PROJET WEB MAIL SERVER

CESI GMSI APL13 – Groupe 1

Membres :

Nicolas BRICNET, Emilien BALTEAU, Remi DITER, Mattéo FOUQUET, Timothée FOUREL, Charles GABRIEL, Maxime GUERESCHI, Raphael HELD, Rémy MANGENOT, Remy SAVONNIERE, Jean-Gabriel DRON

cesi ÉCOLE SUPÉRIEURE DE L'ALTERNANCE

Table des matières

I. Les besoins du projet

Le projet WMS nous impose de déployer les solutions suivantes :

- 2 sites Web (CMS), comprenant les attentes suivantes :
    - Chaque CMS doit être différent, c'est-à-dire qu'ils doivent avoir des Templates différents, comprenant au minimum deux pages présentation
    - Les CMS doivent disposer de liens vers des fichiers PDF stockés sur le serveur
    - Les CMS doivent être sécurisés, ainsi que leurs interfaces d'administration
    - Les 2 sites web doivent être déployés sur leurs domaines respectif
- Un serveur FTP devant :
    - Stocker des fichiers PDF
    - Être sécurisé
    - Être installé sur un système d'exploitation Linux
- Une messagerie multi-domaines avec une base PostFix, devant respecter les impératifs suivants :
    - La messagerie multi-domaines doit fonctionner sous un système d'exploitation Linux
    - Comprendre un Webmail et une interface d'administration Web pour la création de boites aux lettres et d'alias
    - Comprendre une solution anti-spam
    - La messagerie multi-domaine doit comprendre 2 noms de domaine DNS différent (en lien avec les 2 sites web)
- Un outil de monitoring permettant de superviser les solutions déployées

Les solutions à déployer seront hébergées sur un ou plusieurs serveurs OVH

II. Gestion de projet

1. Organisation des équipes

Afin de créer les différents groupes lors du lancement du projet, nous avons fait un tour de table en vocal et également un sondage pour voir qui était plus à l'aise ou non avec l'environnement Debian, une fois les différents profils cernés, j'ai regroupé les équipes du projet afin qu'elles soient le plus homogènes possible.

Les équipes ont été structuré au fur et à mesure de la façon suivante :

L'équipe infrastructure a donc été divisée après l'étude des besoins via OVH parmi les équipes déjà existantes, et une équipe sécurité a été mise en place pour sécuriser les environnements avant l'installation des solutions.

Phase 1 :		Phase 2 :
Mail :	3	**Sécurité**
Timothée FOUREL		Timothée FOUREL
Raphaël HELD		Jean Gabriel DRON
Emilien BALTEAU		
		Mail :
Supervision :	2	Emilien BALTEAU
Charles Gabriel		Remy SAVONNIERE
Nicolas BRICNET		Raphaël HELD
Hébergement Web/FTP	3	**Hébergement Web/FTP**
Remy SAVONNIERE		Remy MANGENOT
Remy MANGENOT		Remi DITER
Mattéo FOUQUET		
		Supervision :
Infrastructure :	2	Charles Gabriel
Remi DITER		Nicolas BRICNET
Maxime GUERESCHI		Mattéo FOUQUET
Procédures :	1	**Infrastructure**
Jean Gabriel DRON		Maxime GUERESCHI
Chef de projet :	1	
Nicolas BRICNET		

2. Tableau de suivi

Une fois les équipes constituées, nous avons mis en place nos différents outils de collaborations :

Lot 1 : Analyse des environnements

	Maxime GUERESCHI		Rémi DITER		Jean-Gabriel DRON		Émilien BALTEAU		Nicolas BRICNET		Mattéo FOUQUET		Charles GABRIEL		Raphaël HELD		Rémy MANGENOT		Rémy SAVONNIÈRE		Timothée FOUREL	
Lot 1 : Analyse de l'environnement	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel	Tps Est	Tps réel
Infrastructure																						
Analyse des offres OVH	3	2,5	3	2,5	3	2,5																
Compilation des configurations de chaque Pôle	1		1		1																	
Comparatif des solutions	1	2	1	2	1	2																
Choix des infrastructures	1	2,5	1	2,5	1	2,5																
CMS/FTP																						
Analyse de la configuration minimale -> Infrastructure																	1	1	0,5	0,5		
Recherche de procédure de mise en place																	2	3	1	1		
Mail																						
Analyse de la configuration minimale -> Infrastructure							0.5	0.10								0.10			0,5	0,5		
Recherche de procédure de mise en place							0.5	0.5							0.5	0.5			1	1	0.5	
Supervision																						
Analyse de la configuration minimale -> Infrastructure													0.10	0.10								
Recherche de procédure de mise en place													0.5	0.5								
Procédural																						
Template des Procédures																						
Gestion de Projet																						
Création des équipes									1	2												
Tableau de suivit V1									4	6												
Compte rendu de la mise en route du projet									0.5	0.5												
Page Source avec les différentes procs d'installation																						

Lot 2 : Sécurité des environnements

Lot 2 : Sécurité & Procédure																						
Infrastructure																						
Création Keepass																		2				
Configuration Putty																						
Changement de l'accès ssh																			0,5	0,5		
Changement de PORT SSH																			1	1,5		
Installation Fail2ban																	0,5	0,5	1	1		
Création des différents profils Admin																			0,5	1,5		
Prévisionnel DNS																						
Schéma d'infra Système (Dépendance entre les technos)			2,5	3,5																		
Maquette Local :																						
Maquette WEB (WP et DRUPAL)																	3	3				
Maquette Nagios													2	4								
Maquette Mail							2.5	2.5							2.5				2	2		
Proc d'installation de base																						

Lot 3 : Configuration & installation

Lot 3 : Mise en production des solutions																						
CMS/FTP																						
Installation Web																						
Apache, MariaDB, PHP																	0,5	0,5				
Installation Bind9																						
Gestion des DNS																						
Paramétrage Apache																						
Paramétrage des alias DNS																						
Installation des CMS																						
Création des bases de données.																	0,2	0,2				
Installation Wordpress																	2	2				
Installation Drupal																	2	3				
Installation du FTP																						
Configuration des Profils FTP																						
Configuration des Accès FTP																						
Screen pour Procédure																						
CMS :																						
Certificat SSL																						
Configuration HTTPS																						
FTP :																						
Gestion des droits Fichiez																						
Gestion des accès																						
Procédure																						
Mail																						
Installation PostFix																			1	1		
Configuration DNS																			0,5	0,5		
Paramétrage Postfix																			0,5	0,75		
Installation Interface User																			2	2		
Installation Interface Admin																			2	2		
Paramétrage boite mail																			1	1		
Screen pour Procédure							2	2														
Procédure															4	4						
Supervision																						
Création de la base de données Nagios																						
Installation Nagios XI																						
Configuration Nagios XI																						
Installation des Agents																						
Monitoring des services																						
Screen pour Procédure																						
Procédure													3									

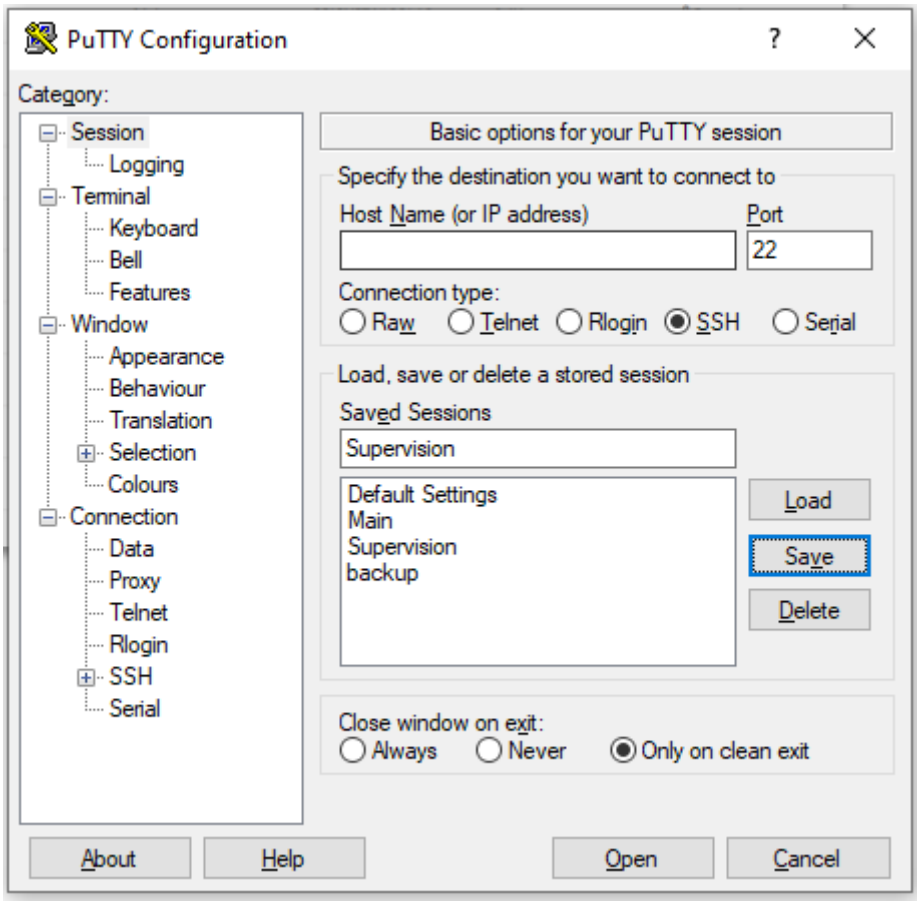
Lot 4 : Documentation

Lot 4 : Documentation et présentation																						
PCI / PRI																						
Chriffrage des solutions																						
Chriffrage de la main d'œuvre																						
PowerPOINT																						
Dossier Final																						
Cahier de recette																						

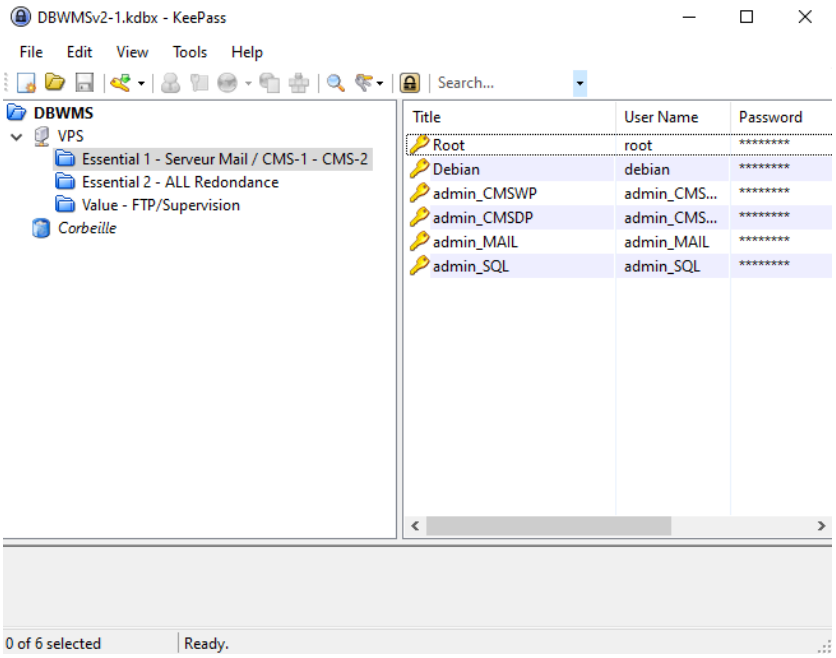
3. Nos outils

3.1. Sharepoint

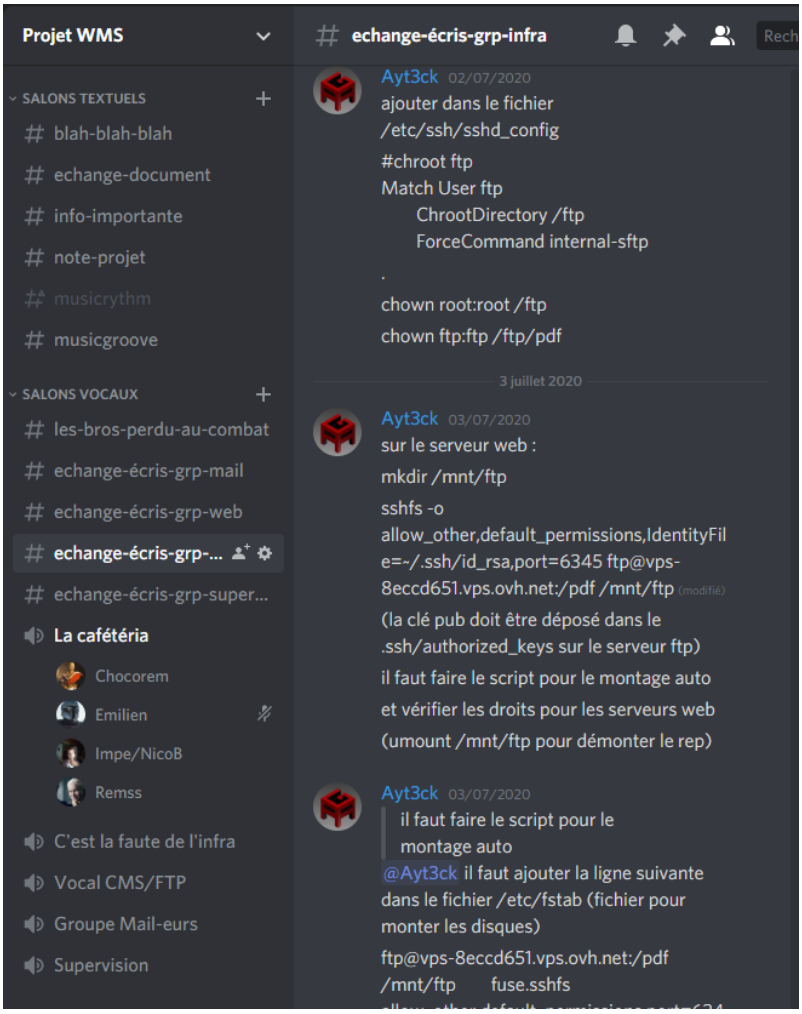
3.2. Paramétrage Putty



3.3. Base Keepass



3.4. Discord



Une fois toutes nos plateformes de communication mises en place, chaque équipe a analysée les prérequis à la mise en place de leur solution, et ainsi déterminé quelle infrastructure nous allions mettre en place et ainsi déterminer également le tableau de suivi autour du projet.

Afin d'avancer correctement sur le projet, chaque journée de travail autour du projet, une répartition des taches a été postée sur notre discord afin de répartir correctement les tâches au fur et à mesure du projet.

Exemple :

Maxime :

Automatisation des sauvegardes des configs

- Base de données Mail
- Conf Mail
- Fichier de conf FTP
- Fichier FTP
- Dossier Wordpress
- Dossier Drupal
- Base de Donnée WP & Drupal Maria DB
- Conf Pare-feu
- Conf Fail2ban
- Conf Virtual Host
- Conf SSH
- Clef SSH

Charles | Mattéo :

Paramétrage supervision :

- Personnalisation de l'interface
- Mapping du VPS
- Mapping des services manquant (Mail etc..)
- Envoi de Mail.
- Procédure Supervision.
- Choix de la supervision.

Remy M | Remi D :

- Personnalisation Drupal Wordpress
- Liaison CMS & PDF
- Configuration Virtual Host

Timothée :

- Certificat SSL
- Installation SFTP
- Ajout des pares-feux sur les Serv 1 & 3

Raphael | Remy S | Emilien :

- Réinstallation avec apache2
- Test d'envoi de mail avec la mise en place du pare-feu
- Paramétrage Mail (Création des boites mail &
- Choix des solutions

Jean-Gabriel :

- Pare-feu & certif SSL avec Timothée
- Assemblage et rédaction du Dossier

III. Analyse de l'environnement

1. Infrastructure

1.1. Comparatifs des VPS OVH

Ci-dessous, un comparatif des VPS (Serveurs Privés Virtuels) proposés par OVH :

	Offre VALUE	Offre ESSENTIAL	Offre COMFORT
Processeur	1 vCore	2 vCore	4 vCore
Mémoire	2 Go	4 Go	8 Go
Stockage	40 Go NVMe	80 Go NVMe	160 Go NVMe
Bande passante	250 Mbit/s	500 Mbit/s	1 Gbit/s
Prix (sans engagement)	**5,00€**	**10,00€**	**20,00€**

Options de sauvegarde		
Sauvegarde manuelle	**Sauvegarde automatique**	**Espace de sauvegarde supplémentaire**
1 €	**3 €**	À partir de **5 €**

La sauvegarde manuelle : créer un instantané, ou Snapshot, de votre machine virtuelle. Contrairement à une sauvegarde complète, vous n'avez pas à verrouiller les données pour empêcher leur modification en cours de procédure. Vous disposez ainsi en permanence d'un point de restauration intégral.

La sauvegarde automatique : sauvegardez efficacement votre VPS (hors disques additionnels) grâce à une tâche planifiée quotidienne, qui sera ensuite exportée puis répliquée trois fois avant d'être disponible dans l'espace client.

