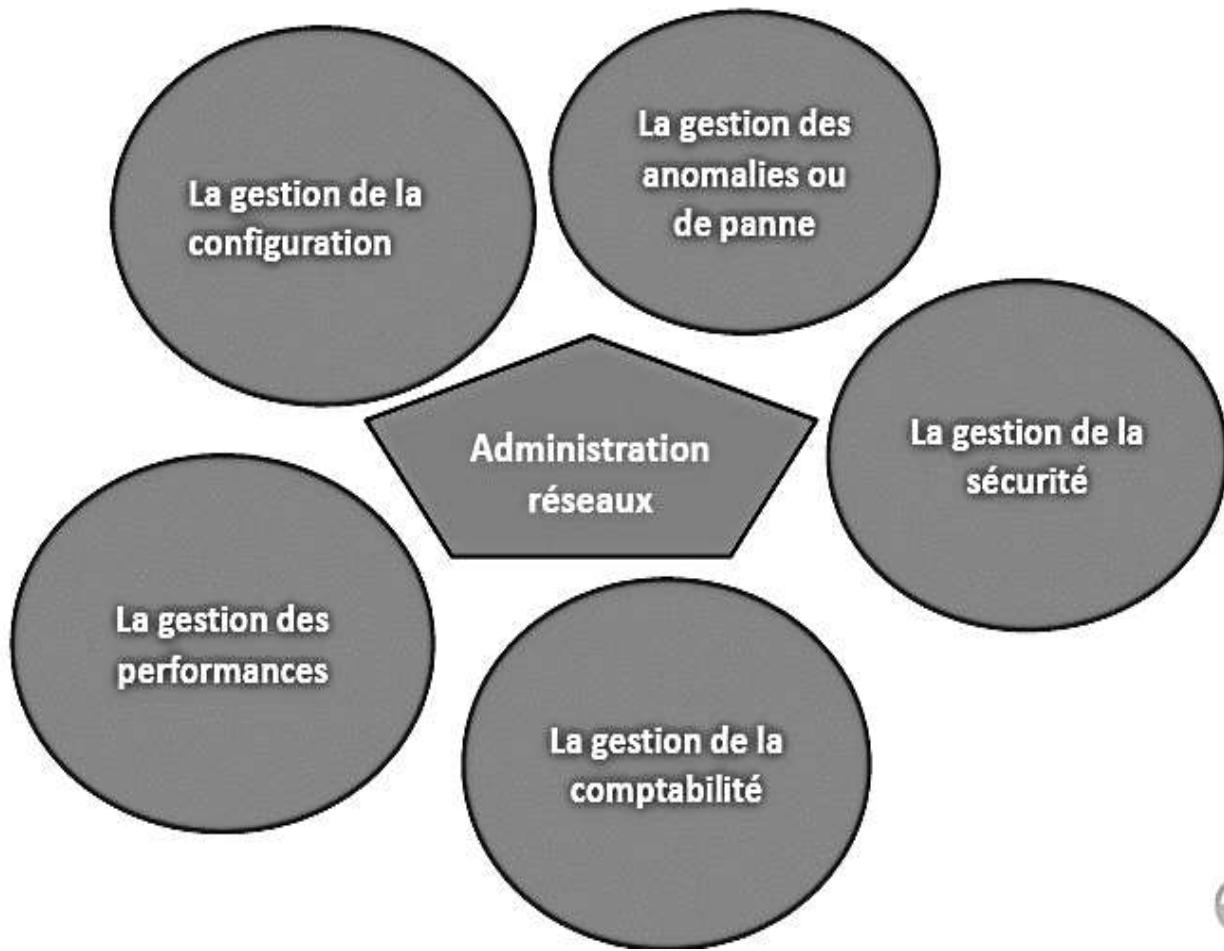
II.1.2. LE MODELE INFORMATIONNEL

Un modèle informationnel aussi appelé «*Management Information Base (MIB)*» ou «*Base de l'Information d'Administration*» est un modèle qui constitue la base de données des informations d'administration en énumérant les objets administrés et les informations s'y rapportant (*attributs*). L'ensemble des objets gérés constitue la MIB (ISO 10165). La MIB contient toutes les informations administratives sur les objets gérés (*ponts, routeurs, cartes, ...*). La norme ne spécifie aucune organisation particulière des données ; Seul, le processus agent a accès à la MIB et le processus manager accède aux données via le processus agent.

II.1.3. LE MODELE FONCTIONNEL

L'OSI a regroupé les activités d'administration en cinq groupes fonctionnels « *Specific Management Function Area (SMFA)* » ou « *Aire de Fonction d'Administration Spécifique* »:

- Gestion de configuration ;
- Gestion de performance ;
- Gestion de panne ;
- Gestion de comptabilité ;
- Gestion de sécurité.



Modèle de fonctionnel d'administration selon OSI

- ***La gestion des anomalies ou de panne (Fault Management)*** : elle a pour objectif de faire le diagnostic rapide de toute défaillance interne ou externe du système (*par exemple la panne d'un routeur*). Ces pannes peuvent être d'origine interne résultant d'un élément en panne ou d'origine externe dépendant de l'environnement du système (*coupure d'un lien publique*). Cette gestion implique :
 - La surveillance des alarmes (*filtre, report, ...*) ; il s'agit de surveiller le système et de détecter les défauts. On établit un taux d'erreurs et un seuil à ne pas dépasser.
 - Le traitement des anomalies ;
 - La localisation et le diagnostic des incidents (*séquences de tests*) la journalistique des problèmes, etc.
- ***La gestion de la configuration (Configuration Management)*** : elle a pour objectif d'identifier de manière unique chaque objet administré par un nom ou un identificateur d'objet (*OID : Object Identifier*). Il s'agit également de :
 - gérer la configuration matérielle et logicielle et ;
 - préciser la localisation géographique.
- ***La gestion des performances (Performance Management)*** : elle a pour objectif de contrôler, à évaluer la performance et l'efficacité des ressources comme le temps de réponse, le débit, le taux d'erreur par bit, la disponibilité (*aptitude à écouler du trafic et à répondre aux besoins de communication pour lequel la ressource a été mise en service*). Elle comprend :
 - la collecte d'informations, statistiques (*mesure du trafic, temps de réponse, taux d'erreurs, etc.*), le stockage et l'interprétation des mesures (*archivage des informations statistiques dans la MIB, calculs de charge du système, tenue et examen des journaux chronologiques de l'état du système*).
 - Elle est réalisée à l'aide d'outil de modélisation et simulation permettant d'évaluer l'impact d'une modification de l'un des paramètres du système.
- ***La gestion de la sécurité (Security Management)*** : Elle couvre tous les domaines de la sécurité afin d'assurer l'intégrité des informations traitées et des objets administrés. L'ISO a défini cinq services de sécurité :

- Les contrôles d'accès au réseau ;
- La confidentialité (*les données ne sont communiquées qu'aux personnes, ou processus autorisés*) ;
- L'intégrité (*les données n'ont pas été accidentellement ou volontairement modifiées ou détruites*) ;
- L'authentification (*l'entité participant à la communication est bien celle déclarée*) ;
- La non-répudiation (*impossibilité pour une entité de nier d'avoir participé à une transaction*).

Pour cela l'ISO utilise les mécanismes d'encryptage, l'authentification des extrémités (*source et destinataire*) et le contrôle des accès aux données. Notons également que c'est au niveau de la gestion de sécurité que l'on trouve la notion de configuration ***du serveur AAA***³ (*Authentification – Authorization – Accounting*).

- ***La gestion de la comptabilité (Accounting Management)*** : elle permet de connaître les charges des objets gérés, les coûts de la consommation... cette évaluation est établie en fonction du volume et la durée des transmissions. La gestion de la comptabilité comporte les tâches suivantes :

- la consommation réseau par abonné ;
- la définition des centres de coût ;
- la mesure des dépenses de structure (*coûts fixes*) et répartitions ;
- la mesure des consommations par services ;
- l'imputation des coûts.

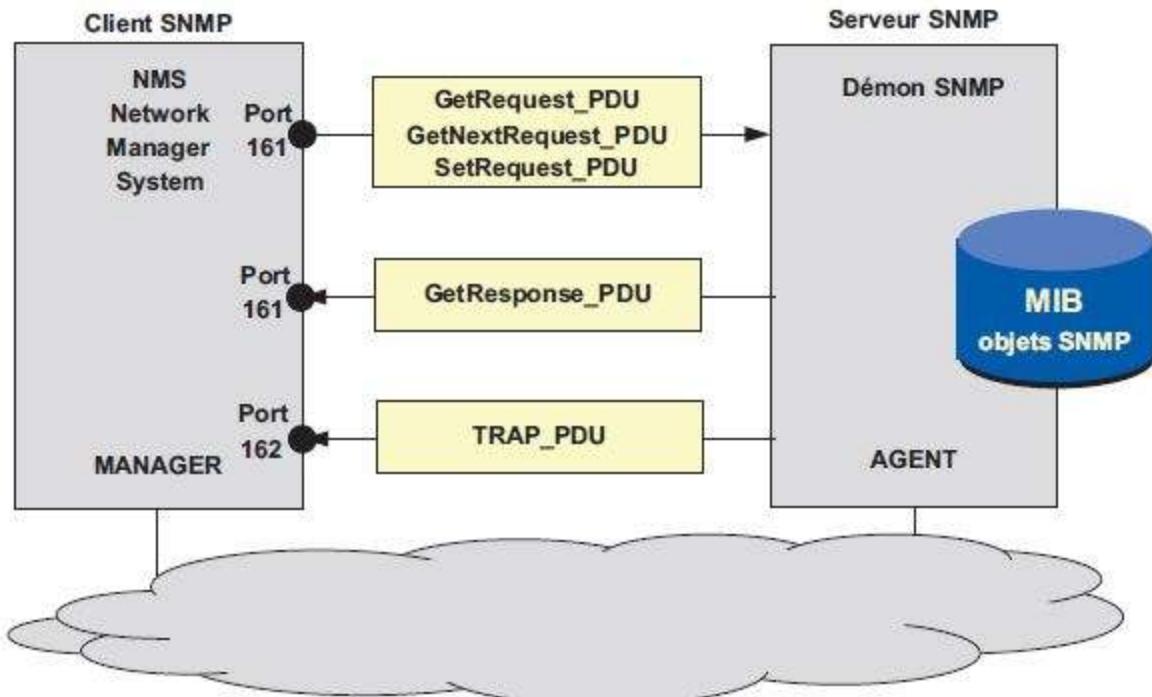
³ La configuration du serveur AAA consiste à une méthode de définition du cadre de référence pour l'utilisation sécurisée des ressources en réseau c'est-à-dire l'administrateur sera en mesure de connaître qui se connecte, et qui a le droit d'accéder à quoi et qui consomme quoi...

II.2. MODELES DE L'ADMINISTRATION DES RESEAUX INFORMATIQUES SELON TCP/IP

Le Standard de fait dans l'administration des réseaux TCP/IP, le protocole **SNMP** (*Simple Network Management Protocol*) est proche des concepts ISO. Cependant, non orienté objet SNMP confond la notion d'attribut et d'objet. Issu du protocole de gestion des passerelles IP (**SGMP**, *Simple Gateway Monitoring Protocol* – RFC 1028), SNMP est décrit dans la RFC 1157. Ce document est complété par de nombreuses RFC dont :

- les RFC 1155 qui spécifient comment les objets gérés sont représentés dans les bases d'informations (**SMI**, *Structure of Management Information*). SMI utilise la notation ASN1 (*Abstract Syntax Notation I*) ;
- les RFC 1156 et 1213 qui définissent les MIB (MIB I et MIB II). Les MIB décrivent les objets gérés (attributs ISO). Une MIB particulière (**RMON MIB**, *Remote Monitor Network MIB*) est spécifiée pour les réseaux locaux (Ethernet et Token Ring), les objets RMON sont implémentés dans des sondes d'analyse et de surveillance. Cependant en environnement commuté, les sondes RMON n'ont accès qu'aux segments sur lesquels elles sont installées.

Pour assurer un accès aux différents éléments des réseaux commutés, une sonde spécifique a été définie (RFC 2613, **SMON**, *Switched RMON*). Le SNMP spécifie les échanges entre la station d'administration et l'agent. S'appuyant sur UDP (*User Datagram Protocol*), SNMP est en mode non connecté. De ce fait, les alarmes (*trap*) ne sont pas confirmées. La plus grande résistance aux défaillances d'un réseau d'un protocole en mode datagrammes vis-à-vis d'un protocole en mode connecté ainsi que la rapidité des échanges justifient le choix d'UDP. Les messages SNMP permettent de lire la valeur (exemple : compteur de collisions) d'un objet administré (attribut d'ISO) (**GetRequest** et **GetNextRequest**), de modifier la valeur d'un objet (**SetRequest**). L'agent administré répond à ces sollicitations par le message **GetResponse**. Le message **Trap** est émis sur l'initiative de l'agent qui notifie ainsi, à l'administrateur, qu'une condition d'alarme a été détectée.



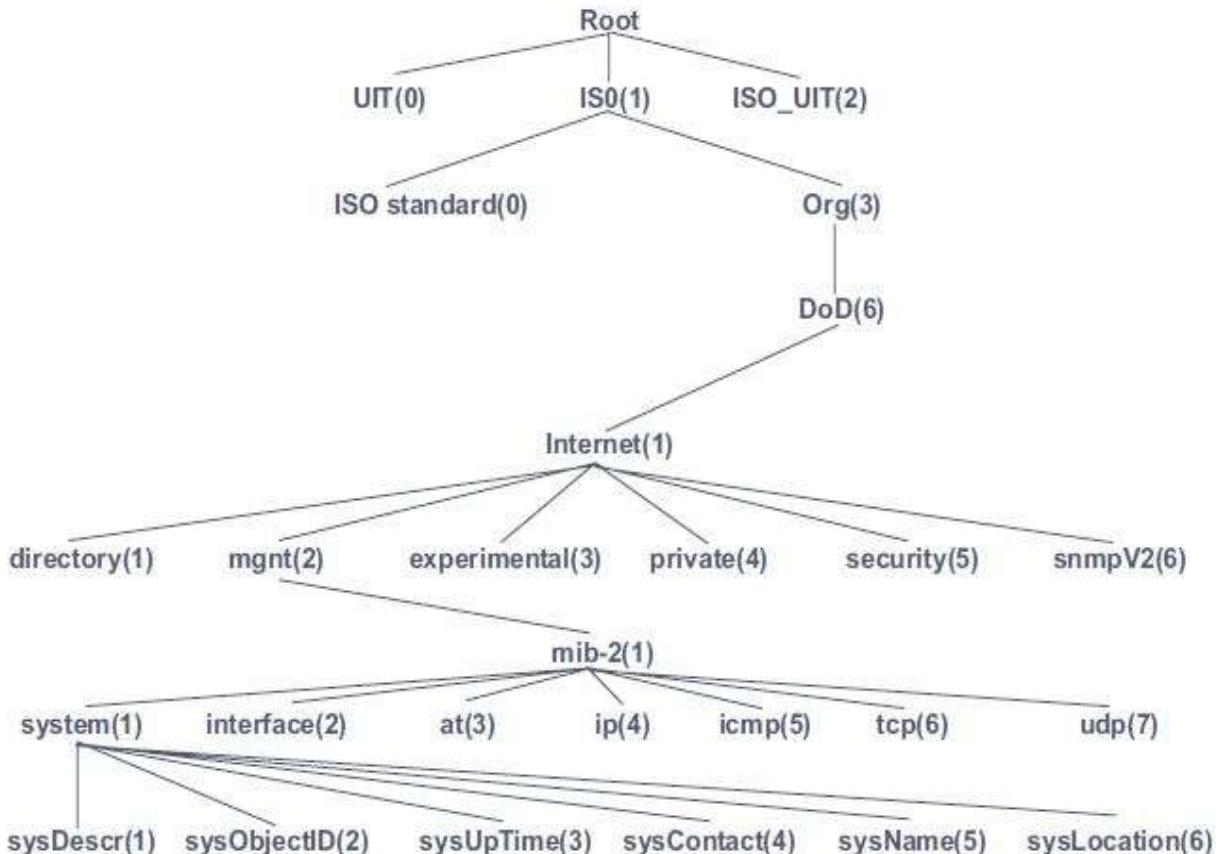
Principe d'administration des réseaux informatiques selon TCP/IP

Les MIB (Management Information Base)

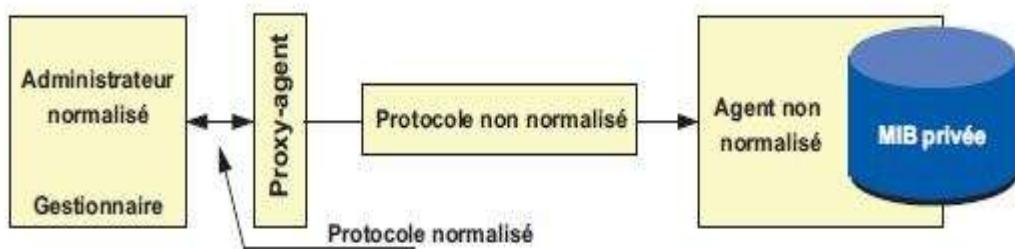
Les MIB décrivent les objets gérés, en définissent le nommage, ils en précisent le type, le format et les actions. Les différentes valeurs des objets ne sont pas contenues dans la MIB, mais dans des registres externes que l'agent vient consulter à la demande du manager. La RFC 1213 (MIB II) formalise une structure de définition des objets.

Ainsi, l'objet « *SysUpTime* » qui mesure le temps, en centième de seconde, depuis que l'agent a été réinitialisé, est de type *TimeTicks* (type de variable défini dans la SMI, *TimeTicks* mesure le temps en centièmes de seconde) et est accessible uniquement en lecture (*read_only*). Cet objet obligatoire (*mandatory*) est le troisième objet décrit dans la MIB system.

Les objets (variables) gérés par les MIB sont désignés selon une hiérarchie définie par l'ISO selon un arbre dit « *arbre de nommage* ». Dans l'arbre de la figure 18.7, chaque organisation de normalisation possède une entrée au premier niveau. Les différentes branches permettent de nommer un objet de manière unique. Les MIB standard établies par l'IETF appartiennent à la branche « *internet* » et sont classées dans la sous-branche mgmt(2).



Il sied également de signaler que l'accès aux variables des MIB dites privées est assuré par un agent spécifique qui effectue les conversions nécessaires : le **proxy-agent**. Le proxy-agent permet ainsi le dialogue entre deux systèmes d'administration différents. Le principe du proxy-agent est illustré ci-dessous. Celui-ci peut être localisé dans le serveur pour l'utilisation d'une MIB privée, ou dans le manager si l'agent serveur n'est pas conforme au standard (*conversion de protocole*).



II.3. LES LOGICIELS DE SUPERVISION RESEAUX INFORMATIQUES

II.3.1. LA GESTION DE RESEAU AVEC SNMP

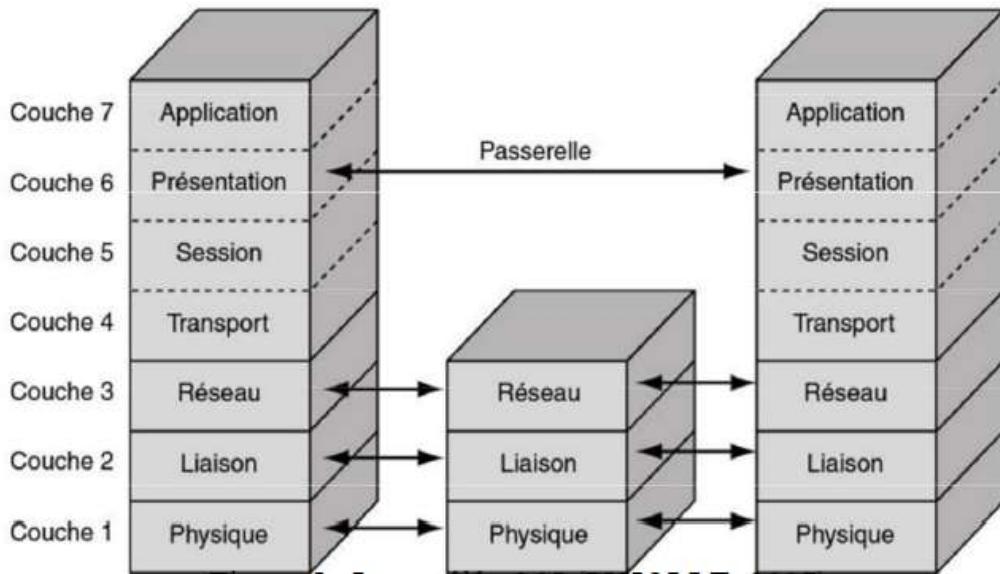
Le logiciel SNMP est né pour répondre aux difficultés de surveillance et de maintien des réseaux informatiques, un protocole d'administration, intitulé SNMPv1 (*Simple Network Management Protocol*) a été finalisé en 1990. Ce protocole permet :

- de modifier la configuration des équipements ;
- de détecter et d'analyser les problèmes du réseau par interrogation ou remontée d'alarmes ;
- de surveiller ses performances et ;
- de réaliser des statistiques.

Dans cette première version, le protocole est défini par un standard IETF (*Internet Engineering Task Force*) intitulé RFC 1157 (*Request For Comments*) « *A Simple Network Management Protocol (SNMP)* » datant de mai 1990. Le but de cette architecture est de faciliter son utilisation, d'être suffisamment extensible pour être compatible dans le futur et qu'elle soit indépendante de l'architecture et des mécanismes des hôtes ou serveurs particuliers. (*IETF, 1990*).

La sécurité de SNMPv1 est basée sur des noms de communautés qui sont utilisés comme des mots de passe pour accéder à une arborescence de données de l'équipement appelée MIB (*Management Information Base*). Le nom de la communauté est transmis en clair dans le message SNMP. La première version n'étant pas sécurisée, le protocole SNMP a ainsi évolué en une deuxième version finalisée en janvier 1996, intitulée SNMPv2C (*RFC 1901 à 1908*). La sécurité de cette version est encore faible car elle s'appuie sur le modèle de SNMPv1 en réutilisant les noms de communauté, d'où la lettre C de SNMPv2C. Cependant, elle comble des lacunes de la version 1, en particulier au niveau de la définition des objets, du traitement des notifications et du protocole lui-même. Une troisième version finale, intitulé SNMPv3, a été approuvée comme projet de norme en avril 1999. Elle est devenue un standard en décembre 2002 (*RFC 3410 à 3418*). Elle a pour but principal d'assurer la sécurité des échanges.

La technologie SNMP s'appuie sur le modèle OSI (*Open System Interconnection*). Ce modèle de communication mis en place par l'Organisation internationale de normalisation (*ISO : International Organization for Standardization*) comporte 7 couches (1 = *Physique*, 2 = *Liaison Données*, 3 = *Réseau*, 4 = *Transport*, 5 = *Session*, 6 = *Présentation* et 7 = *Application*). Le rôle du modèle OSI, décrit dans la norme ISO 7498-1, est de standardiser la communication entre les machines.



SNMP est un protocole situé entre la couche 4 et la couche 7 de ce modèle OSI. Il s'appuie sur le protocole de télécommunication UDP (*User Datagram Protocol*). Le paquet UDP est encapsulé dans un paquet IP (*Internet Protocol*). UDP est plus simple à utiliser que TCP (*Transmission Control Protocol*) car il fonctionne en mode non connecté. Le mode non connecté n'oblige pas les deux entités à établir une connexion entre elles avant de transférer des données puis de mettre fin à leur connexion. En revanche, UDP ne permet pas de savoir si les datagrammes sont bien arrivés et s'ils sont arrivés dans un ordre différent de celui d'émission.

Cette architecture SNMP fonctionne sur un modèle client-serveur. Le client correspond à la station de gestion de réseau, souvent appelée Manager ou encore Network Management Station (*NMS*) par certains éditeurs. Les serveurs correspondent aux agents SNMP qui enregistrent en permanence des informations les concernant dans leur MIB. La station interroge les MIB des différents agents pour récupérer les informations qu'elle souhaite.

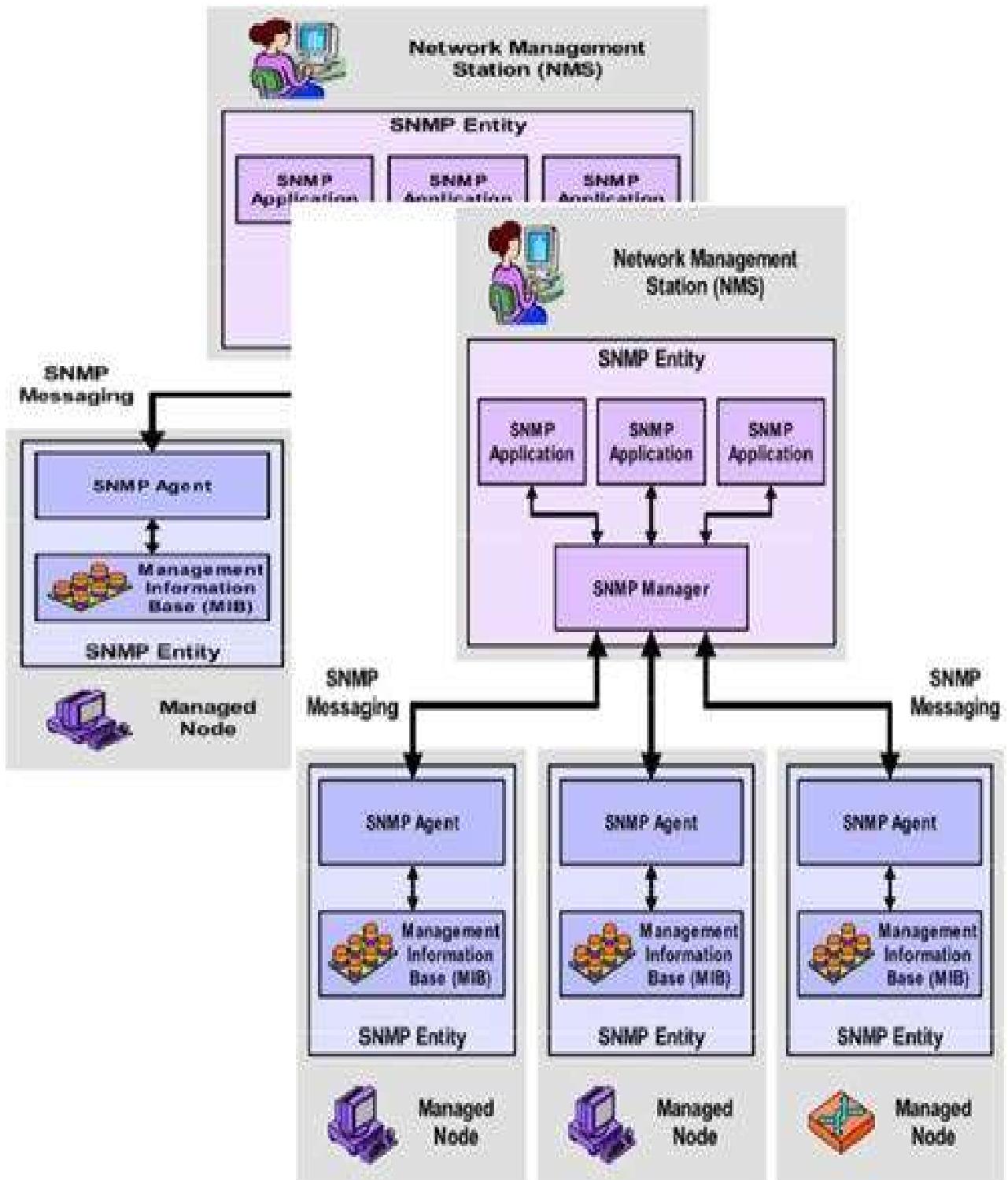


Illustration de la gestion d'un réseau avec SNMP

II.2.2. LES LOGICIELS DE SUPERVISION « OPEN SOURCE »

Tout d'abord, il sied de rappeler que les logiciels dits « *Open Source* »⁴ sont définis particulièrement comme *des « logiciels libres »*, c'est-à-dire que ce sont des logiciels qui rassemblent les applications livrées avec leurs codes sources, que l'on peut donc modifier à volonté pour l'adapter à ses besoins... afin de dire qu'un logiciel est libre, il faudrait tenir compte des 9 aspects suivants :

- la libre distribution ;
- la mise à disposition du code source ;
- la possibilité de distribuer ses travaux dérivés ;
- le respect du code source originel ;
- l'absence de la discrimination envers les personnes ;
- l'absence de la limitation sur le domaine d'application du logiciel ;
- la distribution de la licence ;
- la non-spécificité à un produit ;
- elle ne doit pas contaminer les travaux des autres ;

Les logiciels de supervision dits « Open Source », les plus utilisées sont :

- le logiciel NAGIOS ;
- le logiciel CACTI ;
- Le logiciel CENTREON ;
- Etc.

⁴Ils ont été mis au point en 1988 par **Eric Raymond**, cherchant à adapter le principe de l'entreprise

A. LE LOGICIEL NAGIOS

Le logiciel de supervision « *Nagios* »⁵ (*anciennement appelé « Netsaint »*) est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes ont des dysfonctionnements et quand ils repassent en fonctionnement normal. C'est un logiciel libre sous licence GPL (*Generic Public License*)⁶. Le logiciel Nagios⁷, est un programme modulaire qui se décompose en trois parties :

- *Le moteur d'application* qui permet d'organiser ou d'ordonnancer les tâches de supervision.
- *L'interface web*, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies ou (*permettant de visualiser l'état du fonctionnement du système d'information*).
- *Les sondes* (*appelées greffons ou plugins*), permettant d'ajouter de nouvelles fonctionnalités au logiciel). Ces plugins peuvent être écrits dans de nombreux types de langages.

Ce logiciel a l'avantage de pouvoir superviser tous les types de ressources et de services grâce à des centaines de « *plugins* ». Nagios est bien adapté aux systèmes d'information de taille moyenne et aussi de taille importante. Nagios a comme défaut d'être difficile à administrer et de ne fonctionner que sous Linux ou une variante Unix. Le logiciel de supervision *Nagios* a la Possibilité de :

⁵ Nagios est un logiciel open source de supervision. Il permet de surveiller aussi bien les réseaux que les systèmes. Il peut, par exemple, suivre l'évolution d'une charge processeur, le fonctionnement d'un service précis ainsi que la bande passante internet. Une fois une anomalie détectée il est capable d'alerter d'un dysfonctionnement. Présentation Rebaptisé en 2002, il tire alors son nom du grec ἀγιος (agios0) signifiant saint. Puis en rétro acronymie Nagios Ain't GonnaInsist On Sainthood.

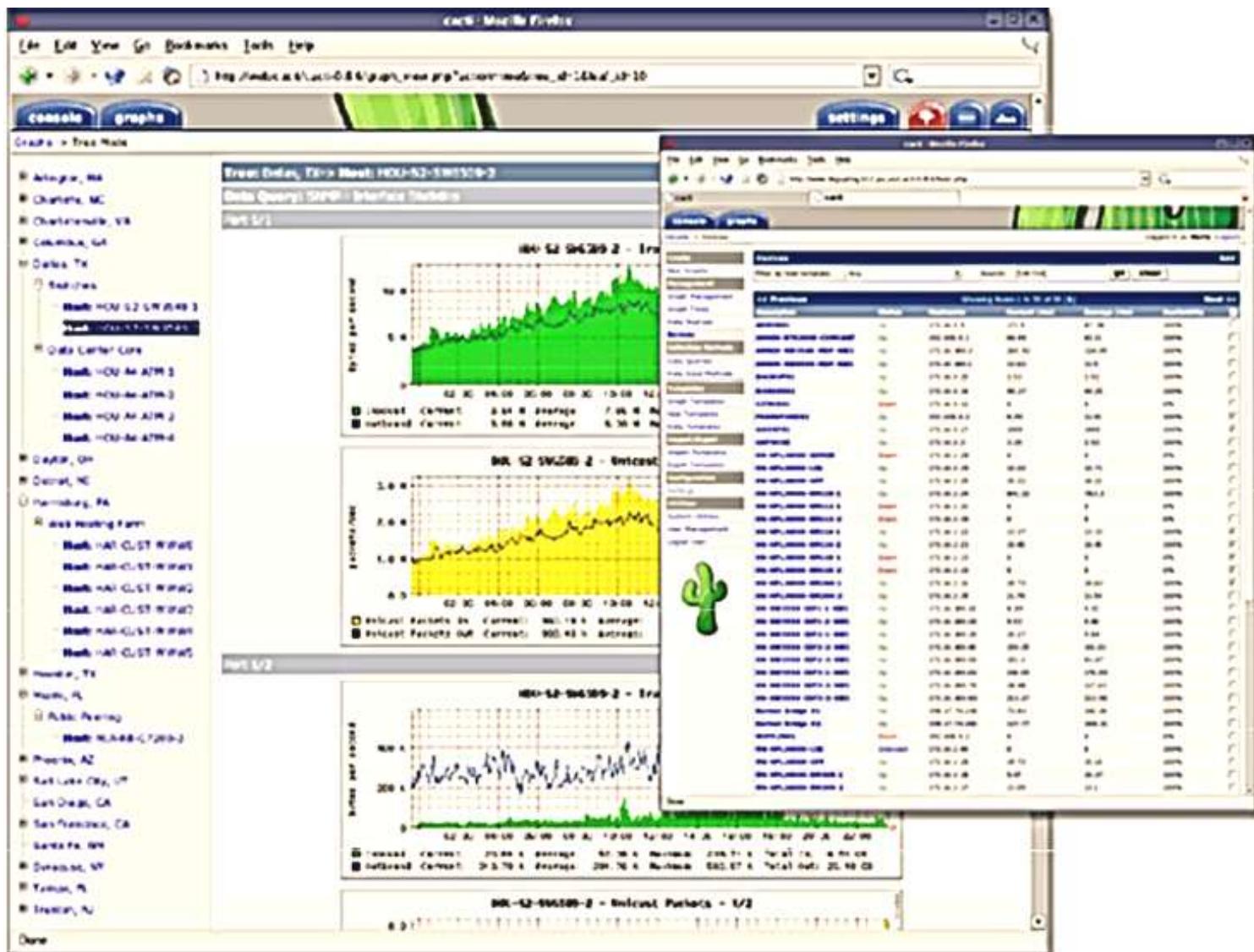
⁶ GPL est tout simplement le statut juridique des logiciels distribués librement, jadis a l'origine utilisé pour le projet GNU.

⁷ Vu le manque de réactivité du développeur principal de Nagios et sa volonté de ne plus diffuser tous les modules sous licence libre, certains développeurs actifs sur le projet ont fait diverger Nagios pour créer « Icinga ».

- Superviser des services réseaux : (*SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP, etc.*) ;
- Superviser les ressources des serveurs (*charge du processeur, occupation des disques durs, utilisation de la mémoire paginée*) et ceci sur les systèmes d'exploitation les plus répandus ;
- Interfacer avec le protocole SNMP.
- La supervision à distance peut utiliser SSH ou un tunnel SSL (*notamment via un agent NRPE*).
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche : scripts shell (*Bash, ksh, etc.*), C++, Perl, Python, Ruby, PHP, C#, etc.
- La vérification des services se fait en parallèle.
- Possibilité de définir une hiérarchie dans le réseau pour pouvoir faire la différence entre un serveur en panne et un serveur injoignable.
- La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins (*alerte par courrier électronique, SMS, etc.*).
- Acquittement des alertes par les administrateurs.
- Gestion des escalades pour les alertes (*une alerte non acquittée est envoyée à un groupe différent*).
- Limitation de la visibilité, les utilisateurs peuvent avoir un accès limité à quelques éléments.
- Capacité de gestion des oscillations (*nombreux passages d'un état normal à un état d'erreur dans un temps court*).
- Créer ses propres plugins, dans le langage désiré. Il suffit de respecter la norme Nagios des Codes retour ;
- Les possibilités de tests deviennent donc infinies, il suffit d'écrire tout plugin qui n'existerait pas déjà sur les sites spécialisés.

B. LE LOGICIEL CACTI

Le logiciel « *Cacti* » est un logiciel libre ayant pour but principal de mesurer les performances du réseau. Il permet de réaliser principalement des graphiques et de faire des statistiques grâce à ces graphiques. Il fonctionne grâce à un serveur web et une base de données. Il est possible d'ajouter des plugins afin de lui apporter des services supplémentaires. Le logiciel de supervision Cacti est gratuit. Il fonctionne aussi bien sous Unix que Windows. Il peut déclencher des alertes par mail en cas de dépassement de certains seuils d'alerte par l'ajout d'un plugin appelé « *Thold* ».



Présentation du monitoring sous Cacti (The Cacti Group, 2010)

Le logiciel Cacti⁸ est un *logiciel libre* de mesure de *performances réseau et serveur* basé sur la puissance de stockage de données de « *RRD-Tool* ». Il est souvent utilisé avec des logiciels de supervision (*par exemple Nagios*), mais il ne fait pas de supervision en tant que tel. Il ne fait pas de corrélation d'incidents ni d'alerte en cas d'incident (*bien que des plugins existent, ce n'est pas son but premier*). Par ailleurs, il permet de faire l'étude d'indicateurs sur une période donnée (*moyenne sur le mois par exemple, ou maximum de la semaine, etc....*) et contrairement à la supervision qui permet de connaître l'état de l'indicateur en temps réel. Il fonctionne grâce à *un serveur web* équipé d'une *base de données MySQL* et du *langage PHP*. Il peut être considéré comme le successeur de *MRTG* et également comme une interface d'utilisation de *RRD-Tool*.

Il permet de représenter graphiquement divers états de *périphériques et équipements réseau* utilisant *SNMP* pour connaître la charge processeur, le débit des interfaces réseau, *utilisation de la Qualité de service* sur une ligne, la qualité d'une liaison (*CRC/s*) ou encore la latence réseau. Le logiciel Cacti utilise aussi un système de *scripts* (*Bash, PHP, Perl, VBs...*) pour effectuer des mesures plus complexes, par exemple l'espace disque restant, la charge processeur pour un processus donné ou le temps de réponse applicatif⁹.

L'attrait de ce logiciel réside principalement dans son principe de modèles (*Templates*) qui permet de créer de manière générique les graphiques afin de pouvoir les réutiliser. Ce système peut sembler déroutant pour les nouveaux utilisateurs, mais montre vite ses avantages lorsqu'il s'agit de superviser un grand nombre d'indicateurs et/ou d'équipements. Les possibilités d'import et d'export de ces *templates* permettent de les partager avec toute la communauté des utilisateurs.

⁸Historiquement c'est un script PHP (cmd.php) qui réalise cette collecte de mesures (polling). Depuis la version 0.8.6, il est possible d'utiliser un exécutable écrit en C, cacti-spine (initialement cactid), qui améliore énormément la vitesse de mesure grâce à l'utilisation directe de la bibliothèque net-snmp et l'utilisation des threadsPOSIX. À intervalles réguliers (par défaut toutes les 5 min), le poller (spine ou cmd.php) réalise les requêtes SNMP, ordonne les scripts et enregistre les résultats.

⁹Contrairement à MRTG qui régénère l'ensemble des graphiques toutes les 5 minutes, Cacti génère les images dynamiquement à l'affichage à partir des fichiers de données RRD-Tool. Cela permet par exemple de pouvoir zoomer sur une période ou changer dynamiquement la période du graphique. Il est également possible d'effectuer des opérations simples (et des combinaisons d'opérations) avec les différentes données, avant leur affichage, grâce à une interface graphique qui permet l'utilisation simplifiée de la commande CDEF de RRD-Tool. On peut ainsi convertir les octets en bits ou visualiser facilement un graphique en pourcentage.

