



GREENCOP

Société Greencop

Projet EVOLUTION

Auteurs :

Louis ROUX

Vincent BAUDVIN

Salima DOUDANE

Lucas MORGANTE

Table des matières

Greencop :	4
Qui sommes-nous ?	4
Organigramme :	4
Compléments d'informations :	5
Localisations :	5
Charte graphique :	6
Gestion du projet :	7
Contexte :	9
Objectif.....	9
Solution technique	10
Virtualisation :	11
Hyperviseur :	12
Serveur Physique :	12
Stockage :	14
Sauvegarde :	15
Hébergeur :	16
Softwares	17
VSphere	17
Windows Server	18
Veeam	21
Antivirus	21
Choix matériel	22
Calcul des ressources	22
Serveur :	24
Baie de stockage :	25
Calcul des licences :	27
Windows Serveur 2019 :	27
Licences CAL	29
VSphere :	30
VCenter serveur :	31
Veeam :	31
Budget :	32



Réseau.....	32
Découpage réseau et adressage IP :	33
Charte de nommage	34
PCA – PRA :	35
Procédure d’installation :	36
Windows serveur :	36
Linux :	44
Mise en place solution technique :	47
Windows serveur :	47
Linux :	54
Conclusion.....	54
Annexes.....	56
Bibliographie	Erreur ! Signet non défini.
Devis.....	56
.....	57
Glossaire.....	59



Greencop :

Qui sommes-nous ?

Fondée en 2011, Greencop est une nouvelle centrale d'achat pour un regroupement de franchisés qui vient de s'installer dans ses nouveaux locaux d'Aix-en-Provence.

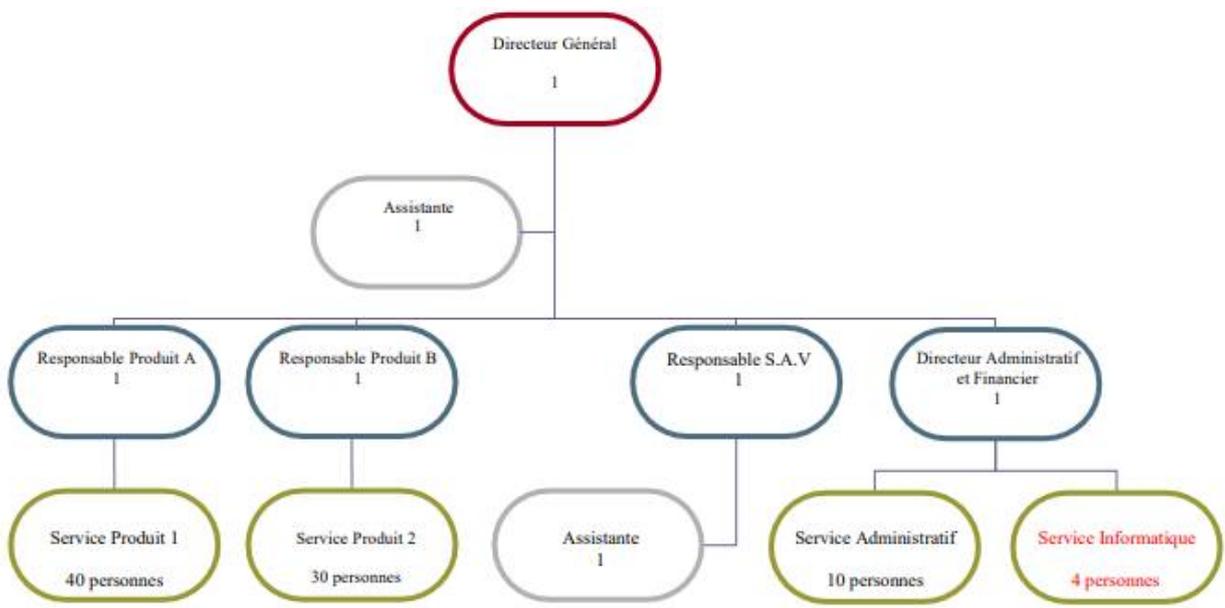
Elle génère, répond et négocie des appels d'offres pour deux lignes de produits qu'elle fournit aux franchisés selon un approvisionnement optimisé.

Sa structure offre à la fois les meilleures conditions d'achat et des services de promotion pour l'ensemble de ses membres.

Elle emploie 91 salariés à pleins temps.

Organigramme :

Voici l'organigramme de la société pour une meilleure représentation des services.



Compléments d'informations :

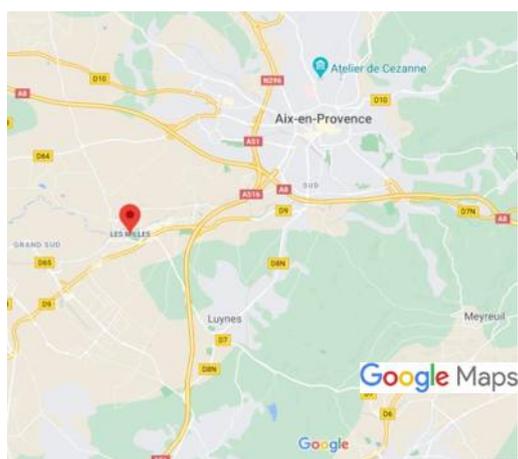
Raison sociale	Greencop
Dirigeants	Corinne AMAR et Luc VELAVON
Date de création RCS	29/11/2011
Adresse	536, Euro-pôle de l'Arbois 13290 Aix-en-Provence
Téléphone	04.42. XX. XX. XX
Adresse Mail	contact@greencop-aix.com
Site Web	www.greencop-aix.com
LinkedIn	www.linkedin.com/in/Greencop
Forme juridique	SAS
Capital Social	325 555€
SIREN	444 444 441
SIRET	444 444 441 00011
Code APE / NAF	4619A / Intermédiaires du commerce en produits divers

Localisations :

La société se situe dans les Bouches-du-Rhône (13), région PACA (Provence-Alpes-Côte d'Azur).

Plus localement, nous la retrouvons, au Sud-Ouest de la ville d'Aix-en-Provence. Cette situation géographique lui permet de bénéficier d'un carrefour d'autoroute comme l'A6, l'A7, l'A8, l'A51 qui desservira des grandes villes tel que Valence, Lyon, Paris, Nice et en particulier Marseille. Grâce au Port de cette ville, celui-ci fournit un accès au Fret maritime et permet le transport de marchandise en dehors de la France et Hors U-E.

Un choix d'emplacement qui impacte directement l'évolution et la réussite de Greencop.

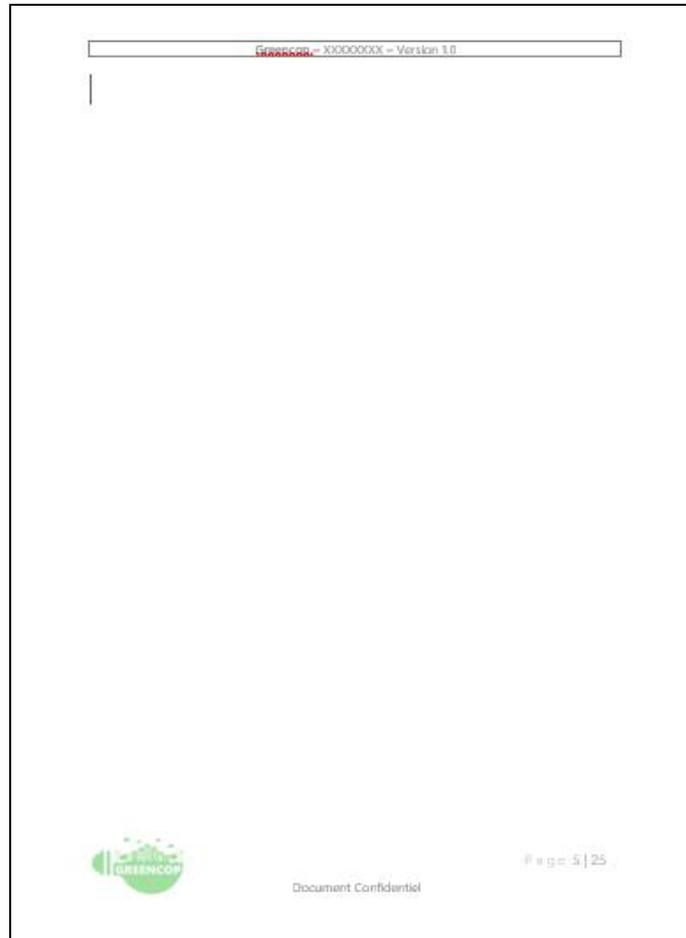


Représentation de la carte de France, en bleu foncé la région PACA et son emblème



Charte graphique :

Les polices ainsi que le modèle de mise en page suivant devront être utilisés pour tous les documents rédigés par le service informatique :



Normal : Segoe UI Semilight (11)

Titre 1 : Calibri Light (Titres) (22) Souligné

Titre 2 : Calibri Light (Titres) (13) Souligné

Accentuation : Segoe UI Semibold (11) Gras



Gestion du projet :

Dans le but de mener à bien ce projet et atteindre les objectifs demandés par le D.A.F, nous avons dû l'organiser en plusieurs étapes :

- ✓ Définir les objectifs, établir la liste des besoins et comment y répondre.
- ✓ Découper le projet, dresser la liste des tâches à réaliser, répartir les rôles et partager les tâches.
- ✓ Organiser des réunions efficaces pour connaître l'avancement de chaque collaborateur.
- ✓ Prendre des décisions sur des solutions techniques.
- ✓ Centraliser et mettre à jours les données/documents etc.
- ✓ Mutualiser les ressources et les compétences.
- ✓ S'assurer d'avoir atteints objectifs et clôturer le projet.

Nous nous sommes appuyés sur des outils collaboratifs, notamment TEAMS pour les échanges d'idées et les différents documents. Cela nous a permis d'échanger rapidement par écrit et aussi à l'oral pour les réunions et des visio-conférences pour la réalisation des maquettes.

SHAREPOINT, pour le partage sécurisé et la modification de documents en ligne.

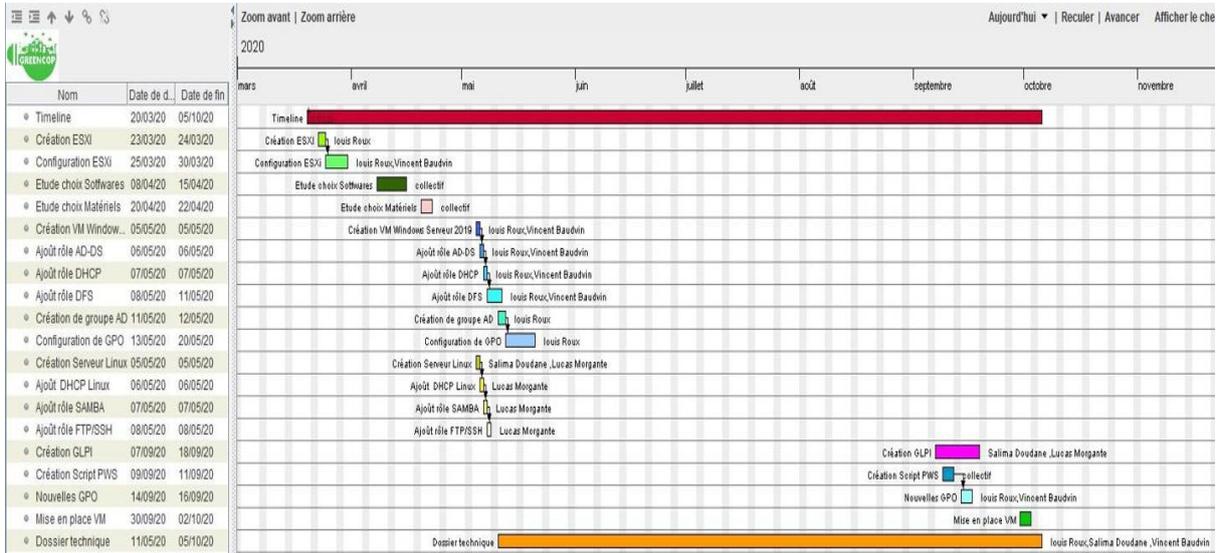
The screenshot shows a SharePoint site interface for 'Evolution : Greencop'. The top navigation bar includes a search box and the site name. The main content area is divided into several sections:

- Actualités (News):** A section titled 'Restez à la page avec votre équipe grâce aux actualités sur votre site d'équipe'. It features a green button labeled 'Ajouter des actualités'.
- Activité (Activity):** A grid of activity cards showing recent updates. Examples include:
 - 'Compte-rendu Juin' by BAUDVIN VINCENT, added about a minute ago.
 - 'Compte-rendu Avril' by BAUDVIN VINCENT, added about a minute ago.
 - 'Documents partagés Dossier tech evolution 1' by MORGANTE LUCAS, modified about 9 minutes ago.
- Liens rapides (Quick Links):** A list of links for team site navigation, such as 'En savoir plus sur un site d'équipe' and 'Découvrez comment ajouter une page'.
- Documents (Documents):** A list of documents with columns for 'Nom' and 'Modifié'. The list includes:
 - Compte-rendu (lundi à 09:12)
 - Devis (vendredi à 01:15)
 - Plan Visio (lundi à 09:13)
 - Dossier tech evolut... (il y a 9 minutes)
 - Projet EVO Greenc... (lundi à 09:11)

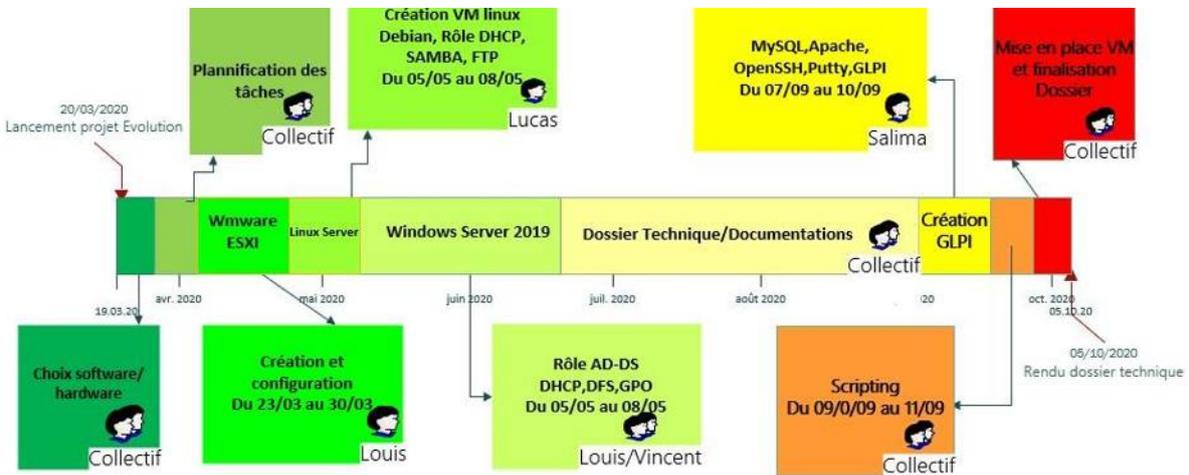


Ces outils et une alternance de notre présence sur site nous a permis de poursuivre l'avancement du projet durant la crise sanitaire du COVID-19.

Ci-dessous vous trouverez un diagramme de Gant avec toutes les tâches que l'on a réalisé.



Un autre planning réalisé sous Visio donne une meilleure visibilité :



Contexte :

Dans la continuité du projet START durant lequel nous avons réalisé le câblage structuré sur l'ensemble des nouveaux bâtiments, le renouvellement du parc informatique et le déménagement de l'entreprise.

Nous travaillons depuis six mois dans les nouveaux locaux, nous constatons des problèmes d'organisation, de gestion et de sécurité du système d'information.

Pour résumer ces problèmes :

- Pas d'inventaire ni de renseignement des postes
- Pas de gestion des droits utilisateurs
- Besoin d'un accès à certains fichiers depuis le siège social (extérieur du réseau)
- Pas de sauvegarde ni de redondance du stockage des données

Objectif

Après avoir étudié avec le Directeur Administratif et Financier, les différents dysfonctionnements organisationnels, les risques de sécurité et leurs potentiels impacts sur l'entreprise ; nous nous sommes réunis afin d'établir les besoins et solutions pour l'amélioration de la gestion et l'administration de notre Système d'Information.

Pour résumer les besoins :

- Mise en place d'une infrastructure serveur pour la gestion du stockage et de l'accès aux données de l'entreprise
- Tolérance à la panne de cette infrastructure
- Sauvegarde des données et du parc serveur
- Accès sécurisé aux données de la centrale d'achat depuis le siège social



Solution technique

Pour s'assurer de répondre à l'ensemble des besoins, autant sur le choix matériel que logiciel, nous devons d'abord étudier l'architecture de notre Système d'Information.

