CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

2017/2018

Bluefarma®
Votre santé, notre devoir depuis 1998

PROJET EVOLUTION

GMSI 16
Pierrick CHIROL
Nicolas DRONIER
Nicolas GERARD
Quentin ZANTEDESCHI

Table des matières

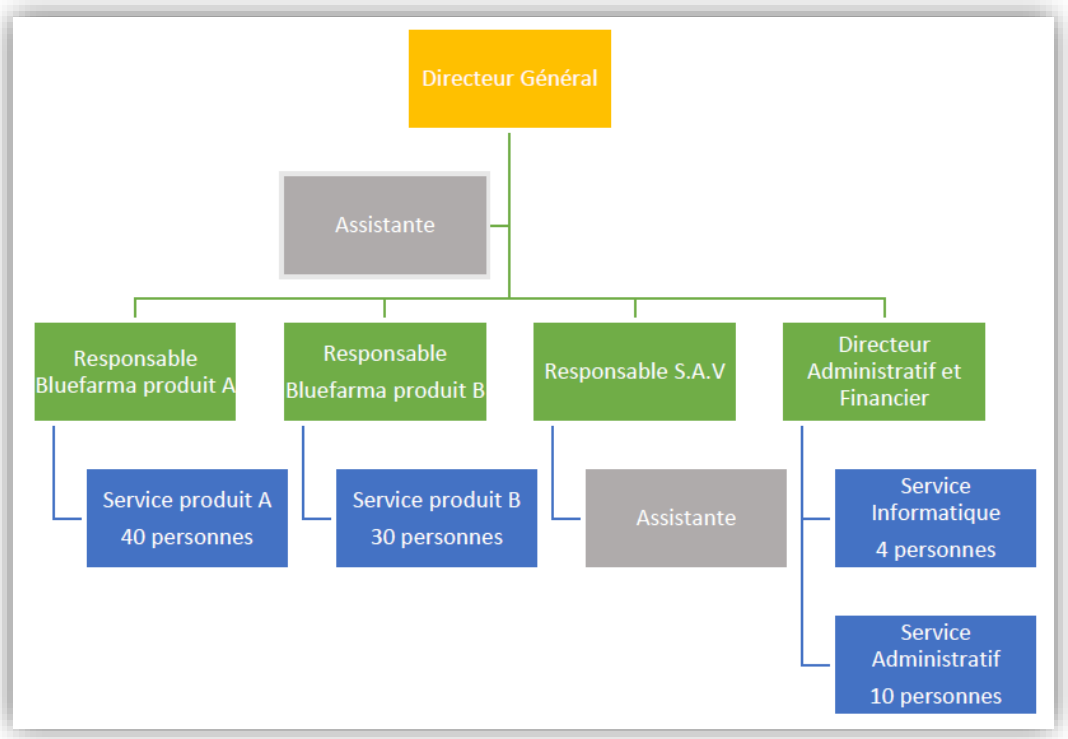
1. INTRODUCTION

1.1. Présentation de l'entreprise

Fondée en 1997, Bluefarma est une société spécialisée dans la commercialisation de médicaments en assurant, en tant que grossiste-répartiteur, un rôle d'intermédiaire entre les laboratoires pharmaceutiques et les pharmacies d'officine. Bluefarma a su affirmer sa place sur le marché de la pharmaceutique en nouant des partenariats solides et pérennes avec des laboratoires de recherche renommés.

En assurant la distribution de plus de 90% des références de médicaments Bluefarma s'est lancé dans la commercialisation de traitements médicamenteux de pointe. Soucieuse d'étendre ses activités dans les secteurs de pointe de la pharmaceutique, Bluefarma a connu ces dernières années une forte croissance. Ces mutations nous ont conduit à opter pour un nouveau site plus adapté aux nouveaux besoins de la société. Dans ce contexte, le siège de Bluefarma a été transféré sur un nouveau site.

Le site actuel comprend actuellement 90 collaborateurs répartis dans plusieurs services :



1.2. Contexte récent : le déménagement du site et rappel de l'existant

Il convient à présent de revenir sur les travaux effectués par le service informatique durant le précédent projet (START). Ce tour d'horizon nous aidera à mieux appréhender les enjeux du projet en cours afin de dégager une problématique de travail.

Nos activités se sont ainsi concentrées autour des points suivants :

- Étude et analyse des locaux techniques pour l'installation des équipements réseaux.
- Câblage complet de tous les espaces de travail avec l'installation de prises réseaux.
- Installation de la fibre optique entre les 3 bâtiments du site.
- Installation et interconnexion des équipements réseaux.
- Renouvellement des postes bureautiques des utilisateurs.
- Achats des licences des logiciels.
- Masterisation des postes : déploiement de Windows et Linux.

Nous avons procédé à l'installation complète d'une nouvelle infrastructure réseau (câblage des locaux et mise en relation des équipements réseaux) et des nouveaux postes informatiques sur lesquels a été déployé un master Windows 10 via le MDT sur le réseau.

Le parc existant se compose ainsi de 90 postes informatiques et ordinateurs portables répartis dans plusieurs zones de travail. Les prises RJ45 de ces zones sont alimentées par des switchs 24 ports de marque Cisco installés dans des locaux techniques sécurisés. De plus, la liaison inter-bâtiment est faite via un câblage fibre optique.

Des bornes d'accès WIFI ainsi que des imprimantes ont été installées afin de répondre aux besoins des différents services de l'entreprise. À l'issue de ce projet, les utilisateurs ont pu récupérer leurs données de travail qui ont été backupées sur un NAS connecté au réseau via des login d'accès individuel.

1.3. Contexte actuel et analyse du besoin

L'installation du siège dans de nouveaux locaux a impacté les différents services de notre société qui ont dû s'adapter à ces nouvelles conditions. Ce fut notamment le cas de notre service informatique. Depuis le déménagement de notre société il y a six mois, la direction a confié au SI un nouveau projet visant à améliorer les pratiques liées à la gestion, le support et la maintenance du parc informatique. Ainsi, il convient dès à présent d'identifier les besoins sur la base des documents ressources.

1.3.1. Cahier des charges

Le D.A.F a consigné dans un cahier des charges l'ensemble des difficultés rencontrées dans la gestion du parc informatique. Voici un résumé des principaux points relevés par le D.A.F :

1. Les membres du service informatique se trompe souvent de lieu lors d'un dépannage : aucune information sur le parc informatique (nom d'hôte, type de machines, etc.) n'est renseignée dans une base.
2. Il n'y a pas de gestion de droits utilisateurs.
3. Le siège social a besoin d'un serveur FTP pour récupérer des données : ceci passera par la mise en service d'un serveur Linux.
4. Implémentation d'Active Directory (nous verrons les consignes demandées).
5. 6 sessions seront nécessaires pour l'aboutissement du projet.
6. Un compte rendu faisant état de l'avancée mensuelle de l'équipe sera présenté (planning, répartition des tâches, etc.)
7. Le présent rapport fera état de la faisabilité des solutions proposées en tenant compte du cahier des charges tout en suivant la charte de l'entreprise.

Les points soulevés par le D.A.F se répartissent en trois catégories :

- **Problème d'organisation** dans le support matériel : (1).
- **Absence de moyens techniques pour administrer les droits des utilisateurs** (2, 4) et gérer les données (3).
- Mise en place d'un planning faisant état de l'organisation et de la **progression du projet** (5, 6, 7).

1.3.2. Audit technique

Les remarques d'ordre organisationnel et technique ci-dessus, ont été prises en compte par une ***SSII*** qui a réalisé un audit. Les solutions informatiques proposées répondent aux besoins exprimés dans le cahier des charges et s'articulent autour des trois volets techniques suivants :

- Environnement **Windows Server.**
- Environnement **Linux.**
- Administration d'une **base de données.**

Les attentes exprimées dans le cahier des charges s'articulent autour de ces aspects sans toutefois rentrer dans le détail des solutions à choisir (le type de distribution Linux, quel logiciel de base de données, etc.).

1.4. Définition de la problématique et présentation du plan

La définition d'une ou plusieurs problématiques de travail est primordiale avant d'amorcer les grands axes de cette étude. Ainsi, notre approche a consisté à identifier les besoins au moyen du cahier des charges et à proposer des solutions techniques à partir de l'audit technique.

Ainsi, cet examen préliminaire des ressources nous a permis de mener une réflexion sur les principaux enjeux de ce projet qui gravitent autour des points suivants :

- Tolérances aux pannes.
- Gestion et protection des données.
- Gestion efficace des utilisateurs.
- Organisation du support et de la maintenance.
- Analyse des risques.

En outre, nous avons tenu compte de l'organigramme de la société dans la conception de notre infrastructure système.

Au cours de cet exposé, la tâche du service informatique sera d'apporter son expertise à dessein d'avancer des solutions techniques pour des environnements Windows et Linux autour du plan suivant :

- **Présentation de l'existant** : il s'agit de l'infrastructure mise en place lors du projet START.
- **Choix du matériel :** Après un rappel de l'infrastructure réseau existante, nous déterminerons le type de matériel dont nous aurons besoin.
- **Présentation de l'hyperviseur** : mise en place de l'hyperviseur depuis lequel nous dimensionneront nos machines virtuelles.
- **Windows Server** : installation, configuration et administration du parc.
- **Linux** : installation et configuration des fonctionnalités présentent sous Linux (HTTP, FTP, samba, etc.
  Les rôles respectifs de ces deux environnements seront expliqués ainsi que la stratégie que nous mettrons en œuvre pour la gestion et la protection du système d'informations de notre société.
- **Administration de la base de données** : celle-ci se fera via l'interface de gestion GLPI ou directement en SQL.
- **Présentation du PCA** : nous monterons en quoi notre infrastructure remplie les exigences relatives à la tolérance aux pannes ainsi qu'à la protection et la sauvegarde des données de Bluefarma.

2. PRÉSENTATION DU MATÉRIEL SERVEUR

Nous tenions à définir dans ce chapitre le choix des équipements qui vont permettre d'acheminer du service jusqu'aux postes utilisateurs. Après un bref rappel de l'infrastructure réseau existante mise en place lors du projet START, nous aborderons le choix du matériel pour l'installation des serveurs et de leur redondance pour assurer une continuité de service en cas de panne.

Plus globalement, la description de nos infrastructures sera déterminante pour mieux appréhender la configuration logicielle des serveurs dans le prochain chapitre.

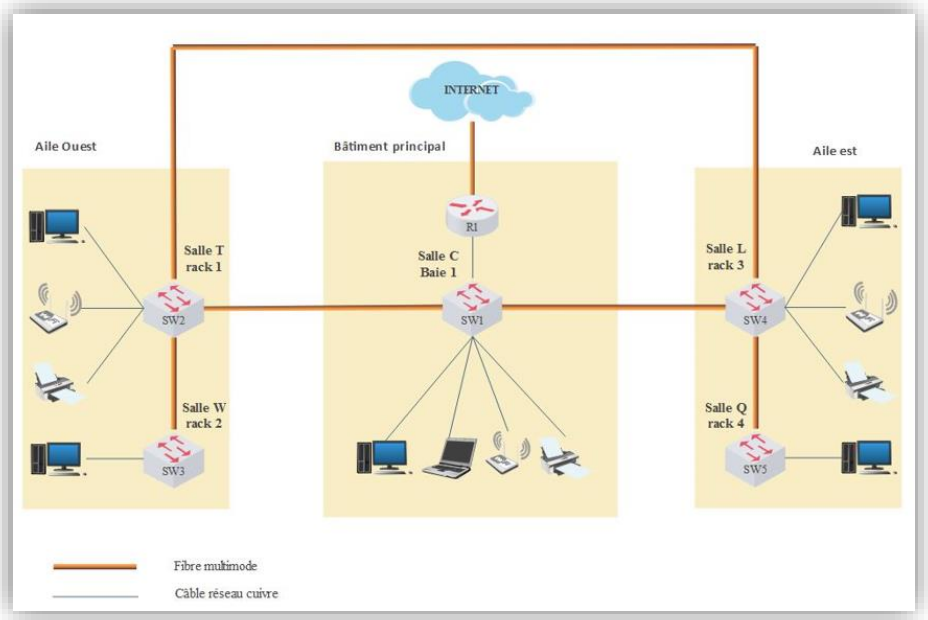
2.1. Rappel de l'infrastructure réseau existante

Cette partie reprend ce qui a déjà été défini lors du projet START. Ce rappel succinct décrit notamment la redondance du réseau au moyen d'une fibre de secours reliant les bâtiments les plus éloignés entre eux.

Description :

Le local technique principal (salle C) accueille le cœur de réseau composé d'un routeur Cisco connecté en backbone cuivre avec un commutateur Cisco Catalyst de 24 ports. Ce modèle a été utilisé pour les 4 autres commutateurs qui se répartissent au niveau des rez-de-chaussée et étages de chaque bâtiment.

Les trois bâtiments sont reliés par une fibre multimode qui forme un réseau que nous avons volontairement bouclé. Effectivement, une fibre de secours relie les ailes est et ouest. Ainsi, en cas de rupture d'une des trois liaisons optiques, le réseau dispose automatiquement d'un lien alternatif qui permettra d'assurer une continuité de service via la mise en place du ***STP***, ***Spanning Tree Protocol***.



2.2. Serveurs et stockages

Nous ne pouvions pas commencer cette partie sur les serveurs sans aborder la notion de « ***continuité d'activités*** ». En effet, les serveurs représentent les équipements les plus critiques de l'entreprise. Comme le stipule la ***CNIL***, il est indispensable d'adopter plusieurs mesures de sécurité pour consolider leur sécurité.

Quand ceci sera défini, nous serons à même de proposer une solution matérielle et logicielle qui répondra aux exigences de sécurité requis pour la protection des données de l'entreprise.

Dans son guide pour la sécurité des données personnelles, la CNIL énonce plusieurs précautions concernant la mise en place de la continuité d'activité. Dans le cadre de cette partie, nous aborderons :

- La redondance matérielle.
- La technologie RAID pour les unités de stockage.

2.2.1. Redondance des serveurs

Conformément aux recommandations ci-dessus, la redondance est une notion à prendre en considération pour consolider la sécurisation des données et de l'infrastructure système. Les serveurs effectueront un travail de réplication ou de sauvegarde incrémentielle entre eux mais ceci n'a de sens que si ces serveurs sont hébergés dans des locaux différents et distants.

Ils seront installés respectivement dans le local C du bâtiment principal et dans le local T de l'aile ouest.

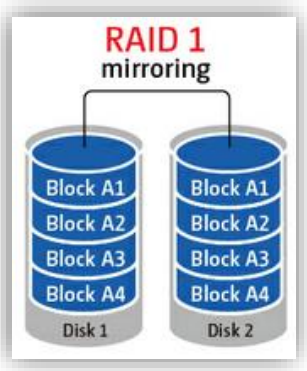
SERVEURS	EMPLACEMENT	SALLE
SRV1	Bâtiment principal	Local C
SRV2	Aile ouest	Local T

2.2.2. Redondance du stockage : la technologie RAID

La technologie **RAID** (« *Redondancy Arrays of Inexpensive Disk* ») est une solution matérielle ou logicielle qui apporte une tolérance de panne pour un système de fichiers : elle est basée sur la redondance des disques durs. Il est important de définir le type de RAID en fonction de l'usage attendu. Nos disques de stockage seront tournés vers 3 types d'utilisation :

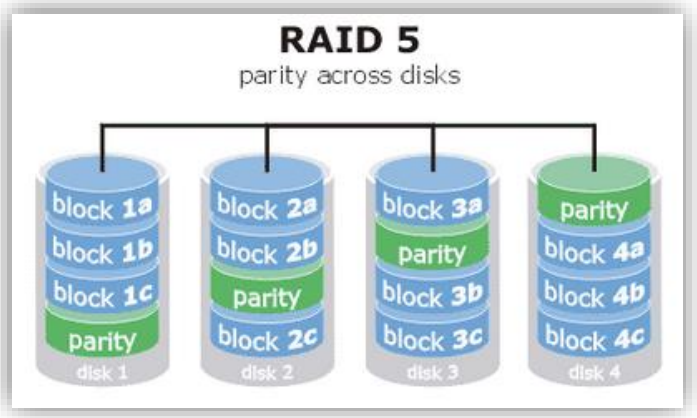
- Fonctionnement d'un système d'exploitation.
- Hébergement de données (redondance ou sauvegardes).

RAID 1



Le RAID 1 nécessite deux disques durs. L'écriture des données s'effectuent simultanément sur les deux disques : on parle alors de mirroring. Si un disque tombe, le contrôleur RAID désactive ce dernier avant que le second prenne le relais. Ce système présente un compromis intéressant entre rapidité et protection des données et sera employé pour répliquer les systèmes hébergeant les systèmes d'exploitation Windows et Linux.

RAID 5



Le RAID 5 nécessite trois disques durs. Ce dernier mélange le RAID 0 (*stripping*) et le RAID 1. Les données ne sont jamais répliquées à l'identique d'un disque à l'autre car leur écriture est basée sur la construction de données de parité. Si un disque tombe, les bits de parité permettent de reconstruire les données à partir des autres disques. Cette solution apporte une meilleure protection des données utilisateurs. Toutefois, le temps d'écriture est bien plus important. Ainsi le RAID 5 conviendra parfaitement pour les serveurs de fichiers Windows.

Une base de données engendre de nombreuses écritures nécessitant des temps rapides d'enregistrement. Nous opterons aussi pour le RAID 1 qui nous semble plus adapté à cet usage.

2.2.3. Choix du matériel

Pour nous deux serveurs, nous nous sommes tournés vers la marque **DELL** en raison de la fiabilité de cette marque et du support de garantie proposé (5 ans de garantie avec intervention sur site en 4 heures).

Le modèle retenu est le **Dell PowerEdge R440**

- Processeur : 2 x Intel Xeon Silver 4110 2.1 G, 8C/16T
- Mémoire : 2 x 16 G
- Baies de stockage : 10
- Alimentation redondée : de 550W
- Carte réseau : 2 x Broadcom 5720 Dual Port 1 Gbe

Ce modèle dispose de 10 baies de stockage 2.5' qui permettra la mise en œuvre de nos disques SAS montés en RAID 1 et 5.

Un modèle identique de ce serveur ainsi que des disques durs supplémentaires sont compris dans le budget en guise d'équipement de **spare**.

Les serveurs de taille 1U seront hébergés dans les baies de stockage précédemment installées lors du projet START pour accueillir les équipements réseaux (switchs et routeur).

Enfin, le matériel sera sécurisé au moyen d'onduleur contre les surtensions et de climatisations pour éviter la surchauffe.

Ce rappel de l'infrastructure existante nous a permis de mieux comprendre dans quel contexte nos serveurs physiques seront installés avec toutes les précautions de sécurisation nécessaires.

Nous avons justifié l'intérêt de posséder plusieurs serveurs et de les séparer géographiquement pour une raison de sécurité et de redondance.

Ceci va permettre de comprendre comment nos machines vont s'organiser d'un point de vue logique en abordant la virtualisation des systèmes.

3. VIRTUALISATION ET GESTION DES SYSTÈMES

3.1. Virtualisation

3.1.1. Intérêts de la virtualisation

Ces dernières années, de plus en plus de sociétés ont recours à la virtualisation. Cette technologie consiste à simuler un serveur physique sous forme logicielle en faisant fonctionner un ou plusieurs systèmes d'exploitation en même temps. La virtualisation peut s'effectuer sur un ordinateur ou un serveur. Ainsi, un hyperviseur facilite le dimensionnement d'un serveur en simulant des ressources matérielles (CPU, RAM, HDD, etc.) et logicielles dans une machine émulée que l'on appelle machine virtuelle (*VM*, « *Virtual Machine* ») : c'est à l'intérieur de cette machine que s'exécute le système d'exploitation.

La virtualisation de systèmes d'exploitation apporte des avantages dans les domaines suivants :

- **Performances** : Les configurations matérielles peuvent être modulées au niveau des VM en fonction des besoins et des tâches applicatives recherchées. En outre, les migrations à chaud de VM apportent une répartition des charges.
- **Haute disponibilité** : Si une VM ou un serveur tombent en panne, la migration à chaud d'une VM se déroule de façon transparente sans interrompre la production. Cette fonctionnalité améliore un PRA.
- **Sécurité** : Le fonctionnement de plusieurs VM cloisonne les services : si l'une des VM est infectée par un virus ou rencontre une panne, elle n'impactera pas les autres services.
- **Sauvegarde et restauration simplifiée** : Certains hyperviseurs peuvent faire des snapshots ou des sauvegardes des VM qui sont ensuite restaurées en cas de crash.
- **Réduction des coûts** : L'utilisation de plusieurs VM permet des économies financières (moins de serveurs physiques à l'achat) et énergétiques (utilisation de moins de machines).
- **Gestion améliorée** : La mutualisation des VM simplifie l'administration de l'infrastructure tout en apportant une réduction des coûts d'entretien.
- **Impact environnemental :** Le procédé de virtualisation entre en résonnance avec la notion de « ***Green IT*** » qui est en vogue depuis quelques années et qui s'impose déjà comme un des enjeux liés au monde du numérique.

En somme, tous ces éléments nous apprennent que la virtualisation impacte plusieurs domaines et doit être prise en considération par les sociétés souhaitant disposer d'une infrastructure optimisée.

L'enjeu pour le SI est de déterminer le bon ratio entre les performances, l'optimisation et l'investissement tout en ayant conscience des besoins de leur société. Face aux potentialités offertes par cette technologie, il convient maintenant de faire un tour d'horizon des différentes solutions présentes sur le marché à ce jour.

3.1.2. Comparaison des solutions

Le marché ainsi que le monde du logiciel libre proposent de logiciels pour émuler des environnements virtuels. Parmi ceux-ci, trois ont retenu notre attention : VMware vSphere, Hyper-V et Proxmox VE.

Il n'y a pas de solutions meilleures qu'une autre ni de choix parfait dans la mesure où ces hyperviseurs fournissent les mêmes fonctionnalités de base dont une infrastructure aura besoin pour s'assurer de bonnes performances et des services de haute-disponibilité. Citons parmi celles-ci la gestion optimisée de la mémoire, clonage/snapshot, migration, sauvegarde et restauration à chaud des VM.

Si l'on souhaite s'orienter vers des solutions payantes, VMware vSphere et Hyper-V présentent des caractéristiques très analogues. Une solution VMware est réputée plus onéreuse et la segmentation importante des offres en fonction du besoin peut s'avérer déroutante pour l'administrateur système qui doit opérer un choix. De plus, l'ajout de fonctionnalités engendre des frais supplémentaires. A contrario, Hyper-V est réputé être une solution moins dépensière, quoique le modèle des licences a évolué depuis Windows Server 2016 et Hyper-V avec un modèle par processeur et par cœur.

Face à la complexité de certaines offres qui impactent fatalement l'investissement, VMware et Microsoft propose des versions gratuites de leurs hyperviseurs qui sont respectivement VMware vSphere Hypervisor 6.0 et Microsoft Hyper-V Server 2012 R2 : ces dernières conservent leurs fonctionnalités de base quoique Hyper-V soit dépourvu d'interface graphique pour la configuration des VM qui s'opère seulement via le CLI Powershell.

Proxmox se situe au même niveau en termes de fonctionnalités et n'a rien à envier à ses concurrents. Notre choix, qui se portera sur ce dernier nous parait cohérent puisqu'il nous permet de rester sur un budget équilibré sans lésiner sur la qualité de cet hyperviseur qui tire parti de la stabilité de Debian tout en apportant le même lot de fonctionnalités.

3.1.3. Proxmox

Proxmox VE (« *Virtual Environnement* ») est un logiciel open source dédié à la virtualisation de systèmes d'exploitation. Cette solution développée par l'entreprise Proxmox, est basée sur l'hyperviseur KVM et Debian. Sa prise en main s'effectue au travers d'une interface web grâce à l'intégration du service apache.

Si sa licence est gratuite, la société qui le développe propose un support payant par CPU. Quatre niveaux de prestation sont possibles : *Community*, *Basic*, *Standard* et *Premium*. Nous souscrirons à la version ***Premium*** car elle possède le plus haut niveau de prestation et d'accompagnement. Nous justifions ce choix par le fait que nous ne comptons pas lésiner sur un des aspects systèmes les plus critiques de notre infrastructure.

	PREMIUM	STANDARD	BASIC	COMMUNITY
Stable updates via Enterprise repository	Yes	Yes	Yes	Yes
Technical support	via Customer Portal	via Customer Portal	via Customer Portal	via Community Forum
Support tickets included	Unlimited	10 per year	3 per year	None *
Response time	1 business day	1 business day	1 business day	n/a
Remote support (via SSH)	Yes	Yes	No	No
Pricing	€ 66,33 per month & CPU-socket	€ 33,17 per month & CPU-socket	€ 19,99 per month & CPU-socket	€ 5,83 per month & CPU-socket

* Support via public Proxmox support forum

Proxmox se dote des fonctionnalités suivantes :

- Gestion du stockage par partition avec LVM ou LXC pour la mise en place de conteneurs.
- Sauvegardes et restauration de VM.
- Exploitation du protocole de partage NFS.
- Clustering pour effectuer des migrations à chaud des VM sans coupure entre serveurs physiques (au moyen d'un SAN ou d'un stockage partagé).
- Snapshots à chaud des VM.
- Administration de rôles et de groupes.
- Gestion de réseau et VLANs avec Open vSwitch.
- Authentification PAM ou Active Directory.

La redondance des services étant traitée dans la partie système de Windows, nous utiliserons pour le moment Proxmox pour l'installation des machines virtuelles Windows et Linux uniquement.

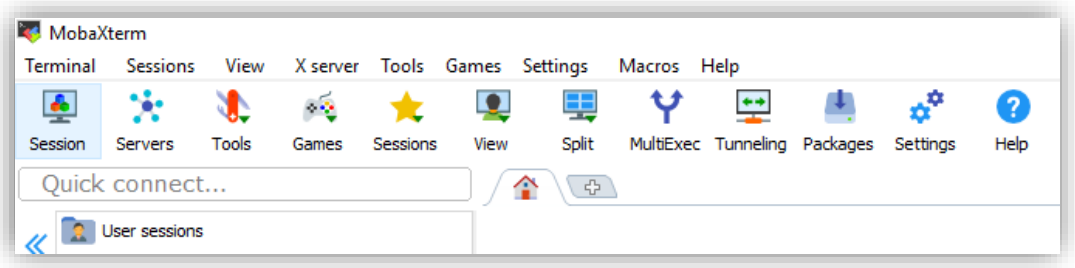
3.2. Administration des VM

3.2.1. Utilisation de MobaXterm

MobaXterm est un émulateur de terminal basé sur Linux capable d'établir des connexions à distance sur plusieurs machines en intégrant un client SSH basé sur PuTTY. De plus, il comporte un serveur X11 qui assure un export d'écran. De cette façon, il est possible de monter plusieurs sessions sécurisées simultanément sur des machines à distances.

À noter que l'accès aux machines virtuelles peut aussi s'effectuer depuis Proxmox en renseignant l'adresse IP de l'hyperviseur dans le navigateur

Il intègre en outre la possibilité d'établir une ***session SFTP*** si l'on souhaite copier manuellement des données, en assurant un accès complet à l'arborescence de fichiers contenus dans la VM.



Enfin, il possède une interface ergonomique et intuitive par laquelle il est possible d'enregistrer plusieurs sessions utilisateur. De cette manière, on peut enregistrer plusieurs profils avec leurs clés SSH que l'on pourra générer grâce à Mobaxterm en vue de sécuriser chaque accès.

3.2.2. Sécurisation des accès

Les accès s'effectuant en local, les risques d'intrusions sont minimes. Toutefois, nous avons sécurisé l'accès à Proxmox et à nos VM puisque cette partie logicielle est à la racine de notre infrastructure systèmes avec le haut degré de criticité qu'elle implique.

Configuration [annexe **9.4**]

SSH : Tous les accès aux VM s'effectueront au moyen d'une connexion SSH lancée depuis Mobaxterm. Pour ce faire, nous modifierons le port d'écoute de base de SSH (le 22) en le remplaçant par le 37913 afin de limiter les risques de scans. Les clés RSA des utilisateurs autorisés à accéder aux machines seront stockées dans le fichier **.ssh/authorized_key**. La sécurisation des VM jongle ainsi entre haute protection et souplesse puisque la suppression d'une clé d'un utilisateur ne nous contraint pas à redéfinir toute la sécurité d'ensemble : Il suffira simplement d'éditer le fichier **.ssh/authorized_keys** qui héberge les clés pour retirer les droits d'accès d'un utilisateur.

Faitoban : Le logiciel fail2ban limite les tentatives de mots de passe au bout d'un nombre d'essais défini dans le fichier de configuration **/etc/fail2ban/jail.conf.**

3.2.3. Dimensionnement et rôles des machines virtuelles

Proxmox sera installé sur les deux serveurs de l'entreprise et se nommeront **SRV1** (local C) et **SRV2** (local T). Tout comme les VM de chaque serveur, les hyperviseurs seront présents dans le réseau 192.168.40.0 avec les adresses suivantes :

- SRV1 : 192.168.40.1
- SRV2 : 192.168.40.2

Toutes les VM Windows et Linux sont comprises dans le pool d'IP 192.168.40.0/24.

Les VM fonctionnent autour de deux systèmes d'exploitation différents :

- **Windows Server** :
  - SRV-AD1, SRV-AD2 : Réplication des rôles Active Directory, DNS et DHCP.
  - SRV-DFS1, SRV-DFS2 : Réplication DFS entre serveurs de fichiers.
- **CentOS** :
  - SRV-NUX1 : Serveur NFS, serveur de fichiers et base de données.
  - SRV-NUX2 : Client NFS, sauvegarde de SRV-NUX1.
  - SRV-FTP : serveur FTP.

SERVEURS	VM	Rôles et logiciels installés	ADRESSAGE RÉSEAU
SRV1	SRV-AD1	Active Directory DNS DHCP	Adresse IP : 192.168.40.10 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.40.10
	SRV-DFS1	Serveur de fichiers Windows	Adresse IP : 192.168.40.30 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.40.10
	SRV-NUX1	Serveur de fichiers Base de données SQL Logiciel gestion de parc GLPI Serveur NFS	Adresse IP : 192.168.40.50 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.40.10
SRV2	SRV-AD2	Active Directory DNS DHCP	Adresse IP : 192.168.40.20 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.40.10
	SRV-DFS2	Serveurs de fichiers Windows	Adresse IP : 192.168.40.40 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.40.10
	SRV-NUX2	Sauvegarde du serveur de fichiers et de la base de données Client NFS	Adresse IP : 192.168.40.60 Masque de sous-réseau : 255.255.255.0 Serveur DNS primaire : 192.168.40.10
	SRV-FTP	vsFTPd	Adresse IP : 192.168.40.99 Masque de sous-réseau : 255.255.255.0

La réplication des rôles Windows et la duplication des données sur plusieurs machines virtuelles apporte un équilibrage de la charge d'utilisation des serveurs dans un souci de performance. En effet, la réplication des données engendre des flux réguliers et une sollicitation particulière des serveurs.

Les deux premières machines Linux seront liées via le protocole de partage NFS afin d'effectuer des sauvegardes régulières des données du serveur de fichiers et de la base de données (voir partie **5.5**).

Une dernière machine Linux de taille modeste nous servira à configurer un serveur FTP isolée du reste du réseau. Elle sera en libre accès et contiendra de la documentation à destination des visiteurs.

Le dimensionnement des systèmes émulés représente un enjeu important dans la manière d'appréhender l'optimisation et la sécurisation d'une infrastructure système. Ce fractionnement des services a des conséquences sur les performances et la sécurisation de notre infrastructure. Une telle configuration va dorénavant nous permettre de configurer la haute disponibilité des services et la sauvegarde des données à partir des environnements Windows et Linux.

4. WINDOWS SERVER

4.1. Choix de la version Windows Server 2016

La mise en place de notre nouvelle infrastructure serveur est l'occasion d'installer la toute dernière version de Windows Server. Assez similaire à Windows Server 2012 R2, Windows Server 2016 a pourtant été amélioré au niveau de plusieurs fonctionnalités.

L'accent a notamment été mis sur l'administration des VM depuis Hyper-V (composant que nous n'utiliserons pas dans ce projet) et sur la gestion du système. En effet, Windows Server voit son **administration améliorée** sur les points suivants :

- Meilleure qualité de gestion au moyen de plus de scripts.
- Automatisation des tâches grâce à PowerShell.
- Possibilité de recourir à une version Windows Server Core, sans interface graphique allégée et configurable qu'en ligne de commande pour réduire la surface d'attaque.

Par ailleurs, des problématiques liées à la compatibilité et à l'**évolutivité des systèmes** ont influencé notre décision pour cette version. En effet, l'environnement de la version 2016 s'adapte mieux avec les versions Windows 10 : puisque nous partons d'une base neuve, il nous parait plus pertinent d'installer la dernière version afin de contourner toutes les contraintes inhérentes à la migration future d'un système vers un autre (ralentissement de la production, maintenance lourde, vulnérabilité des données, etc.).

Enfin, Microsoft s'est tourné sur l'avenir en adaptant son OS au monde de la **mobilité.** En effet, la sécurité s'est vue améliorée en prenant en compte de nouvelles pratiques telles que le **BYOD** et l'utilisation du **cloud**. Ces fonctionnalités ne seront pas abordées mais il est important de les signaler puisque les responsables et commerciaux possèdent des ordinateurs portables, ce qui présente un enjeu important dans le cadre de la sécurité et l'administration des terminaux mobiles.

4.2. Serveur DNS

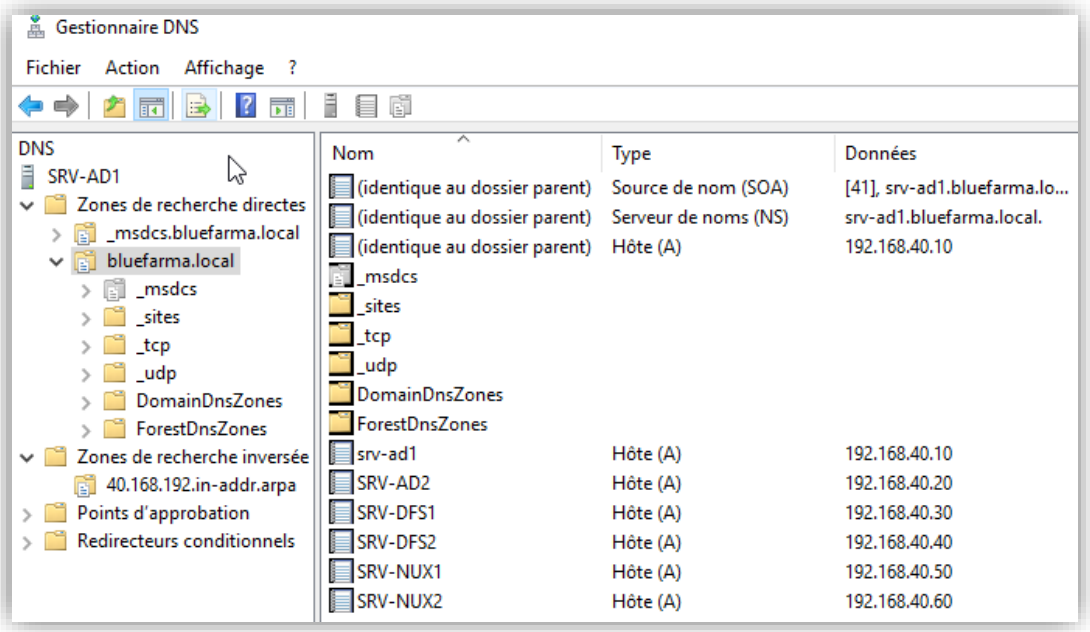
Le service DNS (« *Domain Name Service* ») est un protocole qui permet de convertir un nom de domaine en adresse IP et inversement sur un réseau. Ce protocole s'utilise pour la navigation internet ou pour communiquer avec un serveur et accéder à ses services. Un serveur DNS est construit sur un système hiérarchique lui permettant d'avoir autorité sur leurs zones. Par conséquent, ce dernier ne peut résoudre que les enregistrements de sa zone.

Un serveur DNS est important sur deux points :

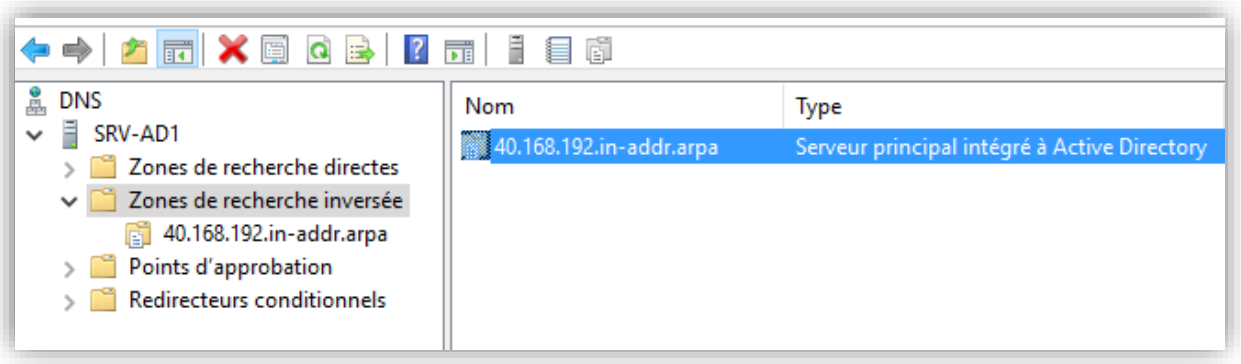
- **Lorsqu'un poste client souhaite joindre son *contrôleur de domaine*** : Le DNS est indispensable pour l'utilisation d'un annuaire Active Directory car il permet aux postes clients de localiser le contrôleur de domaine. Active Directory va pouvoir ainsi traiter chaque requête. Le serveur DNS crée alors une zone correspondante au domaine en produisant plusieurs enregistrements indispensables au fonctionnement d'Active Directory.
- **Attribuer un nom de domaine à plusieurs machines virtuelles** : le nom de domaine « bluefarma.local » sera utilisé afin d'éviter de renseigner l'adresse IP d'un serveur (notamment les serveurs GLPI et MySQL, voir partie **5.6**).

Notre serveur DNS sera automatiquement créé lors de l'installation d'un contrôleur de domaine pour Active Directory (voir partie **4.3.2**).

Le serveur DNS installé sur SRV-AD1 aura une fonction maîtresse dans la gestion générale du DNS puisqu'il délivrera un nom de domaine à chaque machine virtuelle Windows ou Linux présentent sur les serveurs.



L'ajout d'une zone supplémentaire de recherche s'effectuera depuis le Gestionnaire DNS. Elle nous aidera à résoudre une adresse IP en noms de machine. Une zone de recherche inversée est créée dans un premier temps : il s'agit d'un sous-domaine du domaine **in-addr.arpa**. Le nom de la zone sera ensuite construit en effectuant une inversion de l'ordre des octets de l'adresse réseau (ID réseau) + in-addr.arpa, ce qui donne dans notre cas **40.168.192.in-addr.arpa**.



On parle aussi de pointeur ou d'enregistrement **PTR** (« *Pointer Record* ») qui associe une adresse IP à un nom d'hôte sous la forme ***50.40.168.192.in-addr.arpa. IN PTR SRV-NUX1.bluefarma.local***.

Il est d'ailleurs possible de créer des alias afin de simplifier le nom à renseigner dans la barre d'adresse du navigateur. **Configuration** [annexe **9.1.3**].

4.3. Active Directory

4.3.1. Définition

Active Directory, ou **AD DS** (« *Active Directory Domain Services* ») est un annuaire qui fournit des identités et administre les accès des utilisateurs. Ainsi, il référence des comptes utilisateurs, des ordinateurs, des partages, des groupes, etc. qu'il gère sous forme d'objets qui sont centralisés au sein d'un annuaire pour faciliter la gestion du système d'information.

L'AD est compris dans un domaine qui constitue son unité de base (on parle alors de « domaine racine ») et par lequel il regroupe tous les objets qui partagent le même espace de noms. Le domaine représente ainsi une limite de sécurité pour l'ensemble des comptes utilisateurs.

Le domaine racine possède un nom DNS, à savoir dans notre cas **bluefarma.local**. Ce domaine contient un contrôleur de domaine.

4.3.2. Le contrôleur de domaine

Le contrôleur de domaine est un serveur en charge de la gestion des authentifications des utilisateurs et des ordinateurs, de l'accès aux ressources partagées, etc.. Plus précisément, on peut appréhender le contrôleur de domaine comme un rôle du serveur depuis lequel est créé le domaine. De cette manière, le contrôleur de domaine est au cœur des requêtes

(identification des objets, demandes d'authentification, application des stratégies de groupes, etc.).

Le service DNS est donc intimement lié au contrôleur de domaine puisque son installation s'effectue très souvent dans le cadre de l'installation de l'Active Directory dont il dépend.

4.3.3. Haute-disponibilité de l'Active Directory

Dans le but de respecter un niveau de tolérance aux pannes, nous allons effectuer une réplication de l'annuaire Active Directory. Cette redondance s'effectue au niveau du contrôleur de domaine. De fait, si le serveur principal tombe en défaillance, le contrôleur de domaine secondaire prendra le relais en assurant la continuité des services suivants :

- Continuité de service de l'annuaire.
- Pérennité de la base de l'annuaire.

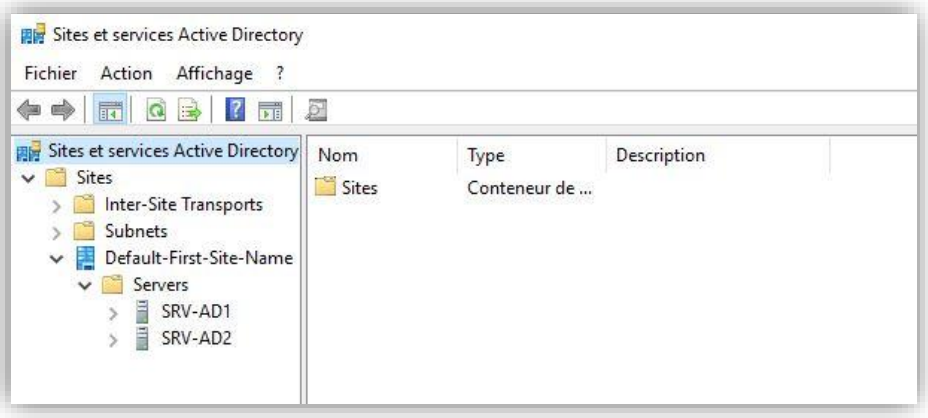
Cette réplication s'inscrit dans la démarche qui consiste à appliquer de la haute disponibilité sur un maximum de services.

Configuration de la réplication [annexe **9.1.2**]

La configuration de cette réplication s'effectuera sur les machines SRV-AD1 et SRV-AD2. Le principe consiste à installer un contrôleur de domaine sur chacune des deux machines. Il faut veiller à ce que SRV-AD2 appartienne préalablement au domaine de SRV-AD1. Après l'installation classique du rôle AD DS, SRV-AD2 est ensuite promu en tant que contrôleur de domaine. Ce dernier est enfin ajouté au domaine existant tout en veillant à activer sa réplication avec SRV-AD1.

L'annuaire Active Directory sera alors accessible depuis SRV-AD2. D'ailleurs, l'accès sur cette dernière machine s'effectuera avec le login et mot de passe définis sur SRV-AD1 lors de la première installation d'AD DS et de son contrôleur de domaine.

À la fin de cette configuration, les deux Active Directory fonctionnent en miroir pour constituer une seule unité logique.



4.4. Serveur DHCP

Le protocole réseau DHCP (« *Dynamic Host Configuration Protocol* ») permet d'allouer de façon automatique des adresses IP à des postes ou des machines clients qui se connectent à un réseau. Cette affectation passe par une configuration réseau comprenant une adresse IP, un masque de sous-réseau, une passerelle ou encore des serveurs DNS. Ainsi, un serveur DHCP apporte beaucoup plus de facilité dans la gestion des réseaux de grandes tailles puisque l'administrateur n'a pas besoin de renseigner manuellement la configuration réseau via un adressage statique.

4.4.1. Configuration du serveur DHCP

Il est important de préciser que DHCP est réservé la plupart du temps aux postes utilisateurs et aux imprimantes. Son utilisation pour les serveurs doit rester exceptionnelle.

Pour le moment, les postes utilisateurs seront présents dans le même réseau 192.168.40.0 que les serveurs. Des adresses IP statiques ont été attribuées pour les serveurs :

Serveurs	**Adressage IP**
SRV-AD1	192.168.40.10
SRV-AD2	192.168.40.20
SRV-DFS1	192.168.40.30
SRV-DFS2	192.168.40.40

Le serveur allouera dynamiquement des adresses IP dans une étendue comprise entre **192.168.40.100 et 192.168.40.200** pour chaque poste client qui en fera la demande.

Afin d'augmenter la sécurité, il est même possible de créer des listes pour que le DHCP distribue des baux en fonction des adresses MAC des cartes réseaux des postes clients via la « réservation de bail » ou la création de « filtres ». Ceci engendre une administration assez lourde, toutefois, cette démarche améliore la sécurité puisque seuls les postes enregistrés auront l'autorisation de se voir délivrer une autorisation d'accès sur le réseau de l'entreprise (filtres à activer sur les deux serveurs en cas de fonction de basculement). Toutes ces configurations peuvent être conservées et restaurées dans une base de données.

4.4.2. Haute-disponibilité du service DHCP

Comme pour Active Directory notre serveur DHCP qui a été installé sur SRV-AD1 bénéficiera d'une redondance sur SRV-AD2 afin d'assurer une continuité d'activité en cas de panne d'un des deux serveurs. En effet, l'arrêt de ce service stoppe la délivrance d'adresses IP et par extension, la perte d'accès au réseau pour les postes utilisateurs.

Plusieurs solutions sont envisageables pour pallier ce risque. Elles sont basées sur l'utilisation d'au moins deux serveurs :

- Le **cluster DHCP**.
- L'**étendue DHCP fractionnée.**
- **DHCP Failover** ou « bascule d'étendue DHCP ».

Le principe d'un **cluster DHCP** consiste à installer deux serveurs dans un cluster de sorte à ce que le serveur secondaire prenne le relais en cas de défaillance du serveur principal. En plus de nécessiter beaucoup de paramétrages, le cluster a besoin d'un espace de stockage partagé unique : cette option offre une haute disponibilité mais elle est contraignante puisqu'elle requière une redondance pour prévenir une panne et constitue en soi un *point d'échec*.

L'**étendue fractionnée** nécessite également l'utilisation de deux serveurs indépendants qui possèdent la même configuration DHCP. Ces deux serveurs pratiquent l'équilibrage de charge en se partageant la plage distribuée (en général, 70% des adresses pour le premier serveur et 30 % pour le second). Dans plusieurs cas de figures, il n'y a pas de continuité de service avec cette configuration.

Le **DHCP failover** est une configuration qui existe depuis Windows Server 2012. Cette option fonctionne avec un maximum de deux serveurs et contourne tous les problèmes que l'on peut rencontrer avec les options précédentes. Le failover fonctionne avec deux serveurs au maximum et permet de gérer le même réseau et la même étendue. Il existe deux configurations possibles :

- Mode **actif/actif** correspondant à un « ***équilibrage des charges*** ».
- Mode **actif/passif** utilisant un « ***serveur de secours*** ».

La seule contrainte est que le failover fonctionne sur deux serveurs maximums mais ces derniers ne doivent pas faire forcément partie d'un domaine. D'autre part, il faut veiller à ce que leur horloge de temps soit réglée à moins d'une minute d'intervalle.

Les informations et les baux sont répliqués dans les deux modes, assurant la conservation de la même configuration pour les clients.

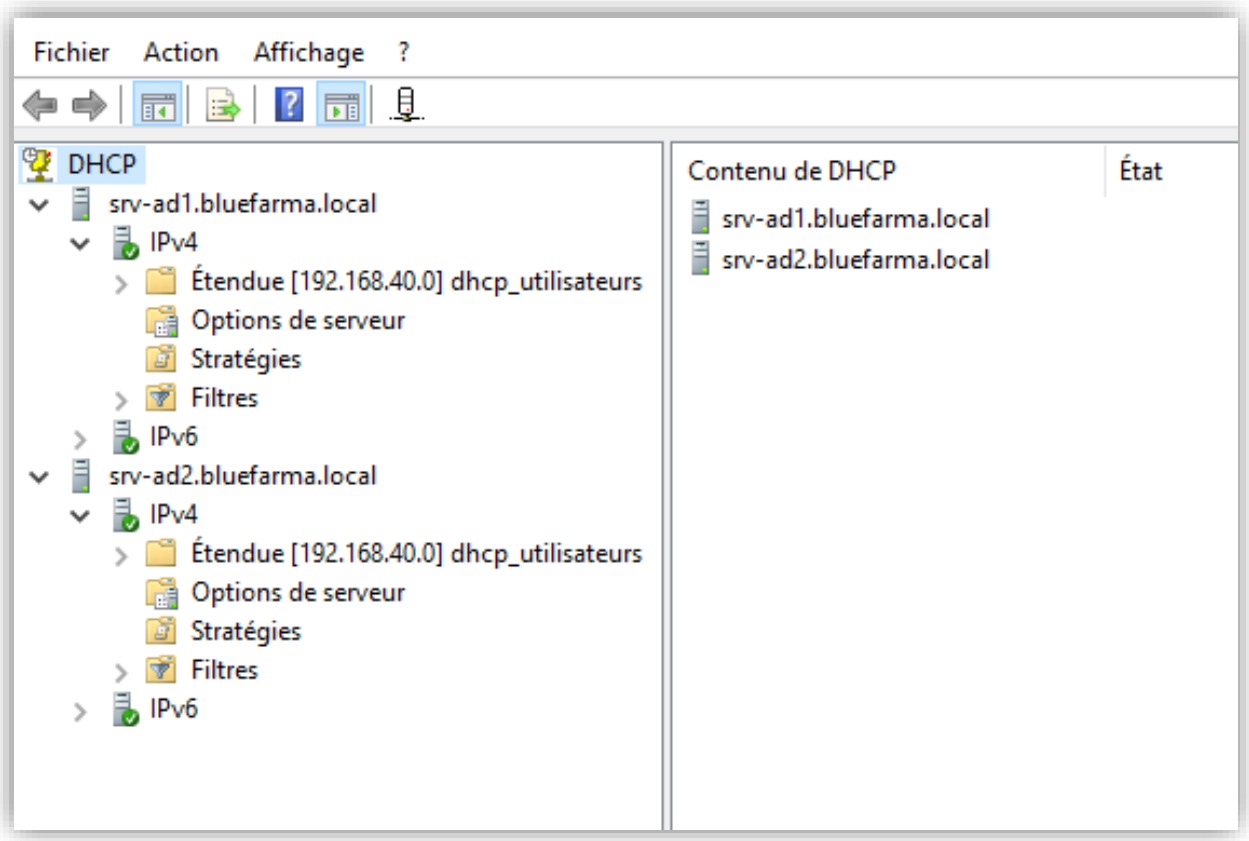
Le mode actif/actif assure l'attribution d'adresses IP au moyen des deux serveurs qui fonctionnent de façon simultanée, d'où le nom d'**équilibrage de charge** pour cette fonction.

Le mode actif/passif assure une haute disponibilité du service via l'option **serveur de secours** : en cas de panne du serveur distribuant des baux, c'est le « serveur partenaire » qui prendra la main.

Nous avons opté pour le mode actif/actif. Ce mode apporte une équilibration de la charge réseau entre deux serveurs tout en rendant l'infrastructure hautement disponible puisqu'en cas de panne, le second serveur pourra continuer à attribuer dynamiquement des adresses IP.

Configuration du basculement [annexe **9.1.5**]

Les rôles DHCP seront installés sur SRV-AD1 et SRV-AD2. Après avoir configuré une étendue sur SRV-AD1, un basculement sera configuré. Lors du paramétrage, SRV-AD2 sera lié à ce dispositif pour répliquer l'étendue dans son rôle DHCP.



4.5. Serveurs de fichiers : la technologie DFS

4.5.1. Le système de fichiers DFS

La technologie **DFS** (« *Distributed Files System* ») ou « système de fichiers distribués » permet d'organiser de manière logique les fichiers qui sont partagés dans un réseau local. De fait, cette structure référence et centralise tous les partages issus des différents espaces de stockage. Ainsi, cette organisation logique apporte une vision unique et hiérarchisée des données qui ne sont plus liées à ses serveurs physiques.

Une telle organisation comporte plusieurs avantages :

- **Économie d'unités réseaux** : une seule lettre permet d'atteindre plusieurs partages physiques.
- **Administration simplifiée** : en cas de panne d'un serveur physique, la liaison DFS est déplacée sur un autre serveur contenant les mêmes données répliquées : le chemin d'accès reste inchangé, rendant ce processus transparent pour l'utilisateur.
- **L'équilibrage et la tolérance aux pannes** : ceci peut se configurer sur les racines ou les liaisons en précisant plusieurs serveurs ou ressources cibles.
- **Évolutivité** : Des capacités de stockage supplémentaires peuvent être ajoutées en étendant dynamiquement l'*espace de noms*.
- **Performances** : Des fonctions de mise en cache sur les postes clients optimisent et accélèrent la recherche et le parcours de l'arborescence DFS.
- **Sécurité** : DFS prend en compte les ACLs situées sur les dossiers répliqués.

En somme, tous les postes utilisateurs auront un accès simplifié au même lecteur qui comporte des partages sous forme de dossiers fonctionnant comme des raccourcis. De plus, la technologie DFS garantie une haute disponibilité des données en les répliquant sur d'autres serveurs grâce à la **réplication DFS**, appelée aussi **RDC** (« *Remote Differential Compression* », compression différentielle à distance). Ainsi, en cas de panne d'un serveur, l'utilisateur continue à avoir accès à ses données de travail.

4.5.2. Haute disponibilité de l'infrastructure DFS

Fonctionnement du système de fichiers DFS :

Le **serveur DFS** héberge la **racine DFS espace de noms**. Il s'agit d'une **racine de noms de domaine** qui base son activité sur la résolution DNS de noms de domaine. Cette racine est inscrite dans l'Active Directory pour faciliter l'accès des utilisateurs de la forêt aux unités DFS. Il est possible d'associer un autre serveur DFS de sorte à ce que la même racine utilise plusieurs serveurs, ce qui augmentera la redondance et la haute disponibilité.

Un dossier, également appelé **liaison DFS**, est ensuite créé. C'est à l'intérieur de ce dossier que seront ajoutées les liaisons pointant sur les **dossiers cibles** présents sur les serveurs de stockage. Une liaison peut viser plusieurs cibles que l'on peut synchroniser ensemble afin

d’effectuer une **réplication** et obtenir ainsi la même donnée à plusieurs emplacements 'à condition d'avoir installé le rôle DFSR). La réplication est basée sur la technologie **RDC**.

Ainsi, une liaison DFS établit un lien avec une **cible** sous la forme d'un chemin d’accès pointant sur les serveurs ou leurs ressources.

En définitive, un serveur d’espace de noms ne reçoit pas directement les données : il ne contient que les dossiers virtuels qui pointent sur des données réelles présentes sur les serveurs de stockage.

Il restera plus qu'à mapper les utilisateurs sur leurs dossiers respectifs en utilisant le chemin d’accès qui a été créé. Pour ce dernier, son dossier personnel apparaîtra sous la forme d'un dossier partagé.

Configuration de la réplication DFS [annexe **9.1.6**]

La configuration s'effectue depuis la console « **Gestion du système de fichiers distribués DFS** ». Les machines suivantes se répartiront les rôles suivants :

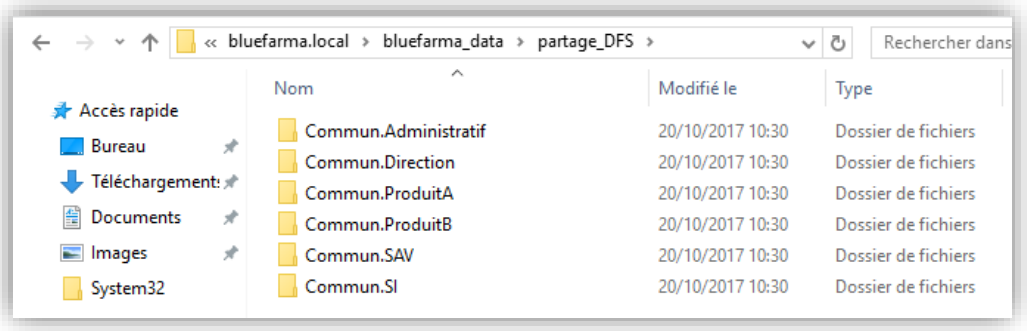
- SRV-AD1 : serveur DFS.
- SRV-AD2 : serveur DFS
- SRV-DFS1 : serveur de stockage.
- SRV-DFS2 : serveur de stockage.

Le rôle de « **Services de fichiers et de stockage** » étant nativement installés dans Windows Server, il convient d’ajouter les rôles « **Espaces de noms DFS** » et « **Réplication DFS** » sur ces machines.

Des dossiers partagés seront ensuite créés sur les deux serveurs de stockage SRV-DFS1 et SRV-DFS2 et dans lesquelles seront répliquées les données utilisateurs.

Le serveur DFS, SRV-AD1, hébergera la **racine DFS espace de noms** que l'on nommera ***bluefarma_data***. Fonctionnant par résolution DNS, cette dernière sera accessible par le chemin \\bluefarma.local\bluefarma_data. Nous ajouterons SRV-AD2 en tant que serveur d'espace de noms supplémentaire pour augmenter la tolérance aux pannes.

Une liaison DFS (dossier), que l'on nommera ***partage_DFS***, sera créé dans l'espace de noms et pointera sur les ressources partagées de SRV-DFS1 et SRV-DFS2. Le chemin **\\bluefarma.local\bluefarma_data\partage_DFS** aboutit directement sur les répertoires des différents services de l'entreprise.



Il s'agit d'une représentation virtuelle des dossiers partagés dont le chemin d'accès se rapproche du chemin **UNC** (« *Universal Naming Convention* ») qui a pour fonction de centraliser l'accès aux dossiers partagés de tous les serveurs depuis un emplacement unique.

4.6. Serveur d'impression

Un serveur d'impression est une application qui partage une ou plusieurs imprimantes qu'il va rendre accessibles dans un réseau local en gérant les demandes émanant des clients finaux.

Consignes du cahier des charges

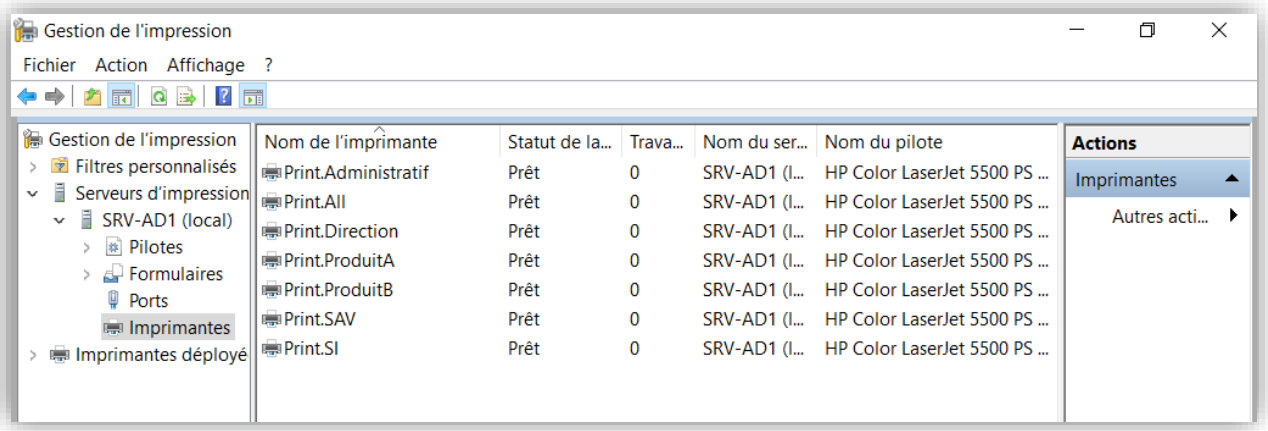
Chaque service doit posséder sa propre imprimante. Une autre imprimante réseau doit être configurée pour que tous les services puissent l'utiliser. Afin que les imprimantes réseaux soient facilement reconnaissables, nous utilisons la convention de nommage suivante **[Print + < nom du service >]**. Chacune d'entre elles se verra attribuer une adresse IP fixe comme synthétisé dans le tableau suivant :

Nom de l'imprimante	Adressage IP (/24)
Print.ALL	192.168.40.240
Print.Direction	192.168.40.241
Print.Administratif	192.168.40.242
Print.SAV	192.168.40.243
Print.SI	192.168.40.244
Print.ProduitA	192.168.40.245
Print.ProduitB	192.168.40.246

L'attribution des imprimantes pour les utilisateurs se fera par GPO (voir partie **4.7.5**).

Configuration [annexe **9.2.4**]

L'installation du serveur d'impression s'effectue comme d'habitude par l'ajout d'un rôle depuis l'interface ***Gestionnaire de serveur***. Lors de la configuration de l'installation, nous veillerons à sélectionner l'option ***Service LPD*** (« *Line Printer Daemon* ») pour installer le serveur d'impression TCP/IP qui permet aux ordinateurs Linux (comme le service SAV) ou à d'autres ordinateurs utilisant le service LPR, d'imprimer sur des imprimantes partagées dans le même réseau.



4.7. Stratégies d'administration et maintenance des systèmes

Les GPO et les scripts Powershell seront les outils principaux que nous utiliserons pour mettre en œuvre la gestion des utilisateurs, du système d'information ainsi que les droits, la sécurité et l'administration des postes qui peuplent notre parc informatique.

4.7.1. Active Directory et création des utilisateurs

Administrer un parc de 90 utilisateurs peut vite devenir complexe si l'on ne cherche pas à se simplifier la tâche.

Même si Active Directory apporte de la simplification dans la gestion et l'organisation des utilisateurs, certaines actions peuvent être très longues si elles ne sont pas automatisées. On peut pour cela passer par divers scripts, notamment en ***PowerShell***.

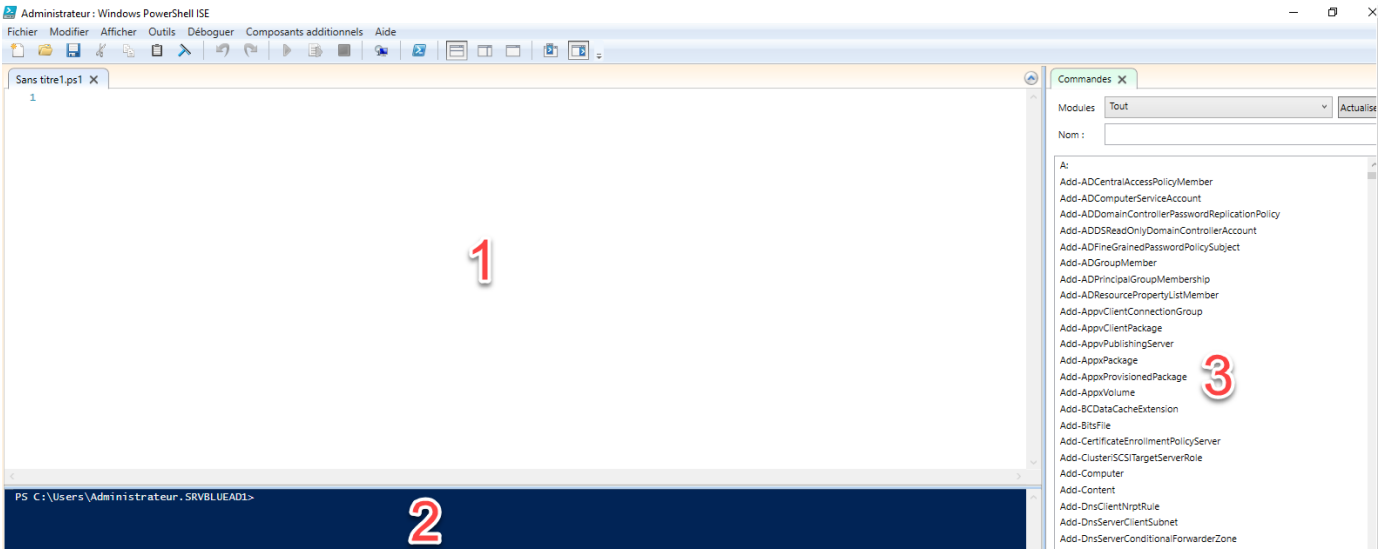
PowerShell est un outil efficace pour Windows, et reste simple d'utilisation car il utilise des ***commandlets*** qui sont constituées de *verbes*, *préfixes* et *noms* en anglais et donc facilement compréhensibles. De plus, on a la possibilité d'ajouter des modules supplémentaires afin d'apporter des compléments à PowerShell (simplification de certaines tâches ou ajouts de fonctionnalités, par exemple).

De plus, chaque action effectuée sur l'Active Directory via la GUI a un équivalent en PowerShell. Ainsi, la création de comptes pour 90 utilisateurs va pouvoir être automatisée grâce à un script. Il contiendra les process suivants :

- Création des différentes ***Unités d'Organisation*** (***OU***) dans lesquelles seront placés les utilisateurs, puis les groupes de sécurité qui serviront également à leur attribuer des permissions.
- **Association des comptes à leur OU** et **groupe de sécurité** respectif à chaque service.
- Création d'un **répertoire par utilisateur** : Chaque utilisateur doit avoir accès à son dossier personnel sur le réseau, mais il ne doit pas avoir accès à ceux des autres. Plutôt que de créer chacun des 90 dossiers à la main, ce qui demanderait considérablement de temps, nous automatiserons cette tâche via le script en créant les dossiers au nom des utilisateurs et en attribuant les bons droits NTFS sur les dossiers.

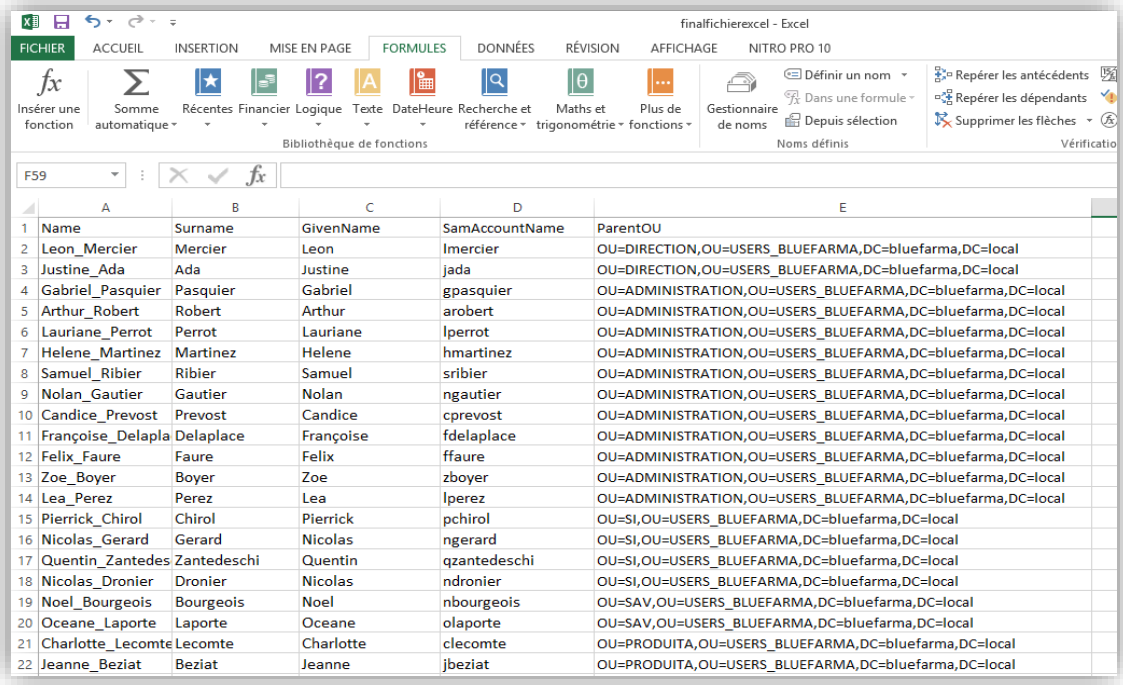
Nous nous baserons sur un fichier CSV afin d'importer les informations qui ne peuvent pas être automatisées, à savoir les noms des employés et les services dans lesquels ils se trouvent. **Windows PowerShell ISE** (« *Integrated Scripting Environment* ») est l'interface graphique qui permet de créer et modifier les scripts. Windows PowerShell ISE est installé par défaut et permet la coloration de la syntaxe, la saisie semi-automatique, l'aide contextuelle, etc. Quant au module « *File System Security PowerShell Module* », il permet l'administration des permissions sur les fichiers et dossiers de façon simplifiée grâce à PowerShell.

Aperçu de l'interface Windows Powershell ISE. 1) Zone d'édition du script. 2) Affichage du script. 3) Liste des commandes.



<u>Explication du script PowerShell</u> :

- Créer le fichier CSV contenant l'ensemble des utilisateurs de l'AD avec les attributs : *Name*, *Surname*, *GivenName*, *SamAccountName* et *ParentOU*.



	A	B	C	D	E
1	Name	Surname	GivenName	SamAccountName	ParentOU
2	Leon_Mercier	Mercier	Leon	lmercier	OU=DIRECTION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
3	Justine_Ada	Ada	Justine	jada	OU=DIRECTION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
4	Gabriel_Pasquier	Pasquier	Gabriel	gpasquier	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
5	Arthur_Robert	Robert	Arthur	arobert	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
6	Lauriane_Perrot	Perrot	Lauriane	lperrot	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
7	Helene_Martinez	Martinez	Helene	hmartinez	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
8	Samuel_Ribier	Ribier	Samuel	sribier	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
9	Nolan_Gautier	Gautier	Nolan	ngautier	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
10	Candice_Prevost	Prevost	Candice	cprevost	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
11	Françoise_Delapla	Delaplace	Françoise	fdelaplace	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
12	Felix_Faure	Faure	Felix	ffaure	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
13	Zoe_Boyer	Boyer	Zoe	zboyer	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
14	Lea_Perez	Perez	Lea	lperez	OU=ADMINISTRATION,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
15	Pierrick_Chirol	Chirol	Pierrick	pchirol	OU=SI,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
16	Nicolas_Gerard	Gerard	Nicolas	ngerard	OU=SI,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
17	Quentin_Zantedes	Zantedeschi	Quentin	qzantedeschi	OU=SI,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
18	Nicolas_Dronier	Dronier	Nicolas	ndronier	OU=SI,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
19	Noel_Bourgeois	Bourgeois	Noel	nbourgeois	OU=SAV,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
20	Oceane_Laporte	Laporte	Oceane	olaporte	OU=SAV,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
21	Charlotte_Lecomte	Lecomte	Charlotte	clecomte	OU=PRODUITA,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local
22	Jeanne_Beziat	Beziat	Jeanne	jbeziat	OU=PRODUITA,OU=USERS_BLUEFARMA,DC=bluefarma,DC=local

- Le début du script correspond à la création des différentes OU : un nom pour l'OU est indiqué ainsi qu'un chemin « *path* ». Les groupes de sécurité sont également créés et placés dans une OU « *Groupes* ».

```powershell
Import-Module ActiveDirectory
Import-Module 'Microsoft.PowerShell.Security'

#******************Création des OU*******************************

Write-Host "---------------------------------"
Write-Host "Creation des Unites d'Organisation"
Write-Host "---------------------------------"

New-ADOrganizationalUnit -Name "Utilisateurs_Bluefarma" -Path "dc=bluefarma,dc=local"
New-ADOrganizationalUnit -Name "Administratif" -Path "ou=Utilisateurs_Bluefarma,dc=bluefarma,dc=local"
New-ADOrganizationalUnit -Name "Direction" -Path "ou=Utilisateurs_Bluefarma,dc=bluefarma,dc=local"
New-ADOrganizationalUnit -Name "ProduitA" -Path "ou=Utilisateurs_Bluefarma,dc=bluefarma,dc=local"
New-ADOrganizationalUnit -Name "ProduitB" -Path "ou=Utilisateurs_Bluefarma,dc=bluefarma,dc=local"
New-ADOrganizationalUnit -Name "SAV" -Path "ou=Utilisateurs_Bluefarma,dc=bluefarma,dc=local"
New-ADOrganizationalUnit -Name "SI" -Path "ou=Utilisateurs_Bluefarma,dc=bluefarma,dc=local"


#******************Création des groupes*******************************

Write-Host "---------------------------------"
Write-Host "Creation des groupes"
Write-Host "---------------------------------"

New-ADOrganizationalUnit -Name "Groupes" -Path "dc=bluefarma,dc=local"
New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"Administratif" -Path:"OU=Groupes,DC=Bluefarma,DC=local"
New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"Direction" -Path:"OU=Groupes,DC=Bluefarma,DC=local"
New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"ProduitA" -Path:"OU=Groupes,DC=Bluefarma,DC=local"
New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"ProduitB" -Path:"OU=Groupes,DC=Bluefarma,DC=local"
New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"SAV" -Path:"OU=Groupes,DC=Bluefarma,DC=local"
New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -Name:"SI" -Path:"OU=Groupes,DC=Bluefarma,DC=local"


```

- Les 90 utilisateurs sont créés lors de l'importation du fichier CSV. Une boucle est lancée afin de récupérer pour chaque objet les informations du CSV en les associant aux critères d'une création d'utilisateur sur l'AD : nom, prénom, le « *GivenName* » qui équivaut à l'alias sur l'AD, et qui sera le nom affiché dans la liste des utilisateurs, etc. Un mot de passe par défaut « *MyPassword123ADF* » est spécifié par défaut. On précise que l'utilisateur sera contraint de le modifier lors de l'ouverture de sa première session.

```powershell


 Write-Host "---------------------------------"
 Write-Host "Creation des dossiers persos utilisateurs"
 Write-Host "---------------------------------"


 $CheminCommun = "C:\Bluefarma\Commun.SI\Utilisateurs.SI"
 $ListeMembres = (Get-ADGroupMember SI)
 $IdentifiantSession = $ListeMembres.SamAccountName

foreach($Identifiant in $IdentifiantSession){

    # Creation du dossier personnel
    New-Item -ItemType Directory -Path "$CheminCommun\$Identifiant"

    # Desactiver l'heritage tout en copiant les autorisations NTFS héritées
    Get-Item "$CheminCommun\$Identifiant" | Disable-NTFSAccessInheritance

    # Ajout des autorisations NTFS
    Add-NTFSAccess -Path "$CheminCommun\$Identifiant"  -Account "$Identifiant@bluefarma.local" -AccessRights FullControl

    # Modifier le proprietaire sur le dossier
    Set-NTFSOwner -Path "$CheminCommun\$Identifiant" -Account "$Identifiant@bluefarma.local"

    # Supprimer des autorisations NTFS
    Remove-NTFSAccess -Path "$CheminCommun\$Identifiant"  -Account "Utilisateurs" -AccessRights FullControl

}
```

- Les utilisateurs sont ensuite ajoutés au groupe de sécurité correspondant à leurs services respectifs. Par exemple, les utilisateurs de l'UO « Administratif » sont ajoutés au groupe de sécurité « Administratif » seulement si l'utilisateur n'est pas présent, au moyen de la condition « ***if*** ».

```powershell
#**********Ajout des utilisateurs dans les groupes******************

Write-Host "---------------------------------"
Write-Host "Ajout des utilisateurs aux groupes de sécurité"
Write-Host "---------------------------------"

$users = Get-ADUser -Filter * -SearchBase "OU=Administratif,OU=Utilisateurs_Bluefarma,DC=bluefarma,DC=local"
$group = "Administratif"
$members = Get-ADGroupMember -Identity $group -Recursive | Select -ExpandProperty Name
$users | ForEach-Object {
$user = $_.Name
If (-not($members -contains $user)) {
      Add-ADGroupMember -Identity $group -Members $users
}}

$users = Get-ADUser -Filter * -SearchBase "OU=Direction,OU=Utilisateurs_Bluefarma,DC=bluefarma,DC=local"
$group = "Direction"
$members = Get-ADGroupMember -Identity $group -Recursive | Select -ExpandProperty Name
$users | ForEach-Object {
$user = $_.Name
If (-not($members -contains $user)) {
      Add-ADGroupMember -Identity $group -Members $users
}}
```

- Le dossier personnel de chaque utilisateur est ensuite créé en basant son nom sur son identifiant AD (exemple : ngerard) et ce pour chaque service.
  Dans un premier temps, on crée plusieurs variables stockant le chemin d'accès au dossier du service, la liste des membres du groupe du service et l'identifiant de chaque membre de ce service. Ensuite, on fait une boucle qui crée le dossier pour chaque utilisateur du service. Le propriétaire à un **contrôle total** sur son dossier personnel tandis que son accès est verrouillé pour les autres utilisateurs.