C. LE LOGICIEL CENTREON

Le logiciel « *Centreon* » est également un logiciel open source permettant de superviser le réseau. Il fonctionne grâce au moteur de récupération d'informations de Nagios. Il s'agit en fait d'une surcouche web de Nagios. Centreon est un logiciel de supervision informatique édité par la société du même nom.

Ce logiciel gratuit a été conçu pour faciliter l'administration de Nagios et avoir une interface simplifiée. Il permet de faire du monitoring en temps réel ainsi que de la remontée d'alerte en cas d'incident. En revanche, le logiciel Centreon ne fonctionne que sous Linux ou Solaris. *Le logiciel Centreon* s'articule autour de trois composants open source :

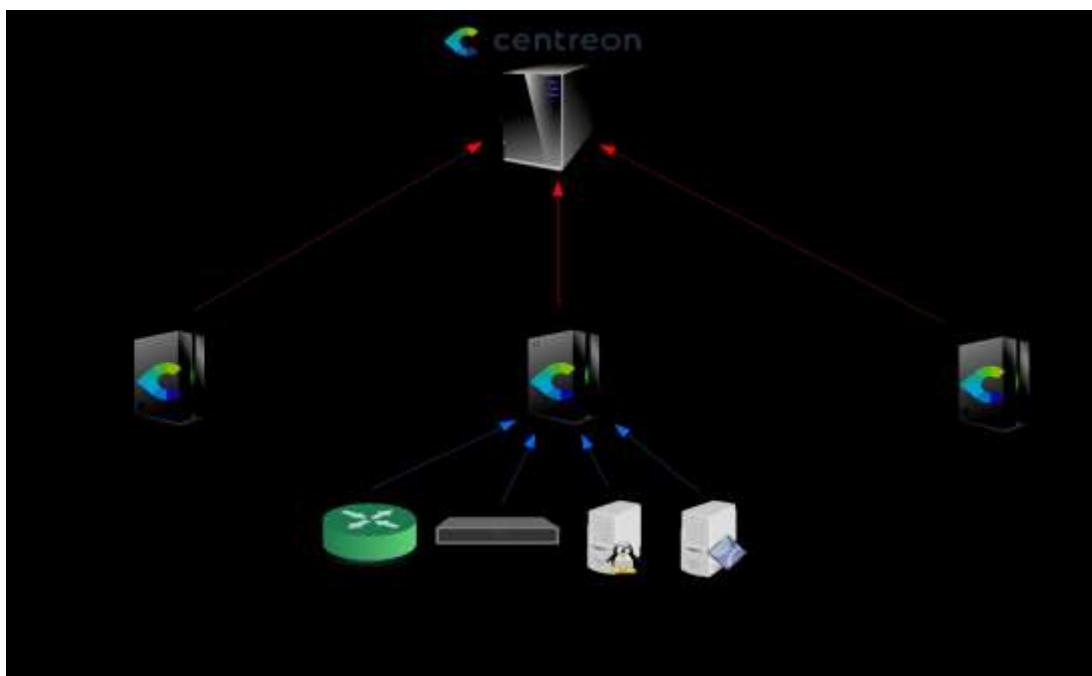
- *Centreon Web*, l'interface de visualisation ;
- *Centreon Engine*, le moteur de collecte de données (basé sur Nagios 3) ;
- *Centreon Broker*, le gestionnaire d'événements



Présentation du monitoring sous Centreon (MERETHIS, 2010)

L'ensemble des solutions Centreon reposent sur un environnement de base, totalement open source, baptisé OSS pour Open Source Software :

- La possibilité d'avoir une vue synthétique de la supervision de son système d'informations ;
- La visualisation de graphiques de performances ;
- Des rapports de disponibilités des ressources supervisées : hôtes, services et groupes de ressources (*disponible via IHM et exportables en csv*) ;
- Une interface de configuration intuitive pour les différents objets et fichiers de configurations des ordonnanceurs ;
- La possibilité d'administrer chaque paramètre de l'interface web ;
- La possibilité de mettre en place des accès restreints aux ressources et pages de l'interface, configurables de manières fines (*via des LCA : Liste de Contrôles d'Accès*) ;
- La possibilité de suivre des logs d'utilisation de la solution (logs de modifications des ressources) ;
- La possibilité de construire un « *dashboard* » ou « *console* » à l'aide de widgets graphiques (*carte Google Maps, listing des ressources, graphiques de performance...*) ;
- La possibilité de développer des modules additionnels pour étendre les fonctionnalités de la solution.



II.3.2. LES LOGICIELS DE SUPERVISION « PROPRIÉTAIRES »

Les logiciels de supervision dits « *propriétaires* » sont des logiciels caractérisés par l'appartenance à une personne ou à une société en particulier. Ce sont des logiciels qui ne sont pas des standards à l'origine et ne sont pas compatibles avec d'autres logiciels comparables de la concurrence. Les logiciels de supervision dits « *propriétaires* », les plus utilisées sont :

- le logiciel HP - OPENVIEW ;
- le logiciel PRTG NETWORK MONITOR ;
- Le logiciel MEMO GUARD ;
- Etc.

A. LE LOGICIEL HP –OPENVIEW

Le logiciel de supervision « *HP OpenView* » est une application logicielle de Hewlett Packard Enterprise pour les entreprises de l'informatique. Le produit fondateur d'OpenView était « *Network Node Manager : NNM* », un logiciel de surveillance de réseau basé sur SNMP. Le NNM a été utilisé pour gérer les réseaux et pourrait être utilisé conjointement avec d'autres logiciels de gestion, tels que « *CiscoWorks* ».

Le logiciel de supervision OpenView est un ensemble de modules permettant la supervision des infrastructures informatiques. Chaque module a sa spécificité et possède un coût élevé. Seuls les trois modules ci-dessous correspondent aux besoins :

- *Le module OpenView Network Node Manager* est un logiciel permettant d'avoir une représentation cartographique d'un réseau selon la typologie des équipements. Les alertes sont ainsi visibles par un code couleur. A partir d'une alarme, il est possible de zoomer sur la partie du réseau en dérangement afin de mieux comprendre la panne pour intervenir plus efficacement. Les alertes peuvent également être envoyées par mail.
- *La version Starter Edition illimitée* en nombre de nœuds.
- La version « *Advanced Edition illimitée* », Ce logiciel fonctionne aussi bien sous Windows que Linux ainsi que d'autres systèmes d'exploitation.

B. LE LOGICIEL PRTG NETWORK MONITOR

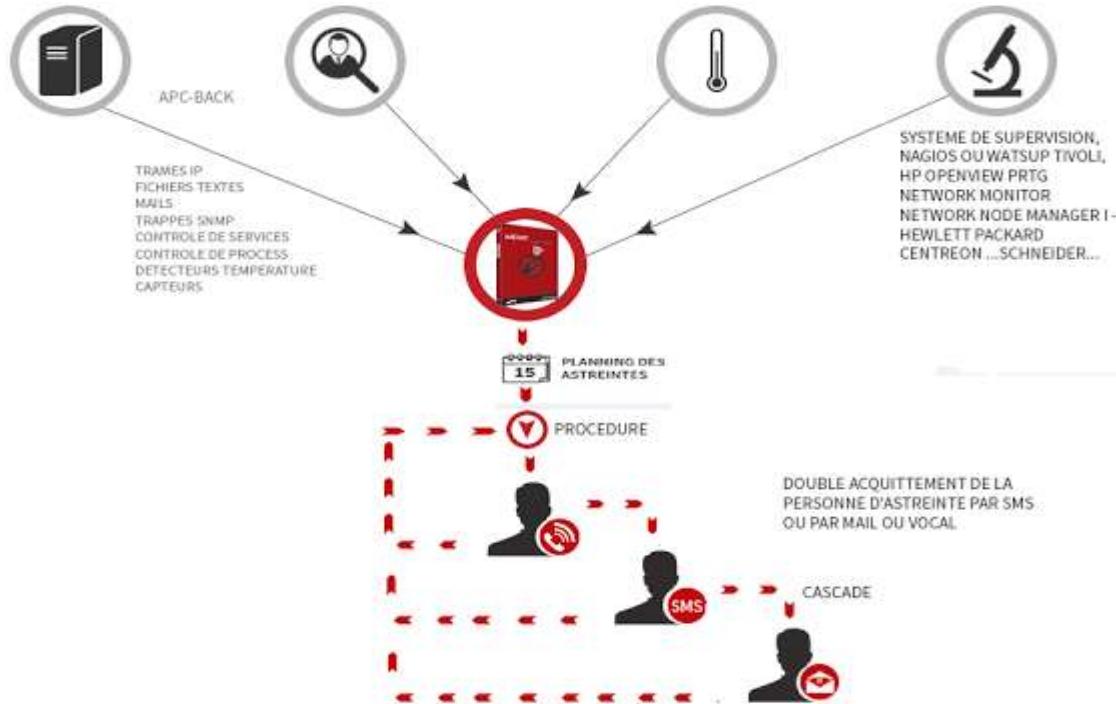
Le logiciel PRTG Network Monitor (Paessler Router Traffic Grapher), est un logiciel conçu par l'éditeur allemand *Paessler AG* spécialiste dans le domaine de la surveillance réseau. Principalement dédié aux administrateurs réseau, cet outil permet de surveiller la bande passante des réseaux LAN, des serveurs et des sites Web. Vous pourrez ainsi visualiser graphiquement l'occupation de la bande passante afin d'ajuster au mieux les paramètres de votre réseau et pour déceler de nombreux dysfonctionnements. Il fournit ainsi les outils nécessaires pour surveiller le réseau, l'utilisation du disque, de la mémoire ainsi que divers paramètres liés à l'infrastructure d'un réseau.



rités de **PRTG Network Monitor** est sa prise en charge de plus de 200 types de capteurs qui couvrent de nombreux protocoles tels que DNS, IMAP, Ping, POP3 ou encore SNMP. Il est aussi compatible avec de nombreux autres capteurs spécifiques aux serveurs VMWare et Windows. En outre, le logiciel se distingue par ses nombreuses interfaces, il peut ainsi être lancé via un logiciel classique appelé *Enterprise Console* ou sous la forme d'une interface web compatible avec une grande majorité de navigateurs web. Des applications iOS et Android sont également disponibles. Le logiciel *PRTG Network Monitor* fournit une grande quantité de tableaux de bord et une foule de rapports détaillés. Sur ce dernier point, vous disposerez d'une trentaine de modèles qui comprennent des graphiques et des tableaux pour chacune des sondes.

C. LE LOGICIEL MEMO GUARD

Le Logiciel MemoGUARD est un logiciel de supervision qui identifie une alarme ou une alerte et traite les alertes selon des procédures et des plannings d'astreinte prédéfinis. Le logiciel de supervision MemoGUARD avertit ensuite le personnel d'astreinte sur téléphone mobile (SMS, appel vocal), pager, téléphone filaire, mail, SMS to mail ou mail to SMS, et peut aller jusqu'à les mettre en relation (aboutement).



Le logiciel MemoGUARD, véritable logiciel de supervision, en mode *SaaS* ou en mode local, en toute sécurité, vous pouvez gérer les crises et les alertes grâce à la plate-forme qui prévient automatiquement le personnel de garde via SMS, mail, appel vocal, SMS to mail, mail to SMS ... et les relance autant de fois que nécessaire. Les messages d'alertes du logiciel de supervision peuvent être envoyés de deux façons : Par Modem GSM en envoyant directement sur le réseau opérateur des alertes SMS Par la plate-forme sécurisée multi-opérateurs CLEVER, dans le cas où des messages prioritaires, sécurisés ou cryptés sont nécessaires. « Gestion du personnel d'astreinte ». Le logiciel de supervision permet, notamment, de créer et gérer facilement des cellules de crise pour les situations d'urgence. Il s'adapte aussi au secteur industriel, aux réseaux informatiques, aux institutions et à tout ce qui touche à la sécurité et les formes d'activités liées aux interventions urgentes (*pompiers, sécurité ...*).

II.4. LES PLATES-FORMES D'ADMINISTRATION DES RESEAUX INFORMATIQUES

Les outils d'administration se répartissent en trois catégories :

- les systèmes de gestion des couches basses ;
- les hyper viseurs donnant une vue d'ensemble du réseau ;
- les systèmes d'exploitation avec administration partiellement intégrée.

A. LES OUTILS D'ADMINISTRATION DES COUCHES BASSES

Dans cette catégorie, on trouve les consoles d'administration de câblage et les analyseurs de protocoles. Les gestionnaires de câblage permettent de suivre les évolutions du câblage et le brassage de celui-ci. Compte tenu de la charge de travail imposée par l'acquisition préalable des données et la mise à jour des évolutions, ces outils ne sont justifiés que pour les réseaux importants en nombre de prises. Les sondes sont des éléments insérés dans un réseau pour en surveiller le fonctionnement. Elles fournissent, en temps réel, toutes les informations utiles au gestionnaire pour connaître l'état actuel de son réseau (taux d'erreurs, trafic...).

B. LES HYPERVISEURS

Les hyperviseurs sont de véritables plates-formes complètes d'administration de réseau. Ils permettent de superviser le réseau global de l'entreprise. Offrant les services d'une administration propriétaire (ex. : NetView d'IBM pour le réseau SNA) ou ouverte (ex : OpenView d'HP pour les environnements Unix), les hyperviseurs offrent une vue d'ensemble du réseau (*état des liens, des nœuds, d'un port d'un routeur, d'une carte...*).

C. LES SYSTEMES INTEGRES AU SYSTEME D'EXPLOITATION

Les **NOS** (*Network Operating System*) comportent un ensemble d'outils non seulement pour la gestion des utilisateurs, des ressources et de la sécurité, mais aussi de supervision du fonctionnement général du réseau et tout particulièrement de la machine serveur (charge du CPU, *swapping...*).

TROISIEME CHAPITRE – INSTALLATION ET CONFIGURATION D’UN SYSTEME WINDOWS SERVER « 2012 R₂ ».

Le système d’exploitation réseau Microsoft « aussi appelé Windows Serveur 2012 R2 » s'est focalisé sur 3 aspects :

- l'accès extranet aux dossiers ;
- la prise de contrôle bureau distant ;
- la sauvegarde du serveur et des postes clients.

Ces 3 aspects fournissent les fonctionnalités telles que :

- Gestion centralisée des utilisateurs ;
- Espace de stockage commun sur le serveur ;
- Partage de fichiers avec les autorisations en fonction des utilisateurs ;
- Partage d'imprimante ;
- Sauvegarde journalière des postes clients sur le serveur au travers du réseau local ;
- Sauvegarde journalière du serveur sur disque externe ;
- Possibilité de sauvegarde du serveur dans les nuages ;
- Accès à distance pour les utilisateurs : (portail Web, connexion des postes clients à distance en VPN, possibilité de faire du Direct Access).

III.1. PREREQUIS TECHNIQUES

Configuration minimum requise :

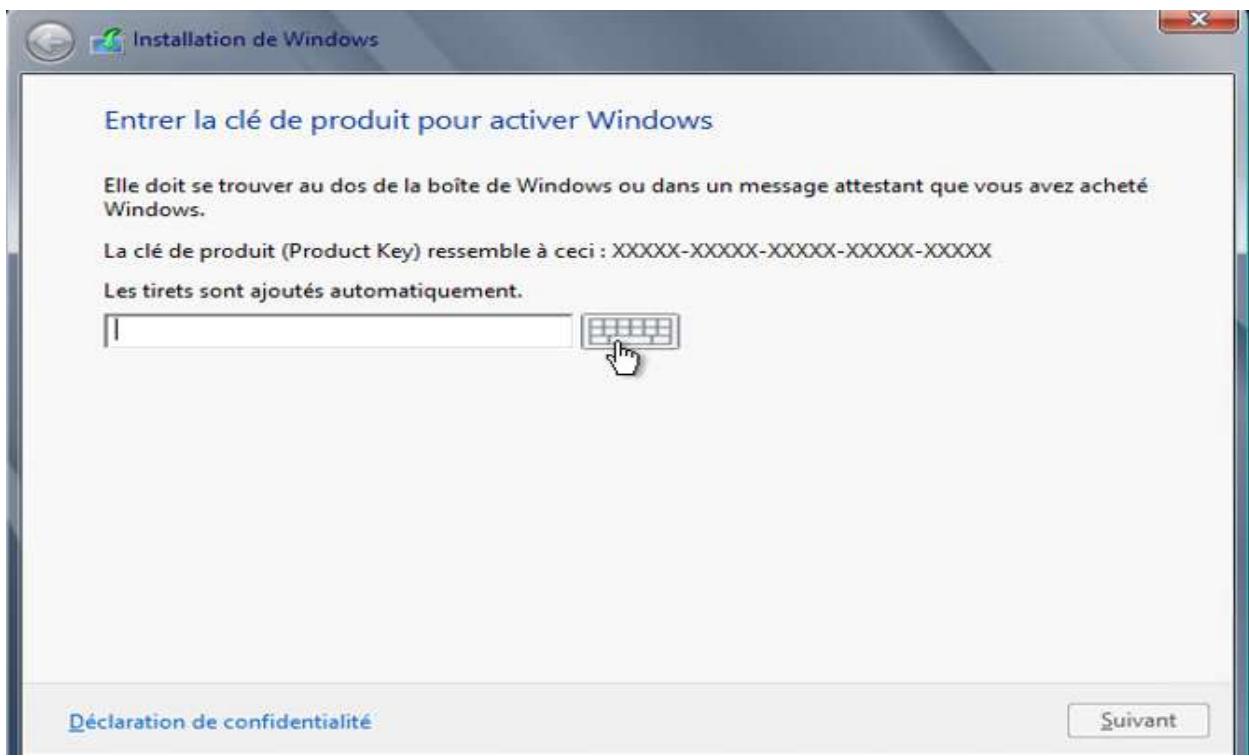
- CPU : 1.4 GHz (3.1 GHz 64 bits recommandé);
- Mémoire : 2 Go (8 Go recommandé);
- Disque : 160 Go;
- Réseau : 1 carte réseau;
- Clients : Windows 7/8 et MAC OS 10.5;
- Routeur ou BOX : IPv4 NAT (si possible UPnP et DHCP)

III.2. INSTALLATION DE WINDOWS SERVER 2012 R2

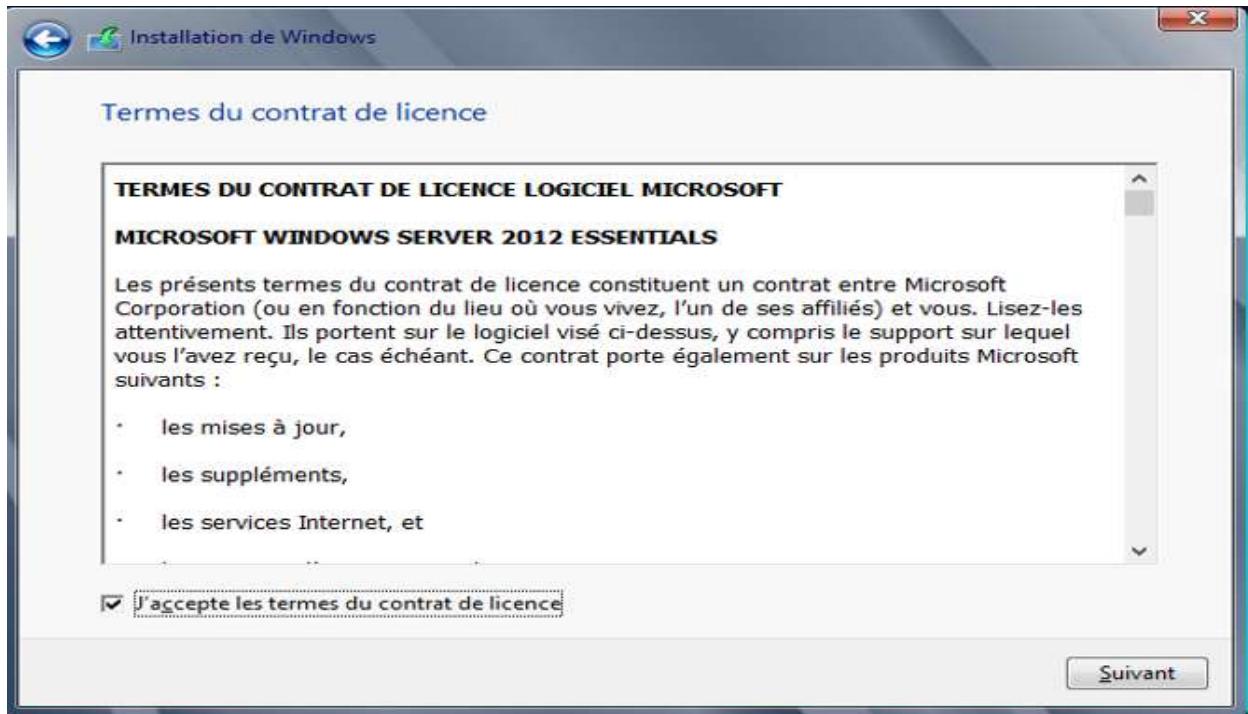
L'installation de Win 2012 R2 Server de base est classique, donc, il faudra booter sur le DVD Windows serveur 2012 R2. Cela signifie tout simplement, il faudra lancé le NOS lors du démarrage de l'ordinateur, ce qui donnera l'image suivante :



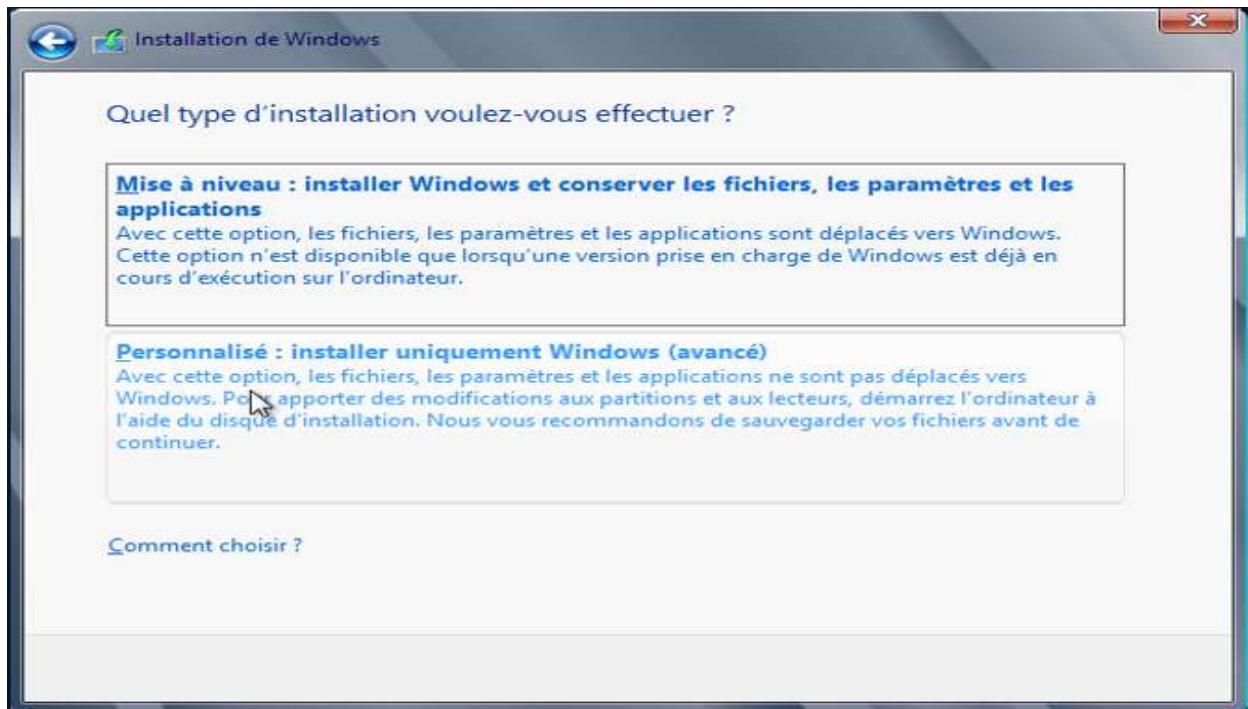
Ensuite, il faudra tout simplement entrer la clé de chiffrement:



Le contrat d'utilisateur se présente :



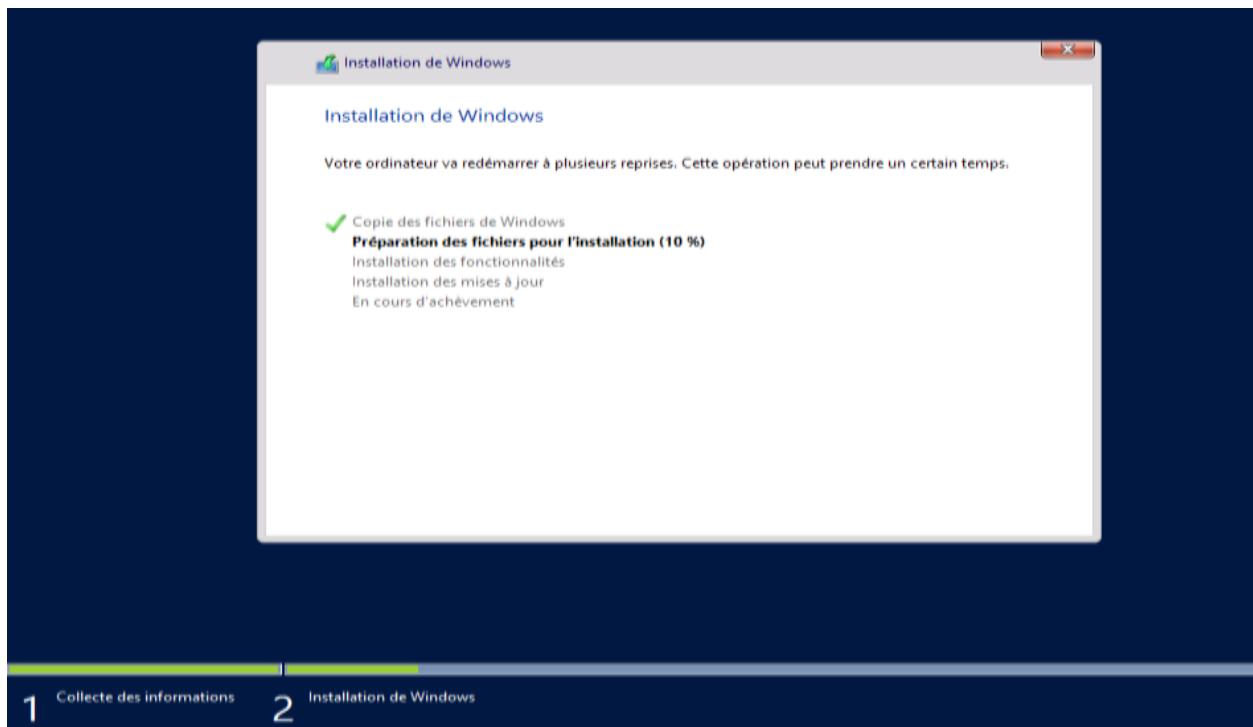
A ce niveau, Vous devez maintenant choisir l'installation personnalisée :



Il faudra alors choisir le disque accepté par le formatage du système et le partitionnement automatique :



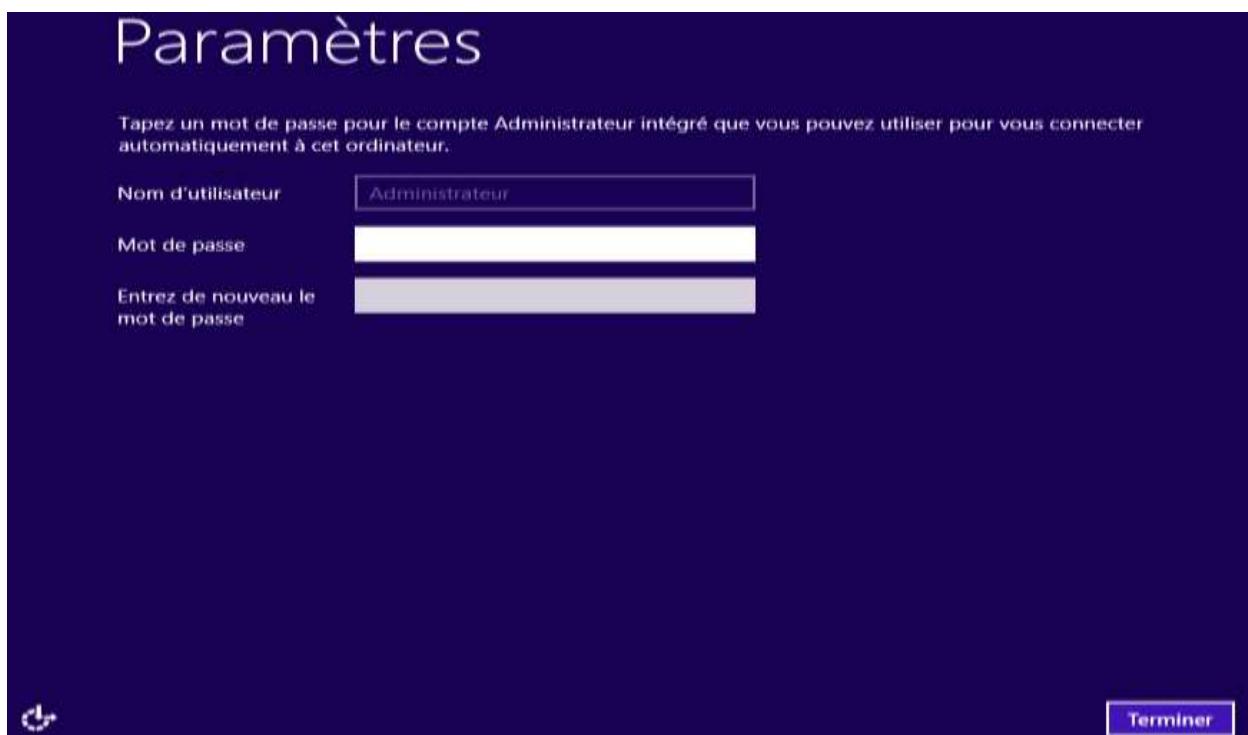
Après quoi, L'installation du système Windows serveur démarre :



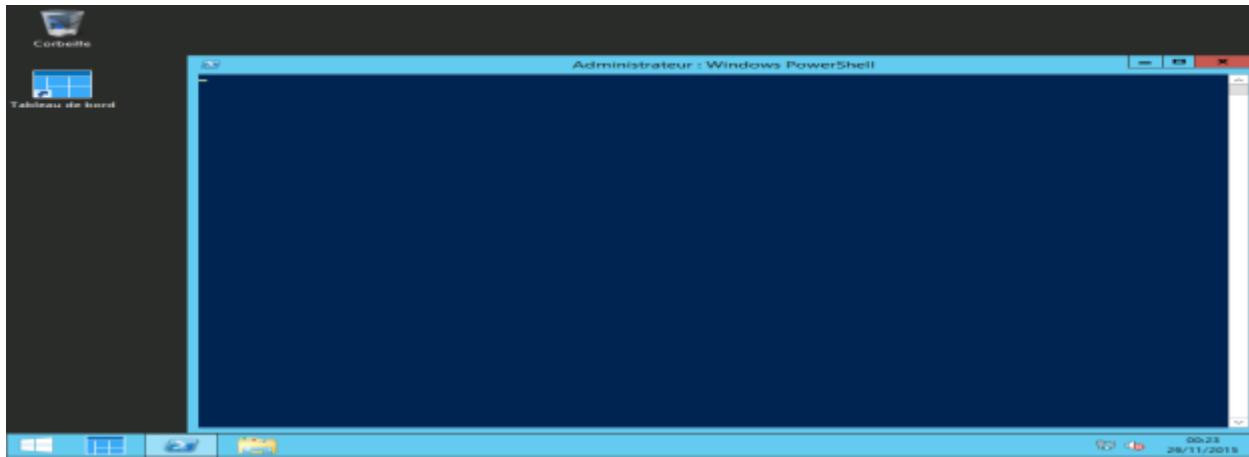
La suite des étapes d'installation s'exécute automatiquement. Et après redémarrage, il faut paramétriser la date et l'heure :



Puis entrez le mot de passe du compte administrateur :



L'installation du système est terminée. Et une session s'ouvre automatique avec le compte administrateur :

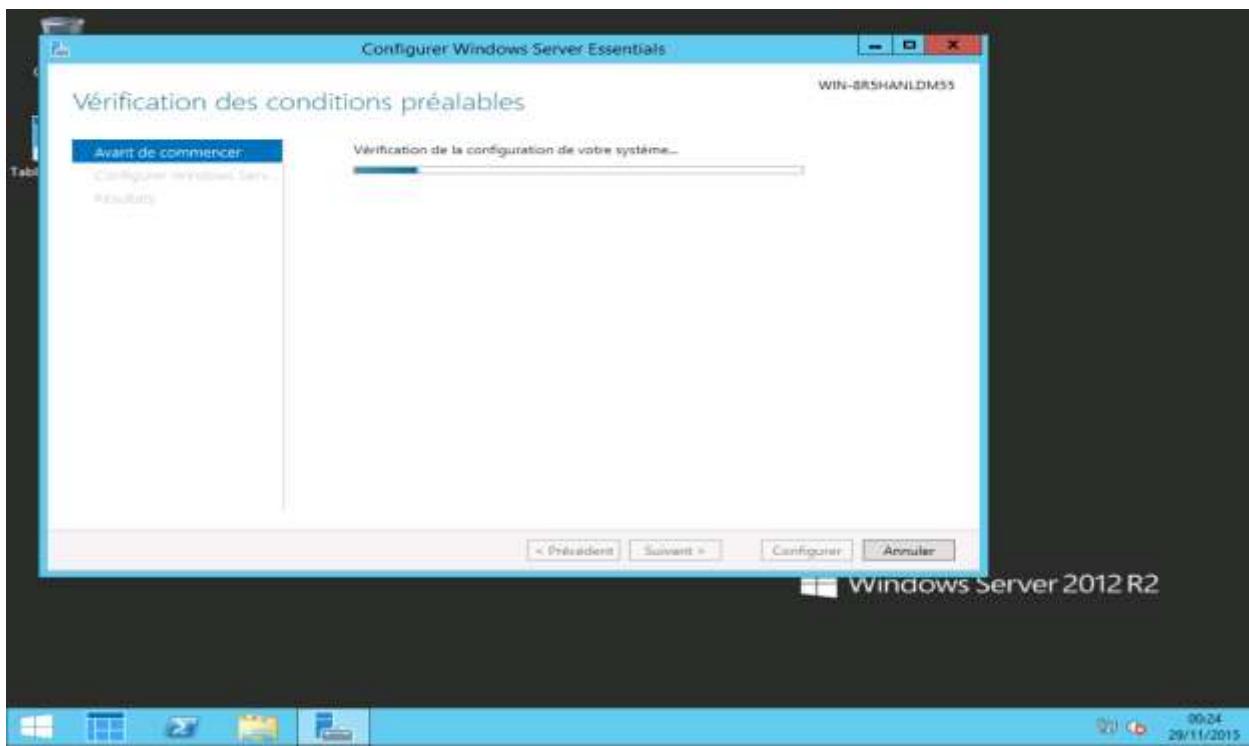


L'installation du système Windows serveur 2012 R2 est maintenant terminée. A ce stade,
Nous allons maintenant passer aux étapes de configuration.