Il nous faudra prendre en compte plusieurs données essentielles telles que :

- Le nombre d'utilisateurs finaux (salariés) et les répertorier pour améliorer la gestion.
- Le nombre de service de l'entreprise pour la gestion des droits
- Le nombre de poste client
- Le nombre de machines virtuelles qui seront déployer en production avec leurs rôles et leur configurations minimales requises.
- L'architecture du réseau et des bâtiments.
- Les éventuels prestataires.

Greencop employant 91 salariés et pratiquant une politique de recrutement continu proportionnelle à l'évolution de son activité, nous devons penser nos solutions techniques en fonction.

A ce jour nous disposons déjà de 91 postes de travaux configurés dont 45 nouveaux avec leurs licences activées. La suite OFFICE 365 pour 100 postes, une solution Antivirus Bitdefender Business, AnyDesk comme logiciel de prise en main à distance pour 2 sessions en simultanées, de l'ensemble des équipements réseaux déjà configurés et installés.

Solutions :

- Virtualisation des serveurs afin d'optimiser et rentabiliser l'achat de serveurs physiques
- Administration des accès utilisateurs aux ressources de l'entreprise via un serveur Active Directory
- Inventaire et supervision du parc, gestion des incidents par ordre de priorité avec GLPI
- Création d'un serveur FTP pour l'accès sécurisé aux données depuis l'extérieur du réseau



Virtualisation :

Virtualiser une infrastructure serveur est indispensable pour répondre aux besoins techniques et d'évolution du système d'information.

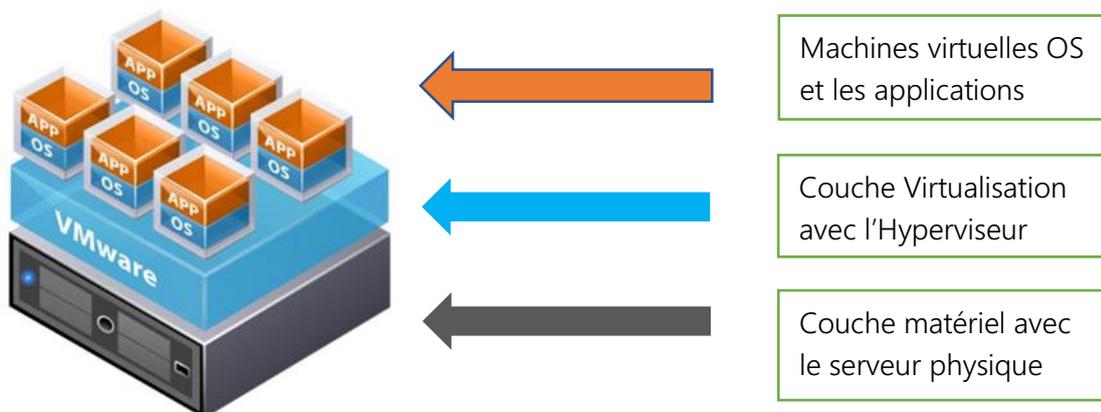
La virtualisation présente de multiples avantages :

- La centralisation de l'ensemble des serveurs et de leur gestion sur un environnement unifié.
- L'optimisation des ressources matérielles. Réduit en moyenne de 50% le nombre de serveur physique pour une entreprise.
- Un gain de place dans les locaux et baie de stockage.
- Coût des licences.
- L'optimisation du temps de travail.
- Une économie énergétique (Green-IT).
- Coût du stockage.

Quelques inconvénients sont tout de même à prendre en compte, par exemple :

- Les compétences techniques pour l'utilisation et le déploiement de cette technologie.
- La mise en œuvre d'un plan de maintenance.
- La dépendance à un éditeur (encombrement sur le disque/ gestion avancée du stockage/ pilotes renforcés etc....)
- La centralisation elle-même avec le SPOF (Single Point of Failure = point unique de défaillance).

Pour pallier cela, nous mettrons en place une solution de tolérance à la panne en redondant l'ensemble des serveurs.



Hyperviseur :

Un hyperviseur est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps.

Il existe en existe deux types :

- Type 1 (nommé « bare metal ») : il s'exécute au démarrage de la machine physique pour en prendre le contrôle, il est alors considéré comme outil de contrôle de système d'exploitation.
- Type 2 (nommé « hébergé ») : s'exécute sous forme d'une couche logicielle sur un système d'exploitation, comme n'importe quel autre programme informatique.

À la suite de la formation reçue et aux différents tests effectués, notre choix s'est porté sur VMware ESXi (hyperviseur de type 1 « bare metal »).

Nous avons appuyé ce choix technique sur ses principaux atouts comme son administration (par navigateur WEB ou logiciel), sa prise en main, la sécurité sur le réseau et le stockage, la possibilité de migration à chaud de machine virtuelle

Il est cependant onéreux comparé à Hyper-V de chez Microsoft puisque ce dernier est offert et intégré directement à l'installation d'un Windows Serveur.

Notre choix se justifie sur la rentabilité de notre temps de travail avec les possibilités de VMware ESXi et leur cohérence avec nos besoins.

Serveur Physique :

Pour pouvoir installer l'Hyperviseur, nous avons besoin de la couche matériel et donc pour cela un serveur physique. Celui-ci apportera les composants nécessaires (RAM, processeur) pour faire fonctionner l'environnement virtualisé.

Plusieurs choix de modèles et de constructeurs s'offrent à nous tel que HPE, Lenovo, DELL... Les modèles sont des serveurs tours, rack et LAME.

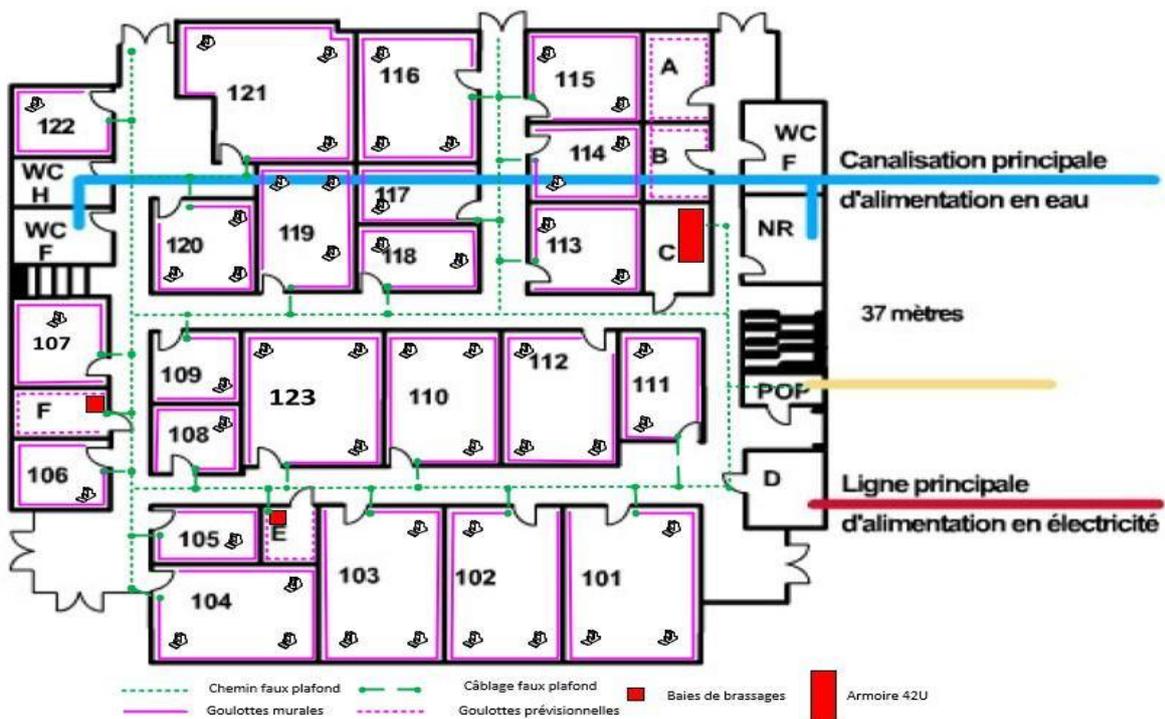
Pour la continuité des projets de l'entreprise et en restant cohérent dans nos choix, nous avons préalablement commandé et installé une baie serveur de 19" à 42U dans la salle dédiée. Celle-ci accueillera nos serveurs.





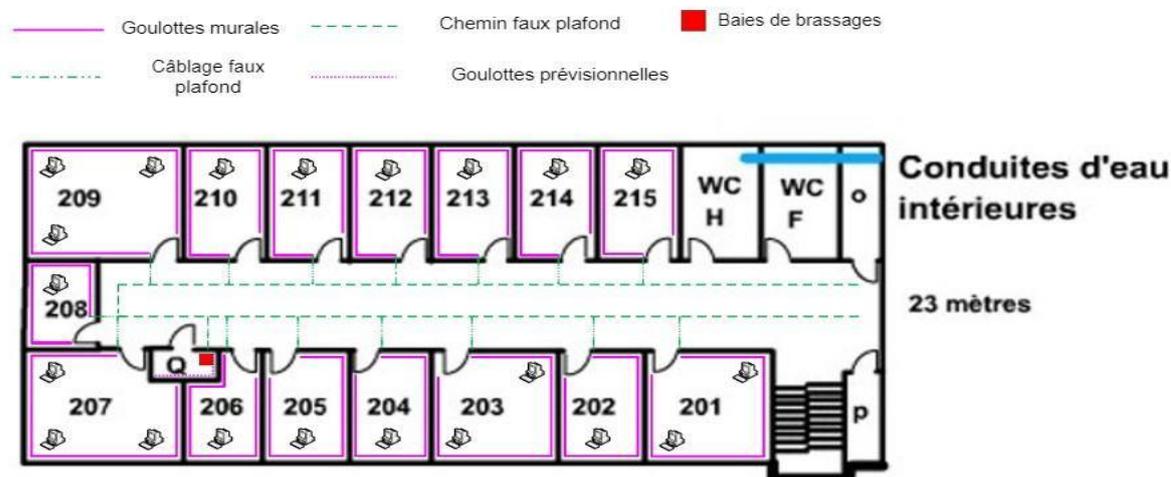
Voici la représentation en image d'un serveur RACK avant/arrière.

Pour rappel, voici le plan avec les pièces qui accueilleront la baie serveur (1^{er} bâtiment principal).



La baie principale se trouvera dans la pièce C du 1^{er} étage du bâtiment principal que l'on nommera « Local_Info ».

Premier étage de l'aile est



Nous installerons le NAS de sauvegarde dans l'Aile EST au 1^{er} étage dans la pièce Q.

Stockage :

Pour donner suite à l'acquisition de la fibre, il est plus pertinent de s'orienter sur une solution SAN plutôt qu'un NAS. Ce choix est également cohérent avec notre solution de virtualisation que propose VMware.

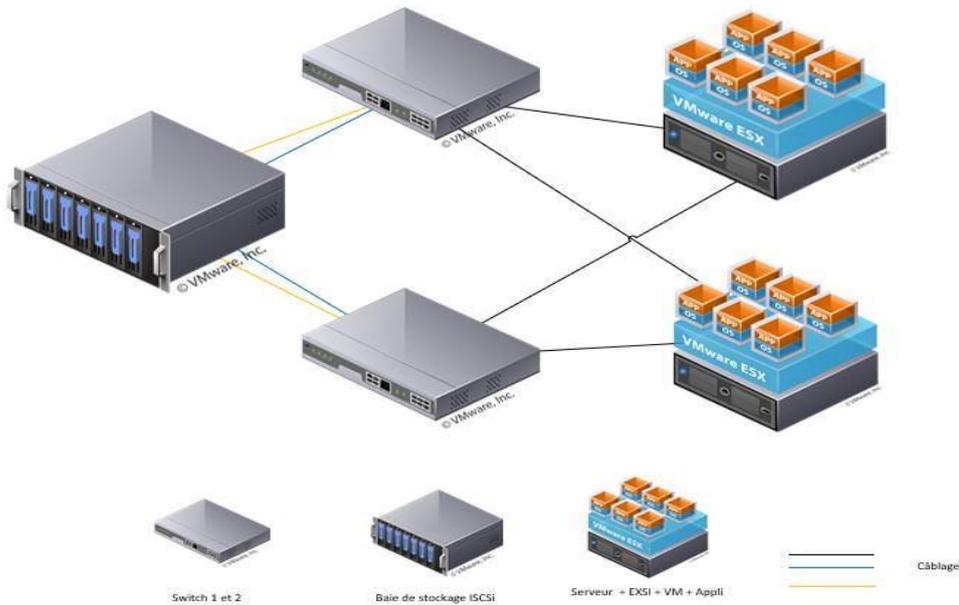
Contrairement au NAS, le SAN est un réseau dédié combiné entre des commutateurs, les différents serveurs le tout relié à la baie pour le stockage.

En plus d'être séparé du réseau des utilisateurs, son système est très performant en termes d'échange de données grâce à la vitesse et au débit de la fibre donc offrira de la performance supplémentaire sur la bande passante.

Il permet d'acquérir des environnements de serveur redondé et propose une solution de partage des ressources afin que plusieurs serveurs physiques se partagent plusieurs serveurs virtuels ce qui reste un très gros avantage en cas de panne.

Le protocole iSCSI consiste à créer un disque local virtuel sur les serveurs (physiques ou virtualisés) qui est mappé vers la baie de stockage. Ceci permet d'installer uniquement l'OS de l'hyperviseur sur les disques durs du serveur et donc de déporter les bases de données, les systèmes d'exploitation des serveurs virtuels et les fichiers. Le SAN apportera aux serveurs une

grande capacité de stockage et leur libérer des ressources en prenant en charge les opérations de lecture/écriture sur les fichiers confiés.



Sauvegarde :

Les incendies, les catastrophes naturelles, la possibilité de l'erreur humaine ou encore d'un dysfonctionnement sont des exemples de menaces liés à l'environnement et sont à prendre en considération.

Pour cela et pour protéger les données de Greencop qui comprends les fichiers mais également l'ensemble de l'infrastructure serveur virtuelle, nous avons mis en place une sauvegarde journalière et incrémentielle en interne.

Elle est également externalisée tous les jours sur une baie de stockage que nous avons installé dans un datacenter OVH.

The screenshot displays the Veeam Backup and Replication console. The main window shows a table of backup jobs. The selected job, 'Sauvegarde journalière', is a 'Windows Agent Backup' of 1 object, which has completed successfully 6 hours ago. The summary section provides detailed metrics: a duration of 41:14, a processing rate of 26 MB/s, and a bottleneck at the proxy. The data section shows that 19 GB (100%) were processed, with 17.8 GB read and 10.1 GB transferred. The status is 'Success' with 0 warnings and 0 errors. A throughput graph shows the data transfer rate over time, peaking at 77.1 MB/s. The action log details the job's progress, including host discovery, processing of 'vm-ad2', and a primary bottleneck at the proxy.

NAME	TYPE	OBJECTS	STATUS	LAST RUN	LAST RESULT	NEXT RUN	TARGET	DESCRIPTION
Externalisation	Windows Agent Backup Copy	1	Stopped	6 hours ago	Success	<As new restore...	Externalisation	de NAS Aix vers SAN hébergé
Sauvegarde journalière	Windows Agent Backup	1	Stopped	6 hours ago	Success	04/10/2020 22:00	Default Backup Repository	To NAS Alle-Est

SUMMARY		DATA		STATUS	
Duration:	41:14	Processed:	19 GB (100%)	Success:	1
Processing rate:	26 MB/s	Read:	17,8 GB	Warnings:	0
Bottleneck:	Proxy	Transferred:	10,1 GB (1,8s)	Errors:	0

NAME	STATUS	ACTION	DURATION
vm-ad2	Success	Job started at 04/10/2020 15:27:46	
		Building hosts list	04:04
		Waiting for rescan job Rescan of Sauvegarde journalière to complete	04:01
		Processing vm-ad2	36:43
		Load: Source 37% > Proxy 39% > Network 13% > Target 0%	
		Primary bottleneck: Proxy	
		Job finished at 04/10/2020 16:09:01	

La sauvegarde journalière est exécutée automatiquement tous les jours à 22h, une sauvegarde complète est faite tous les mois dans laquelle s'incrémente la journalière.

