



PROJET EVOLUTION

Omar AIT-MOULID / Julien VILLARD
CENTRAL S.A | 10 RUE DES PYRENEES 64000 PAU



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 0/93

Auteur	Vérificateur	Date	Version	Commentaires
AIT-MOULID Omar	VILLARD Julien	23/07/2018	01	Création Sections 1 à 3
VILLARD Julien	AIT-MOULID Omar		02	Section 4.1
AIT-MOULID Omar	VILLARD Julien		03	Sections 4.2 à 4.6
VILLARD Julien	AIT-MOULID Omar		04	Section 5 et 6
AIT-MOULID Omar	VILLARD Julien	27/09/2018	05	Sections 7 et 8

Ce document est la propriété de CENTRAL S.A,
merci de ne pas le diffuser à l'extérieur de
l'entreprise.



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 1/93

Table des matières

1	Cadre du projet	5
1.1	Contexte	5
1.2	Problématiques.....	5
1.3	Objectifs	5
1.4	Contraintes	5
2	Méthodes de travail.....	6
2.1	Réunions	6
2.2	Partage des ressources.....	6
2.3	Tableau de suivi	6
2.4	Procédures	6
2.5	Transfert de connaissances	6
2.6	Sauvegardes et plan de secours	7
3	Mind Map préliminaire.....	8
4	L'infrastructure informatique.....	9
4.1	Les différents types d'infrastructure.....	9
4.1.1	L'infrastructure classique	9
4.1.2	L'infrastructure centralisée	9
4.1.3	L'infrastructure hyperconvergée.....	10
4.1.4	Virtualisation	10
4.1.5	Solution choisie.....	14
4.2	Stockage	15
4.2.1	Données en production	15
4.2.2	Sauvegardes.....	18
4.3	Systèmes et applications.....	24
4.3.1	Rôles et fonctionnalités attendues	24
4.3.2	Windows Server.....	25
4.3.3	Distribution Linux	30
4.4	Réseau	31
4.4.1	Vlans.....	31



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 2/93

4.4.2	Routage	32
4.4.3	Listes d'accès (ACL)	32
4.4.4	Plan d'adressage général	33
4.4.5	Plan d'adressage détaillé	33
4.5	Schéma	36
4.6	Liste des serveurs	37
5	Application gestion de parc	38
5.1	Cahier des charges	38
5.2	Langages.....	39
5.2.1	Base de données	39
5.3	Interface web	40
5.3.1	HyperText Markup Language (HTML)	40
5.3.2	Cascading Style Sheets (CSS)	40
5.3.3	PHP	41
5.3.4	Javascript (JS)	41
5.4	Framework et librairies	42
5.4.1	Bootstrap.....	42
5.4.2	jQuery	42
5.5	Modélisation	43
5.5.1	Base de données	43
5.5.2	Interface web	47
5.6	Fonctionnalités	48
5.6.1	Administrateur.....	48
5.6.2	Ajouter	50
5.6.3	Consulter.....	51
5.6.4	Modifier	52
5.6.5	Supprimer	53
5.6.6	Recherche.....	54
5.6.7	Sécurisation	55
5.7	Résultat final de la version bêta.....	55
5.8	Evolutions.....	56



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 3/93

6	Chiffrage	57
6.1	Serveurs	57
6.2	Licences	59
6.3	NAS	59
6.4	Sauvegarde cloud.....	61
6.5	Onduleur.....	62
6.6	Chiffrage global	63
7	Recettage.....	65
7.1	Maquette réseau.....	65
7.1.1	Résultats.....	66
7.2	Serveurs Windows.....	67
7.2.1	DNS	67
7.2.2	Complexité des mots de passe	68
7.2.3	Impressions.....	68
7.2.4	Restriction des horaires de connexion	72
7.2.5	Administrateurs locaux.....	74
7.2.6	Désactivation du lecteur CD et disquettes	75
7.2.7	Serveur de fichiers	75
7.2.8	Quotas espace disque	75
7.2.9	Dossier de base utilisateur local	77
7.2.1	Dossier de base utilisateur du domaine	77
7.2.2	Planification d'audits	77
7.2.3	Configuration des journaux à 3 jours	79
7.2.4	Désactivation moniteur d'événement	80
7.2.5	Accès à distance.....	80
7.3	Script PowerShell de gestion des utilisateurs AD	81
7.3.1	Script de sauvegarde	84
7.4	Serveurs Linux.....	85
7.4.1	Samba Server	86
7.4.2	Serveur NFS	86
7.4.3	Serveur FTP.....	86



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 4/93

7.4.4	Application Web	88
7.5	Tolérance de panne.....	89
8	Table des illustrations et tableaux.....	90



1 Cadre du projet

1.1 Contexte

Notre entreprise « Central » a récemment déménagé dans des nouveaux locaux. Nous avons acquis des nouveaux ordinateurs et mis en place une nouvelle infrastructure réseau. Nous avons dorénavant besoin d'améliorer nos pratiques en matière de gestion du système d'information.

1.2 Problématiques

- Nous ne disposons pas encore de serveurs
- La gestion du parc et des droits utilisateurs n'est pas centralisée
- Les opérations de dépannage sont fastidieuses (déplacements trop fréquents, manque de suivi...)

1.3 Objectifs

- Implémenter Active Directory pour gérer les droits des utilisateurs
- Centraliser les fichiers de travail sur serveur
- Créer un outil accessible sur un navigateur pour gérer le parc matériel
- Implémenter une solution de tolérance de panne pour éviter les pertes de productivité

1.4 Contraintes

- Budget soumis au DAF
- Maquette fonctionnelle et dossier projet à fournir avant le 21 septembre 2018



2 Méthodes de travail

2.1 Réunions

Des réunions régulières sont programmées entre les membres de l'équipe projet (Julien Villard et Omar Ait-Moulid). Les réunions se font soit par Skype soit en face à face. A l'issue de ces réunions, un compte rendu est systématiquement rédigé.

2.2 Partage des ressources

Les documents sont rédigés sur un site Sharepoint dédié permettant un travail collaboratif.

2.3 Tableau de suivi

L'avancement des tâches est suivi grâce à un fichier excel (annexe).

2.4 Procédures

Une procédure de configuration de la maquette a été créée. A chaque étape du projet (installation, configuration, modification...), la procédure est mise à jour par celui qui est responsable de cette tâche. Chaque modification de la procédure est vérifiée et validée par le collaborateur qui n'est pas à l'origine de la modification.

2.5 Transfert de connaissances

Chaque membre de l'équipe dispose du matériel nécessaire pour faire fonctionner l'ensemble de la maquette. Nous disposons ainsi de deux environnements complets. En cas de perte totale de données, il sera toujours possible de récupérer l'environnement complet et à jour chez l'autre collaborateur.

Chaque validation d'une nouvelle version de la procédure implique donc un transfert complet de connaissances, puisqu'elle sera non seulement lue, mais également exécutée, testée et sauvegardée.

Ainsi, chaque membre de l'équipe sera capable de réaliser l'ensemble des opérations permettant d'installer l'ensemble la maquette.



2.6 Sauvegardes et plan de secours

Chaque membre de l'équipe est responsable de la sauvegarde de son environnement. Une sauvegarde des documents de travail, un point de restauration et un export des machines virtuelles sur un disque externe est à faire après chaque validation d'une mise à jour de la procédure. En cas de perte totale de données, il sera toujours possible de récupérer l'environnement complet et à jour chez l'autre collaborateur.



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 8/93

3 Mind Map préliminaire

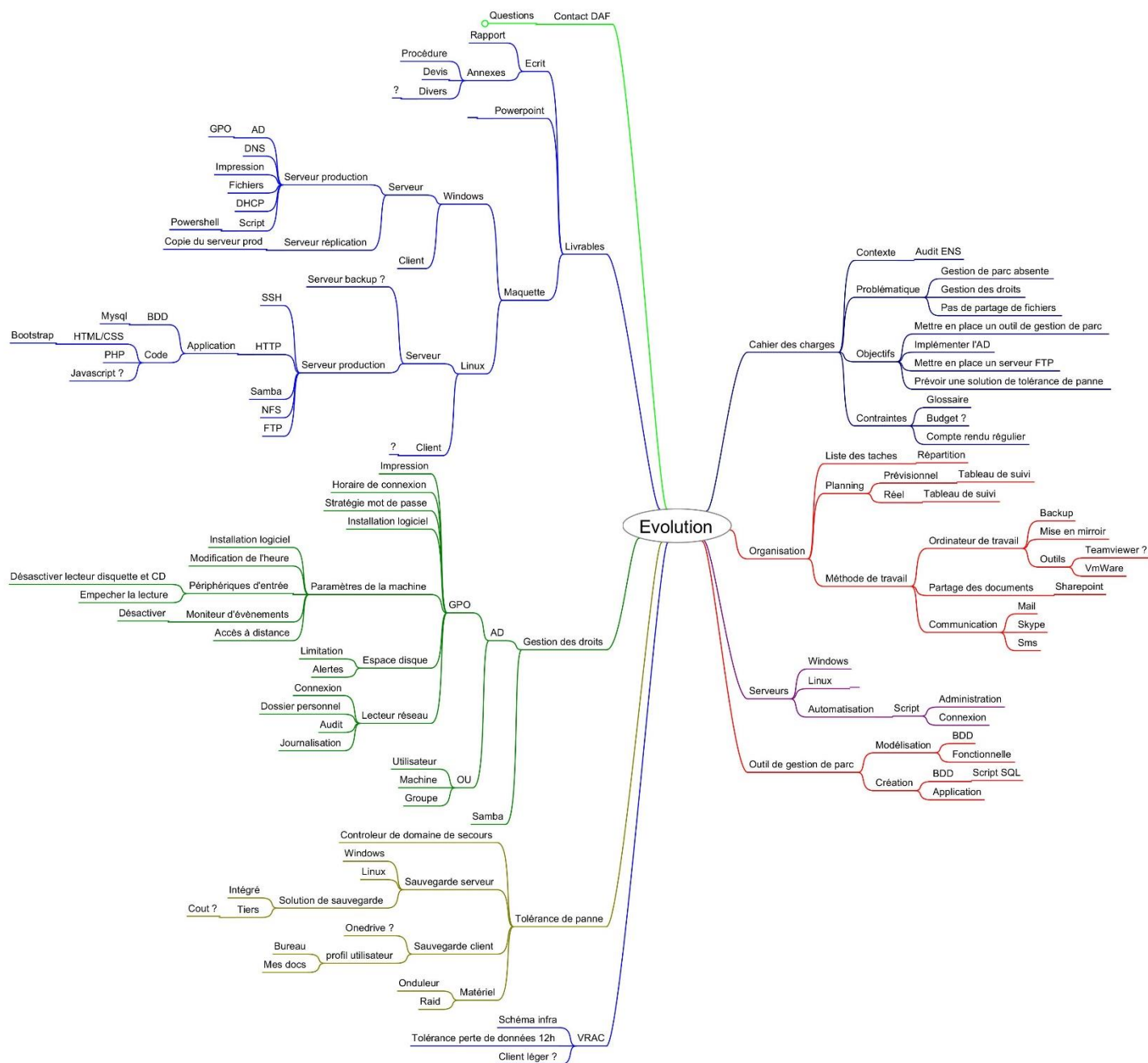


Figure 1 - Mind Map

4 L'infrastructure informatique

Le système d'information tient une place prépondérante dans notre organisation. Il a pour objectif de structurer l'ensemble des ressources de notre entreprise dans le but de collecter des données, puis de les traiter, stocker et de les communiquer.

Dans les ressources nous prenons en compte le personnel, le matériel, les logiciels et les procédures accompagnant la production informatique.

Ici nous nous attarderons davantage sur l'aspect matériel du système d'information et notamment sur l'infrastructure matérielle que nous souhaitons mettre en œuvre.

4.1 Les différents types d'infrastructure

4.1.1 L'infrastructure classique

Le premier type d'infrastructure est celle dite classique. Dans cette dernière, chaque ordinateur est relié au réseau, mais aucune gestion centralisée n'est opérée et les données sont stockées individuellement sur chaque machine.

D'un point de vue de la sécurisation des données, cela représente aujourd'hui une infrastructure complètement dépassée. De même avec l'accroissement des parcs informatiques, il est impensable de mettre en place ce type d'infrastructure au-delà d'une dizaine de poste informatique pour des soucis d'administration et d'exploitation. De plus, cela impose un support dédié pour chaque site distant.

4.1.2 L'infrastructure centralisée

Le deuxième type d'infrastructure correspond à celle dite centralisée. Elle a pour objectif de centraliser la gestion des ressources informatiques, tout en consolidant les systèmes et en permettant l'accroissement du taux d'utilisation des ressources. Le principal bénéfice est de réduire les coûts d'exploitation.

En règle générale, ces infrastructures peuvent être qualifiées de convergées¹ lorsqu'elles correspondent à une solution préconfigurée et pré-validée en usine, intégrant serveurs, équipements réseaux et stockage. Par opposition, le choix peut se porter sur une approche « Best of Breed » apportant les meilleurs composants mais ne garantissant pas un fonctionnement optimal.

¹ <https://www.lemagit.fr/definition/Infrastructure-convergee>



Ainsi, la convergence permet de mettre en œuvre une infrastructure très rapidement tout en apportant une courbe d'apprentissage plus aisée pour les équipes informatiques. Cela se traduit par une exploitation facilitée liée à une administration centralisée.

La convergence permet de se rapprocher du stockage IP permettant une transition facilitée vers les infrastructures intégrées dans le cloud.

D'un point de vue matériel, l'infrastructure convergée correspond à une ou plusieurs baies informatiques intégrant les serveurs, le stockage et le matériel réseau. Les postes clients viennent ainsi se connecter sur ces serveurs pour accéder aux données et aux applications de l'entreprise.

4.1.3 L'infrastructure hyperconvergée

Selon LeMagIT, les infrastructures convergées n'ont que le nom de convergées et correspondent plus à des systèmes traditionnels et devraient être appelés « pré-intégrés »². La réelle convergence se situe dans l'hyperconvergence.

Dans une architecture hyperconvergée, chaque serveur est un élément de calcul virtualisé et de stockage. Ainsi, le nombre de nœuds présent dans le cluster détermine la puissance du système mis en place. La force de l'hyperconvergence repose ainsi plus sur la couche logicielle que le matériel.

Le principal problème de cette infrastructure est sa jeunesse et la compatibilité avec les infrastructures déjà existantes. Cependant, l'hyperconvergence propose une flexibilité dans le déploiement de nouvelles technologies et ressources sans avoir à renouveler l'environnement de production, des outils d'administration centralisés et l'accès à des systèmes de sauvegardes avancés permettant une reprise d'activité très rapide après un incident.

4.1.4 Virtualisation

4.1.4.1 Principes

« La virtualisation consiste en la création d'une version virtuelle (par opposition à réelle) d'un ou de plusieurs éléments, tel qu'un système d'exploitation, un serveur, un dispositif de stockage ou des ressources réseau. »³

² <https://www.lemagit.fr/conseil/Converge-integre-hyperconverge-quelles-differences>

³ <https://www.lemagit.fr/definition/Virtualisation>



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 11/93

La virtualisation dans l'informatique n'est pas une technologie récente, elle existe en effet depuis les années 60. Les mainframes⁴ ont été ainsi capable très tôt de virtualiser leurs systèmes d'exploitation.

Même si la virtualisation concerne les systèmes d'exploitation, les serveurs, le stockage et les équipements réseaux, nous allons nous concentrer ici sur les serveurs notamment au travers de la virtualisation via les hyperviseurs⁵ de type 1.

Extrait d'un cours de virtualisation d'Alexandre Hernert au CESI :

« Au sein d'une entreprise, la multiplication des serveurs est un phénomène récurrent. Les opérations de maintenance, les besoins de ressources électriques et de refroidissement sont des problèmes liés à leur accroissement. Les performances techniques ne cessent d'évoluer. De manière générale, les spécialistes s'accordent à dire que les entreprises s'orientent vers une sous-utilisation générale des serveurs. Une étude a estimé que l'utilisation moyenne d'un serveur était de 15%. « La charge moyenne d'un processeur est généralement comprise entre 9 et 12 %. », constate Harold LICARI de Netfective Technology. Pour pallier à ce problème, la virtualisation bouleverse depuis plusieurs années le paysage informatique. Elle est aujourd'hui incontournable pour les moyennes et grandes entreprises et tend à se démocratiser dans les plus petites.

La virtualisation peut être comparée au covoiturage. Le serveur joue le rôle de la voiture et le système d'exploitation celui du passager. Un monospace avec quatre passagers est plus adapté que quatre citadines avec un conducteur. Même si sa consommation est plus élevée qu'une voiture, le monospace sera plus économique que quatre automobiles et les routes seront moins encombrées. Sur ce même principe, la virtualisation fait fonctionner simultanément plusieurs systèmes d'exploitation sur un seul serveur physique en faisant croire au système d'exploitation qu'il possède son propre matériel. Ainsi, le serveur physique n'est plus exploité à 15% mais plutôt entre 60% et 80%. Le schéma ci-dessous explique simplement ce principe »

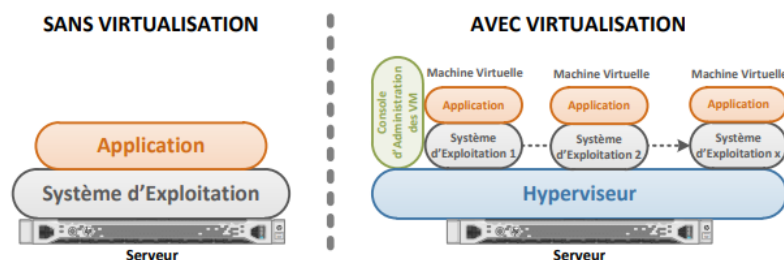


Figure 2 – Schéma Virtualisation

⁴ Ordinateur de grande puissance de traitement et qui sert d'unité centrale à un réseau de terminaux.

⁵ Un hyperviseur est une plate-forme de virtualisation permettant à plusieurs systèmes d'exploitation de travailler simultanément sur une même machine physique.



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 12/93

Les infrastructures centralisées, convergées et surtout hyperconvergées sont exploitées à leur plein potentiel grâce à la virtualisation. Cette dernière leur permet :

- D'utiliser de manière optimale les ressources des serveurs
- De faciliter le déploiement et la migration de machines virtuelles d'un support physique à un autre
- De mettre en place un système de redondance efficace garantissant un retour en production rapide
- De pouvoir sauvegarder un système à un moment donné et pouvoir le restaurer très rapidement en cas de problème via le système d'images instantanées

Certains points négatifs liés à la virtualisation pouvant empêcher le déploiement tendent à disparaître. La puissance des machines physiques actuelles permet d'avoir une infrastructure totalement virtualisée sans perte de performances par rapport à des machines physiques dédiées. Les difficultés de mise en place et d'administration liées à la jeunesse des solutions proposées sont aujourd'hui effacées par des solutions logicielles puissantes et proposant des outils d'administration centralisés.

Nous avons sélectionné deux solutions de virtualisation qui sont :

- Hyper-V développé par Microsoft et fourni sous licence commerciale, une version Microsoft Hyper-V Server est fournie gratuitement
- vSphere développé par VMware et fourni sous licence propriétaire, une version gratuite vSphere Hypervisor est également disponible

4.1.4.2 Clustering

Un Cluster est un « groupe » de serveurs fonctionnant comme un seul système. Chaque serveur est un « nœud » du cluster.

L'un des intérêts majeurs de la virtualisation est d'offrir la capacité de déplacer des machines virtuelles d'un hyperviseur à un autre sans interruption de service. Lorsque ces déplacements sont automatisés en fonction de la disponibilité des nœuds d'un cluster, on parle de « Haute Disponibilité ». Une machine virtuelle peut être paramétrée pour être déplacée automatiquement en cas de panne ou de maintenance du serveur qui l'héberge à cet instant.

Pour fonctionner, un Cluster a besoin que chaque nœud ait accès aux mêmes ressources partagées. Pour faire simple, voici un schéma qui résume ce principe :

Cluster avec 2 nœuds
Chaque nœud a accès au stockage et dispose
d'assez de puissance pour héberger les
machines virtuelles de l'autre nœud

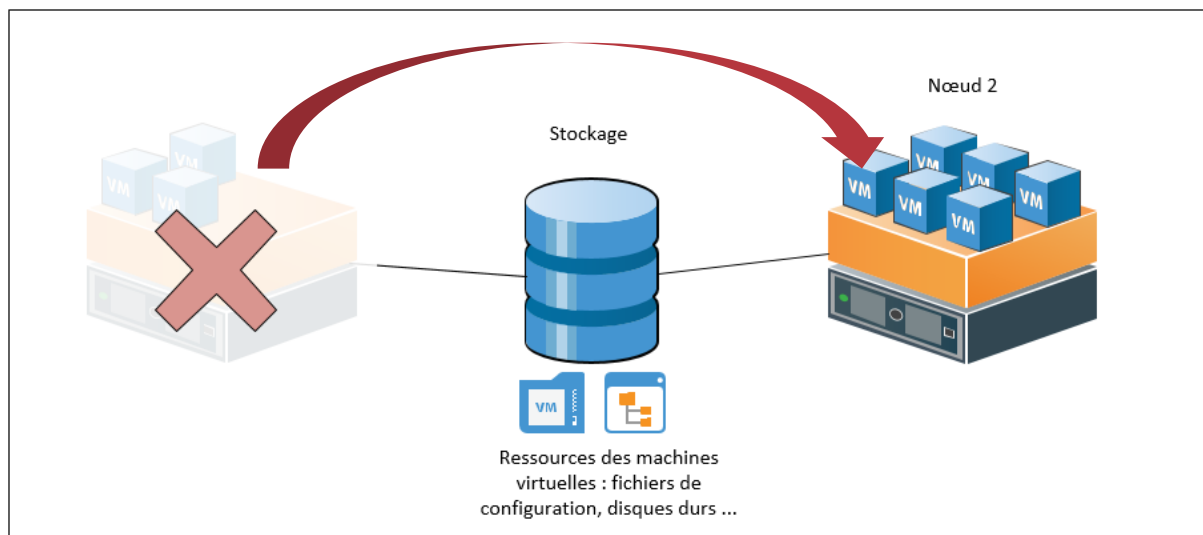
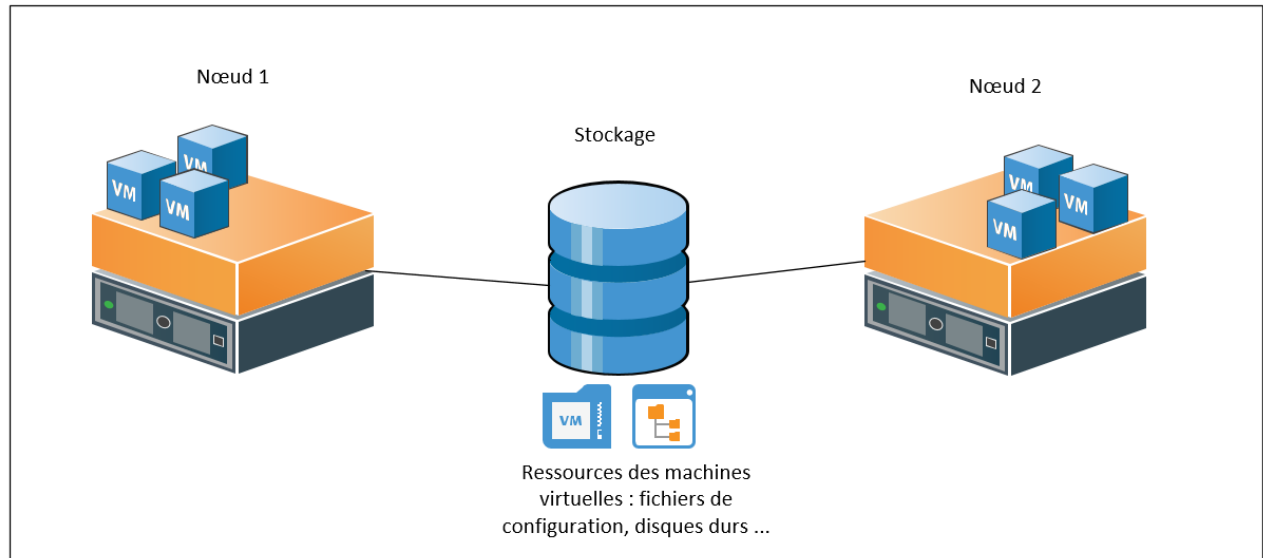


Figure 3 – Schéma Clustering

Dans la réalité, il est assez rare que chaque nœud ait la capacité d'héberger l'ensemble des VM. Chaque VM a une criticité qui lui est propre, selon ce critère nous pouvons définir quelles machines basculeront en priorité, et quelles machines peuvent être mises en attente le temps d'un dépannage ou d'une maintenance.



