PROJET ZEROK

Réponse à une appel d'offre

4A SRC 3

Année 2016-2017

CAMUZARD Léo
CENATUS Jean-Luc
KARTIT Taïb
SAHIN Onur
GUILLEMOT Erwan

Table des matières

1. INTRODUCTION

Nous répondons à l'appel d'offre de l'entreprise **ZEROK** qui est est une ESN spécialisée dans les développements d'application capable d'apporter des solutions globales, durables, innovantes et adaptées aux besoins de ses clients, son siège social est situé à Paris.

Son expertise en matière de programmation et de systèmes de bases de données relationnelles lui permet de réaliser, de A à Z, le développement de projets auprès d'une clientèle composée de sociétés et d'institutions.

Avec près de 800 salariés, **ZEROK** intervient auprès de ses 2 implantations en Île-de-France dont un site situé dans la ville de Puteaux et le second à vélizy. Avec un chiffre d'affaire de 100 Millions d'euros en 2016, l'entreprise est en constante évolution de nouveaux sites en province devront ouvrir à la fin de l'année..

2. GESTION DE PROJET

2.1. ORGANISATION DU PROJET

2.1.1. Expression du besoin

L'entreprise **ZEROK** a décidé de migrer son siège social vers un nouveau bâtiment situé à la Défense et en même temps, profite de ce déménagement pour repenser son infrastructure informatique. **ZEROK** nous a ainsi mandaté pour la réalisation de ce projet important, sur les deux sites.

Le nouveau siège social sera composé de 7 étages où les différents services s'y trouvent.
Quant au site secondaire situé à Vélizy-Villacoublay, ce dernier est composé de 3 étages.

Les exigences de la société **ZEROK** sont les suivantes:

- Une infrastructure sous un domaine afin de gérer les utilisateurs
- Une infrastructure redondée et sauvegardée
- Une possibilité de filtrage des sites web
- Une possibilité de filtrage des flux réseaux

- Une possibilité de connexion à distance pour les sociétés externes
- La possibilité de connaitre les pannes grâce à la supervision
- La possibilité de connaître les performances réseau grâce à la métrologie
- Un cloud hybride, avec une possibilité de mettre les données sensibles et importantes dans le cloud privé et le reste dans le cloud public.
- Cloud privé pour fournir à aux développeurs un nouveau service simplifié de mise à disposition de machines virtuelles à la demande.

Infrastructure de la société:

- 1 bâtiment composé de 7 étages (siège social)
- 1 bâtiment composé de 3 étages (site secondaire).
- Data Center pour les serveurs
- PRA

Infrastructure réseau:

- Liaisons VPN IPSEC sur GNS
- Switching en VLAN (Téléphonie, ordinateurs…), ACL
- Redondance de firewalls
- Routage avec les firewalls
- Redondance Sortie WAN
- Redondance réseau HSRP
- QOS sur les switches pour la TOIP (latence/gigue/paquets)
- DMZ et serveurs Web en haute disponibilité

Infrastructure virtualisation:

- Serveurs sous VMware
- Gestion des serveurs avec vCenter
- Haute dispo des VM
- Migration à chaud des VM
- Cloud et Datacenter virtualisé
- Docker
- Jenkins
- Vagrant

Infrastructure sauvegarde:

- Sauvegarde des VM avec Veeam Backup
- Backup Exec pour les serveurs physique

Infrastructure Sécurité :

- HIDS : Ossec

Infrastructure stockage:

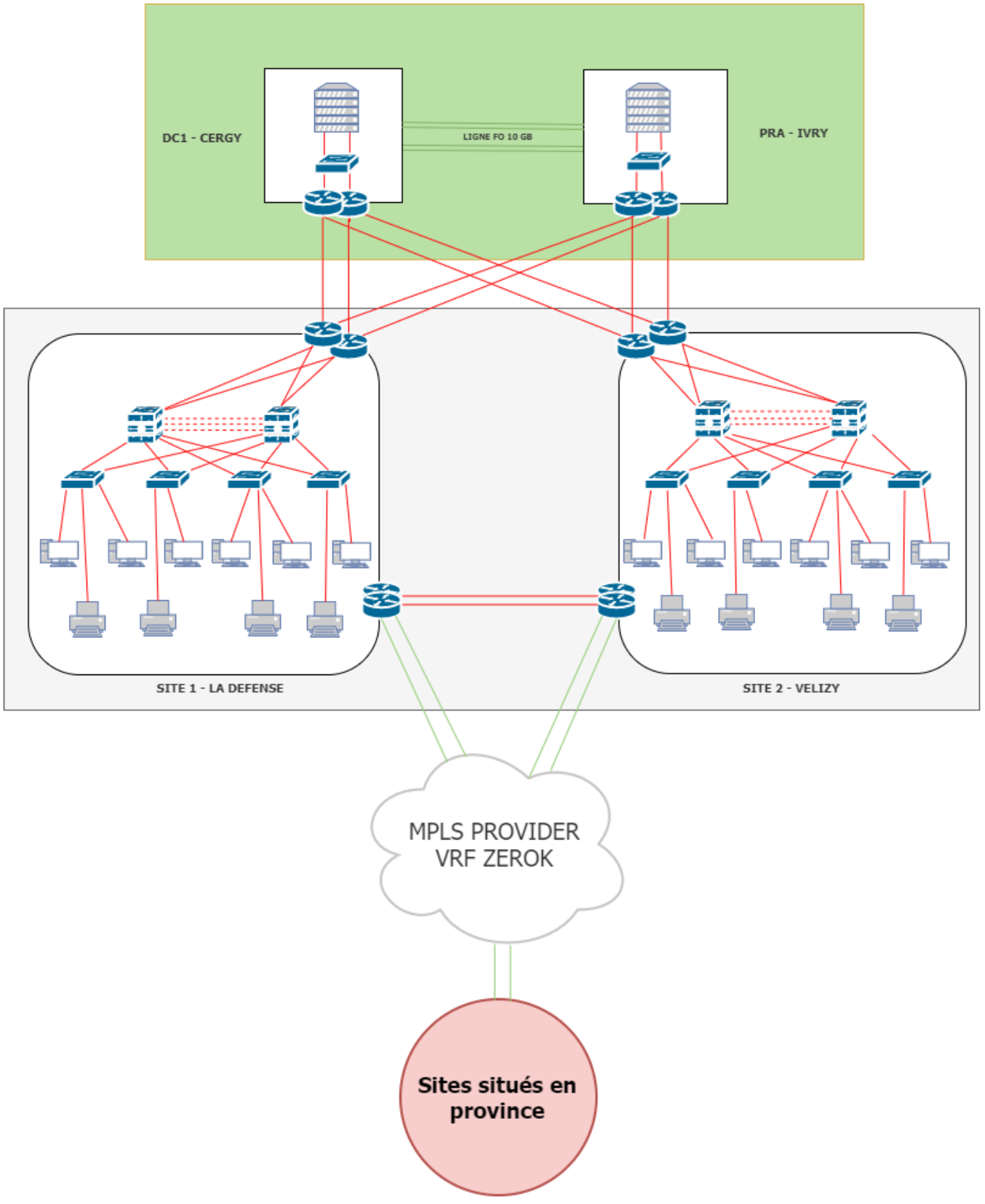
- "Dropbox" maison avec Owncloud

Infrastructure système:

- Serveurs sous Windows 2016 (Contrôleur de domaine,LDAP...) redondés
- Messagerie Exchange
- Clients sous Windows 10 et Linux
- Proxy avec PfSense
- Serveur RADIUS pour gérer l'authentification
- Serveur de fichiers partagés sous Windows Server

Infrastructure supervision:

- Monitoring des serveurs avec PRTG
- Serveur syslog et gestion des logs avec splunk
- Elastic Stack pour Ossec


DC1 - CERGY
LIGNE FO 10 GB
PRA - IVRY
SITE 1 - LA DEFENSE
SITE 2 - VELIZY
MPLS PROVIDER
VRF ZEROK
Sites situés en province

2.1.2. Equipe projet

L'équipe projet se compose de quatre personnes :

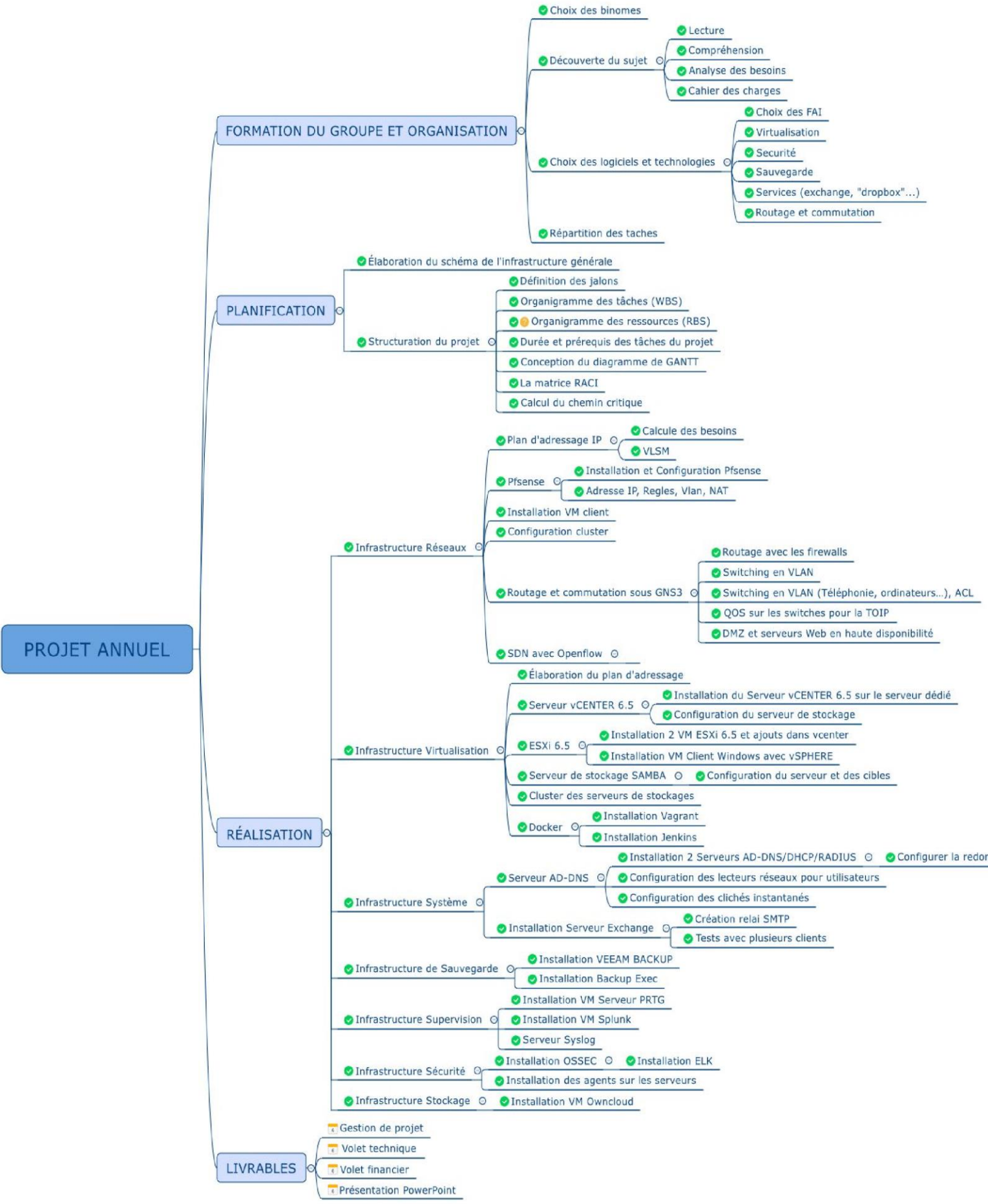
- Un chef de projet et ingénieur réseau représenté par Kartit Taïb
- Un ingénieur DevOps / Sécurité représenté par Camuzard Léo
- Un ingénieur Cloud / Virtualisation représenté par Cenatus Jean-Luc
- Un ingénieur Système représenté par Sahin Onur

2.1.3. Tâches

La première des choses à faire a été de lister l'ensemble des tâches à réaliser puis de regrouper dans un ensemble logique. On retrouve la formation du groupe et l'organisation de celui-ci, la planification du projet, la réalisation et les livrables à fournir. Chacun de ses groupes sont composés de sous-groupe (Infrastructure réseaux, virtualisation, sauvegarde …) qui contiennent des tâches plus précises tel que Installation du serveur Exchange ou encore configuration du serveur de stockage.