Hébergeur :

ASP SERVEUR

Aix-Marseille

Datacenter ASP SERVEUR

785 voie Antiope

13600 – LA CIOTAT, France

Tél. [0805 360 888](tel:0805360888)

Nous avons choisi cet hébergeur, car c'est un hébergeur qui se situe à proximité de nos locaux, dans notre département.

Ils font partis des rares acteurs au monde à prendre en considération la sécurité et la confidentialité des premiers échanges commerciaux jusqu'à l'administration et la supervision. Nous devons mettre en place par unité de 10 pour chaque équipement des demi-baie dans un datacenter PA3 des switch routeur et de baie de stockage.



Softwares

VSphere

En premier lieu, nous devons faire l'acquisition de la suite VSphere 7.0. C'est une plateforme de virtualisation de serveur. Elle permet de créer et gérer des machines virtuelles à grande échelle. Elle réduit les coûts de matériel et accélère le déploiement des applications, sans interruption de service grâce à de la haute disponibilité, de la tolérance de panne ainsi que de la sécurité avec le chiffrement des VM.

Dans cette suite, on y retrouve principalement :

1. L'hyperviseur ESXi est le système d'exploitation installé sur le serveur physique.
2. VMotion permet la migration à chaud des machines virtuelles sans interruption ni perte de service pour les utilisateurs ce qui facilite grandement la maintenance des serveurs.



3. VCenter Server s'installe sur une VM. Depuis la version 7.0 de VSphere, il n'est plus possible de le déployer sur Windows. Ce sera donc sous Linux.

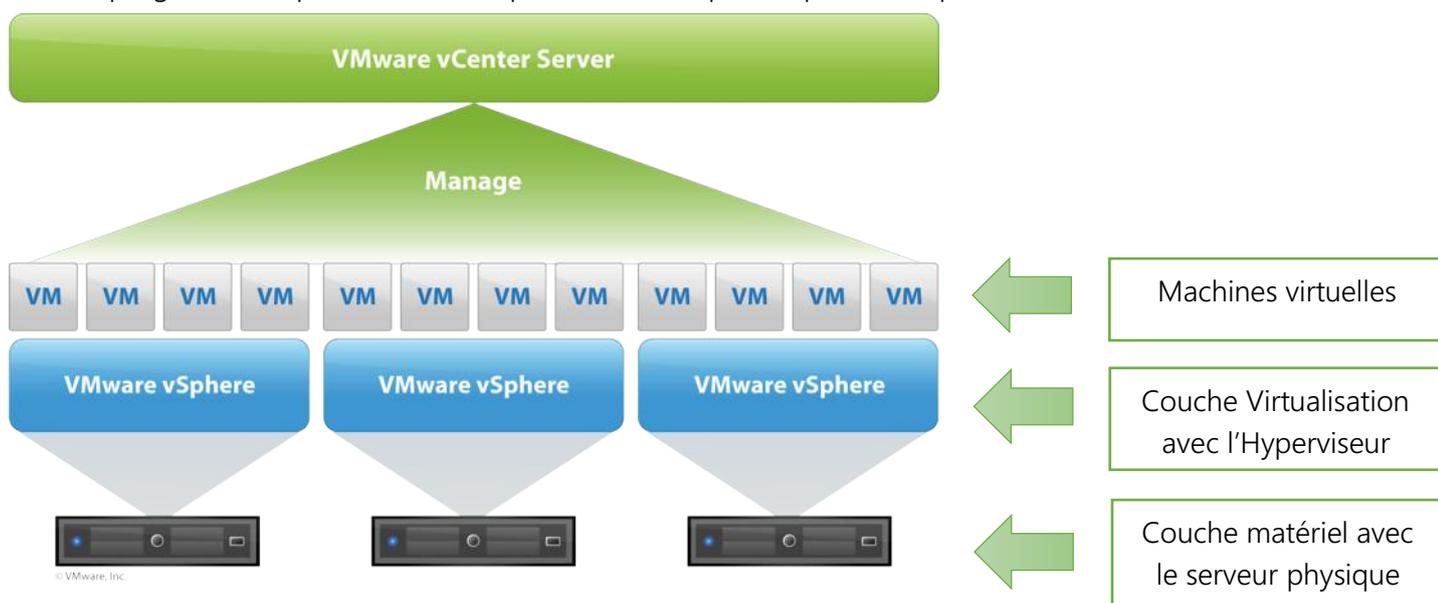
Cela permettra avec VCenter server :

- La gestion centralisée qui permet de configurer l'infrastructure virtualisée grâce à la même interface.
- Une surveillance rigoureuse et en temps réelle sur les performances de tous les composants (processeurs, RAM, stockage) peut être mise en place avec des déclencheurs d'alarmes ainsi que des planifications de tâches (par exemple : effectuer un snapshot d'une VM, migrer une VM etc....)

- Il assure également la surveillance en continue de l'utilisation des pools de ressources. Avec VMWare RDS. Il permet aussi la migration intelligente des VM sans provoquer d'interruption de service.
- Coté GREEN-IT en plus du clustering, un outil permet de placer les hôtes en veille pour réduire la consommation électrique.

Nous devons prendre une licence VCenter server qui lui est indépendant de la licence VSphere.

Le programme vSphere client 6.0 quant à lui n'est plus disponible depuis la version 6.5.



Ci-dessus, un schéma illustrant le fonctionnement du software.

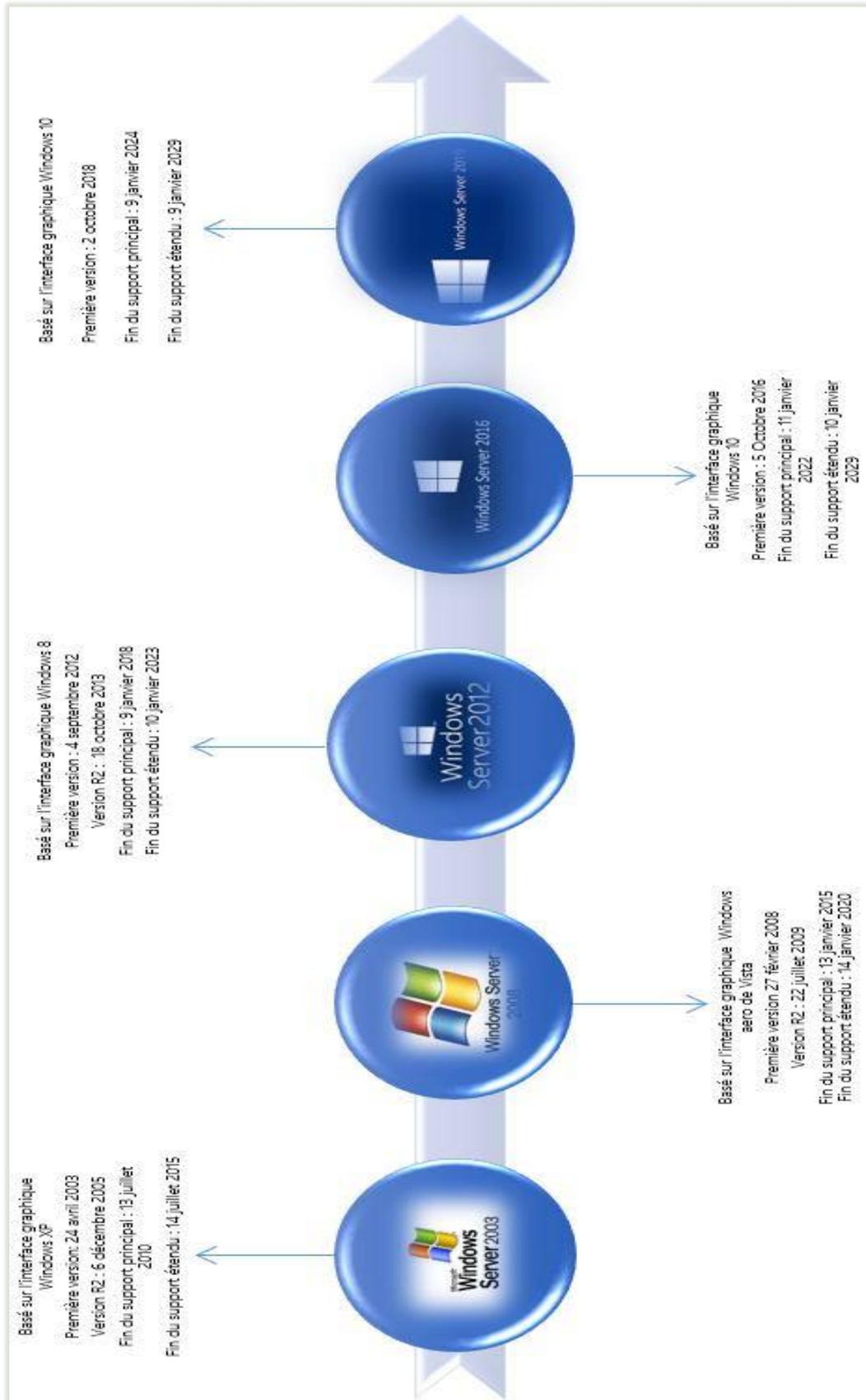
Windows Server

Windows serveur est un système d'exploitation pour serveur Microsoft, basé sur l'architecture Windows NT. Il est principalement destiné aux entreprises pour la gestion des ressources entre les utilisateurs et les applications et fournir différents services qu'un système d'exploitation Windows classique ne le permet pas.

Voici les différentes versions dans l'ordre chronologique à partir de Windows Server 2003 :

(D'autres versions antérieures qui ne sont pas représentées ici comme la version Windows NT Server 3.1 à 4.0 et Windows Serveur 2000 ont été également disponible).





Pour donner suite aux idées et remarques soumises de la part de notre D.A.F et pour répondre à ces besoins spécifiques, nous installeront un "Windows Server 2019" sur laquelle nous avons été formé.

Dans cette version, nous retrouverons trois éditions :

Editions	Essentials	Standard	Datacenter
Limitation utilisateurs / Périphériques	25 / 50	Basé sur les licences d'accès clients	Basé sur les licences d'accès clients
Modèles de licences	Pas de licences requise	Par nombre de cœurs	Par nombre de cœurs
Environnement d'OS virtualisé	2	2	Illimité

Notre choix s'est porté sur l'édition "Datacenter". Un choix tourné sur l'évolutivité de l'entreprise.

En effet, la version standard ne bénéficie que de deux Machines par licences et est destiné vers les environnements à faible densité ou non virtualisé contrairement à l'édition Datacenter.

En plus de serveur redondé en production, nous prévoyons par la suite le déploiement de plusieurs machines virtuelles avec l'ajout de nouveaux rôles pour optimiser l'administration de notre parc. Elles sont actuellement au stade de test en laboratoire

Ceci nous permettra d'avoir accès aux différents rôles et fonctionnalités de Microsoft et ainsi avoir une meilleure gestion des ressources entre les utilisateurs et les Applications.

- Le rôle lui définit la fonction d'un serveur, il fournit un service aux postes clients et autres périphériques. En voici quelques exemples :
 - Active Directory
 - DNS
 - DHCP
 - ...



Plusieurs rôles peuvent être ajoutés sur le même serveur, mais il est déconseillé d'en installer trop sur le même.

- Les fonctionnalités elles, servent au serveur lui-même comme :
 - Le clustering avec basculement qui permet de faire fonctionner un groupe de serveurs entre eux, ceci offre de la haute disponibilité. En cas de panne d'un des serveurs, le service est assuré par un autre serveur.
 - Client telnet pour prendre le contrôle à distance.
 - Gestion de stratégie de groupe qui permet l'administration et la gestion d'objet dans l'environnement Active Directory grâce à une console de composant enfichable (Console MMC).

Veeam

Pour la solution de sauvegarde, notre choix s'est porté sur Veeam Backup & Replication qui permet une sauvegarde des machines virtuelles et leurs données exécutées avec VMware ESX(i). Il assurera une reprise d'activité rapide en effectuant une restauration fiable de nos données au détail ou globale, des applications virtualisées et des services.



Une VM sera dédiée à l'installation de ce logiciel. La sauvegarde se fera sur le NAS Synology déjà acquis précédemment pour le projet Start.

Antivirus

En plus de la sauvegarde et pour veiller à la sécurité des données, nous rajouterons un antivirus sur l'ensemble de nos serveurs. Cela permettra de lutter contre toute attaque malveillante venant de l'extérieur tel que le vol de données, tous types de malwares (virus, vers, cheval de Troie ...), de cybermenace (ransomware, phishing, attaque Zero-day...).



Nous avons choisi précédemment Bitdefender GravityZone business Security comme solution payante d'une part pour sa sécurité qui protège des attaques citées plus haut et de l'autre sa facilité de gestion grâce à une console WEB. De plus il est largement plébiscité et a fait ses preuves durant des années de services.

Choix matériel

Pour pouvoir déterminer le choix du matériel, nous devons faire une étude sur le nombre de serveur et machine virtuelle à déployer.

Calcul des ressources

Après avoir étudié les informations et les recommandations sur chaque site officiel, nous sommes en mesure de réaliser un tableau récapitulatif des caractéristiques minimum requises pour l'installation de matériel et logiciel de notre infrastructure.

Caractéristiques requises	minimum ESXI	VM Windows serveur 2019	VM Linux (GLPI)	VM Veeam
RAM	4go / 8go pour exécuter les VM	512 MO	512 MO	512 MO
Stockage	32GO pour un SSD	32GO	32GO	32GO
Processeur /core	2 cores	1.4 GHZ	2 cores	1.4 GHZ

Pour plus de réactivité et de performance, nous augmenterons la RAM de chaque machine virtuelle de 512MO à 2GO. L'ESXi sur lequel tout repose, lui recevra 16 go de RAM.

Voici un tableau récapitulatif des machines virtuelles et leur rôle qui seront déployé :



	SRV01	SRV02	RAM/VM	Total
ESXI	1	1	16 GO	32 GO
VM AD-DS	1	1	2 GO	4 GO
VM DHCP	1	1	2 GO	4 GO
VM DFS	1	1	4 GO	8 GO
VM Veeam	1		8 GO	8 GO
VM GLPI (linux)	1		2 GO	2 GO
VM Serveur linux (debian) Samba/NFS/FTP	1		4 GO	4 GO
VM vCenter (linux)	1		2 GO	2 GO
VM WDS (Prévisionnelle)	1		2 GO	2 GO
VM WSUS (Prévisionnelle)	1		2 GO	2 GO
	Total		30	70 GO

Nous aurons donc 70 GO de RAM utilisées sur l'ensemble de l'infrastructure.

Dans le tableau, nous avons rajouté une VM WDS et WSUS qui sont prévisionnelle car elles ne sont encore qu'au stade de labo et ne seront donc pas déployées immédiatement.

Le WDS nous permettra de préparer une image du système d'exploitation Windows 10 pro. Pour faciliter la gestion du parc, nous pourrons affiner la configuration de l'image selon le profil de l'utilisateur, son service et ses besoins en termes d'application et de softwares.

Le WSUS quant à lui, stockera les mises à jour et viendra les installer automatiquement.

En prenant une version Datacenter de Windows serveur 2019, cela nous aidera à améliorer drastiquement notre parc informatique. Nous disposerons de ressources supplémentaires et pourrons automatiser les tâches de fonds comme les mises à jour logiciels sur l'ensemble des machines du parc. Les mises à jour ne sont pas à prendre à la légère, elles corrigent les failles de sécurité. Ceci représente un gain de temps précieux et donc de la productivité.

Nous pourrons également prétendre à déployer un serveur de messagerie (Exchange) ou encore un ERP si le besoin s'en fait ressentir selon la progression de l'entreprise et sur demande de nos supérieurs hiérarchiques.



Serveur :

Après avoir calculé les ressources nécessaires, nous pouvons déterminer le type de serveur physique que nous avons besoin.

Notre choix c'est porté sur la marque DELL, ayant déjà fait l'acquisition de laptop chez ce constructeur pour le renouvellement du parc et en étant très satisfaits en termes de performances et de support, nous avons retenu comme solution un serveur rack DELL PowerEdge R640.

Voici sa configuration :



Nous avons préféré configurer notre serveur nous-même en termes de processeur. En effet, selon les recommandations de Microsoft, un processeur avec beaucoup plus de cœurs et de la mémoire cache L3 plus élevée, couplés avec les 64 GO de RAM sera bien plus performant.

Également les SSD seront un gain en termes de vitesse d'écriture et lecture. L'alimentation sera redondée en cas de panne d'une des deux et éviter une coupure de service.

Si la capacité de nos serveurs sont trop faibles leur services et fonctionnalités en seront ralenties ce qui impacte directement le coût de production de l'intégralité de l'entreprise.

Afin d'améliorer notre système d'information, nous avons prévu de redonder nos serveurs ce qui fournira une haute disponibilité et de la qualité de services.