1.2. Couts

Concernant l'espace de sauvegarde supplémentaire, OVH propose les options suivantes :

- 50 Go pour **5 € HT/mois**
- 100 Go pour **10 € HT/mois**
- 200 Go pour **15 € HT/mois**
- 500 Go pour **30 € HT/mois**

OVH propose également plusieurs services pour le stockage et la sauvegarde des données :

Type de stockage	Intitulée de la technologie de sauvegarde		
Stockage en réseau	NAS HA	Backup Storage	Veeam Backup
Prix	À partir de **59 € HT/mois**	À partir de **12 € HT/mois**	À partir de **10 € HT/mois**
Stockage Hardware	Serveur stockage		
Prix	À partir de **84,99 € HT/mois**		
Stockage Cloud	Object Storage	Additional Disks	Veeam Cloud Connect
Prix	À partir de **0,01 € HT/mois**	À partir de **0,04 € HT/mois/Go**	À partir de **14,99 € HT**

2. Choix des VPS

Dans un premier temps, nous avons simulé deux configurations différentes pour le déploiement des solutions :

Simulation 1			Simulation 2		
Offre VPS	-1 offre VALUE	-FTP -Les 2CMS	**Offre VPS**	-1 offre VALUE	-Supervision -FTP (redondant)
	-1 offre VALUE	Supervision		-1 offre ESSENTIAL	-Messagerie multi-domaines -Les 2 CMS
	-1 offre ESSENTIAL	Messagerie multi-domaines		-1 offre ESSENTIAL	-Messagerie multi-domaines (réplication) -Les 2 CMS (réplication) -FTP
Sauvegarde	Une sauvegarde manuelle pour le VPS ESSENTIAL		**Sauvegarde**	Une sauvegarde automatique pour les 1 VPS ESSENTIAL	
	Veeam Backup managed				
Total		**27 €**	**Total**		**31 €**

Nous avons choisi de prendre le **Choix 2** pour un total de **31€.**

Choix des VPS et des OS :

<u>Sur l'offre Essential 1 : (Serveur Mail 1 / CMS 1 et 2)</u>

- **Debian 10**

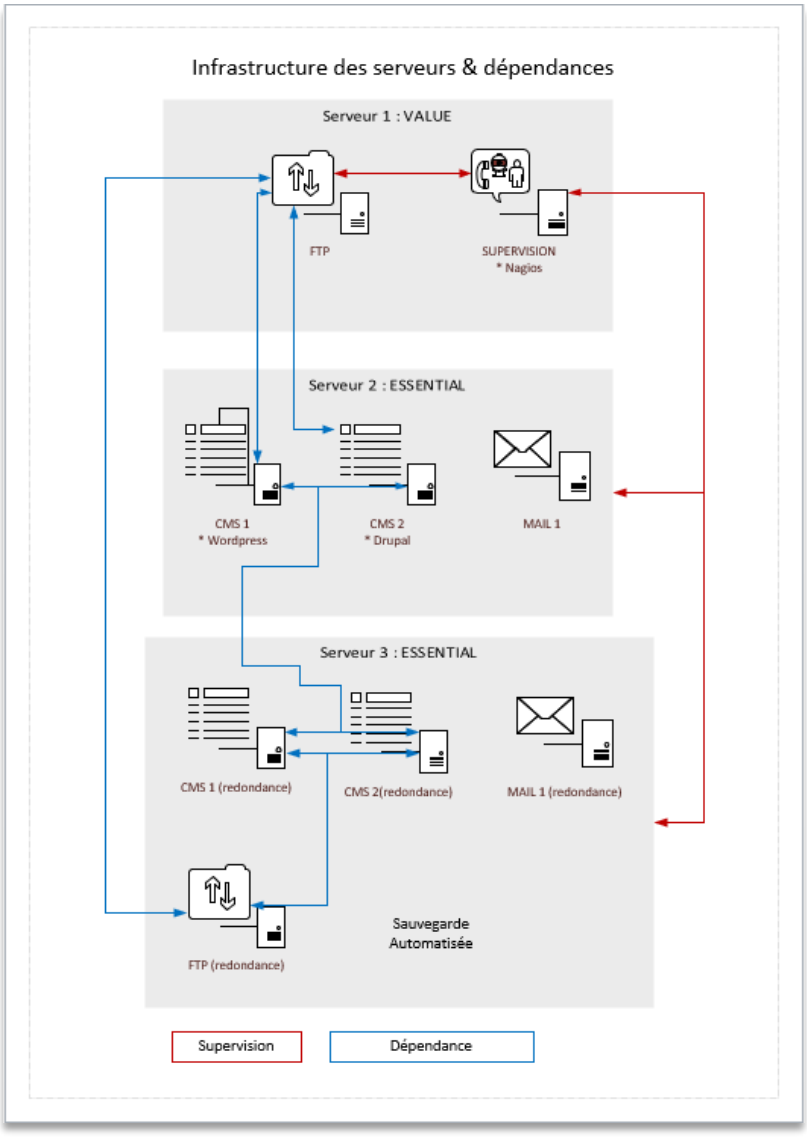
<u>Sur l'offre Essential 2 : (Serveur Mail 2 (réplication) / CMS 1 et 2 (réplication) / FTP / Sauvegarde automatique)</u>

- **Debian 10**

<u>Sur l'offre Value : (FTP (redondant)/Supervision)</u>

- **Debian 10**

3. Schéma relationnel applicatif

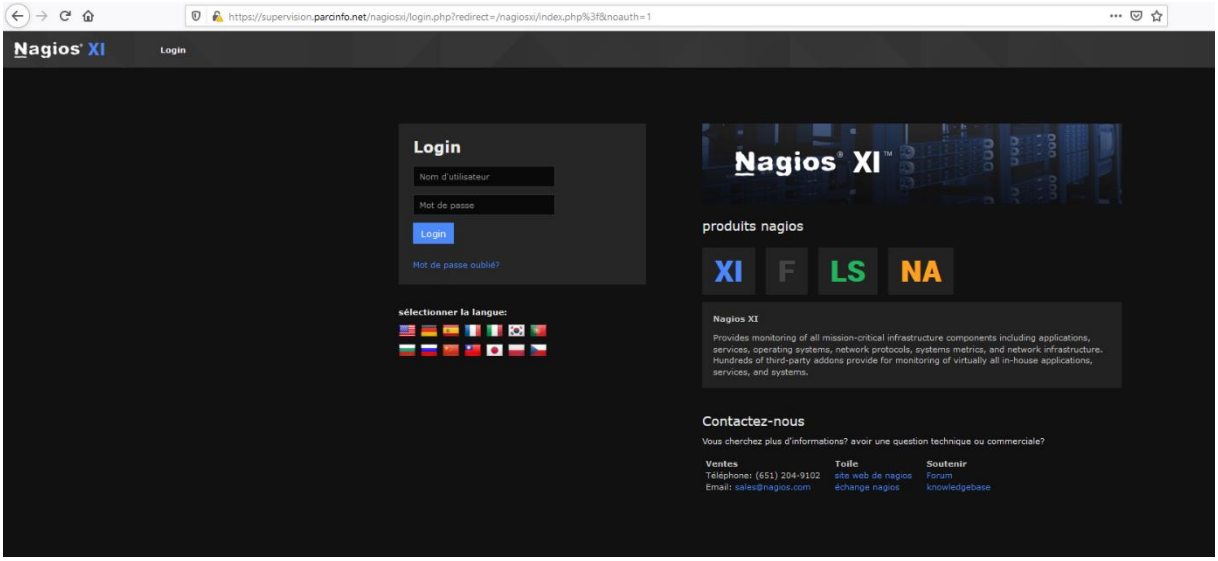


Paramétrage DNS :

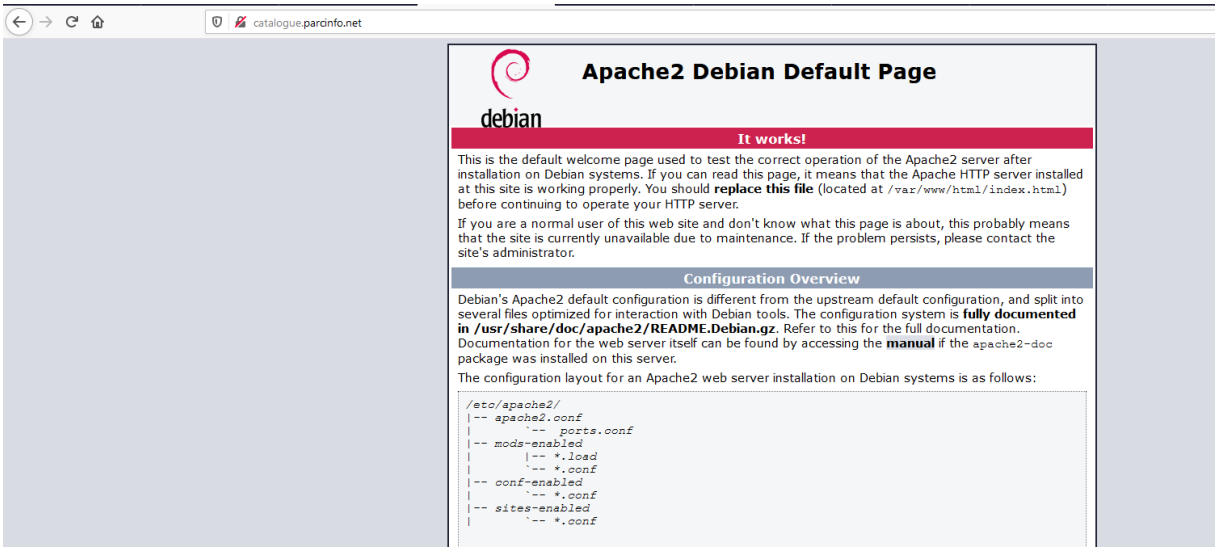
Domaine	TTL	Type	Cible
parcinfo.net.	0	NS	dns19.ovh.net.
parcinfo.net.	0	NS	ns19.ovh.net.
catalogue.parcinfo.net.	0	A	51.75.64.79
commande.parcinfo.net.	0	A	51.75.79.200
supervision.parcinfo.net.	0	A	51.75.73.103

Test :

Supervision.parcinfo.net (Supervision/ftp)



Catalogue.parcinfo.net :



IV. PCI / PRI

1. PCI

Un plan de continuité informatique (PCI) consiste, pour ce projet, à garantir le bon fonctionnement des solutions mises en place. Pour garantir l'intégrité de ces solutions, nous prévoyons notamment la mise en place de moyens de sauvegardes, nous permettant de rétablir rapidement les solutions et les données qui s'en suivent en cas de sinistre.

1.1. Intégrité matérielle

L'intégralité des solutions et des données seront déployées et stockées sur les serveurs privés virtuels (VPS) de OVH, signifiant que nous n'aurons pas la main sur ce matériel en cas de dysfonctionnement. Néanmoins, OVH garantit tout de même pour ses VPS :

- Des performances élevées
- Une disponibilité adaptée aux environnements de production ou de préproduction
- De la simplicité et de l'autonomie sur les VPS, nous permettant de nous affranchir des contraintes matérielles

1.2. Réplication

Nous comptons répliquer les services qui doivent être déployés sur un serveur de secours. C'est pour cette raison que nous avons fait le choix d'acquérir trois VPS qui devrons être déployés de la manière suivante :

- Serveur 1 (offre VALUE) : Déploiement de la solution de supervision, du serveur FTP ainsi que le stockage des documents PDF
- Serveur 2 (offre ESSENTIAL) : Déploiement de la messagerie multi-domaine fonctionnement sous Postfix, ainsi que les deux CMS
- Serveur 3 (offre ESSENTIAL avec sauvegarde automatique) : Ce serveur étant le seul à bénéficier d'une option de sauvegarde, il nous servira à l'avenir, à répliquer les services des deux premiers serveurs, seule la solution de supervision ne sera pas répliquée

1.3. Sauvegarde et archivage

Nous installerons également le logiciel BorgBackup qui est un outil de sauvegarde incrémentiel en ligne de commande sur le serveur 3 pour :

- Sauvegarder les données des serveur 1 et 2
- Archiver les données des serveurs 1 et 2, nous permettant de conserver les données sur le long terme

Nous avons choisi ce logiciel pour la sauvegarde des données car il permet d'optimiser l'espace disque lors des sauvegardes grâce à la déduplication, d'améliorer la vitesse de transfert des données en fonction de la compression choisi et de chiffrer les données sauvegardées.

1.3.1. Fréquences de l'archivage des données

Les sauvegardes des données seront effectuées quotidiennement, et nous conserverons les archives de la manière suivante :

- Une archive par jour les 7 derniers jours
- Une archive par semaine pour les 4 dernières semaines
- Une archive par mois pour les 6 derniers mois

Les archives qui ne seront pas conservées seront supprimer automatiquement à l'aide borg prune.

1.4. Rétablissement des VPS et des solutions durant un sinistre

Dans l'éventualité où les serveurs et les solutions déployés seraient amenés à subir un quelconque sinistre, nous avons prévu de mettre en place les mesures suivantes pour rétablir les services le plus rapidement possible :

- Sinistre sur un ou plusieurs VPS :
    - Si le ou les VPS ne disposant pas de la sauvegarde automatique (snapshot) venaient à subir un sinistre, nous les réinstallerons intégralement les solutions grâce aux fichiers de configurations sauvegardés sur le serveur N°3
    - Si le serveur disposant des sauvegardes automatiques (snapshot) venait à subir un sinistre, nous restaurerions le VPS grâce au précèdent snapshot disponible
- Sinistre sur les solutions mises en place :
    - Si nous sommes amenés à subir un sinistre sur une ou plusieurs solutions déployées, nous les réinstallerons grâce aux fichiers de configurations sauvegardées

2. PRI

Le plan de reprise informatique (PRI), permet de déterminer par anticipation, les actions à mettre en place en cas sinistres, visant à remettre le plus rapidement possible le système informatique.

2.1. VPS

Concernant les VPS choisis, nous sommes dans l'obligation de laisser notre entière confiance aux services fournies par OVH en cas de sinistres.

2.2. Pannes ou pertes de services

Dans l'éventualité où un crache matériel ou logiciel se produirai, nous avons la possibilité de rétablir les services perdus de la manière suivante :

- Restauration des serveurs disposant de sauvegardes automatiques
- Mise en place de réplications des services sur le VPS ESSENTIAL disposant des sauvegardes automatiques, nous permettant de redéployer intégralement les services sur le serveurs indisponible, grâce aux sauvegardes effectuées sur le serveur de réplication

2.3. Les sauvegardes

Pour nous assurer que les sauvegardes sont correctement effectuées sur le serveur servant à la réplication des services, nous feront dans un premier temps, des consultations régulières du fichier journal (log) de BORG Backup. Par la suite, nous exporterons le fichier journal via un courrier électronique (email), étant donné que nous disposons d'une messagerie multi-domaine local, nous permettant d'automatiser ce processus.

V. Solution de sauvegarde

1. Comparatif des solutions existante

Dans le but de sélectionner la meilleure solution de sauvegarde qui répondra au mieux aux attentes du projet, nous avons décidez de comparer les trois outils suivants :

	FreeFileSync	Borg	bareos
Sauvegarde incrémentielle	Oui	Oui	Oui
Sauvegarde différentielle	Oui	Oui	Oui
Mise à disposition de plusieurs outils de compressions des données	Non	lz4, gzip et lzma	Non
Chiffrement des données	Non	Oui	Oui
Vérification de l'intégrité des indexes et des données	Non	Oui	/
Sauvegarde distante sécurisé	Non	Oui via SSH	Oui (utilisation de ports TCP/IP enregistrés auprès de l'IANA)
Reprise intelligente d'une sauvegarde interrompue	Oui	Oui	/
Archivage des données sauvegardées	Oui	Oui	Oui
Sauvegarde prévue de serveur à serveur	Non	Oui	Oui
Prix	Open Source	Open Source	Open Source

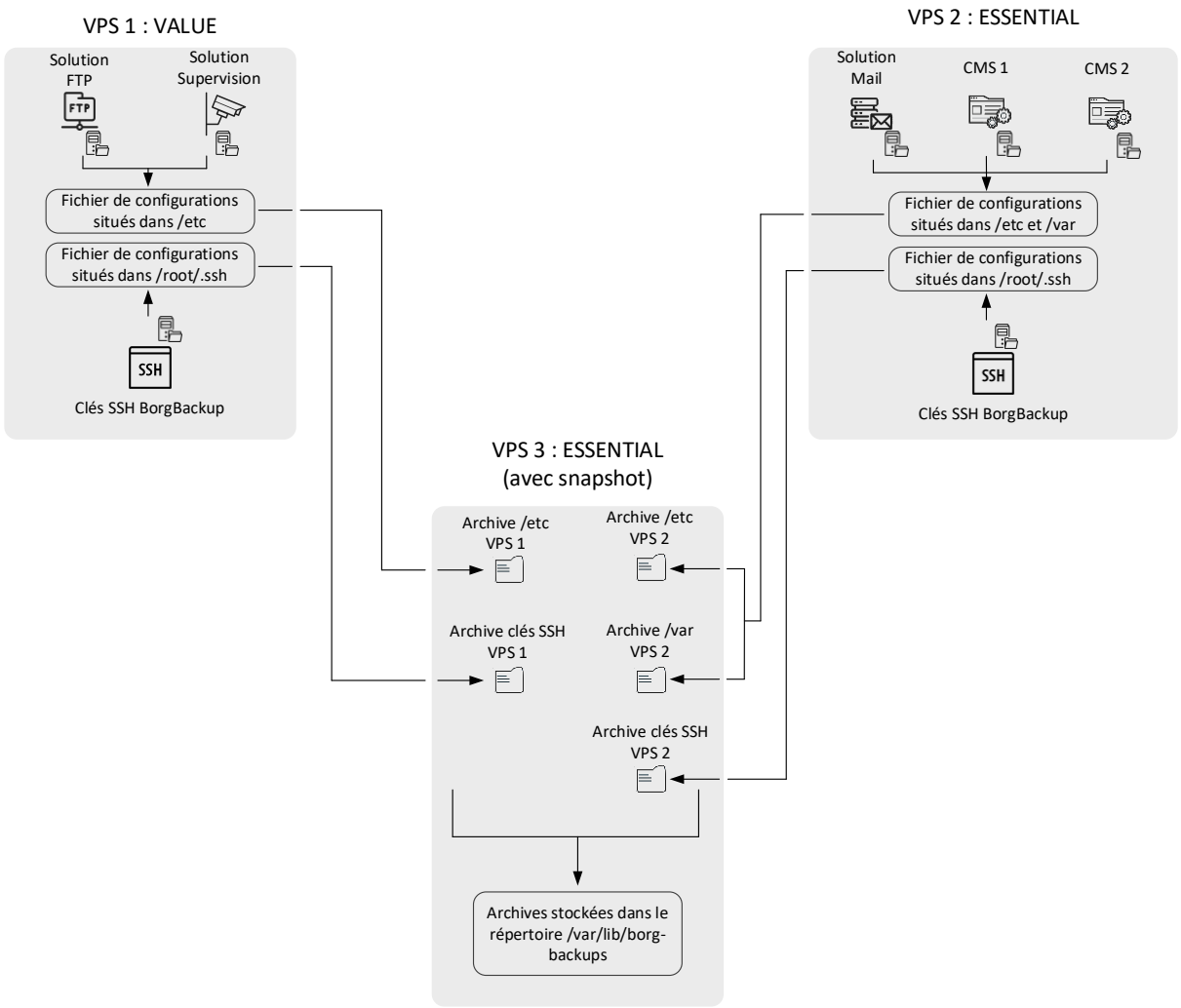
Nous avons choisi d'utiliser Borg Backup pour la sauvegarde des données pour les raisons suivantes :

- Comporte peut de dépendances
- La syntaxe des commandes sont simples d'utilisations
- Dispose de plusieurs moyens de sauvegardes (incrémentielle et différentielle)
- Compression des données sauvegardées, optimisant l'espace occupé sur le disque
- Les sauvegardes effectuées à distance sont sécurisées

De plus, les archives seront conservées de la manière suivante sur le VPS serveur :

- Conservation d'une archive par jour pour les sept derniers jours de la semaine en cours
- Conservation d'une archive par semaine pour les quatre dernières semaines
- Conservation d'une archive par mois pour les six derniers mois

Ci-dessous, vous trouverez un schéma présentant les répertoires sauvegardés des VPS clients :



VI. CMS/FTP

Concernant les CMS, nous avons décidé d'utiliser Apache2 car nous avons été formés sur cette technologie lors de notre formation.