4.1.4.3 Hyper-V ou VmWare ?

Les deux hyperviseurs les plus connus sont Hyper-V et VmWare, ce dernier étant le plus répandu. Ce qui les différencie est tout d'abord leur noyau, Hyper-V est un système Microsoft et VmWare possède un noyau basé sur Linux Red Hat. Ces deux systèmes ont une version gratuite : Hyper-V Server et VmWare vSphere Hypervisor.

Au départ, nous avons opté pour la solution vSphere Hypervisor. Mais après recherches et réflexion, Hyper-V nous paraît à présent plus pertinent. Voici un tableau récapitulatif des caractéristiques essentielles qui nous ont poussé à finalement opter pour HyperV Server :

	Hyper-V Server	vSphere Hypervisor
Tarif	Gratuit	Gratuit
Facilité d'installation	5	5
Facilité de configuration	4	4
Facilité de création des VM	5	5
Facilité d'administration	5	3
Administration via Active Directory	OUI	PARTIELLE
Sauvegardes des VM à chaud	OUI	NON
Haute disponibilité (Clustering)	OUI	NON

Tableau 1 - Comparaison HyperV / VmWare

4.1.5 Solution choisie

Afin de répondre aux besoins de l'entreprise, nous avons choisi de préconiser l'utilisation d'une infrastructure centralisée mettant à profit la virtualisation.



Cela va nous permettre d'administrer les 90 postes utilisateurs, ainsi que les serveurs, d'une manière efficiente.

La virtualisation est une composante clé de l'infrastructure car cela va nous permettre d'utiliser au maximum les capacités techniques des serveurs. Ainsi, un serveur physique ne correspond plus à un seul rôle mais il peut héberger plusieurs machines virtuelles remplissant différentes fonctions tout en conservant un cloisonnement entre chaque rôle. Si une machine virtuelle tombe en panne, cela n'impactera pas les autres et la disponibilité du système d'informations reste garantie.

Nous n'avons pas opté pour une infrastructure convergée, ou hyperconvergée, car cela présente un coût non négligeable alors que nos besoins actuels ne nécessitent pas cela.

La virtualisation nous permettra également d'être ouvert sur l'avenir et de pouvoir adapter l'infrastructure en fonction des besoins. Par exemple, nous pourrions migrer plus facilement notre infrastructure vers le Cloud ou nous diriger vers une solution de convergence.

Afin de résumer, l'infrastructure que nous préconisons nous permettra :

- D'être efficient en termes de coûts matériels et humains
- D'être tourné vers l'avenir en ayant une infrastructure évolutive et adaptable
- De garantir la sécurité des données et du fonctionnement du système d'information

4.2 Stockage

4.2.1 Données en production

4.2.1.1 NAS ou serveur de fichiers ?

Un serveur de fichiers est un serveur classique, qui est configuré pour du stockage de données. Il a besoin d'un système d'exploitation pour fonctionner et être configuré, comme Windows ou Linux. Un NAS⁶ (Network Attached Storage) est un appareil permettant de stocker des données et de les rendre accessibles sur le réseau, le système est généralement propriétaire et est dédié à cette fonction, les performances s'en retrouvent augmentées par rapport à un serveur classique. Ci-dessous un tableau récapitulatif des caractéristiques de ces deux solutions, évalués par une note sur 5 :

⁶ Un serveur de stockage en réseau, également appelé stockage en réseau NAS, boîtier de stockage en réseau ou plus simplement NAS (de l'anglais Network Attached Storage), est un serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes. (Source : Wikipédia)



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 16/93

	NAS	Serveur de fichiers
Tarif	5	2
Facilité d'installation	5	5
Facilité de configuration	5	4
Facilité d'administration	5	3
Facilité de maintenance	5	4
Performances lecture / écriture	5	4
TOTAL	30	22

Tableau 2 - Comparaison NAS / Serveur de fichiers

Le choix du NAS dédié au stockage de données représente donc un choix plus pertinent qu'un serveur classique.

4.2.1.2Cible iSCSI

Pour pouvoir créer un cluster conformément à notre préconisation au chapitre 4.1.4.2, un stockage accessible par les deux serveurs doit être créé. La protocole iSCSI⁷ (Internet Small Computer Interface) permet de monter un partage distant sur un serveur comme s'il s'agissait d'un disque local. En montant le même partage sur tous les nœuds du cluster, chaque serveur pourra ainsi accéder aux mêmes ressources

⁷ iSCSI est une abréviation de Internet Small Computer System Interface. C'est un protocole de stockage en réseau basé sur le protocole IP destiné à relier les installations de stockage de données. En transportant les commandes SCSI sur les réseaux IP, iSCSI est utilisé pour faciliter les transferts de données sur les intranets et gérer le stockage sur de longues distances. iSCSI peut être 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. Le protocole permet aux clients (appelés initiateurs) d'envoyer des commandes SCSI (CDB) à des périphériques de stockage SCSI (targets) sur des serveurs distants. Il s'agit d'un protocole de SAN (Storage Area Network), qui permet de rassembler les ressources de stockage dans un centre de données tout en donnant l'illusion que le stockage est local. Contrairement au fibre channel, qui nécessite une infrastructure matérielle dédiée, iSCSI peut s'utiliser en conservant une infrastructure existante.



simultanément. Le NAS choisi devra donc respecter cette exigence et permettre la création de cibles ISCSI.

4.2.1.3 Haute disponibilité

Afin de minimiser les pertes de productivité liées à la panne du matériel servant au stockage, nous préconisons la mise en place d'une mise en miroir des données sur deux NAS.

Il y a deux manières de gérer la réplication :

- A travers un outil tiers comme DFS⁸ sur Windows Server
- Géré par le système intégré au matériel

Nous préconisons une réplication gérée par le matériel, pour la facilité de configuration et de maintenance que cela représente. En effet pour utiliser DFS il faudra installer un serveur supplémentaire, ce qui nécessitera de le configurer et de le maintenir convenablement. Viendra s'ajouter aussi le coût éventuel d'une licence Windows Server.

Les NAS de la gamme pro des marques Synology et Qnap (les leaders en la matière) permettent la mise en place d'une mise en miroir simple et fiable, sans avoir besoin de passer par un outil tiers.

4.2.1.3.1 RAID

« Le **RAID (Redundant Array of Independent Disks)** est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes. » (source : Wikipedia)

Pour éviter la perte de données suite à la panne d'un disque, il est nécessaire d'utiliser du matériel supportant le système RAID. Sans entrer dans les détails techniques, c'est le système RAID qui permet de garantir la disponibilité des données en cas de défaillance d'un ou plusieurs disques. Dans un RAID1, RAID5 et RAID6, lorsqu'un disque est défectueux, les données restent accessibles mais les performances sont amoindries. Il suffit alors de changer le disque par un nouveau (généralement cela se

⁸ La technologie Distributed File System (DFS), en français «Système de fichiers distribué » est un ensemble de services client et serveur permettant :

- de fournir une arborescence logique aux données partagées depuis des emplacements différents,
- de rassembler différents partages de fichiers à un endroit unique de façon transparente,
- d'assurer la redondance et la disponibilité des données grâce à la réplication.

fait à chaud, sans arrêt de la production) pour retrouver des performances normales après un temps de « reconstruction » des données.

4.2.1.4 Organisation des répertoires de travail

Une bonne organisation des répertoires de travail est essentielle afin de garantir des accès cohérents. L'arborescence suivante est une arborescence classique, qui permet de gérer les autorisations d'accès en fonction de l'appartenance à un service donné, et qui offre aux utilisateurs un espace personnel dédié et limité par des quotas où seuls eux auront accès (et éventuellement les administrateurs en fonction des besoins) :

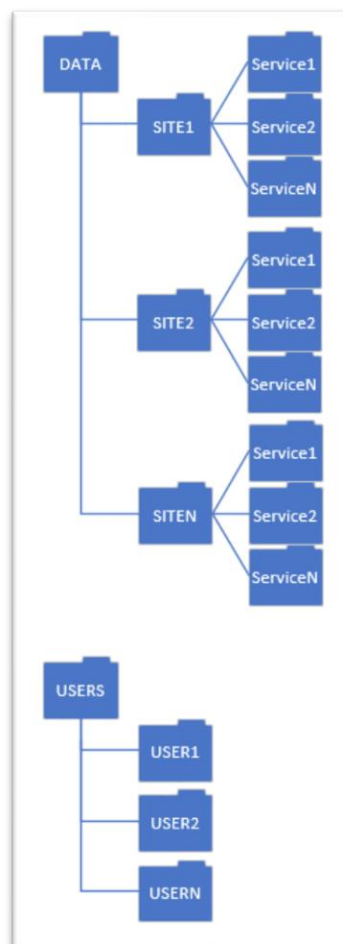


Figure 4 - Exemple d'arborescence des répertoires de travail

4.2.2 Sauvegardes

Les données de l'entreprise représentent un enjeu critique. Préserver leur intégrité contre les attaques malveillantes ou les erreurs de manipulation doit être une priorité

absolue. La perte de donnée représente une menace très sérieuse pour la pérennité d'une entreprise, comme le montre cette infographie réalisée par le leader mondial de la récupération de données, Kroll OnTrack :

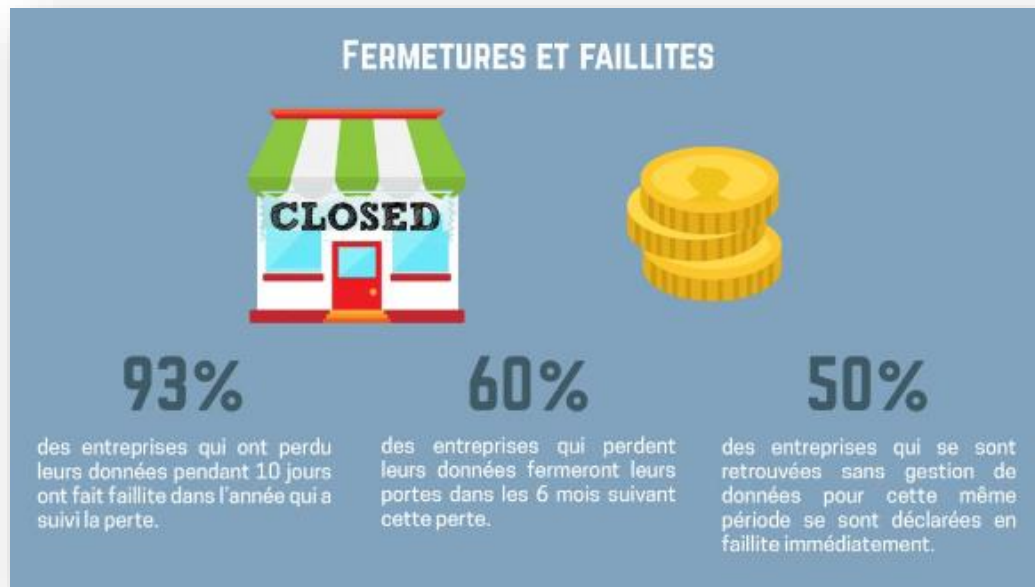


Figure 5 - Infographie : conséquences d'une perte de données

Source : <https://www.informanews.net/perte-de-donnees-cause-faillite/>

4.2.2.1 Principes

Il existe 3 types de sauvegarde de données : complète, incrémentielle et différentielle.

Une sauvegarde complète est une sauvegarde de la totalité des données, elle est indépendante des autres sauvegardes.

Une sauvegarde incrémentielle est une sauvegarde des données créées ou modifiées depuis la dernière sauvegarde, quelle que soit son type.

Une sauvegarde différentielle est une sauvegarde des données créées ou modifiées depuis la dernière sauvegarde complète uniquement.

Nous les comparons dans le tableau suivant :



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 20/93

	Compleète	Incrémentielle	Différentielle
Espace de stockage	Elevé	Faible	Moyen
Vitesse de sauvegarde	Faible	Elevé	Moyen
Vitesse de restauration	Elevé	Faible / Moyen	Moyen

Tableau 3 - Comparaison types de sauvegardes

Une nuance pour la sauvegarde incrémentielle : la rapidité de restauration dépend en grande partie de la quantité de données et du nombre de sauvegardes séparant la date de l'incrémentielle de la dernière complète. La plupart du temps, la restauration est exécutée pour des fichiers supprimés ou modifiés par erreur. Le temps de restauration sera quasiment le même quel que soit le type de sauvegarde lorsque la taille ne dépasse pas quelques dizaines de Mo. C'est lorsqu'on doit restaurer la totalité des données que l'opération devient lente.

4.2.2.2 Supports de sauvegarde

Les sauvegardes sont séparées en deux catégories : les sauvegarde à court terme et l'archivage. Pour chaque catégorie il convient d'utiliser un support adapté.

Quoi qu'il en soit, le support de sauvegarde ne doit jamais se trouver au même endroit que ce qu'il est censé sauvegarder. En cas d'incendie ou inondation, nous perdrons à la fois nos données en production et nos sauvegardes.

4.2.2.2.1 Sauvegardes court terme

A court terme, un support de sauvegarde doit :

- Permettre une grande rapidité d'accès pour les opérations de sauvegarde et de restauration
- Etre accessible depuis le réseau interne
- Offrir une grande capacité (données dupliquées plusieurs fois)
- Etre sécurisé
- Etre fiable (garantie de l'intégrité des données)



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 21/93

	NAS	Disque dur USB	Cloud	Cartouche RDX ⁹
Rapidité d'accès	5	4	1	4
Disponibilité réseau	5	1	5	1
Capacité	5	5	5	3
Sécurité / Confidentialité	5	3	4	5
Fiabilité	5	1	5	5
Coût	4	5	3	4
TOTAL	29	19	23	22

Tableau 4 - Comparaison supports de sauvegarde

Le support le plus adapté dans ce cas est clairement le NAS. Une réplication des sauvegardes sur le cloud peut être envisagée afin de permettre un Plan de Continuité d'Activité (PCA)¹⁰ efficace en cas de sinistre. Ce plan fait partie d'une vision stratégique globale définie par la Politique de Sécurité dans laquelle les risques, les impacts, les pertes acceptables et les investissements nécessaires à la mise en place des différentes solutions techniques sont évalués. Les utilisateurs ayant un pc portable (particulièrement les directeurs et VIP) pourront continuer de travailler depuis l'extérieur avec une connexion internet, même en cas de destruction totale des locaux de l'entreprise.

4.2.2.2 Archivage

Les supports de stockage pour de l'archivage répondent à des critères différents. Ce type de stockage doit :

- Être durable (archivage long terme)
- Être sécurisé (accès physique restreint)
- Être fiable (garantie de l'intégrité des données)

⁹ Disque dur militarisé, avec protection contre les chocs, la poussière, l'humidité, à longue durée de vie.

¹⁰ En informatique, un plan de continuité d'activité a pour but de garantir la survie de l'entreprise après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise. (Wikipedia)



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 22/93

- Rester accessible en cas de catastrophe naturelle, destruction des locaux...

	NAS (en interne)	Disque dur USB (en coffre)	Cloud	Cartouche RDX (en coffre)
Durabilité	4	1	5	5
Sécurité	5	3	4	5
Fiabilité	5	2	5	5
Accessibilité en cas de destruction des locaux	NON	OUI	OUI	OUI
Coût	3	5	3	4
TOTAL	17	11	17	19

Tableau 5 - Comparaison supports de sauvegarde

Le stockage en coffre de cartouches RDX en dehors des locaux semble la solution la plus pertinente pour de l'archivage. Il est cependant possible de la coupler avec une solution Cloud afin de bénéficier des avantages de ces deux solutions.

En effet le stockage en coffre est utile en cas de coupure totale d'internet, et le stockage sur le cloud permet d'éviter de déplacer physiquement les supports pour récupérer une archive (gain de temps et de sécurité). En cas de destruction des locaux, l'archivage sur le cloud permet également la mise en place d'un PRA¹¹ avec un meilleur RTO¹² et RPO¹³ qu'avec un stockage en coffre.

¹¹ En informatique, un plan de reprise d'activité permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation. Le plan de reprise d'activité doit permettre, en cas de sinistre, de basculer sur un système de relève capable de prendre en charge les besoins informatiques nécessaires à la survie de l'entreprise. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entreprise. Le plan de reprise d'activité (PRA) est à distinguer du plan de continuité d'activité (PCA) : ce dernier a pour objectif de poursuivre l'activité sans interruption du service et d'assurer la disponibilité des informations quels que soient les problèmes rencontrés. Le PRA en est un sous-ensemble, qui décrit les mesures qui doivent être déclenchées à la survenue d'un sinistre ou incident majeur ayant entraîné une interruption de l'activité. (Wikipedia)

¹² C'est le délai de rétablissement d'un processus, à la suite d'un incident majeur, pour éviter des conséquences importantes associées à une rupture de la continuité d'activité. Il définit le temps alloué pour faire le basculement vers le nouveau système. (Source : Wikipédia)

¹³ Le RPO commence à s'exprimer à l'instant où l'incident majeur arrive et peut être exprimé en secondes, minutes, heures ou jours. Il s'agit donc de la quantité maximale acceptable de perte de données. C'est la durée des fichiers ou des données dans le stockage de secours exigé par



4.2.2.3 Scénario de sauvegarde

Les NAS de type Synology ou Qnap intègrent un système de sauvegarde performant que nous préconisons d'utiliser afin de rentabiliser ce matériel et éviter d'avoir à gérer manuellement cette tâche.

Pour avoir un système de sauvegarde qui allie faible consommation d'espace disque, rapidité de sauvegarde et de restauration, nous proposons ce scénario de sauvegarde:

- Une sauvegarde complète le dernier dimanche du mois à 19h
- Une sauvegarde incrémentielle les autres jours à 12h et à 19h
- Une synchronisation des sauvegardes sur le Cloud en dehors des heures de production (la nuit par exemple)
- Une durée de rétention de 3 mois
- Une sauvegarde complète en archive tous les 3 mois, durée de rétention illimitée
- Archivage des images système des serveurs une fois par an et à chaque changement majeur, durée de rétention 5 ans

La durée de rétention est la durée au bout de laquelle la sauvegarde sera supprimée automatiquement par roulement avec la suivante.

Attention toutefois aux données à caractère personnel. Ces fichiers ayant une durée limitée de conservation conformément à la loi en vigueur, ils feront l'objet d'une durée de rétention spécifique

Voici un schéma simplifié représentant le principe de fonctionnement du scénario :

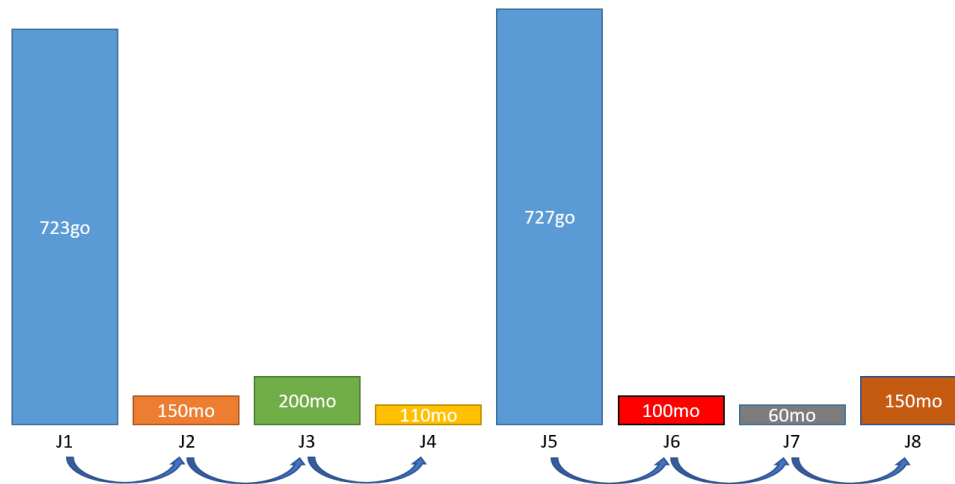


Figure 6 - Politique de sauvegarde

Sur cet exemple, on effectue dans un premier temps une sauvegarde complète le jour J1. Les jours J2, J3 et J4 on effectue une sauvegarde incrémentielle. Seuls les fichiers créés ou modifiés depuis la précédente sauvegarde seront pris en compte. A J5 le cycle recommence. Les sauvegardes de plus de 3 mois sont automatiquement supprimées.

4.3 Systèmes et applications

Dans le cadre du projet, nous devons mettre en place des serveurs Windows et Linux. Le choix de la version Windows et de la distribution Linux sera fait selon des critères veillant au respect du cahier des charges. Pour rappel, nous avons préconisé dans le précédent 4.1 un environnement virtualisé, avec HyperV Server comme système hôte.