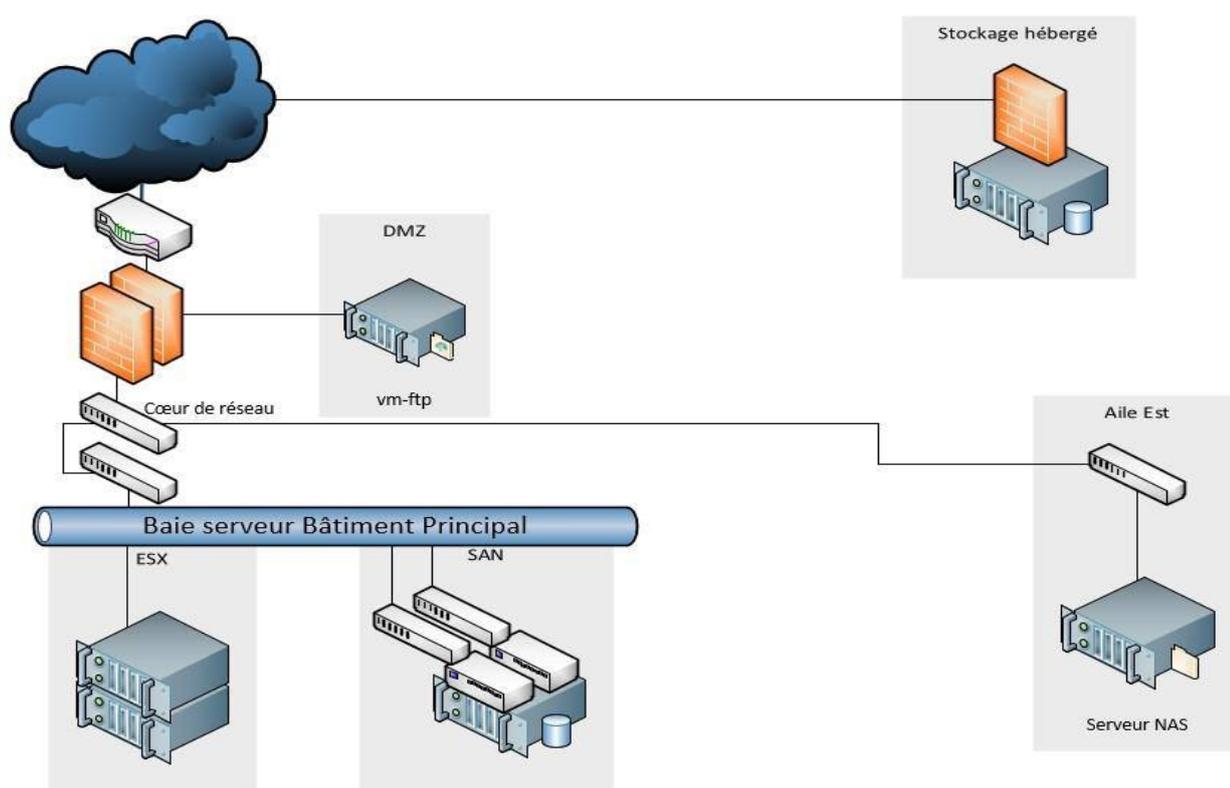
Baie de stockage :

Concernant le stockage de nos données et pour répondre à la demande du D.A.F, nous devons appliquer un quota de 5GO pour les données personnelles de nos utilisateurs. Ce qui fera un total de 455 GO actuellement pour 91 salariés. Un total de 64 TO sera mis à disposition pour le stockage de fichiers en Raid 5. Cela permet d'avoir une quantité plus importante pour les prochaines années.

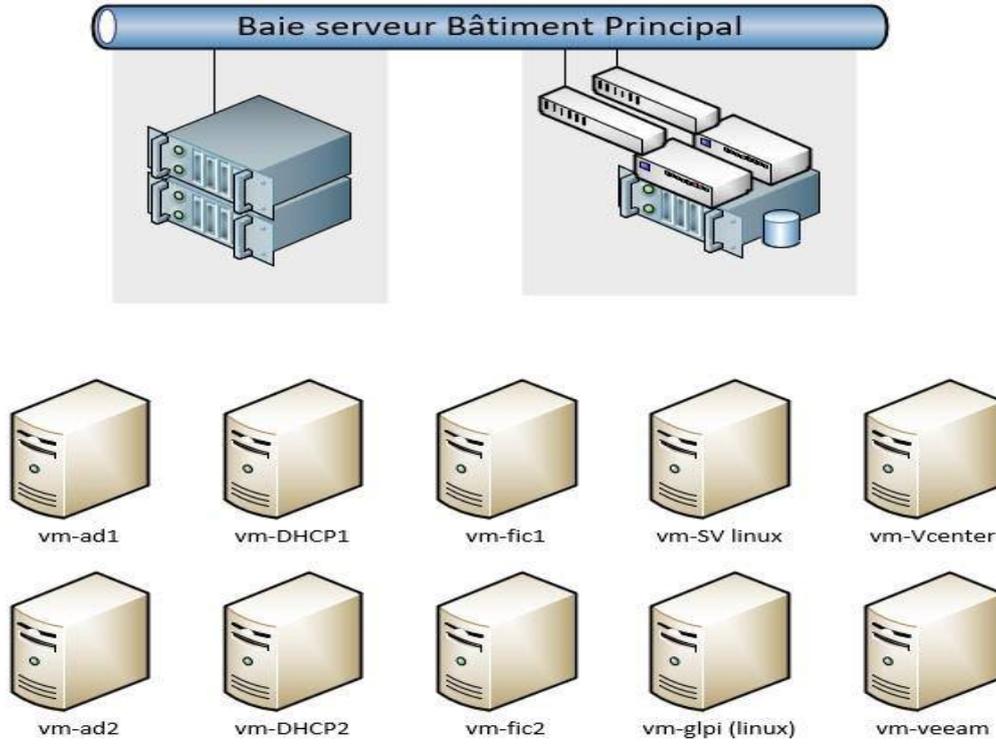
Nous prévoyons de déployer nos VM sur des SSD SAS pour la performance d'exécution que fourni un SSD. Elles seront stockées dans une banque de données qui utilisent le format de fichiers VMFS.

Les banques de données (datastore) sont des conteneurs logiques (disques virtuels) qui masquent les spécificités du stockage physique des machines virtuelles et fournissent un modèle uniforme pour stocker les fichiers de la machine virtuelle. Elles sont utilisées par l'ESXI.

Voici l'infrastructure de Greencop représenté par une topologie physique :



Celle-ci représente la baie de stockage avec l'ensemble des VM :



Calcul des licences :

Pour être dans le respect de la loi et dans les règles, nous devons nous fournir d'une ou plusieurs licences des logiciels que nous utiliserons pour administrer nos différents serveurs.

Les articles L.335-3, L.122-4 et L.335-2 du code de la propriété intellectuelle interdisent la copie et l'installation d'un logiciel sans l'accord du détenteur des droits d'auteur, et définissent les sanctions encourues. L'usage à titre gratuit d'un logiciel qui est protégé par un droit de licence est un délit. L'entreprise utilisatrice ainsi que les dirigeants peuvent être lourdement sanctionnés. En effet, des procédures civiles et pénales peuvent être encourue contre toute personne physique ou morale qui serait soupçonnée de piratage de logiciel protégé. Une amende de 150 000 euros et une peine d'emprisonnement de 2 ans maximum sont encourues. Dans un cadre professionnel, l'employé risque également d'être licencié pour non-respect de la charte informatique de l'entreprise si elle existe.

Dans le cas de fraude au niveau des licences contrefaites ou même travailler sans, Microsoft peut effectuer des contrôles et infliger des pénalités. L'image de notre entreprise en serait ternie et la clientèle méfiante.

Du point de vue technique, notre système d'information en serait impacté à cause de faille de sécurité, les mises à jour ne seraient pas disponibles. Tout ceci causerait la possible perte de données.

Pour éviter tout cela, nous avons fait une étude sur les logiciels dont nous aurons besoin et avons fait un choix.

Après avoir déterminer la liste des logiciels ainsi que le matériel, nous sommes en mesure de calculer le nombre de licences que nous devons nous fournir.

Windows Serveur 2019 :

Depuis Windows serveur 2016, Microsoft a introduit un nouveau système de licences. Il est basé sur le nombre de cœur du processeur. Contrairement, aux anciennes versions qui étaient basés sur les processeurs. Nos serveurs DELL possède deux sockets donc 2 processeurs avec 20 cœurs chacun. Ce qui veut dire 40 cœurs pour un serveur et 80 pour les deux.



Une simulation du nombre de licence que nous devons nous fournir s'avère nécessaire. Le site WEB d'HPE en propose une :



Datacenter Standard

HPE OEM Microsoft Windows Server Datacenter Edition

Datacenter Edition includes unlimited virtual instances of the operating system environment (VMs / OSEs) and Hyper-V Containers on the licensed physical server.

Licensing Requirements:

- All physical cores in the Server must be licensed (Hyperthreading (SMT) does not count as actual physical cores)
- A minimum of 8 cores must be licensed for each processor
- A minimum of 16 cores must be licensed for each Server

Clear All

Licensing Calculator

Input number of physical processors in the server processor(s)
 Input number of physical cores per processor noted above physical cores per processor
 Total of 80 cores need to be licensed

License Requirements

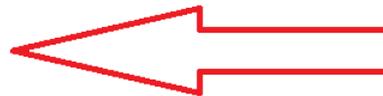
Base License Required

Windows Server® Datacenter (16 core) 1

Additional Cores To Be Licensed 64

Additional Licenses Required for Compliance

Windows Server® Datacenter Additional License (16 core) 4
 Windows Server® Datacenter Additional License (4 core) 0
 Windows Server® Datacenter Additional License (2 core) 0



Nous devons donc nous acquitter d'1 licence Windows Serveur plus 4 licences (16 cores) additionnelles pour être conforme et dans les règles.

Voici le tableau de tarification des différentes licences de chez Microsoft :

Édition de Windows Server 2019	Idéal pour	Modèle de licences	Conditions relatives aux licences d'accès client ^[1]	Tarification Open NL ERP (USD) ^[3]
Datacenter^[2]	Datacenters et environnements cloud hautement virtualisés	Basé sur les cœurs	Licence d'accès client Windows Server	\$6,155
Standard ^[2]	Environnements physiques ou faiblement virtualisés	Basé sur les cœurs	Licence d'accès client Windows Server	\$972
Essentials	Petites entreprises avec jusqu'à 25 utilisateurs et 50 appareils	Serveurs spécialisés (licence serveur)	Aucune licence d'accès client n'est obligatoire	\$501

Nous convertirons en Euro plus tard pour pouvoir estimer un budget.



Licences CAL

Pour qu'un utilisateur puisse accéder au serveur afin d'utiliser ses services comme l'impression et le stockage de fichiers, il faudra nous en acquitter pour que nos collaborateurs puissent travailler sans problème (uniquement pour la version standard et Datacenter).

Il existe deux sortes de CAL :

- CAL Device : est liée à un appareil pour lui fournir un accès aux services de Windows serveur. Quel que soit le nombre d'utilisateurs, ce sera le poste de travail qui en bénéficiera. Ce qui reste pratique dans le cas d'un poste de travail partagé.



- CAL User : à l'inverse celle-ci qui est liée à un utilisateur pour fournir l'accès aux services Windows Serveur depuis n'importe quel poste et appareil.



Avec 91 salariés ayant chacun leur propre ordinateur portable et avec des profils itinérants pour certains, nous préférons prendre des CAL User. Pour pallier la croissance de l'entreprise, nous en prendrons un stock plus conséquent, pour les futurs embauches. Ceci évitera de devoir en recommander à la dernière minute et être dans l'illégalité si un contrôle survient de la part de Microsoft.

Il existe un troisième type de CAL en plus des CAL DEVICE et USER, c'est la CAL RDS. Celle-ci sert à se connecter à distance aux serveurs et application de l'entreprise. Pour prendre un exemple, nous en aurons besoin pour se connecter sur le serveur Active Directory depuis notre PC personnel, par le biais du Remote Desktop Services (Services de Bureau à distances).

VSphere :

Les Hyperviseur ESXi doivent être sous licences VSphere. Selon VMware, avec une licence VSphere 7.0 couvre jusqu'à 32 cœurs. Avec un total de 80 cœurs, nous aurons donc besoin de 3 licences. De plus nous prendrons le niveau support « Production » de 3 ans qui nous garantira un support technique opérationnel H24, 7 j/7 en cas d'incident critique.

Voici le comparatif des prix des deux types de licences disponibles :

VMware vSphere			
VMware vSphere			
TITRE DU PRODUIT	Prix de la licence	Support et abonnement pendant 1 an	
 VMware vSphere Standard	€ 990.50	Basic	€ 271.64
		Production	€ 321.39
 VMware vSphere Enterprise Plus	€ 3,575.00	Basic	€ 751.23
		Production	€ 894.51

Nous avons préféré nous tourner vers la version « Entreprise plus » qui offre bien plus de fonctionnalité en termes de sécurité, de gestions des ressources, l'amélioration de la disponibilité et les performances des applications.

Produit



VMware vSphere 7 Enterprise Plus pour 1 processeur + support Production de 3 ans

Quantité  

Prix : **17809,47 €**

+ Appliquer un code de coupon
Sous-total : 17809,47 €

Total : 17809,47 €



VCenter serveur :

Pour VCenter, la licence est vendue séparément de VSphere. VMware propose une licence VCenter qui couvre 25 VM. Une seule licence sera nécessaire pour notre infrastructure.

Voici le tableau comparatif des prix des versions de VCenter :

Éditions de VMware vCenter Server			
Éditions de VMware vCenter Server			
TITRE DU PRODUIT	Prix de la licence	Support et abonnement pendant 1 an	
 VMware vCenter Server Foundation	€ 1,525.00	Basic	€ 557.20
		Production	€ 658.69
 VMware vCenter Server Standard	€ 6,145.00	Basic	€ 1,290.52
		Production	€ 1,536.28

Dans la même logique et pour rester cohérent dans nos choix, nous prendrons la version « standard » avec le support de Production de 3 ans.

Produit



VMware vCenter Server Standard pour vSphere (Par Instance) + support Production de 3 ans

Quantité  

Prix : **10200,78 €**

+ Appliquer un code de coupon
Sous-total : 10200,78 €

Total : 10200,78 €

Veeam :

Pour assurer la sauvegarde des configuration, systèmes et données des serveurs, nous avons choisi Veeam Backup & Replication car nous en maîtrisons le fonctionnement et sa maintenance.

Il nous offre une interface graphique complète et précise pour la sauvegarde de nos machines virtuelles.



Il est installé sur un serveur dédié et sauvegarde notre parc serveur sur notre NAS.

Budget :

N'ayant pas de limite de budget, nous avons tout de même décidé d'en avoir une projection. Mais par le manque d'information concernant la licence VEEAM Back & Restore, nous ne sommes pas en mesure de le clôturer.

Réseau

Pour une question de sécurité et de qualité du réseau, la bonne pratique est de découper le réseau en plusieurs VLAN (Virtual Local Area Network). C'est à dire isoler les différents réseaux, par exemple : Serveurs, wifi, imprimantes.

Nous préconisons un découpage comme suit :

- VLAN Utilisateurs
- VLAN Serveurs
- VLAN Wifi
- VLAN Imprimantes
- VLAN Management

Il existe plusieurs intérêts de mettre des VLAN en place sur un réseau d'entreprise, en voici quelques-uns :

- La gestion du réseau simplifié
- La sécurité
- L'optimisation de la bande passante
- La qualité de service (QoS)



Gestion simplifiée : Quand le réseau est découpé il est alors plus facile de diagnostiquer une panne car il suffit de la rechercher sur le réseau incriminé et non passer en revue la totalité du réseau.

Optimisation : Quand le réseau est découpé les informations circulent mieux, cela évite la surcharge et les ralentissements.

Sécurité : Une fois les VLAN créés, ils ne peuvent pas communiquer entre eux, le seul de moyen de les faire communiquer entre eux est de passer par un routage inter VLAN sur un routeur.

QoS : Permet de définir des niveaux de priorité aux différents flux réseau.

Découpage réseau et adressage IP :

Pour accéder à nos différents serveurs, nous leur adresseront manuellement une IP statique.

VLAN	Adressage IP
VLAN 10 (Utilisateurs)	192.168.1.0 /24
VLAN 20 (Serveurs)	192.168.2.0 /24
VLAN 30 (Wifi)	192.168.3.0 /24
VLAN 40 (Imprimantes)	192.168.4.0 /24
VLAN 50 (Management)	192.168.5.0 /24



Charte de nommage

Il est fortement recommandé de définir une charte de nommage de l'ensemble des périphériques que ce soit postes de travaux, serveurs, imprimantes etc.