Concernant le FTP nous avons décidé d'utiliser SFTP afin de sécuriser nos accès FTP.

VII. MAIL

1. Tableau comparatif

	Les solutions			
	zimbra	hMailServer	axigen	iRedMail Open Source Mail Server Solution
Les fonctionnalitées				
Linux/Unix	✓	✓	✓	✓
Windows	✗	✓	✓	✓
Mac OS X	✓	✓	✓	✓
SMTP	✓	✓	✓	✓
POP3	✓	✓	✓	✓
IMAP	✓	✓	✓	✓
SSL	✓	✓	✓	✓
Webmail	✗	✓	✓	✗
Base de données	✗	✓	✓	✓
Système de fichier	✓	✗	✗	✗
Anti-Spam	✓	✓	✓	✓
Anti-Virus	✓	✓	✓	✓
Liste noire, blanche et grise	✗	✗	✓	✓
Interface pour mobile	✓	✗	✓	✓
Nombre de compte	?	Illimités	Limité	Illimités
Sauvegarde	✓	✓	✓	✓
Licence	Open Source	Open Source	Propriétaire	Open Source

VIII. Plan de maintenance

		Plan de maintenance des solutions			Niveau 1 (critique) à 4 (peu critique)
		Préventive	Améliorative	Corrective	
Système	Debian 10.4.0	-Superviser -Mise à jour -Sauvegardes -Veille technologique	-Mise à jour semestriel -Mise à jour majeur (version stable uniquement) -Mise à jour des données	-Reconfigurer ou vérifier la configuration -Redéployer le snap shot, la sauvegarde, la configuration ou le système	1
Logiciels	SFTP	-Sauvegarde des fichiers de configurations -Sauvegardes des données -Veille technologique	-Réplication du service	-Reconfigurer -Remonter d'une sauvegarde -Redéployer le service	2
	Nagios	-Sauvegarde des fichiers de configurations -Sauvegardes des données -Analyse des journaux -Veille technologique	-Mise à jour majeur	-Reconfigurer -Remonter d'une sauvegarde -Redéployer le service	3
	IredMail	-Sauvegarde des fichiers de configurations -Sauvegardes des données -Analyse des journaux -Veille technologique	-Réplication du service -Mise à jour majeur	-Reconfigurer -Remonter d'une sauvegarde -Redéployer le service	1
	WordPress	-Sauvegarde des fichiers de configurations -Sauvegardes des données -Veille technologique	-Réplication du service -Mise à jour majeur	-Reconfigurer -Remonter d'une sauvegarde -Redéployer le service	2
	Drupal	-Sauvegarde des fichiers de configurations -Sauvegardes des données -Veille technologique	-Réplication du service -Mise à jour majeur	-Reconfigurer -Remonter d'une sauvegarde -Redéployer le service	2
	BorgBackup	-Analyse des journaux -Remonter des sauvegardes	-Mise à jour majeur	-Reconfiguration de la sauvegarde -Réinstaller le service	1
	FW	-Sauvegarde des fichiers de configurations -Sauvegardes des données -Analyses des journaux -Veille technologique	-Mise à jour majeur	-Reconfigurer -Remonter d'une sauvegarde -Redéployer le service	1
Réseau	/	-Mise en place de règles et de moyens de sécurités -Remonter d'alertes -Analyse du réseau	-Souscrire à une offre offrant plus d'avantages	-Contacter OVH	1
Suivi et maintenance	Incidents	-Rédaction de procédures -Tenir une base de connaissance -Graphiques avec des indicateurs	-Entretenir la base de connaissance -Mise en place d'une démarche d'amélioration continue	/	1
	Supervision	-S'assurer du bon fonctionnement de la solution de supervision	-Maintien de la disponibilité du service	/	2

IX. SUPERVISION

1. Comparatif

Comparatif des solutions de supervision :

	Zabbix	Grafana	Nagios Core	Nagios XI
	ZABBIX	Grafana	Nagios Core	Nagios XI
Prix	**Gratuit (Open Source)**	**Gratuit (Open Source)**	**Gratuit (Open Source)**	**1 153,07 €**
Facilité d'utilisation	3/5	3/5	3/5	5/5
Forte communauté	5/5	5/5	5/5	3/5
Puissance et modularité	3/5	2/5	3/5	5/5
Graphiques intégrés	1/5	5/5	0/5	5/5
Total	**12/20**	**15/20**	**11/20**	**18/20**

Nous avons décidé, d'après les critères que nous avons définis, que la solution de supervision la mieux adaptée est Nagios XI. Malgré son prix onéreux cette solution est très simple d'utilisation car tout peut-être gérer depuis l'interface graphique, en plus de cela nous avons à disposition plusieurs documentations ainsi que plusieurs vidéos fournis de la part de Nagios. Bien sûr Nagios XI est bien plus puissant que les autres outils de supervision ce qui fait de ce dernier une solution de choix pour nous.

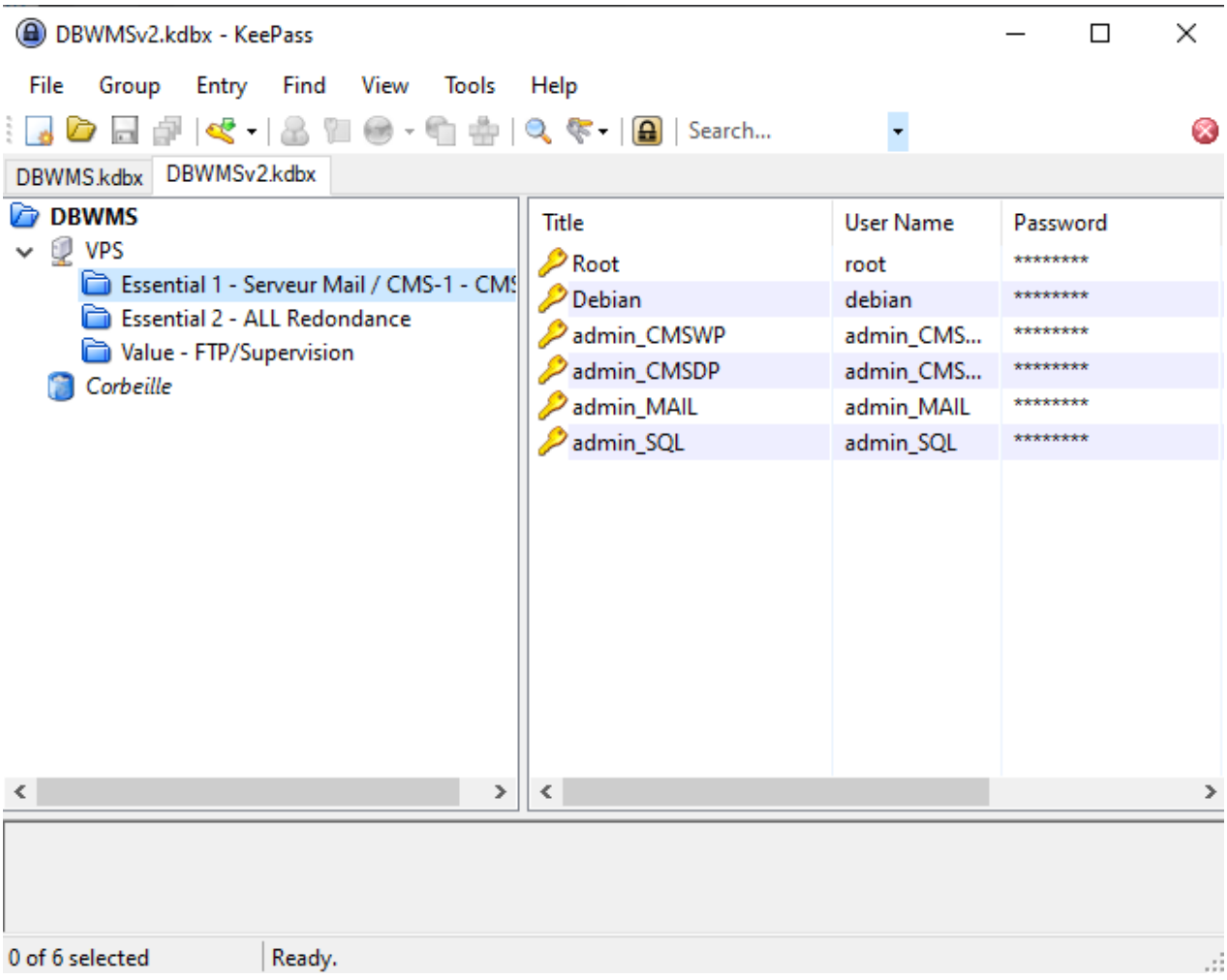
X. Annexe

1. Installation & paramétrage environnement

1.1. Sécurité

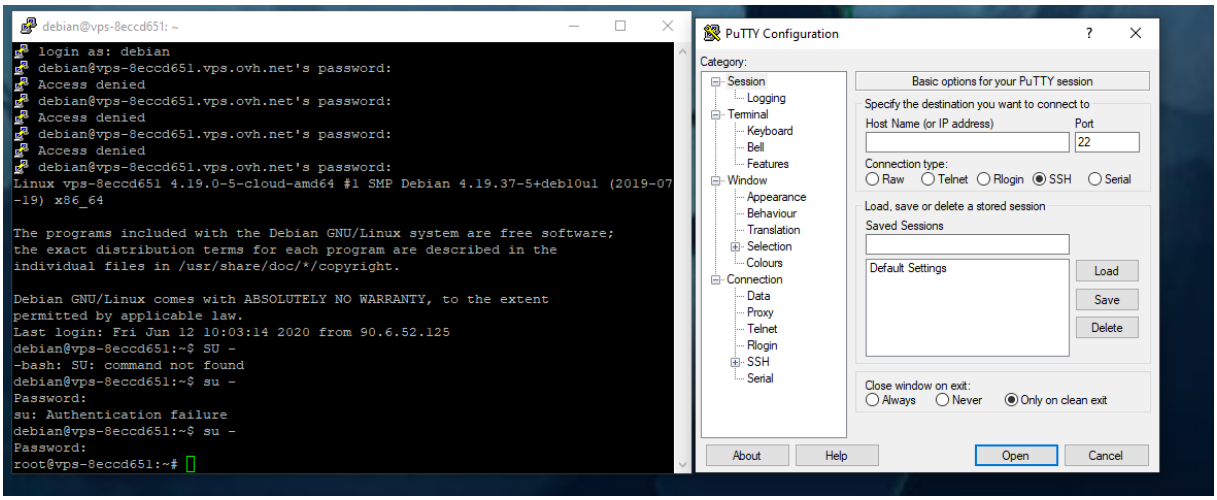
1.1.1. Gestionnaire de mot de passe

Afin d'augmenter la sécurité lors de notre projet, nous avons décidé de mettre en place une base Keepass afin d'enregistrer les différents Identifiants nécessaire :



1.1.2. Gestionnaire d'identification

Putty :



1.1.3. SSH

Changement du port SSH :

Port défini : 6345

Localisation du fichier de configuration qui contient la compilation SSH :

/etc/ssh/ssh_config

Dans ce fichier on doit changer la ligne correspondant au port de communication :

Ensuite il faut changer un deuxième fichier de configuration qui se situe :

/etc/ssh/sshd_config

```
root@vps-ccec9e0f:~# cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port 6345
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
```

```
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp  /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

PasswordAuthentication yes
```

Ensuite on redémarre le service SSHD pour qu'il recharge la configuration :

```
systemctl restart sshd.service
```

Poste Client :

On créer une clé SSH afin de pouvoir se connecter au server

```
ssh-keygen -t ed25519
```

```
timothee@macbook-pro-de-timothee ~ % ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/timothee/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/timothee/.ssh/id_ed25519.
Your public key has been saved in /Users/timothee/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:ozQ+clN9XH8c34GVbULR87p0Esnmbsd5mjrioGlrGI0 timothee@MacBook-Pro-de-Timothee.local
The key's randomart image is:
+--[ED25519 256]--+
|              .o+o|
|               +o+|
|              o.*o|
|          . . .=o*|
|     oo S . oo o*|
|    Eo.+ . .  = o|
|    .o* .    o =.|
|    .oo= .. . +o+|
|     o+. ....+oo.|
+----[SHA256]-----+
timothee@macbook-pro-de-timothee ~ %
```

Une fois que la clé est créée on la dépose sur le serveur afin qu'elle soit en corrélation avec notre client.

```
timothee@macbook-pro-de-timothee ~ % ssh-copy-id -i ~/.ssh/id_ed25519 debian@IP
```

Pour finir on désactive la connexion par mot de passe qui se situe dans le fichier de configuration SSHD. (De manière que seules les personnes ayant la clé puisse s'authentifier)

```
PasswordAuthentication no
```

1.1.4. Fail2ban

Pour utiliser Fail2ban nous devons en amont installé le paquet :

```
apt install fail2ban
```

Afin d'éviter des attaques sur nos ports de connexion, nous allons mettre en place Fail2ban sur chacun de nos serveurs :

1.1.5. Chemin du fichier de configuration

/etc/fail2ban/jail.local

1.1.6. Fichier de configuration

```
[root@vps-ccec9e0f:~# cat /etc/fail2ban/jail.local
[DEFAULT]
# time is in seconds. 3600 = 1 hour, 86400 = 24 hours (1 day)
ignoreip    = 127.0.0.1 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 51.75.79.200 51.75.64.79 51.75.73.103

[sshd] enabled = true
#Port
port = 6345

# 1 jour de ban
bantime = 86400

#Plage sur laquel le nombre d'échec est analyser avant le ban (en
#seconde)
findtime = 1800

#Nombre de tentative
maxretry = 3
```

Dans la partie Default on configure le nombre de tentative sur un certain laps de temps.

Dans ignoreip nous avons listé les différentes adresses IP de confiance.

Dans la partie SSHD on lui demande de superviser le service SSHD en lui indiquant le port de communication.

Ensuite on redémarre le service avec la commande suivante :

```
systemctl restart fail2ban.service
```

1.1.7. UFW

Pour utiliser le pare-feu UFW nous devons installer le paquet :

```
apt install ufw
```

Nous ajoutons les règles d'ouverture de port sur le serveur avec la commande :

```
ufw default allow
```

```
ufw enable
```

```
ufw allow 80/tcp
```

Ensuite nous configurons toutes les règles du pare-feu afin que tous les ports dont nous avons besoins soit ouvert :

- 443
- 5666
- 6345

Le fichier de configurations qui contient ces règles se trouve :

/etc/ufw/user.rules et …/user6.rules

Ensuite on redémarre le pare feu : `ufw disable && ufw enable`

1.1.8. Création des profils Debian d'administrateur

- **ID FTP :** admin_FTP
- **ID Supervision :** admin_SUPERVISION
- **ID Mail :** admin_MAIL
- **ID CMS1 :** admin_CMSWP
- **ID CMS2 :** admin_CMSDP
- **ID MariaDB:** admin_SQL

Chacun de ces différents profils auront des accès spécifiques pour chacun de leurs rôles.

```
root@vps-8eccd651:~# adduser admin_SUPERVISION --force-badname
Allowing use of questionable username.
Adding user `admin_SUPERVISION' ...
Adding new group `admin_SUPERVISION' (1002) ...
Adding new user `admin_SUPERVISION' (1002) with group `admin_SUPERVISION' ...
Creating home directory `/home/admin_SUPERVISION' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin_SUPERVISION
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Récapitulatif des comptes crées :

Serveur :	**vps-8eccd651.vps.ovh.net**			
Role	**FTP / SUPERVISION**			
Nom netbios :	**vps-8eccd651**			
Utilisateur :	admin_FTP	admin_SUPERVISION		
Role :	Compte admin FTP	Compte admin Supervision		
Serveur :	**vps-9c782e98.vps.ovh.net**			
Role	**MAIL1 / SERVEUR MAIL 2 / CMS 1 et 2**			
Nom netbios :	**vps-9c782e98**			
Utilisateur :	admin_MAIL	admin_CMSWP	admin_CMSDP	admin_SQL
Role :	Compte admin Serveur MAIL	Compte admin Wordpress	Compte admin DRUPAL	Compte admin SQL/MariaDB
Serveur :	**vps-ccec9e0f.vps.ovh.net**			
Role	**MAIL1 / SERVEUR MAIL 2 / CMS 1 et 2 / FTP / Save**			
Nom netbios :	**vps-ccec9e0f**			
Utilisateur :	admin_FTP	admin_CMSWP	admin_CMSDP	admin_MAIL
Role :	Compte admin FTP	Compte admin Wordpress	Compte admin DRUPAL	Compte admin Serveur MAIL

1.2. CMS/FTP

1.2.1. Installation CMS

Installation de l'environnement :

- Apache :
  $ apt install apache2
- MariaDB :
  $ apt install mariadb-server
  $ mysql_secure_installation
- PHP :
  $ apt install php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip
  $ systemctl restart apache2

Créer une database pour Wordpress

```
sudo mysql -u root -p
CREATE DATABASE bd_wordpress;
GRANT ALL PRIVILEGES on wordpress.* TO 'wordpress_user'@'localhost' IDENTIFIED
BY 'mdp_wordpress';
FLUSH PRIVILEGES;
EXIT;
```

5) Installation de WordPress