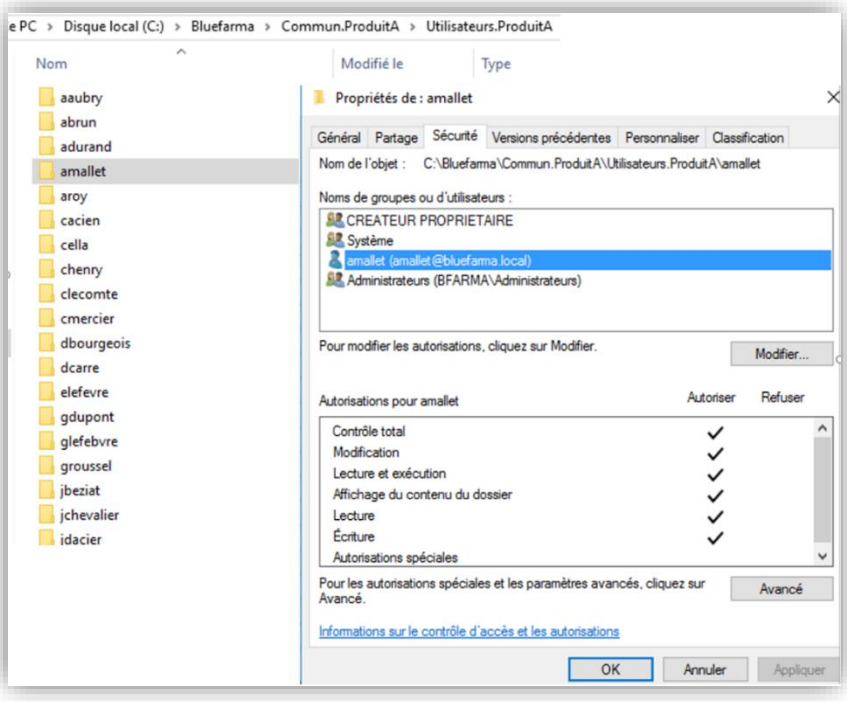
```powershell
#********************Création des utilisateurs**********************

Write-Host "---------------------------------"
Write-Host "Creation des utilisateurs depuis le fichier CSV"
Write-Host "---------------------------------"


<#LOCALISATION FICHIER CSV#>
Import-Csv "C:\NewUsers.csv" | ForEach-Object {
 $userPrincipal = $_."samAccountName" + "@bluefarma.local"
New-ADUser -Name $_.Name `
 <#UNITE ORGANISATION#> `
 -Path $_."ParentOU" `
 <#COMPTE UTILISATEUR#> `
 -SamAccountName  $_."samAccountName" `
  <#PRENOM#> `
 -GivenName $_."givenname" `
  <#Nom#> `
 -Surname $_."surname" `
 <#Spécifie le nom avec lequel l'utilisateur se connectera#> `
 -UserPrincipalName  $userPrincipal `
 <#Généralisation mdp de base#> `
 -AccountPassword (ConvertTo-SecureString "MyPassword123ADF" -AsPlainText -Force)
 <#CHANGEMENT MDP A LA CONNEXION#> `
 -ChangePasswordAtLogon $true  `
 -Enabled $true `

}
```

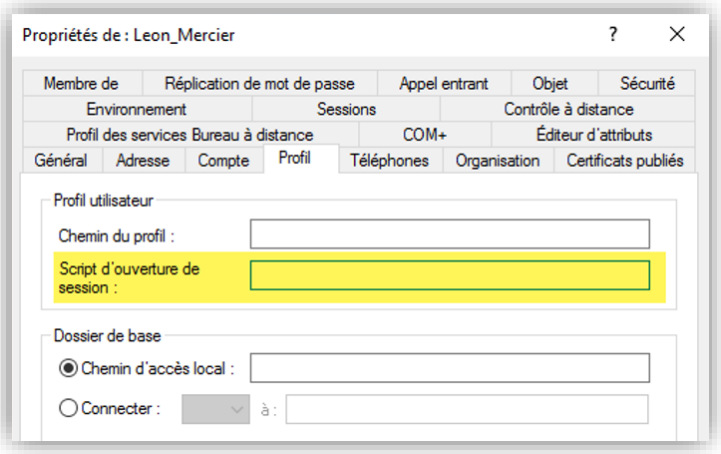
- Le bon fonctionnement du script est ensuite vérifié à partir du serveur de fichiers. On constate que les dossiers sont bien créés au nom de chaque utilisateur avec les droits qui lui sont associés. Exemple : l'utilisateur *Amallet* a un accès unique et total à son dossier personnel.



4.7.2. Configuration des environnements utilisateurs

Un parc informatique correctement administré doit proposer à l'utilisateur un environnement complètement configuré et personnalisé mêlant à la fois des droits et des restrictions. Ainsi, l'utilisateur doit pouvoir accéder à l'ensemble des dossiers dont il aura besoin, sans avoir à effectuer des modifications ou des ajouts sur son poste.
Ceci passe par exemple par la mise à jour des accès, la définition des lecteurs réseaux ou des imprimantes. Les deux solutions principalement utilisées pour la connexion des lecteurs réseaux en entreprise sont les ***logons scripts*** ou scripts d'ouverture de session, et les ***GPO***. Nous avons fait le choix des GPO pour plusieurs raisons :

- **Raisons pratiques et organisationnelles** : nous avons recherché une simplification du process. En effet, les scripts d'ouverture de session sont à configurer au niveau des propriétés de chaque utilisateur. Il faut donc soit passer sur chaque poste utilisateur, soit automatiser ce procédé. Dans tous les cas, nous n'avons pas un aperçu immédiat sur le script appliqué ou non à un utilisateur à moins de rentrer dans les propriétés.
- **Confort pour l'utilisateur** : L'utilisation d'une GPO ne nécessite pas l'affichage d'une invite de commande ou d'un script lors de l'ouverture de session. L'utilisateur pourrait être tenté de les fermer. En passant par GPO, l'utilisateur n'a aucun visuel sur le procédé utilisé.



Connexions aux lecteurs réseaux :

Conformément au cahier des charges, les lecteurs réseaux devront être configurés de la façon suivante :

- **Commun <service>** : aucun accès et aucun visuel sur les communs des autres services
- **Dossier perso utilisateur** : aucun accès et aucun visuel sur les autres dossiers persos (la direction et l'info ont le visu sur tout, l'info a accès en écriture également).

Configuration :

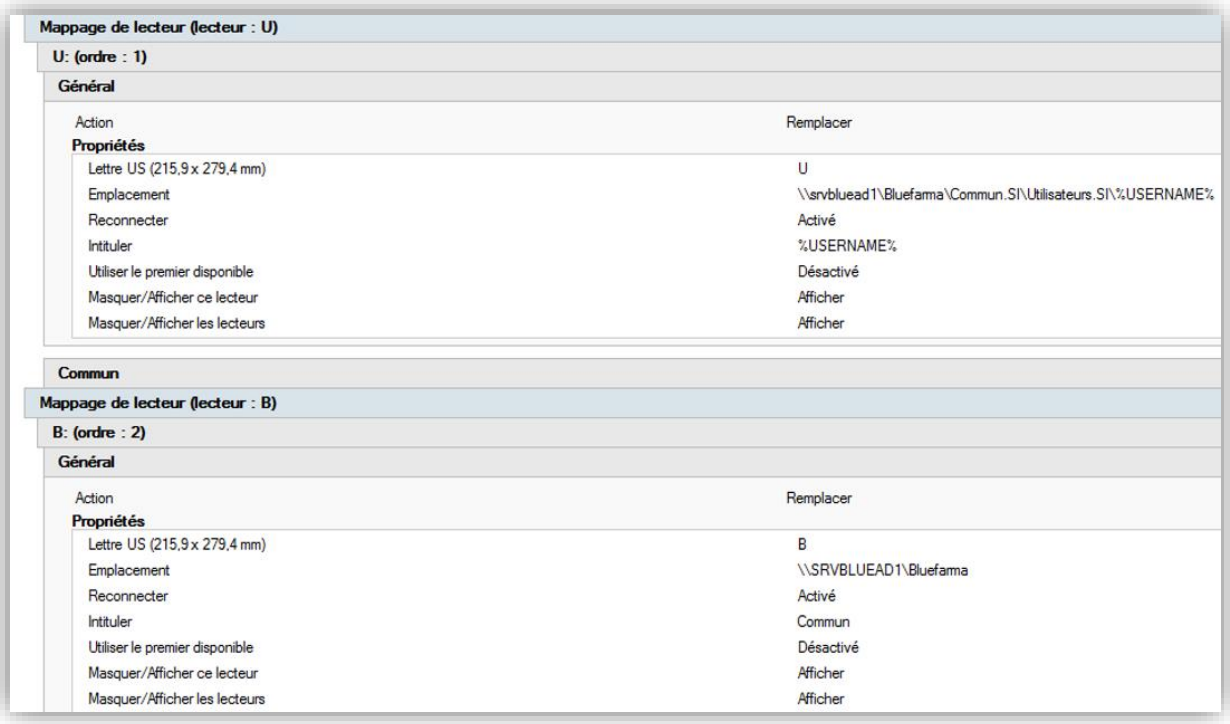
Un fichier script d'ouverture de session est composé de plusieurs commandes. Pour connecter un lecteur réseau, on utilise ***net use***.

Exemple : net use B : \\SRV-AD1\Bluefarma\Commun.SAV

Ce script sera placé dans le répertoire **NETLOGON** afin d'être accessible depuis les postes du domaine. Nous ne passerons donc pas par ces scripts mais bien par des GPO afin de remonter les lecteurs réseaux des utilisateurs. Une GPO ***Mappage_lecteurs*** sera placée pour chaque **OU** correspondant aux services. Ceci apportera plus de souplesse pour l'ajout de nouveaux lecteurs réseaux ou d'accès : au lieu d'appliquer une seule GPO à l'ensemble des utilisateurs, on divise la gestion des lecteurs par services.

On pourra ainsi faire une différence entre le mappage des lecteurs réseaux du Service Informatique et de la Direction, par rapport aux autres services. En effet, la Direction doit avoir accès à l'ensemble des dossiers partagés, en lecture seule. Le SI doit avoir accès à l'ensemble des dossiers en contrôle total (lecture/écriture). On créer donc deux lecteurs réseaux différents :

- **Lecteur U** : Dossier personnel des utilisateurs.
- **Lecteur B** : Répertoire « Bluefarma » contenant répertoires **Communs** de chaque service. Le but est que la Direction et le SI parcourent l'ensemble de l'arborescence des différents dossiers **Communs**.



Mappage de lecteur (lecteur : U)

U: (ordre : 1)

Général

Action	Remplacer
Propriétés	
Lettre US (215,9 x 279,4 mm)	U
Emplacement	\\srvbluead1\Bluefarma\Commun.SI\Utilisateurs.SI\%USERNAME%
Reconnecter	Activé
Intituler	%USERNAME%
Utiliser le premier disponible	Désactivé
Masquer/Afficher ce lecteur	Afficher
Masquer/Afficher les lecteurs	Afficher

Commun

Mappage de lecteur (lecteur : B)

B: (ordre : 2)

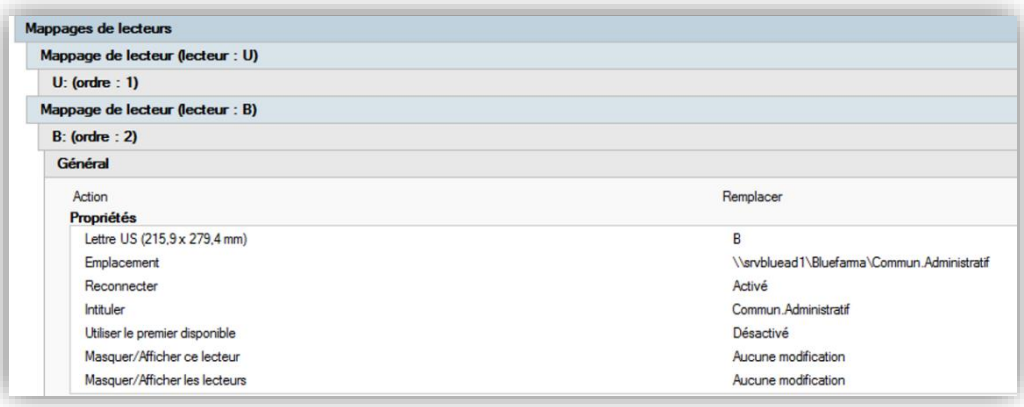
Général

Action	Remplacer
Propriétés	
Lettre US (215,9 x 279,4 mm)	B
Emplacement	\\SRVBLUEAD1\Bluefarma
Reconnecter	Activé
Intituler	Commun
Utiliser le premier disponible	Désactivé
Masquer/Afficher ce lecteur	Afficher
Masquer/Afficher les lecteurs	Afficher

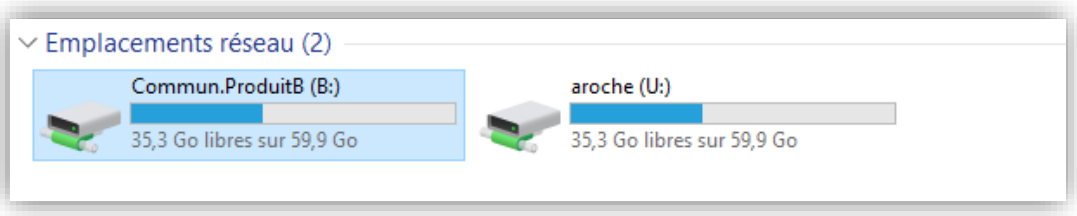
Les autres services auront quant à eux le même lecteur U pointant sur le dossier personnel utilisateur, mais le lecteur B sera configuré pour renvoyer directement sur le dossier commun du service.

Exemple pour le Service Administratif :

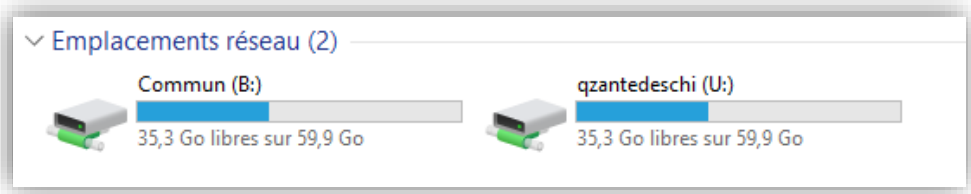
En procédant ainsi, chaque utilisateur détient des accès à deux types de répertoires : **Commun.<*nom du service*>** et un **dossier personnel <*nom de l'utilisateur*>**.



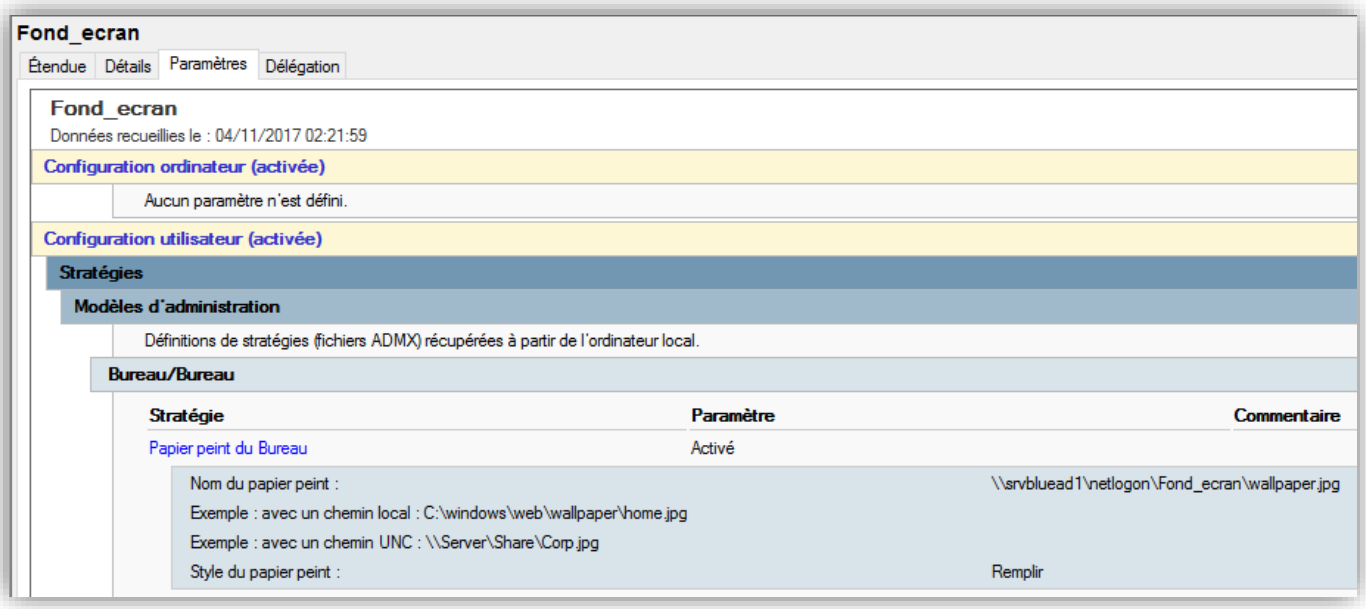
- Aperçu du mappage réseau pour l'utilisateur Adrien Roche du service Produit B : il accède uniquement à « ***Commun.ProduitB*** » et à son dossier personnel « **aroche** » :



- Aperçu pour l'utilisateur Quentin Zantedeschi, du Service Informatique : Il accède à l'ensemble des dossiers « ***Commun*** » et à son dossier personnel :



Propagation du fond d'écran par GPO : Pour standardiser chaque poste de travail aux couleurs de l'entreprise, une GPO va permettre de propager un fond d'écran de base avec le logo Bluefarma.



Fond_ecran

Étendue | Détails | Paramètres | Délégation

Fond_ecran

Données recueillies le : 04/11/2017 02:21:59

Configuration ordinateur (activée)

Aucun paramètre n'est défini.

Configuration utilisateur (activée)

Stratégies

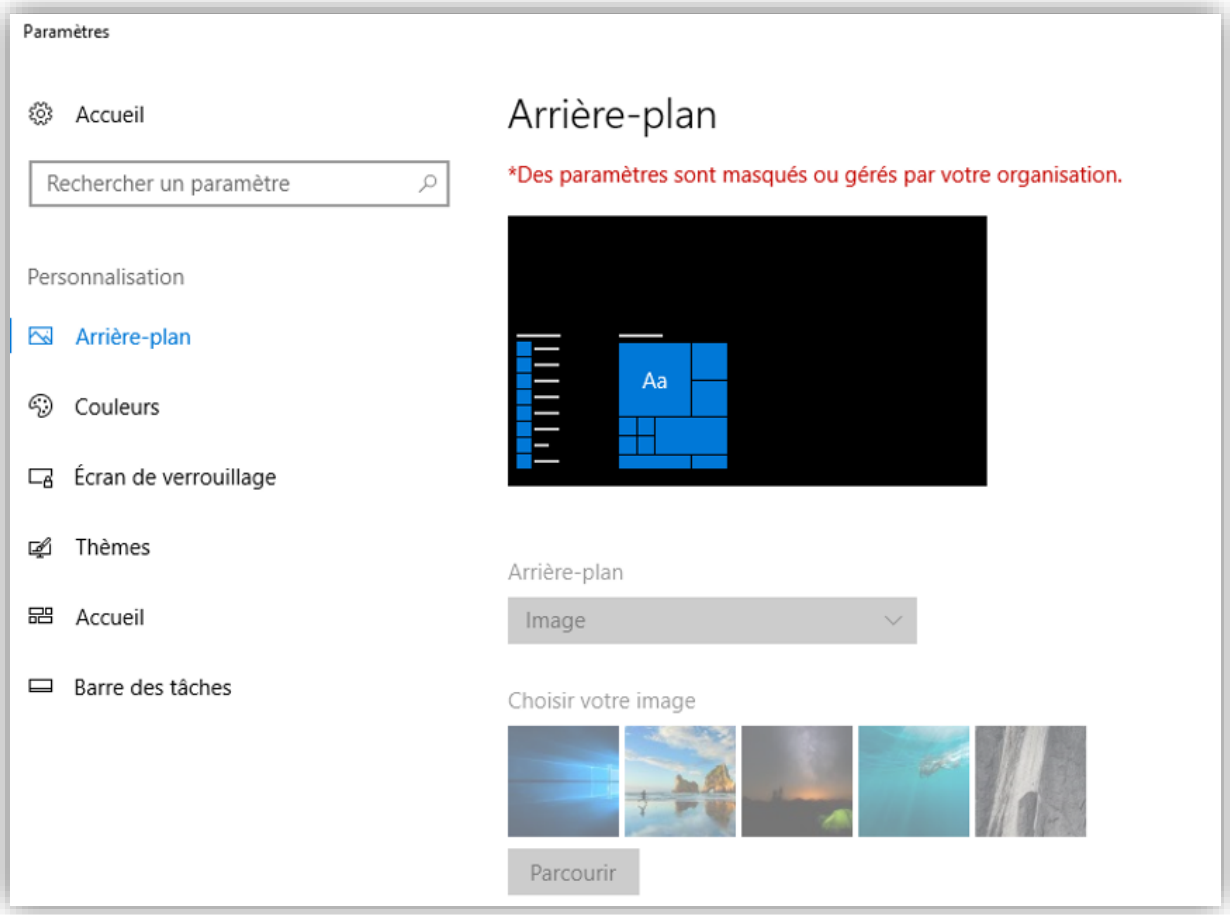
Modèles d'administration

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Bureau/Bureau

Stratégie	Paramètre	Commentaire
Papier peint du Bureau	Activé	
Nom du papier peint :	\\srvbluead1\netlogon\Fond_ecran\wallpaper.jpg	
Exemple : avec un chemin local : C:\windows\web\wallpaper\home.jpg		
Exemple : avec un chemin UNC : \\Server\Share\Corp.jpg		
Style du papier peint :	Remplir	

L’utilisateur n’a pas la possibilité de modifier ce fond d’écran :



4.7.3. Sécurité et gestion des fichiers

La gestion des fichiers dans un contexte d'entreprise est une tâche complexe. Il est très important de mettre en place des stratégies pour ne pas se retrouver avec des problématiques telles que :

- Saturation des espaces de stockages.
- La confidentialité de certaines données en défaut (cf. Direction)
- Le stockage de fichiers non professionnels sur le système de fichiers (musiques, vidéos, etc.)
- Le cryptage de l'ensemble des fichiers par un ***ransomware*** ou ***rançongiciel***.

Active Directory propose plusieurs solutions afin d'organiser au mieux sa politique de partage de fichiers.

Gestion des droits sur les fichiers [annexe **9.2.1**]

Les autorisations de partage régulent l'accès des utilisateurs sur des partages. Les autorisations NTFS permettent de configurer les droits de façon précise sur les dossiers. Un dossier peut ainsi être partagé facilement avec tout le monde en ***contrôle total***, ou avoir des restrictions à partir des paramètres de sécurité NTFS.

Par exemple, les dossiers personnels des utilisateurs du service Produit A seront stockés dans le dossier ***Utilisateurs.ProduitA*** (lui-même présent dans le répertoire Commun.ProduitA) mais chaque utilisateur aura un accès unique à son dossier personnel.

Blocage de fichiers et alerte mails :

Nous limitons l'action d'éventuels ***ransomwares*** cryptant les fichiers au moyen d'une politique de blocage d'extensions de fichiers. Il est à noter qu'il s'agit d'une consolidation de la politique de sécurité, et non d'une solution efficace à elle seule. La prévention auprès des utilisateurs est essentielle pour limiter au maximum les dégâts d'un ransomware. Le SI sera prévenu par mails et pourra réagir en coupant l'accès réseau à une personne qui essaierait de créer des fichiers ***.locky*** sur le serveur de fichiers. D'autres ransomwares ne seront pas bloqués par ces filtres car ils modifieront le fichier en profondeur avant d'en modifier l'extension. Il s'agit néanmoins d'une solution supplémentaire, simple à mettre en place et non contraignante.

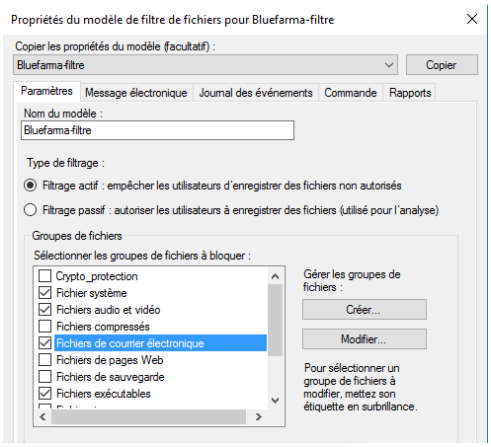
Grâce à ce même outil, on peut ainsi appliquer d'autres filtres proposés de base par Microsoft, ou bien les modifier à notre goût sur des fichiers de type :

- Fichiers systèmes (.dll, .sys)
- Fichiers audio et vidéo (mp3, wav)
- Fichiers mails (msg, pst)
- Fichiers exécutables (.exe, msi, cmd, bat).

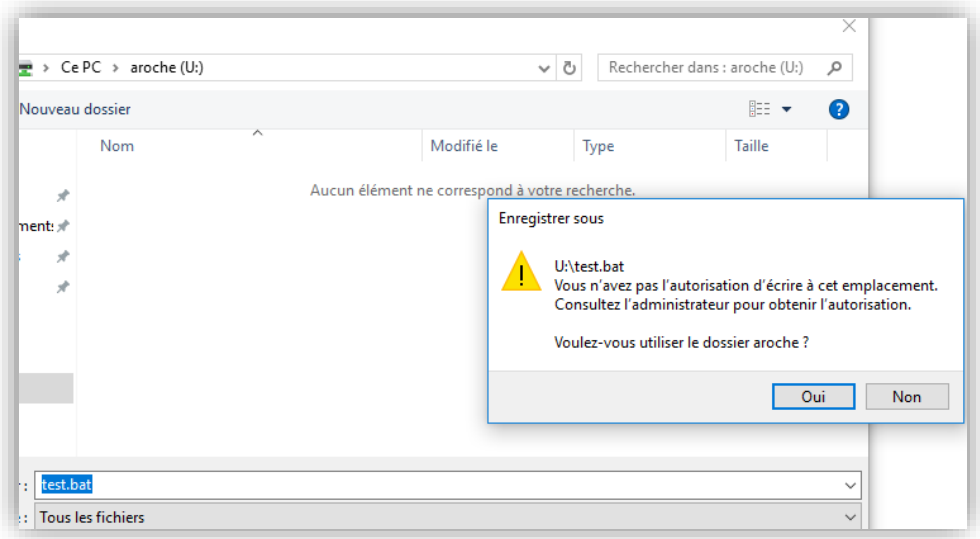
Mails : Il arrive couramment qu'un utilisateur n'aie plus de place de place dans sa boite mail : au lieu de nettoyer sa boite, il décide d'archiver ses fichiers .msg ou bien de créer une archive locale .pst directement ce qui a pour effet d'encombrer le serveur de fichiers.

Fichier audio et vidéos : ces données sont souvent assez lourdes. Une restriction s'appliquera pour éviter qu'un utilisateur ajoute des films ou des musiques personnelles dans son dossier.

De façon plus générale, nous pouvons envisager de bloquer toute extension de fichier exceptés des fichiers Excel ou Word pour maintenir un bon niveau de sécurité, sur l'ensemble du serveur de fichiers ou bien sur le répertoire d'un seul service.



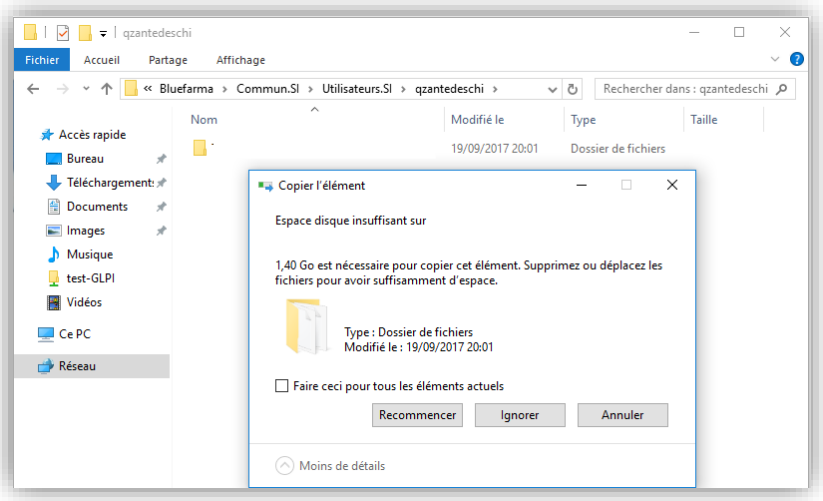
L'application d'un filtre sur des fichiers proscrits génère un fichier bat (script) à l'attention de l'utilisateur :

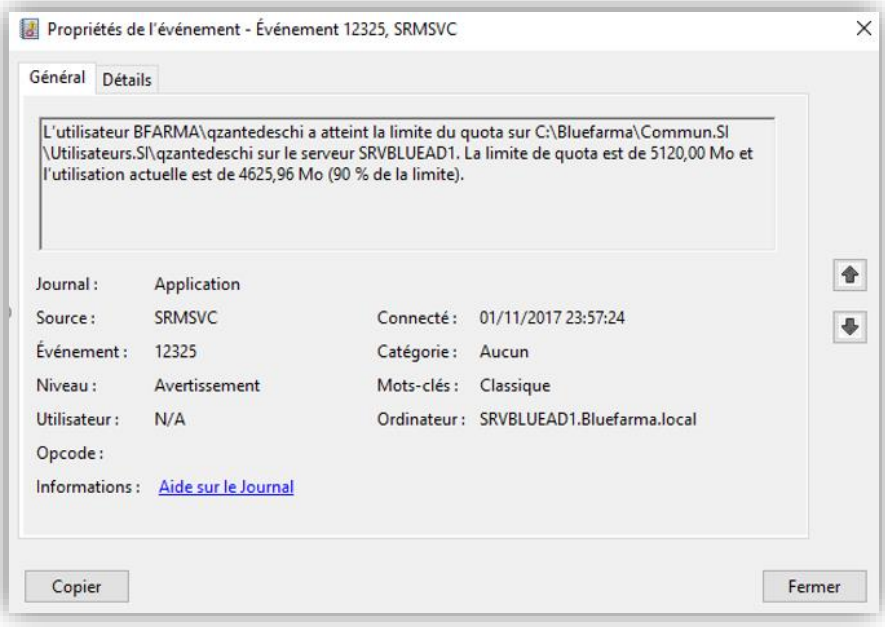


Application d'un quota d'utilisation de l'espace disque :

Conformément au cahier des charges un quota de 5go d'espace disque est attribué pour chaque utilisateur. Lorsqu'un nouveau dossier personnel sera créé, ce quota s'appliquera automatiquement sans manipulation supplémentaire côté SI. En cas de dépassement, l'utilisateur en sera avisé par mail, ainsi que le SI

Par exemple, l'utilisateur reçoit un message d'erreur l'informant qu'il est bloqué s'il tente de transférer plus de 5go dans son dossier personnel.





Des notifications mails et l'inscription dans le journal des évènements sont ajoutées pour informer le SI lorsqu'une limite de quota d'un dossier est atteinte (avec une notification pour l'utilisateur).

4.7.4. Stratégie de sécurité

L'**ANSSI** (« *Agence Nationale de la Sécurité des Systèmes d'Information* »), propose un guide relatif au respect de la vie privée et à la confidentialité des données sous Windows 10. En effet, cette dernière version de Windows a tendance à augmenter la quantité de données partagées avec Microsoft. Il est cependant possible de limiter ces partages de données via certaines GPO.

Plusieurs stratégies recommandées par l'ANSSI seront appliquées au niveau de la configuration des postes.

Voici la liste des stratégies mises en œuvre (leurs configurations sont présentes en annexe **9.2.2**) :

- Blocage de **fonctionnalités et processus Windows** :
  - Blocage de l'utilisation des comptes Microsoft (ceci revient à stocker des informations telles que l'historique de navigation ou bien des mots de passe Wi-Fi dans le cloud Microsoft).
  - Limiter l'envoi de données de télémétrie en configurant le paramètre ***Autoriser la télémétrie*** avec le niveau **1 – De base**. (NB : Il n'est pas possible de bloquer complètement l'envoi d'informations à Microsoft).
  - Désactivation de Onedrive afin d'éviter toute synchronisation de fichiers sur les serveurs de Microsoft.
  - Désactiver Cortana, « l'assistant personnel intelligent » de Microsoft, qui accède aux données personnelles de l'utilisateur. Désactiver la recherche Web et l'affichage des résultats Web dans la barre de recherche (permet de limiter la recherche aux données locales du poste).
  - Désactiver l'envoi de données par Windows Defender aux serveurs de Microsoft.
  - Stopper le service ***DiagTrack***, qui est utilisé pour la télémétrie.

- **Sécurisation des postes et des données** :
  - Verrouillage des sessions. Cette action s'effectue par GPO au bout de 5 minutes d'inactivité.
- **Stratégie de mots de passe**
  - Notre stratégie de mot de passe est basée sur les recommandations de l'ANSSI et de Microsoft. L'ANSSI préconise un mot de passe de **8 caractères minimum** (avec une majuscule et un chiffre) et son renouvellement tous les 90 jours. Il est également recommandé de ne pas laisser un tiers générer le mot de passe. Ainsi, nous mettrons un mot de passe par défaut lors de la création des nouveaux utilisateurs. Ce dernier sera forcé à créer un nouveau mot de passe à la première connexion. Une « ***stratégie de mot de passe affinée*** » s'appliquera à tout utilisateur du domaine depuis le ***Centre d'Administration***

Active Directory afin d'élaborer des stratégies de mot de passe différentes selon les services ou utilisateurs.

- Message d'avertissement du verrouillage du compte au bout de 5 mots de passe erronés : un administrateur pourra alors déverrouiller le compte de l'utilisateur, via les propriétés du compte sur l'AD.

- **Désactivation des périphériques externes :** Ceci limite la propagation de virus via des périphérique externe. Ce blocage s'applique en lecture/écriture le service Produit A, B, et le SAV.

- **Désactivation de l'heure** : Seuls la Direction et le SI peuvent agir sur l'heure.

- **Interdiction d'installer des programmes :** le SI a un contrôle total sur l'installation des logiciels afin que l'utilisateur ne modifie pas son environnement.

- **Configuration des horaires d'accès :** Mise en application du cahier des charges pour les horaires d'accès (ceci se fera par GPO) :
  - 20h et 7h. : Direction, SAV et SI.
  - 8h et 18h pour Mme **BEZIAT**, **ELLA**, **AYO** et **ACIEN** du service Produit A
  - Configuration de deux tâches planifiées : une pour prévenir l'utilisateur, l'autre pour déconnecter la session.

4.7.5. Configuration des droits d'impression

Suite à l'installation du serveur d'impression et de ses imprimantes (partie **4.7.5**), il convient à présent de configurer les droits d'accès aux différentes imprimantes. Le cahier des charges stipule des conditions assez précises que nous avons prises. Il s'agit des points suivants :

Convention de nommage :

- Une imprimante ***Print.All*** sur laquelle tous les services peuvent imprimer.
- Une imprimante ***Print <nom du Service>*** par service.

Attribution des imprimantes par service :

Des restrictions d'utilisation calquées sur des créneaux horaires seront mises en place pour chaque service. Les consignes du cahier des charges sont les suivantes :

- La direction est prioritaire sur toutes les impressions avec la possibilité d'imprimer 24/24.
- Sur l'imprimante réseau « ***Print.All*** », les services produit A et B ne peuvent imprimer qu'entre 8 h et 17 h.
- Le service informatique tenant le rôle du support doit avoir le contrôle total sur toutes les impressions.
- Mme Laporte et Mlle Ada (assistante des services SAV et Direction respectivement), peuvent imprimer chez le service informatique ainsi que chez le service produit A et B.

Service/ Imprimante	Service SI	Service SAV	Service ProduitA	Service ProduitB	Service Direction	Service Administratif	Mlle.ADA	Mme.LAPORTE
Print.SI	✓						✓	✓
Print.SAV	✓	✓						✓
Print.ProduitA	✓		✓				✓	✓
Print.ProduitB	✓			✓			✓	✓
Print.Direction	✓				✓		✓	
Print.Administratif	✓					✓		
Print.ALL	✓	✓	✓	✓	✓	✓	✓	✓

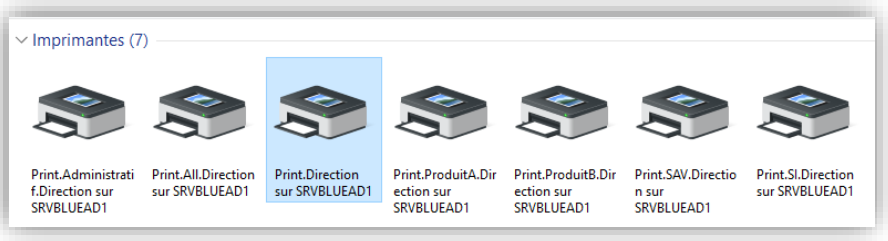
Configuration des permissions [annexe **9.2.4**]

Des imprimantes virtuelles ont été créées : elles nous serviront à appliquer plusieurs permissions en fonction des groupes utilisateurs : il sera ainsi possible d'appliquer des priorités d'accès aux impressions, notamment la Direction. En effet, la Direction est prioritaire sur l'ensemble des impressions, même si des impressions sont en cours dans un service : après la fin d'une impression en cours, les suivantes seront placées en file d'attente pour céder la priorité à celle de la Direction.

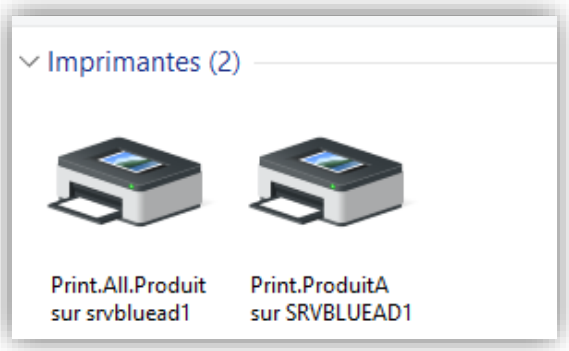
Déploiement des imprimantes par GPO

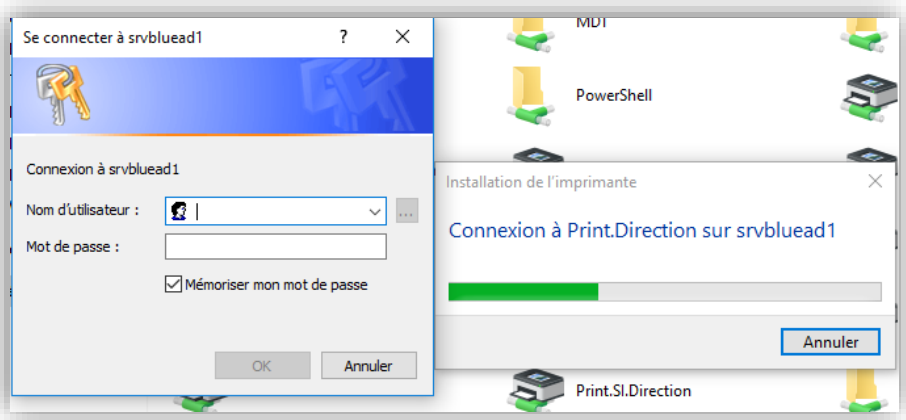
Nous souhaitons que les imprimantes soient attribuées directement à chaque utilisateur en fonction de leur groupe. Pour gagner du temps, nous avons configuré ce déploiement au moyen d'une GPO depuis le rôle ***Gestion de stratégie de groupe*** : c'est depuis cette interface que l'on créé une nouvelle GPO qui aura un nom de type « *Imprimante_<nom du service>.* L'**OU** d'un service est ensuite sélectionnée pour appliquer l'attribution de l'imprimante à l'ensemble des utilisateurs qu'elle contient. Pour finir, on sélectionne l'imprimante à partager puis on valide.

Exemple de ce que visualisera Mme Ada, l'assistante de Direction : On visualise un accès à toutes les imprimantes qui sont connectées automatiquement à son poste grâce à une priorité plus élevée.



Exemple pour Adrien Roy du service ProduitA : On constate que ses accès se restreignent uniquement aux imprimantes qui lui sont réservées. S'il essaye d'accéder à une autre imprimante partagée, il lui sera demandé des identifiants d'accès autorisés à se connecter à l'imprimante.





4.7.6. WSUS : serveur de mises à jour

Afin d'optimiser les performances réseaux de Bluefarma, nous allons mettre en place le service **WSUS** (« *Windows Server Update Services* »). Il s'agit d'une solution gratuite proposée par Microsoft afin de d'économiser de la bande passante sur un réseau d'entreprise. En effet, les postes se mettent à jour par défaut en passant par les serveurs de Microsoft. Ainsi, à la sortie d'une mise à jour, les 90 postes se mettront à télécharger en même temps la même mise à jour.

WSUS peut limiter l'impact des mises à jour sur la bande passante en les téléchargeant uniquement sur le serveur (ici SRV-AD1) avant de les redistribuer à l'ensemble des postes, via le réseau local. Ainsi, seul le serveur centralise les MAJ en désaturant la bande passante.

Cette solution est relativement simple à mettre en œuvre mais elle nécessite une configuration assez pointue afin de ne pas encombrer tout l'espace disque utilisé pour les mise à jour.

Configuration [annexe **9.2.3**]

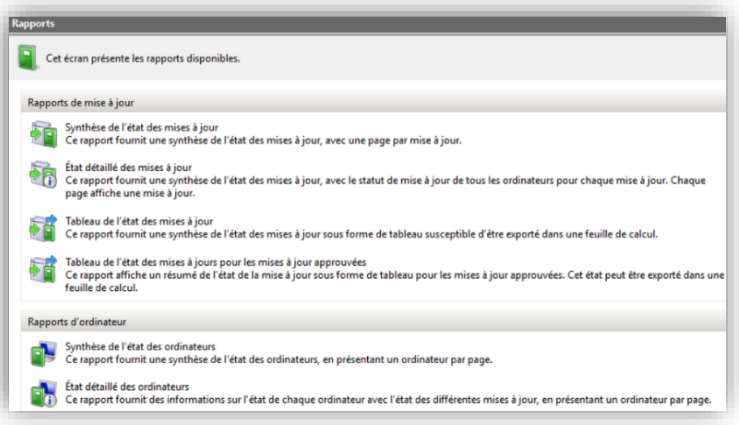
Approbation des mises à jour :

Deux groupes sont créés et comportent chacun 10 postes ayant la même configuration :

- **Alpha** : Il réceptionne les mises à jour pour vérifier les soucis de compatibilité durant 3 jours.
- **Beta** : Son délai de 6 jours permet de confirmer que les mises à jour se comportent correctement sur les postes.

Planification des mises à jour via GPO : Via une GPO, la planification s'effectue tous les jours à 12h pendant l'absence de l'utilisateur : dans les paramètres, on autorise Windows Update à sortir le PC de veille pour installer les mises à jour.

Purge des mises à jour obsolètes : La publication des mises à jour cumulatives fait que certaines deviennent inutiles. Un assistant permet de purger le disque pour prévenir tout risque de saturation de l'espace de stockage.

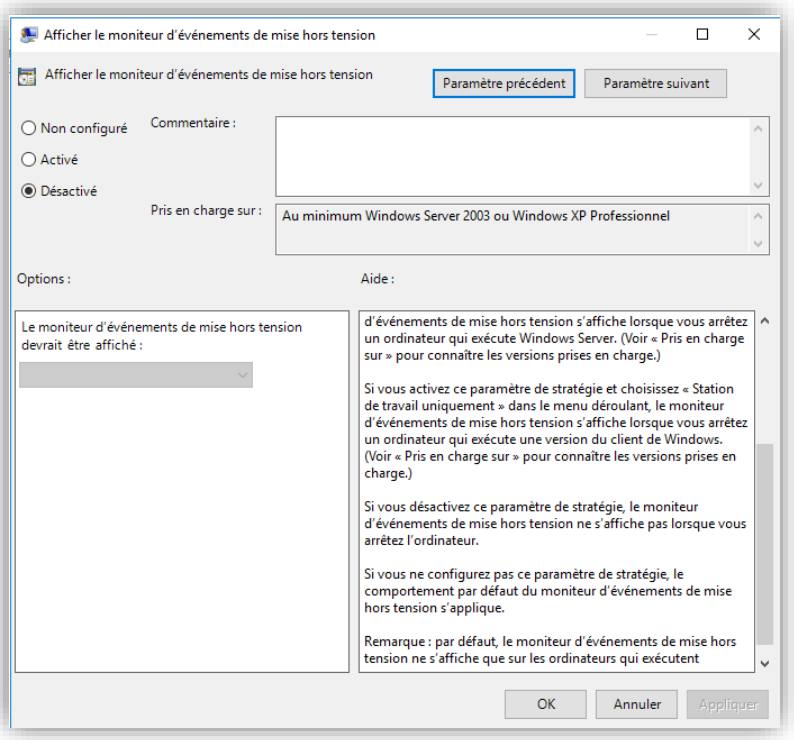


Affichage des rapports :

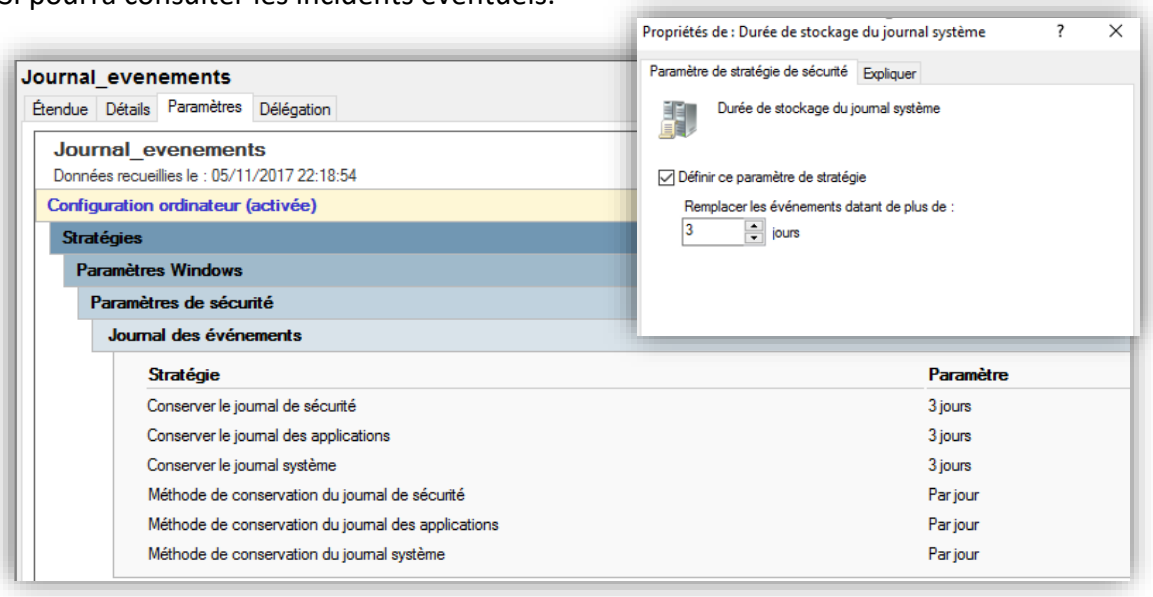
Il existe un outil permettant d'afficher des rapports détaillés concernant les mises à jour, l'état des ordinateurs, etc. Ceci contribue à gérer plus efficacement le parc informatique en vérifiant si l'intégralité des postes est à jour.

4.7.7. Configuration des journaux

Le cahier des charges stipule le besoin de désactiver le moniteur d'évènements sur les postes :

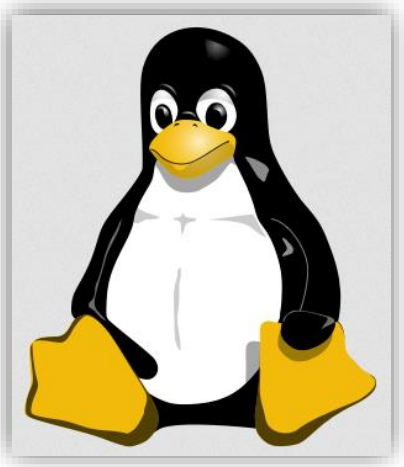


Nous configurons également 3 journaux à 3 jours sur l'ensemble des postes. De cette façon, le SI pourra consulter les incidents éventuels.



5. SERVEURS LINUX

Les systèmes d'exploitation Linux sont très couramment utilisés dans le monde des serveurs informatiques. Effectivement, ils sont réputés en matière de fiabilité, de sécurité et de performance et sont capables d'assurer divers services (HTTP, DHCP, FTP, DNS, etc.) ou d'héberger des applications libres pour des besoins divers (messagerie, téléphonie, base de données, etc.).



Le cahier des charges stipule le besoin de mettre en place une infrastructure serveur Linux. Avant de détailler les différents services, il convient dans un premier temps de définir le choix de notre distribution.

5.1. Choix de la distribution

Il existe une grande quantité de distributions basées sur le noyau Linux. Cette diversité s'explique par le fait qu'elles répondent à des besoins divers : certaines distributions sont orientées pour l'administration de serveurs, d'autres pour la bureautique. Il y a plusieurs manières de répondre à ces besoins si bien que souvent, le choix de préférer une distribution repose sur des raisons assez subjectives.

Toutefois, le choix doit s'opérer autour des distributions réputées pour l'administration des serveurs informatiques. On citera **Red Hat Enterprise Linux** (RHEL) et **Suse** Linux Enterprise Server (SLES) qui sont destinés pour les entreprises. Ces distributions sont stables et puissantes mais leur support est payant.

Debian est une distribution communautaire open source et donc complètement gratuite. Ses cycles de mises à jour, certes lents, garantissent une très grande fiabilité : dans cette optique, la démarche consiste à privilégier la stabilité du système. Cette distribution est ainsi réputée pour sa qualité et son absence de bugs. Elle est en outre dotée d'une communauté très active qui facilite son support.

CentOS est une distribution totalement gratuite fondée sur Red Hat qui est une solution commerciale. CentOS jouie d'une qualité supérieure en se dotant des grandes avancées techniques de Red Hat. Ainsi, elle affiche une très grande stabilité. D'autre part, son support de 7 ans demeure le plus long parmi toutes les distributions et la documentation technique librement accessible sur le site de Red Hat permet de se familiariser avec son fonctionnement. En revanche, CentOS possède moins d'applications compatibles qu'une distribution Debian. Cependant, ceci n'aura pas d'incidence sur l'utilisation qui sera faite de notre serveur.

La stabilité, la qualité et la gratuité d'un produit issu d'une solution commerciale robuste et puissante sont autant d'arguments qui ont orienté notre choix pour CentOS.

5.2. Fonctions des machines Linux

Conformément au cahier des charges, il convient de mettre en place plusieurs serveurs Linux qui hébergeront différents services qui ont été synthétisés dans ce tableau avec leurs logiciels/utilitaires associés :

Services et fonctions	Logiciels/fonctionnalités
Partage de ressources Windows	Samba (version 4)
Serveur FTP	vsFTPd
Service HTTP : hébergement du site intranet	phpmyadmin ; httpd (apache), GLPI
Hébergement de la base de données	mariadb
Serveur/client NFS (pour sauvegardes)	nfs-utils, rsync, mysqldump

Nous allons maintenant présenter chacun des services, leur utilité et la façon dont ils seront mis en œuvre. Un renvoi en annexe sera mentionné au besoin pour consulter les procédures d'installation et de paramétrage des services et des logiciels.

Les services se partageront entre les machines SRV-NUX1 et SRV-NUX2 (voir schéma de l'infra globale, **page 73**).

5.3. Le serveur FTP

FTP (« *File Transfert Protocol* », protocole de transfert de fichier) est un protocole de communication qui fournit un accès à des données informatiques sur le réseau via le protocole TCP/IP. Ce transfert de fichiers est basé sur le modèle serveur-client.

vsFTPd sera installé pour remplir cette fonction. Conformément au cahier des charges, il est capable de mettre en place une connexion anonyme et sécurisée au travers d'un utilisateur unique dans une zone qui ne communiquera pas avec le reste du réseau. Ce dernier ne sera autorisé à accéder qu'au seul dossier partagé comportant la documentation de l'entreprise.

Notre serveur FTP sera isolé du réseau de l'entreprise : seule une connexion FTP entrante est autorisée pour administrer le serveur (rajout de documentation par exemple). Ainsi, un visiteur externe à la société pourra consulter de la documentation sur un poste installé à l'accueil. Aucune donnée critique de l'entreprise ne sera stockée sur ce serveur.

Configuration [annexe 9.3.1]

5.4. Serveur de fichiers Samba

Un serveur de fichiers partagés doit être mis en place pour le partage de ressources entre les utilisateurs Windows et ceux du service SAV.

Le monde linux ne parle pas nativement avec celui de Microsoft. Toutefois, ceci est possible avec le logiciel libre **Samba** qui assure le partage de fichiers. Initialement développé pour les environnements Windows, le protocole **SMB/CIFS** a été plus tard implémenté sous Unix. Depuis, Samba favorise l'interopérabilité entre des machines exploitant des environnements différents (Linux, Windows, MAC OS, etc.). La mise en œuvre d'un partage de ressources depuis un serveur Linux présente plusieurs intérêts :

- Excellente cohabitation entre les serveurs Linux et Windows.
- Stabilité et fiabilité de Linux.
- Gestion avancée des droits d'accès et des comptes utilisateurs Windows

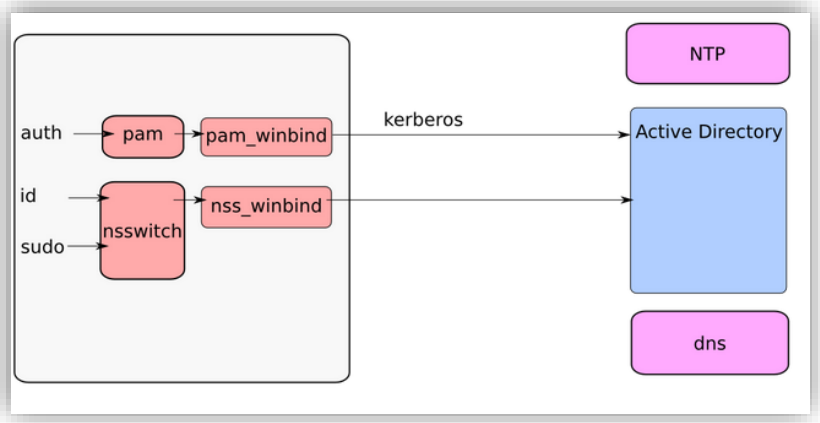
Nous mettrons en place deux types de partage entre Linux et Windows :

- Un ***dossier personnel*** pour utilisateur.
- Un ***répertoire commun*** depuis lequel le SAV qui est sous linux pourra communiquer avec les utilisateurs sous Windows.

Nous tirerons parti des comptes utilisateurs Windows pour gérer les droits grâce à un composant de Samba, ***Winbind*** qui est capable d'intégrer une machine linux dans un environnement Active Directory.

5.4.1. Intégration au domaine Active Directory

L'intégration de Linux sous Windows va se faire au moyen de ***Winbind*** (comprendre, « *Win(dows) Bind* », « liaison de Windows ») qui va fonctionner avec le serveur d'authentification **Kerberos** : il s'agit d'un protocole d'identification réseau reposant sur un système de clés à chiffrement symétrique qui va permettre de ne pas laisser circuler les mots de passe des utilisateurs en clair sur le réseau.



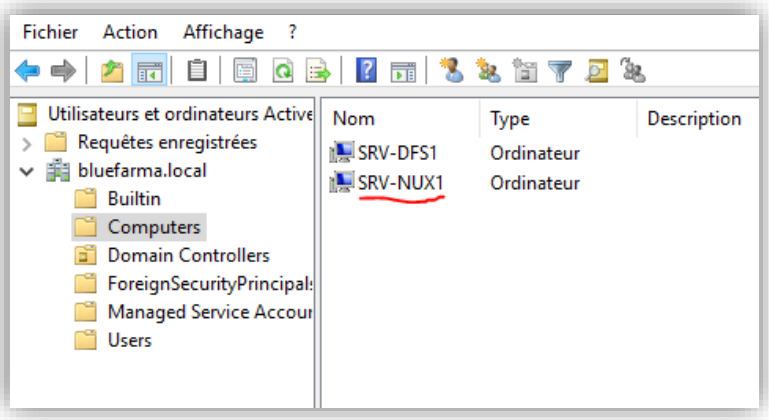
Winbind s'appuie sur les mécanismes suivants pour faire apparaître les utilisateurs du domaine Windows comme utilisateurs Unix :

- **PAM** (« *Pluggable Authentification Modules* »). Offre un mécanisme d'authentification.
- **NSS** (« *Names Service Switch* »). Apporte un mécanisme de service de noms.

Ces deux mécanismes amènent également les applications locales à utiliser les accréditations Kerberos fournies par Active Directory.

Pour résumer, Winbind aura recours à PAM pour authentifier les utilisateurs via l'annuaire **LDAP** en utilisant la configuration de PAM tandis que la résolution des ID, noms d'utilisateurs ou groupes AD au moyen de la recherche NSS.

Configuration [annexe **9.3.2**]



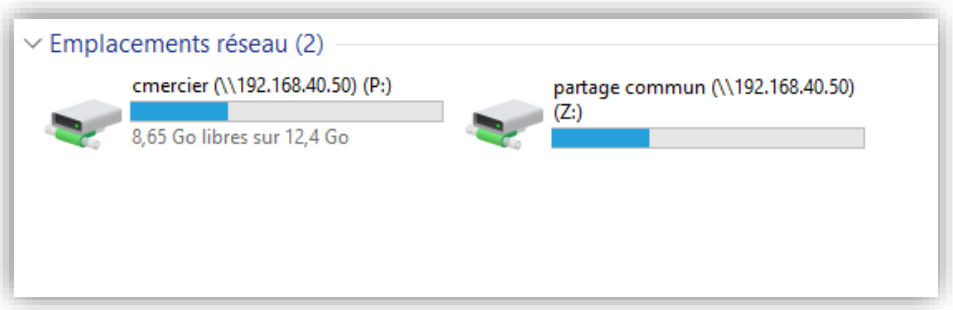
5.4.2. Création d'un répertoire commun et des dossiers personnels

Les deux utilisateurs qui travaillent sous une distribution linux (Fedora 26) s'échangeront des données via le répertoire « partage_commun » avec les utilisateurs sous Windows. Le dossier a été créé sur SRV-NUX1 dans **/home/partage_commun** et nous lui avons attribué tous les droits afin que tous les utilisateurs du domaine puissent y accéder en lecture/écriture sans la moindre contrainte. Depuis Windows, le répertoire partage_commun sera accessible à partir du chemin \\SRV-NUX1\partage_commun.

Quant aux dossiers personnels de chaque utilisateur, ces derniers seront montés côté Linux puis nous mapperons les utilisateurs Windows sur leurs dossiers situés dans **/home/BLUEFARMA**. L'accès pour les utilisateurs Windows est tout à fait transparent puisque ces derniers ne réaliseront mêmes pas que leurs dossiers sont hébergés sur une machine Linux.

Dès que la jonction de la machine Linux avec le domaine AD est faite, nous configurerons côté Linux le fichier **/etc/samba/smb.conf** en mentionnant le chemin du dossier partage_commun et le répertoire BLUEFARMA qui contiendra les dossiers personnels des utilisateurs.

Du côté du poste de l'utilisateur Windows, ces deux lecteurs apparaîtront sous cette forme :



Configuration [annexe **9.3.2**

5.5. Partage NFS et sauvegardes automatiques

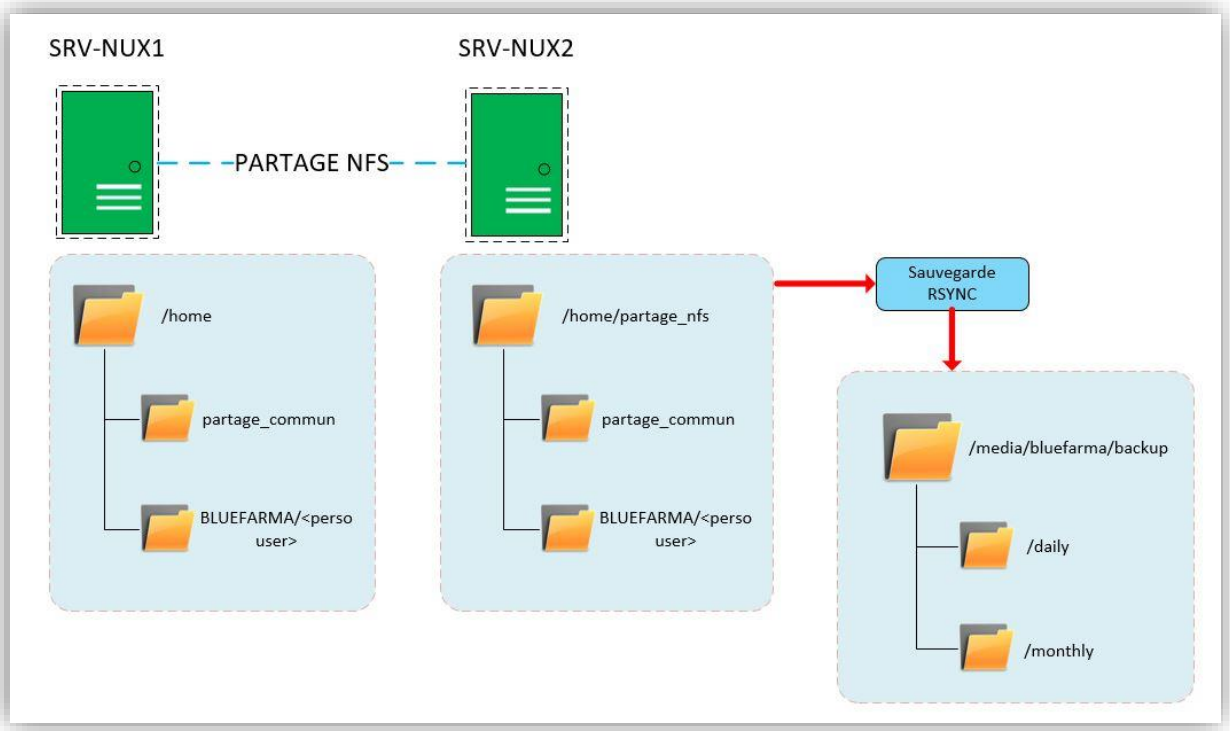
5.5.1. Partage NFS

L'infrastructure système Linux est composée de deux machines selon la configuration suivante :

- SRV-NUX1 : serveurs de fichiers Samba ; serveur HTTP.
- SRV-NUX2 : Espace de sauvegarde.

Le protocole NFS (« *Network File System* » permet de monter plusieurs dossiers partagés en réseau afin d'échanger des fichiers sur le modèle serveur/client.

NFS nous sera très utile pour rendre visibles les ressources entre les deux machines linux : un script répliquera les données contenant dans le dossier /home/partage_nfs comme indiqué ci-dessous (voir partie suivante **5.5.2**).



Configuration [annexe **9.3.3**]

Un partage NFS sera mis en œuvre entre SRV-NUX1 qui fera office de serveur NFS via l'installation du paquet **nfs-utils** et SRV-NUX2 qui sera le client NFS.

Dans la configuration du fichier **exports** mettant en œuvre l' « exportation » des données partagées, le chemin indiqué pointe sur le dossier des utilisateurs (/home/BLUEFARMA) suivi de l'adresse IP du client NFS SRV-NUX2 (192.168.40.60).

Côté client, un dossier de partage est créé (/home/partage_nfs). Le montage est ensuite rendu automatique en modifiant le fichier **/etc/fstab** dans lequel on renseigne les options de montage entre les deux dossiers.

Le montage NFS devient effectif et automatique après l'exécution de la commande **mount -a** qui va exporter le chemin indiqué dans **/etc/fstab**.

Par cette configuration, les données du répertoire sont automatiquement répliquées entre les deux serveurs.

5.5.2. Configuration du script de sauvegarde automatique

Nous voulons que la sauvegarde s'effectue automatiquement au niveau de la machine cliente NFS (SRV-NUX2) à partir de l'utilitaire **rsync**.

Cette sauvegarde s'opèrera entre le dossier de partage **/home/partage_NFS** et le dossier **/media/backup_bluefarma**. Une simple commande de ce type permet d'effectuer une sauvegarde simple entre ces deux dossiers :

```
rsync -r /home/partage_nfs/ /media/bluefarma_backup
```

Cependant, nous souhaitons rendre automatique la sauvegarde en observant les préconisations de la CNIL qui conseille une sauvegarde incrémentielle quotidienne et complète tous les mois (sur la stratégie de sauvegarde, voir partie **6.3.3**).

Leur mise en œuvre se déroulera en utilisant des **scripts bash** et le planificateur de tâches **cron**. Chaque script se trouvera dans le répertoire dans son répertoire de sauvegarde respectif :

- Sauvegarde quotidienne : `/media/bluefarma_backup/daily`
- Sauvegarde mensuelle : `/media/bluefarma_backup/monthly`

Sauvegardes incrémentielles journalières

- Création d'un dossier/jours de la semaine : ces dossiers de sauvegardes sont générés au moyen d'un petit script que l'on nomme ***script_jours.sh*** présent dans le répertoire **/media/bluefarma_backup/daily** :

```
#!/bin/bash
for x in lundi mardi mercredi jeudi vendredi
do
mkdir $x
done
```

Après avoir lancé le script, on constate que nos dossiers de sauvegarde ont bien été générés (prévoir de bien lancer le script depuis le dossier qui devra accueillir ces répertoires !).

Nous créons ensuite un autre fichier bash nommé **script_backupdaily.sh** dans le répertoire

```
JOUR=$(date +%A)

# date et heure de création du dossier contenant la sauvegarde
DATE=$(date +%y%m%d-%H:%M)

# dossier source NFS depuis lequel les données seront sauvegardées
source=/home/partage_nfs

# dossier de destination des sauvegardes journalières
CHEMIN=/media/bluefarma_backup/daily

#commande rsync
rsync -av --progress --delete --stats $source $CHEMIN/$JOUR/bluefarma_backup_$DATE

find $CHEMIN -maxdepth 5 -name "*bluefarma_backup*" -mtime +7 -exec rm -rf {} \;
```

root (nous le rendons ensuite exécutable en faisant chmod +x script_backupdaily.sh).

Explication du script :

- JOUR=$(date +$A) : cette variable comporte le format de la date en français. Les sauvegardes seront automatiquement redirigées dans le répertoire portant le nom d'un jour de la semaine.
- DATE=$(date +%y%m%d-%H:%M) : Cette variable permettra de nommé le dossier de la sauvegarde selon le format suivant : 171130-13h30 (30 novembre 2017 à 13h30).
- rsync : Cette commande appel l'utilitaire rsync faisant appel pour effectuer la sauvegarde. Il est accompagné des options suivantes :
    - -a : cette option équivaut à l'ensemble des options -rlptgoD. Elle va permettre entre autres de préserver les droits des propriétaires des données tout en mettant en œuvre une sauvegarde incrémentielle.
    - -v : affiche toutes les étapes pendant la sauvegarde.
    - --progress : affiche l'avancement pendant le transfert.
    - --delete : les fichiers qui n'existe plus dans le fichier source seront effacés avant le transfert.
    - --stats : génération d'un rapport quand la sauvegarde est terminée.
- find : cette commande permet de faire du tri dans les données selon les options suivantes :
- -maxdepth 5 : définie jusqu'à quel niveau de l'arborescence il faut remonter pour rechercher le nom.
- -name : option permettant d'indiquer le mot que l'on recherche, ici, bluefarma_backup.

- -mtime +7 : « *modification time* », permet d'indiquer les données qui ont été créées il y a 7 jours.
- -exec rm -rf : exécution de la commande qui va supprimer un dossier de façon récursive (-r).

En somme, ce script ira copier le contenu du dossier partagé par NFS (**/home/partage_NFS**) dans le dossier de sauvegarde (**/media/bluefarma/daily/$jour**), en redirigeant chaque sauvegarde quotidienne dans un dossier qui comportera le nom d'un jour travaillé de la semaine. À chaque lancement automatique, le script vérifie les données vieilles de plus de 7 jours pour les supprimer et les remplacer par les nouvelles.

Nous automatisons cette tâche en éditant le fichier **/etc/crontab** :

```
0 20 * * 1-5 root /root/script_backupdaily.sh
```

Cette ligne indique qu'une sauvegarde aura lieu tous les jours de la semaine (1-5) à 20 heures (0 20).

Sauvegardes complètes mensuelles

Le même principe de sauvegarde sera appliqué pour les mois de l'année :

- Créations des dossier du mois avec **script_monthly.sh** dans le répertoire **/home/bluefarma_backup/monthly** avec la ligne for x in {01..12} pour les 12 mois de l'année.

```
#!/bin/bash
for x in {01..12}
do
mkdir $x
done
```

```
[root@SRV-NUX2 monthly]# ls
01  02  03  04  05  06  07  08  09  10  11  12  script_monthly.sh
```

- Création d'un script permettant de sauvegarder les données partagées dans le répertoire mensuel.

```
#!/bin/bash

# mois de l'année
MOIS=$(date +%m)

# date et heure de création du dossier contenant la sauvegarde
DATE=$(date +%y%m%d-%H:%M)

# dossier source NFS depuis lequel les données seront sauvegardées
source=/home/partage_nfs

# dossier de destination des sauvegardes mensuelles
CHEMIN=/media/bluefarma_backup/monthly

#commande rsync
rsync -av --progress --delete --stats $source $CHEMIN/$MOIS/bluefarma_backup_$DATE
```

Explication du script :

Le script change peu par rapport au précédent, à l'exception de la directive &m pour les mois de l'année ou de la modification du chemin qui pointe sur le répertoire **/media/bluefarma_backup/monthly**.

- Nous mettons ensuite à jour le planificateur en éditant le fichier **/etc/crontab**.

```
0 * * 1-12 * root /root/script_backupmonthly.sh
```

En résumé, le script lancera une sauvegarde mensuelle complète du dossier partagé par NFS tous les mois de l'année. Chaque sauvegarde sera poussée dans un dossier cible comportant le numéro de chaque mois.

5.5.3. Sauvegarde de la base de données avec mysqldump

mysqldump fait partie de la série d'utilitaires livrés avec MySQL. Il permet de sauvegarder une base de données dans un fichier .sql : ce fichier de backup comporte un ensemble de commandes SQL et d'instructions utiles pour la restauration des données telles qu'elles étaient durant la sauvegarde. Les tables sont verrouillées pendant le processus de création du fichier de backup, rendant toute écriture impossible.

Configuration de la sauvegarde : Il faudra veiller à installer mariadb sur les deux serveurs. La configuration de la sauvegarde s'effectue depuis SRV-NUX2 qui viendra placer dans le dossier **/media/backupdb** les sauvegardes qu'il aura récupérées dans les bases de SRV-NUX1.

Les sauvegardes se feront tous les jours à 20 heures et seront conservées durant une semaine. Une seconde sauvegarde complète s'effectuera tous les mois.

Côté serveur (SRV-NUX1)

- Créer sur SRV-NUX1 l'utilisateur « backup » à qui on attribue tous les privilèges. Ce dernier se chargera de faire que les sauvegardes.

- Se rendre dans le fichier de configuration de mariadb **/etc/my.cnf** puis ajouter la ligne ***bind-adress = <ip du serveur>*** pour autoriser mariadb à écouter sur l'IP de SRV-NUX1.
- Relancer le service mariadb (`systemctl restart mariadb.service`).

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
symbolic-links=0
bind-address = 192.168.40.50
```

- Ouvrir le port 3306 avec le firewall :

```
firewall-cmd --zone=public --add-port=3306/tcp --permanent
```

Côté client (SRV-NUX2)

- La commande suivante va permettre de sauvegarder la base de données à distance grâce à mysqldump.