4.3.1 Rôles et fonctionnalités attendues

Avant d'étudier les solutions qui s'offrent à nous, rappelons le périmètre, les rôles et les fonctionnalités attendues dans le cahier des charges :

- 90 utilisateurs et au moins autant d'ordinateurs
- Plusieurs imprimantes réseau
- Serveurs Windows et Linux
- Active Directory (gestion des utilisateurs et droits d'accès)
- DNS (service de résolution de noms en adresse ip)
- DHCP (service de distribution automatique d'adresse ip)
- Serveur de fichiers



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 25/93

- Serveur d'impression
- Serveur Samba (synchronisation des droits depuis Active Directory sur Linux)
- Serveur NFS (service de partage de fichiers sur le réseau)
- Serveur FTP (transfert de fichiers)

A cela, nous préconisons d'ajouter :

- Serveur de supervision et monitoring

4.3.2 Windows Server

4.3.2.1 Editions

Windows Server 2016 est la dernière version des systèmes serveurs Microsoft. Il existe 3 éditions à l'heure actuelle : Datacenter, Standard et Essentials.

Essentials	Standard	Datacenter
Pour les petites entreprises jusqu'à 25 utilisateurs et 50 appareils	Pour les environnements avec des serveurs physiques ou virtualisés	Pour les environnements hautement virtualisés de type datacenter et architectures cloud

Tableau 6 - Comparaison éditions Windows Server

La version Essentials est éliminée d'office car notre entreprise compte au moins 90 utilisateurs et autant d'appareils.

La différence entre la version Standard et Datacenter réside dans certaines fonctionnalités avancées liées à la virtualisation et à la gestion du stockage (Shielded Virtual Machines, software-defined networking, Storage Spaces Direct, Storage Replica)¹⁴ Ces deux éditions bénéficient d'un modèle de licence commun, basé sur le nombre de cœurs physiques dont dispose le serveur sur lequel le système est installé.

¹⁴Voir la liste des fonctionnalités dans la documentation fournie par Microsoft :
http://download.microsoft.com/download/E/1/F/E1F21239-8A97-472A-A52C-CD83A89B5EAE/Windows_Server_2016_Secure_Evolve_Innovate_Solution_Brief_EN_US.pdf



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 26/93

	Standard	Datacenter
Processeur	2	2
Nombre de cœurs	16	16
Nombre de VM	2	Illimité
Prix	882\$	6155\$

Tableau 7 - Comparaison licences Windows Server

Chaque licence est valable pour 2 processeurs physiques et 16 cœurs. Si notre serveur a plus de 16 cœurs, il faudra acheter des « compléments de licence » permettant d'ajouter autant de cœurs que nécessaires.

La licence Standard permet d'installer 2 machines virtuelles. Au-delà, il faudra ajouter une licence. La version Datacenter permet un nombre illimité de machines, la limitation sera due aux capacités physiques du serveur, en sachant que plus le serveur dispose de cœurs, plus il faudra acheter de licences.

Dans le cas d'une VM mise en cluster, les licences ne couvrent qu'un seul hôte. Il faudra donc autant de licences que de nœuds de cluster.

Calculons, du point de vue du tarif, à partir de combien de VM il vaut mieux passer à une édition Datacenter :

$$6155 / (882 * 2) = 13,9$$

A partir de 14 VM Windows Server sur un hôte, il serait préférable de passer sur une version Datacenter du point de vue du tarif. Dans notre cas, la version Datacenter ne paraît pas pertinente, la version standard pourra couvrir l'ensemble de nos besoins.

4.3.2.2 Licences d'accès (CAL)

Il faudra par ailleurs ajouter des licences d'accès, appelées CAL. Il y a deux types de licences :

- Basée sur l'utilisateur : chaque utilisateur qui se voit attribuer une licence peut accéder aux ressources du serveur à partir de n'importe quel appareil

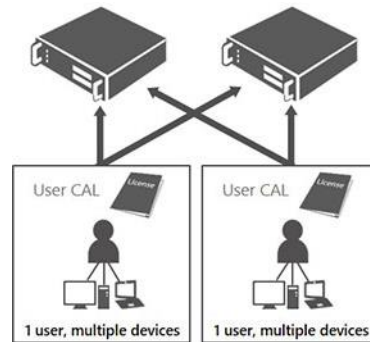


Figure 7 - Licences CAL utilisateur

- Basée sur l'appareil : chaque appareil qui se voit attribuer une licence permet à n'importe quel utilisateur connecté dessus d'accéder aux ressources du serveur

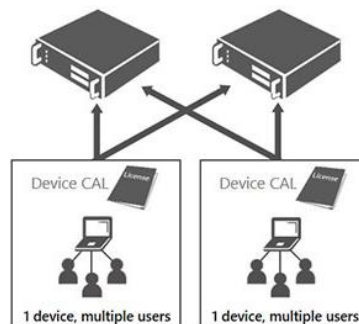


Figure 8 - Licences CAL périphériques

Dans notre cas chaque utilisateur a au moins un ordinateur, il y a donc plus d'appareils que d'utilisateurs en comptant les serveurs et autres périphériques. Il est donc plus pertinent de choisir des User CAL.

4.3.2.3 Active Directory

L'AD est le service d'annuaire LDAP¹⁵ développé par Microsoft. Il a été présenté en 1996 et mis en service sur Windows 2000 Server Edition en 1999.

L'objectif principal de l'AD est de centraliser les ressources de l'entreprise dans un service, notamment l'identification et l'authentification. Il répertorie les éléments du réseau de l'entreprise tel que les comptes utilisateurs, les serveurs, les postes de travail, les imprimantes, les partages réseau. Il permet également d'appliquer des

¹⁵ Lightweight Directory Access Protocol est un protocole permettant l'interrogation et la modification des services d'annuaire reposant sur TCP/IP. Source https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol



stratégies de groupe et de déployer des applications facilement pour les administrateurs.

Ainsi les administrateurs peuvent contrôler facilement l'accès aux ressources de l'entreprise grâce à un service centralisé, il n'est plus nécessaire de se déplacer sur chaque poste utilisateur un à un pour effectuer les paramétrages.

L'AD repose sur une base de données pour stocker les différentes informations. Il organise de manière hiérarchisé chaque objet qui le compose. Les objets peuvent être classés en différents types :

- Les ressources
- Les services
- Les utilisateurs

Les principaux objets sont les suivants :

- Les unités d'organisation, ou Organisational Unit (OU), qui sont des conteneurs permettant de créer une hiérarchie et de faciliter la gestion de droits et l'application des stratégies de groupes
- Les ordinateurs qui représentent les machines du parc informatique
- Les utilisateurs qui représentent les comptes
- Les groupes qui servent à attribuer des droits ou des services. Il y a trois types de groupes :
 - Les groupes globaux qui peuvent être utilisé dans le domaine¹⁶ local mais aussi dans les domaines approuvés
 - Les groupes locaux qui peuvent être utilisé uniquement dans le domaine où ils ont été créés
 - Les groupes universels qui ont une portée sur l'ensemble de la forêt¹⁷

Chaque objet est défini de manière unique et peut contenir différents attributs.

Lors de l'installation des services d'annuaires sur un serveur celui-ci est appelé contrôleur de domaine.

La perte des données de l'annuaire ou l'inaccessibilité du contrôleur de domaine d'une entreprise présente un risque majeur, ainsi il est possible d'activer une réplication entre différents contrôleurs de domaine permettant de palier à ses problèmes. Cette fonctionnalité est prise en charge de manière native.

Il faut toutefois faire attention au niveau fonctionnel du domaine, celui-ci détermine les fonctionnalités des services disponibles dans le domaine ou la forêt. Il est défini par la

¹⁶ Le domaine défini l'ensemble des machines partageant les informations de l'annuaire.

¹⁷ La forêt est un ensemble d'un ou plusieurs domaines



version de Windows Serveur utilisé. Il est possible de basculer vers un niveau supérieur mais impossible de rétrograder le niveau fonctionnel.

Le service d'annuaire pour notre entreprise se présente de la sorte :

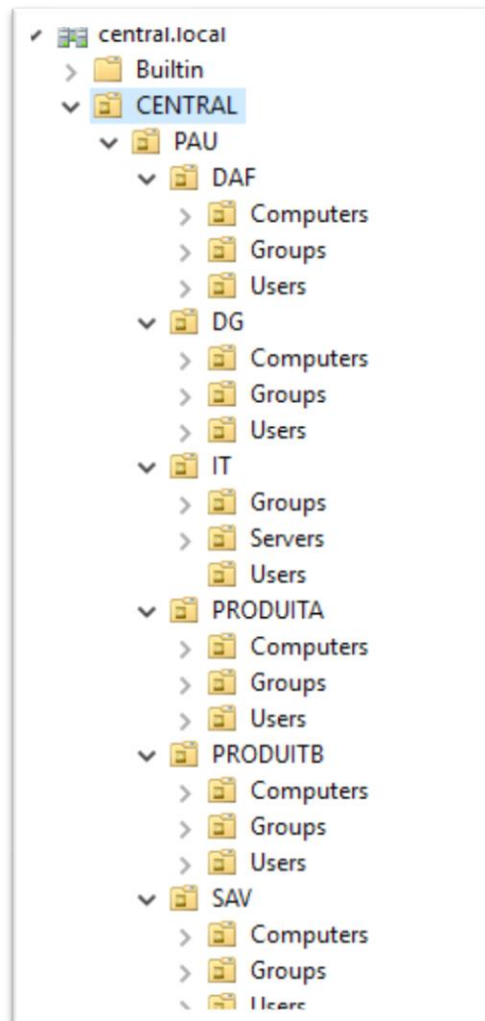


Figure 9- Organisation de l'AD

La hiérarchie proposée ici permet de pouvoir bien classer les différentes ressources de l'entreprise tout en permettant de pouvoir cibler l'application des stratégies à un service défini.

4.3.2.4 Stratégies de groupes ou Group Policy (GP)

Dans un environnement AD, les GP permettent une gestion centralisée des ordinateurs et des utilisateurs. Elles peuvent contrôler la politique de sécurité, des clés



de registre, les paramètres d'Internet Explorer et les scripts de connexion et de déconnexion entre autres.

Grace à des modèles d'administrations, les GP permettent notamment de modifier selon les besoins les fonctionnalités et la présentation d'un poste client sous Windows 10 de manière plus accessible.

Les stratégies de groupes sont mises en place en utilisant des objets de stratégie de groupe (GPO). Ainsi en appliquant un objet à un domaine ou une OU, il est possible de cibler les stratégies sur un groupe d'utilisateurs ou d'ordinateurs, ou à l'ensemble du domaine.

Afin d'obtenir un degré de ciblage plus élevé, il est également possible d'utiliser des filtres WMI. Ces derniers permettent de focaliser le champ d'applications des GPO en spécifiant des conditions d'applications tel que la quantité d'espace disque disponible, la quantité de mémoire vive par exemple.

4.3.2.5 DNS

Le DNS (Domain Name System) permet la résolution de noms de domaine en adresses ip. C'est l'équivalent d'un répertoire téléphonique, il est plus aisé de se souvenir et d'appeler un correspondant grâce à son nom que de retenir tous les numéros.

Dans tout environnement avec Active Directory, le DNS est un élément obligatoire de l'infrastructure. Dans un petit environnement comme le nôtre, la pratique courante est d'installer un serveur DNS sur chaque contrôleur de domaine.

4.3.2.6 DHCP

Le serveur DHCP (Dynamic Host Configuration Protocol) permet d'attribuer automatiquement une configuration réseau aux machines (adresse ip, masque de sous réseau, passerelle, dns ...).

Dans le cahier des charges, le serveur DHCP doit être installé sur un serveur Linux. Cela dit, nous préconisons une installation sous Windows au vu de la simplicité de la mise en place d'une redondance. Tout comme le DNS, un serveur DHCP sera installé sur chaque contrôleur de domaine, ainsi l'ensemble des services essentiels seront doublés et offriront une tolérance de panne accrue.

4.3.3 Distribution Linux

Il existe une grande quantité de distributions Linux. Nous comparons dans le tableau suivant les distributions plus connues.



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 31/93

	Debian	Ubuntu	Fedora
Facilité d'administration	4	4	3
Documentation et support	4	5	4
Stabilité	5	5	3
TOTAL	13	14	10

Tableau 8 - Comparaison distributions Linux

Chaque critère est évalué de 0 à 5

Nous préconisons d'utiliser Ubuntu Server, sa dernière version stable est la 18.04. Ubuntu est basé sur Debian, il offre donc les mêmes avantages en termes de stabilité, de facilité d'administration et de gestion, mais dispose d'une plus large communauté d'utilisateurs et donc d'un meilleur support technique et d'une documentation très complète.

4.4 Réseau

4.4.1 Vlans

Afin de sécuriser au maximum notre infrastructure, nous avons préconisé la mise en place de Vlans¹⁸ dans le projet Start lors du déménagement de nos locaux et de la mise en place de la nouvelle infrastructure réseau. Le matériel réseau (switchs, routeurs, firewall) en place étant déjà conforme, il ne reste qu'à le configurer afin de respecter cette exigence. Le schéma à la section 4.5 montre les différents Vlans à mettre en place afin de respecter les bonnes pratiques de séparation. Chaque lien représenté est également un lien physique, nous pouvons donc déterminer combien de ports réseaux seront nécessaires sur chaque serveur et autres équipements.

- **MGMT** : Management des serveurs et équipements réseaux
- **LAN** : Clients (ordinateurs, imprimantes, périphériques...)
- **STORAGE** : Réseau dédié au stockage (cibles ISCSI, sauvegardes)
- **SERVICE** : Services délivrés par les serveurs et accès à ceux-ci vers internet
- **EXT** : Equipements réseaux délivrant la connexion à internet

¹⁸ Un réseau local virtuel, communément appelé VLAN (pour Virtual LAN), est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur réseau.



- HEARTBEAT : Connexion entre les nœuds du Cluster permettant de voir quels sont ceux qui sont actifs ou pas (peuvent passer par un switch, mais il est fortement recommandé d'établir un lien direct)
- TRUNK : Lien d'interconnexion entre deux switches laissant passer plusieurs Vlans

4.4.2 Routage

4.4.2.1 Inter-Vlans

Afin de pouvoir faire communiquer différents Vlans, le cœur de réseau (Backbone) devra être capable faire du routage. C'est la raison pour laquelle nous avons prévu un commutateur de niveau 3 lors du projet START. Les Vlans devant communiquer entre eux sont : **EXT**, **LAN** et **SERVICE**, les autres doivent être isolés.

4.4.2.2 NAT

Le routeur devra être configuré en NAT¹⁹ pour permettre l'accès à internet. Il faudra également penser à paramétrer la passerelle par défaut du Backbone vers l'adresse ip interne du routeur situé dans le Vlan EXT afin de permettre un accès à internet.

4.4.3 Listes d'accès (ACL)

Le routage au niveau du Backbone ne permettant pas d'isoler un Vlan en particulier (par défaut tous les Vlans sont autorisés à prendre les nouvelles routes créées), nous devons mettre en place des ACL²⁰ pour interdire les connexions entre un Vlan isolé et les autres.

Sur les switchs Cisco, l'application d'une ACL sur une interface implique une interdiction par défaut de tout ce qui n'a pas été autorisé explicitement.

De manière générale, les règles à appliquer devront être conformes à ce tableau :

¹⁹ En réseau informatique, on dit qu'un routeur fait du network address translation (NAT) (« traduction d'adresse réseau » ou « translation d'adresse réseau ») lorsqu'il fait correspondre des adresses IP à d'autres adresses IP. En particulier, un cas courant est de permettre à des machines disposant d'adresses qui font partie d'un intranet et ne sont ni uniques ni routables à l'échelle d'Internet, de communiquer avec le reste d'Internet en semblant utiliser des adresses externes uniques et routables. Ainsi, il est possible de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, afin de pallier l'épuisement des adresses IPv4.

La fonction NAT dans un routeur de service intégré (ISR) traduit une adresse IP source interne en adresse IP globale. (Source : Wikipédia)

²⁰ Une ACL sur un pare-feu ou un routeur filtrant, est une liste d'adresses ou de ports autorisés ou interdits par le dispositif de filtrage. (source : Wikipédia)



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 33/93

Destination Source	EXT	STORAGE	HEARTBEAT	MGMT	SERVICE	LAN
EXT	OUI	NON	NON	NON	OUI	OUI
STORAGE	NON	OUI	NON	NON	NON	NON
HEARTBEAT	NON	NON	OUI	NON	NON	NON
MGMT	NON	NON	NON	OUI	NON	NON
SERVICE	OUI	NON	NON	NON	OUI	OUI
LAN	OUI	NON	NON	NON	OUI	OUI

Tableau 9 - ACL réseau

Il y a toutefois une exception pour le service interne de résolution de noms DNS (qui se trouvera sur le Vlan SERVICE) qui doit pouvoir être joint depuis le Vlan MGMT. Les ACL configurées devront en tenir compte.

4.4.4 Plan d'adressage général

Vlan	Plage IP	Adresse de début	Adresse de fin	Broadcast	Masque	Adresses disponibles
EXT	192.168.0.0/28	192.168.0.1	192.168.0.14	192.168.0.15	255.255.255.240	14
STORAGE	192.168.0.16/28	192.168.0.17	192.168.0.30	192.168.0.31	255.255.255.240	14
HEARTBEAT	192.168.0.32/28	192.168.0.33	192.168.0.46	192.168.0.47	255.255.255.240	14
MGMT	192.168.0.64/27	192.168.0.65	192.168.0.94	192.168.0.95	255.255.255.224	30
SERVICE	192.168.0.96/27	192.168.0.97	192.168.0.126	192.168.0.127	255.255.255.224	30
LAN	192.168.1.0/24	192.168.1.1	192.168.1.254	192.168.1.255	255.255.255.0	254

Tableau 10 - Plan d'adressage général

4.4.5 Plan d'adressage détaillé

EXT	Adresse IP	Masque	Passerelle	DNS1	DNS2
Backbone	192.168.0.1	255.255.255.240	192.168.0.1	1.1.1.1 (externe)	8.8.8.8 (externe)
Routeur ADSL	192.168.0.2				

Tableau 11 - Plan d'adressage VLAN EXT



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 34/93

STORAGE	Adresse IP	Masque	Passerelle	DNS1	DNS2
Backbone	192.168.0.17	255.255.255.240	192.168.0.17	192.168.0.103	192.168.0.104
NASData1	192.168.0.18				
NASData2	192.168.0.19				
NASBackup	192.168.0.20				
Hyperv-1	192.168.0.21				
Hyperv-2	192.168.0.22				
VM-WINFS-1	192.168.0.23				

Tableau 12 - Plan d'adressage VLAN STORAGE

HEARTBEAT	Adresse IP	Masque	Passerelle	DNS1	DNS2
Backbone	192.168.0.33	255.255.255.240	N/A	N/A	N/A
Hyperv-1	192.168.0.34				
Hyperv-2	192.168.0.35				
NASData1	192.168.0.36				
NASData2	192.168.0.37				

Tableau 13 - Plan d'adressage VLAN HEARTBEAT

MGMT	Adresse IP	Masque	Passerelle	DNS1	DNS2
Backbone	192.168.0.65	255.255.255.224	192.168.0.65	192.168.0.103	192.168.0.104
Switch1	192.168.0.66				
Switch2	192.168.0.67				
Switch3	192.168.0.68				
Switch4	192.168.0.69				
Switch5	192.168.0.70				
Switch6	192.168.0.71				
NASData1	192.168.0.72				
NASData2	192.168.0.73				
NASBackup	192.168.0.74				
Hyperv-1	192.168.0.75				
Hyperv-2	192.168.0.76				
VM-WINDC-1	192.168.0.77				
VM-WINDC-2	192.168.0.78				
CLUSTER-HYPERV	192.168.0.79				
VM-UBUSRV-1	192.168.0.80				
VM-WINFS-1	192.168.0.81				

Tableau 14 - Plan d'adressage VLAN MGMT



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 35/93

Service	Adresse IP	Masque	Passerelle	DNS1	DNS2
Backbone	192.168.0.97	255.255.255.224	192.168.0.97	192.168.0.103	192.168.0.104
NASData1	192.168.0.98				
NASData2	192.168.0.99				
NASBackup	192.168.0.100				
Hyperv-1	192.168.0.101				
Hyperv-2	192.168.0.102				
VM-WINDC-1	192.168.0.103				
VM-WINDC-2	192.168.0.104				
CLUSTER-HYPERV	192.168.0.105				
VM-UBUSRV-1	192.168.0.106				
VM-WINFS-1	192.168.0.107				

Tableau 15 - Plan d'adressage VLAN SERVICE

LAN	Adresse IP	Masque	Passerelle	DNS1	DNS2
Backbone	192.168.1.1	255.255.255.0	192.168.1.1	192.168.0.103	192.168.0.104
Autres	192.168.1.X				

