

# CURRICULUM VITAE

TOVONAY Sily Soa**Faniry**

24 ans Célibataire

034 50 820 54

faniry.tovonay@gmail.com

Antanifotsy V Andrainjato Fianarantsoa



## Formations et Diplômes

---

- 2018** : Deuxième année de formation en Master Professionnel à l'Ecole Nationale d'Informatique, Université de Fianarantsoa  
**Parcours :** Informatique Générale
- 2017** : Première année de formation en Master Professionnel à l'Ecole Nationale d'Informatique, Université de Fianarantsoa  
**Parcours :** Informatique Générale
- 2016** : Obtention du diplôme Licence Professionnelle en Informatique de l'Ecole Nationale d'Informatique, Université de Fianarantsoa  
**Parcours :** Informatique Générale
- 2015** : Troisième année de formation en Licence Professionnelle à l'Ecole Nationale d'Informatique, Université de Fianarantsoa  
**Parcours :** Informatique Générale  
**Diplôme :** Licence Professionnelle
- 2014** : Deuxième année de formation en Licence Professionnelle à l'Ecole Nationale d'Informatique, Université de Fianarantsoa  
**Parcours :** Informatique Générale
- 2013** : Première année de formation en Licence Professionnelle à l'Ecole Nationale d'Informatique, Université de Fianarantsoa  
**Parcours :** Informatique Générale
- 2012** : Baccalauréat Série « D », Lycée privé La Providence Tuléar

## Stages et Expériences Professionnels

---

- 2018-2019** : Stage au sein de la Société Groupe AXIAN Antananarivo  
**Thème :** « Déploiement et Implémentation d'une Solution de Sauvegarde Réseau ET Serveur VPN ».  
**Durée :** Six (06) mois
- 2018** : . Reporting Database sous Oracle Business Intelligence Publisher
  - Projet sur VoIP/ToIP
  - Projet OpenStack : Fonctionnement, installation et configuration
  - Gestion des notes en Python Flask avec Triggers
  - Gestion de réservation de place en Train sous Android

- 2017** : • Application mobile : Gestion de note soutenance sous Android :  
                   • Création d'un système embarqué avec une application Domotique  
                        Maison sous Raspberry Pi 3  
                   • Application Java socket  
                   • Gestion de projet  
                   • Ingénierie de besoin : « Cahier de charge fonctionnelle »  
                   • Développement d'une application interactive d'un site e-commerce
- 2016-2017** : Stage au sein de la Direction Général du Trésor Antaninarenina Antananarivo  
Thème : « Mise en place MPLS VPN et un system de continuité de service VRRP ».  
Durée : Trois (03) mois
- 2016** : Routage :  
                   • RIP, OSPF et MPLS  
                   • Application :  
                        Gestion étudiante : En Java Applet, Java avec Framework, JSP  
                        Windows server :  
                        • Domaine Contrôleur Active Directory et le système de nom de domaine  
                        • Dynamic Host Configuration Protocol  
                        • Serveur de Déploiement Windows  
                        • Connexion à distance au serveur depuis un client
- 2015-2016** : Stage au sein de la Faculté des Science Université Fianarantsoa  
Thème : « Mise en place d'un serveur VPN et d'un serveur d'authentification OpenLDAP »  
Durée : Trois (03) mois
- 2015** : Création d'une application web :  
                   • Gestion de Prestation Médecine  
                   • Site web du Centre Hospitalier Universitaire Andrainjato
- 2014-2015** : Montage et mise en place du réseau local informatique du Centre Hospitalier Universitaire Andrainjato  
                        Création d'une application bureau : Gestion de Réservation de Place en Avion avec QtCreator  
                        Création d'une application bureau : Gestion de Réservation de Place en Avion avec QtCreator

## Compétences en informatique

---

- Système** : • Windows  
                        ✓ Windows Serveur : Serveur 2008, Serveur 2012  
                        ✓ Windows : XP SP2 et SP3, 7, 8 et 10  
                   • GNU/Linux : Debian, Ubuntu, LinuxMint, Kali Linux  
                   • RedHat : CentOs  
                   • Ios Routeur : Cisco, Mikrotik
- Bureautique** : • Word, Excel, PowerPoint, Internet  
                   • Installation et configuration :  
                        ✓ Des systèmes Windows et GNU/Linux  
                        ✓ Des logiciels Windows et GNU/Linux  
                   • Montage et démontage des matériels informatiques

- Réseaux et Sécurité :**
- TCP/IP LAN/WAN, VPN, DNS, DHCP, LDAP
  - Load Balacing : VRRP, HSRP
  - MPLS, QoS
  - VPN : OpenVPN, IPSec
  - GSM, USSID
  - Système CLOUD
  - VoIP/ToIP, Asterisk, OpenIms
  - Firewall
    - ✓ Iptables, PfSense
  - Routage : RIP, OSPF, MP-BGP

### Génie Logiciel et Base de données :

- Programmation
  - ✓ Langage C, C++, C#, Visual Basic, JAVA, JSP, ASP.Net
- Script
  - ✓ Shell, Python
- Système de Gestion de Base de Données : MySQL, ORACLE, PostgreSQL
- Technologie Web
  - ✓ HTML5, CSS3, JavaScript, Ajax, PHP, Java
  - ✓ Applet, Java Socket
- Framework
  - ✓ Symphony, CodeIgniter, Flask
- Méthode de conception
  - ✓ UML et MERISE II, Méthode AGILE

### Connaissances linguistiques

---

	Lire	Ecrire	Parler
Français	1	2	2
Anglais	2	2	2
Espagnol	3	3	3

Grille d'évaluation : 1 : Très bien 2 : Bien 3 : Assez-bien

### Diverses connaissances et club

---

- Interaction homme-machine, Intelligence artificielle, Comptabilité générale, Organisation et Marketing
- Membre du club Linux au sein de l'ENI Fianarantsoa
- Membre du club d'Entraide de l'ENI Fianarantsoa
- Membre du club Multimédia de l'ENI Fianarantsoa

### Loisirs

---

Lecture, Musique, Jeux PC, Football, Basket-ball

# DEDICACE

« Que le sage écoute, il augmentera son savoir, et celui qui est intelligent acquerra de l'habileté.  
Ecoute, mon fils, l'instruction de ton père et ne rejette pas l'enseignement de ta mère ».  
Proverbes 1 : 5 et 8.

Je dédie ce mémoire :

A mon feu père TOVOSOA, décédé trop tôt, qui m'a toujours poussé et motivé  
dans mes études : l'éducation que j'ai reçue de lui est un bien précieux. Puisse  
Dieu, Le Tout Puissant, l'avoir en Sa Sainte Miséricorde !

A ma mère LALAO Solomampianina, pour son amour, son soutien, pour toute  
son assistance, sa présence dans ma vie, tous les sacrifices consentis et ses  
précieux conseils qu'elle ne cesse de me prodiguer !

A mes tantes et oncles, particulièrement à Tatie Hangy, qui a aussi œuvré pour  
ma réussite, de par son amour, son aide, et sa bénéfique influence, reçois à travers  
ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle  
gratitude !

A ma famille, à mes frères et sœurs qui n'ont cessé d'être pour moi des modèles  
de persévérance, de courage et de générosité !

A mes professeurs qui verront dans ce travail la fierté d'un savoir bien acquis !

A mes amis et amies, à tous mes camarades de promotion, de par le monde, qui  
n'ont cessé de m'encourager.

A toutes et à tous, trouvez ici l'expression de ma profonde gratitude et  
reconnaissance !

# REMERCIEMENTS

En premier lieu, nous tenons tout d'abord à rendre grâce à notre Seigneur Dieu, Le Très Haut Tout Puissant, qui nous a donné le temps, le courage, la force, la santé, le savoir et la connaissance, et nous a bénis à tout moment. Nous voulons également adresser nos remerciements aux personnes qui nous ont apporté leur aide et qui ont pris part à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire, tout particulièrement à :

- Professeur RAMAMONJISOA Bertin Olivier, Directeur de l'Ecole Nationale d'Informatique, non seulement pour son exonération de droits afin d'effectuer ce stage mais aussi pour les aides et les conseils qu'il a apportés.
- Docteur RAKOTOASIMBAHOAKA Cyprien Robert, Responsable de Parcours « Informatique Générale » de l'Ecole Nationale d'Informatique, pour son aide précieuse tout au long de notre année universitaire.
- Monsieur RAZAFINDRANDRIATSIMANIRY Marie Dieudonné Michel, pour avoir accepté de bien vouloir nous encadrer pédagogiquement et pour nous avoir beaucoup aidés durant ce travail.
- Monsieur FOCK LAW Denis, Chef de Pôle Exploitation, pour nous avoir accueillis en stage et aussi pour sa générosité et pour la grande patience dont il a fait preuve malgré ses charges académiques et professionnelles ; il a en outre accepté de bien vouloir nous encadrer professionnellement durant notre stage et n'a pas hésité à nous consacrer du temps et à partager son savoir-faire.
- Messieurs les membres du jury : le Président et l'Examinateur.
- Tout le personnel du Pôle Exploitation et du Groupe AXIAN pour leur aide et leur collaboration.
- Tous les membres du corps enseignant de l'Ecole Nationale d'Informatique pour les connaissances et les savoirs dont ils nous ont laissés hériter au sein de l'établissement.

Et enfin, nous ne pouvons ignorer notre famille qui a fait preuve d'amour, et qui nous a épaulés par son aide indispensable et par son soutien moral. Nous n'oublions pas non plus nos amis et condisciples qui n'ont pas hésité à nous rendre service.

A vous tous, nous adressons notre reconnaissance la plus sincère !

Merci infiniment !

# SOMMAIRE

CURRICULUM VITAE .....	I
DEDICACE .....	IV
REMERCIEMENTS .....	V
SOMMAIRE .....	VI
NOMENCLATURE .....	VII
LISTE DES TABLEAUX .....	IX
LISTES DES FIGURE.....	X
INTRODUCTION GENERALE .....	1
PARTIE I : PRESENTATION GENERALE.....	1
Chapitre 1 : Présentation de L'ENI .....	2
Chapitre 2 : Présentation du Groupe Axian .....	13
Chapitre 3 : Description du Stage.....	19
PARTIE II : GENERALITE ET ANALYSE .....	23
Chapitre 4 : Généralités sur La Sauvegarde et Le VPN.....	24
Chapitre 5 : Analyse Préalable.....	32
PARTIE III : CHOIX DE L'OUTIL.....	44
Chapitre 6 : Comparaison des outils .....	44
Chapitre 7 : Présentation de l'Outil Choisi .....	54
PARTIE IV : MISE EN OEUVRE ET VALIDATION .....	75
Chapitre 8 : Réalisation .....	74
Chapitre 9 : Validation et Perspective.....	107
CONCLUSION GENERALE .....	114
REFERENCES BIBLIOGRAPHIQUES .....	115
REFERENCES WEBOGRAPHIQUES.....	115
GLOSSAIRE.....	116
ANNEXE .....	117
TABLES DES MATIERES .....	XIII
R E S U M E .....	XVIII
ABSTRACT .....	XVIIIVIII

# NOMENCLATURE

AD	: Active Directory
AES	: Advanced Encryption Standard
AITS	: Axian Information Technology Services
API	: Application Program Interface
AWS	: Amazon Web Services
CD	: Compact Disc
CPU	: Central Processing Unit
CRAM	: Challenge-Response Authentication Mechanism
CVE	: Common Vulnerabilities and Exposures
DH	: Diffie-Hellman
DHCP	: Dynamic Host Configuration Protocol
DNS	: Domain Name Server/Service
DSI	: Direction des Systèmes d'Information
DVD	: Digital Video Disc
EDM	: Electronique De Madagascar
ENI	: Ecole Nationale d'Informatique
ESP	: Encapsulating Security Payload
FTP/FTPS	: File Transfer Protocol / File Transfer Protocol SFTP
GNU	: GNU's Not UNIX
GPL	: General Public License
HDD	: Hard Disk Drive
HOTP/TOTP	: HMAC-based One Time Password/ Time-based One-time Password
HSM	: Hardware Security Module
HTTP/HTTPS	: Hyper Text Transfer Protocol/ Secure Hyper Text Transfer Protocol
IP	: Internet Protocol
IPSec	: Internet Protocol Security
IPv4	: Internet Protocol Version 4
L2TP	: Layer 2 Tunneling Protocol
LAN	: Local Area Network
LDAP	: Lightweight Directory Access Protocol
LMD	: Licence Master Doctorat
MD5	: Message Digest Version 5
NAT	: Network Address Translation
PAM	: Pluggable Authentication Module
PHP	: PHP Hypertext Preprocessor (Personal Home Page)

PPP	: Point-to-Point Protocol
PPTP	: Point-to-point Tunneling Protocol
RAM	: Random Access Memory
RHEL	: RedHat Entreprise Linux
RSA	: Rivest Shamir Adleman
SE	: Système d'Exploitation
SFTP	: Secured File Transfer Protocol
SHA-1	: Secure Hash Algorithm
SMB	: Server Message Block
SQL	: Structured query language
SSH	: Secure Shell
SSL	: Secure Socket Layer
SSO	: Single Sign On
SSII	: Société de Services en Ingénierie Informatique
TCP	: Transmission Control Protocol
TIC	: Technologies de l'Information et de la Communication
TLS	: Transport Layer Security
TOM	: Towerco Of Madagascar
UDP	: User Datagram Protocol
USB	: Universal Serial Bus
VDC	: Virtual Data Center
VLAN	: Virtual Local Area Network
VPC	: Virtual Private Cloud
VPN	: Virtual Private network
WLAN	: Wired Local Area Network

# LISTE DES TABLEAUX

Tableau 1 :	Organisation du système de formation pédagogique .....	5
Tableau 2 :	Architecture des études correspondant au système LMD .....	6
Tableau 3 :	Liste des formations .....	6
Tableau 4 :	Liste des formations existantes à l'ENI .....	11
Tableau 5 :	Moyens matériels .....	20
Tableau 6 :	Chronogramme de stage .....	22
Tableau 7 :	Types de réseaux existant au sein de la société .....	34
Tableau 8 :	Type d'accès à internet .....	34
Tableau 9 :	Type des matériaux d'interconnexion .....	35
Tableau 10 :	Postes de travail .....	36
Tableau 11 :	Serveurs .....	36
Tableau 12 :	Passerelle .....	37
Tableau 13 :	Logiciel de monitoring .....	38
Tableau 14 :	Comparaison des outils de sauvegarde (I) .....	48
Tableau 15 :	Comparaison des outils de sauvegarde (II) .....	49

# LISTES DES FIGURE

Figure 1 :	Organigramme de l'ENI .....	4
Figure 2 :	Historique du Groupe Axian .....	14
Figure 3 :	Implantations de Groupe Axian Entreprise .....	17
Figure 4 :	Activités du Groupe Axian .....	17
Figure 5 :	Organigramme d'Axian It Service .....	18
Figure 6 :	Topologie de Site-to-Site VPN .....	30
Figure 7 :	Topologie de VPN Client-Serveur .....	30
Figure 8 :	Topologie réseau d'AITS .....	33
Figure 9 :	Analyse du trafic réseau I .....	40
Figure 10 :	Analyse du trafic réseau II .....	40
Figure 11 :	Graphe de l'analyse du trafic réseau I .....	41
Figure 12 :	Graphe de l'analyse du trafic réseau II .....	41
Figure 13 :	Architecture du logiciel .....	57
Figure 14 :	Dashboard Bacula .....	67
Figure 15 :	Contenu du fichier MariaDB.repo .....	75
Figure 16 :	Statut MariaDB serveur .....	75
Figure 17 :	Sécurisation de MariaDB .....	76
Figure 18 :	Vérification connexion MariaDB .....	77
Figure 19 :	Contenu du fichier webmin.repo .....	78
Figure 20 :	Message de sortie d'installation Webmin .....	78
Figure 21 :	Bacula-Web dans le serveur .....	79
Figure 22 :	Affichage de bacula.repo .....	80
Figure 23 :	Etape de configuration de base de données .....	82
Figure 24 :	Page d'authentification Webmin .....	83
Figure 25 :	Tableau de bord Webmin .....	83
Figure 26 :	Choix du Bacula Backup System .....	84
Figure 27 :	Page de navigation du « Bacula backup System » .....	84
Figure 28 :	Storage Device .....	85
Figure 29 :	Ajout d'un nouveau « Storage Device » .....	85
Figure 30 :	Champ à remplir du « Storage Device » .....	85
Figure 31 :	Stockage « Storage Device » créée .....	86
Figure 32 :	Storage Daemons .....	86
Figure 33 :	Champ à remplir du « Storage Daemon » .....	86
Figure 34 :	Stockage « Storage daemon » créée .....	86
Figure 35 :	Volume Pools .....	87
Figure 36 :	Champ à remplir du « Volume Pool » .....	87

Figure 37 :	Volume « Volume Pool » créée .....	87
Figure 38 :	Backup Schedules .....	87
Figure 39 :	Champ à remplir du « Backup Schedule » .....	88
Figure 40 :	Schedule « Backup Schedule » créée .....	88
Figure 41 :	FileSets.....	88
Figure 42 :	Champ à remplir du « FileSet » .....	88
Figure 43 :	FileSet créée .....	89
Figure 44 :	Backup Clients .....	89
Figure 45 :	Champ à remplir du « Backup Client » .....	89
Figure 46 :	Client « Backup Client » créé .....	89
Figure 47 :	Backup Job.....	90
Figure 48 :	Backup Job créé.....	90
Figure 49 :	Modification fuseau horaire.....	91
Figure 50 :	Configuration « bacula-fd » Director.....	92
Figure 51 :	Configuration « bacula-fd » FileDaemon.....	92
Figure 52 :	Installation Bacula Client.....	93
Figure 53 :	Configuration fichier Bacula client .....	93
Figure 54 :	Redémarrage du service fichier bacula client .....	94
Figure 55 :	Ouverture du port 9102 étape 1 .....	94
Figure 56 :	Ouverture du port 9102 étape 2 .....	94
Figure 57 :	Spécification du programme bacula.....	94
Figure 58 :	Contenu de « mongodb.repo » .....	95
Figure 59 :	Contenu de « pritunl.repo » .....	96
Figure 60 :	Valeur de SELinux .....	96
Figure 61 :	Page de configuration initiale de Pritunl.....	98
Figure 62 :	Page de connexion de Pritunl.....	98
Figure 63 :	Tableau de bord Pritunl.....	99
Figure 64 :	Architecture VPN Client/serveur.....	99
Figure 65 :	Ajout d'une organisation .....	99
Figure 66 :	Organisation bien créée .....	100
Figure 67 :	Création d'un utilisateur .....	100
Figure 68 :	Utilisateur bien créé .....	100
Figure 69 :	Création du serveur.....	101
Figure 70 :	Serveur bien créé .....	101
Figure 71 :	Attachement de l'organisation au serveur.....	101
Figure 72 :	Serveur bien démarrée.....	102
Figure 73 :	Ajout d'une route .....	102
Figure 74 :	Téléchargement du profil.....	103
Figure 75 :	Liens de profil .....	103
Figure 76 :	Démarrage d'installation Pritunl Client.....	104

Figure 77 :	Installation Pritunl Client .....	105
Figure 78 :	Démarrage installation OpenVPN Client .....	105
Figure 79 :	Composantes d'OpenVPN à installer .....	106
Figure 80 :	Installation OpenVPN Client Complète .....	106
Figure 81 :	Architecture Serveur de sauvegarde .....	107
Figure 82 :	Redémarrage du service Bacula .....	107
Figure 83 :	Etape de lancement d'une sauvegarde .....	108
Figure 84 :	Donnée à sauvegarder .....	108
Figure 85 :	Lancement de la sauvegarde .....	108
Figure 86 :	Sauvegarde réussie .....	108
Figure 87 :	Données compressées dans le serveur .....	109
Figure 88 :	Etapes de lancement d'une restauration .....	109
Figure 89 :	Commencement de la restauration .....	110
Figure 90 :	Restauration réussie .....	110
Figure 91 :	Vérification des données restaurées .....	110
Figure 92 :	Importation et connexion du profil VPN .....	111
Figure 93 :	Connexion au serveur VPN Pritunl réussi .....	111
Figure 94 :	Saisie des informations de connexion au VPN .....	112
Figure 95 :	Connexion vers le serveur .....	112
Figure 96 :	Connexion réussie .....	113
Figure 97 :	Saisie d'adresse et port du serveur d'accès à distance .....	113
Figure 98 :	Accès au serveur Bacula réussi .....	113
Figure 99 :	Connexion et accès « root » réussi .....	113

# INTRODUCTION GENERALE

Aujourd’hui, l’informatique est devenue indispensable dans beaucoup de domaines. La saisie des données sur support informatique facilite le stockage, l’archivage et le transport des données. Pour éviter la perte de données, la sauvegarde est une solution indispensable. Selon les critères et l’usage, nous avons le choix entre différentes solutions de sauvegarde.

Certaines solutions sont gratuites, d’autres payantes. Les techniques de sauvegarde les plus efficaces sont celles qui stockent les données loin de la source originale. Dans ce genre de sauvegarde, une connexion est établie avec un serveur distant sur lequel les données sont copiées, c’est ce qu’on appelle la sauvegarde réseau. Les données sont souvent répliquées ce qui permet d’augmenter le niveau de sécurité. Aujourd’hui le volume de données stockées devient de plus en plus important.

Les entreprises doivent désormais faire face à un nombre croissant d’utilisateurs, de clients que ce soit des concessionnaires, télétravailleurs ou autres, mais aussi avoir des sites ou serveurs distants qui ont besoin d’accès privés, où qu’elles résident les données et quelle que soit la méthode pour les récupérer, les entreprises ont besoin d’une connexion sécurisée, fiable et étanche grâce à des solutions privées.

De ce fait, nous nous posons la question de savoir quelle technologie il faut choisir pour la sauvegarde réseau et les accès privés ?

Le présent mémoire est organisé en quatre parties structurées en chapitres. La première partie traite de la « Présentation générale de l’Ecole Nationale d’Informatique et de l’établissement d’accueil ». La seconde partie s’intitule « Généralité et Analyse », la troisième aborde le « Choix de l’outil » et la dernière repose sur la « Mise en Œuvre et Validation »

# PARTIE I : PRESENTATION GENERALE

# Chapitre 1 : Présentation de L'ENI

## 1.1 Informations d'ordre général

L'Ecole Nationale d'Informatique, en abrégé ENI, est un établissement d'enseignement supérieur rattaché académiquement et administrativement à l'Université de Fianarantsoa.

Le siège de l'ENI se trouve à Tanambao- Antaninarenina à Fianarantsoa.

L'adresse pour la prise de contact est la suivante :

Ecole Nationale d'Informatique Tanambao, Fianarantsoa. Le numéro de sa boîte postale est 1487 avec le code postal 301. Téléphone : 020 75 508 01. Son adresse électronique est : *eni@univ-fianar.mg*. Site Web : [www.eni@univ-fianar.mg/eni](http://www.eni@univ-fianar.mg/eni)

## 1.2 Missions et historique

L'ENI se positionne sur l'échiquier socio-éducatif malgache comme étant le plus puissant vecteur de diffusion et de vulgarisation des connaissances et des technologies informatiques.

Cette école supérieure peut être considérée aujourd'hui comme la vitrine et la pépinière des élites informaticiennes du pays.

L'ENI s'est constituée de façon progressive au sein du Centre Universitaire Régional (CUR) de Fianarantsoa.

De façon formelle, l'ENI a été constituée et créée au sein du CUR par le décret N° 83-185 du 24 Mai 1983, comme étant le seul établissement universitaire professionnalisé au niveau national, destiné à former des techniciens et des ingénieurs de haut niveau, aptes à répondre aux besoins et exigences d'informatisation des entreprises, des sociétés et des organes implantés à Madagascar.

L'ENI a, par conséquent, pour mission de former des spécialistes informaticiens compétents et opérationnels surtout de différents niveaux :

- En fournissant à des étudiants des connaissances de base en informatique ;
- En leur transmettant le savoir-faire requis, à travers la professionnalisation des formations dispensées et en essayant une meilleure adéquation des formations par rapport aux besoins évolutifs des sociétés et des entreprises.
- En initiant les étudiants aux activités de recherche dans les différents domaines des Technologies de l'Information et de la Communication (TIC).

L'implantation de cette école supérieure de technologie de pointe dans un pays en voie de développement et dans une province (ou Faritany) à faible tissu économique et industriel ne lui a pourtant pas porté préjudice, ni ne l'a empêchée de former des spécialistes informaticiens d'excellent niveau, recherchés par les entreprises, les sociétés et les organismes publics et privés sur le marché de l'emploi.

La filière de formation d'analystes programmeurs a été mise en place à l'ENI en 1983 mais a été gelée par la suite en 1996, tandis que celle de formation d'ingénieurs a été ouverte en 1986.

Dans le cadre du Programme de Renforcement de l'Enseignement Supérieur (PRESUP), la filière de formation des techniciens supérieurs en maintenance des systèmes des informatiques a été mise en place en 1986 grâce à l'appui matériel et financier de la Mission Française de Coopération auprès de l'Ambassade de France à Madagascar.

Une formation pour l'obtention de la certification CCNA et / ou NETWORK + appelée « CISCO Networking Academy » a été créée à l'ENI en 2002-2003 grâce au partenariat avec CISCO SYSTEM et l'Ecole Supérieure Polytechnique d'Antananarivo (ESPA). Cependant, cette formation n'avait pas duré longtemps.

Une formation de troisième cycle a été ouverte à l'ENI l'année 2003 – 2004 grâce à la coopération académique et scientifique entre l'Université de Fianarantsoa pour le compte de l'ENI et l'Université Paul Sabatier de Toulouse (UPST).

Cette filière avait pour objectif de former certains étudiants à la recherche dans les différents domaines de l'Informatique, et notamment pour préparer la relève des enseignants-chercheurs qui étaient en poste.

Pendant l'année 2007-2008, la formation en vue de l'obtention du diplôme de Licence Professionnelle en Informatique a été mise en place à l'ENI avec les deux options suivantes de formation :

- Génie Logiciel et base de Données.
- Administration des Système et Réseaux.

La mise en place à l'Ecole de ces deux options de formation devait répondre au besoin de basculement vers le système Licence – Master – Doctorat (LMD).

Mais la filière de formation des Techniciens Supérieurs en Maintenance des Systèmes Informatiques a été gelée en 2009.

En vue de résoudre les difficultés de limitation des effectifs étudiants accueillis à l'ENI, notamment à cause du manque d'infrastructures, un système de « Formation Hybride » a été mis en place à partir de l'année 2010. Il s'agit en effet d'un système de formation semi-présentielle et à distance avec l'utilisation de visioconférences.

Le système de formation hybride a été ainsi créé à Fianarantsoa ainsi qu'à Université de Toliara.

En ce moment, la formation appelée Hybride est devenue Formation Informatique Générale.

### **1.3 Organigramme institutionnel de l'ENI**

L'organigramme de l'ENI est inspiré des dispositions du décret N° 83-185 du 23 Mai 1983.

L'ENI est administrée par un Conseil d'Ecole, et dirigée par un directeur nommé par un décret adopté en conseil des Ministres.

Le Collège des enseignants regroupant tous les enseignants-chercheurs de l'Ecole est chargé de résoudre les problèmes liés à l'organisation pédagogique des enseignements ainsi qu'à l'élaboration des emplois du temps.

Le Conseil Scientifique propose les orientations pédagogiques et scientifiques de l'établissement, en tenant notamment compte de l'évolution du marché de travail et de l'adéquation des formations dispensées par rapport aux besoins des entreprises.

Trois départements de formation caractérisent l'organigramme :

- Le département de formation théorique ;
- Le département de formation pratique pour la coordination et la supervision des stages en entreprise et des voyages d'études ;
- Le département de formation doctorale pour l'organisation de la formation de 3ème cycle.

La figure 1 présente l'organigramme actuel de l'ENI.

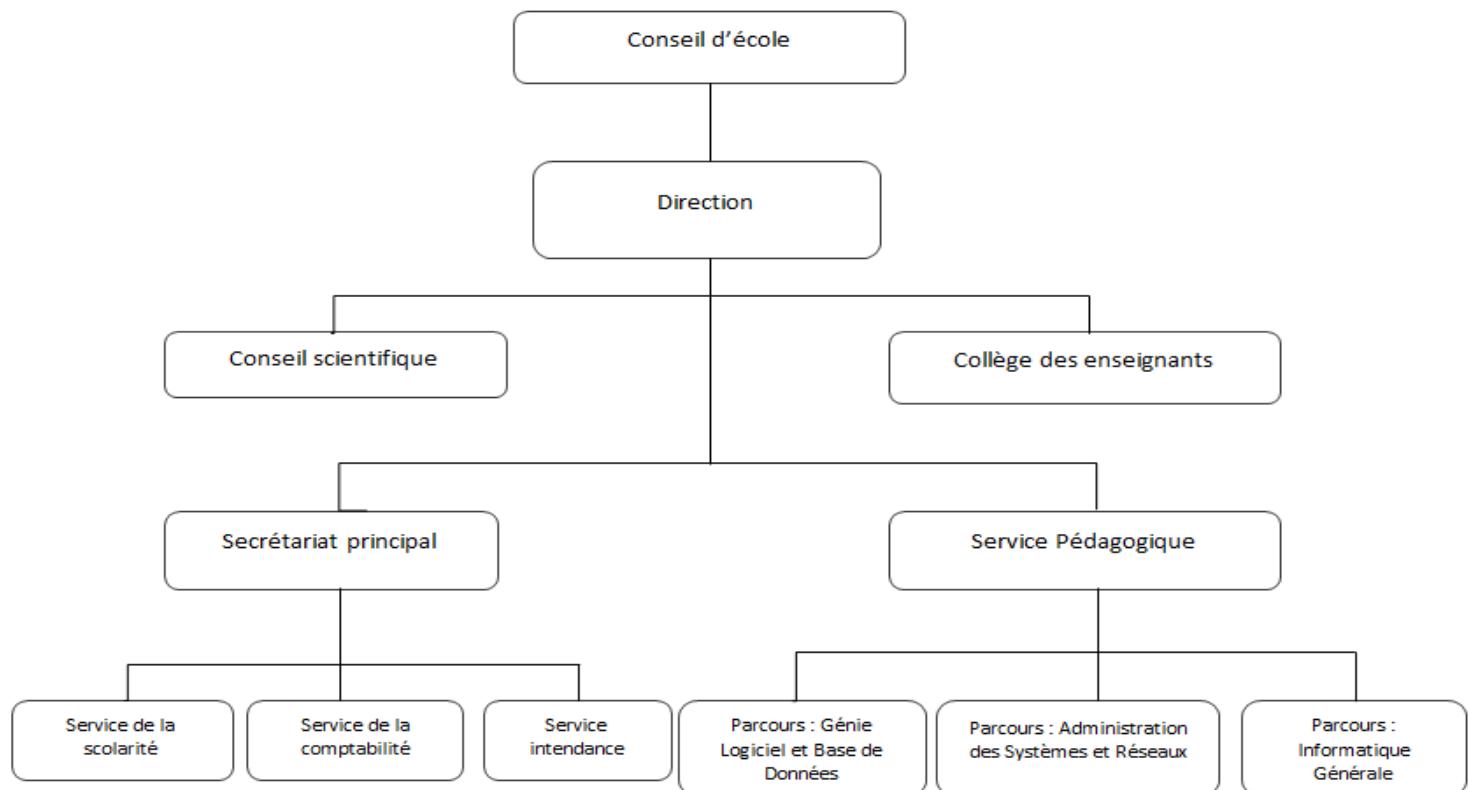


Figure 1 : Organigramme de l'ENI

Sur cet organigramme, l'ENI placée sous la tutelle académique et administrative de l'Université de Fianarantsoa est dirigée par un directeur élu par les enseignants – chercheurs permanents de l'Etablissement et nommé par un décret validé en Conseil des ministres pour un mandat de 3 ans.

Le Conseil de l'Ecole est l'organe délibérant de l'ENI.

Le Collège des enseignants propose et coordonne les programmes d'activités pédagogiques.

Le Conseil scientifique coordonne les programmes de recherche à mettre en œuvre à l'Ecole.

Le Secrétariat principal coordonne les activités des services administratifs (Scolarité, Comptabilité, et Intendance).

Conformément aux textes en vigueur régissant les Etablissements malgaches d'Enseignement Supérieur, qui sont barrés sur le système LMD, les Départements de Formation pédagogique ont été ainsi remplacés par des mentions et des parcours. Et les chefs des Départements ont été ainsi remplacés par des responsables des mentions et des responsables des parcours.

Un administrateur des Réseaux et Systèmes gère le système d'information de l'Ecole et celui de l'Université.

## 1.4 Domaines de spécialisation

Les activités de formation et de recherche organisées à l'ENI portent sur les domaines suivants :

- Génie logiciel et Base de Données ;
- Administration des Systèmes et Réseaux ;
- Informatique Générale
- Modélisation informatique et mathématique des Systèmes complexes.

D'une manière plus générale, les programmes des formations sont basés sur l'Informatique de gestion et sur l'Informatique des Systèmes et Réseaux. Et les modules de formation intègrent aussi bien des éléments d'Informatique fondamentale que des éléments d'Informatique appliquée.

Le tableau 1 décrit l'organisation du système de formation pédagogique de l'ENI.

Tableau 1 : Organisation du système de formation pédagogique

Formation théorique	Formation pratique
- Enseignement théorique - Travaux dirigés - Travaux pratiques	- Etudes de cas - Travaux de réalisation - Projets / Projets tutorés - Voyages d'études - Stages

## 1.5 Architecture des formations pédagogiques

Le recrutement des étudiants à l'ENI se fait uniquement par voie de concours national pour entrer en première année.

Les offres de formation organisées à l'ENI ont été validées par la Commission Nationale d'Habilitation (CNH) auprès du Ministère de l'Enseignement Supérieur et de la Recherche Scientifique selon les dispositions de l'Arrêté N°31.174/2012-MENS en date du 05 Décembre 2012.

Au sein de l'ENI, il existe une seule mention (INFORMATIQUE) et trois parcours :

- Génie logiciel et Base de Données ;
- Administration des Systèmes et Réseaux ;
- Informatique Générale

L'architecture des études à trois niveaux conformes au système Licence-Master-Doctorat (LMD) permet les comparaisons et les équivalences académiques des diplômes au niveau international.

- L = Licence (Bac + 3) = L1, L2, L3 = 6 semestres S1 à S6
- M = Master (Bac + 5) = M1, M2 = 4 semestres S7 à S10

Le diplôme de Licence est obtenu en 3 années d'études après le Baccalauréat. Et le diplôme de Master en deux ans après celui de LICENCE.

Le MASTER PROFESSIONNEL est un diplôme destiné à la recherche d'un emploi au terme des études.

Le MASTER RECHERCHE est un diplôme qui remplace l'ancien Diplôme d'Etudes Approfondies (DEA), et qui permet de s'inscrire directement dans une école doctorale à la fin des études.

- D = Doctorat (Bac +8)

Le Doctorat est un diplôme qu'on peut obtenir en 3 ans après l'obtention du celui de MASTER RECHERCHE.

Le tableau 2 présente l'architecture des études correspondant au système LMD.

Tableau 2 : Architecture des études correspondant au système LMD



DTS : Diplôme de Technicien Supérieur

BTS : Brevet de Technicien Supérieur

DUT : Diplôme Universitaire de Technicien

La Licence peut avoir vocation générale ou professionnelle.

De même, le Master peut avoir vocation professionnelle ou de recherche.

Le tableau 3 ci-après décrit les listes des formations existantes à L'ENI

Tableau 3 : Liste des formations

FORMATION EN		
	LICENCE PROFESSIONNELLE ET INFOMATIQUE GENERALE	MASTER
Condition d'admission	Par voie de concours Formation Professionnelle : 100 candidats Informatique Générale : 150 candidats	
Condition d'accès	Bac de série C, D ou Technique	Etre titulaire de licence professionnelle
Durée de formation	3 années	2 années
Diplôme à délivrer	Diplôme de Licence Professionnelle en Informatique	Diplôme de Master Professionnel Diplôme de Master Recherche

L'entrée en première année de MASTER se fait automatiquement pour les étudiants de l'ENI qui ont obtenu le diplôme de Licence Professionnelle.

Le Master Recherche permet à son titulaire de poursuivre directement des études en doctorat et de s'inscrire directement dans une école doctorale.

Les écoles doctorales jouissent d'une autonomie de gestion par rapport aux établissements de formation universitaire.

Il convient de signaler que par arrêté ministériel N° 21.626/2012 – MESupRES publié le 9 Août 2012 par la Commission Nationale d'habilitation (CNH), l'école doctorale « Modélisation – Informatique » a été habilitée pour l'Université de Fianarantsoa.

Depuis l'année universitaire 2010-2011, l'ENI s'est mise à organiser des formations hybrides en informatique dans les différentes régions (Fianarantsoa, Toliara) en raison de l'insuffisance de la capacité d'accueil des infrastructures logistiques. En effet, le système de formation hybride semi - présentielle utilise des visioconférences pour la formation à distance.

Bien qu'il n'existe pas encore au niveau international de reconnaissance écrite et formelle des diplômes délivrés par l'ENI, ses étudiants diplômés sont plutôt bien accueillis dans les instituts universitaires étrangères (CANADA, Suisse, France...)

## **1.6 Relations de l'ENI avec les entreprises et les organismes**

Les stages effectués chaque année par les étudiants favorisent le développement permanent des relations entre l'ENI et plus de 300 entreprises et organismes publics, semi-publics et privés, nationaux et internationaux.

Elle dispose ainsi d'un réseau d'entreprises, de sociétés et d'organismes publics et privés qui sont des partenaires pour ses étudiants en quête de stage avec éventuellement un recrutement après l'obtention de leurs diplômes.

Les compétences que l'ENI permet d'acquérir aux étudiants sont l'adaptabilité, le sens de la responsabilité, du travail en équipe, le goût de l'expérimentation et l'innovation.

En effet, sa vocation est de former des techniciens supérieurs de niveau LICENCE et des ingénieurs généralistes de niveau MASTER avec des qualités scientifiques, techniques et humaines reconnues, capables d'évoluer professionnellement dans des secteurs d'activité variés intégrant l'informatique.