```
cd /tmp/
wget -c https://wordpress.org/latest.tar.gz
tar -xvzf latest.tar.gz
sudo mv wordpress/ /var/www/html
sudo chown -R www-data:www-data /var/www//html/wordpress/
```

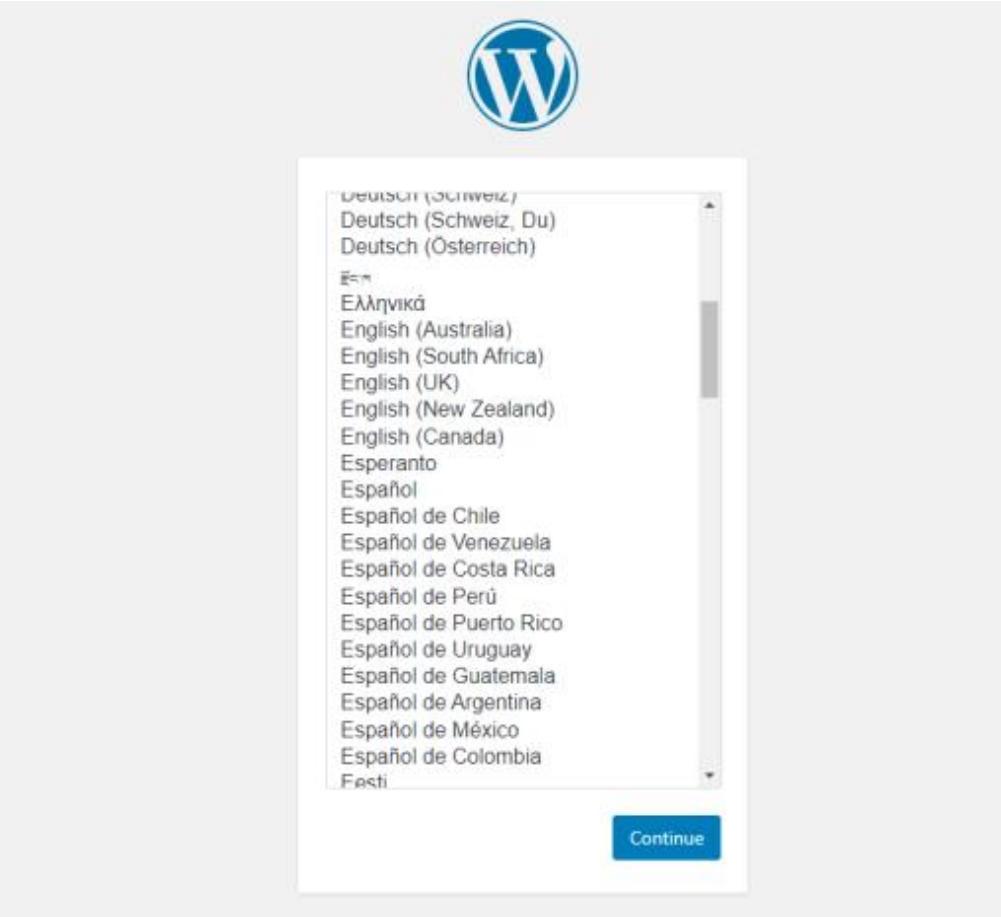
Créer un site pour Wordpress dans /etc/apache2/sites-available/catalogue.conf :

```
 GNU nano 3.2                                    catalogue.conf

<VirtualHost *:80>
    ServerAdmin postmaster@parcinfo.net
    ServerName catalogue.parcinfo.net
    ServerAlias www.catalogue.parcinfo.net
    DocumentRoot /var/www/wordpress
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Activer le site avec sudo a2ensite catalogue.conf

Autoriser Wordpress à réécrire les url avec la commande sudo a2enmod rewrite
Redémarrer Apache pour prendre tout ça en compte avec sudo service apache2 reload

Pour finaliser l'installation rendez-vous sur votre site-web http://votre_ip ou http://votre_nom_de_domaine et suivez les indications de WordPress



Install Drupal

apt -y install php php-{cli,mysql,json,opcache,xml,mbstring,gd,curl}

sudo a2enmod rewrite

systemctl restart apache2

cd /tmp

wget https://ftp.drupal.org/files/projects/drupal-8.9.1.tar.gz

tar xvf drupal-8.9.1.tar.gz

sudo mv drupal-8.9.1 /var/www/drupal

chown -R www-data:www-data /var/www/drupal

nano /etc/apache2/sites-available/drupal.conf

ln -s /etc/apache2/sites-available/drupal.conf /etc/apache2/sites-enabled/drupal.conf

systemctl restart apache2

```
<VirtualHost *:80>
    ServerAdmin postmaster@parcinfo.net
    ServerName commande.parcinfo.net
    ServerAlias www.commande.parcinfo.net
    DocumentRoot /var/www/drupal
  # Redirection 301  vers le site en HTTPS
    Redirect permanent / https://commande.parcinfo.net/

        <Directory /var/www/drupal>
                Options -Indexes +FollowSymLinks +MultiViews
                AllowOverride All
                Require all granted
        </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

1.2.2. HTTP vers HTTPS

1. Activation du module SSL/TLS

    a. **Activation du module SSL**
    sudo a2enmod ssl
    b. **Redémarrer la conf Apache**
    sudo systemctl reload apache2
    c. **Vérification de l'activation du module ssl**
    apache2ctl -M | grep ssl

2. Création du certificat avec Let'encrypt

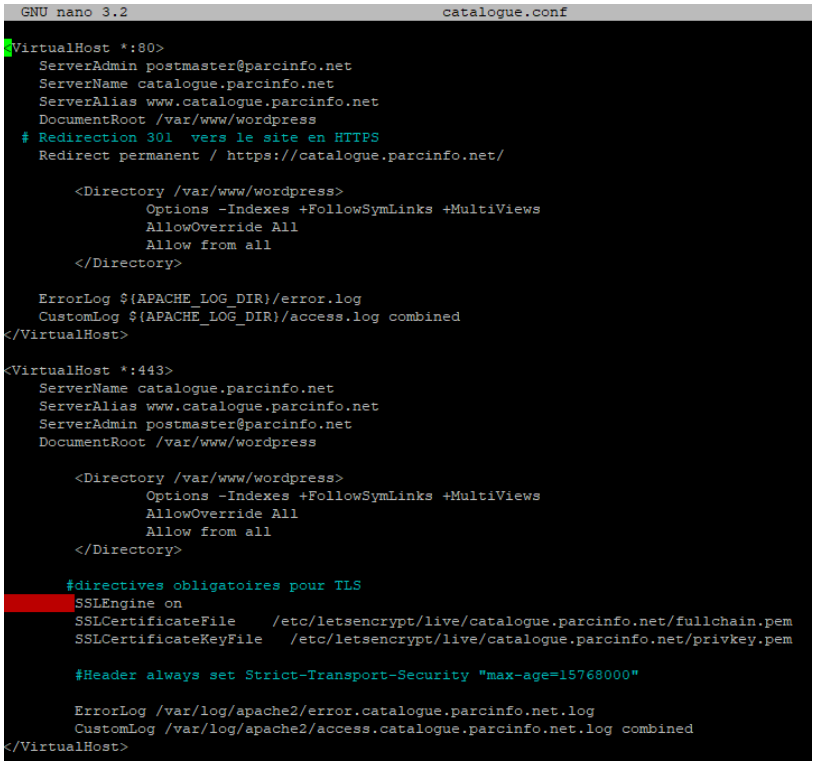
    a. **Instalation Certbot**
    sudo apt update
    sudo apt install software-properties-common
    sudo add-apt-repository ppa:certbot/certbot
    sudo apt update
    sudo apt install certbot
    b. **Générer le certificat**
    sudo certbot certonly --webroot -w /var/www/drupal -d commande.parcinfo.net -d www.commande.parcinfo.net

3. Configuration de l'hôte virtuel pour HTTPS

    a. **Ouvrir le fichier de conf du site dans /etc/apache2/sites-available/commande.conf**
    b. **Editer le fichier :**
        *<VirtualHost *:80>*

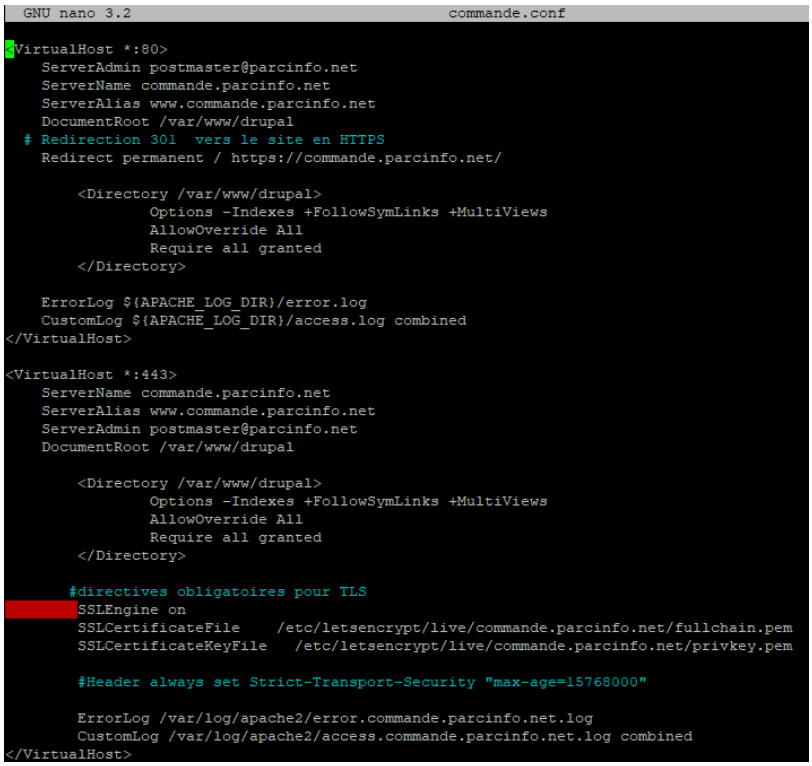
```
   ServerName commande.parcinfo.net
   ServerAlias www.commande.parcinfo.net
   ServerAdmin postmaster@parcinfo.net
   DocumentRoot /var/www/drupal
   # Redirection 301 vers le site en HTTPS
   Redirect permanent / https://commande.parcinfo.net/

        <Directory /var/www/drupal>
              Options -Indexes +FollowSymLinks +MultiViews
              AllowOverride All
              Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR} /error.log
        CustomLog ${APACHE_LOG_DIR} /access/log combined
</VirtualHost>

<VirtualHost *:443>
   ServerName commande.parcinfo.net
   ServerAlias www.commande.parcinfo.net
   ServerAdmin postmaster@parcinfo.net
   DocumentRoot /var/www/drupal

        <Directory /var/www/drupal>
              Options -Indexes +FollowSymLinks +MultiViews
              AllowOverride All
              Require all granted
        </Directory>

     # directives obligatoires pour TLS
        SSLEngine on
        SSLCertificateFile
        /etc/letsencrypt/live/commande.parcinfo.net/fullchain.pem
        SSLCertificateKeyFile   /etc/letsencrypt/live/
        commande.parcinfo.net /privkey.pem

        #Header always set Strict-Transport-Security "max-
age=15768000"

        ErrorLog /var/log/apache2/error.example.com.log
        CustomLog /var/log/apache2/access.example.com.log
combined
</VirtualHost>
```

Fichier de conf final de Wordpress dans /etc/apache2/sites-available :



```
 GNU nano 3.2                                    catalogue.conf

<VirtualHost *:80>
    ServerAdmin postmaster@parcinfo.net
    ServerName catalogue.parcinfo.net
    ServerAlias www.catalogue.parcinfo.net
    DocumentRoot /var/www/wordpress
  # Redirection 301  vers le site en HTTPS
    Redirect permanent / https://catalogue.parcinfo.net/

        <Directory /var/www/wordpress>
                Options -Indexes +FollowSymLinks +MultiViews
                AllowOverride All
                Allow from all
        </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerName catalogue.parcinfo.net
    ServerAlias www.catalogue.parcinfo.net
    ServerAdmin postmaster@parcinfo.net
    DocumentRoot /var/www/wordpress

        <Directory /var/www/wordpress>
                Options -Indexes +FollowSymLinks +MultiViews
                AllowOverride All
                Allow from all
        </Directory>

       #directives obligatoires pour TLS
        SSLEngine on
        SSLCertificateFile    /etc/letsencrypt/live/catalogue.parcinfo.net/fullchain.pem
        SSLCertificateKeyFile   /etc/letsencrypt/live/catalogue.parcinfo.net/privkey.pem

        #Header always set Strict-Transport-Security "max-age=15768000"

        ErrorLog /var/log/apache2/error.catalogue.parcinfo.net.log
        CustomLog /var/log/apache2/access.catalogue.parcinfo.net.log combined
</VirtualHost>
```

Fichier de conf final de Drupal dans /etc/apache2/sites-available :



```
 GNU nano 3.2                                    commande.conf

<VirtualHost *:80>
    ServerAdmin postmaster@parcinfo.net
    ServerName commande.parcinfo.net
    ServerAlias www.commande.parcinfo.net
    DocumentRoot /var/www/drupal
  # Redirection 301  vers le site en HTTPS
    Redirect permanent / https://commande.parcinfo.net/

        <Directory /var/www/drupal>
                Options -Indexes +FollowSymLinks +MultiViews
                AllowOverride All
                Require all granted
        </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerName commande.parcinfo.net
    ServerAlias www.commande.parcinfo.net
    ServerAdmin postmaster@parcinfo.net
    DocumentRoot /var/www/drupal

        <Directory /var/www/drupal>
                Options -Indexes +FollowSymLinks +MultiViews
                AllowOverride All
                Require all granted
        </Directory>

       #directives obligatoires pour TLS
        SSLEngine on
        SSLCertificateFile    /etc/letsencrypt/live/commande.parcinfo.net/fullchain.pem
        SSLCertificateKeyFile   /etc/letsencrypt/live/commande.parcinfo.net/privkey.pem

        #Header always set Strict-Transport-Security "max-age=15768000"

        ErrorLog /var/log/apache2/error.commande.parcinfo.net.log
        CustomLog /var/log/apache2/access.commande.parcinfo.net.log combined
</VirtualHost>
```

1.3. MAIL

1.3.1. Procédure d'installation iRedMail

Prérequis :

Les exigences de base pour installer iRedMail sur Debian 10 Linux sont les suivantes :

- Utiliser l'installation de Debian 10 Linux
- 2 Go de mémoire son requis pour un serveur à faible trafic.
- Avoir un nom de domaine du serveur de messagerie
- Posséder un compte utilisateur « sudo »

Étape 1 : Mise à jour du système

Assurez-vous que votre système exécute la dernière version du système d'exploitation.

```
sudo apt -y update
sudo apt -y upgrade
```

Après une mise à niveau du système, nous vous recommandons de redémarrer.

```
sudo systemctl reboot
```

Étape 2 : Définir le nom d'hôte du serveur :

En premier temps, nous avons défini le nom d'hôte du serveur sur un nom de sous-domaine configuré dans notre serveur DNS

```
export HOSTNAME="mail.parcinfo.net"
```

```
sudo hostnamectl set-hostname $HOSTNAME --static
```

```
sudo hostnamectl set-hostname $HOSTNAME --transient
```

Après avoir mis à jour notre nom d'hôte, nous avons redémarrer la machine pour mettre à jour notre environnement de travail.

```
logout
```

Maintenant, on ajoute l'adresse IP et le mappage du nom DNS au fichier / etc / hosts.

```
nano /etc/hosts
```

Pour confirmer la résolutions DNS, on installe d'abord le package dns-utils.

```
sudo apt -y install dnsutils
```

On utilise la commande hôte pour la résolution locale.

```
host mail.parcinfo.net
```

Étape 3 : Téléchargez la dernière version d'iRedMail :

Visitez la page de téléchargement d'iRedMail pour obtenir la dernière version stable d'iRedMail pour votre plate-forme.

Il faut ensuite qu'on utilise la commande wget pour télécharger le fichier d'installation de iRedMail

```
root@vps-9c782e98:/var/www/html/mail# wget https://github.com/iredmail/iRedMail/releases/download/1.2.1/iRedMail-1.2.1.tar.gz
```

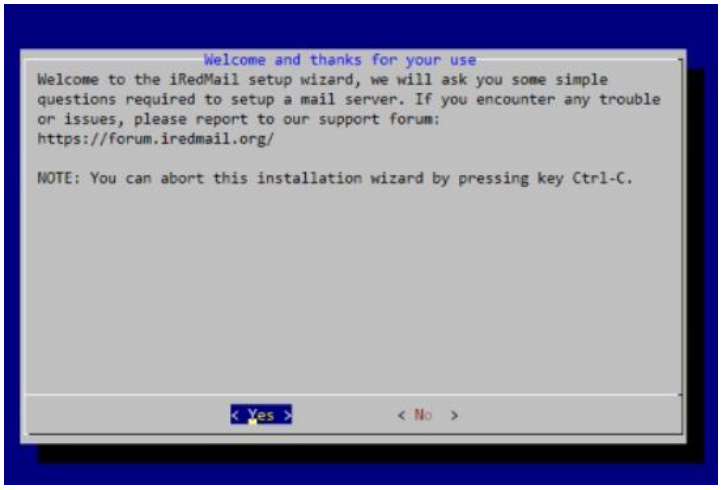
On extrait le fichier d'archive téléchargé.