Pour réaliser ceci, nous avons utilisé Xmind qui est un logiciel de « mind mapping » c'est-à dire qui permet de représenter visuellement le cheminement de la pensée, il permet de mettre en relation les idées et les informations qui leur sont associées.

L'ensemble des tâches à réaliser est représentée ci-dessous :


PROJET ANNUEL
FORMATION DU GROUPE ET ORGANISATION
Choix des binomes
Découverte du sujet
Lecture
Compréhension
Analyse des besoins
Cahier des charges
Choix des logiciels et technologies
Choix des FAI
Virtualisation
Securité
Sauvegarde
Services (exchange, "dropbox"...)
Routage et commutation
Répartition des taches
PLANIFICATION
Élaboration du schéma de l'infrastructure générale
Structuration du projet
Définition des jalons
Organigramme des tâches (WBS)
Organigramme des ressources (RBS)
Durée et prérequis des tâches du projet
Conception du diagramme de GANTT
La matrice RACI
Calcul du chemin critique
RÉALISATION
Infrastructure Réseaux
Plan d'adressage IP
Calcule des besoins
VLSM
Pfsense
Installation et Configuration Pfsense
Adresse IP, Regles, Vlan, NAT
Installation VM client
Configuration cluster
Routage et commutation sous GNS3
Routage avec les firewalls
Switching en VLAN
Switching en VLAN (Téléphonie, ordinateurs...), ACL
QOS sur les switches pour la TOIP
DMZ et serveurs Web en haute disponibilité
SDN avec Openflow
Infrastructure Virtualisation
Élaboration du plan d'adressage
Serveur vCENTER 6.5
Installation du Serveur vCENTER 6.5 sur le serveur dédié
Configuration du serveur de stockage
ESXi 6.5
Installation 2 VM ESXi 6.5 et ajouts dans vcenter
Installation VM Client Windows avec vSPHERE
Serveur de stockage SAMBA
Configuration du serveur et des cibles
Cluster des serveurs de stockages
Docker
Installation Vagrant
Installation Jenkins
Infrastructure Système
Serveur AD-DNS
Installation 2 Serveurs AD-DNS/DHCP/RADIUS
Configurer la redondonce
Configuration des lecteurs réseaux pour utilisateurs
Configuration des clichés instantanés
Installation Serveur Exchange
Création relai SMTP
Tests avec plusieurs clients
Infrastructure de Sauvegarde
Installation VEEAM BACKUP
Installation Backup Exec
Infrastructure Supervision
Installation VM Serveur PRTG
Installation VM Splunk
Serveur Syslog
Infrastructure Sécurité
Installation OSSEC
Installation ELK
Installation des agents sur les serveurs
Infrastructure Stockage
Installation VM Owncloud
LIVRABLES
Gestion de projet
Volet technique
Volet financier
Présentation PowerPoint

2.1.4. Jalons et livrables

Le premier objectif que nous nous sommes fixés a été de nommer et de lister l'ensemble des technologies que l'on connaissait à propos de chaque point du cahier des charges afin d'avoir une visibilité globale sur les solutions que nous pouvions apporter. Pour les firewalls par exemple nous avions mis Pfsense, Cisco, Alcatel, Juniper etc. et cela pour chacun des points. Ensuite chacun d'entre nous a dû pour la semaine suivante fournir sa vision du plan global de l'architecture réseau de l'entreprise afin que nous puissions discuter des erreurs de chacun et qu'à la fin tout le monde reparte avec une idée précise de ce qui nous attendait. Une fois que le plan global a été réalisé, nous nous sommes réparti les blocs en fonction des compétences de chacun : Onur s'est occupé de la partie système et messagerie, Taïb et Jean-Luc de la partie réseau, cloud et virtualisation et Léo de la partie sécurité, docker et sauvegarde. Pour ce qui n'était pas attribué dans ces blocs on les distribuait en fonction de l'avancée de chacun.
De plus, nous nous tenons informé de nos avancées de manière régulière afin que tout le groupe sache ce que les autres on fait et où est ce qu'ils en sont.
Nous avons eu deux livrable à fournir au cours du projet. Le premier à mi-parcours en décembre, pour prendre connaissance de la compréhension du sujet et des premières avancées et le second fin juin pour le compte rendu global du projet. Celui-ci comportant trois volets, une composante gestion de projet avec l'organisation, le pilotage et la communication, une composante technique où chacun devait justifier ses choix sur les technologies qui avaient été prises et une composante financière afin de chiffrer le montant théorique de notre installation.

2.1.5. Planification

La planification et une composante importante du projet car elle permet de fixer des objectifs et il faut tenir les délais de ces objectifs afin de rester dans les temps pour que le projet aboutisse. Nous avons en premier lieu planifié le plan du schéma réseau de l'entreprise pour que tout le groupe ait en tête le résultat attendu. Nous avons ensuite planifié les jalons afin de connaître les délais des objectifs que nous entreprenons. Nous nous sommes répartis les tâches grâce au WBS (Work Breakdown Structure) que nous avions fait qui permet de nous organiser par la constitution et l'organisation d'idée en groupe puis en sous-groupe puis en tâches. Nous avons également listé les ressources dont nous aurons besoin puis nous les avons organisées dans un RBS (Resource Breakdown structure) pour avoir une visibilité globale. Nous avons déterminé les prérequis et la durée théorique de

chaque tâches ainsi que leur dépendance. Une tâche peut-elle démarrer en même temps qu'une autre ou peut aussi attendre la fin de celle-ci pour débuter.

ID	Libellé	Durée	Tâche reliée	Type de relation
1	Choix des binomes	1 jour		
2	Lecture	1 jour	2	FD
3	Compréhension	1 jour	2	FD
4	Analyse des besoins	1 jour	2	FD
5	Cahier des charges	1 jour	2	FD
6	Choix des FAI	1 jour	6	FD
7	Virtualisation	1 jour	7	FD
8	Sécurité	1 jour	7	FD
9	Sauvegarde	1 jour	7	FD
10	Services (exchange, dropbox...)	1 jour	7	FD
11	Routage et commutation	1 jour	7	FD
12	Répartition des taches	1 jour	7	FD
13	Élaboration du schéma de l'infrastructure générale	200 jours	9;14;12;11;10;13;15	FD
14	Définition des jalons	2 jours	15	FD
15	Organigramme des taches (WBS)	5 jours	19	FD
16	Organigramme des ressources (RBS)	5 jours	21	FD
17	Durée et prérequis des tâches du projet	1 jour	22	FD
18	Conception du diagramme de GANTT	12 jours	23	FD

19	La matrice RACI	1 jour	24	FD
20	Calcul du chemin critique	1 jour	24	FD
21	Calcule des besoins	0,7 jour	17	FD
22	VLSM	0,7 jour	30	FD
23	Installation et Configuration Pfsense	5 jours	31	FD
24	Adresse IP, Regles, Vlan, NAT	14 jours	33	FD
27	Installation VM desVM clients	0,7 jour	37	FD
28	Routage et commutation sous GNS3	10 jours	34;37;38	FD
29	Configuration cluster	1,28 jours	34;37	FD
30	Élaboration du plan d'adressage	13 jours	31	FD
31	Installation VM Serveur AD-DNS	2,1 jours	42	FD
32	Installation Exchange	7 jours	44	FD
33	Configuration des lecteurs réseaux pour utilisateurs	10,5 jours	44	FD
34	SDN avec Openflow	14 jours	46	FD
35	Installation Serveur vCENTER 6.5	14 jours	42	FD
36	Installation 2 Servers ESXi 6.5	14,4 jours	49	FD
37	Configuration des ESXi	20 jours	51	FD
38	Installation VM Client Windows avec vSPHERE	1 jour	52	FD
39	Installation VM Serveur de stockage SAN Openfiler	0,7 jour	42	FD
40	Configuration du serveur de stockage Samba	3 jours	35	FD

41	Configuration du serveur et des cibles	2,8 jours	40	FD
42	Installation Serveur Exchange	10 jours	51	FD
43	Installation Docker avec Jenkins	15,3 jours	56	FD
44	Installation VM serveur de sauvegarde	10,5 jours	58	FD
45	Installation VM pour OwnCloud	14 jours	60	FD
46	Installation VM Serveur Splunk	3 jours	42	FD
47	Installation VM Serveur PRTG	3 jours	42	FD
48	Monitoring des serveurs	9 jours	45;46	FD
49	Monitoring des services	7 jours	45;46	FD
50	Metrologie du réseau	7 jours	35	FD
51	Serveur OSSEC/ELK	10 jours	63	FD
52	Installation Backup Exec	3 jours	42	FD
53	Installation Veeam Backup	5 jours	69	FD
54	Gestion de projet	25 jours	58	FD
55	Volet technique	25 jours	58	FD
56	Volet financier	25 jours	58	FD
57	Présentation PowerPoint	25 jours	58	FD
58	Fin du Projet	0	58	FD

Nous avons défini une matrice RACI (Responsible Accountable Consulted Informed) pour déterminer quel rôle chacun des métiers avait dans chacune des tâches. Grâce à toutes ces planification nous avons pu créer un diagramme de Gantt qui rassemble l'ensemble de nos autres recherches et permet d'avoir une visibilité totale à la fois sur le temps, les ressources métiers et consommable et les dépendances.