Les stages en milieu professionnel contribuent à une meilleure adéquation entre les formations à l'ENI et les besoins évolutifs du marché de l'emploi.

Les principaux débouchés professionnels pour les diplômés de l'Ecole concernent les domaines suivants :

- ✓ L'informatique de gestion d'entreprise
- ✓ Les technologies de l'information et de la communication (TIC)
- ✓ La sécurité informatique des réseaux
- ✓ L'administration des réseaux et des systèmes
- ✓ Les services bancaires et financiers, notamment le Mobile Banking
- ✓ Les télécommunications et la téléphonie mobile
- ✓ Les Big Data
- ✓ Le commerce, la vente et l'achat, le Marketing
- ✓ L'ingénierie informatique appliquée
- ✓ L'écologie et le développement durable

Parmi les sociétés, entreprises et organismes partenaires de l'Ecole, on peut citer : ACCENTURE Mauritius, Air Madagascar, Ambre Associates, Airtel, Agence Universitaire de la Francophonie ( AUF) , B2B, Banque Centrale, BFG-SG, BIANCO, BLUELINE, Bureau national de gestion des Risques et des catastrophes (BNGRC), CEDII-Fianarantsoa, Data Consulting, Central Test, Centre National Antiacridien, CNRE, CHU, CNRIT, COLAS, Direction Générale des Douanes, DLC, DTS/Moov, FID, FTM, GNOSYS, IBONIA, INGENOSIA, INSTAT, IOGA, JIRAMA, JOUVE, MADADEV, MAEP, MEF, MEN, MESupRES, MFB, MIC, MNINTER, Min des postes/Télécommunications et du Développement Numérique, NEOV MAD, Ny Havana, Madagascar National Parks, OMNITEC, ORANGE, OTME, PRACCESS, QMM Fort-Dauphin, SMMC, SNEDADRS Antsirabe, Sénat, Société d'Exploitation du Port de Toamasina (SEPT), SOFTWELL, Strategy Consulting, TELMA, VIVETEC, Société LAZAN'I BETSILEO, WWF ...

Les stages en entreprise aident non seulement à renforcer la professionnalisation des formations dispensées au sein de l'ENI, mais surtout à multiplier les opportunités d'embauche pour ses diplômés.

## 1.7 Partenariat au niveau international

Entre 1996 et 1999, l'ENI a bénéficié de l'assistance technique et financière de la Mission Française de Coopération et d'Action Culturelle dans le cadre du Programme de Renforcement de l'Enseignement Supérieur (PRESUP) consacré à l'ENI, lequel a notamment consisté à :

- Une dotation en logiciels, micro-ordinateurs, équipements de laboratoire de maintenance et de matériels didactiques
- La réactualisation des programmes de formation assortie du renouvellement du fonds de la bibliothèque
- L'appui à la formation des formateurs
- L'affectation à l'Ecole d'assistants techniques français

De 2000 à 2004, l'ENI a fait partie des membres du bureau de la Conférence internationale des écoles de formation d'Ingénieurs et Techniciens d'Expression Française (CITEF).

Les enseignants-chercheurs de l'ENI participent régulièrement aux activités organisées dans le cadre du Colloque Africain sur la Recherche en Informatique (CARI).

L'ENI a également signé un accord de coopération inter-universitaire avec l'Institut de Recherche en Mathématiques et Informatique Appliquées (IREMIA) de l'Université de la Réunion, l'Université de Rennes 1, l'INSA de Rennes et l'Institut National Polytechnique de Grenoble (INPG).

A partir du mois de Juillet 2001, l'ENI est devenu le Centre de Réseau Opérationnel (Network Operating Center) du point d'accès à Internet de l'Ecole ainsi que de l'Université de Fianarantsoa. Grâce à ce projet américain qui a été financé par l'USAID Madagascar, l'ENI et l'Université de Fianarantsoa ont été dotées d'une ligne spécialisée d'accès permanent au réseau Internet.

L'ENI a de même noué des relations de coopération avec l'Institut de Recherche pour le Développement (IRD).

L'objet du projet de coopération a porté sur la modélisation environnementale du Corridor forestier de Fandriana jusqu'à Vondrozo (COFAV). Dans ce cadre, un atelier scientifique international a été organisé à l'ENI en Septembre 2008. Cet atelier scientifique a eu pour thème la modélisation des paysages.

A l'occasion du programme scientifique PARRUR, l'IRD a financé depuis 2010 le projet intitulé « Forêts, Parcs et Pauvreté dans le Sud de Madagascar (FPPSM). Des étudiants en DEA et des doctorants issus de l'ENI ont participé à ce Programme.

Par ailleurs, dès l'année 2010, l'ENI de Fianarantsoa a été sélectionnée pour faire partie des organismes partenaires de l'Université de Savoie dans le cadre du projet TICEVAL relatif à la certification des compétences en TIC.

Le projet TICEVAL a été financé, de 2010 à 2012, par le Fonds Francophone des Inforoutes, et il a eu pour objectif de généraliser la certification des compétences en Informatique et Internet du type C2i2e et C2imi.

Lors du projet TICEVAL, une convention de coopération avec l'Université de Savoie a été signée par les deux parties concernées. La mise en œuvre de la Convention de Coopération a permis d'envoyer des étudiants de l'ENI à Chambéry pour poursuivre des études supérieures en Informatique.

Pour finir par l'un des partenariats majeurs, l'ENI a signé en Septembre 2009 un protocole de collaboration scientifique avec l'ESIROI – STIM de l'Université de la Réunion.

Comme l'ENI est un vivier de technologie de pointe, d'emplois et d'entreprises, elle peut très bien servir d'instrument efficace pour renforcer la croissance économique du pays et pour lutter contre la pauvreté.

Notons aussi que le statut de l'ENI permettrait de renforcer la position concurrentielle de la Grande Ile sur l'orbite de la modélisation grâce au développement des nouvelles technologies.

## **1.8 Débouchés professionnels des diplômes**

Le chômage des jeunes diplômés universitaires fait partie des maux qui gangrènent Madagascar. Le contexte socio-politique du pays, depuis 2008, a révélé que le chômage massif sévit parmi les diplômés des établissements d'enseignement supérieur.

Toutefois, les formations proposées par l'ENI permettent à ses diplômés, dotés de toutes les connaissances nécessaires à leur métier, d'être immédiatement opérationnels sur le marché du travail.

L'ENI apporte à ses étudiants un savoir-faire et un savoir-être qui les accompagnent tout au long de leur vie professionnelle. Elle a une vocation professionnalisante.

Les diplômés en LICENCE et en MASTER de l'ENI peuvent faire carrière dans de différents secteurs.

Elle bénéficie aujourd'hui de 34 années d'expériences pédagogiques et de reconnaissance auprès des sociétés, des entreprises et des organismes. C'est une école supérieure de référence en matière informatique.

Par conséquent, en raison du fait que l'équipe pédagogique de l'ENI est expérimentée, les enseignants-chercheurs et les autres formateurs sont dotés d'une grande expérience dans l'enseignement et dans le milieu professionnel.

L'ENI est fière de collaborer de façon régulière avec un nombre croissant d'entreprises, de sociétés et d'organismes publics et privés à travers les stages des étudiants. Les formations dispensées sont ainsi orientées vers le besoin et les attentes des entreprises et des sociétés.

Elle fournit à ses étudiants de niveau LICENCE et MASTER des compétences professionnelles et indispensables pour les intégrer sur le marché du travail.

L'ENI s'efforce de proposer à ses étudiants une double compétence à la fois technologique et managériale combinant l'informatique de gestion ainsi que l'administration des réseaux et systèmes.

D'une manière générale, les diplômés de l'ENI n'éprouvent pas de difficultés particulières à être recrutés au terme de leurs études. Cependant, l'ENI recommande à ses diplômés de promouvoir l'entrepreneuriat en TIC et de créer des cybercafés, des SSII ou des bureaux d'études.

Le tableau 4 représente les débouchés professionnels éventuels des diplômes

Tableau 4 : Liste des formations existantes à l'ENI

LICENCE	<ul style="list-style-type: none"><li>- Analyste</li><li>- Programmeur</li><li>- Administrateur de site web/de portail web</li><li>- Assistant Informatique et internet</li><li>- Chef de projet web ou multimédia</li><li>- Développeur Informatique ou multimédia</li><li>- Intégrateur web ou web designer</li><li>- Hot liner/Hébergeur Internet</li><li>- Agent de référencement</li><li>- Technicien/Supérieur de help desk sur Informatique</li><li>- Responsable de sécurité web</li><li>- Administrateur de réseau</li><li>- Administrateur de cybercafé</li></ul>
MASTER	<ul style="list-style-type: none"><li>- Administrateur de cybercafé</li><li>- Administrateur de réseau et système</li><li>- Architecture de système d'information</li><li>- Développeur d'application /web /java/Python/ IOS /Android</li><li>- Ingénieur réseau</li><li>- Webmaster /web designer</li><li>- Concepteur Réalisateur d'applications</li><li>- Directeur du système de formation</li><li>- Directeur de projet informatique</li><li>- Chef de projet informatique</li><li>- Responsable de sécurité informatique</li><li>- Consultant fonctionnel ou freelance</li><li>- Administrateur de cybercafé</li></ul>

## **1.9 Ressources Humaines**

- Directeur de l'ENI : Professeur RAMAMONJISOA Bertin Olivier
- Responsable de Mention : Docteur MAHATODY Thomas
- Responsable de Parcours « Génie Logiciel et Base de Données » : Docteur RATIARSON Venot
- Responsable de Parcours « Administration Systèmes et Réseaux » : Monsieur SIAKA
- Responsable de Parcours « Informatique Générale » : Docteur RAKOTOASIMBAHOAKA Cyprien Robert
- Nombre d'Enseignants permanents : 13 dont deux (02) Professeurs Titulaires, six (06) Maîtres de Conférences et cinq (05) Assistants d'Assistants d'Enseignement Supérieur et de Recherche
- Nombre d'Enseignants vacataires : 10
- Personnel Administratif : 23

# Chapitre 2 : Présentation du Groupe Axian

## 2.1 Présentation générale du groupe Axian

Axian est un groupe avec une identité forte, qui rassemble des entreprises dynamiques à la réputation reconnue dans la région, conscient du formidable potentiel que représentent Madagascar et les îles de l'Océan indien, Axian a décidé d'investir sur le long terme et d'agir avec efficacité dans les infrastructures et services structurants pour le pays et la région. Énergie, télécoms, services financiers, immobilier, Axian intervient dans les secteurs qui jouent un rôle moteur dans le développement industriel, économique et social, la croissance et le prestige de Madagascar.

## 2.2 Historiques

Axian appartient à la famille Hiridjee, famille française, forte de ses valeurs, d'origine indienne, établie à Madagascar depuis cent cinquante ans forts de ses valeurs. Elle développe, à l'origine, son activité dans l'industrie textile. Fondé sur un management familial, Axian exerce son activité en tant que société de gestion de l'ensemble des actifs et participations détenus par la famille Hiridjee à Madagascar et dans l'Océan indien, dont il définit et conduit la stratégie industrielle, pilote le développement et assure la gestion opérationnelle. Il compte quatre actionnaires : Raza Aly, Bashir, Amin et Hassanein Hiridjee.

### CHIFFRES CLÉS :

- 630 M\$ de chiffre d'affaires globales en 2017
- Un investisseur de premier plan avec 800 M\$ investis dans ses opérations
- Plus de 4 000 salariés, dans l'Océan Indien
- 1 500 collaborateurs formés en 2015
- 50 000 heures de formation au total
- Un portefeuille de sociétés performantes
- N°1 dans les télécoms de l'Océan indien, avec Telma,
- N°1 dans la distribution de produits pétroliers à Madagascar, avec Jovena
- 1er opérateur de mobile money dans l'Océan indien
- 300 000 m<sup>2</sup> de surface immobilière bâtie

En 2018, La société Groupe Axian a acheté NETAPSYS qui est devenu maintenant AITS.

Le groupe Hiridjee est actif dans des activités de télécommunications avec Telma à Madagascar, TRM à La Réunion et Mayotte, Telco-Comores et Towerco à Madagascar. Le groupe opère également dans l'immobilier avec First IMMO, l'énergie avec Jovena et Electricité de Madagascar et enfin la banque avec BNI Madagascar. Désormais toutes ces activités sont rassemblées dans Axian la nouvelle dénomination du groupe familial. Axian est détenu conjointement par Raza-Aly, Bashir, Amin et Hassanein Hiridjee. Par ailleurs, les activités du groupe dans la distribution à travers Ocean Trade et Continental Auto et l'agroalimentaire avec HavaMad sont désormais rassemblées dans Viseo, intégralement repris par Moustafa Hiridjee. L'historique de la société est présenté dans la figure 2.

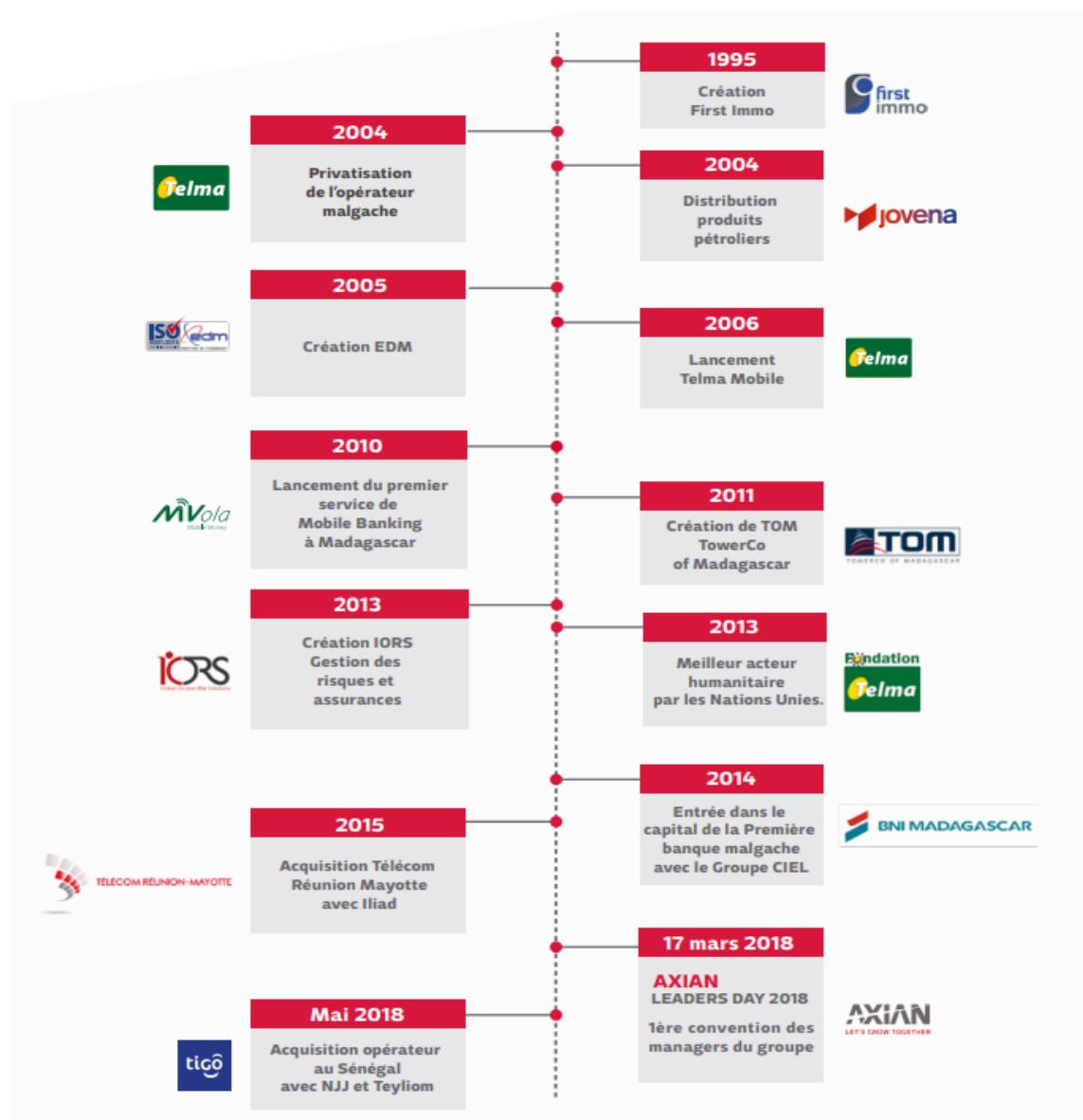


Figure 2 : Historique du Groupe Axian

## **2.3 Visions**

Imaginons et réalisons ensemble un modèle inspirant et impactant, créateur de valeurs et de développement équitable pour Madagascar, notre région et le continent.

- POUR LE PROGRÈS : participer au développement économique et humain
- POUR AVANCER : donner le meilleur de nous-mêmes et nous surpasser
- POUR RAYONNER : étendre nos activités et notre réputation au-delà de nos régions d'intervention

## **2.4 Engagement du groupe**

### **2.4.1 Axian, acteur économique responsable et engagé**

Axian est un opérateur résolument pragmatique qui sait que le développement et le rayonnement du pays passent par une nouvelle approche qui privilégie la performance, la qualité et la responsabilité des orientations et des actions mises en place.

### **2.4.2 Un investissement dans les talents**

Les réussites affichées par ses différentes filiales, Axian les doit également aux nombreux talents qu'elles ont recrutés et formés. Une dynamique d'emploi qui fait du groupe l'un des plus gros recruteurs du pays.

Depuis 2005, plus de 2 000 personnes ont été recrutées portant le nombre total de salariés à plus de 4 000. En 2015, près de 1 500 personnes ont bénéficié d'une formation, pour un équivalent de près de 50 000 heures de formation.

### **2.4.3 Un engagement sociétal fort**

La Fondation Telma intervient dans sept domaines :

- La santé,
- L'aide humanitaire,
- L'éducation,
- Les nouvelles technologies,
- L'aide à l'enfance et à la jeunesse,
- L'environnement
- Le développement durable.

Elle s'appuie notamment sur l'essor des technologies de Telma pour favoriser le développement du pays et améliorer les conditions de vie des populations. Depuis 2011, la Fondation est impliquée aux côtés des autorités malgaches dans la Gestion des Risques et des Catastrophes (GRC). Désignée « Meilleur acteur humanitaire », elle est choisie par les Nations unies en 2014 pour représenter le secteur privé de l'Afrique de l'est et australie au premier sommet

humanitaire mondial. En mai 2016, la Fondation a représenté la plateforme humanitaire du secteur privé, première initiative privée de ce genre au niveau mondial, lors du sommet qui s'est tenu à Istanbul, en Turquie, en mai 2016. La fondation Telma a également comme priorité la construction d'écoles : elle a lancé un programme de construction de 100 nouveaux établissements scolaires à travers tout le pays.

## 2.5 Implantations

A la fois la plus grande et la plus peuplée de l'Océan indien, l'île de Madagascar a naturellement vocation à être une locomotive de développement régional. La région de l'Océan indien bénéficie d'un potentiel immense. Avec un taux de croissance moyen d'environ 4%, des économies principalement portées par les services, une position stratégique au carrefour des continents, 10 aéroports internationaux et régionaux, une population totale de plus de 30 millions d'habitants, jeune et éduquée, les îles de l'Océan indien constituent un véritable bassin d'opportunités.

C'est donc tout naturellement qu'Axian se développe dans la région. En plus de Madagascar, avec Telma, TOM, Jovena, EDM, First IMMO et BNI, le groupe est désormais implanté dans 3 îles : à La Réunion et à Mayotte, où il vient de racheter la branche mobile d'Outremer Telecom (Only) et de créer la société Télécom Réunion Mayotte (TRM) ; aux Comores, où il a remporté l'attribution d'une licence mobile et créé la société Telco SA, illustré dans la figure 3.



Figure 3 : Implantations de Groupe Axian Entreprise

## 2.6 Activités

Axian c'est 15 entreprises œuvrant dans 4 secteurs différents, illuminé sur la figure 4.

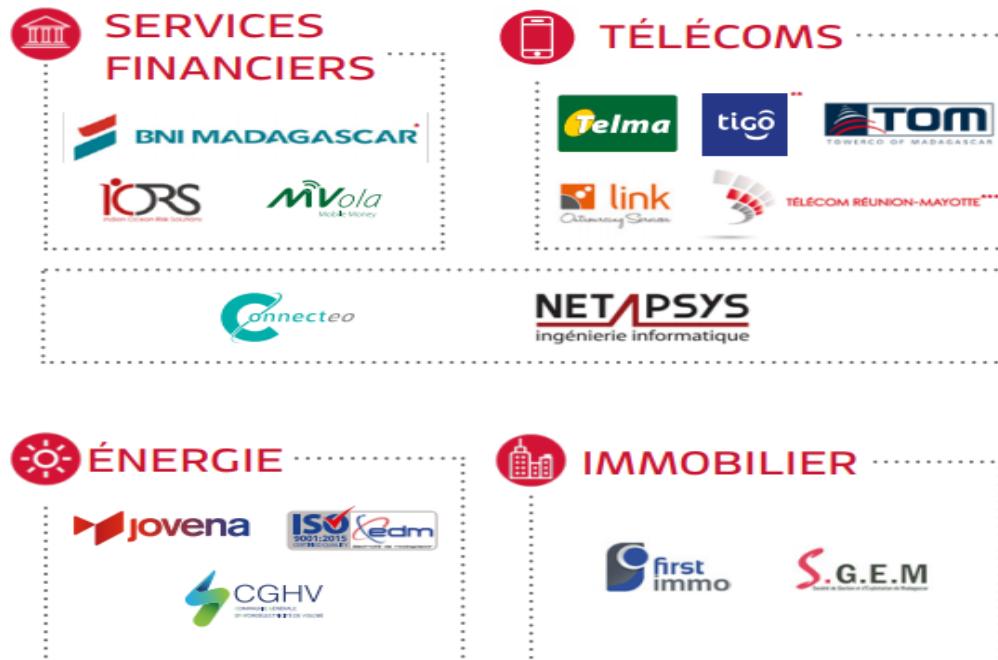


Figure 4 : Activités du Groupe Axian

## 2.7 Organigramme d'Axian IT Services

La figure 5 montre l'organigramme général d'Axian IT Services

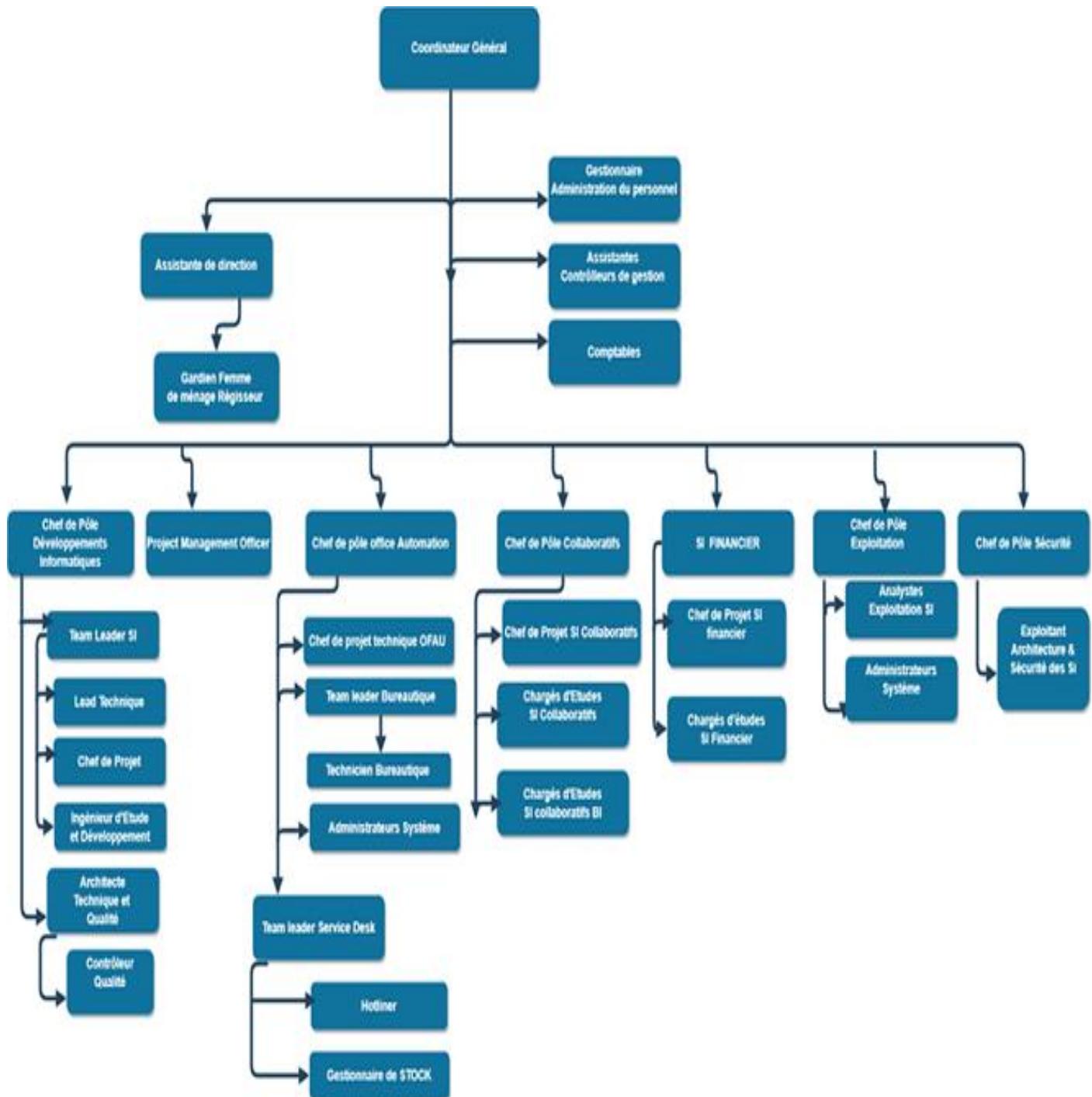


Figure 5 : Organigramme d'Axian It Service

# Chapitre 3 : Description du Stage

## 3.1 Généralités

Comme chaque année, la plupart des étudiants en deuxième année en Master Professionnel à l'Ecole Nationale d'Informatique de l'Université de Fianarantsoa effectuent un stage de durée de six mois au sein d'une entreprise, d'une société ou d'une autre entité pour évaluer ses capacités, mettre en pratique ses connaissances et se familiariser avec le monde de l'entreprise.

Notre stage a débuté le 23 Juillet 2018 et prend fin le 26 Janvier 2019 au sein du Groupe AXIAN/AITS Antananarivo.

Au premier contact, nous avons été reçus par le responsable des Ressources Humaines de la Société qui nous a présentés à notre responsable, Le Chef du Pôle Exploitation. En tant que responsable ainsi que notre encadreur professionnel, le chef de pôle nous a donné des consignes à appliquer et à respecter avec précision et rigueur.

Le Groupe AXIAN dispose de différents services qui sont répartis selon les domaines de spécialisation. L'un de ces services est « AITS » Axian IT Service. Ce dernier constitue l'un de piliers de l'établissement, puisqu'il a la charge d'assurer le bon fonctionnement de tout ce qui concerne les technologies de l'information. Il est responsable du bon fonctionnement des services, de l'administration et de la sécurité ainsi que la maintenance de différentes technologies et matériels informatiques.

L'Axian IT Service est un élément indispensable pour le bon fonctionnement du Groupe AXIAN. Justement, nous avons effectué notre stage au sein de la Société Groupe AXIAN dans le département Axian IT Service. Cependant, l'objet de notre stage dépendait des besoins d'AITS et de ce que notre encadreur professionnel décide de nous confier comme tâches, tout en respectant les exigences de l'ENI.

## 3.2 Description du Projet

Comme actuellement, le Société Group AXIAN utilise un système « CLOUD » pour son Système d'Information, le département AITS/Pôle Exploitation prend en charge de la gestion de la « Virtual Data Center » où des applications et des services de nombreuses entreprises sont y installés, et les données informatiques sont donc très importantes vis à vis de la société. Il est donc nécessaire de mettre en place une stratégie de sauvegarde de ces données, afin qu'elles soient disponibles à tout moment en cas de pertes inattendues. Ainsi, l'entreprise souhaite définir une politique de sauvegardes en mettant en place une machine dédiée aux sauvegardes.

C'est pourquoi le Pôle Exploitation nous a demandé de mettre en place une solution de sauvegarde plus adaptée à ses besoins. Cette intégration, non sans difficultés, a abouti à une phase de tests obligatoires afin de simuler un éventuel incident.

De plus, le projet ne s'est pas limité à la simple mise en place du système de sauvegarde réseau, mais a été amplifié par l'ajout d'autre projet supplémentaire, permettant de répondre aux exigences définies de l'entreprise. D'où notre thème est de « Déploiement et Implémentation d'une solution de sauvegarde réseau et d'un serveur VPN ».

### 3.3 Objectifs du Projet

En effet, le but recherché est de montrer la nécessité d'une solution sauvegarde par le réseau sur une machine centralisée dédiée à la sauvegarde et un accès VPN sécurisé de l'extérieur vers le réseau interne de l'entreprise, il s'agit d'un VPN d'accès, à savoir :

- Créer une nouvelle machine serveur pour la centralisation des sauvegardes ;
- Créer une nouvelle machine serveur pour l'accès privé, VPN ;
- Configurer le routage, NAT, redirection et ouverture des ports pour le serveur de sauvegarde, le serveur VPN pour les clients.

### 3.4 Moyens matériels

La mise en place d'un serveur de sauvegarde nécessite un assez impressionnant dispositif en termes de moyens matériels étant donné la sensibilité de l'opération, la valeur considérable des données à sauvegarder et l'importance de la sécurité. Nous LES récapitulons dans le tableau 5 :

Tableau 5 : Moyens matériels

Serveur	Configuration
Pour la sauvegarde : RedHat Enterprise Linux Server 7.3 x86_64	<ul style="list-style-type: none"><li>● Deux Processeur : 2.27 GHz</li><li>● RAM 8 GB</li><li>● Disque 1 : 60GB</li><li>● Disque 2 : 400 GB</li></ul>
Pour le VPN : RedHat Enterprise Linux Server 7.3 x86_64	<ul style="list-style-type: none"><li>● Deux Processeur : 2.27 GHz</li><li>● RAM 4 GB</li><li>● Disque : 60GB</li></ul>
Client à sauvegarder	Configuration
Windows	<ul style="list-style-type: none"><li>● Windows Serveur 2008 64bits</li><li>● Windows Serveur 2012 64bits</li></ul>
Linux	<ul style="list-style-type: none"><li>● RedHat Enterprise Linux Server 7.2 x86_64</li><li>● RedHat Enterprise Linux Server 7.3 x86_64</li></ul>

### **3.5 Résultats attendus**

Le résultat global espéré de la mise en œuvre de ce projet est l'implémentation d'un système de sauvegarde réseau et d'un serveur VPN :

- Permettre de sauvegarder les données des serveurs en réseau régulièrement ;
- Pouvoir restaurer les données sauvegardées entièrement ou quelque donnés voulu ;
- Permettre d'accéder aux serveurs du site via un accès privé distant ;
- Communiquer entre eux (partage des données, voix, visioconférence...) de façon totalement privée.

### **3.6 Définition du cahier des charges**

Dans un projet informatique comme le nôtre, le cahier des charges est un préalable. Pour réussir, tout projet doit suivre une logique dans laquelle le cahier des charges tient un rôle particulier. Pour notre cas, c'est le cahier des charges qu'on doit suivre pour réaliser notre projet :

- L'étude de l'existant qu'on a déjà entamé précédemment et qui joue un rôle très important;
- L'analyse des besoins de la société ;
- La description de la solution ;
- L'étape de mise en œuvre qui comprend toute la configuration et le test de fonctionnement ;
- L'objectif de tout cela c'est de :
  - Diminuer le risque d'erreurs lors de la réalisation
  - Indiquer les contraintes à respecter impérativement
  - Proposer des solutions fiables et pérennes.

### **3.7 Chronogramme**

Il est toujours convenable d'élaborer un planning, pour bien déterminer les objectifs ainsi que les activités tout au long du projet lui-même. Ainsi, en ce qui concerne notre stage, on a fait manuellement le chronogramme en prenant bien soin de noter tout ce qu'on a fait jusqu'à la finalisation. Le stage a commencé le 23 Juillet 2018 et s'est terminé le 26 Janvier 2019.

Le chronogramme dans le tableau 6 représente les différentes tâches que nous avons faites durant la période de stage.

Tableau 6 : Chronogramme de stage

Activités	Début	Fin
Période de stage	23 Juillet 2018	23 Janvier 2019
Intégration en Entreprise	23 Juillet 2018	27 Juillet 2018
Etude de l'existant	30 Juillet 2018	03 Août 2018
Analyse du trafic réseau	06 Août 2018	10 Août 2018
Détection des problèmes et proposition de solution	13 Août 2018	31 Août 2018
Etude théorique des solutions	03 Septembre 2018	06 Octobre 2018
Mise en place du serveur Bacula	08 Octobre 2018	26 Octobre 2018
Implémentation et test de sauvegarde	29 Octobre 2018	09 Novembre 2018
Mise en place Pritunl	12 Novembre 2018	16 Novembre 2018
Implémentation et test de VPN	19 Novembre 2018	23 Novembre 2018
Implémentation et Test en couplage de deux serveurs	26 Novembre 2018	11 Janvier 2019
Rédaction du mémoire	12 Novembre 2018	19 Janvier 2019

## **PARTIE II : GENERALITE ET ANALYSE**

# Chapitre 4 : Généralités sur La Sauvegarde et Le VPN

## 4.1 Sauvegarde

### 4.1.1 Généralité

Le meilleur moyen de ne pas perdre ses données est d'avoir toujours au moins une copie en lieu sûr, appelée sauvegarde. Il est primordial d'effectuer régulièrement des sauvegardes. La fréquence des sauvegardes dépend de la quantité de données envisagée d'être perdue en cas de destruction des données.

En plus des données, la sauvegarde du système et des logiciels est possible, mais en général ces derniers sont fournis avec des moyens de réinstallation qui rendent cette sauvegarde moins importante que celle des données.

Pour effectuer une sauvegarde, il faut soit utiliser un outil spécialisé soit faire de la simple copie de fichiers.

Il est recommandé, une fois la sauvegarde effectuée, d'entreposer les supports loin de l'ordinateur qui contient les données. Cette précaution évite que la destruction des données d'origine ne puisse s'accompagner de la destruction de leur copie de sauvegarde (ce qui pourrait arriver en cas d'incendie ou d'inondation).

Le support externe utilisé pour stocker la sauvegarde peut être un CD, un DVD enregistrables, un disque dur externe, une bande magnétique...en fonction de l'équipement en possession (interface USB, graveur, lecteur de bande) et de la quantité de données à sauvegarder.

En informatique, la sauvegarde (*backup* en anglais) est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique [19].

Ce terme est proche de deux notions :

- L'enregistrement des données, qui est l'opération d'écriture des données sur un item d'enregistrement durable, tel qu'un disque dur, une clé USB, des bandes magnétiques, etc.
- L'archivage, qui consiste à enregistrer des données sur un support à des fins légales ou historiques.

La sauvegarde passe forcément par un enregistrement des données, mais pas nécessairement dans un but d'archivage.

#### **4.1.2 Finalité**

Les copies de sûreté sont utiles principalement pour deux choses :

- La première et la plus évidente est de permettre de restaurer un système informatique dans un état de fonctionnement à la suite d'un incident (perte d'un support de stockage tel que disque dur, bande magnétique, etc., ou de tout ou partie des données qu'il contient).
- La seconde, incluse dans la première mais certainement la plus courante, est de faciliter la restauration d'une partie d'un système informatique (un fichier, un groupe de fichiers, un système d'exploitation, une donnée dans un fichier, etc.) à la suite d'une suppression accidentelle ou d'une modification non désirée.

La technique la plus fréquente est la recopie des données sur un support indépendant du système initial (ordinateur local, serveur, etc.). L'opération inverse qui consiste à réutiliser des données sauvegardées s'appelle une restauration. On parle de « stockage » pour les données sauvegardées en attente d'une éventuelle restauration.

#### **4.1.3 Critères de choix**

Le choix d'une technique de sauvegarde se fera en prenant en compte :

- La capacité de stockage du support (le volume d'information) ;
- La vitesse de sauvegarde ;
- La fiabilité du support (notamment après une longue période de stockage) ;
- La simplicité de classement ;
- La facilité à restaurer les données ;
- Et bien sûr le coût de l'ensemble.

Intervient également la possibilité de sélectionner les données à sauvegarder. Enfin pour les grands systèmes de sauvegarde, il faut tenir compte de critères physiques : volume physique des supports de stockage, poids, sensibilité à la température, à l'humidité, à la poussière, à la lumière.

#### **4.1.4 Différents types de sauvegarde**

Il existe un certain nombre d'options pour sauvegarder les données qui résident sur des serveurs standard Windows. Ces options se divisent en deux catégories : sauvegarde en local et sauvegarde sur réseau, qui sont présentées en détail dans les sections qui suivent.

#### **4.1.4.1 Sauvegardes des données en local**

La seule façon d'effectuer des sauvegardes de serveurs en local consiste à utiliser un système de sauvegarde connecté en direct dans lequel le lecteur de bande, le chargeur automatique ou la bibliothèque sont connectés directement à chaque serveur via une connexion. La solution de sauvegarde et de restauration est configurée sur chacun des serveurs, ce qui signifie que chaque serveur à sauvegarder requiert une gestion individuelle et un logiciel de sauvegarde dédié. Le logiciel de sauvegarde lit les données de l'emplacement de stockage principal et les écrits sur le périphérique de sauvegarde. L'administration du logiciel de sauvegarde peut s'effectuer en local ou à distance.

#### **4.1.4.2 Sauvegardes des données sur le réseau**

Une sauvegarde réseau utilise le réseau local (LAN) et sauvegarde les données d'un ou de plusieurs serveurs.