```
root@vps-9c782e98:/var/www/html/mail# tar zxf iRedMail-1.2.1.tar.gz
```

Étape 4 : Installer iRedMail sur Debian 10 :

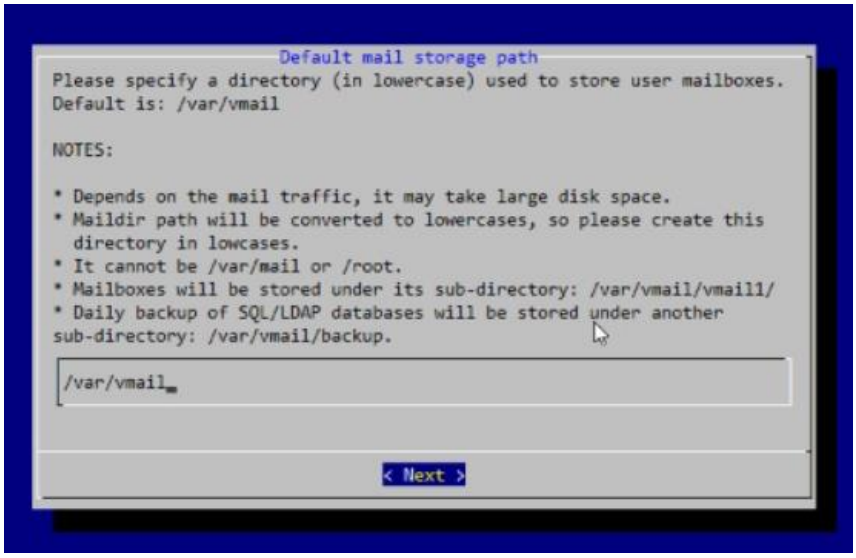
Accepter l'assistant d'installation :

Le premier écran nous demande d'accepter ou de refuser l'installation d'iRedMail sur Debian.



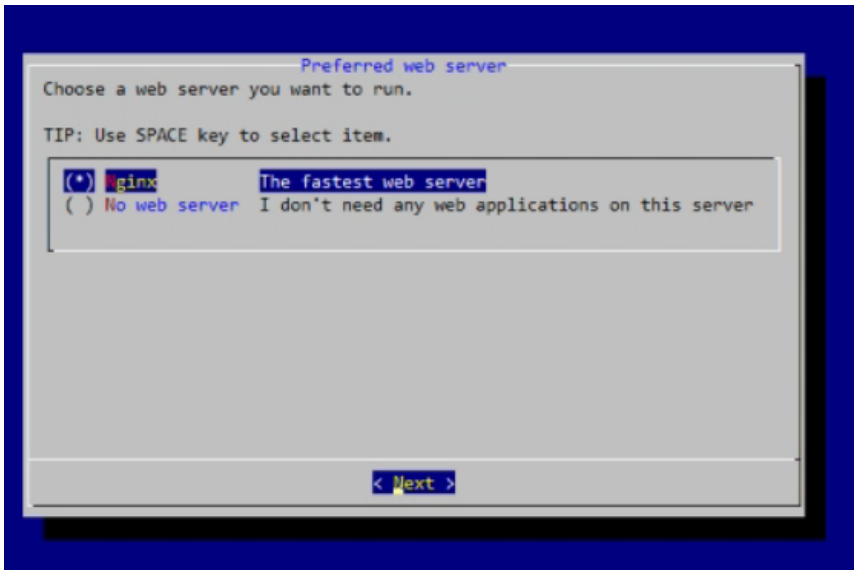
2 - Spécifiez le répertoire utilisé pour stocker les boîtes aux lettres :

Ici, cette étape indique le répertoire de stockage des boites aux lettres par défaut, on peut le modifier si on le souhaite.



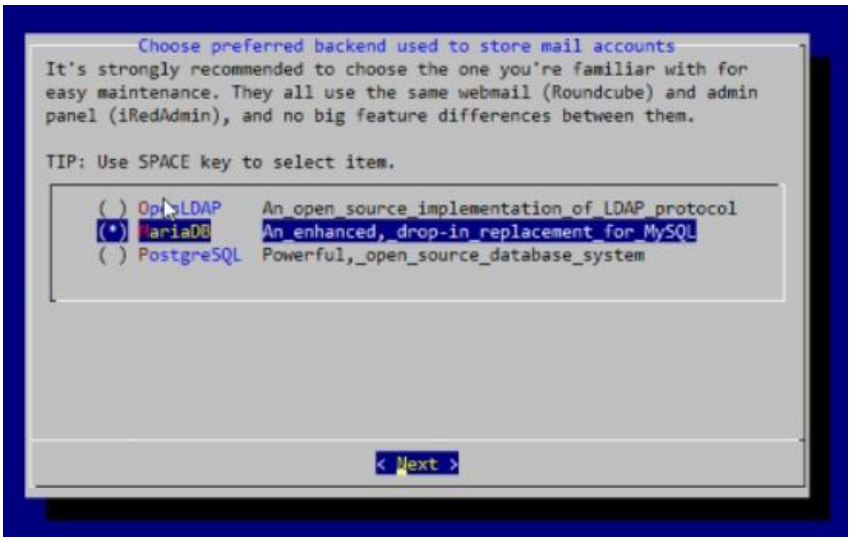
3 - Choisissez le serveur Web à utiliser :

Il faut que l'on sélectionne Nginx en tant que Serveur Web

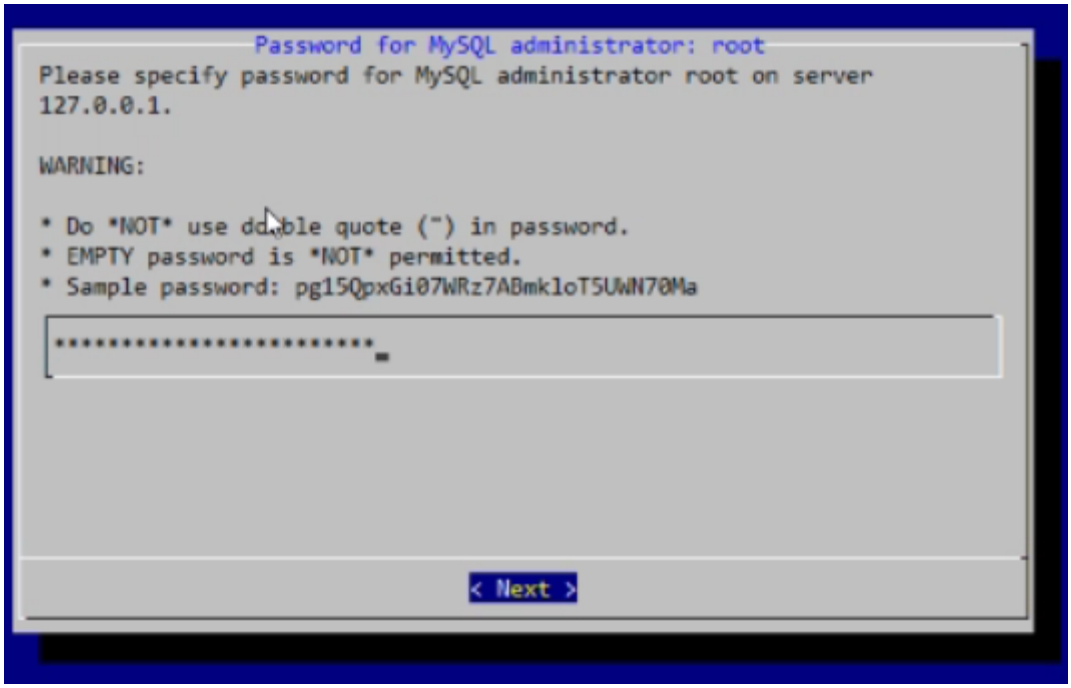


4 - Choisissez le backend utilisé pour stocker le compte de messagerie :

Pour stocker le compte de messagerie, nous avons décidé d'installer MariaDB



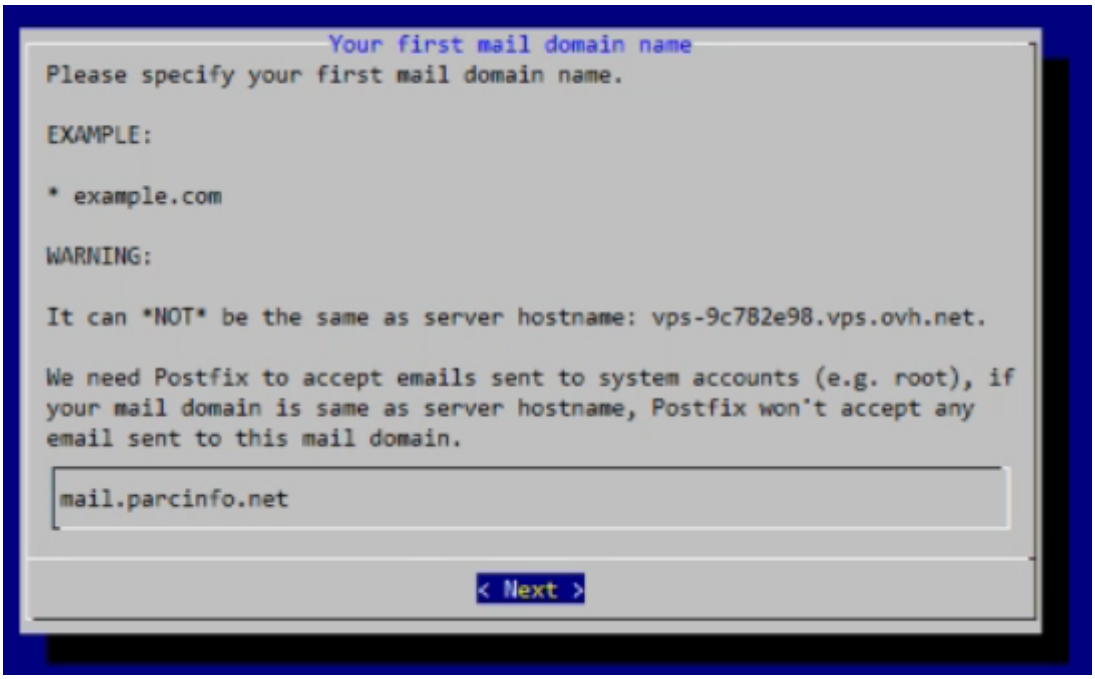
5 - Définir le mot de passe racine MySQL :



On doit indiquer le mot de passe de l'utilisateur root MySQL.

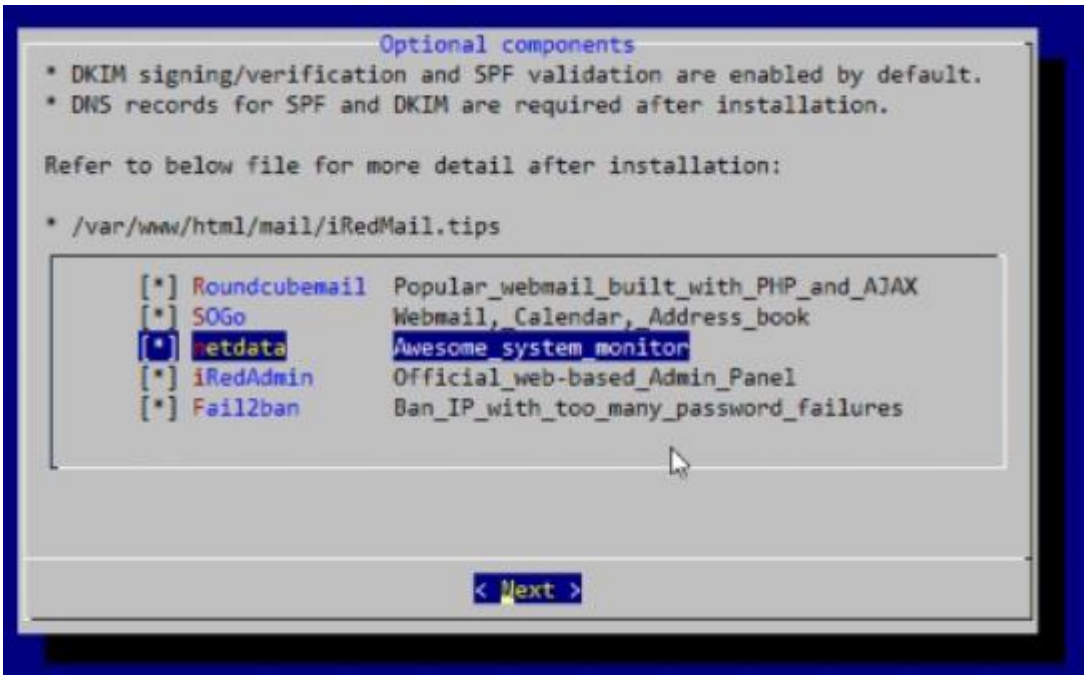
7 - Ajoutez votre premier nom de domaine de messagerie :

On rentre notre nom de domaine de messagerie

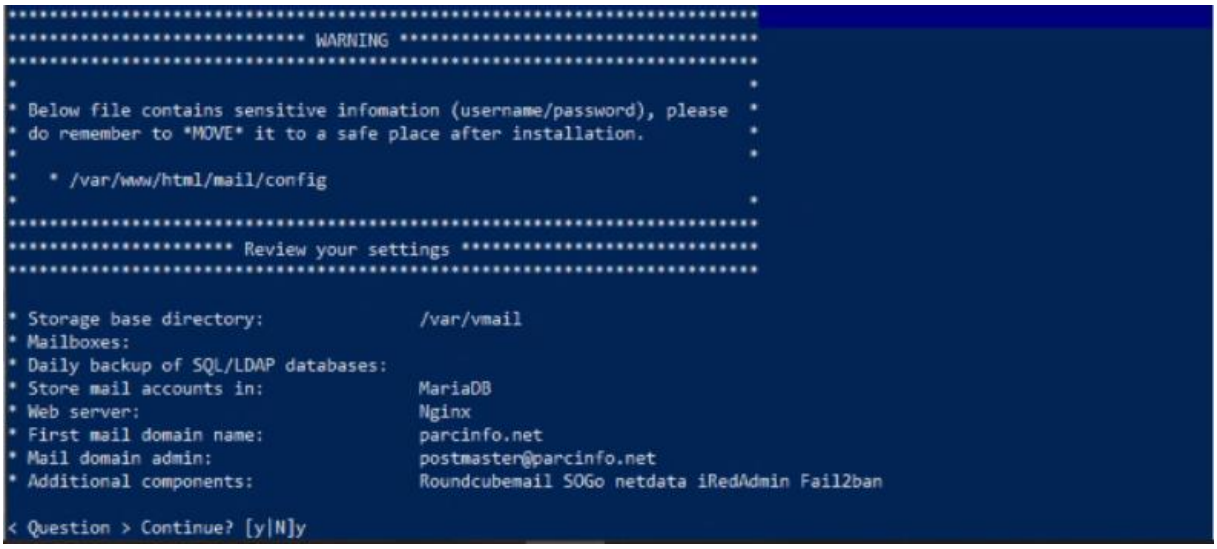


8 - Fournir un mot de passe à l'administrateur du domaine de messagerie :

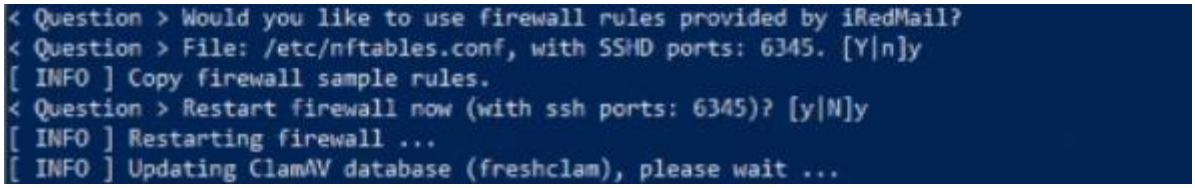
Ici on doit rentrer le mot de passe de l'administrateur du domaine de messagerie et cocher les fonctionnalités à activer.



Ici, nous avons une dernière vérification avant de lancer l'installation.



Il faut sélectionner y ou Y et appuyez sur Entrée pour démarrer l'installation.



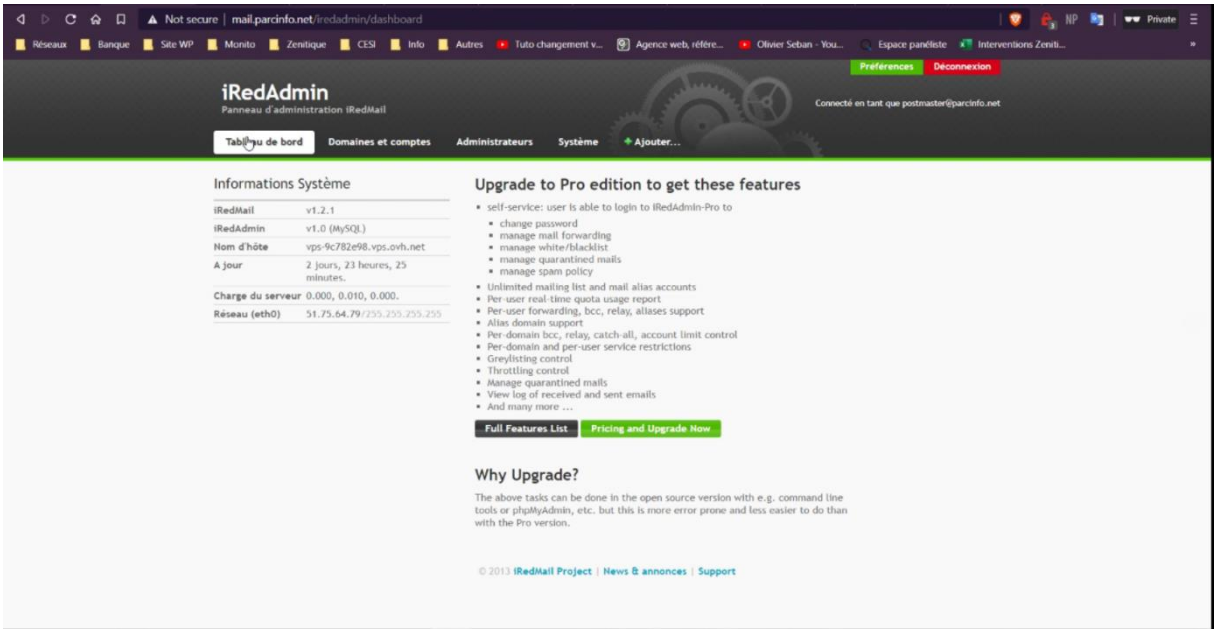
On redémarre notre serveur pour activer les services de messagerie.

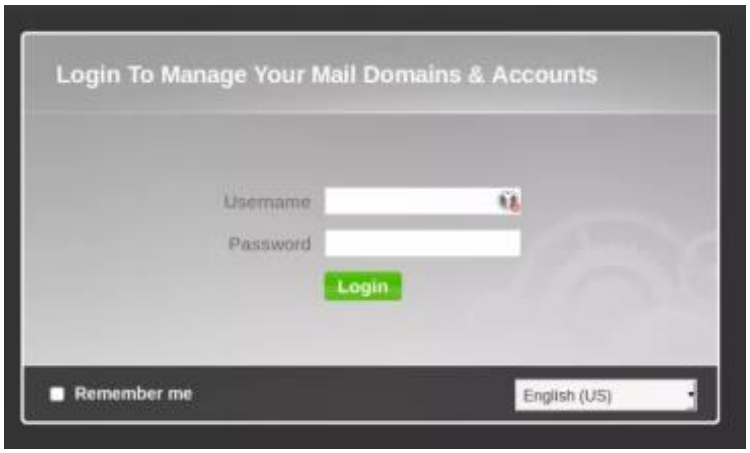
```
reboot
```

À la fin de l'installation, nous avons un récapitulatif de l'ensemble des composants installé :

```
*************************************************************************
* Start iRedMail Configurations
*************************************************************************
[ INFO ] Generate self-signed SSL cert (4096 bits, expire in 10 years).
[ INFO ] Generate Diffie Hellman Group with openssl, please wait.
[ INFO ] Create required system accounts.
[ INFO ] Configure Nginx web server.
[ INFO ] Configure PHP.
[ INFO ] Configure MariaDB database server.
[ INFO ] Setup daily cron job to backup SQL databases with /var/vmail/backup/backup_mysql.sh
[ INFO ] Configure Postfix (MTA).
[ INFO ] Configure Dovecot (POP3/IMAP/Managesieve/LMTP/LDA).
[ INFO ] Configure mlmmj (mailing list manager).
[ INFO ] Configure ClamAV (anti-virus toolkit).
[ INFO ] Configure Amavisd-new (interface between MTA and content checkers).
[ INFO ] Configure SpamAssassin (content-based spam filter).
[ INFO ] Configure iRedAPD (postfix policy daemon).
[ INFO ] Configure iRedAdmin (official web-based admin panel).
[ INFO ] Configure Roundcube webmail.
[ INFO ] Configure SOGo Groupware (Webmail, Calendar, Address Book, ActiveSync).
[ INFO ] Configure Fail2ban (authentication failure monitor).
[ INFO ] Configure netdata (system and application monitor).