2.1.6. Technique de planification

Pour planifier tout cela nous avons utilisé différentes techniques, logiciels qui ont permis d'accroître la visibilité de la planification ainsi que son organisation. On s'est créé un calendrier commun grâce à l'application Calendrier de Google Chrome ce qui nous a permis de nous fixer des rendez-vous, des deadlines pour finir les tâches ou faire un rapport aux autres. Pour des communications plus ponctuelles nous avons utilisé Slack et WhatsApp qui est sont des utilitaires nous permettant de créer un groupe afin que nous puissions échanger en temps réelle nos commentaires, nos avancées, nos interrogations mais aussi des fichiers ou documents. Nous étions constamment notifier au sujet des nouveaux messages.

L'élaboration du journal des tâches sur Excel, du WBS sur Xmind ainsi que du Diagramme de Gantt sur MSprojet nous ont permis de préparer nos projets de meilleur des façons.

2.1.7. Analyse des risques

Les risque présent dans ce projet sont évidemment de finir à temps, les autres projets qui s'accumulent et le travail ont tendance à repousser l'avancée de celui-ci. D'où l'intérêt d'une bonne organisation et d'une bonne planification.

Un autre risque est de ne pas trouver les technologies que nous voulons. Nous travaillons sur du gratuit et il n'est pas forcément évident de trouver sur la bonne version de la bonne technologie adéquat à notre projet.

Il faut penser à la compatibilité de tous les éléments une fois ensemble.

Un autre risque est également le budget, il faut que l'infrastructure soit raisonnable.

Le passage au tout informatique va nécessiter un transfert de compétence basique quant à la gestion des problèmes quotidien. Cela demandera surement de nouvelle embauche.

Une adaptation obligatoire de la part de l'ensemble des salariés à cette nouvelle méthode de travail qui risque d'engendrer une perte de performance de la part de certain le temps de l'adaptation.

Une veille technologique pour éviter le piratage très présent de nos jours.

La gestion des droits et accès aux documents sensibles de l'entreprise comme les plans se fera dorénavant de manière informatique. Le transfert des documents papiers aux documents informatique demandera un long travail.

Ajout de réglementation juridique lors du passage à l'informatique.

2.1.8. Avantages

Les avantages :

- ➔ L'entreprise sera plus concurrente quant aux autres entreprises du même secteur.
- ➔ Elle pourra répondre plus rapidement aux demandes des clients et verra sa communication bien plus rapide qu'auparavant.
- ➔ L'ensemble du personnel pourra avoir accès aux documents qu'ils ont besoin grâce à la gestion des droits s'ils ont une autorisation d'une personne agréée.
- ➔ Plus besoin de gérer les archives papiers, tout se fera en ligne, il y aura donc un gain de place.
- ➔ Economie du au moindre usage du papier.
- ➔ Modification des documents plus rapide.
- ➔ Possibilité de récupération de documents grâce à la sauvegarde en cas de perte.
- ➔ Continuité du travail assuré par la redondance de tous les outils informatiques.

2.2. PILOTAGE DU PROJET

2.2.1. Suivi des ressources

Pour tout ce qui est ressource, qu'elle soit humaine ou consommable, nous nous sommes servis de deux éléments. D' une part le RBS qui utilise Xmind tout comme WBS et qui est donc un « mind mapping » afin de lister et d'organiser l'ensemble des produits que nous aurions besoin.

Ceci a pour finalité leurs injection au sein du diagramme de Gantt en leur assignant un coup ce qui permettra une estimation de coût par tâche. De même pour les ressources humaine, on définit un coût horaire et pour chaque personne assignée à une tâche on peut apercevoir le coût total.

D'autre part, nous avons fait une matrice RACI. La matrice RACI représente une matrice des responsabilités. Elle indique les rôles et les responsabilités des intervenants au sein de chaque tâche à réaliser. Elle nous permet d'avoir une vision simple et clair de qui fait quoi dans le projet. Les lignes de la matrice font références aux activités identifiées et les colonnes aux rôles des personnes dans le projet. Dans chaque cellule on peut trouver quatre lettres : un R, A, C ou I.

Chaque lettre à sa signification :

- R veut dire Responsable
- A veut dire approuvé
- C veut dire Consulté
- I veut dire Informé

2.3. DIAGRAMME DE GANTT

Une fois que le WBS, RBS, la matrice RACI, la liste des tâches ont été réalisés nous pouvons toute les regrouper pour construire notre diagramme de Gantt. Le Diagramme de Gantt est un outil qui sert à représenter de manière visuelle l'état d'avancement des différentes activités qui constituent le projet. La colonne de gauche du diagramme est constituée de la liste des tâches regroupée et hiérarchisée, du temps nécessaire à la réalisation, de la date de début théorique, des ressources utilisées et du coût global. Tout cela est ensuite matérialisé par une barre horizontale, dont la position et la longueur détermine la date de début et de fin et la durée. On peut, grâce au diagramme de Gantt répertorié toutes les tâches à accomplir pour mener le projet à bien en indiquant à quelle date celle-ci doivent débuter.

3. INFRASTRUCTURE RÉSEAU ET SÉCURITÉ

3.1. PFSENSE

Pour les cœurs de réseaux nous avons décidé de prendre des firewalls de type Pfsense, Pfsense est un routeur/firewall open source. Nous avons choisi Pfsense car il combine à la fois le deuxième niveau de firewall ainsi que le routeur interne pour gérer les différents vlan internes. Il est gratuit ce qui permet une importante économie et il est facilement administrable. Il possède des fonctions de routage et de NAT ainsi que les équivalents libre des outils et services utilisés par les autres firewalls propriétaire comme par exemple le filtrage par IP source, destination ou par port, les VPN, le load balancing.

Les possibilités sur Pfsense sont quasiment les mêmes que sur les autres firewalls propriétaires avec moins de support et une réactivité plus lente face aux nouvelles infections.

Il est idéal pour les petites entreprises car il ne consomme que peu de ressources et est adaptable en fonction des besoins.

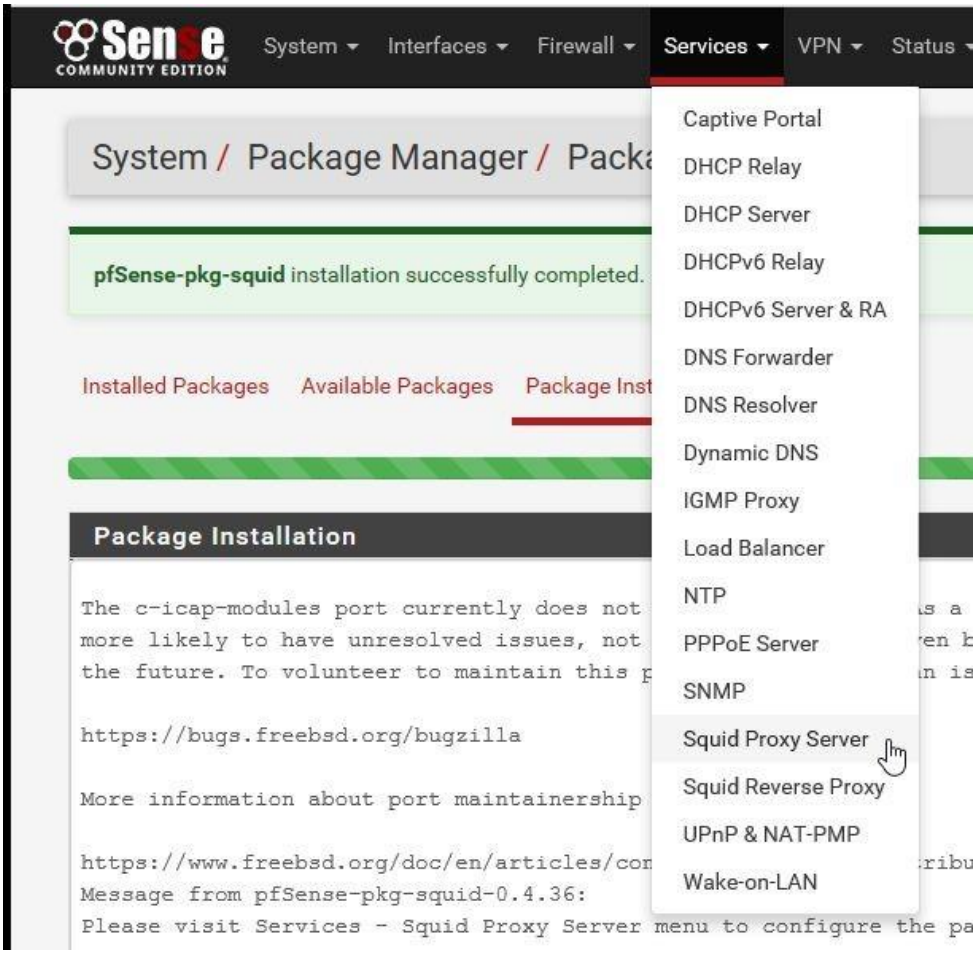
3.1.1 Proxy Squid de PFSENSE

Pour le proxy nous avons la solution “Squid” qu’il faut rajouter à nos routeurs pfsense.

L’intérêt d’avoir un proxy transparent permet plusieurs points :

- ➔ selon la mise en place, possibilité de filtrer les sites web
- ➔ effectuer du cache de site web (pour distribuer plus rapidement les images d’une page web par exemple)
- ➔ effectuer du cache de mise à jour (utile pour Windows Update)
- ➔ comprendre l’utilisation de son réseau en analysant les trames / flux qui transitent au travers de ce proxy.

Un serveur proxy se place entre votre routeur et votre LAN. Tous les utilisateurs de votre LAN accéderont forcément à ce serveur proxy et ce de manière automatique sans avoir de manipulations à effectuer. La mise en place de ce service a été très simple sous pfSense.



3.2. HIDS

3.2.1 OSSEC

Ossec est un détecteur d'intrusion du type HIDS (Host-based Intrusion Detection System). Il est l'un des HIDS des plus utilisés, très facile d'accès tant pour l'installation que pour l'utilisation.