```
/usr/bin/mysqldump -h 192.168.40.50 -u backup -padmin bluefarmadb > /media/backupdb/bluefarmadb.sql
```

Nous souhaitons automatiser la sauvegarde via un script dont le lancement sera planifié par cron. Cette sauvegarde s'effectuera tous les jours à 20 heures et elles seront conservées pour une durée d'une semaine.

Explication des commandes du script :

```
#!/bin/bash

#date et heure de la sauvegarde
DATE=$(date +%y%m%d-%H:%M)

#chemin du dossier qui contiendra la sauvegarde
CHEMIN=/media/backupdb/

#commande qui va dumper la base depuis le serveur SQL distant
mysqldump -h 192.168.40.50 -u backup -padmin bluefarmadb > $CHEMIN/bluefarmadb_$DATE.sql

find $CHEMIN -maxdepth 3 -name "*bluefarmadb*" -ctime +7 -exec rm -f {} \;
```

- date +%y%m%d-%H :%M : ces valeurs permettent d'afficher la date et l'heure de sauvegarde du fichier sous la forme « 171104-17:30 » (4 novembre 2017 - 17h30)
- Dans la commande mysqldump :
  - **-h** rajoute l'IP de l'hôte distant ciblé (SRV-NUX1) ;
  - **-u** introduit l'utilisateur backup que l'on a créé précédemment ;
  - **-p** permet de renseigner le mot de passe.

En somme, la commande mysqldump cible la base SQL bluefarmadb sur le serveur distant puis renvoie la sauvegarde dans le dossier /media/backupdb/ sous la forme d'un fichier SQL portant le nom de la base SQL + DATE.

- La commande find liste les fichiers selon les options que l'on a défini juste après :
  - maxdepth 3 permet de remonter dans l'arborescence sur un maximum de trois niveaux ;
  - -name "*bluefarmadb*" affiche les fichiers contenant « bluefarmadb » ;
  - -ctime +7 présente les fichiers dont la création excède une semaine ;
  - -exec rm -f est une commande qui effectue la suppression du fichier.

Nous planifions l'exécution quotidienne de ce script en éditant le fichier /etc/crontab :

Le cron exécutera le script **/root/script_backupdb.sh** tous les jours à 20 heures (20) durant les jours de travail (1-5).

5.6. Le service HTTP et ses composants

Le service HTTP sera installé au moyen du logiciel Apache pour visualiser les services intranet de notre société qui se composeront d'une base de données SQL (Mariadb) et du logiciel de gestion de parc informatique GLPI. phpMyAdmin sera installé en complément pour nous permettre de visualiser par l'interface web la base de données.

Présentation des logiciels installés :

Apache (*Apache HTTP Server*). Ce logiciel opensource est un serveur HTTP qui partage des pages web stockées localement et qui sont rendues accessible à des clients. Grâce à ce serveur, les pages web sont capables de comprendre faites par le navigateur.

PhpMyAdmin. Cette interface de gestion est codée en PHP afin d'administrer à distance une base de données MySQL au moyen d'un navigateur. Elle procure un accès sur une base de données, ses tables, les utilisateurs et leurs permissions ou permet encore d'importer ou d'exporter des données sous plusieurs formats (csv, pdf, txt, etc.)

Mariadb. Il s'agit d'un système de gestion de base de données. Mariadb est aussi un ***fork*** de MySQL créé par une communauté suite au rachat de MySQL par Sun Microsystems en 2009. Il n'utilise pas les comptes utilisateurs de Linux. En effet, il gère ses propres logins et mots de passe. Lors de l'installation, un compte root est créé par défaut mais il est préférable de paramétrer dès le début un nouvel utilisateur.

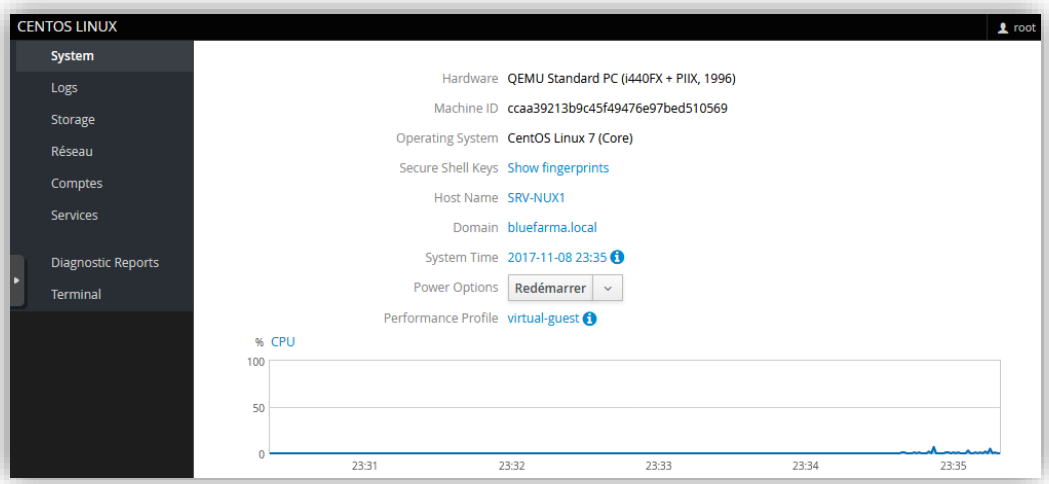
GLPI (« *Gestionnaire Libre de Parc Informatique* »). Ce logiciel libre se concentre sur deux aspects : la gestion de services informatiques et la gestion de services d'assistances (ticketing). En somme, il combine l'ensemble des outils nécessaire à la gestion d'un parc informatique. GLPI s'appuie entre autres sur une base SQL pour construire son inventaire de toutes les ressources techniques et de gestion.

Configuration [annexe **9.3.4**, **9.3.5**]

5.7. Logiciel de monitoring et de management

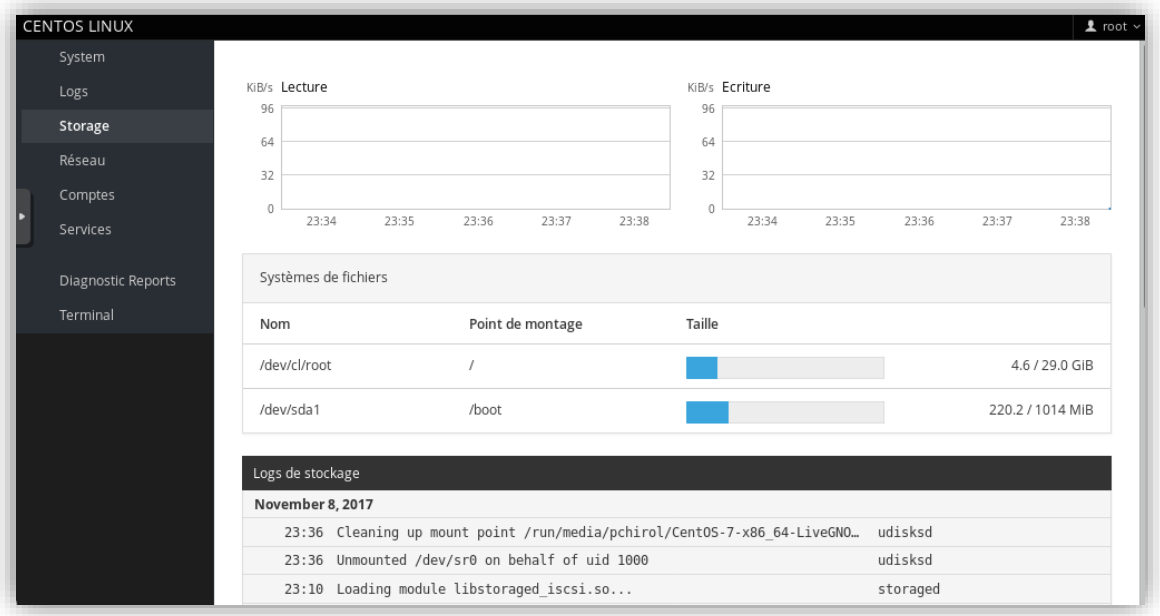
Cockpit : Il s'agit d'un logiciel libre de monitoring qui a été développé sous Fedora. C'est un logiciel assez épuré qui concentre les principaux outils permettant d'administrer une machine linux à distance.

Son **tableau de bord** se présente ainsi :



Depuis la barre de gauche, l'onglet des **logs** affiche tous les messages d'erreurs remontés par la machine Linux. Cette fonction est très pratique pour avoir un premier regard sur les erreurs qui affectent le système.

L'onglet Storage apporte des informations sur l'espace disponible des disques et génère des logs en rapport avec le stockage.

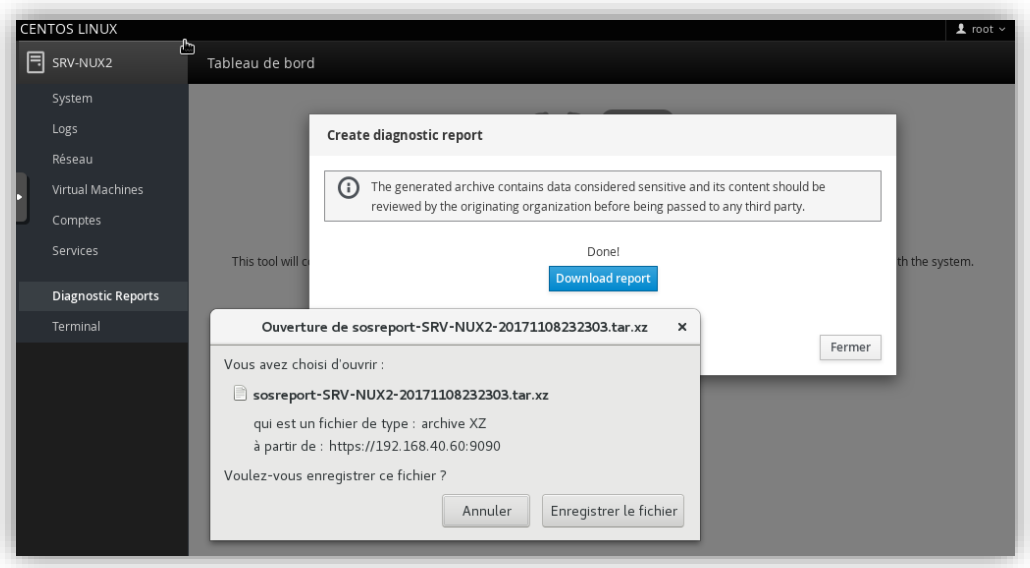


L'onglet des **Services** affiche en temps réel les services (**programmes**) en précisant s'ils sont en actifs, inactifs, etc.

L'onglet **Réseau** affiche l'activité du trafic mais permet également d'ajouter des paramètres réseaux (configuration d'un pont, d'un vlan, d'une interface réseau, etc.). Les journaux d'évènements de **NetworkManager** sont également listés.

L'onglet **Terminal** délivre directement un accès au CLI de la machine. Ainsi, on peut administrer une VM linux depuis un environnement Windows autorisé.

Une dernière fonctionnalités intéressante se situe au niveau de l'onglet **Diagnostic Reports** qui propose de générer puis de télécharger un rapport sur notre système suite à un diagnostic lancé manuellement.



6. PLAN DE CONTINUITÉ D'ACTIVITÉS

6.1. Définition d'un PCA

Le **PCA**, (« *Plan de Continuité d'Activités* ») se formalise sous l'aspect d'un document qui va décrire l'ensemble des moyens techniques, matériels, humains et financiers qui ont été mis en place afin d'assurer une disponibilité continue des applications et des données d'une entreprise, dans le cadre, entre autres, d'une infrastructure informatique. On parle alors de **haute disponibilité**. Le PCA se distingue du PRA qui, à défaut de pallier une panne, s'attardera sur les moyens à déployer pour garantir un redémarrage rapide des activités.

Le PCA repose sur :

- L'analyse du risque : elle identifie les menaces internes ou externes à l'entreprise, la probabilité qu'elles se manifestent voire le niveau d'acceptation que l'on peut observer face à elles.
- L'analyse de l'impact : elle se concentre sur le niveau de tolérance d'un incident avant qu'il devienne bloquant et dangereux pour la survie de l'entreprise. Le résultat principal de cette analyse est une durée maximale acceptable après une interruption de service.

Le temps de rétablissement peut être déduit en fonction des moyens matériels déployés pour le retour du service. Cependant, la définition d'un PCA ne repose pas tant sur un matériel redondé garantissant de la haute disponibilité que sur une action collective qui doit impliquer les techniciens, les responsables de service ou les utilisateurs finaux.

La stratégie de sécurisation d'un PCA se concentre sur deux types de mesures :

- Méthodes préventives : réplication de services, redondance, sécurisation physique sauvegardes régulières, etc.
- Méthodes curatives : remplacement de matériel défectueux, redémarrage des applications, restauration des sauvegardes.

L'intégrité, la sauvegarde et la pérennité des données sont les dénominateurs communs d'une série de mesures à mettre en œuvre pour anticiper les pannes matérielles ou logicielles.

Il convient maintenant de faire une étude des risques afin d'avancer les solutions que nous mettrons en œuvre pour limiter leur impact.

6.2. Analyse du risque et de son impact

Dans notre cas de figure, la criticité d'une panne est considérable car notre site abrite le siège social de la société Bluefarma. De fait, en tant que maison mère, une perte d'activité aurait des conséquences financières désastreuses.

D'un point de vue technique, les risques de panne reposent sur les points suivants :

Risques	Conséquences	Solutions
Sinistre	Incendie/inondation	Protection physique des serveurs
Panne matérielle	Perte de productivité Perte de données Pertes financières	Redondance des services Sauvegardes régulières
Virus	Perte de productivité Perte de données Pas de confidentialité Pertes financières	Antivirus

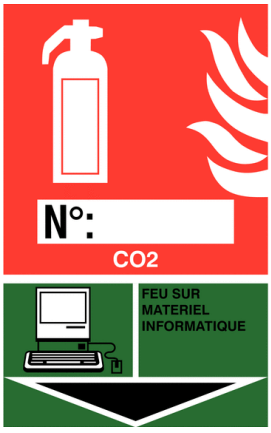
Les risques de sinistres et les pannes matérielles sont les plus impactantes par leur ampleur. Notre site étant le siège social de l'enseigne Bluefarma, nous ne pouvons pas nous permettre une perte d'activité de plus d'une demi-journée.

Nous allons nous attarder dans les prochaines parties sur les solutions proposées dans le tableau que nous mettrons en place.

6.3. Solutions proposées

6.3.1. Sécurisation des locaux et du matériel

Dans le cadre du plan de continuité d'activité, les locaux C et T qui hébergent nos serveurs et le reste des équipements informatiques seront sécurisés pour pallier les risques suivants :



Incendie : Des détecteurs de fumées seront présents dans les locaux afin de donner l'alerte en cas d'incendie.

Les incendies qui affectent le matériel électrique ou électronique (informatique, etc.) sont des feux de classe B. Les extincteurs à **CO2** sont adaptés à cette catégorie et seront installés dans chacun des locaux hébergeant du matériel informatique, et notamment nos serveurs. Il est conseillé d'inspecter les extincteurs tous les 3 mois pour vérifier leur conformité et il est obligatoire de les changer tous les ans.

Inondation : Pour pallier les risques d'inondation (site en zone inondable, canalisation rompue, etc.), les serveurs et l'ensemble du matériel informatique seront "rackés" en hauteur au niveau des baies informatiques.

Surchauffe : Les équipements informatiques génèrent d'importantes quantités de chaleur. Celle-ci augmente dans un espace réduit. Nous installerons des climatisations qui maintiendront de façon constante une température ambiante comprise entre 24 et 27°.

Surtension : Des onduleurs de marque Eaton protègeront nos équipements informatiques des surtensions.

Tous les équipements mentionnés sont compris dans le devis.

6.3.2. Tolérance aux pannes et haute disponibilité

La notion de haute disponibilité est indissociable du PRA puisqu'elle fait appel à l'ensemble des moyens matériels et techniques déployés pour assurer la continuité d'activité. Il s'agit notamment de la redondance du matériel afin que l'un prenne le relai de l'autre en cas de défaillance. Cette redondance assure :

- La cohérence des données entre deux serveurs.
- L'accès par l'utilisateur final aux données et aux applications, même en cas de panne.

Ces points ont été longuement abordés au cours de notre présentation, nous nous contenterons de les énumérer :

- **Redondance matérielle** :
  - Interconnexion des deux serveurs de l'entreprise.
  - Redondance de disque : RAID 1 et RAID 5 selon le type de service en activité ou de données.
  - Redondance de cartes réseau : présence de deux cartes réseau.
  - Présence d'une double alimentation sur chaque serveur
- **Redondance logicielle** :
  - Réplication AD/DNS.
  - Réplication DHCP (failover).
  - Réplication DFS du serveur de fichiers Windows.

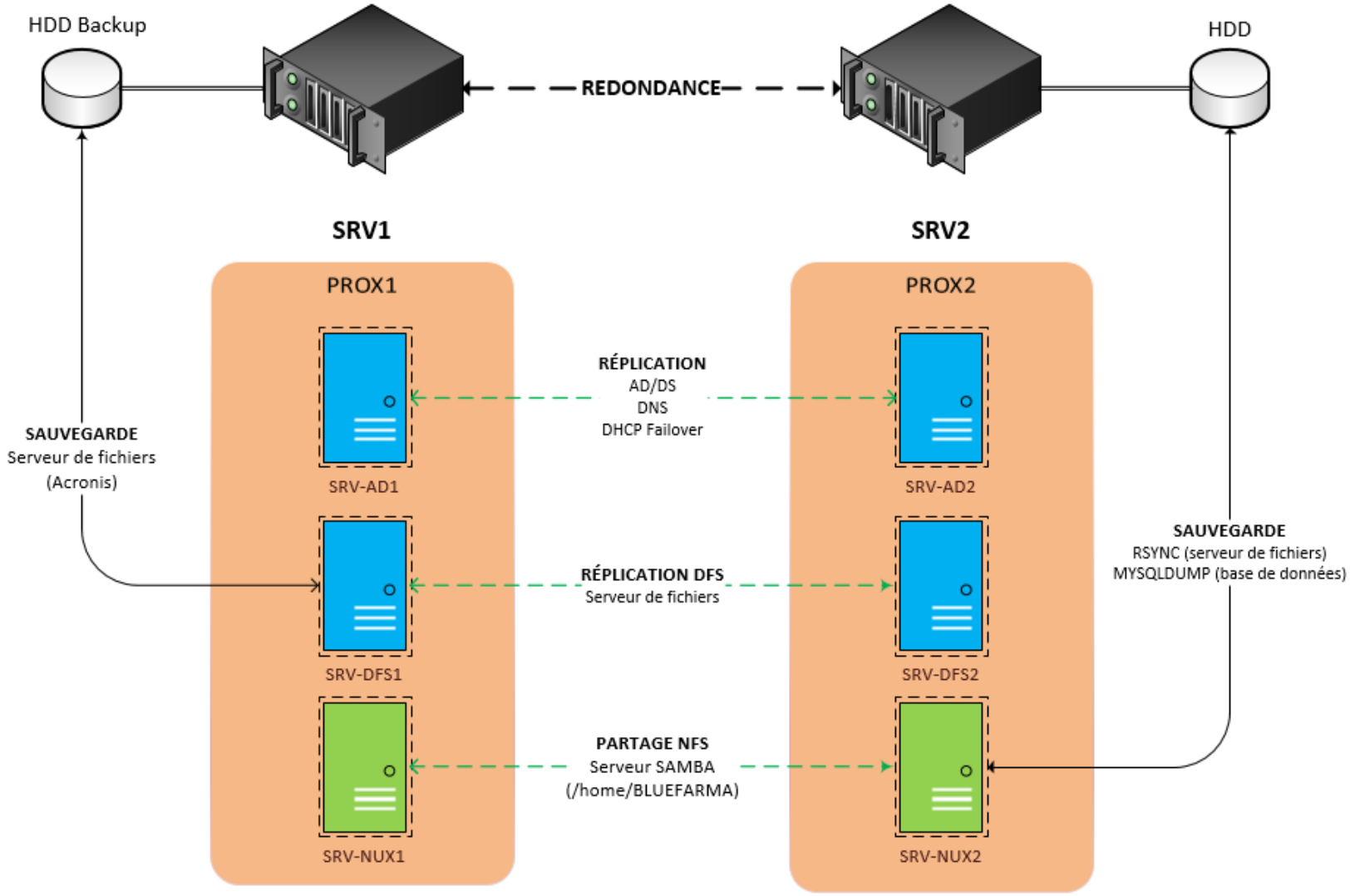


Schéma des services redondés et des dispositifs de sauvegarde

6.3.3. Stratégie de sauvegarde : choix des logiciels et des supports

La redondance des données ne constitue pas une sauvegarde en soit. Or, l'absence de sauvegarde représente un risque et doit être prise en considération dans la gestion des risques inhérents à la perte irrémédiable de données.

Une stratégie doit être développée en vue de pérenniser les données de l'entreprise. Pour ce faire, une réflexion doit être menée sur les aspects suivants :

- Le type de données à "backuper" : fichiers textes, images, vidéos, applications, base de données, etc.
- La fréquence des sauvegardes.
- Le(s) support(s) d'enregistrement (NAS, cloud, etc.)
- La durée de conservation des copies (mois, trimestre, année, etc.).
- La quantité de Gigas générés.

Ces paramètres doivent être pris en compte pour élaborer la stratégie la plus adaptée.

Bluefarma génère surtout des données de types fichiers textes et des images ainsi que de la base de données et plus rarement de la vidéo. Ses besoins en capacité sont donc assez modérés. Il convient ainsi de définir un juste équilibre entre le besoin actuel tout en prenant en compte la croissance des activités et l'évolution du volume de données d'ici les prochains mois et années.

Conformément aux recommandations de la CNIL et de l'ANSSI, notre stratégie de sauvegarde des données sera axée autour de deux types de sauvegardes :

- Sauvegardes **incrémentielles** (ou "incrémentales") quotidiennes durant une semaine. Passé ce délai, les sauvegardes de la semaine seront écrasées.
- Sauvegarde complète **mensuelle** : chacune d'entre elles sera conservées sur un disque dur pour une durée de trois mois.

Logiciels de sauvegarde

Les solutions de sauvegarde changent considérablement entre les environnements Windows et Linux. Toutes nos solutions sont capables d'effectuer des sauvegardes complètes ou incrémentielles. Voici un résumé de ce qui a été mis en œuvre :

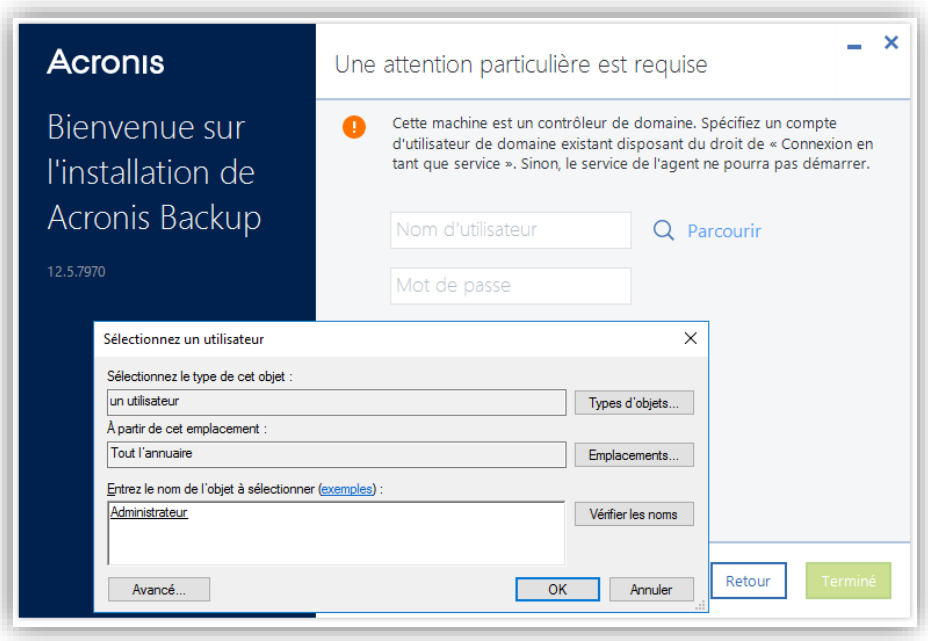
Besoins	**Windows Server**	**CentOS**
Serveur de fichiers	Acronis	rsync (via NFS)
Base de données	n/a	mysqldump

Acronis (sauvegarde Windows)

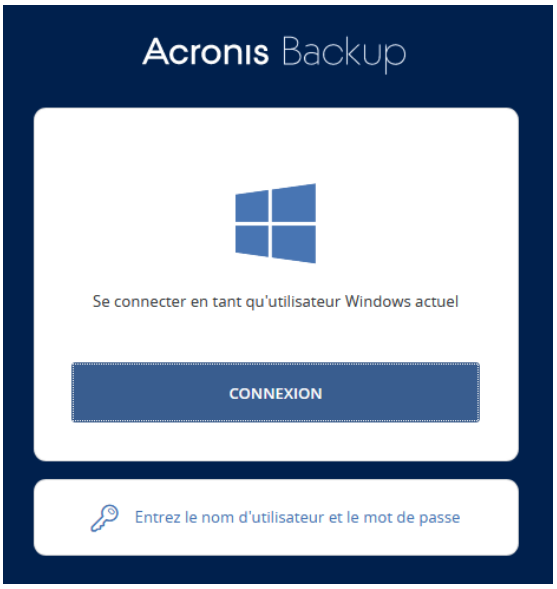
Windows apporte une solution de sauvegarde via le rôle **Sauvegarde Windows Server**. Cette fonctionnalité propose de faire des sauvegardes complètes ou de dossiers de manière planifiée. Il est également possible d'utiliser un outil de restauration de sauvegarde. Malheureusement, ce rôle ne permet pas de programmer plusieurs sauvegardes différentes à la fois depuis la même machine et offre peu de paramètres pour configurer nos sauvegardes.

Nous avons ainsi opté pour le logiciel **Acronis Backup** pour la sauvegarde des données du serveur de fichiers de Windows Server.

Son installation est très simple et se déroule de manière automatisée. L'un de ses avantages réside dans sa capacité à reconnaître et intégrer l'environnement Windows Server en détectant le nom de notre machine et les comptes enregistrés dans Active Directory.



L'interface de gestion d'Acronis est accessible depuis le navigateur en exploitant le port 9877, ce qui donnera l'adresse suivante : **SRV-AD1.bluefarma.local:9877**.



Nous sommes invités à nous logger. On remarque que Acronis prend en charge le compte Administrateur Windows.

Acronis est notamment capable de :

- Sauvegarder une image système : cette opération peut aider à sauvegarder le système si celui-ci a planté.
- Sauvegarder certains dossiers.
- Chiffrer les données derrière un mot de passe (algorithme jusqu'à AES 256).
- Restauration des données.

Acronis Backup procèdera à la sauvegarde entre les machines SRV-AD1 et SRV-DFS2 présentes dans deux bâtiments différents :

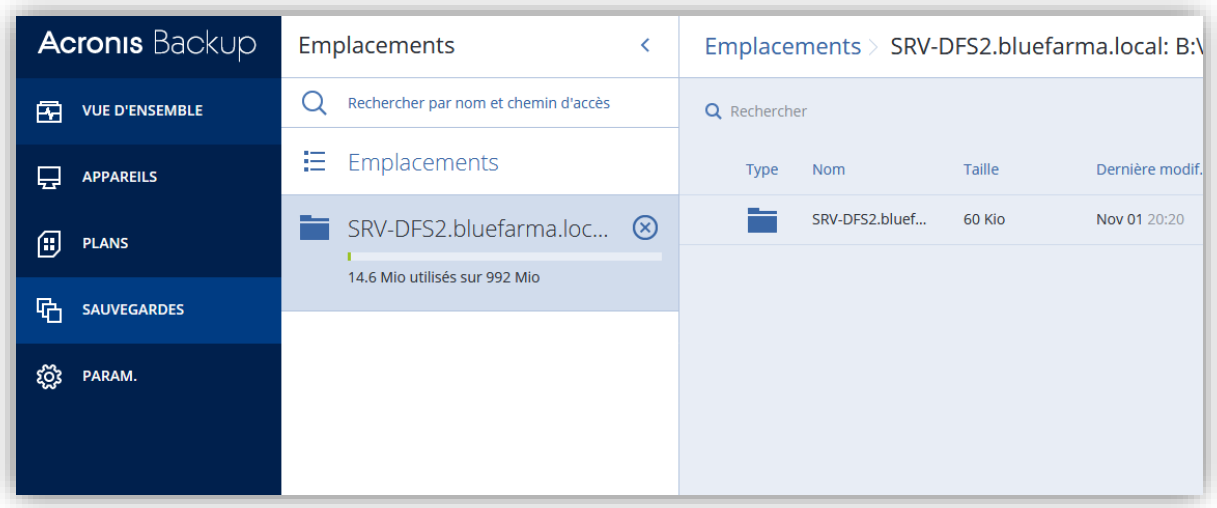
- SRV-AD1 : installation d'Acronis en mode ***Serveur de gestion***.
- SRV-DFS2 : installation d'Acronis en mode **Agent de sauvegarde**.

L'agent de sauvegarde servira à piloter la sauvegarde sur SRV-DFS2 depuis SRV-AD1 (Acronis peut détecter et ajouter d'autres machines faisant partie du domaine).

Conformément à ce qui a été décidé et décrit précédemment, nous avons planifié une sauvegarde incrémentale quotidienne et une complète hebdomadaire.

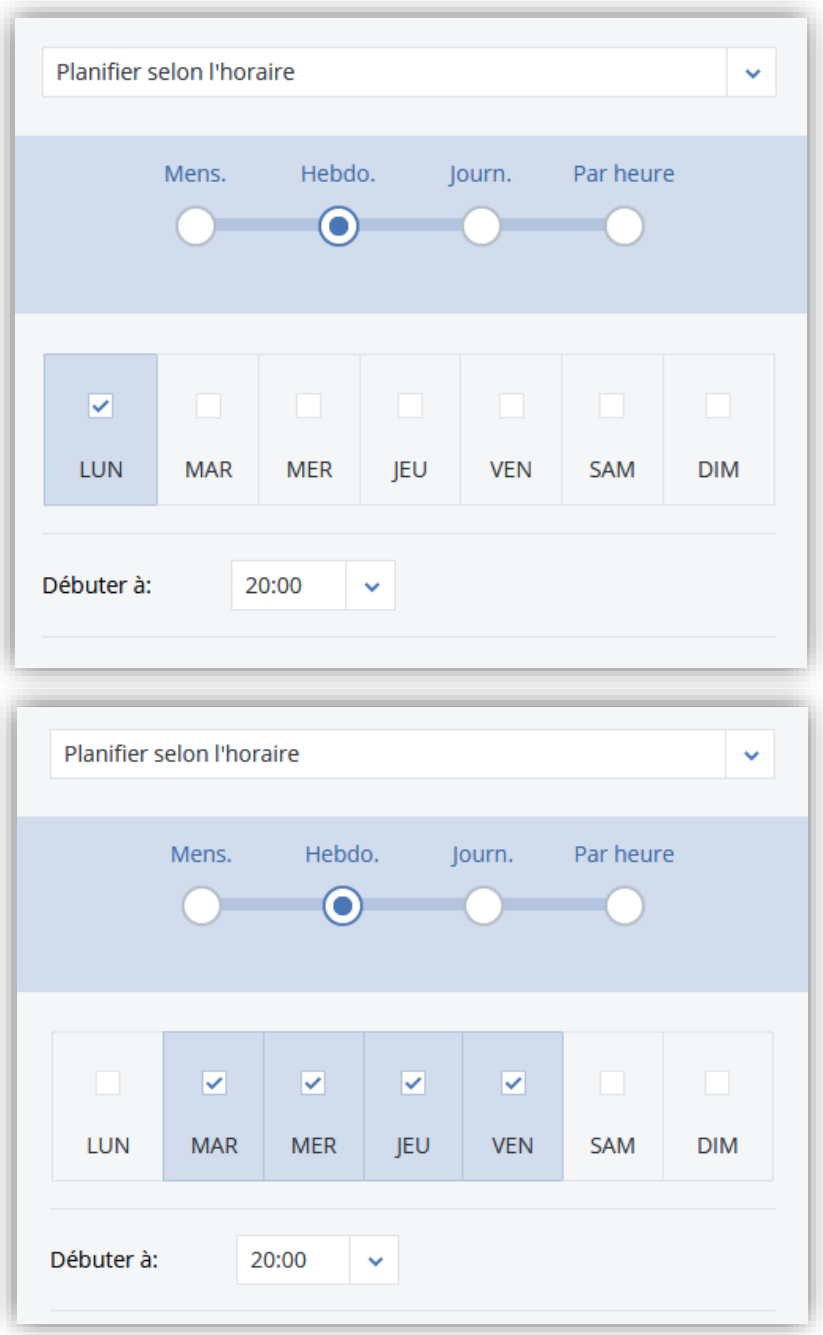
Configuration de la sauvegarde incrémentielle et complète mensuelle

- Depuis l'onglet ***SAUVEGARDES***, cliquer ***Ajouter un emplacement*** puis sélectionner la machine SRV-DFS2 (qui possède un disque dur de backup installé sur le serveur hébergeant cette VM).

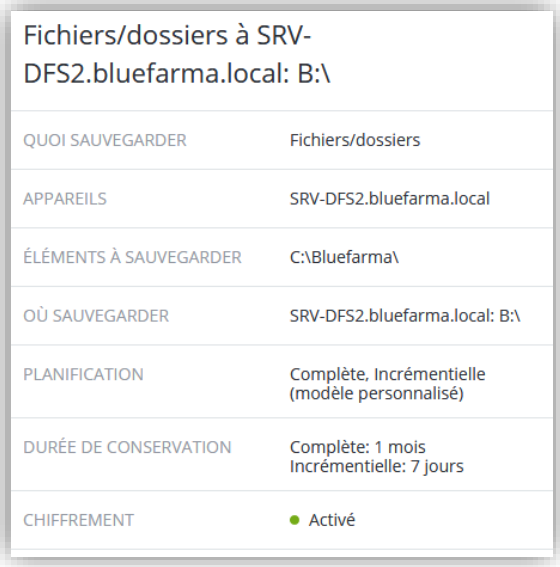


- Se rendre ensuite dans l'onglet ***PLANS*** puis ***Création d'un plan***. D'ici, il convient de sélectionner ce que l'on veut sauvegarder (***Fichiers/dossiers***) et depuis quel appareil (SRV-DFS2.bluefarma.local). On sélectionne ensuite le dossier Bluefarma qui héberge toutes les données utilisateurs.

- Indiquer ensuite que l'on souhaite une sauvegarde complète tous les lundis à partir de laquelle les sauvegardes incrémentielles se baseront entre le mardi et le vendredi.



- Nous souhaitons conserver nos sauvegardes incrémentielles pendant sept jours et les complètes durant un mois.

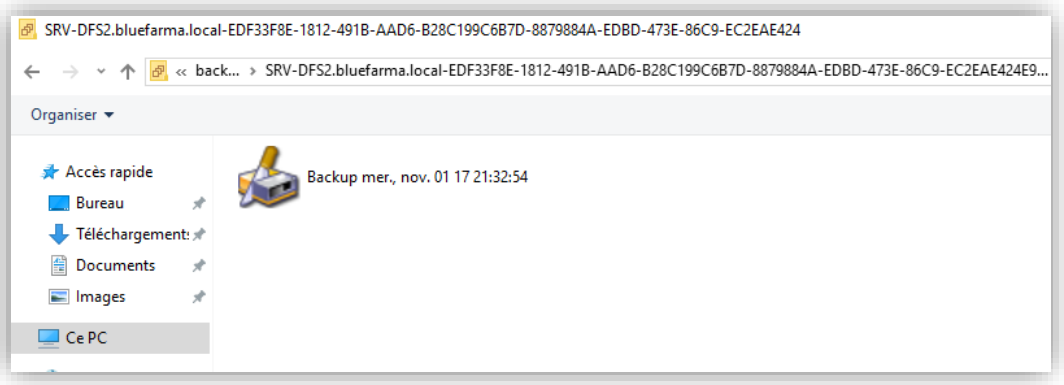


Du chiffrement est appliqué à notre dossier de backup avec l'algorithme AES 256.

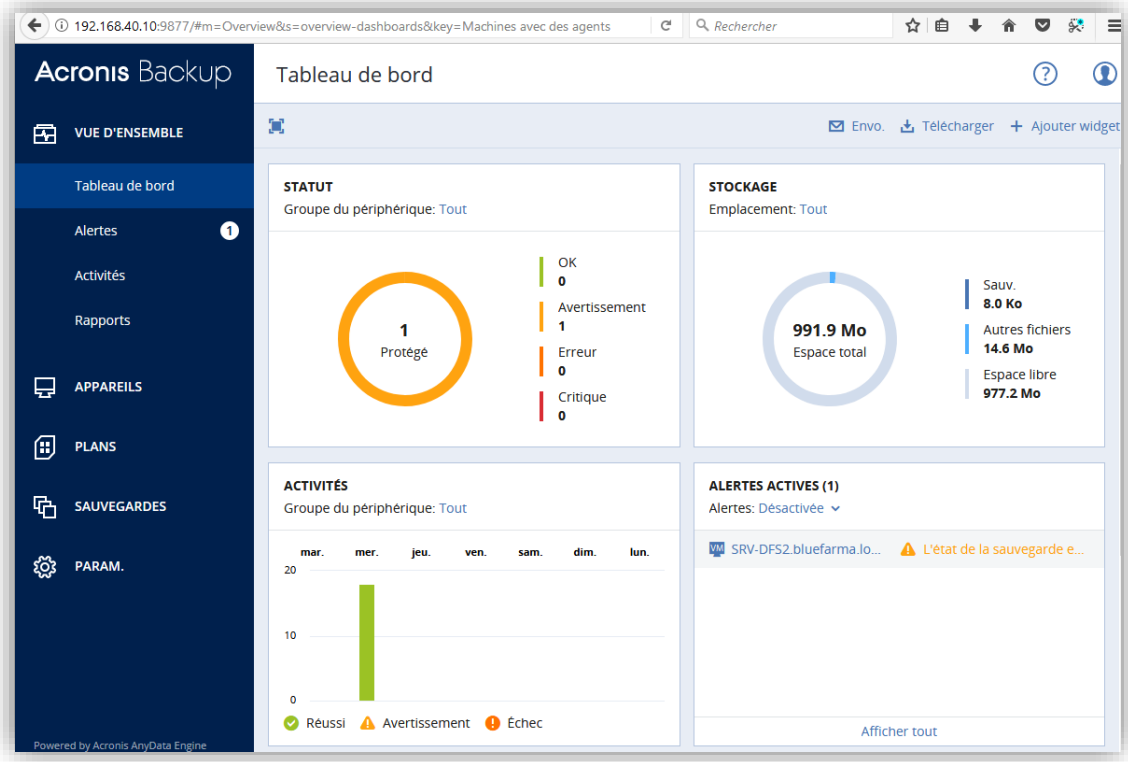
Nous obtenons la synthèse de ce qui a été paramétré juste avant :

- Une sauvegarde complète tous les lundis à 20 heures
- Une sauvegarde incrémentielle du mardi au vendredi à 20 heures.

Nous exécutons maintenant la sauvegarde pour vérifier que cette dernière s'effectue bien sur le disque de SRV-DF2 (le mot de passe défini juste avant nous sera demandé avant d'ouvrir le fichier de backup).



À noter que l'ensemble des évènements liés à la sauvegarde est visible depuis le ***Tableau de bord*** (onglet ***VUE D'ENSEMBLE***). Les sous-onglets ***Alertes***, ***Activités*** et ***Rapports*** rendent compte de toutes les activités qui se sont déroulées sur le serveur à l'attention de l'administrateur.



Rsync & mysqldump (sauvegardes Linux)

Les sauvegardes s'effectueront sur SRV-NUX2 avec les utilitaires suivants :

- ***rsync*** pour le sauvegarde des données utilisateurs.
- ***Mysqldump*** pour la sauvegarde de la base de données MySQL

Nous ne reviendrons pas sur la mise en œuvre de ces sauvegardes qui a été expliquée dans la partie **5.5**.

Supports de sauvegarde

Dans le cadre d'un PRA, la nécessité de récupérer rapidement des données pour les injecter rapidement dans le système d'informations est essentielle. Le **stockage sur bande magnétique**, dont l'usage s'adapte au besoin d'archiver des données sur plusieurs années, présente une robustesse et des volumes importants pour un faible coût. Cependant, cette technologie ne répond pas à notre problématique en raison des fortes latences d'écriture et de lecture des données. Nous préférons donc nous orienter vers un support classique de type **HDD** qui répondra mieux à notre besoin de performances.

Durée de conservation des sauvegardes

Les disques possédant une sauvegarde complète seront conservés hors de nos locaux dans un coffre étanche que nous louerons auprès de la banque Société Générale (voir DEVIS, annexe **9.5**).

Nous effectuerons un dépôt mensuel des disques pour une durée de conservation de trois mois. Dépassé ce délai, les plus anciens disques seront formatés pour accueillir une nouvelle version des données à partir du 4^{e} mois, et ainsi de suite.

Le suivi des sauvegardes sera enregistré dans un tableur enregistrant chaque dépôt de disques de sauvegarde, avec la référence des disques utilisés.

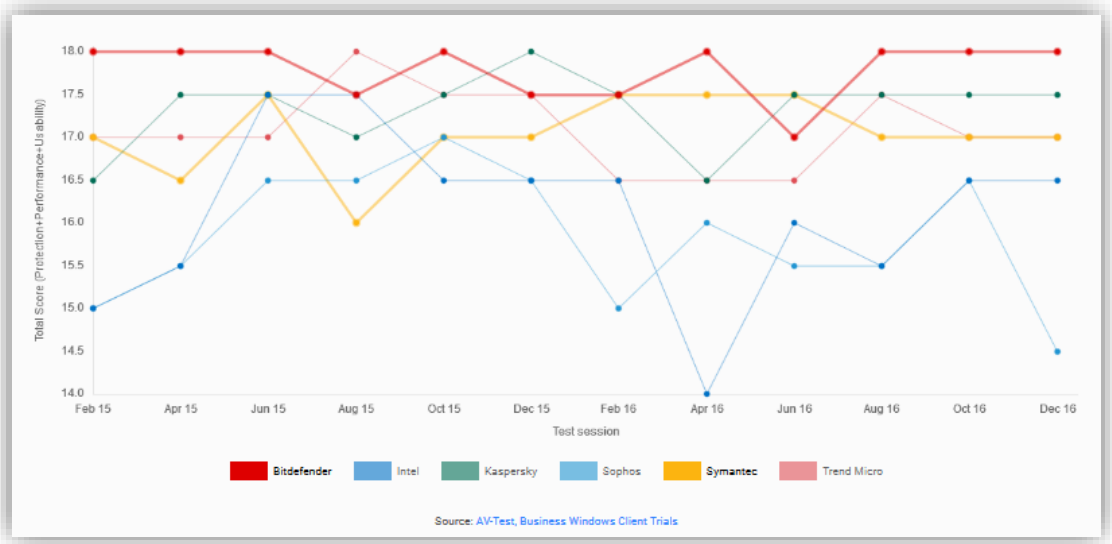