Les sauvegardes de réseaux locaux à l'échelle de l'entreprise nécessitent de solides capacités centralisées de gestion des supports et de sauvegarde des métadonnées qui se définissent comme suit :

- Gestion des métadonnées de sauvegarde

La gestion des métadonnées de sauvegarde est une fonctionnalité critique de la sauvegarde de réseau local car elle offre des possibilités de recherche qui permettent de localiser rapidement les objets de données pour les restaurer.

- Gestion des supports

La gestion des supports est un élément vital puisqu'il s'agit de gérer les supports sur lesquels résident les données de sauvegarde. La gestion de différents types de support (disque et bande) est critique pour un système de sauvegarde centralisé en réseau. En outre, la prise en charge et la gestion des bibliothèques de bandes, des lecteurs de bandes et des cartouches constituent des aspects importants de la gestion des supports dans un système de sauvegarde en réseau.

Les sauvegardes en réseau impliquent généralement l'utilisation d'un serveur de support de sauvegarde dédié qui gère une bibliothèque de bandes automatisée, de grande capacité, composée de plusieurs lecteurs de bande rapides et de chargeurs de médias.

#### **4.1.5 Stratégie de sauvegarde**

On distingue la sauvegarde d'un poste individuel et la sauvegarde sur serveur. L'une et l'autre s'adressent à la même nature d'information (la donnée informatique) et ont le même objectif (protéger l'information et permettre de la retrouver si elle était perdue), mais les méthodes de sauvegarde sont différentes pour plusieurs raisons :

- Les données sur poste client sont réputées moins importantes que les données gérées sur des systèmes centraux ;
- Les utilisateurs sont moins sensibilisés au risque de perte de données que les professionnels de l'informatique ;
- Ils ont également moins de formation sur les techniques de sauvegarde ;
- Les moyens techniques sont moins développés sur poste individuel que sur serveur, même si des progrès importants ont été réalisés ces dernières années (chute du rapport coût/volume des supports de sauvegarde, simplification des interfaces de sauvegarde, sauvegarde sans intervention de l'utilisateur, etc.)

De fait la sauvegarde des données des postes individuels reste marginale dans la stratégie d'utilisation des ordinateurs. Cependant les entreprises, en généralisant l'usage des ordinateurs, de serveurs et du partage des ressources en réseau, ont ressenti un besoin de sécurité qui a favorisé le développement d'outils de sauvegarde.

#### **4.1.5 Méthodes de sauvegarde les plus courantes**

La méthode la plus simple est la sauvegarde complète ou totale (appelée aussi "full backup") ; elle consiste à copier toutes les données à sauvegarder que celles-ci soient récentes, anciennes, modifiées ou non.

Cette méthode est aussi la plus fiable mais elle est longue et très coûteuse en termes d'espace disque, ce qui empêche de l'utiliser en pratique pour toutes les sauvegardes à effectuer. Afin de gagner en rapidité et en temps de sauvegarde, il existe des méthodes qui procèdent à la sauvegarde des seules données modifiées et/ou ajoutées entre deux sauvegardes totales.

On en recense deux :

- La sauvegarde différentielle ;
- La sauvegarde incrémentielle.

La restauration d'un disque avec l'une de ces méthodes s'avère plus longue et plus fastidieuse puisqu'en plus de la restauration de la sauvegarde différentielle ou des sauvegardes incrémentielles, on doit également restaurer la dernière sauvegarde complète. Les fichiers supprimés entre-temps seront restaurés.

Afin de comprendre la différence entre les deux méthodes, nous prendrons l'exemple d'un plan de sauvegarde selon le cycle suivant :

- Une sauvegarde complète au jour J (dimanche soir par exemple)
- Une sauvegarde des fichiers modifiés ou nouveaux du jour J+1 au jour J+6 (du lundi soir au samedi soir inclus)
- Une sauvegarde complète au jour J+7 (dimanche soir suivant).

#### **4.1.6 Techniques complémentaires**

La sauvegarde de données peut être réalisée en utilisant des techniques plus ou moins sophistiquées. La méthode la plus simple est de parcourir les répertoires et les fichiers d'un poste de travail ou d'un serveur, mais on se trouve vite limité par le nombre de fichiers et par le volume de données, qui ont un impact direct sur le temps de sauvegarde. Pour contourner ces limitations, plusieurs approches sont envisageables :

- Compression des données sauvegardées, utilisé par la majorité des solutions de sauvegarde ;
- Technique de snapshot : prise d'image instantanée d'un disque
- Technique de déduplication pour limiter le volume des sauvegardes en éliminant les doublons ;
- Technique de déduplication à la source permettant de ne stocker qu'une seule fois un fichier, même si celui-ci a été dupliqué et renommé sur les postes sauvegardés, les doublons n'étant présents que dans les index ;
- Une combinaison de ces différentes techniques.

## 4.2 VPN « Virtual Private Network »

### 4.2.1 Présentation

Un réseau privé virtuel ou **VPN** (*Virtual Private Network*) permet d'assurer des communications sécurisées entre différents sites d'une entreprise, à travers d'un réseau partagé ou public (réseau de transport, Internet...), selon un mode émulant une liaison privée point à point [2].

Dans un VPN la communication entre deux points du réseau doit être **privée** et des tiers ne doivent pas y avoir accès. Pour émuler cette liaison privée point à point, les données sont encapsulées avec un en-tête contenant les informations de routage ce qui leur permet de traverser le réseau partagé ou public pour atteindre la destination. Cette communication privée étant établie au travers d'une infrastructure de réseau (privé ou public) partagée par plusieurs dispositifs implique un « partitionnement » **virtuel** de la bande passante et des infrastructures partagées. On va donc « isoler » le trafic entre deux points du réseau en créant un chemin d'accès logique (**tunnel** ou canal virtuel) privé et sécurisé, dans lequel les données sont encapsulées et chiffrées au sein d'une trame « conteneur ». Pour émuler cette liaison privée, les données sont cryptées en vue d'assurer leur confidentialité. Les paquets qui pourraient être interceptés sur le réseau partagé ou public sont donc indéchiffrables sans les clés de cryptage. Outre la confidentialité des informations, on garantit également l'identité des utilisateurs en utilisant notamment des certificats d'authentification standardisés.

En général, un réseau privé virtuel de base est composé d'un serveur VPN, d'un client VPN, d'une connexion de réseau privé virtuel VPN (la partie de la connexion où les données sont cryptées) et d'un tunnel (la partie de la connexion où les données sont encapsulées).

### 4.2.2 Principe général

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisément et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet. Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation.

### 4.2.3 Fonctionnalités des VPN

Il existe deux (02) implémentations standards d'utilisation des VPN. En étudiant ces schémas d'utilisation, il est possible d'isoler les fonctionnalités indispensables des VPN.

- Site-to-Site VPN (ou VPN LAN à LAN)
- Client-to-Site VPN (ou VPN Client Serveur)

#### 4.2.3.1 Site-to-Site VPN

La figure 6 présente la topologie de Site-to-Site VPN

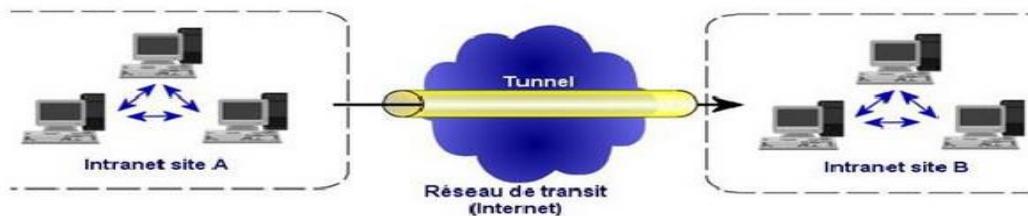


Figure 6 : Topologie de Site-to-Site VPN

Le VPN Site-to-Site est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées [2].

#### 4.2.3.2 Client-to-Site VPN

La Figure 7 décrit la topologie de Client-to-Site VPN :

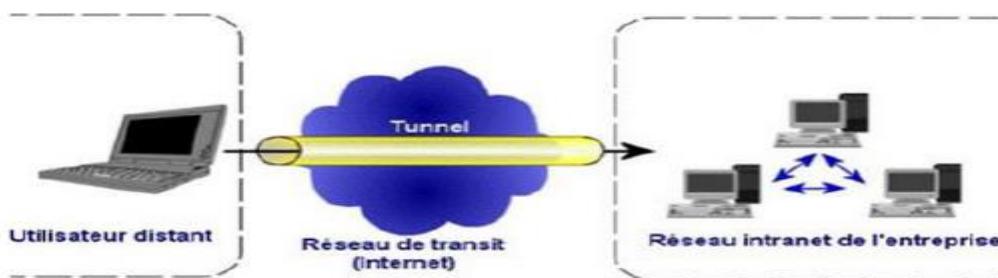


Figure 7 : Topologie de VPN Client-Serveur

Le VPN Client-Serveur est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN [2]. Il existe deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant.
- L'utilisateur possède son propre logiciel client pour le VPN dans ce cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

#### **4.2.4 Protocoles utilisés pour réaliser une connexion VPN**

Nous pouvons classer les protocoles que nous allons étudier en deux catégories :

- Les protocoles de niveau 2 comme PPTP et L2TP.
- Les protocoles de niveau 3 comme IPsec.

Il existe en réalité trois protocoles de niveau 2 permettant de réaliser des VPN : PPTP (de Microsoft), L2F (développé par CISCO) et enfin L2TP. Nous évoquerons dans cette étude que PPTP et L2TP :

- **VPN PPTP**

PPTP signifie Point-to-Point Tunneling Protocol c'est le protocole le plus commun, il permet d'autoriser les utilisateurs distants à se connecter au réseau VPN en utilisant leur connexion Internet existante, puis leur permet de se connecter à l'aide de l'authentification VPN de mot de passe. Les utilisateurs n'ont pas besoin de matériel supplémentaire et ces fonctionnalités sont souvent disponibles en tant que logiciel add-on peu coûteux. L'inconvénient du PPTP est qu'il ne prévoit pas de cryptage et qu'il s'appuie sur le (Protocole Point-to-Point) PPP pour mettre en œuvre les mesures de sécurité [8].

- **VPN L2TP**

L2TP ou calque pour Tunneling Protocol est similaire à PPTP, car il ne prévoit pas de cryptage non plus et s'appuie sur le protocole PPP pour ce faire. La différence entre PPTP et L2TP est que ce dernier ne fournit pas seulement la confidentialité des données mais aussi l'intégrité des données. L2TP a été développée par Microsoft et Cisco [8].

- **IPsec (Internet Protocol Security)**

IPsec est le protocole qui prédomine actuellement dans les VPN car il est disponible sur de nombreuses plates-formes (NT, Linux, Novell, Macintosh...) et géré de manière native avec IPv6. Autrement dit, pas de changement de structure ni d'éventuelles incompatibilités quand le temps sera venu de passer à IPv6. Par contre, IPsec est aussi assez contraignant pour l'entreprise. Compte-tenu du système de clé partagée (si on utilise ce mode d'authentification), retirer l'accès à un utilisateur en cas de départ de la société revient à faire changer la clé à l'ensemble des autres utilisateurs concernés. On peut cependant utiliser une infrastructure à clé publique mais compte-tenu de la difficulté, les entreprises déployant une PKI interne restent rares [8].

# Chapitre 5 : Analyse Préalable

## 5.1 Analyse de l'existant

### 5.1.1 Description

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation de la solution ; l'analyse de l'existant est alors très importante. Il est essentiel d'avoir une vue sur l'architecture interne, le mécanisme et les failles du système en place. On comprendra par la suite les infrastructures en place, les différentes politiques de sécurité du système, les besoins ainsi que les problèmes fréquemment rencontrés.

Le but de cette phase est de connaître le véritable système à étudier. Il nous permet aussi d'énumérer les ressources matérielles et logicielles que l'entreprise utilise.

### 5.1.2 Structure et topologie du réseau

Une topologie de réseau est en informatique une définition de l'architecture d'un réseau. Elle définit la disposition géographique des différents postes ou matériels informatiques du réseau, les connexions entre ces matériels et une hiérarchie éventuelle entre eux.

La figure 8 représente la topologie globale de l'infrastructure réseau d'AITS :

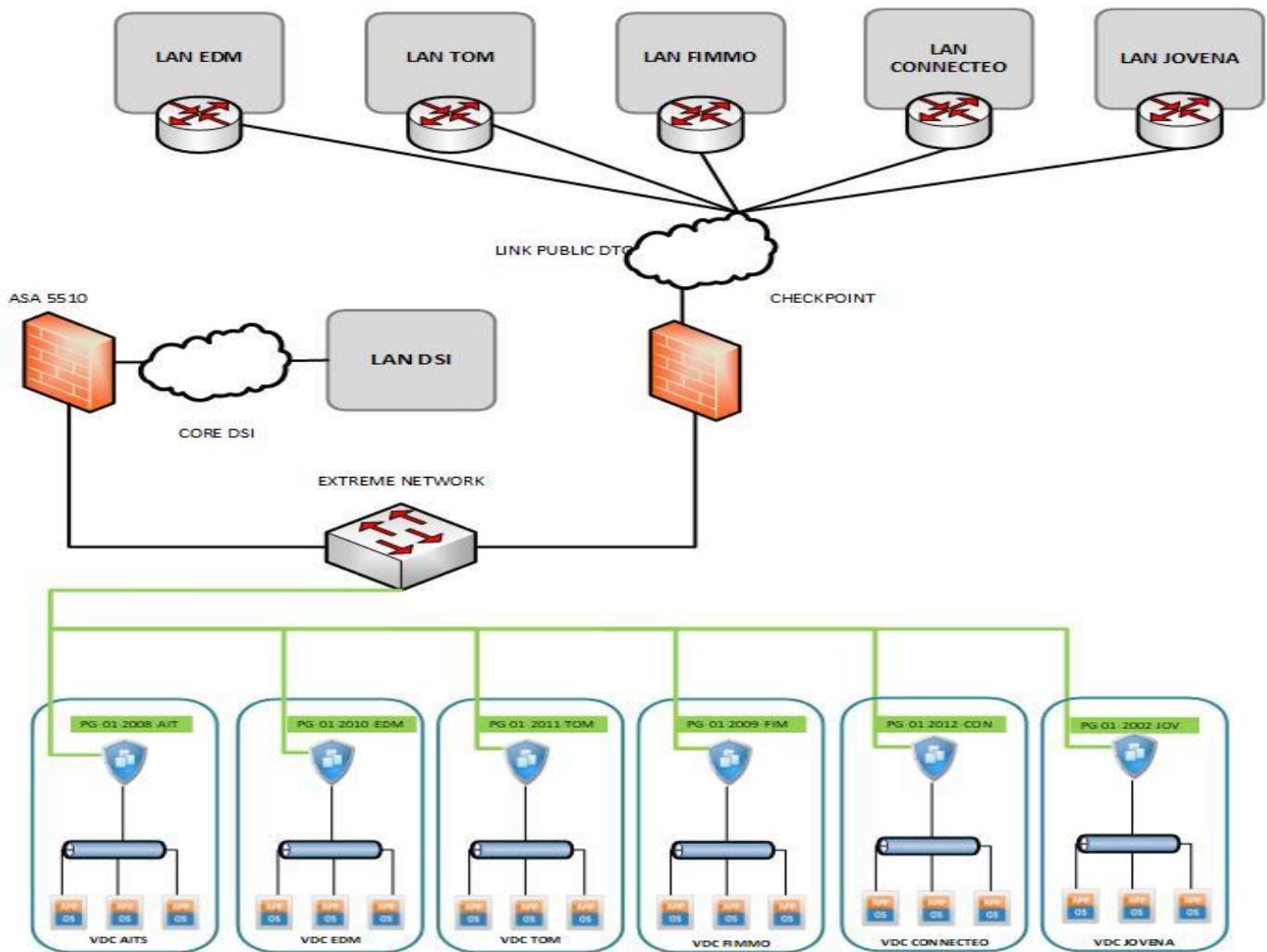


Figure 8 : Topologie réseau d'AITS

Comme l'indique cette figure, l'infrastructure réseaux d'AITS dispose de deux sources de réseaux, l'une, CHECKPOINT est pour la communication entre les entreprises et le VDC d'AITS, l'autre est pour les accès internes et internet qui sont gérées dans le LAN DSI.

### **5.1.3 Type de réseaux**

Connaître les différents types de réseaux est un élément important lors de l'analyse de l'existant. Cela permet de déterminer la vitesse et surtout la protection du réseau.

Les types de réseaux existants au niveau local dans la société sont expliqués en détails dans le Tableau 7.

Tableau 7 : Types de réseaux existant au sein de la société

Type	Caractéristiques	Protection
LAN	100Mbits/s	Authentification A. D
WLAN	30Mbits/s	Filtrage Cellulaire + Authentification A. D

Comme l'indique ce tableau, nous pouvons trouver deux types de réseau local avec un débit allant jusqu'à 100Mbits par seconde mais avec des méthodes de sécurité différentes.

Concernant le type de connexion internet, on a pu recenser dans l'entreprise comme l'indique le tableau 8 le type de liaison d'interconnexion de l'AITS.

Tableau 8 : Type d'accès à internet

Connexion	Fournisseur	Vitesse	Technologie
Liaison Optique	Telma	- 8Mbps modulaire, 20Mbps international, 100Mbps national	Fibre Optique

### **5.1.4 Equipement d'interconnexion**

Pour interconnecter les postes de travail, que ce soit Serveurs ou Clients, des types des équipements d'interconnexion variés sont mis en place dans la topologie du réseau pour assurer le bon fonctionnement du réseau local. Dans une architecture, le matériel d'interconnexion représente le cœur du réseau. S'il est mal configuré (équipement « manageable »), il peut avoir des effets néfastes sur le trafic réseau.

Le tableau 9 ci-après montre ces différents types des équipements d'interconnexion et leurs caractéristiques que nous avons pu recenser :

Tableau 9 : Type des matériaux d'interconnexion

Type	Désignation	Caractéristique	Unité	Emplacement
Router	Mikrotik RouterOS RB1100x5	<ul style="list-style-type: none"> <li>• 10/100/1000 Mbps</li> <li>• Ethernet 13 ports</li> <li>• CPU AL21400, 4 cores, 1.4 GHz</li> <li>• RAM 1 GB</li> </ul>	02	AITS
Switch	D-Link DES-10160	<ul style="list-style-type: none"> <li>• 16 ports 10/100 Mbps</li> </ul>	01	EXP/AITS
VDC	VSphere VMware	<ul style="list-style-type: none"> <li>• Ghz : 12 ghz</li> <li>• vRAM : 24 Go</li> <li>• Stockage : 2T</li> <li>• Dual Socket</li> </ul>	05 Hosts	AITS

### 5.1.5 Postes de travail

L'AITS dispose de centaines d'ordinateurs répartis dans différents domaines et utilisés comme postes de travail.

La plupart de tous les postes de travail sont équipés du système d'exploitation Windows et utilisant l'authentification Active Directory ou LDAP.

Le tableau 10 illustre la répartition de ces derniers.

Tableau 10 : Postes de travail

Désignation	Caractéristiques	Système d'exploitation	Compte d'accès	Type
Dell Hewlett Packard	CPU: cori3 2.20 GHz RAM: 4 Go à 8 Go HDD : 250Go à 1To	Windows 10	Active Directory	PC Portable
Hewlett Packard	CPU: cori5 2.24 GHz RAM: 4 Go à 8 Go HDD : 250Go à 1To	Windows 10	Active Directory	PC Portable
Fujitsu	CPU: cori3 3.70 GHz RAM: 4 Go à 8 Go HDD : 250Go à 1To	Windows 10	Active Directory	PC Bureau

### 5.1.6 Serveurs

Comme nous nous sommes occupés des postes clients au sein du réseau local, nous allons maintenant voir les postes serveurs dans le VDC dans le Tableau 11.

Tableau 11 : Serveurs

Désignation	Caractéristiques	Système d'exploitation	Compte d'accès
Serveurs Windows	Intel® Xeon® CPU E7 2.27GHz x2 RAM 8GB HDD : 60 à 100 GB	Windows Serveur 2012 4bits	Admin Local/Active Directory
	Intel® Xeon® CPU E7 2.27GHz x2 RAM 4GB HDD : 60 à 100 GB	Windows Serveur 2008 64bits	Admin Local/Active Directory
Serveurs Linux	Intel® Xeon® CPU E7 2.27GHz x2 RAM 4GB à 8GB HDD : 60 à 400 GB	RedHat Enterprise Linux Server 7.3 x86_64	Admin Local/Active Directory
	Intel® Xeon® CPU E7 2.27GHz x2 RAM 4GB à 8GB HDD : 60 à 400 GB	RedHat Enterprise Linux Server 7.2 x86_64	Admin Local/Active Directory

### **5.1.7 Passerelle**

Il s'agit de la connexion vers l'extérieur, c'est-à-dire l'internet. Voyons les caractéristiques de l'équipement qui sert de passerelle entre le réseau local et internet dans le tableau 12. L'AITS/EXP se situe dans le local de la société TELMA, dont le matériel est géré par la DSI TELMA

Tableau 12 : Passerelle

Désignation	Système d'exploitation	Caractéristique	Fonctionnalités
Mikrotik RB1100x4	RouterOS	<ul style="list-style-type: none"><li>• 10/100/1000 Mbps</li><li>  Ethernet 13 ports</li><li>• CPU AL21400, 4 cores, 1.4 GHz</li></ul>	NAT, QoS, Firewall

### **5.1.8 Partage**

Au cœur de la société, il existe des partages de données. AITS utilise un serveur (Windows serveur 2012) qui assure ce dernier. En effet, les dossiers à partager sont stockés dans ce serveur et on peut y accéder depuis les autres machines clientes grâce à l'authentification à Active Directory. Il s'agit d'un partage hétérogène et local vu que le serveur est accessible via Windows (7,10) et Mac OSX.

### **5.1.9 Routage**

Le routage est un processus qui permet de sélectionner des chemins dans un réseau pour transmettre des données depuis un expéditeur jusqu'à un ou plusieurs destinataires. IP est un protocole de réseau fonctionnant dans le mode non connecté, cela veut dire que tous les paquets d'un même message sont indépendants les uns des autres et peuvent emprunter des itinéraires différents. Des protocoles de routage interviennent alors pour acheminer les paquets sur le réseau et entre les routeurs. L'AITS dans le VDC, VSphere VMware utilise le routage statique pour chaque serveur virtuel.

### **5.1.10 Disponibilité**

Durant notre stage, nous avons pu recenser les principales disponibilités qui existent dans la société. A ce sujet, nous pouvons évoquer dans les différents points ci-après qu'ils y avaient de disponible de :

- Ressources : matériellement, la société est bien équipée. Les équipements d'interconnexion assurent la connectivité dans les réseaux 24h/24 et 7jours/7.
- Serveurs : ils offrent aussi des services 24h/24. La bande passante est équilibrée et bien gérée.
- Applications : il existe différentes applications dans l'entreprise. La plupart de ces applications fonctionnent bien et sont accessibles par des utilisateurs.
- Données : grâce au service du serveur d'applications, les données sont accessibles localement aux personnels de société à société par VPN site to site. Pour ceux qui sont en dehors du Groupe, ils ne peuvent pas y accéder.
- Internet : l'internet est bien évidemment disponible au sein de l'Organisation et son utilisation est surveillée afin de ne pas saturer la bande passante.
- Politique de sauvegarde et de restauration : au niveau du système, aucune politique de sauvegarde et de restauration n'a été constatée.
- Plates-formes logicielles : la société a choisi les systèmes d'Exploitation « Microsoft Windows » pour la plupart des postes clients. Nous avons recensé également l'antivirus « Symantec Endpoint Protection ».

### **5.1.11 Surveillance**

La surveillance d'un réseau informatique consiste à indiquer et/ou commander l'état d'un serveur, d'un équipement réseau, de la disponibilité de la bande passante pour anticiper les pannes ou diagnostiquer rapidement les réseaux en cas de congestion.

Elle peut s'effectuer par un moyen logiciel représentée dans le tableau 13.

Tableau 13 : Logiciel de monitoring

<b>Logiciel</b>	<b>Version</b>	<b>Licence</b>	<b>Description</b>
Nagios	v4.3.4	GPL	Utilisé comme moniteur réseau

Une surveillance complète des systèmes d'exploitation serveur et serveur Microsoft Windows - y compris les mesures systèmes, les états de service, les états de processus, les compteurs de performance, les journaux des événements, les applications, les services et plus encore.

### 5.1.12 Analyse du trafic

Pour pouvoir apporter une amélioration au réseau existant, il est indispensable d'effectuer une analyse du trafic. Grâce à cette dernière, il nous sera possible de déterminer les protocoles les plus utilisés au sein du réseau et pouvant consommer trop de bande passante. La détermination de ces protocoles nous permettra ainsi d'apporter une ou des solutions aux problèmes et d'améliorer la performance au niveau des trafics réseaux.

Afin d'effectuer une analyse du trafic, il nous faut des outils spécifiques. Nous avons choisi « **Wireshark** » pour cela. Cet outil est très puissant et offre beaucoup de fonctionnalités telles que les captures des paquets, l'analyse de trafic, l'affichage de graphe pour la statistique (permettant d'illustrer dans un graphe la statistique des paquets et l'utilisation des protocoles), le « sniffing » et beaucoup d'autres encore.

Pour avoir des résultats fiables et pour pouvoir mieux analyser le trafic du réseau de la société, nous avons effectué plusieurs captures à différentes heures de travail mais nous n'avons pas pu recueillir beaucoup plus d'informations sur le trafic réseau ni faire de capture des trames ni même interviewer les utilisateurs à cause de la sécurité et de la confidentialité des données et des informations pertinentes que le trafic pourrait révéler.

Nous avons effectué l'analyse du trafic dans un serveur se trouvant dans le VDC et dans le même réseau. Ce serveur sert pour l'accès sécurisé vers les autres serveurs en utilisant l'accès par navigateur web pour les applications, ssh, bureau à distant et autres.

La figure 9 et la figure 10 illustrent les extraits de ces captures :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.102.152	172.20.32.4	TCP	60	56522 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=0
2	0.007272	172.20.40.204	172.20.32.4	UDP	60	52171 → 3389 Len=12
3	0.010951	172.20.40.204	172.20.32.4	UDP	60	52171 → 3389 Len=12
4	0.016021	192.168.101.240	172.20.32.4	TCP	60	63256 → 443 [ACK] Seq=1 Ack=1 Win=2016 Len=0
5	0.026216	172.20.40.204	172.20.32.4	TLSv1.2	139	Application Data
6	0.050081	172.20.32.4	172.20.40.204	TCP	54	3389 → 64683 [ACK] Seq=1 Ack=86 Win=63219 Len=0
7	0.050297	172.20.32.4	192.168.101.240	TLSv1.2	715	Application Data
8	0.051877	172.20.32.2	172.20.32.4	TLSv1.2	155	Application Data
9	0.065667	172.20.32.4	172.20.32.2	TCP	54	57622 → 3389 [ACK] Seq=1 Ack=102 Win=4101 Len=0
10	0.091306	192.168.101.240	172.20.32.4	TCP	60	63256 → 443 [ACK] Seq=1 Ack=662 Win=2013 Len=0
11	0.112992	172.20.32.4	192.168.101.240	TLSv1.2	1051	Application Data
12	0.132101	192.168.101.240	172.20.32.4	TLSv1.2	299	Application Data
13	0.143757	172.20.32.4	192.168.101.240	TCP	54	443 → 63260 [ACK] Seq=1 Ack=246 Win=509 Len=0
14	0.154844	192.168.101.240	172.20.32.4	TCP	60	63256 → 443 [ACK] Seq=1 Ack=1659 Win=2016 Len=0
15	0.154893	172.20.32.4	192.168.101.240	TLSv1.2	603	Application Data
16	0.190802	172.20.32.4	172.20.40.204	UDP	1264	3389 → 52171 Len=1222
17	0.190865	172.20.32.4	172.20.40.204	UDP	69	3389 → 52171 Len=27
18	0.198437	192.168.101.240	172.20.32.4	TCP	60	63256 → 443 [ACK] Seq=1 Ack=2208 Win=2013 Len=0
19	0.222100	172.20.32.4	172.20.40.204	UDP	1260	3389 → 52171 Len=1218
20	0.222153	172.20.32.4	172.20.40.204	UDP	1260	3389 → 52171 Len=1218

Figure 9 : Analyse du trafic réseau I

No.	Time	Source	Destination	Protocol	Length	Info
3376	17.456259	172.20.32.4	192.168.101.240	TCP	54	443 + 63260 [ACK] Seq=1 Ack=104978 Win=506 Len=0
3377	17.464322	192.168.101.240	172.20.32.4	TLSv1.2	251	Application Data
3378	17.468370	172.30.31.21	172.20.32.4	TLSv1.2	779	Application Data
3379	17.469542	172.20.40.204	172.20.32.4	TLSv1.2	155	[TCP Previous segment not captured] , Application Data
3380	17.469570	172.20.32.4	172.20.40.204	TCP	66	[TCP Dup ACK 3359#1] 3389 → 64683 [ACK] Seq=1531 Ack=57864 Win=63495 Len=0 SLE=57965 SRE=58066
3381	17.469600	172.20.40.204	172.20.32.4	TLSv1.2	155	Application Data
3382	17.469610	172.20.32.4	172.20.40.204	TCP	66	[TCP Dup ACK 3359#2] 3389 → 64683 [ACK] Seq=1531 Ack=57864 Win=63495 Len=0 SLE=57965 SRE=58167
3383	17.469631	172.20.40.204	172.20.32.4	TLSv1.2	155	Application Data
3384	17.469639	172.20.32.4	172.20.40.204	TCP	66	[TCP Dup ACK 3359#3] 3389 → 64683 [ACK] Seq=1531 Ack=57864 Win=63495 Len=0 SLE=57965 SRE=58268
3385	17.469836	172.20.40.204	172.20.32.4	TLSv1.2	139	Application Data
3386	17.469846	172.20.32.4	172.20.40.204	TCP	66	[TCP Dup ACK 3359#4] 3389 → 64683 [ACK] Seq=1531 Ack=57864 Win=63495 Len=0 SLE=57965 SRE=58353
3387	17.469980	172.20.40.204	172.20.32.4	TLSv1.2	155	Application Data
3388	17.469989	172.20.32.4	172.20.40.204	TCP	66	[TCP Dup ACK 3359#5] 3389 → 64683 [ACK] Seq=1531 Ack=57864 Win=63495 Len=0 SLE=57965 SRE=58454
3389	17.470366	172.20.40.204	172.20.32.4	UDP	60	52171 → 3389 Len=12
3390	17.470542	172.20.40.204	172.20.32.4	TLSv1.2	155	Application Data
3391	17.470553	172.20.32.4	172.20.40.204	TCP	66	[TCP Dup ACK 3359#6] 3389 → 64683 [ACK] Seq=1531 Ack=57864 Win=63495 Len=0 SLE=57965 SRE=58555
3392	17.470933	172.20.40.204	172.20.32.4	TLSv1.2	155	Application Data
3393	17.470942	172.20.32.4	172.20.40.204	TCP	66	[TCP Dup ACK 3359#7] 3389 → 64683 [ACK] Seq=1531 Ack=57864 Win=63495 Len=0 SLE=57965 SRE=58656
3394	17.471873	172.20.32.4	192.168.101.240	TCP	54	443 + 63260 [ACK] Seq=1 Ack=105175 Win=512 Len=0
3395	17.472027	172.20.32.4	192.168.101.240	TLSv1.2	395	Application Data
3396	17.478374	172.20.40.204	172.20.32.4	TLSv1.2	846	[TCP Fast Retransmission] , Application Data, Application Data, Application Data, Application Data
3397	17.478417	172.20.32.4	172.20.40.204	TCP	66	3389 → 64683 [ACK] Seq=1531 Ack=58656 Win=62703 Len=0 SLE=57965 SRE=58656
3398	17.478684	172.20.40.204	172.20.32.4	TLSv1.2	139	Application Data
3399	17.483046	172.20.40.204	172.20.32.4	TLSv1.2	139	Application Data
3400	17.483074	172.20.32.4	172.20.40.204	TCP	54	3389 → 64683 [ACK] Seq=1531 Ack=58826 Win=64000 Len=0
3401	17.487513	172.20.32.4	172.30.31.21	TCP	54	50570 + 3389 [ACK] Seq=1 Ack=2443 Win=513 Len=0

Figure 10 : Analyse du trafic réseau II

Afin d'avoir une vue plus globale des trafics et de pouvoir mieux distinguer les protocoles les plus utilisés, nous allons utiliser le « IO Graph » de l'outil menu statistique dans « Wireshark ». Celui-ci va générer un ou plusieurs graphes selon le nombre de graphes choisis. Ces graphes sont coloriés distinctement, et chaque graphe correspond à un protocole. Pour attribuer une couleur à un protocole, il suffit de mettre le nom du protocole dans le champ correspondant à la couleur en question.

Nous avons choisi d'utiliser cinq graphes, et nous avons utilisé la couleur :

- ✓ Noir : pour tous les paquets
- ✓ Vert : pour le protocole « tcp »
- ✓ Orange : pour le protocole « udp »
- ✓ Rouge : pour le protocole « tls »
- ✓ Bleu : pour les erreurs tcp « tcp.analysis.flag »

Ces graphes sont illustrés par la figure 11 et la figure 12 :

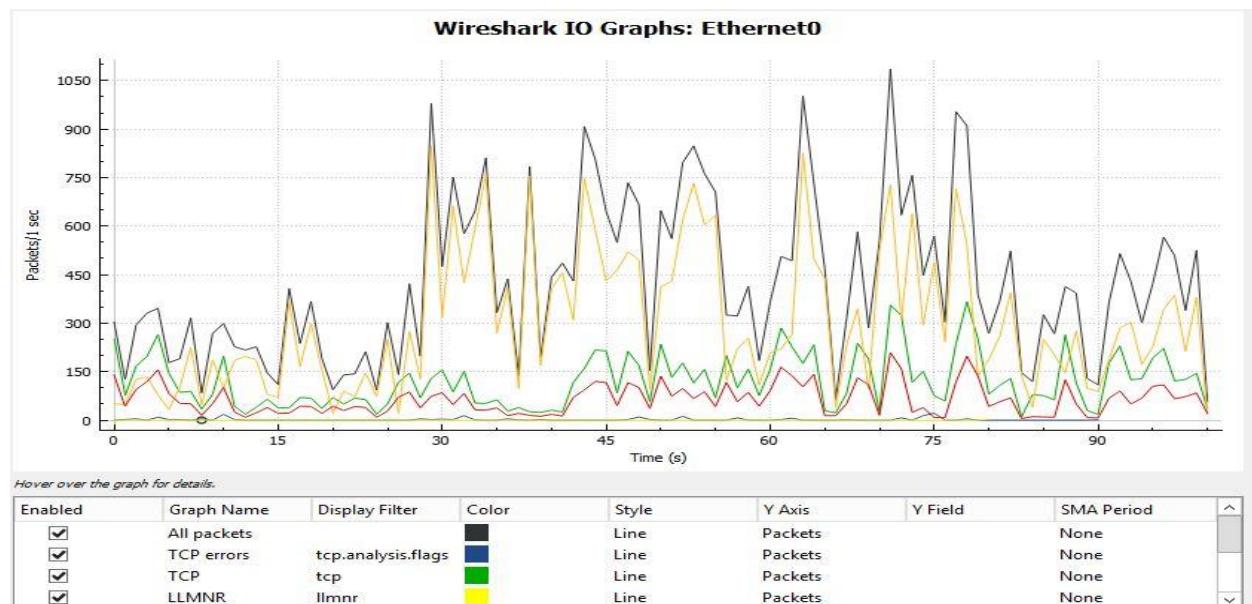


Figure 11 : Graphe de l'analyse du trafic réseau I

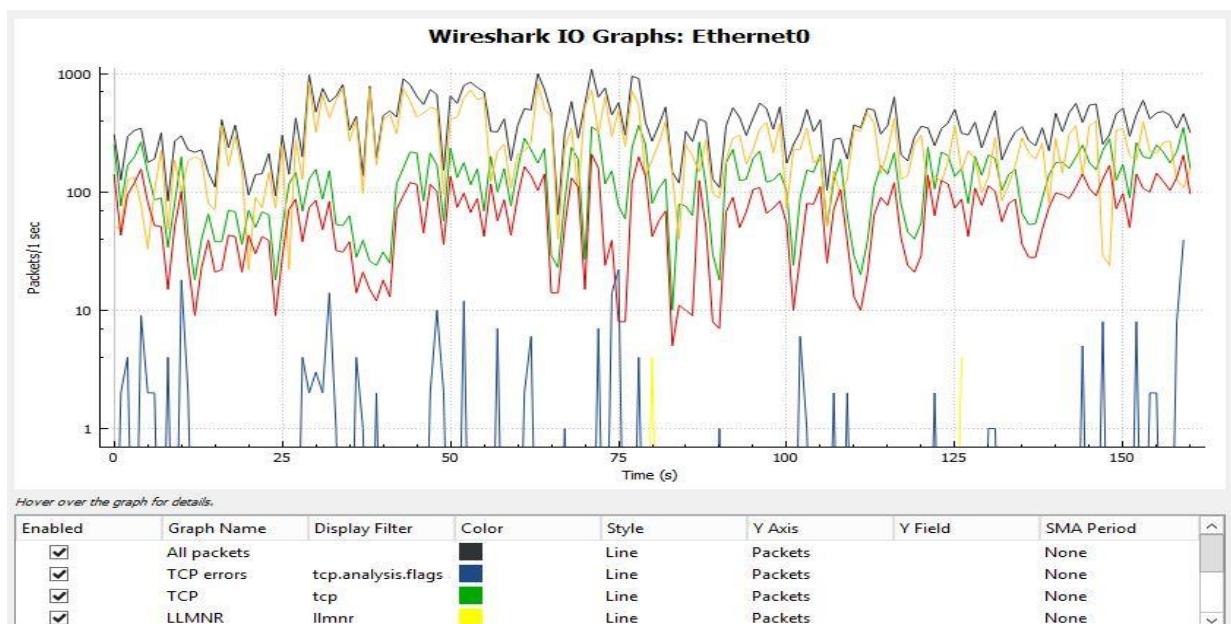


Figure 12 : Graphe de l'analyse du trafic réseau II

Comme on peut le constater dans la figure ci-dessus, les graphes correspondants aux protocoles « UDP » et « TCP » sont un peu élevés, ce qui signifie que l'utilisation des protocoles « UDP » et « TCP » occupe une certaine place dans la bande passante.