*************************************************************************
* iRedMail-1.2.1 installation and configuration complete.
*************************************************************************
```

Il faut qu'on se connecte ici pour accéder aux portails avec les informations d'identification enregistrées.





Voici l'apparence par défaut du tableau de bord Admin iRedMail lors de la connexion initiale.

Ici il faut rentrer notre nom d'utilisateur et notre mot de passe

9 - Sécurisation d'iRedMail avec les certificats SSL

Obtention du certificat de chiffrement

On installe l'outil « certbot » afin d'obtenir un certificat SSL Let's Encrypt.

```
root@vps-ccec9e0f:~# wget https://dl.eff.org/certbot-auto
--2020-07-05 15:02:58--  https://dl.eff.org/certbot-auto
Resolving dl.eff.org (dl.eff.org)... 151.101.112.201, 2a04:4e42:1b::201
Connecting to dl.eff.org (dl.eff.org)|151.101.112.201|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 79897 (78K) [application/octet-stream]
Saving to: 'certbot-auto'

certbot-auto                100%[=========================================>]  78.02K  --.-KB/s    in 0.004s

2020-07-05 15:02:59 (19.8 MB/s) - 'certbot-auto' saved [79897/79897]

root@vps-ccec9e0f:~# chmod +x certbot-auto
root@vps-ccec9e0f:~# mv certbot-auto /usr/local/bin/certbot-auto
```

Après avoir installé l'outil « certbot-auto », on doit enregistrez l'adresse e-mail et le domaine pour le serveur iRedMail.

```
root@vps-ccec9e0f:/usr/local/bin# DOMAIN="mail.parcinfo.net"
root@vps-ccec9e0f:/usr/local/bin# EMAIL="postmaster@parcinfo.net"
```

On doit stopper le service Nginx.

```
root@vps-ccec9e0f:/usr/local/bin# systemctl stop nginx
```

Ici, avec cette commande, on obtient un certificat gratuit « Let's Encrypt » pour notre serveur de messagerie.

```
root@vps-ccec9e0f:/usr/local/bin# sudo /usr/local/bin/certbot-auto certonly --standalone -d $DOMAIN --preferred-chall
enges http --agree-tos -n -m $EMAIL --keep-until-expiring
```

1.4. Supervision

1.4.1. Installation des composantes

Web :

```
root@vps-8eccd651:~# apt-get install apache2 php php-gd php-imap php-curl
```

Librairie Pearl :

```
root@vps-8eccd651:~# apt-get install libxml-libxml-perl libnet-snmp-perl libperl-dev libnumber-format-perl libconfig-inifiles-perl libdatetime-perl libnet-dns-perl
```

Librairie Graphique :

```
root@vps-8eccd651:~# apt-get install libpng-dev libjpeg-dev libgd-dev
```

Compression :

```
apt-get install gcc make autoconf libc6 unzip
```

Ajout de l'utilisateur admin_SUPERVISION & www-data dans le groupe nagcmd (Groupe d'administration nagios)

```
root@vps-8eccd651:~# groupadd nagcmd
root@vps-8eccd651:~# usermod -a -G nagcmd admin_SUPERVISION
root@vps-8eccd651:~# usermod -a -G nagcmd www-data
```

Création d'un répertoire de téléchargement :

```
root@vps-8eccd651:~# groupadd nagcmd
root@vps-8eccd651:~# usermod -a -G nagcmd admin_SUPERVISION
root@vps-8eccd651:~# usermod -a -G nagcmd www-data
```

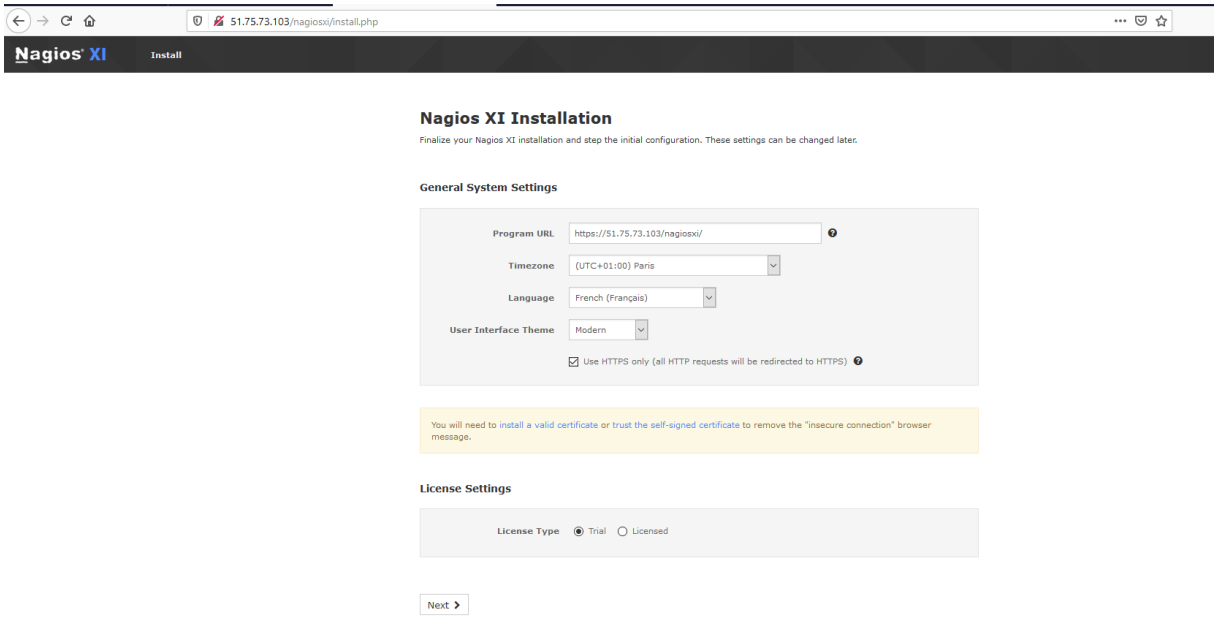
Téléchargement des sources :

```
root@vps-8eccd651:~# cd /home/nagios/downloads
root@vps-8eccd651:/home/nagios/downloads# wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
```

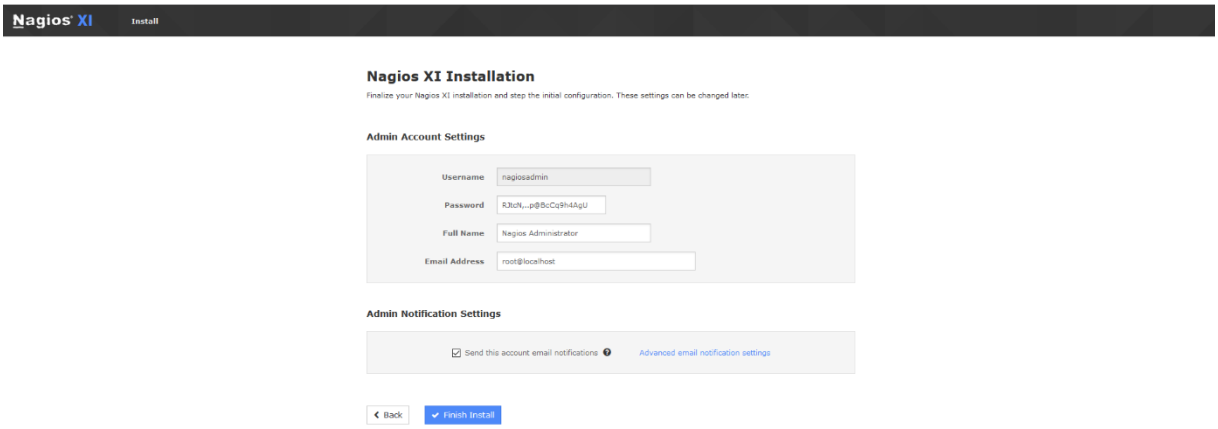
Lancement de l'installation :

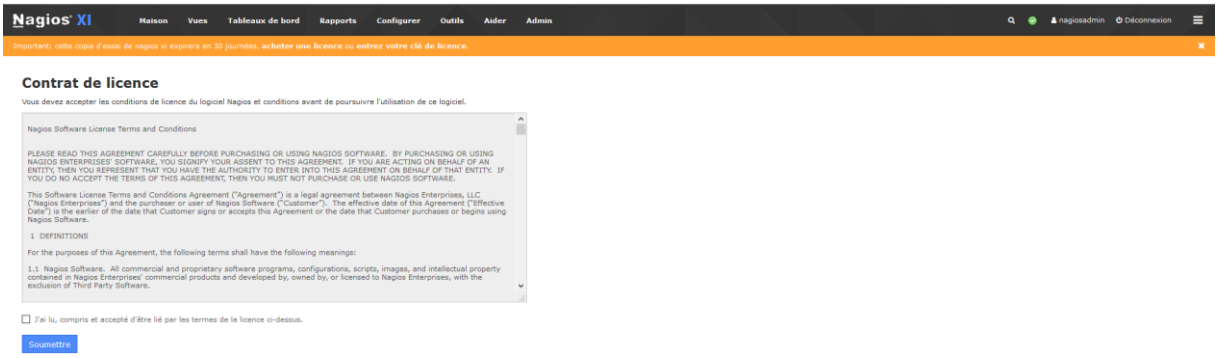
```
cd /tmp
wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
tar xzf xi-latest.tar.gz
cd nagiosxi
./fullinstall
```

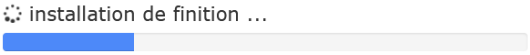
Installation graphique de nagios XI :



Création du compte admin :




Nagios XI
Maison
Vues
Tableaux de bord
Rapports
Configurer
Outils
Aider
Admin
nagiosadmin
Déconnexion
Contrat de licence
Vous devez accepter les conditions de licence du logiciel Nagios et conditions avant de poursuivre l'utilisation de ce logiciel.
Nagios Software License Terms and Conditions
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PURCHASING OR USING NAGIOS SOFTWARE. BY PURCHASING OR USING NAGIOS ENTERPRISES' SOFTWARE, YOU SIGNIFY YOUR ASSENT TO THIS AGREEMENT. IF YOU ARE ACTING ON BEHALF OF AN ENTITY, THEN YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THAT ENTITY. IF YOU DO NO ACCEPT THE TERMS OF THIS AGREEMENT, THEN YOU MUST NOT PURCHASE OR USE NAGIOS SOFTWARE.
This Software License Terms and Conditions Agreement ("Agreement") is a legal agreement between Nagios Enterprises, LLC ("Nagios Enterprises") and the purchaser or user of Nagios Software ("Customer"). The effective date of this Agreement ("Effective Date") is the earlier of the date that Customer signs or accepts this Agreement or the date that Customer purchases or begins using Nagios Software.
1 DEFINITIONS
For the purposes of this Agreement, the following terms shall have the following meanings:
1.1 Nagios Software. All commercial and proprietary software programs, configurations, scripts, images, and intellectual property contained in Nagios Enterprises' commercial products and developed by, owned by, or licensed to Nagios Enterprises, with the exclusion of Third Party Software.
J'ai lu, compris et accepté d'être lié par les termes de la licence ci-dessus.
Soumettre


installation de finition ...

Installation de l'agent NRPE sur le serveur Debian de supervision

Déplacement dans le répertoire temporaire pour télécharger l'agent NRPE :

```
root@vps-ccec9e0f:/home/debian/.ssh# cd /tmp
root@vps-ccec9e0f:/tmp# wget https://assets.nagios.com/downloads/nagiosxi/agents/linux-nrpe-agent.tar.gz
--2020-06-25 07:19:36--  https://assets.nagios.com/downloads/nagiosxi/agents/linux-nrpe-agent.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 72.14.181.71, 2600:3c00::f03c:91ff:fedf:b821
Connecting to assets.nagios.com (assets.nagios.com)|72.14.181.71|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3588623 (3.4M) [application/x-gzip]
Saving to: 'linux-nrpe-agent.tar.gz'

linux-nrpe-agent.tar.gz       100%[=============================================>]   3.42M  4.02MB/s    in 0.9s

2020-06-25 07:19:37 (4.02 MB/s) - 'linux-nrpe-agent.tar.gz' saved [3588623/3588623]

root@vps-ccec9e0f:/tmp# tar xzf linux-nrpe-agent.tar.gz
```

Décompression du dossier tar et installation de l'agent :

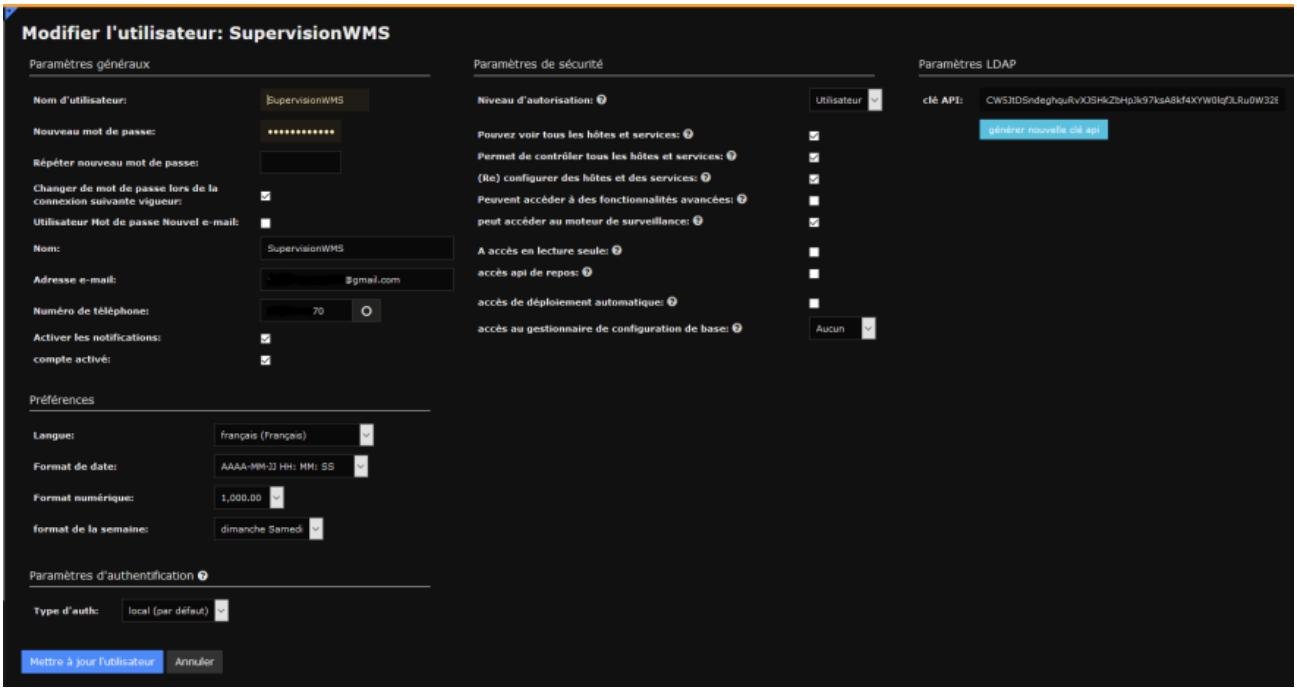
```
root@vps-ccec9e0f:/tmp/linux-nrpe-agent# ls
0-repos    2-usergroups  4-firewall       CHANGES.txt  get-os-info  nagios.firewallapps  subcomponents  xivar
1-prereqs  3-services    A-subcomponents  fullinstall  init.sh      packages             xi-sys.cfg
root@vps-ccec9e0f:/tmp/linux-nrpe-agent# ./fullinstall
============================
Nagios Linux Agent Installer
============================

This script will install the Nagios Linux Agent by executing all necessary
sub-scripts.

IMPORTANT: This script should only be used on a clean installed system:

    RedHat Enterprise, CentOS, Fedora, Cloud Linux or Oracle
    OpenSUSE or SUSE Enterprise
    Ubuntu or Debian

Do NOT use this on a system running any other distro or that
does not allow additional package installation.

Do you want to continue? [Y/n]
```

L'agent est bien installé sur la machine. Il ne reste plus qu'à renseigner les différentes informations nécessaires :

```
################################################################################
###                                                                          ###
### NRPE is currently set to allow connections only from these IP addresses: ###
###                                                                          ###
### 127.0.0.1                                                                ###
### ::1                                                                      ###
###                                                                          ###
### If you would like to change this list, enter all IP addresses to allow,  ###
### separated by SPACES only, and then press Enter.                    ###
### (Put the address(es) of your Nagios XI servers(s) here.)                 ###
###                                                                          ###
################################################################################