Tableau 16 - Plan d'adressage VLAN LAN

4.5 Schéma

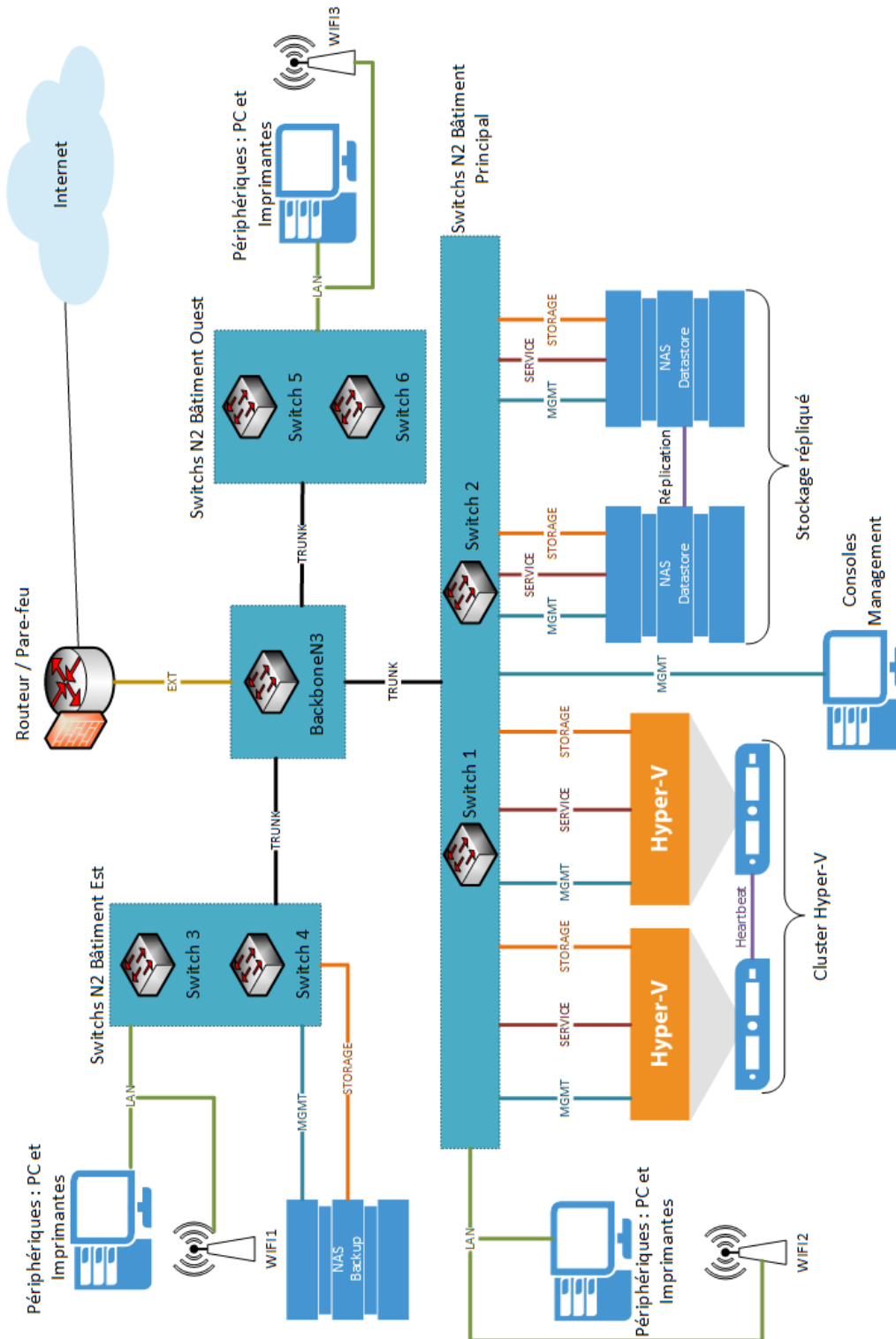


Figure 10 – Schéma infrastructure



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 37/93

4.6 Liste des serveurs

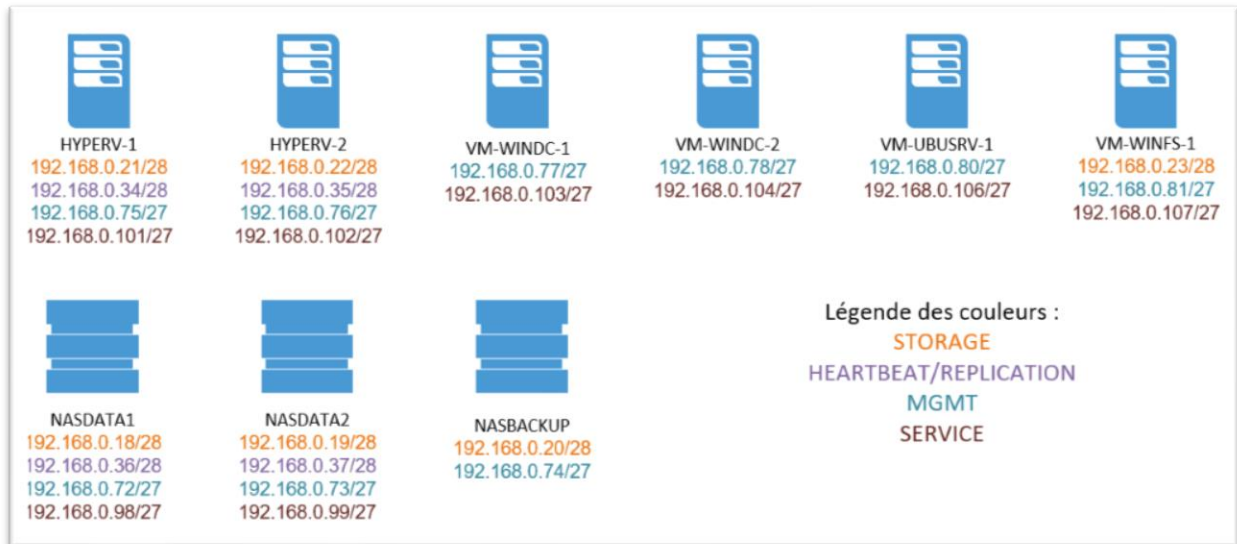


Figure 11 - Liste des serveurs



5 Application gestion de parc

5.1 Cahier des charges

Afin de gérer au mieux le parc informatique de notre entreprise, il nous a été demandé de réaliser une application permettant de pouvoir consulter celui-ci de manière simple et efficace.

Pour répondre à ce besoin nous avons choisi de développer une application web de gestion de parc informatique.

Dans le cadre du projet plusieurs fonctionnalités sont imposées :

- Avoir un mode gestion, réservé au service informatique, et un mode de consultation
- Avoir accès aux ordinateurs et à leurs caractéristiques
- Avoir accès aux périphériques associés comme les imprimantes et écrans
- Intégrer une fonctionnalité de recherche multicritère concernant les ordinateurs
- Pour la partie gestion :
 - o Pouvoir ajouter, modifier et supprimer les utilisateurs, les locaux, les écrans, les imprimantes et les ordinateurs

Le code source de l'application Web est disponible dans un dossier fourni en supplément de la version numérique de ce rapport. Certains extraits, jugés importants, seront fournis en annexe du document.

5.2 Langages

5.2.1 Base de données

5.2.1.1 Structured Query Language (SQL)



Le SQL est un langage informatique normalisé qui permet l'exploitation des bases de données relationnelles.

Il a été créé en 1974 et normalisé en 1987 avec la norme internationale SQL ISO/CEI 9075 :1986. La dernière révision de cette norme date de 2011.

La base de données relationnelles correspond à une base de données où les informations sont stockées dans des tableaux à deux dimensions appelés relations ou tables.



Nous avons choisi d'utiliser MySQL, un serveur de bases de données relationnelles SQL, qui a été créé en 1995 et dont la dernière version date de cette année. Il est développé par MySQL AB et Oracle.

MySQL est un logiciel libre et open source qui est intégré à LAMP²¹. Cela nous permet d'avoir un ensemble de logiciels libres permettant la création de serveurs de sites web.

Nous utilisons également phpMyAdmin pour gérer la base de données MySQL. C'est une application Web qui nous permet d'administrer de manière facile et intuitive la base de données dans un premier temps.

²¹ Acronyme faisant généralement référence à Linux, Apache, MySQL, PHP.

5.3 Interface web

Afin de générer une interface Web à la fois moderne et efficace nous avons choisi d'utiliser différents types de langages, mais aussi des librairies et framework²².

5.3.1 HyperText Markup Language (HTML)



Le HTML est le langage de balisage permettant de représenter les pages Web. C'est un standard international correspondant à la norme ISO/IEC 15445 :2000 et à la norme W3C HTML5 pour sa dernière version.

C'est un langage incontournable dans la création d'un site Web.

5.3.2 Cascading Style Sheets (CSS)



Le CSS est un langage informatique permettant de décrire la présentation des documents HTML. Les standards le définissant sont publiés par le World Wide Web Consortium (W3C).

Le principal objectif du CSS est de permettre une séparation entre la structure et la présentation d'une page Web. Ainsi cela permet de réduire la taille du code HTML tout en permettant l'uniformisation des différentes pages d'un site Web.

²² Aussi appelé infrastructure logicielle ou cadre d'applications.

5.3.3 PHP



PHP est un acronyme récuratif pour PHP Hypertext Preprocessor. C'est un langage de script généraliste et Open Source. Il est maintenu par The PHP Group. La version actuelle est la 7.2.9 en date du mois d'aout 2018.

Le langage est utilisé généralement du coté du serveur, il permet de générer du code et des données pouvant être interprétés et rendus par un navigateur.

5.3.4 Javascript (JS)



JS est un langage de programmation de script orienté objet. Nous utilisons ici le JS dans la partie cliente il est ainsi intégré aux pages Web et exécuté par le navigateur.

Il a été créé en 1995 et sa dernière version en date est de 2017. Il est développé par Netscape Communications et Mozilla Foundation.

JS a été standardisé sous le nom d'ECMAScript par Ecma International et il en est à sa 8^{ème} édition.

L'ajout de l'architecture informatique Ajax²³ permet de faciliter la construction de sites Web dynamiques interactifs. Le principal avantage est l'échange des données entre le client et le serveur en arrière-plan, évitant de devoir transmettre et afficher une nouvelle page à chaque échange. Le fonctionnement asynchrone permet au navigateur Web de continuer à exécuter le programme JavaScript sans avoir à attendre les réponses du serveur Web.

²³ Asynchronous JavaScript and XML

5.4 Framework et librairies

5.4.1 Bootstrap



Bootstrap est un framework dédié à la création du design d'un site Web, il contient du code HTML, CSS et en option du Javascript.

Il est développé par Twitter sous licence MIT²⁴, il a été mis en service en 2011 et la dernière version est la 4.1.1 en date de cette année.

Certaines des fonctionnalités permettent notamment de générer des formulaires, des barres de navigation et des boutons. L'un des principaux atouts de Bootstrap est sa facilité d'utilisation ainsi que l'interactivité qu'il propose.

5.4.2 jQuery



jQuery est une bibliothèque²⁵ JS développée par John Resig sous licence MIT depuis 2006. La dernière version en date, la 3.3.1, est sortie cette année.

L'objectif de cette bibliothèque est de faciliter la création des scripts du côté client, donc dans les pages Web. Cela se voit notamment lors de l'utilisation d'Ajax.

²⁴ Licence logicielle provenant du Massachusetts Institute of Technology. C'est une licence de logiciel libre et open source.

²⁵ C'est un ensemble de routines prêt à être utilisé par un programme.

5.5 Modélisation

5.5.1 Base de données

Afin de modéliser la base de données, nous avons utilisé le logiciel JMerise²⁶. Il permet de générer un modèle conceptuel de données (MCD) via la méthode Merise²⁷. Le MCD est basé sur des notions d'objets ou d'entités et d'associations.

Les objets représentent ici les tables de notre base de données et sont composés de plusieurs propriétés faisant référence aux champs de la table. Ainsi sur JMerise, nous pouvons modéliser nos tables en incluant les différents champs et leur appliquer des spécificités comme le fait d'être unique.

Voici la représentation d'un objet :

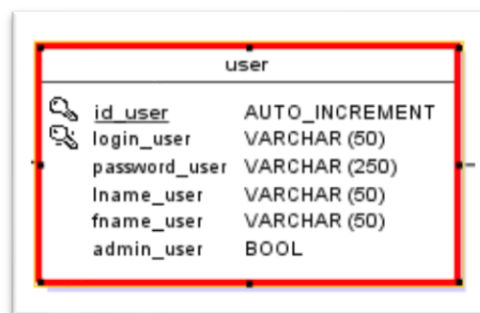


Figure 12- Table des utilisateurs

Dans cette table :

- *id_user* représente l'identifiant de l'objet
- *login_user* est un identifiant alternatif

Les associations dans notre MCD correspondent aux relations dans notre base de données. Ces dernières sont dites de type binaire car la relation se fait entre deux entités.

Voici la représentation d'une association :

²⁶ <http://www.jfreesoft.com/JMerise/>

²⁷ Méthode d'analyse, de conception et de gestion de projet informatique

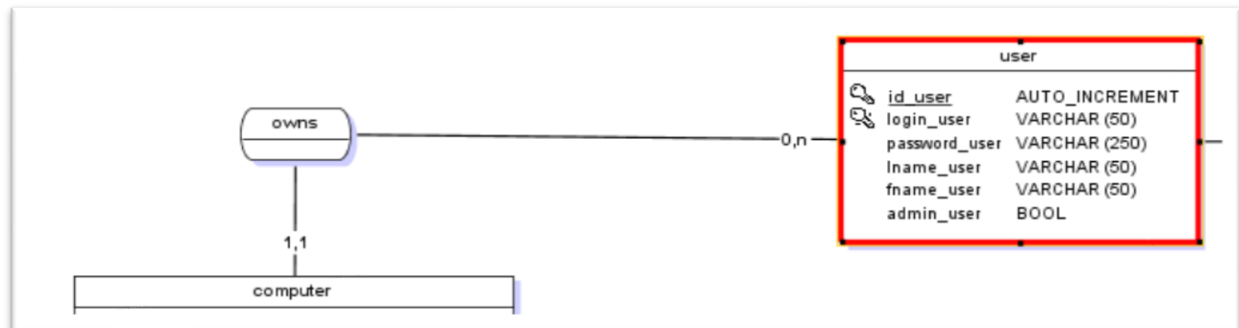


Figure 13- Relation entre la table utilisateur et la table ordinateur

Cette relation montre le lien entre les utilisateurs et les ordinateurs, elle peut être décrite de cette manière :

- « Utilisateur possède ordinateur »

Les cardinalités²⁸ permettent d'enrichir la relation entre différentes tables en ajoutant les nombres minimum et maximum où l'occurrence peut participer à l'association.

Les cardinalités sont représentées de cette manière :

- 0,1 les clés de l'entité migrent
- 1,1 les clés de l'entité migrent
- 0,n les clés de l'entité ne migrent pas
- 1,n les clés de l'entité ne migrent pas

Les associations peuvent être regroupés en deux types d'associations :

- Les contraintes d'intégrité fonctionnelles (CIF) sont binaires et ont une cardinalité minimum à 0 ou 1 et une cardinalité maximum à 1 ou n
- Les contraintes d'intégrité multiple (CIM) ont toutes les cardinalités maximums à n et on peut leur adjoindre des propriétés

Dans la figure 2 nous pouvons décrire les cardinalités de cette manière :

- 0,n se traduit par : « un utilisateur peut posséder 0 ou plusieurs ordinateurs »
- 1,1 se traduit par : « un ordinateur ne peut être posséder que par 1 et 1 seul utilisateur »
- L'association est de type CIF

Voici le MCD dans sa globalité :

²⁸ Source : [https://fr.wikipedia.org/wiki/Merise_\(informatique\)](https://fr.wikipedia.org/wiki/Merise_(informatique))

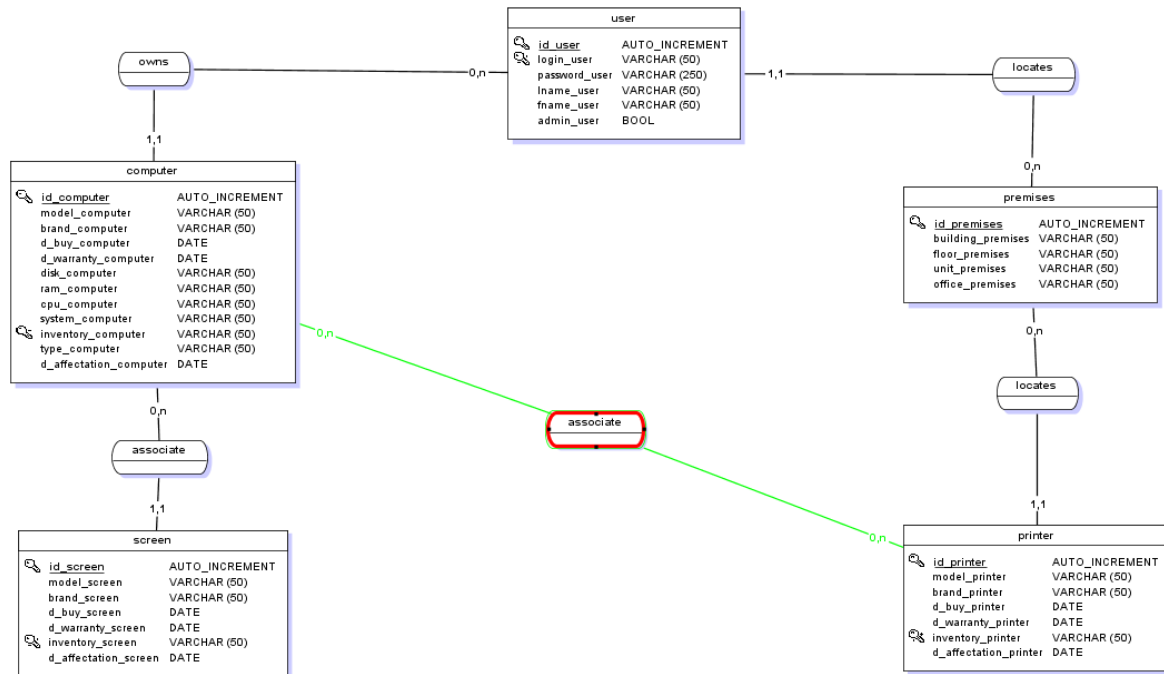


Figure 14- MCD

A partir de ce MCD, le logiciel JMerise nous permet de créer automatiquement un modèle logique des données (MLD). Lors de cette étape une vérification est effectuée permettant de valider le MCD.

Le MLD se base sur le MCD tout en précisant l'organisation des données, on peut ainsi parler de modèle relationnel. C'est à partir du MLD que l'on peut connaître le nombre de table à créer dans la base de données relationnelle.

La transformation du MCD en MLD s'effectue de cette manière :

- Les entités sont transformées en tables
- Les propriétés sont transformées en champs, les identifiants sont transformés en clés primaires, les identifiants alternatifs sont transformés en attribut « unique »
- Les associations sont transformés en relations, les cardinalités permettent l'importation de clés étrangères dans les tables pour les CIF et la création d'une nouvelle table contenant des clés étrangères primaires dans le cas des CIM

Voici la représentation d'une table :

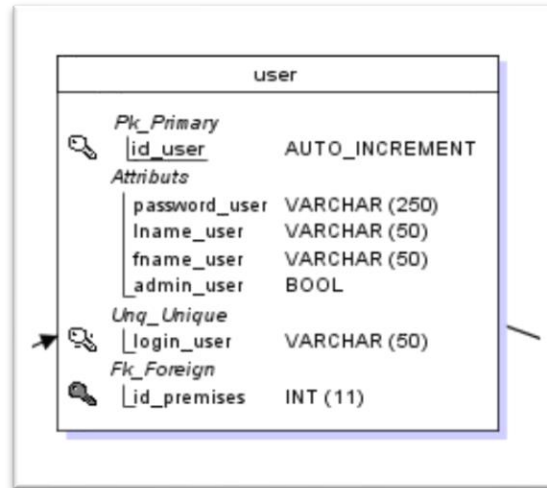


Figure 15- Table des utilisateurs

Ici nous pouvons voir l'apparition de la clé étrangère *id_premises* dans la table des utilisateurs. De même, le champ *id_user* est devenu une clé primaire et on peut voir que *login_user* est un identifiant unique.

La relation 0,n / 0,n entre les ordinateurs et les imprimantes a été transformé en une table distincte incluant deux clés étrangères primaires comme suit :

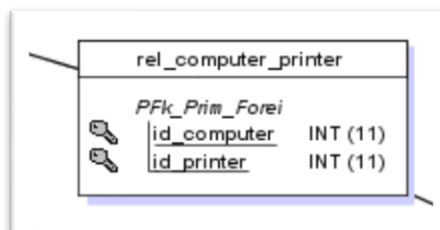


Figure 16- Table de relation imprimante/ordinateur

Cette table va nous permettre d'établir un lien direct entre une imprimante de bureau et son ordinateur associé.

Voici le MLD dans sa globalité :

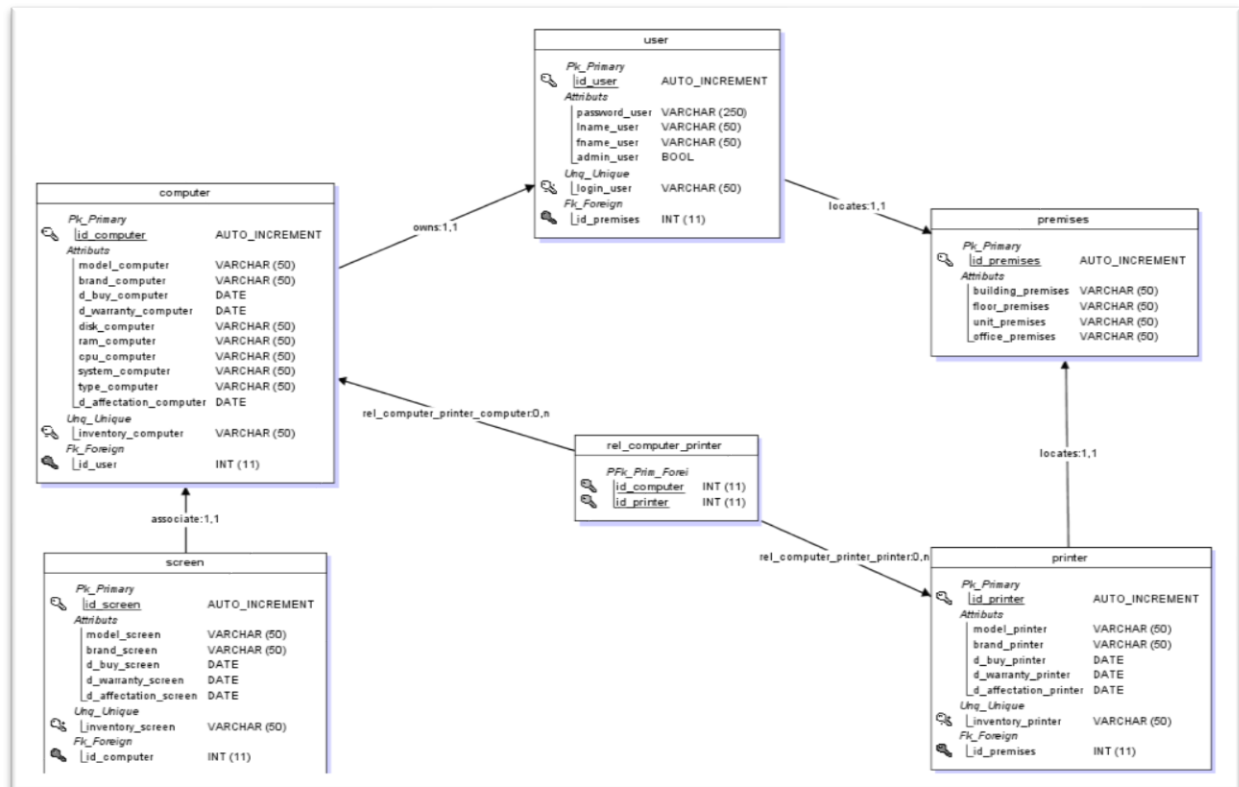


Figure 17- MLD

Lors de la transformation du MCD en MLD, JMerise génère également un script SQL permettant la création instantanée de la base de données relationnelle. Ce dernier nous a servi de base, en effet nous avons apporté quelques ajouts et modifications afin qu'il corresponde exactement à nos besoins. Le script de création est disponible en annexe de ce document²⁹.

Une des limites de ce modèle concerne l'optimisation ou la définition des ressources nécessaires à l'application de ce dernier dans l'environnement de production. Cela devra être estimé et calibré afin de fournir une architecture matérielle suffisamment puissante pour pouvoir exécuter la base de données relationnelle.

5.5.2 Interface web

Afin de modéliser une maquette de l'interface Web, nous avons utilisé le site Mockflow³⁰ qui permet de générer rapidement une interface navigable afin d'avoir un visuel et une idée de l'apparence du site Web.

²⁹ Annexe numéro ??