Les fréquences des sauvegardes et la quantité de disques durs pourront faire l'objet d'ajustements selon le besoin des services et la quantité de données générées.

6.3.4. Solution Antivirale

Les PME font partie des cibles privilégiées pour les cybercriminels (au moins 50% des PME d'après plusieurs études). Les conséquences d'une attaque sont multiples. Voici un rappel succinct des principaux virus et de leurs conséquences sur les activités d'une entreprise :

Type de virus	Actions	Conséquences
Malware/adwares	▪ Publicités intempestives ▪ Ralentissements des postes ▪ Ralentissement de la bande passante	Perte de productivité Perte de performances
Cryptowares/ransomwares	▪ Données cryptées définitivement	Perte totale des données sur le poste infecté
Cheval de Troie	▪ Introduction dans le système	Perte de confidentialité des données

Nous avons opté pour la solution antivirale **Bitdefender GravityZone Business Security** capable de détecter 99% de menaces inconnues. Il est particulièrement aguerri contre les ransomwares (établissement d'une liste noire de près de 2,8 millions d'échantillons) et les processus de cryptage.



Bitdefender surveille en outre tous les processus en cours d'exécution pour détecter les comportements malveillants. De plus, la tâche de l'administrateur système est simplifiée grâce au déploiement à distance de la protection sur d'autres postes.

6.4. Synthèse des solutions et scénarios de panne

Conformément aux recommandations énoncées par l'ANSSI, tout un ensemble de solutions a été présenté pour garantir l'intégrité, la disponibilité et la sauvegarde des données de l'entreprise face aux risques les plus courants.

Les mesures présentées prennent en compte notamment :

- La **protection physique des serveurs** : contre les sinistres, la surchauffe des équipements ou les surtensions.
- La **protection des données contre les cyberattaques** : Antivirus et réglages du pare-feu.
- La **sauvegarde des données** : sauvegardes incrémentielles et complètes avec Acronis pour Windows, rsync et mysqldump pour Linux.
- La **redondance :** apporte de la haute-disponibilité aux services et aux données.

Sur ce dernier point, nous tenions à rappeler que la redondance de l'infrastructure offre une disponibilité proche de 100% des services AD/DNS, DHCP et serveur de fichiers si un des deux serveurs venait à tomber en panne (pour rappel, toute l'infrastructure réseau a été volontairement bouclée lors du projet START en appliquant du ***spanning tree*** pour pallier une rupture de liaison inter-bâtiment). Grâce à cette infrastructure, on peut envisager les scénarios suivants :

Haute-Disponibilité des services et des données		
Bât. Principal (SRV1) Panne de **SRV1**	Aile ouest (**SRV2**) Bascule des services sur : - SRV-AD2 (AD, DNS, DHCP) - SRV-DFS2 (serveur de fichiers) - SRV-NUX2 (Sauvegardes Linux)	Aile est (aucun serveur) Service OK
Pas de bascule Services disponibles sur : - SRV-AD1 (AD, DNS, DHCP) - SRV-DFS1 (serveur de fichiers) - SRV-NUX (données + base de données	Panne de **SRV2**	Service OK

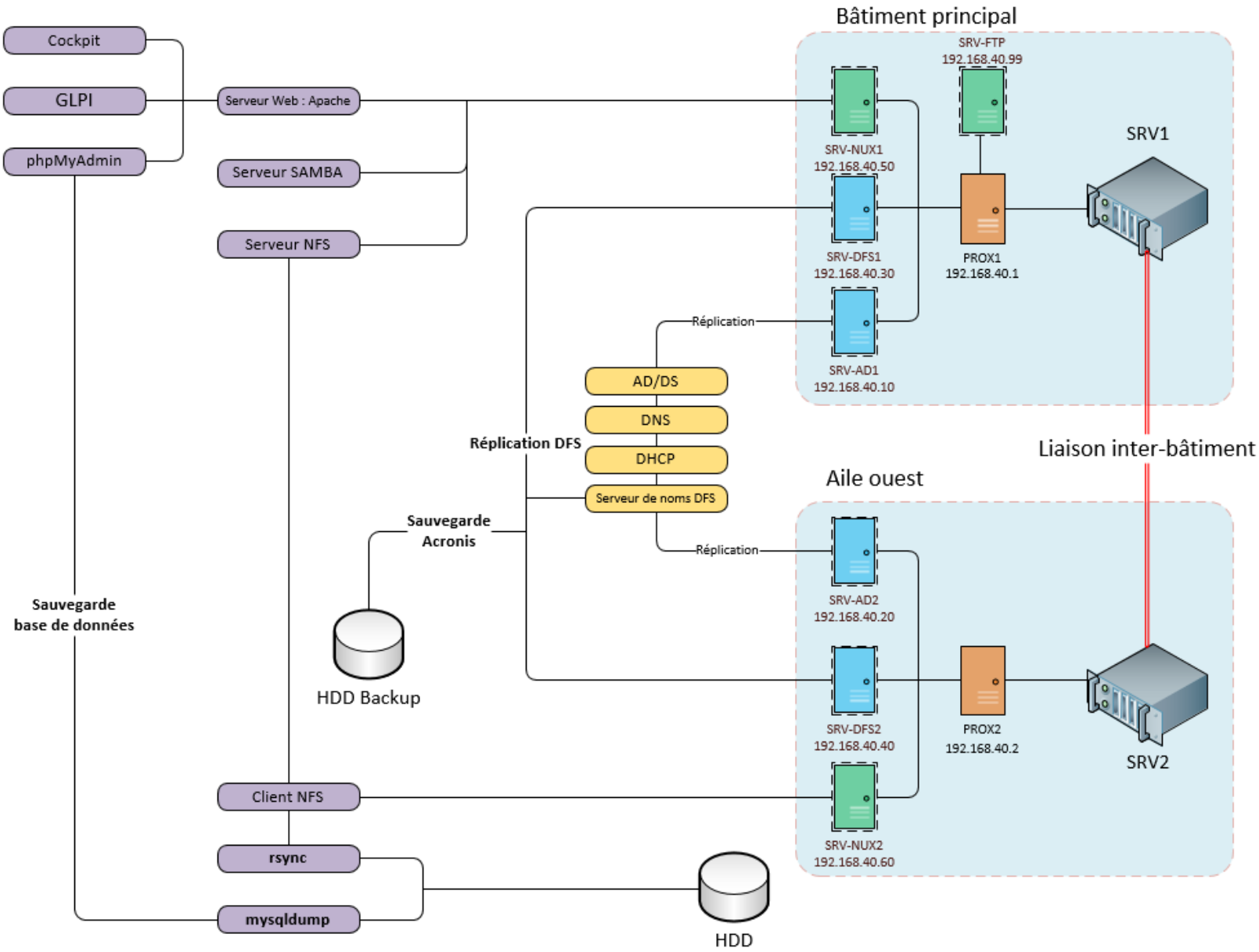


Schéma de l'infrastructure système complète avec ses différents services

7. BASE DE DONNÉES

7.1. Rappel du cahier des charges et présentation de GLPI

Conformément au cahier des charges, deux fonctionnalités sont attendues pour la base de données :

- Mode consultation pour les utilisateurs.
- Mode gestion (lecture, écriture, suppression) pour le SI.

Nous avons choisi **GLPI** comme interface web de gestion de la base de données. Cette solution est très flexible et relativement simple à mettre en œuvre. On peut effectivement personnaliser GLPI en l'adaptant aux besoins de l'entreprise. Les principales fonctionnalités de GLPI sont les suivantes :

- Inventaire du parc informatique de l'entreprise.
- Monitoring de la gestion du parc informatique avec la gestion des connexions aux ordinateurs.
- Inventaire du matériel réseau avec gestion des connexions aux périphériques.
- Gestion des licences avec leurs dates d'expiration.
- Gestion des demandes et des incidents utilisateurs.
- Archivage des matériels sortis de l'inventaire.
- Sauvegarde/Restauration de la base de données au format SQL.
- Intègre facilement les applications de superviseur comme Nagios, Centreon.
- Possibilité d'installer des plugins afin d'ajouter des fonctionnalités.
- Création d'une FAQ
- Établissement de statistiques

7.2. Importation LDAP des utilisateurs dans GLPI

Nous avons mis en place une authentification LDAP sur GLPI. De cette façon, les utilisateurs pourront renseigner leur identifiant et mot de passe de session AD dans GLPI pour accéder à l'interface à l'interface. L'avantage est double :

- Simplification d'administration : il n'y a pas besoin de créer les 90 utilisateurs du côté du GLPI grâce à l'importation LDAP.
- Les utilisateurs n'auront pas à retenir un deuxième couple identifiant/mot de passe.

Par ailleurs, un utilisateur supprimé de l'Active Directory pourra également être automatiquement désactivé du GLPI, par exemple :

Configuration : [annexe **9.5**]

7.3. Configuration des droits utilisateurs

Il existe plusieurs profils de base, sur GLPI, qui correspondent aux rôles et qui réglementent les accès des utilisateurs.

Nom	Interface du profil	Profil par défaut
Admin	Interface standard	Non
Hotliner	Interface standard	Non
Observer	Interface standard	Non
Read-Only	Interface standard	Non
Self-Service	Interface simplifiée	Non
Super-Admin	Interface standard	Non
Supervisor	Interface standard	Non
Technician	Interface standard	Non
Utilisateurs	Interface standard	Oui

Il est possible de créer des profils personnalisés. Dans notre cas, nous utiliserons deux types de profil :

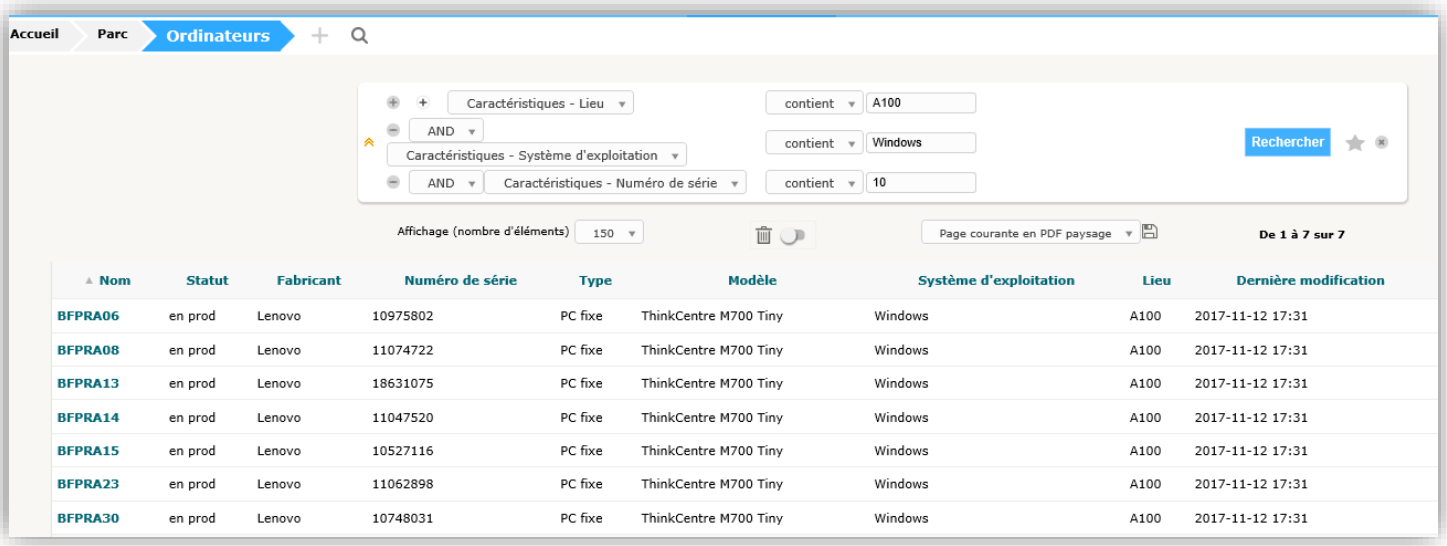
- Service informatique : accès total à toute l'administration du GLPI
- Utilisateurs : mode lecture pour consulter le parc, créer des tickets, accéder aux FAQ, etc..

Conformément au cahier des charges, les éléments à consulter ou à gérer sont les suivants :

- Utilisateurs : liste des postes, écrans, imprimantes associées via une recherche multicritères (local, mémoire vive, disque dur, etc.)/
- Service informatique : gestion des utilisateurs (ajout/modification/suppression) et du matériel du parc (PC, écrans, imprimantes, etc.).

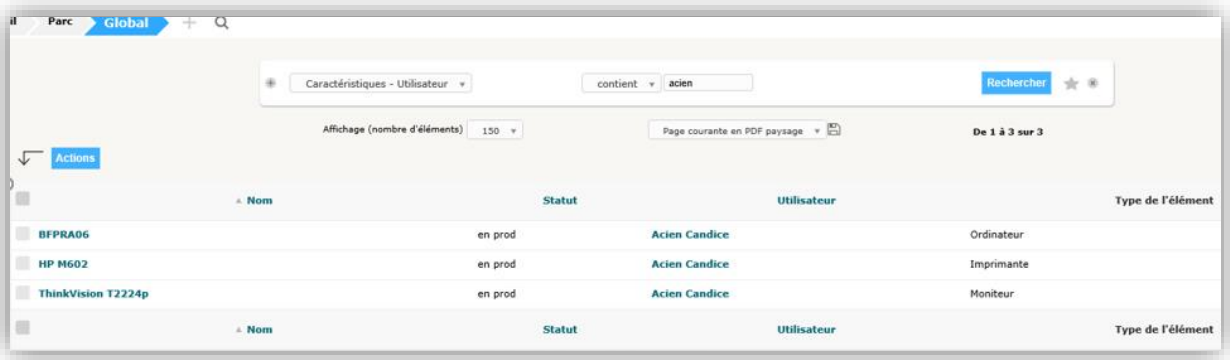
Recherche multicritère :

L'utilisateur peut effectuer une recherche en fonction du lieu, du système d'exploitation, des composants, des ordinateurs, des imprimantes ou des écrans.



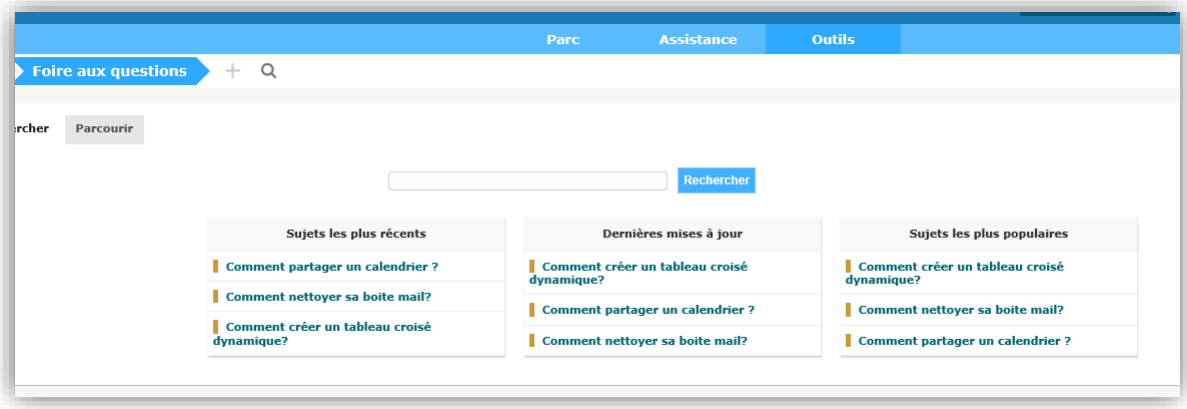
Nom	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation	Lieu	Dernière modification
BFPRA06	en prod	Lenovo	10975802	PC fixe	ThinkCentre M700 Tiny	Windows	A100	2017-11-12 17:31
BFPRA08	en prod	Lenovo	11074722	PC fixe	ThinkCentre M700 Tiny	Windows	A100	2017-11-12 17:31
BFPRA13	en prod	Lenovo	18631075	PC fixe	ThinkCentre M700 Tiny	Windows	A100	2017-11-12 17:31
BFPRA14	en prod	Lenovo	11047520	PC fixe	ThinkCentre M700 Tiny	Windows	A100	2017-11-12 17:31
BFPRA15	en prod	Lenovo	10527116	PC fixe	ThinkCentre M700 Tiny	Windows	A100	2017-11-12 17:31
BFPRA23	en prod	Lenovo	11062898	PC fixe	ThinkCentre M700 Tiny	Windows	A100	2017-11-12 17:31
BFPRA30	en prod	Lenovo	10748031	PC fixe	ThinkCentre M700 Tiny	Windows	A100	2017-11-12 17:31

<u>Exemple de recherche utilisateur</u> : on visualise l'ordinateur, l'écran et l'imprimante associées au poste.



Nom	Statut	Utilisateur	Type de l'élément
BFPRA06	en prod	Acien Candice	Ordinateur
HP M602	en prod	Acien Candice	Imprimante
ThinkVision T2224p	en prod	Acien Candice	Moniteur

L'utilisateur a également accès à une Foire Aux Questions, qui peut alléger le travail du support informatique :



Pour le SI, l'interface d'administration de GLPI se présente avec les éléments suivants qui apportent un contrôle total sur la base de données :

- Gestion de tous les éléments matériels composant le parc.
- Gestion des tickets.
- Visuel sur les contrats et budgets en cours, coordonnées des fournisseurs, etc.
- Administration avancée des utilisateurs.

8. CONCLUSION

Au terme de cette présentation, nous pouvons affirmer que notre infrastructure est sécurisée et hautement disponible pour parer aux risques les plus courants. Le ratio entre les dépenses pour les équipements et la fiabilité de l'infrastructure est très satisfaisant puisqu'il s'élève à près de 50000 euros HT (annexe, **9.6**).

Nous avons ainsi pu mettre en œuvre une infrastructure présentant une très bonne tolérance à la panne tout en respectant les conditions imposées dans le cahier des charges concernant notamment la gestion des utilisateurs, celle des données et l'organisation de la maintenance des serveurs.

Toutefois, l'évolution du système d'informations, des pratiques et des besoins utilisateurs nécessitera à l'avenir des ajustements qui devront être décidés en concertation avec les différents acteurs de notre société.

9. ANNEXES

9.1. CONFIGURATION DE WINDOWS SERVER

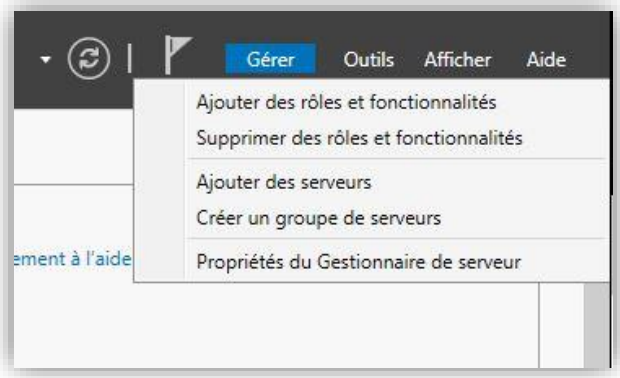
9.1.1. Installation du rôle AD DS et du DNS

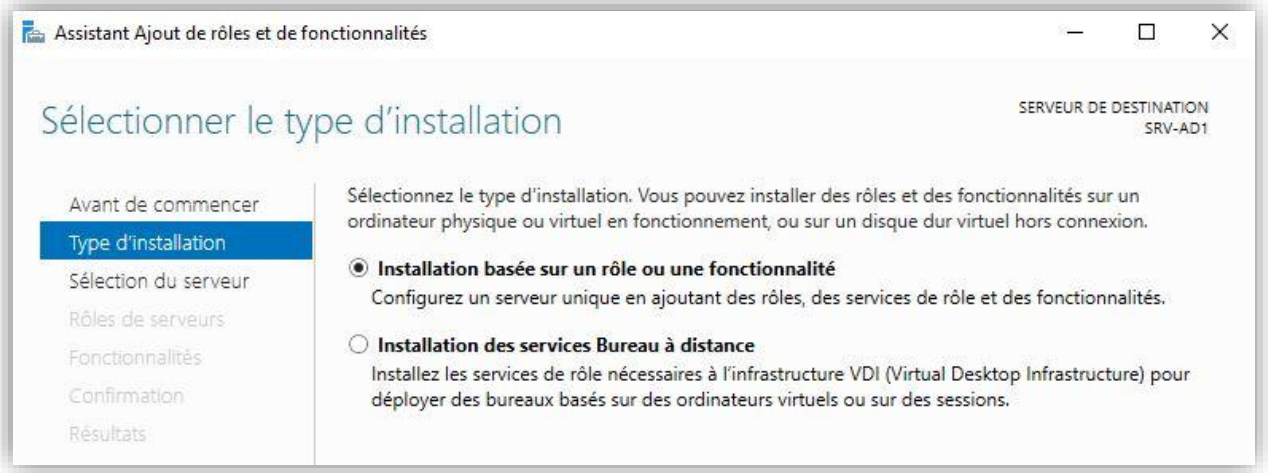
Prérequis :

- Il est conseillé de renommer le nom de la machine avant l'installation du contrôleur de domaine : toute modification postérieure est source de bug : nous l'appellerons SRV-AD1.
- Passer le serveur en IP statique en passant par le chemin suivant : Centre réseau et partage > Modifier les paramètres de la carte > Ethernet > Propriétés (clic-droit) > Protocole Internet version 4.

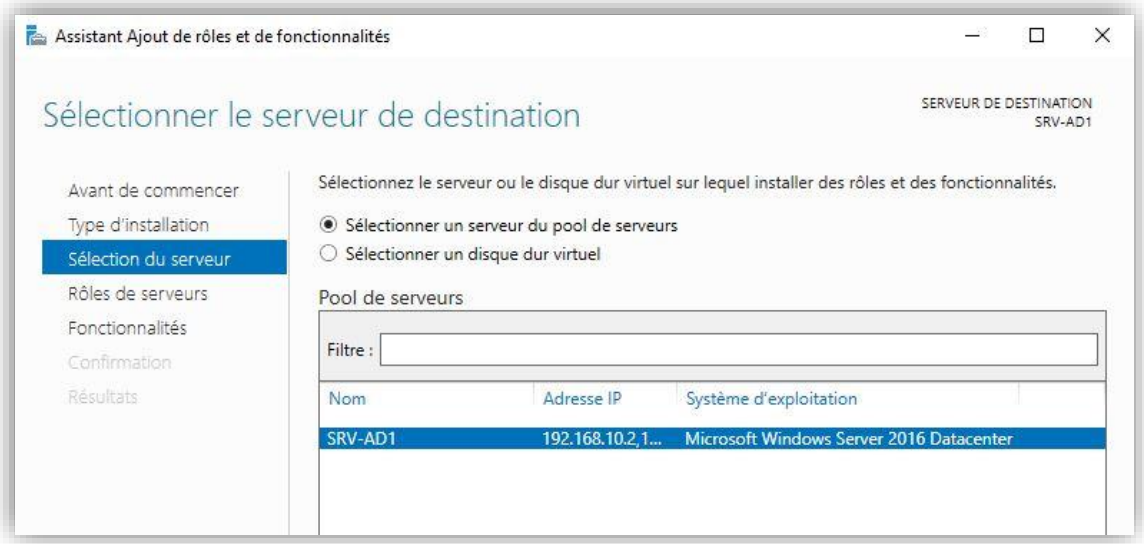
Installation du rôle AD DS :

- Dans ***Gérer***, cliquer ***sur Ajouter des rôles et des fonctionnalités*** puis sélectionner ***Installation basée sur un rôle ou une fonctionnalité*** :

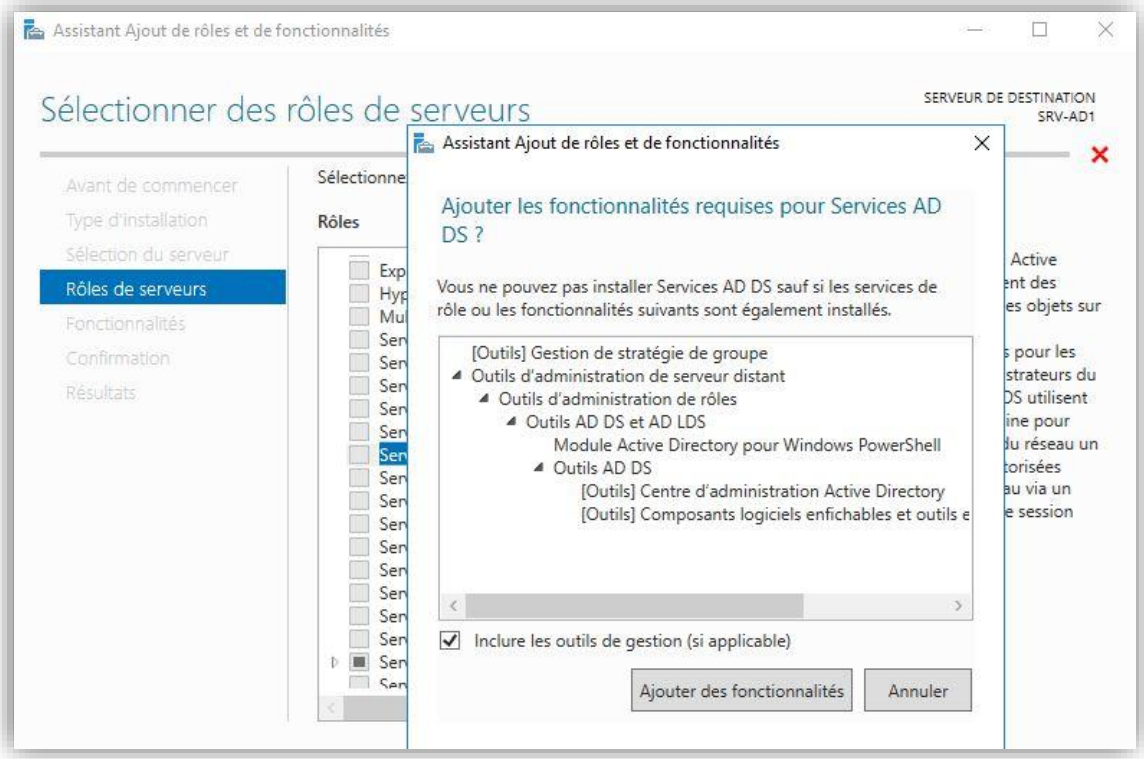




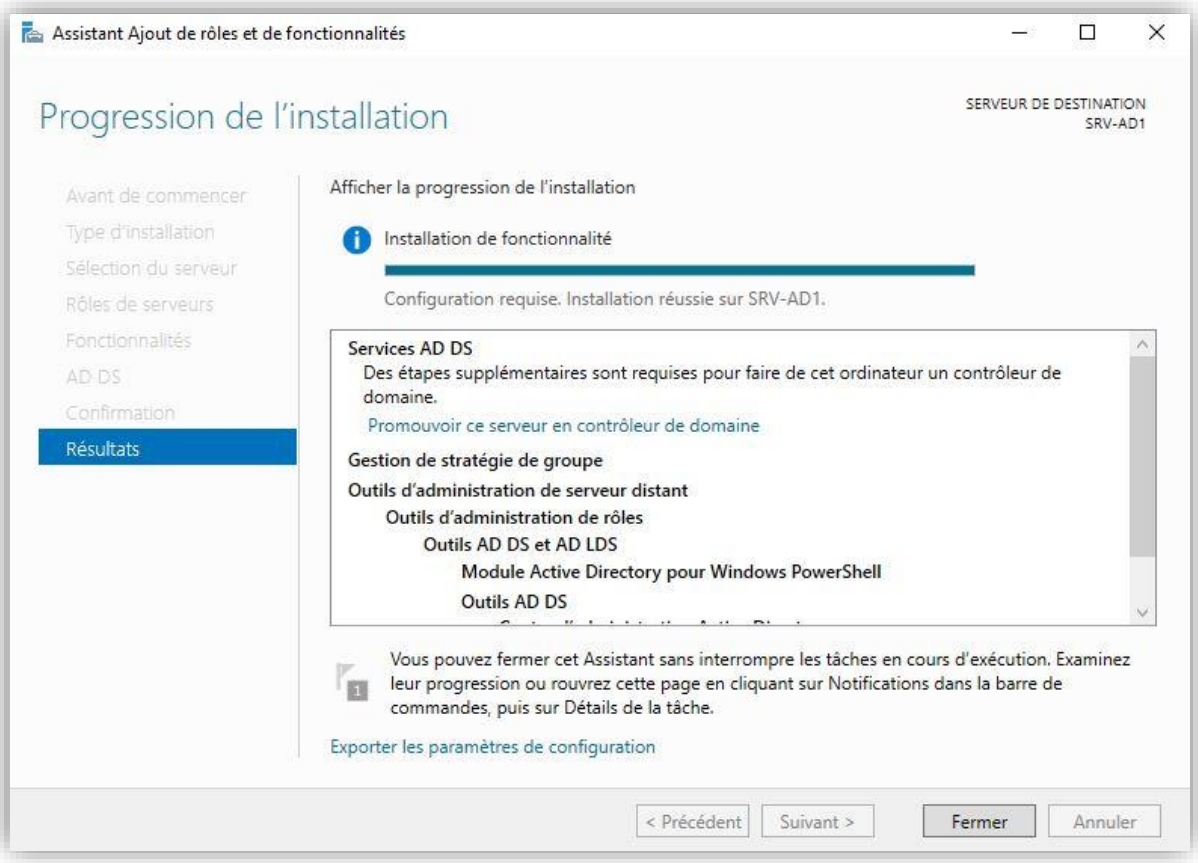
- Sélectionner le serveur SRV-AD1 comprenant l'adresse IP 192.168.40.10 :



- Sélectionner les rôles du serveur puis ***Ajouter les fonctionnalités*** :

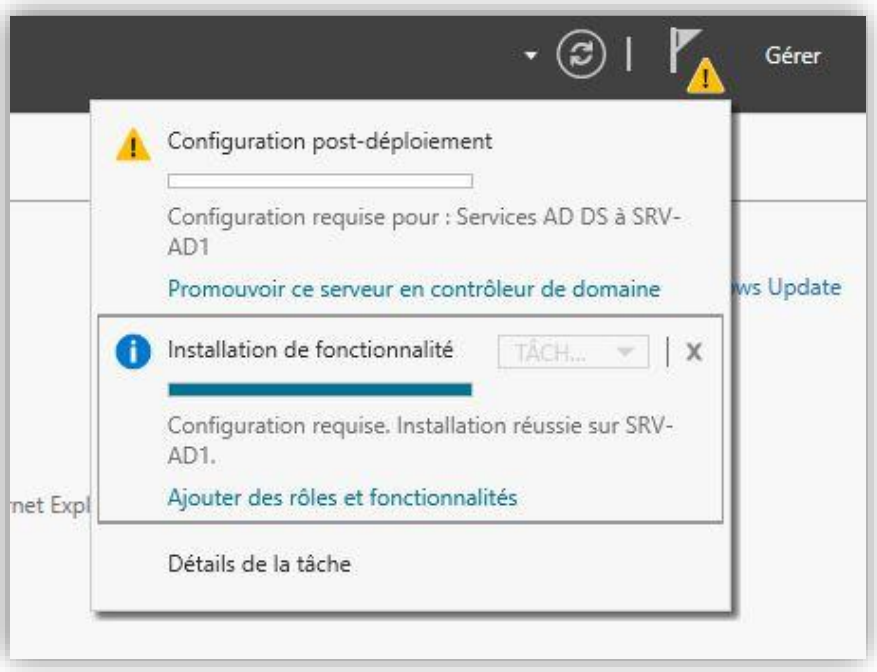


- Cliquer sur ***suivant*** jusqu'à la fin de l'installation du rôle AD DS :

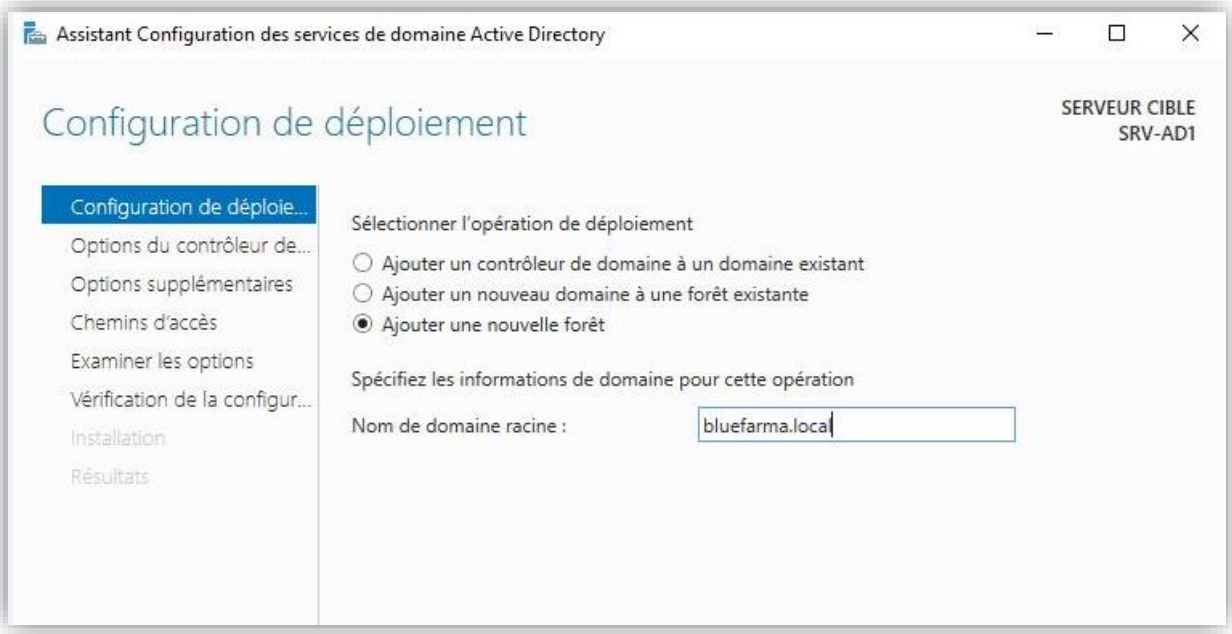


Configuration du contrôleur de domaine :

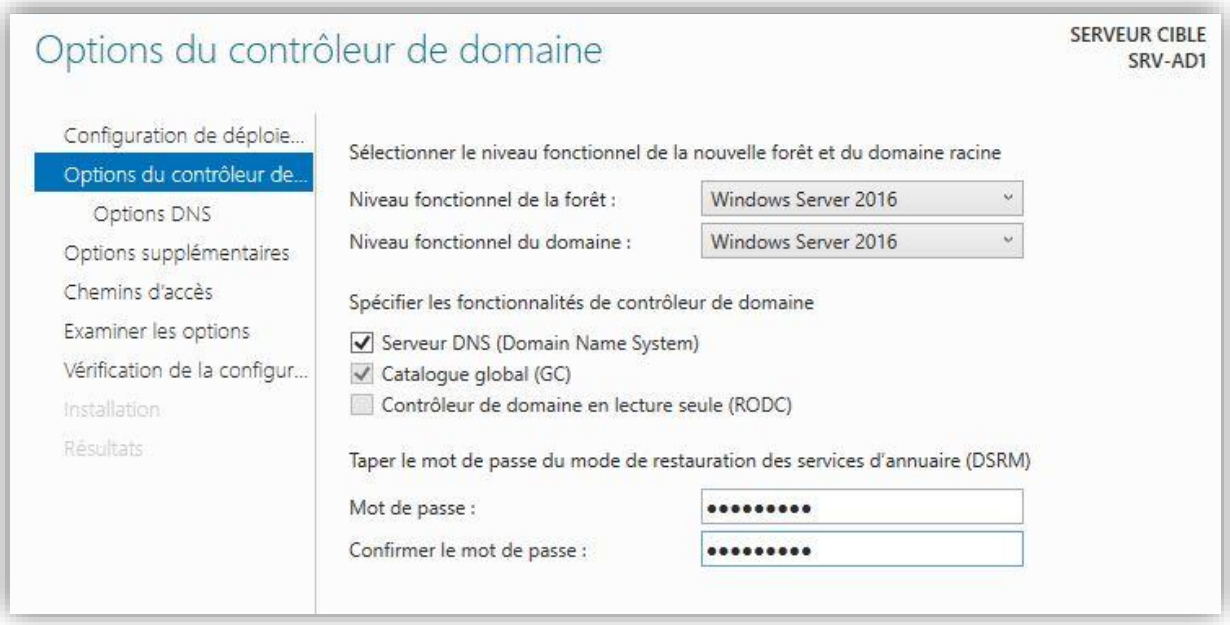
- Après l'installation du rôle AD DS, il convient de promouvoir le serveur en contrôleur de domaine :



- Durant cette étape, sélectionner ***Ajouter une nouvelle forêt*** puis renseigner dans le champ ***Nom de domaine racine*** le nom de domaine « bluefarma.local » :



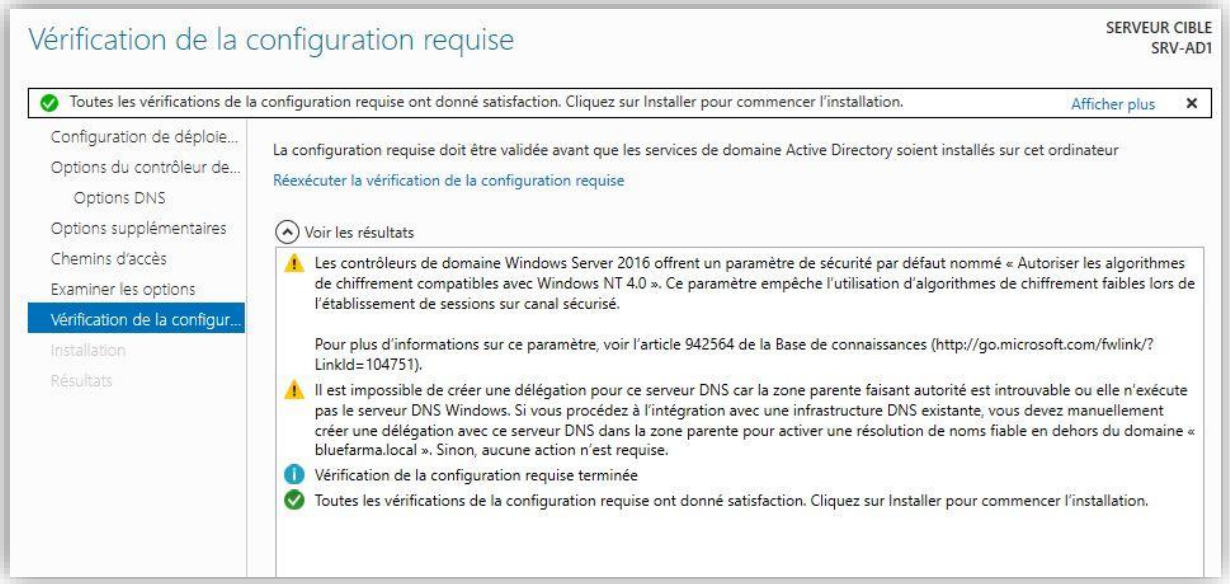
- Définir un mot de passe pour la restauration des services d'annuaire (DSRM) lors de la configuration des options du DNS :



- Spécifier ***le nom de domaine NetBIOS*** avec BLUEFARMA :

- Conserver les chemins d'accès proposés :

- Après la vérification de l'installation requise, cliquer sur ***Installer*** :

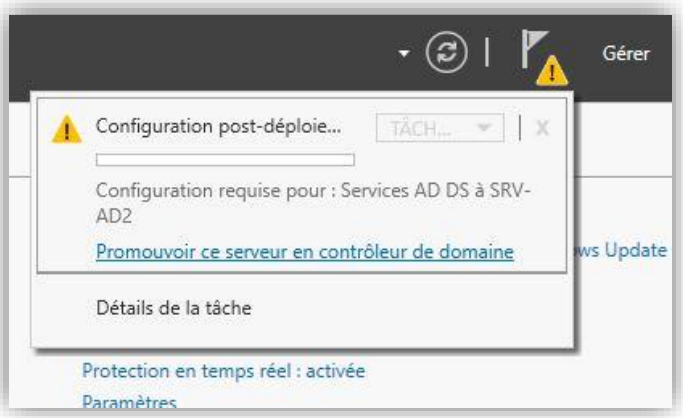


9.1.2. Réplication du contrôleur de domaine

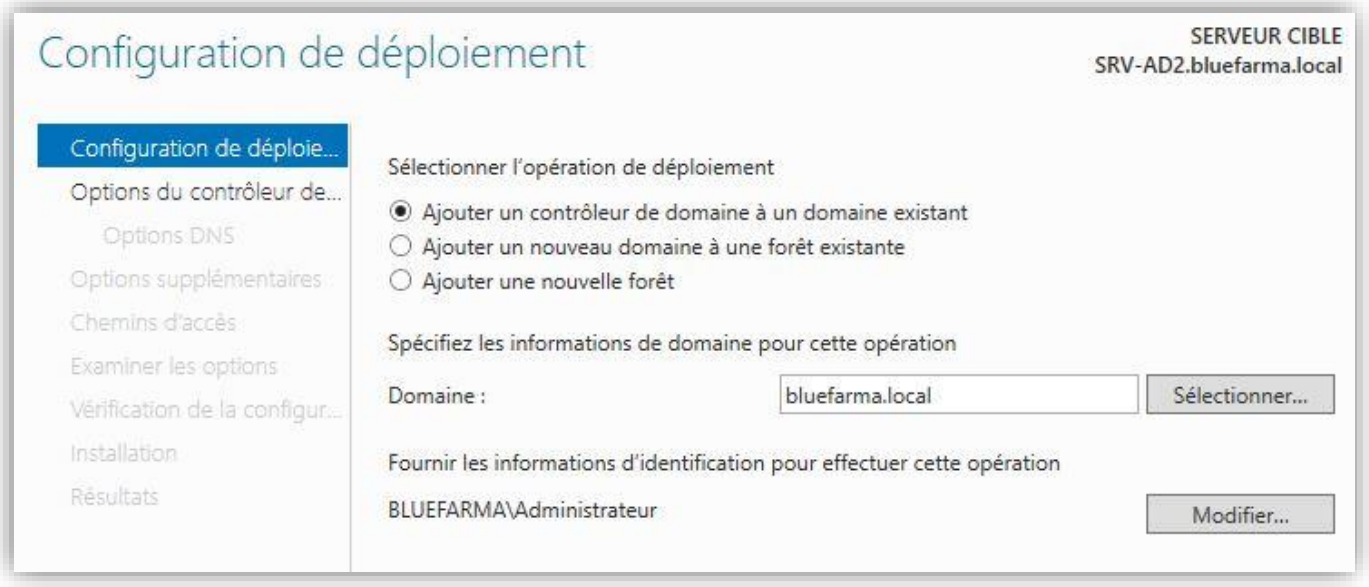
Prérequis :

- Comme pour le contrôleur de domaine installé sur SRV-AD1 (DC1), il faut procéder de la même manière à l'installation du rôle **AD DS** sur SRV-AD2.
- SRV-AD2 doit appartenir au même domaine bluefarma.local que SRV-AD1.
- Il faut indiquer dans la configuration DNS de la carte réseau l'adresse IP de SRV-AD1.

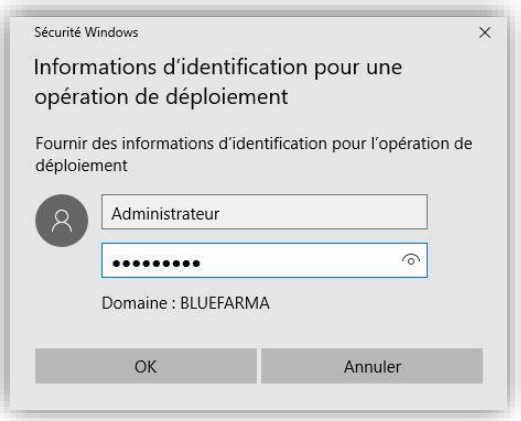
- Cliquer sur ***Promouvoir serveur en contrôleur de domaine*** :



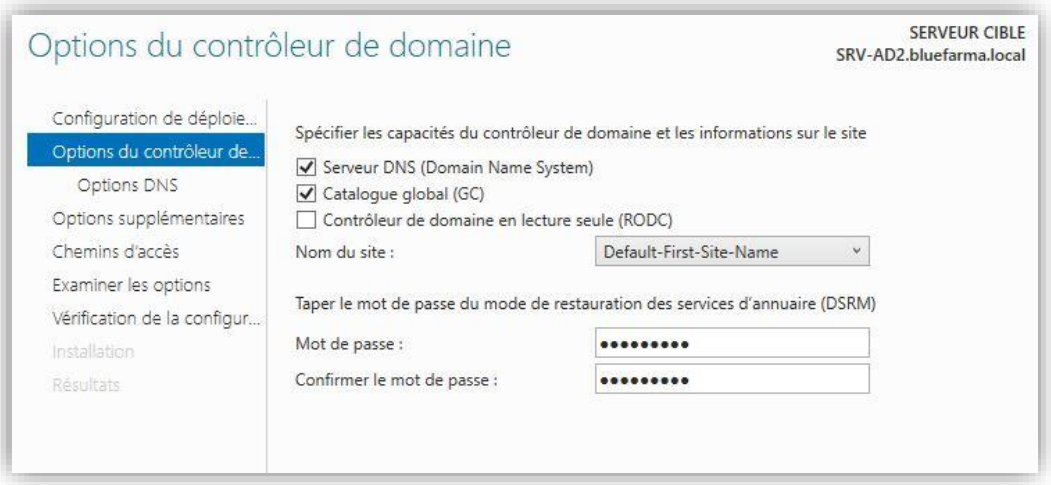
- Sélectionner ***Ajouter un contrôleur de domaine au domaine existant*** puis vérifier que la case ***Domaine*** est bien renseignée avec le nom de domaine de la société : bluefarma.local :



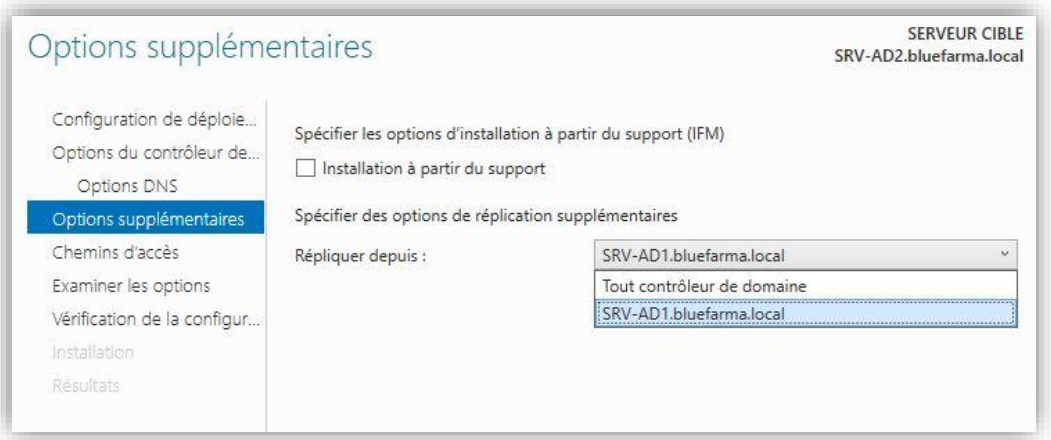
- Une fenêtre s'ouvre afin de renseigner le login et mot de passe de l'administrateur de SRV-AD1 pour intégrer son domaine :



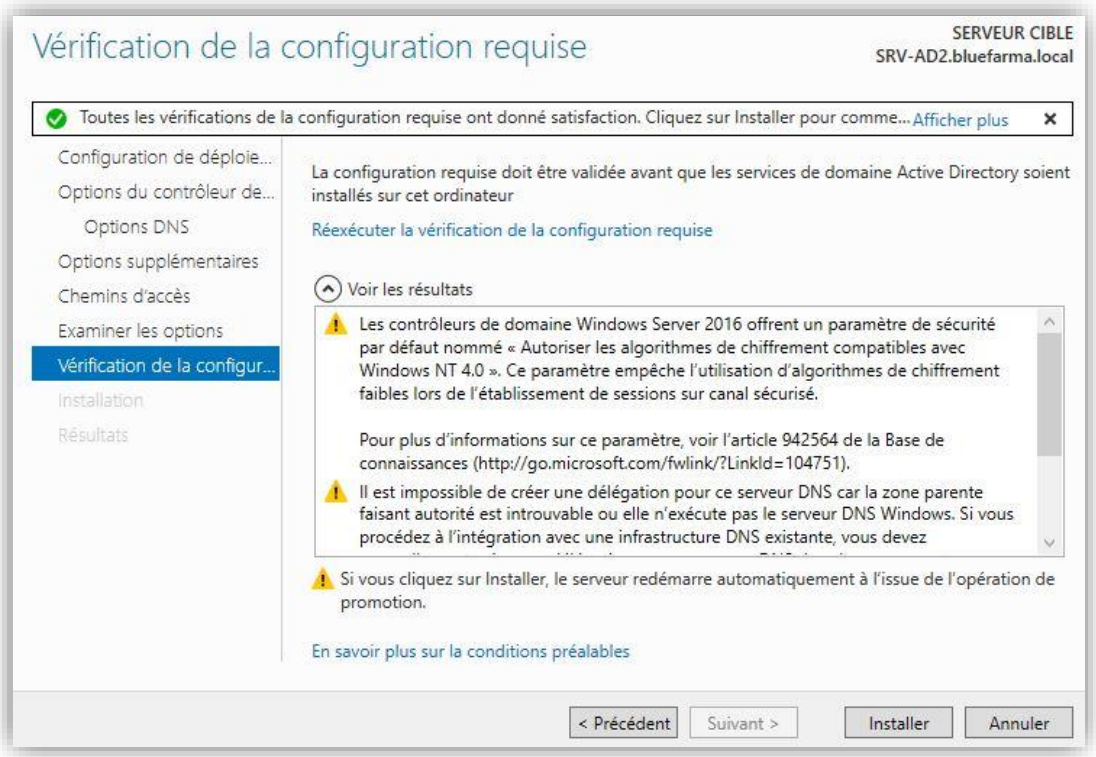
- Renseigner un mot de passe pour la restauration des services d'annuaire (DSRM) :



- Sélectionner le contrôleur de domaine source « **SRV-AD1.bluefarma.local** » dans ***Répliquer depuis*.** Ceci permettra d'importer les groupes, utilisateurs, objets, stratégie, etc. depuis le contrôleur de domaine source :

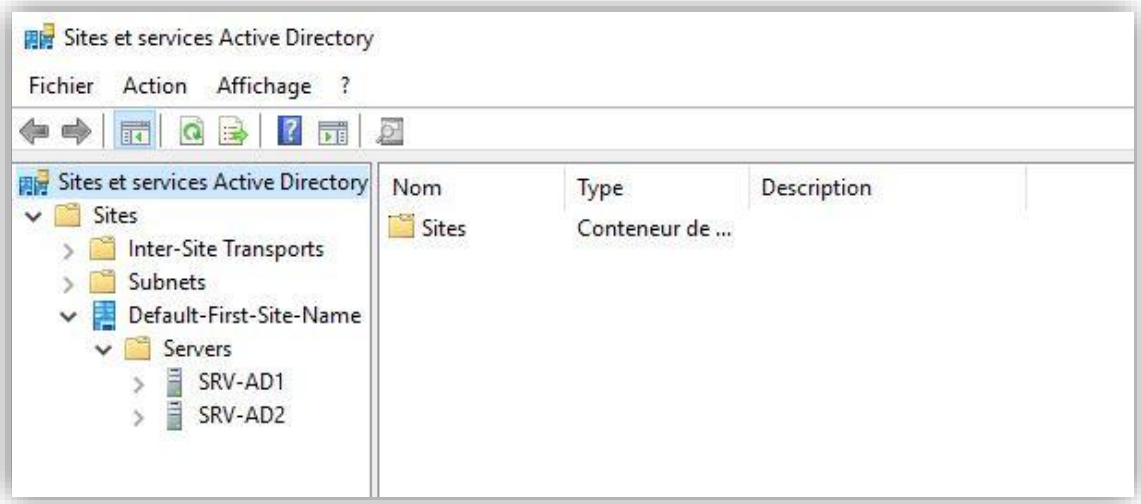


- Cliquer sur ***installer*** :



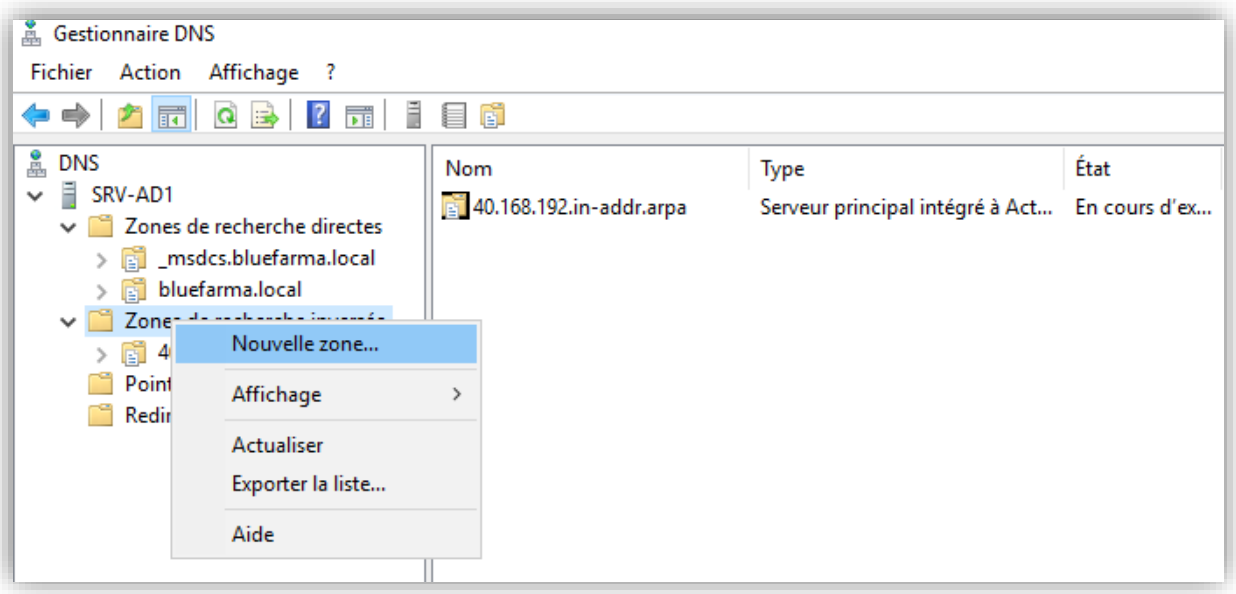
NB : Au redémarrage de SRV-AD2, c'est le mot de passe Administrateur de SRV-AD2 qui est demandé.

- Terminer en vérifiant depuis le gestionnaire ***Sites et services Active Directory*** que l'on peut accéder à l'annuaire Active Directory depuis le second contrôleur de domaine (DC2) :

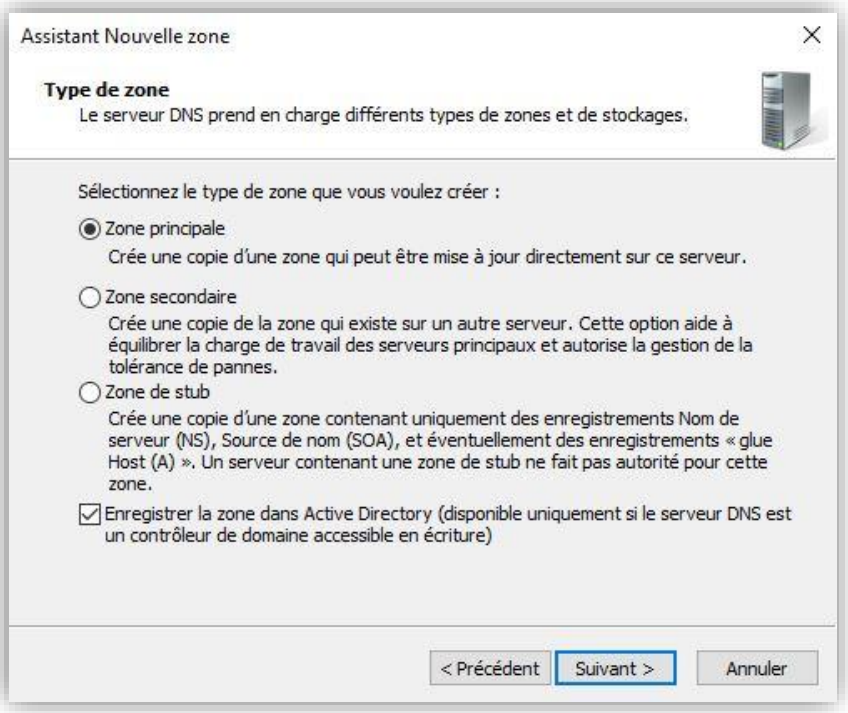


9.1.3. Configuration du DNS

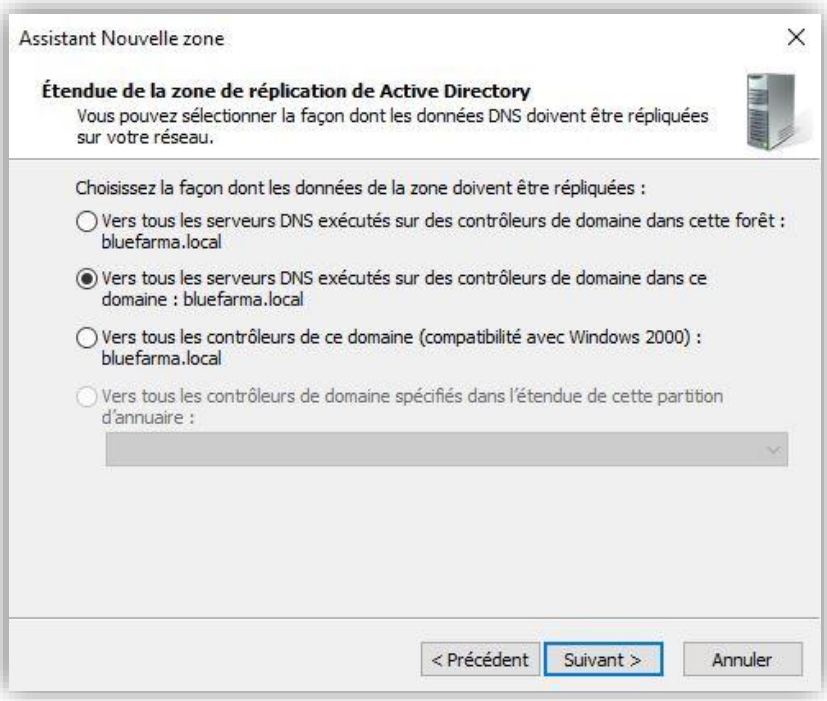
- Se rendre dans le ***Gestionnaire DNS*** puis faire un clic-droit sur ***Zones de recherche inversée*** puis ***Nouvelle zone…*** *:*



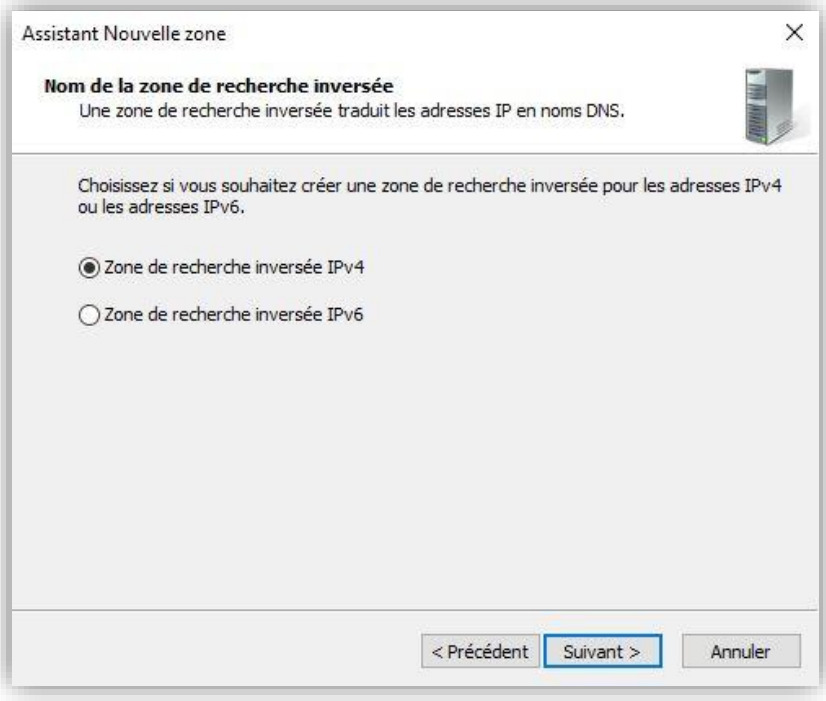
- Dans l'***Assistant Nouvelle zone***, sélectionner ***Zone principale*** :



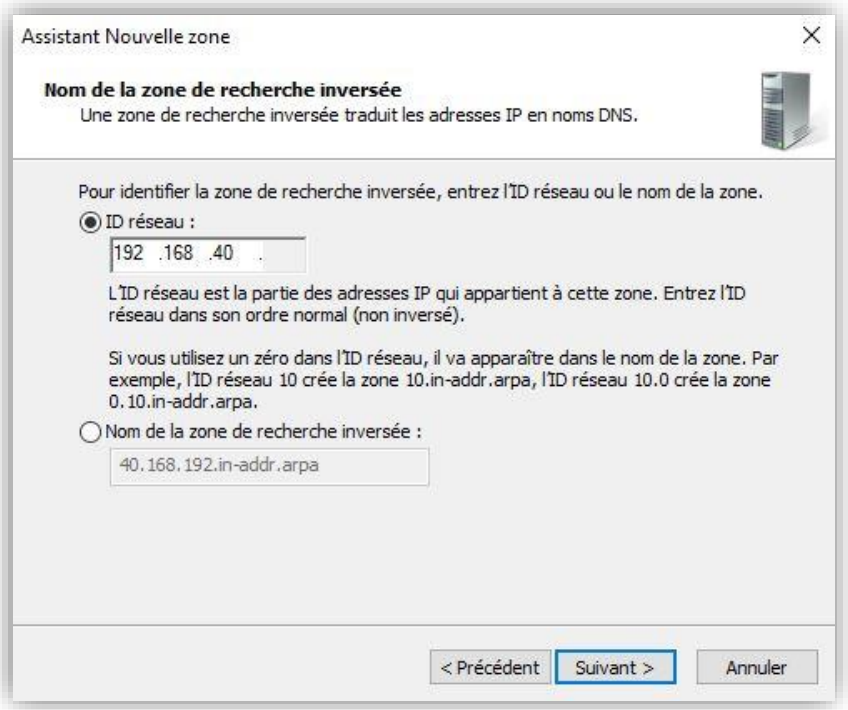
- À La fenêtre suivante, sélectionner la seconde option :



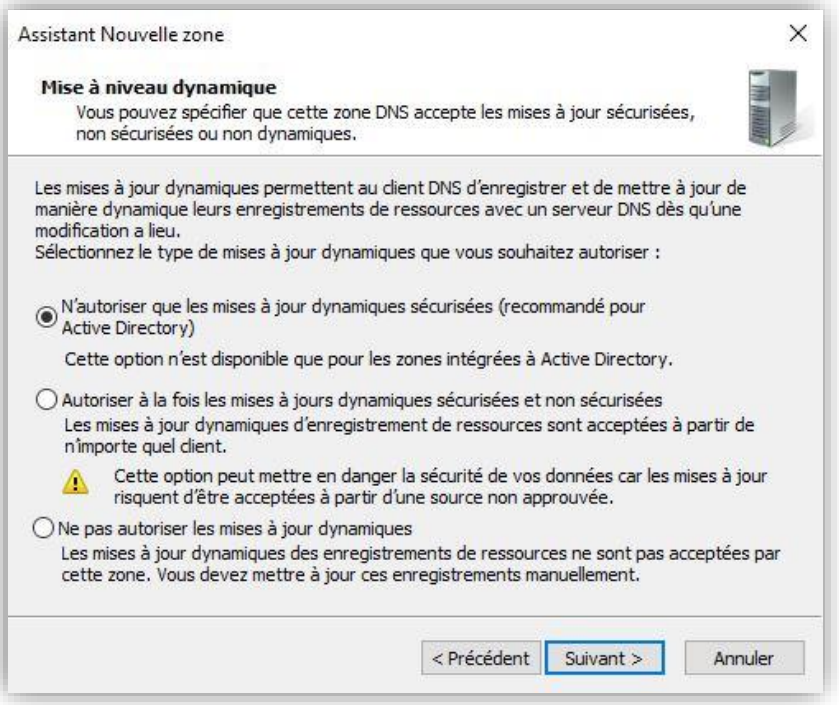
- La zone de recherche inversée s'effectuera en IPv4 :



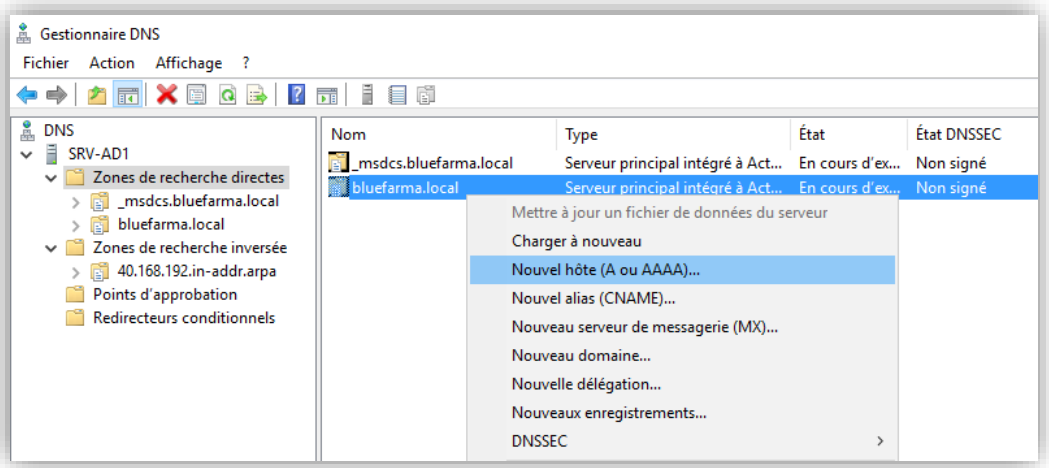
- Renseigner l'***ID réseau*** suivant : **192.168.40** :



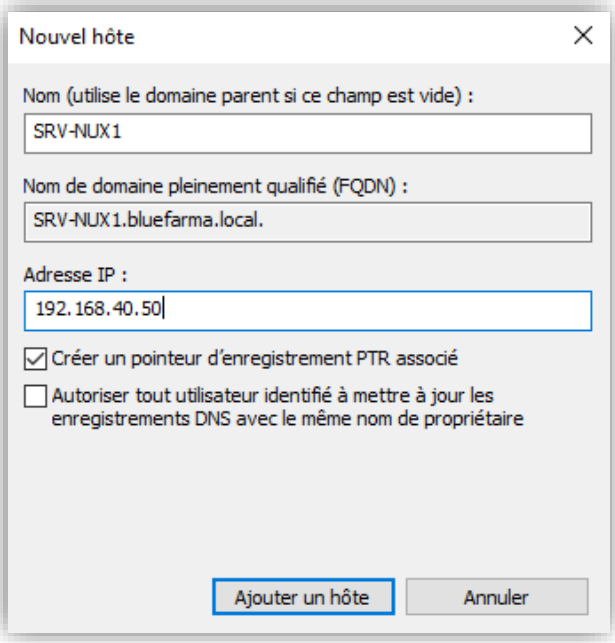
- Autoriser que cette zone DNS accepte des mises à jour dynamiques et sécurisées :



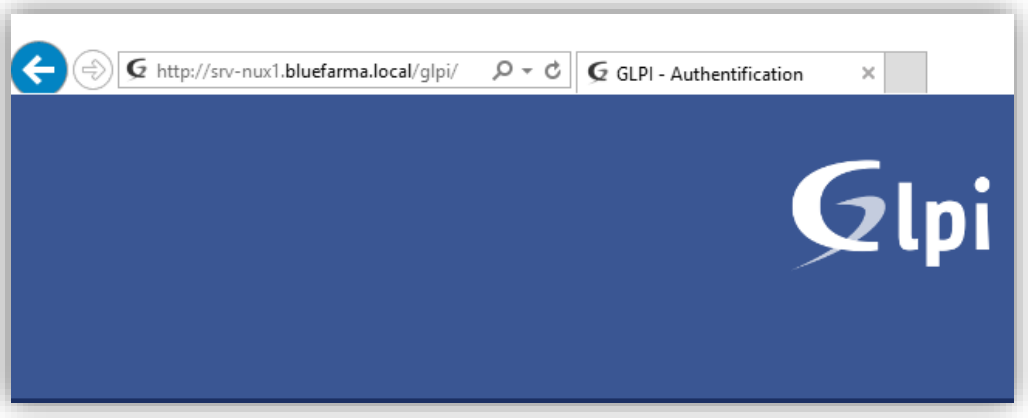
- On peut à présent se rendre dans ***Zones de recherche directes*** afin d'ajouter un ***Nouvel hôte (A)*** dans le fichier de zone de recherche **bluefarma.local** :



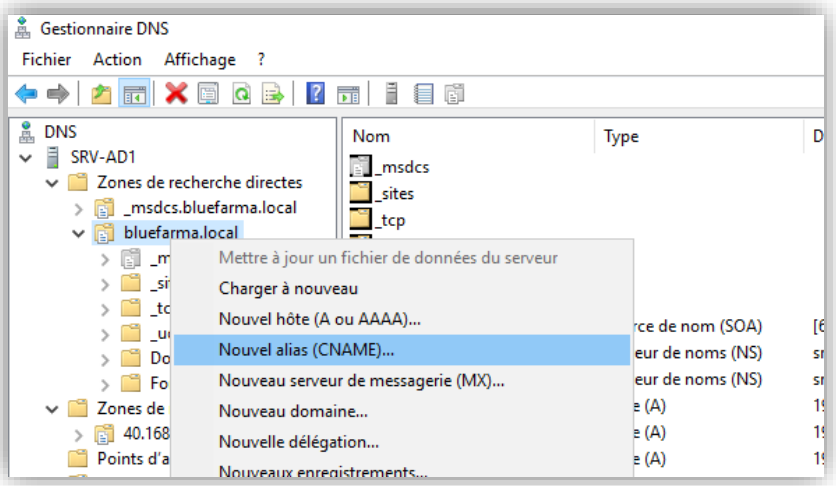
- Renseigner le nom d'hôte de la machine que l'on souhaite (**SRV-NUX1**) ajouter dans la ***fenêtre Nouvel hôte*** ainsi que son adresse IP (192.168.40.50) :

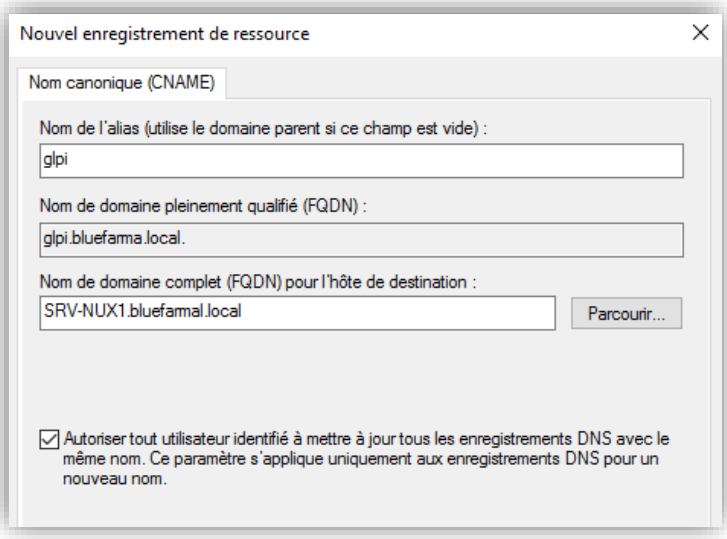


- Nous vérifions que le nom d'hôte s'est bien lié avec le nom de domaine en lançant le navigateur :



- Nous avons la possibilité de créer un ***Nouvel alias (CNAME)*** afin de rendre le nom du lien plus explicite que le nom d'hôte de la machine. Renseigner le nom de l'***alias*** ainsi que ***le nom de domaine complet (FQDN)*** puis valider :

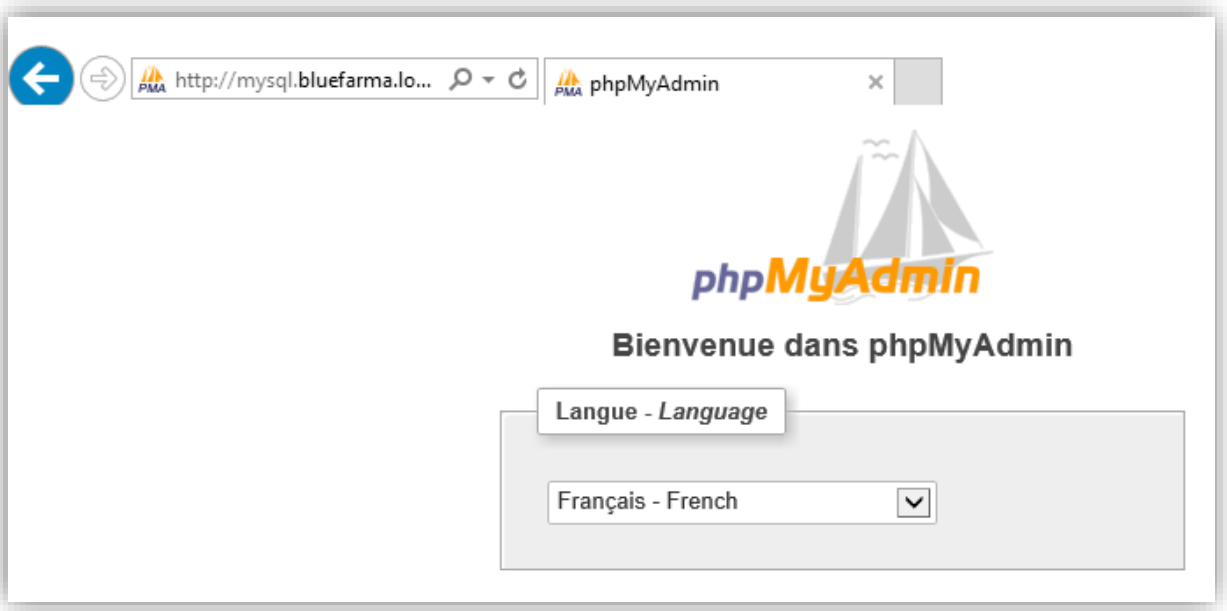




- Nous constatons à présent que l'alias "**glpi.bluefarma.local**" a bien été pris en compte dans le navigateur :

NB : si la résolution de l'alias ne fonctionne plus, effectuer depuis le terminal un `ipconfig /flushdns`.

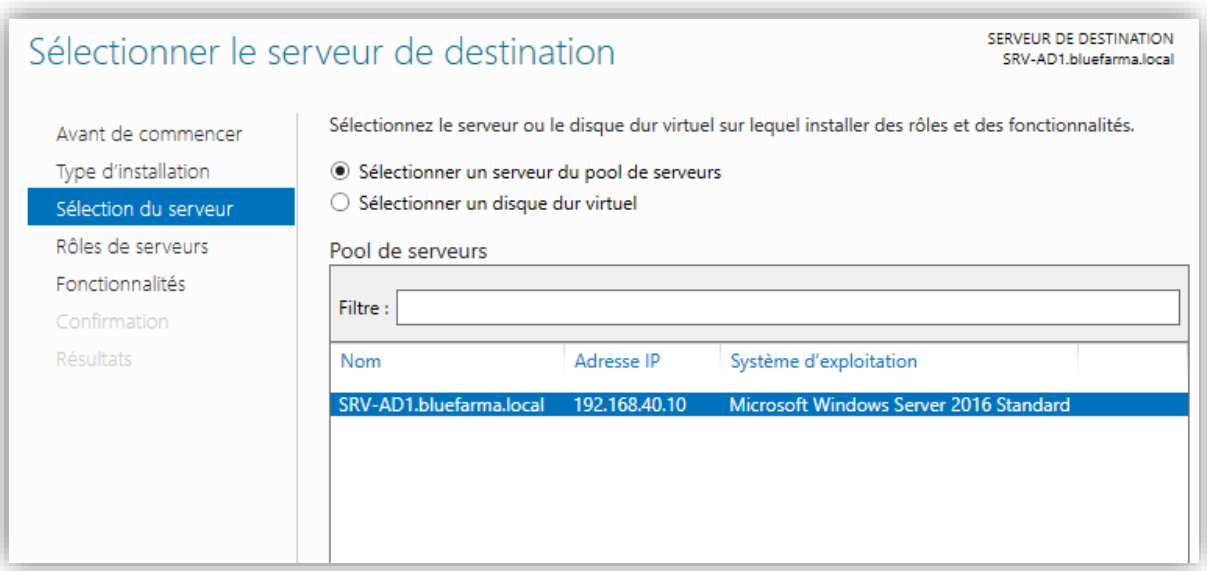
- En suivant la même procédure, un second alias a été créé pour accéder à la base SQL avec l'adresse mysql.bluefarma.local/phpMyAdmin :



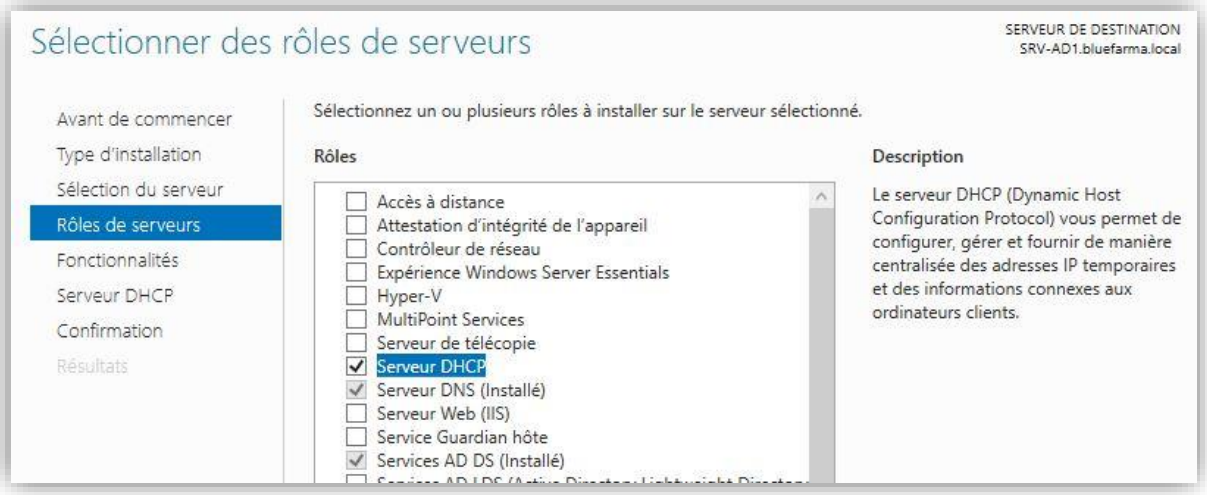
9.1.4. Serveur DHCP

Installation du serveur DHCP

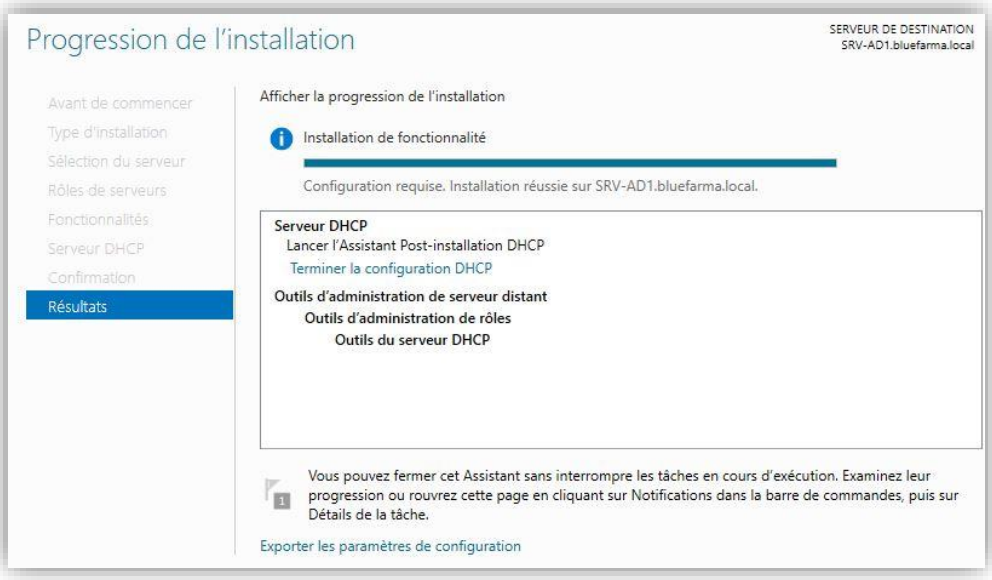
- Comme pour les installations de rôles, on passe par le ***Gestionnaire de serveur***, on fait ensuite ***Ajouter des rôles et des fonctionnalités*** puis on reste sur une ***Installation basée sur un rôle ou une fonctionnalité***.
- Sélectionner le ***serveur de destination*** :



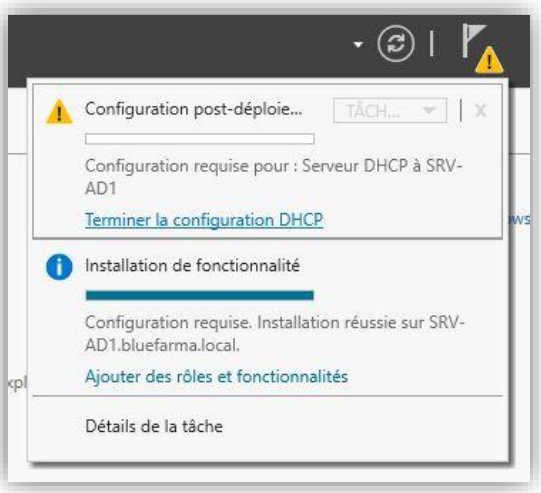
- Ajouter le rôle ***Serveur DHCP*** en sélectionnant la case :

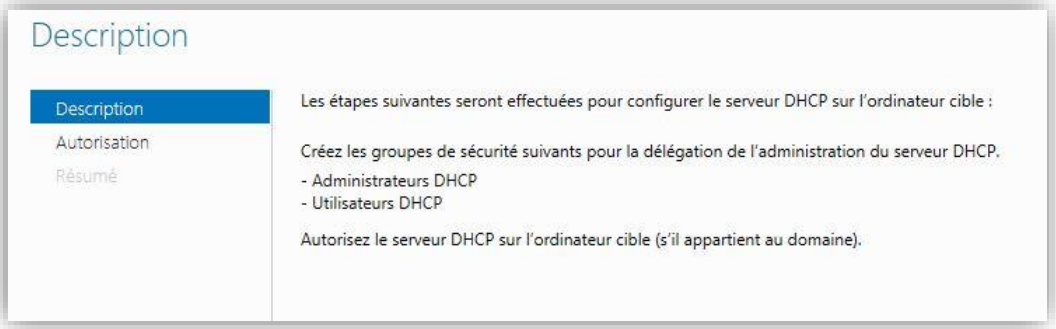


- Cliquer sur ***Installer*** une fois arrivé dans la fenêtre de confirmation :

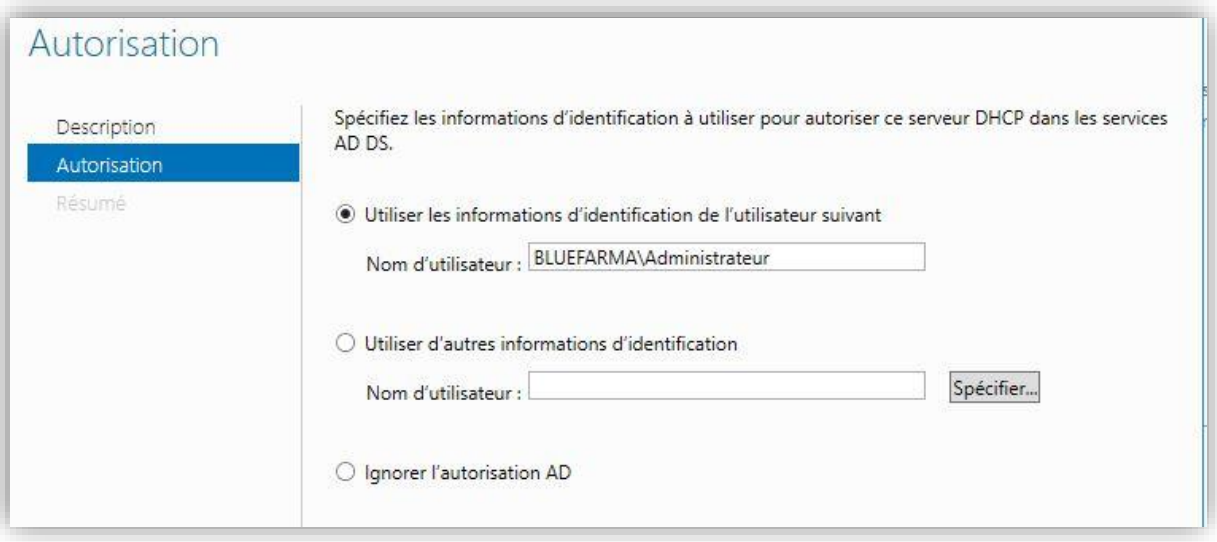


- Retourner dans le Gestionnaire de serveur, cliquer sur le drapeau de notification puis sur ***Terminer la configuration DHCP*** :
- L'assistant de ***Configuration post-installation DHCP*** se lance :

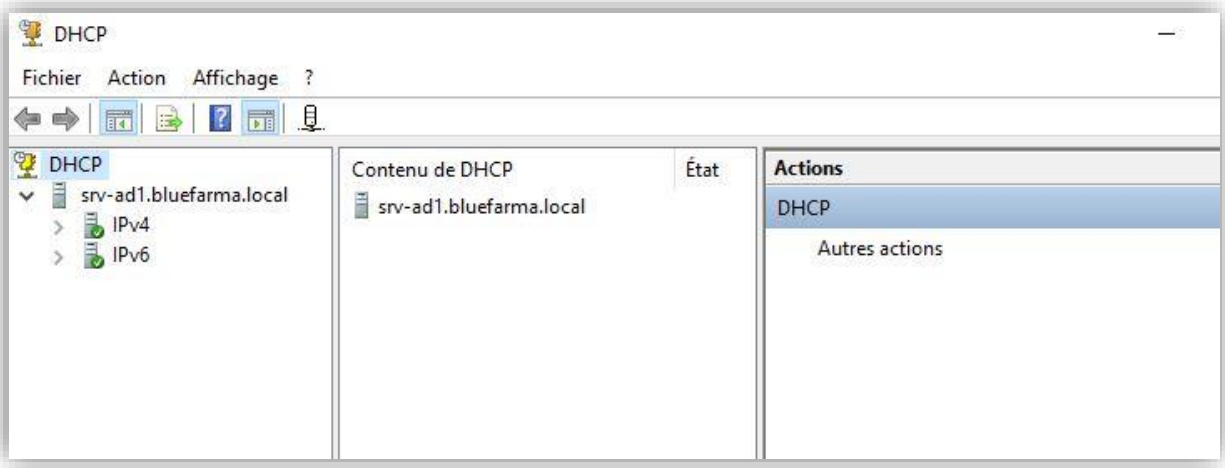




- ***Valider*** cette étape concernant les autorisations d'identification pour l'utilisation du serveur AD :

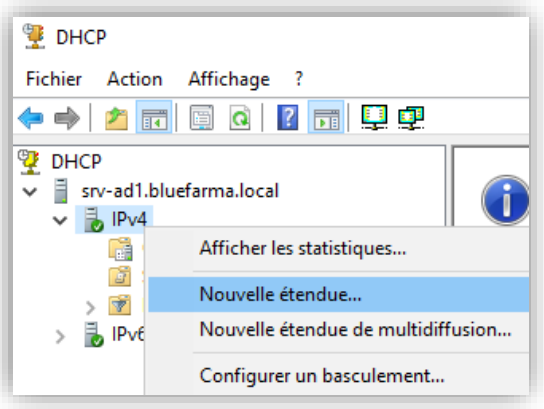


- Vérifier dans ***Outils d'administration*** que le rôle s'est bien installé en double-cliquant sur ***DHCP*** :

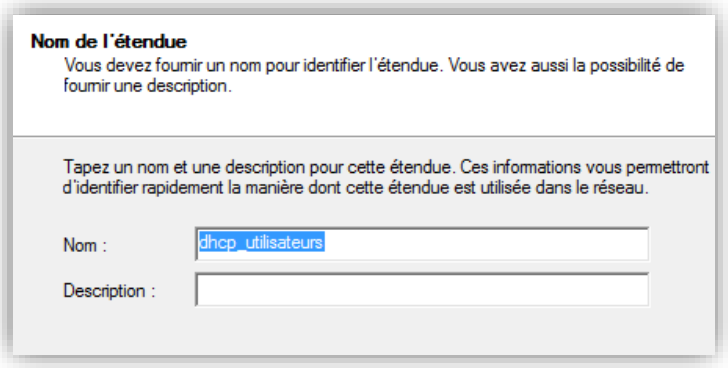


Configuration d'une étendue DHCP

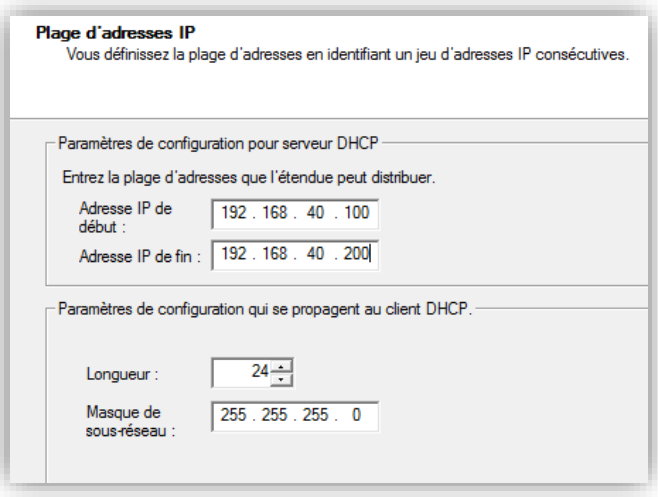
- Se rendre dans l'assistant **DHCP**. Dans l'arborescence à gauche, déplier DHCP > srv-ad1.bluefarma.local > IPv4 puis faire un clic droit sur IPv4 :



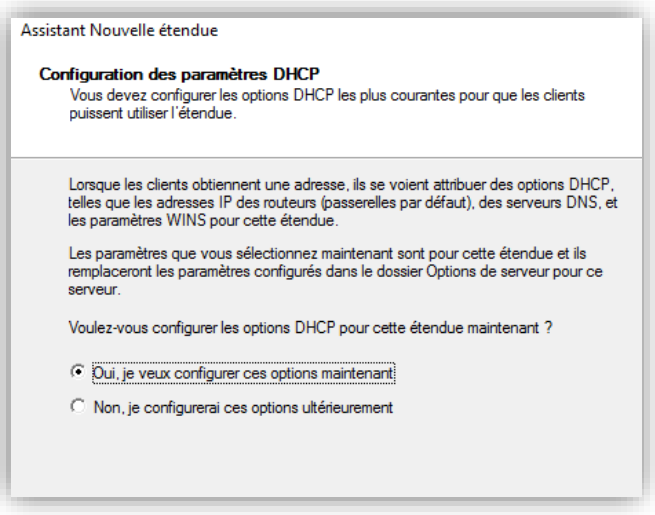
- L'***Assistant Nouvelle étendue***. Faire suivant puis renseigner un nom pour notre étendue dans la fenêtre suivante. Nous l'appellerons ici "dhcp_utilisateurs" :



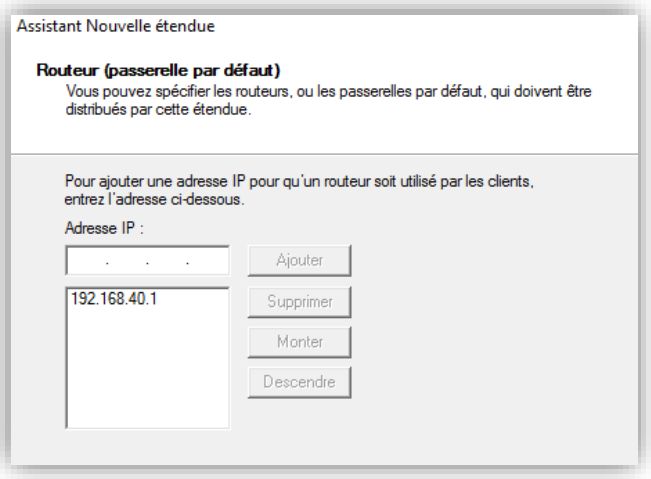
- Définir une plage d'adresses entre 192.168.40.100 et 192.168.40.200 : l'étendue DHCP distribuera dynamiquement ces adresses aux postes clients :



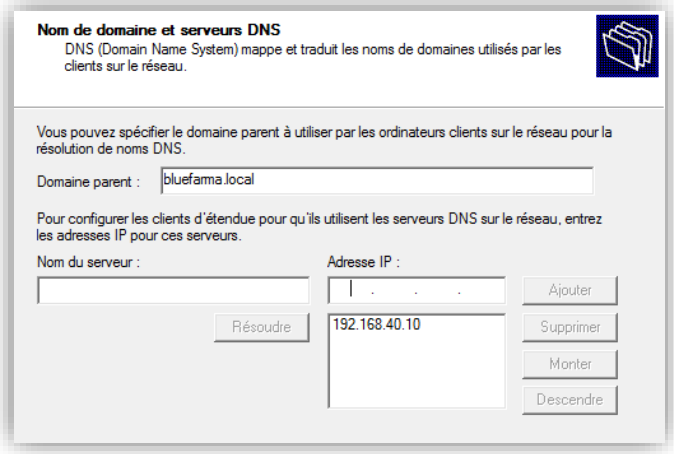
- Nous ne renseignons pas d'exclusion d'adresses et laissons la durée du bail par défaut. Configurer les options ainsi définies lorsqu'on nous le propose :



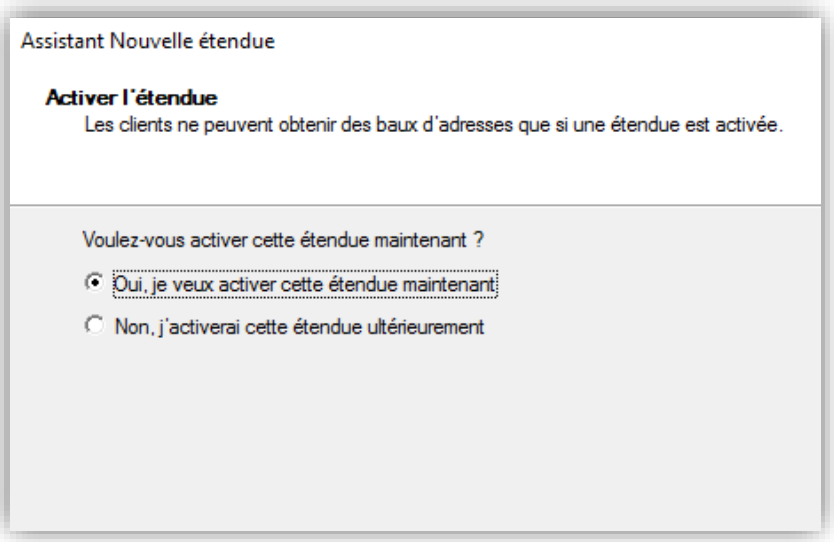
- Indiquer l'adresse IP de la passerelle par défaut puis cliquer sur ***Ajouter*** :



- Par défaut, le nom de domaine parent indique **bluefarma.local**. Laisser tel quel puis valider :



- Ne rien changer dans la fenêtre évoquant le serveur WINS. Finaliser la configuration et activer l'étendue :

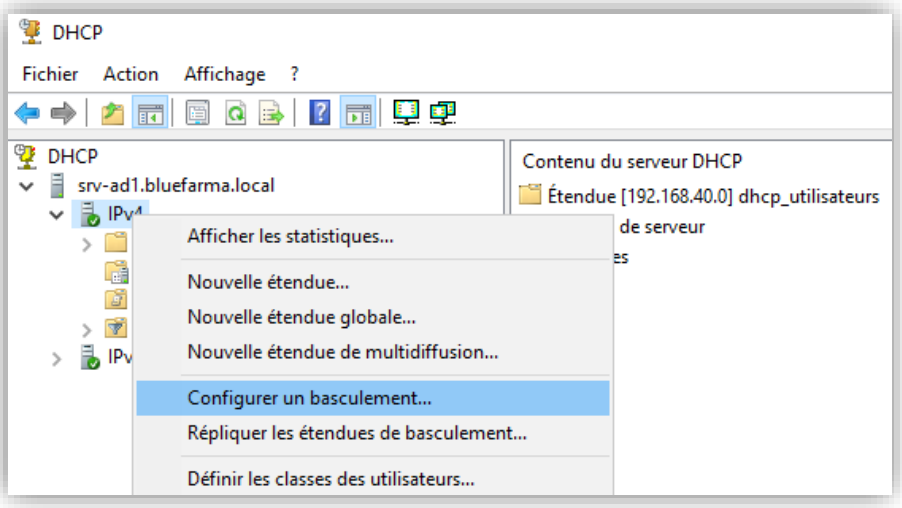


9.1.5. Réplication avec DHCP Failover

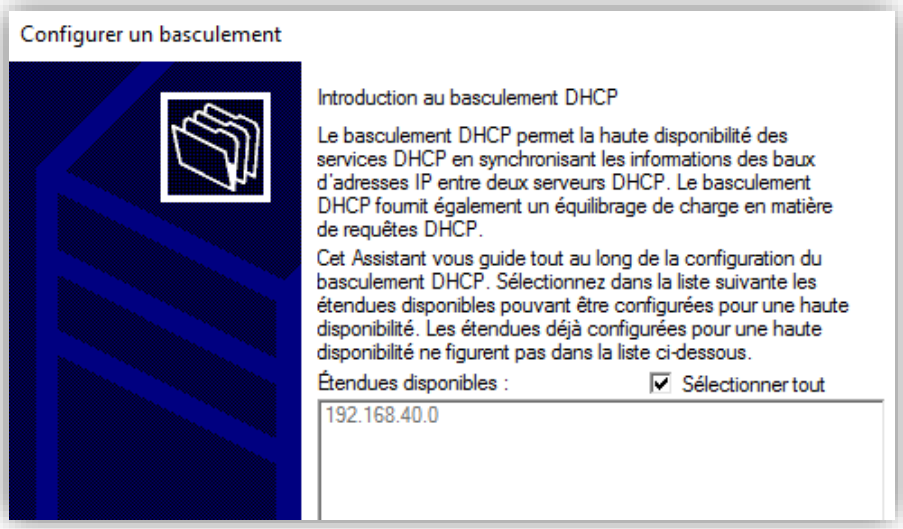
Prérequis :

- Le service DHCP doit être installé sur le serveur partenaire (SRV-AD2).
- Au moins une étendue doit être présente sur l'un des deux serveurs.
- Les horloges des deux serveurs doivent avoir moins d'une minute d'écart.
- Les deux serveurs ne font pas nécessairement partie du même domaine.

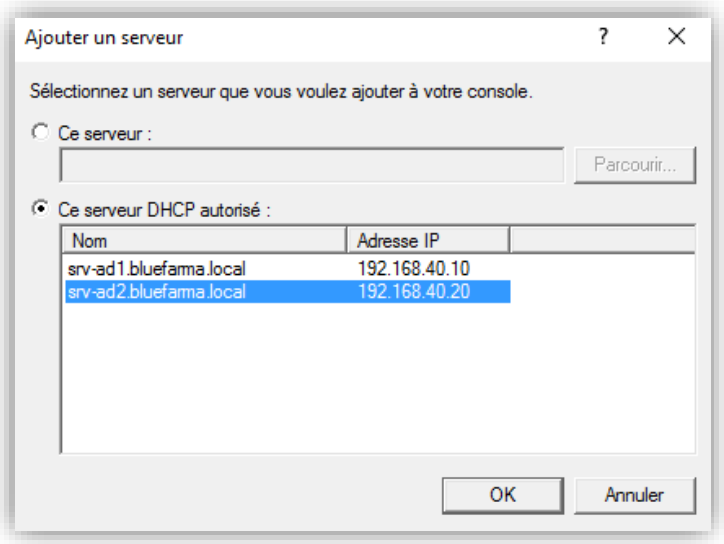
- Dans la machine SRV-AD1, se rendre dans ***Outils d'administration*** puis cliquer sur ***DHCP*** :
- Faire un clic-droit sur IPv4 puis sélectionner ***Configurer un basculement…*** :



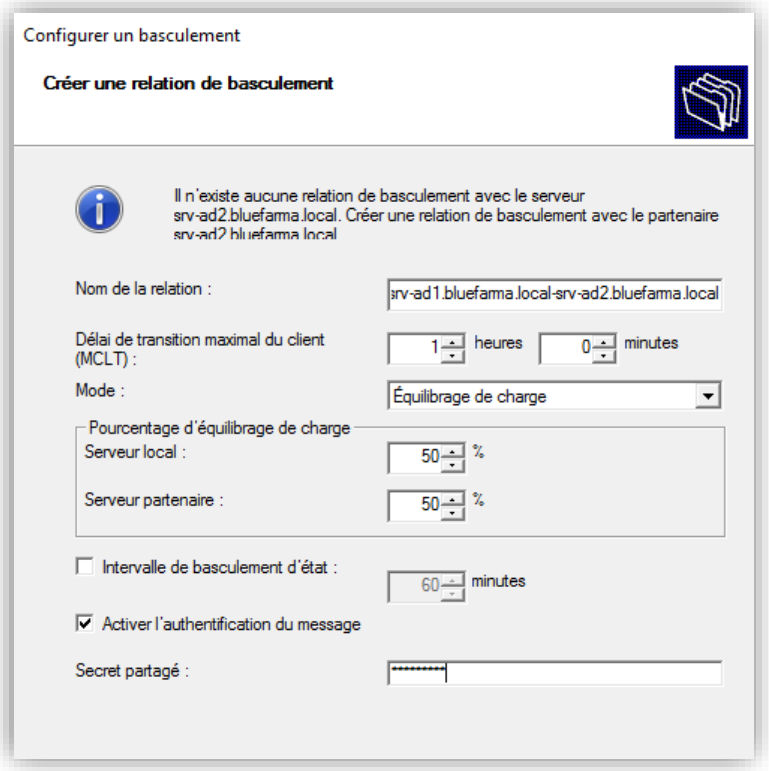
- La fenêtre qui s'affiche présente l'étendue que l'on souhaite répliquer sur l'autre serveur :



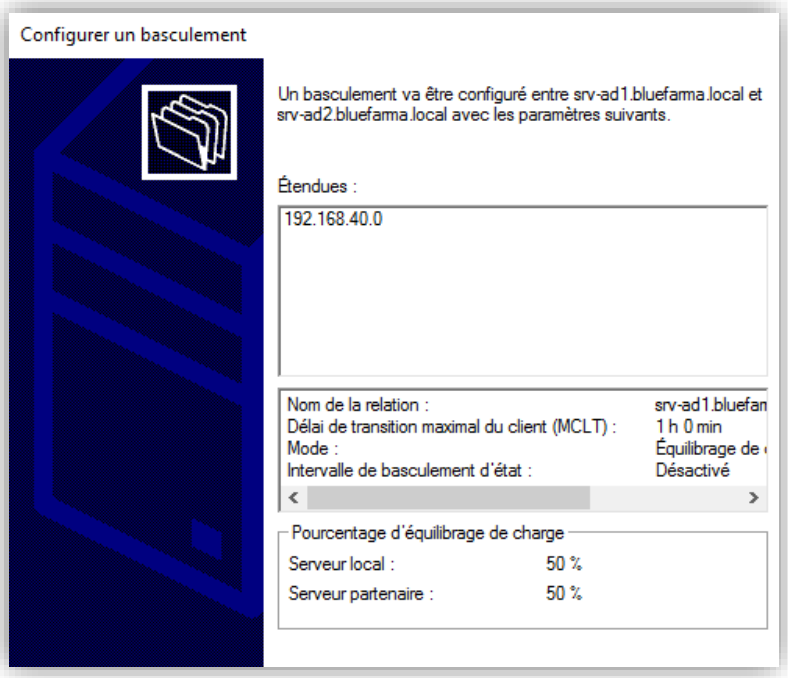
- Renseigner le serveur DHCP partenaire en faisant ***Ajouter un serveur*** puis sélectionner **srv-ad2.bluefarma.local** en tant que ***serveur partenaire*** puis faire suivant :
- Lors de la création de relation de basculement, paramétrer les éléments suivants :



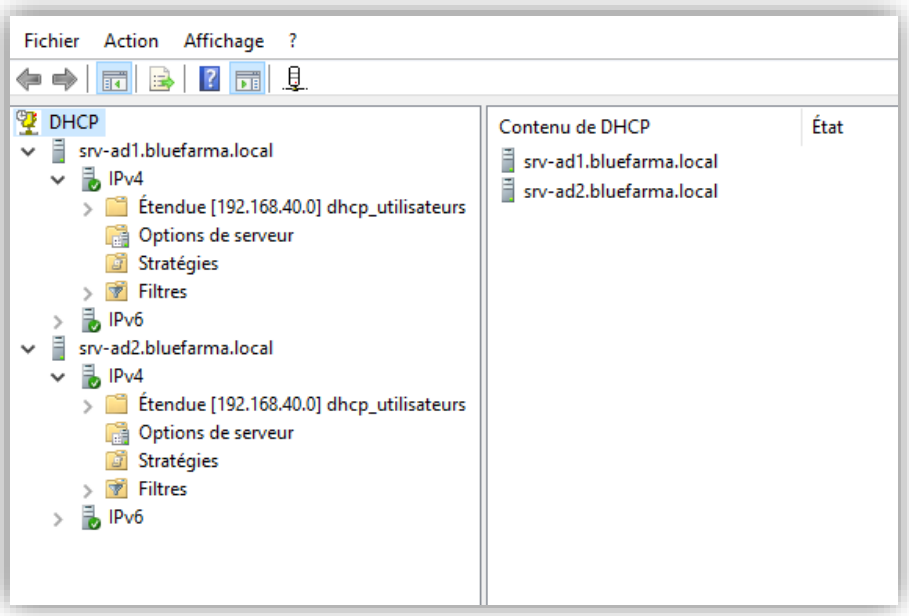
  - Mode ***équilibrage de charge*** : actif/actif.
  - On définit les ***pourcentages d'équilibrage de charge*** selon nos besoins, ici 50/50.
  - Une chaîne de cryptage est sélectionnée dans le champ ***secret partagé***.



- Un résumé de la configuration s'affiche dans la fenêtre suivante avant validation. Cliquer sur ***Terminer*** :



- Se rendre dans la console DHCP sur SRV-AD2 afin de vérifier que la réplication DHCP s'est bien déroulée :



NB : Pour visualiser le second serveur DHCP répliqué on fait ***Action*** > ***Ajouter un serveur …*** > puis chercher SRV-AD1.

9.1.6. Configuration de la réplication DFS