III.3. CONFIGURATION DE WINDOWS SERVER 2012 R2

III.3.1. CONFIGURATION ETAPE 1 : PARAMETRES DE BASE

À ce stade, votre serveur effectue les tâches de vérification de base, et crée votre serveur suivant vos choix (Nom de l'entreprise, du domaine, du serveur); et Il commence de prime abord, par vérifier la configuration du système :



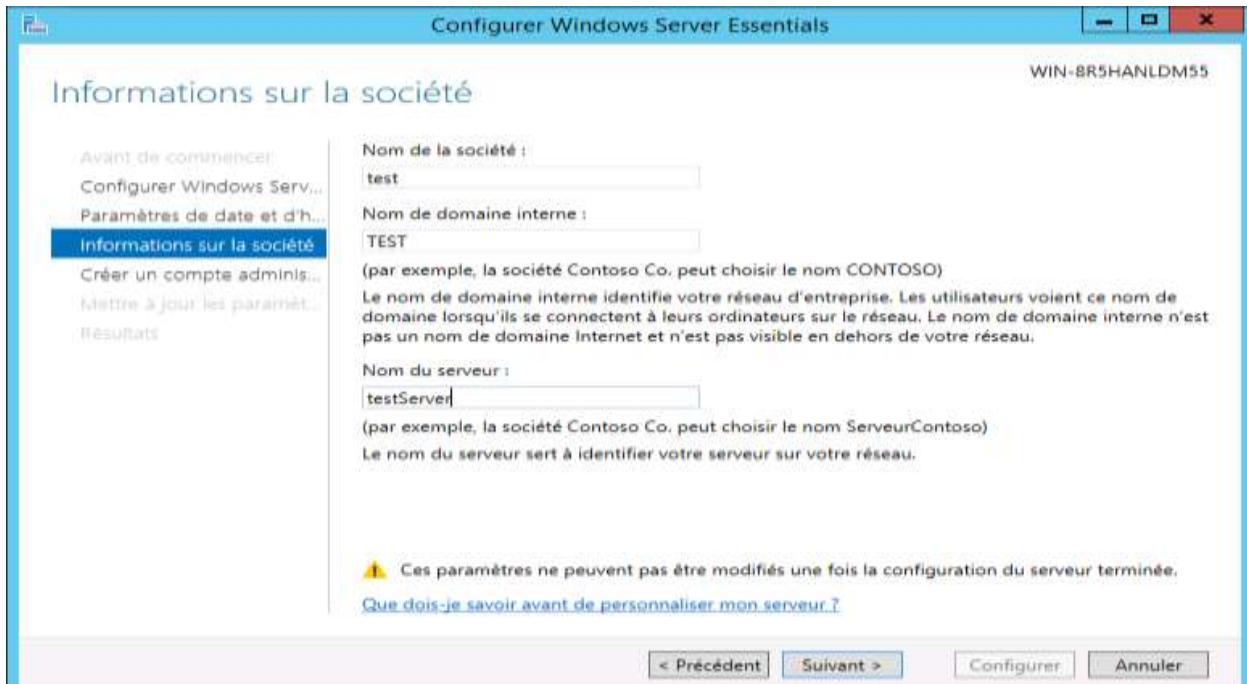
Dès que terminé, il auto démarre l'assistant de configuration pour que vous entriez les paramètres de base :



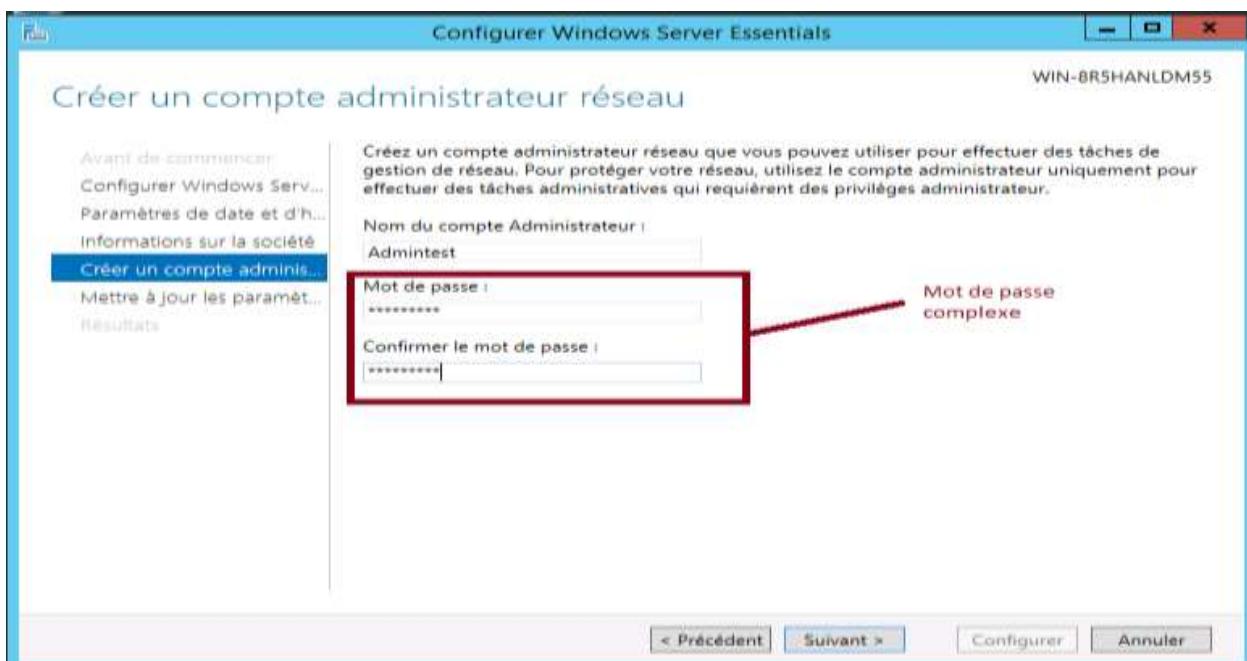
Entrez les paramètres horaires :



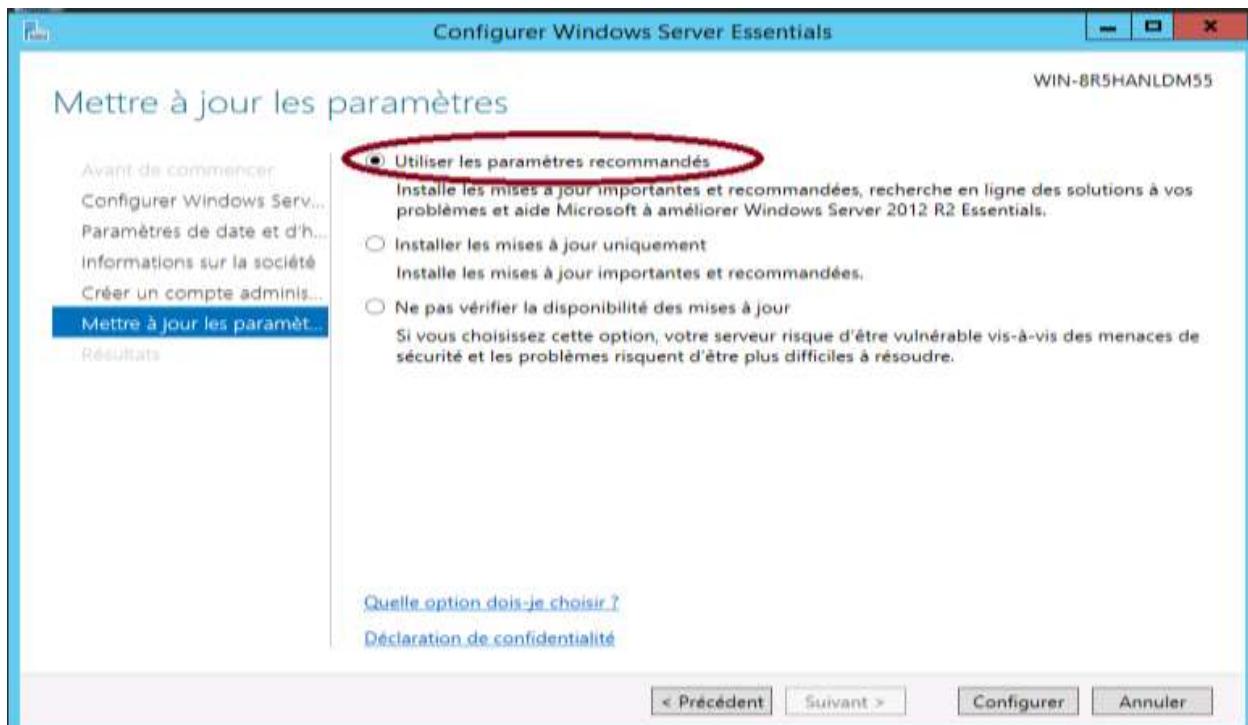
Entrez maintenant le nom de votre société, le domaine Windows interne et le nom du serveur :



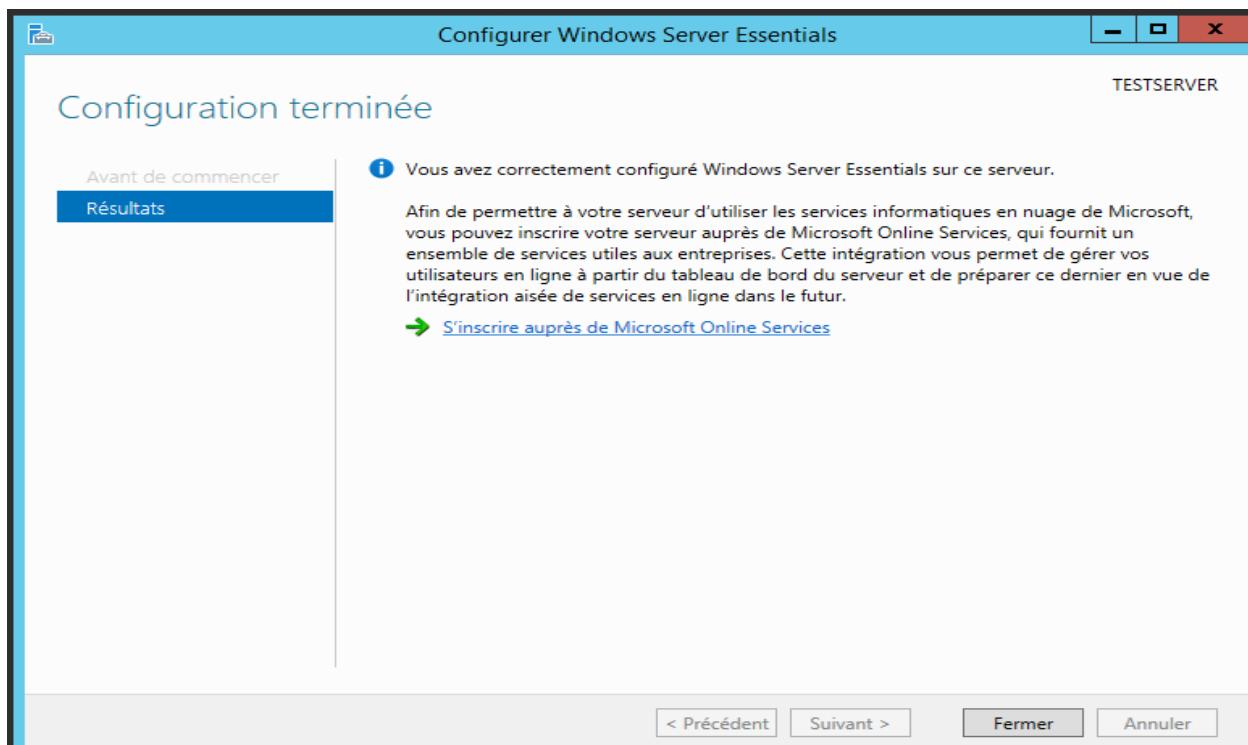
Fournissez le compte administrateur et le mot de passe :



Pour l'option des mises à jour, il est mieux d'utiliser les paramètres recommandés :



La configuration de Base est maintenant terminée :



A ce niveau Cinq répertoires, par défaut, ont été créés :

- C:\ServerFolders\Redirection de dossiers ;
- C:\ServerFolders\Sauvegarde de l'historique des fichiers ;
- C:\ServerFolders\sauvegarde d'ordinateurs clients ;
- C:\ServerFolders\Société ;
- C:\ServerFolders\Utilisateurs.

Cependant, La configuration étant terminée, il est recommandé à cette étape de créer un point de contrôle, pour avoir une image propre sauvegardée de notre système.

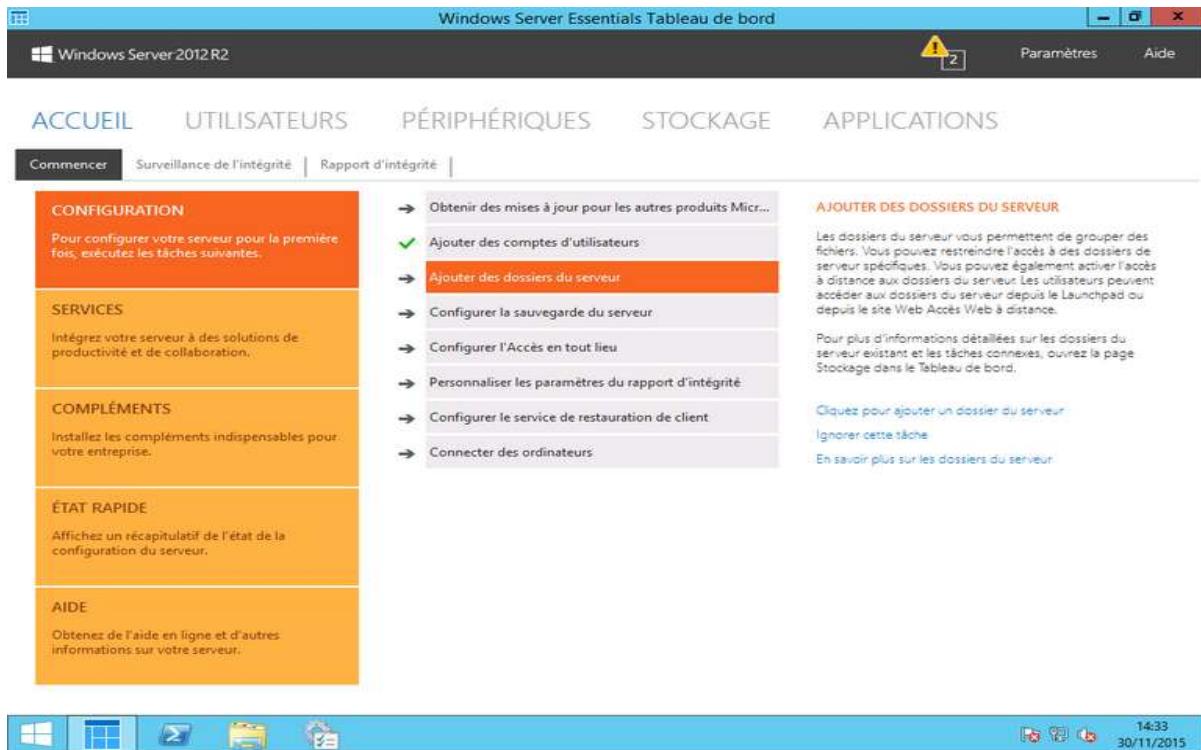
III.3.2. CONFIGURATION ETAPE 2 : PARAMETRES AVANCES

Nous arrivons à la configuration, proprement dite, Qui concerne, comment configurer votre serveur Windows. Microsoft a mis en place un tableau de bord regroupant les différentes tâches d'administration dont :

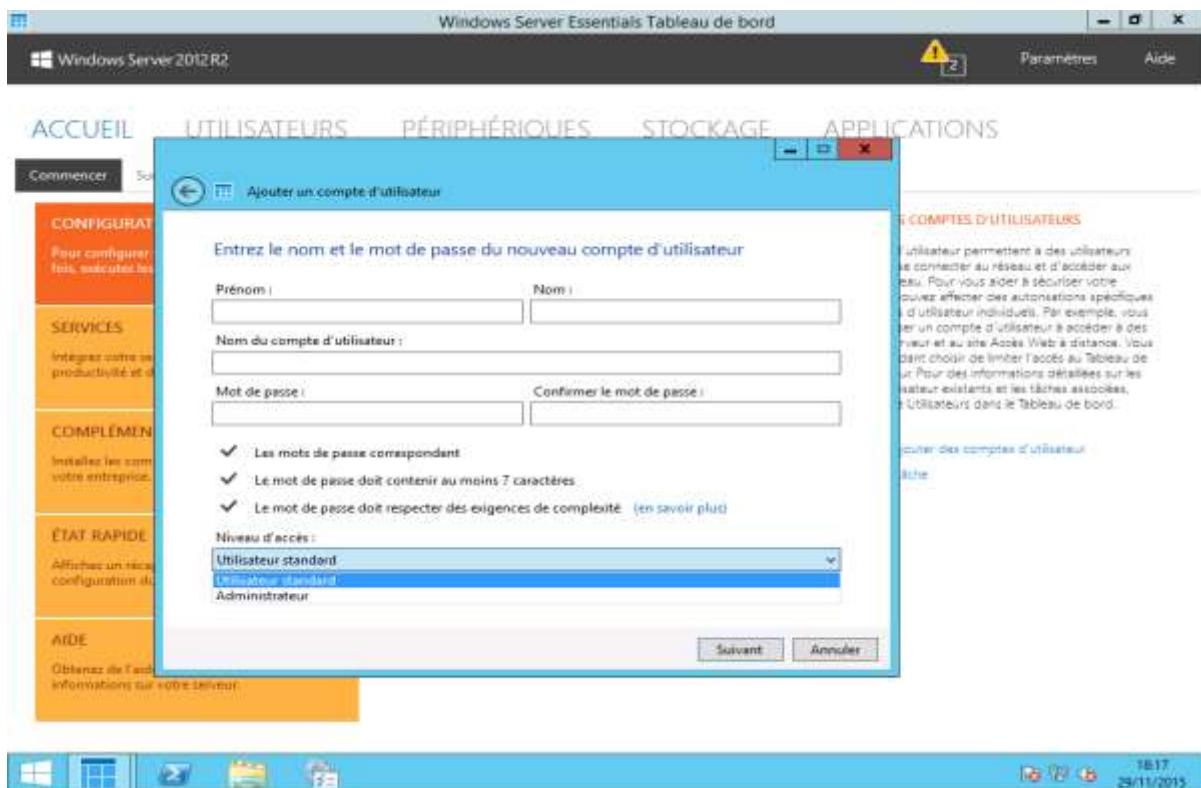
- créer un compte ;
- partager un dossier ;
- connecter un PC ;
- configurer la sauvegarde du serveur.

A. CRÉATION D'UN COMPTE UTILISATEUR

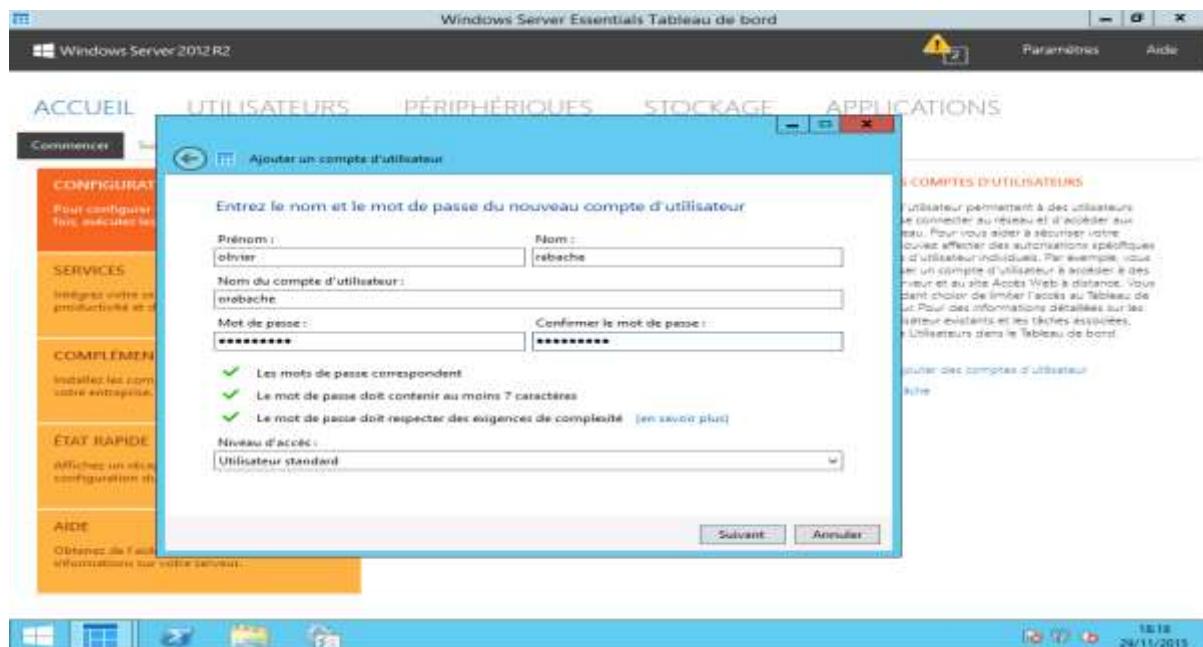
Pour commencer la création d'un utilisateur. Il faut d'abord ouvrir le tableau de bord, puis sélectionnez « *Ajouter des comptes utilisateurs* » :



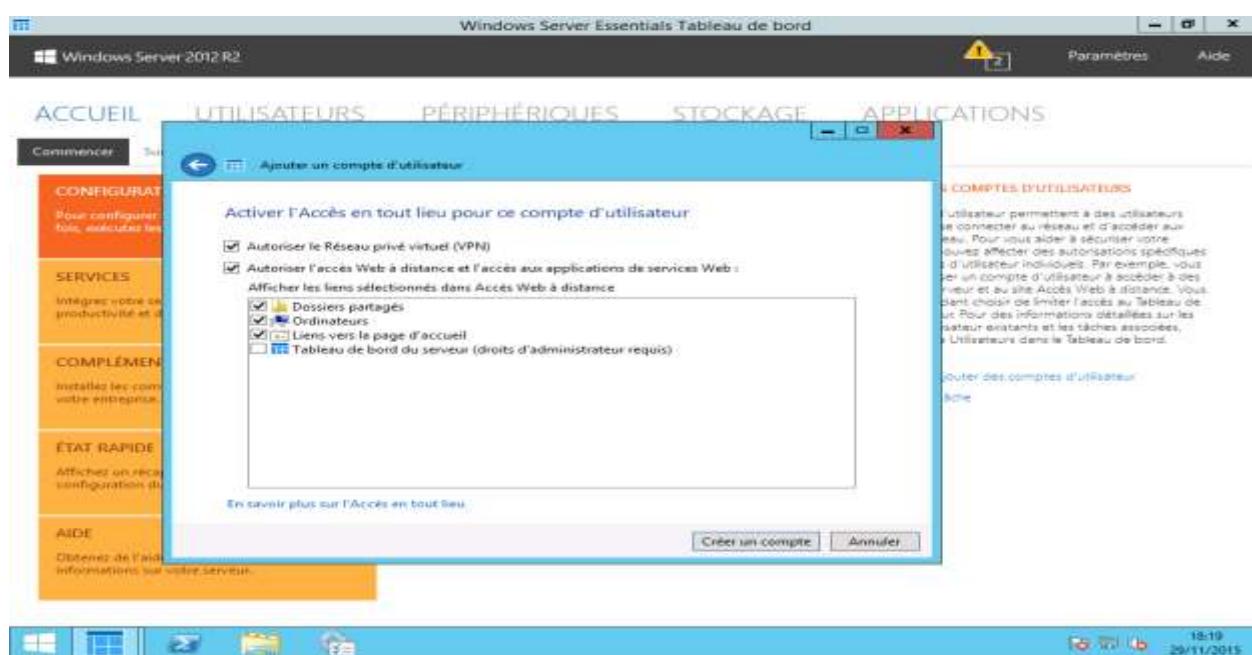
Puis, choisir le type du compte (utilisateur ou administrateur), généralement utilisateur :



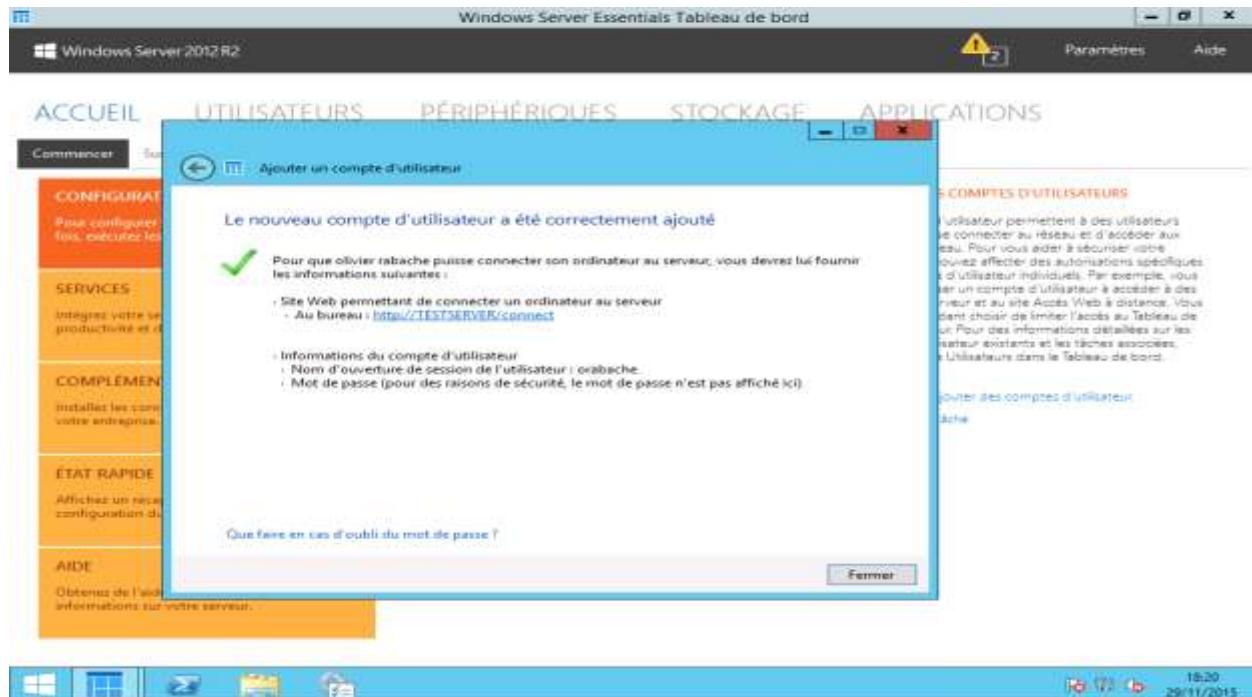
Ensuite, Il faut maintenant entrer les informations sur l'utilisateur. Ce qui conduira à la stratégie de sécurité sur le mot de passe doit passer au vert pour les trois différents points, sinon l'utilisateur ne sera pas créé. Enfin, On sélectionne maintenant son niveau d'accès sur le répertoire de base de la société : l'image ci-dessous illustre clairement les explications ci-dessus :



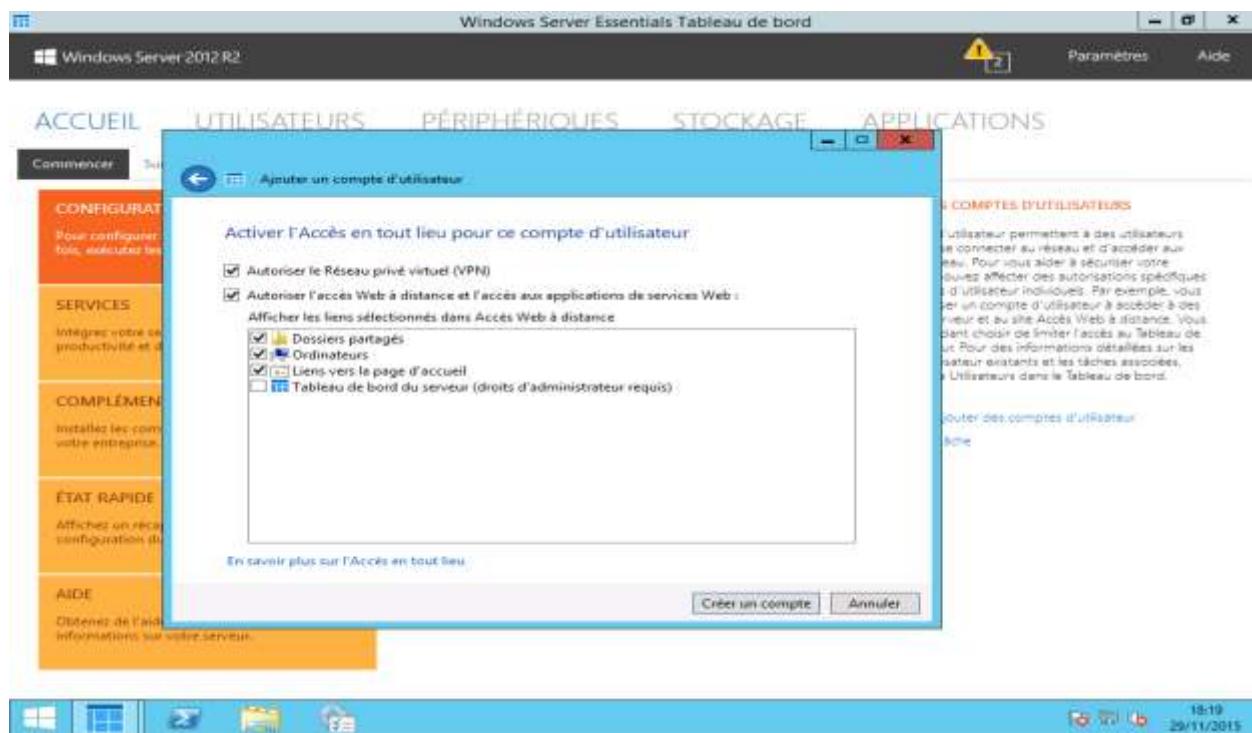
Puis on active ses accès en réseau au serveur :



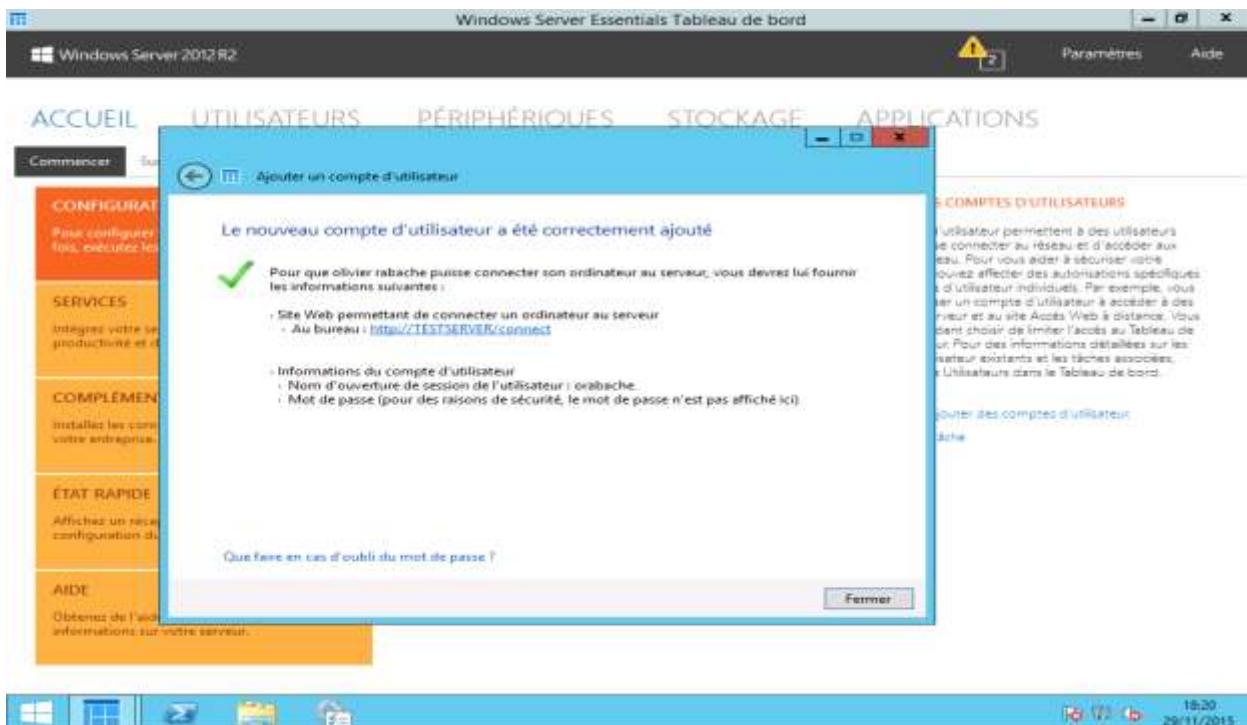
Après quoi, Le compte utilisateur est maintenant correctement configuré :



Puis on active ses accès en réseau au serveur :



Après quoi, Le compte utilisateur est maintenant correctement configuré :



B. SAUVEGARDE DU SERVEUR

Revenons au tableau de bord pour démarrer la configuration de la sauvegarde, en cliquant sur le bouton indiqué ci-dessous :

L'assistant de configuration charge :

CONFIGURATION

Pour configurer votre serveur pour la première fois, exécuter les tâches suivantes.

- Obtenir des mises à jour pour les autres produits Micr...
- ✓ Ajouter des comptes d'utilisateurs
- ✓ Ajouter des dossiers du serveur

SERVICES

Intégrez votre serveur à des solutions de productivité et de collaboration.

COMPLÉMENTS

Installez les compléments indispensables pour votre entreprise.

ÉTAT RAPIDE

Affichez un récapitulatif de l'état de la configuration du serveur.

AIDE

Obtenez de l'aide en ligne et d'autres informations sur votre serveur.

CONFIGURER LA SAUVEGARDE DU SERVEUR

Vous pouvez protéger les données de votre serveur en sauvegardant vos données stratégiques à intervalles réguliers. Vous pouvez choisir de sauvegarder les données de serveur sur un disque dur externe. Lorsque vous utilisez l'Assistant Configurer la sauvegarde du serveur, vous sélectionnez la fréquence de l'exécution de la sauvegarde et l'heure à laquelle elle doit être effectuée. Vous pouvez également choisir d'exécuter une sauvegarde une ou plusieurs fois par jour. Pour afficher les détails de la sauvegarde et les tâches connexes, ouvrez la page Sauvegarde dans le Tableau de bord.

Vous pouvez également choisir de sauvegarder les données de serveur vers un service de sauvegarde en ligne. Pour en savoir plus, cliquez sur l'onglet Modules complémentaires de la Page d'accueil.

Cliquez pour configurer la sauvegarde du serveur.
Ignorer cette tâche.

Puis, on a un résumé des actions à définir :

CONFIGURATION

Pour configurer votre serveur pour la première fois, exécuter les tâches suivantes.

SERVICES

Intégrez votre serveur à des solutions de productivité et de collaboration.

COMPLÉMENTS

Installez les compléments indispensables pour votre entreprise.

ÉTAT RAPIDE

Affichez un récapitulatif de l'état de la configuration du serveur.

AIDE

Obtenez de l'aide en ligne et d'autres informations sur votre serveur.

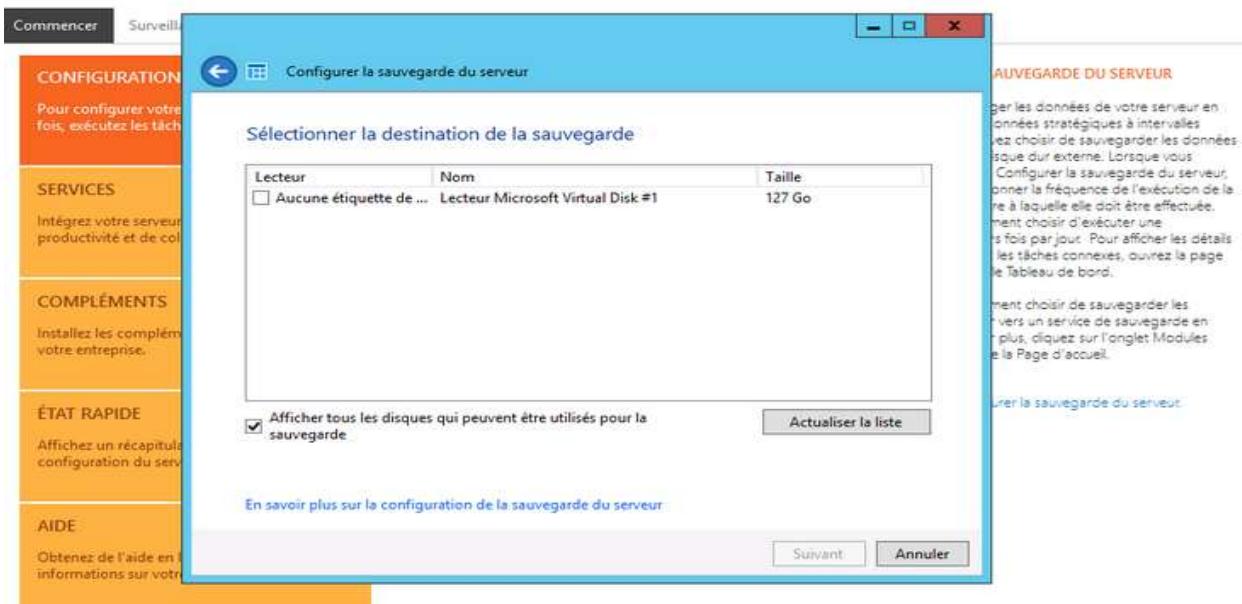
SAUVEGARDE DU SERVEUR

Configurez les données de votre serveur en sauvegardant vos données stratégiques à intervalles réguliers. Vous pouvez choisir de sauvegarder les données de serveur sur un disque dur externe. Lorsque vous utilisez l'Assistant Configurer la sauvegarde du serveur, vous sélectionnez la fréquence de l'exécution de la sauvegarde et l'heure à laquelle elle doit être effectuée. Vous pouvez également choisir d'exécuter une sauvegarde une ou plusieurs fois par jour. Pour afficher les détails de la sauvegarde et les tâches connexes, ouvrez la page Sauvegarde dans le Tableau de bord.

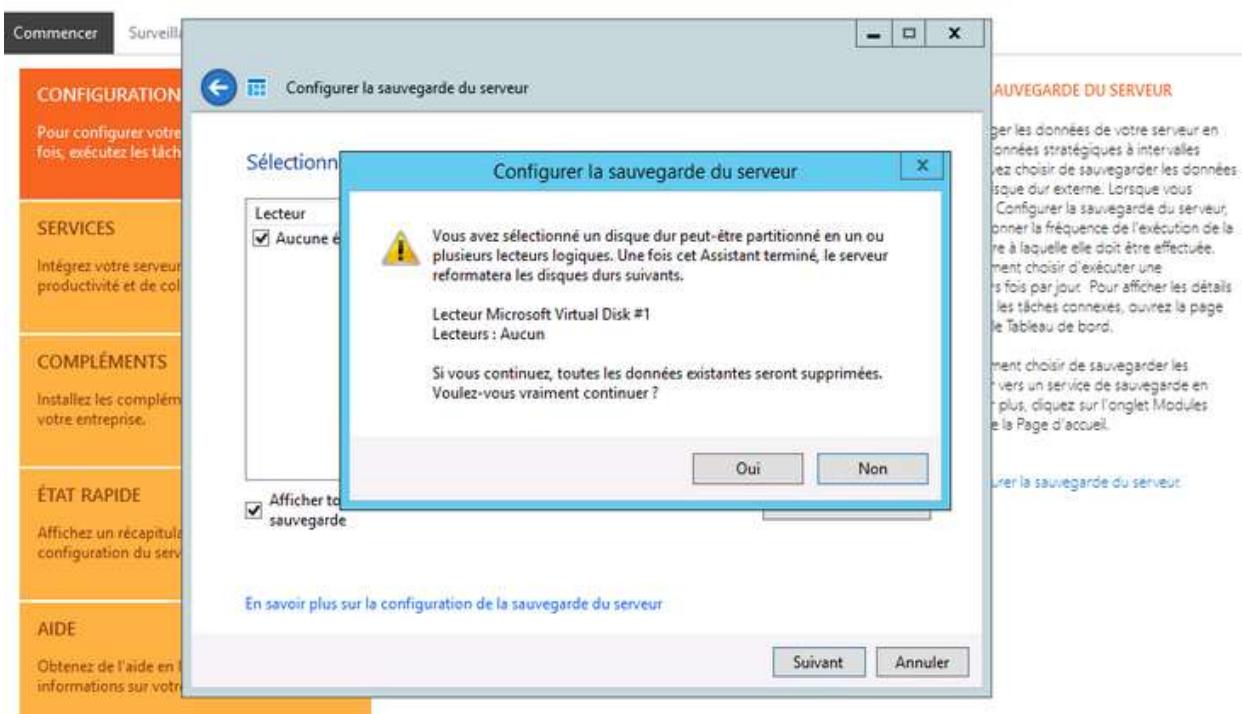
Vous pouvez également choisir de sauvegarder les données de serveur vers un service de sauvegarde en ligne. Pour en savoir plus, cliquez sur l'onglet Modules complémentaires de la Page d'accueil.

Cliquez pour configurer la sauvegarde du serveur.
Ignorer cette tâche.