³⁰ <https://mockflow.com/>

L'intégration en glisser/déposer des différents composants de Bootstrap nous a permis de générer très rapidement une maquette.

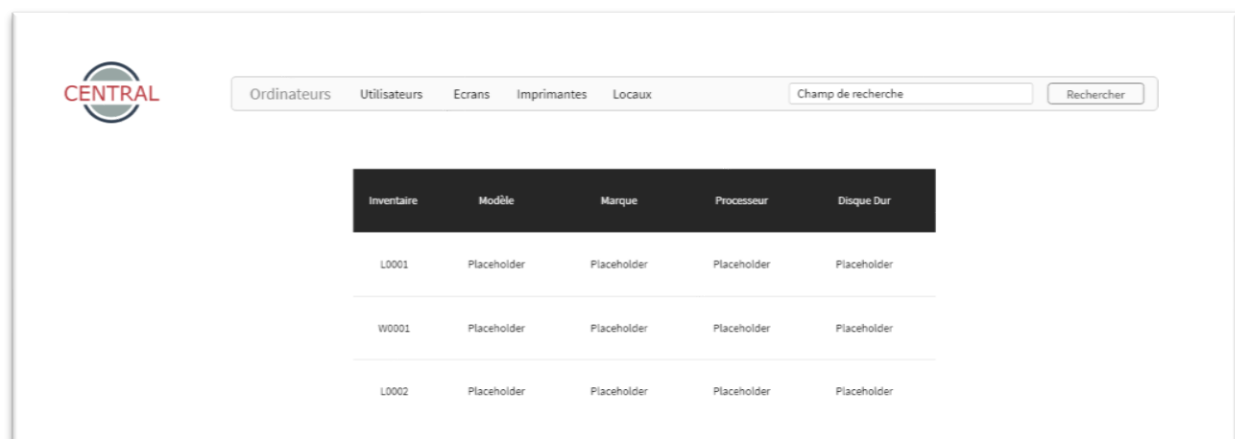
Cet outil en ligne propose dans sa version d'essai le travail sur un seul projet avec une limitation à 4 pages. Pour ce projet cela était largement suffisant, mais dans le cas où de futur projets Web seraient ajoutés ou le travail collaboratif absolument nécessaire le passage à un abonnement mensuel d'équipe serait nécessaire.

Voici une présentation de la maquette :



Maquette de la page de connexion. Elle contient le logo CENTRAL à gauche, deux champs de saisie pour 'Nom d'utilisateur' et 'Mot de passe' au centre, et deux boutons 'Connexion' (vert) et 'Réinitialiser' (orange) à droite.

Figure 18- Page de connexion



Maquette de la page d'accueil et vue des données. Elle présente le logo CENTRAL, une barre de navigation avec des liens (Ordinateurs, Utilisateurs, Ecrans, Imprimantes, Locaux), un champ de recherche et un bouton 'Rechercher'. En dessous, un tableau à 5 colonnes (Inventaire, Modèle, Marque, Processeur, Disque Dur) affiche des données avec des placeholders.

Inventaire	Modèle	Marque	Processeur	Disque Dur
L0001	Placeholder	Placeholder	Placeholder	Placeholder
W0001	Placeholder	Placeholder	Placeholder	Placeholder
L0002	Placeholder	Placeholder	Placeholder	Placeholder

Figure 19- Page d'accueil et vue des données

5.6 Fonctionnalités

5.6.1 Administrateur

Une des contraintes du cahier des charges concerne l'accès à la base de données relationnelle :

- Un accès doit être fait en consultation uniquement pour les utilisateurs
- Un accès doit être fait en contrôle total pour les administrateurs

Afin de répondre à cette contrainte, nous avons choisi d'ajouter un attribut administrateur, de type booléen³¹, à la table des utilisateurs.

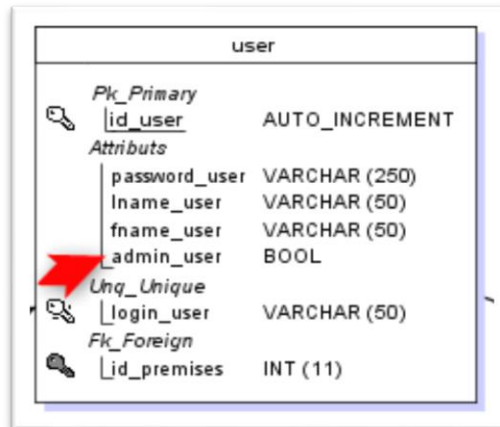


Figure 20- Attribut administrateur


Dans l'application Web, cette valeur va nous permettre de valider la connexion avec les droits administrateurs, mais aussi apporter un contrôle continu lors de chaque ajout/modification/suppression de données.

Voici deux exemples de vérification des droits administrateurs :

```
if (isset($_POST['username']) && isset($_POST['password'])) {
    if(password_verify($passuser, $resultpass)){
        if($adminuser){
            session_start();
            echo 'admin';
            $_SESSION["fname_user"] = $data["fname_user"];
            $_SESSION["admin_user"] = $adminuser;
            $_SESSION["connection"] = 1;
        } else {
            session_start();
            echo 'user';
            $_SESSION["fname_user"] = $data["fname_user"];
            $_SESSION["admin_user"] = $adminuser;
            $_SESSION["connection"] = 1;
        }
    } else {
        echo 'fail';
    }
}
```

Figure 21- Droits administrateurs lors de la connexion

³¹ « En informatique, un booléen est un type de variable à deux états (généralement notée vrai et faux), destiné à représenter les valeurs de vérité de la logique et l'algèbre Booléenne. » Source : <https://fr.wikipedia.org/wiki/Bool%C3%A9en>

	PROJET EVOLUTION	Omar AIT-MOULID / Julien VILLARD Date : 21/09/2018 V.05 Page : 50/93
	Etude de faisabilité	

```
if (isset($_SESSION["connection"]) && $_SESSION["admin_user"]){
    require "../fonction.php";
    delComputer($condition);
}
```

Figure 22- Droits administrateur lors de la suppression d'un ordinateur

5.6.2Ajouter

L'ajout de données dans la base se fait via l'utilisation d'un modal³² sur chaque page concernant le matériel.

Le modal contient ici un formulaire permettant de saisir les données. Il se compose d'un bouton permettant d'appeler la boîte de dialogue et la boîte de dialogue en elle-même. L'accès à ce bouton est réservé aux personnes possédant des droits administrateurs.

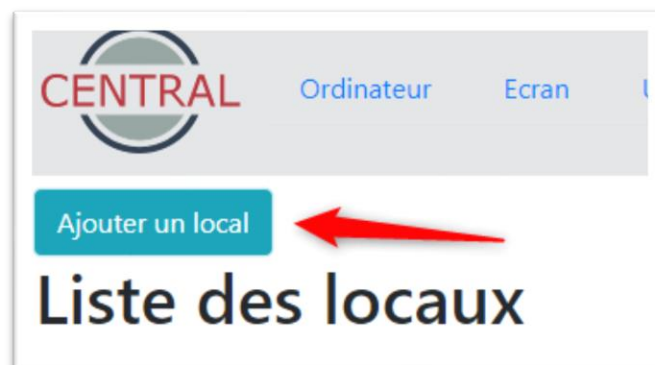
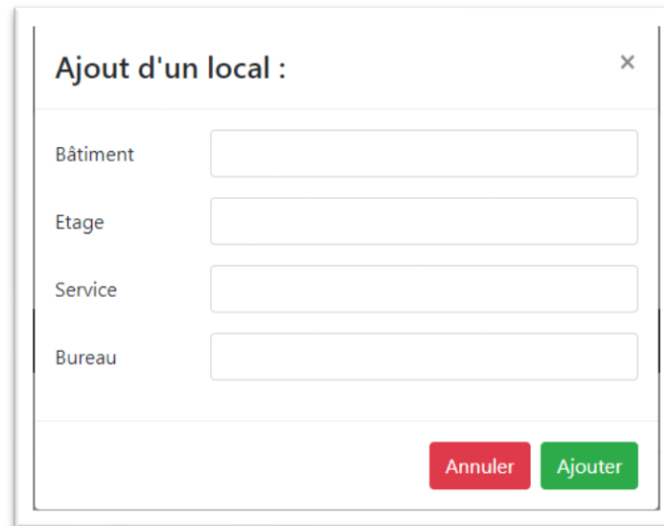


Figure 23- Bouton pour ajouter un local

³² Le modal est une fonctionnalité de Bootstrap faisant appel au langages HTML, CSS et JS et permettant d'afficher une boîte dialogue.



Ajout d'un local :

Bâtiment

Etage

Service

Bureau

Figure 24- Formulaire d'ajout d'un local

Lors de l'appui sur le bouton *Ajouter*, un script JS envoie les données via une méthode POST³³ à une fonction PHP, qui les vérifie et exécute la requête SQL ajoutant les données à la table concernée.

5.6.3 Consulter

La consultation des données est accessible à la fois aux administrateurs et utilisateurs.

Les éléments sont chargés en cliquant sur l'élément correspondant dans la navbar³⁴. A noter qu'elle contient également le bouton servant à la déconnexion en rouge. Le logo Central permet de revenir à l'accueil de la page.

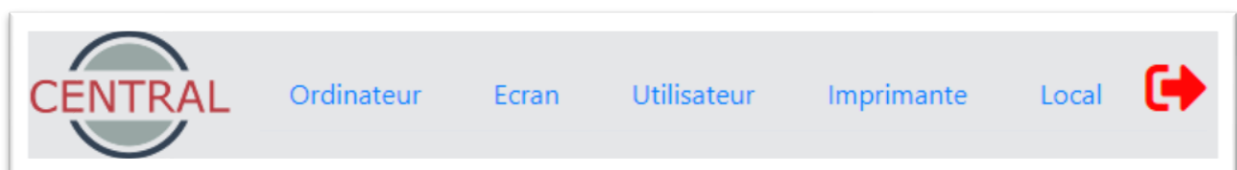



Figure 25- Navbar

Lors de la sélection d'un des éléments de la navbar, une requête est envoyée à la base de données par des scripts JS et PHP.

³³ Méthode de requête supporté par HTTP, les données sont contenues dans le corps du message de demande envoyé au serveur.

³⁴ La navbar est un des composants fournis par le framework Bootstrap.

	PROJET EVOLUTION	Omar AIT-MOULID / Julien VILLARD Date : 21/09/2018 V.05 Page : 52/93
	Etude de faisabilité	

En retour les données sont formatées dans un tableau et ainsi accessible à la consultation.

Numéro d'inventaire	Type	Modèle	Marque	Utilisateur	Bureau
L0001	Portable	5580	DELL	stock ▼	BP101
W0001	Fixe	5060	DELL	stock ▼	BP101
Numéro d'inventaire	Type	Modèle	Marque	Utilisateur	Bureau

Figure 26- Extrait du tableau des ordinateurs

5.6.4 Modifier

La modification des données s'effectue directement en cliquant sur la cellule concernée, ou en déroulant le menu inclus dans cette dernière. Cette fonctionnalité n'est accessible qu'aux comptes administrateurs.

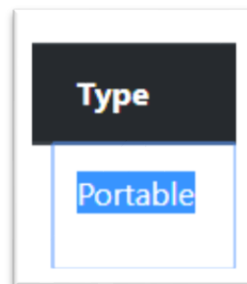


Figure 27- Modification dans le tableau

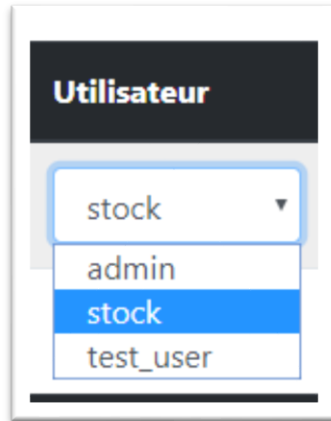


Figure 28- Menu déroulant de modification dans le tableau

Un script JS se déclenche dès lors que l'on clique en dehors de la cellule concernée où que l'on sélectionne un nouvel élément dans la liste déroulante.

Une demande de confirmation est alors envoyée en haut de la page dans une boîte de dialogue, permettant de pouvoir annuler une action si nécessaire et empêchant la modification par erreur.



Figure 29- Boîte de dialogue de confirmation de modification

Le script envoie les nouvelles données à un script PHP qui vérifie et exécute la requête de modification des données de la table.

Ainsi, seules les données ayant été changées dans le tableau sont modifiées dans la table évitant de devoir envoyer toutes les données d'une ligne à chaque petite modification. D'un autre côté, la modification complète d'une ligne n'est pas prise en charge dans cette version du site.

5.6.5 Supprimer

Afin de supprimer les données, un bouton est prévu en face de chaque ligne. Ce dernier n'est accessible qu'aux administrateurs.



Figure 30- Bouton de suppression

Lors de la suppression, un script JS ouvre une boîte de dialogue demandant la confirmation puis actionne un script PHP exécutant la requête de suppression dans la base de données.

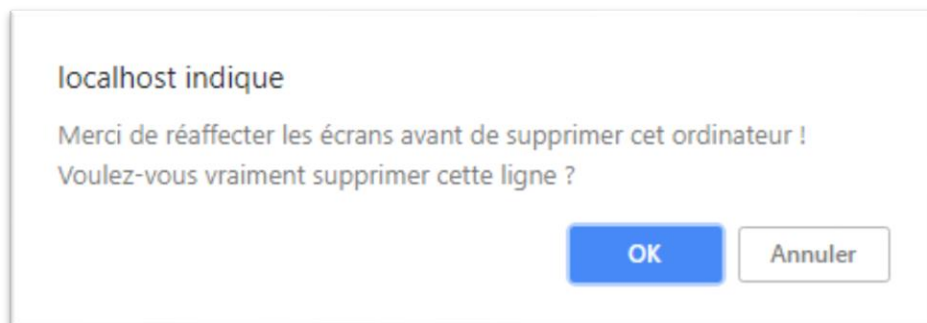


Figure 31- Boîte de dialogue de confirmation de suppression

Dans la base de données relationnelle, les données étant liées par des clés étrangères sont protégées contre la suppression. Ainsi dans le cas de suppression d'un ordinateur, cette dernière ne pourra être effective que lorsque le ou les écrans auront été au préalable affecté à un autre ordinateur.

Le script JS supprime également de manière dynamique la ligne du tableau lors de la suppression des données.

5.6.6 Recherche

La fonctionnalité de recherche est obtenue par le biais de deux manières différentes.

- La première consiste en une recherche dans la base de données relationnelle via une requête SQL, cela correspond à la barre de recherche en haut de la page.

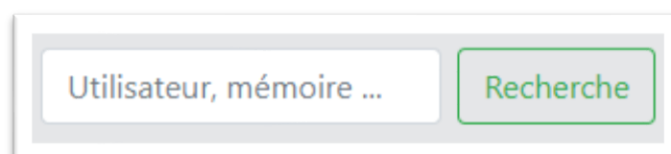



Figure 32- Barre de recherche

	PROJET EVOLUTION	Omar AIT-MOULID / Julien VILLARD Date : 21/09/2018 V.05 Page : 55/93
	Etude de faisabilité	

Dans cette version du site, elle ne prend en compte la recherche que pour les ordinateurs sur les utilisateurs, la mémoire, le disque dur et le local.

- La deuxième méthode consiste en un filtrage du tableau via un script JS se déclenchant dès que l'on entre des caractères dans cette zone de texte.

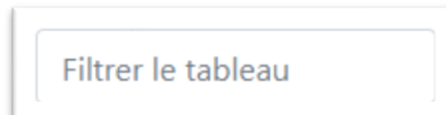


Figure 33- Filtrage du tableau

Le filtrage s'effectue sur toutes les données du tableau à l'exception des menus déroulants et des dates. Une version ultérieure du site modifiera cela afin de fournir un filtrage complet.

5.6.7 Sécurité

Chaque action sur le site entraîne une vérification de l'état de connexion et le cas échéant des droits administrateurs. Ainsi, même après la vérification lors de la connexion, un contrôle continu est effectué.

5.7 Résultat final de la version bêta

Voici une présentation de quelques pages de l'application Web. Cette version sera celle mise en production puis améliorée en continu.

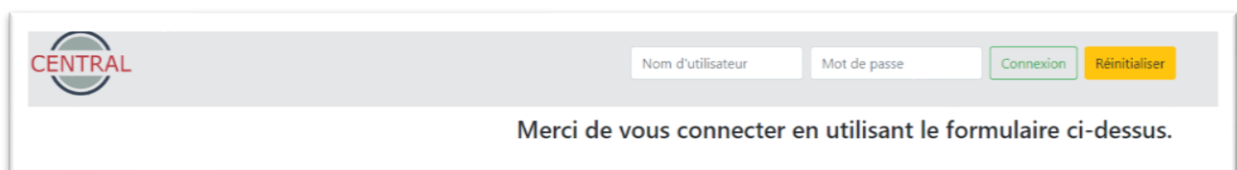


Figure 34- Page de connexion



Figure 35- Page d'accueil



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 56/93

Nom	Prénom	Login	Bureau	Service
Administrateur	Administrateur	admin	BP101	Informatique
Test	User	test_user	BP101	Informatique
Stock	Informatique	stock	BP101	Informatique

Figure 36- Page de consultation des utilisateurs

Cette version, même si elle n'est pas parfaite, propose à ce jour un environnement fonctionnel répondant au cahier des charges, comme décrit dans le tableau de recettage.

5.8 Evolutions

- Les premières évolutions à venir concernant l'application Web seront les corrections de bugs et l'optimisation du code.
- La mise en place d'une fonctionnalité de gestion des incidents et également à l'étude et pourrait être déployée lors d'une mise à jour majeure.
- L'interface Web est optimisée pour une utilisation sur un ordinateur ayant une résolution de 1080p. En fonction des besoins le site pourra être rendu responsive afin de s'adapter aux différentes tailles d'écrans et être utilisable sur tablette et smartphone. Cela rentrera également dans le cadre d'une mise à jour majeure.
- L'amélioration de l'expérience utilisateur sera un des points essentiels concernant les évolutions. Les retours des utilisateurs nous permettront d'améliorer les points les plus désagréables et rendre ainsi l'utilisation plus facile et agréable. Une des premières mises à jour concernera la représentation visuelle des actions par l'utilisation de diverses couleurs et animations afin de permettre à l'utilisateur de mieux cerner ce qu'il est en train de faire.

6 Chiffrage

6.1 Serveurs

Les serveurs représentent l'un des composants essentiels de notre infrastructure système.

L'infrastructure préconisée reposant essentiellement sur la virtualisation et le stockage déporté via un NAS, les serveurs doivent répondre à des critères spécifiques afin d'être dimensionnés en conséquence.

Des serveurs surdimensionnés, en termes de capacité, représentent un coût important à l'achat mais permettent d'avoir une flexibilité accrue et des possibilités d'évolutions intéressantes. Cependant, leur durée de garantie étant limitée et l'évolution vers des infrastructures dans les nuages ne permettront possiblement l'exploitation des machines à leur plein potentiel avant leur renouvellement.

Afin de répondre à ces contraintes, nous avons choisi de nous porter vers des serveurs de la marque DELL pouvant s'intégrer à l'infrastructure présente. Le parc client reposant sur des machines DELL, la configuration personnalisée des serveurs et les garanties ainsi que le service après-vente de DELL nous ont convaincu de préconiser des serveurs de leur marque.

Le modèle retenu est le PowerEdge R740. Il propose un large choix de processeurs ainsi que des emplacements mémoire et des baies de stockage suffisantes pour l'infrastructure retenue.



Figure 37- PowerEdge R740



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 58/93

Voici ces caractéristiques techniques principales :

Processeur (1 CPU)	Intel® Xeon® Silver 4110 2.1G, 8C/16T, 9.6GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400
Mémoire (2x16Go)	32GB RDIMM, 2666MT/s, Dual Rank
Disque dur (2x300Go en RAID 1)	300GB 15K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive
Réseau	Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T
Alimentation redondante	750W
Garantie	5 ans de garantie basique le jour ouvré suivant
Tarif HT à l'unité	3 170,47 €

Tableau 17 - Caractéristiques serveurs

- Le processeur, grâce à son nombre de cœur suffisant et à l'Hyper-Threading³⁵, va permettre d'héberger les machines virtuelles de manière efficiente tout en nous permettant d'avoir une puissance de calcul suffisante en cas d'ajout de nouvelle machine virtuelle
- La mémoire est un des composant essentiel et est nécessaire en grande quantité afin de pouvoir allouer le montant nécessaire à chaque machine virtuelle. Si le montant initial s'avère insuffisant des emplacements supplémentaires sont disponibles afin de l'étendre
- Le disque dur représente ici le stockage pour l'hyperviseur ainsi qu'une seule machine virtuelle et ne nécessite pas une quantité importante. En cas de besoin, le serveur propose des baies de stockage supplémentaires permettant d'accroître rapidement la capacité totale de stockage. L'utilisation du RAID 1 est une solution de tolérance aux pannes rendant le serveur plus sûr
- La carte réseau Broadcom va permettre la connexion via 2 ports 10Gb permettant des accès ultra rapides et 2 ports 1Gb permettant une connexion moins rapide. Grâce aux 2 ports 10Gb, le serveur ne se retrouvera pas bridé par le réseau et proposera une connexion optimale au sein de l'infrastructure déployée
- L'alimentation redondante de 750W permet d'assurer à la fois une tolérance aux pannes et permet de couvrir les besoins en énergie du serveur
- La garantie de 5 ans permet de s'assurer que l'investissement initial permettra de couvrir une période suffisante avant un potentiel renouvellement

³⁵ « L'hyper-threading consiste à créer deux processeurs logiques sur une seule puce, chacun doté de ses propres registres de données et de contrôle, et d'un contrôleur d'interruptions particulier. Ces deux unités partagent les éléments du cœur de processeur, le cache et le bus système. Ainsi, deux sous-processus peuvent être traités simultanément par le même processeur. Cette technique multitâche permet d'utiliser au mieux les ressources du processeur en garantissant que des données lui sont envoyées en masse. » Source : <https://fr.wikipedia.org/wiki/Hyper-Threading>

Afin de permettre la mise en place du cluster, il est nécessaire de prendre deux serveurs. Ainsi, le coût total concernant les serveurs DELL s'élève à 6 340,94 € HT.