Mais que fait Ossec exactement :

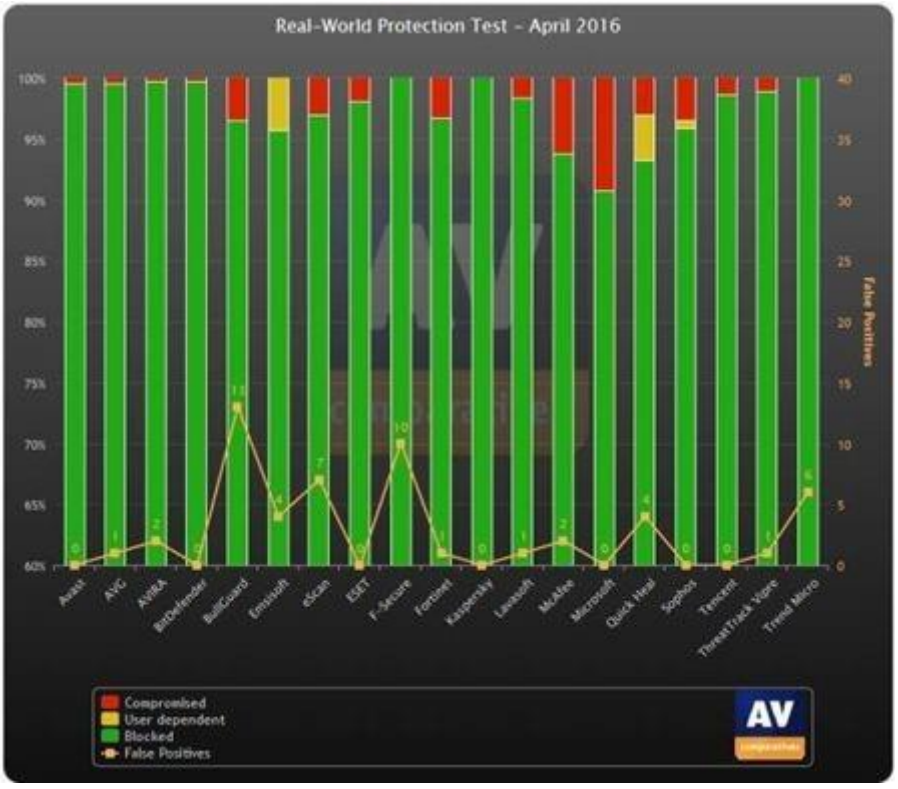
➔ Vérification de l'intégrité des fichiers systèmes.
➔ Analyse des logs et remontée
➔ Détection des rootkits
➔ Mécanisme de prévention actif (lancement de règle iptables par exemple) ➔ Sévérité des alertes classés de 0 à 15

3.3. TREND MICRO OFFICE

Afin d'assurer la sécurité de nos postes et de nos serveurs, nous avons fait le choix d'installer un antivirus de la marque Trend Micro. D'après l'étude mené par Gartner, c'est le logiciel de protection des périphériques le performant du marché (Etude de février 2016).

Trend Micro investit énormément dans la filière de développement pour le contrôle applicatif, vulnérabilité, détection, sandbox sur Windows et sur MAC. Il peut également protéger les applications de téléphone portable professionnel lorsque les entreprises en fournissent à leurs employés (Android, IOS, Windows et BlackBerry). Il offre une gamme de

protection très large incluant le filtrage URL, les ressources critiques, la protection des processus, la protection des moteurs de recherche et plein d'autre. L'entreprise Trend Micro est en étroite collaboration avec VMware ce qui assure une protection efficace sur l'ensemble des VM même dans le Cloud. Il a une interface visible avec une prise en main Facile pour l'administrateur. Il inclut également le support, ses mises à jour applicatives et le déploiement de sources sûres.



De plus l'entreprise AV Compare teste, chaque mois qu'un panel d'une vingtaine d'antivirus, le blocage des virus. Nous pouvons constater qu'en Avril 2016 Trend Micro a bloqué l'ensemble de leur test ce qui montre la fiabilité de cet antivirus face à leur test.

La configuration comprend :

- Installation sur le serveur
- Installation sur le client

3.4. SWITCH

Pour le switching nous avons opté pour les Switch Cisco 2960-X. Cisco est un leader du marché pour ce qui est du switching and du routing, même si son coût peut être un peu élevé, celui-ci offre des switches de qualités. Ils assurent au réseau une robustesse et une fiabilité qui permettra une disponibilité sur le long terme. Le support est disponible et compétent. Il est facilement configurable par ses lignes de commandes intuitives, il peut être administré à distance ou en
local par son câble console. Il offre des protocoles propriétaire plus performant tel que LACP, VTP ou PVST permettant de faciliter et d'optimiser la configuration du réseau.
Les switches 2960-x propose :

- 48 ports Gigabit
- Port SFP ou SFP+ pluggable
- FlexStack pour stacker jusqu'à 8 switches
- Power Over Ethernet Plus (PoE+)
- Interface USB et Ethernet pour le management

La configuration comprend :

- Configuration des interfaces
- Connexion SSH
- Sécurité lors de la connexion

Fournisseur d'accès internet :

Pour nous donner un accès internet nous avons choisi Orange. C'est un leader du marché Français. Il offre une qualité assurée et a de l'expérience au niveau des entreprises. Ce qui est un avantage considérable pour l'entreprise ZEROK qui pourra bénéficier d'un accès internet en toute sécurité.

L'installation pour la société ZEROK comprend :

- Deux sorties internet 20Mo dimensionnées en fonction des besoins pour permettre un trafic fluide et une marge d'évolutivité. Nous avons pris 100 Mo

plutôt que 10 car pour le double de débit, le prix n'augmente que très peu avec l'évolution actuelle

- Un Lan to Lan de 200km entre les deux datacenters de 1 Gbps pour assurer la redondance, la téléphonie et les flux des deux sites.

En cas de panne du Lan to Lan, l'engagement de service dans le contrat fait avec Orange assure une résolution dans les 4h. Ce laps de temps n'étant pas critique pour l'entreprise, nous assurons une solution de contournement par l'activation d'un VPN entre les sites.

Quant à la gestion de la sauvegarde pour le PRA, nous ferons des sauvegardes sur bande grâce au logiciel Veeam entreprise plus que nous enverrons de manière quotidienne au PRA. Dans le contrat avec notre PRA, il est indiqué qu'il utilise un robot permettant d'exploiter nos bandes de sauvegarde afin de nous les réinjecté.

- Interco redondé par VPN entre les sites 10Gbps ou engagement de réparation en 4h par l'opérateur acceptation de contournement par VPN pendant 4h

- 500 Mo en sortie pour sauvegarde PRA avec replicator (transfert) ou VEEAM sauvegarde sur bande -> 10Mo suffit

4. INFRASTRUCTURE SYSTÈME

4.1. ACTIVE DIRECTORY

L'active Directory est un composant essentiel aujourd'hui à n'importe quel réseau d'entreprise. Active Directory est le nom du service d'annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire Active Directory est basé sur les standards TCP/IP : DNS, LDAP etc.

Le service d'annuaire Active Directory doit être entendu au sens large, c'est-à-dire qu'Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone, etc.) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, etc Ce qu'il fait qu'aujourd'hui un bon Active Directory peut simplifier notre réseau et surtout le rendre très efficace.

Dans notre situation, l'active directory va nous permettre de référencer les comptes des utilisateurs afin qu'ils puissent se connecter à leurs sessions avec lancements des scripts à l'ouverture de la session pour ajouter et installer l'imprimante, puis l'ajout des lecteurs réseaux pour les fichiers partagés, cela va nous permettre notamment de pouvoir accorder des droits à certains dossiers en fonction du service de l'utilisateur, la gestion des ACL sera notamment plus facile.

4.2. DHCP

Pour la redondance du service DHCP, nous allons utiliser deux serveurs installés dans les deux sites afin de pouvoir mettre en place la haute disponibilité des serveurs.

Depuis Windows Server 2008 R2, il existe deux options à haute disponibilité dans le cadre du déploiement du serveur DHCP. Chacune de ces options est liée à certains défis.

- Protocole DHCP dans un cluster de basculement Windows. Cette option place le serveur DHCP dans un cluster accompagné d'un serveur supplémentaire configuré

à l'aide du service DHCP qui suppose la charge si le serveur DHCP principal

échoue. L'option de déploiement du clustering utilise un espace de stockage partagé unique. L'espace de stockage est ainsi un point d'échec unique, et implique un investissement supplémentaire en termes de redondance de stockage. En outre, le clustering entraîne une configuration et une maintenance complexes.

Protocole DHCP de l'étendue fractionnée. Le protocole DHCP de l'étendue fractionnée utilise deux serveurs DHCP indépendants qui partagent la responsabilité pour une étendue. Généralement 70 % des adresses de l'étendue

sont attribuées au serveur principal et les 30 % restantes sont affectées au serveur de sauvegarde. Si les clients ne peuvent pas atteindre le serveur principal, ils peuvent récupérer une configuration IP à partir du serveur secondaire. Le déploiement de l'étendue fractionnée ne fournit pas de continuité d'adresse IP et s'avère inutilisable

dans les scénarios où l'étendue est déjà intensément utilisée par l'espace d'adressage, ce qui est fréquent avec IPv4 (Internet Protocol version 4).

Ce basculement nous permet de déployer un service DHCP à haute résilience pour prendre en charge une grande entreprise sans devoir relever les défis que représentent les options abordées précédemment.

Les principaux objectifs de cette fonctionnalité sont les suivants :

- Offrir un service DHCP disponible en continu sur le réseau d'entreprise ; - Si un serveur DHCP n'est plus joignable, le client DHCP est capable d'étendre le bail sur son adresse IP actuelle en contactant un autre serveur DHCP sur le réseau d'entreprise.

- Optimisation et Sécurisation de l'Infrastructure

Nous avons choisi de mettre en place la solution de basculement à l'étendue fractionnée.

4.3. SERVEUR EXCHANGE

Nous avons choisi de mettre en place Exchange 2016 pour notre serveur, la version 2016 étant la plus récente afin d'avoir un serveur de messagerie dernier cri. Exchange est l'une des solutions payante les plus utilisés. Il offre de nombreuses fonctionnalités comme l'autodiscover ou le Outlook anywhere, il est plus facile d'administration et possède des fonctionnalités plus intéressantes qu'une solution open-source et il permet de gérer efficacement la messagerie de l'entreprise. Pour le relay, nous avons choisi d'utiliser les fonctionnalitées SMTP et IIS sur un serveur Windows 2016

Exchange à pour avantage de pouvoir être reliée à l'AD. Cela permet de lier les comptes AD et les comptes Exchange afin d'avoir une gestion plus claire et simplifiée des utilisateurs.

Le but de la mise en place d'un serveur de messagerie est de pouvoir communiquer vers des adresses mail du même domaine mais aussi vers des adresses d'un autre domaine. Théoriquement, il est possible de faire sortir les mails vers l'extérieur pour que nos utilisateurs puissent communiquer et avec des utilisateurs ayant une adresse sous un autre domaine, gmail.com par exemple.

4.4. OWN CLOUD

OwnCloud est une application open source de stockage en ligne et de gestion de fichiers. Il permet de stocker et de synchroniser des fichiers entre plusieurs postes client et le serveur OwnCloud. Les fonctionnalités fournies sont le partage de fichiers, la lecture de musique en ligne, la visualisation et l'édition de documents et de photos en ligne… Il est aussi possible d'implémenter OwnCloud avec de nombreux plugins. Nous l'avons choisi car c'est une solution gratuite, possédant des fonctionnalités très intéressantes, simple à mettre en place et facile d'administration grâce à son interface web. Nous l'avons installé sur un Debian 7.

La configuration comprend :

- Installation d'apache2 pour l'interface web
- Installation de OwnCloud (L'installation et la configuration de MYSQL se fera automatiquement)
- Sécurisation de OwnCloud avec le protocole HTTPS.
- Création des comptes utilisateurs et des dossiers partagés. (La stratégie de partage sera ainsi faite : Chaque service aura son propre répertoire et chaque personne du service y aura accès. Il y aura en plus dans les répertoires de chaque service un dossier direction auquel seule la direction du service aura accès. Chaque utilisateur aura bien évidemment un dossier qui lui sera propre.)
- Mise en place du client OwnCloud sur les postes client.