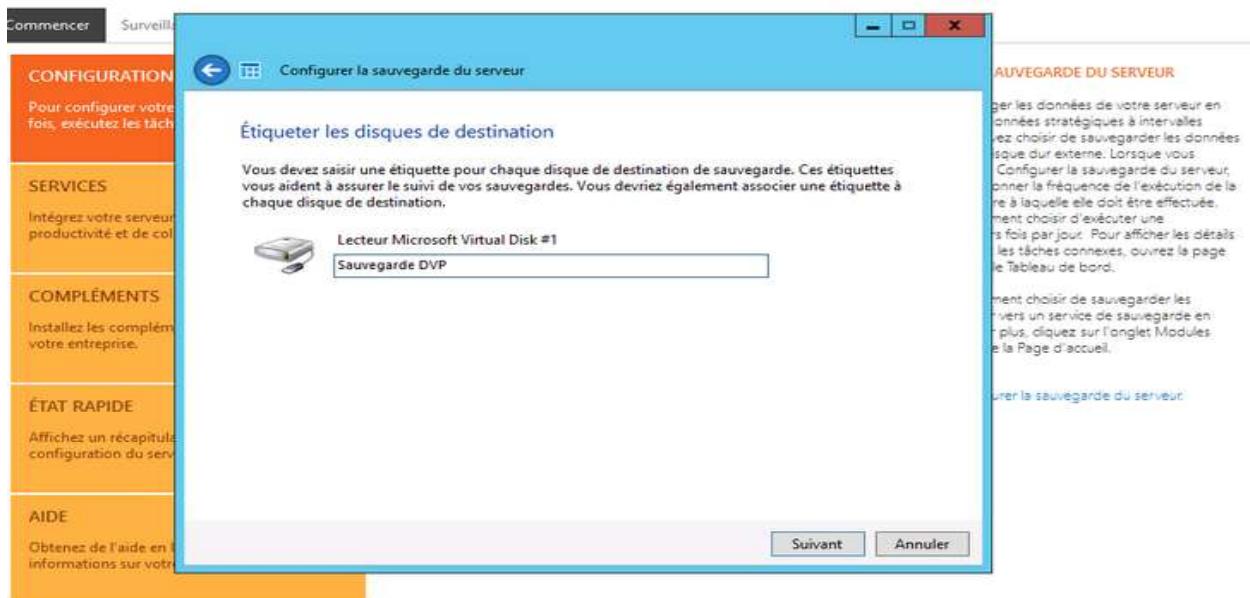
Il faut maintenant choisir de la destination de la sauvegarde, qui peut être un disque externe connecté au serveur :



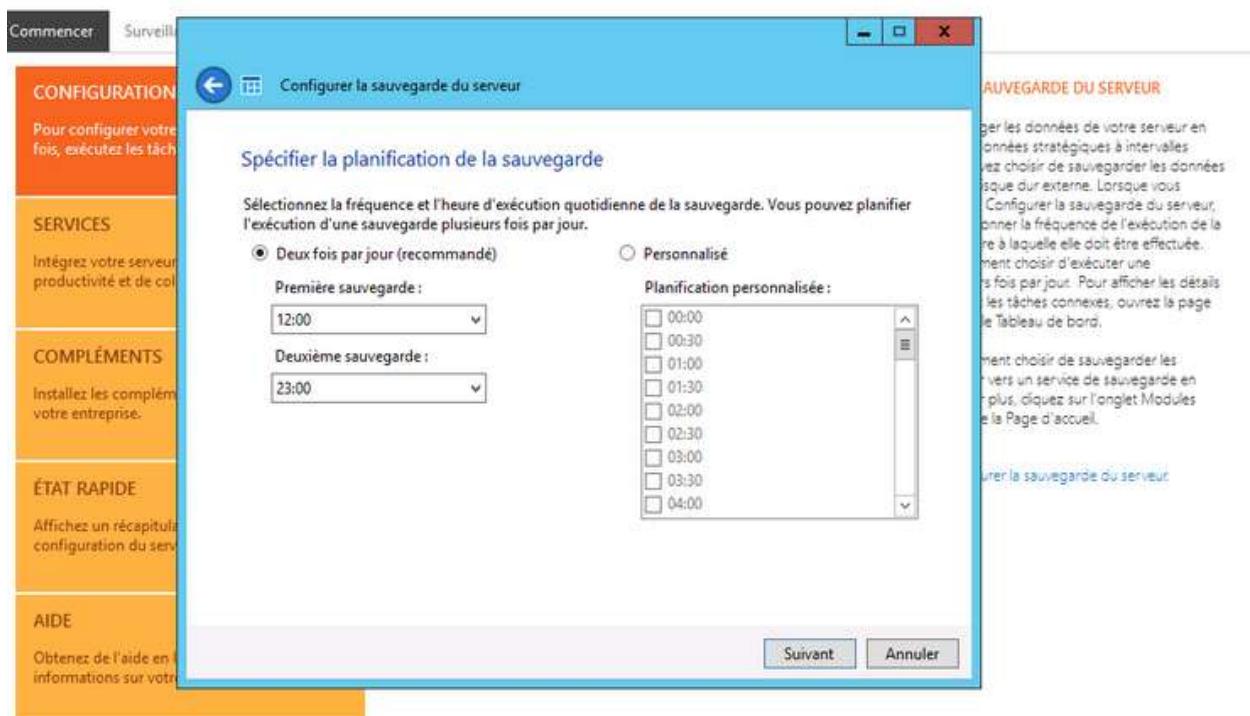
Attention, ce disque sera partitionné :



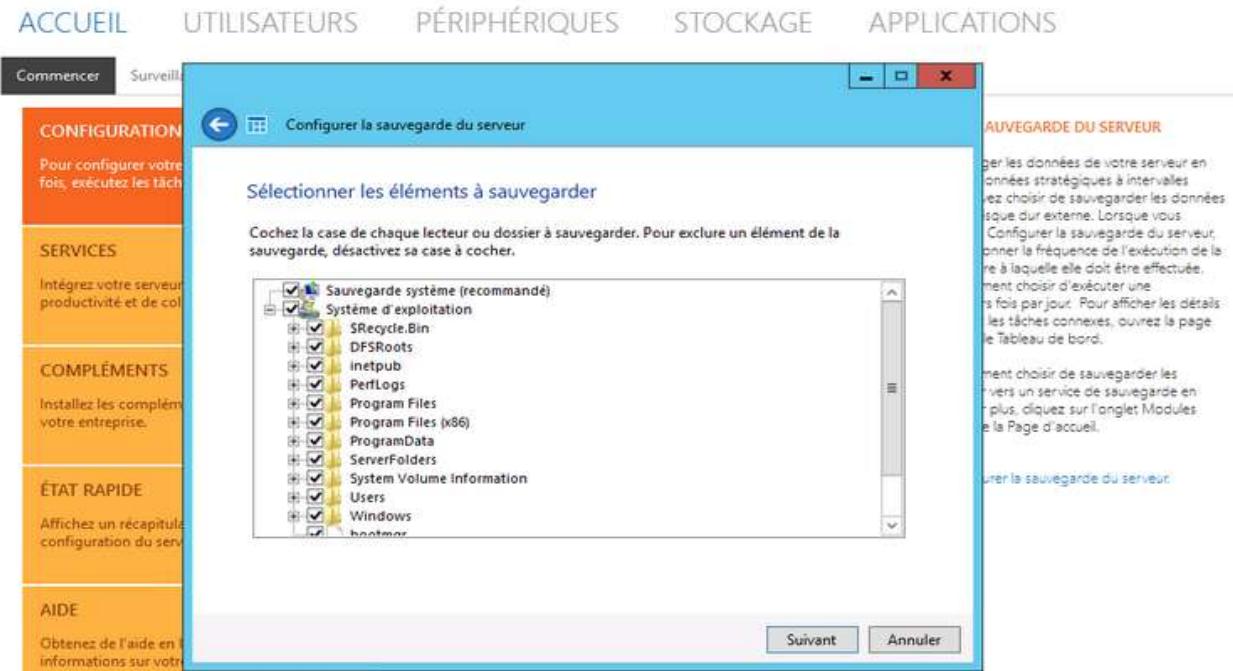
Une fois, la préparation du disque achevée, il faut lui donner un nom :



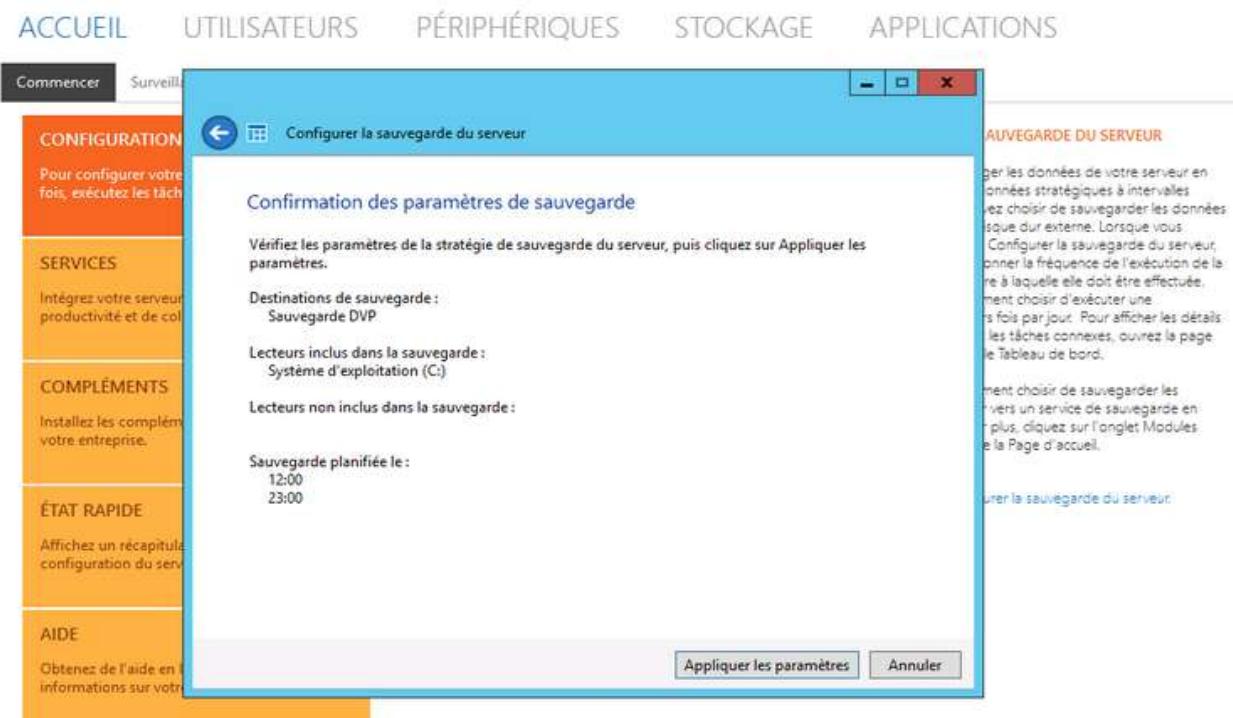
A ce niveau, Nous sommes maintenant à la définition de la planification de notre sauvegarde. Dans notre exemple, nous voulons faire une sauvegarde deux fois par jour, aux heures creuses, pour ne pas impacter l'activité du serveur, pendant les heures de travail:



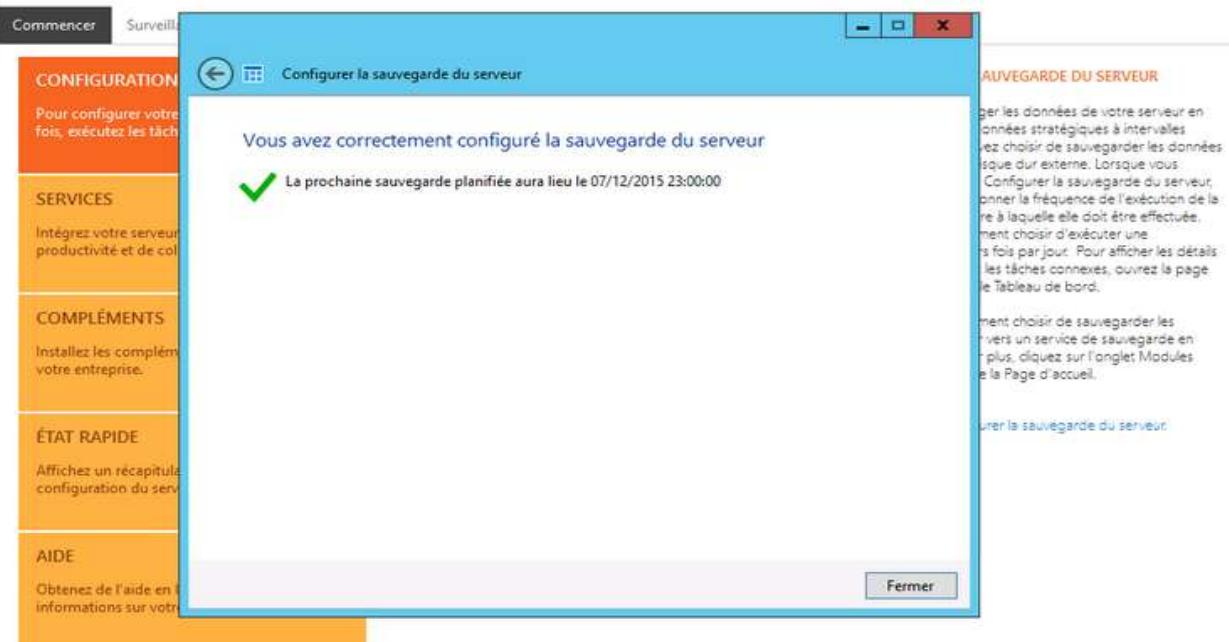
D'abord, Nous choisissons les éléments à sauvegarder :



Ensuite, Il faut appliquer nos paramètres et lancer la configuration :



Enfin! La configuration de notre sauvegarde est achevée :



C. CRÉATION DU PARTAGE RÉSEAU

Retournons encore sur notre tableau de bord pour lancer l'assistant de configuration du partage réseau :

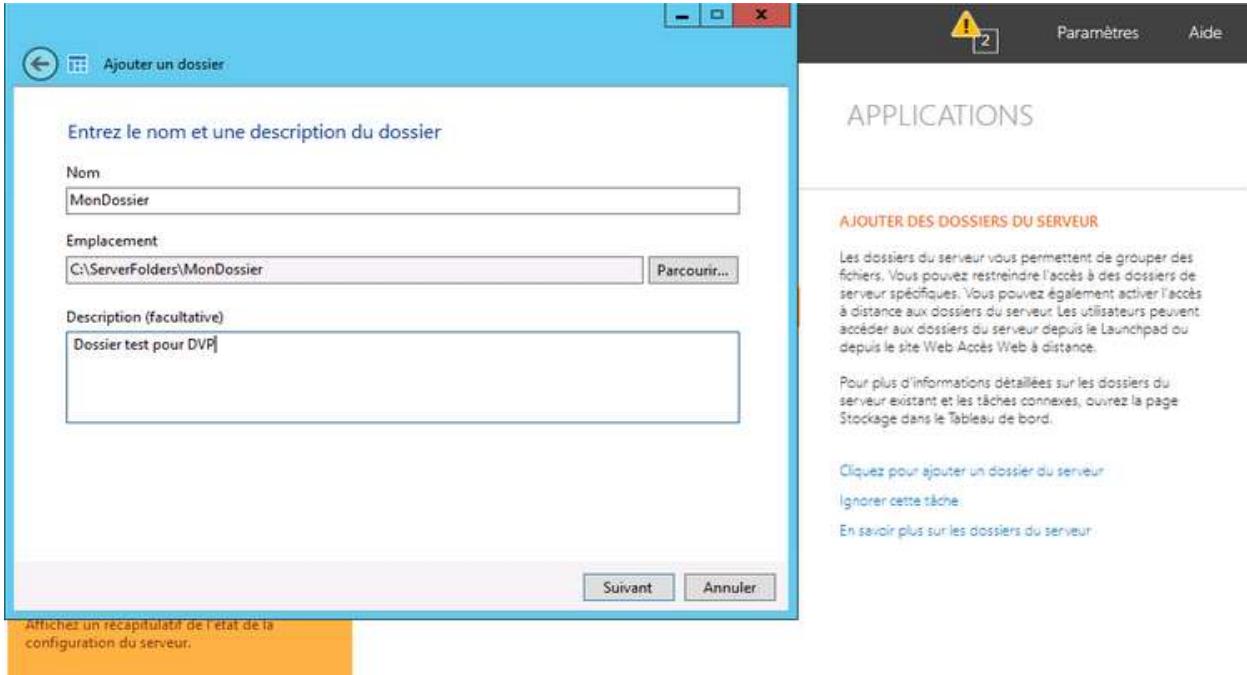
Configuration Task	Status
Obtenir des mises à jour pour les autres produits Microsoft	→
Ajouter des comptes d'utilisateurs	✓
Ajouter des dossiers du serveur	✓
Configurer la sauvegarde du serveur	✓
Configurer l'Accès en tout lieu	Configurer l'Accès en tout lieu
Personnaliser les paramètres du rapport d'intégrité	→
Configurer le service de restauration de client	→
Connecter des ordinateurs	→

CONFIGURER L'ACCÈS EN TOUT LIEU

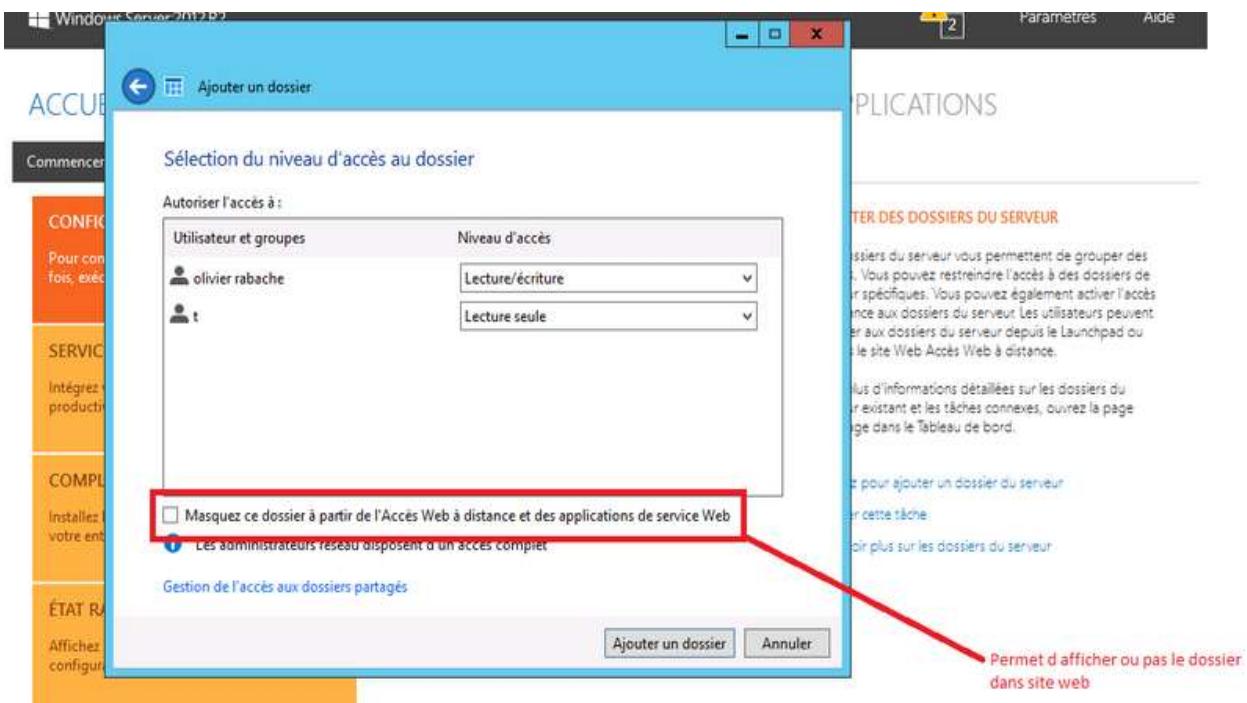
Avec l'Accès en tout lieu, les utilisateurs du réseau peuvent partager et accéder facilement à des fichiers, exécuter des applications et sauvegarder leurs périphériques depuis n'importe quel endroit à l'aide d'un ordinateur ou d'un périphérique compatible Internet.

[Cliquez pour configurer l'Accès en tout lieu](#)
[Ignorer cette tâche](#)
[En savoir plus sur l'Accès en tout lieu](#)

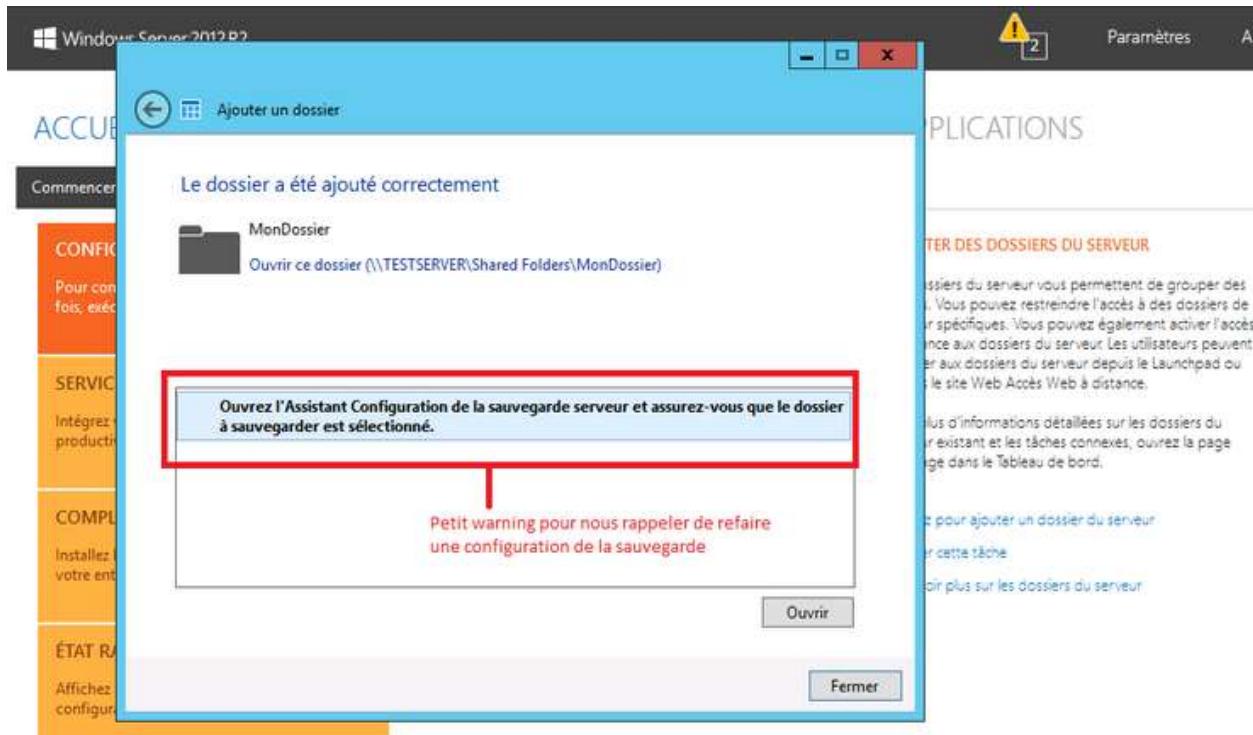
Une fois que l'assistant est chargé, faites « *Suivant* », puis entrez le nom et la description du dossier : « *ici, L'emplacement est généré automatiquement par l'assistant* » :



Il faut définir le niveau d'accès à ce dossier, pour les utilisateurs et/ou les groupes :



Le dossier est créé. Il est important de l'ajouter aux éléments à sauvegarder :



D. CONFIGURATION DE L'ACCÈS DISTANT

Retournons toujours au tableau de bord pour charger l'assistant en cliquant sur « Configurer l'accès en tout lieu » :

ACCUEIL UTILISATEURS PÉRIPHÉRIQUES STOCKAGE APPLICATIONS

Commencer Surveillance de l'intégrité | Rapport d'intégrité |

CONFIGURATION
Pour configurer votre serveur pour la première fois, exécutez les tâches suivantes.

SERVICES
Intégrez votre serveur à des solutions de productivité et de collaboration.

COMPLÉMENTS
Installez les compléments indispensables pour votre entreprise.

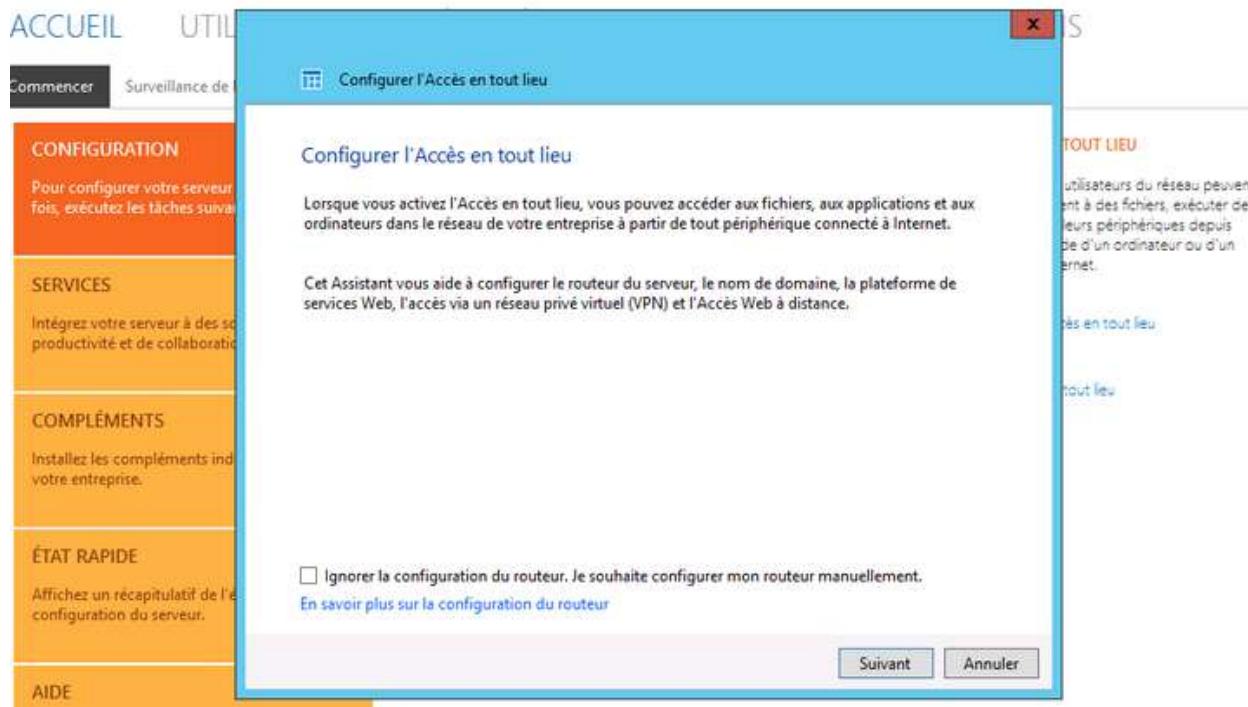
ÉTAT RAPIDE
Affichez un récapitulatif de l'état de la configuration du serveur.

AIDE
Obtenez de l'aide en ligne et d'autres informations sur votre serveur.

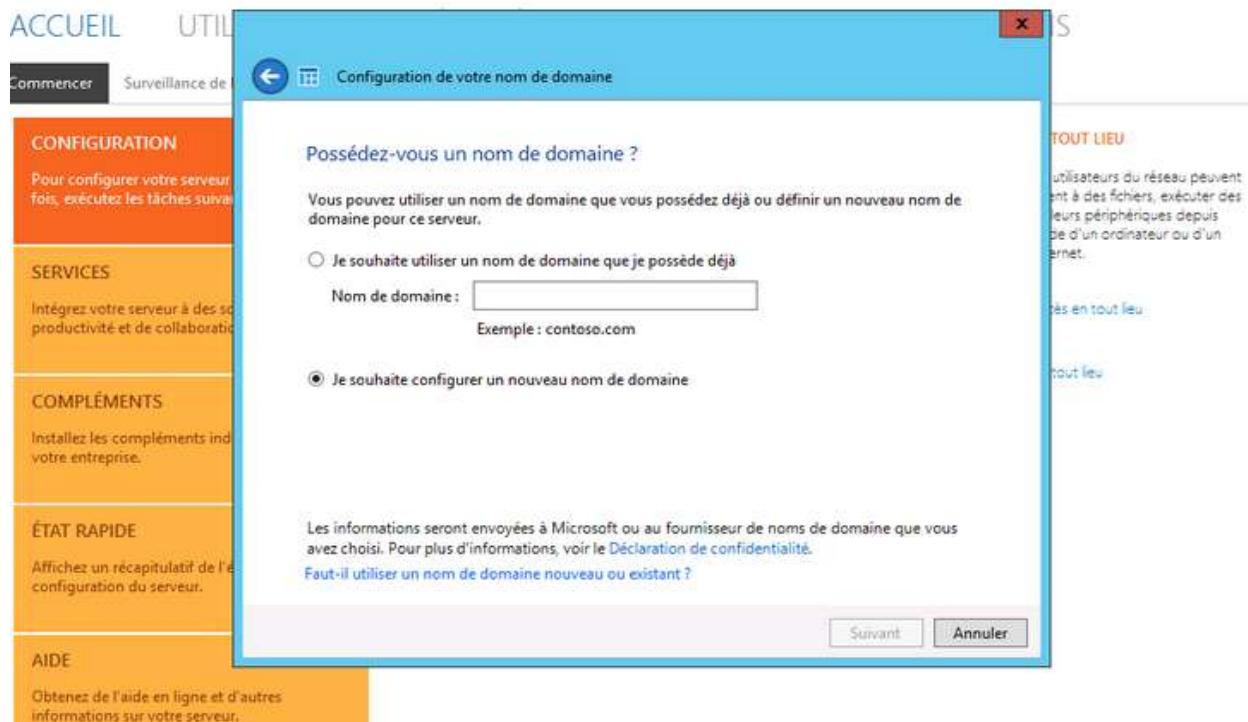
CONFIGURER L'ACCÈS EN TOUT LIEU
Avec l'Accès en tout lieu, les utilisateurs du réseau peuvent partager et accéder facilement à des fichiers, exécuter des applications et sauvegarder leurs périphériques depuis n'importe quel endroit à l'aide d'un ordinateur ou d'un périphérique compatible Internet.

Cliquez pour configurer l'Accès en tout lieu
Ignorer cette tâche
En savoir plus sur l'Accès en tout lieu

L'assistant de la configuration s'ouvre automatiquement :



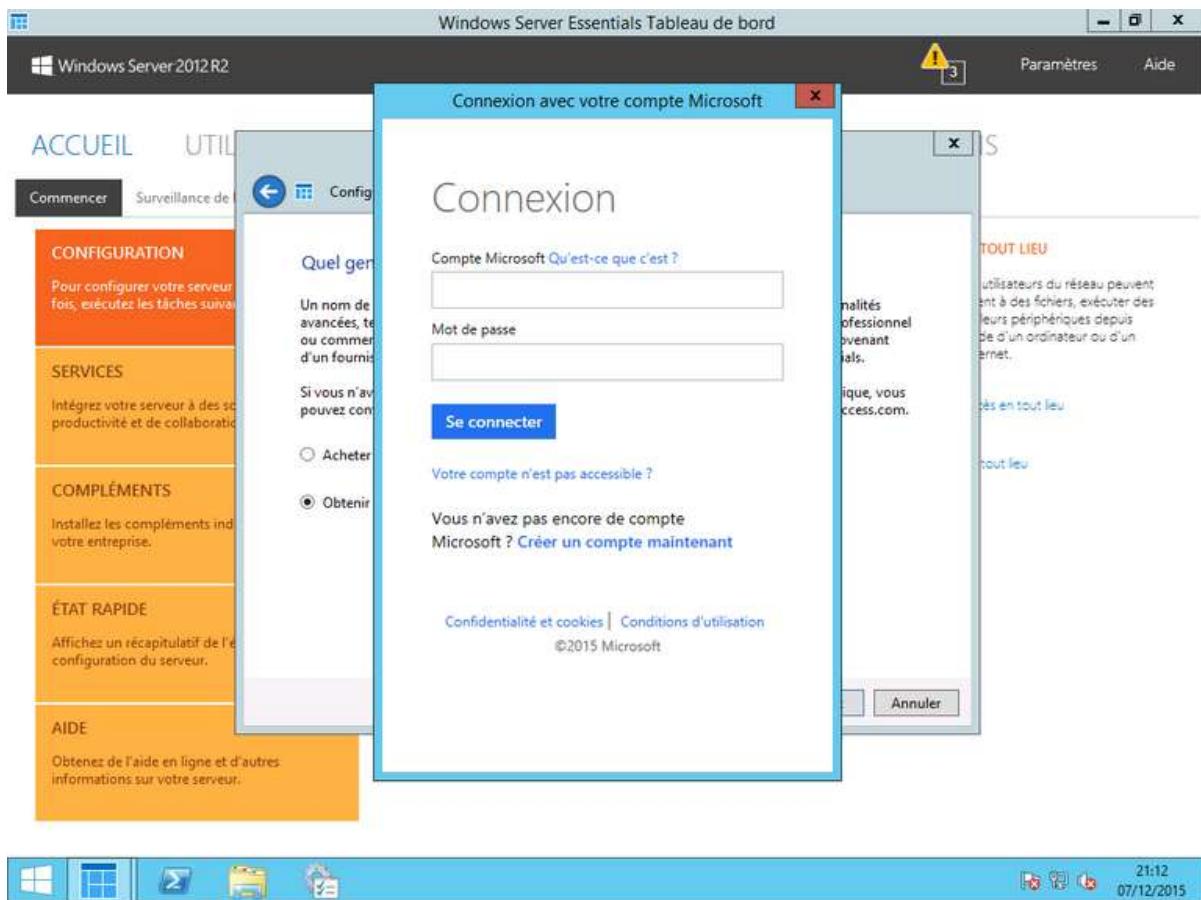
On choisit une option pour la configuration du domaine :



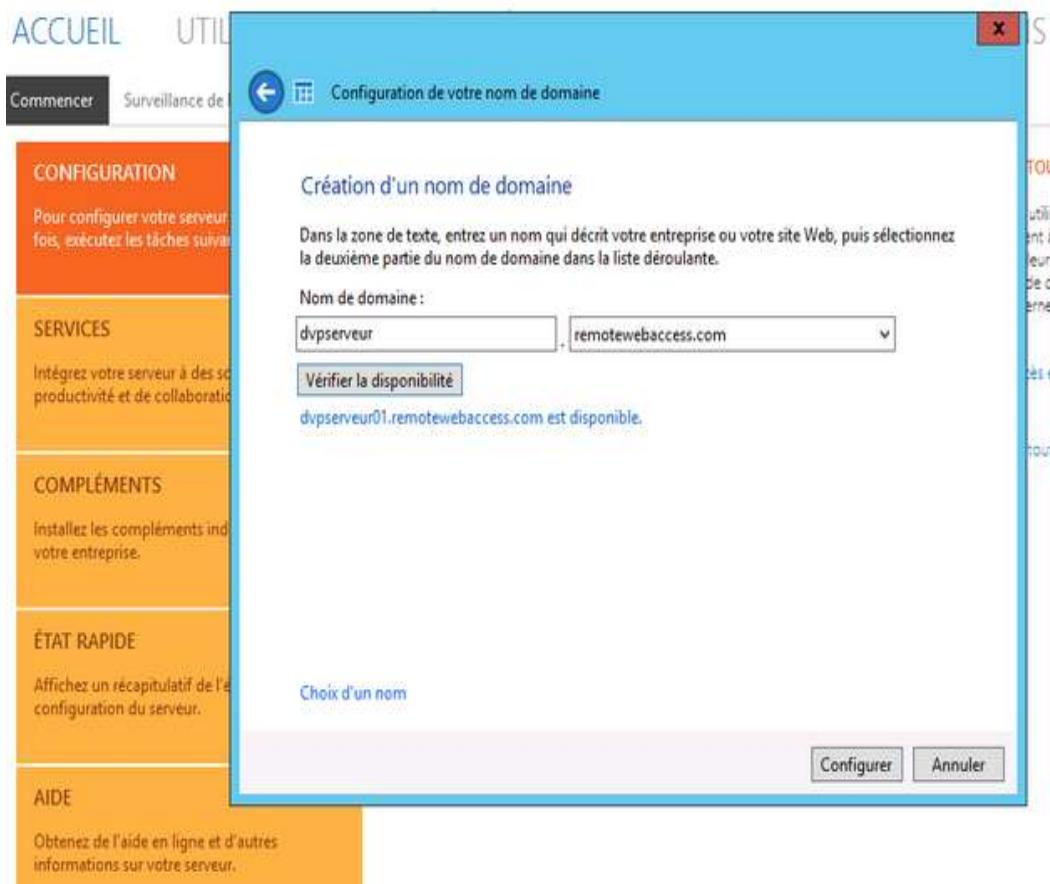
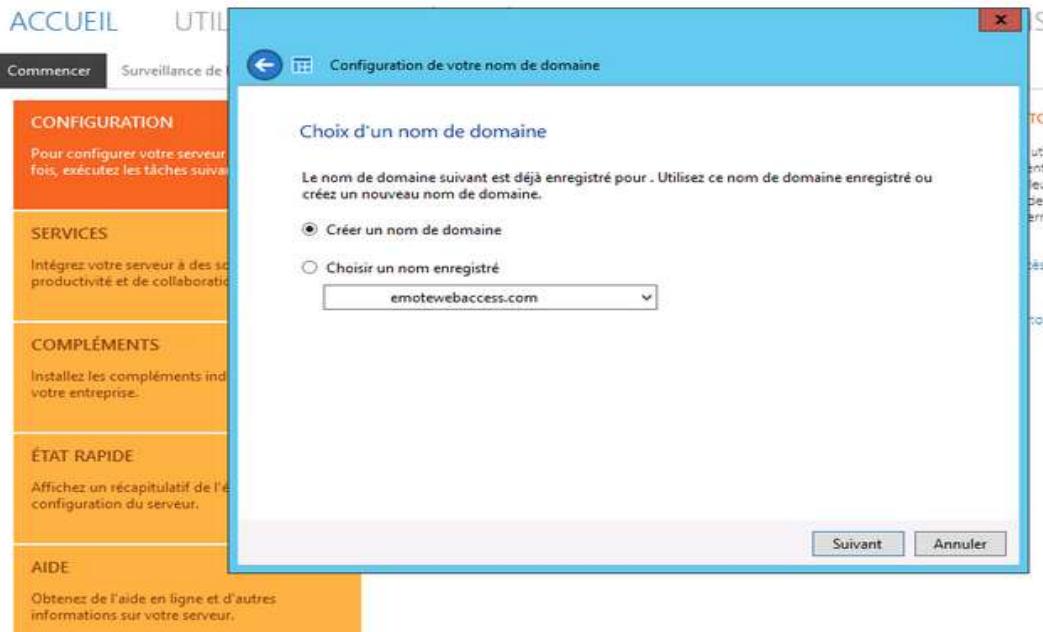
Comme nous pouvons le voir, deux choix s'offrent à nous :

- utiliser un nom de domaine qu'on possède, ce qui veut dire qu'on l'a déjà acheté chez un fournisseur (OVH, Online, etc.) ;
- configurer un nouveau nom de domaine : qui sera créé gratuitement chez Microsoft. Pour cela, il faut posséder un compte Microsoft ou en créer un (toujours gratuit).