En ce qui concerne les autres protocoles, leur niveau est encore tolérable, bien que celui des « erreurs tcp » présente très souvent quelques pics.

### 5.1.13 Sécurité

Avec l'apparition des nouvelles technologies et la diversification des types de réseaux comme la multiplication des mobiles connectés et le développement des solutions de « cloud computing », la gestion des solutions de sécurité réseau est devenue une tâche complexe.

En ce qui concerne la sécurité dans le VDC de l'AITS : elle est assurée par des serveurs Proxy qui agissent comme un filtre afin de définir les règles d'accès à une application et à un réseau comme Internet à cause des risques que peut représenter une connexion normale dans certain cas : d'une part il y a le pare-feu local sur le système pour appliquer les stratégies d'accès et d'autre part les règles de routages déterminant la manière dont les serveurs accèdent à Internet.

## 5.2 Critique de l'existant

Vu l'infrastructure du réseau informatique actuel et à partir de notre étude détaillée du réseau existant dans l'établissement, nous avons remarqué l'existence de points faibles sur différents niveaux :

- Le contrôle et la gestion des sauvegardes réseaux et restaurations sur le site sont absents ;
- Pas de plateforme ou système de sécurité dans le VDC, aucun mécanisme de détection et de prévention d'intrusions. Le pare-feu local est obsolète contre les nouvelles menaces.
- L'absence d'accès privés, depuis l'extérieur, au serveur surtout le serveur d'application qui est le plus utilisé : nous prenons l'exemple de certains responsables qui peinent à y accéder depuis l'extérieur (Internet)...Il peut y avoir soit une indisponibilité au sein du serveur au moment voulu soit une certaine difficulté en cas de besoin majeur.

### Points forts de l'établissement :

- Sécurisé par portail captif les logiciels et applications (Authentification par nom d'utilisateur et mot de passe) pour toutes les personnes qui veulent utiliser une de ses applications. Et l'accès réseau et machine est aussi authentifié par un compte Active Directory.
- Réseau bien segmenté c'est-à-dire les réseaux existants sont séparés en VLAN : il en résulte davantage de bande passante et les réseaux existants ne rencontrent pas de surcharges pour les utilisateurs.
- Très bien doté en équipements de matériels informatiques.

## **5.3 Solutions**

### **5.3.1 Proposition de solutions**

Beaucoup de solutions sont envisageables et disponibles, on a donc effectué l'ébauche des solutions suivantes :

Sauvegarde : les données sont vitales pour toutes les entreprises, qu'elle soit grande ou petite. Ce constat, banal pour tout décideur, masque la complexité des solutions techniques à mettre en œuvre pour en assurer au quotidien le caractère opérationnel, à savoir le stockage de ces données, leur sauvegarde et en cas de crash leur restauration dans les plus brefs délais. Autant de fonctions critiques pour le système d'information de l'entreprise, d'où la nécessité d'un montage d'une politique de sauvegarde et récupération réseau.

Sécurité : la sécurité est un enjeu majeur pour les entreprises. Elle ne relève plus seulement du rôle de l'informaticien. Sa finalité, sur le long terme, est de maintenir la confiance des utilisateurs et des clients. D'où l'importance de la sécurisation du système de l'information et la mise en œuvre d'un système de sécurité inviolable dans le VDC.

Surveillance : la surveillance du réseau est un élément indispensable de la sécurité informatique. Installer d'autres outils de supervision peut avoir une grande valeur dans le suivi de l'infrastructure de l'entreprise.

Accès privé : créer un serveur VPN pour les accès externes dans du réseau interne afin de pouvoir améliorer la gestion de tâches respectives et faciliter ainsi la communication interne ou même externe en cas de besoin de ceux de l'extérieur.

### **5.3.2 Solutions retenues**

Le responsable EXPLOITATION AITS nous a confirmé le choix de la mise en place d'un système de sauvegarde réseau comme solution pour sauvegarder toutes les données des données et d'un serveur VPN pour accéder à l'infrastructure VDC depuis l'extérieur.

## **PARTIE III : CHOIX DE L'OUTIL**

# Chapitre 6 : Comparaison des outils

## 6.1 Outils de Sauvegarde

A l'ère du numérique, les données informatiques ont une valeur indéniable : valeur économique importante pour les entreprises. Pour parer aux éventuels risques de perte de données, la sauvegarde est la seule solution. En général, il existe des outils de sauvegarde pour la mise en place d'une solution de sauvegarde de données en réseau et les plus connus sont :

- Amanda
- Areca Backup
- BackupPC
- Bacula

### 6.1.1 Amanda

AMANDA « Advanced Maryland Automatic Network Disk Archiver » est une solution de sauvegarde qui permet à l'administrateur informatique de configurer un seul serveur de sauvegarde maître pour sauvegarder plusieurs hôtes sur le réseau sur des lecteurs / changeurs de bandes, des disques ou des supports optiques. Amanda utilise des utilitaires et des formats natifs (par exemple, dump et / ou GNU tar) et peut sauvegarder un grand nombre de serveurs et de stations de travail exécutant plusieurs versions de Linux ou Unix. Amanda utilise un client Windows pour sauvegarder les ordinateurs de bureau et les serveurs Microsoft Windows [4].

#### Points forts :

- Configure un seul serveur pour sauvegarder plusieurs clients en réseau sur un système de stockage sur bande ou sur disque.
- Amanda est bien documentée et peut être installée très rapidement.
- Amanda offre la possibilité unique d'écrire des sauvegardes sur bande et sur disque simultanément
- Étant donné qu'Amanda n'utilise pas de pilotes de périphérique propriétaires, tout périphérique pris en charge par un système d'exploitation fonctionne bien avec Amanda.
- Amanda utilise des utilitaires natifs de viddage et / ou de GNU. Les données peuvent être récupérées à l'aide des utilitaires natifs, qu'Amanda soit toujours installée ou non.
- Amanda est très sécurisée. Le cryptage sur un client assure la sécurité des données en transit et le cryptage sur un serveur de sauvegarde.
- Un planificateur unique optimise le niveau de sauvegarde pour différents clients.
- Amanda est stable et robuste grâce à un code de haute qualité.
- Le projet Open Source Amanda a une communauté vaste et productive qui grandit chaque jour.

### **Points faibles :**

- Nécessité d'un lecteur de bande
- Sauvegarde TAR / DUMP
- Temps de sauvegarde long

Site officiel : <http://www.amanda.org/>

Site de téléchargement : <http://www.amanda.org/download.php>

Installation : <https://www.zmanda.com/quick-backup-setup.html>

### **6.1.2 Areca Backup**

Areca Backup est un outil de sauvegarde open source, écrit en java, pratique qui peut fonctionner non seulement sur l'ordinateur local mais aussi en réseau, sur un serveur FTP voire une clé USB. Pour la sécurité des données, il utilise les algorithmes de cryptage DES et AES [5].

Areca Backup propose différents types de filtres et offre à l'utilisateur le contrôle total sur les droits des visiteurs. Après chaque sauvegarde, il peut générer un rapport détaillé de l'opération qui, d'ailleurs, peut être conservé sur le disque ou envoyé directement par email. Comme fonctionnalités supplémentaires, cet outil supporte également la compression des archives ZIP, la récupération des fichiers supprimés accidentellement ainsi que la fusion de deux fichiers.

Logiciel compatible multi-plateforme [5].

### **Points forts :**

- Gestion en ligne de commande possible
- Interface graphique simplifié
- Sauvegarde possible depuis disque dur local, disque réseau, clé USB, FTP, FTPS (ou un serveur SFTP).
- Chiffrement des sauvegardes (AES128 et AES256)
- Propose un système de filtrage puissant (par extension, répertoire, expression régulière, la taille, la date, le statut)
- Propose une sauvegarde incrémentale, différentielle ou complète
- Rapport de sauvegarde qui est stocké sur un disque ou envoyé par mail
- Compresse les archives en zip
- Permet de lancer des scripts Shell après la sauvegarde
- Restauration incorporée

### **Points faibles :**

- Très peu de plugins disponibles à ce jour (disponible seulement SFTP, FTP, FTPS)
- Ne sauvegarde pas les fichiers de configuration d'autres programmes
- Absence de planificateur intégré (peut être intégré à celui de Windows via un script)
- Indisponible en français

Site du produit : <http://www.areca-backup.org/>

Téléchargement : <http://sourceforge.net/projects/areca/files/areca-stable/>

Installation : [http://doc.ubuntu-fr.org/areca\\_backup](http://doc.ubuntu-fr.org/areca_backup)

### **6.1.3 BackupPC**

BackupPC est un logiciel libre de sauvegarde de données informatiques, publié sous licence GPL. Il est utilisé pour sauvegarder un ensemble de postes. Il possède une interface Web pour configurer, lancer des sauvegardes ou restaurer des fichiers [6]. Il est également possible de sauvegarder des bases de données. Les protocoles utilisables pour les transferts sont : SMB, tar over SSH, et rsync. Il ne nécessite l'installation d'aucun logiciel client sur les machines à sauvegarder. Ce produit est multiplateforme [6].

### **Points forts :**

- Interface simple (configuration interface web)
- Pas de client nécessaire si on utilise SMB sous Windows, ou ssh/rsync sous Linux
- Possible de sauvegarder des bases de données via un script Shell lancé avant la sauvegarde
- L'interface web permet aux administrateurs de visualiser les fichiers journaux, la configuration, l'état actuel et permet aux utilisateurs de lancer des sauvegardes, d'annuler, de parcourir et de restaurer des fichiers.
- Un ensemble complet de restauration des options est pris en charge, y compris la restauration directe
- Paramètres de configuration flexibles permettant plusieurs sauvegardes à effectuer en parallèle
- Possible de faire différents plannings de sauvegardes complètes et incrémentielles
- Outil très puissant permettant de sauvegarder plusieurs clients (Linux ou Windows)

### **Points faibles :**

- Les portables sont fortement ralenties lors de la sauvegarde (sollicitation CPU mais surtout accès disque)
- Les données ne sont pas chiffrées sur le serveur
- Problème avec les dual-boots
- Pas de Plugins ni de prise en charge pour les autres programmes

Téléchargement : <http://sourceforge.net/projects/backuppc/?source=navbar>

<https://github.com/backuppc/backuppc/releases>

Site officiel : <http://backuppc.sourceforge.net/info.html>

Installation : <http://doc.ubuntu-fr.org/backuppc>

### **6.1.4 Bacula**

Bacula est un logiciel de sauvegarde, de vérification et de restauration de fichiers en mode client-serveur dans un réseau, distribué en Open Source. Ses composants serveurs tournent sur Linux, Solaris ou FreeBSD. Ses composants clients existent pour de nombreuses autres plateformes, dont MacOs et Windows [7].

Il utilise une base de données relationnelle motorisée par MySQL, PostgreSQL ou SQLite, crée des signatures SHA-1 (ou MD5) pour chaque fichier sauvegardé, permet le chiffrement des données et des commandes transitant sur le réseau et peut sauvegarder des fichiers de plus de 10 Go. Il sait également gérer les robots changeurs de bandes. Enfin, il peut exécuter des scripts avant et après chaque travail. Il possède également plusieurs interfaces graphiques disponibles sous Linux et Windows pour visualiser les sauvegardes, effectuer des sauvegardes et des restaurations [7].

### **Points forts :**

- Multi-plateforme
- Sauvegardes complètes, différentielles ou incrémentales disponibles et très paramétrables
- Accès facile à plusieurs versions d'un même fichier
- Restauration de tout ou partie d'une sauvegarde
- Peut sauvegarder/restaurer sur différentes plateformes (Windows/linux)
- Fonctionne en réseau ou non
- Planification intégrée
- Envoi de mail de compte rendu des sauvegardes
- Restauration des fichiers disponibles
- Sauvegarde sous plusieurs supports (HDD, CD/DVD, bandes magnétiques, USB...)

## Points faibles :

- Avoir une bonne connaissance des principes de sauvegardes pour pouvoir le paramétrier
- Interface graphique pas forcément très intuitive
- Trop complexe
- Beaucoup de documentation disponible
- On ne peut pas reprendre une sauvegarde qui a été interrompue

Site officiel : <http://blog.bacula.org/>

Téléchargement : <http://sourceforge.net/projects/bacula/files/#files>

Installation : <http://doc.ubuntu-fr.org/bacula>

Les tableaux 14 et 15 montrent donc la comparaison entre ces différents utilitaires :

Tableau 14 : Comparaison des outils de sauvegarde (I)

	<b>Areca Backup</b>	<b>Amanda</b>
SE	Linux, Windows	Windows
Type	Local	Client/Serveur
Sauvegarde	Complètes, différentielles, incrémentale	Complètes, différentielles, incrémentale
Restauration	OUI (avancé)	OUI
Planification	Manuelle	OUI
Compression	OUI (zip/zip64)	GZIP
Chiffrement	OUI (AES)	OUI (TLS/SSL optionnel)
Communication	Dépôt FTP/FTPS/SFTP	Agent Amanda installé sur l'hôte client
Administration	Interface graphique/Console	Console

Tableau 15 : Comparaison des outils de sauvegarde (II)

	BackupPC	Bacula
SE	Linux, Windows	Linux, Solaris, FreeBSD
Type	Client/Serveur	Client/Serveur
Sauvegarde	Complètes, différentielles, incrémentale	Complètes, différentielles, incrémentale
Restauration	OUI	OUI
Planification	OUI	OUI
Compression	OUI	OUI (GZIP/LZO)
Chiffrement	NON (Seulement disponible via une connexion SSH)	OUI (MD5, SHA-1)
Communication	SSH, NFS, SMB, rsync	Agent Bacula installé sur l'hôte client
Administration	Interface Web/Console	Interface Web/Console

## 6.2 Serveurs VPN

### 6.2.1 OpenVPN Server

OpenVPN est la solution VPN open source la plus répandue, qui comporte à la fois des solutions VPN open source. Ce logiciel de réseau virtuel est disponible pour Windows, Linux, Solaris, OpenBSD, FreeBSD, NetBSD et Mac. OpenVPN offre une interface de gestion centrale permettant de contrôler à distance le démon OpenVPN [9]. L'interface de gestion peut également être utilisée pour développer une interface graphique ou une application frontale Web pour OpenVPN. Ce serveur VPN open source offre des fonctionnalités de serveur et d'entreprise pour la connexion OpenVPN.

#### ❖ Fonctionnalités clés du serveur OpenVPN

- Access Server est basé sur un logiciel open source .
- VPN de site à site,
- Accès à distance
- Sécurité Wi-Fi
- OpenSSL
- SSL / TLS pour l'authentification de session
- Intégration MacOs X Keychain et Windows Crypto API
- ESP IPSec pour le transport de tunnel sur le protocole UDP
- VPN sans Web
- Fonctions d'équilibrage de charge / de basculement
- Support CRL (Compatible avec)
- Certificats SSL / TLS, RSA
- Protocole de configuration d'hôte dynamique (DHCP)
- Traduction d'adresses réseau (NAT)
- Périphériques virtuels TUN / TAP.

## 6.2.2 Pritunl Server

Pritunl est une bonne alternative au serveur OpenVPN. Il s'agit également d'un serveur VPN distribué open source et à source libre. Pritunl peut virtualiser vos réseaux privés dans des centres de données et fournir un accès simple à distance. Il a à la fois la version gratuite et premium. Dans sa version payante, il faut payer le prix par utilisateur et pouvant créer un réseau VPN cloud prenant en charge des milliers d'utilisateurs simultanés avec un meilleur contrôle de votre serveur VPN [9].

Il possède également un système de plug-in de base Python qui permet d'étendre et de modifier les fonctionnalités de Pritunl. L'administrateur peut également créer des plug-ins pour prendre en charge les systèmes d'authentification personnalisés et le contrôle. Pritunl prend en charge tous les clients OpenVPN disponibles sur Windows, MacOs, Linux, Android, Apple iOS et Chromebook. Avec l'aide du plugin Pritunl pour Ubiquiti EdgeMax, l'intégration aux routeurs Edge pour une gestion facile est possible. Pour d'autres services, cela permet également l'intégration de l'API RESTful.

### Fonctionnalités clés de Pritunl Server :

- Port Forwarding
- Liens de passerelle
- Passerelle de basculement
- Contourner l'authentification secondaire
- Support Chromebook
- Email des clés d'utilisateur
- Authentification unique
- Basculement automatique
- Serveurs répliqués
- Intégration AWS VPC
- VPN de site à site
- Route du serveur
- Contrôle NAT
- Cartographie DNS
- Mode VPN ponté
- Accès API
- Liens de site à site IPSec
- Peering VPC
- Basculement automatique de lie

### **6.2.3 SoftEther Server**

**SoftEther VPN** signifie « logiciel Ethernet » et un autre logiciel serveur VPN open source multi-protocole facile à utiliser qui peut être exécuté sur Windows, Linux, Mac, FreeBSD et Solaris. L'utilisation de ce logiciel VPN à des fins personnelles et commerciales gratuitement. SoftEther VPN prend également en charge Microsoft SSTP VPN pour Windows Vista / 7/8/10 [9].

#### **Fonctionnalités clés de SoftEther VPN**

- Accès à distance et VPN de site à site.
- Tunneling SSL-VPN sur HTTPS pour passer à travers les NAT et les pare-feux.
- Fonctionnalités VPN sur ICMP et VPN sur DNS révolutionnaires.
- Résistance au pare-feu hautement restreint.
- DNS dynamique intégré et traversée NAT.
- Cryptages AES 256 bits et RSA 4096 bits.
- SSL-VPN (HTTPS) et 6 principaux protocoles VPN (OpenVPN, IPsec, L2TP, MS-SSTP, L2TPv3 et EtherIP) sont tous pris en charge en tant que protocoles sous-jacents de tunneling VPN.
- La fonction de clonage OpenVPN prend en charge les clients OpenVPN hérités.
- Double pile IPv4 / IPv6.
- Le serveur VPN fonctionne sous Windows, Linux, FreeBSD, Solaris et Mac OS X.
- Configurez tous les paramètres sur l'interface graphique.
- Fonction d'authentification de certificat RSA.
- Fonction de liste de contrôle d'adresse IP source.

### **6.2.4 Server VPN OpenConnect**

Le serveur OpenConnect est un serveur VPN SSL open source, de petite taille, rapide, sécurisé et facilement configurable. Ce serveur utilise le protocole VPN SSL OpenConnect pour fournir un service VPN, ainsi que la compatibilité avec les clients utilisant le protocole VPN SSL AnyConnect de Cisco. Cette implémentation de serveur VPN prend actuellement en charge la plate-forme GNU / Linux et d'autres variantes UNIX. Un double canal VPN TCP / UDP et les protocoles de sécurité IETF standard utilisés par le protocole OpenConnect pour assurer la sécurité [9].

## **Caractéristiques clés du serveur VPN OpenConnect**

- Méthodes d'authentification prises en charge : PAM, Radius, fichier de mot de passe, HOTP / TOTP, authentification par clé publique (certificat) ;
- Prise en charge de la clé de serveur, d'un module de sécurité matérielle (HSM) ou d'une carte à puce.
- Prend en charge deux canaux VPN simultanés, IPv6 et IPv4.
- Peut gérer les limites de ressources
- Prend en charge le protocole proxy.
- Prise en charge de l'itinéraire poussant
- Prise en charge de la limitation (par le pare-feu) des clients aux routes autorisées
- La capacité de traitement varie en fonction du nombre de processeurs et plus.

Tous les outils présentés ci-dessus sont utilisables pour parer à tout risque de perte de précieuses données mais après avoir comparé les différents outils, nous avons opté pour ceux-ci :

- BACULA pour la mise en place d'un serveur de sauvegarde et restauration réseau ;
- PRITUNL pour la mise en place d'un serveur VPN.

# Chapitre 7 : Présentation de l’Outil Choisi

## 7.1 Bacula

### 7.1.1 Introduction

La sauvegarde (*backup*, en anglais) consiste à dupliquer des données stockées dans le Système Informatique (SI) de l’entité, afin de les mettre en sécurité [19].

Cette mise en sécurité a pour but de répondre à deux éventualités de restauration (l’opération inverse de la sauvegarde) :

- La restauration de tout ou partie du SI, suite à une dégradation importante du SI
- La restauration de quelques fichiers, suite à une *corruption* ou une *destruction* limitée de données.

Si celle-ci doit, de plus, se faire au travers des réseaux de machines, de systèmes d’exploitation nombreux et variés, les solutions deviennent alors plus rares. Parmi le peu de solutions libres disponibles, il existe Bacula. Celle-ci n’est pas suffisamment connue malgré ses nombreuses qualités. La question se pose : pourquoi sauvegarder ?

Étant donné que des dysfonctionnements peuvent apparaître sur les applications et le matériel informatique indépendamment du degré de fiabilité d’un ordinateur ou d’un serveur, il est essentiel de posséder une bonne solution de sauvegarde. Auparavant coûteuses et compliquées, ces solutions sont à présent très abordables, faciles d’utilisation, et, selon un certain choix, peuvent être complètement automatisées.

Si les données et le temps sont primordiaux, il est dans l’intérêt de l’utilisateur de développer une stratégie basée sur ses besoins pour sécuriser les données et de choisir les logiciels et le matériel qui conviennent à cette stratégie.

Bacula est une solution de sauvegarde par le réseau sur un modèle client/serveur, c’est un logiciel libre sous licence GNU version 2. Il est développé depuis 2000 et dispose d’un grand nombre de fonctions parmi lesquelles le multi-volume et le multi-support.

Il est libre, extrêmement puissant, le logiciel dispose d’un ensemble de fonctionnalités extrêmement intéressant, et d’une qualité professionnelle. Bacula peut également fonctionner entièrement sur un seul ordinateur et peut sauvegarder sur différents types de supports, notamment des bandes et des disques.

En termes techniques, il s’agit d’un programme de sauvegarde réseau client / serveur, tout en offrant de nombreuses fonctionnalités avancées de gestion du stockage facilitant la recherche et la récupération de fichiers perdus ou endommagés. En raison de sa conception modulaire, Bacula est extensible depuis des systèmes informatiques simples jusqu’aux systèmes comprenant des centaines d’ordinateurs situés sur un grand réseau [7].

## **7.1.2 Principales caractéristiques**

Bacula est un ensemble de programmes sous licence libre GNU Public Licence, permettant à un administrateur système de contrôler la sauvegarde, la restauration et la vérification de données informatiques par le réseau. Les clients peuvent être de types variés. Des pré- et post- scripts aux travaux de sauvegardes, voire de restauration, permettent une flexibilité importante et ouvrent des choix limités uniquement par l'imagination des administrateurs systèmes. Le premier exemple est bien entendu la création d'instantanés des systèmes de fichiers clients le permettant, comme pour les clients sous Linux. Les clients Windows profitent directement de la fonction d'instantanés offerte par VSS. Le nombre de clients peut être très important et ces derniers sont potentiellement répartis sur de larges réseaux. Les systèmes d'exploitation pouvant faire tourner la partie serveur du projet sont beaucoup moins nombreux. Linux est celui préféré pour cette tâche et le reste de l'article sera basé sur ce choix.

### **7.1.2.1 Généralité**

Bacula est le seul projet libre de sauvegarde à baser son catalogue sur une base de données relationnelle de type SQL. Cet élément est donc le seul à n'être pas écrit par les développeurs du projet. Le choix de la base est laissé à la discréption de l'utilisateur lors de l'installation. Les supports de sauvegardes sont variés. Les disques durs et bandes magnétiques sont bien évidemment supportés, avec, en option, des bibliothèques robotisées pour ces dernières. Mais il est aussi possible d'utiliser des CD ou des DVD. Les sauvegardes pourront ensuite migrer d'un support à un autre. Toutes les informations permettant de retrouver les données souhaitées se trouvent ainsi stockées dans le catalogue.

Le logiciel se découpe en 4 parties :

- Une ou plusieurs bases de données qui servent de catalogue (tâches, liens vers les fichiers, événements...)
- Un ou plusieurs directeurs qui gèrent l'ensemble des stratégies de sauvegarde et référencent les clients
- Un ou plusieurs services de stockage qui vont gérer un ensemble de volumes virtuels ou physiques
- Des clients à sauvegarder.

### **7.1.2.2 Avantages**

Bacula offrent les avantages suivants :

- Base de données supportée par MySQL, PostgreSQL ou SQLite
- Signature sécurisée (cryptage SHA-1 ou MD5)
- Chiffrement des données et des commandes transitant sur le réseau
- Sauvegarde de fichiers de plus de 10 Go
- Gestion des bandes automatisée
- Scripts personnalisables
- Sélection d'interfaces graphiques préinstallées (Template)
- Sauvegardes complètes, incrémentales et différentielles
- Multi-serveurs / multi-stations en réseau (Unix ou Windows)
- Accès facile à plusieurs versions d'un même fichier
- Restauration de tout ou partie d'une sauvegarde
- Peut sauvegarder/restaurer sur différentes plateformes (Windows/linux)
- Fonctionne en réseau ou non
- Planification intégrée
- Envoi d'e-mails de compte-rendus des sauvegardes

### **7.1.3 Architecture**

Comme vu précédemment, le projet Bacula se base sur le principe de client-serveur. Les tâches sont séparées. Une tâche correspondant à un démon et toutes les communications s'effectuant sur le réseau en TCP/IP, il est facile de répartir les tâches sur des machines distinctes.

La Figure 13 présente l'architecture d'une installation de Bacula :

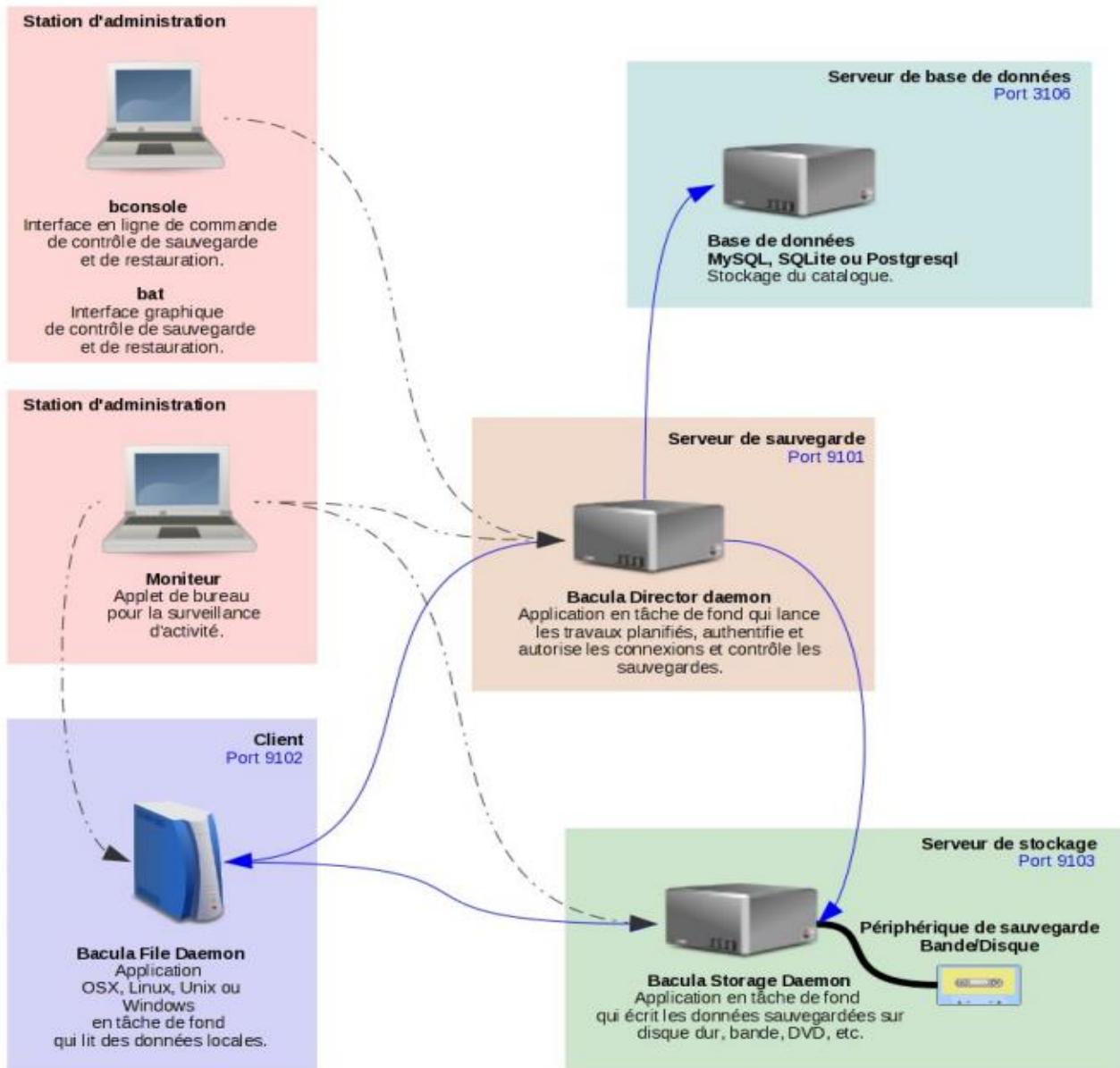


Figure 13 : Architecture du logiciel

Source [12]

### 7.1.3 Composants de Bacula

Bacula est composé de plusieurs composants et services utilisés pour gérer les fichiers vers les emplacements de sauvegarde et de sauvegarde :

- Bacula Director, « Directeur » ;
- Bacula Storage, « Storage Daemon » ;
- Bacula File, « Filer Daemon » ;
- Bacula Console, « Console » ;
- Catalog, « Catalogue ».

#### 7.1.3.1 Directeur

Directeur, est le cœur du système, il centralise, dirige et planifie toutes les opérations de sauvegarde, restauration, vérification et archivage de Bacula. Directeur est exécuté en tant que daemon ou service (tâche de fond) [11].

L'administrateur système utilise Bacula Directeur pour planifier des sauvegardes et récupérer des fichiers. Il se présente sous la forme d'un daemon : « **bacula-dir** » qui écoute sur le port 9101, Il ne peut y avoir qu'un directeur par architecture de sauvegarde (pas de réPLICATION).

#### 7.1.3.2 Storage Daemon

Les services « Bacula Storage » sont constitués des programmes logiciels qui effectuent le stockage et la récupération des attributs de fichier et des données sur le support ou les volumes de sauvegarde physiques. En d'autres termes, le « Storage Daemon » est responsable de la lecture et de l'écriture des bandes (ou de tout autre support de stockage, par exemple, des fichiers) [12].

Le matériel doit donc être connecté “logiquement” au serveur qui exécute ce « Storage daemon » (il doit être “monté”). Ce daemon, « **bacula-sd** » écoute sur le port 9103.

Il reçoit les ordres du directeur mais aussi et surtout les données directement du « Filer Daemon » (voir ci-dessous). A noter qu'il peut évidemment y avoir plusieurs « Storage daemon » par architecture de sauvegarde.

#### 7.1.3.3 Filer Daemon

Le service « Bacula File » (ou le programme client) est le programme installé sur la machine à sauvegarder. Il est spécifique au système d'exploitation sur lequel il s'exécute et doit fournir les attributs des fichiers et les données demandés par le directeur Bacula [12]. Il s'appelle « **bacula-fd** » écoute sur le port 9102, reçoit les ordres du directeur et envoie les données directement au « Storage Daemon ».

Les services de fichier sont également responsables de la partie du système de fichiers liées à la restauration des attributs de fichiers et des données aux cours d'une opération de récupération. Ce programme est exécuté en tant que démon sur la machine client. En plus des démons de fichiers Unix/Linux, il existe un démon de fichiers Windows. Le « File Daemon » de Windows fonctionne sur les toutes versions de Windows (depuis NT, 2000, XP, Server).

#### **7.1.3.4 Console**

Le service « Bacula Console » est le programme qui permet à l'administrateur ou à l'utilisateur de communiquer avec le directeur Bacula. C'est elle qui permet de contrôler le directeur, mais aussi directement les « filer » et « Storage Daemons ». Elle peut être exécutée sur une machine distincte (connexion par le port 9101) [12].

Quatre (4) Consoles sont aujourd'hui disponibles :

- Bconsole, accessible en mode texte (ligne de commande), est un outil très puissant pour des sysadmin.
- BAT, client lourd graphique écrit en QT, sait gérer plusieurs Directeurs.
- Baculum, console graphique
- Bweb, écrit en Ajax et full web, intègre des modules de « reporting » et des fonctions avancées.

#### **7.1.3.5 Catalogue**

Les services de catalogue comprennent les logiciels responsables de la maintenance des index de fichiers et des bases de données de volumes pour tous les fichiers sauvegardés. Ces services de catalogue permettent à l'administrateur système ou à l'utilisateur de localiser et de restaurer rapidement le fichier souhaité. Ils distinguent Bacula des programmes de sauvegarde simples tels que tar et bru, car le catalogue conserve un enregistrement de tous les volumes utilisés, de toutes les tâches exécutées et de tous les fichiers enregistrés, ce qui permet une restauration et une gestion des volumes efficaces. Bacula supporte actuellement trois bases de données différentes, MySQL, SQLite et PostgreSQL, dont l'une doit être choisie lors de la construction de Bacula [12]. Les deux bases de données SQL actuellement prises en charge (MySQL et PostgreSQL) fournissent un grand nombre de fonctionnalités, notamment l'indexation rapide, les requêtes arbitraires et la sécurité (communication par le port 3106 avec le Directeur).

## 7.1.4 Tâche de sauvegarde

### 7.1.4.1 Concept de « job »

Les tâches de sauvegardes et de restauration sont appelées « **job** ». Pour chacune des tâches définies on peut définir les propriétés (ou ressources) suivantes :

- La planification de la tâche (Schedule),
- Un niveau de sauvegarde (Complète, Incrémentielle, Différentielle),
- Une machine cliente,
- Un ensemble de fichiers ou répertoires à sauvegarder ou restaurer,
- Une ou plusieurs adresses email pour envoyer les messages en cas de succès ou d'échec de la tâche,
- Un périphérique de stockage,
- Un script à lancer avant ou après la tâche.

### 7.1.4.2 Ressource « Client »

Le client est la machine- cible qui va être utilisée pour le job.

Pour chaque client, on définit :

- L'adresse IP et le port du service client,
- Un mot de passe,
- Une période de conservation pour les fichiers et/ou les jobs (durée pendant laquelle les informations vont être stockées dans le catalogue).
- Si la purge des données doit être effectuée de manière automatique lorsque la durée de conservation des données est atteinte.

### 7.1.4.3 Ressource « FileSet »

La ressource « **FileSet** » permet de spécifier l'ensemble des fichiers et répertoires à sauvegarder (ou restaurer) et les options à utiliser pour effectuer la sauvegarde des données définies. La définition d'un **FileSet** permet :

- D'inclure des fichiers et des répertoires récursivement et en utilisant ou non des expressions régulières,
- D'exclure des fichiers et/ou des répertoires (on peut également utiliser des expressions régulières),
- D'activer une option de compression des données,
- De demander le calcul de la signature SHA1 ou MD5 des fichiers.

#### **7.1.4.4 Niveau de sauvegarde**

Il y a trois niveaux de sauvegarde différents :

- **Complète** : sauvegarde de tous les fichiers définis dans le FileSet qu'ils aient changé ou non depuis la dernière sauvegarde.
- **Incrémentale** : sauvegarde de tous les fichiers définis dans le FileSet qui ont été modifiés depuis la dernière sauvegarde réussie pour le même Job pour le même FileSet et le même Client.
- **Differentielle** : sauvegarde de tous les fichiers définis dans le FileSet qui ont été modifiés depuis la dernière sauvegarde complète réussie pour le même Job.

Si le directeur ne peut pas trouver de sauvegarde complète pour le même Job, les sauvegardes incrémentielles et différentielles vont être remplacées par des sauvegardes complètes.

#### **7.1.4.5 Planification d'un Job (Schedule)**

La planification (Schedule) d'un Job consiste à définir la période et les niveaux de sauvegarde pour les différentes programmations d'exécution. La planification d'un Job est la base de la politique de sauvegarde et ceci pour plusieurs raisons :

- La planification des Jobs doit se faire selon la criticité des données et de leur cycle de vie (données peu changeantes, modifiés constamment).

Bacula autorise des planifications complexes en utilisant des combinaisons de mois, jours, heures, périodes (monthly, weekly, daily, hourly) ainsi qu'un niveau de sauvegarde spécifique pour chaque exécution.

Comme on pourrait définir la planification suivante :

- Sauvegarde complète tous les premiers dimanches du mois à 0h00
- Sauvegarde différentielle tous les 2<sup>e</sup> à 5<sup>e</sup> dimanche du mois à 0h00
- Sauvegarde incrémentale du lundi au samedi à 0h00

#### **7.1.4.6 Ressource "Storage"**

La ressource "Storage" permet de définir quel serveur et périphérique de stockage va être utilisé pour un Job donné.

Pour chacune de ces ressources on définit :

- L'adresse IP et le port utilisé pour joindre le service de stockage,
- Un mot de passe,
- Un périphérique à utiliser parmi l'ensemble des périphériques proposés par le service de stockage,
- Le type de média utilisé

#### **7.1.4.7 Ressource "Pool"**

Notion de Volume = stockage physique (fichier sur disque ou bande)

Pool = ensemble de volumes qui sont utilisés pour recevoir des données. Un Pool est un conteneur virtuel qui permet de gérer un ensemble de volumes.

Le Pool possède un ensemble de propriétés qui permettent de définir la gestion des volumes :

- Nommage automatique des volumes grâce à une règle prédefinie,
- Gestion du recyclage des volumes,
- Gestion de l'expiration des volumes.

#### **7.1.4.8 Ressource « Volume »**

Au niveau de Bacula, les volumes peuvent être créées manuellement en utilisant la console Bacula ou bien automatiquement si les supports physiques sont disponibles et une règle de nommage est définie au niveau des Pools qui utilisent ces volumes.