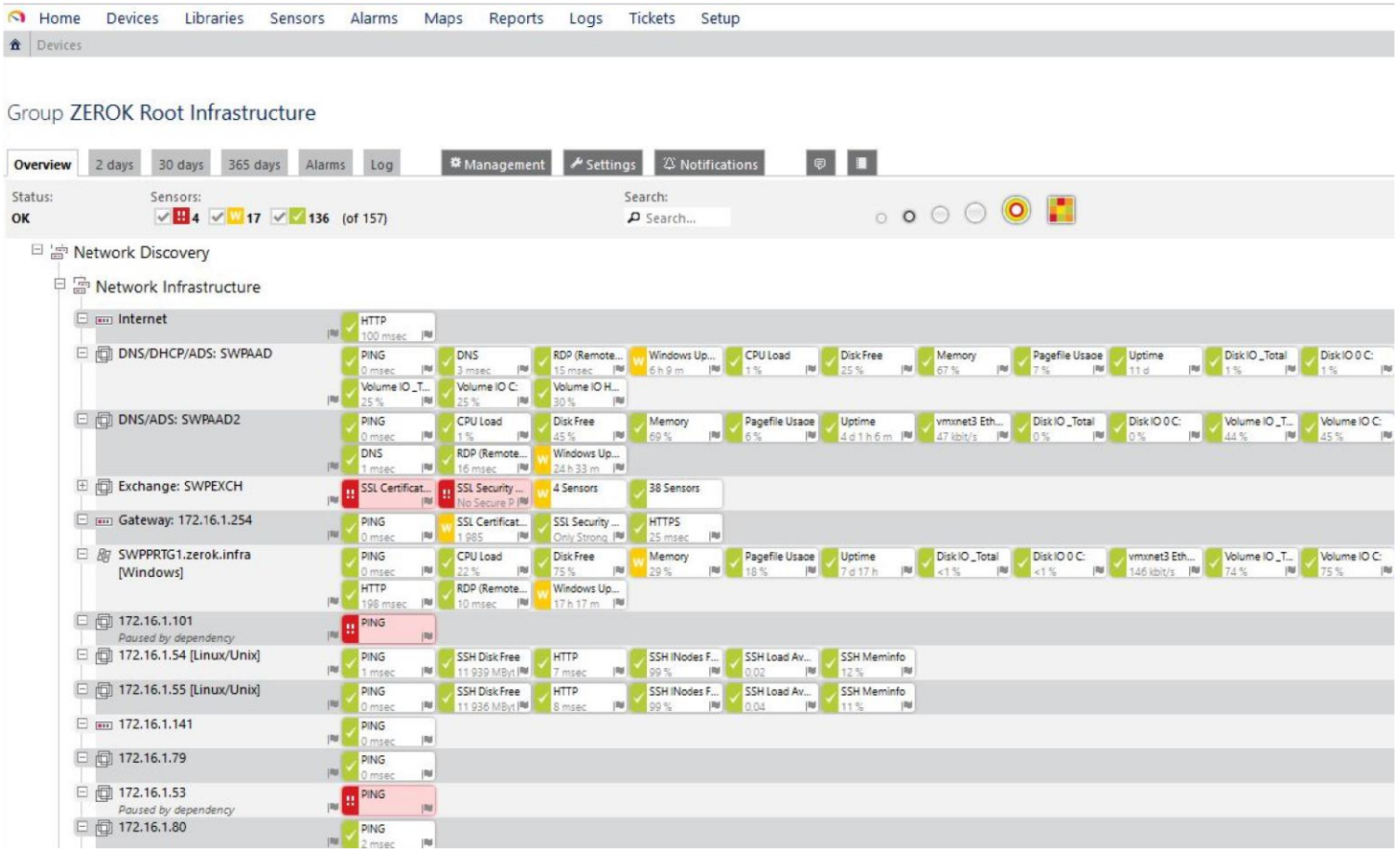
4.5. SUPERVISION

Pour la supervision nous avons opté pour la solution PRTG/SPLUNK.

4.5.1 PRTG

PRTG supervise tous les serveurs que nous possédons (services surveillés : espace disque, ram, cpu, uptime, ping, services spécifiques aux serveurs…) qu'ils soient sous distribution

Windows ou Linux.



4.5.2 SPLUNK

Splunk index en temps réel des données issues de machines (logs, web services, configurations, équipements télécom, GPS, capteurs,...)2 . Les utilisations vont de la sécurité (corrélation, analytics, fraude...) à la supervision d'infrastructure, en passant par le reporting métier.

Les principaux champs d'utilisation de Splunk sont :

- ➔ Reporting pour les métiers,
- ➔ Suivi de la performance et du respect des SLA,
- ➔ Évaluation de la qualité d'une release ou d'un code,
- ➔ Surveillance opérationnelle en 24/7 des infrastructures et de l'utilisation des ressources,
- ➔ Monitoring de la performance et de la montée en charge des applications,
- ➔ Monitoring de tests et de déploiements,
- ➔ Monitoring des applications mobiles,
- ➔ Analyses et monitoring des IoT et des distributeurs automatiques,
- ➔ Supervision des systèmes industriels,
- ➔ Analyses de tendance & planification des capacités,
- ➔ Surveillance des matériels/OS/processus,
- ➔ Monitoring de la sécurité,
- ➔ Investigation d'incidents,
- ➔ Journaux d'Audit et respect des règles de conformité.

La solution est gratuite pour un usage jusqu'à 500 Mo/jour (mais comporte certaines limitations).

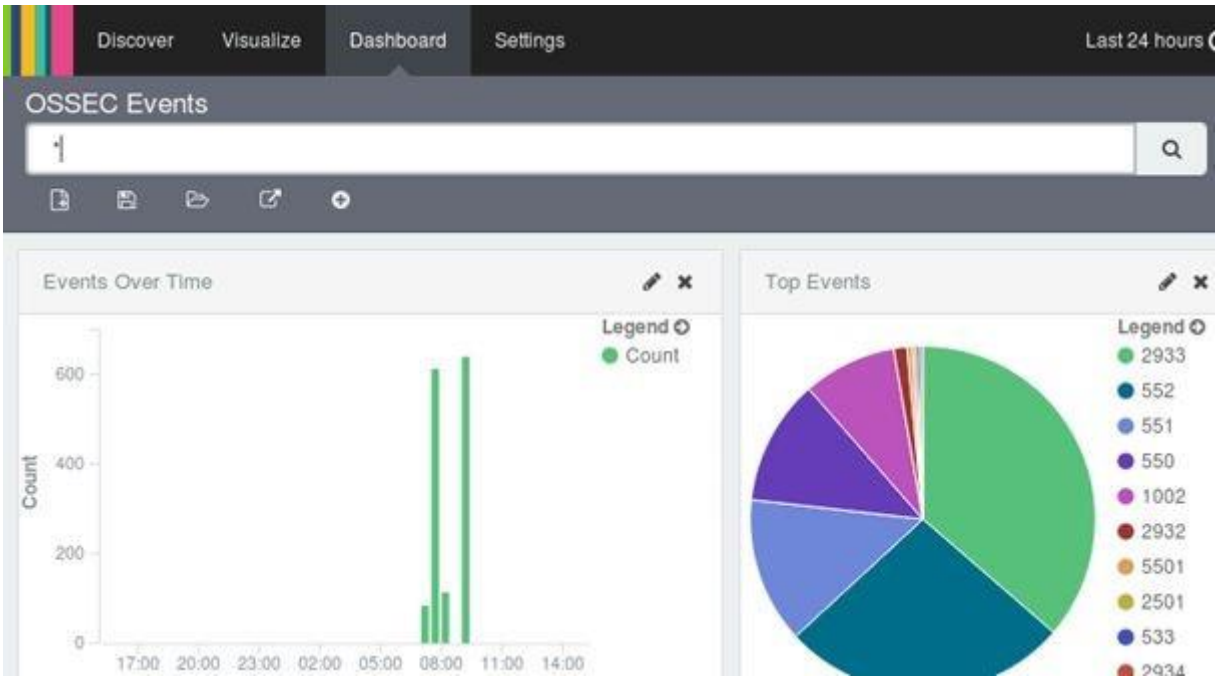
4.5.3 ELK/KIBANA

Elasticsearch est un moteur de recherche et d'analyse RESTful distribué, capable de résoudre un nombre grandissant de cas d'utilisation. Élément clé de la Suite Elastic, il stocke de manière centralisée vos données et vous permet d'être préparé en toutes circonstances.

Les solutions Elasticsearch, Logstash et Kibana sont disponibles en tant que produits ou services.

Logstash fournit un flux d'entrée à ElasticSearch pour le stockage et la recherche, et Kibana accède aux données pour la visualisation, par exemple pour des tableaux de bord.

Kibana est un greffon open source de visualisation de données pour Elasticsearch. Il fournit des fonctions de visualisation sur du contenu indexé dans une grappe Elasticsearch. Les utilisateurs peuvent créer des diagrammes en barre, en ligne, des nuages de points, des camemberts et des cartes de grands volumes de données.



4.6. VIRTUALISATION RÉSEAU

GNS3 est un logiciel de simulation de réseaux informatiques. Nous nous en sommes servis pour virtualiser notre infrastructure réseau. Nous y avons intégré nos firewalls. Nous nous sommes servis de switch afin de faire du VLAN par port.

5. INFRASTRUCTURE DE VIRTUALISATION ET DE STOCKAGE

5.1. INTRODUCTION

Cette phase du projet consiste à mettre en place l'infrastructure virtualisé du datacenter et du PRA en prenant en compte que toute l'infrastructure doit être redondé, de plus nous allons mettre en place des serveurs de stockage avec tous les logiciels de sauvegardes pour les machines virtuelles et les serveurs de sauvegardes.

5.2. ETUDE DU BESOIN

La société ZEROK souhaite mettre en place une solution fiable et redondée, pour cela nous concevoir une architecture qui est dite « haute disponibilité », on entend par disponible le fait d'être accessible et rendre le service demandé. La disponibilité est un enjeu très important et qu'en cas d'indisponibilité, les répercussions en terme de coûts et de production peuvent avoir un effet catastrophique. Cette disponibilité est mesurée par un pourcentage essentiellement composé de 9. Par exemple une disponibilité de 99 % indique que le service ne sera pas disponible pendant 3,65 jours par an maximum (un tableau en dessous est fourni pour les différents taux de disponibilité). On atteint la haute disponibilité à partir de 99,9 %.

Pour cela nous allons mettre en place un cluster d'ESXi pour ainsi augmenter la disponibilité, grâce à la technologie VMware Haute Disponibilité et VMotion.

Pour le stockage il sera assuré par des serveurs SANs, un serveur par site, avec des liaisons ISCSI qui seront en RAID 5.