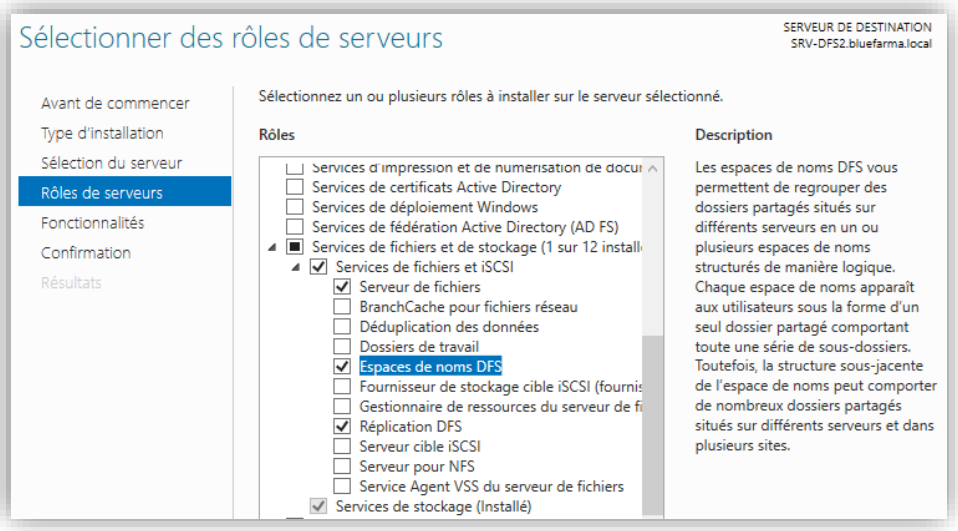
Prérequis :

- Il faut disposer d'au moins 2 machines ou serveurs (3 idéalement).
- Un des serveurs doit disposer d'un Active Directory.
- Les serveurs doivent posséder une IP statique et appartenir au même domaine.

Installation des rôles « Espace de noms DFS » et « Réplication DFS » :

L'installation des deux rôles s'effectue de la même manière sur les machines SRV-AD1, SRV-DFS1 et SRV-DFS2. On procède de la manière habituelle pour installer un rôle en effectuant les tâches suivantes :

- Dans le ***Gestionnaire de serveur***, se rendre dans ***Gérer*** puis cliquer sur ***Ajouter des rôles et des fonctionnalités***.
- Sélectionner ***Installation basée sur un rôle ou une fonctionnalité***.
- Sélectionner le serveur du pool de serveurs proposé.
- Dans Rôles de serveurs, déployer l'arborescence ***Services de fichiers et de stockage*** puis Services de fichiers et ISCSI afin de cocher les rôles ***Espace de noms DFS*** et ***Réplication DFS*** :

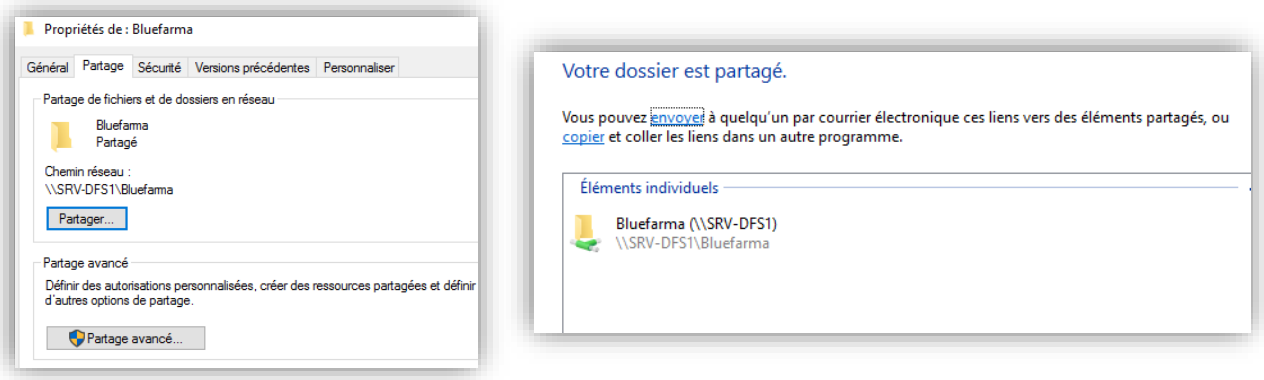


Création des dossiers de partage sur SRV-DFS1 et SRV-DFS2

Le principe consiste à créer des dossiers partagés sur les serveurs de stockage SRV-DFS1 qui seront ensuite répliqués sur SRV-DFS2. Un chemin sera plus tard créé vers ces dossiers depuis l'espace de noms présent sur SRV-AD1.

- Création du dossier **Bluefarma** partagé dans lequel on crée les dossiers communs des différents services (Commun.Direction, Commun.Administratif, Commun.ProduitA, ProduitB, Commun.SAV, Commun.SI) sur le serveur de stockage DFS 1.

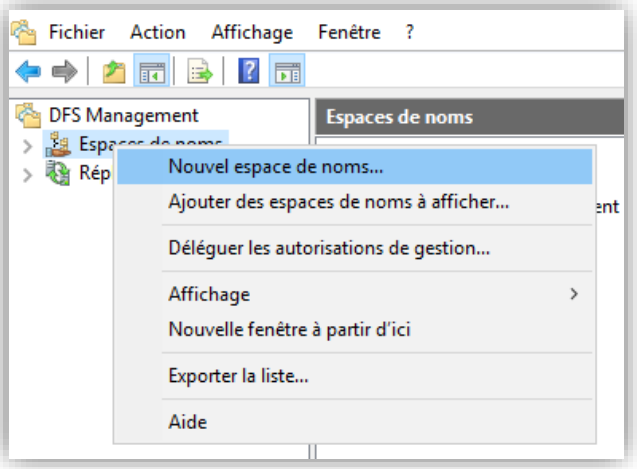
- Clic droit > ***Propriétés*** > onglet ***Partage*** > ***partage avancé***… :



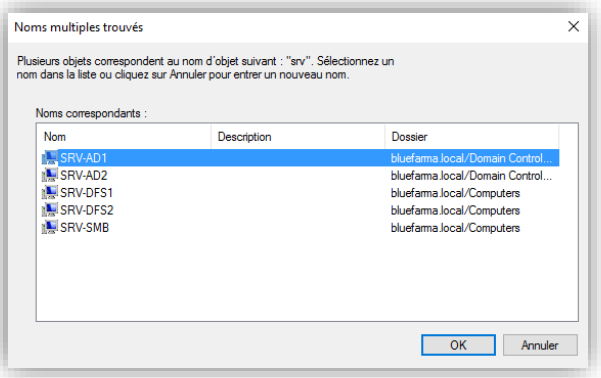
- Cocher partager ce dossier puis Autorisations.

Configuration DFS sur SRV-AD1 :

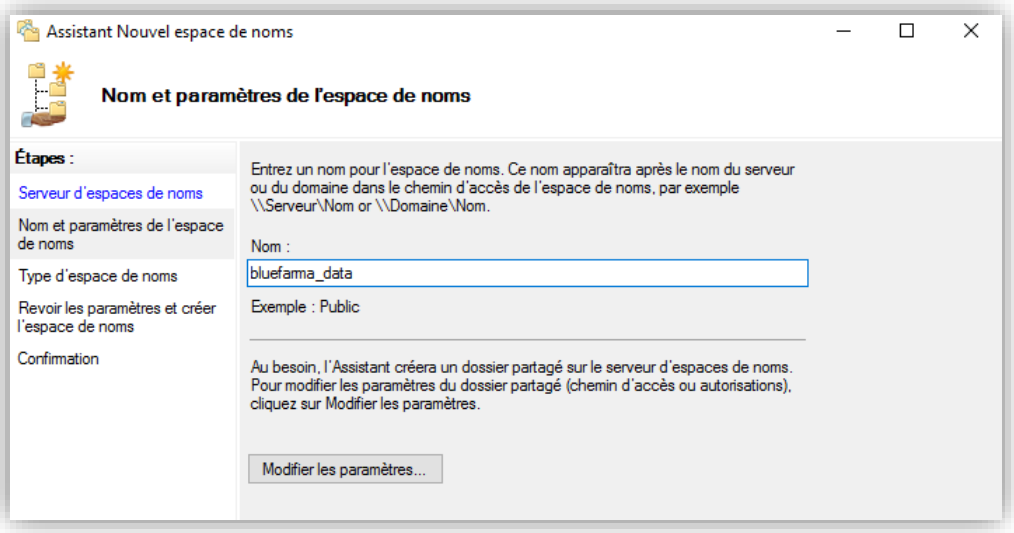
- Lancer ***Gestion du système de fichiers distribués DFS***.
- Clic droit sur Espace de noms puis ***Nouvel espace de noms***.



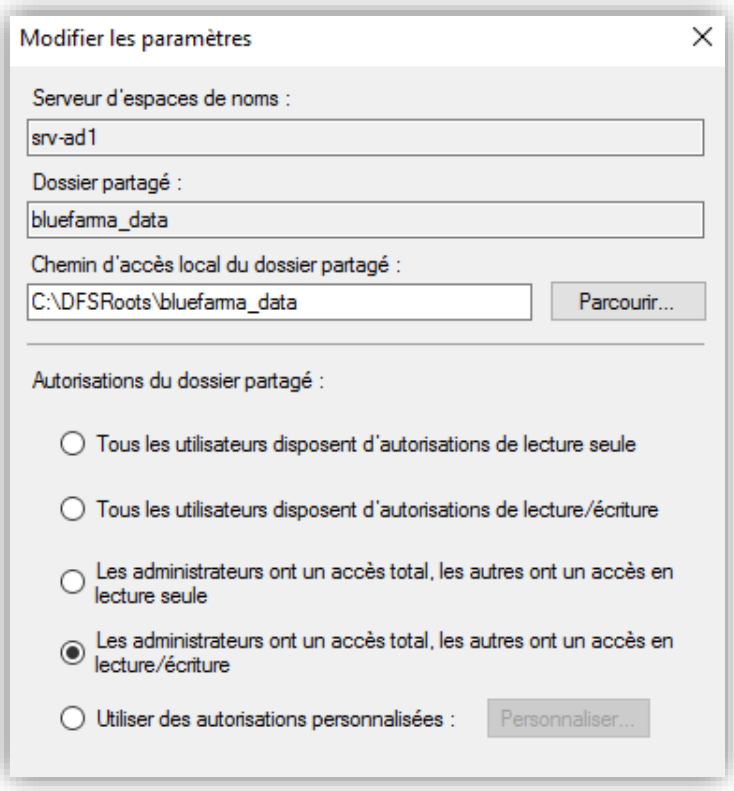
- Choisir un serveur d'espace de noms dans l'assistant qui se lance en cliquant sur parcourir.
- Rechercher ici le serveur qui fera office d'espace de noms, à savoir SRV-AD1 :



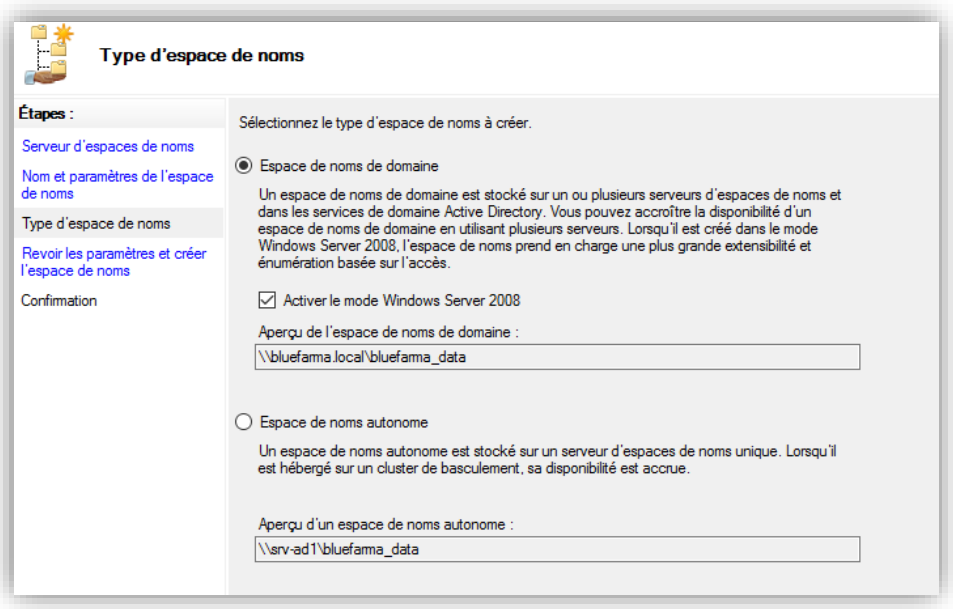
- Renseigner un nom pour notre espace de noms : on le nomme ici « bluefarma_data » puis on clique sur ***modifier les paramètres…*** :



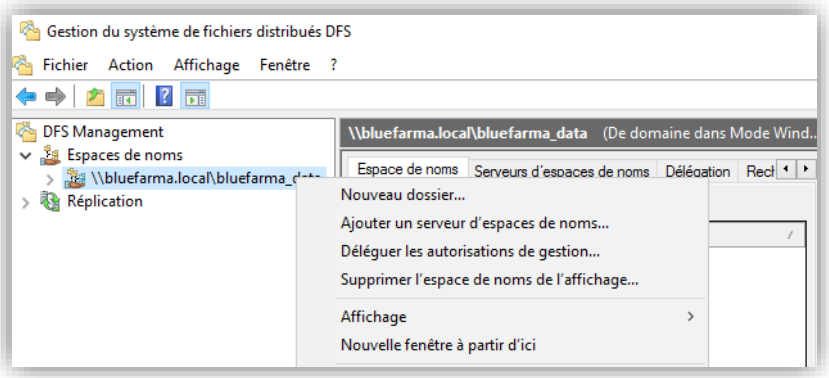
- On détermine un ***accès total*** pour les administrateurs et un accès en lecture/écriture pour les autres.

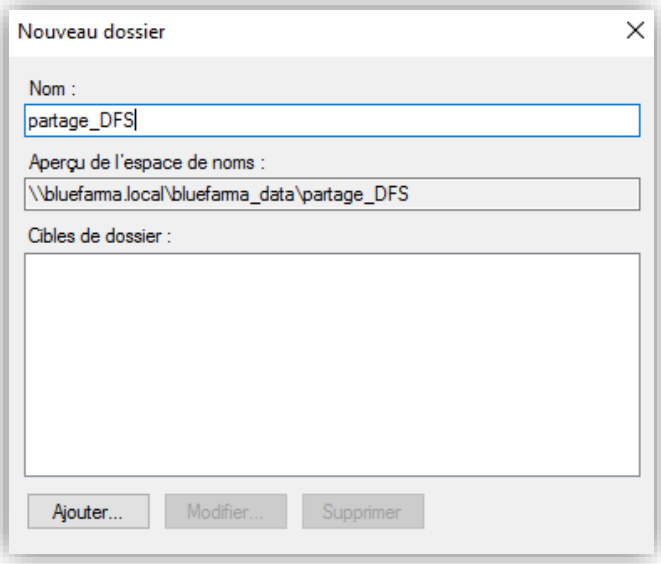


- Sélectionner ***Espace de noms de domaine***, faire ***suivant*** puis ***créer***.

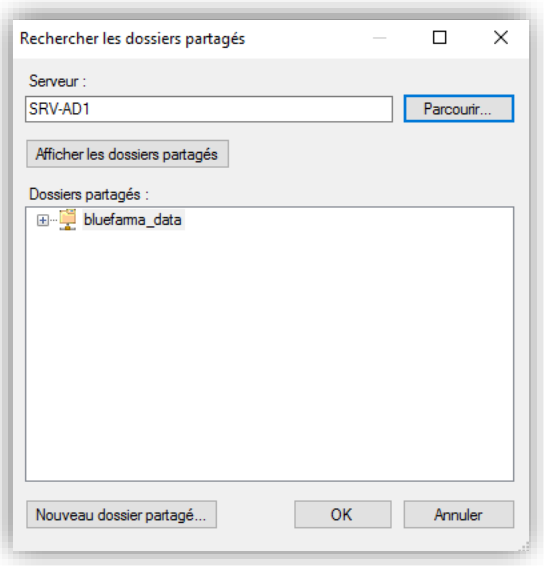


- Créer un dossier à l'intérieur de l'espace de noms en cliquant sur ***Nouveau dossier…*** auquel on donne le nom de « partage_DFS » :

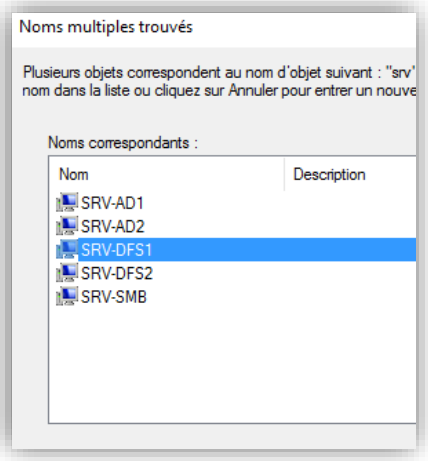


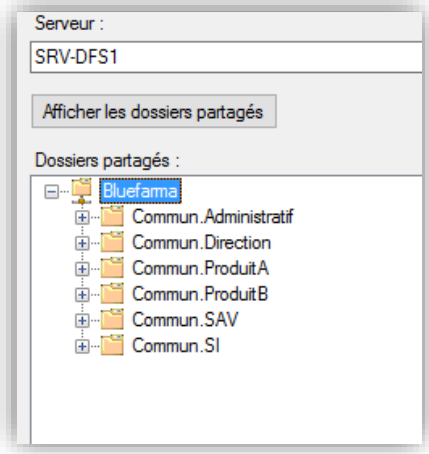


- On va aller chercher les dossiers cibles qui sont partagés sur les serveurs de stockage (DFS1 et DFS2) en faisant ***Ajouter*** puis ***parcourir*** :

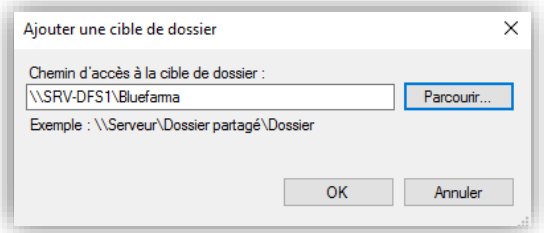


- Une fenêtre ***Rechercher les dossiers partagés*** s'ouvre. Sélectionner ***parcourir*** puis rechercher le serveur de fichiers ***SRV-DFS1*** en s'aidant du bouton ***Vérifier les noms*** :

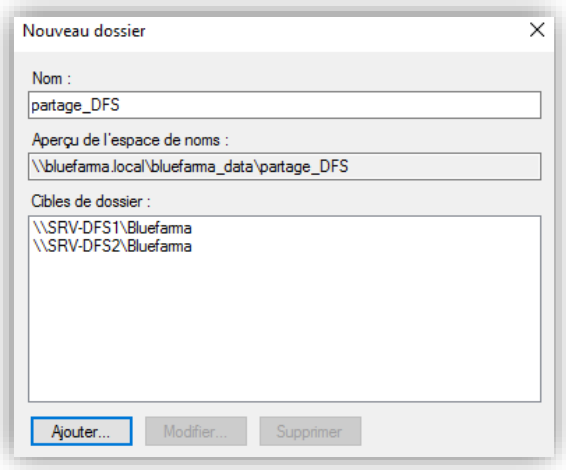




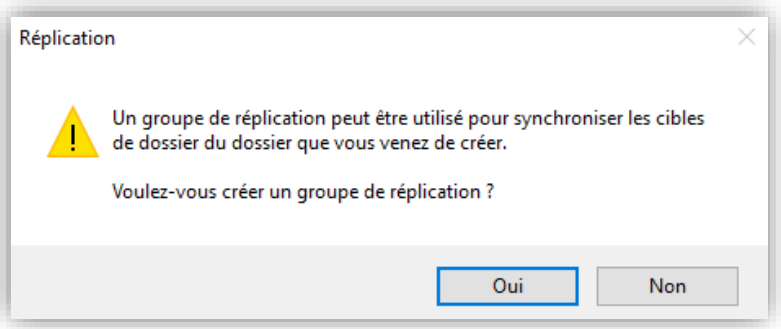
- Sélectionner le dossier partagé sur le serveur de fichiers qui a été créé précédemment dans la fenêtre ***Rechercher les dossiers partagés*** puis confirmer le chemin d'accès du dossier cible \\SRV-DFS1\Bluefarma :



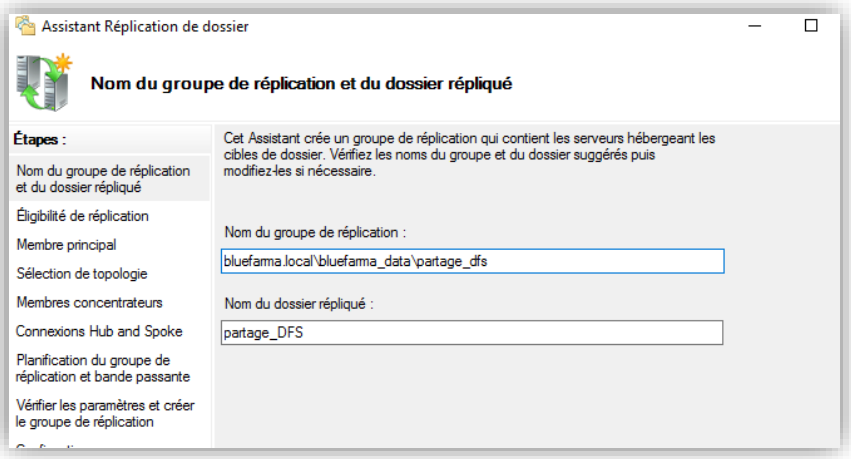
- Réitérer cette opération pour sélectionner le second serveur de fichiers **SRV-DFS2** puis confirmer :



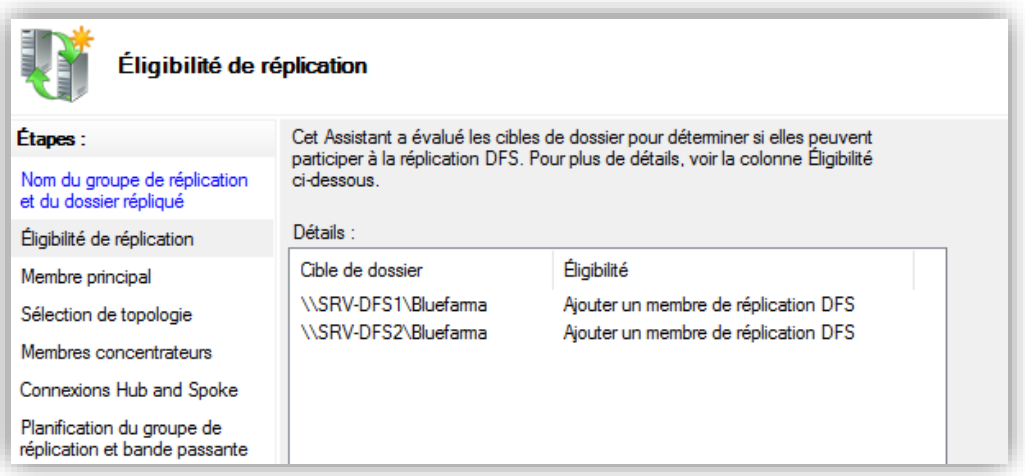
- Accepter lorsque la fenêtre qui s'ouvre nous demande de créer un ***groupe de réplication*** :



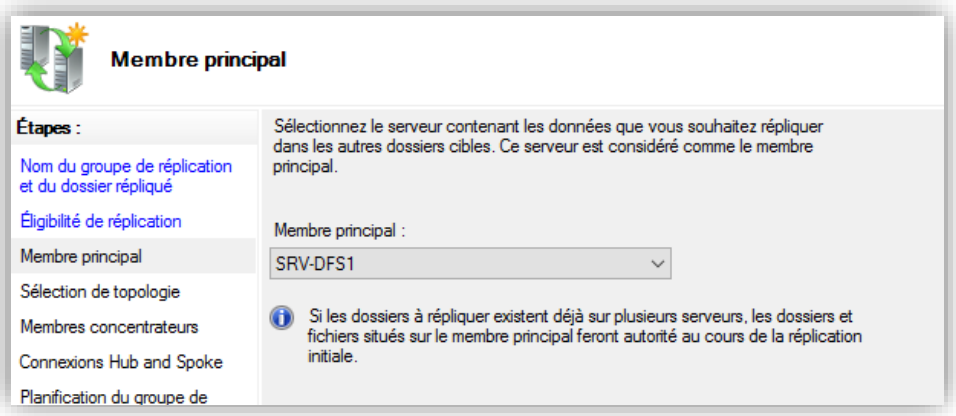
- L'***Assistant Réplication de dossier*** s'ouvre dans une nouvelle fenêtre dans laquelle apparaît le ***Nom du groupe de réplication*** et le ***Nom du dossier répliqué***. Cliquer sur ***suivant*** :



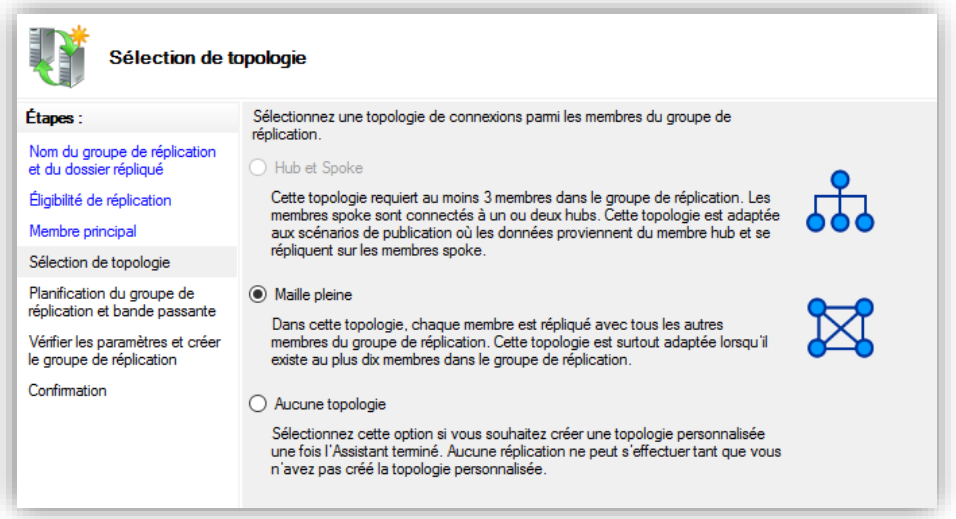
- La fenêtre suivante affiche un récapitulatif des dossiers cibles qui vont être utilisés pour la réplication :



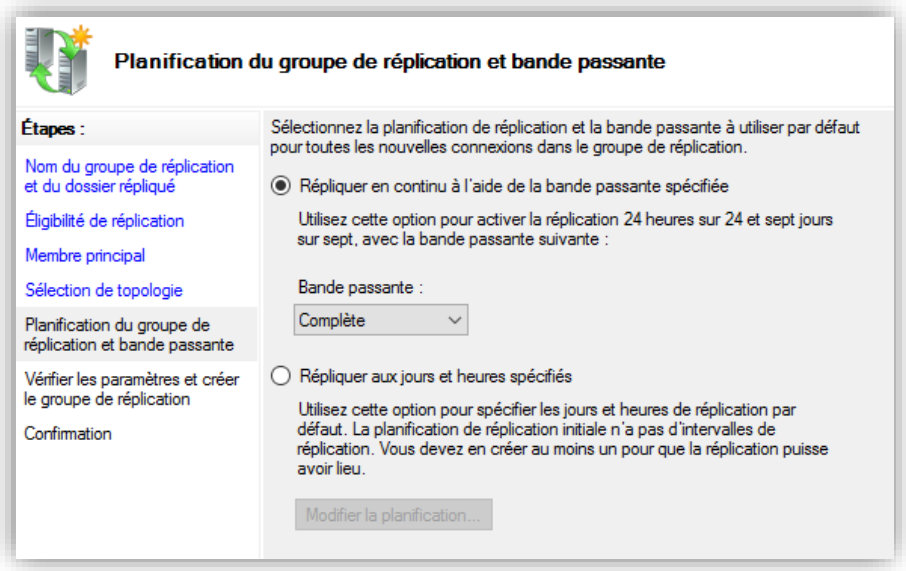
- Choisir le membre principal du groupe de réplication (nous choisissons par convention SRV-DFS1 mais ceci importe peu) :



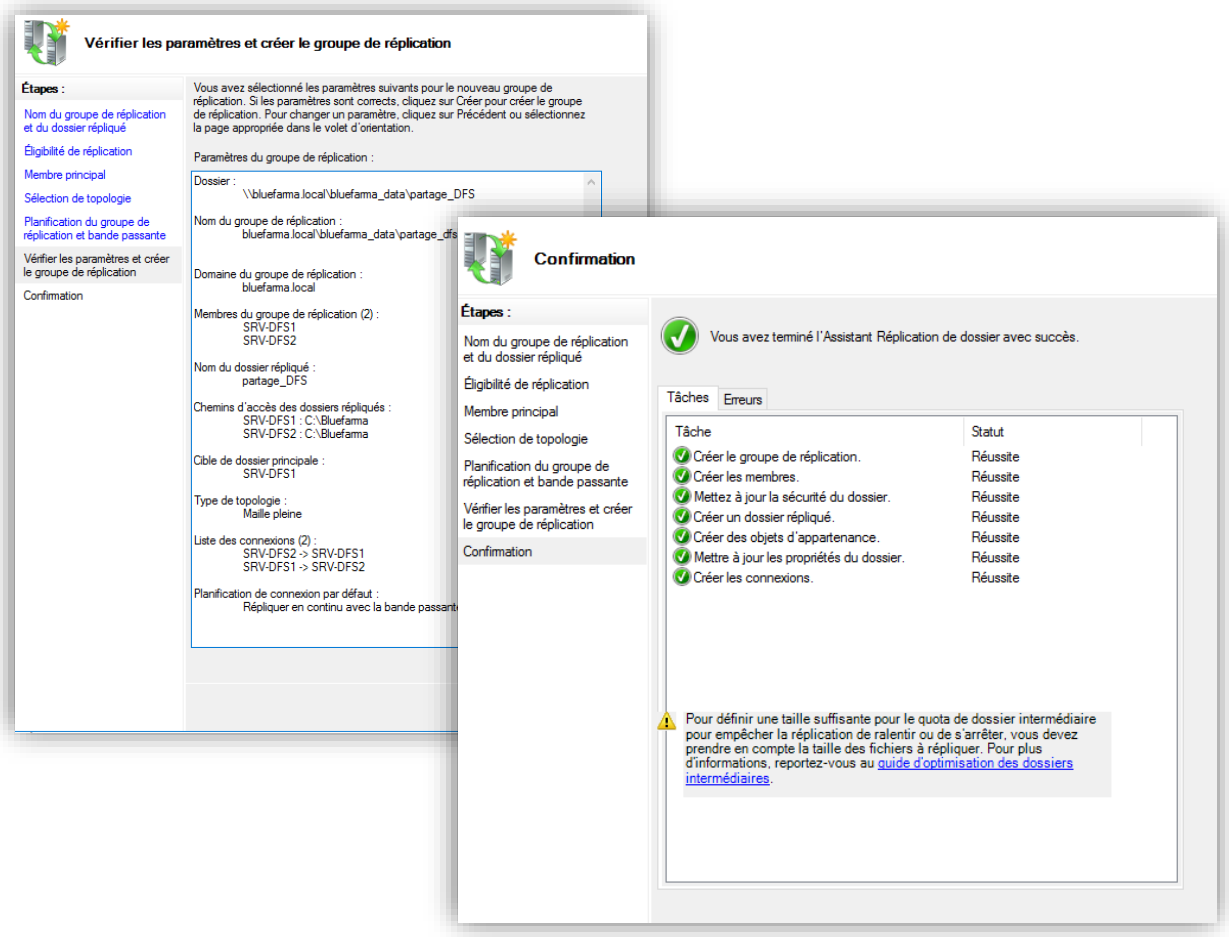
- Lors du choix de la topologie, sélectionner maille pleine :



- Configurer la bande passante avec la planification des horaires de planification. Nous restons sur une réplication 24/24, 7/7 à bande passante pleine :



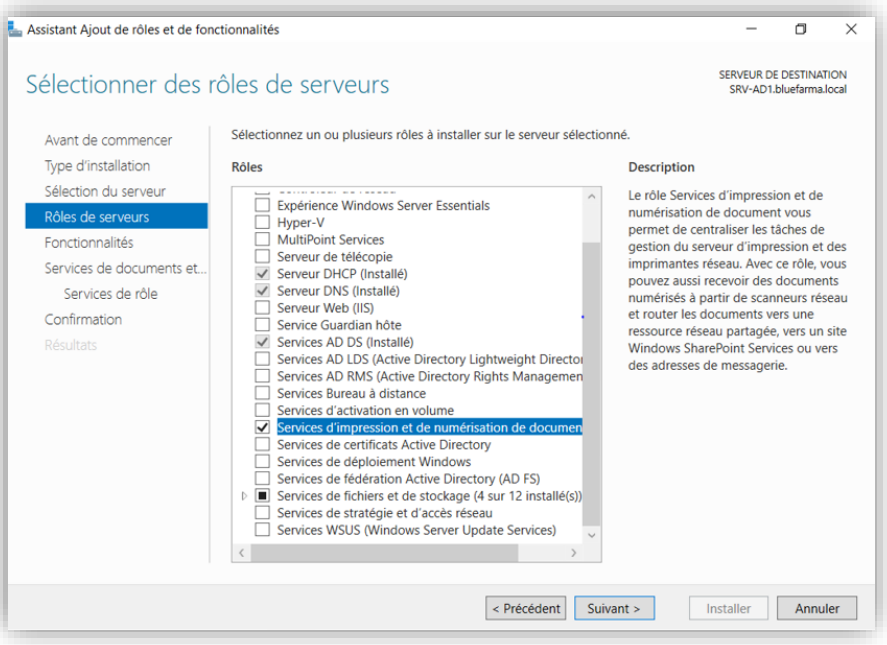
- La fenêtre suivante affiche un récapitulatif des paramètres qui ont été définis avant de créer la réplication :



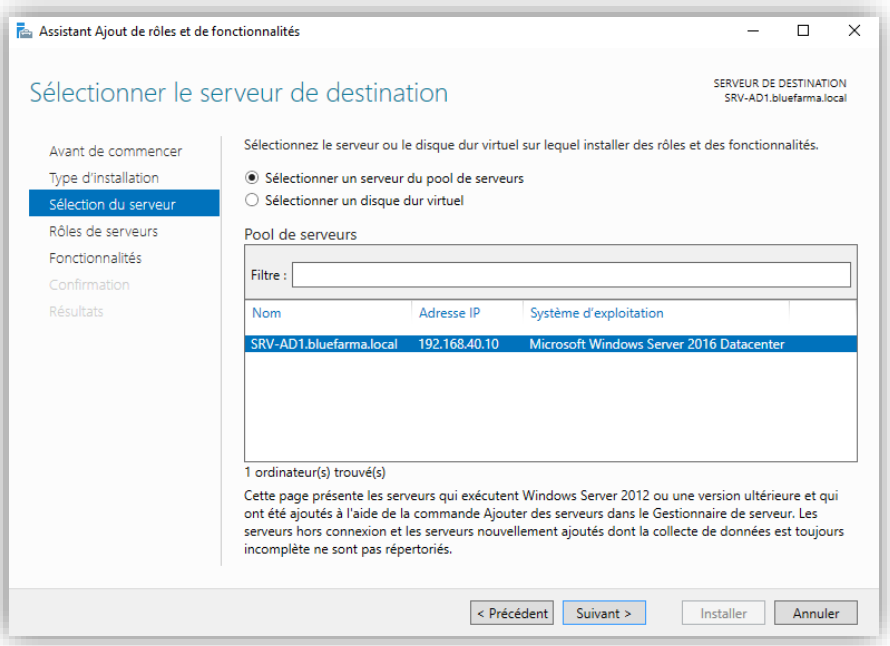
9.1.7. Serveur d'impression

Installation du rôle serveur d'impression

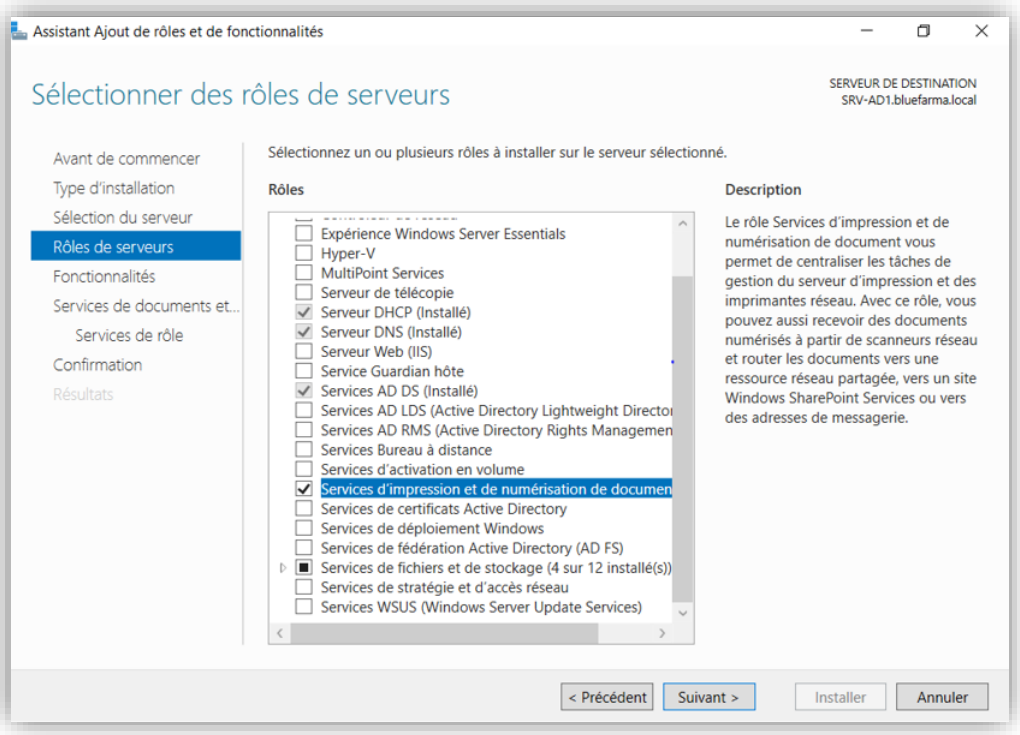
- Depuis le ***Gestionnaire de serveur***, cliquer sur ***Gérer*** puis ***Ajouter des rôles et des fonctionnalités*** :



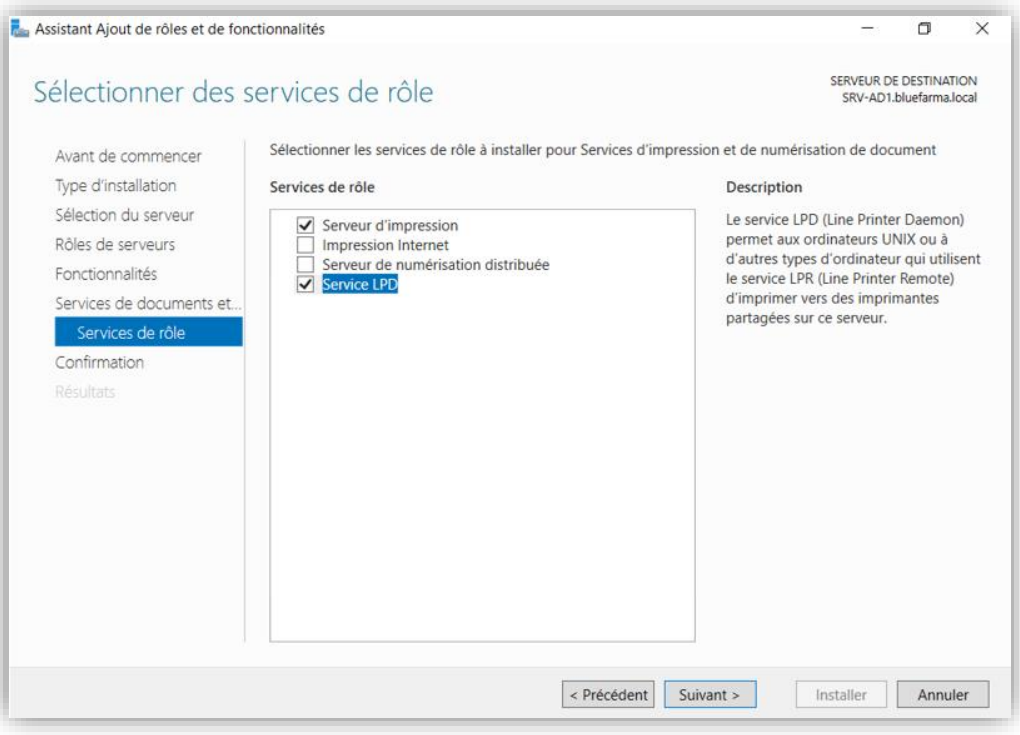
- Après avoir fait suivant dans ***Type d'installation***, sélectionner « ***Installation basée sur un rôle ou une fonctionnalité*** », puis sélectionner le serveur SRV-AD1.bluefarma.local :



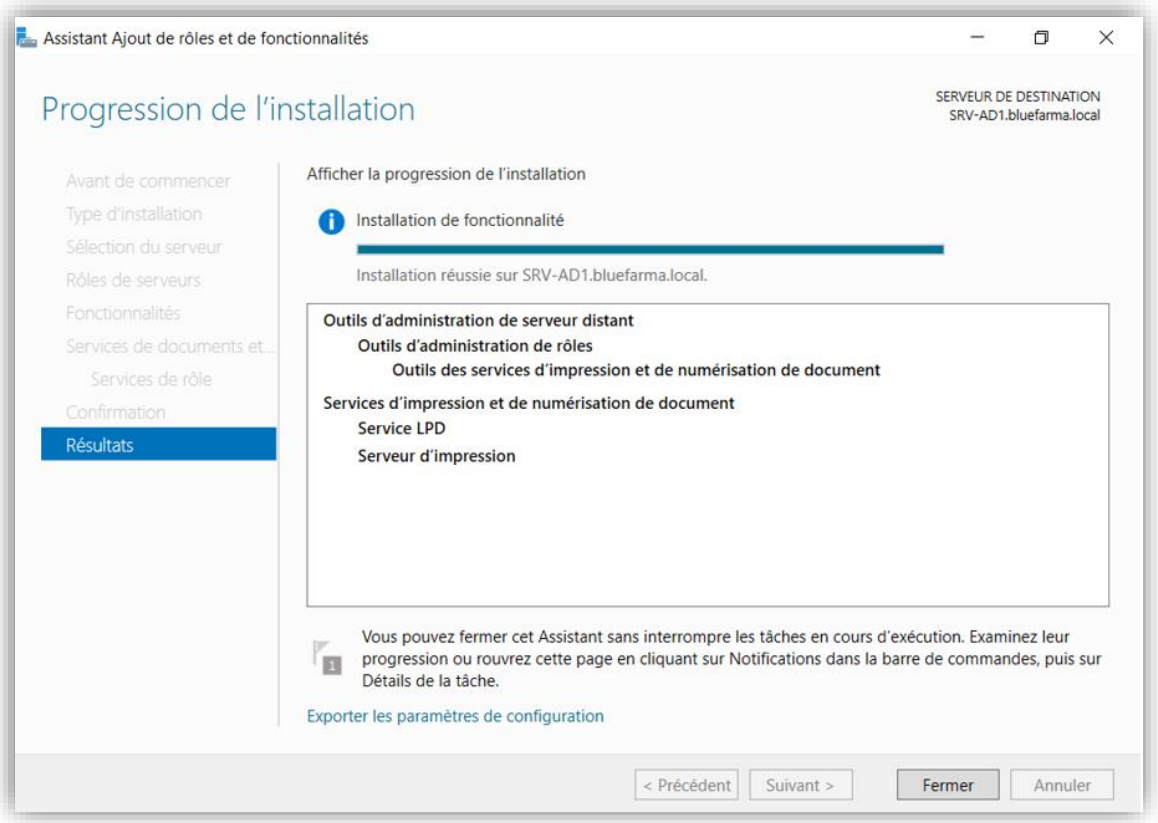
- Sélectionner le rôle ***Services d'impression et de numérisation de document*** puis dans ***Ajouter des fonctionnalités***, faire suivant sans rien sélectionner :



- Faire suivant jusqu'à arriver sur la fenêtre ***Sélectionner des services de rôle*** où rôle d'impression est présélectionné par défaut. Ici, cocher le ***Service LPD*** qui permet aux utilisateurs linux du SAV d'accéder au service d'impression :

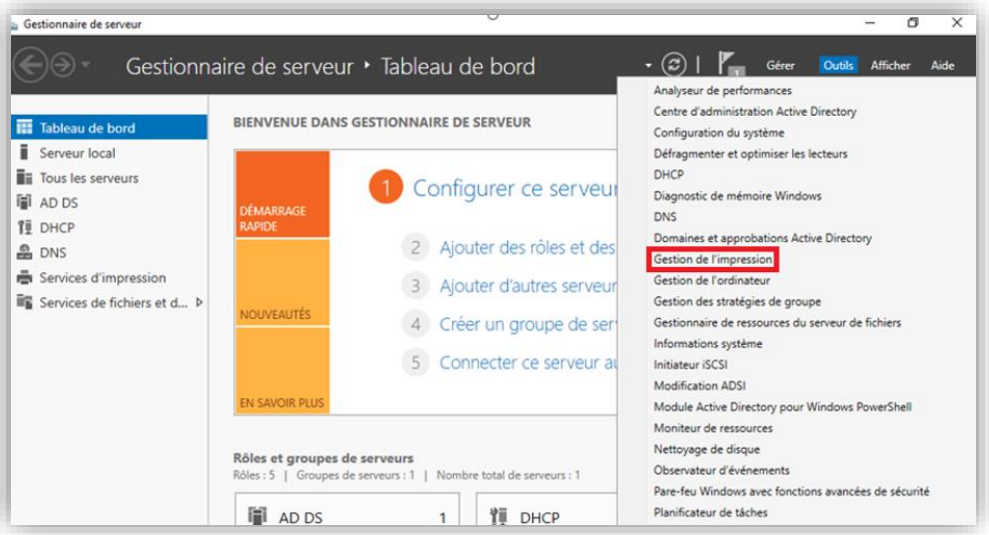


- Cliquer sur ***Installer*** à la page suivante pour finaliser l'installation du serveur d'impression :

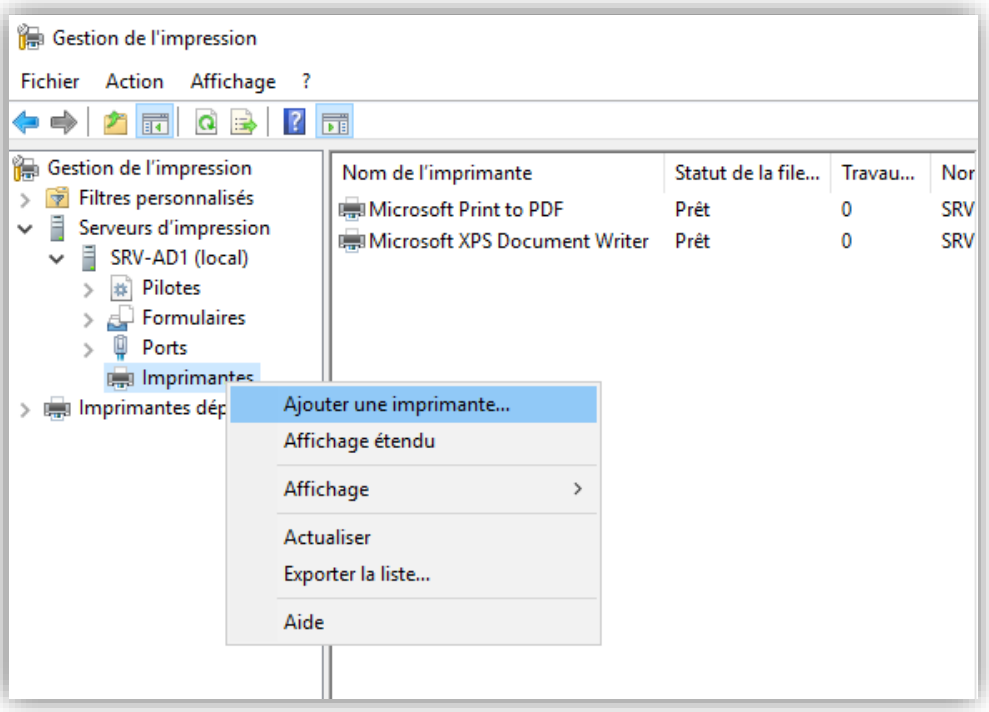


Configuration du serveur d'impression

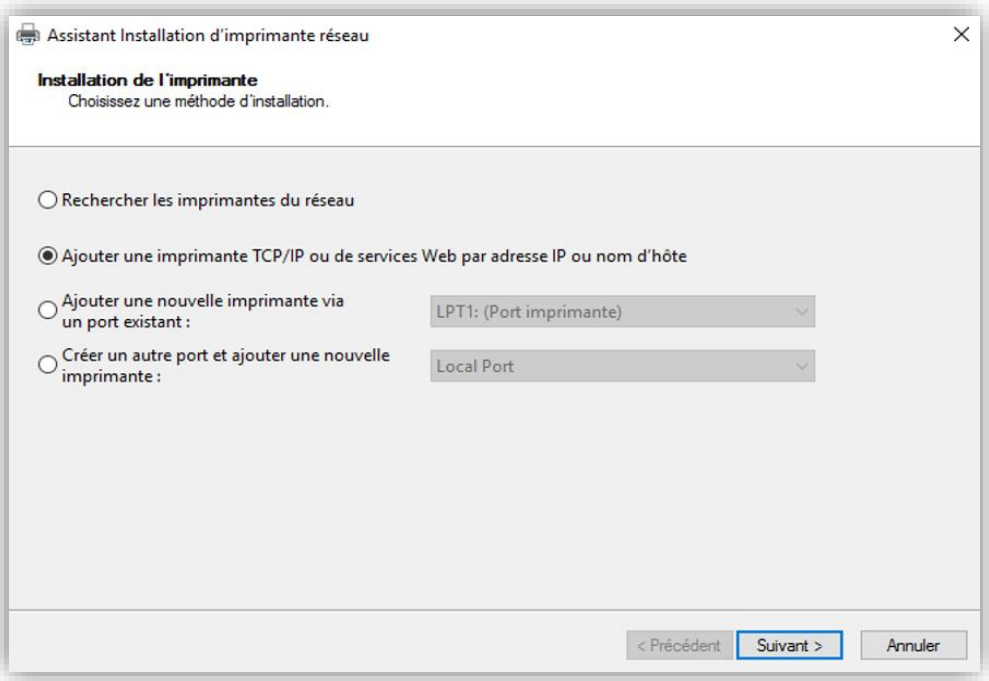
- Depuis le ***Tableau de Bord*** dans les ***Outils***, cliquer sur ***Gestion de l'impression*** :



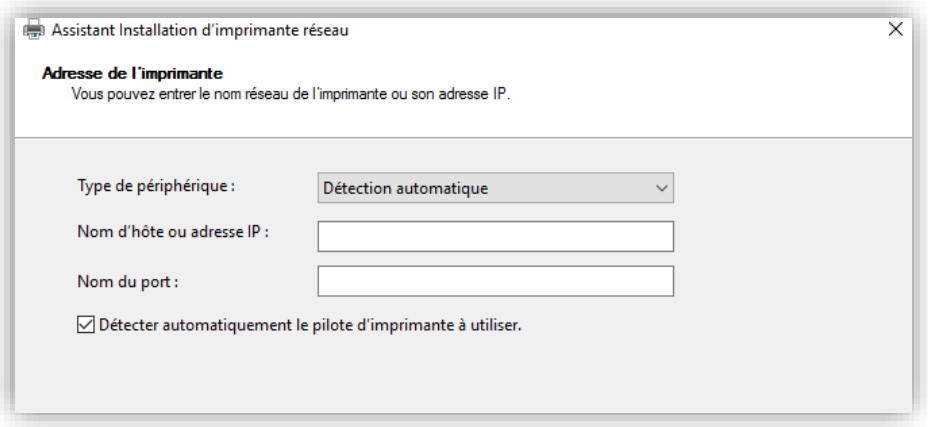
- Une fenêtre ***Gestion de l'impression*** s'ouvre. Depuis l'arborescence, faire clique-droit sur ***Imprimantes*** puis ***Ajouter une imprimante*** :



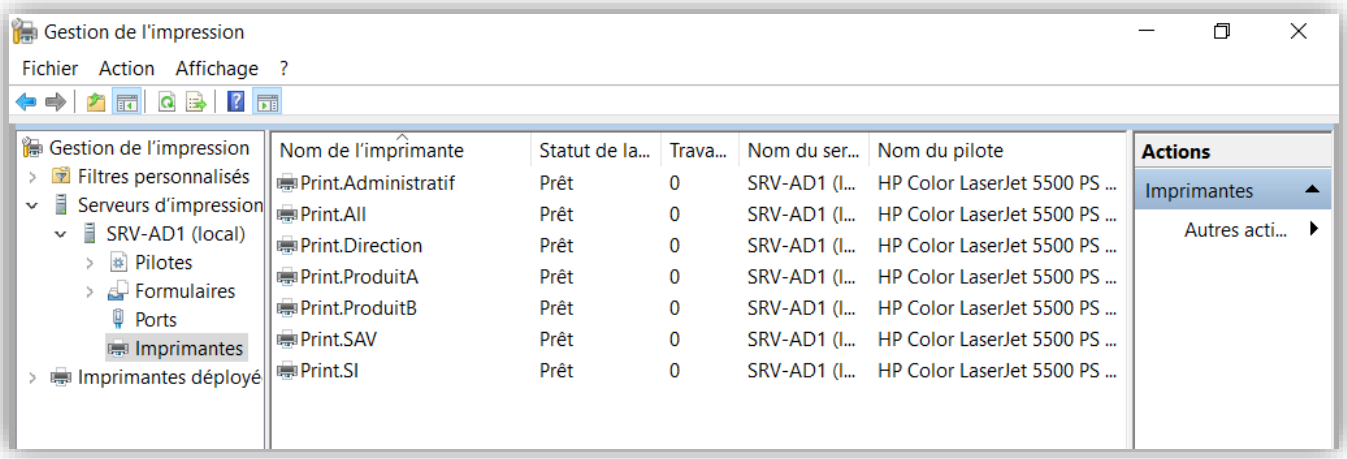
- Chaque imprimante possède une adresse IP. Ainsi, sélectionner ***Ajouter une imprimante TCP/IP ou de services Web par adresse IP ou nom d'hôte*** :



- Renseigner le **Nom d'hôte** et l'**IP** des imprimantes à rajouter.



- Suivant cette méthode, nous pouvons visualiser toutes les imprimantes de notre infrastructure.

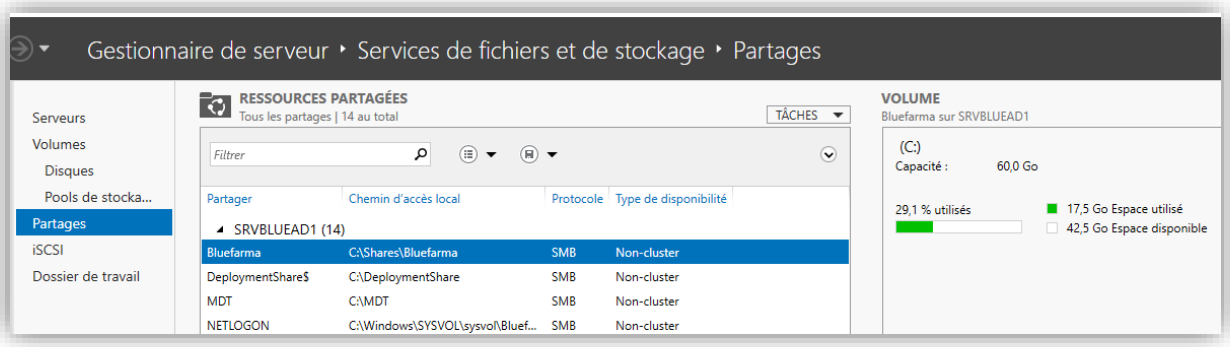


9.2. PROCÉDURE D'ADMINISTRATION WINDOWS SERVER

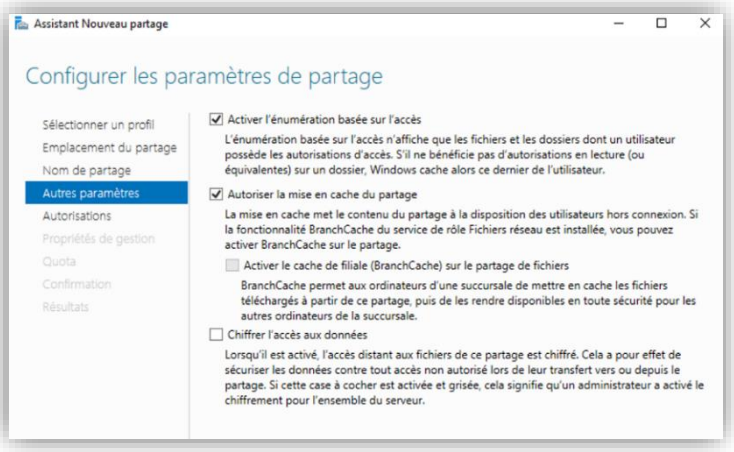
9.2.1. Gestion des accès au serveur de fichiers

Création du partage et gestion des droits d'accès :

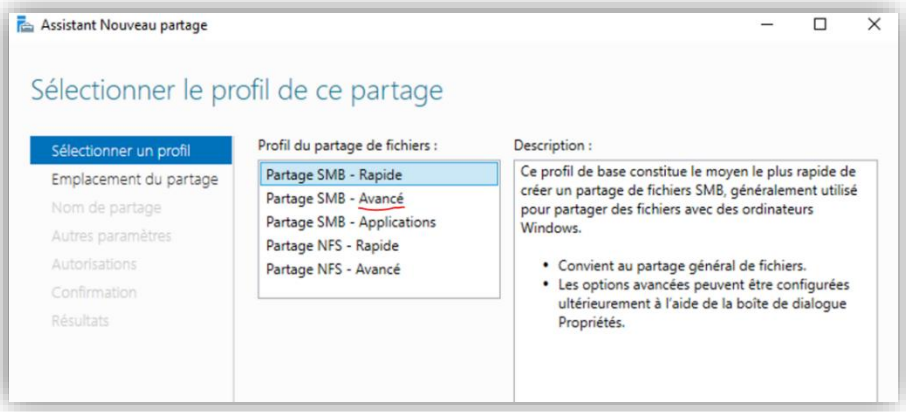
Après avoir installé le rôle ***Services de fichiers et de stockage***, nous allons pouvoir configurer nos différents partages :



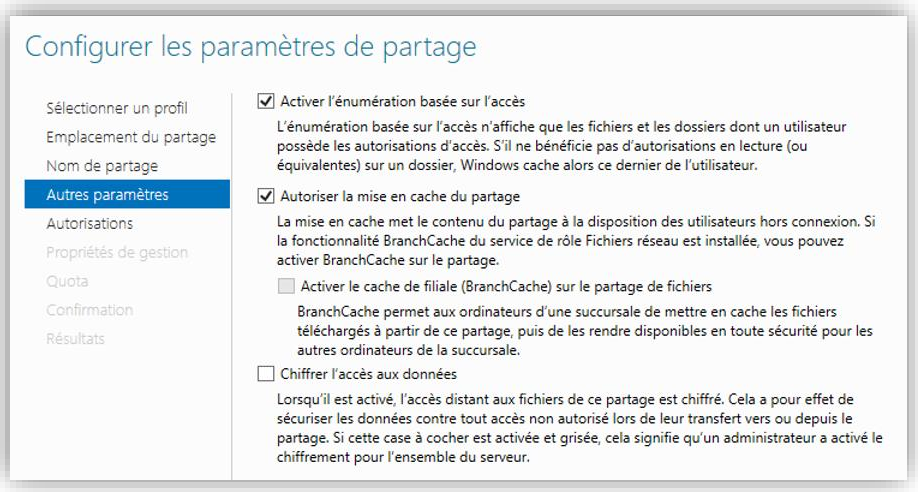
- Créer un nouveau partage « ***Bluefarma*** » qui contiendra l'ensemble des fichiers des utilisateurs :



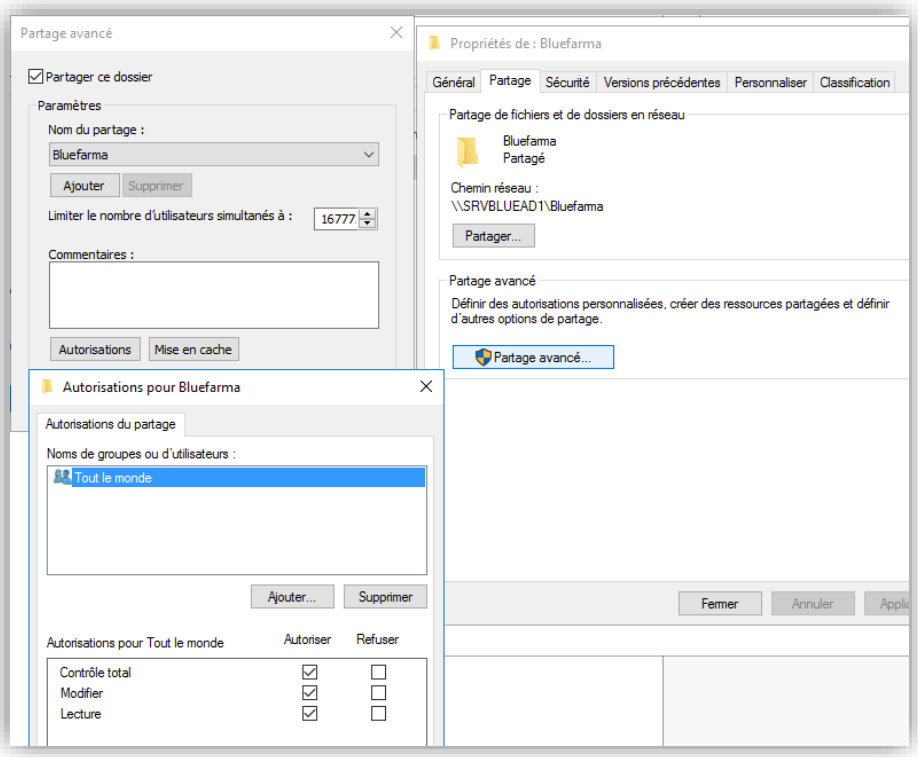
- Sélectionner « ***Partage SMB – Avancé*** »



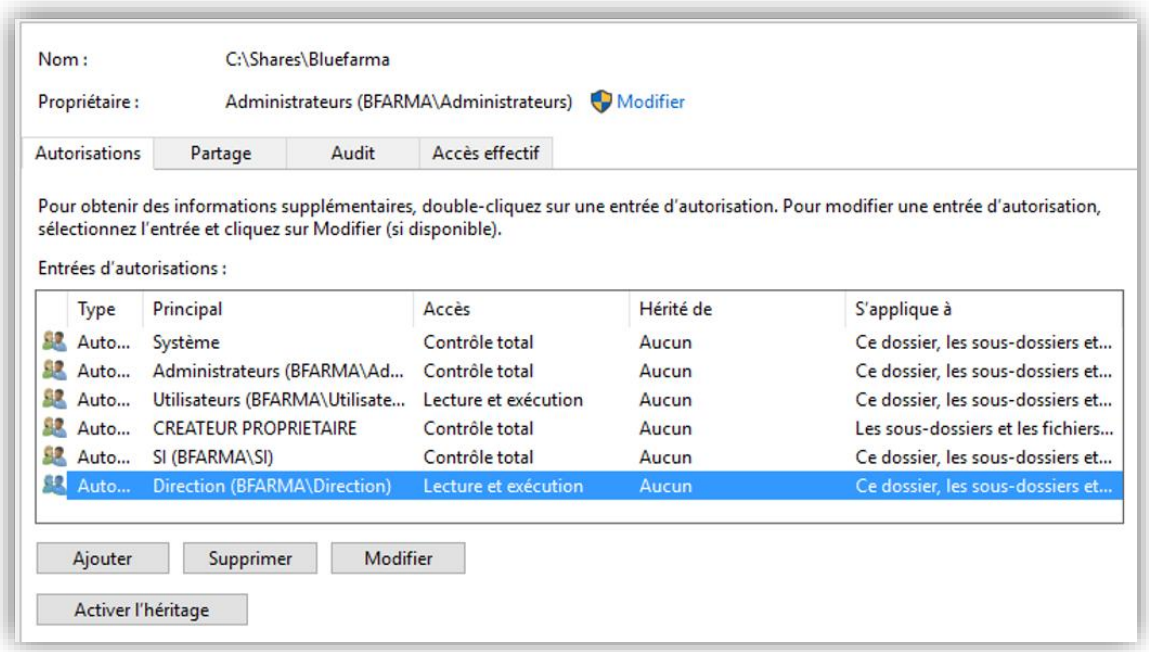
- Cocher la case ***Activer l'énumération basée sur l'accès*** (permet d'afficher uniquement les dossiers et fichiers autorisés en accès à un utilisateur. Les dossiers non autorisés seront masqués).



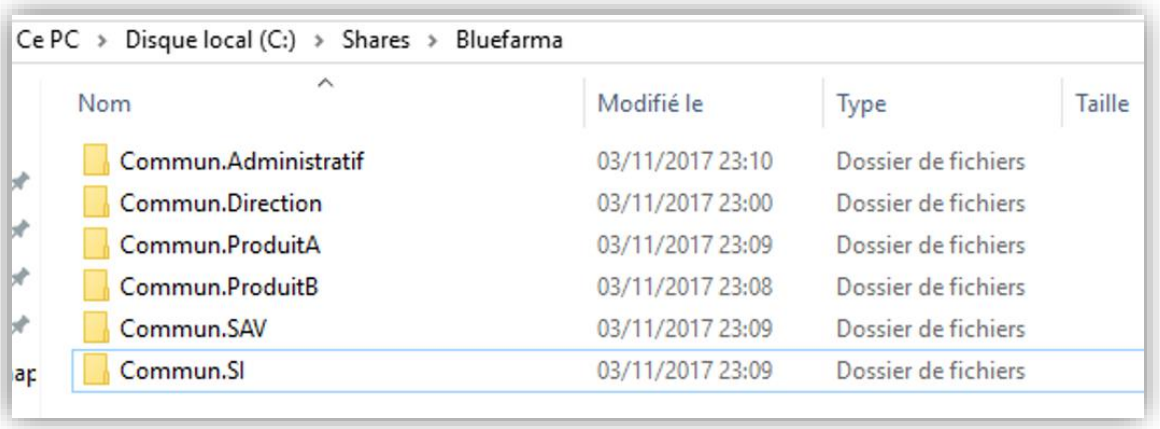
- Une fois le dossier créé et partagé, on peut se rendre sur le dossier pour configurer les droits : Distinguer les autorisations de partage et les autorisation NTFS en configurant un accès pour tout le monde en contrôle total > ***propriétés*** du dossier > Bluefarma > onglet ***Sécurité***.



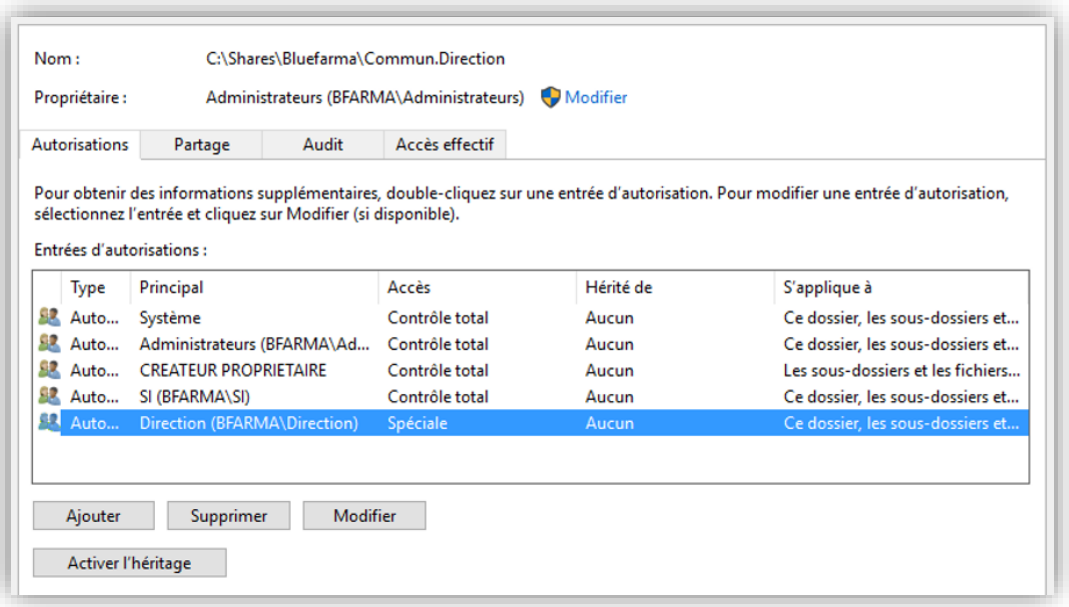
- Paramétrer un accès en lecture seule pour la Direction sur l'ensemble des dossiers partagés et un contrôle total pour le SI (lecture/écriture/modifications des autorisations, etc.). Désactiver l'héritage puis modifier les permissions et laisser le groupe ***Utilisateurs*** en lecture et exécution :



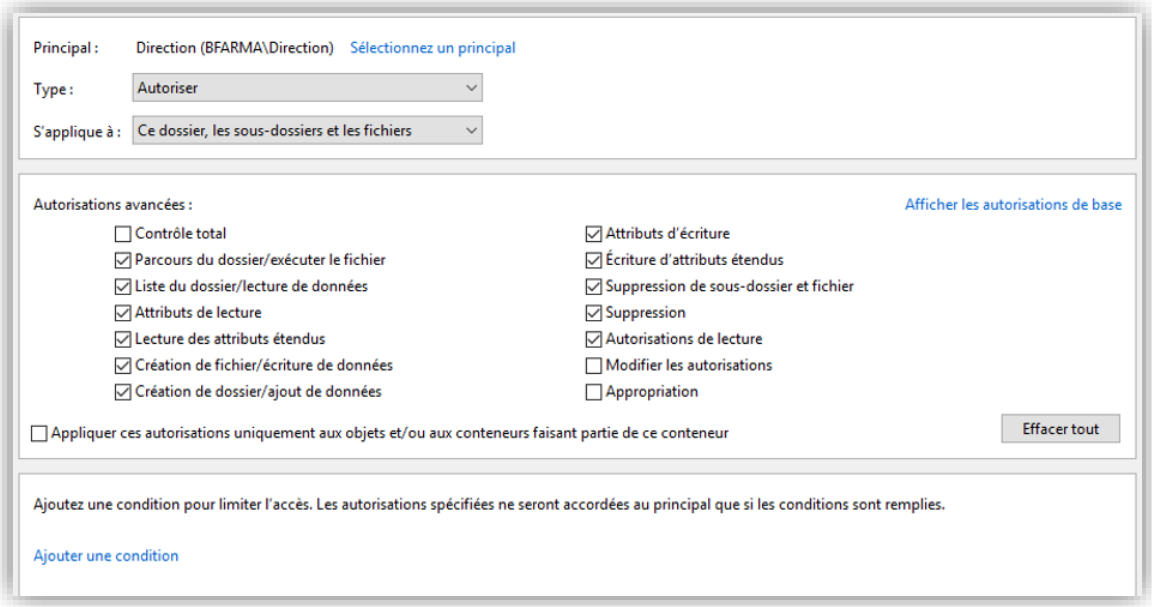
- Dans le dossier Bluefarma, créer les différents répertoires ***Commun <Service>*** :



- Se rendre dans sur chaque répertoire pour configurer les permissions de la même façon que pour le dossier Bluefarma.
  Pour le répertoire Commun.Direction, désactiver l'héritage et supprimer l'autorisation en lecture du groupe ***Utilisateurs***. (pas d'accès ni de visu sur ce répertoire pour les utilisateurs suite à l'activation de l'énumération basée sur l'accès) :
- Ajouter le groupe de sécurité ***Direction*** puis lui affecter tous les droits sauf celui de

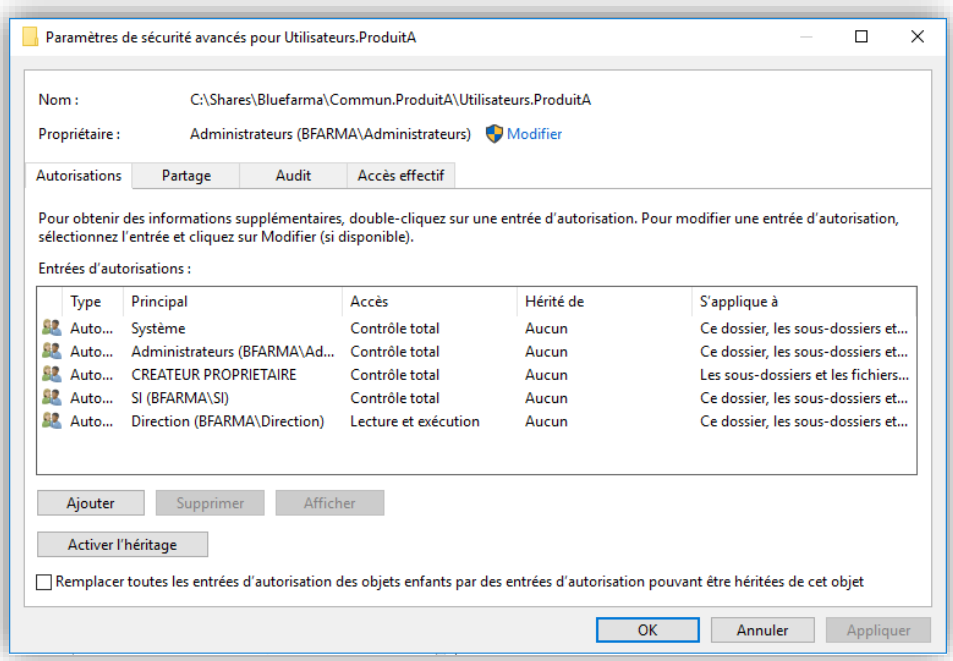


s'approprier le dossier et de modifier les autorisations de partage :

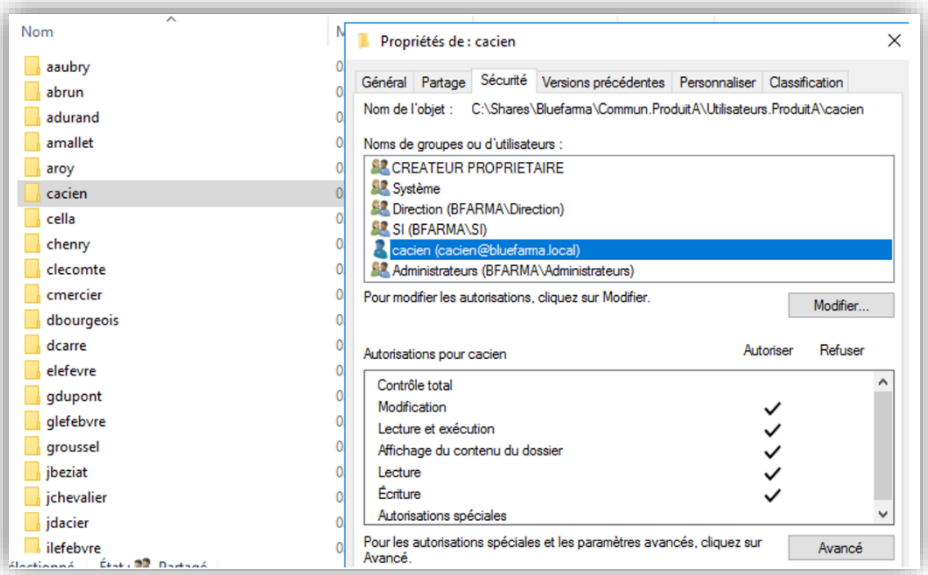


- Réitérer le même procédé pour les autres dossiers ***Commun/<service>***.(toujours laisser le groupe de sécurité Direction en lecture et le groupe Service Informatique en contrôle total

  Un dossier est créé à l'intérieur de chaque répertoire Commun.<Service> nommé ***Utilisateurs.Service*** avec un accès réservé à l'utilisateur uniquement : désactiver l'héritage sur les dossiers ***Utilisateurs.Service*** puis ôter les permissions de groupe du service :

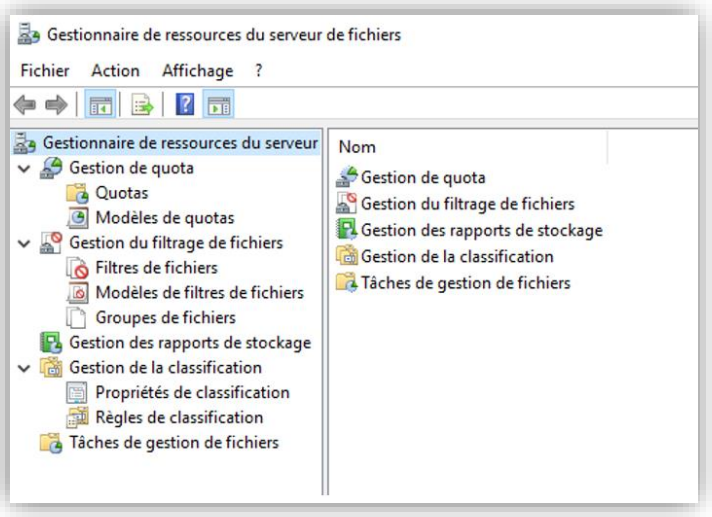


- Lancer ensuite le script powershell pour générer les 90 dossiers utilisateurs à leur nom et avec les permissions associées :

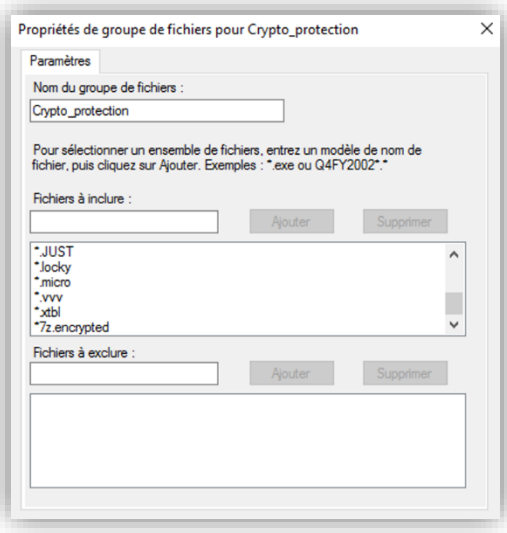


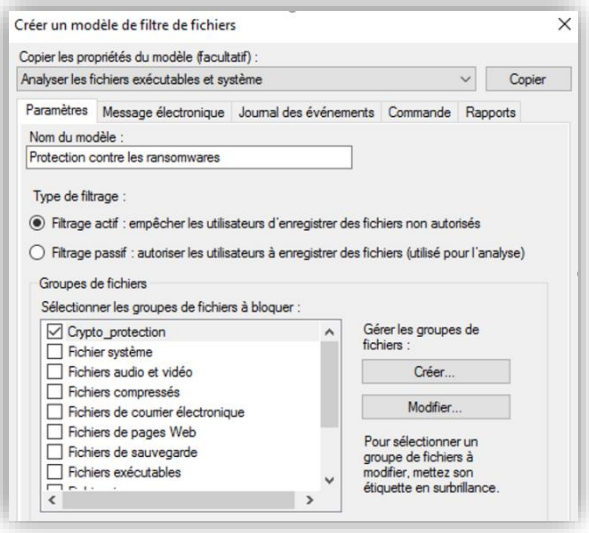
Gestion des quotas

- Depuis le ***Gestionnaire de ressources du serveur de fichiers***, appliquer des quotas, du filtrage de fichiers, création de rapports, etc.) :

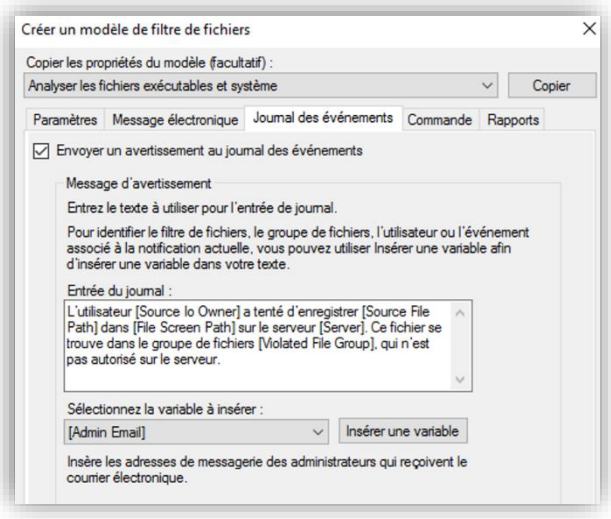


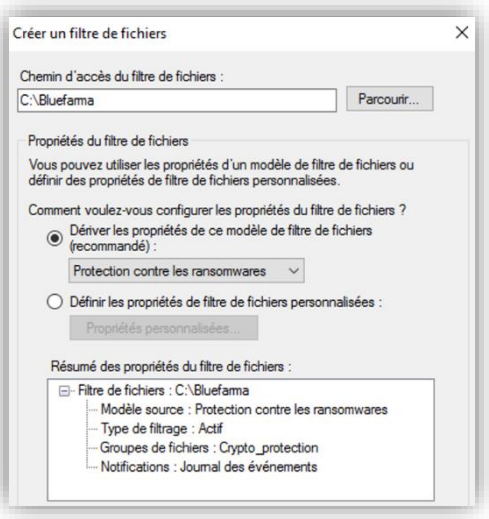
- Afin de consolider la politique de sécurité, créer un groupe de fichiers dans lequel il faut choisir les extensions de fichiers à bloquer (exemple : *.locky) puis créer un modèle de filtre de fichiers à partir de ce groupe, en mettant en place un filtrage actif : les utilisateurs ne pourront pas enregistrer de fichiers ayant une extension interdite :



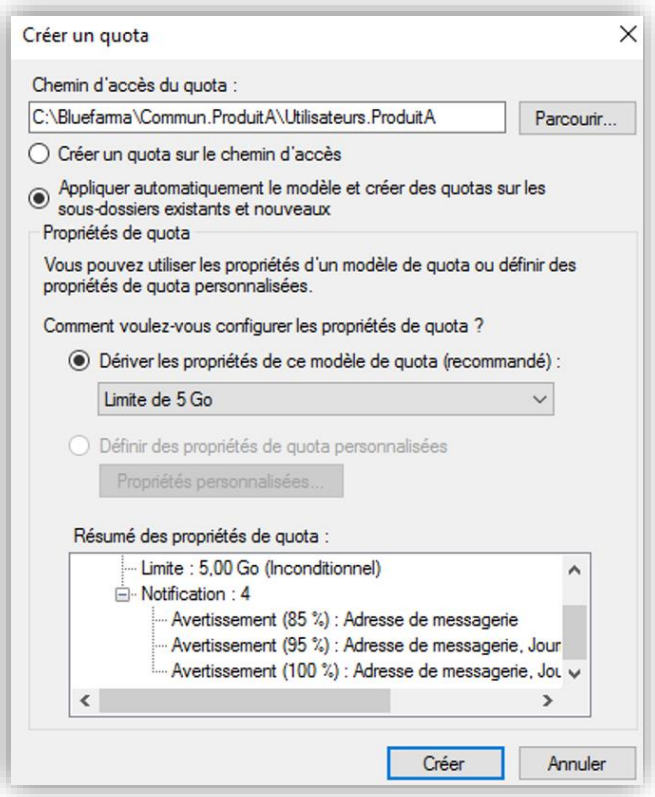


- Activer des ***alertes mails*** et le ***journal des évènements*** puis créer un filtre de fichiers, à appliquer sur le modèle créé précédemment et l'appliquer sur le dossier partagé Bluefarma :





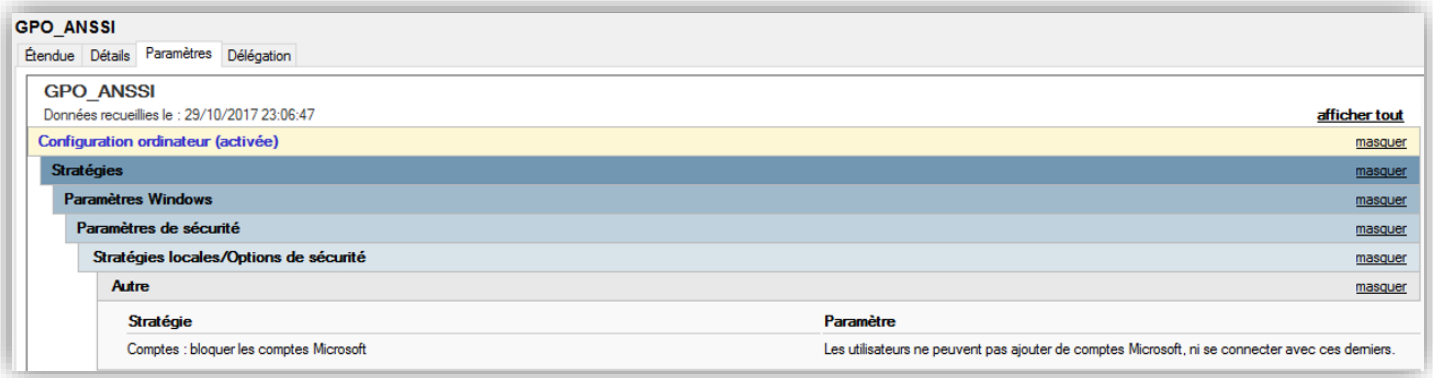
- Mettre en place les quotas pour les dossiers personnels depuis le ***Gestionnaire de ressources du serveur de fichiers*** puis créer un modèle de quota, de la même façon que les modèles de filtre de fichiers.
  Sélectionner ***Appliquer automatiquement le modèle et créer des quotas sur les sous-dossiers existants et nouveaux*** (un quota de 5 Go sera automatiquement appliqué lors de la création d'un nouveau dossier utilisateur) :



9.2.2. Stratégie de sécurité

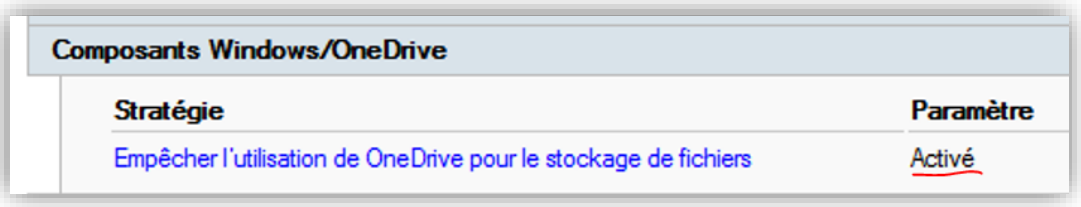
Désactivation de fonctionnalités Windows

- Blocage de l'utilisation des comptes Microsoft (ceci revient à stocker des informations telles que l'historique de navigation ou bien des mots de passe Wi-Fi dans le cloud Microsoft) :



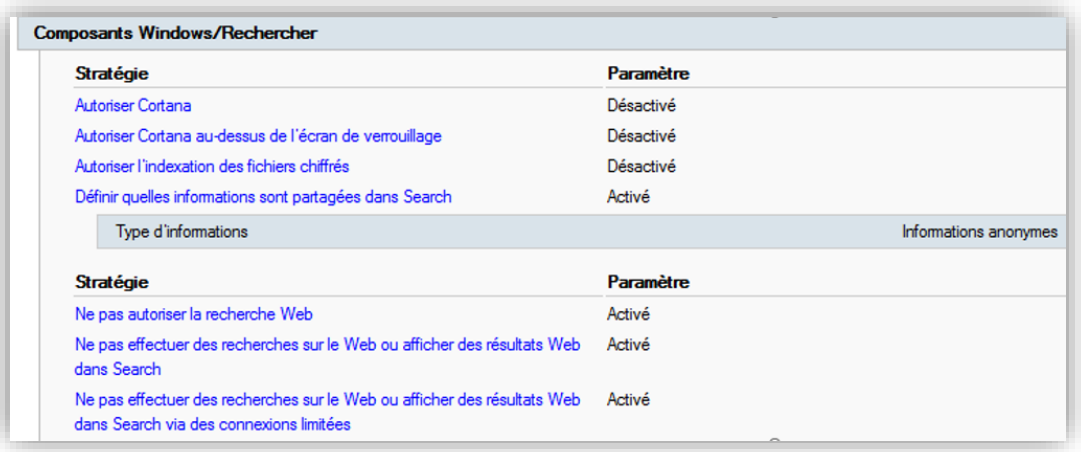
- Limiter l'envoi de données de télémétrie en configurant le paramètre ***Autoriser la télémétrie*** avec le niveau **1 – De base**. (NB : Il n'est pas possible de bloquer complètement l'envoi d'informations à Microsoft) :

- Désactivation de Onedrive afin d'éviter toute synchronisation de fichiers sur les serveurs de Microsoft :



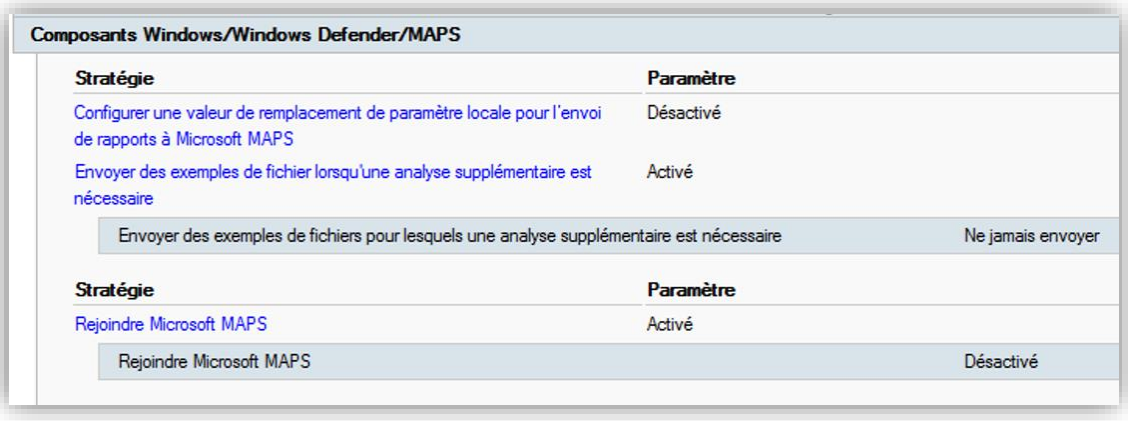
Composants Windows/OneDrive	
Stratégie	**Paramètre**
Empêcher l'utilisation de OneDrive pour le stockage de fichiers	Activé

- Désactiver Cortana, « l'assistant personnel intelligent » de Microsoft, qui accède aux données personnelles de l'utilisateur. Désactiver la recherche Web et l'affichage des résultats Web dans la barre de recherche (permet de limiter la recherche aux données locales du poste) :



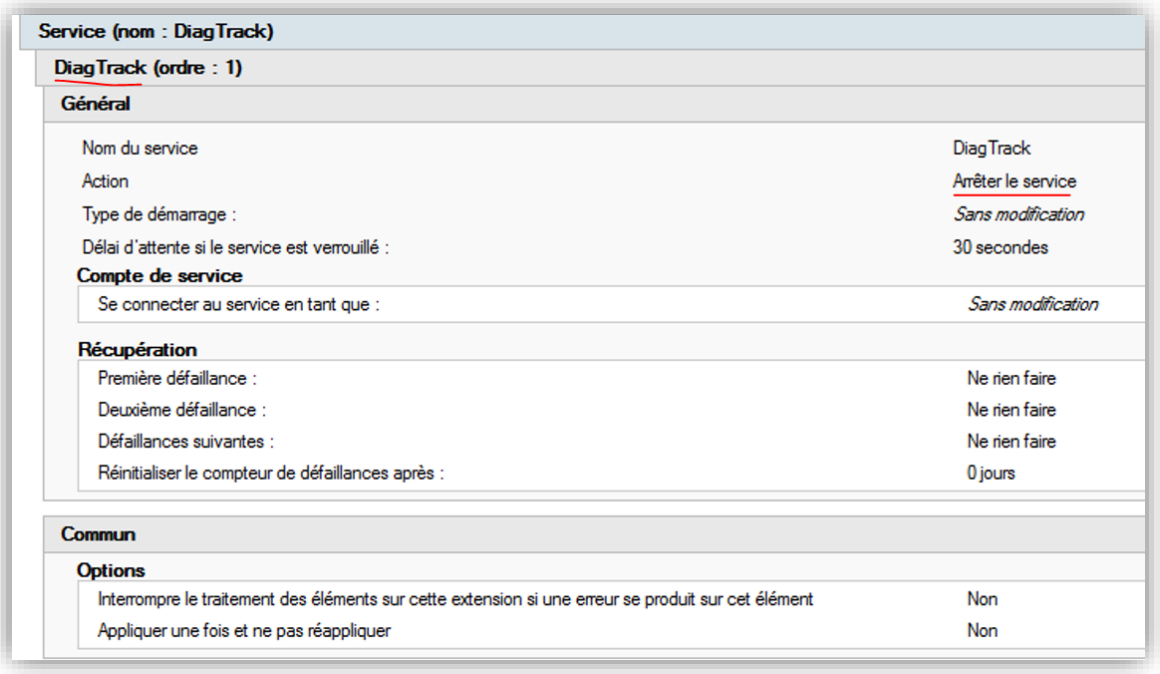
Composants Windows/Rechercher	
Stratégie	**Paramètre**
Autoriser Cortana	Désactivé
Autoriser Cortana au-dessus de l'écran de verrouillage	Désactivé
Autoriser l'indexation des fichiers chiffrés	Désactivé
Définir quelles informations sont partagées dans Search	Activé
Type d'informations	Informations anonymes
Stratégie	**Paramètre**
Ne pas autoriser la recherche Web	Activé
Ne pas effectuer des recherches sur le Web ou afficher des résultats Web dans Search	Activé
Ne pas effectuer des recherches sur le Web ou afficher des résultats Web dans Search via des connexions limitées	Activé

- Désactiver l'envoi de données par Windows Defender aux serveurs de Microsoft :



Composants Windows/Windows Defender/MAPS	
Stratégie	**Paramètre**
Configurer une valeur de remplacement de paramètre locale pour l'envoi de rapports à Microsoft MAPS	Désactivé
Envoyer des exemples de fichier lorsqu'une analyse supplémentaire est nécessaire	Activé
Envoyer des exemples de fichiers pour lesquels une analyse supplémentaire est nécessaire	Ne jamais envoyer
Stratégie	**Paramètre**
Rejoindre Microsoft MAPS	Activé
Rejoindre Microsoft MAPS	Désactivé

- Stopper le service ***DiagTrack***, qui est utilisé pour la télémétrie :



Service (nom : DiagTrack)

DiagTrack (ordre : 1)

Général

Nom du service	DiagTrack
Action	Arrêter le service
Type de démarrage :	*Sans modification*
Délai d'attente si le service est verrouillé :	30 secondes

Compte de service

Se connecter au service en tant que :	*Sans modification*

Récupération

Première défaillance :	Ne rien faire
Deuxième défaillance :	Ne rien faire
Défaillances suivantes :	Ne rien faire
Réinitialiser le compteur de défaillances après :	0 jours

Commun

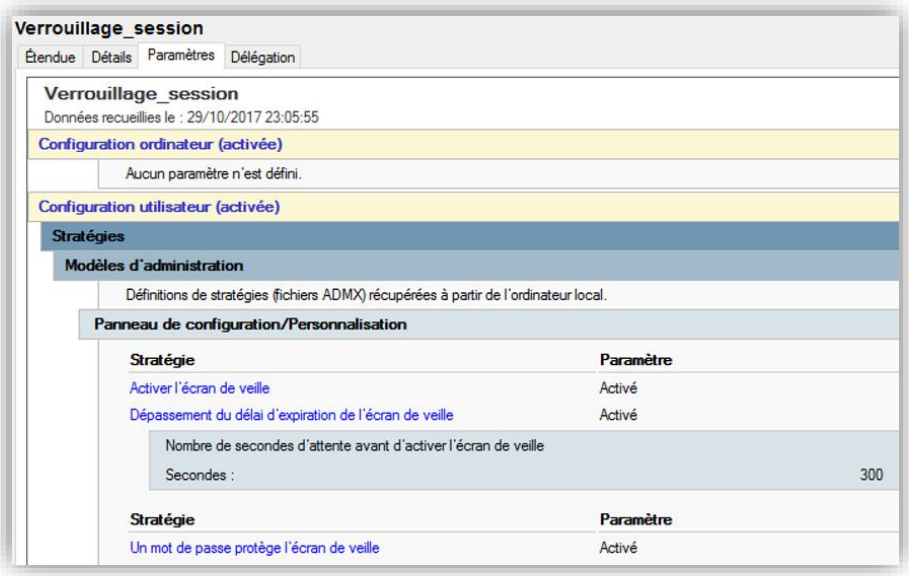
Options

Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément	Non
Appliquer une fois et ne pas réappliquer	Non

Sécurisation des postes et des données :

Plusieurs stratégies permettent de protéger les données entre les différents utilisateurs et services voire même des personnes extérieures à la société.

- Verrouillage des sessions. Une GPO permet de verrouiller les postes automatiquement après 5 minutes d'inactivité : l'utilisateur sera contraint d'entrer son mot de passe afin de déverrouiller sa session. Il est aussi possible de limiter la divulgation d'informations sensibles à des personnes extérieures au service :



Verrouillage_session

Étendue | Détails | Paramètres | Délégation

Verrouillage_session

Données recueillies le : 29/10/2017 23:05:55

Configuration ordinateur (activée)

Aucun paramètre n'est défini.

Configuration utilisateur (activée)

Stratégies

Modèles d'administration

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Panneau de configuration/Personnalisation

Stratégie	Paramètre
Activer l'écran de veille	Activé
Dépassement du délai d'expiration de l'écran de veille	Activé

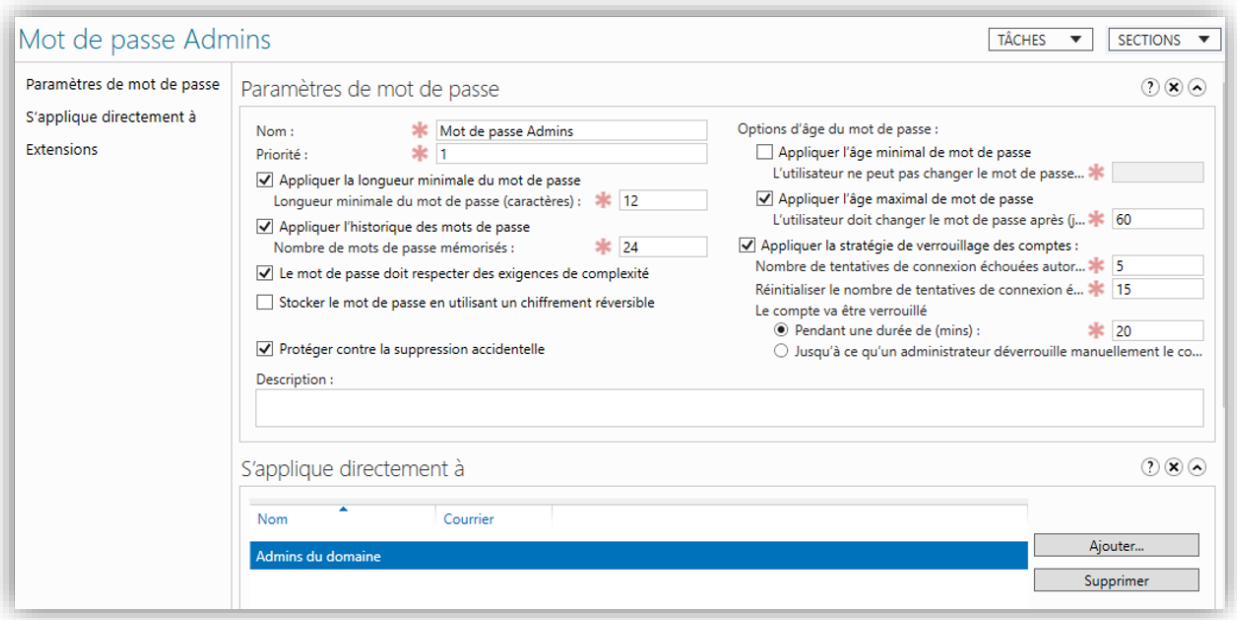
Nombre de secondes d'attente avant d'activer l'écran de veille

Secondes : 300

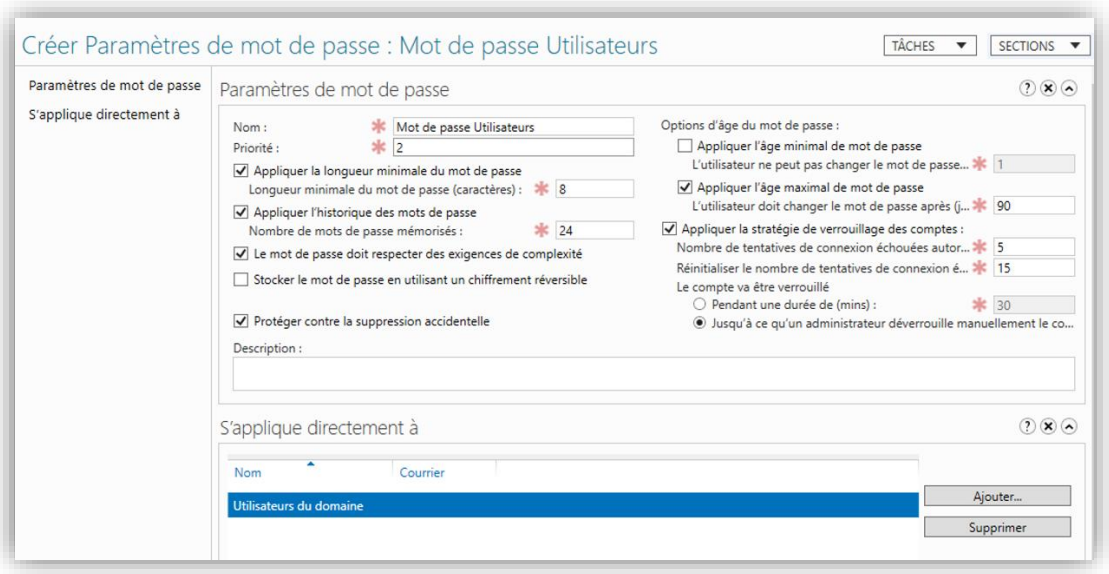
Stratégie	Paramètre
Un mot de passe protège l'écran de veille	Activé

Stratégie de mots de passe :

- <u>Stratégie de mot de passe complexe</u> pour les utilisateurs du groupe ***Admins du domaine***, en raison du caractère sensible de ces comptes. Les membres de ce groupe devront alors utiliser un mot de passe de 12 caractères et ce mot de passe sera à changer tous les 60 jours :

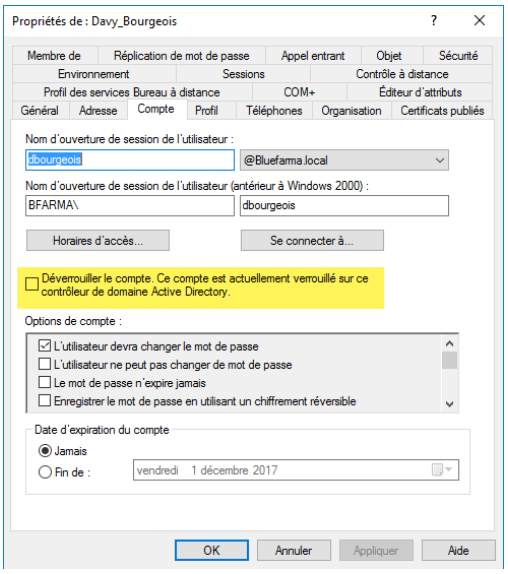


- <u>Stratégie de mot de passe pour les utilisateurs</u> : Mise en place d'un mot de passe d'un minimum de 8 caractères à renouveler tous les 90 jours. Verrouillage au bout de 5 tentatives de connexion échouées :



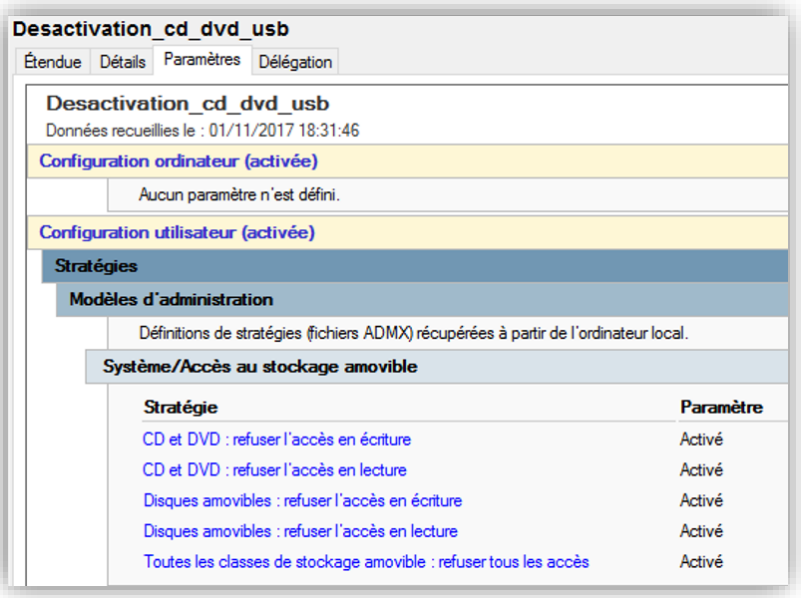
Message d'avertissement du verrouillage du compte au bout de 5 mots de passe erronés :

Un administrateur pourra alors déverrouiller le compte de l'utilisateur, via les propriétés du compte sur l'AD :

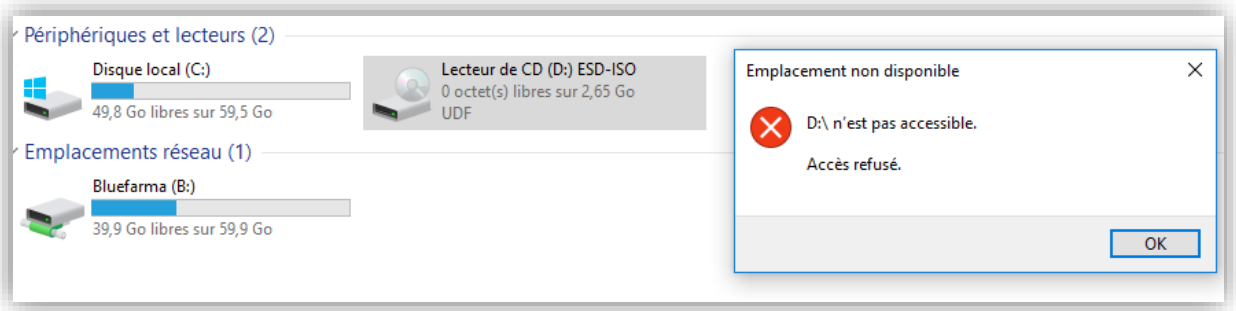


Désactivation des périphériques externes :

Afin de limiter les infections éventuelles via périphérique externe (clé USB, disque dur externe, etc.) ou la récupération de données sensibles, nous bloquons tout accès à un périphérique externe, en lecture comme en écriture, pour les utilisateurs du Service Produit A, B, et le SAV :



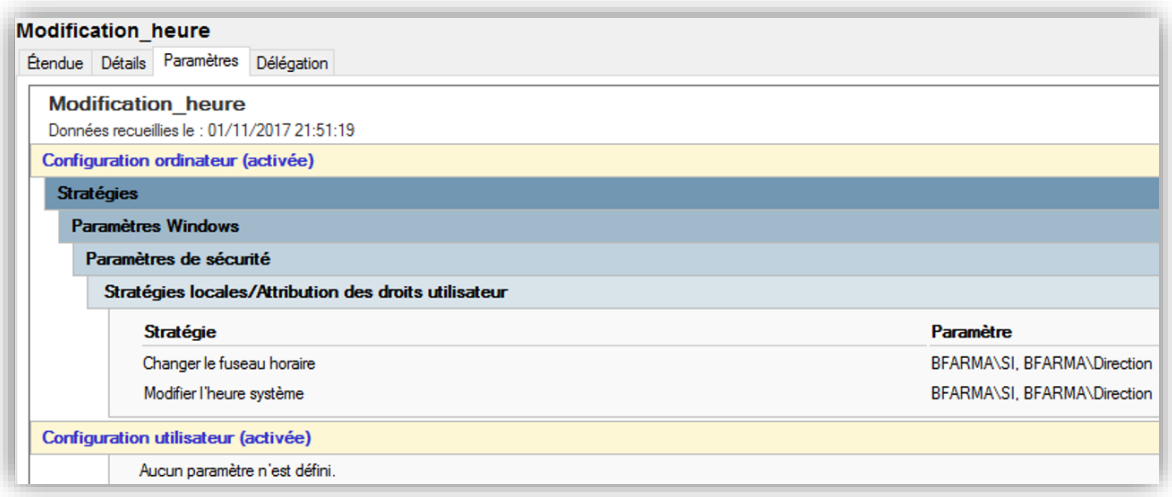
Si l'utilisateur connecte un périphérique USB à son poste et essaye d'y accéder, un message



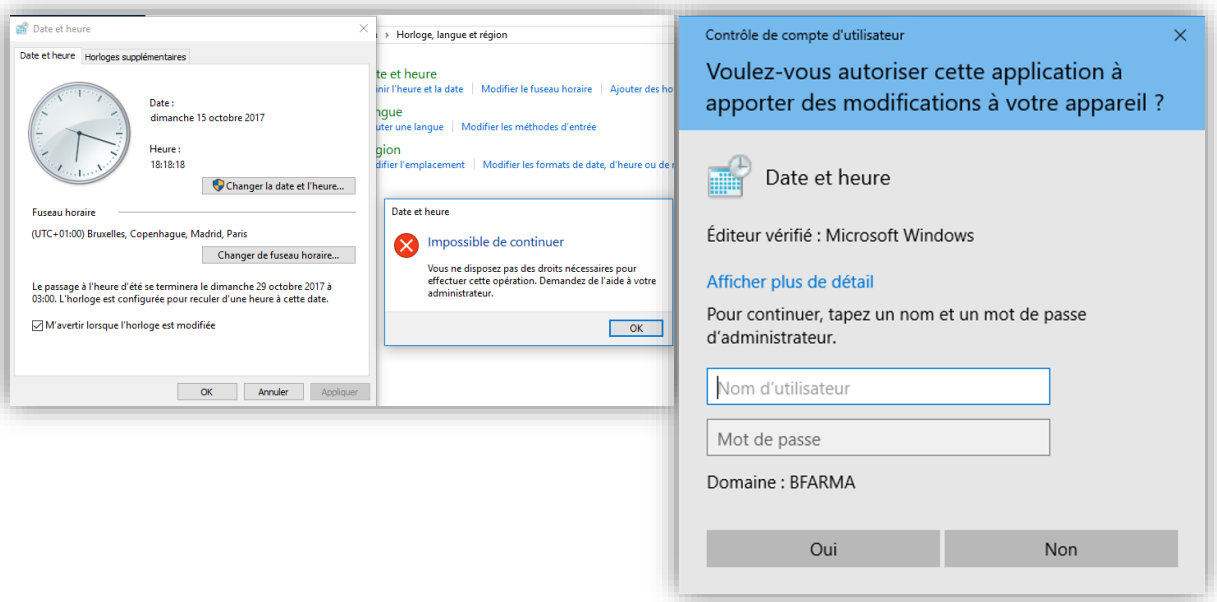
l'informera que l'accès lui est refusé :

Désactivation de l'heure :

Afin d'éviter tout contournement des stratégies par les utilisateurs, la modification de l'heure est bloquée sur le système, ainsi que la modification du fuseau horaire. Seuls la direction et le service informatique sont autorisés à apporter ces modifications :

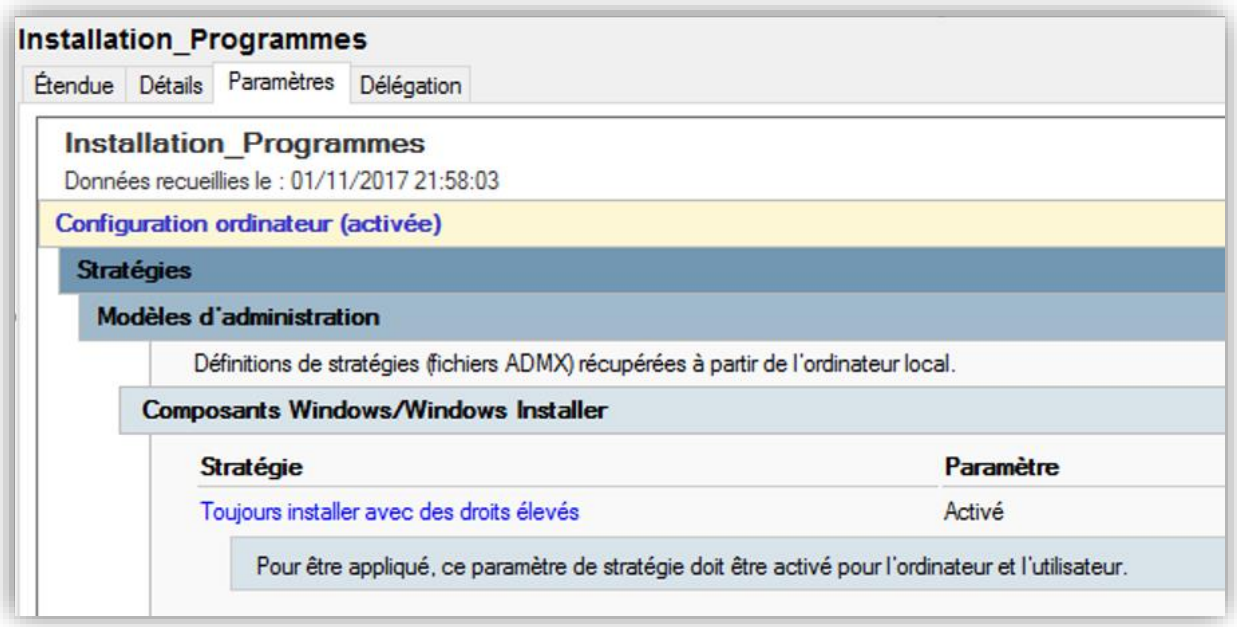


Si l'utilisateur tente de modifier l'heure ou le fuseau horaire sur son poste, est informé qu'il n'a pas les droits nécessaires pour effectuer ces modifications :

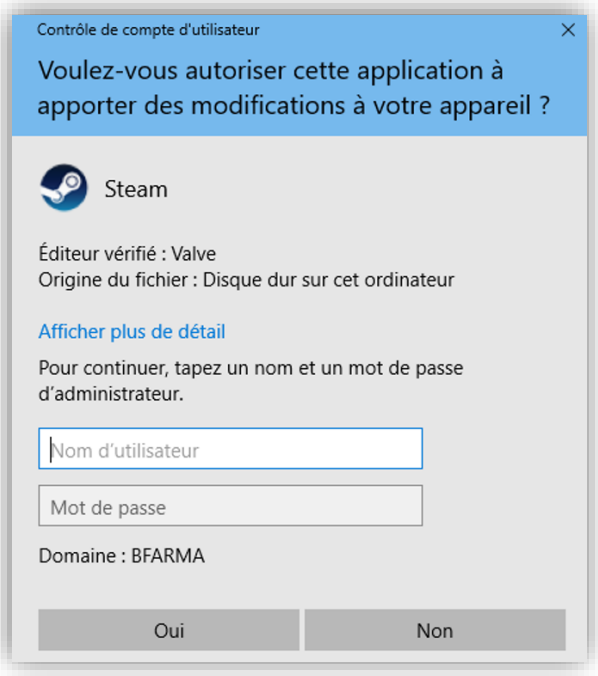


Interdiction d'installer des programmes :

L'installation de tout programme est bloquée à moins d'avoir des droits suffisamment élevés. On peut ainsi contrôler l'installation des logiciels sur les postes des utilisateurs et éventuellement donner une liste de logiciels autorisés avec leurs exécutables préalablement partagés sur un dossier réseau :



Si l'utilisateur essaye d'installer un logiciel, un message l'informe qu'il n'a pas les autorisations nécessaires :

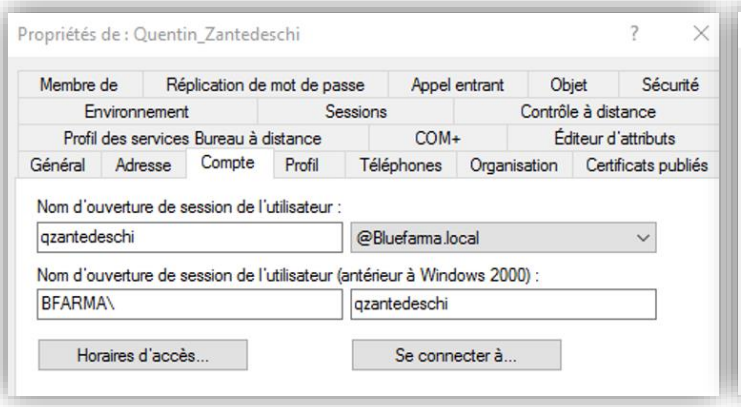


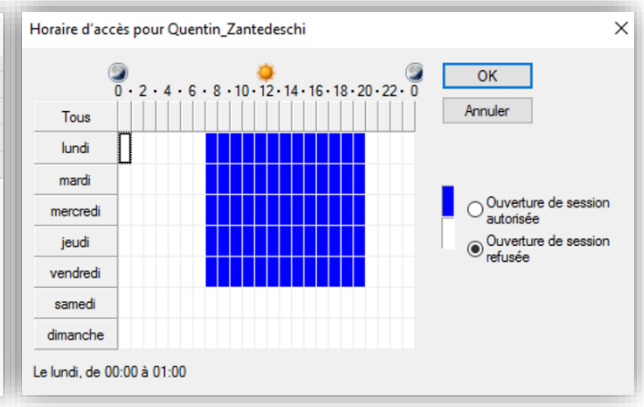
Configuration des horaires d'accès :

Conformément au cahier des charges, des horaires d'accès seront appliqués pour les utilisateurs :

- Aucun utilisateur, exceptés la Direction, le SAV et l'informatique, ne peuvent se connecter entre 20h et 7h.
- Mme **BEZIAT**, **ELLA**, **AYO** et **ACIEN** du service Produit A, ne peuvent quant à elles se connecter qu'entre 8h et 18h.

Pour régler les horaires d'accès, on peut configurer directement sur l'Active Directory de façon graphique via les « ***Horaires d'accès*** » dans les propriétés des comptes (il est possible de faire une sélection de multiples utilisateurs) :





Il est également possible d'intégrer une commande à un script Powershell afin de choisir les horaires d'accès dès la création des utilisateurs :