La création d'un volume est synonyme de labellisation au niveau Bacula. En effet un petit fichier est positionné en début de chaque volume pour l'identifier et ainsi éviter les erreurs de manipulation.

Le format du label peut être composé de variables prédéfinies qui sont traduites au moment de la labellisation d'un volume. On peut ainsi inclure dans le label le nom du Job, la date et l'heure courante, le niveau de sauvegarde.

#### **7.1.4.9 Règles de nommage des volumes**

Il est intéressant de définir des règles de noms pour les volumes afin de les identifier rapidement et pouvoir en cas de défaillance du système restaurer les données manuellement.

Règle de nommage simple :

<nom\_job> (<level>) ?-MM-JJ.hh.mm

Où :

- <nom\_job> est le nom donné au Job,
- <level> est le niveau de sauvegarde utilisé pour le volume (Complète, Incrémentale ou Différentielle),
- MM-JJ.hh.mm est la date de création du volume.

Le fait d'utiliser la date dans le nom d'un volume permet d'identifier facilement les données contenues dans une archive. Toutefois cela interdit toute réutilisation future du volume qui conserve son label.

Sur disque, les fichiers sont produits continuellement sans être pour autant effacés lorsque les informations sont purgées du catalogue si la place disque disponible est suffisante. On pourra utiliser un script pour effacer automatiquement les fichiers sur disque correspondant à des volumes purgés.

#### **7.1.4.10 Utilisation des volumes**

Le cycle de vie des volumes est défini dans la configuration du Pool auxquels ils appartiennent. Ainsi un volume peut être considéré comme utilisé en fixant :

- Un nombre maximum de Jobs pour le volume,
- Une durée maximum d'utilisation (depuis la première écriture),
- Une taille maximum pour le volume.

Si une des limites est atteinte, Bacula va marquer le volume comme étant utilisé ("Used") et va continuer avec le volume disponible suivant dans le pool ou attendre l'introduction d'un nouveau volume si aucun n'est disponible.

#### **7.1.4.11 Conservation des volumes et recyclage**

Les volumes sont référencés dans le catalogue de Bacula pour une période définie dans la configuration du Pool auquel ils appartiennent.

Quand la période de conservation est dépassée, les volumes peuvent être automatiquement supprimés du catalogue ainsi que toutes les informations relatives aux Jobs qu'ils contiennent. Cela évite que le catalogue ne grossisse indéfiniment.

Il est possible de recycler les volumes à l'intérieur d'un pool pour l'utilisation d'un « auto changer » par exemple. Bacula permet de définir que le prochain volume utilisé sera le plus vieux du pool, en tenant compte ou non de la période de conservation.

#### **7.1.4.12 Gestion manuelle des volumes**

La console Bacula permet de gérer les volumes de manière manuelle et notamment de :

- Mettre à jour les propriétés d'un volume (recycle flag, use duration, retention period...),
- Supprimer les informations du catalogue relatives à un volume en tenant compte de la période de conservation,
- Purger les informations du catalogue relatives à un volume,
- Effacer un volume du catalogue,
- Labelliser un nouveau volume.

#### **7.1.4.13 Messages**

Bacula est capable d'envoyer des messages via email quand un job est terminé ou qu'une erreur est détectée mais également de définir les logs des résultats dans un fichier.

Bien que chaque service (ou démon) soit capable d'envoyer des messages indépendamment du directeur, les messages sont routés vers ce dernier. Cela permet de grouper tous les messages relatifs à un Job dans le même mail ou de définir les logs dans le même fichier.

Chaque message généré par Bacula possède un niveau d'information tel qu'INFO, ATTENTION, ERREUR, FATAL, etc. Il est possible de router les messages différemment selon le type du message.

### **7.1.5 Fonctionnalités de Bacula**

Bacula est une solution avancée de sauvegarde réseau pour des systèmes de type Unix mais qui fonctionne également sous Windows.

Il comporte un ensemble de programmes qui permet de gérer les sauvegardes, les restaurations ainsi que les vérifications de données d'un ordinateur sur un réseau hétérogène.

Ses fonctionnalités générales :

- Sauvegarde et restauration Réseau
  - Utilisation de ports déclarés
- Ordonnancement des tâches de sauvegarde et parallélisation
  - Gestion des priorités pour chaque tâche
- Sauvegarde multi-volume s
  - Gestion de pools de cartouches
- Mécanismes d'authentification des modules
  - Utilisation de mots de passe (CRAM-MD5)
- Sécurité des transferts (SSL/TLS)
- Contrôle d'intégrité des fichiers sauvegardés
- Le catalogue peut être recréé à partir des fichiers sauvegardés en cas de perte de la base de données.

#### **7.1.5.1 Exécution de scripts**

Bacula est capable d'exécuter un script sur le serveur lui-même ou sur le client avant et/ou après l'exécution d'un Job.

Cette fonctionnalité peut permettre notamment de faire la sauvegarde d'une base de données avant d'en sauvegarder le dump.

#### **7.1.5.2 Lancement d'une tâche**

Les Jobs qui sont planifiés sont démarrés automatiquement par le programmeur interne de Bacula selon leur configuration.

Un Job planifié ou non peut être démarré ou annulé en utilisant la console Bacula.

La console permet d'obtenir la liste des jobs qui tournent et de ceux qui sont terminés.

#### **7.1.5.3 Clonage de Jobs**

Il est possible de cloner des Jobs afin de faire démarrer deux (02) tâches en même temps par exemple. La définition de la première tâche contient alors une directive qui lui impose de démarrer la seconde tâche lorsqu'elle est elle-même exécutée.

Le clonage des Jobs permet aussi de sauvegarder un même ensemble de fichiers en parallèle sur 2 supports de stockage différents.

#### **7.1.5.4 Lancer des tâches en parallèles**

Bacula est capable d'exécuter plusieurs tâches en parallèle. Ceci permet d'exécuter les tâches plus rapidement sans devoir attendre la fin d'une tâche avant d'en démarrer une autre. De plus, si une tâche est bloquée (en attente d'un changement de bande par exemple), cela permet aux autres tâches de s'exécuter sans devoir attendre le déblocage de la première tâche.

Il y a plusieurs contrôles de concurrence dans le logiciel Bacula :

- au niveau du client,
- au niveau du service de stockage,
- au niveau du directeur pour lui-même et pour chacune des ressources (jobs, clients, stockages).

Attention à ne pas avoir deux (02) tâches en concurrence sur un même volume.

#### **7.1.5.5 Restauration de fichiers**

Bacula permet de restaurer des fichiers et répertoires à la demande en utilisant les archives disponibles.

Il est ainsi possible de restaurer une version particulière d'un fichier en choisissant la date à laquelle il a été sauvegardé s'il est présent dans plusieurs archives. La restauration peut s'effectuer en utilisant la console Bacula ou encore en utilisant le panneau de restauration disponible dans la version graphique de la console.

La restauration de fichiers peut se faire à un endroit différent de celui d'origine afin de conserver les fichiers originaux.

La restauration de fichiers peut se faire sur un client différent de celui d'origine ce qui permet de dupliquer des données sur plusieurs machines.

#### **7.1.5.6 Jobs bloqués**

Il se peut qu'une tâche soit bloquée pour diverses raisons (disque plein, bande pleine, bande manquante dans le lecteur, client déconnecté...). En plus d'envoyer un message aux opérateurs, il est possible de définir des actions automatiques pour éviter l'accumulation de tâches en attente :

- Il est possible d'annuler automatiquement une tâche bloquée pendant une durée maximum,
- Il est possible d'annuler une tâche qui est en attente dans la queue des tâches pendant une durée maximum,

À tout moment il est possible d'annuler une tâche en utilisant la console Bacula ou l'administration graphique.

### **7.1.7 Base de données**

Bacula utilise une base de données SQL, telle que MySQL ou PostgreSQL, pour gérer son catalogue de sauvegardes. Nous allons utiliser MariaDB, un remplaçant instantané de MySQL.

#### **7.1.7.1 Généralités**

MariaDB est une version améliorée et pouvant être utilisée en remplacement direct de MySQL et est disponible sous la licence GPL v2. Il est développé par la communauté MariaDB avec comme principal contributeur la fondation MariaDB [18].

MariaDB est un SGBD (système de gestion de base de données) open source. Il est hautement compatible avec MySQL et permet aux utilisateurs de migrer sans efforts des bases de données depuis MySQL vers MariaDB. Avec MariaDB, nous pouvons lire, mettre à jour et gérer les données facilement et de manière efficace.

#### **7.1.7.2 Sécurité**

La sécurité est l'un des principaux objectifs des développeurs de MariaDB. Le projet maintient ses propres jeux de patchs de sécurité en plus de ceux de MySQL. Pour chaque version de MariaDB, les développeurs incluent également les patchs de sécurité de MySQL et les améliorent si nécessaire. Quand des failles de sécurité critiques sont découvertes, les développeurs préparent et distribuent immédiatement une nouvelle version de MariaDB afin de régler le problème aussi vite que possible [18].

Un grand nombre de failles de sécurité découvertes dans MySQL et MariaDB ont été découvertes et reportées par l'équipe de MariaDB. L'équipe de MariaDB travaille en proche collaboration avec « CVE », « <http://cve.mitre.org/> » afin de s'assurer que toutes les failles de sécurité sont reportées rapidement et avec suffisamment de détails. Les détails sur les failles sont habituellement divulgués après que les versions corrigées de MariaDB ainsi que de MySQL ait été publiées.

**Common Vulnerabilities and Exposures (CVE)** est une liste d'identificateurs communs pour les vulnérabilités de cyber-sécurité connues du public.

#### **7.1.7.3 Compatibilité**

MariaDB est maintenu actualisé en permanence à partir de la dernière version de MySQL de la même branche et à bien des égards MariaDB fonctionneront exactement comme MySQL. Toutes les commandes, les interfaces, les bibliothèques et les APIs qui existent dans MySQL existent également dans MariaDB. Il n'y a pas besoin de convertir les bases de données pour passer à MariaDB. MariaDB peut être utilisé en remplacement direct de MySQL ! En outre, MariaDB dispose de beaucoup de nouvelles fonctionnalités.

## 7.1.8 Outils autour de Bacula

### 7.1.8.1 Bacula Web

Bacula-Web est un outil Web basé sur PHP qui fournit une vue résumée des travaux, des pools et des volumes. Il obtient ses informations dans la base de données de catalogue Bacula [13].

Les principaux avantages de Bacula-Web sont

- Il est basé sur le Web, nous pouvons donc y accéder simplement via votre navigateur préféré depuis n'importe où
- C'est facile à installer
- Il contient beaucoup d'informations sur une seule page
- Réactive et responsive, Bacula Web peut être consulté sur les smartphones, les tablettes ou les ordinateurs de bureau

La figure 14 illumine l'interface web « Dashboard » de Bacula :

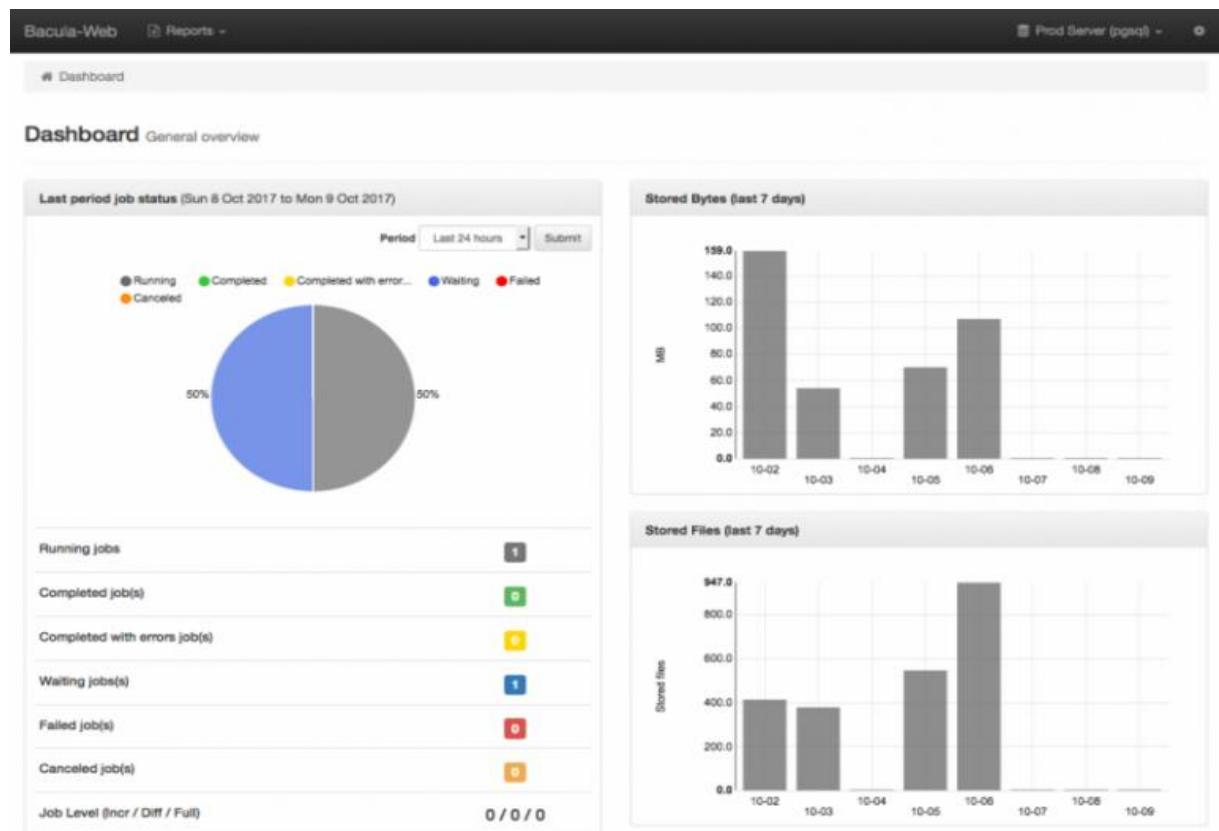


Figure 14 : Dashboard Bacula

Bacula-Web permet de surveiller tous les rapports de travaux effectués par Bacula à partir d'un point unique. Il fournit un aperçu général des tâches, volumes, pools, statistiques du catalogue Bacula, du nombre d'octets / Files protégés par Bacula en choisissant une période prédéfinie comme les dernières 24 heures, la semaine dernière, le mois dernier ou depuis le début de la période.

### 7.1.8.2 Webmin

Webmin est un programme qui simplifie l'administration des systèmes Linux ou Unix. En effet pour créer des comptes, installer un serveur web ou configurer un serveur de messagerie, il faut généralement éditer à la main les fichiers de configuration ou exécuter des commandes. Webmin permet de réaliser ces tâches via une interface web en mettant à jour toute la configuration nécessaire. Le travail d'administration système se trouve alors grandement simplifié [14].

#### ❖ Fonctionnalités :

L'interface de Webmin est accessible avec un navigateur web en HTTPS à l'url <https://machine:10000>. La console se divise en sept (07) catégories qui permettent de gérer l'application Webmin, le système local dans son ensemble mais aussi des systèmes distants. Voici un extrait des menus :

- Webmin
- Système
- Serveurs
- Réseau
- Matériel
- Cluster
- Autres

Beaucoup de modules sont déjà présents dès l'installation du programme et ils ont exploitables si le service ou le package est opérationnel. L'utilisateur accède donc très rapidement, aux points clés de sa configuration aussi simplement qu'avec un environnement graphique. Y compris le module Bacula une fois qu'il est mis en place.

#### ❖ Intérêts pour l'entreprise

- Administration simplifiée
- La délégation des tâches
- L'open source : un petit pas sur la banquise, un grand pas pour l'entreprise
- Administration multi- système

#### ❖ A qui s'adresse Webmin ?

Webmin s'adresse à ceux qui ont une expérience avec Linux mais qui ne sont pas aguerris à l'administration de ce système. Ce dernier requiert toutefois une bonne connaissance des réseaux TCP/IP, mais aussi celle de l'organisation du système de fichier UNIX et la compréhension des principaux services que peut fournir un tel système.

Webmin fonctionne avec les priviléges « **root** », cela signifie qu'il est tout à fait possible de détruire le système en cas de manipulation incorrecte.

Pour les utilisateurs expérimentés en administration UNIX, l'interface un peu lente de Webmin ne fera pas gagner de temps, cependant elle permet de bénéficier du contrôle automatique de la syntaxe et d'un ensemble d'actions qui sont réalisées automatiquement. Il est également possible de donner différents niveaux d'accès dans Webmin. Il est alors possible de déléguer sans risque les tâches d'administration à ses collaborateurs. Par exemple, l'administrateur ne permet à quelqu'un que d'administrer le serveur de bases et données et rien d'autre.

Avec Webmin, l'administration de toutes les tâches de Bacula peut être gérée dans l'interface web.

## 7.2 Pritunl

### 7.2.1 Introduction

Les entreprises ont souvent besoin de donner à leurs salariés en déplacement un accès privé à l'informatique de l'entreprise. Avec un nombre croissant de ménages déposant leurs documents personnels sur de grands disques en réseau, il n'est pas étonnant que beaucoup de personnes aient besoin d'être en mesure d'accéder à leurs données et aux applications de l'entreprise via un VPN lorsqu'elles sont sur la route ou en dehors du la société. Cependant, quel devrait être l'outil de choix pour cette tâche ?

À une époque, IPSec était plus ou moins la norme en matière de VPN ; cependant, OpenVPN s'est construit au fil des années une excellente réputation en matière de sécurité et de facilité d'utilisation. Après une installation d'Ubuntu 14.04, par exemple, il suffit d'ajouter le paquet « OpenVPN » pour faire fonctionner un serveur OpenVPN. De plus, OpenVPN est très facile à configurer côté client : Android est livré avec un client OpenVPN prêt à l'emploi et en utilisant iOS, il y a un outil de correspondance dans l'App Store. Les clients Windows, Linux et OS X sont également disponibles. Dans l'idéal, établir une configuration client-serveur opérationnelle avec OpenVPN ne prend que quelques minutes. Pritunl, basé sur le protocole OpenVPN, promet simplement d'être la solution VPN idéale pour pratiquement n'importe quelle implémentation et pour dépasser les fonctionnalités et le confort d'OpenVPN [15].

### 7.2.2 Généralité

Pritunl est un serveur VPN open source et un panneau de gestion, en utilisant le protocole OpenVPN pour exécuter le serveur VPN. Il utilise le certificat « Let's Encrypt » pour sécuriser le serveur VPN et son interface utilisateur Web. Pritunl utilise MongoDB pour stocker sa base de données [16]. C'est une application très utile car elle utilise le protocole VPN open source le plus répandu, OpenVPN.

L'installation du serveur OpenVPN est très complexe et nécessite une expertise pour l'installation et la configuration. Pritunl automatise le processus d'installation et fournit également une interface utilisateur Web puissante pour gérer les serveurs, les organisations et les utilisateurs VPN.

Il utilise OpenVPN masqué, mais ajoute une interface Web simple (mais complète) pour l'administration et la gestion des serveurs / utilisateurs.

Il est également configuré pour fonctionner avec de nombreux services d'authentification et une API pour l'automatisation et une intégration plus poussée.

**OpenVPN + Interface + Intégrations = Pritunl**

### 7.2.3 Caractéristiques

Pritunl est une plate-forme open source capable de réaliser des réseaux VPN distribués. En exploitant le protocole OpenVPN, il est possible, selon le modèle de licence choisi, de configurer des architectures de réseau virtuel. En pratique, il permet de connecter facilement des périphériques à l'intérieur ou à l'extérieur des murs, y compris dans les entreprises à deux ou plusieurs succursales, créant ainsi un VPN géré avec des règles avancées et un système d'authentification centralisé.

Pritunl intègre plusieurs services de tiers tels que Amazon AWS VPC Cloud privé, il s'agit d'un espace réseau virtuel dans le Cloud disponible pour les utilisateurs de la suite AWS avec basculement automatique et authentification « Single Sign On » (SSO).

Si la licence Enterprise est choisie, ce qui permet l'installation sur un nombre illimité de serveurs Pritunl, il est possible d'exploiter la fonctionnalité de haute disponibilité avec basculement automatique, également en raison du fait qu'il n'existe pas de nœuds maîtres, mais que chaque nœud fonctionne de la même manière. Pritunl intègre également une fonctionnalité de réPLICATION de serveur, offrant ainsi un haut niveau d'évolutivité pour les clusters.

Dans le but de réaliser des installations réparties géographiquement, la plate-forme s'appuie sur la célèbre MongoDB, qui offre un haut niveau de fiabilité (avec notamment l'augmentation du nombre de nœuds et d'utilisateurs) associée aux chances de réPLICATION.

Lors de la réalisation d'une infrastructure étendue et complexe, il est essentiel de disposer des outils de surveillance et de contrôle appropriés. Pritunl prend en charge « Influx DB », une suite d'outils permettant le contrôle des hôtes et des clusters sur le réseau.

**Open source :** Tout le code source de Pritunl est disponible sur GitHub permettant une transparence complète et une personnalisation.

**Libre d'utilisation :** Alternative gratuite et open source. Aucune inscription ou carte de crédit nécessaire.

**Configuration facile :** Toute la configuration est effectuée à partir d'une interface Web permettant une gestion facile des grandes organisations et des configurations complexes.

**Sécurité :** Tout le trafic entre les clients et le serveur est crypté. L'authentification en deux étapes facultatives est disponible.

**OpenVPN et IPsec :** Pritunl est construit avec OpenVPN et tout client OpenVPN existant peut être utilisé. IPsec est utilisé pour les liens de site à site et l'appairage VPC.

**API REST :** Pour intégrer et configurer facilement Pritunl avec d'autres services à l'aide de l'API REST. La documentation est disponible dans la section des plateformes.

### **7.2.4 Modèle de prix**

Pritunl offre l'ensemble de ses logiciels gratuitement en téléchargement. Toutefois, pour pouvoir utiliser toutes les fonctionnalités du serveur VPN, la disposition d'un abonnement basé sur des paiements réguliers est nécessaire. Le fabricant a choisi un modèle à trois niveaux :

- Le programme est disponible gratuitement, mais il n'offre aucune nouvelle fonctionnalité intéressante. Les configurations multi-centres de données ne sont pas prises en charge, par exemple. De nombreuses fonctionnalités de l'interface Web Pritunl sont grises, mais au moins le nombre de connexions simultanées aux clients (utilisateurs et périphériques) n'est pas limité.
- La version Premium est à 10 \$ par mois. Cet abonnement contient les fonctionnalités de l'édition gratuite et prend en charge les liaisons de passerelle grâce auxquelles les serveurs VPN peuvent transférer le trafic du réseau local au client VPN. Cette version permet également de télécharger des profils VPN pour Chrome OS et permet au serveur d'envoyer par courrier électronique les détails de sa configuration aux utilisateurs configurés. Les thèmes supplémentaires pour l'interface Web sont juste une façade.
- La variante Enterprise est réellement intéressante : elle contient toutes les fonctionnalités offertes par les packages de niveau inférieur ainsi que des fonctionnalités réellement pratiques, telles que les VPN de site à site ou le mode pont VPN, dans lequel un client VPN devient une partie directe de la configuration. Réseau local. À 50 dollars par mois, les entreprises pourront probablement se le permettre, même si le prix demandé pourrait faire mal aux utilisateurs privés. Ce package inclut également la configuration automatique des noms DNS pour les clients VPN, ainsi qu'un module de connexion unique pour Google ou Duo Security [15].

### **7.2.5 Fonctionnements**

Pritunl offre les principaux fonctionnements suivants :

- Accéder à un réseau privé
- Serveurs multi-hôtes
- Serveurs répliqués
- Site à Site avec IPSec
- Pritunl Zéro
- Route AWS
- Oracle Route Advertisement
- Port Forwardind
- Client Chrome OS
- Ubiquiti EdgeRouter
- Liens réseau
- Certificats SSH

## Côté client :

Tout en utilisant le protocole OpenVPN, Pritunl offre des outils clients spéciaux pour les systèmes d'exploitation traditionnels, même s'ils sont superflus. Le serveur Pritunl peut générer l'intégralité des fichiers de configuration pour les utilisateurs de réseau privé virtuel sur simple pression d'un bouton. Avec l'utilisation d'un client Pritunl, lorsqu'un utilisateur reçoit par courrier électronique une configuration Pritunl pour un appareil mobile (par exemple, un Chromebook), le client peut l'ouvrir immédiatement et commencer à utiliser le VPN.

### 7.2.6 Sécurité

OpenVPN est l'un des protocoles VPN les plus sécurisés et comme Pritunl utilise le protocole OpenVPN, il est bien sécurisé, de même Pritunl est le serveur VPN le plus sécurisé disponible et le seul serveur VPN à offrir jusqu'à cinq couches d'authentification. Incluant un certificat d'utilisateur, une NIP d'utilisateur à six chiffres, un authentificateur à deux facteurs, une authentification unique et une authentification push mobile [3].

#### ❖ Audit utilisateur

Il faut contrôler les événements des utilisateurs et des administrateurs pour faciliter la détection des intrusions, améliorer la sécurité et répondre aux exigences réglementaires.

#### ❖ Blocage des accès public à la console Web

La console Web ne doit pas être accessible à Internet. Si une connexion unique ou des liens de clé sont utilisés, l'accès à la console Web doit être limité aux environnements sécurisés, par exemple en obligeant les utilisateurs à télécharger leurs clés au bureau, sur le réseau local. Si le serveur Pritunl se trouve sur un hôte distant, utilisez des règles de pare-feu pour autoriser l'accès uniquement à partir des adresses IP publiques de votre organisation (bureau, etc.). Si un accès à distance est nécessaire, envisagez de mettre en liste blanche l'adresse IP des utilisateurs sur le pare-feu ou d'ouvrir temporairement le pare-feu pour permettre aux utilisateurs de télécharger leurs clés.

#### ❖ Utilisation d'un pare-feu externe

Évitez d'utiliser des pares-feux logiciels pouvant exister sur le serveur Pritunl lui-même, tels que « **iptables** ». Utilisez plutôt un pare-feu externe au serveur, tel qu'un pare-feu matériel ou des groupes de sécurité. Seuls les ports VPN doivent être ouverts à l'internet public.

#### ❖ Utilisation d'authentification unique

L'authentification unique est le moyen le plus simple et le plus simple d'authentifier les utilisateurs en leur demandant d'autoriser les téléchargements de clés et les connexions VPN.

Prévenez les attaques de « **phishing** », ajoutez des couches de sécurité supplémentaires et appliquez les stratégies de sécurité des utilisateurs avec l'authentification unique. Pritunl prend totalement en charge plusieurs fournisseurs de connexion unique sans configuration compliquée.

#### ❖ Open source

Tout le code source de Pritunl est ouvert et peut être audité par toute organisation afin de s'assurer qu'il n'y a aucun problème de sécurité. Cela permet également un processus de développement transparent et un produit flexible pouvant être modifié pour répondre aux besoins des organisations.

#### ❖ SELinux

Pritunl prend totalement en charge SELinux avec des stratégies incluses pour limiter chaque composant afin d'améliorer la sécurité.

#### ❖ Utilisation d'un cryptage sécurisé

Utilisation toujours du chiffrement AES 256 bits avec une taille de paramètre DH « **Diffie-Hellman** » d'au moins 2048 bits. Un paramètre DH de 4096 bits offre la meilleure sécurité, mais sa création peut prendre plusieurs heures. Ce processus ne doit être effectué qu'une seule fois pour chaque serveur VPN.

#### ❖ Blocage de tous les accès publics au réseau interne

Tous les ports pour SSH, les outils internes et tous les autres services internes du réseau doivent être bloqués au niveau du pare-feu. Ces services seront accessibles via la connexion VPN.

# PARTIE IV : MISE EN OEUVRE ET VALIDATION

# Chapitre 8 : Réalisation

Dans cette partie, nous verrons les installations et les configurations requises pour la mise en place de notre projet. Ce chapitre se divise en deux grandes parties :

- La solution de la sauvegarde réseau avec Bacula
- Le serveur VPN avec Pritunl

## 8.1 Mise en place BACULA

### 8.1.1 Conditions préalables

Avoir un accès super-utilisateur (sudo) sur le serveur. En outre, le serveur exigera un espace disque suffisant pour toutes les sauvegardes qu'on prévoit de conserver à un moment donné. Une connexion internet et un serveur de base de données.

Ce qui se peut se résumer ainsi :

- Disposer des droits d'administration.
- Disposer d'une connexion à Internet configurée et activée
- Un serveur SQL
- Disque de stockage suffisant

La dernière hypothèse est que SELinux est désactivé

### 8.1.2 Installation de Bacula

Bacula utilise une base de données SQL, telle que MySQL ou PostgreSQL, pour gérer son catalogue de sauvegardes. Nous avons choisi MariaDB, un remplaçant instantané de MySQL pour notre projet.

Dans la suite nous aurons :

- Un server Bacula sur un système GNU/UNIX, plus précisément sur Redhat Enterprise Linux 7.3 où l'on installera le Director, le Catalogue, le Storage et la Console ainsi que le serveur MariaDB.
- Un Client Bacula sur un système Windows, GNU/UNIX où nous installerons le File Daemon.

#### 8.1.2.1 Installer le package MariaDB Server

**Etape 1 :** Ajouter le référentiel MariaDB yum

Commencer par ajouter le fichier de référentiel MariaDB YUM « MariaDB.repo » dans le répertoire « /etc/yum.repos.d/ » pour les systèmes RHEL.

Création du fichier en ligne par la commande suivante :

```
#nano /etc/yum.repos.d/MariaDB.repo
```

Les lignes suivantes seront ajoutées dans le fichier « MariaDb.repo » :

```
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.1/rhel7-amd64
gpgkey = https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck = 1
```

La figure 15 présente le contenu du fichier :

```
[root@APP035AIT ~]# cat /etc/yum.repos.d/MariaDB.repo
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.1/rhel7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
[root@APP035AIT ~]#
```

Figure 15 : Contenu du fichier MariaDB.repo

## Etape 2 : Installer MariaDB dans le serveur

La commande suivante est pour l'installation du package :

```
#yum install mariadb-server
```

Dès que l'installation des packages MariaDB est terminée, démarrer le démon du serveur de base de données pour le moment et l'activer également pour qu'il se lance automatiquement au prochain démarrage de la manière suivante :

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

Commande pour vérification du serveur s'il a été bien démarré.

```
#systemctl status mariadb
```

La figure 16 affiche le statut du serveur MariaDB :

```
[root@APP035AIT ~]# systemctl status mariadb
● mariadb.service - MariaDB 10.1.35 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Drop-In: /etc/systemd/system/mariadb.service.d
             └─migrated-from-my.cnf-settings.conf
     Active: active (running) since jeu. 2018-11-29 15:12:55 EAT; 2 weeks 4 days ago
       Docs: man:mysqld(8)
              https://mariadb.com/kb/en/library/systemd/
    Process: 2356 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=0, status=0/SUCCESS)
   Process: 1087 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR='galera_recovery'; [ $? -eq 0 ] && systemctl set-environment _WSREP_START_POSITION=$VAR || exit 0 (code=0, status=0/SUCCESS)
```

Figure 16 : Statut MariaDB serveur

### Etape 3 : Sécurisation de MariaDB

Sécuriser MariaDB, on définit un mot de passe root, en désactivant la connexion root à distance, en supprimant la base de données de test ainsi que les utilisateurs anonymes, et en rechargeant les priviléges, comme indiqué dans la figure 17 :

Ci-dessous, la commande pour la sécurisation :

```
# mysql_secure_installation
```

```
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Figure 17 : Sécurisation de MariaDB

#### **Etape 4 : Vérification**

Vérification de certaines fonctionnalités de MariaDB, telles que : la version installée, la liste d'arguments du programme par défaut, ainsi que la connexion au shell de commande MariaDB, on procède comme suit :

```
# mysql -V  
# mysql -u root -p
```

La figure 18 montre cette vérification :

```
[root@APP035AIT ~]# mysql -V  
mysql Ver 15.1 Distrib 10.1.35-MariaDB, for Linux (x86_64) using readline 5.1  
[root@APP035AIT ~]# mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 441  
Server version: 10.1.35-MariaDB MariaDB Server  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MariaDB [(none)]> █
```

Figure 18 : Vérification connexion MariaDB

#### **8.1.2.2 Installer les packages Postfix**

Pour la notification par mail des fonctionnements et du suivi du serveur Bacula :

- Rapports des sauvegardes effectuées ;
- Rapports des restaurations effectuées.

```
#yum install -y postfix
```

#### **8.1.2.3 Installer les packages Webmin**

Webmin est un panneau de configuration Web moderne pour toute machine Linux. Il permet d'administrer le serveur via une interface simple, et est prévu pour modifier les paramètres des packages courants à la volée comme le serveur Bacula.

Tout d'abord, nous devons ajouter le référentiel Webmin afin de pouvoir facilement installer et mettre à jour Webmin à l'aide de notre gestionnaire de paquets. Pour ce faire, nous ajoutons un nouveau fichier appelé « /etc/yum.repos.d/webmin.repo » contenant des informations sur le nouveau référentiel.

Pour créer ce nouveau fichier, on utilise la commande suivante :

```
#nano /etc/yum.repos.d/webmin.repo
```

Les lignes suivantes seront ajoutées dans le fichier « webmin.repo » :

```
[Webmin]
name=Webmin Distribution Neutral
#baseurl=http://download.webmin.com/download/yum
mirrorlist=http://download.webmin.com/download/yum/mirrorlist
enabled=1
```

La figure 19 montre le contenu du fichier dans le serveur :



```
GNU nano 2.3.1          Fichier : /etc/yum.repos.d/webmin.repo

[Webmin]
name=Webmin Distribution Neutral
#baseurl=http://download.webmin.com/download/yum
mirrorlist=http://download.webmin.com/download/yum/mirrorlist
enabled=1
```

Figure 19 : Contenu du fichier webmin.repo

Ensuite, ajouter la clé PGP de l'auteur Webmin pour que le système fasse confiance au nouveau référentiel :

```
#wget http://www.webmin.com/jcameron-key.asc
#rpm --import jcameron-key.asc
```

Installer webmin:

```
#yum install webmin
```

Une fois l'installation terminée, le message dans la figure 20 sera affiché dans la sortie :

```
Output
Webmin install complete. You can now login to https://172.20.32.29:10000/ as
root with your root password.
```

Figure 20 : Message de sortie d'installation Webmin

Puis, lancer Webmin et l'activer au démarrage du système.

Pour démarrer Webmin, on utilise la commande suivante :

```
# systemctl start webmin
```

Pour activer Webmin au démarrage du système, on utilise la commande suivante :

```
# systemctl enable webmin
```

Pour le pare-feu :

```
#firewall-cmd --permanent --zone=public --add-port=10000/tcp
```

#### 8.1.2.4 Installer les packages Bacula-Web

Bacula-Web utilise Apache pour servir les pages. Installer Apache et le faire fonctionner à l'aide des éléments suivants :

```
#yum -y install httpd  
#chkconfig httpd on  
#service httpd start
```

Configurer Apache pour qu'il démarre au démarrage :

```
#systemctl start httpd  
#systemctl enable httpd
```

Ensuite, on ajoute le support MySQL à Apache en entrant les éléments suivants :

```
#yum -y install php php-gd php-gettext php-mysql php-pdo
```

Pour qu'Apache puisse franchir le pare-feu, on ouvre les ports à l'aide des éléments suivants :

```
#firewall-cmd --permanent --zone=public --add-service=http  
#firewall-cmd --permanent --zone=public --add-service=https  
#firewall-cmd --reload
```

Ensuite, dans le site Web Bacula-Web, on télécharge la dernière version.

<http://www.bacula-web.org/download.html>

Décompresser l'archive et la placer dans le répertoire « /var/www/html ».

La figure 21 donne l'emplacement du fichier.

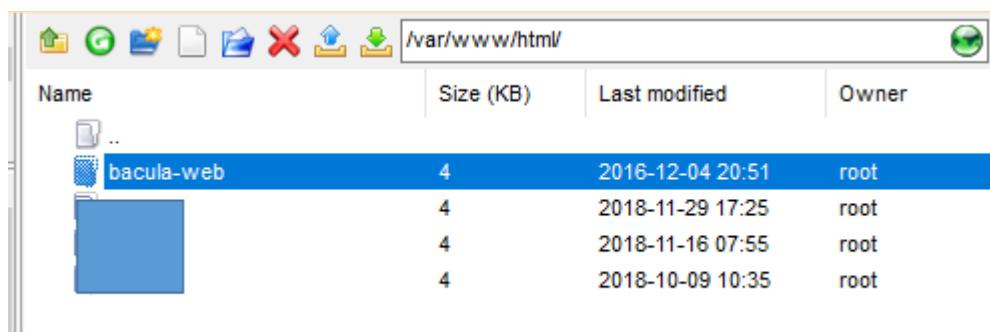


Figure 21 : Bacula-Web dans le serveur

### 8.1.2.5 Installer les packages Bacula

#### Etape 1 : Ajout du référentiel Bacula yum

Par l'ajout du fichier de référentiel BACULA YUM « bacula.repo » dans le répertoire /etc/yum.repos.d/ » pour les systèmes RHEL.

Pour la création du fichier en ligne, on applique la commande suivante :

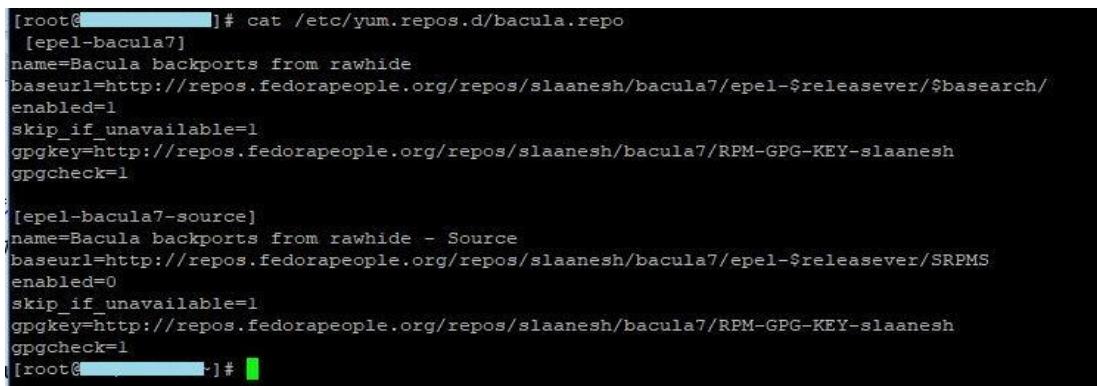
```
#nano /etc/yum.repos.d/bacula.repo
```

On saisit les lignes suivantes dans le fichier « bacula.repo » :

```
[epel-bacula7]
name=Bacula backports from rawhide
baseurl=http://repos.fedorapeople.org/repos/slaanesh/bacula7/epel-
$releasever/$basearch/
enabled=1
skip_if_unavailable=1
gpgkey=http://repos.fedorapeople.org/repos/slaanesh/bacula7/RPM-GPG-KEY-
slaanesh
gpgcheck=1

[epel-bacula7-source]
name=Bacula backports from rawhide - Source
baseurl=http://repos.fedorapeople.org/repos/slaanesh/bacula7/epel-
$releasever/SRPMS
enabled=0
skip_if_unavailable=1
gpgkey=http://repos.fedorapeople.org/repos/slaanesh/bacula7/RPM-GPG-KEY-
slaanesh
gpgcheck=1
```

La figure 22 indique le contenu du fichier :



```
[root@... ]# cat /etc/yum.repos.d/bacula.repo
[epel-bacula7]
name=Bacula backports from rawhide
baseurl=http://repos.fedorapeople.org/repos/slaanesh/bacula7/epel-$releasever/$basearch/
enabled=1
skip_if_unavailable=1
gpgkey=http://repos.fedorapeople.org/repos/slaanesh/bacula7/RPM-GPG-KEY-slaanesh
gpgcheck=1

[epel-bacula7-source]
name=Bacula backports from rawhide - Source
baseurl=http://repos.fedorapeople.org/repos/slaanesh/bacula7/epel-$releasever/SRPMS
enabled=0
skip_if_unavailable=1
gpgkey=http://repos.fedorapeople.org/repos/slaanesh/bacula7/RPM-GPG-KEY-slaanesh
gpgcheck=1
[root@... ]#
```

Figure 22 : Affichage de bacula.repo

#### Etape 2 : Installer Bacula

On applique la commande suivante pour l'installation du package :

```
#yum install -y bacula-director bacula-storage bacula-console bacula-
client
```

Passons maintenant aux différentes configurations nécessaires du projet Bacula.

## 8.1.3 Configuration

### 8.1.3.1 Configuration de la base de données MariaDB

**Etape 1 :** Tout d'abord définir le MySQL Lib pour utiliser Bacula.

Par la commande suivante :

```
#alternatives -config libbaccats.so
```

Il y a 3 programmes qui fournissent le fichier « libbaccats.so » :

1. /usr/lib64/libbaccats-mysql.so
2. /usr/lib64/libbaccats-sqlite3.so
3. /usr/lib64/libbaccats-postgresql.so

Nous utilisons 1 pour sélectionner MySQL.

**Etape 2 :** Création de la base de données, des tables et des privilèges par des scripts déjà créés.

- **Créer une base de données Bacula**

```
#/usr/libexec/bacula/create_mysql_database -u root -p
```

- **Créer des tableaux**

```
#/usr/libexec/bacula/make_mysql_tables -u root -p
```

- **Accorder des privilèges :**

Cette commande crée un utilisateur MySQL “bacula” avec “No Password”.