Périphériques / Application	Désignation
Routeur	RT'local'-GREEN0x
Serveur	SV'local'-GREEN0x
Machines Virtuelles	VM-AD0x
Switch	SW'local'-GREEN0x
Pc fixe	GREENF0x
Pc portable	GREENP0x
Imprimante	PRINT-Nom du service

Dans le tableau ci-dessus le X indiquera le numéro du poste de travail comme par exemple GREENP02 et 'local' pour un switch définir dans quelle pièce il se trouve.

Un inventaire sous format Excel sera aussi créée et tenu à jour régulièrement par nos techniciens. On y retrouvera les informations importantes comme par exemple le nom du PC, son propriétaire, la version de l'OS, le type de processeur, la RAM et sa date de mise en service.

Également, tout notre parc informatique sera inventorié dans GLPI avec le nom de l'utilisateur, le service, le nom/numéro du poste de travail. Ceci nous facilitera grandement la tâche et la recherche pour nos intervention.

Un parc informatique bien géré améliore la productivité des utilisateurs et donc de l'entreprise.



PCA – PRA :

Comme nous l'avons cité plus haut, les incidents (inondation, menace externe, problème réseau, catastrophe naturelle...) qui menacent d'affecter le S.I sont nombreux.

Pour limiter l'ensemble de ses impacts liés à une interruption d'activités, nous devons cibler très clairement les éléments critiques de notre infrastructure.

Un Plan de Continuité d'activité et un Plan de Reprise d'Activité seront mis en place. Nous devons cibler très clairement les éléments critiques de notre infrastructure (Serveur, Application, documents, fichiers).

Il existe la règle du 3.2.1, c'est-à-dire disposer de 3 sauvegardes, les stocker sur 2 supports différents et 1 copie hors site.

Grâce à notre système SAN, la baie de stockage permet également de faire une sauvegarde en plus du stockage. En plus du NAS dans le bâtiment Aile EST, nous disposons du deuxième support et dans un endroit sécurisé qui plus est. Avec la sauvegarde externalisée, nous remplissons le dernier objectifs grâce à cette stratégie.

Cette politique de sauvegarde, nous permettra de sécuriser les données de l'entreprise et d'éviter leur perte. Ainsi l'intégralité de Greencop bénéficiera d'une continuité de services et de la haute disponibilité en cas de sinistre.

Concernant le matériel utilisateur, nous avons toujours une partie de l'ancien parc en Spare en cas de dépannage à court termes. Si une demande de renouvellement de PC est faite, une étude sur la nécessité pour chaque cas sera faite conjointement avec le DAF. Si cette demande est validée, nous nous tournerons chez notre fournisseur habituel.

Concernant la RTO et la RPO, par manque de projection et de tests, nous n'avons pas pu identifier les valeurs pour le moment. Une étude sera réalisée prochainement.



Procédure d'installation :

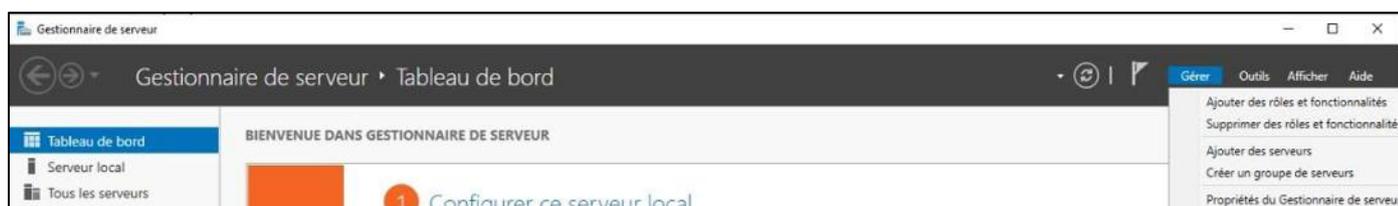
Windows serveur :

- Ajout AD-DS :

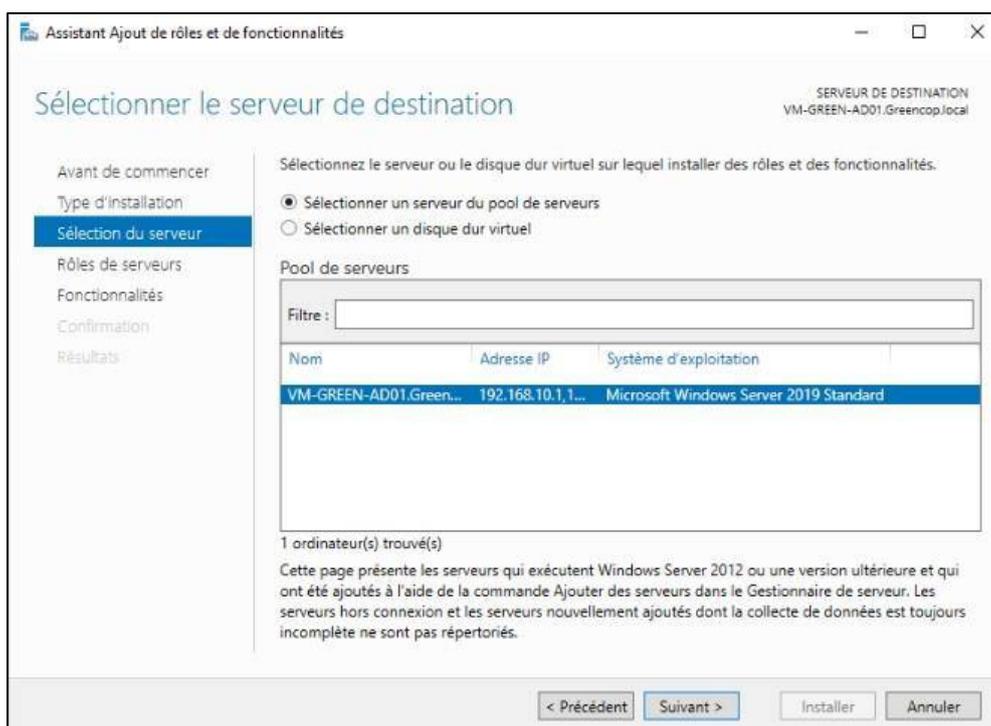
L'Active Directory Domain Service est un service d'annuaire de Microsoft qui utilise le protocole LDAP. Il permet par exemple de stocker des informations sur les comptes d'utilisateurs comme les noms, les mots de passe, les numéros de téléphone et permet aux utilisateurs autorisés du même réseau d'accéder à ces informations.

Le rôle DNS (Domain Name System) qui sert à traduire un nom de domaine en une adresse IP et inversement, sera installé par défaut avec l'ajout de l'AD-DS.

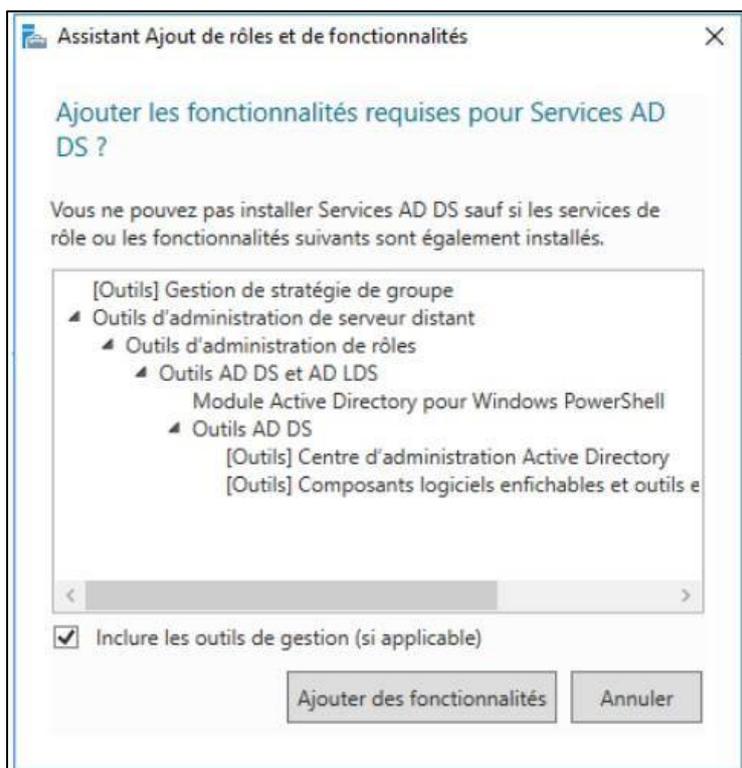
- Dans le gestionnaire du serveur, cliquer sur « Gérer », puis « Ajouter des rôles et des Fonctionnalités ».



- Cliquer sur « Sélectionner un serveur du pool de serveurs »

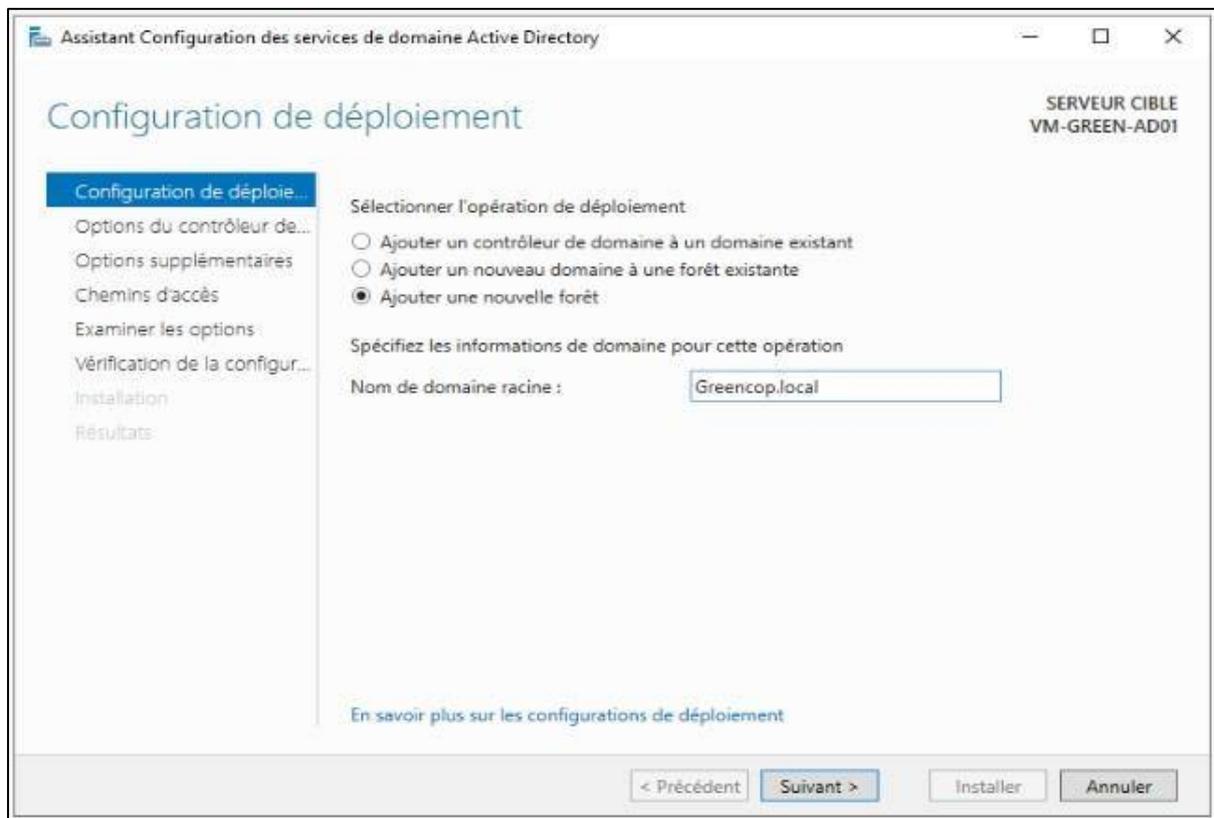


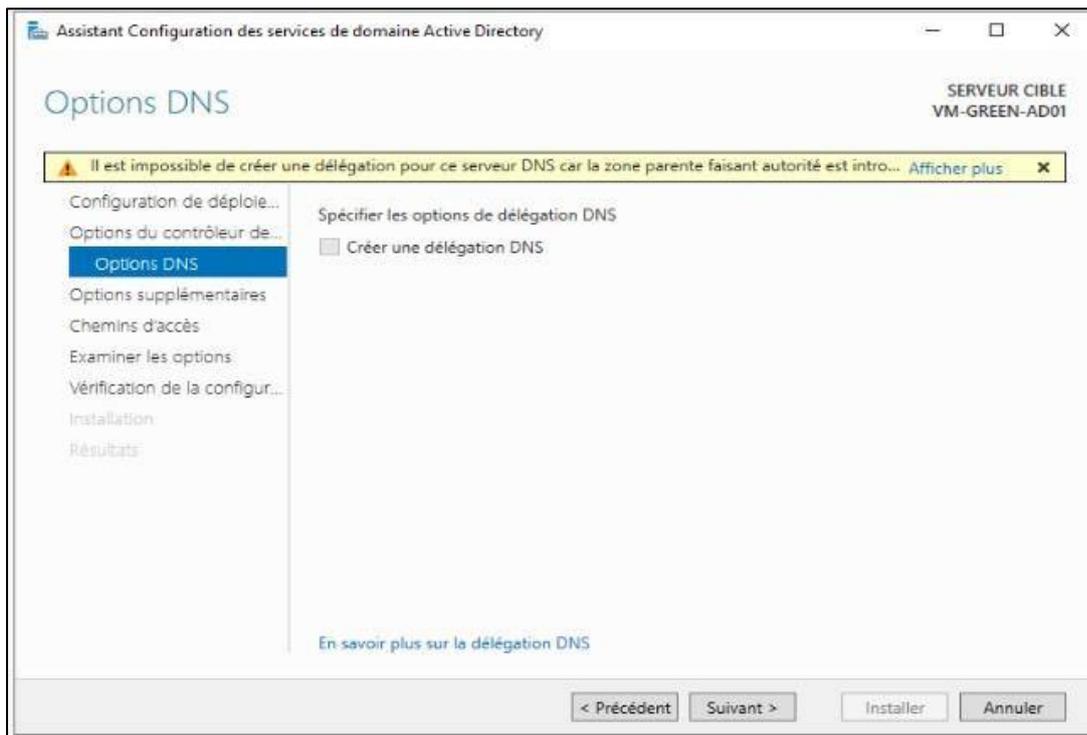
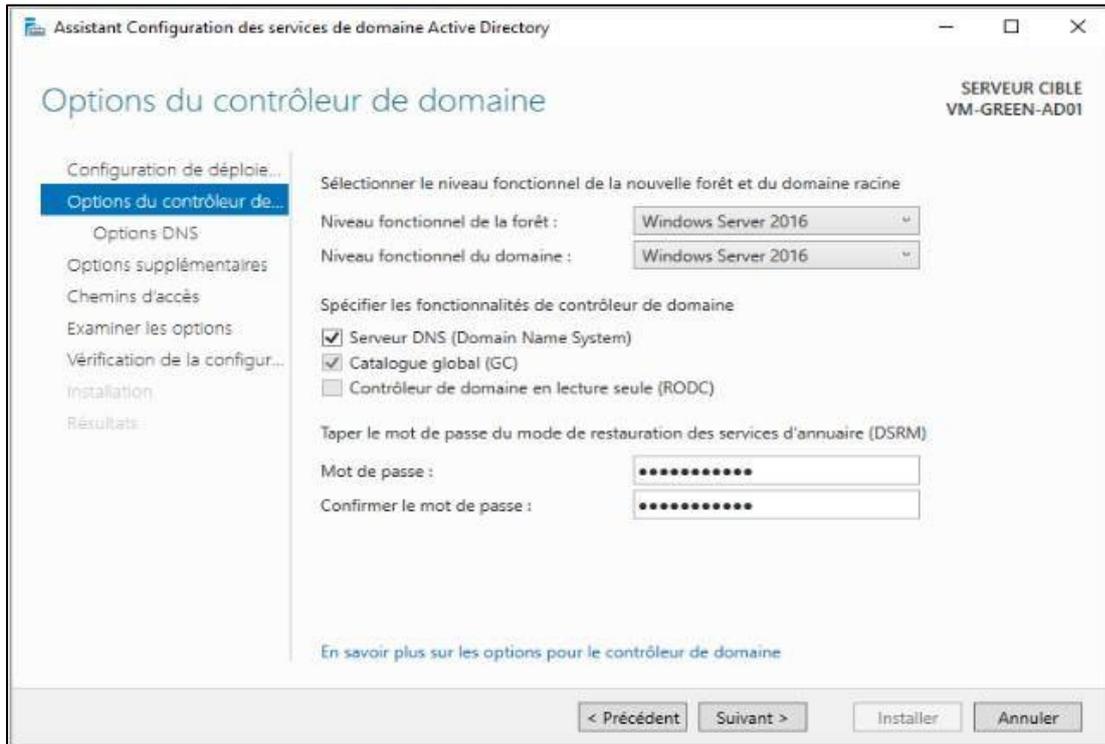
- Dans la liste des rôles, cocher « Services AD-DS »
- Cliquer sur « Ajouter des fonctionnalités »