```
PS C:\Users\Administrateur.SRVBLUEAD1> net user qzantedeschi /times:L-V,07:00-20:00
La commande s'est termin,e correctement.

PS C:\Users\Administrateur.SRVBLUEAD1> |
```

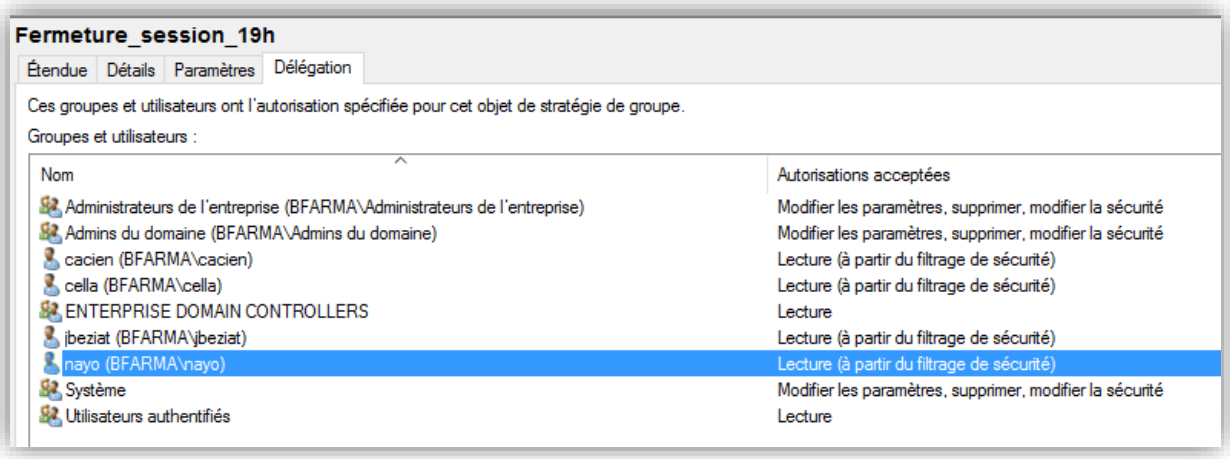
Les horaires d'accès sont réglés de 7h à 20h pour les services Administratif, Produit A et Produit B.

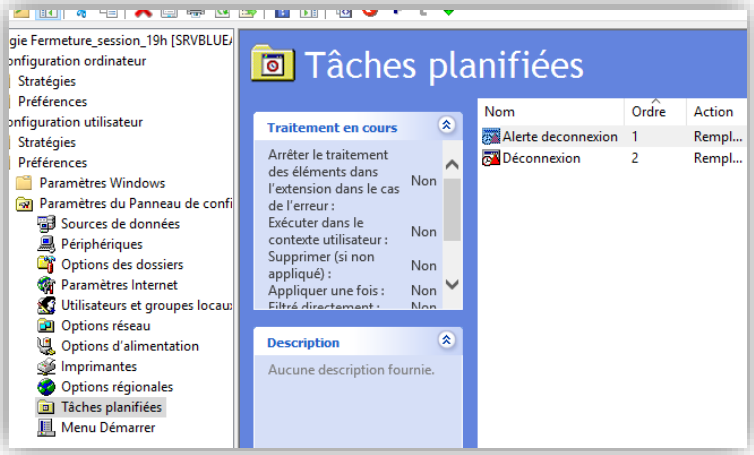
Ceux de Mme Beziat, Ella, Ayo et Acien sont compris entre 8 h et 18h et elles doivent être déconnectées automatiquement à 19h.

La mise en œuvre de ces paramètres passe par la création de deux tâches planifiées :

- La première sert à prévenir l'utilisateur de la déconnexion afin qu'il puisse enregistrer son travail
- La seconde tâche se chargera de déconnecter la session.

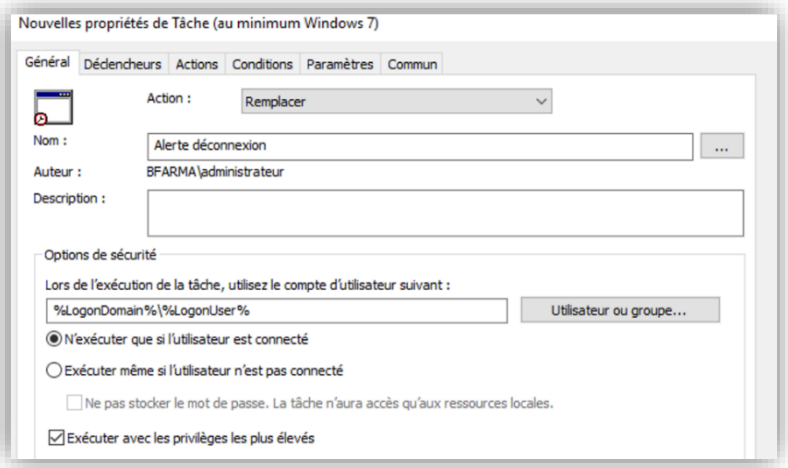
Une nouvelle GPO est créée et appliquée dans l'OU « Service Produit A », puis le filtrage de sécurité est réglé de sorte à ce que la GPO ne s'applique qu'à Mme Beziat, Ella, Ayo et Acien :



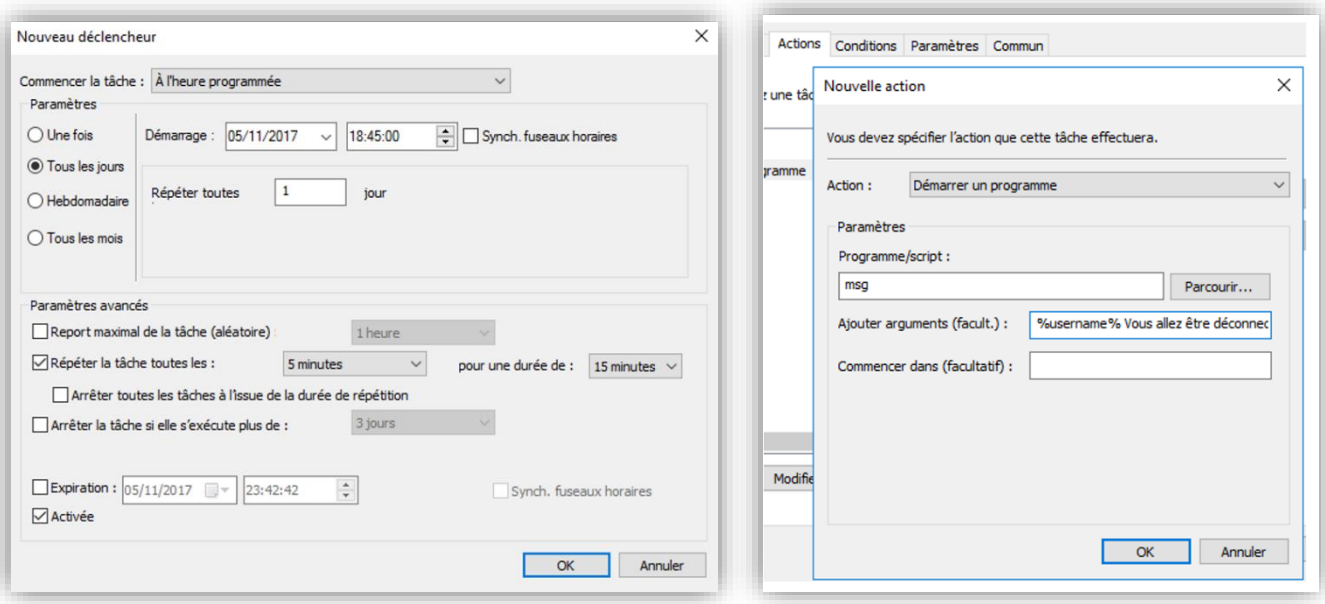


Création de la tâche planifiée « Alerte déconnexion » :

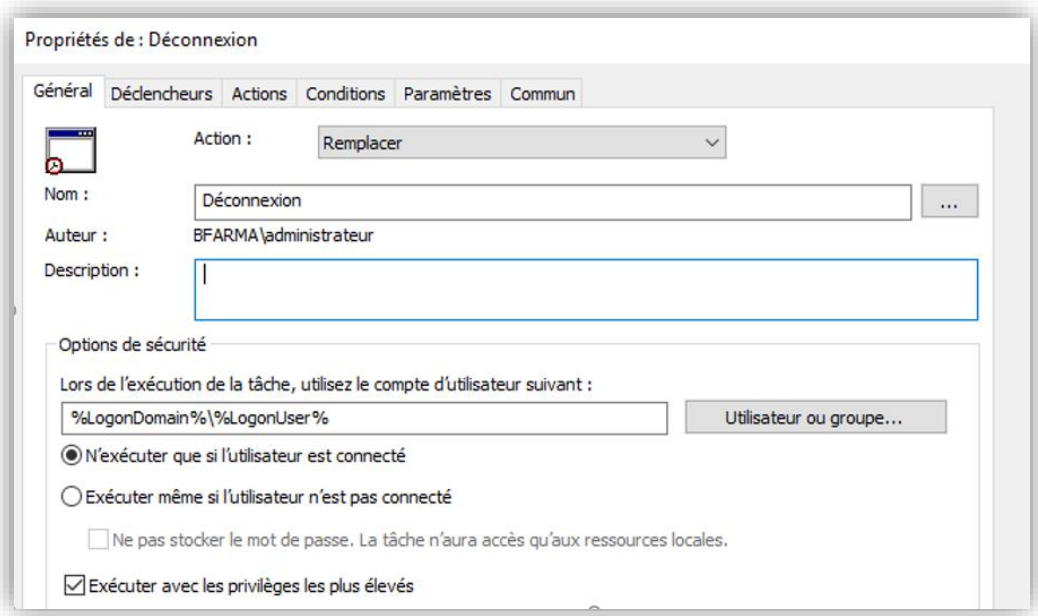
La première tâche « ***Alerte déconnexion*** », informera l'utilisateur d'une déconnexion imminente à 19h par l'affichage d'un message :



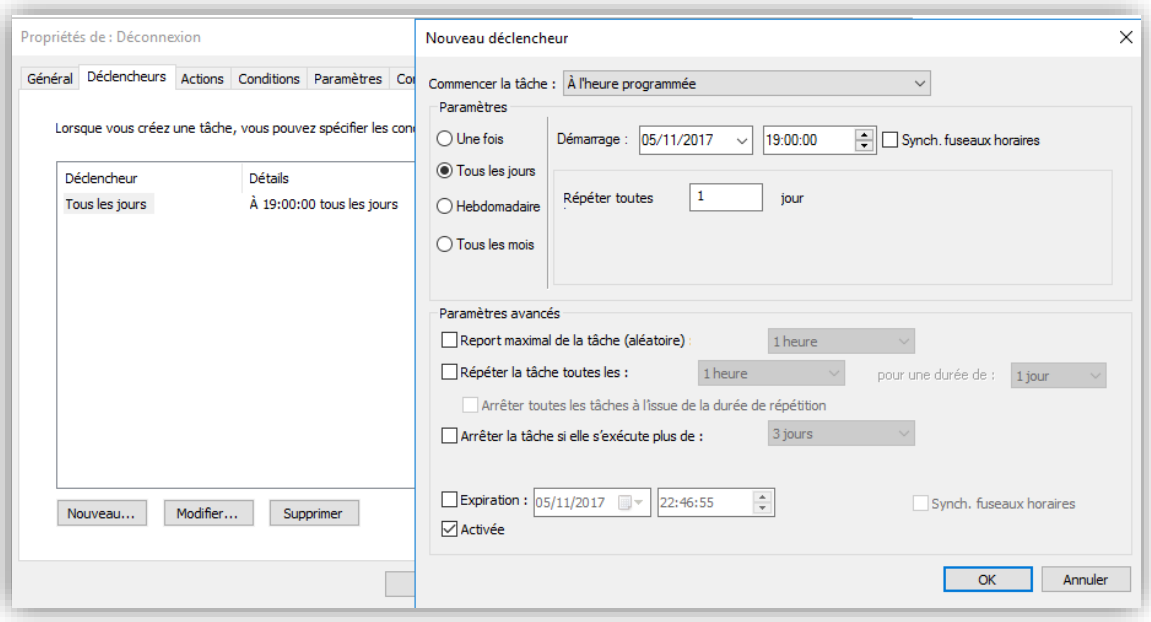
- Dans l'onglet **Déclencheur**, la tâche est programmée tous les jours à 18h45 et elle se répète toutes les 5 minutes. Le message s'affichera donc à 18h45, 18h50 et 18h55 avant la déconnexion de la session à 19h.
- Dans l'onglet **Actions**, on choisit de ***démarrer un programme*** puis démarre le composant « ***msg*** » qui permettra d'afficher une boite de dialogue. Le nom de l'utilisateur est récupéré grâce à la variable ***%username%*** puis le message suivant est renseigné : « *Vous allez être déconnecté à 19 heures. Merci d'enregistrer votre travail*. » :



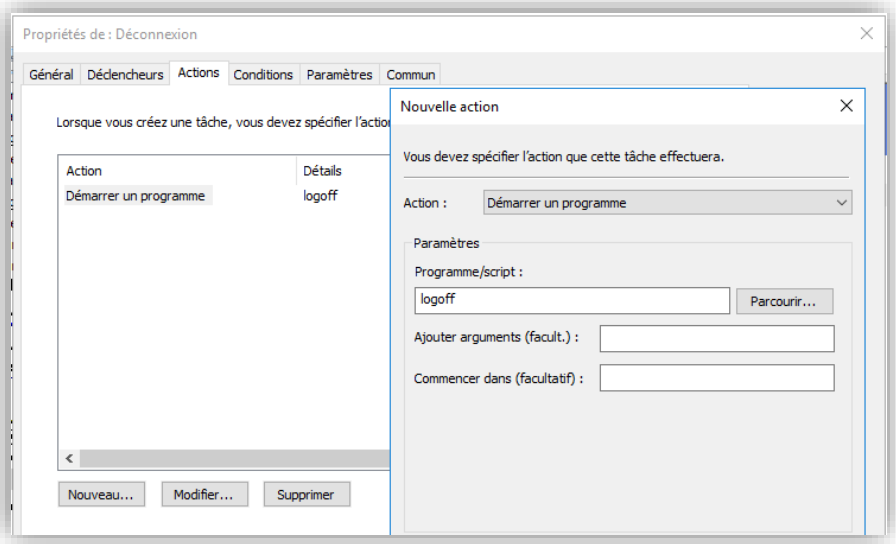
Création de la tâche planifiée chargée de la déconnexion :

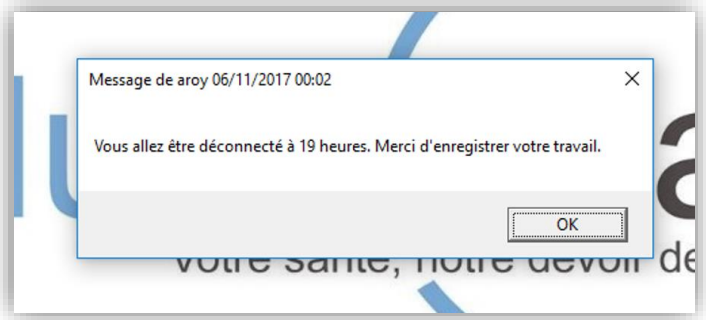


- Cette dernière est planifiée à 19h tous les jours :



- Dans l'onglet En action, on choisit de démarrer un programme **logoff** :



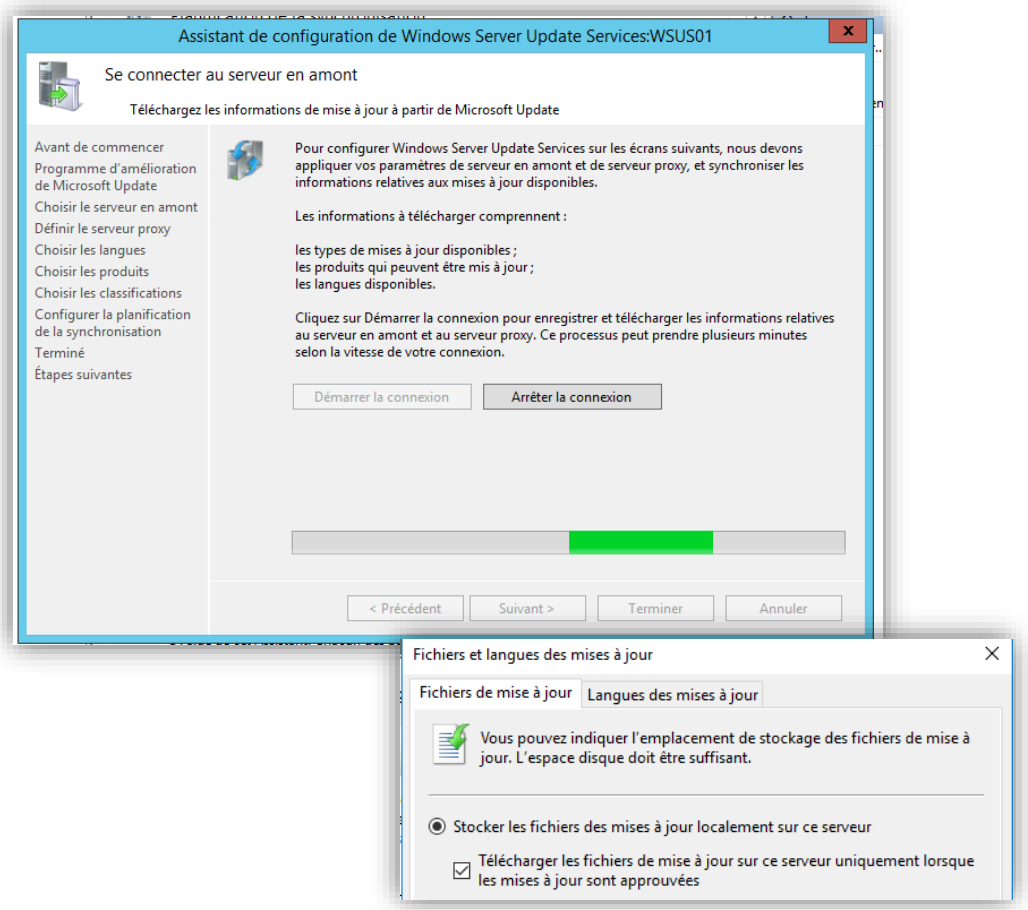


- L'utilisateur est bien informé de la déconnexion de son poste par un message :

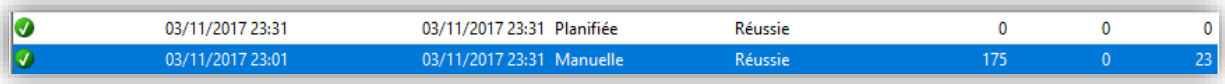
9.2.3. Serveur de mise à jour WSUS

Téléchargement et synchronisation des mises à jour

- Après avoir installé les rôles **WSUS** et **IIS** via l'assistant d'ajout de rôles et fonctionnalités, lancer l'assistant de configuration de WSUS. Choisir la langue des mises à jour : **français** puis les mises à jour que l'on souhaite télécharger (Windows 10 en l'occurrence).
- Faire en sorte que les mises à jour soient téléchargées uniquement après approbation puis effectuer une première synchronisation : le serveur WSUS va chercher les mises à jour applicables (mais il ne les télécharge pas) :



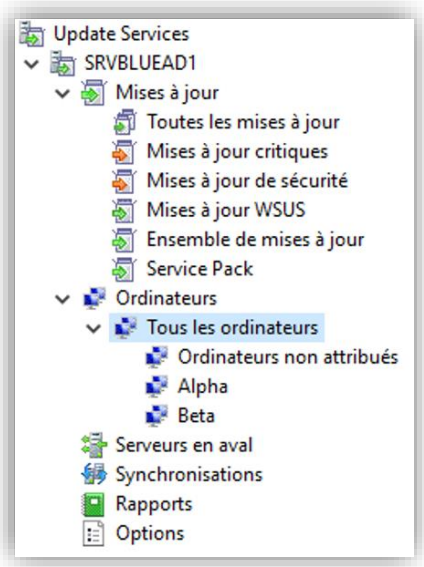
- On constate que la synchronisation manuelle s'est correctement déroulée via l'onglet ***Synchronisations*** (des mises à jours ont été trouvées).



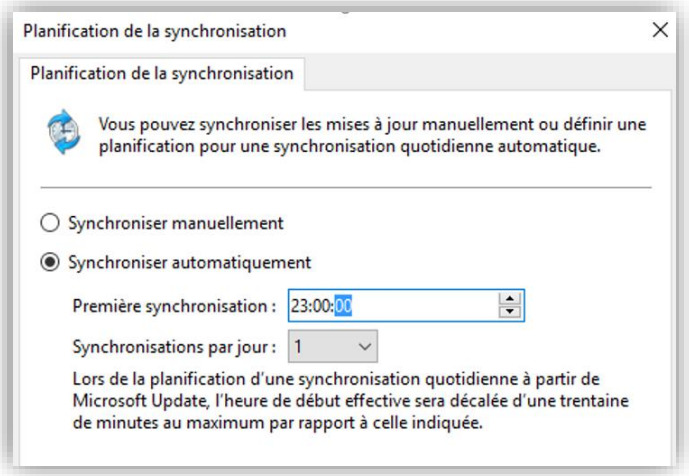
Création des groupes d'approbation

- Dans l'***utilitaire WSUS***, créer des groupes d'ordinateurs : ***Alpha*** et ***Beta***. Le groupe Alpha contient 10 postes « non sensibles » et recevra les mises à jour en premier.

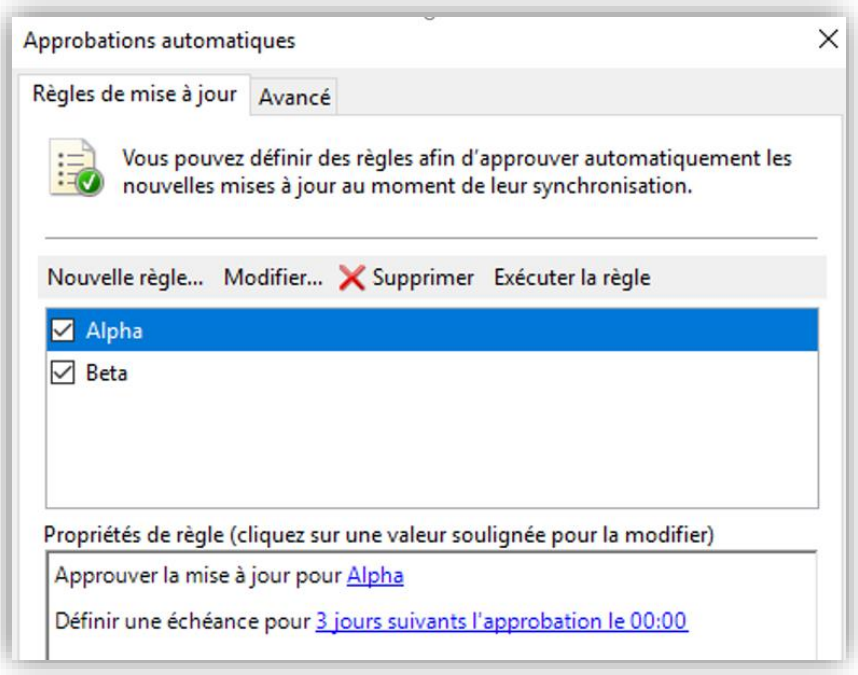
Ayant constaté que les postes du groupe Alpha supportent bien les mises à jour, on approuve– *de façon automatique* – les mises à jour pour le groupe Beta. (Il arrive fréquemment que Windows propose des mises à jour posant des problèmes sérieux entrainant l'impossibilité de démarrer un poste, par exemple la MAJ KB4041676 d'octobre 2017).



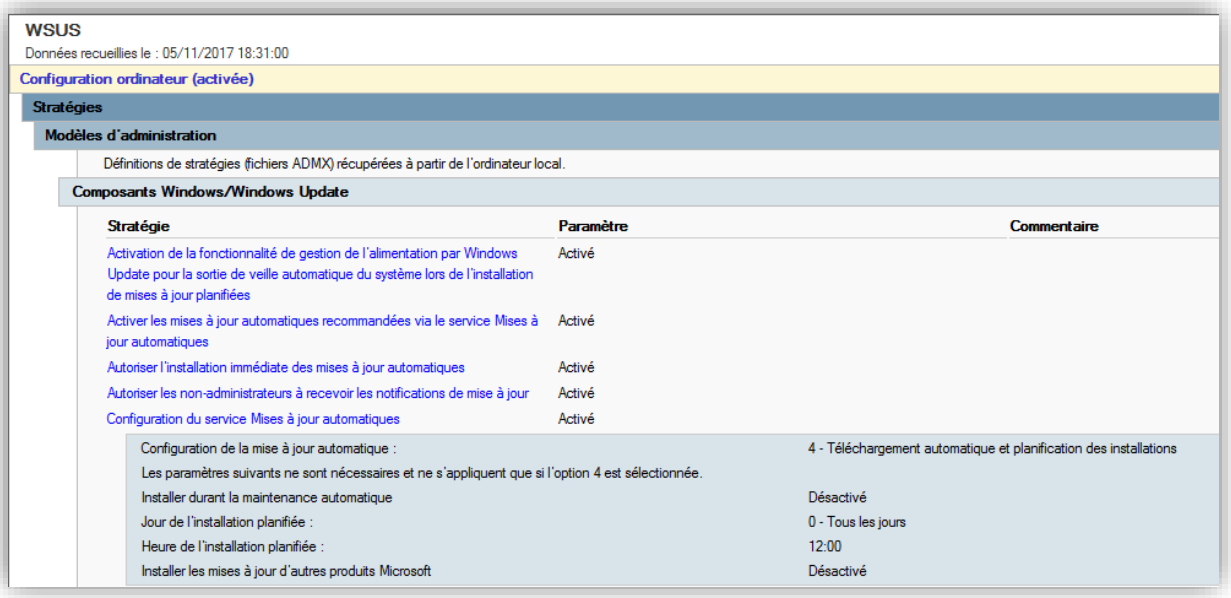
- Planifier synchronisation automatique du WSUS tous les jours à 23h.



- Créer deux règles d'approbation automatique afin d'approuver les mises à jour pour les groupes Alpha et Beta, respectivement (3 et 6 jours) :



- Configurer une GPO sur l'ensemble des ordinateurs de la société afin le point de récupération des mises à jour. L'installation est planifiée à 12h :



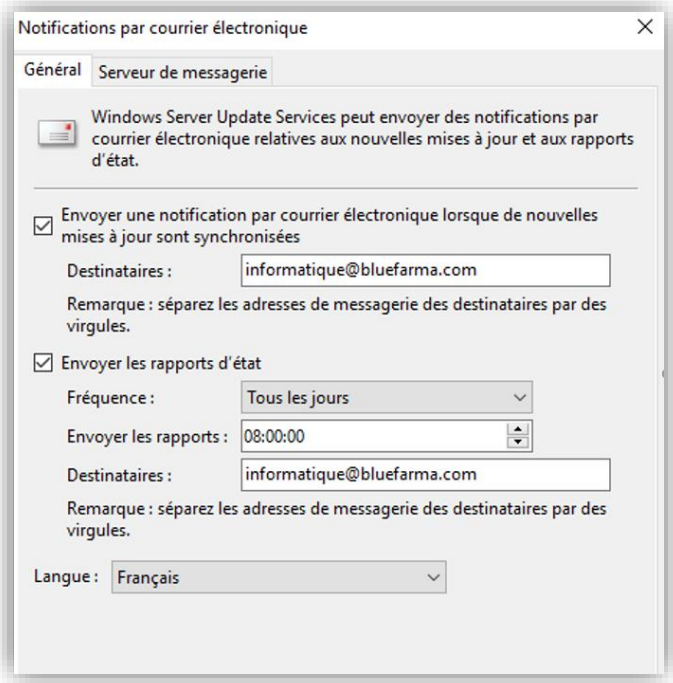
- La fréquence de vérification des mises à jour est configurée pour avoir des rapports fréquents sur l'état des mises à jour des postes sur le WSUS.
  Le redémarrage automatique pour les utilisateurs connectés est désactivé.
  On spécifie également l'adresse IP du serveur WSUS en tant que serveur de mise à jour :

Stratégie	Paramètre	Commentaire
Fréquence de détection des mises à jour automatiques	Activé	
Vérifier la présence de mises à jour à l'intervalle suivant (heures) :	1	

Stratégie	Paramètre	Commentaire
Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées de mises à jour automatiques	Activé	
Redemander un redémarrage avec les installations planifiées	Activé	
Attendre pendant la durée suivante avant de redemander en cas de redémarrage planifié (minutes) :	1440	

Stratégie	Paramètre	Commentaire
Spécifier l'emplacement intranet du service de mise à jour Microsoft	Activé	
Configurer le service de Mise à jour pour la détection des mises à jour :	http://192.168.40.10:8530	
Configurer le serveur intranet de statistiques :	http://192.168.40.10:8530	
Définir le serveur de téléchargement de substitution : (par exemple : http://IntranetUpd01)		
Téléchargez les fichiers sans URL dans les métadonnées si un serveur de téléchargement alternatif est défini.	Désactivé	

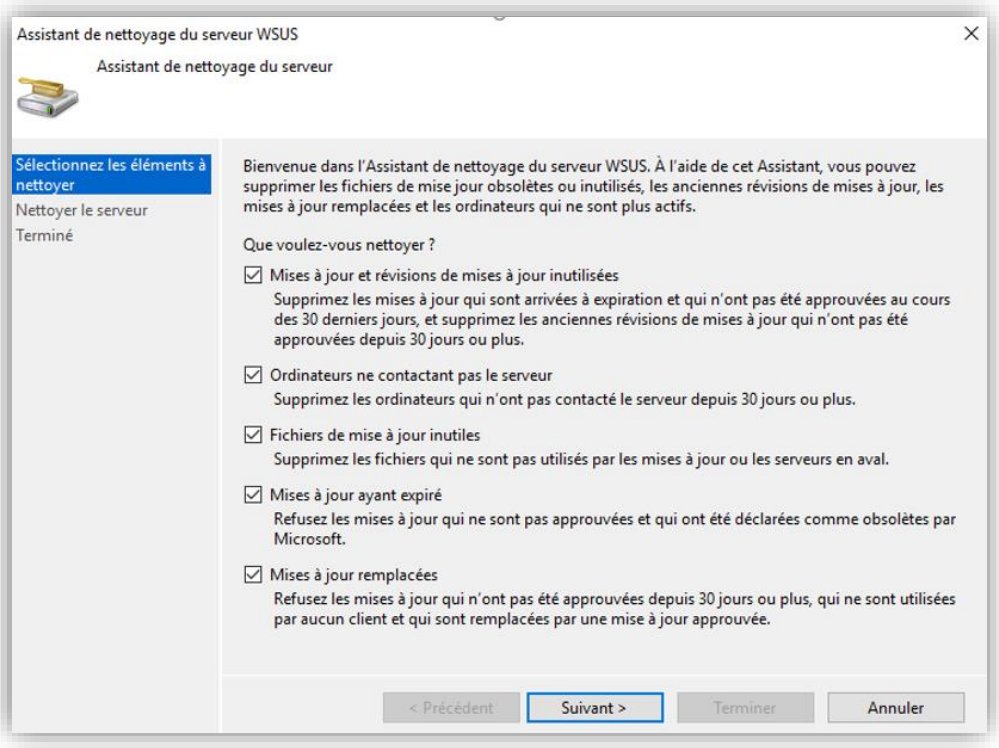
- Cette GPO s'appliquent aux postes de sorte à ce qu'ils contactent le WSUS. Les postes apparaissent ensuite dans l'onglet ***Ordinateurs non attribués*** sur WSUS (Ils ne reçoivent aucune mise à jour dans ce groupe).
  C'est à l'administrateur de les attribuer dans le groupe Alpha ou Beta si les postes doivent recevoir les mises à jour :



- Des mails peuvent être envoyés lorsque des nouvelles mises à jour sont synchronisées ou bien des rapports d'état sur les mises à jour.

Nettoyage du serveur de fichiers

- Le serveur WSUS sera régulièrement nettoyé pour ne pas saturer le disque dur au moyen d'un assistant de nettoyage intégré au serveur WSUS pour supprimer les mises à jour inutilisées, remplacées ou expirées :

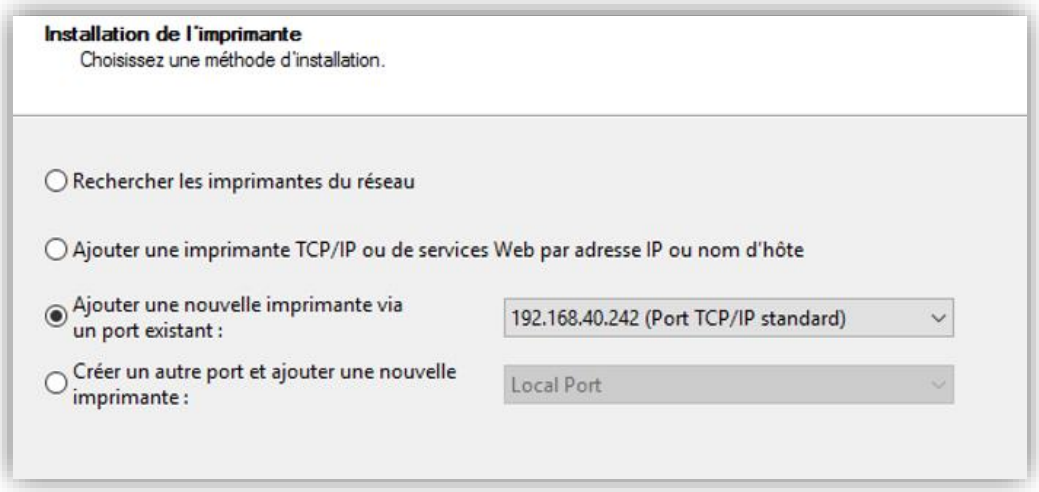


9.2.4. Configuration du serveur d'impression

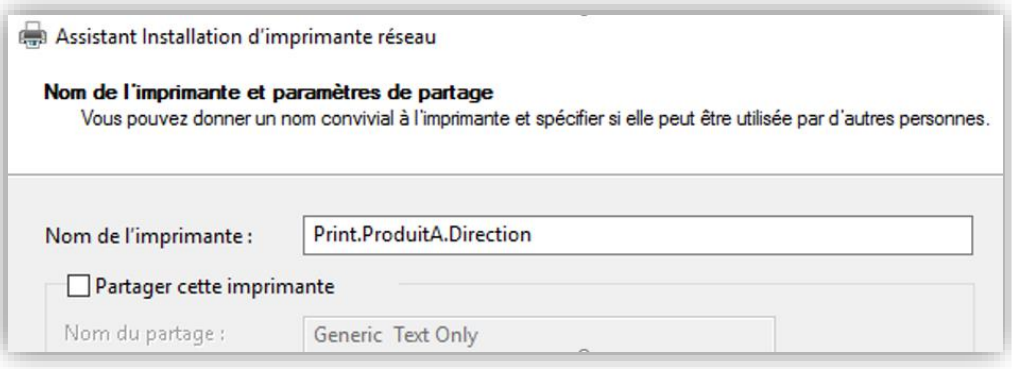
Configuration des attributions et des imprimantes virtuelles

Suite à l'installation du serveur d'impression traité dans la partie, nous montrons ici comment on configure les imprimantes ainsi que leur attribution aux groupes utilisateurs.

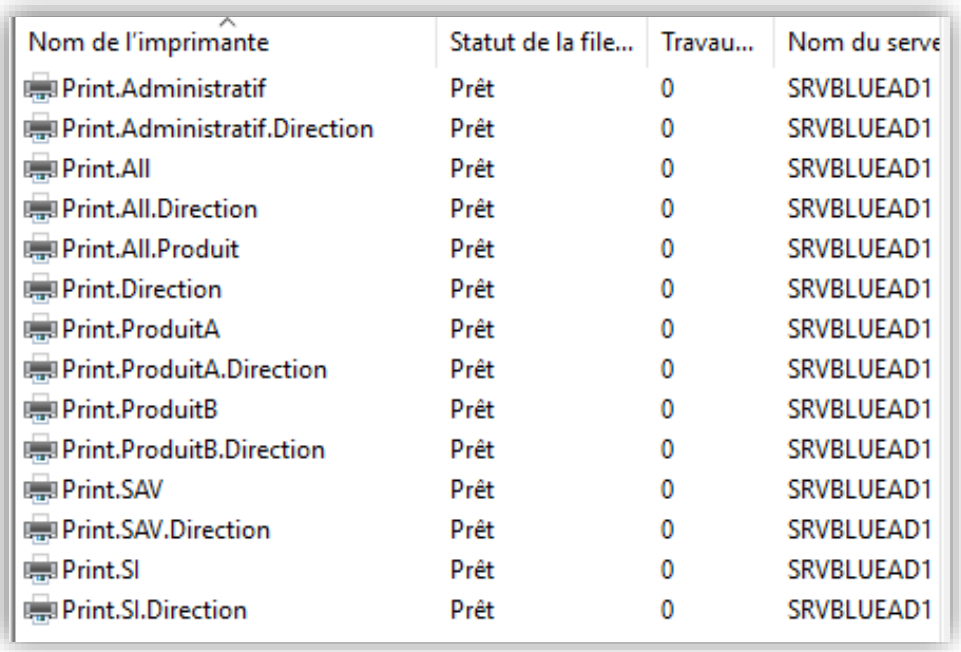
- Créer plusieurs imprimantes virtuelles sur un même port : ceci permettra d'appliquer des permissions différentes selon les groupes. ***Ajouter une nouvelle imprimante via un port existant*** puis renseigner la même adresse IP de l'imprimante en question :



- Configurer son nom en précisant la fonction de cette imprimante virtuelle, afin de pouvoir gérer les imprimantes plus facilement. Ici, on partage l'imprimante du service Produit A avec la direction. Le but va être de donner davantage de priorité aux impressions provenant de la Direction :

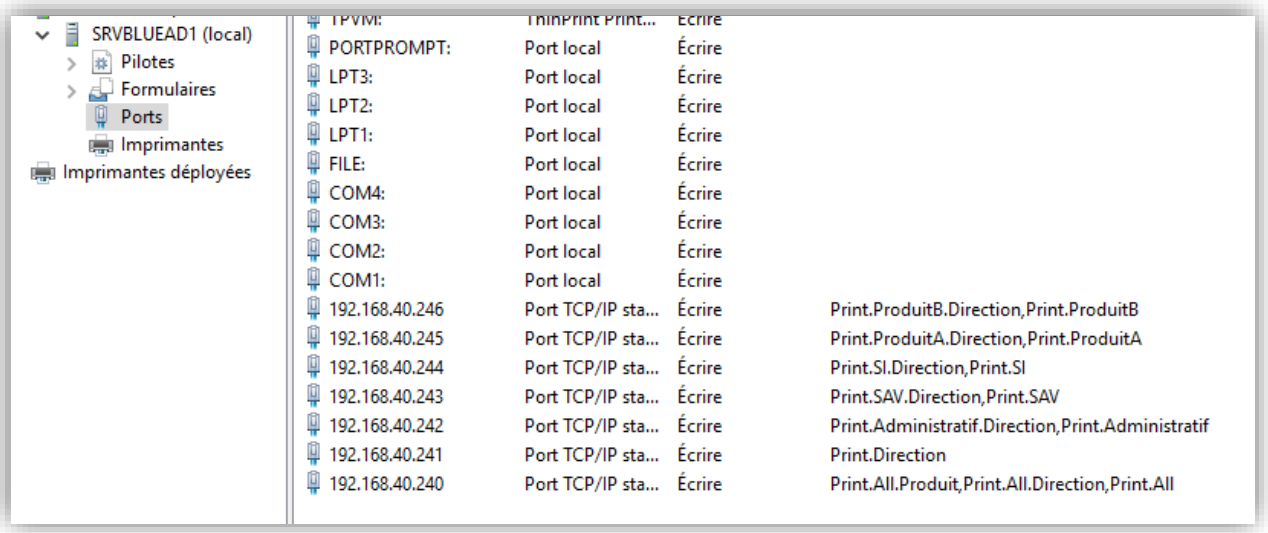


- Ajouter l'ensemble des imprimantes virtuelles nécessaires :

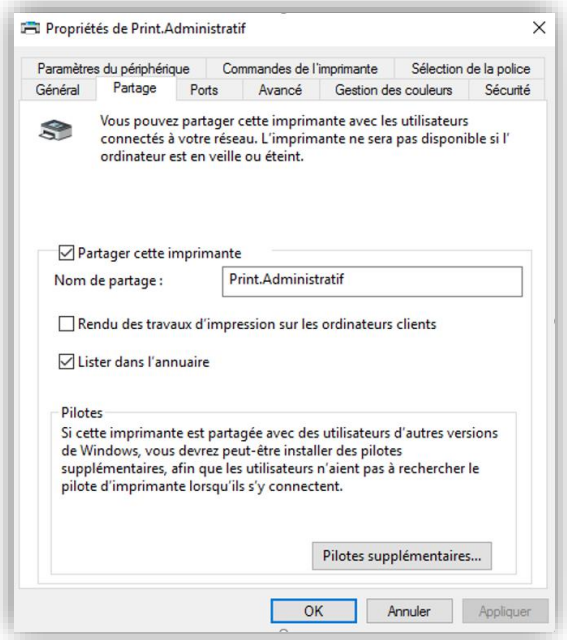


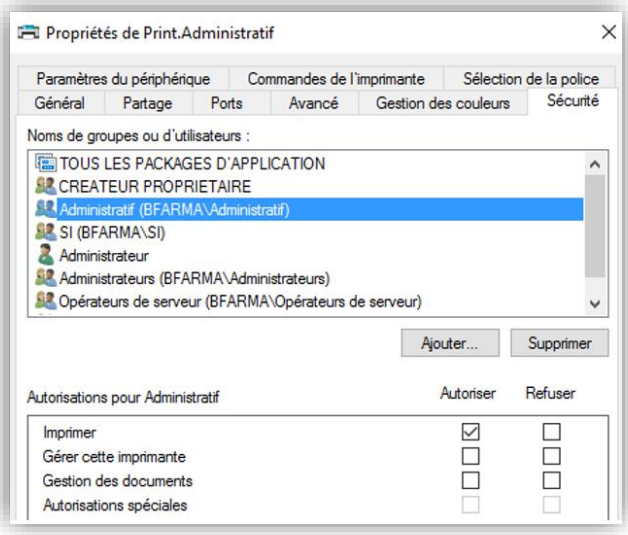
Nom de l'imprimante	Statut de la file...	Travau...	Nom du serve
Print.Administratif	Prêt	0	SRVBLUEAD1
Print.Administratif.Direction	Prêt	0	SRVBLUEAD1
Print.All	Prêt	0	SRVBLUEAD1
Print.All.Direction	Prêt	0	SRVBLUEAD1
Print.All.Produit	Prêt	0	SRVBLUEAD1
Print.Direction	Prêt	0	SRVBLUEAD1
Print.ProduitA	Prêt	0	SRVBLUEAD1
Print.ProduitA.Direction	Prêt	0	SRVBLUEAD1
Print.ProduitB	Prêt	0	SRVBLUEAD1
Print.ProduitB.Direction	Prêt	0	SRVBLUEAD1
Print.SAV	Prêt	0	SRVBLUEAD1
Print.SAV.Direction	Prêt	0	SRVBLUEAD1
Print.SI	Prêt	0	SRVBLUEAD1
Print.SI.Direction	Prêt	0	SRVBLUEAD1

- Se rendre dans l'onglet ***Ports*** pour vérifier quelles imprimantes sont associées à quels ports :

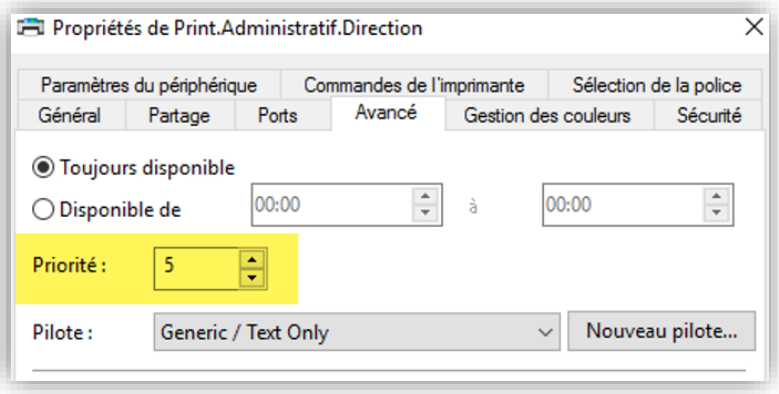


- Configurer les imprimantes pour les partager avec leur groupe utilisateur respectifs et avec la bonne priorité : se rendre dans les ***propriétés*** de l'imprimante puis cocher ***Partager cette imprimante*** et ***Lister dans l'annuaire***. Ajouter ensuite les groupes autorisés à imprimer dans l'onglet ***Sécurité***.
  Puis ajouter le groupe Service Informatique en contrôle total sur toutes les imprimantes, le groupe du service qui a uniquement le droit d'imprimer :



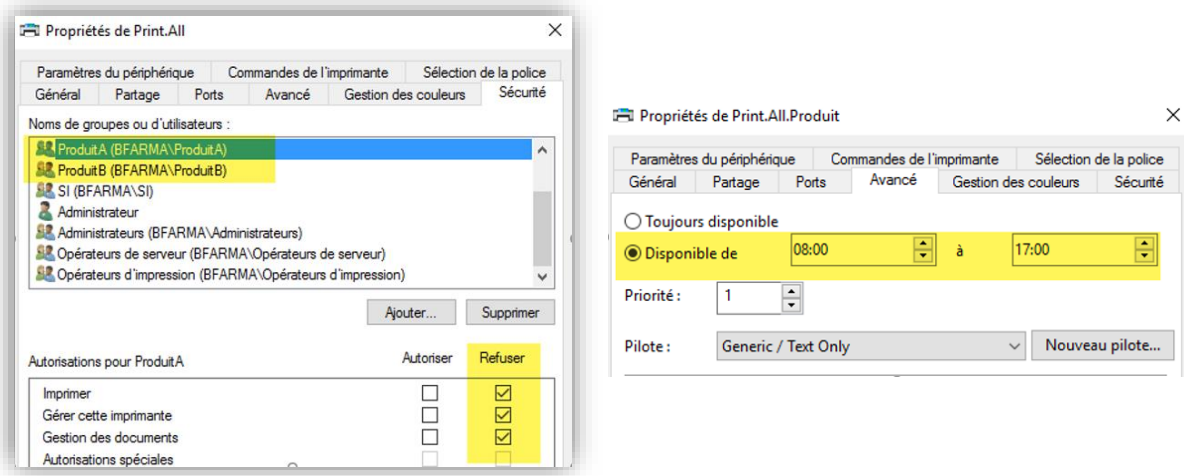


- Procéder de la même manière pour les imprimantes virtuelles partagées avec la Direction, mais en augmentant la priorité : si plusieurs personnes, par exemple du service Administratif, sont en train d'imprimer et qu'une personne de la direction lance une impression sur l'imprimante ***Print.Administratif***, c'est l'impression émanant de la Direction qui sera placée en tête de la file d'attente automatiquement (en second « job ») une fois l'impression en cours terminée. La Direction est ainsi prioritaire sur n'importe quelle imprimante :

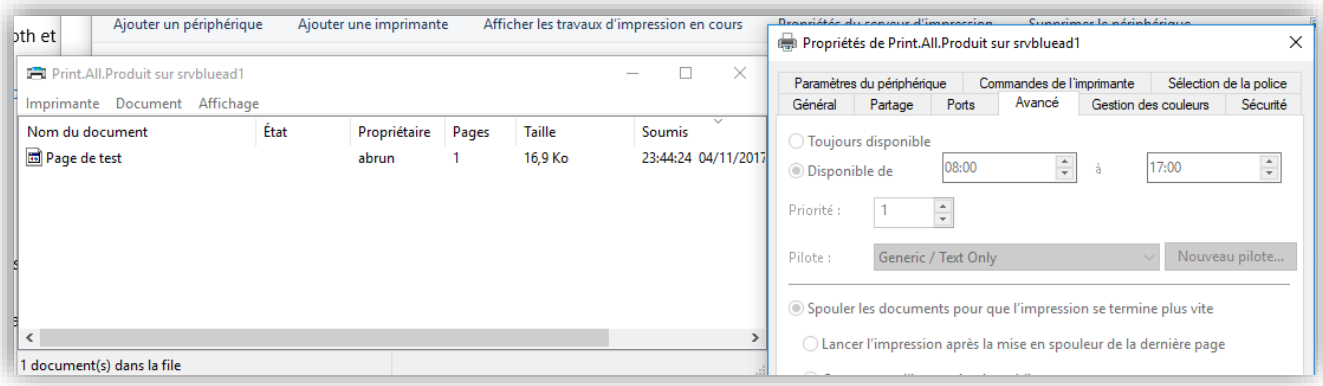


- Restreindre l'utilisation de l'imprimante ***Print.All*** (partagée entre tous les services) aux services Produit A et B seulement entre 8h et 17h : partager l'imprimante Print.All avec tout le monde mais en refusant le partage avec les groupes de sécurité ProduitA et ProduitB.

  Puis créer une nouvelle imprimante virtuelle ***Print.All.Produit***, qui sera partagée uniquement avec ProduitA et ProduitB. Enfin, configurer la disponibilité de l'imprimante de 8h à 17h via les propriétés de cette imprimante :



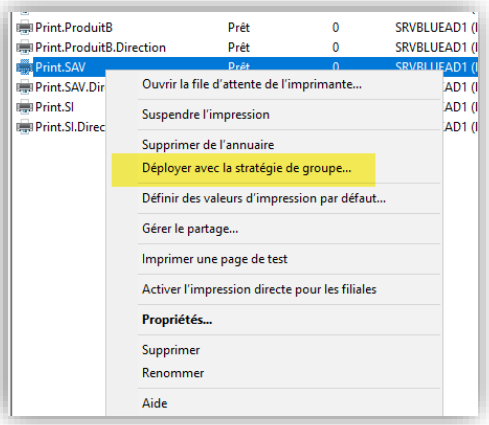
Ainsi, les impressions ne peuvent pas se lancer après 17h pour les services ProduitA et B : elles seront mises en attente :



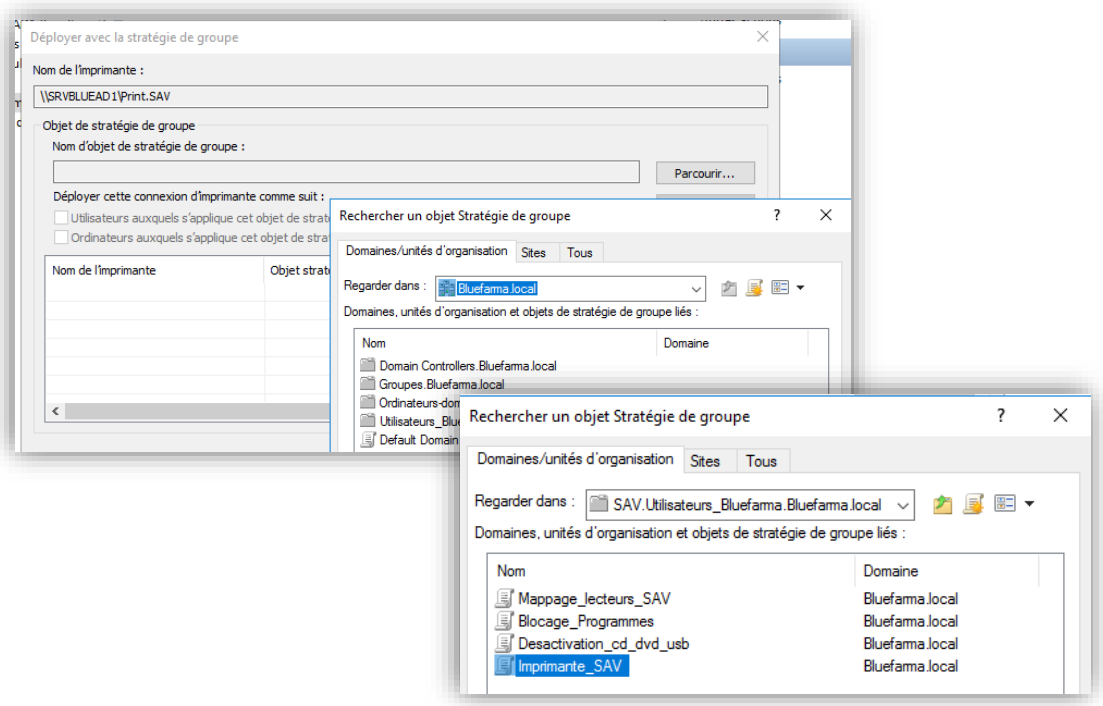
Concernant les assistantes des services SAV et Direction qui peuvent imprimer au Service Informatique et Produit A et B, nous les ajouterons à un ***groupe de sécurité*** « ***Assistantes*** » et autoriseront simplement ce groupe à imprimer sur les imprimantes respectives :

Déploiement des imprimantes par stratégie de groupe

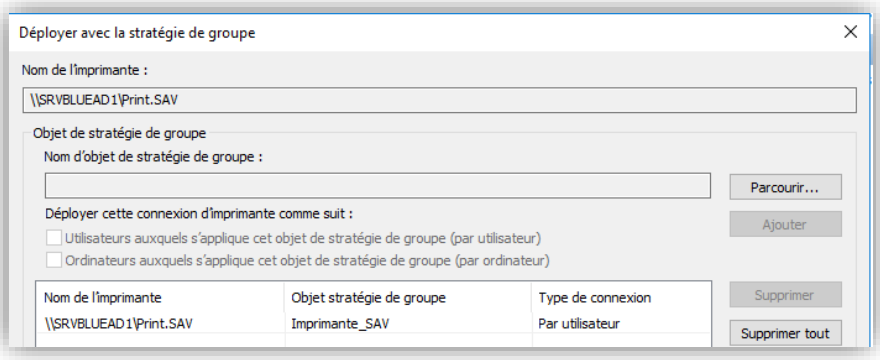
- Déployer les imprimantes afin que les utilisateurs aient directement leurs imprimantes respectives connectées sur leur poste sans avoir à effectuer de manipulation supplémentaire.
  Créer une stratégie de groupe via le rôle ***Gestion de stratégie de groupe*** ou par ***Gestion de l'impression*** » > clic droit puis ***Déployer avec la stratégie de groupe*** sur l'imprimante que nous souhaitons partager :



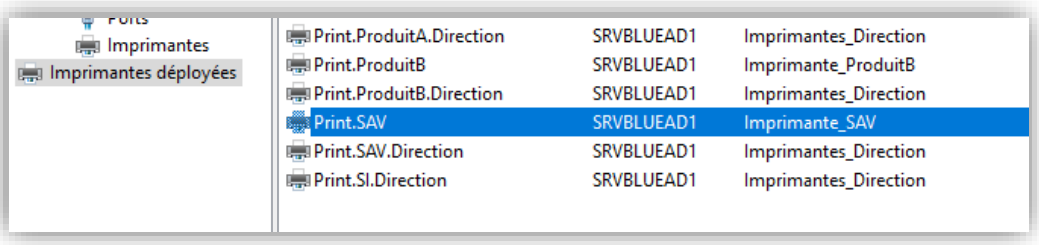
- Cliquer sur ***parcourir*** pour sélectionner l'***OU*** où va se situer la GPO afin de définir à qui elle s'appliquer.
  Pour l'imprimante ***Print.SAV***, se placer dans l'OU ***SAV*** puis créer une nouvelle GPO ***Imprimante_SAV*** :



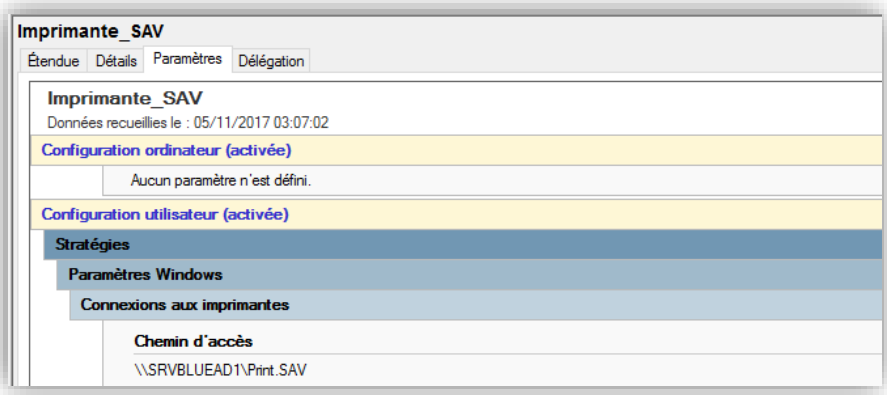
- Déployer les imprimantes pour les utilisateurs en cochant la case à cet effet puis cliquer sur ***Ajouter*** et valider :



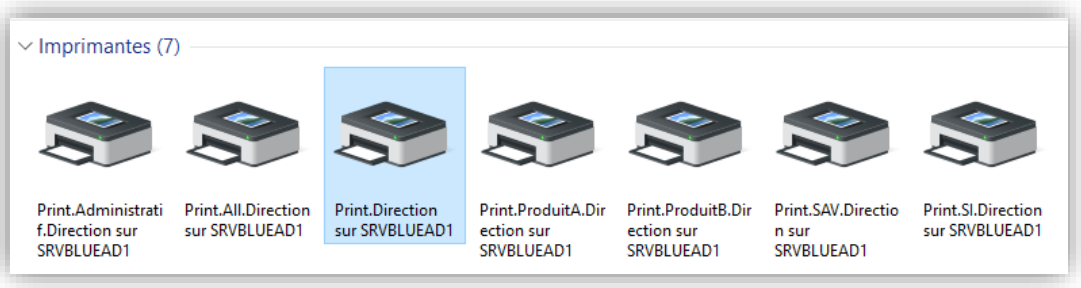
- Les imprimantes déployées par stratégie de groupe sont répertoriées dans ***Imprimantes déployées*** dans l'outil de gestion des impressions :



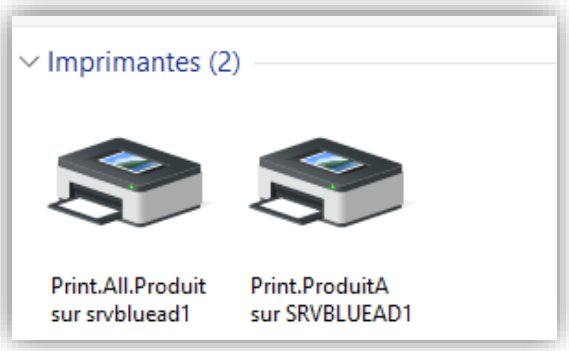
- Se rendre ensuite dans la gestion des stratégies de groupe pour vérifier la création de la GPO de mappage des imprimantes :

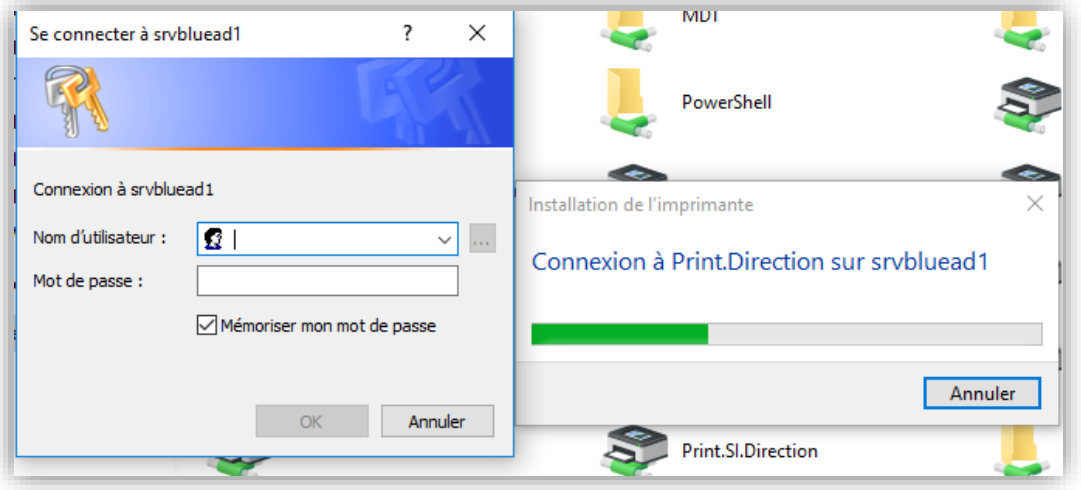


- Depuis le poste de Mme Ada, l'assistante de Direction, on visualise un accès à toutes les imprimantes qui sont connectées automatiquement à son poste grâce à une priorité plus élevée :



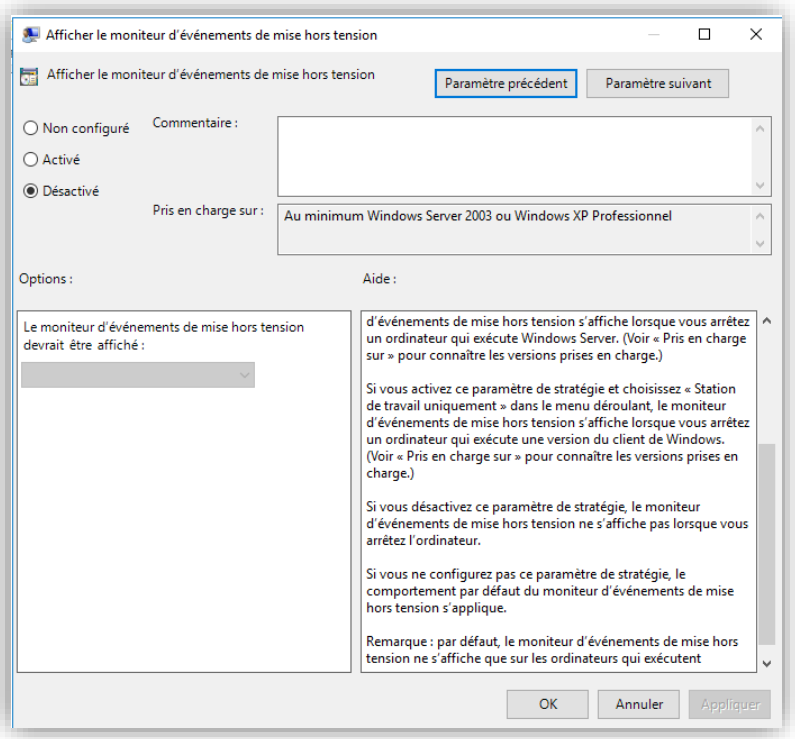
- Depuis le poste d'Adrien Roy du service Produit A, on constate qu'il possède qu'un accès uniquement sur les imprimantes qui lui sont réservées. S'il essaye d'accéder à une autre imprimante partagée, il lui sera demandé des identifiants d'accès autorisés à se connecter à l'imprimante :



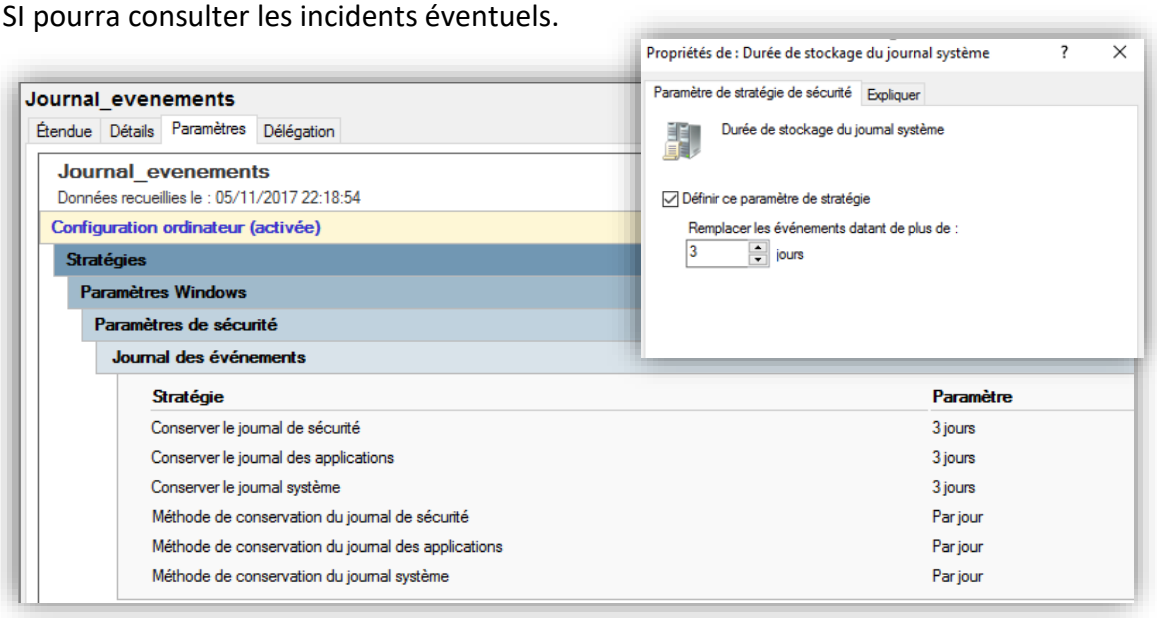


9.2.6. Maintenance des systèmes

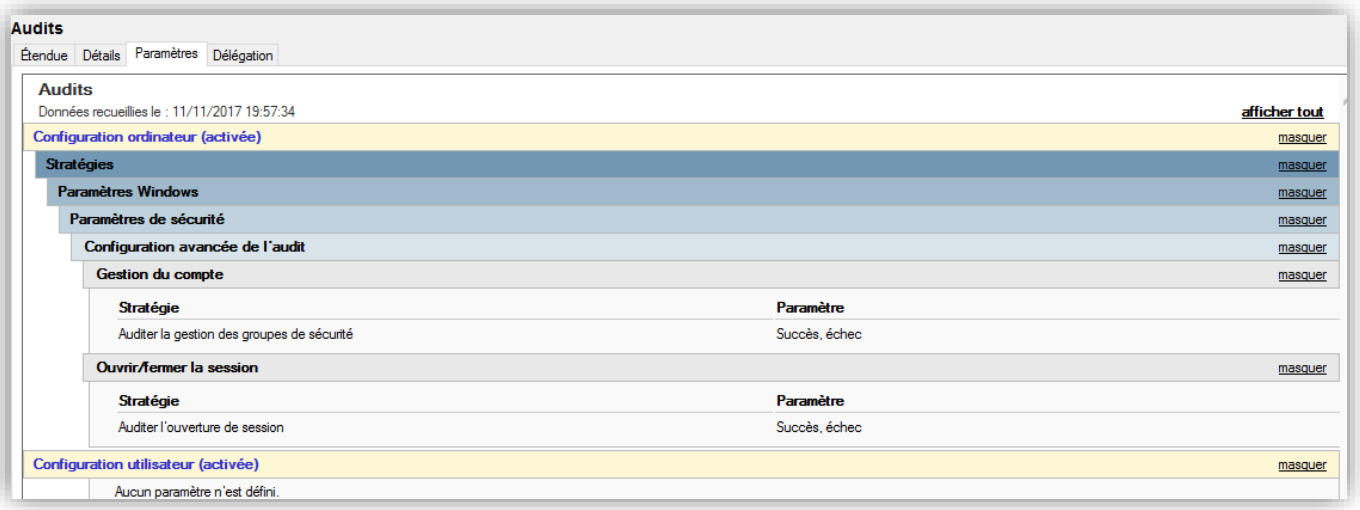
Le cahier des charges stipule le besoin de désactiver le moniteur d'évènements sur les postes :



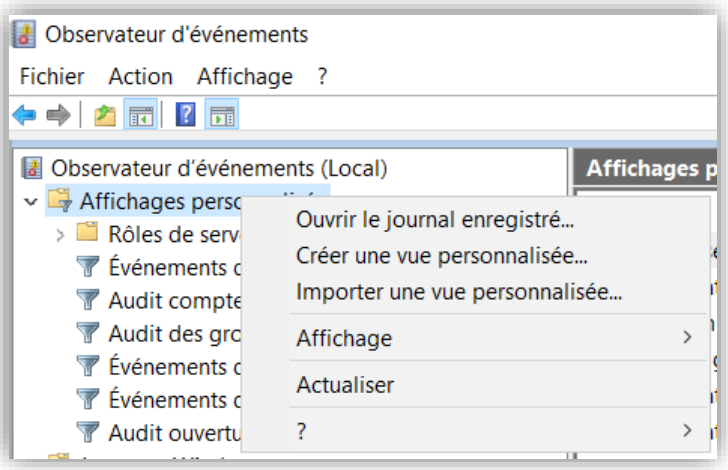
Nous configurons également 3 journaux à 3 jours sur l'ensemble des postes. De cette façon, le SI pourra consulter les incidents éventuels.



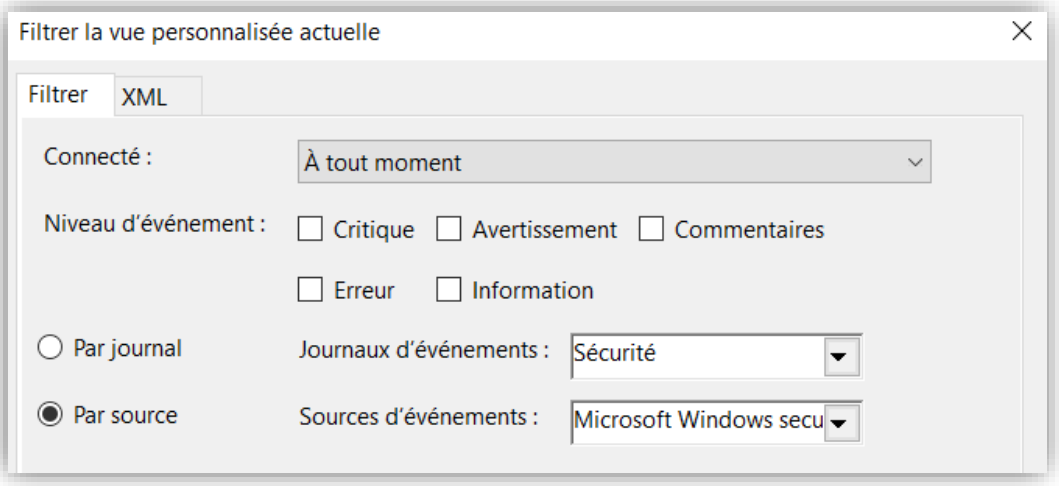
- Configurer les audits pour auditer la création de groupes de sécurité, et l'ouverture/fermeture de session. Pour cela, on créé une GPO à la racine du domaine :



- Il faut ensuite se rendre dans l'observateur d'évènements (***eventvwr***) et configurer une vue personnalisée, afin de filtrer les identifiants (ID) correspondant à nos audits :

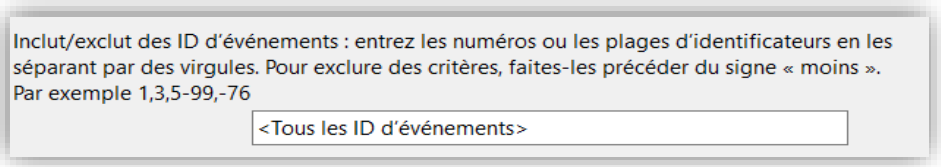


- On configure « par source » et on sélectionne « Microsoft Windows security auditing ».



Cela va nous permettre de réduire le champ de recherche et donc de réduire le temps d'actualisation de la requête effectuée.

- Renseigner les ID d'évènements en rapport avec notre audit :



Pour l'audit concernant les groupes de sécurité, les ID correspondant sont les suivants : 4727,4728,4729,4730,4731,4732,4733,4734,4735,4737,4754,4755,4756,4757,4758,4764

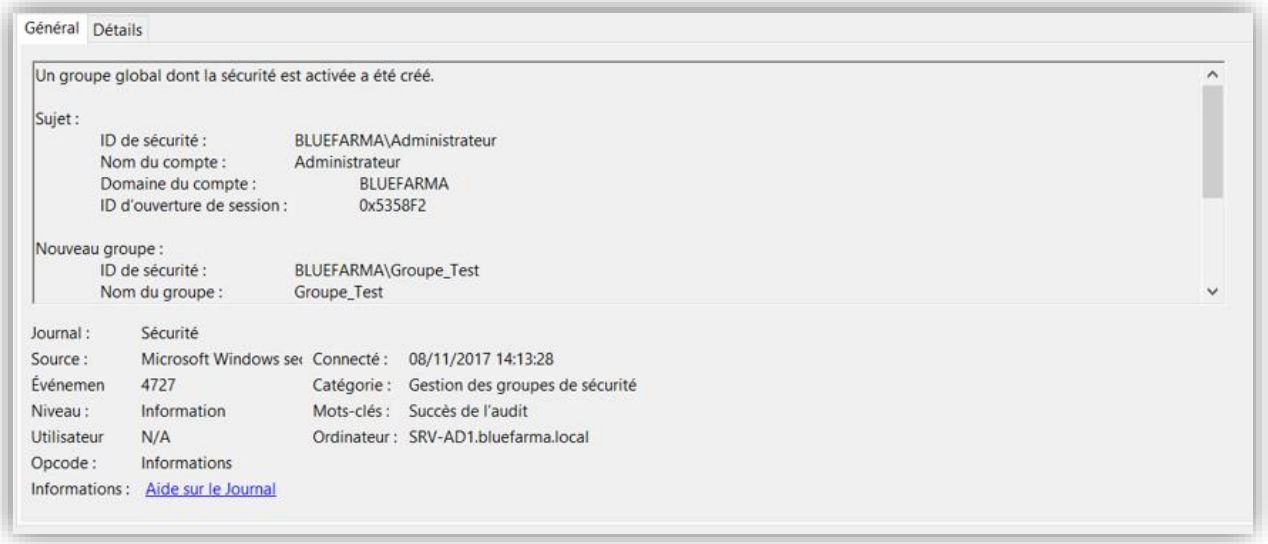
Pour l'audit concernant les ouvertures et fermetures de session, les ID sont les suivants : 4624,4634

Après avoir validé la vue personnalisée, les différents évènements correspondants s'affichent. Par exemple, pour l'audit « groupes de sécurité » :

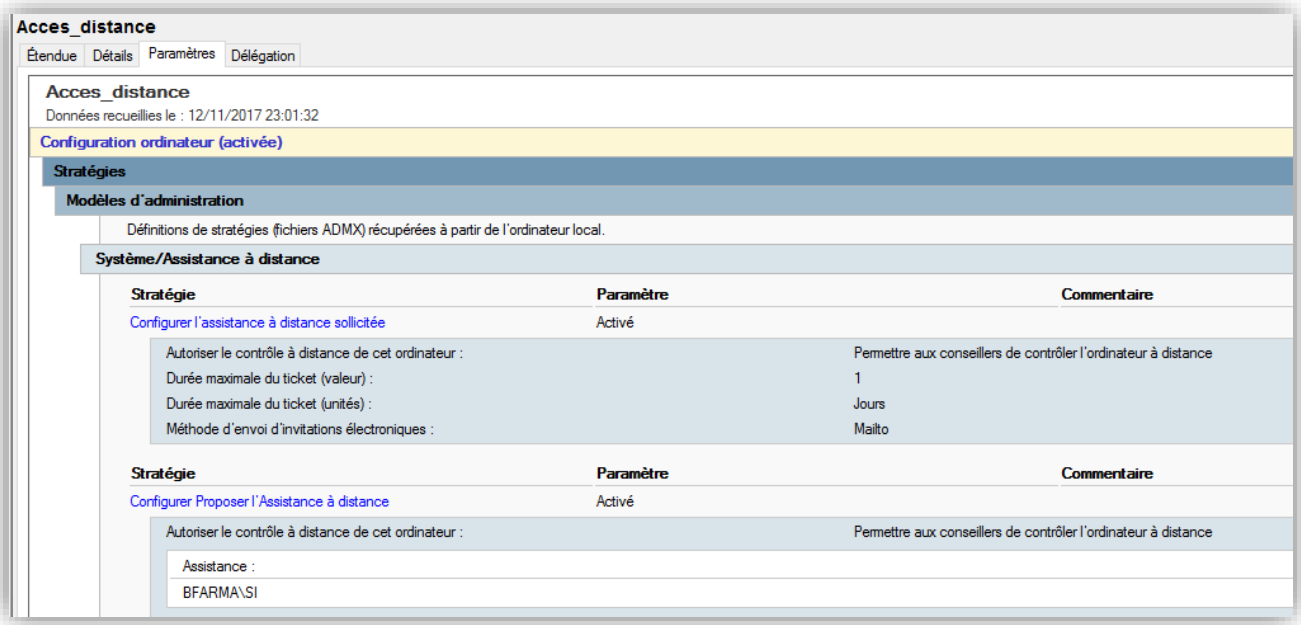
Niveau	Date et heure	Source	ID de l'événement
Information	08/11/2017 11:39:15	Microsoft Windows security auditi...	4730
Information	08/11/2017 11:39:15	Microsoft Windows security auditi...	4730
Information	08/11/2017 11:38:55	Microsoft Windows security auditi...	4727
Information	08/11/2017 11:37:51	Microsoft Windows security auditi...	4727
Information	29/10/2017 12:31:02	Microsoft Windows security auditi...	4727
Information	24/10/2017 21:32:46	Microsoft Windows security auditi...	4728
Information	24/10/2017 21:32:46	Microsoft Windows security auditi...	4728
Information	24/10/2017 21:32:46	Microsoft Windows security auditi...	4728
Information	24/10/2017 21:32:46	Microsoft Windows security auditi...	4728
Information	24/10/2017 21:32:46	Microsoft Windows security auditi...	4728
Information	24/10/2017 21:32:46	Microsoft Windows security auditi...	4728

- Vérifier que l'audit fonctionne, en créant un groupe dans l'AD appelé **Groupe_Test**. On peut voir dans l'observateur qu'un nouvel évènement est apparu. L'ID 4727 correspond à la création d'un groupe de sécurité.

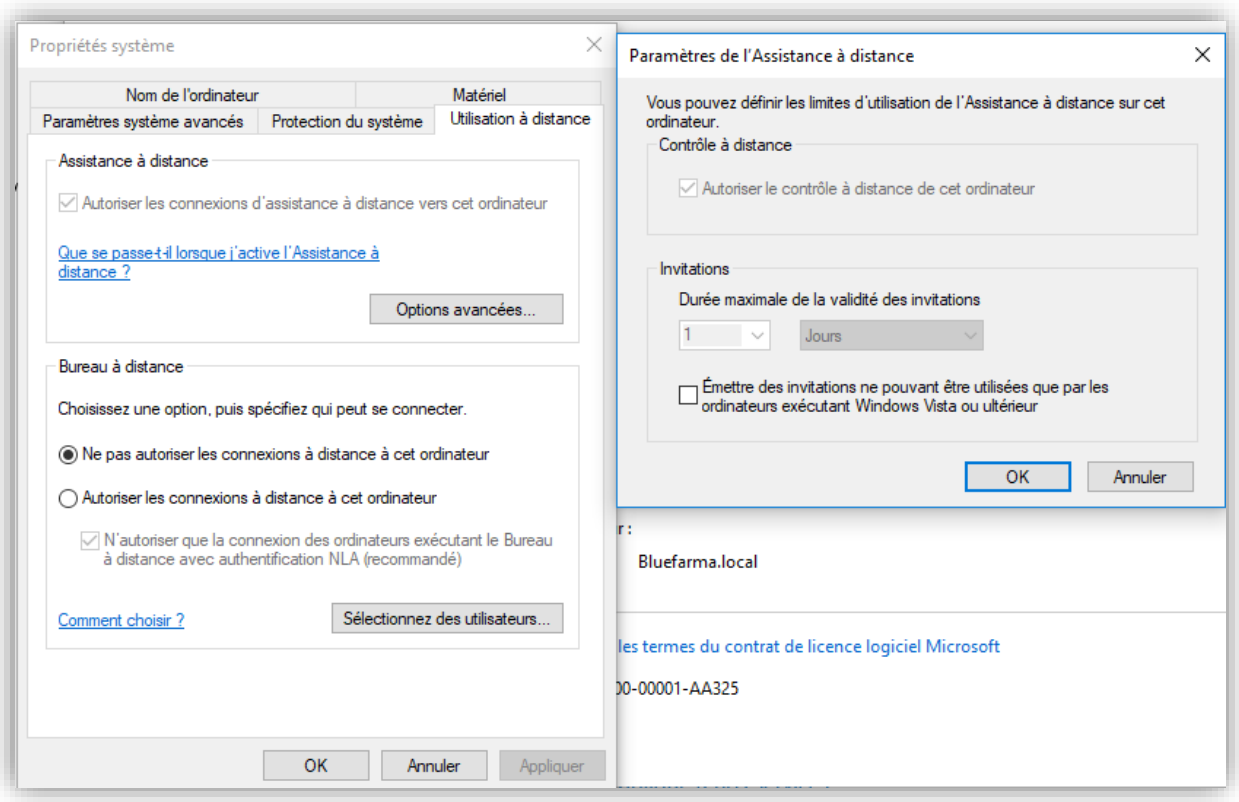
Quand on ouvre l'évènement, on peut voir les détails et notamment le nom du groupe :



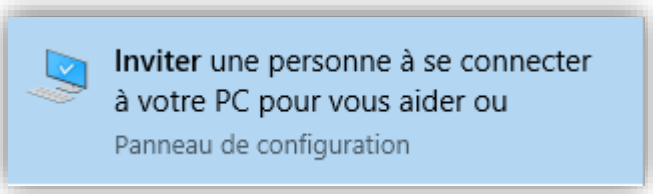
- Pour permettre l'accès à distance des postes, il existe une fonctionnalité intégrée à Windows : l'assistance à distance.
- On peut donc configurer une GPO afin de paramétrer l'ordinateur pour proposer l'assistance à distance aux utilisateurs.



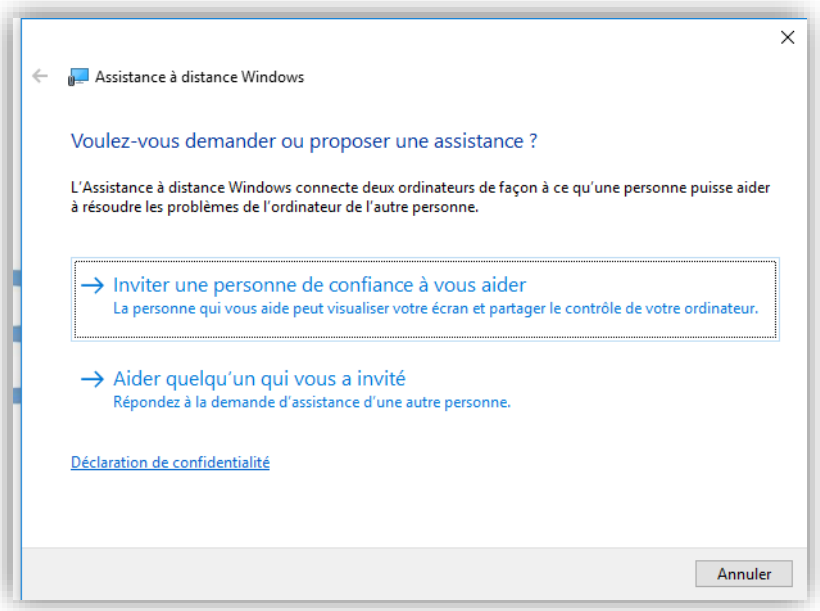
La GPO est bien prise en compte par les postes :

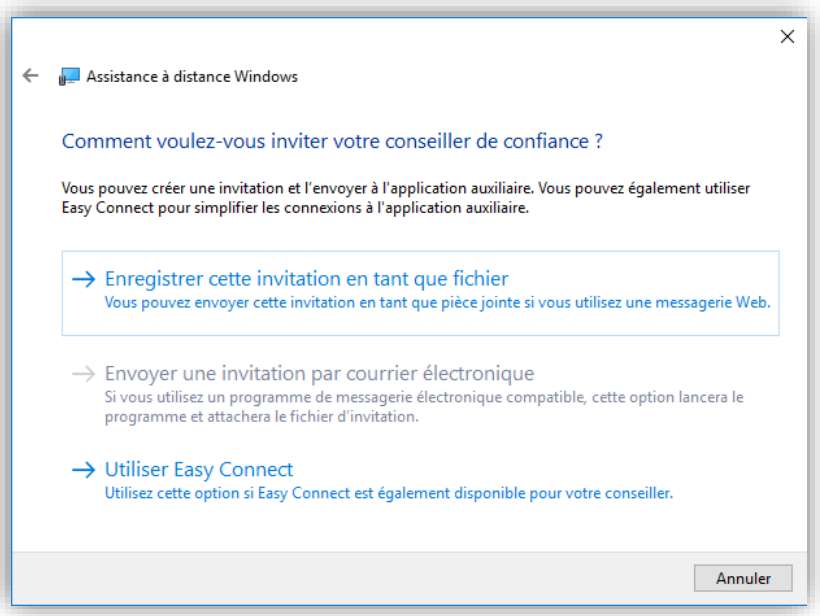


L'utilisateur doit ensuite inviter une personne à prendre contrôle sur le PC :

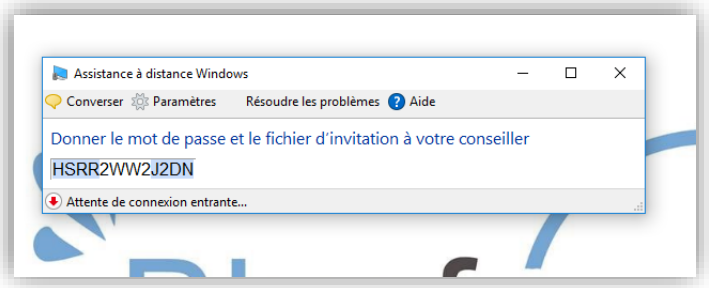


Il est possible de créer une invitation par fichier et de l'envoyer par mail, par exemple :

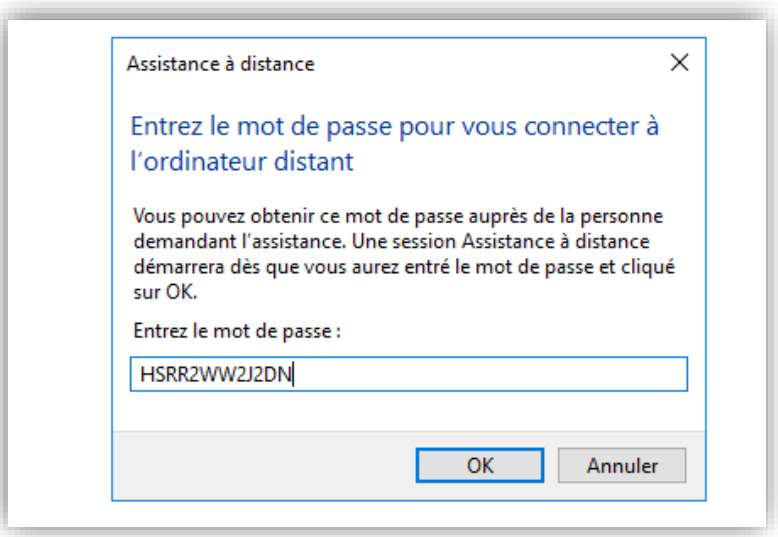




- Après avoir créé le fichier, un mot de passe est à transmettre également :



La personne prenant le contrôle doit lancer le fichier et entrer le mot de passe afin de prendre la main sur le poste :



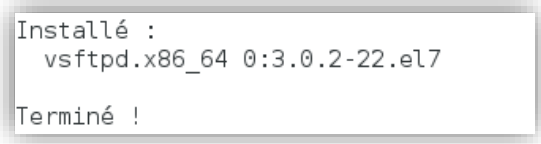
- L'accès est ensuite effectif. Il est possible de n'avoir que le visuel, ou bien de contrôler le poste et effectuer n'importe quelle action. Un système de tchat est également présent afin de communiquer avec l'utilisateur.

9.3. CONFIGURATION DU SERVEUR LINUX

9.3.1. Installation du serveur FTP

- Installer le **paquet vsftpd**.