6.2 Licences

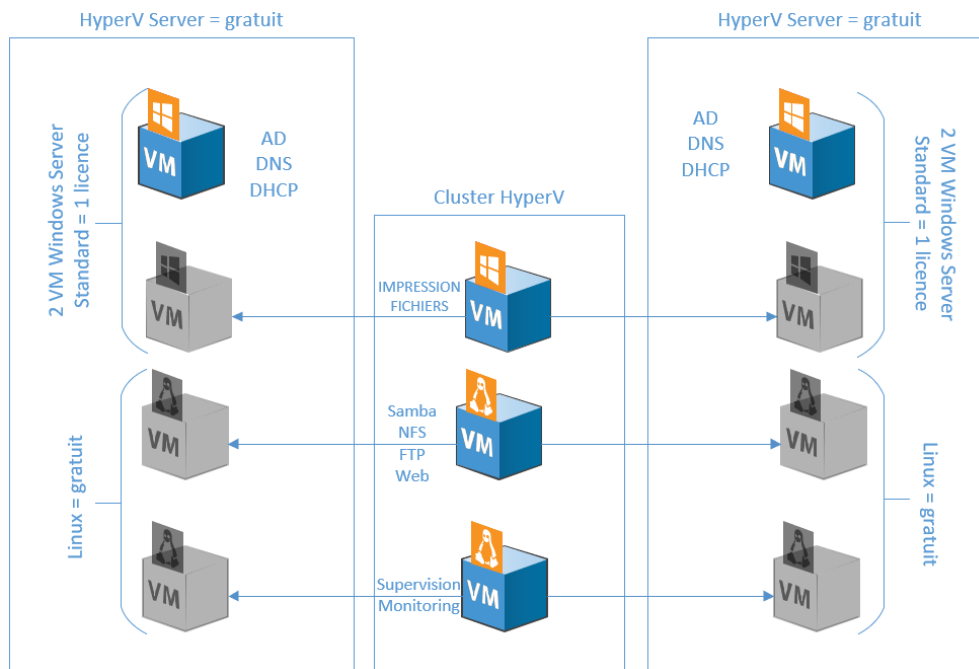


Figure 38- Schéma licences

Désignation	Tarif unitaire	Quantité	Tarif
Windows Server Standard	629,40€ HT	2	1258,80€ HT
CAL 1 user	25,78€ HT	95	2449,10€ HT
		TOTAL	3709,90€ HT

Tableau 18 - Chiffrage licences

6.3 NAS

Dans l'optique d'assurer le stockage des données, mais aussi le stockage des machines virtuelles en cluster, nous préconisons l'utilisation de serveur NAS.

Nous avons sélectionné la marque Synology pour les NAS de l'infrastructure préconisée.

Notre choix s'est porté sur cette marque pour plusieurs raisons :

- La compatibilité avancée avec le stockage ISCSI
- Le cluster high-availability, permettant de réunir 2 NAS Synology afin de fournir une solution de tolérance de pannes. La connexion Heartbeat reliant les NAS permet le basculement automatique sur le deuxième serveur en cas de panne du premier avec une indisponibilité des données et des machines virtuelles de seulement quelques minutes
- Le cache SSD permettant un stockage de machines virtuelles sans compromis entre performance et capacité de stockage. Les données sont écrites en premier sur le cache SSD puis ensuite transférés sur les disques durs

Le modèle retenu est le RackStation RS818+. Ce dernier est totalement compatible avec nos installations et pourra être facilement mis en place.



Figure 39- RackStation RS818+

Voici ces caractéristiques techniques principales :

Processeur (1 CPU)	Intel Atom C2538, Quadruple cœur 2.4 GHz
Mémoire (2x1Go)	2Go DDR3L SO-DIMM 1600 MHZ CL11
Cache SSD	SAMSUNG SSD 860 PRO 256 GO
Disque dur (3x1To en Synology Hybrid RAID)	TOSHIBA P300 2 To de stockage total
Réseau	4 ports 1GbE
Alimentation	100W
Garantie	5 ans de garantie
Tarif HT à l'unité	1 215,65 €

Tableau 19 - Caractéristiques NAS

- Le processeur présente une puissance suffisante pour assurer l'hébergement des machines virtuelles mais aussi le partage de fichier
- La quantité de mémoire et sa vitesse permette de ne pas brider les capacités
- Le cache SSD associé à la capacité de stockage importante permet une utilisation optimale tout en ayant une marge de de sécurité avant de devoir augmenter la capacité de stockage
- La carte réseau permet de couvrir le lien Heartbeat et le lien avec les serveurs avec une bande passante élevée tout en proposant des connexions de secours le cas échéant

Afin de mettre en place le cluster high-availability, il est nécessaire de prendre deux modèles de NAS équivalent ayant les mêmes caractéristiques. Ainsi, le coût total pour deux serveur NAS Synology s'élève à 2 431,30 € HT.

Afin d'assurer une sauvegarde des données en local, nous préconisons l'utilisation d'un NAS supplémentaire servant à héberger les données.

Le modèle retenu est le DS218.



Figure 40- DS218

Nous l'équiperons avec un stockage de 8To avec deux disques dur Toshiba N300 de 8 To en Synology Hybrid RAID. Le tarif s'élève à 712,40 € HT.

6.4 Sauvegarde cloud

Afin d'archiver les données présentes sur le serveur NAS, Synology propose une solution flexible et compatible avec les principaux fournisseurs de stockage cloud.

- Le sens de la synchronisation peut être sélectionné permettant de ne sélectionner que l'envoi des données dans le cas d'un archivage



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 62/93

- Les données sont chiffrées et compressées
- Le traitement simultané peut être configuré afin de ne pas consommer trop de ressources sur le serveur NAS et ainsi impacter les autres fonctionnalités
- Les fichiers peuvent être sélectionnés rendant encore plus flexible la sauvegarde. Cela s'avère essentiel notamment dans le cadre du Règlement général sur la protection des données (RGPD)

Plusieurs sociétés proposent des services de stockage dans le cloud tel que Microsoft et Amazon par exemple.

Notre choix s'est porté sur les solutions Azure proposées par Microsoft car la compatibilité avec notre infrastructure est garantie. De même, dans un souci d'évolution et de tendre vers de la très haute disponibilité, l'ajout d'un hyperviseur au sein des infrastructures de Microsoft hébergées en France nous permettrait de disposer d'une très grande proximité entre l'archive de nos données et nos machines virtuelles. Ainsi en cas de sinistre important entraînant la perte de toutes les données localement, il nous serait possible de redémarrer la production dans un laps de temps réduit.

D'un point de vue tarif, la solution de stockage Microsoft Azure s'élève à 0 € pour l'envoi de données et à 1,69 € pour le stockage de 1 To de données par mois.

Dans le cas de consultation des données ou de récupération des données, le tarif s'élève à 60,29 € pour 1 To de données pour un mois.

Ces tarifs sont donnés à titre indicatif. Pour avoir un ordre d'idée plus précis, il sera nécessaire d'évaluer plus finement la quantité de données envoyée vers le stockage nuagique durant les premiers mois et ainsi pouvoir chiffrer le coût réel mensuel courant et le coût en cas de retrait des données.

6.5 Onduleur

Dans le but de protéger les serveurs et de permettre une extinction propre lors d'une coupure de courant, nous préconisons l'utilisation d'un onduleur.

Afin de couvrir la puissance d'un serveur et d'un serveur NAS, il est nécessaire de sélectionner un onduleur ayant une puissance d'au moins 850W.

Nous avons sélectionné le modèle suivant : EATON 5P 1550IR



Figure 41- EATON 5P 1550IR

Ce dernier, en plus de s'intégrer facilement dans la baie serveur, propose une puissance de 1100W. De plus il intègre des fonctionnalités avancées tel que la mesure la consommation énergétique et la segmentation de charge. Cette dernière fonctionnalité permet en plus d'exécuter un reboot distant et le démarrage séquentiel des serveurs.

Son tarif est de 549,96 €.

6.6 Chiffrage global

Désignation	Prix unitaire HT	Quantité	Tarif HT
Serveur DELL PowerEdge R740	3 170,47 €	2	6 340,94 €
Serveur NAS Synology RackStation RS818+	1 215,65 €	2	2 431,30 €
NAS Synology DS218	712,40 €	1	712,40 €
Onduleur EATON 5P 1550IR	549,96 €	1	549,96 €
Licence Windows Server Standard	629,40 €	2	1 258,80 €
Licence CAL 1 user	25,78 €	95	2 449,10 €
		Total HT	13 742,50 €

Tableau 20 - Chiffrage global



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 64/93

L'archivage dans le cloud ne rentre pas en compte dans ce chiffrage global car celui-ci relève de frais récurrent de fonctionnement et de frais exceptionnel lors d'une récupération des données archivées.

7 Recettage

Dans le cahier des charges il nous a été demandé de configurer les serveurs afin de respecter des exigences précises. Nous reprendrons à présent chacun de ces éléments et montrerons qu'ils ont été configurés conformément au cahier des charges.

7.1 Maquette réseau

Cette partie n'était pas demandée explicitement dans le cahier des charges, mais il nous a paru important de réaliser en premier lieu une maquette simulant le réseau avec l'outil Packet Tracer afin de valider le paramétrage des switchs et des routeurs. La source de cette maquette se trouve dans le dossier de travail sous Sharepoint, nous pourrons y récupérer la configuration du Backbone et l'adapter avant la mise en production.

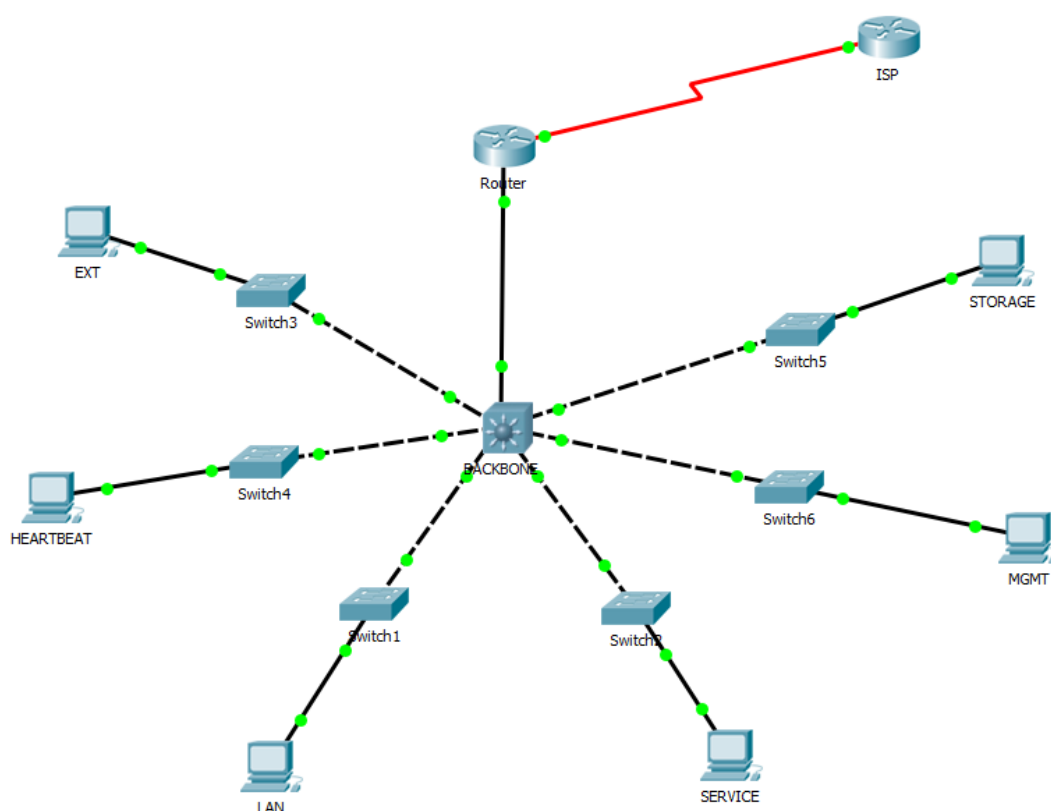


Figure 42 - Schéma réseau



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 66/93

7.1.1 Résultats

Après avoir mis en place les Vlan et les ACL conformément au plan (sauf l'exception pour le DNS, le but étant juste de valider la configuration globale), voici les résultats obtenus en faisant un « ping » entre des machines se trouvant chacune sur un Vlan différent (on simule l'accès à internet via l'adresse ip 8.8.8.8 sur le routeur ISP) :

Source		Destination		Résultat attendu	Résultat obtenu
Network	Vlan	Network	Vlan		
192.168.1.0/24	LAN	192.168.0.0/28	EXT	Autorisé	Autorisé
192.168.1.0/24	LAN	192.168.0.96/27	SERVICE	Autorisé	Autorisé
192.168.1.0/24	LAN	8.8.8.8/0		Autorisé	Autorisé
192.168.1.0/24	LAN	192.168.0.16/28	STORAGE	Interdit	Interdit
192.168.1.0/24	LAN	192.168.0.32/28	HEARTBEAT	Interdit	Interdit
192.168.1.0/24	LAN	192.168.0.64/27	MGMT	Interdit	Interdit
192.168.0.96/27	SERVICE	192.168.0.0/28	EXT	Autorisé	Autorisé
192.168.0.96/27	SERVICE	192.168.1.0/24	LAN	Autorisé	Autorisé
192.168.0.96/27	SERVICE	8.8.8.8/0		Autorisé	Autorisé
192.168.0.96/27	SERVICE	192.168.0.16/28	STORAGE	Interdit	Interdit
192.168.0.96/27	SERVICE	192.168.0.32/28	HEARTBEAT	Interdit	Interdit
192.168.0.96/27	SERVICE	192.168.0.64/27	MGMT	Interdit	Interdit
192.168.0.16/28	STORAGE	ALL	ALL	Interdit	Interdit
192.168.0.32/28	HEARTBEAT	ALL	ALL	Interdit	Interdit
192.168.0.64/27	MGMT	ALL	ALL	Interdit	Interdit

Tableau 21 - Recettage : ACL Réseau

7.2 Serveurs Windows

7.2.1 DNS

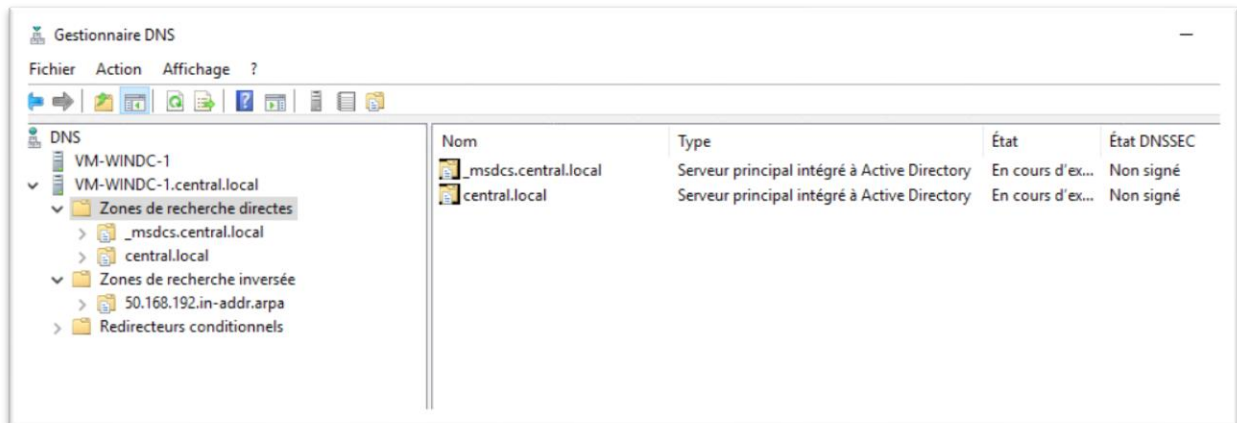


Figure 43 - Zones DNS

Nous avons configuré trois zones : deux zones principales de recherche directe (créées par Active Directory lors de la création du domaine) et une zone de recherche inverse.

- **_msdcs.central.local** : zone répliquée sur l'ensemble des contrôleurs de domaine de la forêt, contient principalement les enregistrements de type SRV (service) nécessaires à l'identification des différents serveurs jouant un rôle dans l'infrastructure Active Directory (kerberos, ldap...)
- **central.local** : zone répliquée sur les contrôleurs de domaine au niveau du domaine uniquement, contient notamment les enregistrements utiles au domaine : une délégation de la zone **_msdcs.central.local** pour l'identification des services Active Directory, les enregistrements de type A (hôte) des machines clientes du domaine...
- **50.168.192.in-addr.arpa** : zone de recherche inverse répliquée sur les serveurs DNS du domaine, contient les enregistrements de type PTR (pointeur) permettant de résoudre une adresse ip en nom

Test effectué	Résultat attendu	Résultat obtenu
Ping avec nom d'hôte	Résolution du nom en ip	Oui
Nslookup sur l'ip	Résolution de l'ip en nom	Oui

Tableau 22 - Recettage : DNS



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 68/93

7.2.2 Complexité des mots de passe

Test effectué	Résultat attendu	Résultat obtenu
Attribution d'un mot de passe faible (que des minuscules)	Erreur	Erreur
Attribution d'un mot de passe complexe avec moins de 8 caractères	Erreur	Erreur

Tableau 23 - Recettage : complexité des mots de passe

7.2.3 Impressions

7.2.3.1 Imprimante par service

Une imprimante a été paramétrée pour chacun des services

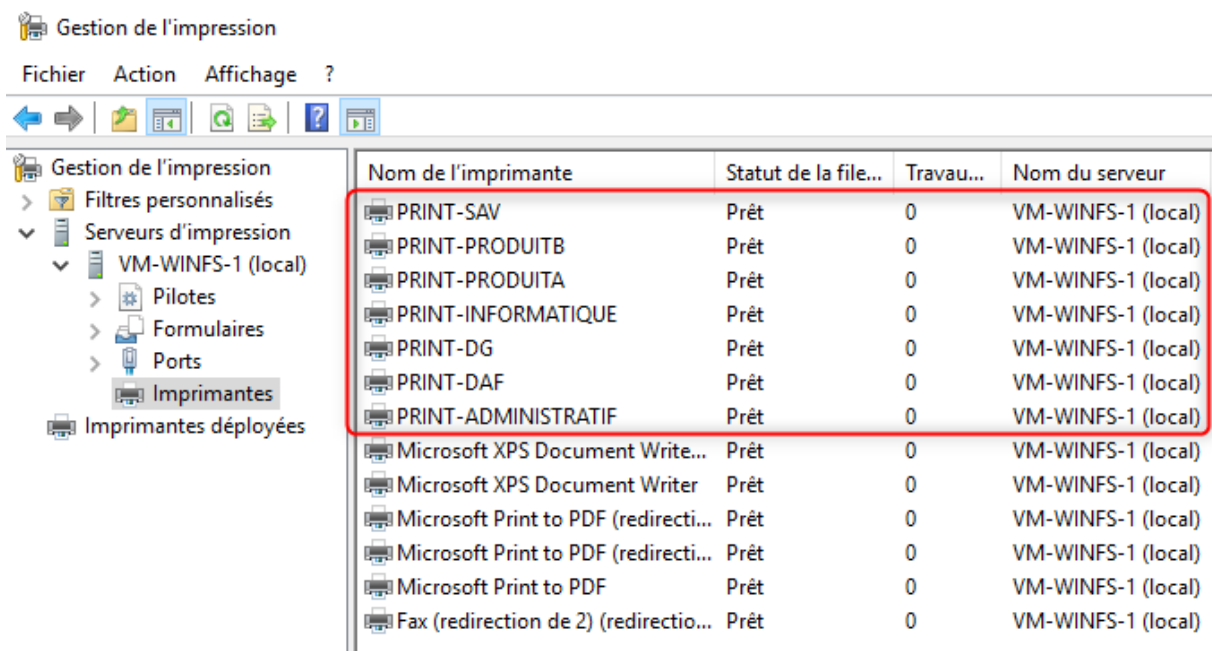


Figure 44 - Liste des imprimantes

7.2.3.2 Restrictions horaires

Les impressions sur les imprimantes des services PRODUITA et PRODUITB sont limités en fonction de l'heure (de 8h à 17h) :



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 69/93

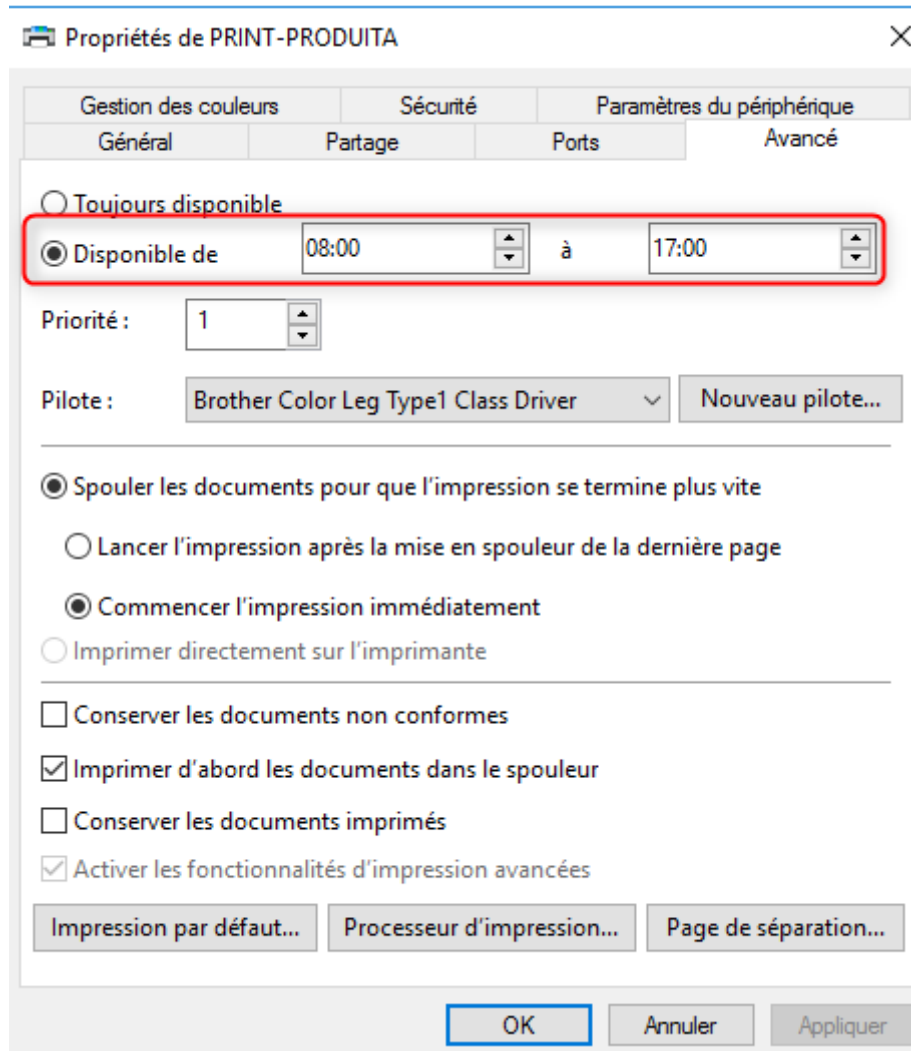


Figure 45 - Restriction horaire impression

7.2.3.3 Priorité d'impression

La priorité a été paramétrée sur les imprimantes de la Direction Générale et de la Direction Administrative et Financière :