Allow from:
```

Création d'un profil

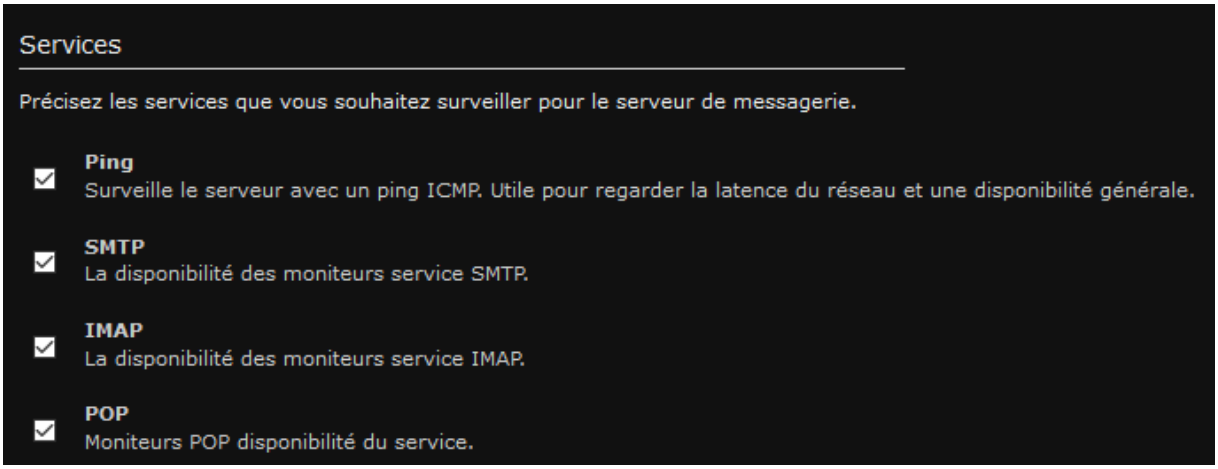
Création d'un profil pour recevoir les alertes de la supervision en cas d'évènement imprévu :



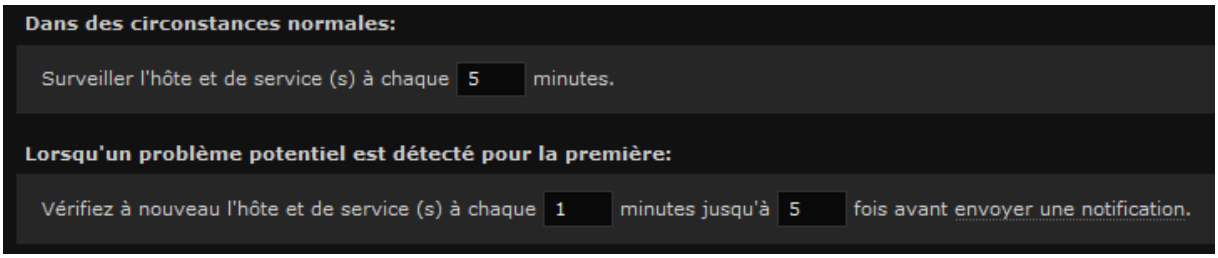
Ajout du serveur mail.parcinfo.net sur Nagios

Configuration du serveur iRedMail qui a pour adresse IP 95.216.98.16 et ajout du nom d'hôte :

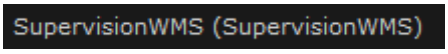
Sélection des services à surveiller :



Réglage des vérifications du bon fonctionnement des services ainsi que des délais de vérifications en cas de problème :

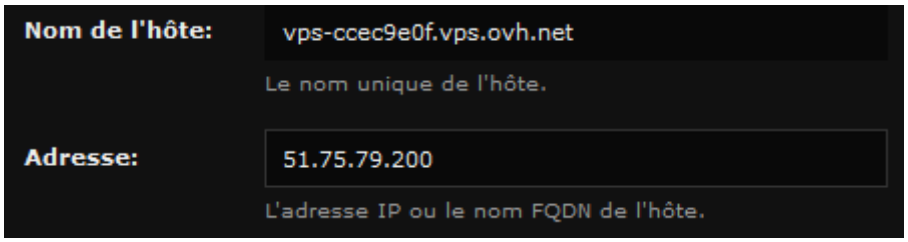


Configuration des contacts en cas l'alerte mail (contact des administrateurs Nagios) :

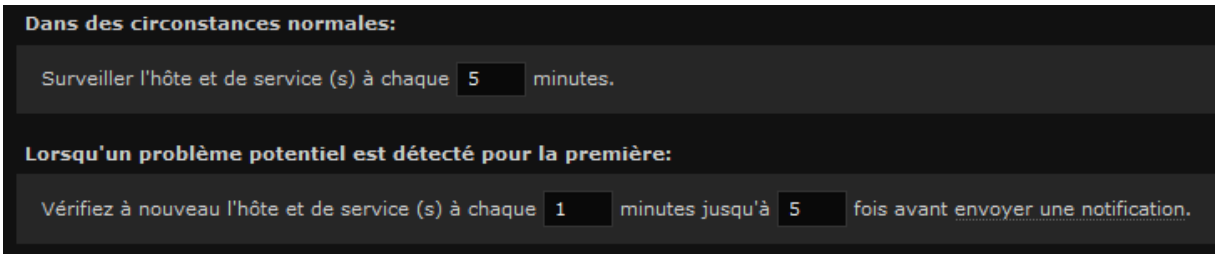


Ajout du serveur de backup sur la supervision.

Ajout du nom d'hôte ainsi que de son adresse IP :

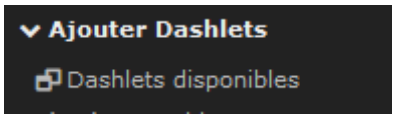


Configuration des délais de vérification du bon fonctionnement des services ainsi que des délais de vérifications en cas de problème :

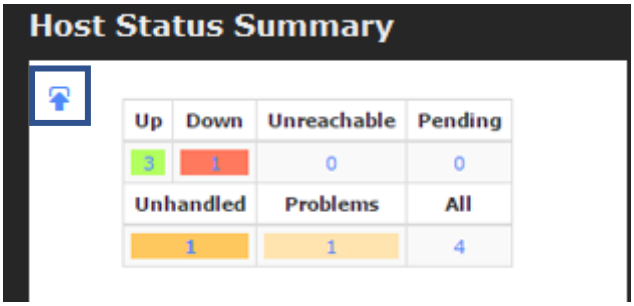


Personnalisation de l'interface

Il ne reste plus qu'à personnaliser le tableau de bord pour choisir les informations à afficher. Pour cela il suffit d'ajouter les dashlets et d'en sélectionner parmi les disponibles :



Une fois le dashlets trouvé il ne reste plus qu'à l'ajouter au tableau de bord :



1.5. Sauvegarde

1.5.1. Installation BorgBackup

Pour installer Borg Backup, taper la commande « apt install borgbackup » :

```
root@debian-value:~# apt install borgbackup
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  fuse libb2-1 libgomp1 python3-llfuse python3-msgpack
Paquets suggérés :
  borgbackup-doc python-llfuse-doc
Les NOUVEAUX paquets suivants seront installés :
  borgbackup fuse libb2-1 libgomp1 python3-llfuse python3-msgpack
0 mis à jour, 6 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 1□140 ko dans les archives.
Après cette opération, 4□250 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian buster/main amd64 fuse amd64 2.9.9-
1+deb10u1 [72,3 kB]
Réception de :2 http://deb.debian.org/debian buster/main amd64 python3-llfuse am
d64 1.3.6+dfsg-1 [194 kB]
Réception de :3 http://deb.debian.org/debian buster/main amd64 python3-msgpack a
md64 0.5.6-1+b1 [104 kB]
Réception de :4 http://deb.debian.org/debian buster/main amd64 libgomp1 amd64 8.
3.0-6 [75,8 kB]
Réception de :5 http://deb.debian.org/debian buster/main amd64 libb2-1 amd64 0.9
8.1-1 [40,8 kB]
Réception de :6 http://deb.debian.org/debian buster/main amd64 borgbackup amd64
1.1.9-2 [653 kB]
1□140 ko réceptionnés en 1s (1□462 ko/s)
Sélection du paquet fuse précédemment désélectionné.
(Lecture de la base de données... 39087 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../0-fuse_2.9.9-1+deb10u1_amd64.deb ...
Dépaquetage de fuse (2.9.9-1+deb10u1) ...
Sélection du paquet python3-llfuse précédemment désélectionné.
Préparation du dépaquetage de .../1-python3-llfuse_1.3.6+dfsg-1_amd64.deb ...
Dépaquetage de python3-llfuse (1.3.6+dfsg-1) ...
Sélection du paquet python3-msgpack précédemment désélectionné.
Préparation du dépaquetage de .../2-python3-msgpack_0.5.6-1+b1_amd64.deb ...
Dépaquetage de python3-msgpack (0.5.6-1+b1) ...
Sélection du paquet libgomp1:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../3-libgomp1_8.3.0-6_amd64.deb ...
Dépaquetage de libgomp1:amd64 (8.3.0-6) ...
Sélection du paquet libb2-1 précédemment désélectionné.
Préparation du dépaquetage de .../4-libb2-1_0.98.1-1_amd64.deb ...
Dépaquetage de libb2-1 (0.98.1-1) ...
Sélection du paquet borgbackup précédemment désélectionné.
Préparation du dépaquetage de .../5-borgbackup_1.1.9-2_amd64.deb ...
Dépaquetage de borgbackup (1.1.9-2) ...
Paramétrage de fuse (2.9.9-1+deb10u1) ...
update-initramfs: deferring update (trigger activated)
Paramétrage de libgomp1:amd64 (8.3.0-6) ...
Paramétrage de python3-llfuse (1.3.6+dfsg-1) ...
Paramétrage de python3-msgpack (0.5.6-1+b1) ...
Paramétrage de libb2-1 (0.98.1-1) ...
Paramétrage de borgbackup (1.1.9-2) ...
Traitement des actions différées (« triggers ») pour man-db (2.8.5-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.28-10) ...
Traitement des actions différées (« triggers ») pour initramfs-tools (0.133+deb1
0u1) ...
update-initramfs: Generating /boot/initrd.img-4.19.0-9-amd64
root@debian-value:~#
```

1.5.2. Création d'une sauvegarde locale

Création du dossier « sauvegarde » dans le répertoire /mnt :

```
root@debian-value:/# mkdir /mnt/sauvegarde
```

Initialisation d'un dépôt vide pour BorgBackup (argument « --encryption » obligatoire), avec initialisation de la « passphrase » :

```
root@debian-value:~# borg init --encryption=repokey  /mnt/sauvegarde/borg_repo
Enter new passphrase:
Enter same passphrase again:
Do you want your passphrase to be displayed for verification? [yN]: y
Your passphrase (between double-quotes): "passphrase"
Make sure the passphrase displayed above is exactly what you wanted.

By default repositories initialized with this version will produce security
errors if written to with an older version (up to and including Borg 1.0.8).

If you want to use these older versions, you can disable the check by running:
borg upgrade --disable-tam /mnt/sauvegarde/borg_repo

See https://borgbackup.readthedocs.io/en/stable/changes.html#pre-1-0-9-manifest-
spoofing-vulnerability for details about the security implications.

IMPORTANT: you will need both KEY AND PASSPHRASE to access this repo!
Use "borg key export" to export the key, optionally in printable format.
Write down the passphrase. Store both at safe place(s).
```

Création de l'utilisateur « jdoe », qui nous servira à sauvegarder ses données par la suite :

```
root@debian-value:~# adduser jdoe
Ajout de l'utilisateur « jdoe » ...
Ajout du nouveau groupe « jdoe » (1001) ...
Ajout du nouvel utilisateur « jdoe » (1001) avec le groupe « jdoe » ...
Création du répertoire personnel « /home/jdoe »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
Aucun mot de passe fourni
Nouveau mot de passe :
Retapez le nouveau mot de passe :
Aucun mot de passe fourni
Nouveau mot de passe :
Retapez le nouveau mot de passe :
Aucun mot de passe fourni
passwd: Erreur de manipulation du jeton d'authentification
passwd: password unchanged
Essayer à nouveau ? [o/N]n
Changing the user information for jdoe
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Cette information est-elle correcte ? [O/n]o
```

Création de la première archive, qui sera stockée dans /mnt/sauvegarde/borg_repo, nommée « lundi » et qui contiendra les données de l'utilisateurs « jdoe » :

```
root@debian-value:~# borg create --info --stats /mnt/sauvegarde/borg_repo::lundi
 /home/jdoe/
Enter passphrase for key /mnt/sauvegarde/borg_repo:
Creating archive at "/mnt/sauvegarde/borg_repo::lundi"
------------------------------------------------------------------------------
Archive name: lundi
Archive fingerprint: 09704ce51c42bdba95d1a97c305aa924bda30979215388e3eccde7e9fd8
a0d68
Time (start): Wed, 2020-06-24 19:47:18
Time (end):   Wed, 2020-06-24 19:47:18
Duration: 0.02 seconds
Number of files: 3
Utilization of max. archive size: 0%
------------------------------------------------------------------------------
                       Original size      Compressed size    Deduplicated size
This archive:                5.68 kB              4.10 kB              4.10 kB
All archives:                5.68 kB              4.10 kB              4.10 kB

                       Unique chunks         Total chunks
Chunk index:                       5                    5
------------------------------------------------------------------------------
```

Créer ensuite plusieurs fichiers txt à la racine de l'utilisateur « jdoe » :

```
root@debian-value:~# for i in {01..20}; do touch /home/jdoe/txt$i.txt; done
root@debian-value:~# ls /home/jdoe
txt01.txt  txt04.txt  txt07.txt  txt10.txt  txt13.txt  txt16.txt  txt19.txt
txt02.txt  txt05.txt  txt08.txt  txt11.txt  txt14.txt  txt17.txt  txt20.txt
txt03.txt  txt06.txt  txt09.txt  txt12.txt  txt15.txt  txt18.txt
```

Une fois les fichiers txt créés, créez une nouvelle archive que vous nommerez « mardi » :

```
root@debian-value:~# borg create --info --stats /mnt/sauvegarde/borg_repo::mardi
 /home/jdoe/
Enter passphrase for key /mnt/sauvegarde/borg_repo:
Creating archive at "/mnt/sauvegarde/borg_repo::mardi"
------------------------------------------------------------------------------
Archive name: mardi
Archive fingerprint: 232155424e93b2544cd8db8d50ae7c42af3240ce68b9e1a138251272f7f
d04af
Time (start): Wed, 2020-06-24 19:50:59
Time (end):   Wed, 2020-06-24 19:50:59
Duration: 0.03 seconds
Number of files: 23
Utilization of max. archive size: 0%
------------------------------------------------------------------------------
                       Original size      Compressed size    Deduplicated size
This archive:                8.50 kB              4.32 kB              1.08 kB
All archives:               14.18 kB              8.42 kB              5.18 kB

                       Unique chunks         Total chunks
Chunk index:                       7                   10
------------------------------------------------------------------------------
```

Supprimer ensuite quelque fichier txt dans la racine du compte jdoe :

```
root@debian-value:~# borg create --info --stats /mnt/sauvegarde/borg_repo::mercr
edi /home/jdoe/
Enter passphrase for key /mnt/sauvegarde/borg_repo:
Creating archive at "/mnt/sauvegarde/borg_repo::mercredi"
------------------------------------------------------------------------------
Archive name: mercredi
Archive fingerprint: bb68a473f80e15918c0f0f7a64ddd39014843b47e7ab022e5b0e351be67
2a090
Time (start): Wed, 2020-06-24 19:56:49
Time (end):   Wed, 2020-06-24 19:56:49
Duration: 0.02 seconds
Number of files: 18
Utilization of max. archive size: 0%
------------------------------------------------------------------------------
                       Original size      Compressed size    Deduplicated size
This archive:                7.80 kB              4.30 kB              1.05 kB
All archives:               21.99 kB             12.72 kB              6.23 kB

                       Unique chunks         Total chunks
Chunk index:                       9                   15
------------------------------------------------------------------------------
```

Pour lister les archives crées par Borg, taper la commande suivante :

```
root@debian-value:/home/jdoe# borg list /mnt/sauvegarde/borg_repo/
Enter passphrase for key /mnt/sauvegarde/borg_repo:
lundi                                Wed, 2020-06-24 19:47:18 [09704ce51c42bdba9
5d1a97c305aa924bda30979215388e3eccde7e9fd8a0d68]
mardi                                Wed, 2020-06-24 19:50:59 [232155424e93b2544
cd8db8d50ae7c42af3240ce68b9e1a138251272f7fd04af]
mercredi                             Wed, 2020-06-24 19:56:49 [bb68a473f80e15918
c0f0f7a64ddd39014843b47e7ab022e5b0e351be672a090]
```

Créez ensuite un dossier « borg_archive » dans le répertoire /mnt, il nous servira par la suite à monter une archive existante :

```
root@debian-value:~# mkdir /mnt/borg_archive
```

Monter ensuite l'archive du mardi dans le dossier précédemment créé. Ceci nous permettra de restaurer les fichiers précédemment supprimés :

```
root@debian-value:~# borg mount /mnt/sauvegarde/borg_repo::mardi /mnt/borg_archi
ve
Enter passphrase for key /mnt/sauvegarde/borg_repo:
root@debian-value:~#
```

Après avoir monté l'archive du mardi, nous avons plusieurs moyens pour restaurer les fichiers précédemment supprimés qui sont les suivants :

1. Pour ne restaurer qu'un fichier en particulier, spécifier l'emplacement source de fichier (qui est contenu dans l'archive du mardi) et copié se dernier à l'emplacement de votre choix (ici nous allons le copier à la racine du compte « jdoe » pour le restaurer) :

```
root@debian-value:~# cp /mnt/borg_archive/home/jdoe/txt01.txt /home/jdoe/
root@debian-value:~# ls /home/jdoe/
txt01.txt  txt08.txt  txt11.txt  txt14.txt  txt17.txt  txt20.txt
txt06.txt  txt09.txt  txt12.txt  txt15.txt  txt18.txt
txt07.txt  txt10.txt  txt13.txt  txt16.txt  txt19.txt
```

2. Nous pouvons également extraire l'intégralité de l'archive « mardi ». Pour ce faire, il faudra que vous vous placiez à l'emplacement exact ou vous souhaitez que l'archive soit extraite. Dans cet exemple, nous nous placerons à la racine du compte « jdoe », facilitant la restauration de l'intégralité des fichiers (ne nécessite pas de monter l'archive comme dans l'exemple précédant) :

```
root@debian-value:/home/jdoe# borg extract /mnt/sauvegarde/borg_repo::mardi
Enter passphrase for key /mnt/sauvegarde/borg_repo:
root@debian-value:/home/jdoe# ls
home       txt07.txt  txt10.txt  txt13.txt  txt16.txt  txt19.txt
txt01.txt  txt08.txt  txt11.txt  txt14.txt  txt17.txt  txt20.txt
txt06.txt  txt09.txt  txt12.txt  txt15.txt  txt18.txt
root@debian-value:/home/jdoe# ls /home/jdoe/home/jdoe/
txt01.txt  txt04.txt  txt07.txt  txt10.txt  txt13.txt  txt16.txt  txt19.txt
txt02.txt  txt05.txt  txt08.txt  txt11.txt  txt14.txt  txt17.txt  txt20.txt
txt03.txt  txt06.txt  txt09.txt  txt12.txt  txt15.txt  txt18.txt
```

Déplacer ensuite les fichiers txt qui vous intéresse (situe dans /home/jdoe/home/jdoe/) dans /home/jdoe :

```
root@debian-value:/home/jdoe# cp /home/jdoe/home/jdoe/txt02.txt /home/jdoe/
root@debian-value:/home/jdoe# cp /home/jdoe/home/jdoe/txt03.txt /home/jdoe/
root@debian-value:/home/jdoe# cp /home/jdoe/home/jdoe/txt04.txt /home/jdoe/
root@debian-value:/home/jdoe# cp /home/jdoe/home/jdoe/txt05.txt /home/jdoe/
root@debian-value:/home/jdoe# ls /home/jdoe/
home       txt03.txt  txt06.txt  txt09.txt  txt12.txt  txt15.txt  txt18.txt
txt01.txt  txt04.txt  txt07.txt  txt10.txt  txt13.txt  txt16.txt  txt19.txt
txt02.txt  txt05.txt  txt08.txt  txt11.txt  txt14.txt  txt17.txt  txt20.txt
root@debian-value:/home/jdoe# rm -r /home/jdoe/home/
```

Une les opérations de restaurations terminées, tapez la commande suivante pour démonter l'archive de son emplacement :