```
yum install vsftp
```



- Faire que le service **démarre automatiquement** au démarrage du système.

```
systemctl enable vsftpd
```

- Supprimer le fichier ftpusers qui ne nous sera pas utile puisqu'il interdit certaines connexions.

```
rm /etc/vsftpd/ftpusers
```

- Configurer le fichier **vsftpd.conf**.

```
vim /etc/vsftpd/vsftpd.conf
```

Contenu du fichier de configuration :

```
#port d'écoute telnet
listen_port=21
#bannière
ftpd_banner=Bienvenue sur le ftp de la société Bluefarma
#fichier de configuration PAM
pam_service_name=vsftpd
#mode standalone=service permettant au serveur de tourner en permanence
listen=YES
#connexion anonyme
anonymous_enable=YES
#connexion des utilisateurs locaux virtuels
local_enable=YES
#fichier des utilisateurs locaux
userlist_file=/etc/vsftpd/user_list
#chargement de user_list
userlist_enable=YES
#refus des utilisateurs de la liste
userlist_deny=YES
#interdiction d'utiliser les commandes influant sur le système de fichier
write_enable=NO

#l'utilisateur virtuel peut télécharger des fichiers sans être world readable
anon_world_readable_only=NO
#interdiction d'uploader des fichiers
anon_upload_enable=NO
#interdiction de créer un répertoire
anon_mkdir_write_enable=NO
#interdiction de créer, supprimer ou renommer un répertoire
anon_other_write_enable=NO

#mapper les utilisateurs non-anonyme (guest) sur le compte local ftp
guest_enable=YES
guest_username=ftp
#chroot des utilisateurs
chroot_local_user=YES
#nombre de connexions simultanées possibles
max_clients=40
#nombre maximum de connexions provenant d'une même IP
max_per_ip=4
#répertoire de configuration spécifique des utilisateurs
user_config_dir=/etc/vsftpd/vsftpd_user_conf
#activation du log
xferlog_enable=YES
```

9.3.2. Intégration de Centos au domaine Active Directory et configuration du serveur samba

Prérequis :

- Le DNS doit être correctement configuré du côté de SRV-AD1.
- SRV-AD1 et SRV-NUX1 doivent être correctement synchronisés avec leur serveur de temps NTP (important pour Kerberos).
- Les ports suivants doivent être ouverts dans le firewall : En TCP/UDP, 135, 137, 445 et 138, 139 et UDP.

- Installer la suite de paquets suivants sur la machine Linux SRV-NUX1 :

```
yum install samba samba-common samba-winbind samba-winbinb-client krb5-workstation krb5-libs oddjob-mkhomedir oddjob pam_krb5 nss samba-client
```

NB : samba et samba-common sont normalement installés

- Éditer le fichier de configuration **/etc/krb5.conf** : indiquer dans les sections colorées en jaune le nom de domaine Bluefarma et celui de machine (srv-ad1.bluefarma.local).

```
includedir /etc/krb5.conf.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = BLUEFARMA.LOCAL
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
BLUEFARMA.LOCAL  = {
  kdc = srv-ad1.bluefarma.local
  admin_server = srv-ad1.bluefarma.local
  default_domain = bluefarma.local
 }

[domain_realm]
 .bluefarma.local = BLUEFARMA.LOCAL
bluefarma.local = BLUEFARMA.LOCAL
```

- Vérifier que les paramètres sont corrects avec le compte administrateur de l'AD au moyen de la commande suivante :
- `kinit Administrateur`
  Le mot de passe de l'Administrateur de l'AD est demandé :

```
[root@SRV-NUX1 pchirol]# kinit Administrateur
Password for Administrateur@BLUEFARMA.LOCAL:
```

- Vérifier que l'utilisateur Administrateur a bien obtenu un ticket de la part de Kerberos avec la commande **klist** :

```
[root@SRV-NUX1 pchirol]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrateur@BLUEFARMA.LOCAL

Valid starting       Expires              Service principal
10/11/2017 00:04:02  10/11/2017 10:04:02  krbtgt/BLUEFARMA.LOCAL@BLUEFARMA.
LOCAL
        renew until 17/11/2017 00:00:20
```

- Éditer le fichier de configuration **/etc/samba/smb.conf** au niveau de la section [**global**] :

```
[global]
        workgroup = BLUEFARMA
        realm = BLUEFARMA.LOCAL
        security = ADS
        log level = 3
        log file = /var/log/samba/%m
        max log size = 50
        printcap name = cups
        printing = cups
        winbind enum users = yes
        winbind enum groups = yes
        winbind use default domain = yes
        winbind nested groups = yes
        winbind separator = /
        idmap uid = 600-20000
        idmap gid = 600-20000
        template shell = /bin/bash
        passdb backend = tdbsam
        printing = cups
        printcap name = cups
        load printers = yes
        cups options = raw
```

- Configurer le dossier ***/home/partage_commun*** qui permettra de partager des données avec le SAV (postes Linux) et le dossier ***/home/BLUEFARMA*** qui hébergera chaque dossier personnel des utilisateurs de Windows.

```
[partage BLUEFARMA]
        comment = répertoire pour les dossiers des utilisateurs
        path = /home/users/%u
        valid users = @"BLUEFARMA/Utilisateurs du domaine"
        browseable = no
        read only = no

[partage commun]
        comment = répertoire d'échange de fichiers
        path = /home/partage_commun
        valid users = @"BLUEFARMA/Utilisateurs du domaine"
        browseable = yes
        read only = no
        writable = yes
        directory mask = 0777
        create mask = 0777
```

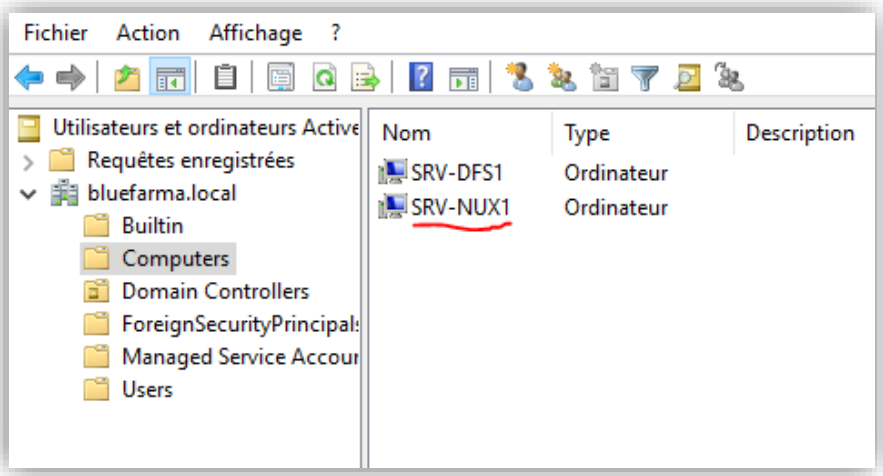
- Procéder à la jonction du domaine avec le compte administrateur du domaine AD avec la commande **net join -U Administrateur** :

```
[root@SRV-NUX1 pchirol]# net join -U Administrateur
Enter Administrateur's password:
Using short domain name -- BLUEFARMA
Joined 'SRV-NUX1' to dns domain 'bluefarma.local'
```

- Vérifier que la jonction s'est bien déroulée par la commande **net ads testjoin** :

```
[root@SRV-NUX1 pchirol]# net ads testjoin
Join is OK
```

On peut aussi se rendre dans le gestionnaire ***Utilisateurs et ordinateurs Active Directory*** sur SRV-AD1 pour voir apparaître notre machine SRV-NUX1 :



- Configurer Winbind via la commande **authconfig** :

```
[root@SRV-NUX1 ~]# authconfig --enablewinbind --enablemd5 --enableshadow --enablewin
bindauth --enablelocauthorize --enablemkhomedir --update
```

- Modifier la configuration de **PAM** en éditant **/etc/nsswitch.conf** :

```
# /etc/nsswitch.conf

passwd:     files winbind
shadow:     files winbind
group:      files winbind

hosts:      files dns wins
```

- Vérifier l'accès aux comptes utilisateurs ou aux groupes de l'AD :

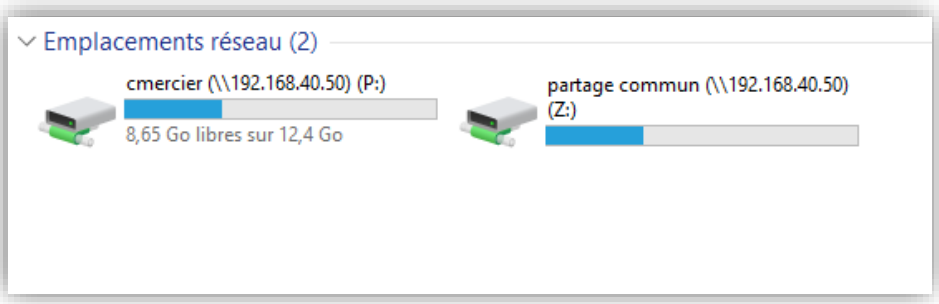
Avec ***wbinfo -u*** : (liste non exhaustive)

```
[root@SRV-NUX1 pchirol]# wbinfo -u
administrateur
invité
defaultaccount
krbtgt
lmercier
jada
gpasquier
arobert
lperrot
hmartinez
sribier
ngautier
cprevost
fdelaplace
ffaure
zboyer
lperez
pchirol
ngerard
qzantedeschi
ndronier
nbourgeois
olaporte
clecomte
jbeziat
cella
nayo
cacien
kbertrand
thumbert
elefevre
aaubry
jlefebvre
lchombier
rgoff
rfrancois
groussel
yaubert
gdupont
amallet
jchevalier
mmoulin
```

Avec ***wbinfo -g*** :

```
[root@SRV-NUX1 pchirol]# wbinfo -g
ordinateurs du domaine
contrôleurs de domaine
administrateurs du schéma
administrateurs de l'entreprise
éditeurs de certificats
admins du domaine
utilisateurs du domaine
invités du domaine
propriétaires créateurs de la stratégie de groupe
serveurs ras et ias
groupe de réplication dont le mot de passe rodc est autorisé
groupe de réplication dont le mot de passe rodc est refusé
contrôleurs de domaine en lecture seule
contrôleurs de domaine d'entreprise en lecture seule
contrôleurs de domaine clonables
protected users
administrateurs clés
administrateurs clés enterprise
dnsadmins
dnsupdateproxy
utilisateurs dhcp
administrateurs dhcp
administratif
direction
produita
produitb
sav
si
```

- Vérifier l'accès aux répertoire partagés de la machine linux depuis un poste client :

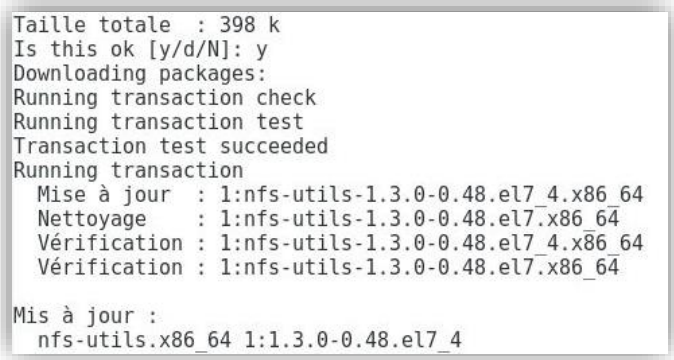


9.3.3. Configuration du partage de fichiers NFS

Configuration du serveur NFS

- Installer le paquet **nfs** :

```
yum install nfs-utils
```



- Attribuer les droits à /home :

```
mkdir /home
```

```
chmod 777 /home
```

- Éditer le fichier `/etc/exports`. C'est dans ce fichier que l'on précise que le dossier `/home/` sera partagé en ajoutant la ligne suivante.

```
/home/ 192.168.40.60(fsid=0,ro)
```

Cette ligne précise que le dossier sera partagé vers notre serveur client ayant pour IP 192.168.40.60. "**ro**" pour "***ro**nly*" précise que l'on souhaite avoir les droits seulement en écriture sur les données partagées.

- Démarrer (**start**) le service nfs puis faire que ce dernier se lance à chaque démarrage du système (**enable**).

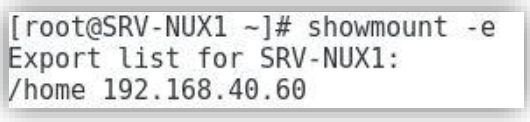
```
systemctl restart nfs.service
```

```
systemctl enable nfs.service rpcbind nfs-lock
```

- Exporter le chemin renseigner dans le fichier exports puis vérifier que le partage est bien actif.

```
exportfs -ra
```

```
showmount -e
```



- Configurer le pare-feu afin que la connexion soit possible en ajoutant les services suivants.

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --permanent --add-service=mountd
systemctl reload firewalld.service
```

Configuration du client NFS

- Créer le répertoire **partage_nfs** dans **/media** en lui attribuant des droits.

```
mkdir /media/partage_nfs
chmod 777 /media/partage_nfs
```

- Configurer un montage automatique en configurant le fichier **/etc/fstab** que l'on édite en rajoutant les lignes suivantes.
  `192.168.40.50:/home/  /media/partage_nfs nfs auto,user,ro 0 0`
  Cette opération permet de rendre le montage du partage NFS permanent, même après un redémarrage.

- Configurer le pare-feu afin que la connexion soit possible en ajoutant les services suivants.

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --permanent --add-service=mountd
```

- Monter les données contenues dans **/etc/fstab**.