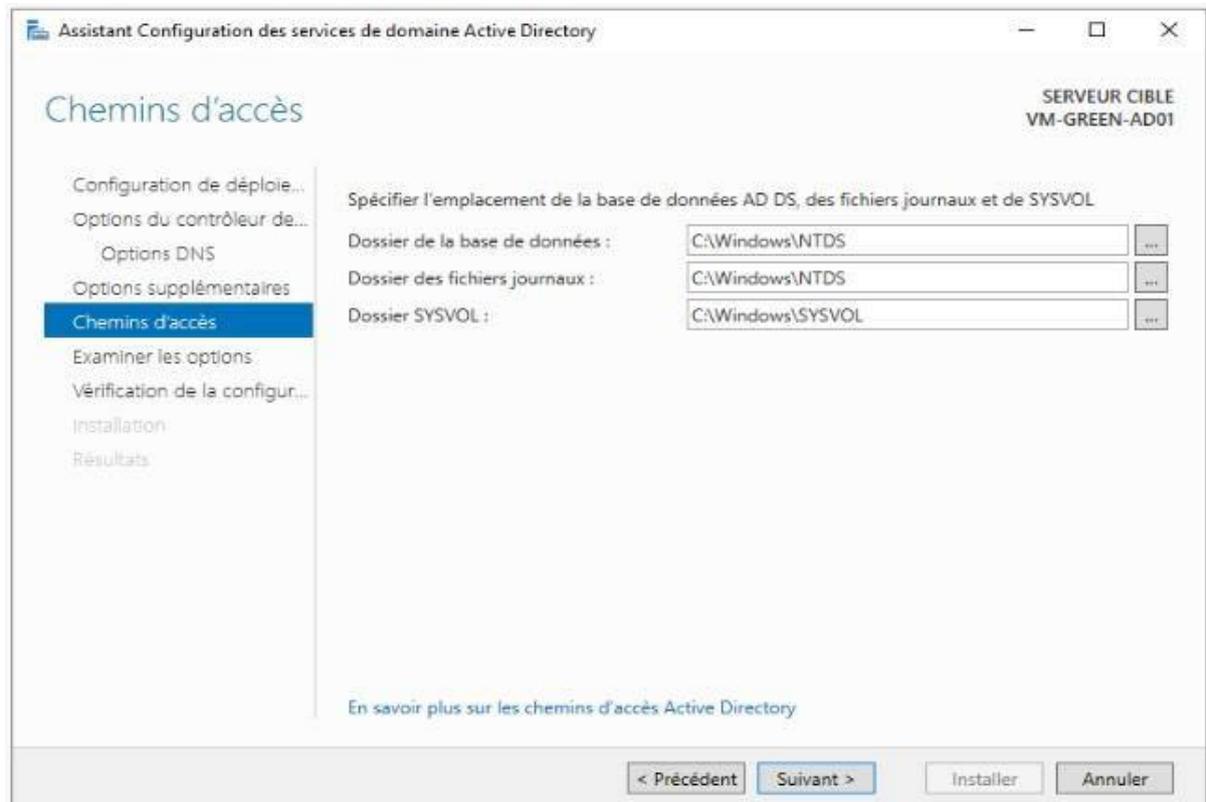
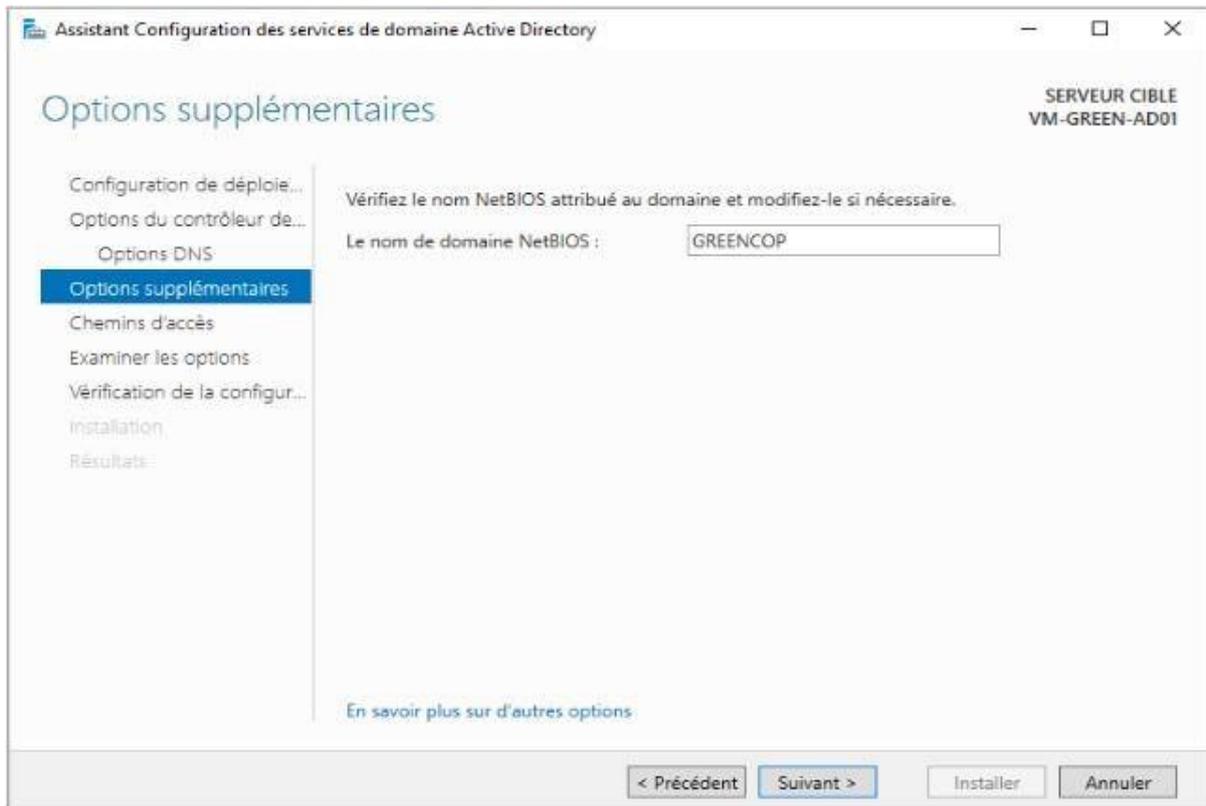


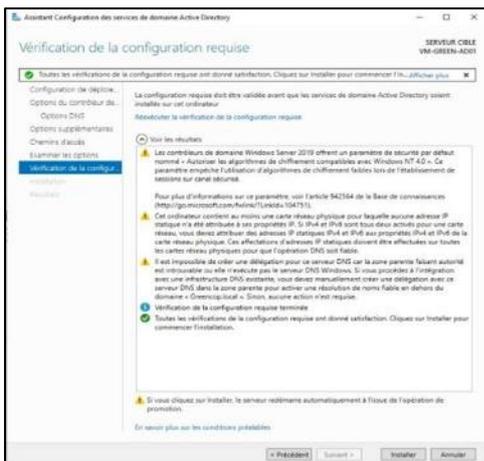
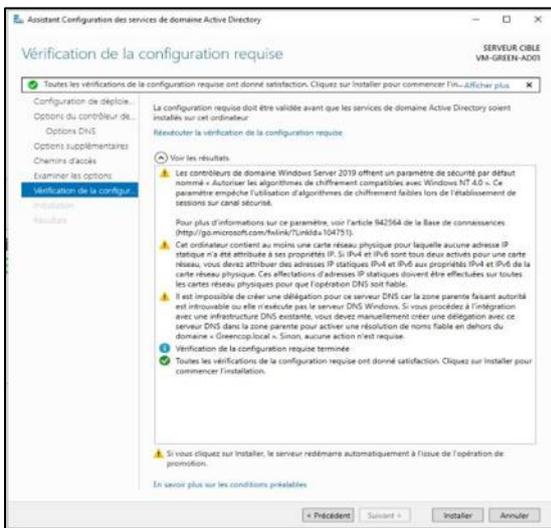
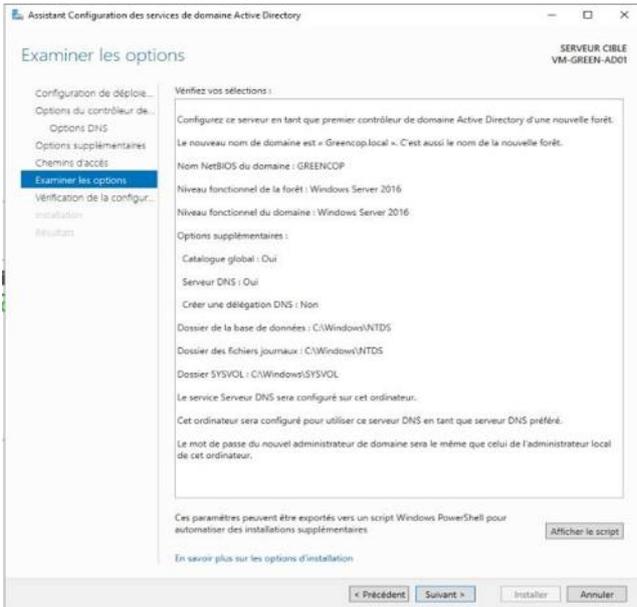
➤ Configuration de l'AD-DS

- Cliquez sur « Notifications »
- Cliquer sur « Promouvoir ce serveur en contrôleur de domaine »

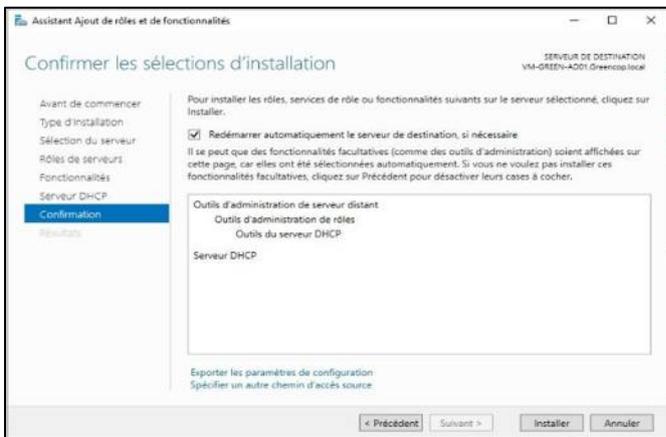
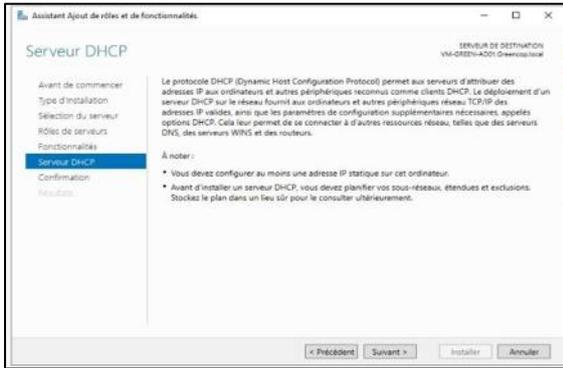
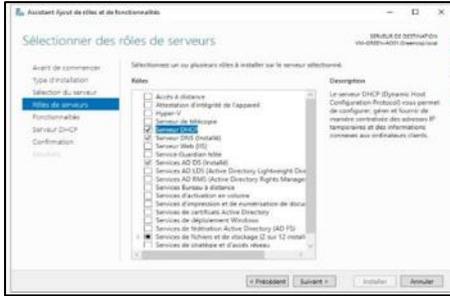


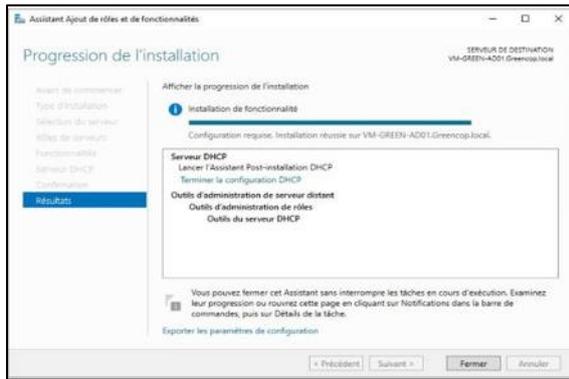




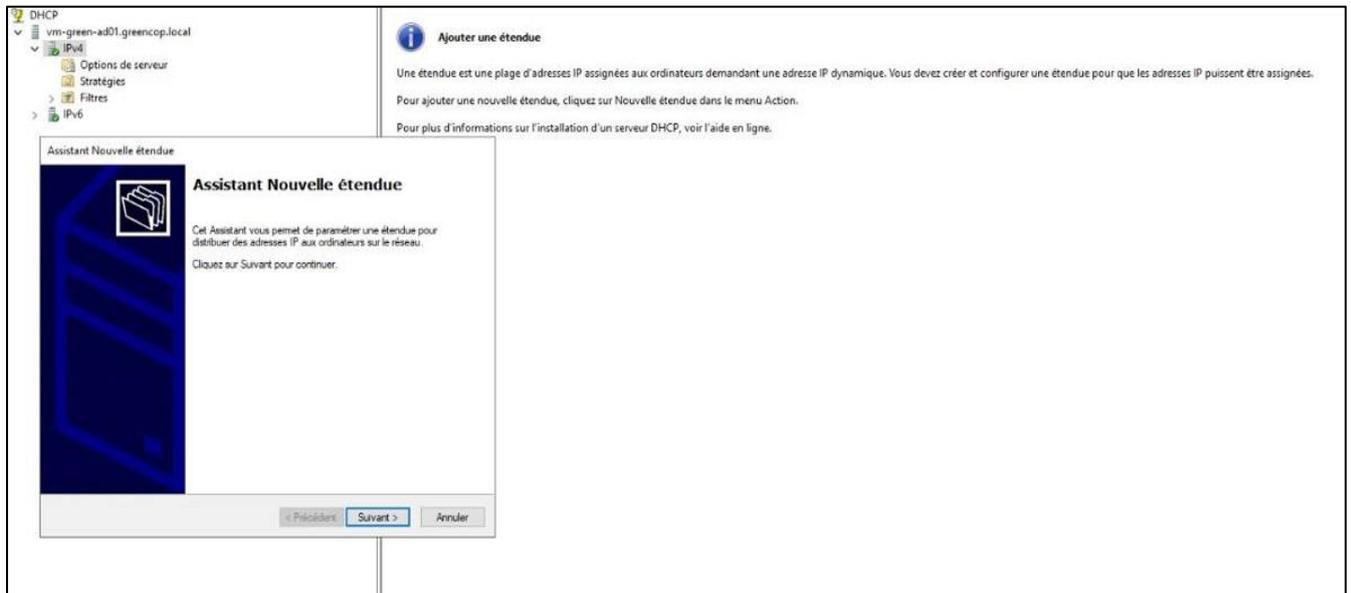


➤ Installation du rôle DHCP :





➤ Configuration de l'étendue DHCP :



Assistant Nouvelle étendue

Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP
Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : 192 . 168 . 20 . 1
Adresse IP de fin : 192 . 168 . 20 . 254

Paramètres de configuration qui se propagent au client DHCP :

Longueur : 24
Masque de sous-réseau : 255 . 255 . 255 . 0

< Précédent Suivant > Annuler

Assistant Nouvelle étendue

Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

192.168.1.1

Appuyer
Supprimer
Monter
Descendre

< Précédent Suivant > Annuler

Linux :

- Debian Server :
- Samba :

En mettant en place le service Samba, nous pouvons permettre le partage et l'échange de fichier entre un système d'exploitation Windows et celui d'un Linux.

a) Voici la première partie d'un Linux vers un Windows :

- Cette commande permet de mettre à jour les dépôts.



```
administrateur@LinuxSRV:~$ sudo apt-get update
```

```
17,3 Mo réceptionnés en 9s (1 991 ko/s)
Lecture des listes de paquets... Fait
administrateur@LinuxSRV:~$
```

- Une fois les mises à jour faites, nous installons samba.

```
administrateur@LinuxSRV:~$ sudo apt-get install samba
```

Dans le cas où le service samba est déjà installé voici la commande pour supprimer le dossier de configuration par défaut :

```
administrateur@LinuxSRV:~$ sudo rm /etc/samba/smb.conf
```

- Un nouveau fichier de configuration doit être créer.

```
administrateur@LinuxSRV:~$ sudo nano /etc/samba/smb.conf
```

- Entre crochet on spécifie le nom du partage.
- La variable 'path=/' contient l'endroit de montage du fichier partagé avec toute son arborescence.
- 'Browseable=yes' signifie le droit de dérouler toute l'arborescence.
- 'Read only=No' spécifie le droit d'écriture à l'intérieure.

```
GNU nano 4.8
```

```
[Processus]
  path=/
  browseable=yes
  read only=no
```

- Il faut donner un nouveau mot de passe pour un nouvel utilisateur (root) pour le partage.