5.3. SERVICES VMWARE

L'environnement de virtualisation et la gestion des ESXi 5.5 sont gérées par l'Appliance vCenter Server 64 bits 5.5 et vSphere Client.

5.3.1. VMotion

De plus nous allons implémenter la fonctionnalité « vMotion » grâce au cluster, cette technologie exploite la virtualisation complète des serveurs, des ressources de stockage et des réseaux pour déplacer une machine virtuelle, en cours d'exécution, d'un serveur vers un autre.

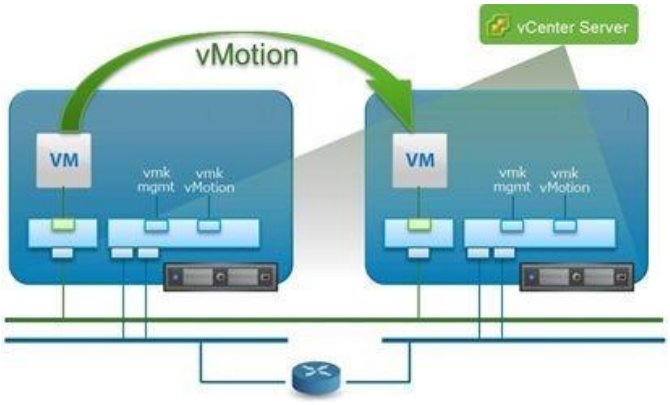
L'état complet d'une machine virtuelle est encapsulé dans des fichiers stockés sur une ressource de stockage partagée. Étant donné que le réseau est également virtualisé par VMware ESX, la machine virtuelle conserve son identité réseau et ses connexions, ce qui garantit une migration transparente, cela a pour avantages :

- Réalisation de migrations à chaud sans interruption de service perceptible par les utilisateurs.

- Optimisation continue et automatique des machines virtuelles au sein des pools de ressources.

- Réalisation de la maintenance matérielle sans interruption de service ni perturbation au niveau des opérations de l'entreprise.

- Déplacement des machines virtuelles afin de les retirer de serveurs défaillants ou présentant des performances insuffisantes.

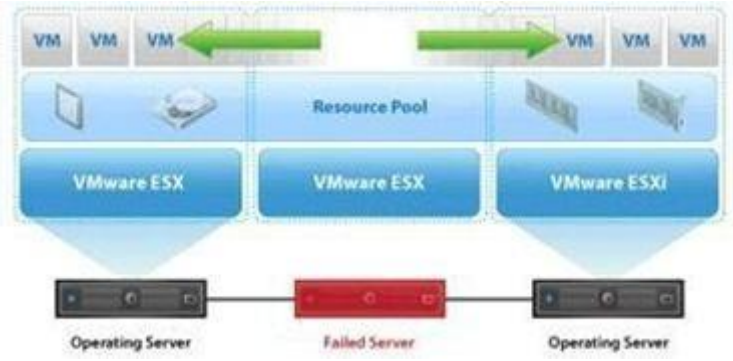


Pour le fonctionnement du VMotion, il faut :

- 1 vCenter
- Au minimum 2 Serveurs ESXi
- Minimum 2 Centres de données
- 1 Port VMKernel dédié au VMotion

5.3.2. Haute disponibilité

Pour protéger notre infrastructure contre des pannes de différentes sources, sur le vCenter des deux sites, on a implémenté, au niveau du cluster la « HA » qui permet le redémarrage des VMs situées sur un hôte du cluster sur un autre hôte en cas de panne sur un ESXi.



VMware HA offre un mécanisme de basculement systématique et économique à votre environnement informatique virtualisé.

- Protection des applications avec aucune autre option de basculement et garantie d'une haute disponibilité des applications logicielles qui pourraient sinon ne pas être protégées.

- Protection des applications contre les pannes liées au système d'exploitation en redémarrant automatiquement les machines virtuelles lorsqu'une panne est détectée.

- Établissement d'une première ligne de défense cohérente pour l'ensemble de l'infrastructure informatique.

Pour la mise en place de la technologie « High Availability », on reprend la même configuration que celle du vMotion puis il faut créer un cluster en y ajoutant les deux serveurs ESXi et il faut modifier les paramètres du cluster en activant l'option du HA.

5.3.3. Vmware vsphere update manager

C'est une solution de gestion automatisée des correctifs des hôtes VMware ESXi et de certaines machines virtuelles Microsoft et Linux, VMware Update Manager offre une solution à l'un des principaux problèmes de tous les services informatiques : suivi des niveaux de correctifs et application des correctifs de bogue/sécurité, cela permet de diminuer la vulnérabilité de l'infrastructure.

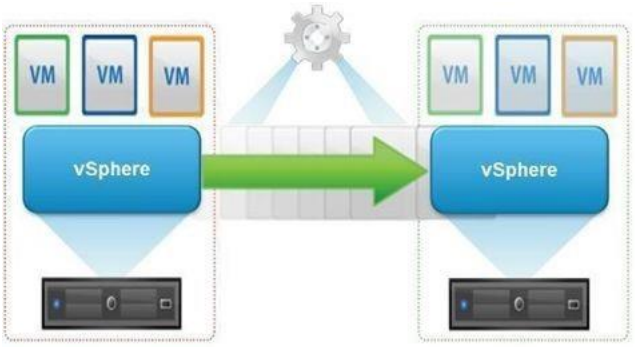
VMware Update Manager réduit les risques de problèmes liés à l'application de correctifs aux machines virtuelles grâce à une fonctionnalité de snapshot des machines virtuelles avant l'application des correctifs et grâce au stockage de ces snapshots pendant une période définie par l'utilisateur. On peut ensuite rétablir les machines virtuelles à un état connu si l'application d'un correctif a des effets secondaires inattendus sur la charge de travail d'une machine virtuelle.

De plus VMware Update Manager applique les correctifs en toute sécurité sur des machines virtuelles hors ligne sans les exposer au réseau, ce qui limite le risque de non-conformité et de survenue de problèmes de sécurité au sein de l'environnement de production.

L'application de correctifs à des machines virtuelles hors ligne est un processus spécifique aux environnements virtuels, qui garantit des niveaux plus élevés de conformité aux normes relatives aux correctifs que dans les environnements physiques.

5.3.4. Vmware vsphere replication

VSphere Replication est outil permettant la réplication de machines virtuelles d'un emplacement à un autre. Cet emplacement (source ou destination) peut être un serveur ESXi, un cluster ou un Datacenter. On peut donc se protéger d'une panne isolée d'une machine virtuelle, mais aussi d'une panne complète de site.



Pour l'installation, il faut récupérer le fichier OVA sur le site de VMware, il faut l'importer à partir de l'interface de vCenter.

5.4. DevOps

Dans cette partie, nous allons apporter une solution de "provisioning" d'environnements grâce à docker, le but étant que chacun puisse obtenir son propre environnement de travail de façon simple et efficace.
Ces environnements seront des containers docker, managés graphiquement depuis le service jenkins, celui-ci faisait appel à des scripts sh archivés sur git.

Nous disposons d'un serveur Debian 9 stretch (172.16.1.141), accessible en ssh.

```
docker@manager: ~
File  Edit  View  Search  Terminal  Help
docker@manager:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 9.0 (stretch)
Release:        9.0
Codename:       stretch
docker@manager:~$
```

Au cours de ce chapitre, nous allons étudier les différentes étapes de mise en place de ces services ainsi que leur utilisation finale.

5.4.1. Docker

Docker est un produit initialement développé par un ingénieur français, Solomon Hykes. Le produit a été dévoilé en mars 2013. Depuis cette date, Docker est devenu LE soft à la mode ! Nous allons voir à quoi il sert et comment vous pouvez vous en servir au quotidien. Docker permet de créer des environnements (appelés containers) de manière à isoler des services.
Contrairement à une machine virtuelle qui isole tout un système (son OS), et dispose de ses propres ressources, le kernel va partager les ressources du système hôte et interagir avec les containers. Techniquement, Docker n'est pas une VM, pas le moins du monde, mais en terme d'utilisation, Docker peut-être apparenté à une VM.

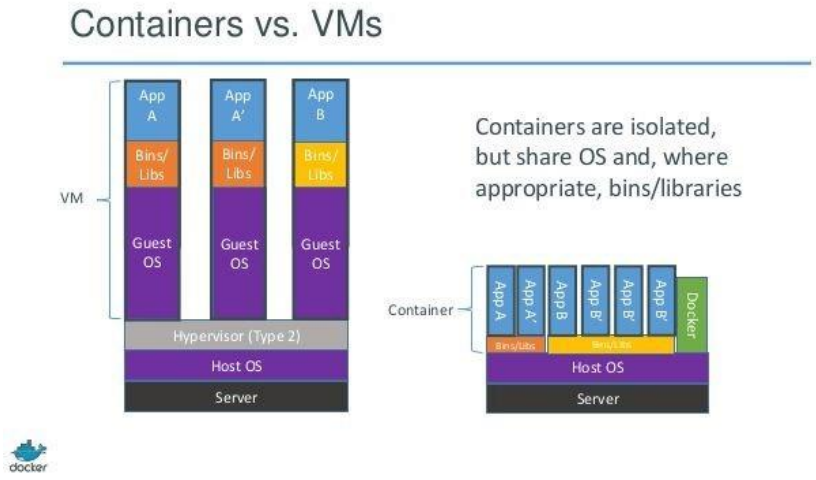
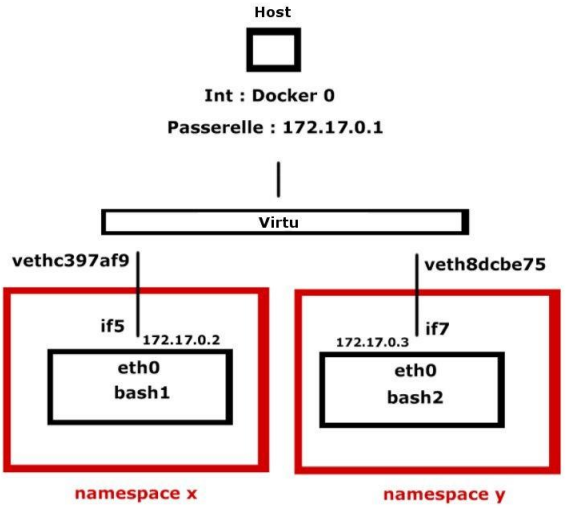


Schéma réalisé par Docker

Le container, qui s'apparente à la VM, s'appuie sur une image docker, qui peut s'apparenter à l'os. A tout moment, un container peut être transformé en images, qui elle servira à créer d'autres containers.

Sur le plan réseau, un container est également le plus souvent isolé dans réseau à part. Par défaut, docker créer une nouvelle interface en bridge sur le réseau 172.17.0.0 /16, qui sera utilisée lors la création d'un nouveau container.