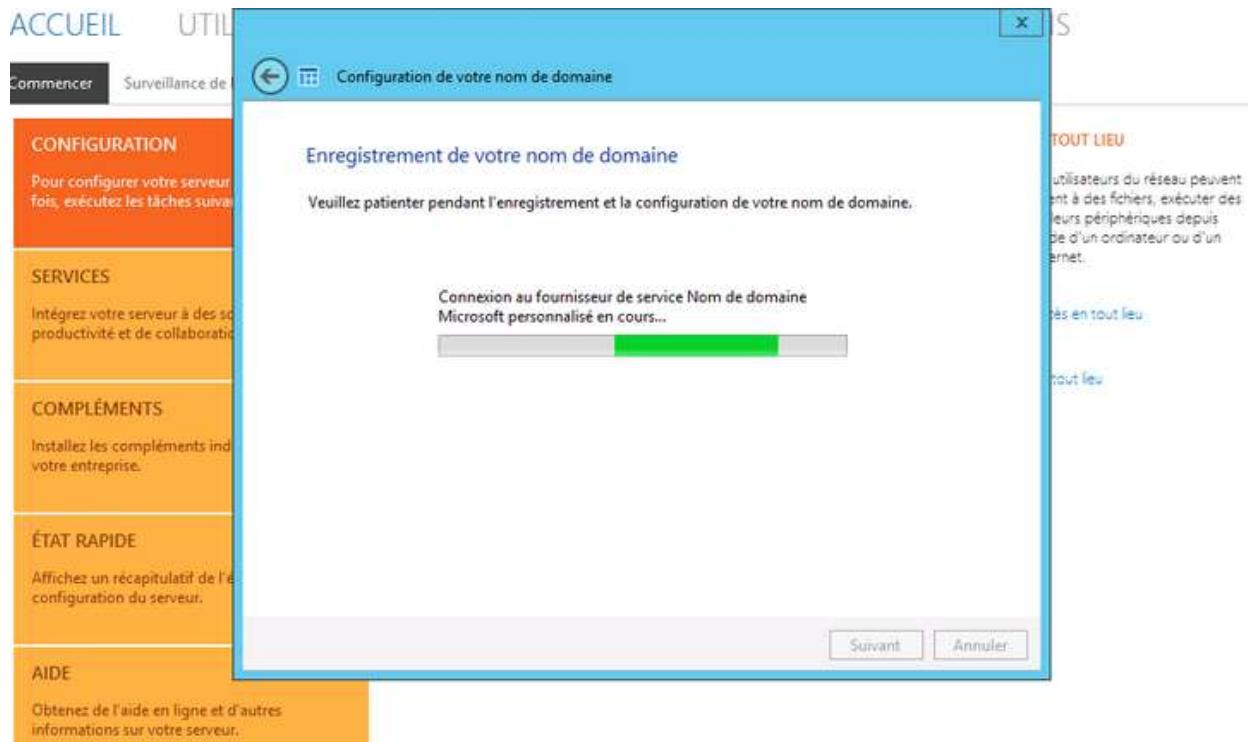
Dans notre exemple nous avons choisi la seconde option avec Microsoft, pour deux raisons : (gratuit, je l'ai déjà dit et pas de problème d'achat de certificat). Ensuite, Connectez-vous avec votre compte Microsoft :



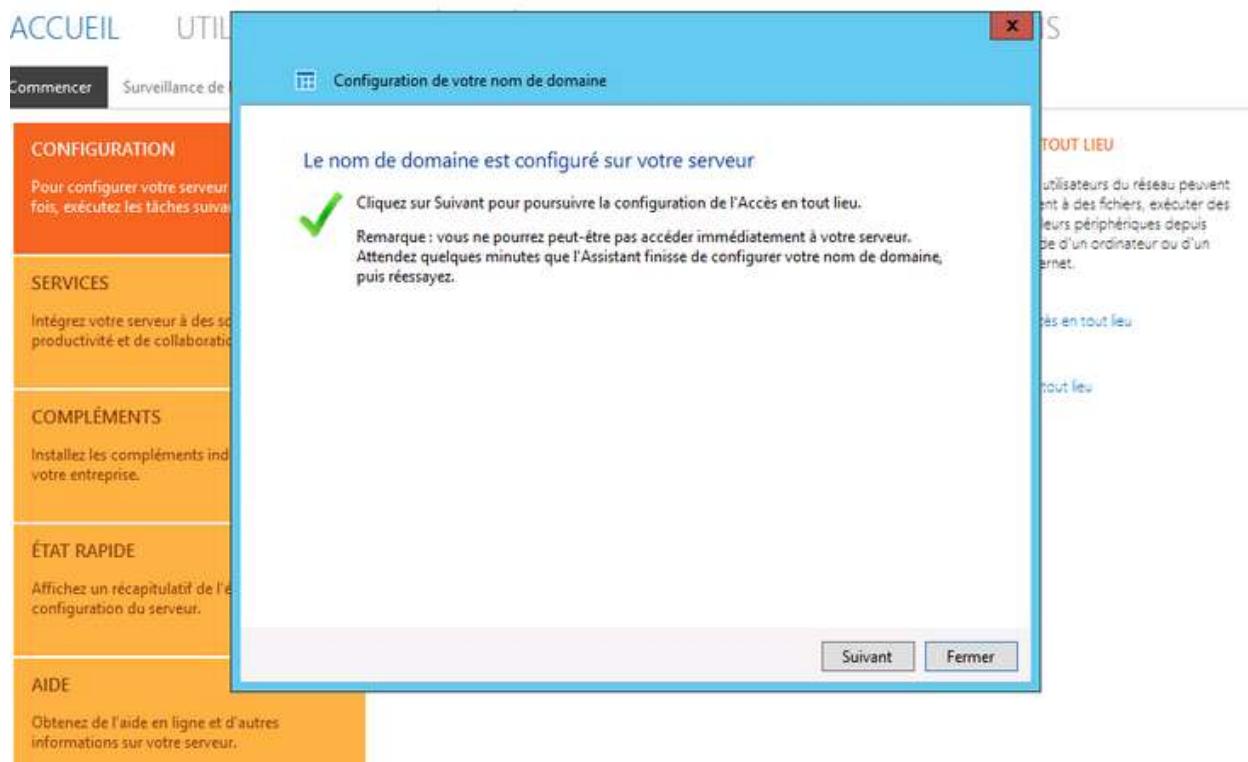
Une fois connecté, on crée son nom de domaine :



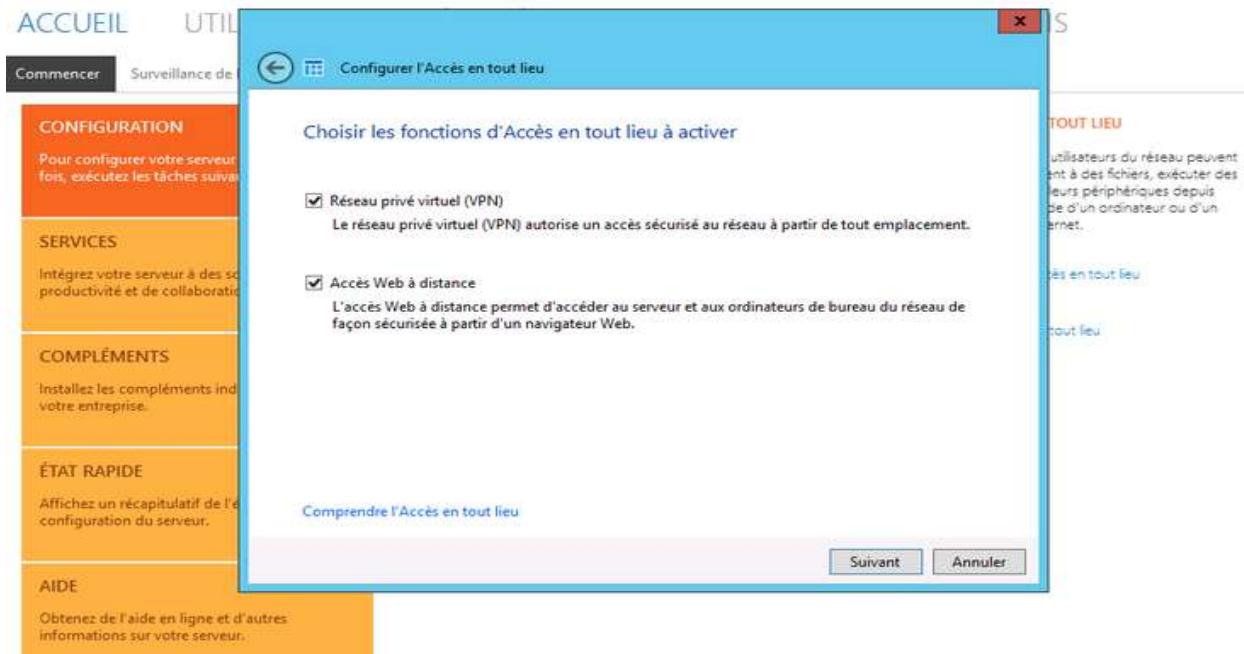
Et on attend la fin de l'enregistrement du nom de domaine :



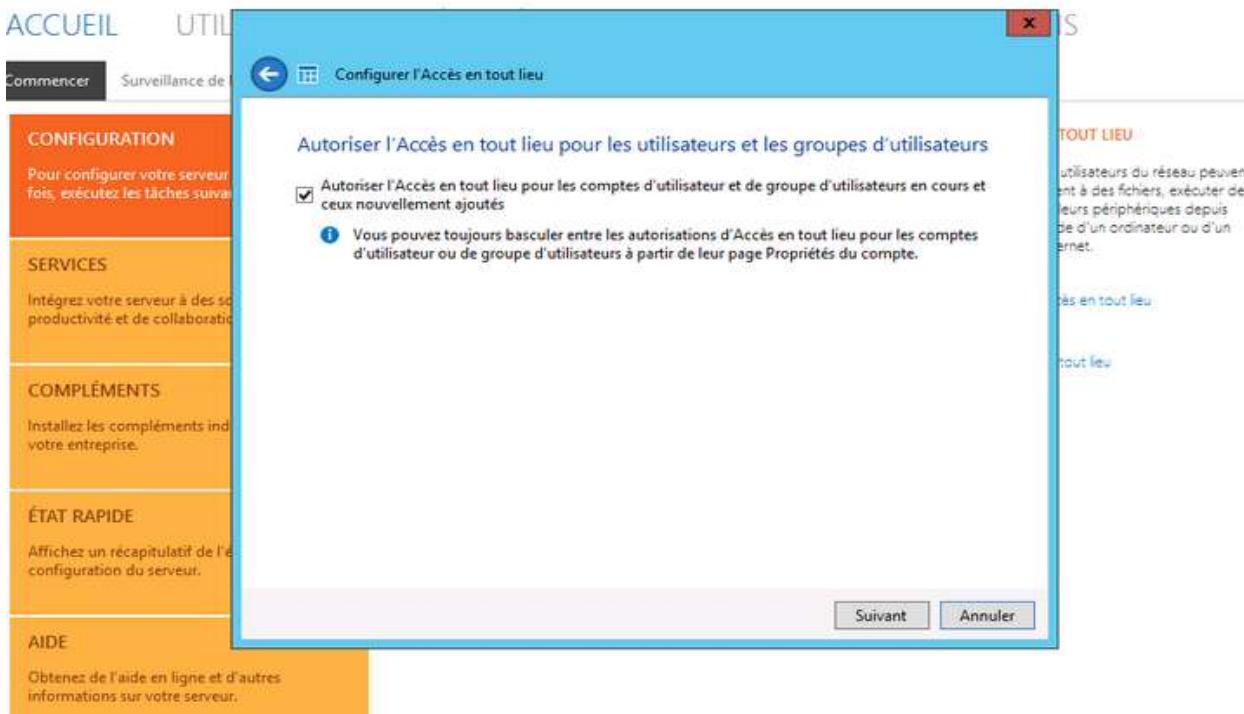
Le domaine est maintenant configuré :



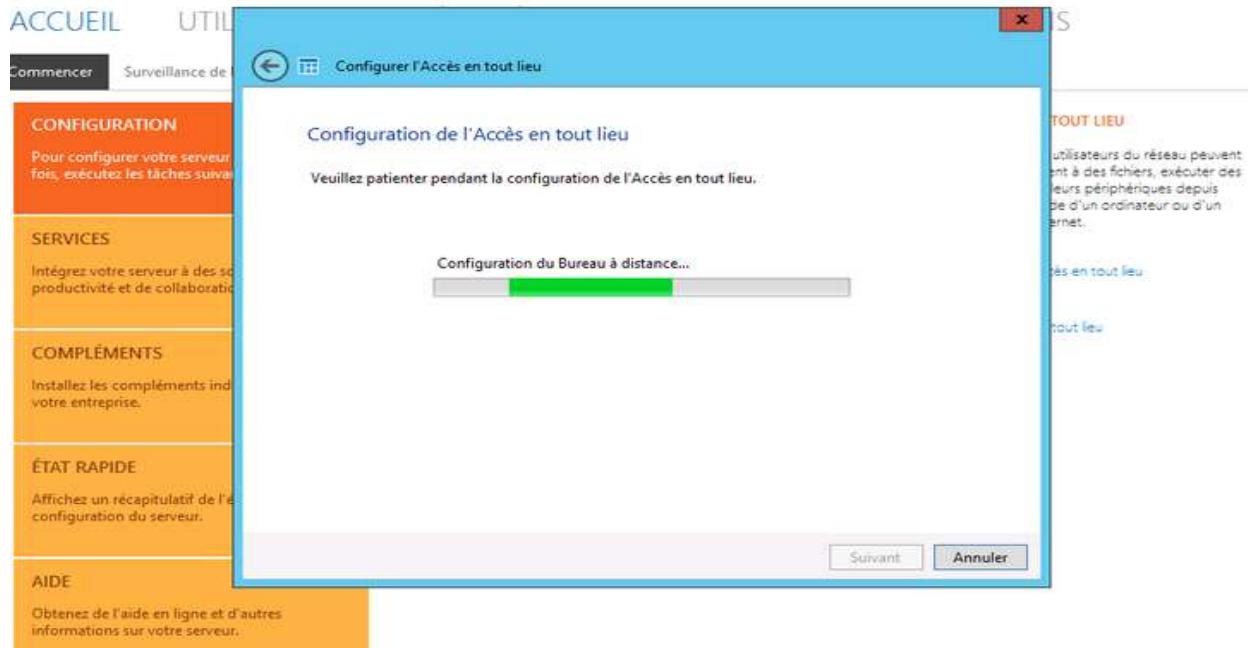
Nous activons alors les fonctions d'accès en tout lieu :



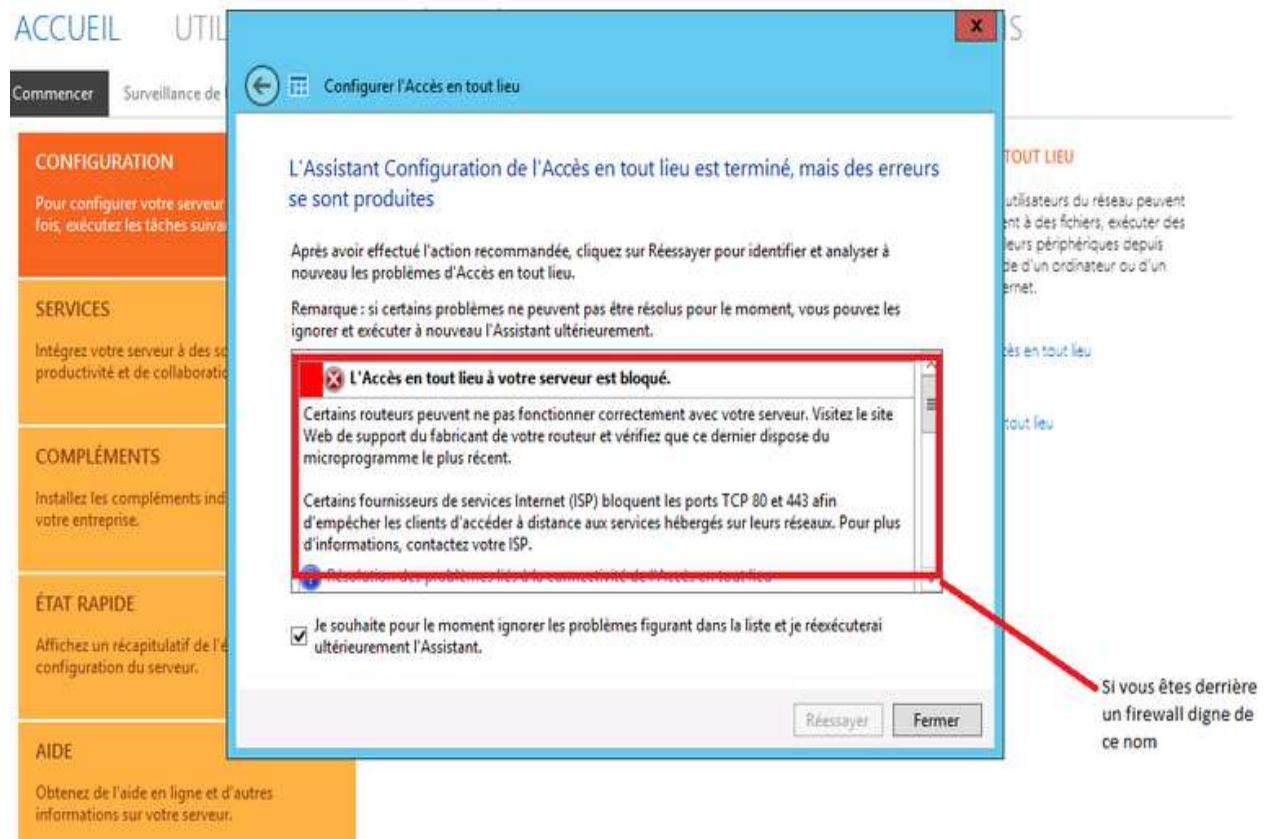
Il faut aussi autoriser cet accès :



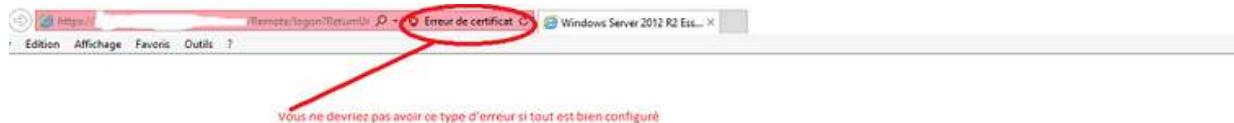
La configuration des nouveaux paramètres se poursuit :



Dans mon cas, j'obtiens un message d'erreur à cause de mon pare-feu qui protège mon serveur. Il faut autoriser la publication du serveur dans le pare-feu réseau.



Une fois la configuration finie, rendez-vous sur votre navigateur internet et entrez l'adresse que vous avez configurée plus haut : (*nom domaine.remotewebaccess.com*). Depuis un site distant (n'importe où via internet) j'accède à mon serveur à partir d'un navigateur : L'erreur ci-dessous est due à un certificat SSL/TLS non valide



Après vous être logué, voici l'interface à laquelle vous avez accès :

Vous avez donc :

- accès par RDP au serveur, si vous êtes administrateur ;
- accès aux différents dossiers du répertoire société ;
- accès au site web Microsoft pour Windows essential.

Si vous vous loguez sur un compte utilisateur, celui-ci ne pourra se connecter.

QUATRIEME CHAPITRE – VUE D’ENSEMBLE DE L’ADMINISTRATION DE MICROSOFT WINDOWS SERVER 2012 R₂.

Le système Windows Server 2012 R2 est un système d’exploitation serveur puissant, souple et complet basé sur les optimisations apportées par Microsoft afin de faciliter l’administration des systèmes informatiques dans toutes ses formes. Cependant, dans ce chapitre, il ne sera pas question de parler de la quasi totalité des fonctionnalités du système Windows server 2012 R2, plutôt, ce chapitre abordera sommairement les points tels que :

- installation du serveur Active Directory / contrôleur du domaine (ADDS) ;
- installation du serveur DNS ;
- installation du serveur DHCP ;
- installation du service SNMP ;
- installation du service DFS.

IV. 1. INSTALLATION DU « ACTIVE DIRECTORY »

Active Directory est le service d'annuaire créé par la société Microsoft, une partie intégrante de l'architecture Windows 2000. Comme d'autres services d'annuaire, tels que Novell Directory Services (NDS), Active Directory est un système centralisé et standardisé qui automatise la gestion du réseau des données utilisateur, de la sécurité et des ressources distribuées, et permet l'interopérabilité avec d'autres répertoires. Active Directory est spécialement conçu pour les environnements réseau.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc.

Active Directory fournit les avantages suivants :

- Nom d'utilisateur et mot de passe unique – Net ID

- Mot de passe synchronisé entre AD et LDAP Directory Services
- Réduire les frais généraux grâce à la normalisation
- Améliorer les services grâce à des fonctionnalités de gestion centralisées
- Fournir des bases pour les services suivants : Exchange et SharePoint.
- Améliorer la sécurité des postes de travail
- Stockage central fourni aux particuliers et aux départements
- Services de sauvegarde et de restauration pour le stockage centralisé
- Espace de stockage du serveur pour les documents utilisateur
- Sauvegarde des données sur les lecteurs à domicile

Il existe **5 rôles** Active Directory qui sont :

- **AD Domain Services (AD DS)** : Annuaire
- **AD Certificate Services (AD CS)** : PKI
- **AD Federation Services (AD FS)** : Ressources partagées
- **AD Right Management Services (AD RMS)** : Sécurisation des données
- **AD Lightweight Directory Services (AD LDS)**

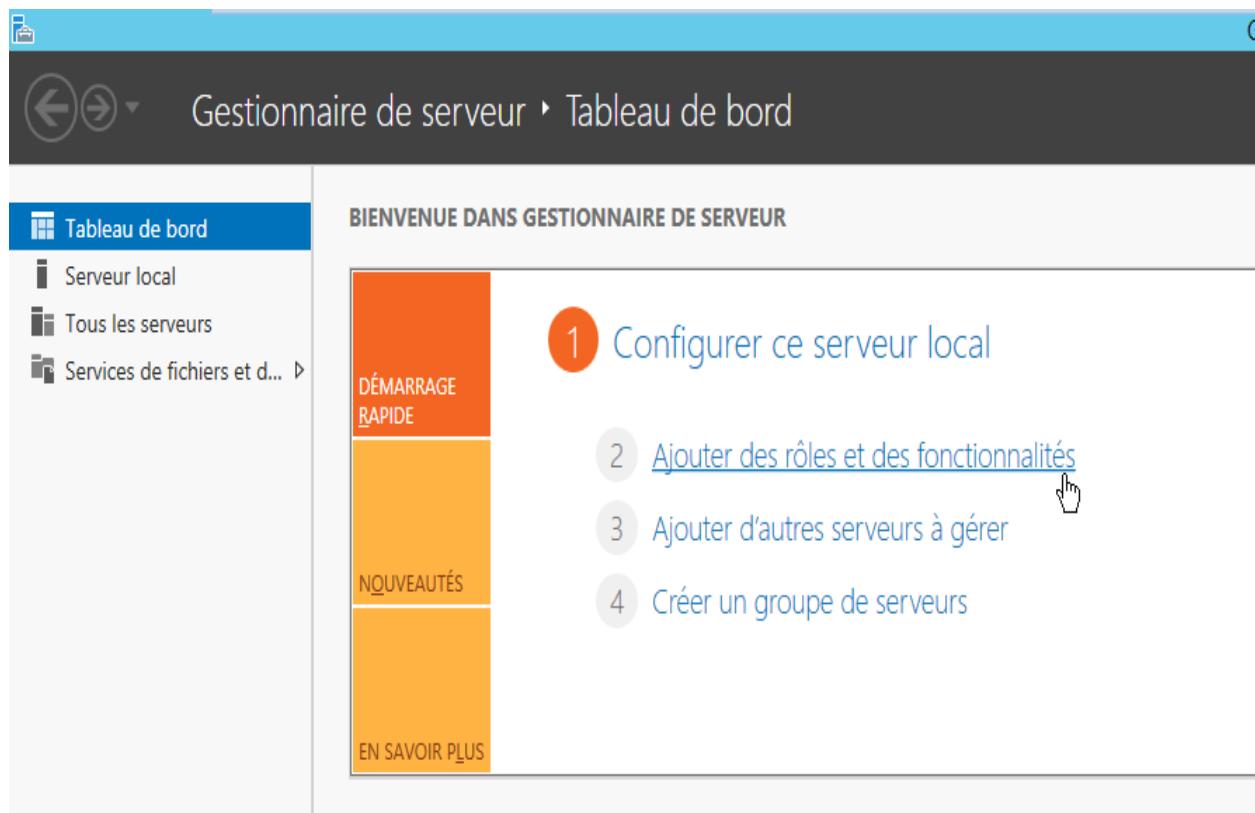
Installer un contrôleur sur Windows Serveur 2012 R2 n'a rien de vraiment compliqué. Cependant pour aller un peu plus loin, il est important de comprendre certaines terminologies :

- **Forêt Active Directory** : Quand vous créez le premier contrôleur de domaine de votre organisation, vous créez le premier domaine (ou domaine *racine de la forêt*) et la première forêt. La forêt Active Directory est un regroupement d'un ou plusieurs arbres de domaine. Un arbre peut avoir un ou plusieurs domaines et une organisation peut disposer de plusieurs forêts. **Une forêt** est une limite de sécurité et d'administration pour tous les objets qu'elle contient.
- **Domaine Active Directory** : Un domaine est une limite d'administration destinée à faciliter la gestion d'objets tels qu'utilisateurs, groupes et ordinateurs. De plus, chaque domaine applique ses propres stratégies de sécurité et relations d'approbation avec les autres domaines.
- **Contrôleur de domaine** : Un contrôleur de domaine est un serveur qui exécute le rôle AD DS. Active Directory est une base de données centrale qui stocke les comptes d'utilisateurs, les comptes d'ordinateurs, des unités organisationnelles, des domaines Active Directory et les forêts. La gestion des utilisateurs, des ordinateurs ou encore l'application de politiques se font depuis l'active directory du serveur (qu'il est possible de lancer via la commande **dsa.msc**).

Ainsi, pour installer et déployer le serveur Active directory, quelques notions de prérequis sont essentielles :

- Un serveur fonctionnel sous **Windows 2012 R2** (vous pouvez vous rendre sur le site de Microsoft pour les spécificités) ;
- Votre serveur doit avoir une **configuration IP statique** ;
- Le compte « **Administrateur** » de votre serveur doit avoir un mot de passe fort, sinon l'installation ne pourra pas se faire (l'AD utilisant ce compte lors de l'initialisation du domaine).

Sur le tableau de bord de votre serveur, cliquez sur « **Ajouter des rôles et des fonctionnalités** » :



Dans la nouvelle fenêtre qui s'ouvre, cliquez sur « **Suivant** » :

Avant de commencer

SERVEUR DE DESTINATION
AS-AD01

Avant de commencer

- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités
- Confirmation
- Résultats

Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.

Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
[Démarrer l'Assistant Suppression de rôles et de fonctionnalités](#)

Avant de continuer, vérifiez que les travaux suivants ont été effectués :

- Le compte d'administrateur possède un mot de passe fort
- Les paramètres réseau, comme les adresses IP statiques, sont configurés
- Les dernières mises à jour de sécurité de Windows Update sont installées

Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.

Cliquez sur **Suivant** pour continuer.

Ignorer cette page par défaut

< Précédent **Suivant >**

[Installer](#)

[Annuler](#)

Cochez « **Installation basée sur un rôle ou une fonctionnalité** », puis cliquez sur « **Suivant** » :

Sélectionner le type d'installation

SERVEUR DE DESTINATION
AS-AD01

Avant de commencer

- ### Type d'installation
- Sélection du serveur
 - Rôles de serveurs
 - Fonctionnalités
 - Confirmation
 - Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

Installation basée sur un rôle ou une fonctionnalité

Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

Installation des services Bureau à distance

Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent **Suivant >**

[Installer](#)

[Annuler](#)

Sélectionnez ensuite le serveur concerné par l'installation (ici « **AS-AD01** »), puis « **Suivant** » :

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
AS-AD01

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Nom	Adresse IP	Système d'exploitation
AS-AD01	172.16.235.10	Microsoft Windows Server 2012 R2 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors ligne et les serveurs nouvellement ajoutés dont la collection de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

Dans la partie « Rôles de serveurs », sélectionnez « Service AD DS » et cliquez sur « Ajouter des fonctionnalités » :

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
AS-AD01

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles et fonctionnalités à installer.

Rôles

- Accès à distance
- Expérience Windows
- Hyper-V
- Serveur d'application
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS
- Serveur Web (IIS)
- Services AD DS
- Services AD FS (édition Premium)
- Services AD LDS
- Services AD RMS
- Services Bureau
- Services d'activation

Assistant Ajout de rôles et de fonctionnalités

Ajouter les fonctionnalités requises pour Services AD DS ?

Vous ne pouvez pas installer Services AD DS sauf si les services de rôle ou les fonctionnalités suivants sont également installés.

[Outils] Gestion de stratégie de groupe
 Outils d'administration de serveur distant
 Outils d'administration de rôles
 Outils AD DS et AD LDS
 Module Active Directory pour Windows PowerShell
 Outils AD DS
 [Outils] Centre d'administration Active Directory
 [Outils] Composants logiciels en fichiers et outils de gestion

Inclure les outils de gestion (si applicable)

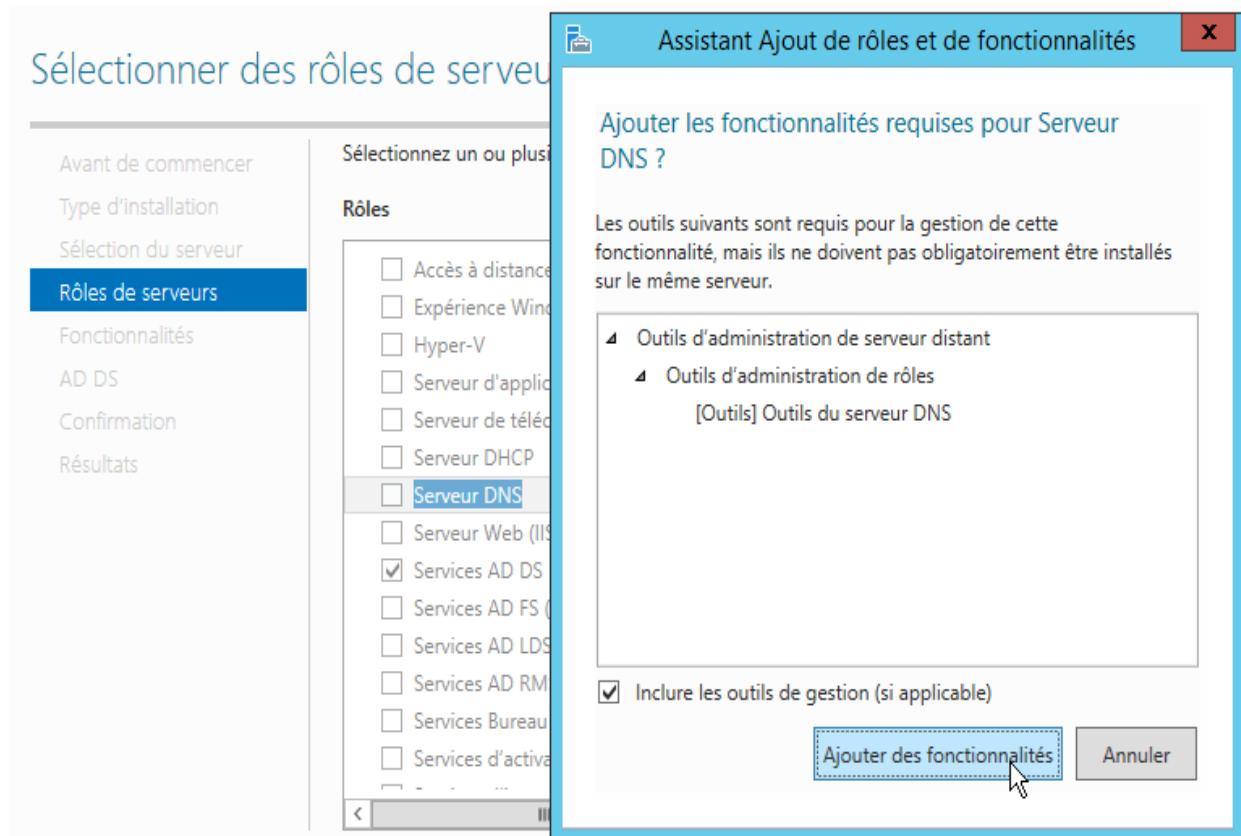
Ajouter des fonctionnalités Annuler

L'installation de « Active Directory » est maintenant terminer.

IV. 2. INSTALLATION DU SERVEUR DNS

Le DNS (Domain Name System) est un service permettant de traduire un nom de domaine à une adresse IP associé. Pour accéder à un site internet nous devons taper son adresse ip, Par exemple 172.217.16.78 pour accéder à Google, par contre pour les utilisateurs, il est difficile de retenir les adresses numériques du genre 172.217.16.78, mais avec un nom alphabétique il est plus facile de retenir les adresses des sites internet, par exemple "www.google.com". Ceci est applicable pour tous les adresses IP. Dans cet article nous verrons comment installer et utiliser un serveur DNS sur un Windows Serveur 2012 et voir les différents enregistrements DNS

Sélectionnez ensuite « **Serveur DNS** », puis une nouvelle fois cliquez sur « **Ajouter des fonctionnalités** » puis « **Suivant** » :



Laissez les fonctionnalités proposées par défaut, puis cliquez sur « **Suivant** » :

Sélectionner des fonctionnalités

SERVEUR DE DESTINATION
AS-AD01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Serveur DNS

Confirmation

Résultats

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités

<input type="checkbox"/> Extension IIS Management OData
<input type="checkbox"/> Extension WinRM IIS
<input type="checkbox"/> Fonctionnalités de .NET Framework 3.5
<input checked="" type="checkbox"/> Fonctionnalités de .NET Framework 4.5 (2 sur 7 ins)
<input checked="" type="checkbox"/> Gestion de stratégie de groupe
<input type="checkbox"/> Gestion du stockage Windows basé sur des normes
<input type="checkbox"/> IFilter TIFF Windows
<input type="checkbox"/> IIS Hostable Web Core
<input checked="" type="checkbox"/> Interfaces utilisateur et infrastructure (2 sur 3 installées)
<input type="checkbox"/> Kit d'administration du Gestionnaire des connexions
<input type="checkbox"/> Media Foundation
<input type="checkbox"/> Message Queuing
<input type="checkbox"/> Moniteur de port LPR
<input type="checkbox"/> MPIO (Multipath I/O)
<input checked="" type="checkbox"/> Outils d'administration de serveur distant

Description

Grâce à l'assistance à distance, vous (ou une personne du support technique) pouvez aider les utilisateurs à résoudre leurs problèmes ou à répondre à leurs questions en rapport avec leur PC. Vous pouvez afficher et prendre le contrôle du Bureau des utilisateurs pour dépanner et résoudre les problèmes. Les utilisateurs ont également la possibilité de solliciter l'aide de leurs amis ou de leurs collègues de travail.

< Précédent **Suivant >** Installer Annuler

Cliquez sur « Suivant »:

Services de domaine Active Directory

SERVEUR DE DESTINATION
AS-AD01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Serveur DNS

Confirmation

Résultats

Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs. Ils sont aussi nécessaires pour certaines applications fonctionnant avec annuaire, telles que Microsoft Exchange Server, et pour d'autres technologies Windows Server, telles que les Stratégies de groupe.

À noter :

- Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine.
- Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur.
- L'installation des services de domaine Active Directory installe aussi les espaces de noms DFS, la réplication DFS et les services de réplication de fichiers nécessaires aux services de domaine Active Directory.

< Précédent **Suivant >** Installer Annuler

Cliquez sur « Suivant » :

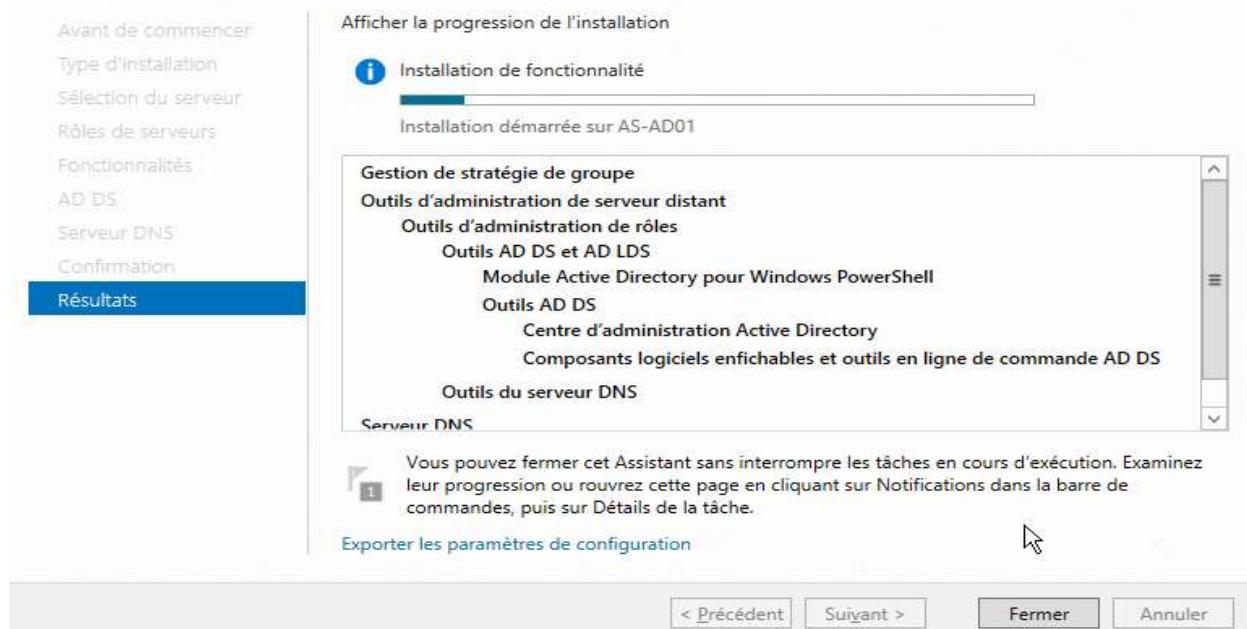
Cocher « Redémarrer automatiquement le serveur de destination, si nécessaire », confirmez avec « Oui » puis cliquez sur « Installer » :

Confirmer les sélections d'installation

Attendez brièvement que l'installation se fasse :

Progression de l'installation

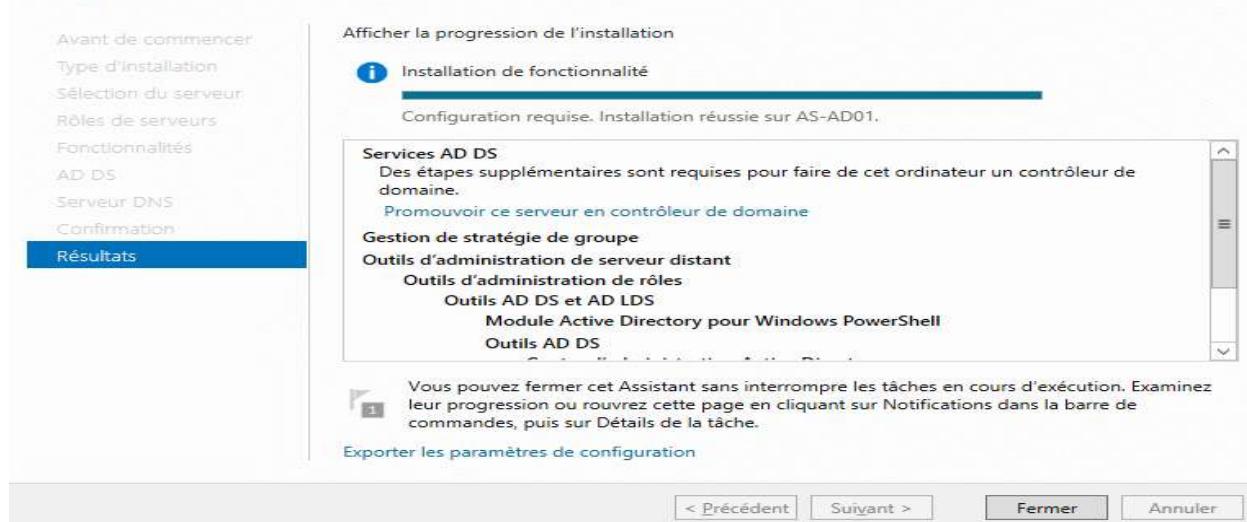
SERVEUR DE DESTINATION
AS-AD01



Une fois l'installation terminée, cliquez sur « Fermer » :

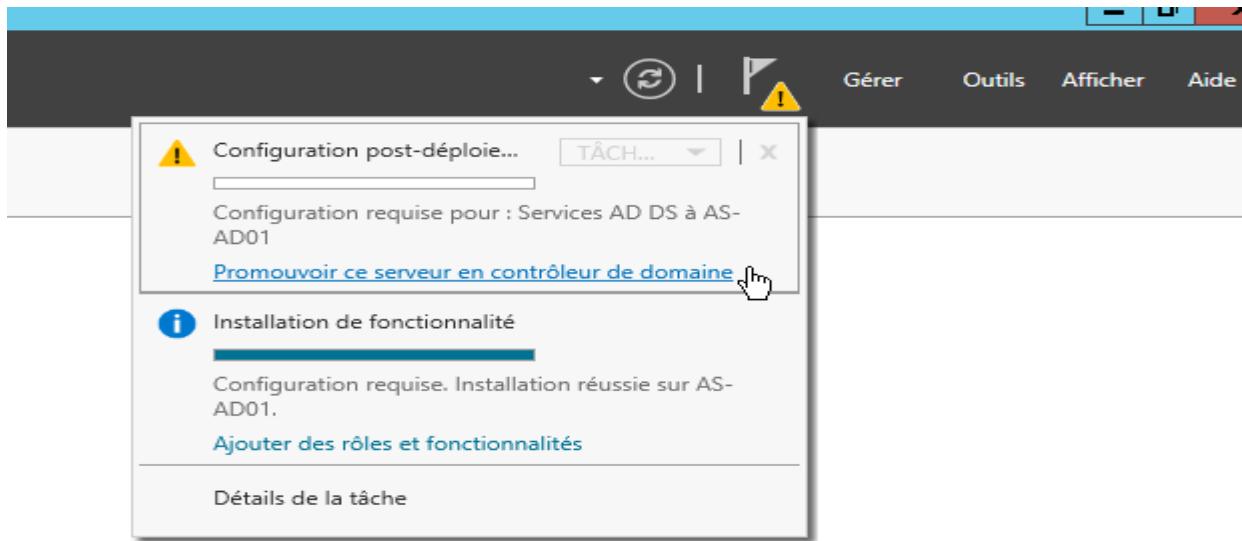
Progression de l'installation

SERVEUR DE DESTINATION
AS-AD01



PROMOUVOIR LE SERVEUR EN CONTROLEUR DE DOMAINE

Dans le tableau de bord de votre serveur, vous verrez en haut à droite qu'un **icône d'avertissement** est apparu près de votre **zone de notifications**. Cliquez dessus, puis sélectionnez « **Promouvoir ce serveur en contrôleur de domaine** » :



Dans cet exemple nous partons de zéro, sélectionnez donc « **Ajouter une nouvelle forêt** » et renseignez le « **Nom de domaine racine** », avant de cliquer sur « **Suivant** » :

Attention : pour que votre « Nom de domaine racine » soit valide, il ne peut pas être en une partie ; vous devez donc au minimum y mettre un « point ».