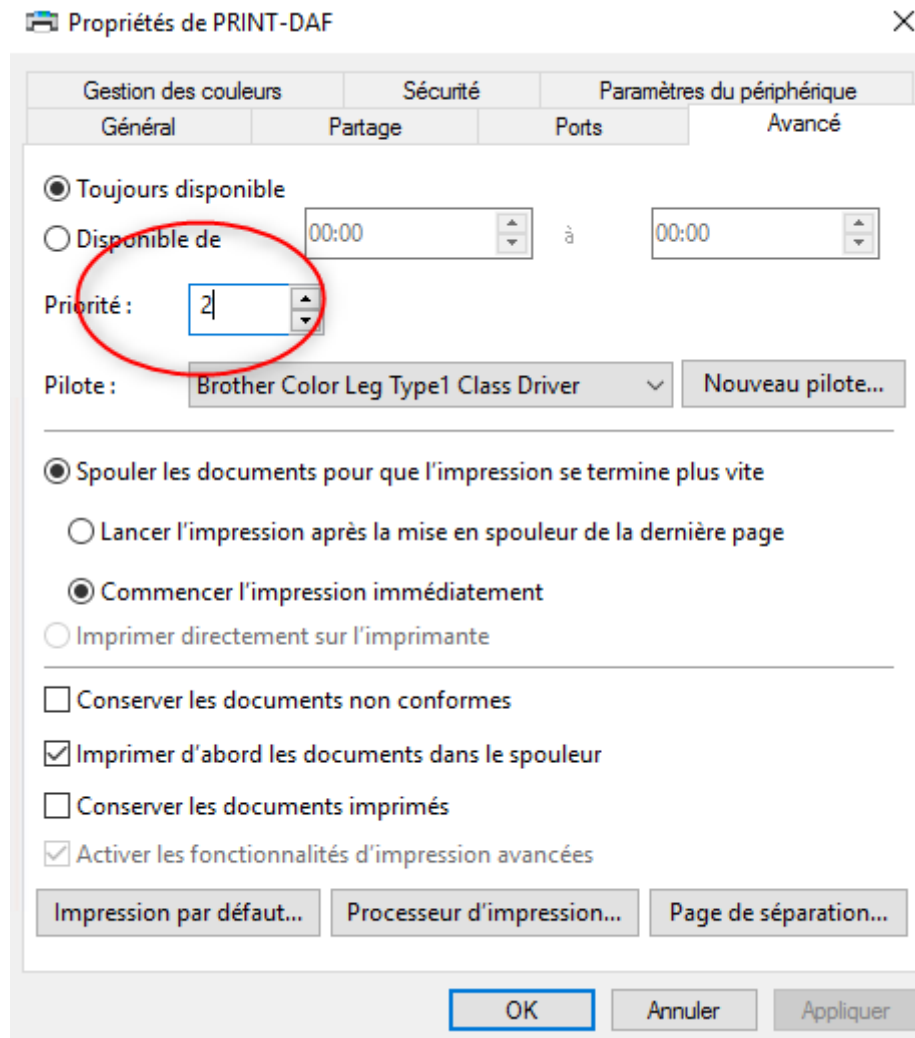


Figure 46 - Priorité d'impression

7.2.3.4 Contrôle total pour le service informatique

Toutes les imprimantes ont été paramétrées pour donner le contrôle total au service informatique :

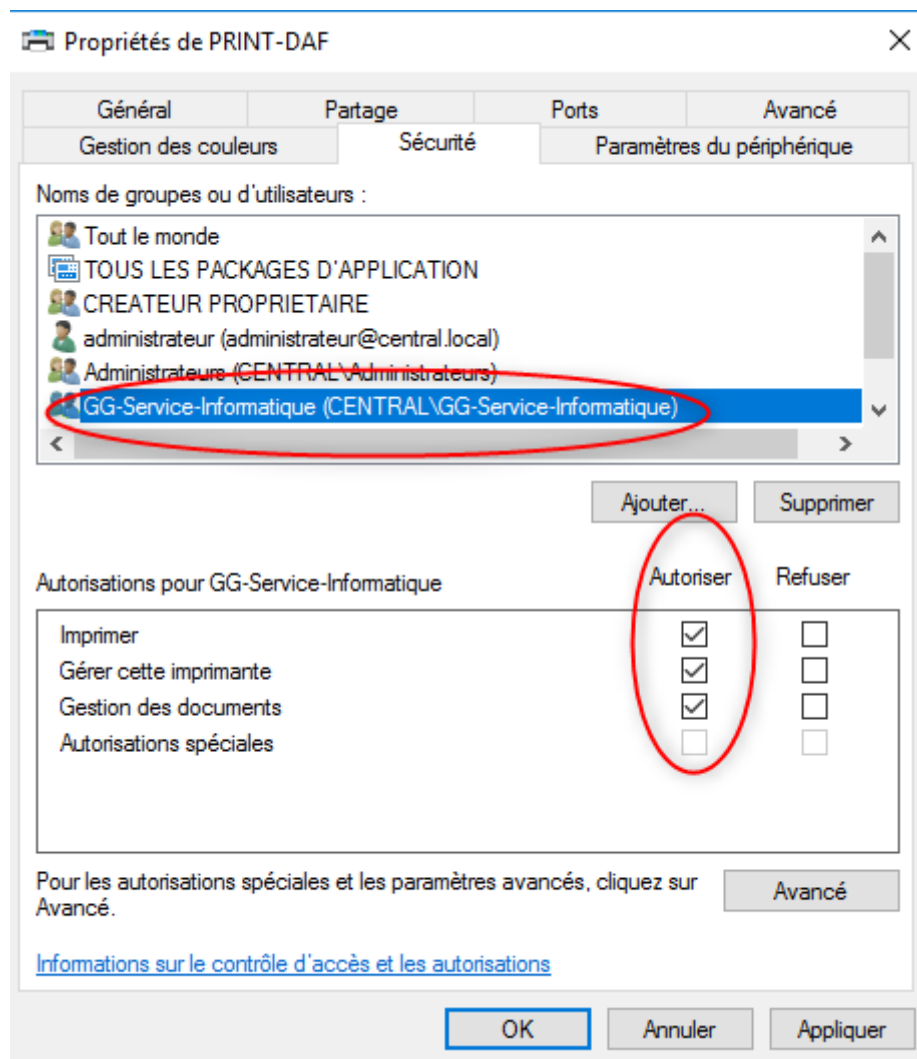


Figure 47 - Contrôle total impressions service informatique

7.2.3.5 Impression au service informatique

Les assistantes de Direction et du service SAV peuvent imprimer chez le service informatique :

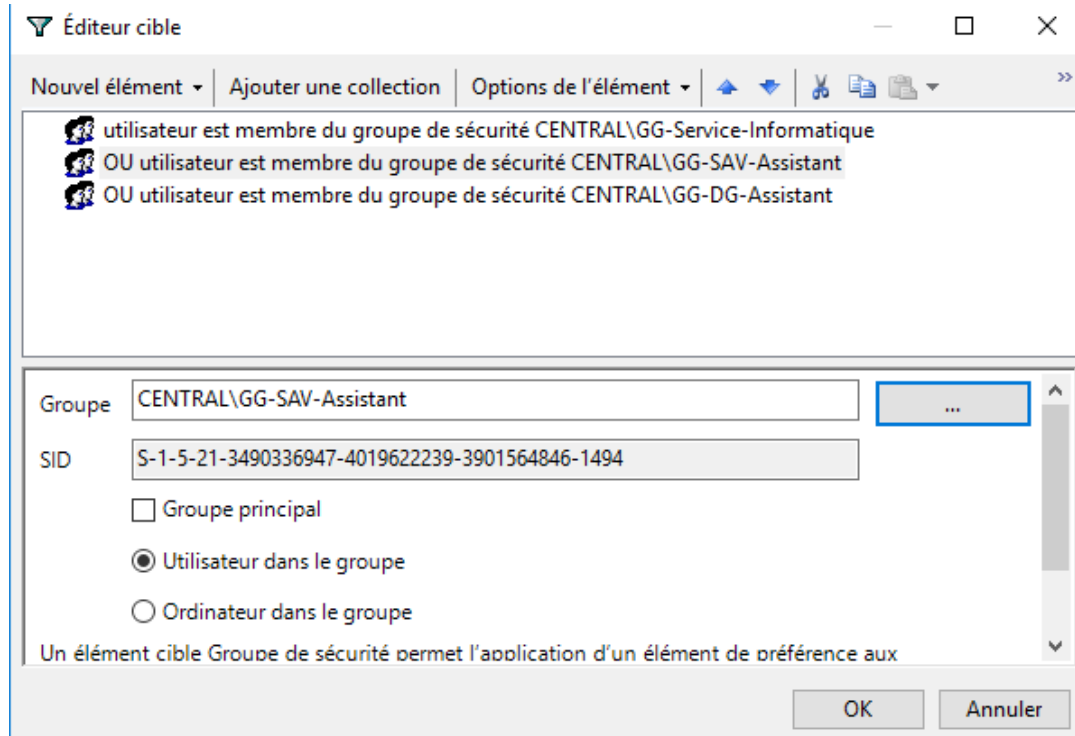


Figure 48 - GPO impression au service informatique

7.2.4 Restriction des horaires de connexion

Le script fourni « logon-time.ps1 » permet d'appliquer les restrictions sur les utilisateurs conformément au cahier des charges. Une GPO est également appliquée pour forcer la déconnexion à 19h pour certaines personnes. Voici le fichier de log après le lancement du script :



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 73/93

Processus démarré le mercredi 12 septembre 2018 14:43:03 sur le poste VM-WINDC-1
Fichier log : C:\Users\Administrateur.WIN-G1AF2JL2SER\Desktop\logon-time.log

L'utilisateur dg peut se connecter à n'importe quelle heure

Modification des horaires de connexion de l'utilisateur : dgassistante peut se connecter de 7h à 20h

Modification des horaires de connexion de l'utilisateur : ada peut se connecter de 7h à 20h

Modification des horaires de connexion de l'utilisateur : produitaresp peut se connecter de 7h à 20h

Modification des horaires de connexion de l'utilisateur : produitaservice peut se connecter de 7h à 20h

Modification des horaires de connexion de l'utilisateur : beziat peut se connecter de 8h à 18h

Modification des horaires de connexion de l'utilisateur : ella peut se connecter de 8h à 18h

Modification des horaires de connexion de l'utilisateur : ayo peut se connecter de 8h à 18h

Modification des horaires de connexion de l'utilisateur : acien peut se connecter de 8h à 18h

Modification des horaires de connexion de l'utilisateur : produitbresp peut se connecter de 7h à 20h

Modification des horaires de connexion de l'utilisateur : produitbservice peut se connecter de 7h à 20h

L'utilisateur savresp peut se connecter à n'importe quelle heure

L'utilisateur savassistante peut se connecter à n'importe quelle heure

L'utilisateur laporte peut se connecter à n'importe quelle heure

L'utilisateur daf peut se connecter à n'importe quelle heure

Modification des horaires de connexion de l'utilisateur : serviceadministratif peut se connecter de 7h à 20h

L'utilisateur serviceinformatique peut se connecter à n'importe quelle heure

L'utilisateur adminIT peut se connecter à n'importe quelle heure

Processus terminé le mercredi 12 septembre 2018 14:43:11 - Temps de traitement : 8.3286575 secondes

Tableau 24 - Recettage : Logs - Script restrictions horaires

La GPO « Users-Deconnexion-Auto » force la déconnexion des utilisateurs ciblés à 19h via une tâche planifiée :



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 74/93

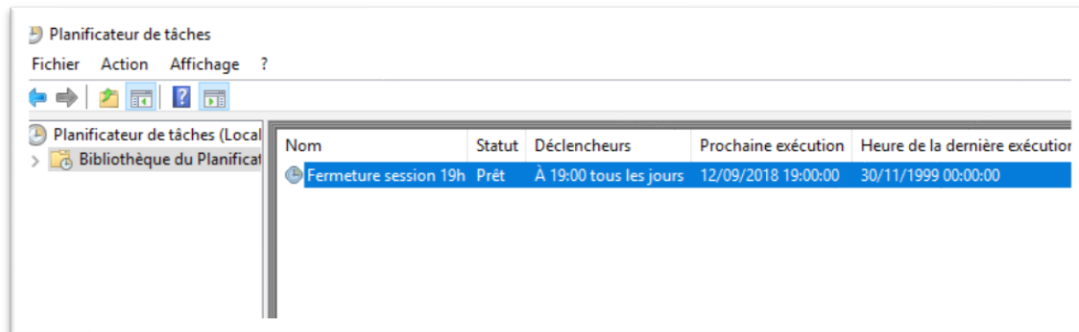


Figure 49 - Planificateur de tâches : fermeture de session forcée

Test effectué	Résultat attendu	Résultat obtenu
Connexion en dehors des horaires autorisés	Refusé	Refusé
Déconnexion automatique à 19h pour BEZIAT, ELLA, AYO et ACIEN	Déconnexion forcée	Déconnexion

Tableau 25 - Recettage : horaires de connexion

7.2.5 Administrateurs locaux

Le Directeur Général a été mis administrateur local de son poste, et le service informatique l'est sur tous les postes. Les administrateurs locaux sont les seuls à pouvoir modifier l'heure et à installer des logiciels.

Test effectué	Résultat attendu	Résultat obtenu
Modifier l'heure / installer un logiciel avec un utilisateur non autorisé	Refusé	Refusé
Modifier l'heure / installer un logiciel avec le compte du DG sur son poste	Autorisé	Autorisé
Modifier l'heure / installer un logiciel avec le compte du DG sur un autre poste	Refusé	Refusé
Modifier l'heure / installer un logiciel avec le compte du service informatique sur n'importe quel poste	Autorisé	Autorisé

Tableau 26 - Recettage : administrateurs locaux



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 75/93

7.2.6 Désactivation du lecteur CD et disquettes

Test effectué	Résultat attendu	Résultat obtenu
Lecture du contenu d'un CD ou d'une disquette sur les postes de PROUITA et PROUITB pour tous les utilisateurs	Refusé	Refusé
Lecture du contenu d'un CD ou d'une disquette sur tous les postes pour les membres de PROUITA, PROUITB et SAV	Refusé	Refusé

Tableau 27 - Recettage : Désactivation médias amovibles

7.2.7 Serveur de fichiers

Test effectué	Résultat attendu	Résultat obtenu
Accès à un dossier partagé avec un user qui en a les droits	Autorisé	Autorisé
Accès à un dossier partagé avec un user qui n'a pas les droits	Refusé	Refusé

7.2.8 Quotas espace disque

Dans le cahier des charges il a été demandé de mettre en place un quota au niveau du disque. Cette opération est fastidieuse et contreproductive dans un environnement où l'arborescence est partagée en fonction du service auquel appartient l'utilisateur :

- Elle nécessite un paramétrage à chaque création et suppression d'utilisateur (cf Figure 66) car elle ne peut être configurée sur des groupes
- Elle implique que le quota est sur l'ensemble du disque, il n'y a pas de possibilité d'affiner en fonction du service (un utilisateur qui change de service verra cumuler l'espace occupé durant son précédent poste avec le nouveau)



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 76/93

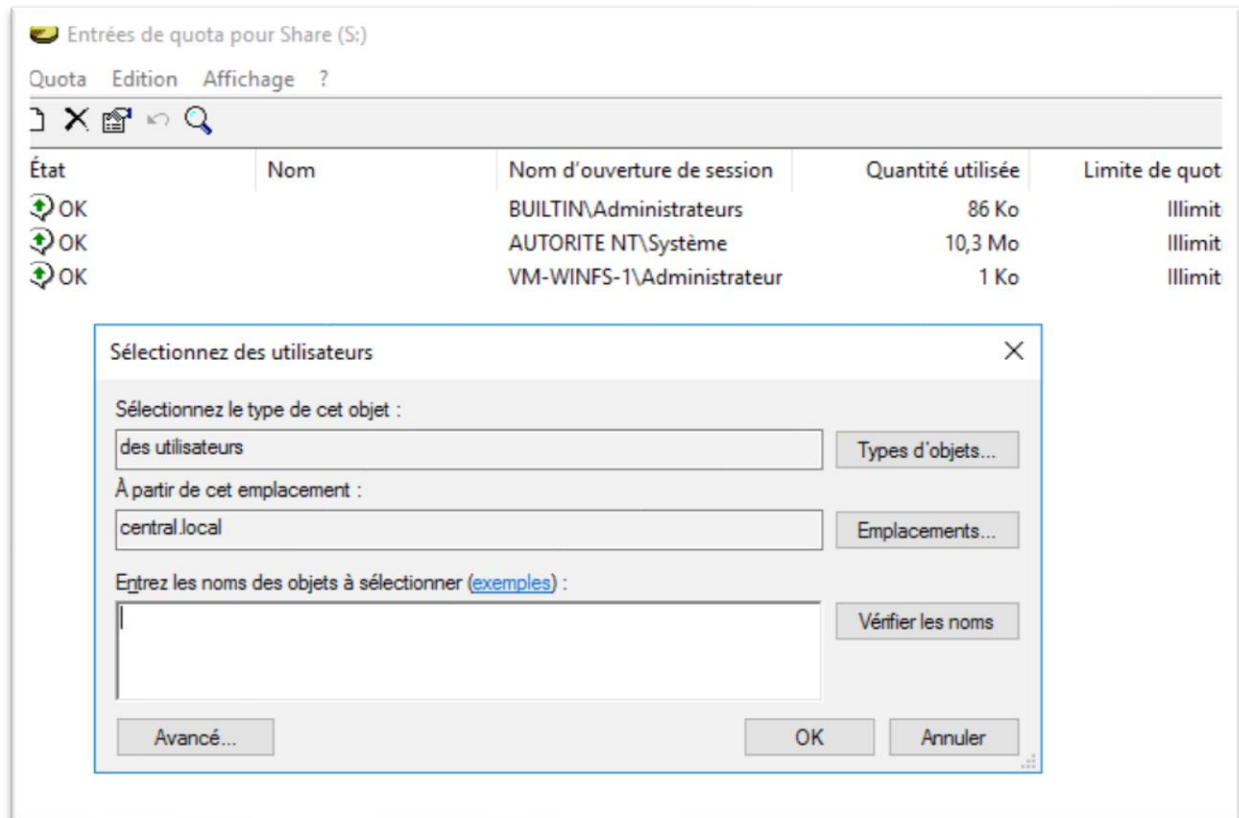


Figure 50 - Quota de disque

Si la finalité est la gestion de l'espace disque du serveur, ce que nous préconisons et avons mis en place dans notre maquette est une gestion des quotas par répertoire. Les quotas ont été mis en place depuis le gestionnaire de ressources du serveur VM-WINFS-1 sur les répertoires « CommunService » qui contiennent les dossiers de base des utilisateurs. Chaque dossier est limité à 5go. Nous pourrions ensuite attribuer un quota à chaque service en fonction de ses besoins lorsque l'arborescence sera définie.

Test effectué	Résultat attendu	Résultat obtenu
Dépassement du quota par copie d'un fichier de + de 5go	Refusé	Refusé
Copie d'un fichier de + de 4go	Avertissement (journal d'événements, mail non testé)	Avertissement (journal d'événement)

Tableau 28 - Recettage : quotas



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 77/93

7.2.9 Dossier de base utilisateur local

Test effectué	Résultat attendu	Résultat obtenu
Création automatique du dossier de base lors de son attribution	Dossier créé	Dossier créé
Droits correctement paramétrés lors de la création (lecture pour DG et modification pour service informatique)	Droits appliqués	Les droits ne s'appliquent pas comme attendu pour les utilisateurs locaux, une action supplémentaire est systématiquement nécessaire (cf Procédure de configuration en annexe, Section 25.7)
Montage du lecteur réseau lors de la connexion	Lecteur monté et accessible	Lecteur monté et accessible

Tableau 29 - Recettage : dossier de base user local

7.2.1 Dossier de base utilisateur du domaine

Test effectué	Résultat attendu	Résultat obtenu
Création automatique du dossier de base lors de son attribution	Dossier créé	Dossier créé
Droits correctement paramétrés lors de la création	Droits appliqués	Droits appliqués
Montage du lecteur réseau lors de la connexion	Lecteur monté et accessible	Lecteur monté et accessible

Tableau 30 - Recettage : dossier de base user du domaine

7.2.2 Planification d'audits

Deux audits ont été planifiés via la GPO « Computers-Audits » : les modifications apportées aux groupes, et les modifications apportées aux comptes utilisateurs.

Lorsque la GPO n'est pas appliquée, le journal d'événement ne génère rien lors de la création d'un utilisateur local :



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 78/93

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Succès de l'a...	14/09/2018 13:42:50	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:48	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:46	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:46	Microsoft Wind...	4826	Other Policy Ch...
Succès de l'a...	14/09/2018 13:42:46	Microsoft Wind...	4696	Process Creation
Succès de l'a...	14/09/2018 13:42:46	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:33	Eventlog	1100	Service en cours...

Lorsque la GPO est appliquée, les événements sont bien générés :

Mots clés	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Succès de l'a...	14/09/2018 13:51:04	Microsoft Wind...	4726	User Account Management
Succès de l'a...	14/09/2018 13:51:04	Microsoft Wind...	4729	Security Group Management
Succès de l'a...	14/09/2018 13:51:04	Microsoft Wind...	4733	Security Group Management
Succès de l'a...	14/09/2018 13:51:04	Microsoft Wind...	4798	User Account Management
Succès de l'a...	14/09/2018 13:50:41	Microsoft Wind...	4732	Security Group Management
Succès de l'a...	14/09/2018 13:50:41	Microsoft Wind...	4733	Security Group Management
Succès de l'a...	14/09/2018 13:50:41	Microsoft Wind...	4799	Security Group Management
Succès de l'a...	14/09/2018 13:50:25	Microsoft Wind...	4719	Audit Policy Change
Succès de l'a...	14/09/2018 13:50:25	Microsoft Wind...	4719	Audit Policy Change
Succès de l'a...	14/09/2018 13:42:50	Microsoft Wind...	4688	Process Creation
Succès de l'a...	14/09/2018 13:42:49	Microsoft Wind...	4688	Process Creation

Événement 4726, Microsoft Windows security auditing.

Général Détails

Un compte d'utilisateur a été supprimé.