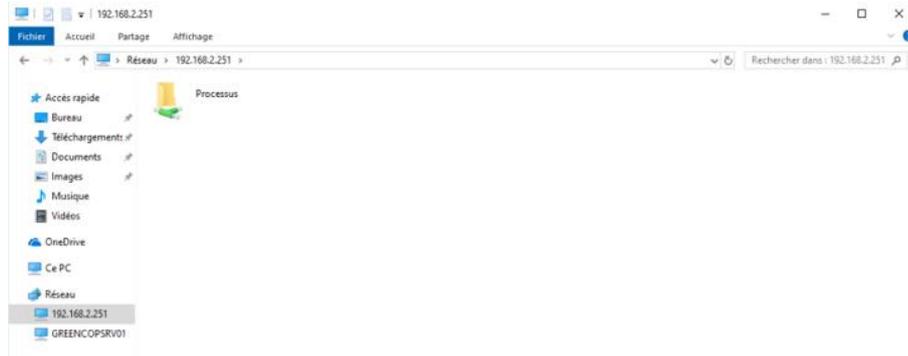
```
administrateur@LinuxSRV:~$ sudo smbpasswd -a root
New SMB password:
Retype new SMB password:
Added user root.
administrateur@LinuxSRV:~$
```



- Il faut relancer le service SAMBA.

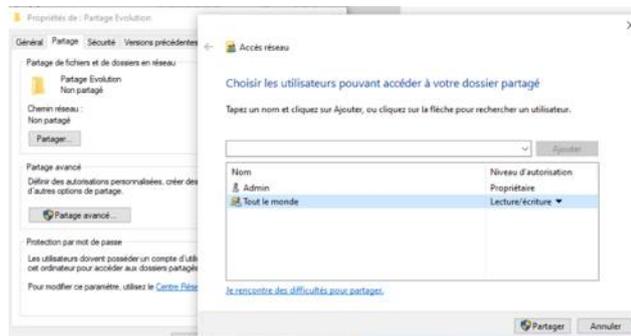
```
administrateur@LinuxSRV:~$ sudo /etc/init.d/smbd restart
Restarting smbd (via systemctl): smbd.service.
administrateur@LinuxSRV:~$
```

- Vérification sous Windows, il faut rentrer l'adresse du Serveur, puis se connecter avec les identifiants avec le mot de passe.



b) Deuxième partie Windows vers Linux :

- Créer un dossier (dans l'exemple à la racine de C :) puis le partager avec 'Tout le monde' en lecture/écriture.



- Il faut initier le point de montage avec le protocole CIFS



```
administrateur@LinuxSRV:~$ sudo mkdir /mnt/Evolution
```

- On change les permissions de droits sur le répertoire.

```
administrateur@LinuxSRV:~$ sudo chmod 777 /mnt/Evolution
```

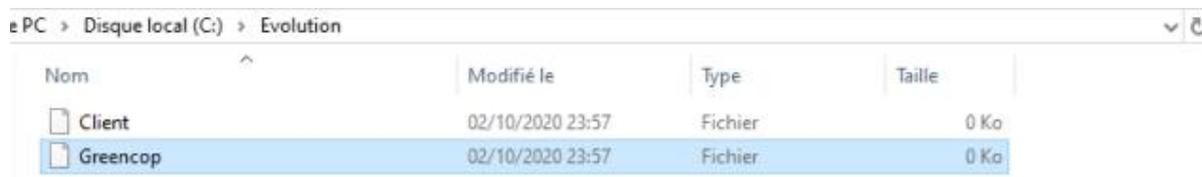
- Il faut ensuite monter la partition avec l'adresse du serveur, l'ajout d'un compte utilisateur et le mot de passe.

```
administrateur@LinuxSRV:~$ sudo mount -t cifs -o username=,password= //192.168.2.250/Evolution /mnt/Evolution/
```

- Pour naviguer dans le dossier et rajouter un fichier voici la commande.

```
administrateur@LinuxSRV:~$ cd /mnt/Evolution
administrateur@LinuxSRV:/mnt/Evolution$ sudo touch Client Greencop
administrateur@LinuxSRV:/mnt/Evolution$
```

- Vérification sous Windows :



Nom	Modifié le	Type	Taille
Client	02/10/2020 23:57	Fichier	0 Ko
Greencop	02/10/2020 23:57	Fichier	0 Ko

Mise en place solution technique :

Pour donner suite à l'audit réalisé par une SSII, voici les solutions techniques que nous avons apporté concernant l'administration de nos serveurs.

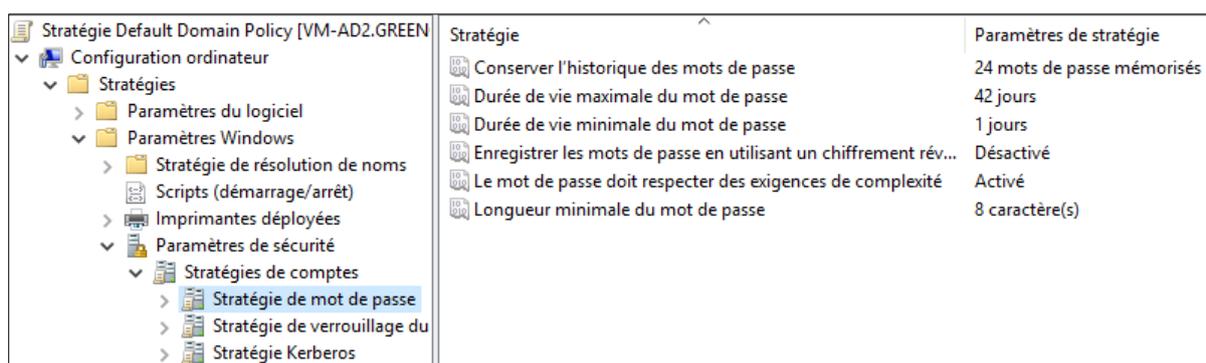
Windows serveur :



➤ Sécurité :

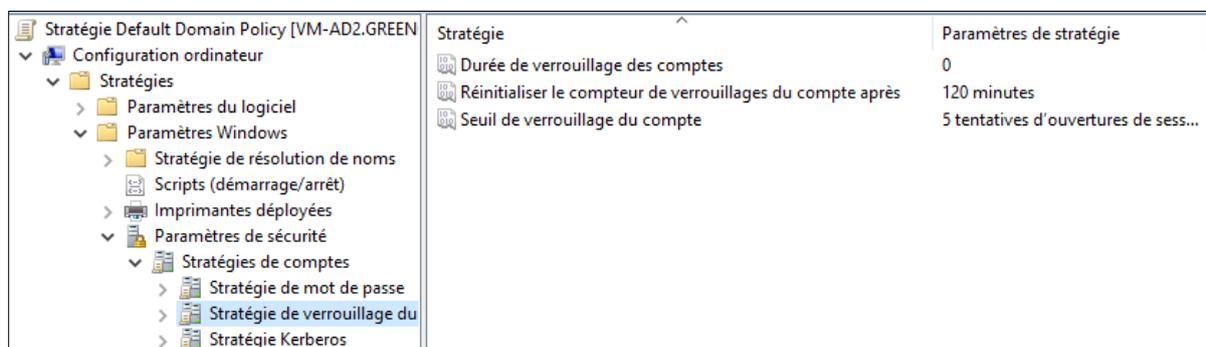
Dans un premier temps, pour la sécurité des comptes utilisateurs, nous avons configuré la stratégie de mot de passe comme le préconise Windows avec :

- Un minimum de 8 caractères.
- Une lettre majuscule.
- Une lettre minuscule.
- Un chiffre entre 0 à 9.
- Un caractère spécial (non alphanumériques).



Un changement de mot de passe sera demandé tous les 42 jours.

Pour renforcer cette sécurité, nous appliquons une stratégie de 5 essais maximum et une fois le compte bloqué il sera verrouillé pendant 120 minutes.

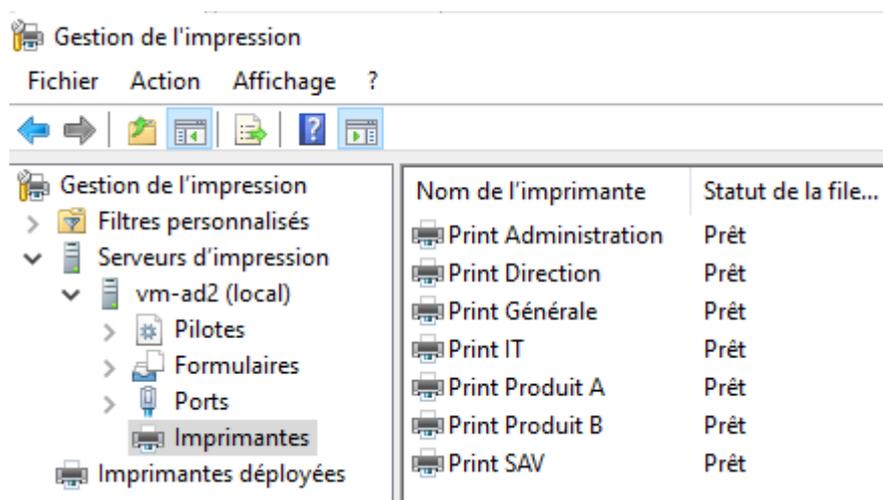


➤ Impressions :



▪ Les impressions

- Il faut 1 imprimante pour chaque service nommée « Print nom du service »
- 1 imprimante réseau pour tout le monde (les services Produit 1 et 2 ne peuvent imprimer qu'entre 8h et 17h)
- La direction est prioritaire sur toutes les impressions et les utilisent 24h/24
- Le service informatique dispose d'un contrôle total sur toutes les impressions
- Mme. LAPORTE et Mlle ADA (les assistantes des services SAV et Direction peuvent imprimer chez les Services Informatique et Services Produit A et B)



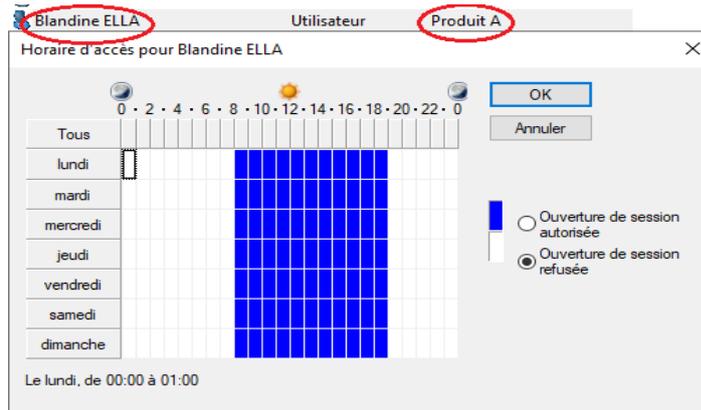
Pour l'ajout d'imprimante, nous avons rajouté le rôle de serveurs d'impression à notre DC.

➤ Connexions au réseau de l'Entreprise :

▪ Les connexions réseaux

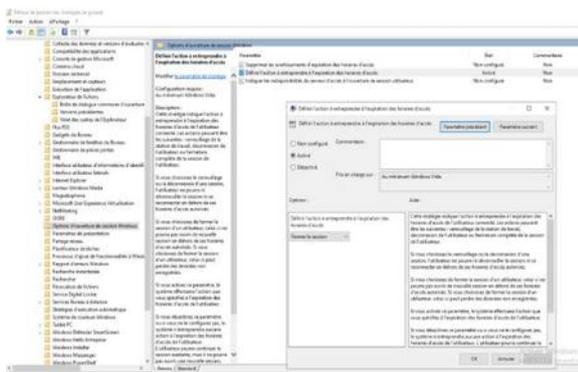
- Mme BEZIAT, ELLA, AYO et ACIEN ne peuvent se connecter qu'entre 8h et 18 h et à 19h elles doivent être déconnectées (elles sont du service Produit A)
- Aucun salarié (exceptés la direction, le SAV et l'informatique) ne peut se connecter entre 20h et 7h

Pour cette demande, n'ayant que 4 personnes concerné, nous l'avons appliqué directement sur le compte des utilisateurs en question.



La même manipulation a été également faite sur les 3 autres comptes. Nous prévoyons de créer un script si une demande viendrait à être rédigé pour d'autre utilisateur.

Une GPO a été créée pour forcer la fermeture de session et interdire la connexion entre 20h et 7h sauf pour la Direction, le SAV et l'IT. La GPO a été appliqué pour les autres services.



➤ Connexion aux lecteurs réseau et gestions de droits NTFS :

■ **Connexion aux lecteurs réseau**

- Chaque service doit avoir un répertoire nommé « Commun *nom du service* » qui sera attribué à chacun des salariés lors de sa connexion réseau
- A l'intérieur de chaque répertoire, vous créez un dossier pour chaque salarié (contrôle total sur celui-ci et aucun accès sur ceux des collègues)
- Seuls la direction et l'informatique peuvent y accéder en plus (lecture seule pour la direction)
- Attribuer un dossier de base à 2 users locaux au choix
- Attribuer un dossier de base à 2 users du domaine au choix
- Planifier 2 audits au hasard
- Configurer au moins 3 journaux à 3 jours
- Désactiver le moniteur d'évènements



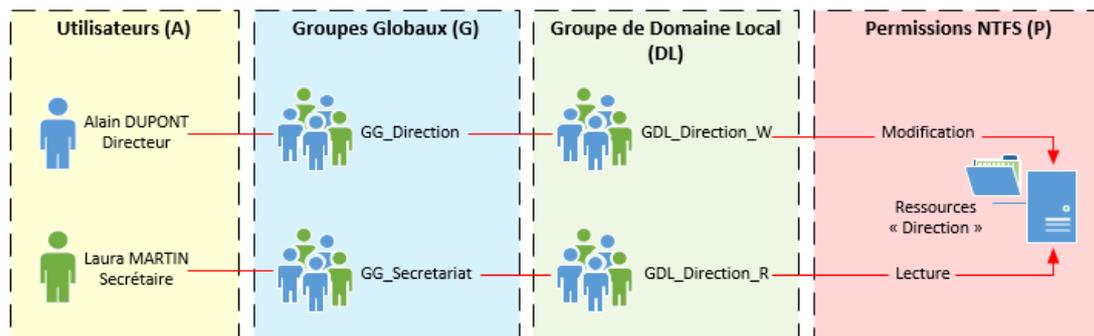
Dans un premier temps, nous avons créé différentes UO dans la console Active Directory.

Une UO sera nommée « groupes » dans laquelle des groupes de sécurité seront également créés.

Pour la création des groupes de sécurité et les gestions des droits, nous nous sommes appuyés sur la méthode que préconise Microsoft une fois de plus, c'est-à-dire le AGDLP (Account, Global, Domain Local, Permission). C'est une bonne pratique pour définir et gérer les accès aux ressources partagées, principalement sur les fichiers et imprimantes dans un domaine AD. Il facilite la tâche pour l'ajout de nouveaux utilisateurs et permet de limiter les erreurs.

Fonctionnement :

- Un utilisateur est relié à un des groupes globaux symbolisé par son service
- Chaque groupe global est relié (membre) d'un ou plusieurs groupes locaux symbolisé par le type d'accès aux ressources.
- Chaque ressource (dossier, fichier, imprimante) est assignée par des permissions vers les groupes locaux.