Configuration de déploiement

**SERVEUR CIBLE
AS-AD01**

Configuration de déploie...

- Options du contrôleur de...
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la config...
- Installation
- Résultats

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

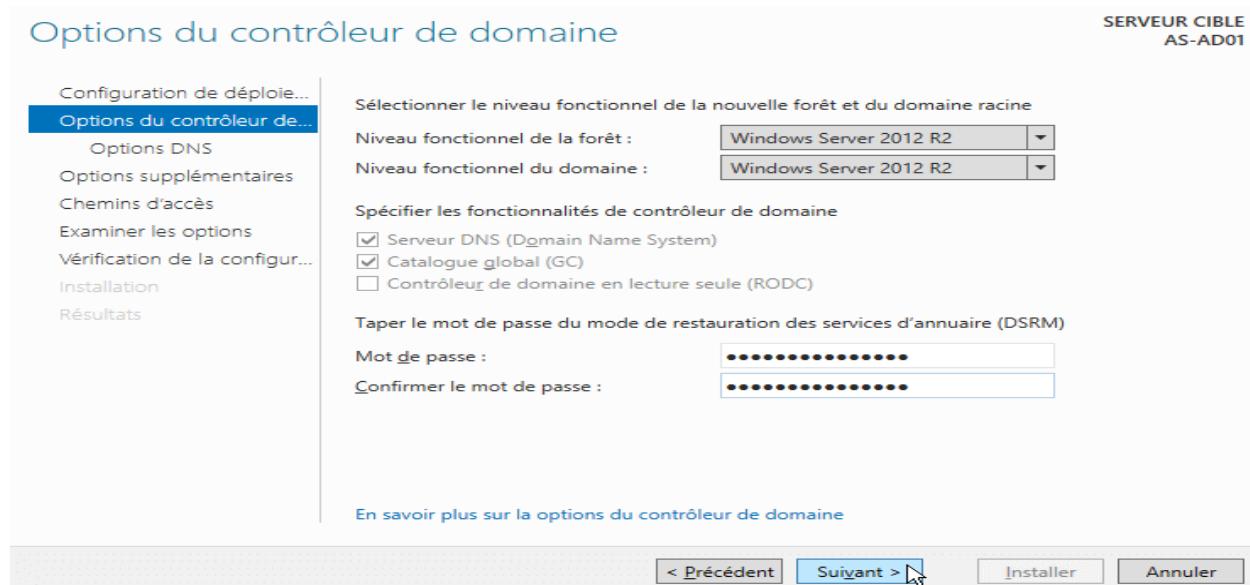
Nom de domaine racine : aide-sys.local

En savoir plus sur la configurations de déploiement

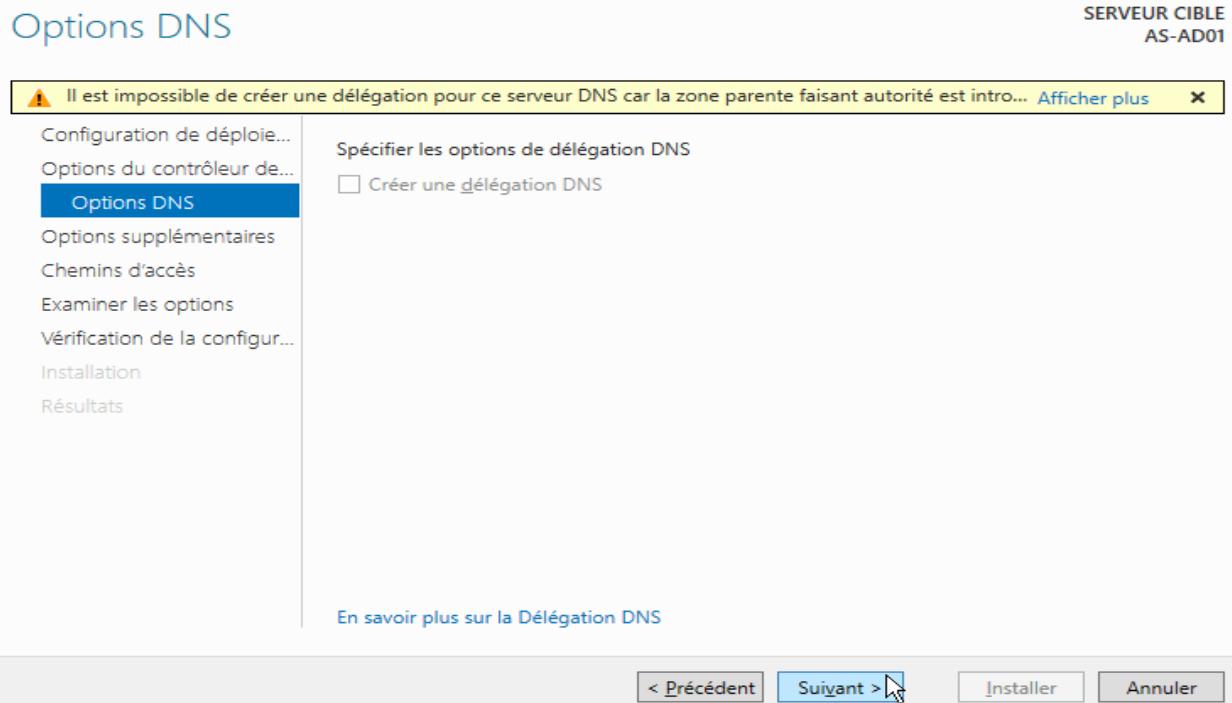
[< Précédent] [Suivant >] [Installer] [Annuler]

Ajoutez un **mot de passe fort** pour DSRM et cliquez sur « **Suivant** » :

DSRM (Directory Services Restore Mode) est une option de démarrage disponible sur les contrôleurs de domaine, permettant la réparation ou encore la restauration d'une base de données Active Directory.

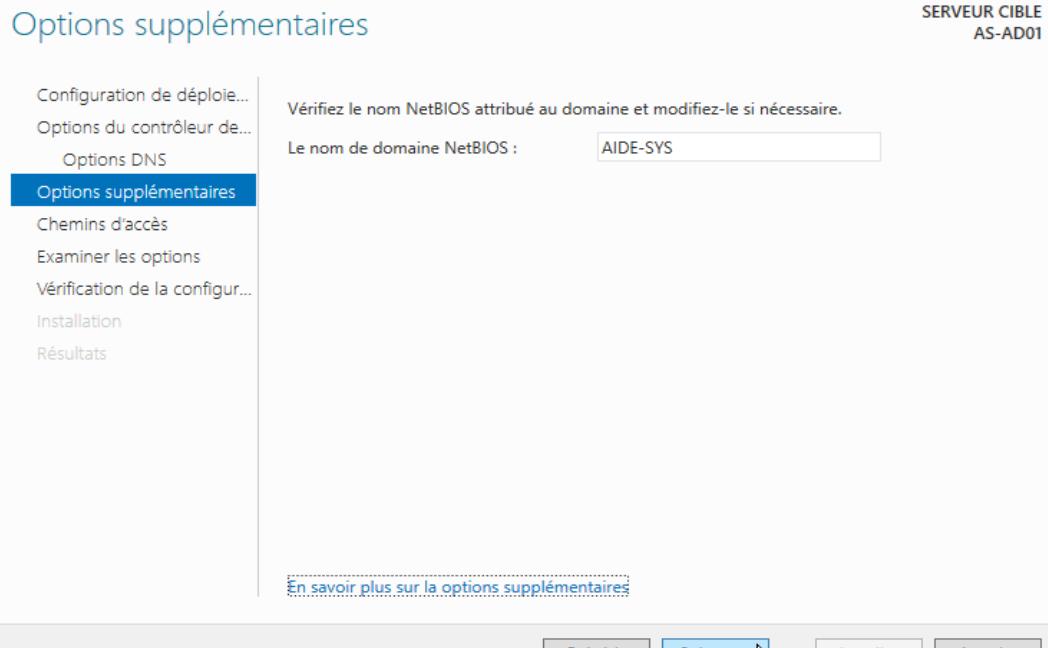


Ne prenez pas attention à l'avertissement, cliquez sur « **Suivant** » :

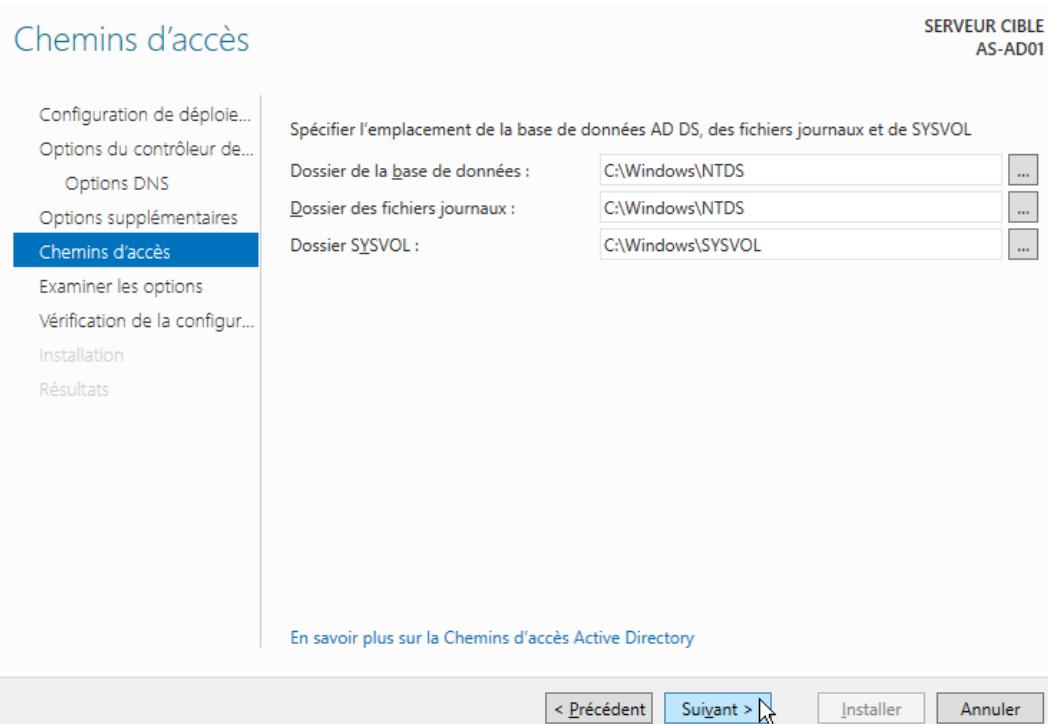


Indiquez ensuite le « **nom de domaine NetBIOS** » désiré, puis faites « **Suivant** » :

Le nom de domaine NetBIOS est le nom simple (par opposition au FQDN défini plus haut) qui sera par exemple utilisé par les utilisateurs pour se connecter au domaine



Cliquez sur « Suivant » :



Cliquez sur « Suivant » :

Examiner les options

SERVEUR CIBLE
AS-AD01

Vérifiez vos sélections :

Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.

Le nouveau nom de domaine est « aide-sys.local ». C'est aussi le nom de la nouvelle forêt.

Nom NetBIOS du domaine : AIDE-SYS

Niveau fonctionnel de la forêt : Windows Server 2012 R2

Niveau fonctionnel du domaine : Windows Server 2012 R2

Options supplémentaires :

Catalogue global : Oui

Serveur DNS : Oui

Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires.

[Afficher le script](#)

[En savoir plus sur la options d'installation](#)

[**< Précédent**](#) [**Suivant >**](#) [**Installer**](#) [**Annuler**](#)

Attendez que la vérification se finisse, ignorez les messages d'erreurs et cliquez sur « Installer » :

Vérification de la configuration requise

SERVEUR CIBLE
AS-AD01

Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... Afficher plus

Configuration de déploi...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur... (highlighted)

Installation

Résultats

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

▲ Voir les résultats

go.microsoft.com/fwlink/?LinkId=104751.

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine « aide-sys.local ». Sinon, aucune action n'est requise.

ⓘ Vérification de la configuration requise terminée

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation.

⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur la conditions préalables](#)

[**< Précédent**](#) [**Suivant >**](#) [**Installer**](#) [**Annuler**](#)

Une fois l'installation terminée, votre serveur redémarre :

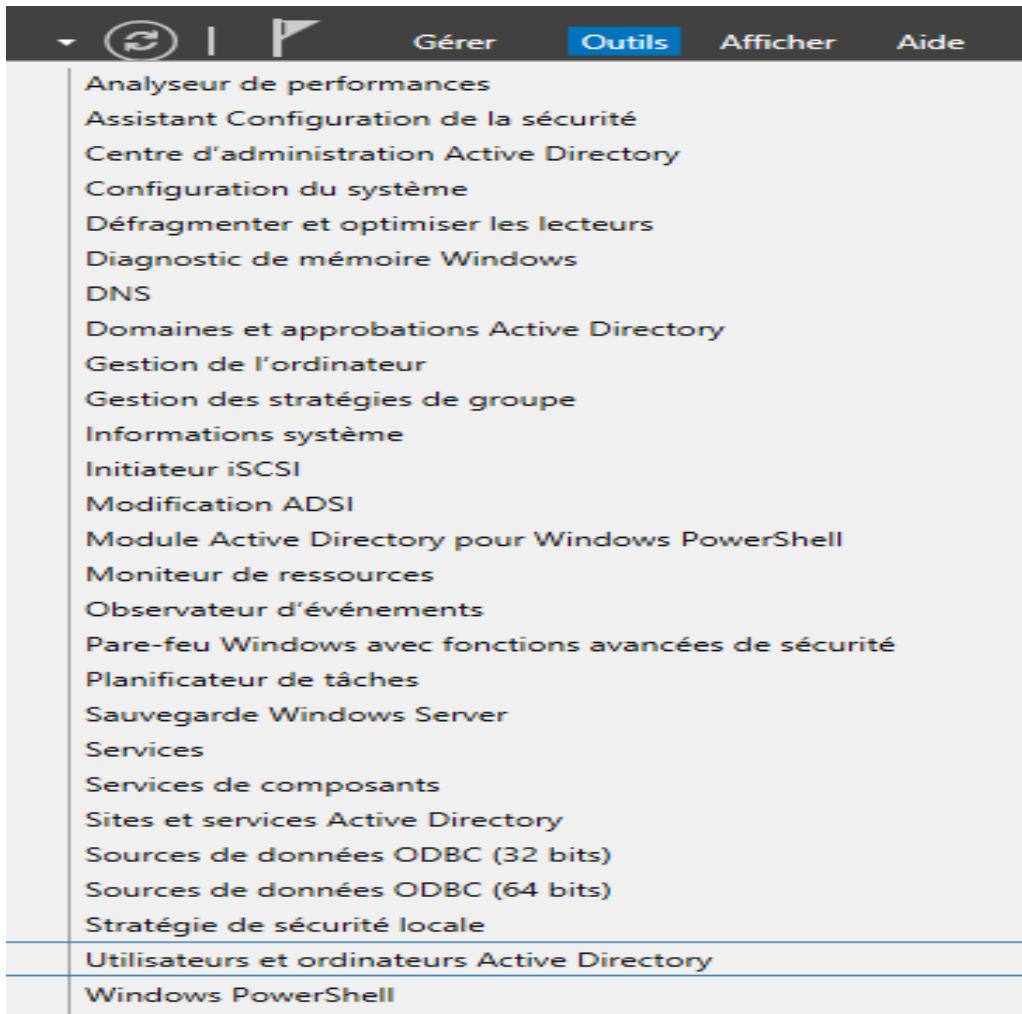


Vérification : Lorsque le serveur est redémarré, il vous propose automatiquement de vous connecter avec un compte sur le domaine créé :



Une fois connecté, pour vous assurer que l'installation est effective :

Tableau de bord > Outils > Utilisateurs et ordinateurs Active Directory :



La fenêtre suivante devrait alors s'ouvrir :

The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' snap-in window. The left pane displays the domain structure:

- Utilisateurs et ordinateurs Active Directory [AS-AD01.aide-sys.local]
 - Requêtes enregistrées
 - aide-sys.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users

The right pane shows a list of objects with their types:

Nom	Type
Builtin	builtinDomain
Computers	Conteneur
Domain Controllers	Unité d'organisation
ForeignSecurityPrincipals	Conteneur
Managed Service Accounts	Conteneur
Users	Conteneur

C'est terminé, vous pouvez configurer et alimenter votre Active Directory.

IV.3. INSTALLATION DU SERVEUR DHCP

Le DHCP (Dynamic Host Configuration Protocol) : Un serveur DHCP délivre des adresses IP de façon automatique aux ordinateurs se connectant au réseau. En plus d'une adresse IP le serveur DHCP vous informe de la configuration réseau tel que la passerelle par défaut et le masque de sous-réseau.

Installer un serveur DHCP sur Windows Serveur 2012 R2 n'a rien de vraiment compliqué. Cependant pour aller un peu plus loin, il est important de comprendre certaines terminologies :

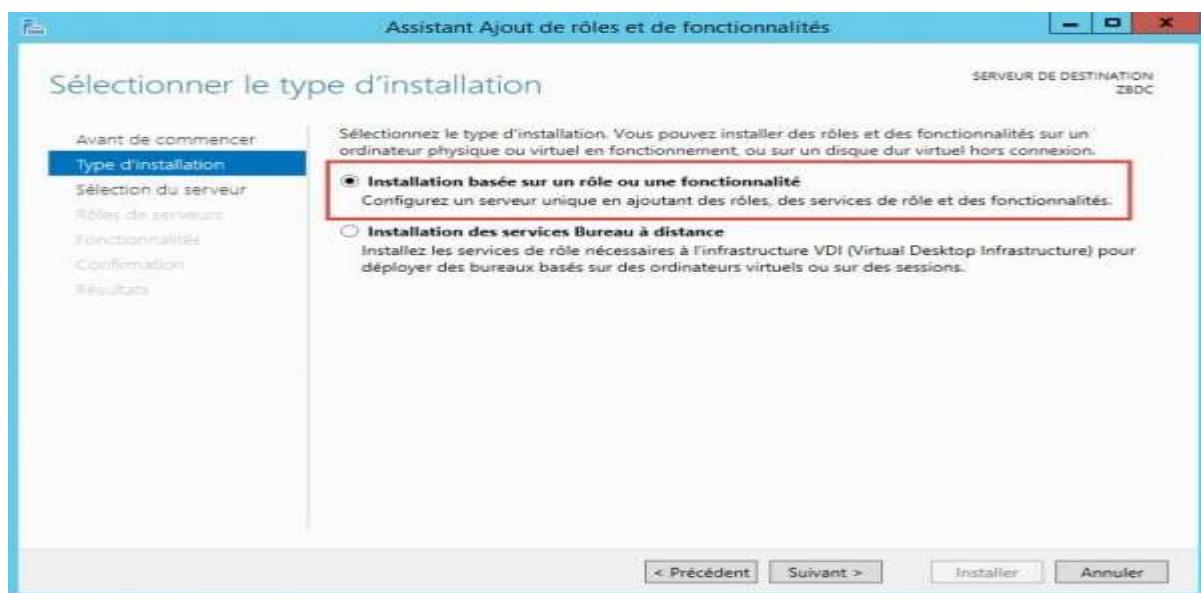
- **Étendue** : Une *étendue* est la plage consécutive complète des adresses IP probables d'un réseau. Les étendues désignent généralement un sous-réseau physique unique de votre réseau auquel sont offerts les services DHCP. Les étendues constituent également pour le serveur le principal moyen de gérer la distribution et l'attribution d'adresses IP et de tout autre paramètre de configuration associé aux clients du réseau.
- **Étendue globale** : Une *étendue globale* est un regroupement administratif des étendues pouvant être utilisé pour prendre en charge plusieurs sous-réseaux logiques IP sur le même sous-réseau physique. Les étendues globales contiennent uniquement une liste d'*étendues membres* ou d'*étendues enfants* qui peuvent être activées ensemble. Les étendues globales ne sont pas utilisées pour configurer d'autres détails concernant l'utilisation des étendues. Pour configurer la plupart des propriétés utilisées dans une étendue globale, vous devez configurer individuellement les propriétés des étendues membres.
- **Plage d'exclusion** : Une *plage d'exclusion* est une séquence limitée d'adresses IP dans une étendue, exclue des offres de service DHCP. Les plages d'exclusion permettent de s'assurer que toutes les adresses de ces plages ne sont pas offertes par le serveur aux clients DHCP de votre réseau.
- **Pool d'adresses** : Une fois que vous avez défini une étendue DHCP et appliqué des plages d'exclusion, les adresses restantes forment le *pool d'adresses* disponible dans l'étendue. Les adresses de pool peuvent faire l'objet d'une affectation dynamique par le serveur aux clients DHCP de votre réseau.

- **Bail** : Un *bail* est un intervalle de temps, spécifié par un serveur DHCP, pendant lequel un ordinateur client peut utiliser une adresse IP affectée. Lorsqu'un bail est accordé à un client, le bail est *actif*. Avant l'expiration du bail, le client doit renouveler le bail de l'adresse auprès du serveur. Un bail devient *inactif* lorsqu'il arrive à expiration ou lorsqu'il est supprimé du serveur. La durée d'un bail détermine sa date d'expiration et la fréquence avec laquelle le client doit le renouveler auprès du serveur.
- **Réservation** : Utilisez une *réservation* pour créer une affectation de bail d'adresse permanente par le serveur DHCP. Les réservations permettent de s'assurer qu'un périphérique matériel précis du sous-réseau peut toujours utiliser la même adresse IP.
- **Types d'options** : Les *types d'options* sont d'autres paramètres de configuration client qu'un serveur DHCP peut affecter lors du service de baux aux clients DHCP. Par exemple, certaines options régulièrement utilisées comprennent des adresses IP pour les passerelles par défaut (routeurs), les serveurs WINS et les serveurs DNS. Généralement, ces types d'options sont activés et configurés pour chaque étendue. La console DHCP vous permet également de configurer les types d'options par défaut utilisés par toutes les étendues ajoutées et configurées sur le serveur. La plupart des options sont prédéfinies via la RFC 2132, mais vous pouvez utiliser la console DHCP pour définir et ajouter des types d'options personnalisés si nécessaire.
- **Classes d'options** : Une *classe d'options* est un moyen pour le serveur de continuer à gérer les types d'options proposés aux clients. Lorsqu'une classe d'options est ajoutée au serveur, les clients de cette classe peuvent être fournis en types d'options spécifiques à la classe pour leur configuration. Pour Microsoft® Windows® 2000 et Windows XP, les ordinateurs clients peuvent également spécifier un ID de classe lorsqu'il communique avec le serveur. Pour des clients DHCP plus récents qui ne prennent pas en charge le processus d'ID de classe, le serveur peut être configuré avec les classes par défaut à utiliser lors du placement des clients dans une classe. Les classes d'options peuvent être de deux types : les classes de fournisseurs et les classes d'utilisateurs.

Avant de commencer, Il est nécessaire de configurer son serveur en **IP fixe** et de l'avoir renommé. Nommer votre serveur en fonction de la convention de nommage de votre entreprise. Ici, nous installerons le rôle DHCP sur notre contrôleur de domaine, celui-ci porte déjà le nom **ZBDC** (**ZB** pour **ZeroBug**, mon domaine et **DC** pour **Domain Controller**). Et depuis le **Gestionnaire de serveur**, cliquer sur l'étape **Gérer** puis **Ajouter des rôles et fonctionnalités** :



Sélectionner le type d'installation « **Installation basée sur un rôle ou une fonctionnalité** ».

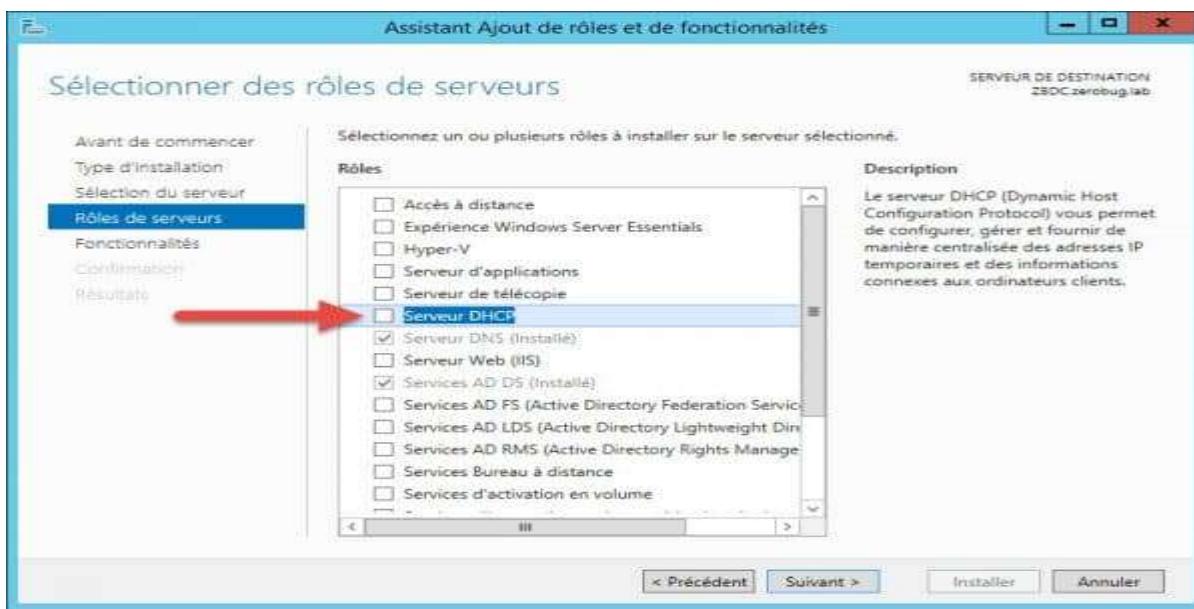


Pour le moment, j'ai qu'un seul serveur dans le pool, j'ai donc juste à le sélectionner et cliquez sur **Suivant** :

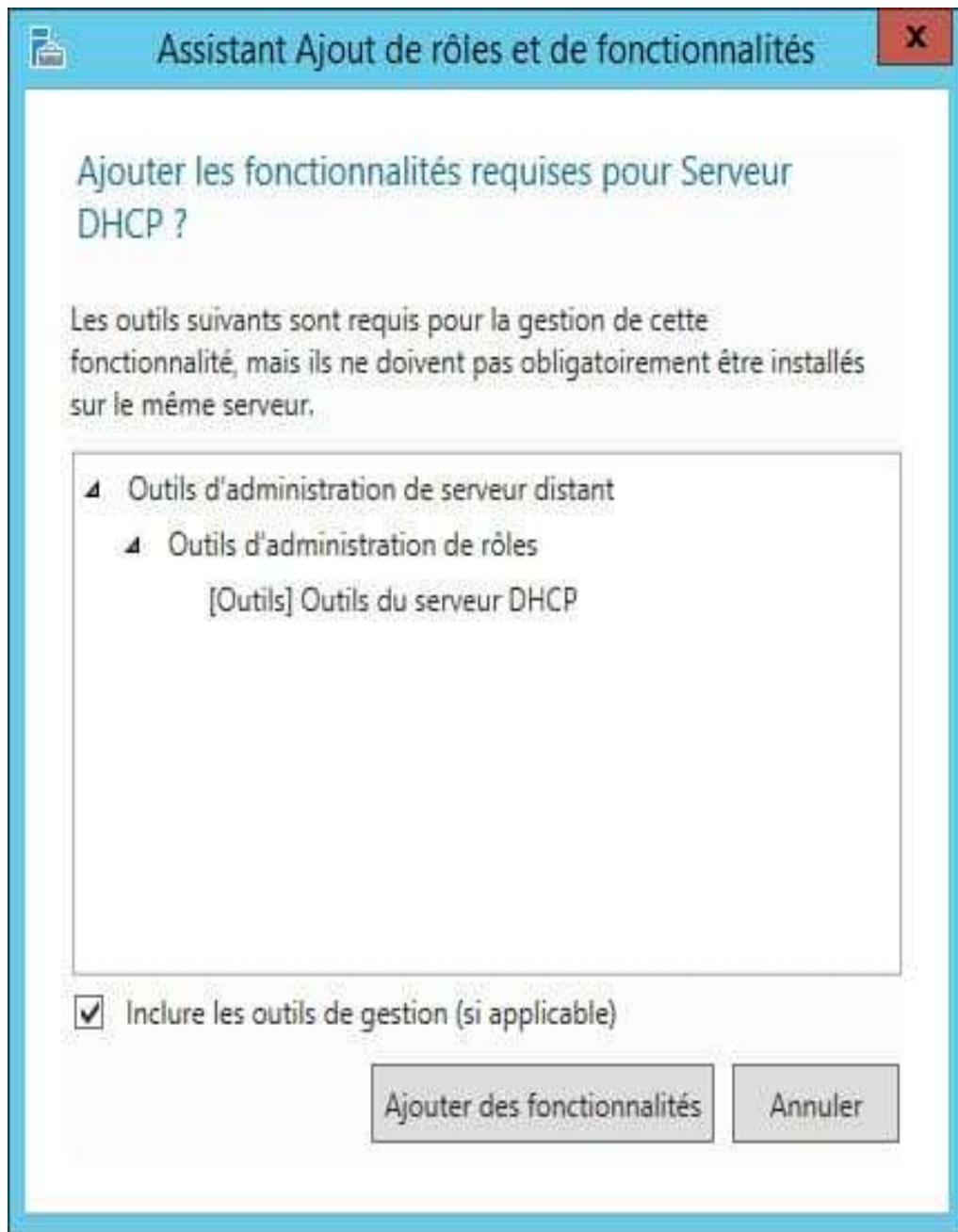


Vous êtes maintenant sur la fenêtre de sélection des rôles. Nous allons donc installer le rôle DHCP. Pour cela, cocher simplement **DHCP** dans la fenêtre de sélection des rôles.

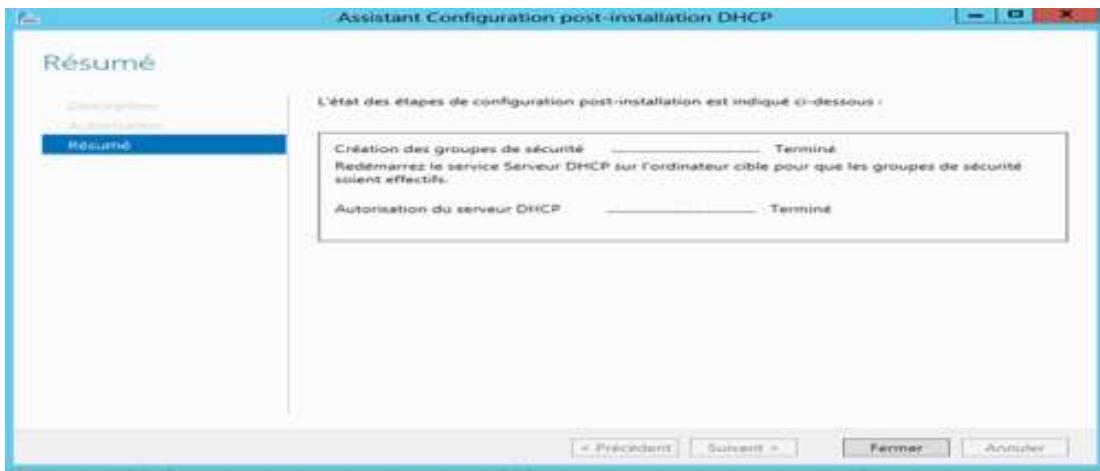
Enfin, cliquer sur **Suivant**:



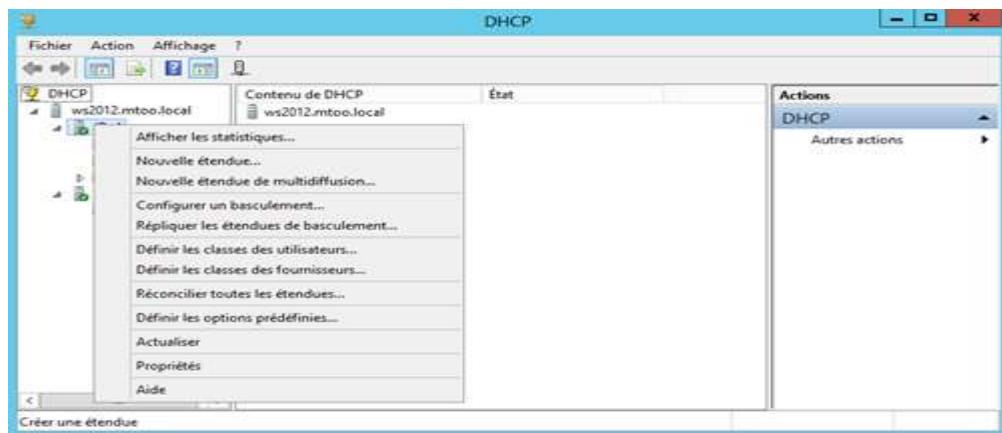
Des fonctionnalités supplémentaires sont automatiquement sélectionnées pour vous, ajoutez-les :



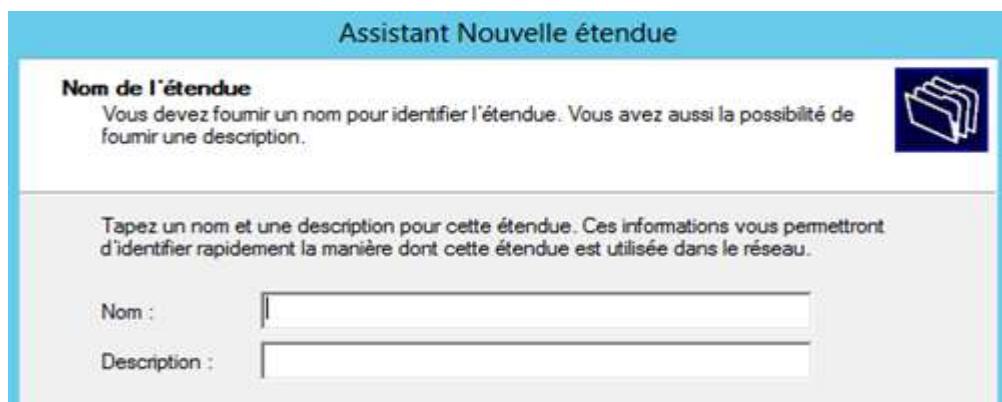
Après avoir ajouté des rôles, vous pouvez ajouter des fonctionnalités supplémentaires. En général, toutes les caractéristiques qui sont nécessaires pour soutenir le rôle de cible sont déjà sélectionnées de sorte que vous pouvez simplement cliquer sur le bouton Suivant pour continuer. Vous aurez alors quelques infos sur le rôle que vous êtes en train d'ajouter. Cliquez sur suivant après en avoir pris connaissance.