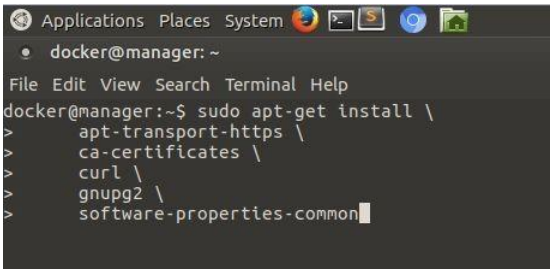
Ce schéma représente deux containers isolés dans le réseau 172.17.0.0

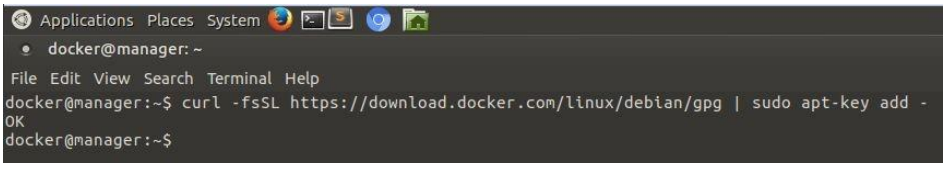


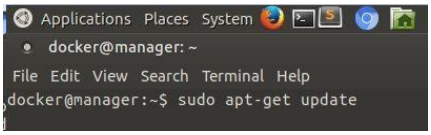
Cependant, il est possible de créer un container qui possède la même configuration réseau que son hôte, ou encore de lui attribuer une ip dans le réseau local en utilisant **Linux Bridge devices ou Open vSwitch**

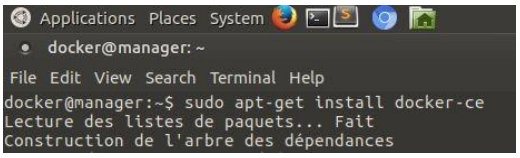
Configuration :

L'installation se fait via gestionnaire de paquet apt







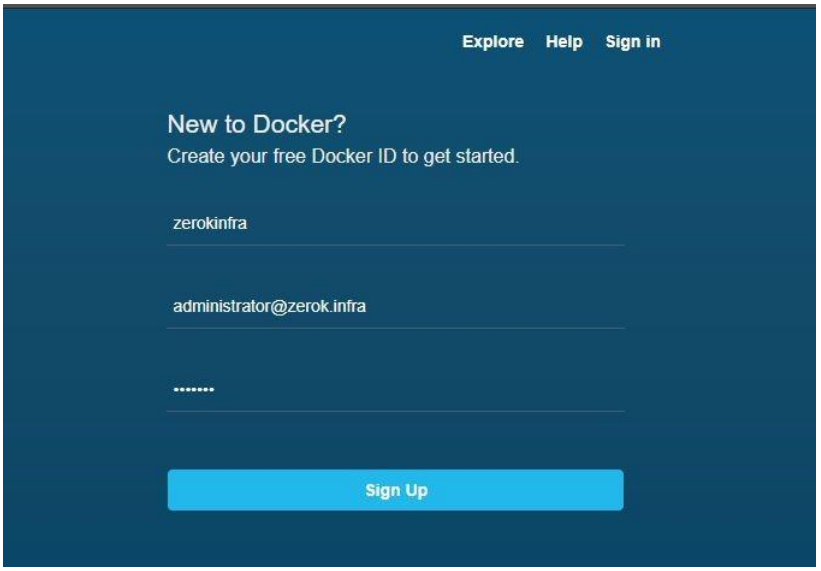


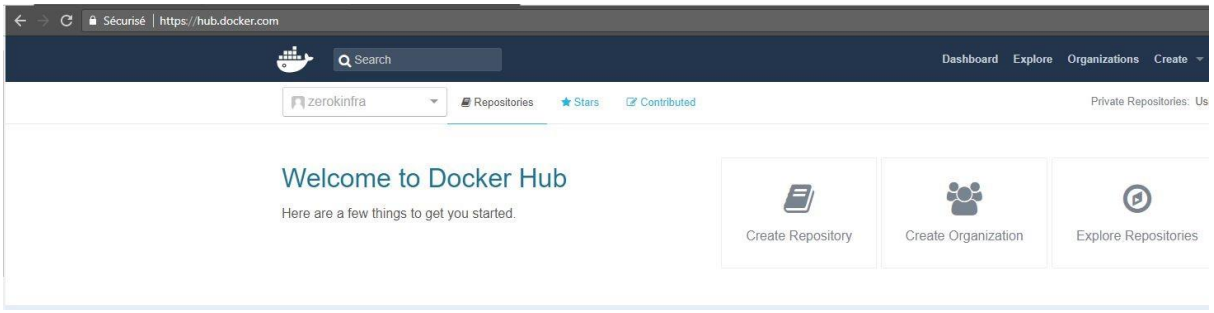
Une fois l'installation terminée, nous allons créer notre propre réseau virtuel. C'est sur ce réseau qu'on lancera nos containers :

```
docker@manager:~$ docker network create --subnet=172.18.0.0/24 docker_network
0e260a97bb68e59847ed93a9e14fe2b6cccbb0726ac87ee60d8d76f9fa55a36b
docker@manager:~$ ip a
```

```
21: br-0e260a97bb68: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:ea:6a:73:be brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/24 scope global br-0e260a97bb68
       valid_lft forever preferred_lft forever
```

Enfin, nous allons créer un compte "zerokinfra" sur le Docker Hub. Docker Hub est le portail de Docker pour poster ses images.





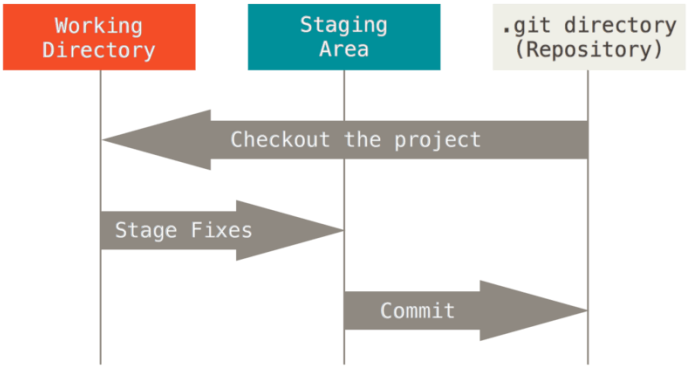
Afin d'automatiser la gestion de nos containers, nous allons créer des scripts sh que nous allons archiver sur le logiciel de gestion de code : git.

5.4.2. Git

Bien qu'il existe à ce jour de nombreuses solutions comme CVS, SVN, Mercurial, Git, etc., Git est devenu incontournable ces dernières années notamment grâce à Github, service web très populaire qui repose sur l'utilisation de Git.

Git a été créé par Linus Torvalds également créateur du noyau Linux.
Le principe est le suivant. Les fichiers versionnés sont mis à disposition sur un dépôt, c'est-à-dire un espace de stockage géré par le logiciel de gestion de versions. Pour pouvoir effectuer des modifications, le développeur doit d'abord faire une copie locale des fichiers qu'il souhaite modifier, ou de tout le dépôt.

Le développeur fait ses modifications et effectue ses premiers tests localement, indépendamment des modifications faites sur le dépôt du fait du travail simultané d'autres développeurs. Il doit ensuite faire un commit (une soumission), c'est-à-dire soumettre ses modifications, afin qu'elles soient enregistrées sur le dépôt.



Ici, Git nous servira à travailler sur les scripts de management des containers Docker, mais pourra par la suite être utilisé pour n'importe quel chantier de développement au sein de la société.

Configuration :

L'installation s'effectue également avec apt:

```
git@manager:~$ sudo apt-get install git
```

Le répertoire du projet sera /data/git/docker

```
root@manager:/home/deploy# mkdir -p /data/git
root@manager:/home/deploy# chown -R git:git /data/git/
```

Nous pouvons également ajouter des utilisateurs au groupe git pour qu'ils possèdent le permissions requises: deploy est un user dédié à la connexion des utilisateurs au serveur

```
git@manager:/var$ sudo usermod -G git deploy
git@manager:/var$ sudo usermod -G git jenkins
```

On peut maintenant initialisé notre repo git

```
git@manager:~$ cd /data/git/docker/
git@manager:/data/git/docker$ git init --bare --shared=group
Dépôt Git vide partagé initialisé dans /data/git/docker/
git@manager:/data/git/docker$
```

Pour récupérer le repository sur sa machine, il suffit de le récupérer par ssh :
git clone ssh://deploy@172.16.1.141/var/git/docker

Exemple depuis un client 172.16.1.142

```
leo@vagrant:~$ mkdir git && cd git
leo@vagrant:~/git$ git clone ssh://deploy@172.16.1.141/data/git/docker
Clonage dans 'docker'...
deploy@172.16.1.141's password:
warning: Vous semblez avoir cloné un dépôt vide.
leo@vagrant:~/git$
```

Ajoutons maintenant notre premier script

```
leo@vagrant:~/git$ mkdir scripts
leo@vagrant:~/git$ vi scripts/get-ip.sh
```

```
#!/bin/bash

sudo su -c "docker inspect --format '{{ .NetworkSettings.IPAddress }}' $1" -s /bin/sh docker
```

```
leo@vagrant:~/git/docker$ git add scripts/
leo@vagrant:~/git/docker$ git status
Sur la branche master

Validation initiale

Modifications qui seront validées :
  (utilisez "git rm --cached <fichier>..." pour désindexer)

        nouveau fichier : scripts/get-ip.sh

leo@vagrant:~/git/docker$
```

```
leo@vagrant:~/git/docker$ git commit -m "script pour recuperer l'ip d'un container"
[master (commit racine) d7c8e8f] script pour recuperer l'ip d'un container
 Committer: leo <leo@debian.zerok.infra>
Votre nom et votre adresse e-mail ont été configurés automatiquement en se
fondant sur votre nom d'utilisateur et le nom de votre machine. Veuillez
vérifier qu'ils sont corrects. Vous pouvez supprimer ce message en les
paramétrant explicitement. Lancez les commandes suivantes et suivez les
instruction dans votre éditeur pour éditer votre fichier de configuration :

    git config --global --edit

Après ceci, vous pouvez corriger l'identité utilisée pour cette validation avec :

    git commit --amend --reset-author

 1 file changed, 4 insertions(+)
 create mode 100644 scripts/get-ip.sh
leo@vagrant:~/git/docker$
```

```
leo@vagrant:~/git/docker$ git push origin master
deploy@172.16.1.141's password:
Décompte des objets: 4, fait.
Compression des objets: 100% (2/2), fait.
Écriture des objets: 100% (4/4), 353 bytes | 0 bytes/s, fait.
Total 4 (delta 0), reused 0 (delta 0)
To ssh://172.16.1.141/data/git/docker
 * [new branch]      master -> master
```

Pour la partie sh, les scripts seront synchronisés sur git pour être utilisé sur Jenkins.

5.4.3. Jenkins

Jenkins est un outil très apprécié des entreprises dans le cadre de l'intégration continue. Il peut également être une solution très pratique pour réaliser des builds ponctuels, et ainsi automatiser et centraliser différentes tâches de scripting.