```
#/usr/libexec/bacula/grant_bacula_privileges -u root -p
```

La figure 23 montre ce déroulement :

```
[root@XXXXXX ~]# alternatives --config libbaccats.so
There are 3 programs which provide 'libbaccats.so'.
Selection  Command
-----
1      /usr/lib64/libbaccats-mysql.so
2      /usr/lib64/libbaccats-sqlite3.so
*+ 3    /usr/lib64/libbaccats-postgresql.so

Enter to keep the current selection[+], or type selection number: 1

[root@XXXXXX ~]# /usr/libexec/bacula/create_mysql_database -u root -p
Enter password: #
Creation of bacula database succeeded.

[root@XXXXXX ~]# /usr/libexec/bacula/make_mysql_tables -u -root -p
Enter password: #
Creation of Bacula MySQL tables succeeded.

[root@XXXXXX ~]# /usr/libexec/bacula/grant_mysql_privileges -u root -p
Enter password: #
Privileges for user bacula granted on database bacula.

[root@XXXXXX ~]# mysql -u root -p
Enter password: #

Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 13

Server version: 5.5.41-MariaDB MariaDB Server

Copyright (c) 2000, 2014, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> set password for bacula@'%'=password('Aits@Bacula++');

Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> set password for bacula@'localhost'=password('password');

Query OK, 0 rows affected (0.00 sec)
```

Figure 23 : Etape de configuration de base de données

### 8.1.3.2 Configuration de sauvegarde Bacula avec Webmin

Pour accéder, ouvrir un navigateur et saisir l'adresse IP du serveur et le port pour Webmin :

**Https:// Adresse-IP serveur : 10000/**

Authentification par l'utilisateur « root » ou un utilisateur ayant un accès administrateur au serveur avec le mot de passe approprié: elle est montrée dans la figure 24 :

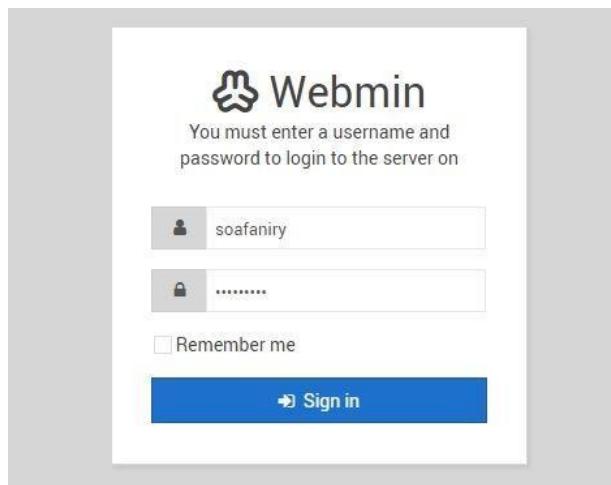


Figure 24 : Page d'authentification Webmin

**Redirection vers la page d'accueil de Webmin :**

La figure 25 présente le tableau de bord de Webmin :

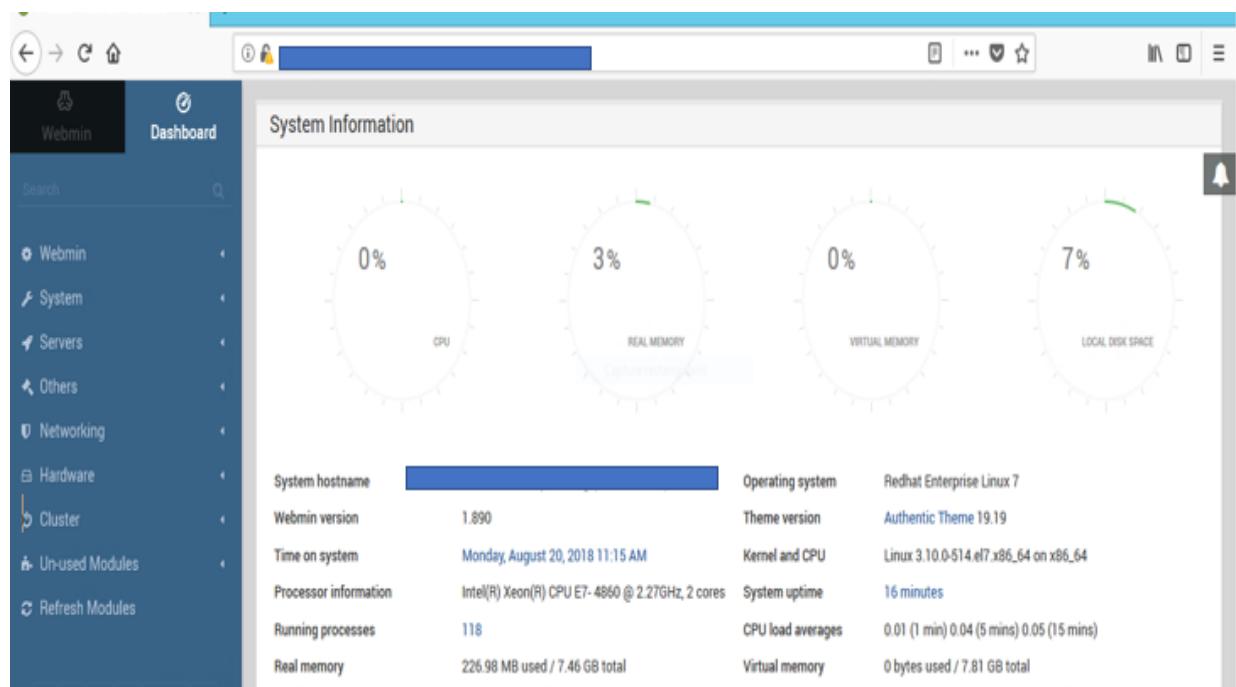


Figure 25 : Tableau de bord Webmin

## ❖ Bacula Backup System

Navigation dans **System** ==> **Bacula Backup System**

Le choix d'utilisation du serveur de sauvegarde est montré dans la figure 26 :

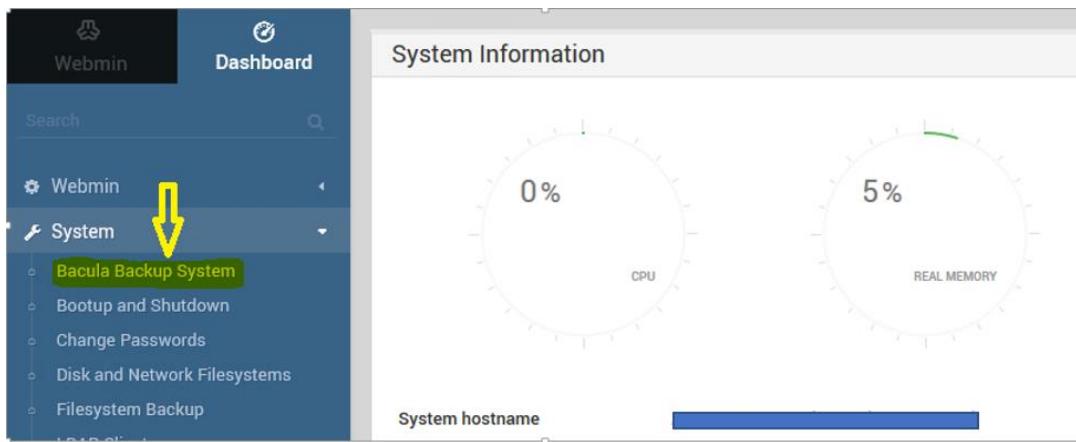


Figure 26 : Choix du Bacula Backup System

Toutes les tâches de sauvegardes et de restaurations sont effectuées dans cette interface.

La figure 27 illustre la page de navigation du « Bacula backup System »

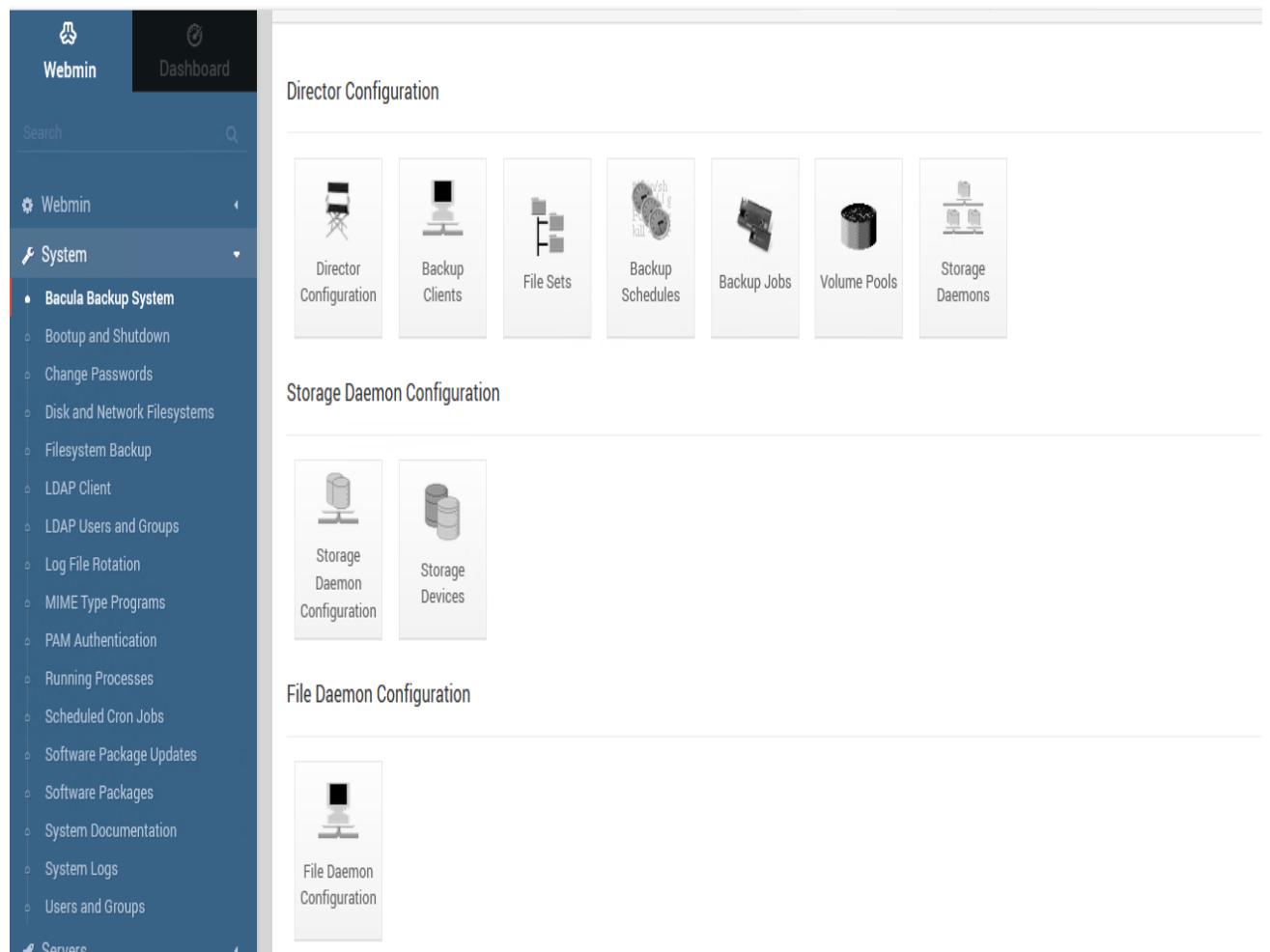


Figure 27 : Page de navigation du « Bacula backup System »

Et maintenant les étapes pour faire une sauvegarde et une restauration.

## ❖ Configuration de la sauvegarde

### 1° Configuration du Storage Device

Le « Storage Device » est destination physique de la sauvegarde, c'est-à-dire le chemin du dossier où les données vont être sauvegardées. La figure 28 montre le choix du « Storage Device » :

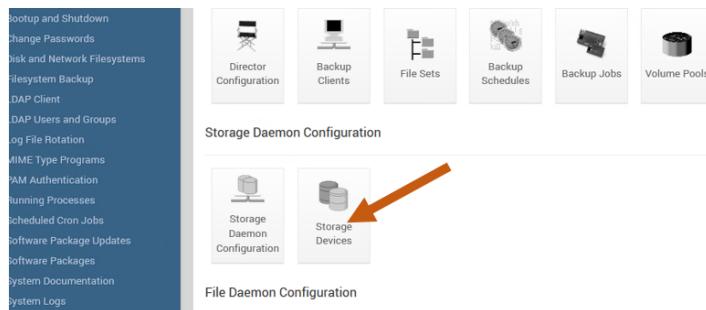


Figure 28 : Storage Device

- Ajout d'un nouveau « storage device » (voir figure 29 ci-dessous) :

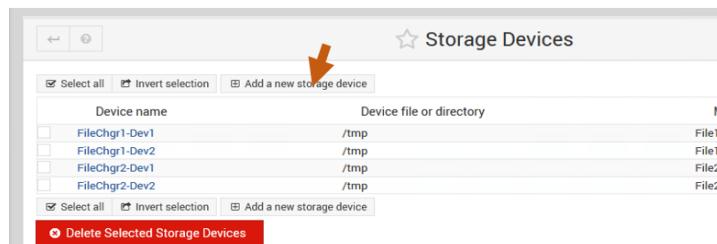


Figure 29 : Ajout d'un nouveau « Storage Device »

Pour notre validation, nous avons créé un dossier pour le chemin de stockage de la sauvegarde dans le serveur avec la commande suivante :

```
#mkdir /data/Backup
```

Les figures 30 et 31 montrent comment créer ce stockage

A screenshot of a software interface titled 'Details of file storage device'. It shows a form for creating a new storage device. The 'Storage device name' field contains 'StoreDev1'. The 'Archive device or directory' field contains '/data/Backup'. A blue oval highlights the 'Nom du Storage' label above the 'Storage device name' field, and an orange arrow points to it. Another blue oval highlights the 'Chemin de stockage' label above the 'Archive device or directory' field, and an orange arrow points to it. Other fields include 'Media type name' (set to 'File'), 'Random access medium?' (radio button 'Yes' selected), 'Removable media?' (radio button 'No' selected), 'Automatically label media?' (radio button 'Yes' selected), 'Mount automatically?' (radio button 'Always keep open?' selected), and a 'Create' button at the bottom left.

Figure 30 : Champ à remplir du « Storage Device »

Device name	Device file or directory	Media type
FileChgr1-Dev1	/tmp	File1
FileChgr1-Dev2	/tmp	File1
FileChgr2-Dev1	/tmp	File2
FileChgr2-Dev2	/tmp	File2
StoreDev1	/data/Backup	File

Select all    Invert selection    Add a new storage device

Delete Selected Storage Devices

Figure 31 : Stockage « Storage Device » créée

## 2° Configuration du Storage Daemon

Le « Storage Daemon » gère les médias où seront écrites les données.

- Ajout d'un nouveau « storage deamon » : voir ci-dessous figure 32 :

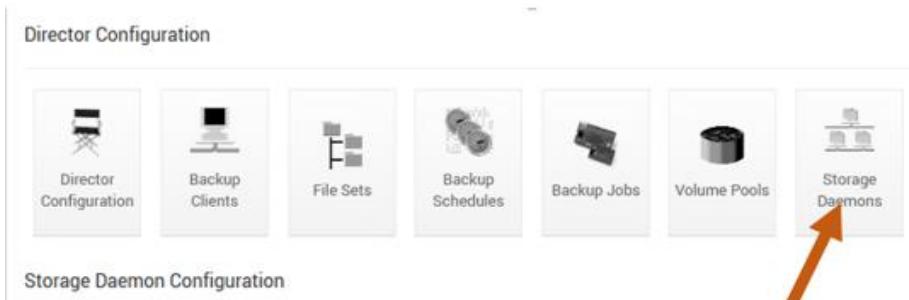


Figure 32 : Storage Daemons

Les figures 33 et 34 montrent comment créer ce daemon :

Details of remote storage daemon	
Storage daemon name	Store_Deamon_1
Bacula SD password	bacula@DIR
Hostname or IP address	APP035AIT.corp.ait.org
Storage device name	StoreDev1
Maximum concurrent jobs	20
Bacula SD port	9103
Media type name	File

Figure 33 : Champ à remplir du « Storage Daemon »

Storage name	Hostname or address	Storage device	Media typ
Stor05		Stor5	File
Store_Deamon_1		StoreDev1	File
StoreD-Gran		StoreGran	File

Select all    Invert selection    Add a new storage daemon

Figure 34 : Stockage « Storage daemon » créée

### 3° Configuration du Volume Pools

Le « Volume Pools » sert à spécifier et à définir le volume de sauvegarde. La figure 35 montre le choix du « Volume Pools » dans la navigation :

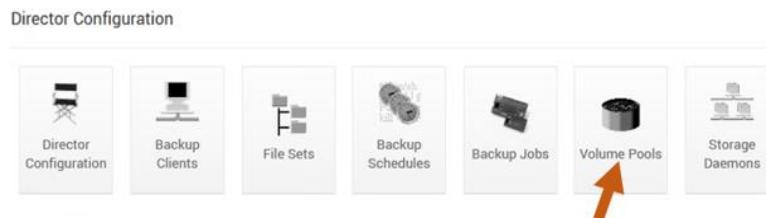


Figure 35 : Volume Pools

- Ajout d'un nouveau « volume pool »

Les figures 36 et 37 illustrent la création du « Volume Pool » :

The screenshot shows the 'Details of backup volume pool' configuration window. It includes the following fields:

- Nom du volume**: Volume pool name (Volum\_Pool\_1)
- Spécifié le type du volume**: Volume pool type (Backup)
- Préfix du volume**: Volume prefix (VolPool1)
- La taille maximale du donné à sauvegarder**: Maximum volume size (100G)
- Maximum jobs per volume**: 365 days
- Automatically recycle volumes?**: Yes
- Create**: A green button at the bottom left.

Figure 36 : Champ à remplir du « Volume Pool »

	Vols	Backup	365 days
	Volum_Pool_1	Backup	365 days
<input checked="" type="checkbox"/>	<input type="checkbox"/> Vol5	Backup	365 days
<input checked="" type="checkbox"/>	<input type="checkbox"/> Volum_Pool_1	Backup	365 days
	<input checked="" type="checkbox"/> Select all <input type="checkbox"/> Invert selection <input type="checkbox"/> Create a new volume pool	Crée	
	<input type="checkbox"/> Delete Selected Volume Pools		

Figure 37 : Volume « Volume Pool » créé

### 4° Configuration du Backup Schedules

Le « Backup Schedules » sert à définir le moment où l'on veut exécuter la sauvegarde. La figure 38 illustre le choix du « Backup Schedules »

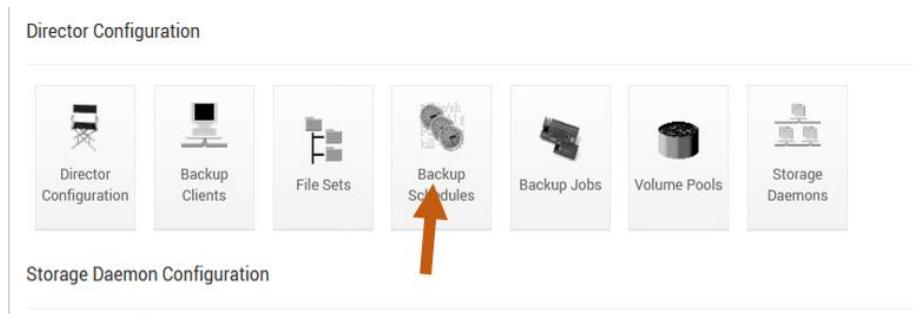


Figure 38 : Backup Schedules

- Ajout d'un nouveau « backup schedule »

Les figures 39 et 40 illustrent la création du « Backup Schedules » :

Figure 39 : Champ à remplir du « Backup Schedule »

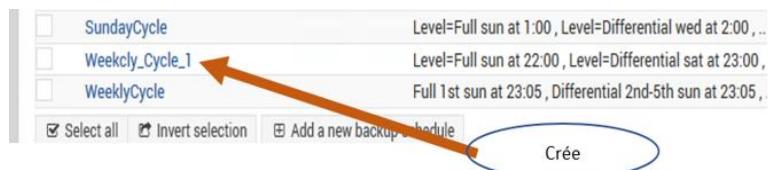


Figure 40 : Schedule « Backup Schedule » crée

## 5° Configuration du « FileSets »

Le « FileSets » est utilisé pour définir les fichiers à sauvegarder. La figure 41 montre le choix du « FileSets » :

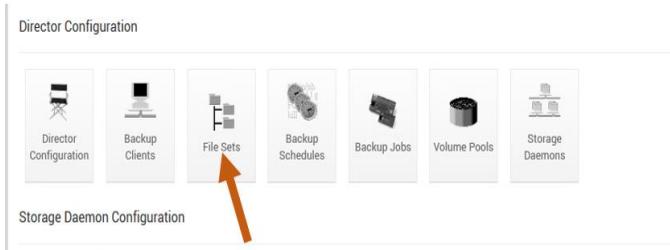


Figure 41 : FileSets

- Ajout d'un nouveau « Fileset »

Les figures 42 et 43 montrent la création du « FileSet » :

Figure 42 : Champ à remplir du « FileSet »

File set name	Included files
Catalog	/var/spool/bacula/bacula.sql
File5	/ , /boot , /home , /usr , ...
File_Set_01	/data/TestBackup/
FileS-Gran	* , / , /* , /root , ...
FileS1	/ , /boot , /home , /usr , ...
FileS2	... , /etc , /var , /tmp , /root , ...

Crée

Figure 43 : FileSet créé

## 6° Configuration du « Backup Client »

Le client ici est la machine client où se trouvent les données à sauvegarder. La figure 44 indique le choix du « Backup Clients »

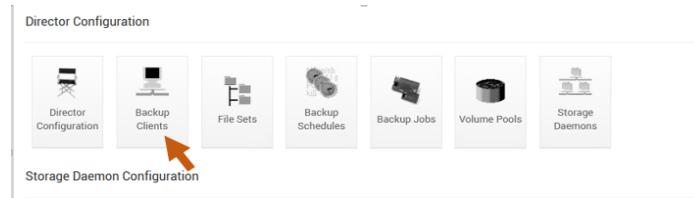


Figure 44 : Backup Clients

- Ajout d'un nouveau client :

Les figures 45 et 46 décrivent la création du « Backup Client » :

Details of client to be backed up

Nom du Client	APP037AIT	Mot de passe correspondant dans la config du bacula-dir.conf sur le serveur
Client FD name	APP037AIT	Bacula FD port
Bacula FD password	[REDACTED]	Prune expired jobs and files?
Hostname or IP address	[REDACTED]	Keep backup jobs for
Catalog to use	MyCatalog	Keep backup files for
Keep backup files for	30 years	
Adresse IP du client		

Figure 45 : Champ à remplir du « Backup Client »

Client crée

<input checked="" type="checkbox"/> Select all	<input type="checkbox"/> Invert selection	<input type="checkbox"/> Add a new backup client
Client name	Hostname or address	
APP037AIT	[REDACTED]	
Server-fd	[REDACTED]	

Figure 46 : Client « Backup Client » créé

## 7° Configuration du Backup Job

Le « **Backup Job** » sert à définir la tâche à effectuer : un **Job** est une ressource de configuration qui définit le travail que Bacula doit effectuer pour sauvegarder ou restaurer un client.

Il consiste en l'association d'un type d'opération à effectuer (**Type** : backup, restore, etc.), temps d'exécution, de la définition d'un ensemble de fichiers et répertoires à sauvegarder (**FileSet**), et d'un lieu de stockage où écrire les fichiers (**Storage, Pool**).

- Ajout d'un nouveau « backup Job » : Ici, sélection de tous les objets créés précédemment.

Cette opération est illustrée par les figures 47 et 48.

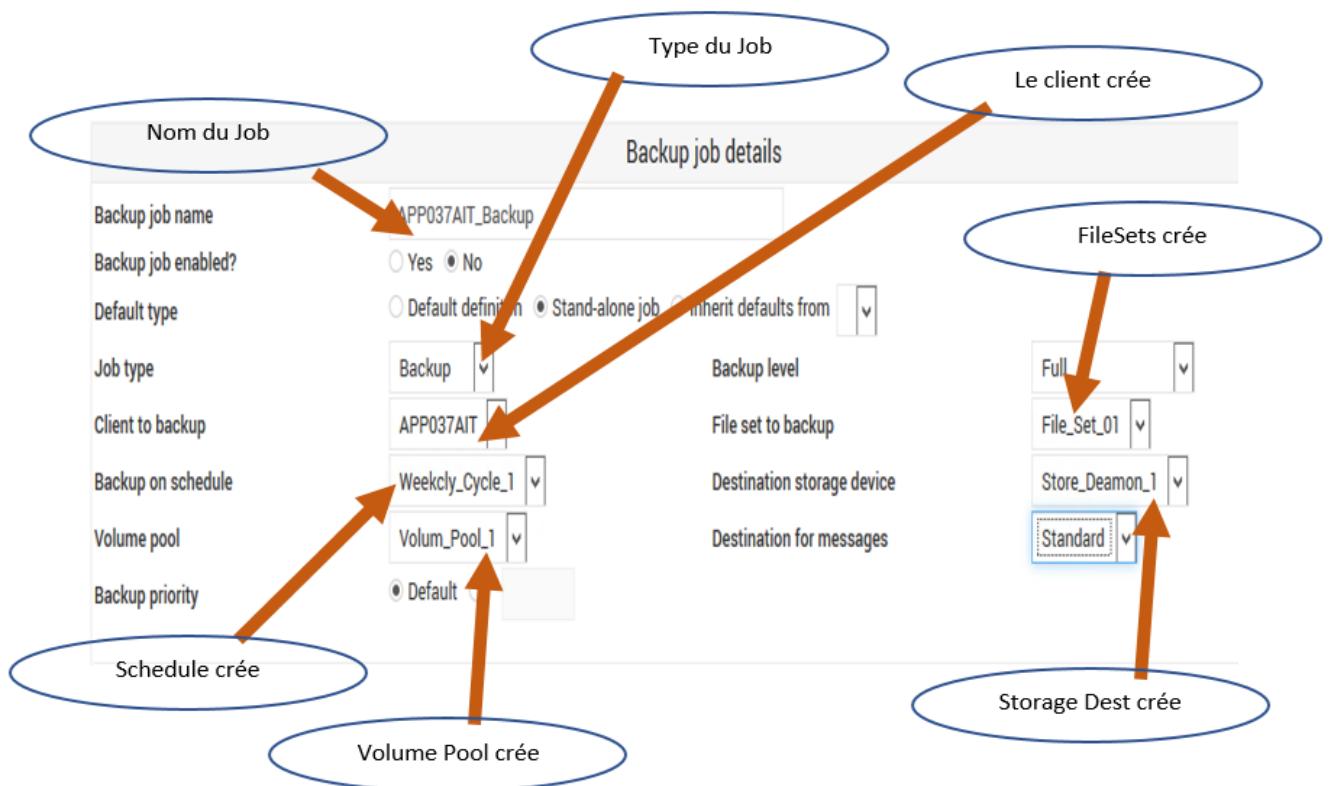


Figure 47 : Backup Job

The screenshot shows a list of backup jobs in a table format. The columns are:

Job name	Defaults?	Job type	Client to backup	File set to backup	Backup schedule
APP037AIT_Backup	No	Backup	APP037AIT	File_Set_01	Weekly_Cycle_1
Job-Gran	No	Backup	APP001AIT	Catalog	SundayCycle

A red arrow points from the "Job crée" oval to the "APP037AIT\_Backup" row in the table.

Figure 48 : Backup Job créé

### 8.1.3.3 Configuration de Bacula-Web

Dans le répertoire Application / Config et renommage du « config.php.sample » en « config.php », puis faire des modifications.

Dans la zone MySQL on modifie comme suit des paramètres pour qu'ils correspondent au serveur :

```
#cd /var/www/html/bacula-web/  
#cd application/config/  
#mv config.php.sample config.php  
#nano config.php
```

On a juste besoin de modifier le mot de passe à ce stade :

```
// MySQL bacula catalog  
$config[0]['label'] = 'Backup Server';  
$config[0]['host'] = 'localhost';  
$config[0]['login'] = 'bacula';  
$config[0]['password'] = 'Mot de passe Mysql Server';  
$config[0]['db_name'] = 'bacula';  
$config[0]['db_type'] = 'mysql';  
$config[0]['db_port'] = '3306';
```

Puis édition du fichier php.ini pour qu'il ait le fuseau horaire correct pour le système :

```
#nano /etc/php.ini
```

La figure 49 présente cette modification.

```
[Date]  
; Defines the default timezone used by the date functions  
; http://php.net/date.timezone  
;date.timezone = America/Chicago  
date.timezone = EAT/Madagascar
```

Figure 49 : Modification fuseau horaire

### 8.1.3.4 Configuration de pare-feu et ports

Pour permettre à Bacula de se connecter au service client ou au service de stockage, des ports spécifiques devront être ouverts comme suit :

```
#firewall-cmd --permanent --zone=public --add-port=9101/tcp  
#firewall-cmd --permanent --zone=public --add-port=9102/tcp  
#firewall-cmd --permanent --zone=public --add-port=9103/tcp  
#firewall-cmd --reload
```

## 8.1.4 Installation et Configuration Client

### 8.1.4.1 Client Linux

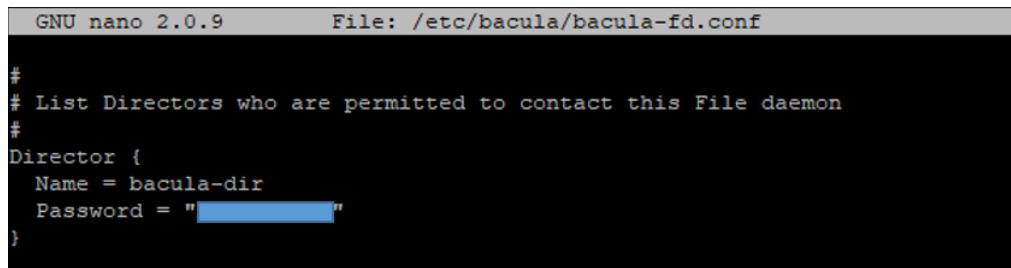
Installation du paquet Bacula Client « bacula-fd ». Avec la commande suivante :

```
#yum install bacula-fd
```

Une fois le paquet installé, on ouvre le fichier de configuration :

```
#nano /etc/bacula/bacula-fd.conf
```

Dans la balise « Director », dans « Name » on saisit le nom de serveur Bacula (director), et le mot de passe correspondant au mot de passe du serveur Bacula (director), comme suit dans la figure 50 :



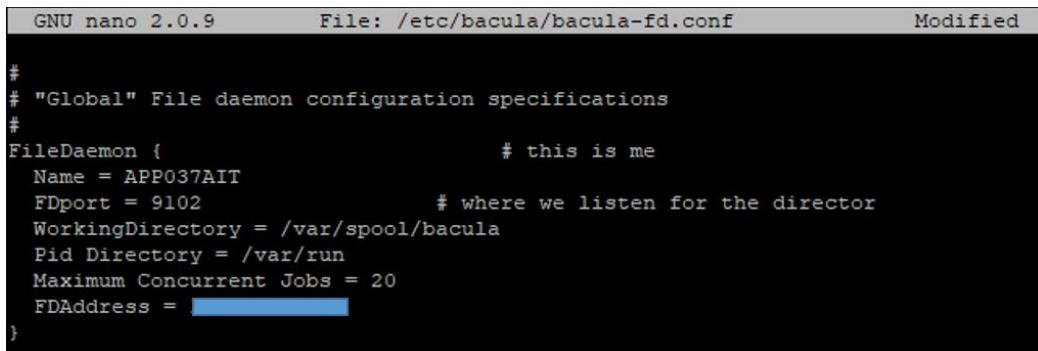
```
GNU nano 2.0.9          File: /etc/bacula/bacula-fd.conf

#
# List Directors who are permitted to contact this File daemon
#
Director {
    Name = bacula-dir
    Password = "████████"
}
```

Figure 50 : Configuration « bacula-fd » Director.

Et dans la balise « FileDaemon », dans « Name » édition du nom de client et dans « FDAddress » saisie de l'adresse IP du client Linux.

La figure 51 affiche cette modification :



```
GNU nano 2.0.9          File: /etc/bacula/bacula-fd.conf          Modified

#
# "Global" File daemon configuration specifications
#
FileDaemon {                                # this is me
    Name = APP037AIT
    FDport = 9102                         # where we listen for the director
    WorkingDirectory = /var/spool/bacula
    Pid Directory = /var/run
    Maximum Concurrent Jobs = 20
    FDAddress = ██████████
}
```

Figure 51 : Configuration « bacula-fd » FileDaemon.

Redémarrage du service « bacula-fd » avant d'activer le service au démarrage du système.