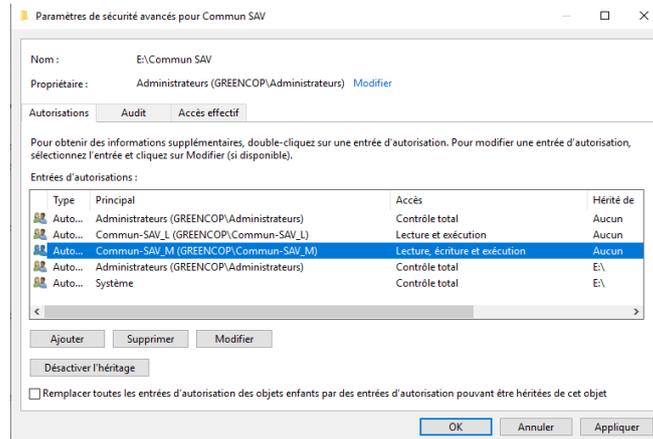
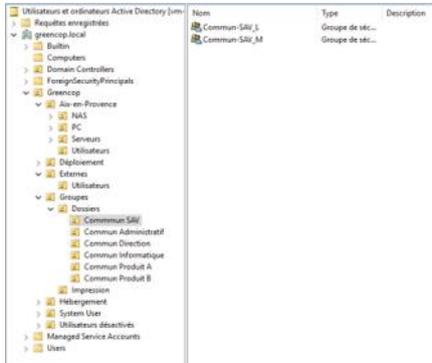


Ci-dessus, un schéma représentant la méthode.

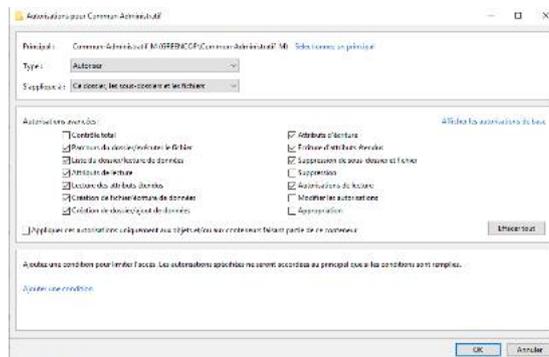
Un lecteur réseau commun par service est provisionné par GPO sur les sessions utilisateurs auquel seuls les membres du groupe de sécurité peuvent accéder.

- Commun Administratif
- Commun Direction
- Commun Informatique
- Commun Produit A
- Commun Produit B
- Commun SAV

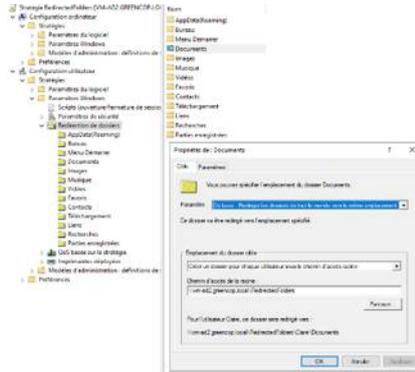




Les utilisateurs ayant les droits en modification sur ces dossiers peuvent créer et modifier des sous-dossiers et fichiers mais ne peuvent pas supprimer les dossier communs.

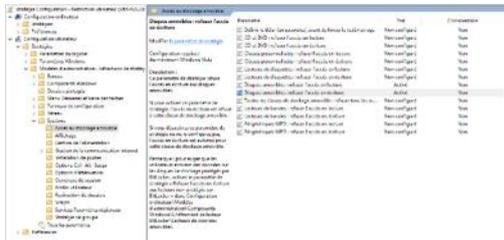


- L'ensemble des données utilisateurs seront centralisé sur le serveur grâce à une GPO qui redirige les chemins d'accès vers un des disques du serveur prévu à cet effet :



- Blocage des accès aux périphériques USB pour les Produit A et B :

Une GPO appliqué aux utilisateurs faisant partis des groupes Produit A et B empêche l'utilisation



- Pour l'ajout de nouveau utilisateur dans l'Active Directory, nous avons créé un fichier csv qui sera importé dans un script PowerShell qui nous facilitera la tâche au quotidien.

	A	B	C	D	E
1	prenom	nom	password	ou	group
2	Bertrand	TENOND	user@GCop*:	OU=Utilisateur Externes	
3	Hugues	COHEN	user@GCop*:	OU=Utilisateur Externes	
4					



```

1 1
2 1
3 1
4 1
5 1
6 1
7 1
8 1
9 1
10 1
11 1
12 1
13 1
14 1
15 1
16 1
17 1
18 1
19 1
20 1
21 1
22 1
23 1
24 1
25 1
26 1
27 1
28 1
29 1
30 1
31 1
32 1
33 1
34 1
35 1
36 1
37 1
38 1
39 1
40 1
41 1
42 1
43 1
44 1
45 1
46 1
47 1
48 1
49 1
50 1
51 1
52 1
53 1
54 1
55 1
56 1
57 1
58 1
59 1
60 1
61 1
62 1
63 1
64 1
65 1
66 1
67 1
68 1
69 1
70 1
71 1
72 1
73 1
74 1
75 1
76 1
77 1
78 1
79 1
80 1
81 1
82 1
83 1
84 1
85 1
86 1
87 1
88 1
89 1
90 1
91 1
92 1
93 1
94 1
95 1
96 1
97 1
98 1
99 1
100 1

```

Linux :

Pour répondre à la demande du DAF, nous mettrons en place comme solution dans un premier temps le services SAMBA entre le serveur de fichiers sous Windows Server vers un serveur Linux.

Ce serveur Linux sera déployé dans une DMZ. Ce qui permettra d'isolé ce serveur du reste du LAN tout en étant accessible depuis Internet en garantissant la sécurité du LAN. Le personnel d'entreprise qui se trouve hors-site pourra avoir accès aux fichiers en se connectant au serveur Linux.

Grâce à SAMBA, l'opération de partage de fichier sera complètement transparente pour l'utilisateur.

Pour se connecter au serveur Linux, nous installerons un client FTP. Il permettra donc la recherche de dossiers ou de fichiers de manière que rien ne soit stocké sur le serveur Linux

Conclusion

À la suite des cours donnés par les intervenants lors des sessions de formations, aux diverses ressources en ligne et aux échanges d'informations entre collaborateur et tuteurs de formation, nous avons d'abord pu déployer un parc informatique composé d'ordinateur avec différents systèmes d'exploitation ainsi que plusieurs suite Logiciels.

Nous sommes désormais capables d'installer et administrer des serveurs (de différents environnements) qui viendront ajouter des rôles et des services au parc informatique tel que



l'Active Directory ou le DHCP, le tout en améliorant les pratiques quotidiennes d'un Service Informatique. Nous sommes également en mesure d'apporter une solution de stockage, et de sauvegarde interne et externalisée.



Annexes

Devis



CoffeeSoft
8 Rue des Frères Lumière
77100 Meaux
France
Tél : 0185490879
Fax : NC
Email : contact@coffeesoft.fr

DEVIS N° 001
Date d'émission : 28/09/2020

Code client : 0011
Greencop
536, Euro-pôle de l'Arbois
13290 Aix-en-Provence
France
contact@greencop-aix.com
N°TVA : 444 444 441

Licences Windows Serveur

Les prix sont valables jusqu'au 08/10/2020

Référence	Désignation	Quantité	Prix U HT	Remise %	Montant HT	TVA %
30092020	Windows Serveur 2019 USER CAL édition : 20 Utilisateurs	1.00	909.67	17.00	755.03	20.00
31092020	Windows Serveur 2019 USER CAL éditions : 50 Utilisateurs	2.00	1 772.04	17.00	2 941.59	20.00
32092020	Windows Serveur 2019 RDS/TSE USER CAL édition : 5 Utilisateurs	1.00	724.80	17.00	601.58	20.00
22092020	Windows Serveur 2019 Datacenter (16 cœurs)	5.00	4 768.10	5.00	22 648.48	20.00
Total HT					28 946.68	
Total TVA 20.00%					5 389.34	
Total TTC					32 336.02	
Net à payer (€)					32 336.02	

Règlement

- Date limite : 28/09/2020 (À la commande)
- Mode : Virement bancaire
- Taux d'escompte en cas de paiement anticipé : néant
- Taux annuel de pénalité en cas de retard de paiement : 3 fois le taux légal selon la loi n°2008-778 du 4 août 2008

Vu avec notre service commercial pour la remise, bonne réception de nos produits.

Bon pour accord le :
Signature





Détails du devis

Date de création
02/10/2020

Numero du devis
8031997

Référence client
0001

Livraison

Mode de livraison
Standard

Paiement

Mode de paiement
Carte de crédit

Montant total dû
15 482,48 € HT

Siège social

inmac wstore
125 avenue du bois de la pie
95921 Roissy-en-France Cedex
France Métropolitaine

Tél : 01 41 84 41 84
Fax : 01 48 17 81 61
Web : www.inmac-wstore.com

SIRET : 38805549300059
TVA : FR 39388055493

DEVIS

N° 8031997

Adresse de livraison

Greencop
536 Europole de l Arbois
13290 Aix-en-Provence

Description	Prix unitaire	Qté	Total
Lenovo - Disque SSD - 1.6 To - SAS 12Gb/s réf. Inmac : 7205284 <u>Commentaire :</u>	1 181,97 €	2	2 363,94 € HT
Lenovo ThinkSystem DE2000H Hybrid 2U24 SFF controller enclosure - baie de disques réf. Inmac : 7174140 <u>Commentaire :</u>	5 934,70 €	1	5 934,70 € HT
HPE Midline - disque dur - 8 To - SAS 12Gb/s réf. Inmac : 2978375 <u>Commentaire :</u>	897,98 €	8	7 183,84 € HT
Total HT			15 482,48 €
Livraison Standard			50,00 €
TVA 20%			3 106,50 €
Total TTC			18 638,98 €

Observations :

Merci pour votre confiance !

M. PARTICULIER :
Gestionnaire de compte
01 41 84 41 84





DELL France
 1 rond-point Benjamin Franklin
 34000 Montpellier
 France
 Tél : NC
 Fax : NC
 Email : NC
 351528229 / 35152822900088
 NC
 Code NAF : 4851Z
 N°TVA : FR20351528229

DEVIS N° 123456
 Date d'émission : 07/09/2020

Code client : 2986378
 Greencop
 536 europole de Tarbois
 13290 Aix-en-Provence
 France
 contact@greencop-aix.com
 N°TVA : 444 444 441

Serveur rack DELL

Les prix sont valables jusqu'au 07/10/2020

Référence	Désignation	Quantité	Prix U HT	Remise %	Montant HT	TVA %
Référence	Smart value Power Edge r640 Serveur Optimal	2.00	8 801.73	40.00	10 562.08	20.00
Référence	Entrer ici le nom du produit	0.00	0.00	0.00	0.00	0.00
Référence	Entrer ici le nom du produit	0.00	0.00	0.00	0.00	0.00
Total HT					10 562.08	
Total TVA 20.00%					2 112.42	
Total TTC					12 674.50	
Net à payer (€)					12 674.50	

Règlement	
-	Date limite : 07/10/2020 (30 jours)
-	Mode : Prélèvement

Bon pour accord le :
Signature



Glossaire

- Active Directory : Service d'annuaire de Microsoft utilisant le protocole LDAP, contenant divers objets, ayant pour objectif de centraliser l'authentification des utilisateurs au sein d'un système d'information
- Adresse IP (Internet Protocol) : est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol.
- CAL (Licences Accès Client) : Une CAL pour Windows Server est une License qui permet aux clients (Utilisateurs) d'accéder à Windows Server. Elles sont conjointement utilisées avec les licences logicielles Microsoft Windows Server pour permettre aux utilisateurs ou aux périphériques d'accéder aux services sur le serveur.
- DFS (Distributed File System) : Ce système de fichier hiérarchisé permet de structurer les fichiers partagés sur différents serveurs du réseau de façon logique. Un utilisateur ne verra pas le nom du serveur où se trouve les fichiers. L'avantage c'est que si le serveur vient à changer à cause d'une panne ou pour cause d'évolution, le chemin d'accès restera le même.
- DHCP (Dynamic Host Configuration Protocol) : Protocol réseau servant à fournir une adresse IP, un masque de sous-réseau et une passerelle par défaut automatiquement à un poste client en faisant une demande au serveur.
- DNS (Domain Name System) : le service DNS a pour fonction de traduire un nom de domaine en adresse IP et inversement.
- ERP (Entreprise Resource Planning) : est un logiciel de gestion qui permet à l'entreprise d'intégrer différentes fonctionnalités telles que la gestion comptable et financière, la gestion des ressources humaines, des stocks, des fournisseurs, de l'e-commerce etc.
- Fibre Channel : est un protocole utilisé pour transporter des données entre des appareils.
- Hyperviseur : En informatique, un hyperviseur est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps.
- iSCSI (Internet Small Computer System Interface) : Protocole de stockage en réseau basé sur le protocole IP destinée à relier les installations de stockage de données. Il est utilisé pour faciliter les transferts de données. Également utilisé pour transmettre des données sur des réseaux locaux (LAN), réseaux étendus (WAN) ou Internet et peut permettre d'être indépendant sur l'emplacement physique du stockage ou de la récupération de données.
- LDAP (Lightweight Directory Access Protocol) : Protocole standard qui permet de gérer des annuaires en accédant à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP. Permet d'interroger et modifier un service annuaire.
- LUN (Logical Unit Number) : est le numéro d'identification d'un espace de stockage d'un équipement SCSI présenté à un plusieurs serveurs.
- NAS (Network Area Storage) : traduit en français par stockage en réseau, est un serveur de fichier (boîtier ou rack avec des disque durs) relié à un réseau dont la principale fonction est le stockage de données en volume centralisé pour un LAN.



- NFS (Network File System) : est un protocole standard de partage de répertoire (dossiers) sous Unix/Linux. Il faut deux ordinateurs au moins, un serveur sous GNU/Linux où se trouve les fichiers à partager et un client qui doit pouvoir accéder aux fichiers du serveur. Il utilise les protocoles de communications CIFS, SMB, NFS, FTP, IP, etc.
- SAMBA : est une mise en œuvre de protocole SMB « écrite pour les systèmes Unix. Il a été conçu pour permettre aux PC/Serveurs Windows d'accéder aux répertoires et aux fichiers UNIX en utilisant le protocole SMB, donnant aux utilisateurs l'illusion d'utiliser un serveur Windows.
- SAN (Storage Area Network) : Zone de stockage en réseau en français, composé de switches, des baies de disques durs et d'un câblage spécifique.
Il permet de mutualiser des ressources de stockage. Il est implanté en tant que réseau sur lequel sont connectés les serveurs et les périphériques de stockage. Tous les serveurs peuvent y accéder. Il utilise les protocoles de communications ISCSI, SAS et Fiber channel.
- SAS (Serial Attached SCSI) : est une technique d'interface pour disques durs, elle constitue une évolution des bus SCSI en termes de performances, et apporte le mode de transmission en série de l'interface SATA (Serial Advanced Technology Attachment).
- SCSI (Small Computer System Interface) : est une norme (bus informatique) qui permet de relier un ordinateur à un périphérique en mode bloc. C'est un protocole client/serveur.
- SMB (Serveur Message Block) : est un protocole de partage de fichier inventé par IBM en 1995. Celui-ci a permis aux ordinateurs de partager des fichiers sur un hôte distant via un LAN.
- VMFS (Vsphere Virtual Machine File System) : est un format de système de fichiers spécial hautes performances optimisé pour le stockage des machines virtuelles dans des banques de données sous Vsphere.
- WAN (Wide Area Network) : Réseau informatique étendu, qui couvre une grande zone géographique qui relie plusieurs petits réseaux comme des LAN entre eux. Le fonctionnement d'un WAN repose sur la technique de la liaison point à point qui consiste à établir une connexion entre un fournisseur d'accès Internet et le réseau d'un client via une ligne louée (cuivre ou fibre). Cela impose l'utilisation d'un routeur pour déterminer le trajet optimal pour atteindre un nœud de réseau.
- WDS (Windows Deployment Services) : est un service Windows server utilisant l'environnement PXE pour booter par le réseau sur une image (OS) Windows sur un poste de travail. Il est possible de lui configurer les drivers, les logiciels, les applications grâce à sa console de gestion.
- Windows NT (NT : New Technology) : désigne la série de système d'exploitation (multitâche, multi-utilisateur, multiprocesseur) que Microsoft a créé et qui ne repose pas sur le système MS-DOS.
- WSUS (Windows Server Update Services) : est un service permettant de distribuer les mises à jour pour Windows et d'autres applications Microsoft sur les postes de travail fonctionnant sous Windows sur le parc informatique. WSUS est un rôle pour serveur Windows lui permettant de devenir un serveur de mise à jour local. Il télécharge et stocke l'ensemble des mises à jour disponibles auprès de Windows Update de Microsoft.