```
mount -a
```

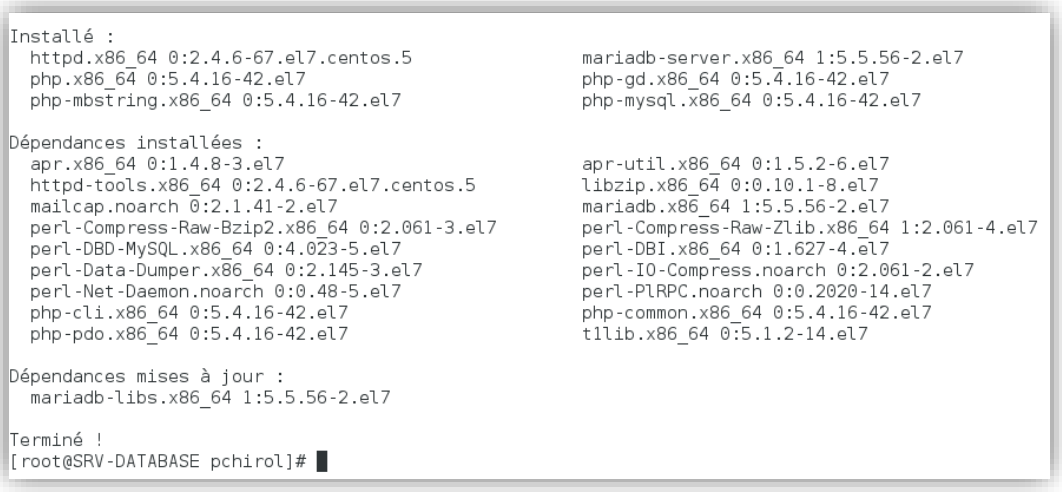
Un redémarrage complet des systèmes peut s'avérer nécessaire pour faire fonctionner le partage.

9.3.4. Installation de GLPI et de la base de données

Installation de GLPI et de ses dépendances :

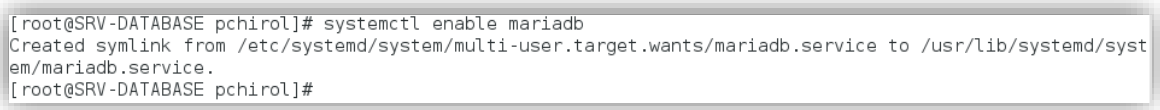
- **Installer les paquets** nécessaires à l'utilisation de GLPI :

```
yum install httpd php php-mysql php-gd php-mbstring
mariadb-server
```

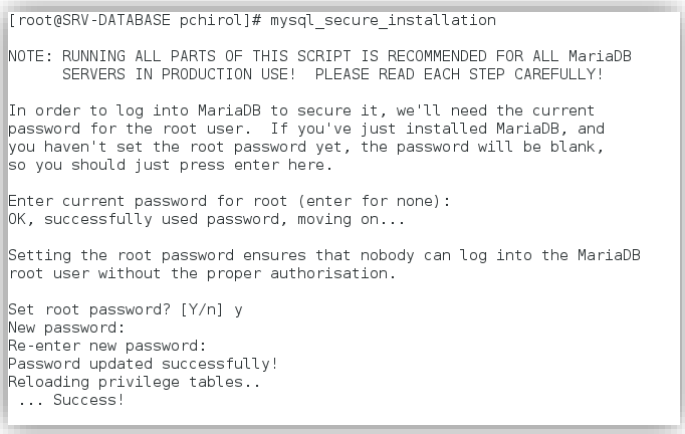


- **Lancer** et **configurer** le lancement du serveur **MariaDB** pour le prochain démarrage :

```
systemctl start mariadb
systemctl enable mariadb
```

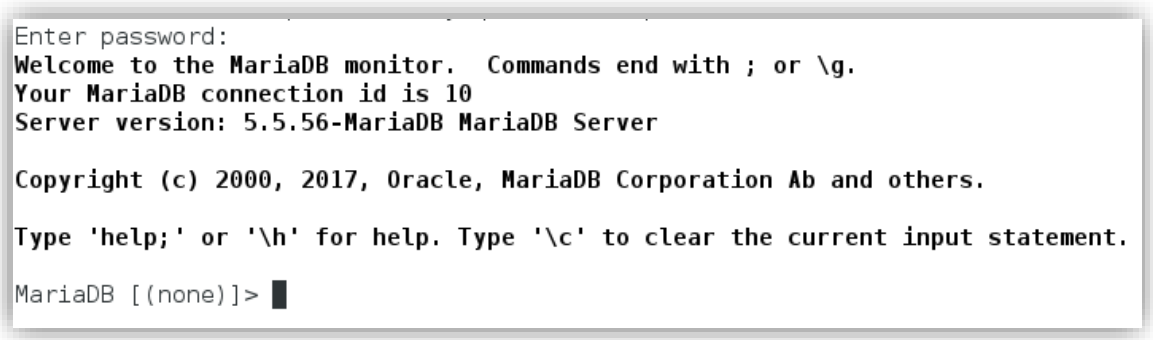


- Sécurisation de l'installation de mariadb :
- `mysql_secure_installation`



- Création de la **base de données** :

```
mysql -u root -p
```




```
MariaDB [(none)]> CREATE DATABASE bluefarmadb;

MariaDB [(none)]> GRANT ALL PRIVILEGES ON bluefarmadb .* TO
'ngerard'@'localhost' IDENTIFIED BY 'admin';

MariaDB [(none)]> quit
```

- Configuration du **serveur web** : éditer le fichier **php.ini**

```
vim /etc/php.ini
```

Renseigner ensuite la ligne suivante :

```
[Date]

date.timezone = "Europe/Paris"
```

- Interdire l'accès aux répertoire "**config**" et "**files**" : création du fichier **glpi.conf**

```
vim /etc/httpd/conf.d/glpi.conf
```

Écrire le contenu suivant :

```
<Directory "/var/www/html/glpi/config">
        AllowOverride None
        Require all denied
</Directory>

<Directory "/var/www/html/glpi/files">
        AllowOverride None
        Require all denied
</Directory>
```

- **Lancer** et **configurer** le lancement du serveur **apache/httpd** :

```
systemctl enable httpd

systemctl start httpd
```

```
[root@SRV-DATABASE pchirol]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system
/httpd.service.
```

Installation de GLPI :

- **Téléchargement et décompression de l'archive :**
  - Se rendre dans le répertoire **/src/** :
    `cd /usr/local/src`
  - Télécharger GLPI avec l'outil **wget** :

```
wget https://github.com/glpi-
project/glpi/releases/download/9.1/glpi-9.1.tar.gz
```

```
100%[=============================================================>] 32 950 680  2,31MB/s   ds 14s

2017-10-14 16:45:59 (2,23 MB/s) - «glpi-9.1.tar.gz» sauvegardé [32950680/32950680]
```

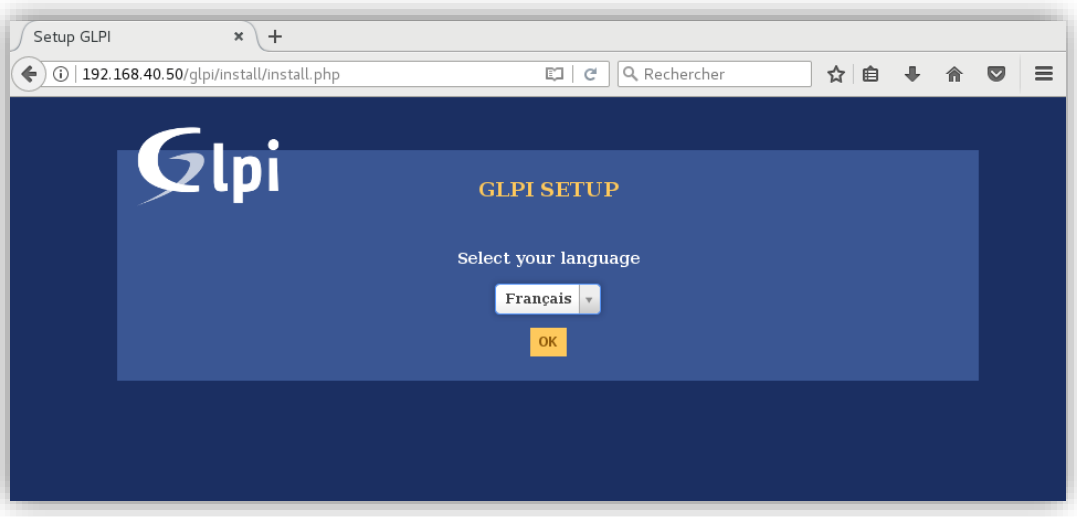
  - Décompresser l'archive "**glpi-9.1.tar.gz**" dans la racine du serveur web :

```
tar -xzvf glpi-9.1.tar.gz -C /var/www/html/
```

  - Modifier les droits de manière récursive sur le répertoire GLPI :

```
chown -R apache:apache /var/www/html/glpi/
```

- Renseigner l'adresse **https://192.168.40.50/glpi/** dans le navigateur web puis sélectionner la langue :

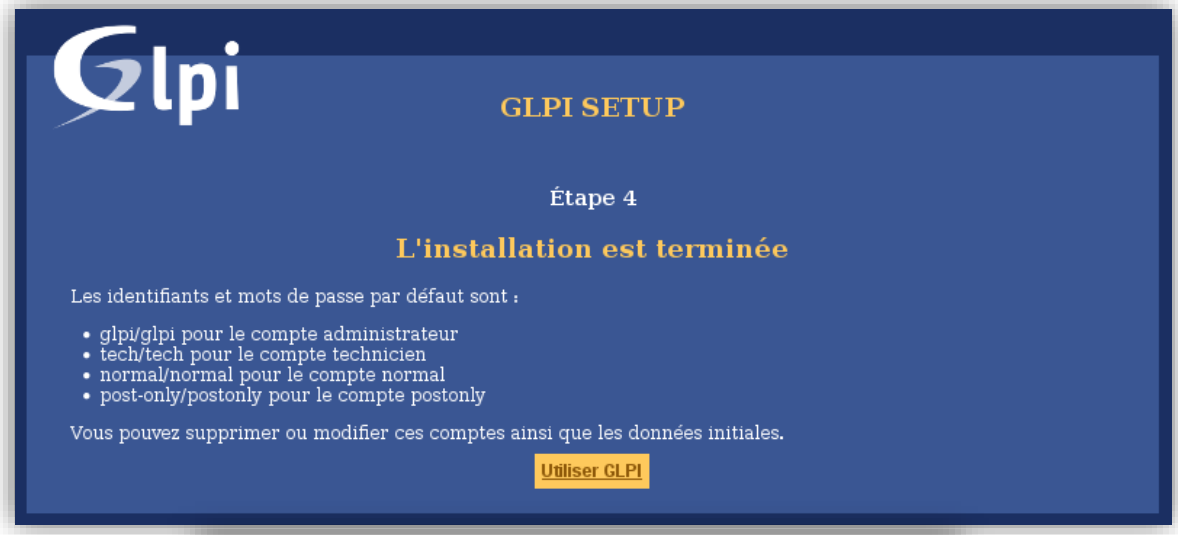


- Après avoir accepté le **contrat de licence**, cliquer sur **Installer** :

- Après quelques tests de vérifications, cliquer sur ***Continuer*** pour poursuivre l'installation :

- Renseigner les **paramètres de connexions** de la base de données :

- Sélectionner la base de données "**bluefarmadb**" que nous avons créée précédemment puis finaliser l'installation :



NB : la première connexion se fait avec les ID et mot de passe « glpi ».

9.3.5. Installation et configuration de phpMyAdmin :

Prérequis :

- S'assurer qu'Apache est bien installé (paquet **httpd**).
- Vérifier qu'Apache est bien activé en cas de reboot.

- Installation de **php** (certains des paquets sont déjà présents depuis l'installatiion de GLPI) :

```
yum install php php-mbstring php-pear
```

NB : il faut ensuite relancer Apache après cette installation.

- Le paquet phpMyAdmin se trouve dans le dépôt Fedora EPEL :

```
rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- Installer le paquet **phpMyAdmin** :

```
yum --enablerepo=epel -y install phpMyAdmin php-mysql php-mcrypt
```

- Modifier le fichier **phpMyAdmin.conf** présent dans Apache pour permettre un accès à distance depuis un autre réseau :

```
vim /etc/httpd/conf.d/phpMyAdmin.conf
```

Ensuite, renseigner le(s) pool(s) d'ip afin que les postes qui s'y trouvent puissent accéder à la page dans la section **<Directory /usr/share/phpMyAdmin/>** :

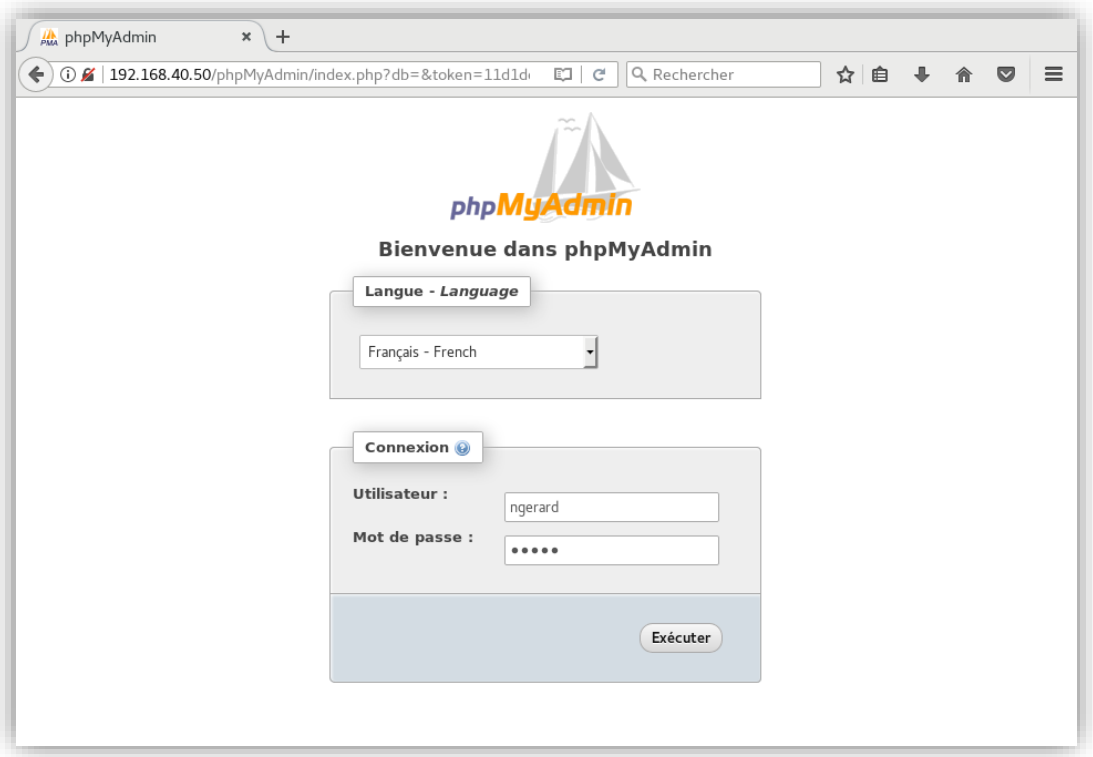
```
<Directory /usr/share/phpMyAdmin/>
   AddDefaultCharset UTF-8

   <IfModule mod_authz_core.c>
     # Apache 2.4
     <RequireAny>
       Require ip 127.0.0.1
       Require ip ::1
       Require ip 192.168.40.0/24
     </RequireAny>
```

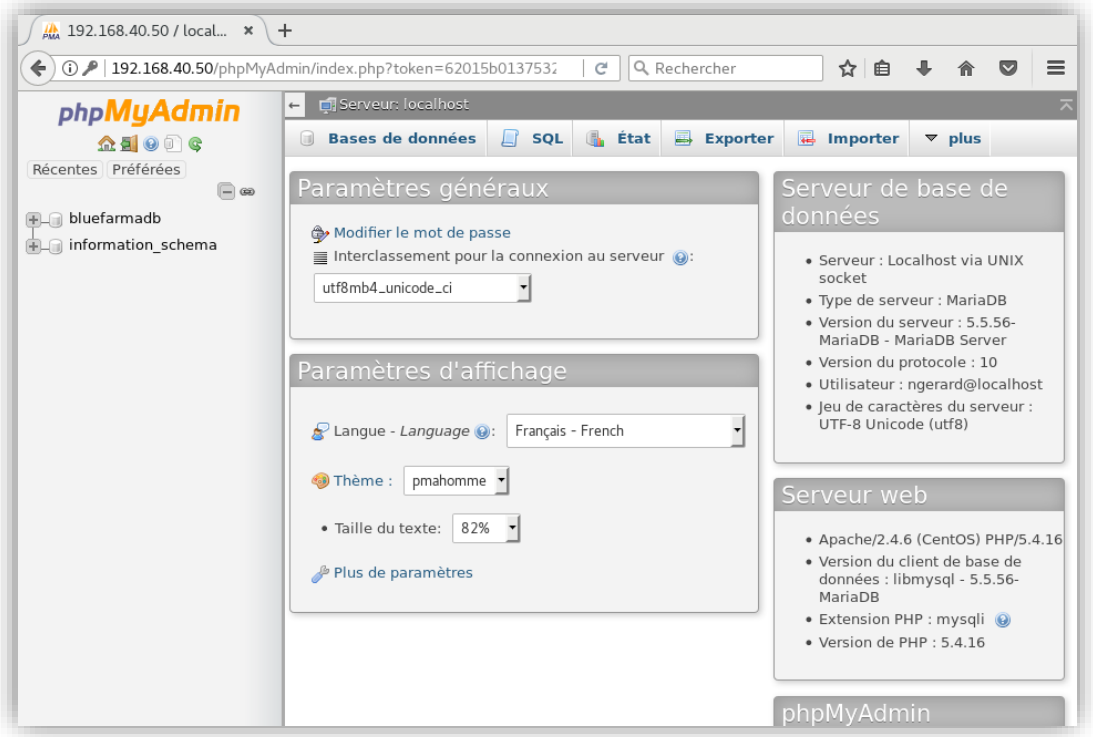
- Relancer Apache :

```
systemctl restart httpd
```

- Renseigner l'adresse suivante dans le navigateur pour vérifier que phpMyAdmin est maintenant accessible puis procéder à l'authentification :



- Nous pouvons dès présent accéder à la base de données SQL et l'administrer depuis l'interface du navigateur web :



9.4. CONFIGURATION DE PROXMOX

9.4.1. Configuration des accès en SSH

Prérequis :

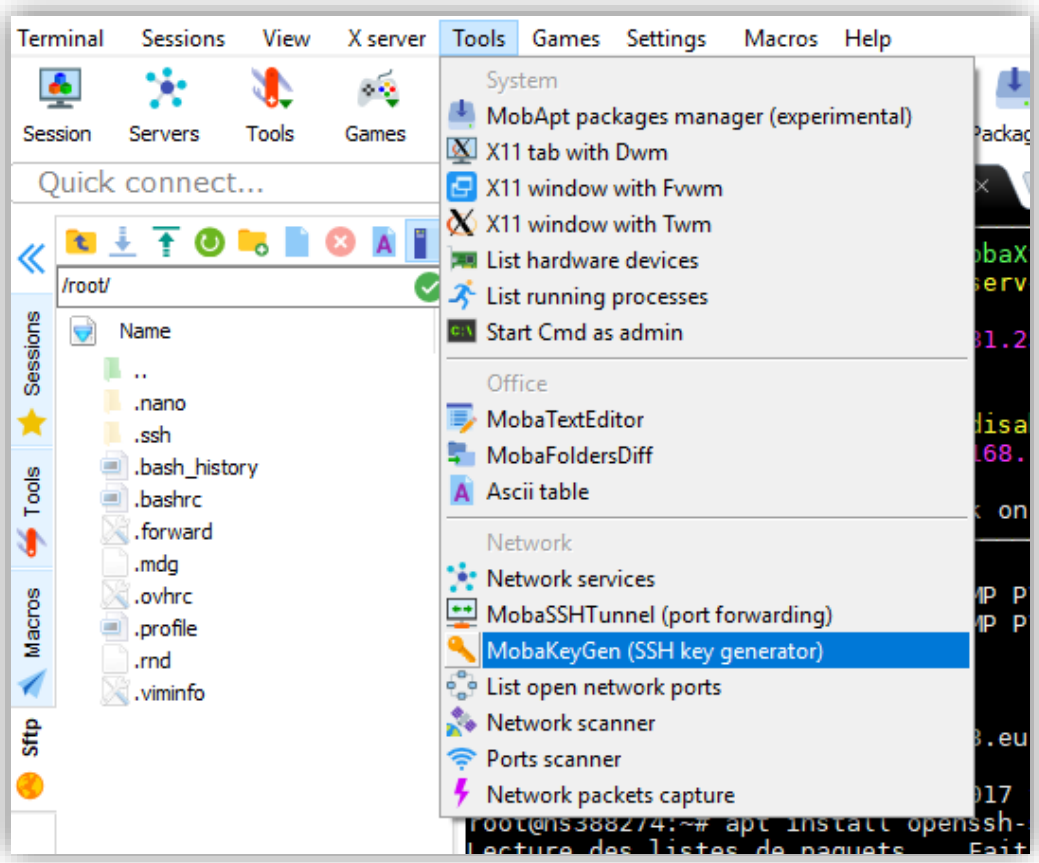
- L'émulateur de terminal Mobaxterm doit être déjà installé sur le poste de l'administrateur.
- Il doit posséder le mot de passe d'accès à la machine.

- Installer **OpenSSH**.

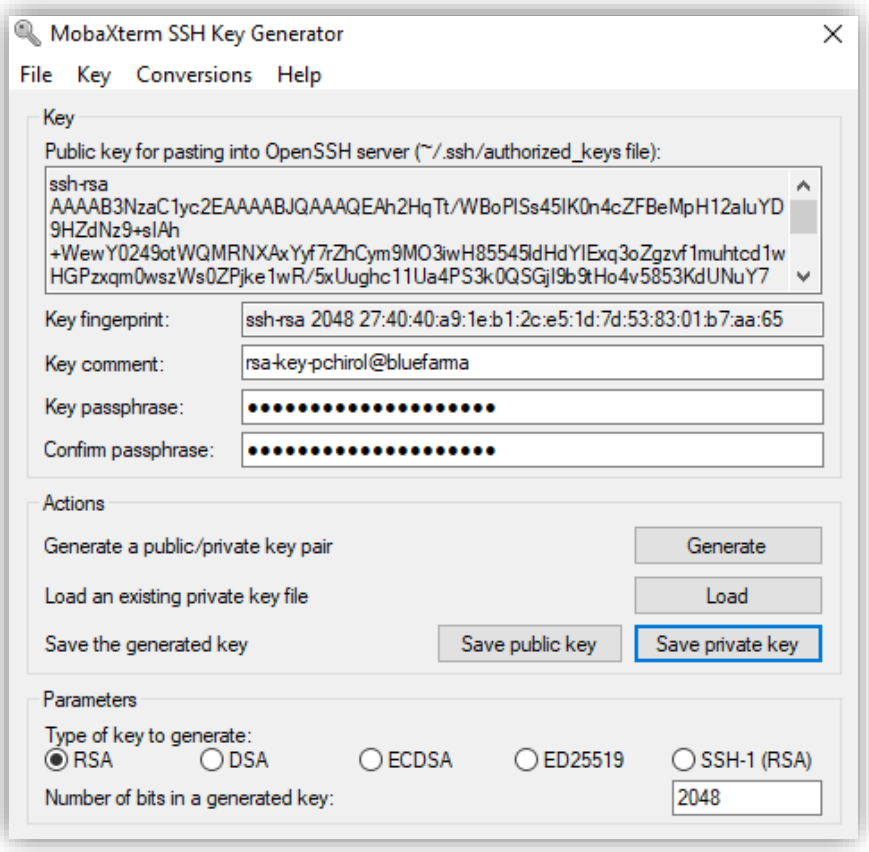
```
apt install openssh-server
```

NB : Normalement, Openssh est nativement installé.

- Ajouter le port d'écoute 37913 en se rendant dans le fichier **/etc/ssh/sshd_config**.
- Générer des clés pour faciliter la connexion au serveur. Dans Mobaxterm, se rendre dans ***Tools*** > ***MobaKeyGen (SSH key generator)***.



Cliquer sur **Generate** puis déplacer le curseur au hasard dans l'espace affiché, ce qui va générer par entropie des données pour la création de notre clé.



Renseigner une **passphrase** (qui correspondra au mot de passe de l'administrateur pour un serveur proxmox avec ses critères de robustesse requis) puis sauvegarder la clé privée dans un répertoire.

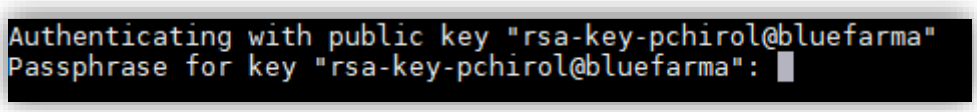
NB : on peut renommer la fin de la clé en commentaire pour indiquer le propriétaire de la clé, ici pchirol@bluefarma.

- Sur le serveur, mettre à jour le fichier **./ssh/authorized_keys** en copiant le contenu de la clé publique à partir du générateur précédent.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAh2HqTt/WBoPlSs45IK0n4cZFBeMpH12aIuYD9HZdNz9+sIAh+
WewY0249otWQMRNXAxYyf7rZhCym9MO3iwH85545ldHdYIExq3oZgzvf1muhtcd1wHGPzxqm0wszWs0ZPjkel
wR/5xUughc11Ua4PS3k0QSGjI9b9tHo4v5853KdUNuY7WNhrtGGT8F5OZIHH+rn9Rf1v3XmmHtZKZSSKniRx5
Tp8Pe+J6ifSLpLoMXBaaQACWs7Fgu+cU6wEeAEYox1s8oVSxP62cXp0N9LZgDvU/gUq+auNeIZXm9zlWU1JAu
kVe+qBL9eKCXJfD+onk/V2xitGr6NKRcFwYEgw== rsa-key-pchirol@bluefarma
```

- Créer une session en allant dans ***Session*** > ***onglet SSH*** > puis renseigner l'hôte (Remote host), l'utilisateur (username) et le port d'écoute (pour nous, 37913). Enfin, cliquer sur l'onglet ***Advanced SSH settings*** puis cocher ***Use private key*** afin d'ajouter la clé privée de l'administrateur autorisé à ouvrir une session sécurisée sur la machine

- Il restera à renseigner une dernière fois la passphrase lors de la prochaine connexion. Durant les connexions suivantes, un simple double-clique sur la session suffira pour établir une session cryptée et sécurisée sans devoir rentrer de mot de passe.



NB : le fait de fermer l'émulateur oblige l'utilisateur à renseigner de nouveau la passphrase. Il est conseillé de fermer le terminal qu'en fin de journée pour ne pas être obligé de le renseigner à chaque fois

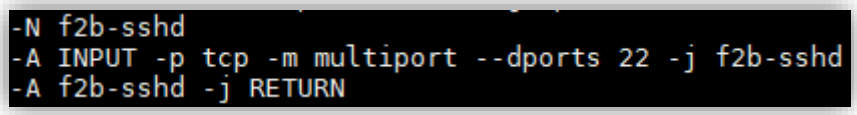
9.4.2. Configuration de fai2ban

Fail2ban est un logiciel qui limite le nombre de tentatives d'essais de mot de passe avant de bannir pendant une certaine durée l'auteur de cette action.

- Installer le paquet **fail2ban**

```
apt install fail2ban
```

- Pour vérifier sur quel port écoute fail2ban, exécuter la commande **iptables -S | grep f2b**.

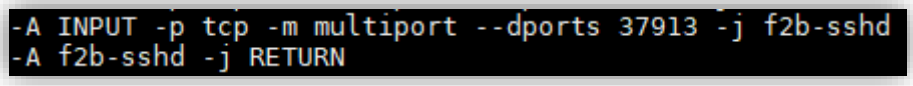


- Supprimer la règle dans le pare-feu **iptables** indiquant que fail2ban écoute sur le port ssh (22).

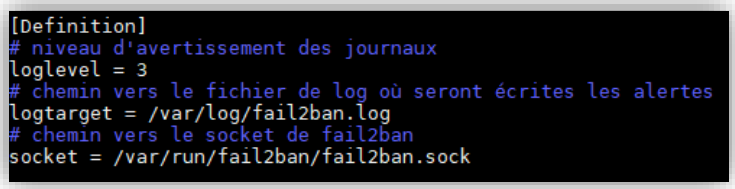
  `iptables -D INPUT -p tcp -m multiport --dports 22 -j f2b-sshd`

  Puis la remplacer par

  `iptables -A INPUT -p tcp -m multiport --dports 37913 -j f2b-sshd`
- Par la même commande de vérification, on constate que fail2ban écoute dorénavant sur le port 37193.



- Modifier le fichier **/etc/fail2ban/fail2ban.conf**.



- Éditer le fichier **/etc/fail2ban/jail.conf** puis modifier les lignes suivantes.

```
ignoreip = 192.168.40.101 #mention des IP des postes administrateurs qui ont le droit de se tromper

Bantime = 600 #durée du bannissement exprimée en secondes

[sshd]

Enabled = true #activation du service

port = 37913

filter = sshd #nom du filtre associé

maxretry = 3 #nombre maximal de tentatives
```

- Relancer le service (**restart**) et faire en sorte qu'il soit actif en cas de reboot (**enable**).

```
systemctl start fail2ban

systemctl enable fail2ban
```

9.4.3. Configuration du pare-feu IPTABLES

La configuration consiste à fermer tous les ports pour rejeter tout le trafic entrant, à l'exception des ports que nous utilisons pour différents services (ssh, port proxmow, icmp).

- La commande **iptables -L** montre que notre pare-feu accepte en l'état tous les flux entrants. Avant de droper tous les paquets, il convient d'ouvrir notre port d'accès en premier (sous peine de bloquer l'accès à notre machine)

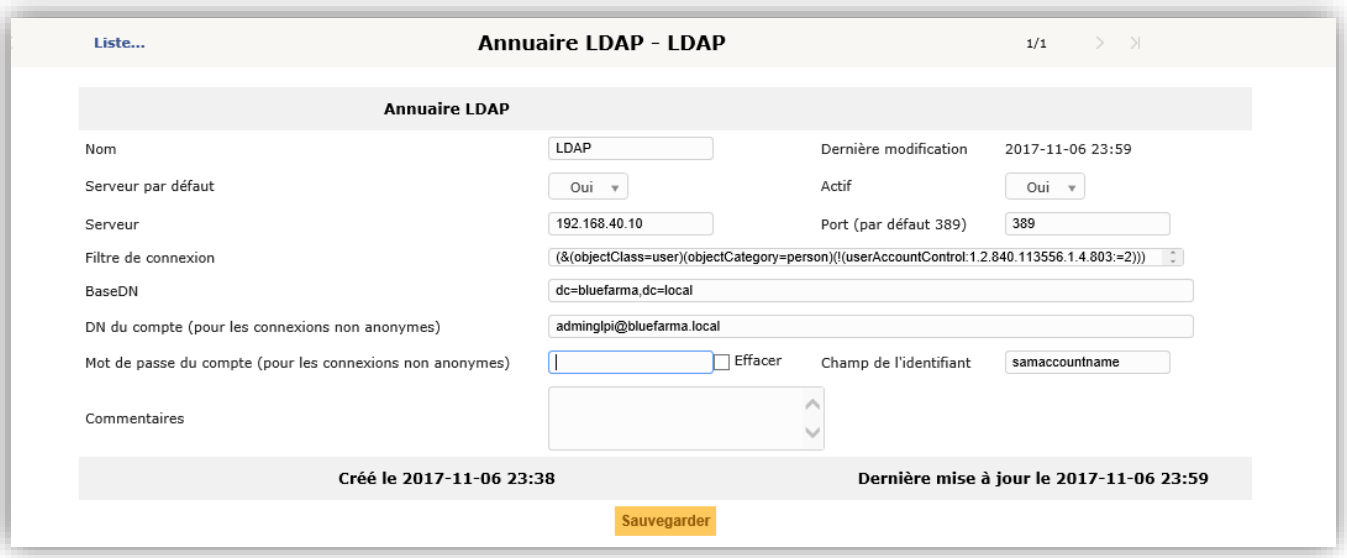
```
iptables -A INPUT -p tcp -m multiport --dport 37913 -j ACCEPT
```

Nous acceptions aussi l'icmp pour pinger notre machine.

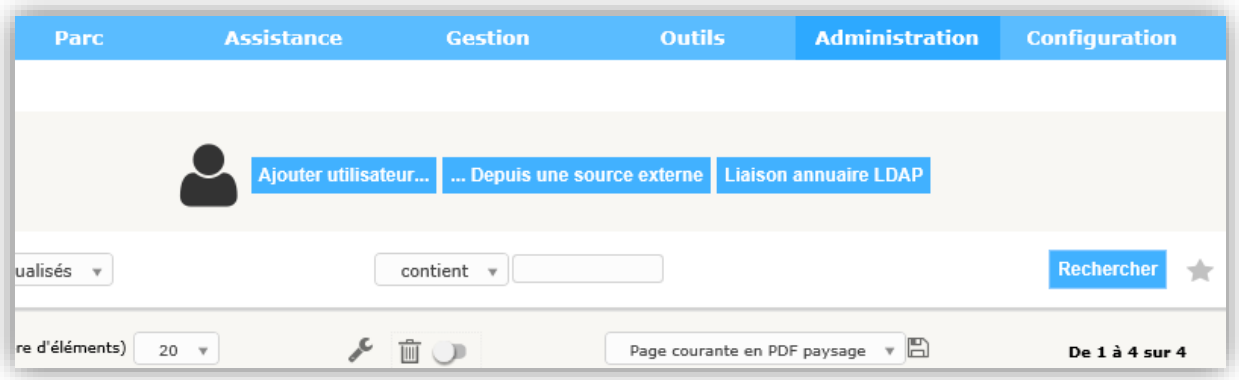
```
iptables -A INPUT -p icmp -j ACCEPT
```

9.5. CONFIGURATION DE LA BASE DE DONNÉES

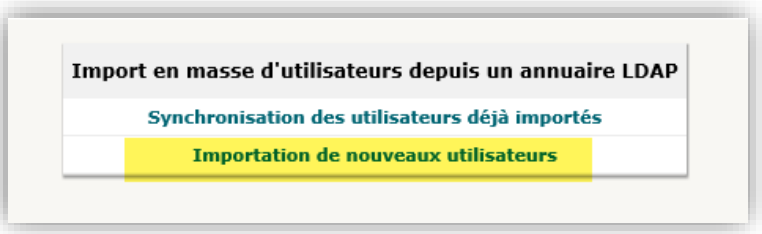
- Se rendre dans l'onglet ***Configuration*** puis ***Authentification*** et créer une nouvelle liaison LDAP, que l'on configure en fonction de nos paramètres du domaine :



- Se rendre dans l'onglet ***Administration***, ***Utilisateurs*** puis cliquer sur ***Liaison annuaire LDAP*** :

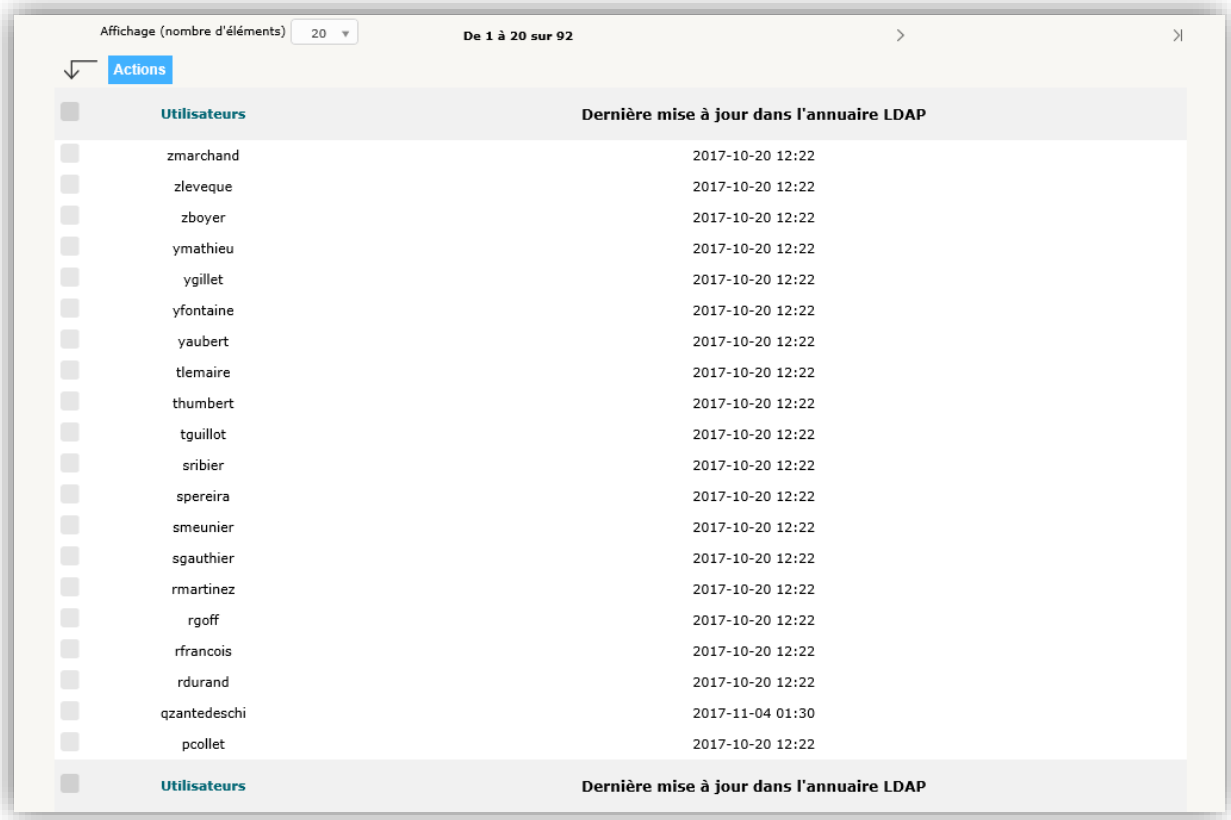


- Cliquer sur ***Importation de nouveaux utilisateurs*** :

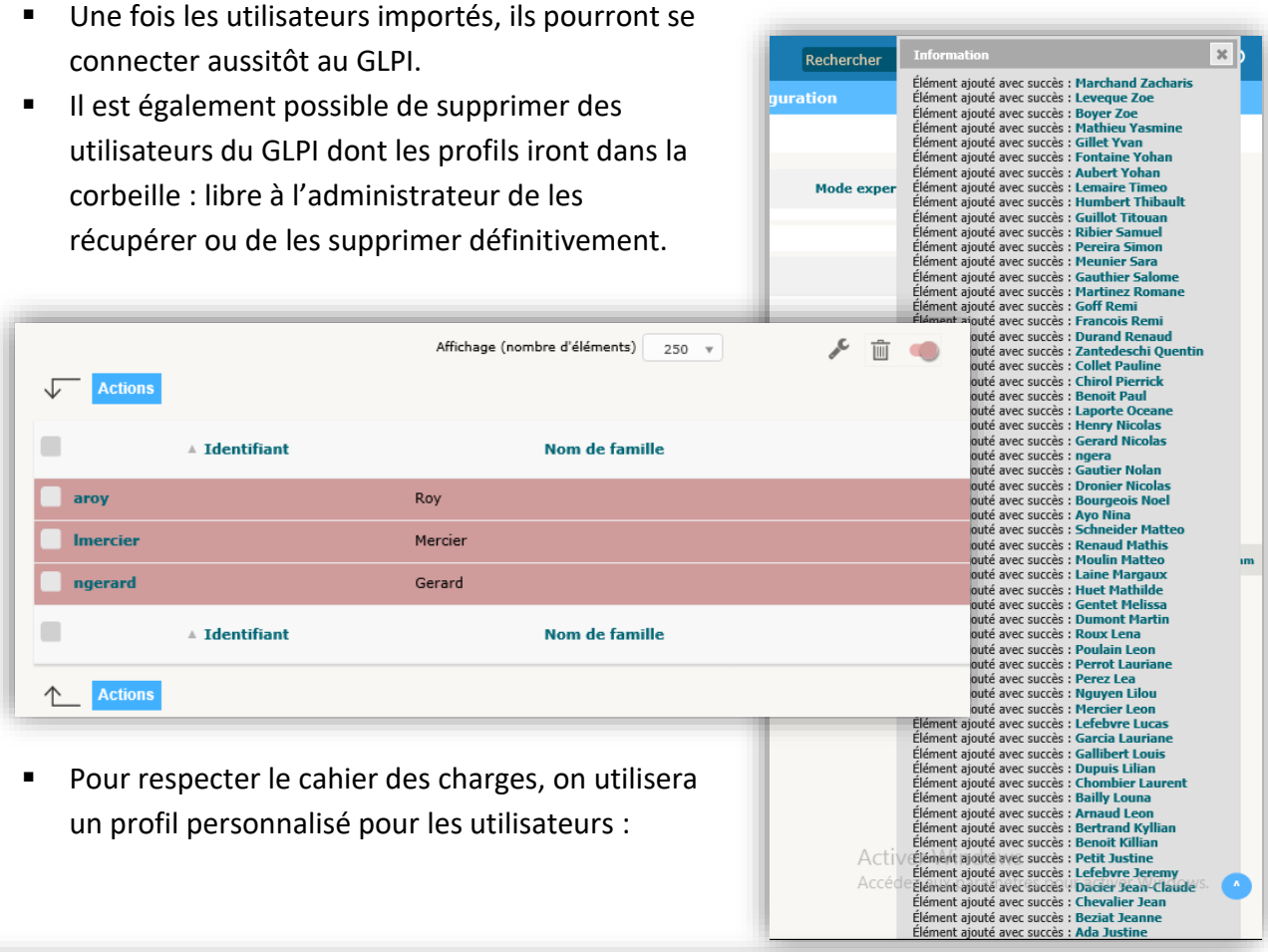


- Puis sur ***Rechercher*** :

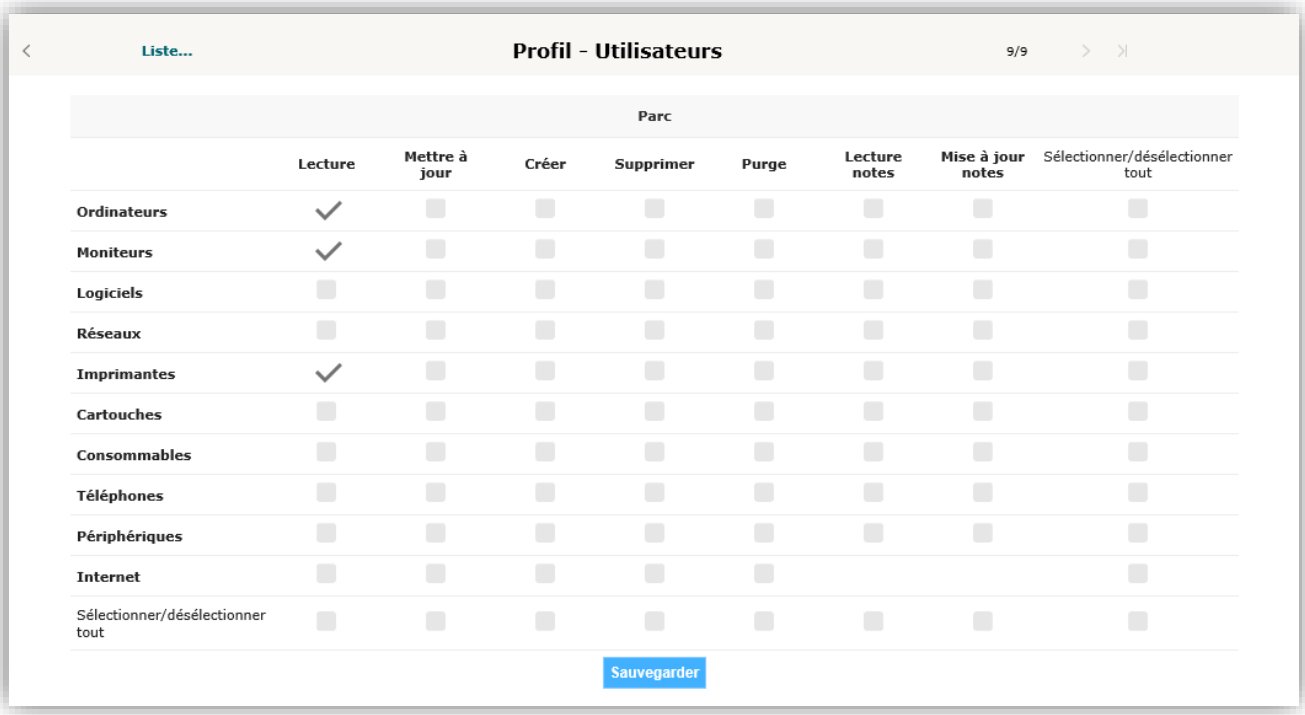
Les utilisateurs apparaissent, mais ne sont pas directement importés. On peut donc importer seulement certaines personnes, ou bien tout le monde.



- Une fois les utilisateurs importés, ils pourront se connecter aussitôt au GLPI.
- Il est également possible de supprimer des utilisateurs du GLPI dont les profils iront dans la corbeille : libre à l'administrateur de les récupérer ou de les supprimer définitivement.



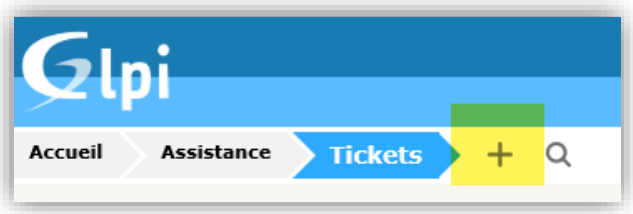
- Pour respecter le cahier des charges, on utilisera un profil personnalisé pour les utilisateurs :



On pourra consulter le parc depuis ce profil, créer des tickets, consulter la FAQ. Toutefois, toute modification ou suppression est impossible tandis que l'accès à la configuration et à la gestion du GLPI est bloquée.

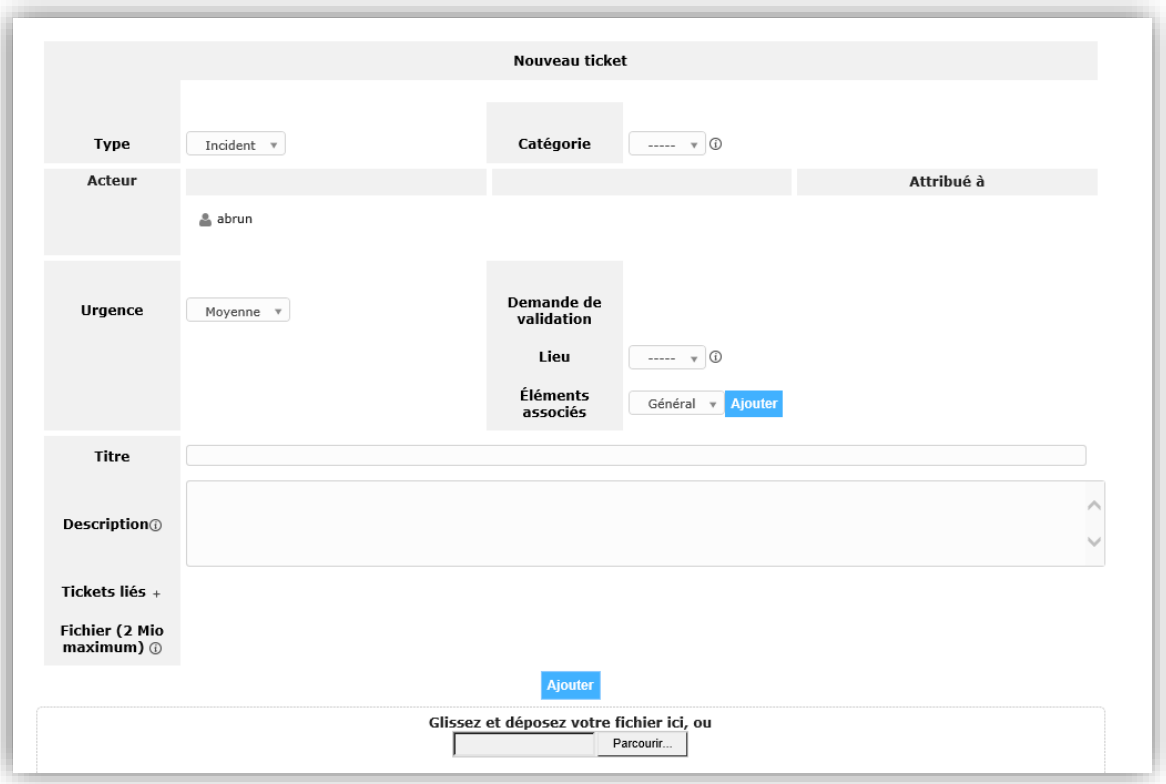
Ceci sera appliqué par défaut à tous les nouveaux utilisateurs (et donc à l'ensemble des utilisateurs importés)

- L'utilisateur peut également créer un ticket :



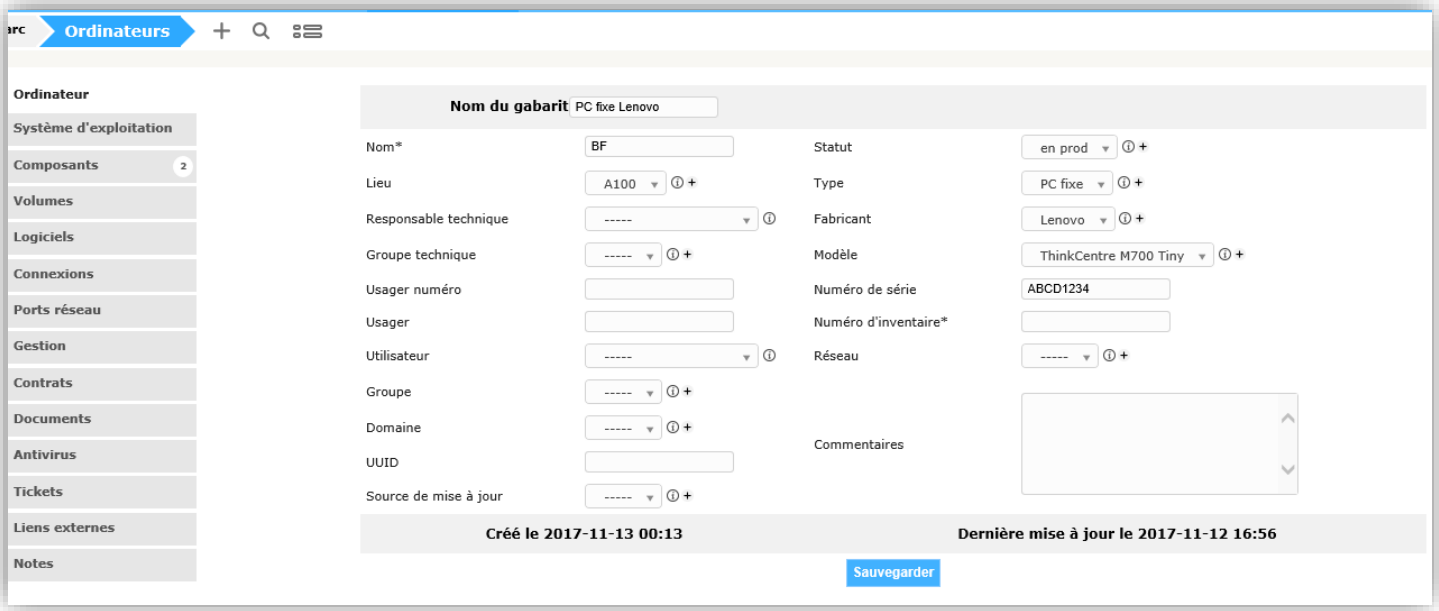
GLPI peut vite devenir déroutant pour l'utilisateur, c'est pourquoi on limite les fonctionnalités au maximum, afin de ne montrer à l'utilisateur que ce dont il a réellement besoin.

L'interface de création de tickets est ainsi épurée. L'utilisateur a accès aux fonctionnalités principales : priorité, ajout de pièce jointe, titre, description du problème ou de la demande, lieu, éléments associés au problème (ordinateur, imprimante) :



Afin de simplifier l'administration de GLPI et l'ajout de données, il est possible de créer des gabarits : ordinateur, écran, imprimante, etc.

Lors de la création d'un nouvel équipement, on peut donc choisir de se baser sur ce gabarit pour que certaines informations soient déjà préremplies.



9.6. DEVIS DÉTAILLÉ

Serveurs : Nous optons pour la gamme DELL pour nos serveurs et nos disques. La fiabilité du matériel et du support de garantie est tout à fait adaptée à l'enjeu critique que représente le fonctionnement de nos machines. Nous avons commandé deux serveurs dotés des configuration suivantes :

DELL POWEREDGE R440

- Processeur : 2 x Intel Xeon Silver 4110 2.1 G, 8C/16T
- RDIMM : 2 x 16 G
- RAID 1 : 2 x PERC H730P+ de 4 SSD SAS de 400 Go (2.5') (pour les systèmes Windows et Linux
- RAID 5 : 1 x PERC H730P+ de 3 x HDD 1,2 TB (2,5')
- Alimentation redondée : Dual Hot Plug Redundant Power Supply (1+1) de 550W
- Carte réseau : 2 x Broadcom 5720 Dual Port 1 Gbe
- Garantie : 5 ans avec intervention sur site en 4 heures

Prix unitaire : 9537,83 HT

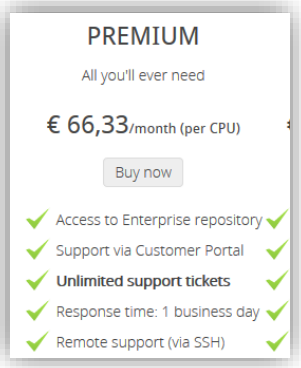
Spare :

- 1 x serveur DELL Poweredge R440 (avec les mêmes configurations que ci-dessus).
- 4 x 400 Gb SSD SAS 12 Gbps (prix unitaire : 981 HT)
- 6 x 1,2 TB 10K RMP SAS 12 Gbps (prix unitaire : 474 HT)
- 2 x PERC H730P+ (prix unitaire : 474 HT)

Support Proxmox :

Le support *Premium* nous permet de solliciter sans limitation de ticket le support avec une garantie de réponse d'un jour.

Ce support s'applique par CPU : nous paieront donc 4 support mensuel par mois (prix/mois : 265.32 HT).



Licence Windows

- **Windows Server 2016 Standard :** Disposant de quatre environnement Windows virtualisés, deux licences Microsoft Windows Server 2016 Standard seront nécessaires : chacune des deux peut prendre en charge 2 serveurs virtuels (prix unitaire : 902,48 HT)
- **CAL Windows Server** : ce type de licence est requis pour que les postes utilisateurs puissent être administrés par Windows Server. Nous commandons 90 licences (prix unitaire : 34.65 HT).

Licence ACRONIS : Cette licence court sur un an.

Prix unitaire : 729 HT/an

Licence Bitdefender GravityZone Business Security : La licence choisie court sur une période d'un an pour protéger nos 4 serveurs Windows.

Prix unitaire : 436.99 HT/an

Climatisation : une climatisation réversible est prévue pour chacun des deux locaux qui abrite nos équipements serveurs et réseaux.

(Prix unitaire : 1489 HT)

FICHE TECHNIQUE DE L'UNITÉ INTÉRIEURE DAIKIN FTXS42J

Puissance calorifique restituée à +7°CBS ext (kW)	1,7 / 5,4 / 6,0
Niveau de pression sonore froid (dB(A))	21 / 33 / 39 / 45
Encombrement de l'unité intérieure H x L x P (mm)	295 x 900 x 215
Poids de l'unité (Kg)	10
Couleur	Blanc
Référence de la télécommande IR	ARC452A3
Label énergétique froid / chaud	A+ / A++
EER / COP froid / chaud nominal	3,44 / 4,39
Conso. électrique annuelle (500h en froid) nominal kW/h	610

FICHE TECHNIQUE DE L'UNITÉ EXTÉRIEURE DAIKIN RXS42K

Encombrement de l'unité intérieure H x L x P (mm)	550 x 765 x 285
Poids de l'unité (Kg)	39
Type de compresseur	swing
Type de réfrigérant	R-410A
Plage de fonctionnement température extérieure mode chaud (°CBS)	-15 ~ +20
Plage de fonctionnement température extérieure mode froid (°CBS)	+10 ~ +46
Préchargé d'usine jusqu'à (m)	10
Raccordements frigorifiques longeur / déniv max (m)	20 / 15
Raccordements frigorifiques diamètre liquide / gaz (m)	1/4 - 3/8
Raccordements électriques alimentation V/Ph/Hz	230/1/50
Raccordements électriques protection** disjoncteur courbe D	16 A
Raccordements électriques câble liaison int / ext (mm²)	4G1,5

** Valeurs indicatives, à vérifier en fonction du site et dans le respect de la norme NFC 15-100

Onduleur : Deux onduleurs par serveurs sont à prévoir afin de protéger les équipements des surtensions. Nous avons choisi la marque Eaton qui offre un bon ratio entre rendement et consommation (modèle Eaton 5PX 1500i RT2U).

Prix unitaire : 699,95 HT

Caractéristiques techniques :

- Onduleur Line interactive
- Puissance (VA/W) : 1500 VA / 1350 W
- Format : Tour convertible Rack 2U
- Technologie : Line-Interactive Haute Fréquence (Sinusoïde pure, Booster + Fader)
- Plages de tension et de fréquence sans sollicitation des batteries : 160V-294V (ajustable à 150V-294V) 47 à 70 Hz (système 50 Hz), 56.5 à 70 Hz (système 60 Hz), jusqu'à 40 Hz en mode basse sensibilité
- Tension et fréquence de sortie 230 V (+6/-10 %) (ajustable à 200V / 208V / 220V / 230V / 240V), 50/60 Hz +/- 0.1 % (auto-détection)
- Entrées 1 prise IEC C14 (10 A)
- Sortie 8 prises IEC C13 (10 A)
- Prises commandables à distance 2 groupes de 2 prises IEC C13 (10 A)
- Autonomies typiques à 50 et 70% de charge : 19/11 min
- Ports de communication 1 port USB + 1 port série RS232 et contacts (les ports USB et RS232 ne peuvent pas être utilisés simultanément) + 1 mini connecteur pour démarrage/arrêt à distance
- Emplacement pour carte de communication 1 slot pour carte NMC Minislot (non incluse)
- Niveau sonore : < 45 dB
- Dimensions : 441 x 522 x 86,2 (2U) mm
- Poids : 27.6 kg

Extincteur : Comme vu précédemment, les extincteurs à CO2 sont les plus adaptés pour éteindre les feux d'origine électrique. Nous en achèterons trois (un par local qui abrite du matériel réseau ou serveur). Les extincteurs doivent être renouvelés tous les ans et il est conseillé de les inspecter tous les trois mois. Ils doivent être conforme à la norme CE-EN3.

Prix unitaire : 60 HT

Détecteurs de fumée : Appelé aussi détecteur avertisseur autonome de fumée (DAAF) 3 détecteurs de fumée sont obligatoires dans les entreprises depuis mars 2015. Il doit être certifié ***CE*** et ***NF EN 14604***.

Nous en installerons dans les trois locaux de télécommunications.

Prix unitaire : 19,90 HT

Location d'un coffre-fort : les disques de sauvegardes de données seront protégés dans un coffre-fort que nous louons à la Société Générale (taille de 30 dm3).

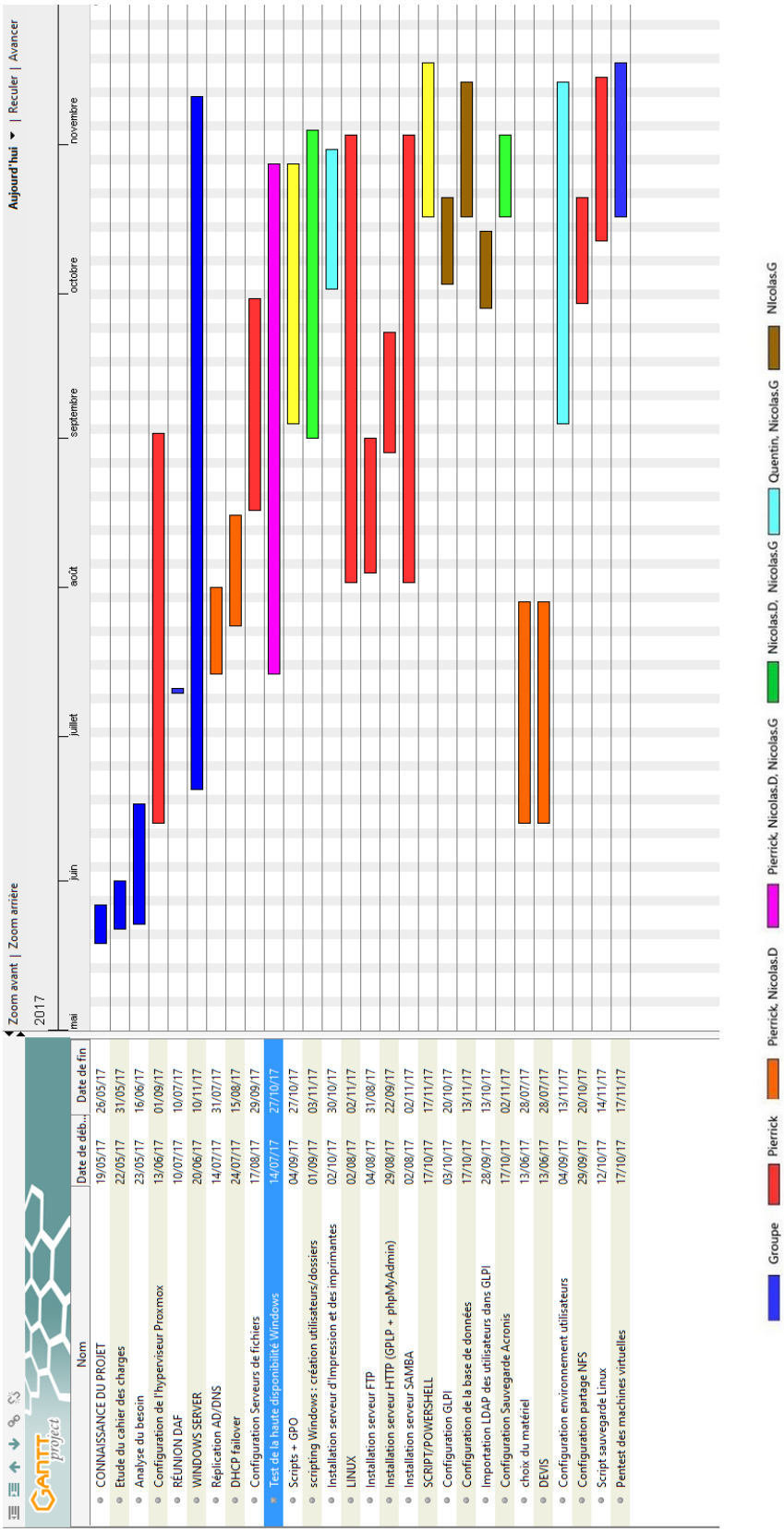
Prix unitaire : 110 HT/an

Tableau récapitulatif du devis :

Produit	*Prix unitaire HT*	*Quantité*	*Prix Total HT*
Serveur Dell Poweredge R440	9537,83	3	28613,49
400 Gb SSD SAS	981	4	3924
1,2 TB 10K RMP SAS	474	6	2844
PERC H730P+	474	2	948
Licence Windows Server 2016 Standard	902,48	2	1804,96
Licence CAL Windows Server	34,65	90	3118,5
Licence Acronis	729	1	729
Licence Bitdefender GravityZone Business	436,99	1	436,99
Climatisation	1489	2	2978
Pose climatisation - main d'œuvre	495.83	1	495.83
Onduleur	699,95	2	1399,9
Extincteur	60	2	120
Détecteur de fumée	19,90	2	39,8
Location d'un coffre-fort (Société Générale)	110	12	1320
		TOTAL HT	**48772,47**

NB : Le devis tient compte des abonnements et locations sur un an.

9.7. PLANNING ET RÉPARTITION DES TÂCHES



10. GLOSSAIRE

Active Directory. Il s'agit d'un annuaire LDAP pour les environnements Windows qui contient différents objets (utilisateurs, ordinateurs, groupes, etc.). Le but est d'administration et de centraliser tous les objets présents sur le réseau de manière simplifiée.

Base de données relationnelle. Elle concentre une collection de données qui sont organisées dans des tableaux à deux dimensions qui se nomment « relations » ou « tables ». Ce système est basé sur le modèle proposé en 1970 par Edgar F. Codd, l'inventeur du modèle relationnel. Ainsi, les données peuvent être assemblées via une ou plusieurs relations (appelées « *nuplets* » ou « enregistrements ») sans avoir besoin de réorganiser les tables. Ce principe permet d'étendre facilement les tables.

Les logiciels qui permettent de créer, interroger et maintenir les bases de données relationnelles sont appelés des *systèmes de gestion base de données relationnels* (*SGBDR*) : ils utilisent essentiellement le langage ***SQL***.

Crontab. Il s'agit d'un service ou démon (**crond**) sous linux permettant de planifier l'exécution de tâches spécifiques sur des intervalles de temps définis.

DHCP. (« *Dynamic Host Configuration Protocol* »), est un protocole réseau qui permet d'attribuer dynamiquement des adresses IP à des postes ou des périphériques autorisés sur le réseau.

DNS, « *Domain Name Service* ». Le protocole DNS se charge de convertir le nom d'un site en adresse IP : on parle alors de résolution. Son rôle principal est de permettre d'identifier plus facilement des machines sur un réseau.

FTP, « *File Transfer Protocol* ». Ce protocole de transfert de fichier permet l'échange de fichiers sur un réseau. Il permet également de charger des fichiers sur un site web ou de les télécharger. Ces transferts s'effectuent selon le modèle client-serveur (le client envoie des requêtes et le serveur réagit) : un logiciel installé sur le serveur (appelé serveur FTP) permet de rendre visible une arborescence de fichiers qui est accessible à l'aide d'un logiciel client (exemple : FileZilla). Ainsi, on utilise le FTP pour télécharger ou envoyer un fichier d'un serveur en utilisant le protocole TCP/IP.

FTP connait deux variantes : FTPS qui utilise les protocoles SSL/TSL et SFTP qui est basé sur le protocole SSH. FTP relève de la couche application du modèle OSI.

GPO. « *Group POlicy* ». Il s'agit de fonctions de gestions centralisées permettant de mettre en place des stratégies de groupe dans un environnement Windows afin de faciliter l'administration d'un parc, notamment au niveau de la gestion des utilisateurs et des ordinateurs.

Monitoring, **ou monitorage**. Cette activité permet d'assurer la supervision des équipements et des logiciels informatiques. Ainsi, le monitoring effectue des mesures afin de surveiller plusieurs paramètres tels que l'état physique d'une machine, sa charge, l'activité des processus, les performances et la nature des protocoles du réseau, etc.

Généralement, ces mesures permettent la construction de graphiques, alerter l'administrateur d'éventuels dysfonctionnements voir d'exécuter des actions programmées.

NFS, « *Network File System* ». Il s'agit d'un protocole permettant d'accéder à des fichiers centraux communs distants via le réseau sur des systèmes Unix sur un modèle serveur/client. Cet accès s'établie via une interface appelée système de fichiers virtuel (*VFS*) qui fonctionne sur le protocole TCP/IP. Le NFS monte des dossiers distants partagées comme un dossier local dans l'arborescence de fichiers de la machine cliente.

Samba : Cet outil est basé sur le protocole SMB (« *Server Message Block* ») qui permet le partage de ressources telles que des fichiers ou des imprimantes sur un LAN composé de postes tournant sous Windows. Sa structure est basée sur le modèle client/serveur. Les ressources sont accessibles via une adresse UNC utilisant la syntaxe \\192.168.10.15\partage\administratif.

Son implémentation au logiciel Samba permet d'assurer l'interopérabilité entre différentes machines (ordinateurs, smartphones, tablettes) tournant sur différents systèmes (Windows, Linux, OSX, etc.).

SGBD, « *système de gestion de base de données* ». Il s'agit d'un logiciel permettant de manipuler les données d'une base de données en effectuant un groupe de quatre opération appelé CRUD (*Create*, *Read*, *Update*, *Delete*).

Un SGBD est souvent basé sur le modèle client-serveur : la base de données sera hébergée sur un serveur dédié à cet usage tandis qu'un logiciel « client » sera nécessaire pour interroger la base de données qui utilise le langage SQL pour émettre des requêtes.

SGBDR : Il s'agit d'un SGBD qui manipule la théorie relationnelle (exemple : MySQL). La différence réside dans le fait qu'un SGBDR contient ses données dans des « relations » apparaissant sous forme de « tables ».

SQL, « *Structured Query Language* ». SQL est un langage informatique permettant d'interroger une base de données relationnelles. Ayant été recommandé en 1986 par l'ANSI puis normalisé sous le nom de l'ISO/CEI 9075, il est aujourd'hui largement présent dans les SGBDR (exemple : MySQL).

SSH, « *Secure Shell* ». Il s'agit d'un protocole de communication qui permet d'administrer à distance un équipement (routeur, switch, etc.) ou un serveur de façon sécurisée. Ceci passe par l'utilisation de clés de chiffrement qui vont permettre d'authentifier et de « crypter » tous les segments TCP. Depuis janvier 2006, la version SSH-2 a été officialisée par l'*IETF* (plus sécurisé que SSH-1) et possède un protocole de transfert de fichiers sécurisé appelé SFTP

(« *SSH File Transfer Protocol* ») : SFTP encapsule le protocole dans une couche « sécurisée » SSH.

OpenSSH, la version libre du client et du serveur SSH permet de chiffrer le trafic via la combinaison de clés symétriques et asymétriques.

Telnet, « *Terminal/Telecommunication/Teletype Network* ». Ce protocole est utilisé pour communiquer avec un serveur distant sur un réseau TCP/IP. Toutefois, les données n'étant pas chiffrées, l'utilisation de ce protocole de communication est déconseillée pour des raisons de sécurité.

11. RESSOURCES INTERNET ET BIBLIOGRAPHIE

BONNET Nicolas, ***Windows Server 2016. Les bases indispensables pour administrer et configurer votre serveur***, *ENI édition*, 2016

DEMAN Thierry, DESFARGES Guillaume, ELMALEH Freddy, ***Windows Server 2016. Administration avancée***, *ENI édition*, 2016

Virtualisation

http://www.lemagit.fr/conseil/VMware-vs-Hyper-V-qui-gagne

http://www.hyperv.fr/vmware-vs-hyper-v-quoi-choisir/

http://www.lemagit.fr/conseil/Windows-Server-2016-et-Hyper-V-attention-aux-nouvelles-licences

Proxmox

https://www.proxmox.com/en/proxmox-ve/pricing

https://documentation.online.net/fr/dedicated-server/tutorials/network/rpn-proxmox-openvswitch

https://www.it-connect.fr/kvm-proxmox/

AD et DC

https://www.it-connect.fr/chapitres/les-protocoles-ldap-dns-et-kerberos/

https://www.it-connect.fr/chapitres/controleur-de-domaine-et-domaine/

https://www.it-connect.fr/creer-un-domaine-ad-avec-windows-server-2016/

https://www.it-connect.fr/ajouter-un-controleur-windows-server-2012-dans-un-domaine-existant/

http://www.supinfo.com/articles/single/462-installation-replication-active-directory-windows-2012-r2

DHCP

https://www.it-connect.fr/windows-server-2012-r2-failover-de-serveurs-dhcp/

DFS

https://www.it-connect.fr/windows-server-2012-r2-installation-du-role-dfs/

https://www.it-connect.fr/cest-quoi-le-dfs-windows-server/

https://www.supinfo.com/articles/single/2629-architecture-configuration-dfs

CentOS

http://www.tophebergeur.com/articles/les_bases_de_lhebergement/comparaison_entre__centos_debian_et_ubunto/

http://www.silicon.fr/hub/hpe-intel-hub/quel-systeme-dexploitation-linux-pour-mon-serveur?inf_by=596a7f50681db82d6b8b457c

FTP

http://smnet.fr/centos/centos-vsftpd.html

https://doc.fedora-fr.org/wiki/Vsftpd_:_Installation_et_configuration

https://fr.wikipedia.org/wiki/File_Transfer_Protocol

https://doc.ubuntu-fr.org/vsftpd

SAMBA

https://wiki.kogite.fr/index.php/Samba_avec_authentification_sur_Active_Directory

https://fr.wikipedia.org/wiki/Samba_(informatique)

https://dev.tranquil.it/wiki/Samba4

https://doc.ubuntu-fr.org/samba

NFS

https://doc.fedora-fr.org/wiki/Partage_de_disques_en_r%C3%A9seau_avec_NFS

https://fr.wikipedia.org/wiki/Network_File_System

rsync, cron

https://doc.ubuntu-fr.org/rsync

https://doc.ubuntu-fr.org/tutoriel/sauvegarder_home_avec_rsync

https://doc.ubuntu-fr.org/cron

https://doc.ubuntu-fr.org/tutoriel/script_shell

https://doc.fedora-fr.org/wiki/CRON_:_Configuration_de_t%C3%A2ches_automatis%C3%A9es

http://www.linux-france.org/article/man-fr/man1/date-1.html

http://pwet.fr/man/linux/commandes/date

mysqldump

https://www.it-connect.fr/sauvegarder-une-base-de-donnees-rapidement-sous-mysql-avec-mysqldump/

https://www.citizenz.info/sauvegardes-journalieres-et-acces-a-distance-sur-votre-serveur-mysql

https://doc.ubuntu-fr.org/tutoriel/sauvegarder_automatiquement_ses_bases_de_donnees

Sauvegarde incrémentielle et différentielle

https://www.it-connect.fr/comprendre-la-sauvegarde-incrementielle-et-differentielle/

Acronis

https://www.acronis.com/fr-fr/business/backup/

https://doc.fedora-fr.org/wiki/Installation_et_configuration_de_MySQL

https://doc.ubuntu-fr.org/mysql

GLPI, apache et phpmyadmin

http://www.be-root.com/2015/12/30/installation-glpi-centos-7/

http://www.pegasus45.lautre.net/index.php/CentOS_7:_Installation_de_phpMyAdmin

http://glpi-project.org/DOC/FR/glpi/config_auth_ldap.html

Monitoring linux

https://www.dsfc.net/logiciel-libre/linux/centos-linux-logiciel-libre/installer-cockpit-sur-centos-7/

https://korben.info/cockpit-un-tableau-de-bord-pour-vos-serveurs.html

https://fr.wikipedia.org/wiki/Surveillance_(informatique)

Failtoban

https://doc.fedora-fr.org/wiki/SSH_:_Se_prot%C3%A9ger_des_attaques_avec_fail2ban

https://doc.ubuntu-fr.org/fail2ban

https://doc.fedora-fr.org/wiki/SSH_:_Authentification_par_cl%C3%A9

IPTABLES

https://wiki.archlinux.fr/Iptables

https://doc.fedora-fr.org/wiki/Parefeu_-_firewall_-_netfilter_-_iptables

Durée de conservation des données et PCA

https://www.cnil.fr/fr/dispense/di-018-plan-de-continuite-dactivite-pca-des-ministeres

https://www.cachem.fr/plan-reprise-activite-pra-comment-pourquoi/

https://www.1and1.fr/digitalguide/serveur/know-how/creer-un-plan-de-reprise-dactivite-informatique/

https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

Base de données

https://fr.wikipedia.org/wiki/Structured_Query_Language

https://sql.developpez.com/#commencer-sql

https://openclassrooms.com/courses/apprenez-a-programmer-en-vb-net/introduction-au-langage-sql

https://openclassrooms.com/courses/administrez-vos-bases-de-donnees-avec-mysql

https://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es_relationnelle

http://www.lemagit.fr/definition/Base-de-donnees-relationnelle