```
#systemctl start bacula-fd
#systemctl enable bacula-fd
```

Ouverture de port de communication avec le serveur :

```
#firewall-cmd --permanent --zone=public --add-port=9102/tcp
```

### 8.1.4.2 Client Windows

Pour le client Windows, il faut :

- Télécharger l'outil pour Windows à partir du site ci-dessous :  
<http://www.bacula.org/fr/?page=downloads>
- Procéder à l'installation en indiquant les informations sur le « director »

La figure 52 montre l'installation du bacula client sous Windows.

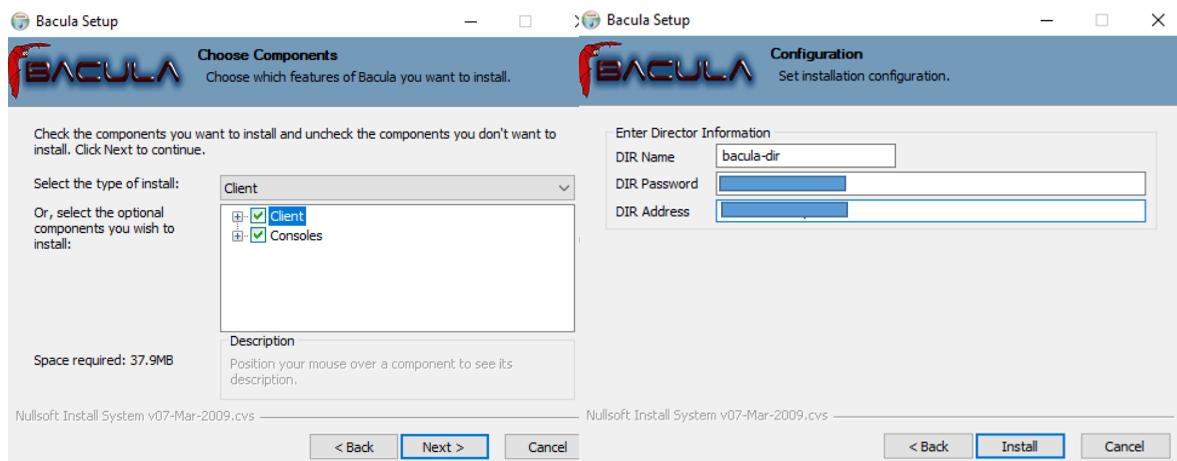


Figure 52 : Installation Bacula Client

Après l'installation, ouvrir le fichier de configuration et l'éditer comme suit dans la figure 53 :

```
8 #
9
10 #
11 # "Global" File daemon configuration specifications
12 #
13 FileDaemon {
14     Name = CClient-Win
15     FDport = 9102
16     WorkingDirectory = "C:\\\\Program Files\\\\Bacula\\\\working"
17     Pid Directory = "C:\\\\Program Files\\\\Bacula\\\\working"
18     # Plugin Directory = "C:\\\\Program Files\\\\Bacula\\\\plugins"
19     Maximum Concurrent Jobs = 10
20     FDAddress =
21 }
22 #
23 #
24 # List Directors who are permitted to contact this File daemon
25 #
26 Director {
27     Name = bacula-dir
28     Password =
29 }
```

Figure 53 : Configuration fichier Bacula client

Redémarrage du service de fichiers pour activer les nouveaux paramètres. Et aussi, autoriser le port 9102 sur le pare-feu Windows : voir ci-dessous (figure 54) :

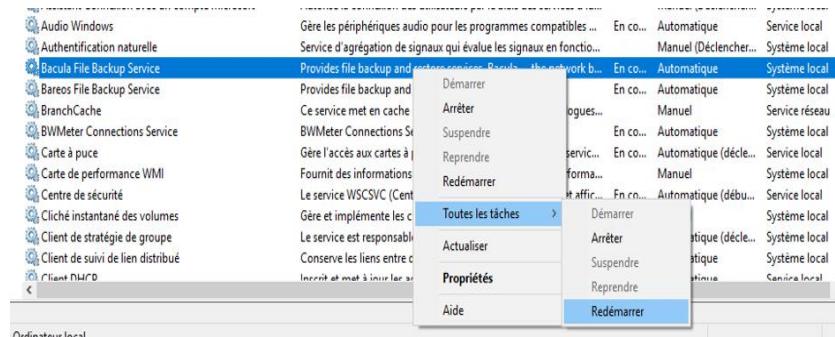


Figure 54 : Redémarrage du service fichier bacula client

Autorisation du port 9102 sur le pare-feu sous Windows :

Dans Panneau de configuration Windows, ouvrir le Pare-feu Windows et ajouter une nouvelle règle ; voir les figures 55 et 56 ci-dessous :

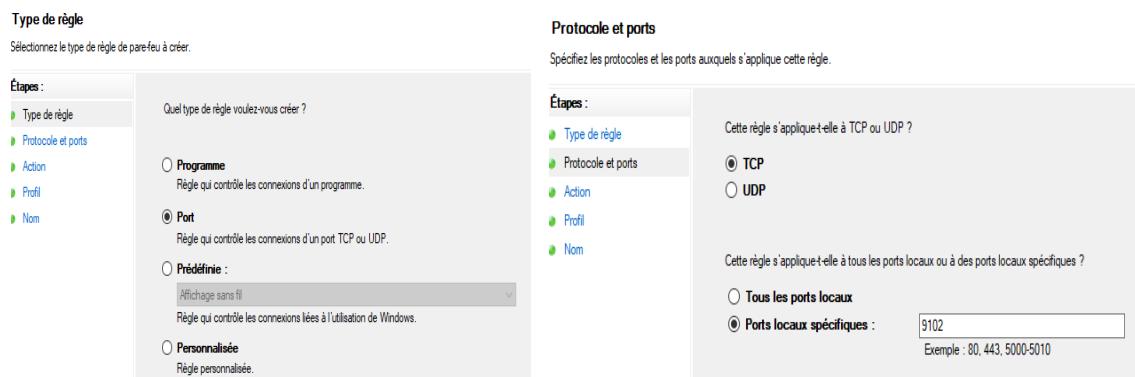


Figure 55 : Ouverture du port 9102 étape 1



Figure 56 : Ouverture du port 9102 étape 2

Spécifier le programme bacula dans la propriété dans le rôle présenté dans la figure 57.

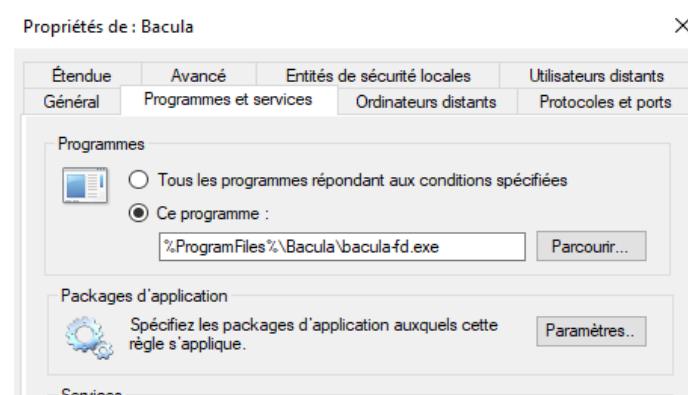


Figure 57 : Spécification du programme bacula

## 8.2 Mise en place du Serveur VPN « Pritunl »

### 8.2.1 Conditions préalables

Pour installer Pritunl, les prérequis sont :

- Accès root
- Un minimum de 512 Mo de RAM, ou le plan le plus bas.
- MongoDB
- Soit nano ou vim (éditeur de texte).
- SELinux désactivé

### 8.2.2 Installation des dépendances

Tout d'abord, nous devrons ajouter les référentiels nécessaires à « yum ». Yum est essentiellement le gestionnaire de paquets pour les systèmes RHEL. C'est semblable à « apt-get »

- La première chose à faire est d'ajouter le référentiel MongoDB :

```
#nano /etc/yum.repos.d/mongodb.repo
```

Les lignes suivantes seront ajoutées dans le fichier « **mongodb.repo** » :

```
[mongodb-org-3.2]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/3.2/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-3.2.asc
```

La figure 58 présente le contenu du fichier :

```
GNU nano 2.3.1      Fichier : /etc/yum.repos.d/mongodb.repo

[mongodb-org-3.2]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/3.2/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-3.2.asc
```

Figure 58 : Contenu de « **mongodb.repo** »

- La seconde chose à faire est d'ajouter le référentiel Pritunl :

```
#nano /etc/yum.repos.d/pritunl.repo
```

Nous ajoutons les lignes suivantes dans le fichier « **pritunl.repo** » :

```
[pritunl]
name=Pritunl Repository
baseurl=https://repo.pritunl.com/stable/yum/centos/7/
gpgcheck=1
enabled=1
[pritunl]
name=Pritunl Repository
baseurl=https://repo.pritunl.com/stable/yum/centos/7/
gpgcheck=1
enabled=1
```

La figure 59 montre le contenu après création :

```
GNU nano 2.3.1      Fichier : /etc/yum.repos.d/pritunl.repo

[pritunl]
name=Pritunl Repository
baseurl=https://repo.pritunl.com/stable/yum/centos/7/
gpgcheck=1
enabled=1
[pritunl]
name=Pritunl Repository
baseurl=https://repo.pritunl.com/stable/yum/centos/7/
gpgcheck=1
enabled=1
```

Figure 59 : Contenu de « pritunl.repo »

- Désactivation de SELinux

Désactiver le module SELinux par la commande suivante pour modifier le fichier de configuration SELinux :

```
#nano /etc/selinux/config
```

Changer la valeur de SELINUX, d' « **enforcing** » à « **disabled** ».

Cela devrait ressembler à la figure 60 :

```
GNU nano 2.3.1      Fichier : /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are pr$#
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Figure 60 : Valeur de SELinux

### **8.2.3 Installation de Pritunl**

Avant d'installer, le redémarrage du serveur est obligatoire après l'étape ci-dessus, et l'ajout de la clé est requis pour valider l'installation à l'aide des commandes suivantes :

```
#gpg --keyserver hkp://keyserver.ubuntu.com --recv-keys  
7568D9BB55FF9E5287D586017AE645C0CF8E292A  
  
#gpg --armor --export 7568D9BB55FF9E5287D586017AE645C0CF8E292A >  
key.tmp; sudo rpm --import key.tmp; rm -f key.tmp
```

Installation des logiciels :

```
#yum -y install pritunl mongodb-org
```

Lancement du MongoDB et Pritunl en les configurant pour qu'ils démarrent au démarrage :

```
#systemctl start mongod  
  
#systemctl start pritunl  
  
#systemctl enable mongod  
  
#systemctl enable pritunl
```

## 8.2.4 Configuration de Pritunl

### 8.2.4.1 Configuration initiale de Pritunl

Maintenant, accéder au tableau de bord Pritunl en cliquant sur le lien suivant. On utilise https, car Pritunl est configuré pour charger sur un port 443 qui est un port http sécurisé et accessible via une connexion sécurisée uniquement.

```
https://Adresse-IP du serveur
```

La figure 61 montre la page de configuration initiale de Pritunl :



Figure 61 : Page de configuration initiale de Pritunl

Pour continuer, entrer la clé d'installation. Pour obtenir la clé, exécuter la commande suivante dans le terminal.

```
#pritunl setup-key
```

Coller la clé qui a été donnée par la commande « **pritunl setup-key** ».

Après avoir cliqué sur le bouton « Save », définir les informations d'identification. Ensuite on est redirigé vers la page de connexion : voir figure 62.

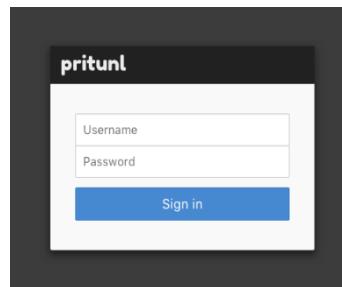


Figure 62 : Page de connexion de Pritunl

Après authentification, nous serons redirigés vers le tableau de bord de Pritunl : voir figure 63 :

The screenshot shows the Pritunl dashboard with three main sections: 'Organizations' (6/6 available), 'Users' (3/14 online), and 'Servers' (1/1 online). Below these are 'Recent log entries' which list various system and user actions with their timestamps.

Action	Date
Created new organization "Utilisateurs".	12:06 am - Jan 8 2019
Created new user.	11:56 am - Jan 8 2019
Deleted user "Admin".	11:07 am - Jan 8 2019
Created new user.	11:57 am - Dec 14 2018
Created new user.	11:56 am - Dec 14 2018
Started server "AITS-SRV".	12:54 am - Dec 5 2018
Stopped server "AITS-SRV".	12:52 am - Dec 5 2018
Created new user.	12:51 am - Dec 5 2018
Created new organization "USERS".	12:50 am - Dec 5 2018
Deleted organization "users".	12:50 am - Dec 5 2018
Created new organization "users".	12:50 am - Dec 5 2018
Created 0 new users.	12:47 am - Dec 5 2018
...	...

Figure 63 : Tableau de bord Pritunl

#### 8.2.4.1 Configuration de Client et Serveur

L’architecture à réaliser pour une connexion client/serveur avec Pritunl est donnée dans la figure 64 :

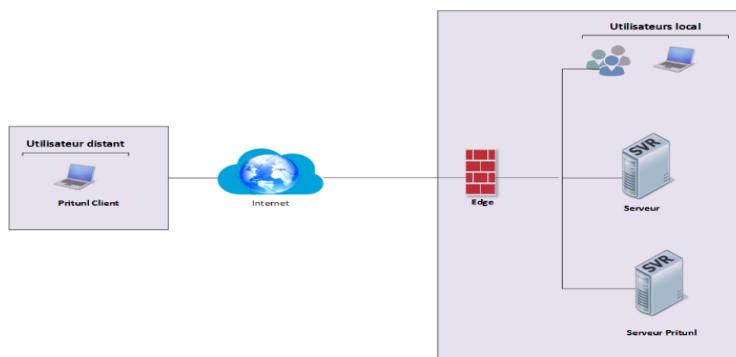


Figure 64 : Architecture VPN Client/serveur

Pour se connecter à un serveur VPN sur une organisation Pritunl, il faut créer un utilisateur et un serveur.

#### Etape 1° : Création d'organisation et d'utilisateur

Pour la création d'une organisation, cliquer sur « *Ajouter* » une organisation dans la page « *Organisation* » de la console Web.

Cliquer ensuite sur « *Ajouter un utilisateur* ». Une adresse électronique et un PIN d'utilisateur peuvent éventuellement être inclus.

The dialog box titled 'Add Organization' has a 'Name' field containing 'Utilisateurs'. At the bottom are 'Cancel' and 'Add' buttons.

Figure 65 : Ajout d'une organisation

Créer l’organisation « Utilisateurs », la figure 66 illustre la création de cette organisation :

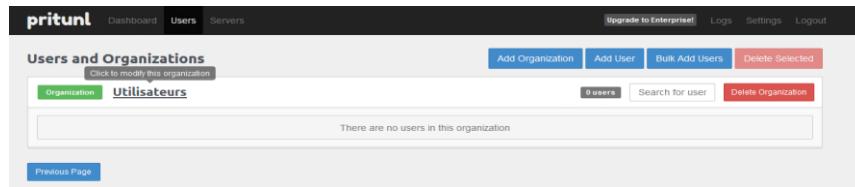


Figure 66 : Organisation bien créée

Maintenant, on procède à l'ajout d'un Utilisateur, que nous allons nommer « Zaho » avec un code PIN : voir la figure 67.

The screenshot shows the 'Add User' form. It has fields for Name (containing 'Zaho'), Select an organization (containing 'Utilisateurs'), Email (optional) (containing 'Enter email address'), and Pin (containing '\*\*\*\*\*'). At the bottom right are 'Cancel' and 'Add' buttons.

Figure 67 : Création d'un utilisateur

L'utilisateur « Zaho » sera créé, la figure 68 illustre la création de cet utilisateur :



Figure 68 : Utilisateur bien créé

## Etape 2° : Création de serveur

Une fois l'organisation et l'utilisateur créés, aller dans la page « Serveurs » et sur « Ajouter un serveur ». Par défaut, un port UDP aléatoire et un réseau VPN aléatoire seront sélectionnés. Le réseau ne doit pas entrer en conflit avec un réseau local sur l'ordinateur client, mais doit également être suffisamment grand pour tous les utilisateurs qui seront connectés au serveur. Le serveur DNS sera automatiquement défini sur le serveur DNS public de Google.

Une fois le serveur créé, continuons sur « Attacher une organisation » et attachez l'organisation créée précédemment au serveur. Ensuite sur « Démarrer le serveur » pour démarrer le serveur VPN.

La figure 69 indique la création du serveur :

The screenshot shows the 'Add Server' dialog box. It has fields for 'Name' (set to 'AITS-SRV'), 'DNS Server' (set to '8.8.8.8'), 'Port' (set to 80), 'Protocol' (set to 'tcp'), 'Virtual Network' (set to '253 Users'), and checkboxes for 'Enable IPv6' and 'Enable Two-Step Authentication'. At the bottom are 'Cancel' and 'Add' buttons.

Figure 69 : Crédit du serveur

Le serveur est bien créé, comme montré dans la figure 70.

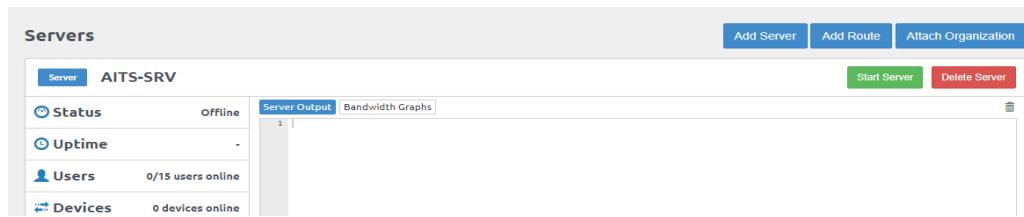


Figure 70 : Serveur bien créé

Et la figure 71 explique l'attachement de l'organisation au serveur créé :

The screenshot shows the 'Attach Organization' dialog box. It has a dropdown for 'Select an organization' (set to 'Utilisateurs') and a dropdown for 'Select a server' (set to 'AITS-SRV'). At the bottom are 'Cancel' and 'Attach' buttons.

Figure 71 : Attachement de l'organisation au serveur

Maintenant le démarrage du serveur, comme montré dans la figure 72 :

The screenshot shows the 'Servers' interface with the 'AITS-SRV' server selected. The 'Status' is 'Online'. The 'Uptime' is '0d 0h 9m 40s'. There are 2/15 users online and 2 devices online. The 'Network' and 'Port' sections show some activity. The 'Server Output' tab is active, displaying a log of 48 entries from the server's perspective. The log includes messages like 'User connected', 'Peer info' details, and 'Peer Connection Initiated'. At the top right, there are buttons for 'Add Server', 'Add Route', and 'Attach Organization'.

Figure 72 : Serveur bien démarrée

### Etape 3° : Configuration des itinéraires du serveur

Les itinéraires de serveur contrôlent le trafic qui sera « tunnelisé » sur le serveur VPN. Par défaut, un serveur inclura la 0.0.0.0/0 route. Cet itinéraire « tunnelera » tout le trafic Internet sur le serveur VPN. Pour router uniquement un réseau local sur le serveur VPN, commencer par supprimer la 0.0.0.0/0 route et cliquer sur « Ajouter une route » pour ajouter la route du réseau local telle que 192.168.0.0/24, comme présenté sur la figure 73.

The screenshot shows the 'Add Route' dialog box. It has a 'Network' field containing a blue bar icon, a 'Select a server' dropdown set to 'AITS-SRV', and an 'Advanced' button. At the bottom are 'Cancel' and 'Attach' buttons.

Figure 73 : Ajout d'une route

#### **Etape 4° : Téléchargement du profil utilisateur**

Une fois le serveur créé, le profil de l'utilisateur peut être téléchargé sur la page « *Utilisateurs* » en cliquant sur le bouton de téléchargement ou sur le bouton des liens de profil sur le côté droit de l'utilisateur. Le profil peut ensuite être importé dans le client Pritunl ou tout autre client OpenVPN, comme affiché dans les figures suivantes 74 et 75.

The screenshot shows a web-based management interface for users and organizations. At the top, there are buttons for 'Add Organization', 'Add User', 'Bulk Add Users', and 'Delete Selected'. Below this, a navigation bar includes tabs for 'Organization' and 'Utilisateurs', with 'Utilisateurs' selected. A search bar shows '1 users' and a 'Search for user' input field. On the right, there are icons for 'Delete Organization', 'Offline' status (red dot), and other user actions. The main list area shows a single user entry for 'Zaho', which includes a small icon, the name 'Zaho', and a download link icon. At the bottom left, there is a 'Previous Page' button.

Figure 74 : Téléchargement du profil

This screenshot shows a modal dialog titled 'Temporary Profile Link'. It contains four sections, each with a temporary URL and a download icon. 1. 'Temporary url to download profile, expires after 24 hours': [https://1\[REDACTED\]/key/2ae341aa487d471bb280f45d6273adce.tar](https://1[REDACTED]/key/2ae341aa487d471bb280f45d6273adce.tar). 2. 'Temporary url to download zip profile, expires after 24 hours': [https://1\[REDACTED\]/key/2ae341aa487d471bb280f45d6273adce.zip](https://1[REDACTED]/key/2ae341aa487d471bb280f45d6273adce.zip). 3. 'Temporary url to view profile links, expires after 24 hours': [https://1\[REDACTED\]/k/Dr3Rp9Cr](https://1[REDACTED]/k/Dr3Rp9Cr). 4. 'Temporary uri link for Pritunl Client, expires after 24 hours': [pritunl://1\[REDACTED\]/ku/Dr3Rp9Cr](pritunl://1[REDACTED]/ku/Dr3Rp9Cr). At the bottom right of the dialog is a 'Close' button.

Figure 75 : Liens de profil

## 8.2.5 Installation et configuration Client VPN

### 8.2.5.1 Pritunl Client

#### ❖ Linux

Un référentiel Linux est disponible pour plusieurs distributions. Les instructions pour installer le client à partir du référentiel sont disponibles sur la page d'accueil du site principal de Client Pritunl « <https://client.pritunl.com/#install> ». Installer le « `pritunl-client-gtk` » package pour les ordinateurs de bureau et les « `pritunl-client` » serveurs.

#### ❖ MacOs

Le package MacOs peut être téléchargé à partir de la page d'accueil « <https://client.pritunl.com/#install> ». Après le téléchargement, extraire le package du fichier zip et l'ouvrir.

#### ❖ Appareils mobiles

Un client Pritunl officiel n'est pas disponible sur les appareils mobiles, mais tout client OpenVPN peut être utilisé pour se connecter à Pritunl.

#### ❖ Windows

Le package Windows peut être téléchargé dans « <https://client.pritunl.com/#install> ». Une fois le téléchargement terminé, double-cliqué pour lancer le programme d'installation. Windows posera des questions de sécurité pour confirmer l'exécution du programme d'installation en répondant simplement « oui ».

Il devrait ressembler à pratiquement tout ce qui a été déjà installé sous Windows. Choisir d'accepter les conditions et procéder en utilisant les boutons « Suivant » de l'assistant d'installation.

Les figures 76 et 77 montrent l'installation de Pritunl Client.

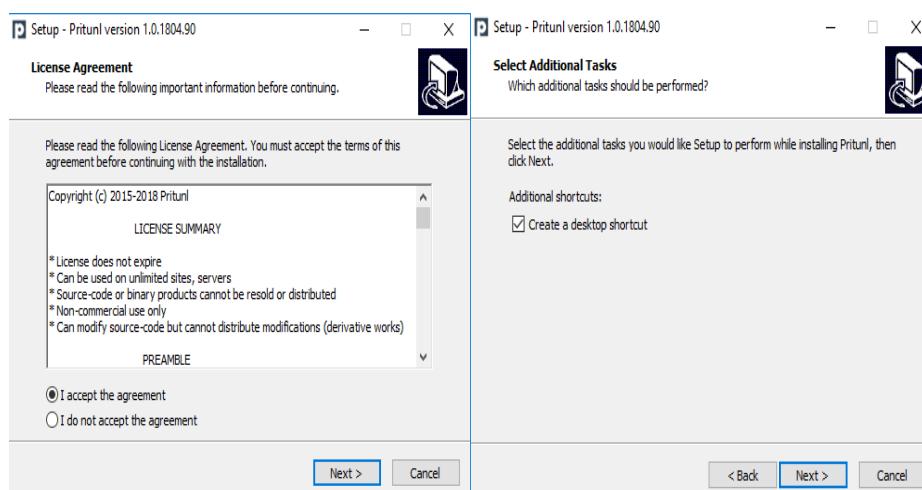


Figure 76 : Démarrage d'installation Pritunl Client

En cliquant sur « Install », le programme va être installé.

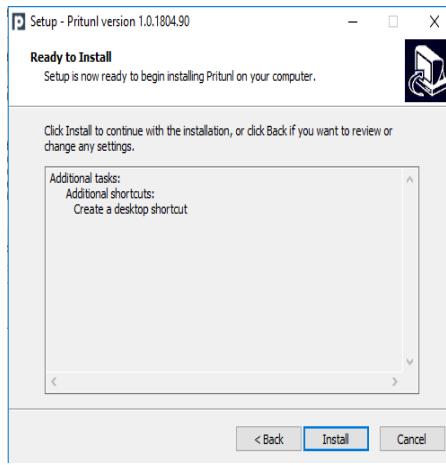


Figure 77 : Installation Pritunl Client

Une fois le programme d'installation installé, il devrait ressembler à pratiquement tout ce qui a déjà été installé sous Windows. Choisir d'accepter les conditions et procéder en utilisant les boutons « Suivant » de l'assistant d'installation.

À la fin, il devrait ajouter un raccourci sur le bureau et lancer l'application automatiquement.

### 8.2.5.2 OpenVPN Client

Nous allons configurer l'OpenVPN sur un client Windows. Il est nécessaire d'installer une application spécifique OpenVPN GUI for Windows qui se trouve à l'adresse suivante : <http://openvpn.net/index.php/download.html>.

Une fois l'application téléchargée, il faut lancer l'installateur du programme pour l'installer : cliquer sur « Next » et dans la fenêtre suivante, cliquer « I Agree », comme illustré dans les figures 78 et 79.

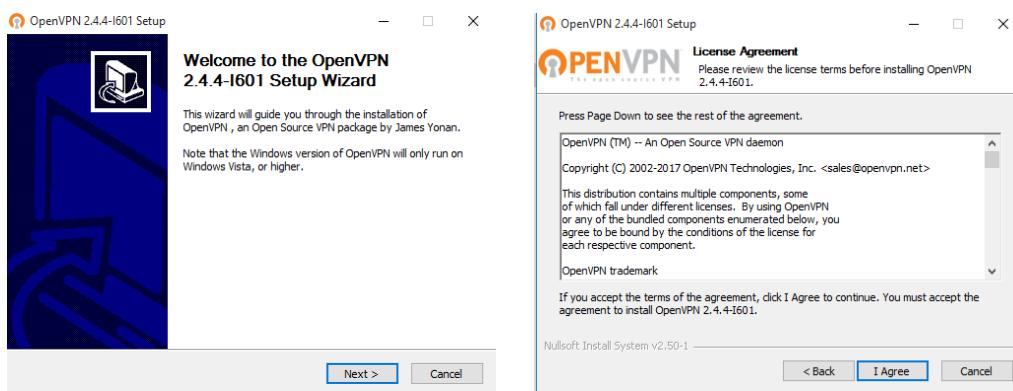


Figure 78 : Démarrage installation OpenVPN Client

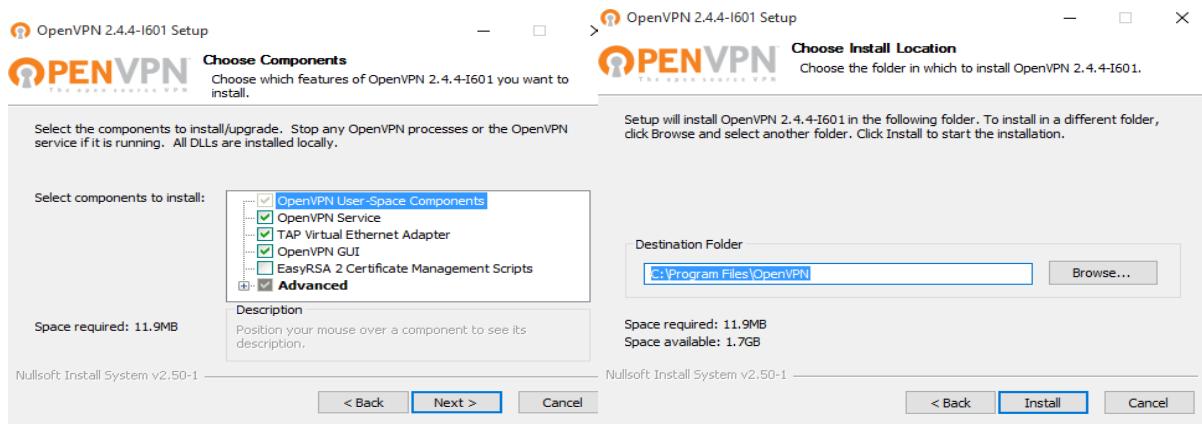


Figure 79 : Composantes d'OpenVPN à installer

Lorsqu'il nous sera demandé si nous souhaitons installer « **TAP-Win Provider** », sélectionner **"Installer"** : voir figure 80.

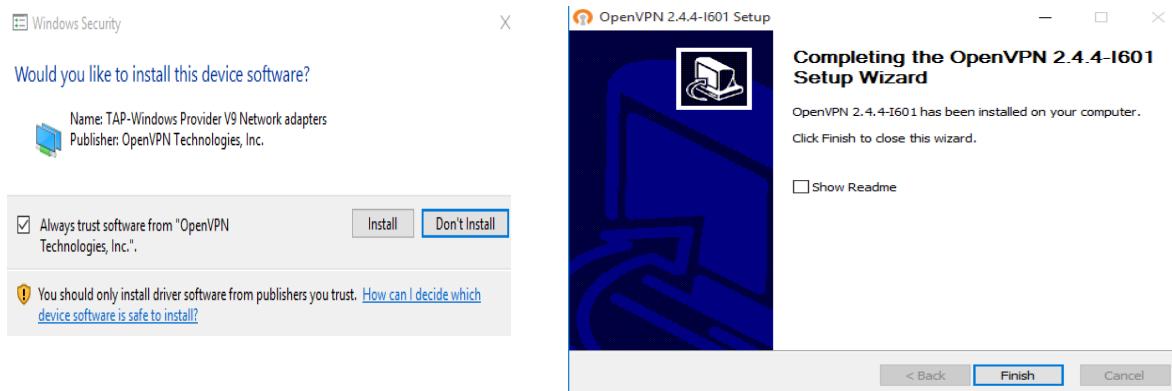


Figure 80 : Installation OpenVPN Client Complète

# Chapitre 9 : Validation et Perspective

## 9.1 Test et validation Sauvegarde et Restauration avec Bacula

L'architecture de d'utilisation du serveur de sauvegarde avec Bacula est illustrée dans la figure 81 :

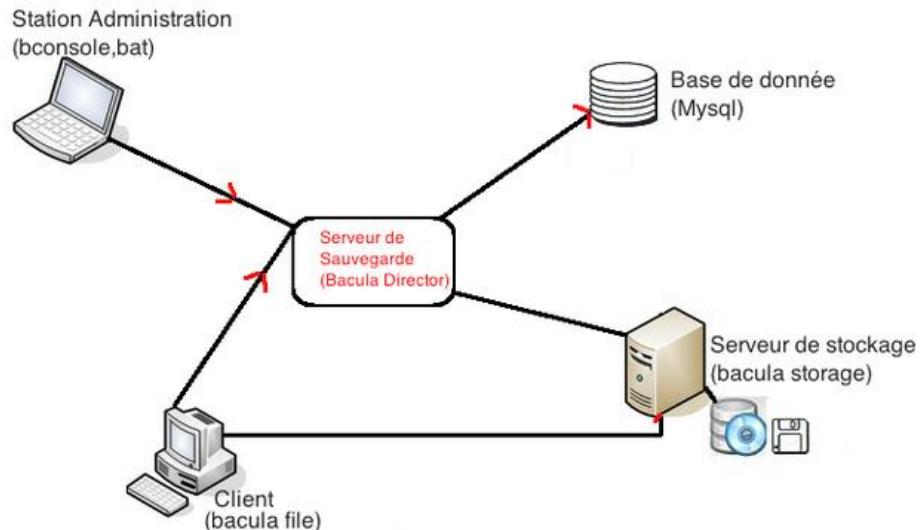


Figure 81 : Architecture Serveur de sauvegarde

La figure 83 présente les étapes de lancement d'une sauvegarde.

### 9.1.1 Lancement d'une sauvegarde

Avant tout, redémarrer le service Bacula, comme dans la figure 82.

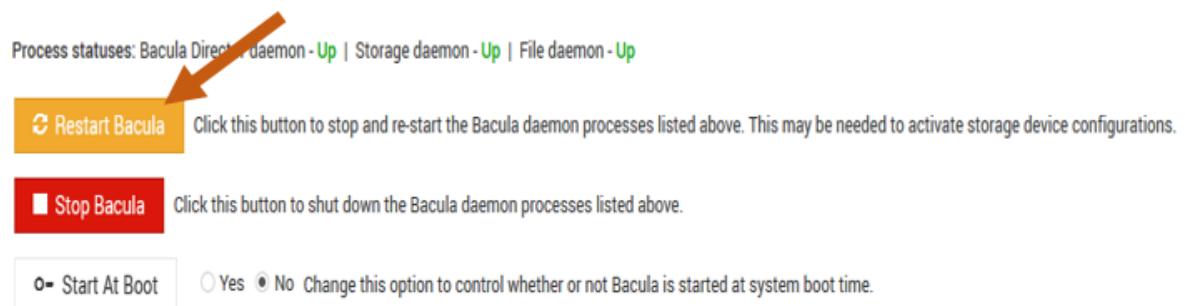


Figure 82 : Redémarrage du service Bacula

Les étapes de lancement de sauvegarde sont les suivantes :

- cliquer sur « Run Backup Job » ;
- choisir le « Job » à exécuter ;
- cliquer sur « Backup Now ».

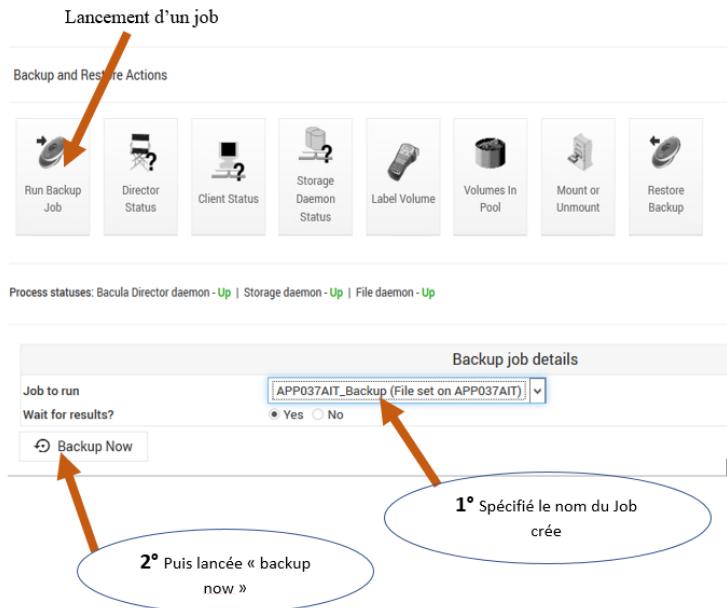


Figure 83 : Etape de lancement d'une sauvegarde

Voici dans la figure 84, le contenu du /data/TestBackup/ sur le client APP037AIT :

```
[root@APP037AIT data]# cd TestBackup/
[root@APP037AIT TestBackup]# ls
mysqlDataBase  OpenFile  OpenVPN  repose  yum.repos.d
[root@APP037AIT TestBackup]#
```

Figure 84 : Donnée à sauvegarder

Les figures 85 et 86 illustrent le lancement de la sauvegarde :

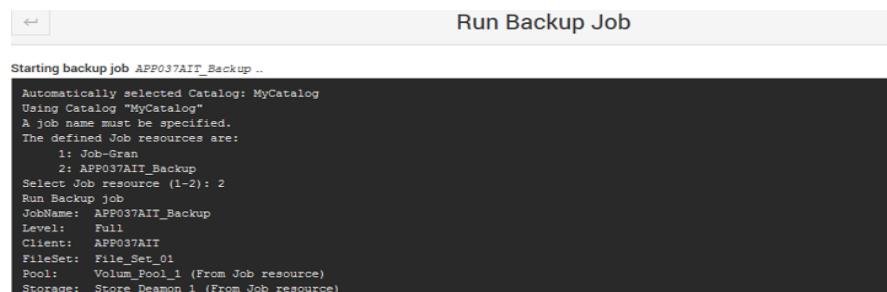


Figure 85 : Lancement de la sauvegarde

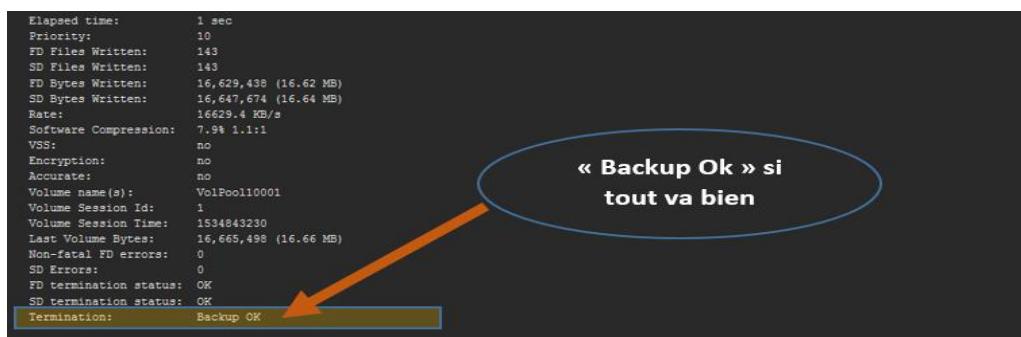
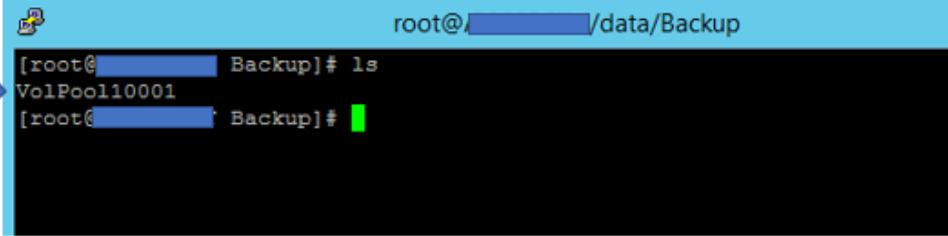


Figure 86 : Sauvegarde réussie

Les données sont compressées dans le serveur.



```
root@...:/data/Backup
[root@... Backup]# ls
VolPool10001
[root@... Backup]#
```

A blue arrow points from the left towards the terminal window.

Figure 87 : Données compressées dans le serveur

### 9.1.2 Lancement d'une restauration

Il faut définir un client pour la redirection de la restauration. La restauration se fait après une sauvegarde effectuée.

Dans la navigation, choisir « Restore Backup ». La figure 88 fournie détaille les étapes de lancement d'une restauration en cliquant sur « Restore Now ».