Sujet :

ID de sécurité : CENTRAL\dg
Nom du compte : dg
Domaine du compte : CENTRAL
ID d'ouverture de session : 0x29801

Compte cible :

ID de sécurité : S-1-5-21-1669285990-3343282853-3196066304-1002
Nom du compte : test
Domaine du compte : LAP-DG-01

Informations supplémentaires :

Privileges -

Journal : Sécurité

Source : Microsoft Windows security Connecté : 14/09/2018 13:51:04

Événement : 4726 Catégorie : User Account Management

Niveau : Information Mots-clés : Succès de l'audit

Utilisateur : N/A Ordinateur : LAP-DG-01.central.local

Opcode : Informations

Informations : [Aide sur le Journal](#)



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 79/93

Test effectué	Résultat attendu	Résultat obtenu
Création / Modification / Suppression d'un compte	Evénement généré dans le journal	Evénement généré
Création / Modification / Suppression d'un groupe	Evénement généré dans le journal	Evénement généré

Tableau 31 - Recettage : planification d'audits

7.2.3 Configuration des journaux à 3 jours

Les journaux d'événements suivants ont été configurés pour conserver 3 jours de données dans la GPO « Computers-Journaux » :

- Journal de sécurité
- Journal des applications
- Journal système

Test effectué	Résultat attendu	Résultat obtenu
Vérification du journal d'événement après plus de 3 jours d'utilisation	Evénements de plus de 3 jours supprimés	Evénements de plus de 3 jours toujours présents

Tableau 32 - Recettage : journaux à 3 jours

Après recherches, il semble que cette fonctionnalité ne soit plus d'actualité sur les versions récentes de Windows. La GPO a pour effet de modifier la clé de registre suivante :

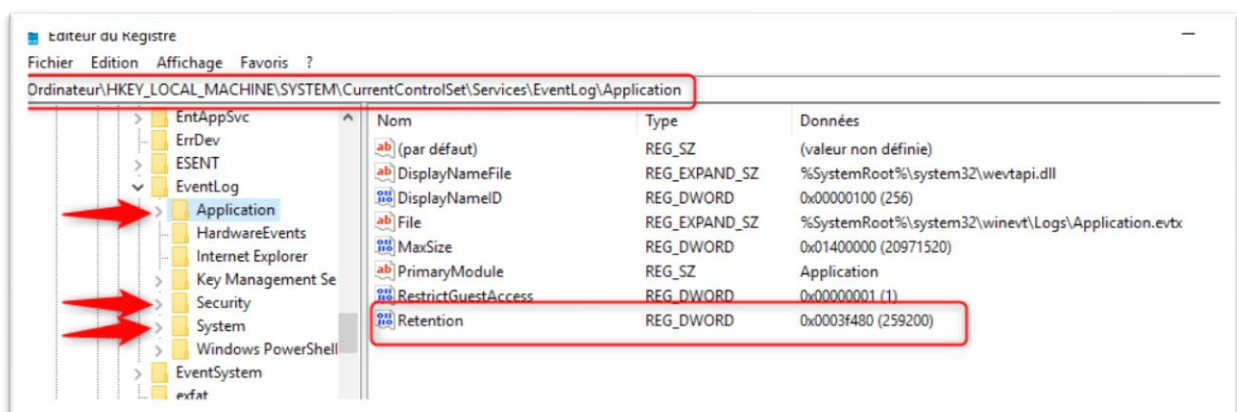


Figure 51 - Rétention journaux d'événements

La clé « Retention » contient la valeur en secondes de la durée de rétention (259200 secondes = 3 jours)

Dans la documentation Microsoft il est indiqué :



« This value is of type REG_DWORD. The default value is 0. If this value is 0, the records of events are always overwritten. **If this value is 0xFFFFFFFF or any nonzero value, records are never overwritten.** When the log file reaches its maximum size, you must clear the log manually; otherwise, new events are discarded. You must also clear the log before you can change its size. **Windows Server 2003 and Windows XP/2000:** This value is the time interval, in seconds, that records of events are protected from being overwritten. When the age of an event reaches or exceeds this value, it can be overwritten. »

L'effet de la GPO sera donc l'inverse de ce que l'on souhaite, les logs ne seront jamais écrasés. Nous préconisons à la place de laisser les options par défaut qui limitent la taille des fichiers logs à 20mo. Nous pourrions toujours modifier ce paramètre et augmenter la taille maximale si 20mo ne suffisent pas à couvrir 3 jours de logs.

7.2.4 Désactivation moniteur d'événement

La GPO « Computer-Event-Monitor » désactive le moniteur d'événement.

Test effectué	Résultat attendu	Résultat obtenu
Redémarrage serveur sans préciser l'événement	Moniteur non présent à la reconnexion	Moniteur non présent

Tableau 33 - Recettage : désactivation moniteur d'événement

7.2.5 Accès à distance

L'accès à distance se fait grâce à l'outil natif inclus dans Windows « Assistance rapide ». La GPO « Computers-Assistance » paramètre le pare-feu et gère l'autorisation d'utilisation de l'outil.

Test effectué	Résultat attendu	Résultat obtenu
Prise en main à distance	Prise en main à distance après autorisation de l'utilisateur	Prise en main à distance après autorisation de l'utilisateur

Tableau 34 - Recettage : accès à distance

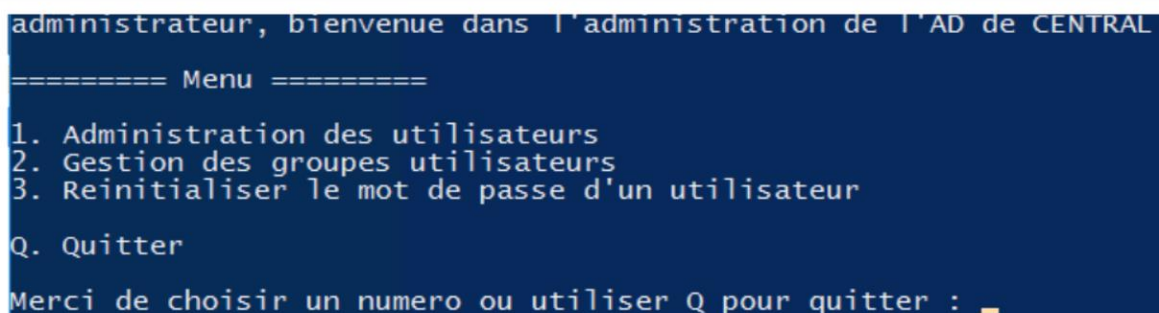
7.3 Script PowerShell³⁶ de gestion des utilisateurs AD

Dans l'optique de faciliter la gestion des utilisateurs AD, nous avons choisi de développer un script de gestion nous permettant de procéder à diverses modifications de compte fréquentes. Voici les actions prises en compte dans le script :

- Création d'un utilisateur
- Désactivation d'un utilisateur
- Recherche d'utilisateurs
- Déplacement d'un utilisateur
- Réinitialisation du mot de passe
- Ajout de groupes
- Suppression de groupes

L'objectif du script est de permettre, en plus de faciliter certaines tâches, de limiter le risque d'erreur tout en traçant dans un fichier de log les actions accomplies.

Lors du lancement du script, un premier menu apparait et propose différents choix.



```
administrateur, bienvenue dans l'administration de l'AD de CENTRAL
===== Menu =====
1. Administration des utilisateurs
2. Gestion des groupes utilisateurs
3. Reinitialiser le mot de passe d'un utilisateur
Q. Quitter
Merci de choisir un numero ou utiliser Q pour quitter : _
```

Figure 52- Menu principal

Grace à l'utilisation des numéros et de la lettre Q, il est possible de sélectionner parmi les 4 options présentées dans la capture ci-dessus.

Le premier choix propose le menu suivant :

³⁶ « PowerShell est une suite logicielle développée par Microsoft qui intègre une interface en ligne de commande, un langage de script nommé PowerShell ainsi qu'un kit de développement. [11] est le successeur des interfaces en ligne de commande DOS/Windows » Source : https://fr.wikipedia.org/wiki/Windows_PowerShell

```
Gestion des utilisateurs :  
-----  
1. Ajouter un utilisateur  
2. Rechercher un utilisateur  
3. Desactiver un utilisateur  
4. Deplacer un utilisateur  
  
R. Retour  
  
Merci de choisir un numero ou utiliser R pour revenir au menu precedent: _
```

Figure 53- Menu utilisateur

Lors de l'ajout d'un utilisateur, un générateur de mot de passe aléatoire crée le mot de passe initial de l'utilisateur.

À la suite de la création de l'utilisateur, le login et le mot de passe sont copiés automatiquement dans le presse-papier permettant de les transférer rapidement dans un email. De plus, un fichier au format .txt est créé automatiquement au nom de l'utilisateur permettant de pouvoir retrouver facilement ces informations.



Figure 54- Login et mot de passe nouvel utilisateur

Le menu des groupes utilisateurs se présente comme ceci :

```
Gestion des groupes utilisateurs :  
-----  
1. Ajouter un groupe a un utilisateur  
2. Supprimer un groupe d'un utilisateur  
  
R. Retour  
  
Merci de choisir un numero ou utiliser R pour revenir au menu precedent: _
```

Figure 55- Menu de gestion des groupes utilisateur

Il permet de facilement ajouter ou supprimer un groupe à un utilisateur grâce à une recherche des utilisateurs et à la proposition des groupes via une liste permettant de choisir le bon groupe.



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 83/93

Voici la liste des groupes :

- 0 - GS-DG
- 1 - GS-DG-Assistant
- 2 - GS-DAF-Direction
- 3 - GS-DAF-Service-Administratif
- 4 - GS-DAF-Service-Informatique
- 5 - GS-PRODUITA-Responsable
- 6 - GS-PRODUITA-Service
- 7 - GS-PRODUITB-Responsable
- 8 - GS-PRODUITB-Service
- 9 - GS-SAV-Responsable
- 10 - GS-SAV-Assistant
- 11 - GS-ALL
- 12 - GS-Linux-Admins
- 13 - GS-Ftp-Users

Sélectionner le groupe à ajouter en entrant son numero: _

Figure 56- Liste des groupes

Lors de chaque action, avant d'exécuter la commande une vérification est proposée via une fonction permettant de choisir oui (o) ou non (n).

Les informations sont-elles correctes ? (o / n) : _

Figure 57- Fonction de validation

La fonctionnalité de log vient renseigner dans un fichier .txt chaque action effectuée en écrivant la date, l'heure, le login de l'utilisateur ayant fait l'action et l'action effectuée.

```
20/09/2018 22:06:24 // administrateur => L'utilisateur test.test a bien ete ajoute au groupe GS-PRODUITA-Service
21/09/2018 19:14:04 // administrateur => Ajout de l'utilisateur Nom : Test1 / Prenom : Test1 / Login : test1.test1 /
```

Figure 58- Logs



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 84/93

Test effectué	Résultats attendu	Résultats obtenus
Ajout d'utilisateur	Oui	Oui
Recherche d'utilisateur	Oui	Oui
Désactivation d'utilisateur	Oui	Oui
Déplacement d'utilisateur	Oui	Oui
Réinitialisation de mot de passe	Oui	Oui
Ajout de groupe	Oui	Oui
Suppression de groupe	Oui	Oui
Fonctionnalités de logs	Oui	Oui

Tableau 35 - Recettage : script administration AD

Le script d'administration des utilisateurs AD n'en est qu'à une première version qui sera améliorée et enrichie en fonctionnalité

Certaines des fonctionnalités présentes, même si fonctionnelles, peuvent encore être grandement améliorée afin de correspondre aux critères de qualité que nous nous fixons et aux besoins identifiés à l'usage.

Le but est d'obtenir à terme une gestion intégrale des actions courantes effectuées sur les comptes utilisateurs afin d'obtenir des logs de chaque action mais aussi de permettre de mieux les cadrer afin de limiter le risque d'erreur humaine.

7.3.1 Script de sauvegarde

Dans le cahier des charges il a été demandé de sauvegarder les ressources des serveurs Windows vers un partage NFS sous linux. Dans l'infrastructure proposée, le serveur linux est dans le cluster Hyper-V, les données de production et les sauvegardes sont sur NAS. Il n'est pas pertinent de procéder comme l'exige le cahier des charges, néanmoins nous avons réalisé un script afin de montrer que cela reste possible.

Les hôtes Hyperv n'ont pas de client NFS, le script doit donc être exécuté dans une VM Windows Server avec les outils RSAT installés et un droit d'accès sur le partage NFS.



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 85/93

Test effectué	Résultat attendu	Résultat obtenu
Sauvegarde automatisée d'une VM à l'aide du script « backup-vm.ps1 »	VM Sauvegardée sur le partage NFS, logs correctement générés	VM Sauvegardée sur le partage NFS, logs correctement générés

Tableau 36 - Recettage : script de sauvegarde sur NFS

7.4 Serveurs Linux

Afin de profiter de la centralisation de la gestion des utilisateurs et de leurs habilitations sous Active Directory, nous avons intégré le serveur Linux au domaine et paramétré son mode d'authentification afin de pouvoir gérer les utilisateurs depuis Active Directory. La gestion se fait grâce à Kerberos³⁷, SSSD³⁸ et PAM³⁹. Un groupe « GS-Linux-Admins » a été créé pour accorder des droits d'administrateur sur le serveur (connexion en SSH et intégration aux Sudoers »

Test effectué	Résultat attendu	Résultat obtenu
Insertion dans le domaine	Machine intégrée dans AD et DNS	Machine intégrée dans AD et DNS
Connexion SSH avec un utilisateur autorisé	Utilisateur connecté au système	Utilisateur connecté au système
Connexion SSH avec un utilisateur non autorisé	Utilisateur rejeté	Utilisateur rejeté

Tableau 37 - Recettage : linux - gestion des users depuis l'AD

³⁷ Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. (source : Wikipedia)

³⁸ Le démon System Security Services est un logiciel développé à l'origine pour le système d'exploitation Linux qui fournit un ensemble de démons pour gérer l'accès aux répertoires distants et aux mécanismes d'authentification. Les débuts de SSSD se trouvent dans un projet open source appelé FreeIPA. (source : Wikipedia)

³⁹ Pluggable Authentication Modules : PAM est une création de Sun Microsystems et est supporté en 2006 sur les architectures Solaris, Linux, FreeBSD, NetBSD, AIX et HP-UX. L'administrateur système peut alors définir une stratégie d'authentification sans devoir recompiler des programmes d'authentification. (source : Wikipedia)



7.4.1 Samba Server

Le serveur Linux permet de partager des ressources avec des machines Windows. L'authentification se fait grâce à Active Directory.

Test effectué	Résultat attendu	Résultat obtenu
Accès à une ressource autorisée pour l'utilisateur	Ressource accessible	Ressource accessible
Accès à une ressource interdite pour l'utilisateur	Ressource inaccessible	Ressource inaccessible

Tableau 38 - Recettage : samba server

7.4.2 Serveur NFS

Pour le serveur NFS, la gestion des autorisations se fait grâce à l'adresse ip ou au nom d'hôte.

Test effectué	Résultat attendu	Résultat obtenu
Accès à une ressource autorisée pour la machine	Ressource accessible	Ressource accessible
Accès à une ressource interdite pour la machine	Ressource inaccessible	Ressource inaccessible

Tableau 39 - Recettage : serveur NFS

7.4.3 Serveur FTP

Le serveur VSFTP a été configuré avec un cryptage SSL. L'authentification est gérée grâce à Active Directory. Un groupe « GS-FTP-Users » a été créé pour permettre l'accès au serveur. Les administrateurs ont un accès étendu à tout le système de fichiers grâce au paramétrage du « chroot »



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 87/93

Test effectué	Résultat attendu	Résultat obtenu
Accès avec un utilisateur autorisé	Serveur accessible, limité au dossier home	Serveur accessible, limité au dossier home
Accès avec un utilisateur non autorisé	Serveur inaccessible	Serveur inaccessible
Accès anonyme	Serveur accessible, limité à son dossier	Serveur accessible, limité à son dossier
Accès administrateur	Serveur entièrement accessible	Serveur entièrement accessible

Tableau 40 - Recettage : serveur FTP



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 88/93

7.4.4 Application Web

		Administrateur		Utilisateur	
		Résultats attendu	Résultats obtenus	Résultats attendu	Résultats obtenus
Connexion		Oui	Oui	Oui	Oui
Recherche		Oui	Oui	Oui	Oui
Créer	Ordinateur	Oui	Oui	Non	Non
	Utilisateur	Oui	Oui	Non	Non
	Ecran	Oui	Oui	Non	Non
	Imprimante	Oui	Oui	Non	Non
	Local	Oui	Oui	Non	Non
Lire	Ordinateur	Oui	Oui	Oui	Oui
	Utilisateur	Oui	Oui	Oui	Oui
	Ecran	Oui	Oui	Oui	Oui
	Imprimante	Oui	Oui	Oui	Oui
	Local	Oui	Oui	Oui	Oui
Modifier	Ordinateur	Oui	Oui	Non	Non
	Utilisateur	Oui	Oui	Non	Non
	Ecran	Oui	Oui	Non	Non
	Imprimante	Oui	Oui	Non	Non
	Local	Oui	Oui	Non	Non
Supprimer	Ordinateur	Oui	Oui	Non	Non
	Utilisateur	Oui	Oui	Non	Non
	Ecran	Oui	Oui	Non	Non
	Imprimante	Oui	Oui	Non	Non
	Local	Oui	Oui	Non	Non

Tableau 41 - Recettage : application gestion de parc



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 89/93

7.5 Tolérance de panne

Le basculement entre NAS n'a pas pu être testé car nous avons besoin du matériel pour ce faire.

Test effectué	Résultat attendu	Résultat obtenu
Eteindre un hôte Hyper-V	Basculement automatique des VM du cluster sur le second hôte (serveur de fichiers et serveur linux)	Basculement des VM du cluster sur le second hôte
Eteindre un contrôleur de domaine	Fonctionnalités AD, DNS et DHCP maintenues par le second DC	Fonctionnalités AD, DNS et DHCP maintenues par le second DC

Tableau 42 - Recettage : tolérance de panne

8 Table des illustrations et tableaux

Figure 1 - Mind Map	8
Figure 2 – Schéma Virtualisation	11
Figure 3 – Schéma Clustering	13
Figure 4 - Exemple d'arborescence des répertoires de travail.....	18
Figure 5 - Infographie : conséquences d'une perte de données	19
Figure 6 - Politique de sauvegarde	24
Figure 7 - Licences CAL utilisateur	27
Figure 8 - Licences CAL périphériques.....	27
Figure 9- Organisation de l'AD	29
Figure 10 – Schéma infrastructure	36
Figure 11 - Liste des serveurs	37
Figure 12- Table des utilisateurs	43
Figure 13- Relation entre la table utilisateur et la table ordinateur.....	44
Figure 14- MCD	45
Figure 15- Table des utilisateurs	46
Figure 16- Table de relation imprimante/ordinateur	46
Figure 17- MLD.....	47
Figure 18- Page de connexion.....	48
Figure 19- Page d'accueil et vue des données	48
Figure 20- Attribut administrateur	49
Figure 21- Droits administrateurs lors de la connexion.....	49
Figure 22- Droits administrateur lors de la suppression d'un ordinateur.....	50
Figure 23- Bouton pour ajouter un local.....	50
Figure 24- Formulaire d'ajout d'un local.....	51
Figure 25- Navbar.....	51
Figure 26- Extrait du tableau des ordinateurs.....	52
Figure 27- Modification dans le tableau	52
Figure 28- Menu déroulant de modification dans le tableau	53
Figure 29- Boîte de dialogue de confirmation de modification	53
Figure 30- Bouton de suppression.....	54
Figure 31- Boîte de dialogue de confirmation de suppression	54
Figure 32- Barre de recherche.....	54
Figure 33- Filtrage du tableau.....	55
Figure 34- Page de connexion.....	55
Figure 35- Page d'accueil	55
Figure 36- Page de consultation des utilisateurs	56
Figure 37- PowerEdge R740	57
Figure 38- Schéma licences	59



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 91/93

Figure 39- RackStation RS818+	60
Figure 40- DS218	61
Figure 41- EATON 5P 1550IR	63
Figure 42 - Schéma réseau	65
Figure 43 - Zones DNS.....	67
Figure 44 - Liste des imprimantes	68
Figure 45 - Restriction horaire impression	69
Figure 46 - Priorité d'impression.....	70
Figure 47 - Contrôle total impressions service informatique	71
Figure 48 - GPO impression au service informatique	72
Figure 49 - Planificateur de tâches : fermeture de session forcée.....	74
Figure 50 - Quota de disque	76
Figure 51 - Rétention journaux d'événements	79
Figure 52- Menu principal	81
Figure 53- Menu utilisateur	82
Figure 54- Login et mot de passe nouvel utilisateur	82
Figure 55- Menu de gestion des groupes utilisateur.....	82
Figure 56- Liste des groupes	83
Figure 57- Fonction de validation	83
Figure 58- Logs	83

Tableau 1 - Comparaison HyperV / VmWare	14
Tableau 2 - Comparaison NAS / Serveur de fichiers	16
Tableau 3 - Comparaison types de sauvegardes	20
Tableau 4 - Comparaison supports de sauvegarde.....	21
Tableau 5 - Comparaison supports de sauvegarde.....	22
Tableau 6 - Comparaison éditions Windows Server.....	25
Tableau 7 - Comparaison licences Windows Server	26
Tableau 8 - Comparaison distributions Linux.....	31
Tableau 9 - ACL réseau.....	33
Tableau 10 - Plan d'adressage général	33
Tableau 11 - Plan d'adressage VLAN EXT.....	33
Tableau 12 - Plan d'adressage VLAN STORAGE	34
Tableau 13 - Plan d'adressage VLAN HEARTBEAT	34
Tableau 14 - Plan d'adressage VLAN MGMT	34
Tableau 15 - Plan d'adressage VLAN SERVICE	35
Tableau 16 - Plan d'adressage VLAN LAN.....	35
Tableau 17 - Caractéristiques serveurs	58
Tableau 18 - Chiffrage licences	59
Tableau 19 - Caractéristiques NAS	60



PROJET EVOLUTION

Etude de faisabilité

Omar AIT-MOULID /
Julien VILLARD
Date : 21/09/2018
V.05
Page : 92/93

Tableau 20 - Chiffrage global	63
Tableau 21 - Recettage : ACL Réseau	66
Tableau 22 - Recettage : DNS	67
Tableau 23 - Recettage : complexité des mots de passe	68
Tableau 24 - Recettage : Logs - Script restrictions horaires	73
Tableau 25 - Recettage : horaires de connexion	74
Tableau 26 - Recettage : administrateurs locaux	74
Tableau 27 - Recettage : Désactivation médias amovibles	75
Tableau 28 - Recettage : quotas	76
Tableau 29 - Recettage : dossier de base user local	77
Tableau 30 - Recettage : dossier de base user du domaine	77
Tableau 31 - Recettage : planification d'audits	79
Tableau 32 - Recettage : journaux à 3 jours	79
Tableau 33 - Recettage : désactivation moniteur d'événement	80
Tableau 34 - Recettage : accès à distance	80
Tableau 35 - Recettage : script administration AD	84
Tableau 36 - Recettage : script de sauvegarde sur NFS	85
Tableau 37 - Recettage : linux - gestion des users depuis l'AD	85
Tableau 38 - Recettage : samba server	86
Tableau 39 - Recettage : serveur NFS	86
Tableau 40 - Recettage : serveur FTP	87
Tableau 41 - Recettage : application gestion de parc	88
Tableau 42 - Recettage : tolérance de panne	89