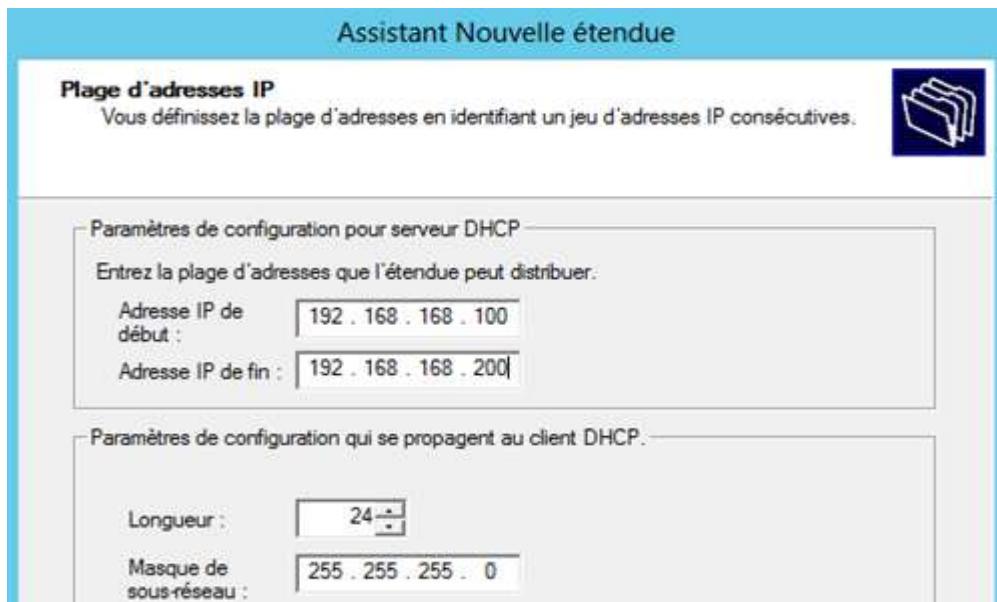
Vous devez maintenant créer vos étendues DHCP à l'aide de la console d'administration DHCP que vous pouvez lancer depuis le menu Outils du gestionnaire de serveur. Pour créer une étendue IPV4, cliquez avec le bouton droit sur IPV4, puis en choisissant Nouvelle étendue



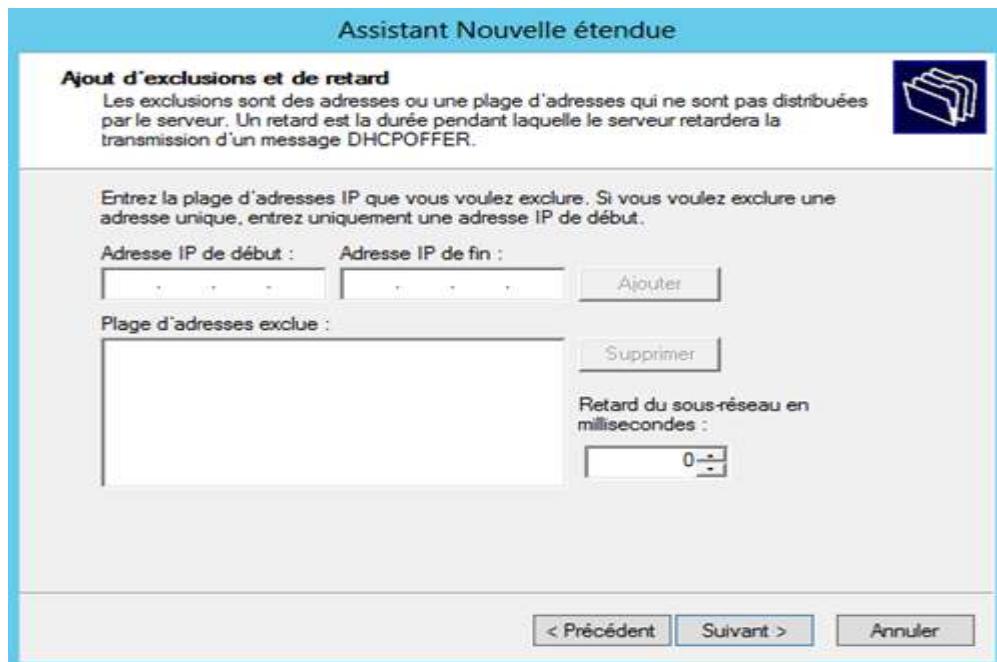
L'assistant de création de nouvelle étendue vous permettra ensuite : Quant à vous, de donner un nom et une description à votre étendue



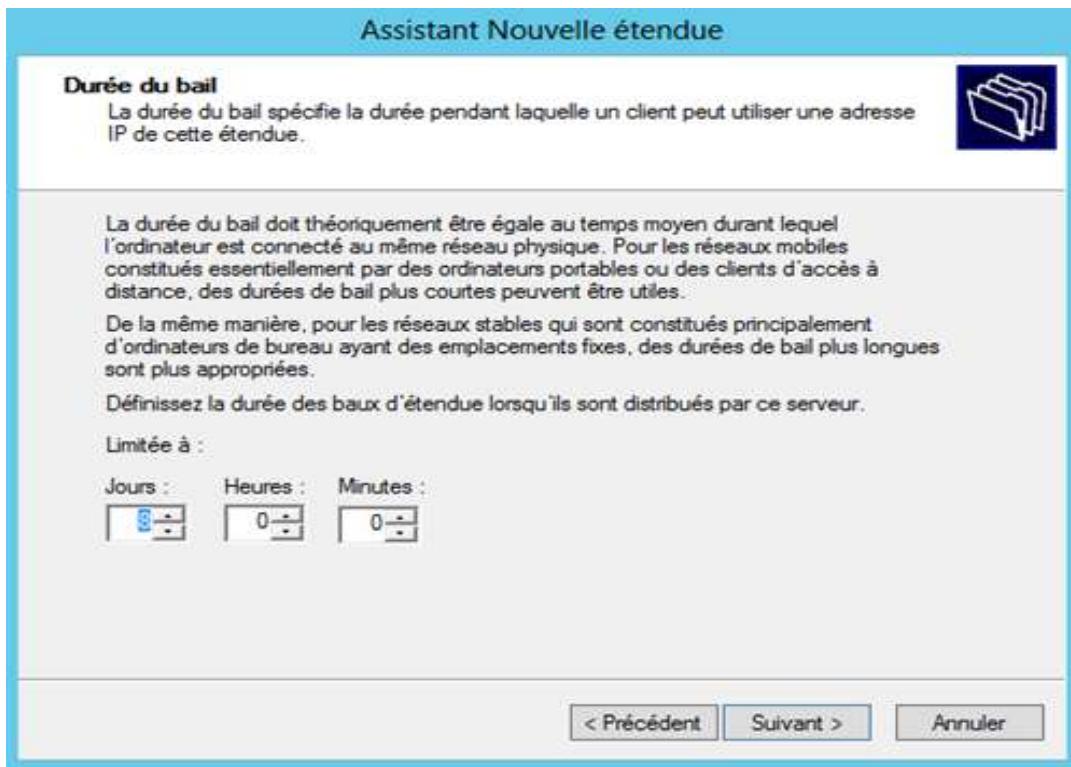
Quant à vous, de définir la plage d'adresse à distribuer et le masque de sous réseau :



Quant à vous, d'y ajouter d'éventuelles exclusions afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (imprimante, webcam IP, PC en adresse fixe, serveur,...) :

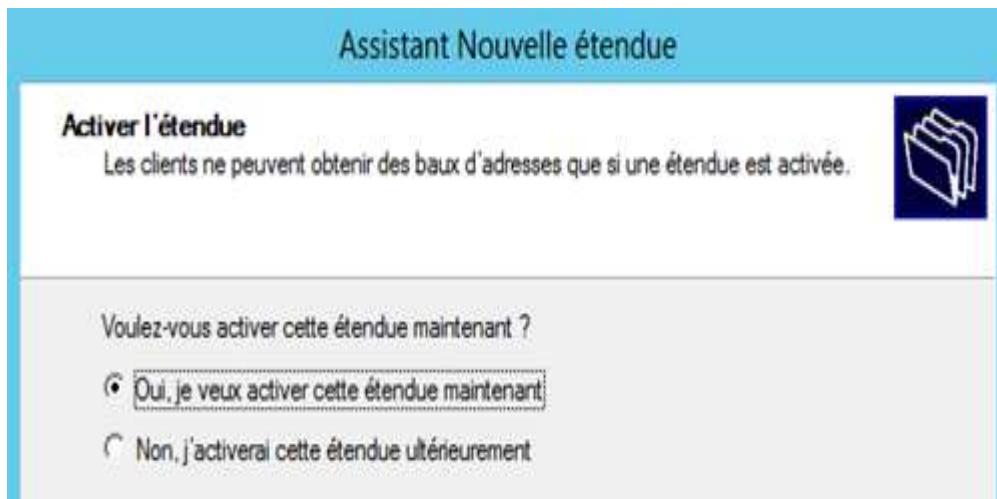


Puis la durée du bail, c'est à dire le temps pendant lequel le PC est autorisé à utiliser cette adresse sans la renouveler :

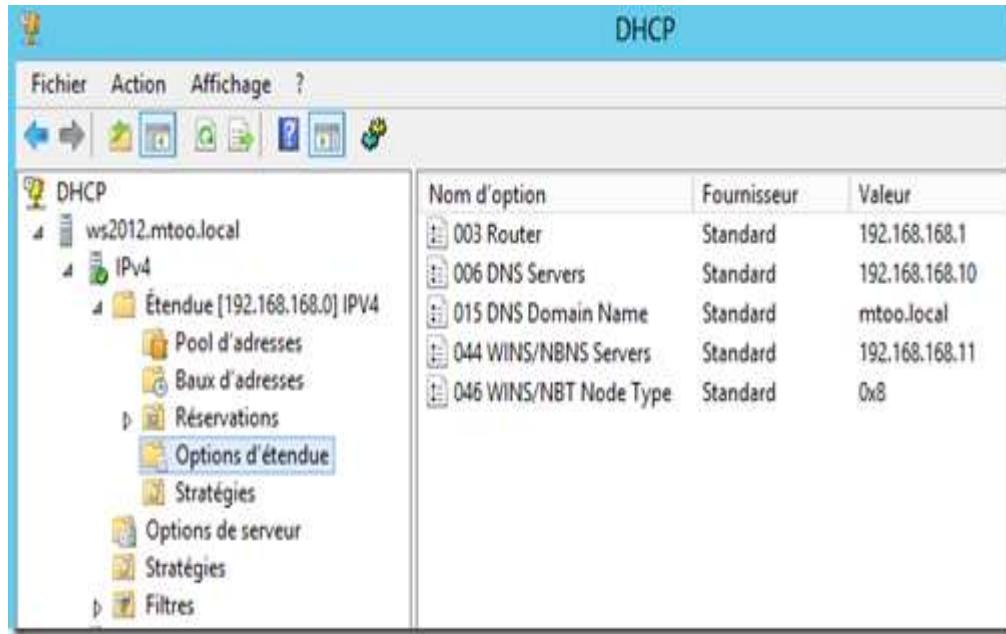


Vous pouvez ensuite configurer des options : les options sont des paramètres supplémentaires que vous pouvez configurer : comme l'adresse de la passerelle, des serveurs DNS et WINS.

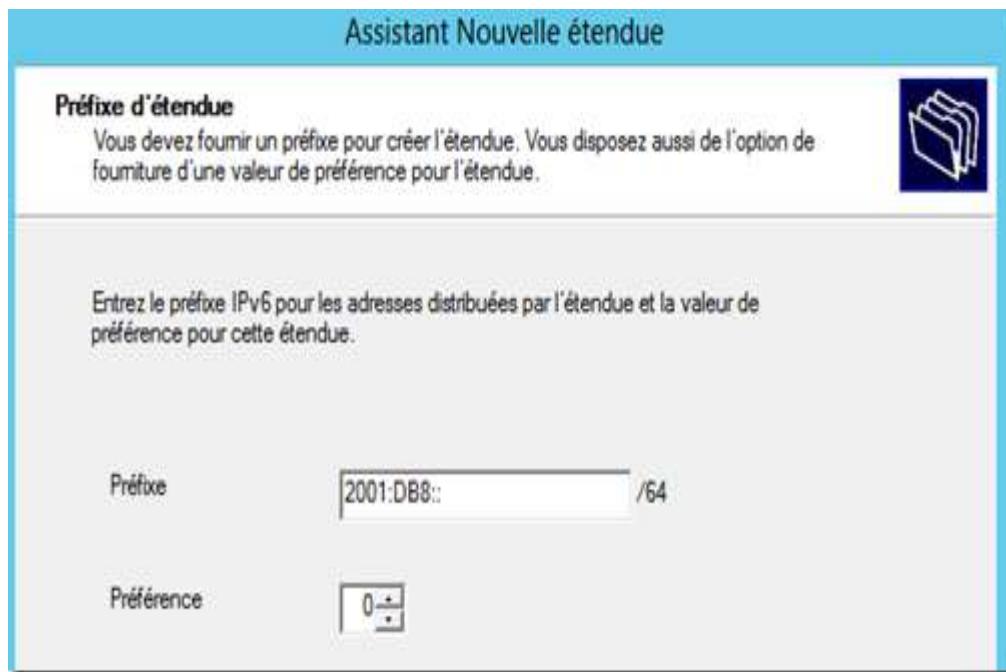
Vous pouvez ensuite activer l'étendue :



Vous pouvez vérifier les options d'étendue dans la console, voici un exemple avec les paramètres usuels :



Si vous souhaitez configurer une étendue IPV6, il faudra définir un préfixe :



La configuration des options reste identique. Vos PC peuvent maintenant disposer des paramètres IP corrects automatiquement.

IV.4. INSTALLATION DU SERVICE SNMP

L'un des protocoles les plus utilisés pour la supervision des systèmes d'informations, est bien évidemment le protocole SNMP (Simple Network Management Protocol). C'est en effet ce protocole qui va nous permettre de superviser et de diagnostiquer un certain nombre de problèmes sur nos machines.

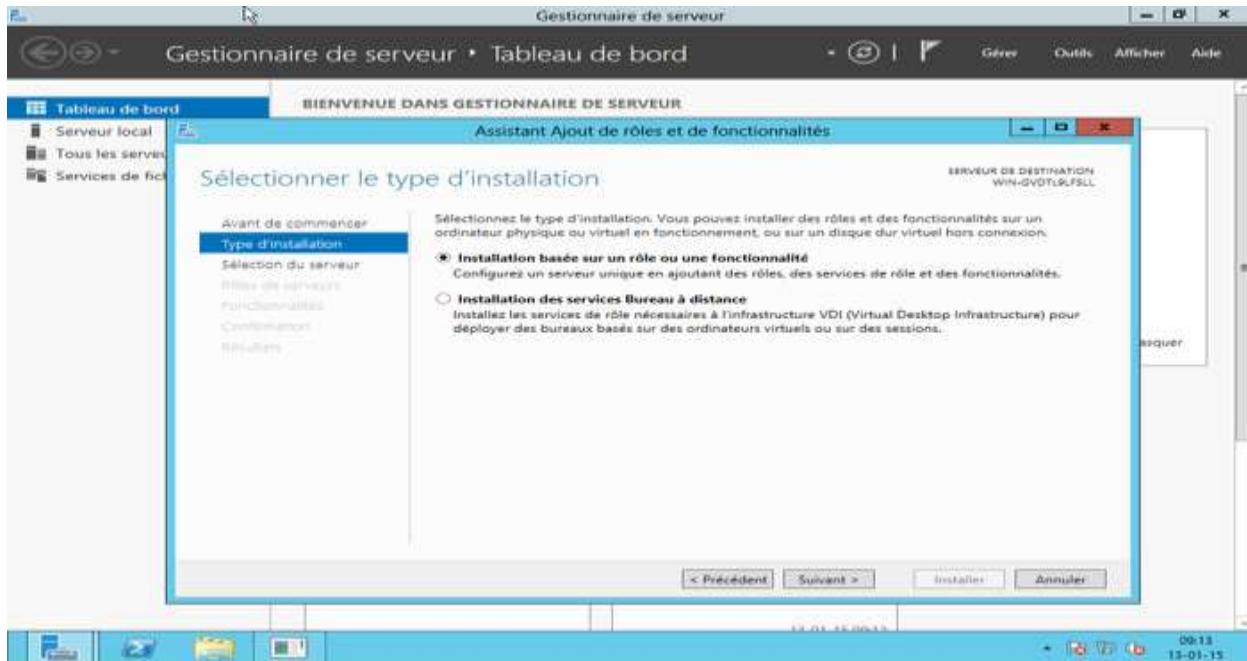
Pour activer SNMP sur les serveurs Windows, il faut se rendre dans le « Gestionnaire de serveur » (Server Manager). Ensuite, cliquez sur Ajouter des rôles et des fonctionnalités.



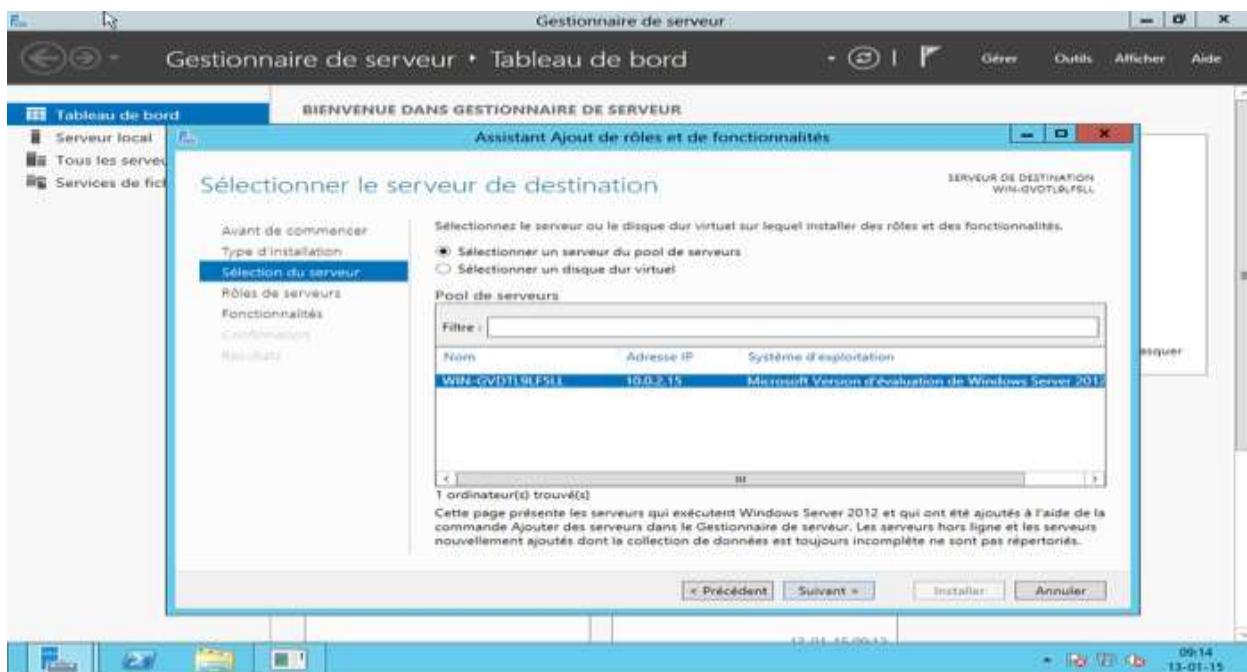
L'assistant va s'afficher. Cliquez sur suivant :



Laissez cocher « Installation basée sur un rôle ou une fonctionnalité » et cliquez sur suivant :

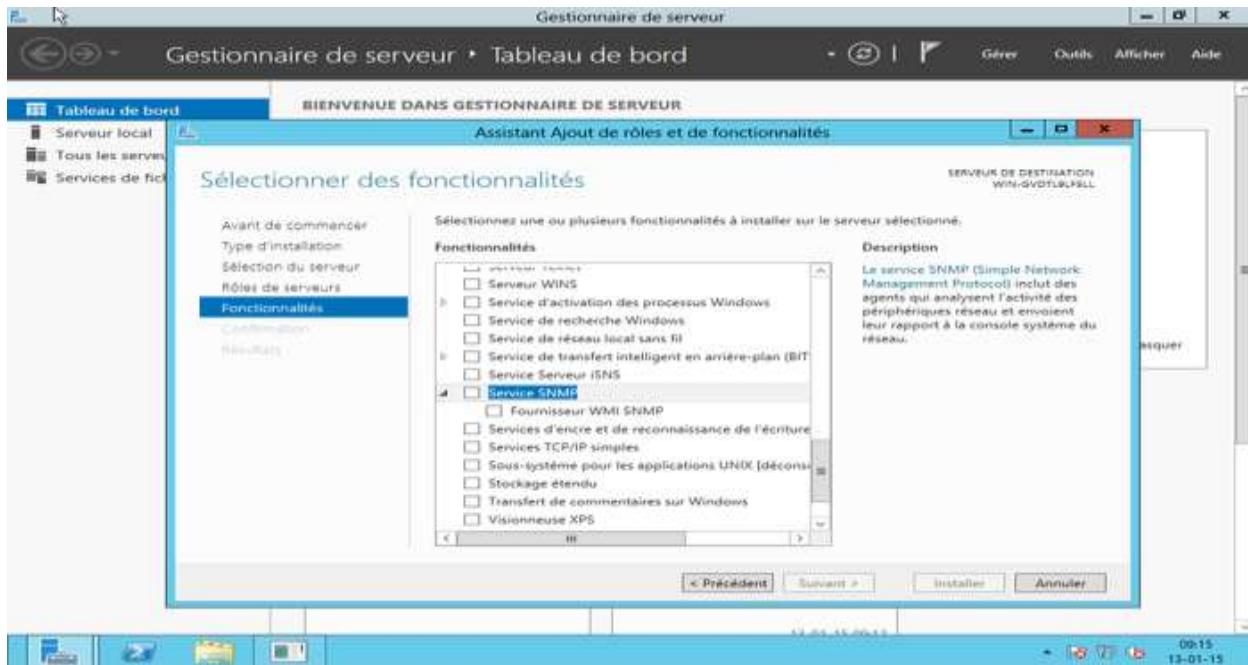


Sélectionnez le serveur ou le pool à configurer. Cliquez ensuite sur suivant:

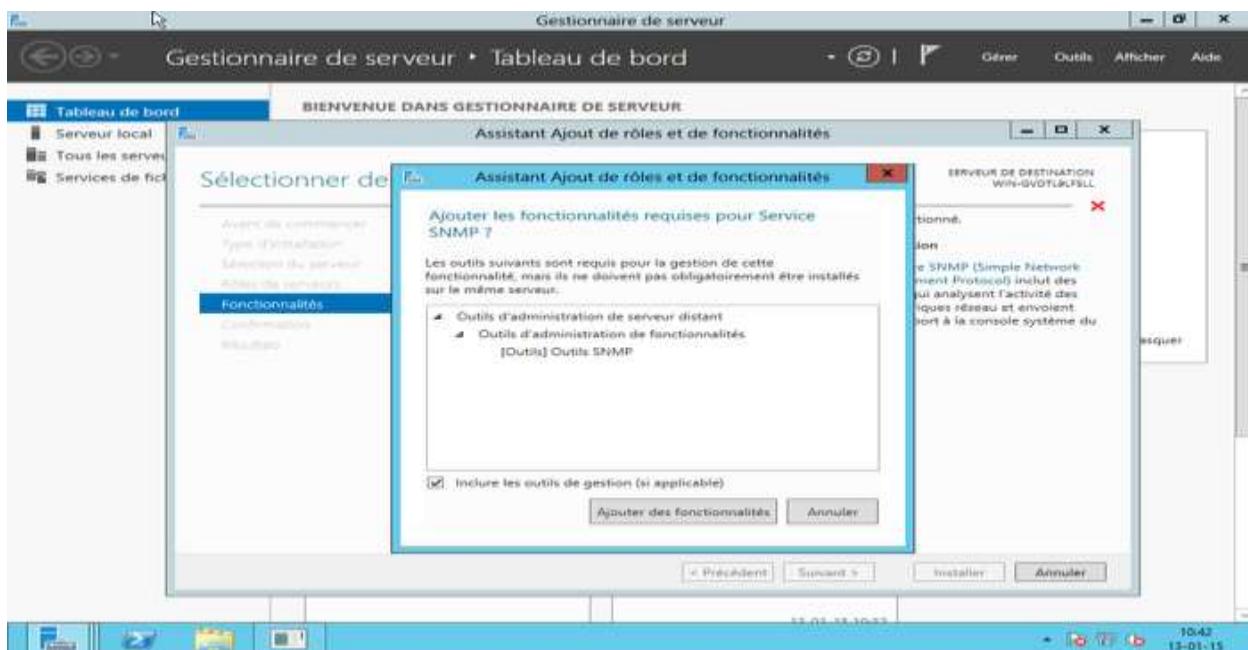


La fenêtre d'installation des « rôles » apparaît, mais SNMP étant une fonctionnalité, cliquez directement sur suivant sans rien cocher. Nous voici donc sur la fenêtre gérant les fonctionnalités.

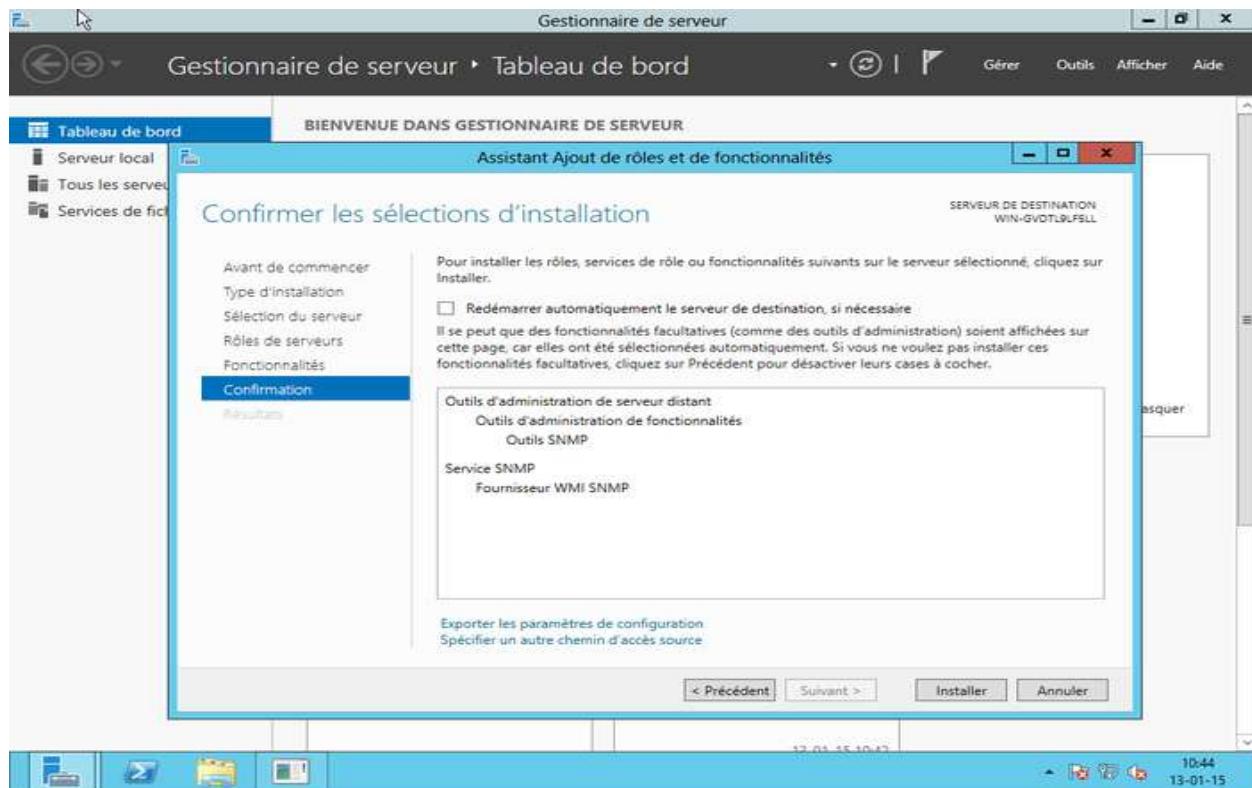
Faites défiler la liste déroulante et sélectionnez les cases « Service SNMP » et « Fournisseur WMI SNMP ».



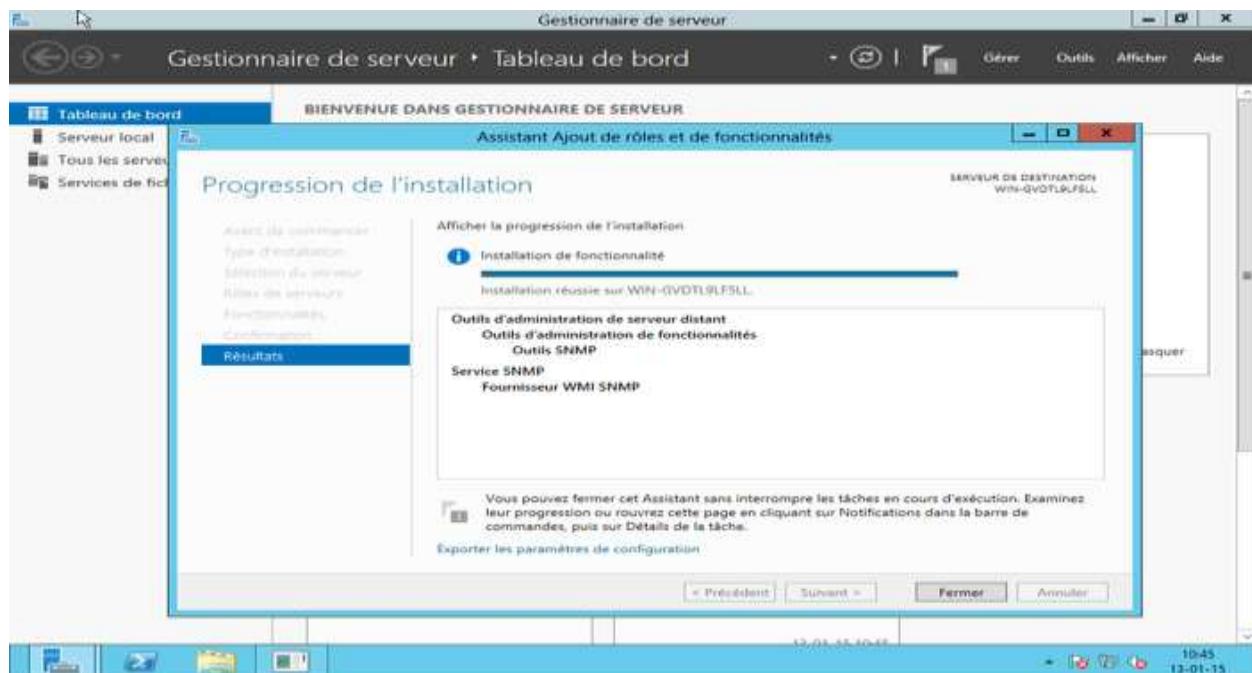
Une fenêtre apparaît « Ajouter les fonctionnalités requises pour Service SNMP ». Cliquez sur « Ajouter des fonctionnalités » en ne modifiant rien:



Cliquez ensuite sur suivant:

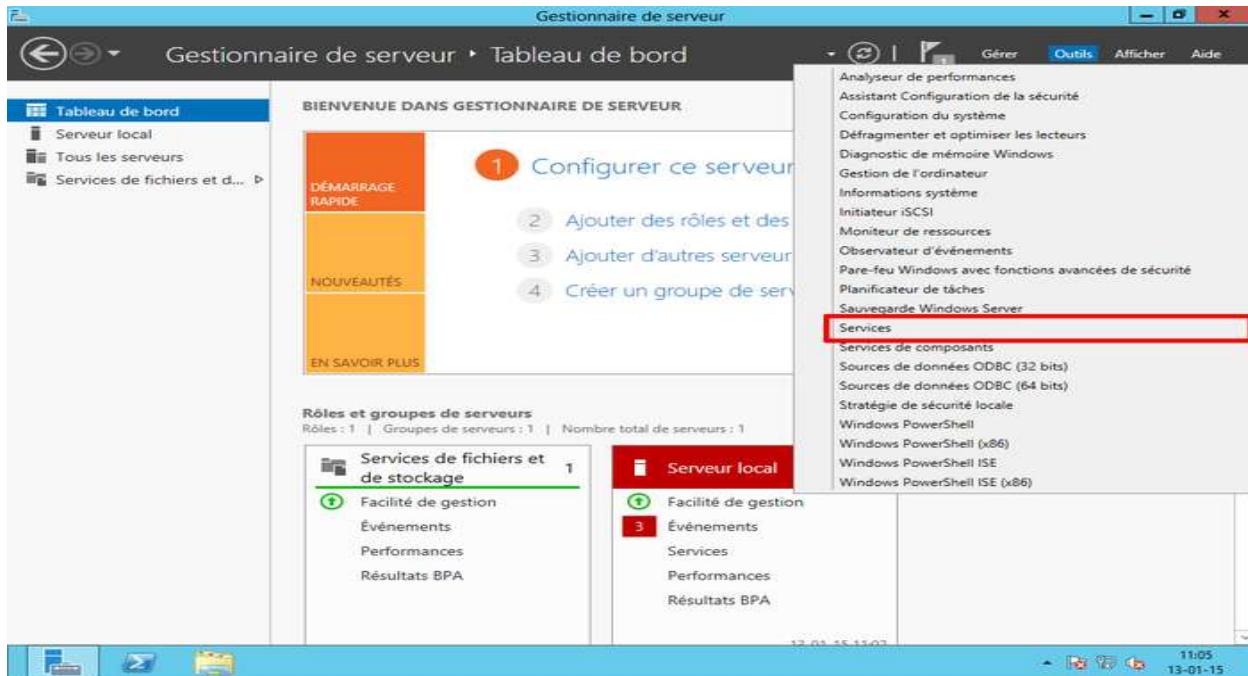


Et pour finir sur « Installer » :

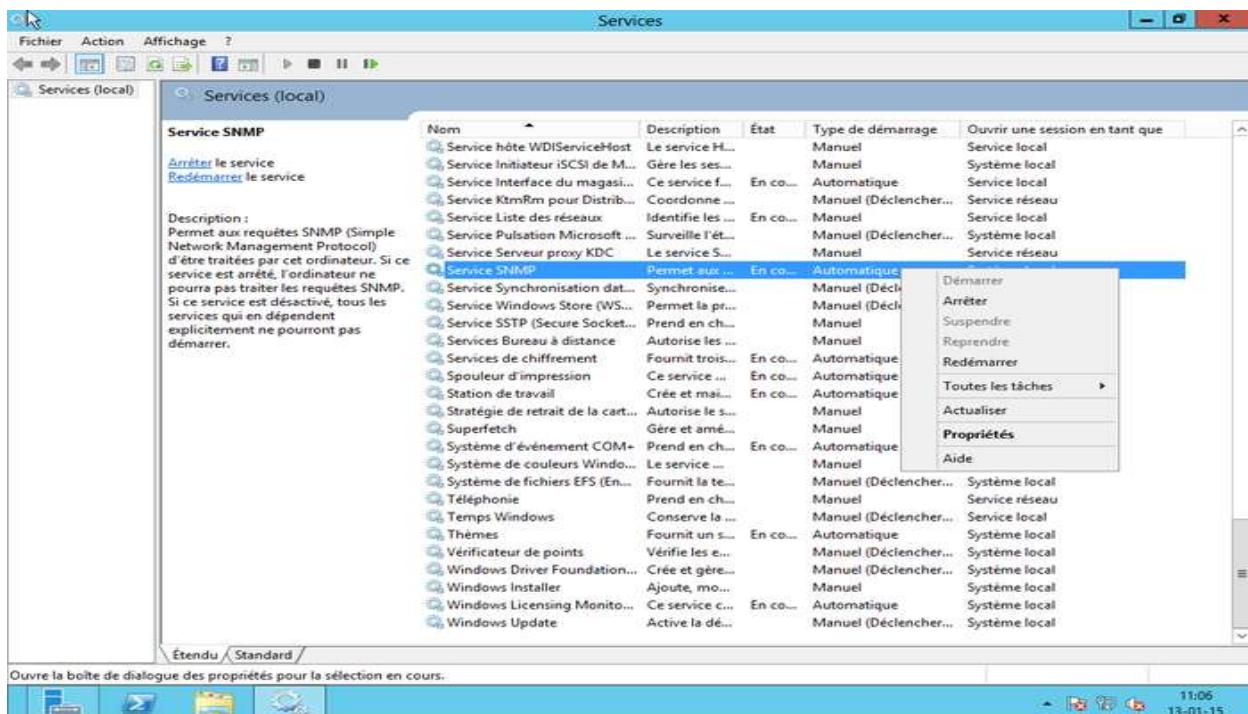


Vous pouvez maintenant fermer l'assistant d'installation et passer à la suite la configuration du service SNMP.

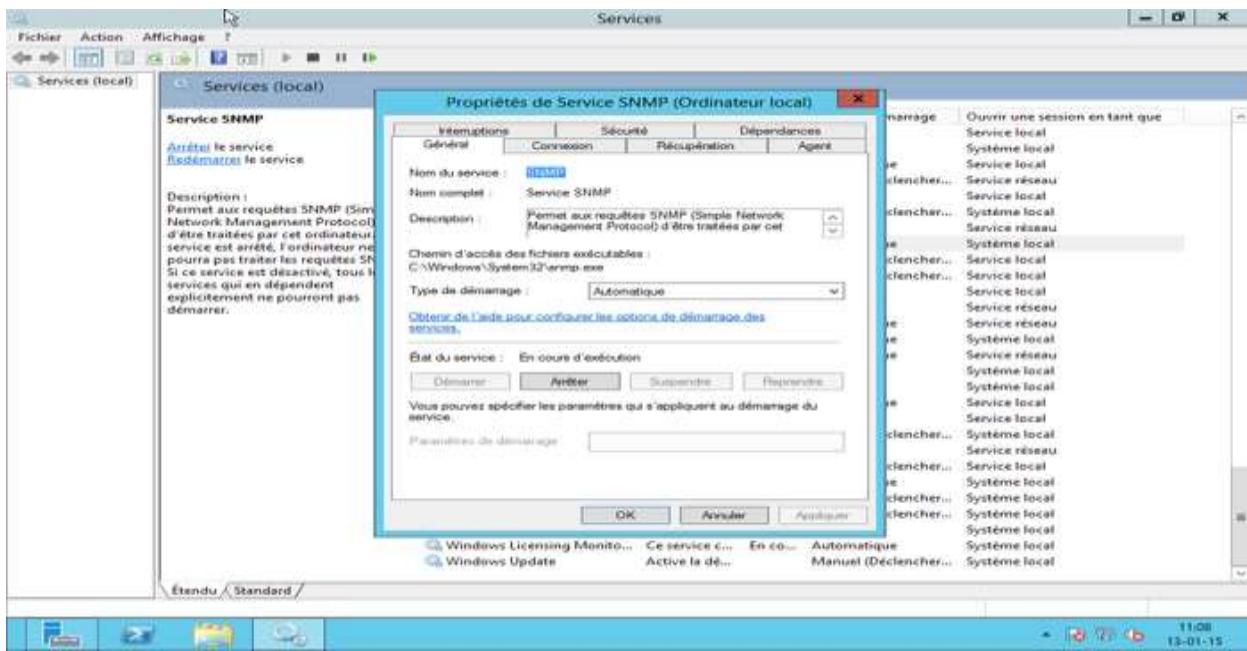
Pour configurer le service SNMP, cliquez sur « Outils » dans le gestionnaire de serveur et ensuite cliquez sur « services » :



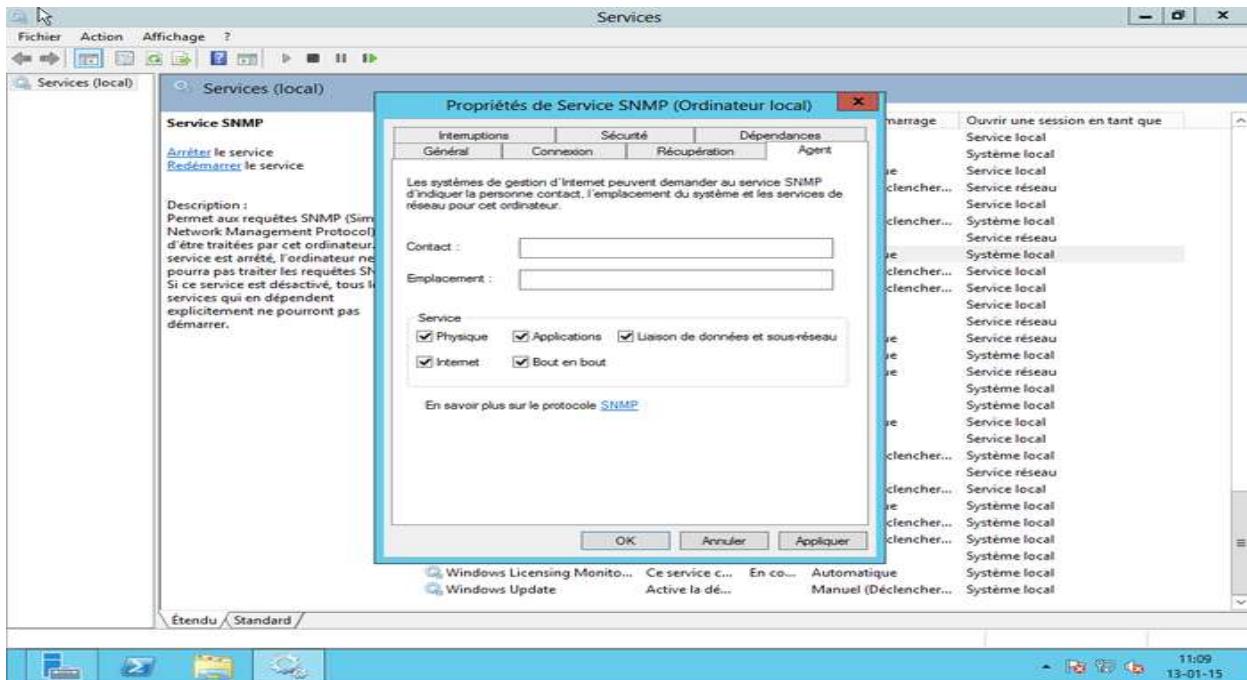
La fenêtre des services exécutés apparaît. Descendez et faites un clic-droit sur « Service SNMP » puis cliquez sur « Propriétés » :