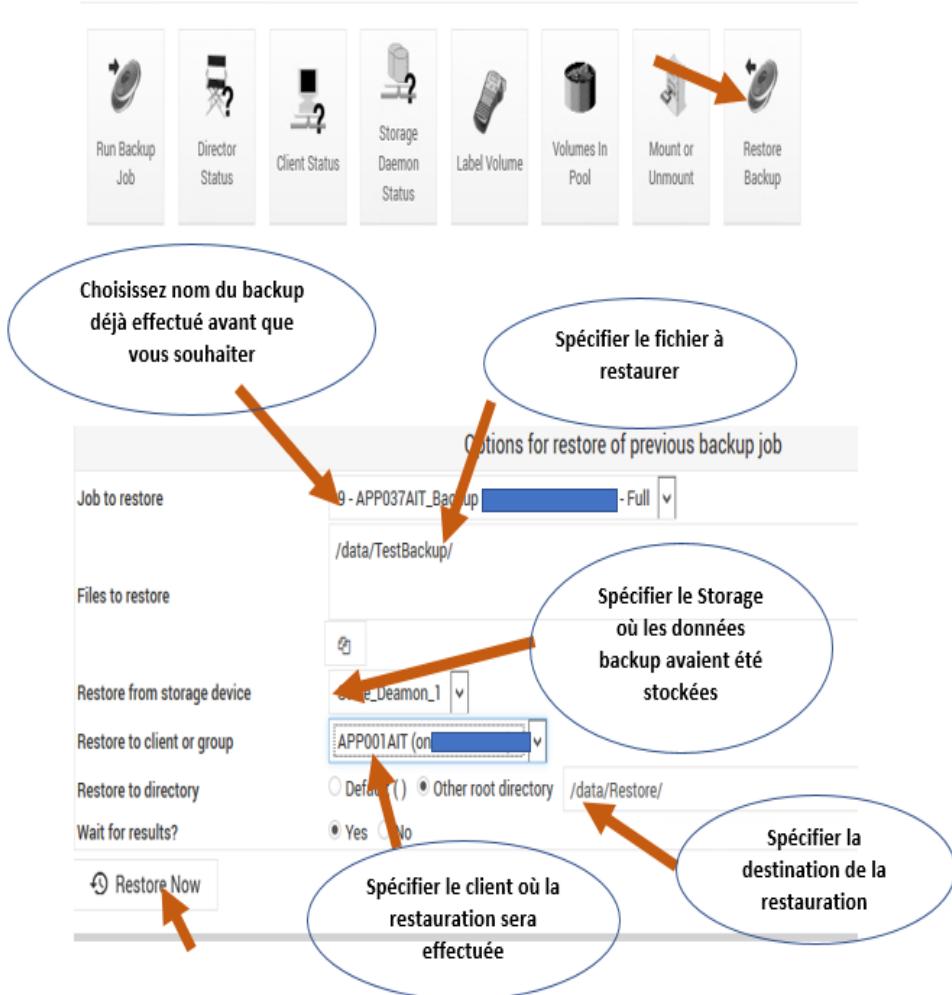


Figure 88 : Etapes de lancement d'une restauration

Les figures 89 et 90 illustrent le lancement de la sauvegarde.

Commencement de la restauration...

```
Starting restore of job APP037AIT_Backup to client APP001AIT from storage Store_Deamon_1 ..  
restore client=APP001AIT jobId=9 storage=Store_Deamon_1 where="/data/Restore/"  
Using Catalog "MyCatalog"  
You have selected the following JobId: 9  
  
Building directory tree for JobId(s) 9 ... ++++++  
135 files inserted into the tree.  
  
You are now entering file selection mode where you add (mark) and  
remove (unmark) files to be restored. No files are initially added, unless  
you used the "all" keyword on the command line.  
Enter "done" to leave this mode.  
  
 cwd is: /  
 $ cd "/data"  
 cwd is: /data/  
 $ mark "TestBackup"  
143 files marked.  
$ done
```

Figure 89 : Commencement de la restauration

```
Files Expected: 143  
Files Restored: 143  
Bytes Restored: 18,058,276  
Rate: 0.0 KB/s  
FD Errors: 0  
FD termination status: OK  
SD termination status: OK  
Termination: Restore OK
```

Restauration Ok

Figure 90 : Restauration réussie

### 9.1.3 Vérification

Nous allons comparer les données du client APP037AIT et les données restaurées dans le client APP001AIT, cela se résume dans la figure 91 :



The figure shows two terminal windows side-by-side. The left window is titled 'root@APP037AIT:~' and displays the command 'ls /data/TestBackup/' followed by a list of files: mysqlDataBase, Openldap, OpenVPN, repos, and yum.repos.d. The right window is titled 'root@APP001AIT:/tmp/configAPP001R' and displays the command 'ls /data/Restore/'. It shows a directory named 'data' which contains a file named 'TestBackup'. Inside 'data', there is a 'TestBackup' directory containing the same files as listed in the first window: mysqlDataBase, Openldap, OpenVPN, repos, and yum.repos.d. An orange arrow points from the 'data' directory in the right window to the 'TestBackup' file in the left window. A blue oval surrounds the 'TestBackup' file in the left window with the text 'Les données sont semblables' (The data is similar).

Figure 91 : Vérification des données restaurées

## 9.2 Test et Validation de Pritunl

Pour un client :

- ⇒ Récupérer le profile « OVPN » à l'administrateur
- ⇒ Installer le logiciel Pritunl Client ou OpenVPN Client
- ⇒ Importation du profil « OVPN »

### 9.2.1 Pritunl Client

Après avoir installé Pritunl Client, importer le profile « OVPN » et se connecter : les figures 92 et 93 donnent les étapes de connexion du client VPN au Serveur.

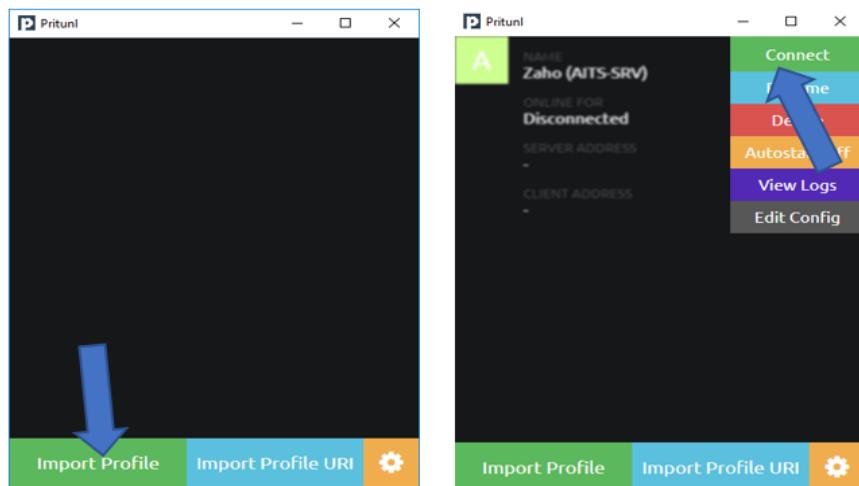


Figure 92 : Importation et connexion du profil VPN

Connecter avec le code PIN créé et cliquer sur OK. La connexion vers le serveur sera réussie une fois que le client aura une adresse IP privée assignée.

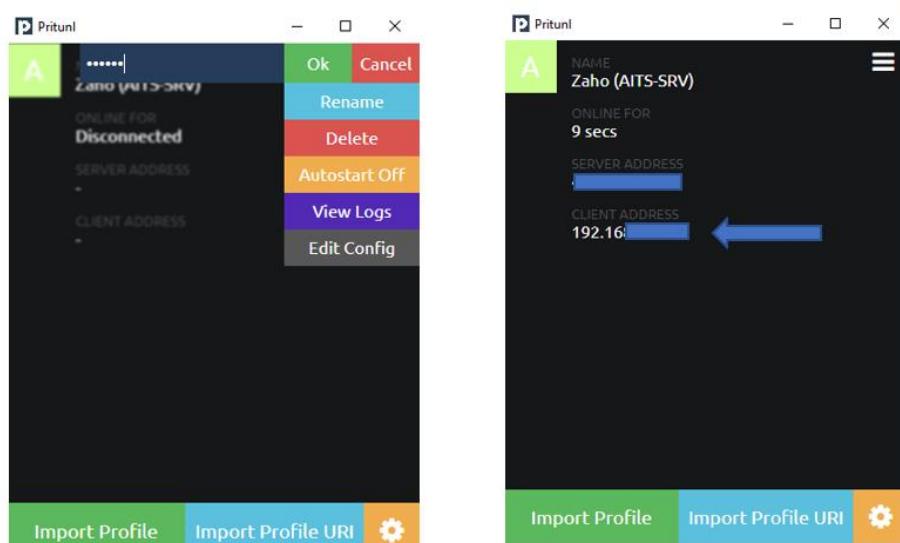


Figure 93 : Connexion au serveur VPN Pritunl réussi

### 9.2.2 OpenVPN Client

- Après installation OpenVPN Client, importer le profile « OVPN » dans le dossier de configuration Openvpn : « C:\Program Files\OpenVPN\config ».
- Lancer OpenVPN et saisir le nom d'utilisateur et le mot de passe avec le code PIN créé avant.

Les figures 93 et 95 expliquent la connexion du client OpenVPN au serveur Pritunl.

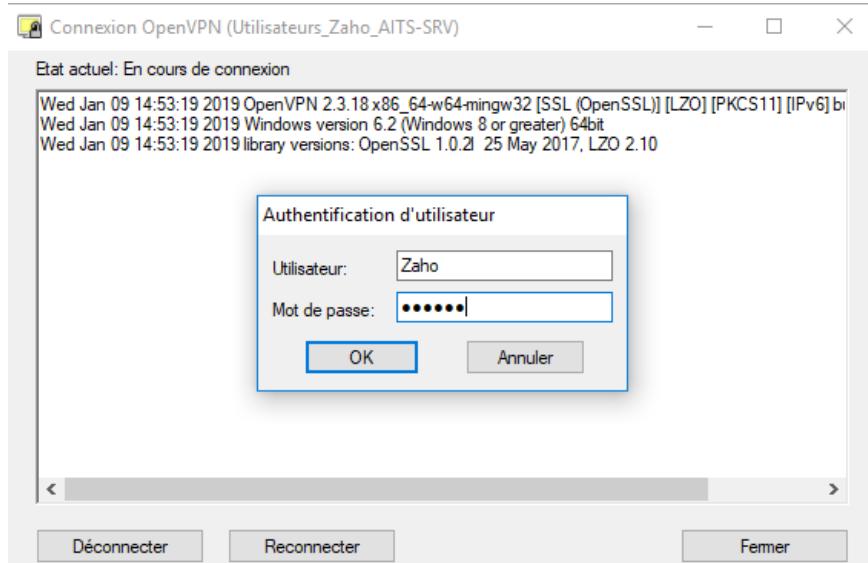


Figure 94 : Saisie des informations de connexion au VPN

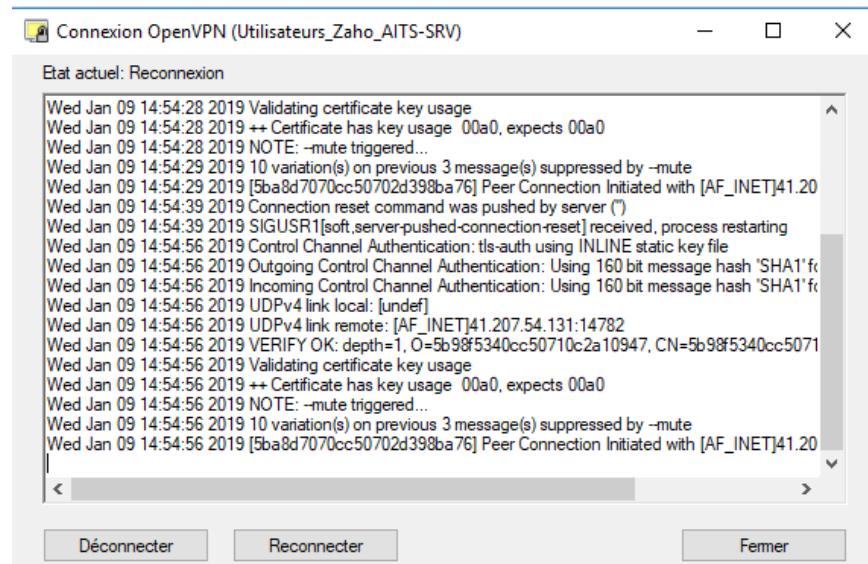


Figure 95 : Connexion vers le serveur

- De même, la connexion vers le serveur est réussie une fois que l'icône d'Openvpn deviendra verte et que le client aura une notification « Connecté » avec une adresse IP privée assignée : voir la figure 96 :



Figure 96 : Connexion réussie

De même façon avec l'OpenVPN sur les smartphones et les tablettes.

Test d'accès au serveur Bacula avec accès VPN à distant.

En utilisant « Putty » : les figures 97 et 98 illustrent l'accès SSH au serveur.

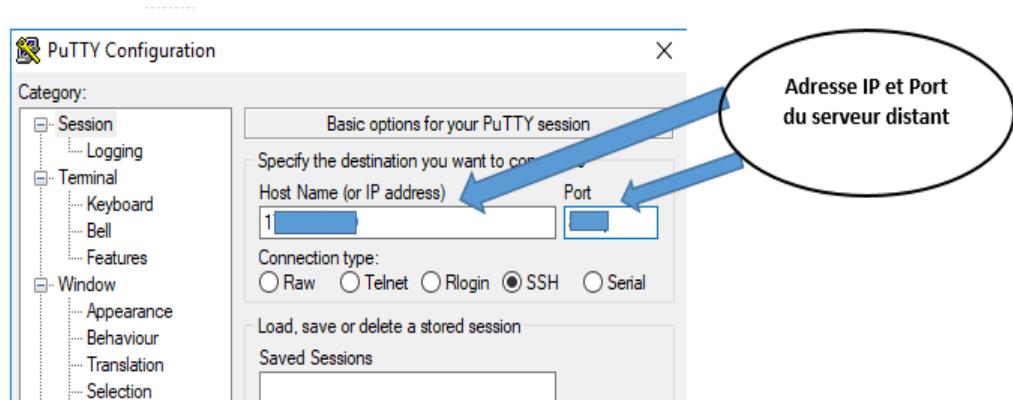


Figure 97 : Saisie d'adresse et port du serveur d'accès à distance

```
login as: soafaniry
soafaniry@[REDACTED]'s password:
Last login: Mon Jan 14 13:47:48 2019 from [REDACTED]
-sh-4.2$
```

Figure 98 : Accès au serveur Bacula réussi

Ensuite, on accède au compte super-utilisateur « root » après notre authentification, présentée dans la figure 99.

```
soafaniry@[REDACTED]:/home/soafaniry
login as: soafaniry
soafaniry@172.20.32.29's password:
Last login: Mon Jan 14 13:49:00 2019 from [REDACTED]
-sh-4.2$ su root
Mot de passe :
[root@[REDACTED] soafaniry]#
```

Figure 99 : Connexion et accès « root » réussi

# CONCLUSION GENERALE

Notre stage se termine après six mois au sein de la Société Group AXIAN, chargé de déployer et implémenter des solutions de sauvegarde réseau et d'un serveur VPN. L'importance des données de l'entreprise a provoqué la remise en question du bon fonctionnement des sauvegardes et l'automatisation de celles-ci.

Notre rôle fut donc de rechercher la solution la plus appropriée. La première phase de ce projet nous a permis d'étudier les différentes solutions de sauvegarde, nous apportant ainsi une meilleure acquisition de connaissances dans ce domaine très vaste et important pour un administrateur.

En effet, nous avons présenté un travail divisé en quatre grandes parties.

**La première partie**, subdivisée en trois chapitres, commence, au premier chapitre, par une présentation de l'Ecole Nationale d'Informatique, suivie de celle, dans le second, de la Société Groupe AXIAN. Enfin, le troisième chapitre fournit une description du projet.

**La deuxième partie** est une approche théorique et comprend deux chapitres. Le premier aborde deux des questions cruciales pour tout administrateur, à savoir la sauvegarde et le VPN. Le deuxième chapitre porte sur l'analyse préalable. Nous y avons effectué l'analyse de l'existant et la critique de l'existant qui nous a mené à proposer une solution de sauvegarde et de mettre en place un serveur VPN.

**La troisième partie** intitulée **Conception du nouveau système d'information** est subdivisée aussi en deux chapitres : le premier étudie les choix et la comparaison des outils pour la mise en œuvre du projet ; le second évoque la présentation des outils choisis, à savoir Bacula et Pritunl. Nous y avons traité de façon claire les notions, le fonctionnement ainsi que les différentes caractéristiques pour leur mise en place de Bacula et Pritunl.

Enfin, la **quatrième et dernière partie** est intitulée **Mise en œuvre et validation**. Le premier chapitre détaille la réalisation et la mise en place de Bacula et Pritunl. Le second chapitre, Validation, décrit les procédures de test.

Ainsi, grâce au système nouvellement mis en place, non seulement les risques liés aux pertes de données sont réduits puisque la sauvegarde est automatisée et tourne en permanence et que nous pouvons restaurer les données à tout moment (notons que l'efficacité de ce système ne dépend pas seulement de la phase initiale, mais aussi du suivi), mais encore l'accès sera possible depuis l'extérieur pour les administrations de tous les services, grâce au Serveur VPN mis en place.

Comme perspectives d'avenir, il sera possible et envisageable non seulement d'étudier la sécurité mais aussi d'explorer et orienter les recherches sur la sauvegarde complète d'un système dédié au virtuel comme Veems Backup surtout pour les entreprises utilisant des systèmes CLOUD.

# REFERENCES BIBLIOGRAPHIQUES

- [1] Eugene Pankov, Network Backup with Bacula How-To, Pack Publishing 2012, 55 pages
- [2] Pierre-Alain Goupille, Technologie des ordinateurs et des réseaux, 8<sup>e</sup> édition, 554 pages

# REFERENCES WEBGRAPHIQUES

- [3] <https://pritunl.com/> : Site officiel du Pritunl, Septembre 2018
- [4] <http://www.amanda.org/> : Site officiel d'Amanda, Septembre 2018
- [5] <http://www.areca-backup.org/> : Site officiel d'Areca Backup, Septembre 2018
- [6] <http://backuppc.sourceforge.net/info.html> : Site officiel BackupPC, Septembre 2018
- [7] <http://blog.bacula.org/> : Site officiel du Sauvegarde Bacula, Septembre 2018
- [8] <https://www.goldenfrog.com/fr/vyprvpn/features/vpn-protocols/> : Les protocoles VPN, Septembre 2018
- [9] <https://www.how2shout.com/tools/free-and-best-open-source-vpn-server-software.html> : Les serveurs VPN, Septembre 2018
- [10] <https://www.secuweb.fr/tutoriels-vpn/> : Différentes protocole d'OpenVPN, Septembre 2018
- [11] <http://www.commeo.eu/bacula-sauvegarde-restore-open-source/> : Sauvegarde et restauration Bacula, Septembre 2018
- [12] [http://www.bacula.org/9.2.x-manuals/en/main/What\\_is\\_Bacula.html](http://www.bacula.org/9.2.x-manuals/en/main/What_is_Bacula.html) : C'est quoi Bacula, Septembre 2018
- [13] [http://docs.bacula-web.org/en/latest/01\\_about/features.html](http://docs.bacula-web.org/en/latest/01_about/features.html) : A propos et Installation Bacula-Web, Octobre 2018
- [14] [http://igm.univ-mlv.fr/~dr/XPOSE2006/Charles\\_Daniel/presentation.html](http://igm.univ-mlv.fr/~dr/XPOSE2006/Charles_Daniel/presentation.html) :
- [15] <http://www.linux-magazine.com/Issues/2016/184/VPN-with-Pritunl> : Le VPN Pritunl, Octobre 2018
- [16] <https://hostpresto.com/community/tutorials/setting-up-a-vpn-server-using-pritunl-on-centos-7/> : Installation et Configuration Pritunl Server, Octobre 2018
- [17] <http://www.openvpn.net/index.php/open-source/overview.html> : Documentation officiel d'OpenVPN : proposant un manuel, des «howto», et de nombreuses informations utiles, Octobre 2018
- [18] <https://mariadb.com/kb/fr/a-propos-de-mariadb/> : Apropos de MariaDB, Octobre 2018
- [19] [https://fr.wikipedia.org/wiki/Sauvegarde\\_\(informatique\)](https://fr.wikipedia.org/wiki/Sauvegarde_(informatique)) : Le sauvegrade en informatique, Octobre 2018

# GLOSSAIRE

**Administrateur** : L'administrateur est une personne du service informatique qui a la responsabilité de gérer le serveur de l'entreprise. Il s'occupe de sa mise à jour, de vérifier son bon fonctionnement et de créer les nouveaux comptes, configurer les autorisations et les fichiers à partager, les mails, les sauvegardes, la sécurité.

**Auto-changeur** : Un périphérique automate qui inclut un robot, un lecteur de bandes et un ou plusieurs magasins pour les cartouches de bandes. Il permet le chargement ou le d'déchargement automatique des bandes de stockage.

**Backup** : Procédure de sauvegarde d'un ensemble de données informatiques sur un autre support que celui où elles se trouvent déjà (d'un disque dur vers une disquette, etc....)

**Daemon** : Programme informatique qui s'exécute en arrière-plan, plutôt que sous le contrôle direct d'un utilisateur. Ce programme est connu sous le nom de service sous *Windows*.

**Job** : ou travail, est le processus exécute dans le but de réaliser une sauvegarde ou restaurer des données.

**Logs** : En informatique, le concept d'historique des événements ou de « logging » désigne l'enregistrement séquentiel dans un fichier ou une base de données de tous les événements affectant un processus particulier (application, activité d'un réseau informatique...). Le fichier log, ou plus simplement, le log, désigne alors le fichier contenant ces enregistrements.

**Package** :(Red Hat Package manager ou rpm) est un système de gestion de paquets de logiciels utilisé sur certaines distributions GNU/Linux.

**Réseau** : Ensemble d'équipements informatiques connectés entre eux.

**Ressource** : Une ressource est une partie d'un fichier de configuration qui d'définit une unité spécifique d'information disponible pour Bacula. Par exemple, la ressource Job d'définit toutes les propriétés d'un Job spécifique : nom, Schedule (planification), volume pool, type de sauvegarde, niveau de sauvegarde.

**Serveur** : Ressource informatique sur laquelle tourne un ensemble de logiciels de gestion d'accès distants. Il fournit des informations et des ressources à d'autres ordinateurs qui s'y connectent.

**Virtualisation** : La virtualisation consiste à faire fonctionner sur un seul ordinateur plusieurs systèmes d'exploitation comme s'ils fonctionnaient sur des ordinateurs distincts

# ANNEXE

## Exemple configuration complet « **bacula-dir.conf** »

### La ressource “Director” :

```
Director {
  Name = bacula-dir
  DIRport = 9101
  QueryFile = "/etc/bacula/query.sql"
  WorkingDirectory = "/var/spool/bacula"
  PidDirectory = "/var/run"
  Maximum Concurrent Jobs = 1
  FD Connect Timeout = 1 mins
  Password = "@@DIR_PASSWORD@@@"
  Messages = Daemon
}
```

### La ressource “Storage” :

```
Storage {
  Name = File
  Address = Nom.de.domaine_ou_IP
  SDPort = 9103
  Password = "@@SD_PASSWORD@@@"
  Device = FileStorage
  Media Type = File
}
```

### La ressource “Pool” :

```
Pool {
  Name = Default
  Label Format = "Default-"
  Pool Type = Backup
  Recycle = yes
  Storage = File
  AutoPrune = yes
  Volume Retention = 40 days
  Maximum Volume Jobs = 3
  Recycle Oldest Volume = yes
}
Pool {
  Name = Full-Pool
  Pool Type = Backup
  Recycle = yes
  AutoPrune = yes
  Volume Retention = 14 days
  #Maximum Volume Jobs = 1
  Label Format = Full-
  Maximum Volumes = 10
  Storage = File
  Recycle Oldest Volume = yes
  #Use Volume Once = yes
  Maximum Volume Bytes = 1000000000000
  Recycle Current Volume = yes
}
Pool {
  Name = Diff-Pool
  Pool Type = Backup
```

```
Recycle = yes
AutoPrune = yes
Storage = File
Volume Retention = 14 days
#Maximum Volume Jobs = 1
Label Format = Diff-
Maximum Volumes = 10
Recycle Oldest Volume = yes
#Use Volume Once = yes
Maximum Volume Bytes = 1000000000000
Recycle Current Volume = yes
}
Pool {
  Name = Inc-Pool
  Pool Type = Backup
  Recycle = yes
  AutoPrune = yes
  Storage = File
  Volume Retention = 14 days
  #Maximum Volume Jobs = 1
  Label Format = Inc-
  Maximum Volumes = 10
  Recycle Oldest Volume = yes
  # Use Volume Once = yes
  Maximum Volume Bytes = 1000000000000
  Recycle Current Volume = yes
}
```

### La ressource “Schedule” :

```
Schedule {
  Name = "WeeklyCycle"
  Run = Level = Full mon at 12:00
  Run = Level = Differential tue-fri at 12:00
}
```

### La ressource “FileSet” :

```
FileSet {
  Name = "Full Set Windows"
  Enable VSS = yes
  Include {
    File = "d:/Documents and Settings"
    Options {
      Signature = MD5
      IgnoreCase = yes
      Exclude=yes
      Compression=GZIP
    }
  }
}
```

```
FileSet {
  Name = "Full Set linux"
  Include {
```

```

Options {
Signature = MD5
IgnoreCase = yes
Compression=GZIP
}
File = "/home/"
File = "/var/www"
File = "/media/commun/Mes documents"
}
Exclude {
File = /proc
File = /tmp
}

```

#### **La ressource "Catalog" :**

```

Catalog {
Name = MyCatalog
# Uncomment the following line if you want the dbi driver
# dbdriver = "dbi:sqlite3"; dbaddress = 127.0.0.1; dbport
=
dbname = nom_de_BDD; DB Address = "localhost";
dbuser = "user_avec_priviléges"; dbpassword =
"mot_de_passe"
}

```

#### **La ressource "Message" :**

```

Messages {
Name = Daemon
mailcommand = "/usr/lib/bacula/bsmtp -h localhost -f
"\\"(Bacula\\) \\<%r\\>" -s \"Bacula daemon message\" %r"
mail = root@localhost = all, !skipped
console = all, !skipped, !saved
append = "/var/lib/bacula/log" = all, !skipped
}
Messages {
Name = Standard
mailcommand = "/usr/lib/bacula/bsmtp -h localhost -f
"\\"(Bacula\\) \\<%r\\>" -s \"Bacula: %t %e of %c %l\\\" %r"
operatorcommand = "/usr/lib/bacula/bsmtp -h localhost -
f "\\"(Bacula\\) \\<%r\\>" -s \"Bacula: Intervention needed
for %j\\\" %r"
mail = root@localhost = all, !skipped
operator = root@localhost = mount
console = all, !skipped, !saved
append = "/var/lib/bacula/log" = all, !skipped
catalog = all
}

```

#### **La ressource "Console" :**

```

Console {
Name = Bacula-mon
Password =
"mot_de_passe_d'accès_pour_les_consoles_d'admin"
CommandACL = status, .status
}

```

#### **La ressource "Client" :**

```

Client {
Name = nom_du_client_fd

```

```

Address = 192.168.0.1
FDPort = 9102
Catalog = MyCatalog
Password = "mot_de_passe"
File Retention = 30 days
Job Retention = 6 months
AutoPrune = yes
}

```

#### **Les ressources "Job" et "JobDefs" :**

```

Job {
Name = "Backup-nom_de_machine-fd"
Client = nom_du_client-fd
JobDefs = "DefaultBackup"
Run Before Job = "script"
Run After Job = "script }}"

```

```

JobDefs {
Name = "DefaultBackup"
Type = Backup
Level = Full
Max Run Time = 360 mins
FileSet = "Full Set Windows"
Schedule = "WeeklyCycle"
Storage = File
Messages = Standard
Accurate = yes
Pool = Full-Pool
Full Backup Pool = Full-Pool
Differential Backup Pool = Diff-Pool
Incremental Backup Pool = Inc-Pool
Priority = 10
Reschedule On Error = yes
Reschedule Interval = 15 minutes
Reschedule Times = 5
Write Bootstrap = "/var/spool/bacula/Client1.bsr"
}

```

# TABLES DES MATIERES

CURRICULUM VITAE .....	I
DEDICACE.....	IV
REMERCIEMENTS .....	V
SOMMAIRE .....	VI
NOMENCLATURE .....	VII
LISTE DES TABLEAUX .....	IX
LISTES DES FIGURE.....	X
INTRODUCTION GENERALE .....	1
PARTIE I : PRESENTATION GENERALE.....	1
Chapitre 1 : Présentation de L'ENI .....	2
1.1 Informations d'ordre général .....	2
1.2 Missions et historique .....	2
1.3 Organigramme institutionnel de l'ENI.....	3
1.4 Domaines de spécialisation .....	5
1.5 Architecture des formations pédagogiques .....	5
1.6 Relations de l'ENI avec les entreprises et les organismes.....	7
1.7 Partenariat au niveau international .....	8
1.8 Débouchés professionnels des diplômes .....	10
1.9 Ressources Humaines.....	12
Chapitre 2 : Présentation du Groupe Axian .....	13
2.1 Présentation générale du groupe Axian.....	13
2.2 Historiques.....	13
2.3 Visions.....	15
2.4 Engagement du groupe .....	15
2.4.1 Axian, acteur économique responsable et engagé .....	15
2.4.2 Un investissement dans les talents .....	15
2.4.3 Un engagement sociétal fort.....	15
2.5 Implantations.....	16
2.6 Activités .....	17
2.7 Organigramme d'Axian IT Services.....	18
Chapitre 3 : Description du Stage .....	19
3.1 Généralités .....	19
3.2 Description du Projet.....	19

3.3 Objectifs du Projet.....	20
3.4 Moyens matériels .....	20
3.5 Résultats attendus.....	21
3.6 Définition du cahier des charges .....	21
3.7 Chronogramme.....	21
PARTIE II : GENERALITE ET ANALYSE .....	23
Chapitre 4 : Généralités sur La Sauvegarde et Le VPN .....	24
4.1 Sauvegarde .....	24
4.1.1 Généralité .....	24
4.1.2 Finalité .....	25
4.1.3 Critères de choix.....	25
4.1.4 Différents types de sauvegarde.....	25
4.1.4.1 Sauvegardes des données en local.....	26
4.1.4.2 Sauvegardes des données sur le réseau.....	26
4.1.5 Stratégie de sauvegarde .....	27
4.1.5 Méthodes de sauvegarde les plus courantes.....	27
4.1.6 Techniques complémentaires .....	28
4.2 VPN « Virtual Private Network » .....	29
4.2.1 Présentation .....	29
4.2.2 Principe général.....	29
4.2.3 Fonctionnalités des VPN.....	30
4.2.3.1 Site-to-Site VPN.....	30
4.2.3.2 Client-to-Site VPN.....	30
4.2.4 Protocoles utilisés pour réaliser une connexion VPN .....	31
Chapitre 5 : Analyse Préalable.....	32
5.1 Analyse de l'existant.....	32
5.1.1 Description .....	32
5.1.2 Structure et topologie du réseau .....	32
5.1.3 Type de réseaux.....	34
5.1.4 Equipement d'interconnexion.....	34
5.1.5 Postes de travail .....	35
5.1.6 Serveurs.....	36
5.1.7 Passerelle.....	37
5.1.8 Partage .....	37
5.1.9 Routage .....	37
5.1.10 Disponibilité.....	38

5.1.11 Surveillance .....	38
5.1.12 Analyse du trafic.....	39
5.1.13 Sécurité.....	42
5.2 Critique de l'existant .....	42
5.3 Solutions .....	43
5.3.1 Proposition de solutions.....	43
5.3.2 Solutions retenues.....	43
PARTIE III : CHOIX DE L'OUTIL.....	44
Chapitre 6 : Comparaison des outils.....	44
6.1 Outils de Sauvegarde.....	44
6.1.1 Amanda .....	44
6.1.2 Areca Backup .....	45
6.1.3 BackupPC.....	46
6.1.4 Bacula .....	47
6.2 Serveurs VPN .....	50
6.2.1 OpenVPN Server.....	50
6.2.2 Pritunl Server.....	51
6.2.3 SoftEther Server .....	52
6.2.4 Server VPN OpenConnect.....	52
Chapitre 7 : Présentation de l'Outil Choisi .....	54
7.1 Bacula .....	54
7.1.1 Introduction.....	54
7.1.2 Principales caractéristiques.....	55
7.1.2.1 Généralité.....	55
7.1.2.2 Avantages.....	56
7.1.3 Architecture.....	56
7.1.3 Composants de Bacula .....	58
7.1.3.1 Directeur.....	58
7.1.3.2 Storage Daemon.....	58
7.1.3.3 Filer Daemon.....	58
7.1.3.4 Console.....	59
7.1.3.5 Catalogue.....	59
7.1.4 Tâche de sauvegarde .....	60
7.1.4.1 Concept de « job » .....	60
7.1.4.2 Ressource « Client » .....	60
7.1.4.3 Ressource « FileSet » .....	60

7.1.4.4 Niveau de sauvegarde.....	61
7.1.4.5 Planification d'un Job (Schedule) .....	61
7.1.4.6 Ressource "Storage".....	61
7.1.4.7 Ressource "Pool".....	62
7.1.4.8 Ressource « Volume » .....	62
7.1.4.9 Règles de nommage des volumes.....	62
7.1.4.10 Utilisation des volumes.....	63
7.1.4.11 Conservation des volumes et recyclage.....	63
7.1.4.12 Gestion manuelle des volumes.....	63
7.1.4.13 Messages.....	63
7.1.5 Fonctionnalités de Bacula.....	64
7.1.5.1 Exécution de scripts.....	64
7.1.5.2 Lancement d'une tâche.....	64
7.1.5.3 Clonage de Jobs.....	64
7.1.5.4 Lancer des tâches en parallèles.....	65
7.1.5.5 Restauration de fichiers.....	65
7.1.5.6 Jobs bloqués.....	65
7.1.7 Base de données.....	66
7.1.7.1 Généralités.....	66
7.1.7.2 Sécurité.....	66
7.1.7.3 Compatibilité.....	66
7.1.8 Outils autour de Bacula .....	67
7.1.8.1 Bacula Web.....	67
7.1.8.2 Webmin.....	68
7.2 Pritunl .....	70
7.2.1 Introduction.....	70
7.2.2 Généralité .....	70
7.2.3 Caractéristiques.....	71
7.2.4 Modèle de prix .....	72
7.2.5 Fonctionnements.....	72
PARTIE IV : MISE EN OEUVRE ET VALIDATION.....	75
Chapitre 8 : Réalisation .....	74
8.1 Mise en place BACULA.....	74
8.1.1 Conditions préalables .....	74
8.1.2 Installation de Bacula .....	74
8.1.2.1 Installer le package MariaDB Server.....	74

8.1.2.2 Installer les packages Postfix.....	77
8.1.2.4 Installer les packages Bacula-Web.....	79
8.1.2.5 Installer les packages Bacula.....	80
8.1.3 Configuration .....	81
8.1.3.1 Configuration de la base de données MariaDB.....	81
8.1.3.2 Configuration de sauvegarde Bacula avec Webmin.....	83
8.1.3.3 Configuration de Bacula-Web.....	91
8.1.3.4 Configuration de pare-feu et ports.....	91
8.1.4 Installation et Configuration Client .....	92
8.1.4.1 Client Linux.....	92
8.1.4.2 Client Windows.....	93
8.2 Mise en place du Serveur VPN « Pritunl » .....	95
8.2.1 Conditions préalables .....	95
8.2.2 Installation des dépendances .....	95
8.2.3 Installation de Pritunl .....	97
8.2.4 Configuration de Pritunl .....	98
8.2.4.1 Configuration initiale de Pritunl.....	98
8.2.5 Installation et configuration Client VPN .....	104
8.2.5.1 Pritunl Client.....	104
Chapitre 9 : Validation et Perspective .....	107
9.1 Test et validation Sauvegarde et Restauration avec Bacula .....	107
9.1.1 Lancement d'une sauvegarde .....	107
9.1.2 Lancement d'une restauration.....	109
9.1.3 Vérification .....	110
9.2 Test et Validation de Pritunl .....	111
9.2.1 Pritunl Client.....	111
9.2.2 OpenVPN Client .....	112
CONCLUSION GENERALE .....	114
REFERENCES BIBLIOGRAPHIQUES .....	115
REFERENCES WEBOGRAPHIQUES.....	115
GLOSSAIRE .....	116
ANNEXE .....	117
TABLES DES MATIERES .....	XIII
R E S U M E.....	XVIII
ABSTRACT .....	XVIIIVIII

# RESUME

Dans ce projet, nous avons conçu et mis en place une solution de sauvegarde réseau et un serveur VPN dans le Groupe AXIAN.

Le système de sauvegarde de la société est assuré maintenant par les administrateurs au moyen du logiciel Bacula, une solution de sauvegarde centralisée. Ainsi que les accès sécurisés aux serveurs via le serveur Pritunl qui est le principal outil permettant d'implémenter les VPN, l'accès était possible en interne pour les utilisateurs du réseau local de l'entreprise, mais aussi en externe pour les utilisateurs situés en dehors du réseau.

La réalisation du projet nécessite une recherche et une analyse de la documentation technique de Bacula, Pritunl et tous les éléments dont dépend leur fonctionnement ; ces solutions sollicitent aussi des connaissances soutenues en administration systèmes et réseaux. De plus ce projet se différencie des autres de par ses nombreuses fonctionnalités et sa flexibilité, et il correspond parfaitement aux attentes des administrateurs de la société concernant une sauvegarde fiable et un accès sécurisé

**Mots-clés :** Sauvegarde, logiciel libre, réseau, auto-changeur, GPL, linux, VPN

## ABSTRACT

In this project, we designed and implemented a network backup solution and a VPN server in the AXIAN Group.

The company's backup system is now supported by administrators using Bacula, a centralized backup solution. As well as secure access to servers by the Pritunl server which is the main tool for implementing VPNs, access was possible internally for the users of the local network of the company, but also externally for the users located in outside the network.

The realization of the project requires a research and analysis of the technical documentation of Bacula, Pritunl and all the elements on which their functioning depends; theses solutions also require substained knowledge in systems and network administration. Moreover, this project differs from others in its many features and flexibility, and it perfectly corresponds to the expectations of the administrators of the company concerning a reliable backup and secure access.

**Keywords:** Backup, free software, network, auto-changer, GPL, linux, VPN