```
root@debian-value:/home/jdoe# umount /mnt/borg_archive
root@debian-value:/home/jdoe#
```

La configuration de la sauvegarde locale est à présent terminée.

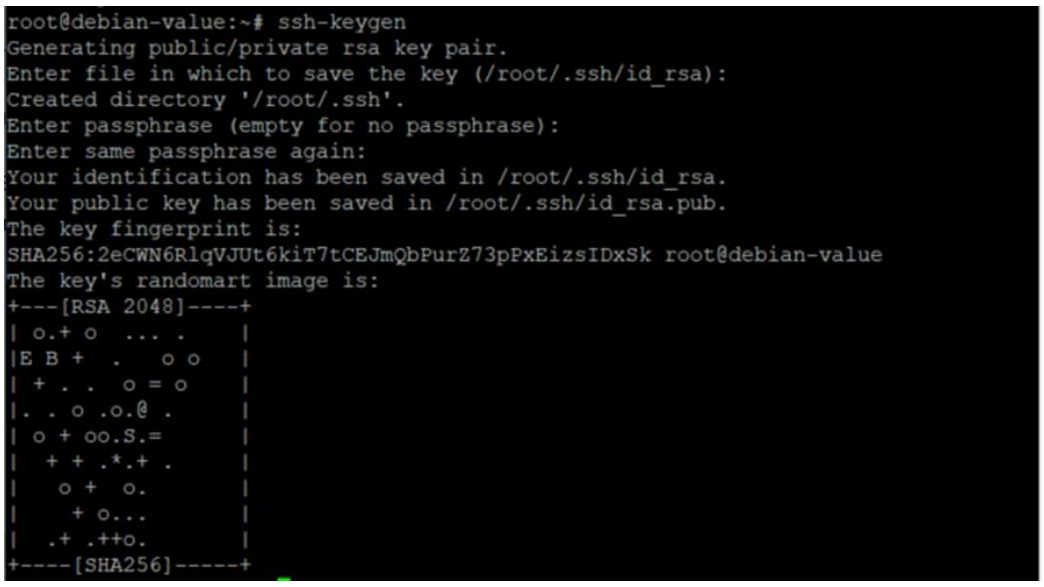
1.5.3. Création d'une sauvegarde distante

1.5.3.1. Préparation du client (machine à sauvegarder)

Avant de commencer la configuration du client, il devra disposer des prérequis suivants :

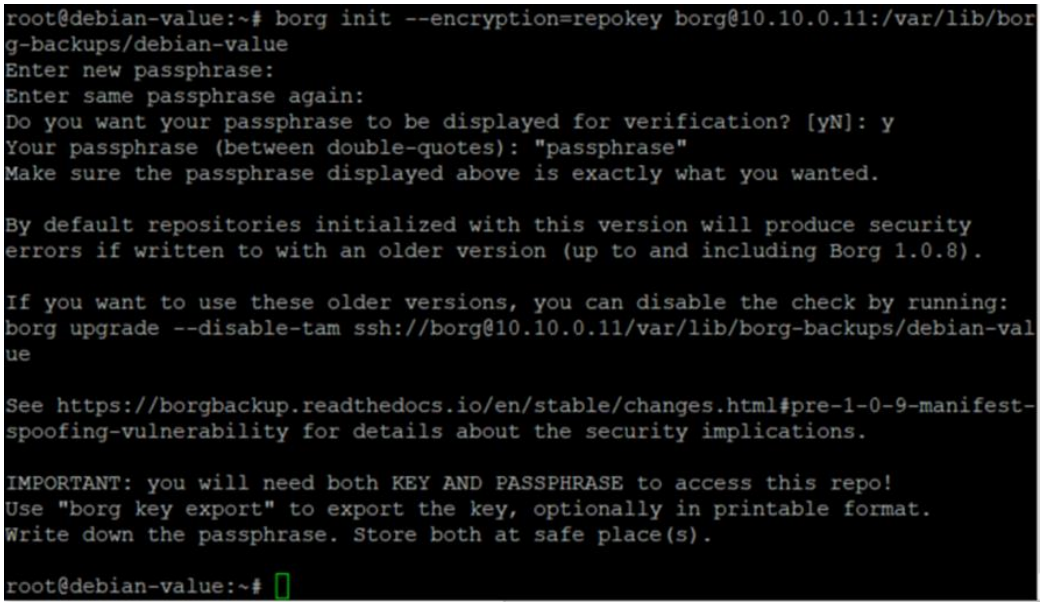
- Avoir installer SSH (client et serveur afin d'éviter tout problème)
- Avoir installer le paquet BorgBackup

Générer une clé SSH :



/!\Avant de continuer les étapes suivantes vis-à-vis de la configuration du client, vous devrez dans un premier, avoir copié la clé SSH du client sur le serveur/!\

Nous allons ensuite initialiser une première archive du client vers le serveur :



Créez ensuite l'archive du client vers le serveur, en la nommant à la date du jour (dans cet exemple, nous archivons la racine du compte jdoe, comme dans la procédure « Sauvegarde locale ») :

```
root@debian-value:~# borg create borg@10.10.0.11:/var/lib/borg-backups/debian-va
lue::2020-06-25 /home/jdoe
Enter passphrase for key ssh://borg@10.10.0.11/var/lib/borg-backups/debian-value
:
root@debian-value:~#
```

Si nous nous rendons ensuite sur la machine serveur, nous pourrons apercevoir que Borg à bien créé les fichiers nécessaires à l'archivage des données du clients (situé dans /var/lib/borg-backups/debian-value) :

```
root@debian-essential:/var/lib/borg-backups# ls /var/lib/borg-backups/debian-val
ue/
config  data  hints.5  index.5  integrity.5  nonce  README
```

Avant d'effectuer une restauration, nous allons supprimer un fichier txt dans le compte jdoe :

```
root@debian-value:~# rm /home/jdoe/txt20.txt
root@debian-value:~# ls /home/jdoe/
txt01.txt  txt04.txt  txt07.txt  txt10.txt  txt13.txt  txt16.txt  txt19.txt
txt02.txt  txt05.txt  txt08.txt  txt11.txt  txt14.txt  txt17.txt
txt03.txt  txt06.txt  txt09.txt  txt12.txt  txt15.txt  txt18.txt
```

Monter ensuite l'archive précédemment créée sur la machine cliente pour restaurer le fichier txt supprimé :

```
root@debian-value:~# borg mount borg@10.10.0.11:/var/lib/borg-backups/debian-val
ue::2020-06-25 /mnt/borg_archive
Enter passphrase for key ssh://borg@10.10.0.11/var/lib/borg-backups/debian-value
:
root@debian-value:~#
```

Restaurez ensuite le fichier txt20.txt :

```
root@debian-value:~# cp /mnt/borg_archive/home/jdoe/txt20.txt /home/jdoe/
root@debian-value:~# ls /home/jdoe/
txt01.txt  txt04.txt  txt07.txt  txt10.txt  txt13.txt  txt16.txt  txt19.txt
txt02.txt  txt05.txt  txt08.txt  txt11.txt  txt14.txt  txt17.txt  txt20.txt
txt03.txt  txt06.txt  txt09.txt  txt12.txt  txt15.txt  txt18.txt
```

Il est également possible d'extraire l'archive entière comme dans la procédure « Sauvegarde locale ».

Une fois les opérations de restauration terminées, démonter l'archive de son répertoire :

```
root@debian-value:~# umount /mnt/borg_archive
root@debian-value:~#
```

La configuration de la machine cliente est à présent terminée.

1.5.3.2. Préparation du serveur (machine accueillant les sauvegardes du client)

Les prérequis pour le serveur sont les même que pour le client.

Créer un utilisateur « borg » qui sera uniquement dédié aux sauvegardes (vous pouvez définir un autre emplacement que /var/lib/borg-backups si vous le désirez) :

```
root@debian-essential:~# useradd borg --create-home --home-dir /var/lib/borg-bac
kups/
```

Créer ensuite un dossier que vous nommerez « .ssh » dans /var/lib/borg-backups :

```
root@debian-essential:~# mkdir /var/lib/borg-backups/.ssh
```

Copier/coller ensuite la clé ssh que vous avez obtenu avec votre client. Pour se faire, retournez sur votre machine faisant office de serveur, et créé à l'aide de nano le fichier « authorized_keys » dans /var/lib/borg-backups/.ssh, puis coller la clé ssh de votre à l'intérieur de ce fichier :

Clé SSH du client

```
root@debian-value:~# vi /root/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCyW+MxknT4eUP8Y00YCl8YeHV6Uc7Ke8G4L00/Jd2H
YRhzEht8936G+sbs05DcD+zeK2fBHsmk7I7la8jfxuaTuMDBATCVXaGjGfyEvp8Nc4ySYqBFfGvghkRf
xFBQo38brR3EShOSZpNWrIwzEjUj7TqL7fjBVuDqSvaZhcc5EavSLiddvUuglWObdTCNRb+kAVAZSlfQ
P7/bKefr34LrO+2e8ZC0hv+49xYZ7uwlKqVhm57dchyeSziuAOInaOapZ4zGlkLNheMlVZqQNaoHqiw9
6jmgPpmQyQqUkbyOmm0ZtdgKcqtzniwXeWHgQkhZy9qusNPyIcauV4soxXHx root@debian-value
```

Copie de la clé SSH du client sur le serveur

```
root@debian-essential:~# nano /var/lib/borg-backups/.ssh/authorized_keys
  GNU nano 3.2       /var/lib/borg-backups/.ssh/authorized_keys        Modifié

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCyW+MxknT4eUP8Y00YCl8YeHV6Uc7Ke8G4L00/Jd2$
```

Le résultat obtenu doit être identique au fichier présent sur votre machine cliente :

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCyW+MxknT4eUP8Y00YCl8YeHV6Uc7Ke8G4L00/Jd2H
YRhzEht8936G+sbs05DcD+zeK2fBHsmk7I7la8jfxuaTuMDBATCVXaGjGfyEvp8Nc4ySYqBFfGvghkRf
xFBQo38brR3EShOSZpNWrIwzEjUj7TqL7fjBVuDqSvaZhcc5EavSLiddvUuglWObdTCNRb+kAVAZSlfQ
P7/bKefr34LrO+2e8ZC0hv+49xYZ7uwlKqVhm57dchyeSziuAOInaOapZ4zGlkLNheMlVZqQNaoHqiw9
6jmgPpmQyQqUkbyOmm0ZtdgKcqtzniwXeWHgQkhZy9qusNPyIcauV4soxXHx root@debian-value
```

La configuration du serveur est à présent terminée.

1.5.4. Automatisation des sauvegardes

L'automatisation des sauvegardes de borg ne doivent être configurer uniquement sur les **clients**.

Dans un premier temps, créez le répertoire /.borg à la racine du compte « root » :

```
root@debian-value:~# mkdir /root/.borg
```

Créez ensuite le fichier « passphrase » afin de stocker la passphrase que vous avez défini lors de la première initialisation de l'archive entre le client et le serveur :

```
root@debian-value:~# nano /root/.borg/passphrase
  GNU nano 3.2                  /root/.borg/passphrase                  Modifié

votre passphrase
```

Protéger ensuite le fichier « passphrase » des autres utilisateurs :

```
root@debian-value:~# chmod 700 /root/.borg/passphrase
```

À présent, nous allons créer le srcipt permettant d'automatiser les sauvegardes, et qui sera stocké dans /etc/cron.daily :

```
root@debian-value:~# nano /etc/cron.daily/borg-backup
```

```
#!/bin/sh
#
# Script de sauvegarde.
#
# Envoie les sauvegardes sur un serveur distant, via le programme borg.
# Les sauvegardes sont chiffrées
#
# http://borgbackup.readthedocs.org/g
#
# Est lancé quotidiennement.

set -e

ts_log()
{
    echo `date '+%Y-%m-%d %H:%m:%S'` $1 >> ${LOG_PATH}
}

# Trap on non-zero exit
trap '[ "$?" -eq 0 ] || cleanup' EXIT

BACKUP_DATE=`date +%Y-%m-%d`
LOG_PATH=/var/log/borg-backup-ftp.log

BORG=/usr/bin/borg
# Fichier dans lequel est stocké la passphrase du dépôt borg
# (attention aux permissions)
export BORG_PASSPHRASE="`cat ~root/.borg/passphrase`"
BORG_REPOSITORY=borg@10.10.0.11:/var/lib/borg-backups/debian-value-ftp
BORG_ARCHIVE=${BORG_REPOSITORY}::${BACKUP_DATE}

ts_log "Starting new backup ${BACKUP_DATE}..."

ts_log "Pushing archive ${BORG_ARCHIVE}"
$BORG create \
     -v --stats --compression lzma,9 \
     $BORG_ARCHIVE \
     /home/jdoe \
     >> ${LOG_PATH} 2>&1

ts_log "Rotating old backups."
$BORG prune -v $BORG_REPOSITORY \
      --keep-daily=7 \
      --keep-weekly=4 \
      --keep-monthly=6 \
      >> ${LOG_PATH} 2>&1
```

Nous allons ensuite donner les droits uniquement à l'utilisateur root (lecture, écriture et exécution) :

```
root@debian-value:/etc/cron.daily# chmod 0700 /etc/cron.daily/borg-backup
```

Forcer ensuite l'exécution du script :

```
root@debian-value:/etc/cron.daily# ./borg-backup
```

Allez ensuite sur la machine serveur, afin de vous assurer que l'archive a été correctement créée :

```
root@debian-essential:/var/lib/borg-backups# borg list /var/lib/borg-backups/deb
ian-value/
Enter passphrase for key /var/lib/borg-backups/debian-value:
2020-06-25                           Thu, 2020-06-25 11:25:12 [b0315db50875183c4
e217dcc6047c3db4bbfc2794c1d2d0efa438d8a6ac04884]
root@debian-essential:/var/lib/borg-backups#
```

L'automatisation des sauvegardes est à présent terminée.

1.5.4. Documentation supplémentaire

Si vous désirez en apprendre plus sur le logiciel Borg Backup, veuillez consulter le lien suivant :
https://borgbackup.readthedocs.io/en/stable/index.html

1.5.6. Cahier de recettes Borg Backup

N°	Actions	Résultat attendu	Nombre d'essai avant résultat attendu	Résultat
1	Installation de BorgBackup	Dépendances correctement installées	1	1-ok
2	Création de l'utilisateur Borg sur la machine serveur	Utilisateur Borg et répertoires correctement crées	1	1-ok
3	Génération des clés SSH sur les serveurs clients	Clés SSH correctement crées	1	1-ok
4	Création du répertoire /borg_archive dans le répertoire /mnt pour remonter les sauvegardes sur les serveurs clients	Répertoire correctement créé	1	1-ok
5	Création du répertoire /.ssh dans le répertoire /root sur la machine serveur	Répertoire correctement créé	1	1-ok
6	Importation des clés SSH publique dans le répertoire /root/.ssh	Clés SSH des clients correctement importées	1	1-ok
7	Initialisation d'une archive sur un serveur client	Création d'un répertoire sur la machine serveur	2	1-commande incorrecte 2-ok
8	Création de la première archive sur un serveur client	Archive présente sur la machine serveur	1	1-ok
9	Création du répertoire /.borg dans le répertoire /root sur la machine serveur	Répertoire correctement créé	1	1-ok
10	Création d'un fichier dans le répertoire /root/.borg pour stocker la passphrase	Fichier correctement créé	1	1-ok
11	Restreindre les droits du fichier pour la passphrase uniquement à l'utilisateur root	Droits correctement définis	1	1-ok
12	Création des script bash sur les serveurs clients pour automatiser les sauvegardes	Script bash fonctionnel avec création d'une archive sur la machine serveur	2	1-Script incorrect 2-ok
13	Restreindre les droits sur les scripts bash uniquement à l'utilisateur root	Droits correctement définis	1	1-ok

1.6. Installation FTP

Pour la configuration du service FTP coté serveur on créé un utilisateur avec son home à /ftp :

```
adduser ftp --home /ftp
```

Ajouter dans le fichier /etc/ssh/sshd_config

```
#chroot ftp
Match User ftp
        ChrootDirectory /ftp
        ForceCommand internal-sftp
```

On change le propriétaire du dossier /ftp et on créé un sous-dossier « PDF » qui appartient à FTP

```
chown root:root /ftp
chown ftp:ftp /ftp/pdf
```

Pour le coté client :

On créé un dossier dans lequel nous allons monter le serveur ftp :

```
mkdir /mnt/ftp
```

Ensuite on dépose notre clé publique dans le répertoire :

```
.ssh/authorized_keys
```

Ensuite on rajoute une ligne dans le fichier `/etc/fstab` pour monter automatiquement le répertoire.

```
ftp@vps-8eccd651.vps.ovh.net:/pdf /mnt/ftp fuse.sshfs
allow_other,default_permissions,port=6345 0 0
```

On lance la commande `mount -a` pour remonter (il monte automatiquement au démarrage).

XI. GLOSSAIRE

FTP : File Transfer Protocol, ou FTP, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

SSH : Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés.

SMTP : Simple Mail Transfer Protocol est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique. SMTP est un protocole assez simple.

Serveur de messagerie : Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre.

Supervision : La supervision est une technique industrielle de suivi et de pilotage informatique de procédés de fabrication automatisés. La supervision concerne l'acquisition de données et des paramètres de commande des processus généralement confiés à des automates programmables.

Sauvegarde : En informatique, la sauvegarde est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.

Archivage : L'archivage désigne le stockage à long terme de documents et données numériques. Les problématiques liées sont le coût et la durée de vie des supports, mais aussi l'accès au contenu malgré les avancées technologiques rendant les anciens supports obsolètes.

CMS : Un système de gestion de contenu ou SGC est une famille de logiciels destinés à la conception et à la mise à jour dynamique de sites Web ou d'applications multimédia. Ils partagent les fonctionnalités suivantes : ils permettent à plusieurs individus de travailler sur un même document.

Sécurité : La sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information.

XII. SOURCES

Ovh.com. Consulté le 16 juin 2020, à l'adresse : https://www.ovh.com/fr/

Debian.org. Consulté le 18 juin 2020, à l'adresse : https://www.debian.org/doc/index.fr.html

Wpmarmite.com. Consulté le 19 juin 2020, à l'adresse : https://wpmarmite.com/wordpress-vs-drupal/

Borgbackup.readthedocs.io. Consulté le 20 juin 2020 à l'adresse : https://borgbackup.readthedocs.io/en/stable/index.html

Tecmint.com. Consulté le 22 juin 2020, à l'adresse : https://www.tecmint.com/install-wordpress-alongside-lamp-on-debian-10/

Computingforgeeks.com. Consulté le 23 juin 2020, à l'adresse : https://computingforgeeks.com/install-drupal-on-debian-linux/

Linuxbabe.com. Consulté le 25 juin 2020, à l'adresse : https://www.linuxbabe.com/mail-server/debian-10-buster-iredmail-email-server

Wiki.debian-fr.xyz. Consulté le 29 juin 2020, à l'adresse : https://wiki.debian-fr.xyz/Fail2ban

Doc.fedora-fr.org. Consulté le 30 juin 2020, à l'adresse : https://doc.fedora-fr.org/wiki/SSH_:_Authentification_par_cl%C3%A9