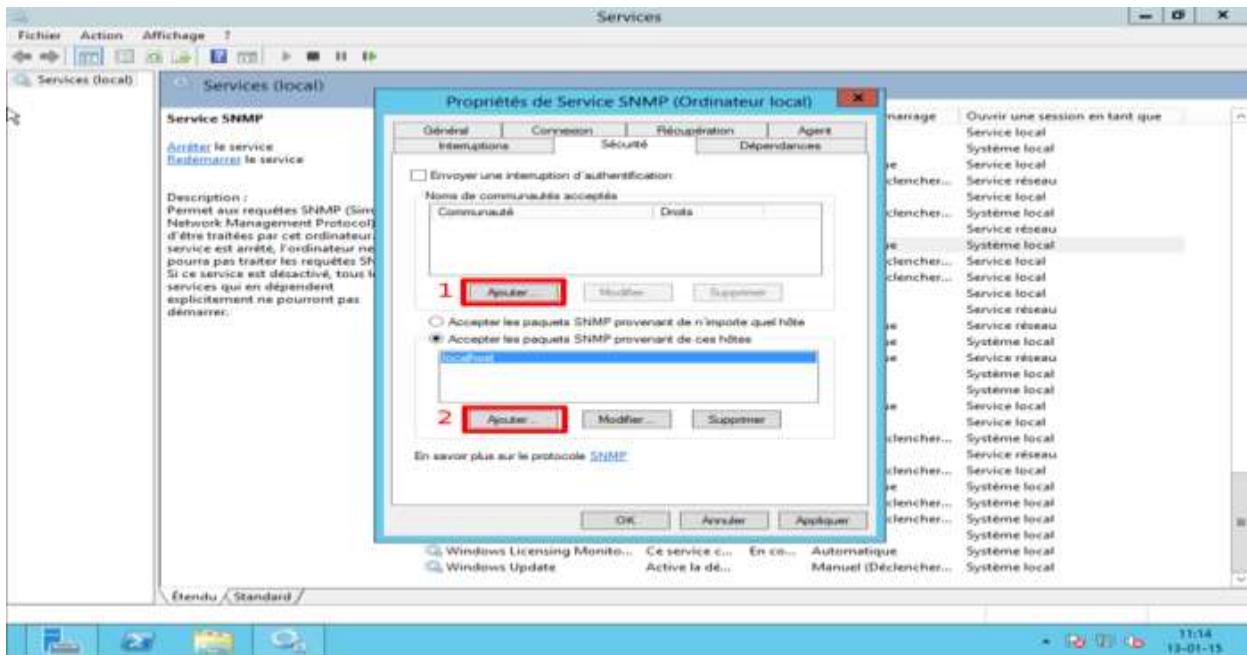
Vous êtes maintenant sur la fenêtre de configuration du service :



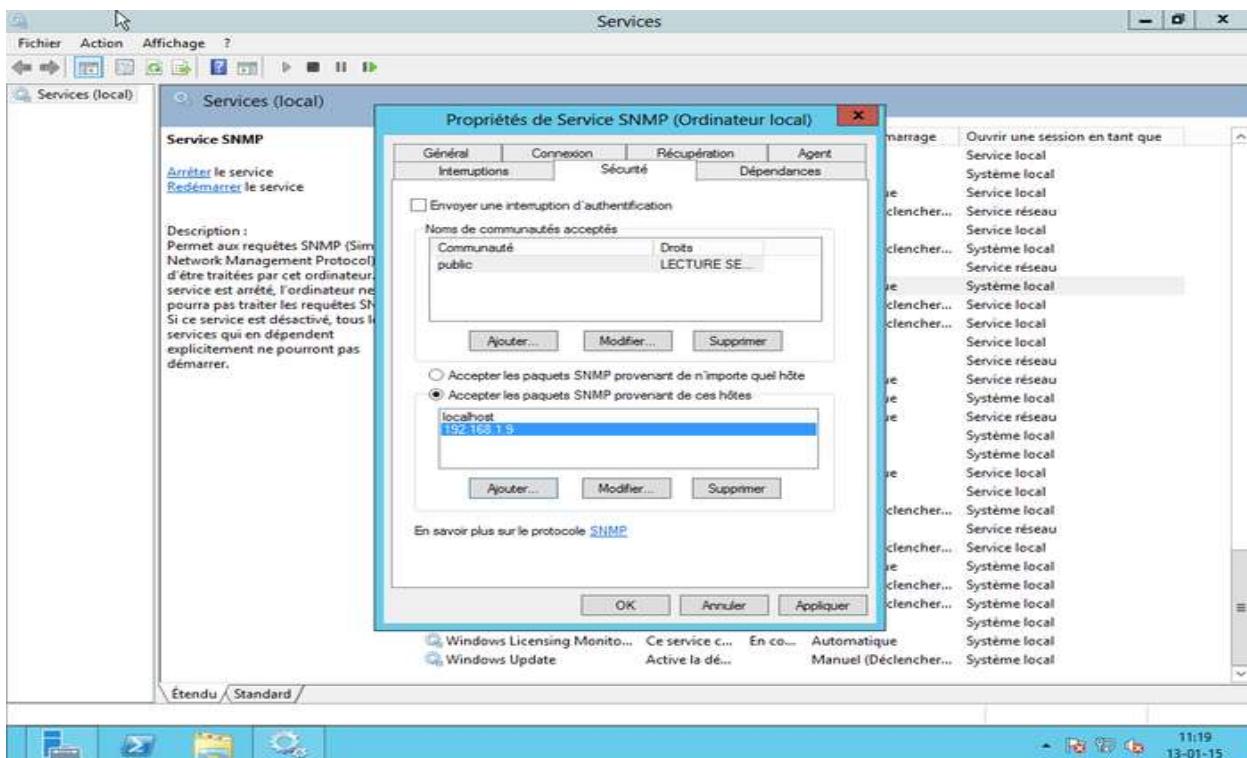
Cliquez sur l'onglet « Agent » et sélectionnez toutes les cases « Services ». Vous pouvez aussi ajouter un contact ou un emplacement si vous le souhaitez. Cliquez sur « Appliquer »:



Ensuite, cliquez sur « Sécurité ». Vous pouvez décocher la case « Envoyer une interruption d'authentification ». Pour ajouter une communauté SNMP ayant des accès en lecture seulement, cliquez sur « Ajouter ». Une fenêtre apparaîtra. Rentrez le nom de la communauté (ici : public) et terminez en cliquant sur « Ajouter » :

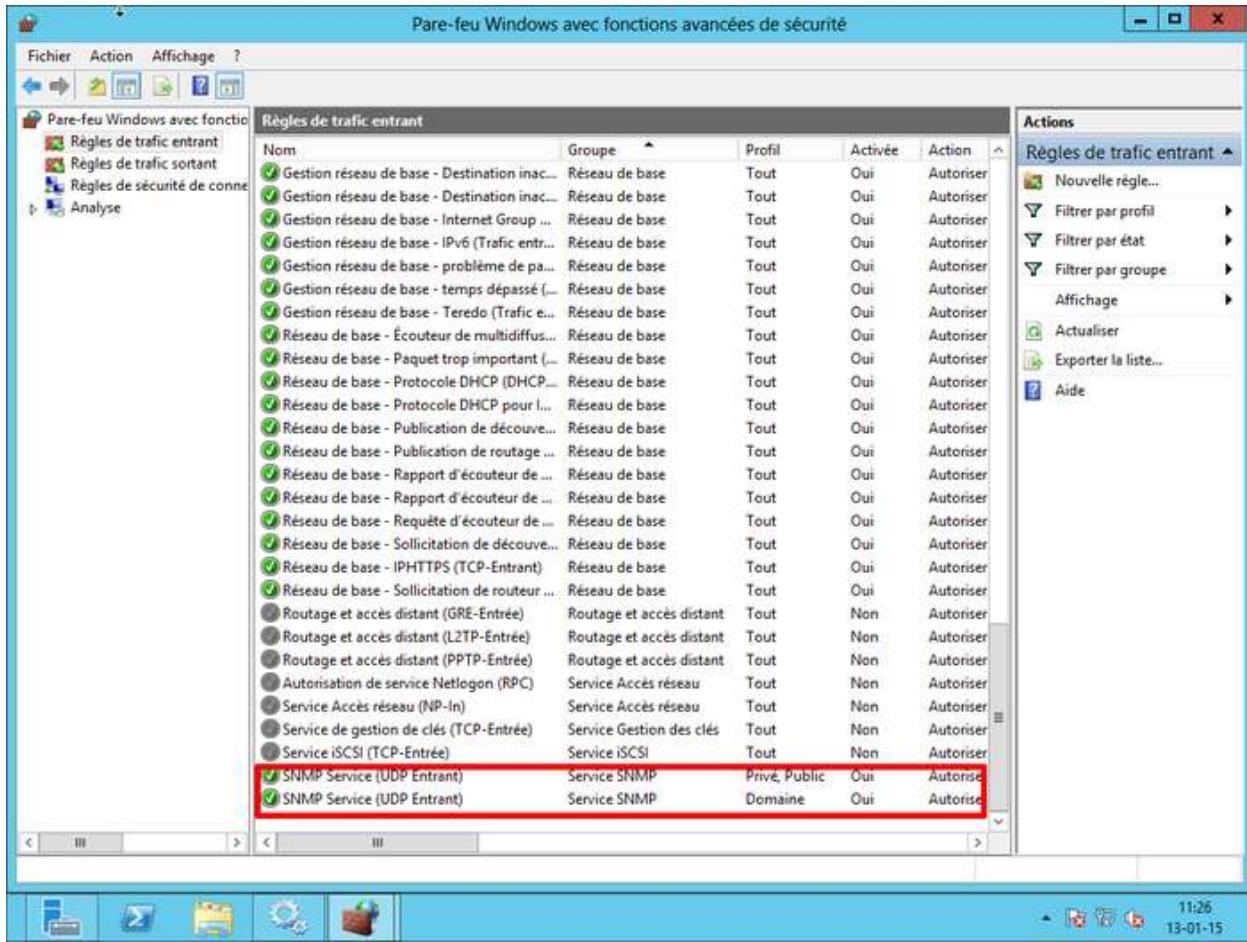


Pour finir la configuration, il nous reste à ajouter l'adresse IP de la Unity pour autoriser celle-ci à interroger notre serveur 2012. Cliquez sur « Ajouter ». Entrez l'adresse IP (ici : 192.168.1.9) et cliquez sur « Ajouter ». Normalement après cette étape, vous devriez avoir une fenêtre comme si dessous :



ATTENTION : SNMP utilise le port 161 en UDP pour fonctionner. Vérifiez bien que votre pare-feu autorise bien le trafic entrant sur le port 161.

En principe, Windows 2012 a ajouté automatiquement une règle à son pare-feu. Pour vérifier, dans le gestionnaire de serveur, cliquez sur « Outils » et puis sur « Pare-feu Windows avec fonctions avancées de sécurité ». Dans les règles de trafic entrant, vous devriez voir 2 lignes « SNMP Service » :



Le service SNMP est maintenant activé et configuré sur notre serveur Windows 2012. La prochaine étape est d'ajouter le serveur à l'application.

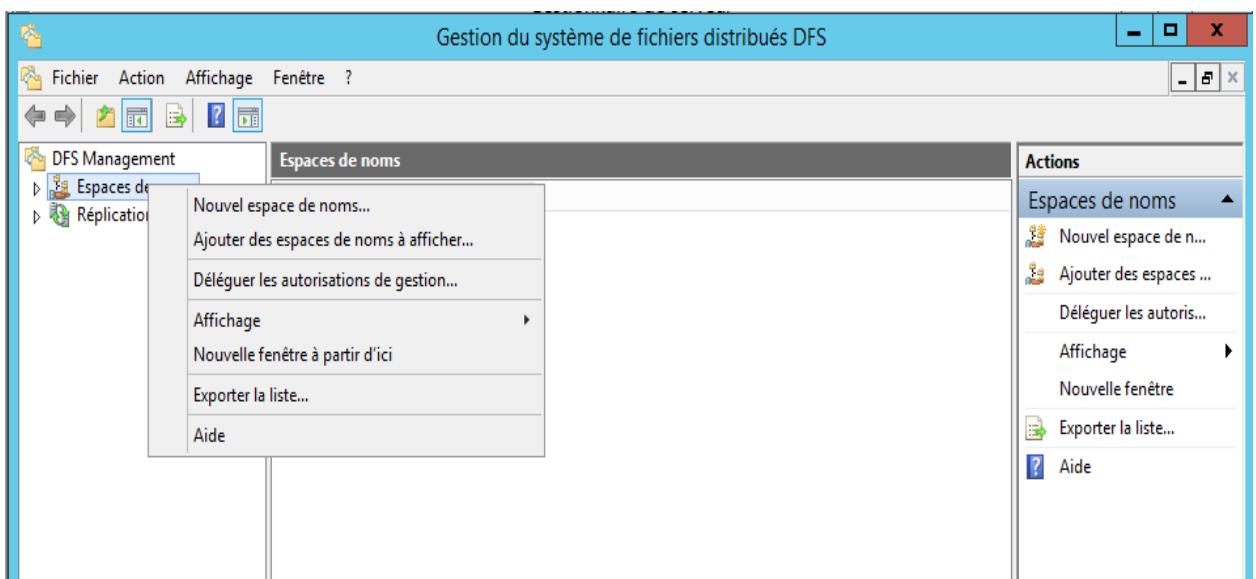
IV.5. INSTALLATION DU SERVICE DFS

Le DFS (*Distributed File System ou Système de Fichiers Distribué*) est un système de fichier hiérarchisé permettant de structurer les fichiers partagés sur différents serveurs de façon logique. A noter que le DFS a un impact sur l'utilisateur. Comme le DFS synchronise les données disponibles sur plusieurs serveurs, l'utilisateur ne verra pas le nom du serveur sur lequel il accède pour lire les données.

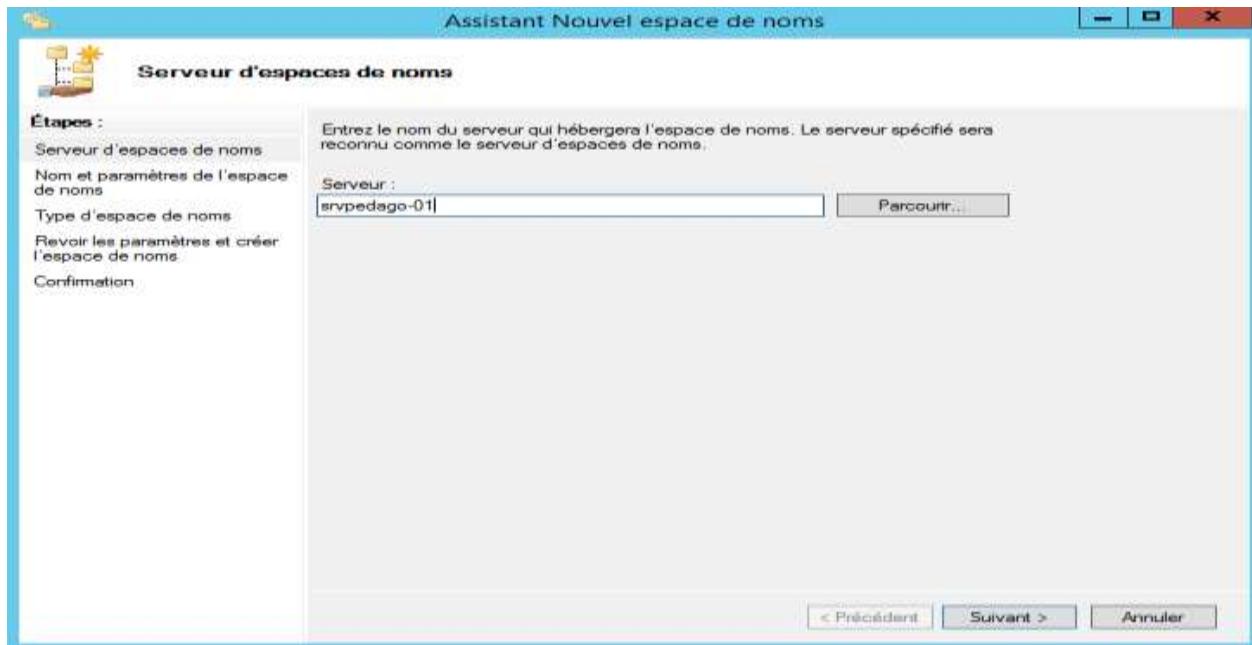
Retour au panneau de contrôle, cliquer sur « **Gérer** » puis « **Ajouter des rôles et des fonctionnalités** ». Cliquer sur suivant jusqu'à tomber sur "Pool de serveur" puis sélectionner votre ordinateur (ici « *srvpedago-01* »). Sélectionner « **Services de fichiers et de stockage** », « **Services de fichier et iSCSI** » et ajouter les fonctionnalités suivantes:

- **RéPLICATION DFS** ;
- **Espaces de noms DFS**.

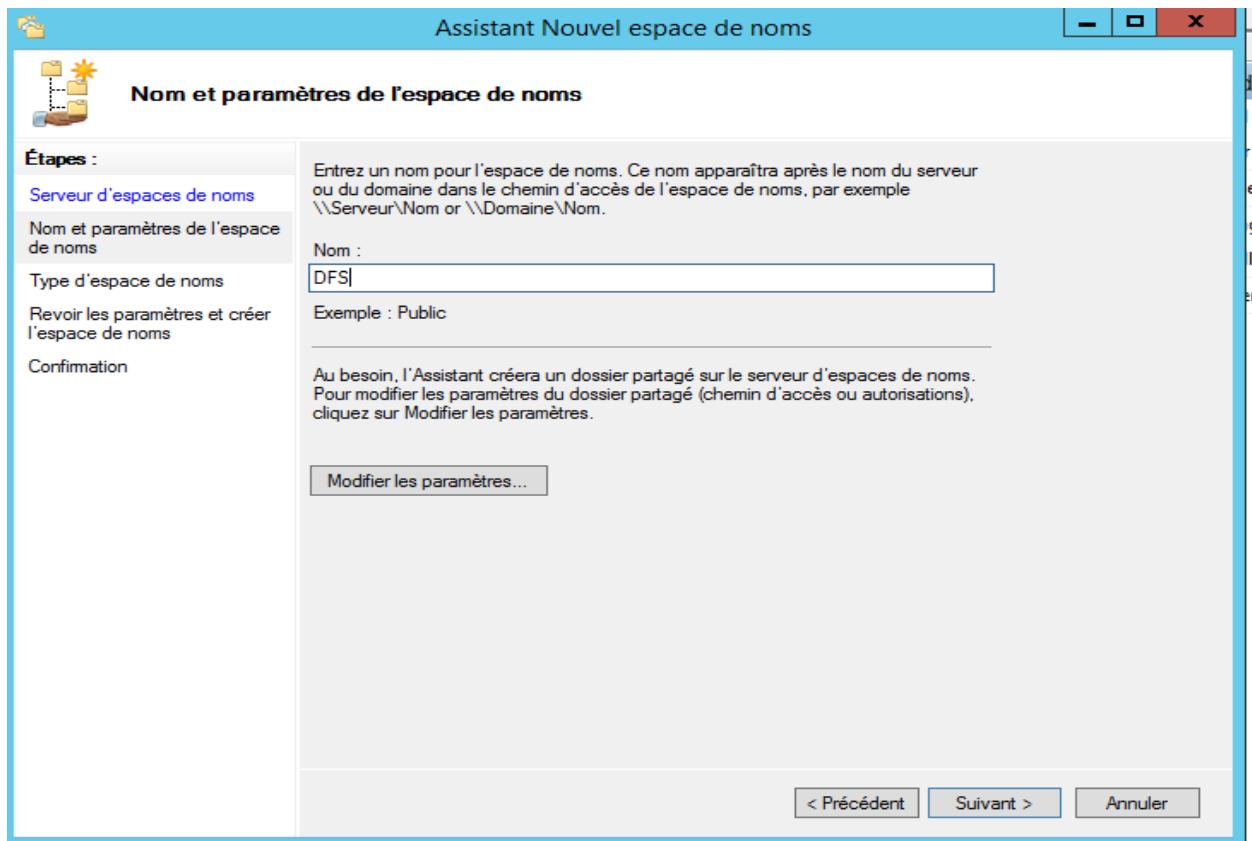
Valider jusqu'à l'étape d'installation, valider et fermer la page. Ensuite ouvrir le gestionnaire de serveur, cliqué sur « **Outils** » puis ouvrir la console « **Gestion du système de fichiers distribués DFS** ». Faite un clique droit et sélectionner « **Nouvel espace de noms** » :



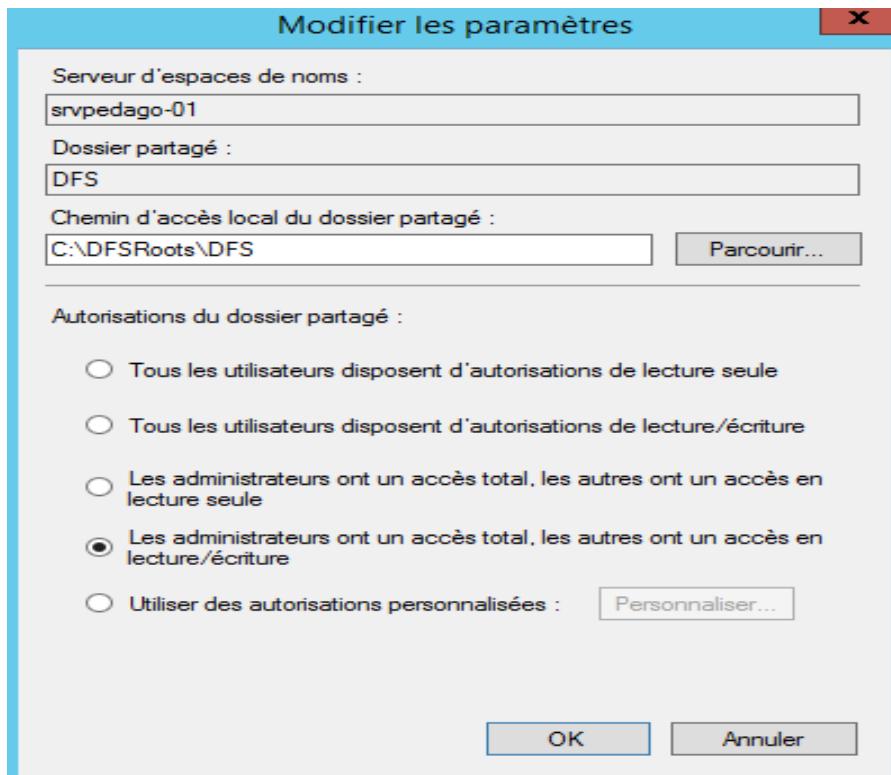
Entrer l'adresse du serveur



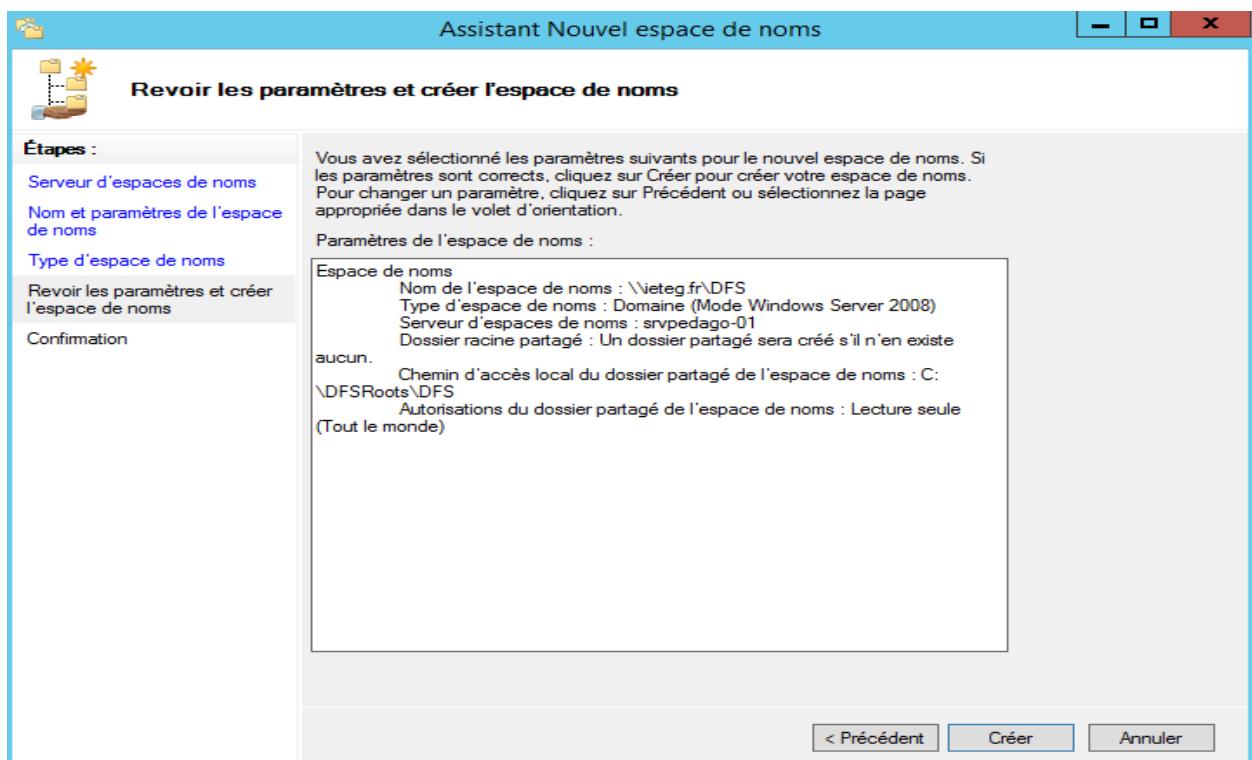
Entrer ensuite « DFS » comme nom comme ceci :



Cliquer sur paramètre et entrer les paramètres suivant :



Valider la page et cliquer sur « Crée »

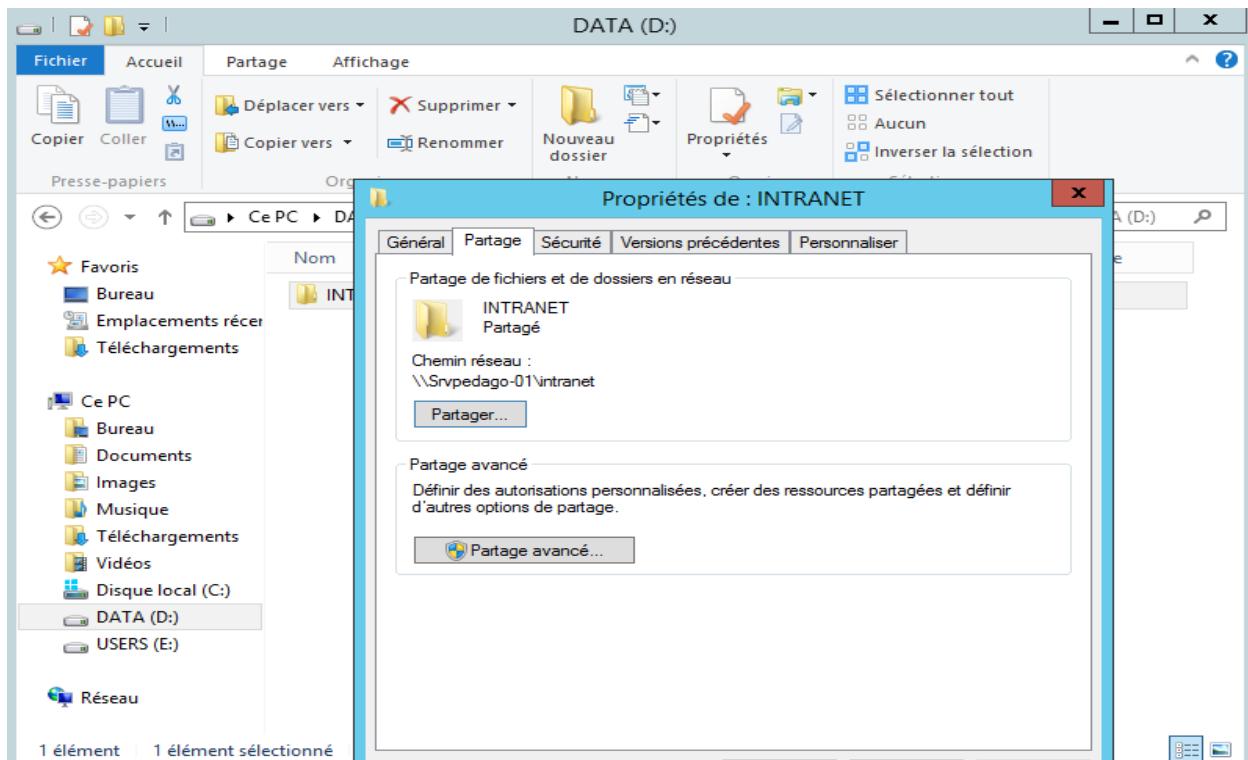


Pour la suite des opérations, vous devez créer une partition D: (nommée DATA) et une autre partition E: (nommée USERS). Créer ensuite les dossiers et sous dossiers au besoin en respectant ces deux arborescences :

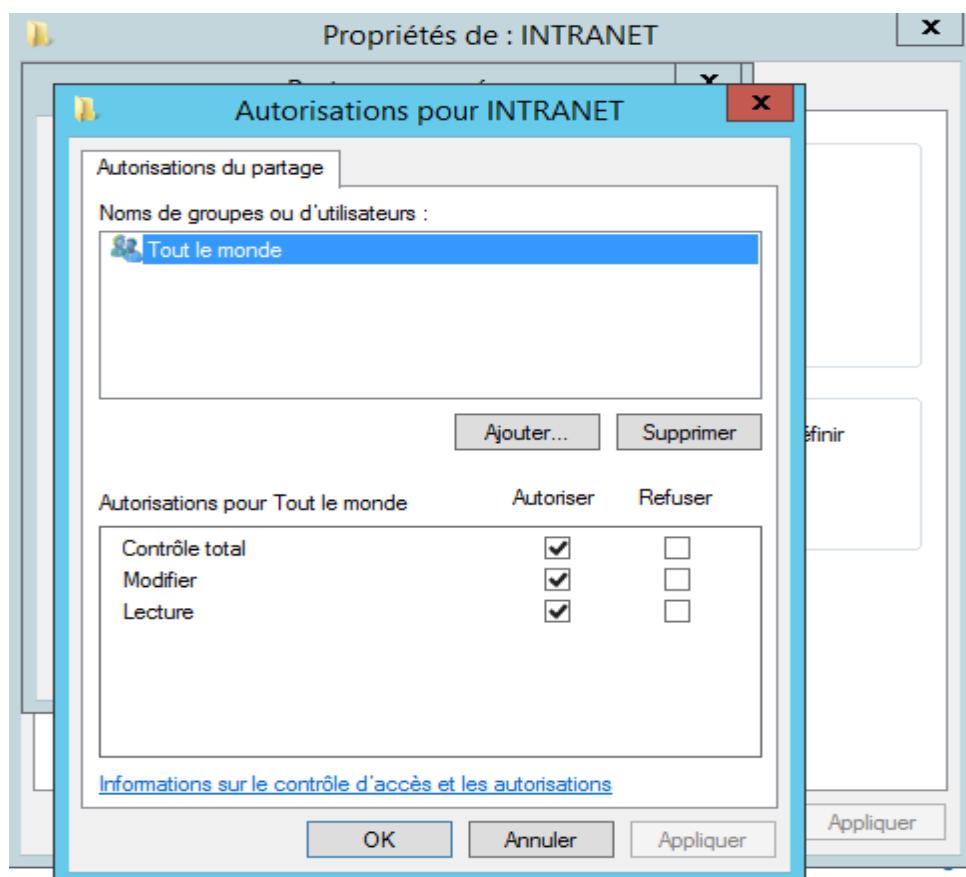
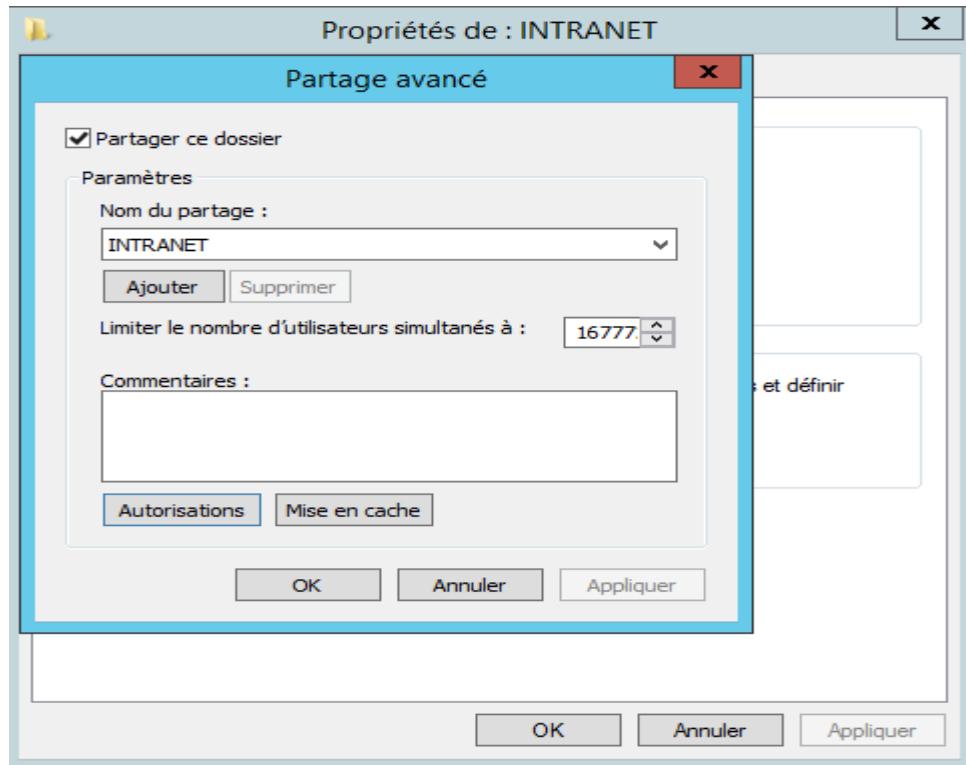
```
Structure du dossier pour le volume DATA
Le numéro de série du volume est C0C0-597F
D:\|
  └── INTRANET
      ├── GRP1
      ├── GRP2
      └── TRANSFERT
```

```
Structure du dossier pour le volume USERS
Le numéro de série du volume est 3480-A04F
E:\|
  └── GRP1-PERSO
      └── GRP2-PERSO
```

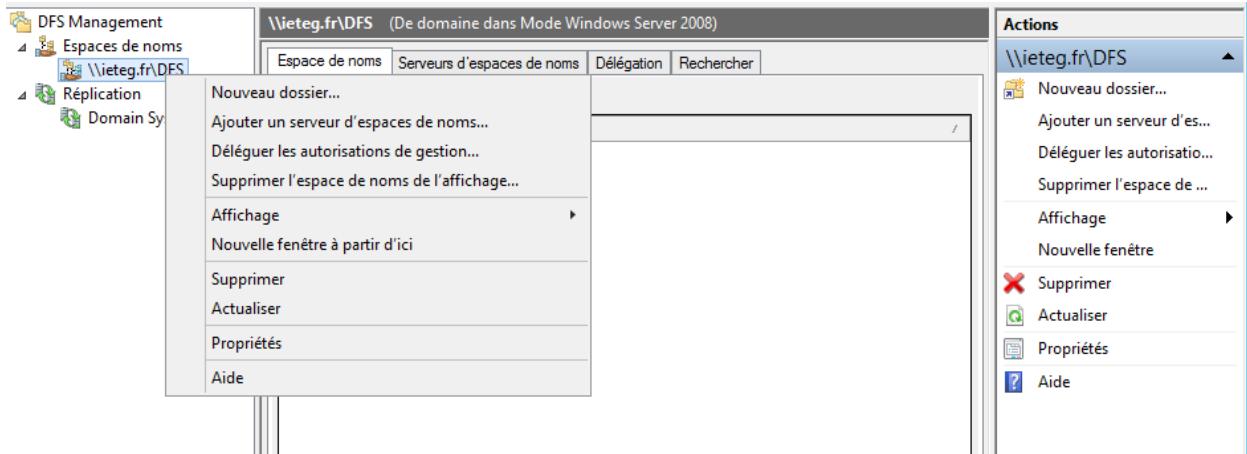
Une fois fait, vous devez partager les dossiers **INTRANET**, **GRP1-PERSO** et **GRP2-PERSO** sur le réseau. Pour se faire, cliquer droit sur le dossier en question, puis « Propriété ».



Cliquez sur « **Partage avancé** » et modifier les autorisations pour laisser l'accès à « **Tout le monde** » comme ceci :

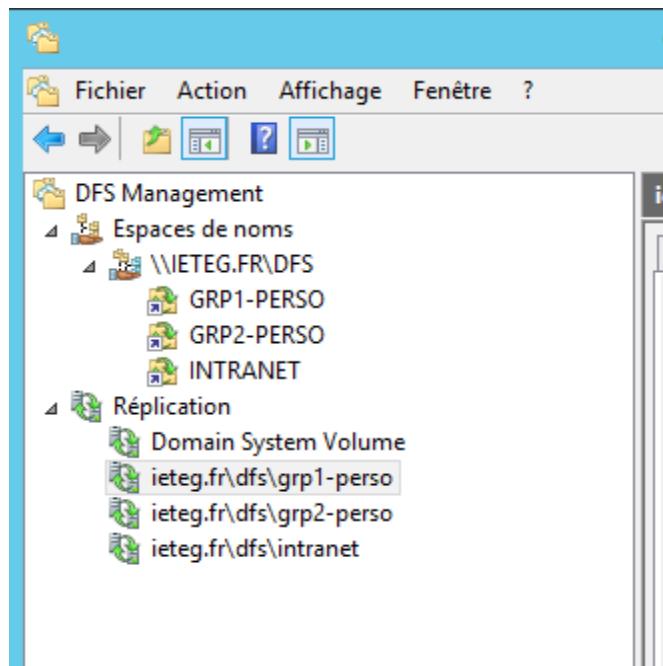


Effectuez cette opération sur tous les dossiers que vous souhaitez répliquer. Retournez sur « **DFS Management** » et cliquer droit sur (domaine)\FDFS (ici ieteg.fr\DFS) puis « **Nouveau dossier** ».



Remplissez le champ « Nom » par « INTRANET» par exemple.

Valider et ajoutez comme cible de dossier les chemins d'accès suivant : \\srvpedago-01\intranet et [\\srvpedago-02\intranet](#). Validez ensuite pour créer un groupe de réplication. Adaptez la configuration à votre besoin et validez l'ensemble. Recommencez ces opérations de façon à créer l'arborescence présentée sur le schéma ci-dessous:



Voilà, vous avez terminé votre configuration DFS.

CONCLUSION

Dans ce monde actuel où tout devient automatisé, l'administration, la connaissance du fonctionnement, la création et la configuration des réseaux informatiques paraît indispensable pour un étudiant en Informatique. Ce cours d'administration des réseaux informatiques est rédigé tout en tenant compte du niveau de compréhension des étudiants et leurs prérequis en générale. Les chapitres sont présentés dans le but de permettre aux apprentis dans le domaine de comprendre les notions de base d'administration des réseaux informatiques.

Il sied de rappeler que l'environnement de travail de l'administrateur réseau exige qu'il soit un spécialiste d'une pluralité technique, d'une flexibilité et de compétences humaines tout à fait particulières. En effet, les administrateurs réseau travaillent dans des environnements très variés, comprennent les grandes entreprises, les petites et moyennes entreprises, des institutions académiques et de formation, des organisations gouvernementales, du domaine de la santé ou à but non lucratif. La sensibilité et les défis des aspects centraux de l'administration varient d'un environnement à l'autre. En plus, l'administrateur réseau doit disposer des compétences techniques irréprochables ; il doit également présenter des compétences humaines déterminantes telles que :

- Capacité de résolution analytique de problèmes et de communication ;
- Capacité de se concentrer sur des détails et d'y accorder une attention particulière ;
- Capacité de travailler aussi bien indépendamment qu'en tant que membre d'une équipe ;
- Motivation à continuer d'acquérir les connaissances et les compétences les plus récentes.

Il est à noter que dans la chaîne de l'exploitation de l'infrastructure informatique, l'administrateur réseau est considéré comme dernier recours dans la résolution de problèmes ou lorsqu'on est à la recherche d'aide. C'est vers lui que sont dirigés tous les problèmes qui n'ont pas trouvé de solution au niveau de l'assistance à l'utilisation (Delp Desk) ou au niveau des administrateurs des équipements et des systèmes particuliers.

L'administration réseau amène les techniciens et spécialistes de la profession à être en contact avec les composants et systèmes informatiques et de télécommunications de tout genre et de toutes les tailles. Raison pour laquelle l'administrateur réseau doit disposer de connaissances techniques larges et avoir la flexibilité nécessaire pour suivre l'évolution de la science et des technologies.