Configuration :

Installation via apt :

```
jenkins@manager:~$ wget -q -O - https://pkg.jenkins.io/debian/jenkins-ci.org.key | sudo apt-key add -
OK
jenkins@manager:~$ ll
```

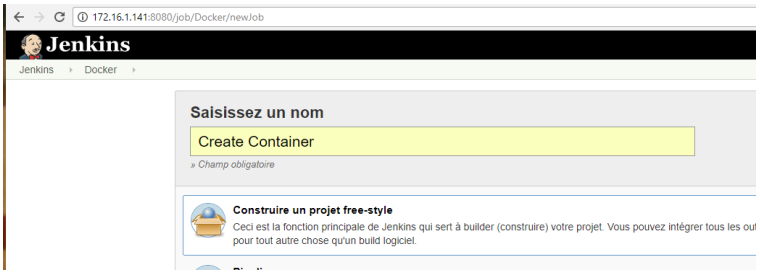
```
jenkins@manager:~$ sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
jenkins@manager:~$
```

```
jenkins@manager:~$ sudo apt-get update
Ign:1 http://ftp.fr.debian.org/debian stretch InRelease
Atteint:2 http://ftp.fr.debian.org/debian stretch-updates InRelease
Atteint:3 http://security.debian.org/debian-security stretch/updates InRelease
Atteint:4 http://ftp.fr.debian.org/debian stretch Release
Ign:5 http://pkg.jenkins.io/debian-stable binary/ InRelease
Atteint:6 https://download.docker.com/linux/debian stretch InRelease
Réception de:7 http://pkg.jenkins.io/debian-stable binary/ Release [2 042 B]
Réception de:9 http://pkg.jenkins.io/debian-stable binary/ Release.gpg [181 B]
Réception de:10 http://pkg.jenkins.io/debian-stable binary/ Packages [12,5 kB]
14,7 ko réceptionnés en 0s (26,6 ko/s)
Lecture des listes de paquets... Fait
jenkins@manager:~$ sudo apt install -y jenkins
```

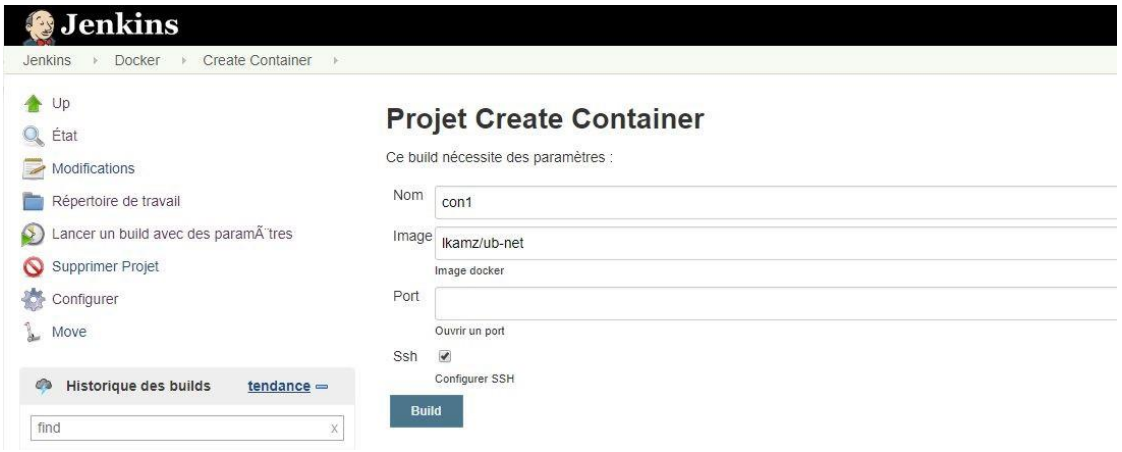
Nous disposons maintenant de notre interface web par défaut sur le port 8080

5.4.4. Jenkins et scripts bash

Création d'un container :



Création d'un container :



Notre premier job permet la création d'un container.
Il faut indiquer son nom, l'image docker a utiliser, d'éventuels ports à ouvrir. Et s'il faut réaliser la configuration ssh.

Le script ssh de création de container sera ensuite exécuté avec les différents paramètres

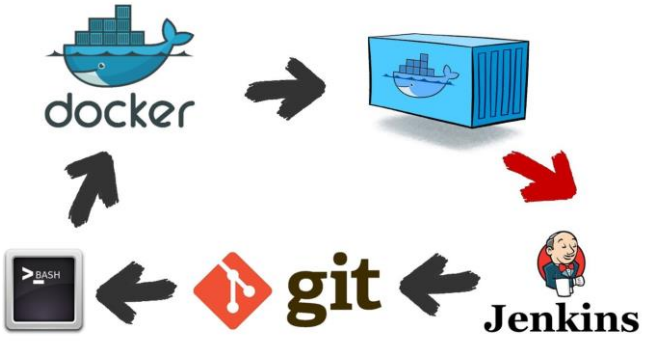
Voici le script create-container.sh qui a été push sur git

```
Applications Places System
jenkins@manager: ~/git/docker/scripts
File Edit View Search Terminal Help
#!/bin/bash

#sudo su -c 'docker inspect --format \'{{ .NetworkSettings.IPAddress }}\' "$@"' -s /bin/sh docker
#sudo su -c "docker inspect --format '{{ .NetworkSettings.IPAddress }}' $1" -s /bin/sh docker

echo "Création du container :"
echo "---"

#S'il n'y a que le port 22 à rattacher
if [ $1 -eq 0 ]; then
    sudo su -c "docker run -d -expose=22 --network=bridge --name=$2 -ti $3 /bin/bash" -s /bin/sh docker
else
    #on cherche un port non utilisé sur l'hote
    p_sup=50000
    for check in $(sudo netstat -ntpul | grep $p_sup); do
        if [[ $check == '' ]]; then
            echo "check:"$check
        else
            let "p_sup++"
        fi
    done;
    sudo su -c "docker run -d -expose=22 -p $p_sup:$4 --network=bridge --name=$2 -ti $3 /bin/bash" -s /bin/sh docker
fi;

printf "\n\n\n\n\n"
echo "Informations du container :"
echo "Nom = $2"
echo "Image = $3"
echo "Ip = $(./get-ip.sh $2)"
echo "New port = $4 -> $p_sup"
echo "Connexion au container :"
echo "ssh root@$(./get-ip.sh $2)"
echo "Pwd : root"
printf "\n\n\n\n\n"

sudo su -c "docker exec -ti $2 sed -i 's/PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config" -s /bin/sh docker
sudo su -c "docker exec -ti $2 bash -c '(echo root; sleep 3; echo root) | passwd'" -s /bin/sh docker
sudo su -c "docker exec -ti $2 /etc/init.d/ssh start"
~
```

Les autres jobs jenkins qui ont été mis en place sont les suivant :

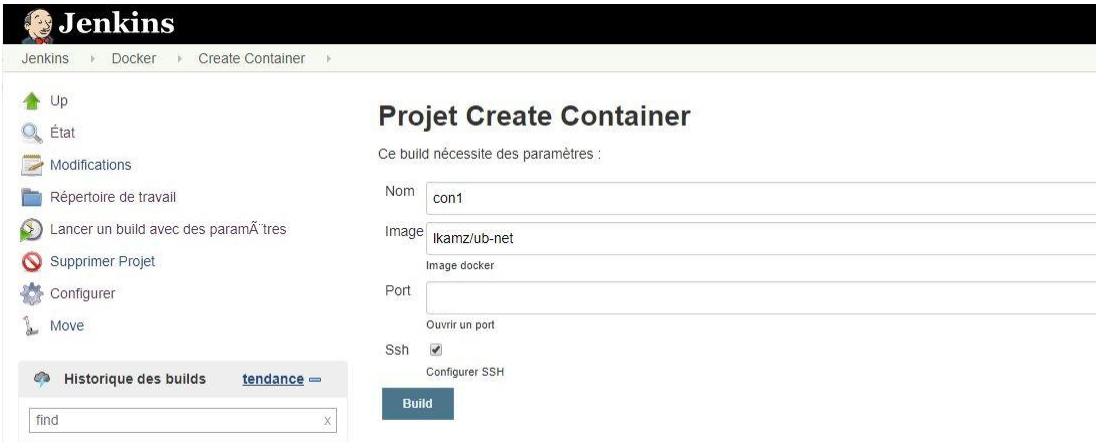
- lister toutes les images docker présentes en local
- lister tous les containers actifs
- lister tous les containers actifs ou non
- supprimer un container
- transformer un container en image
- envoyer son image sur le docker hub

Voici une maquette qui résume très brièvement notre modèle :

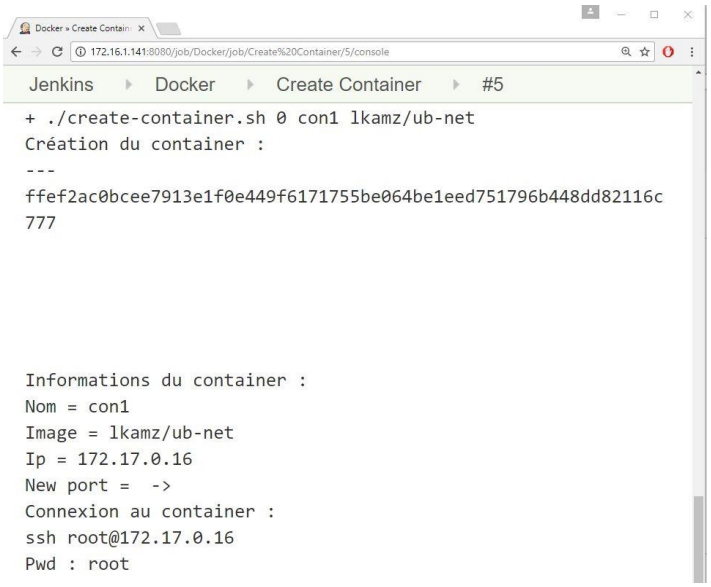


5.4.5. Démonstration

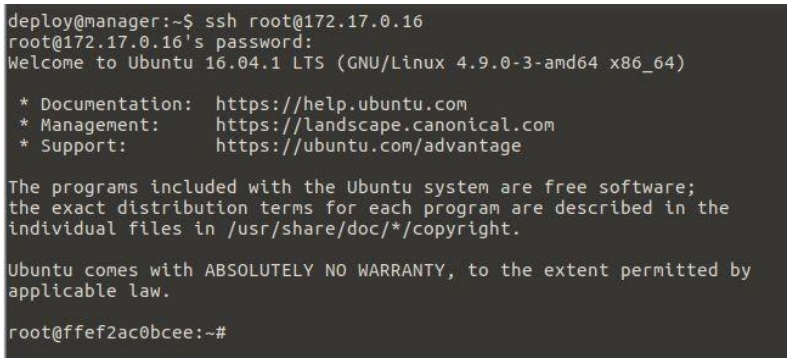
Un utilisateur souhaite créer un container faisait tourner une image locale d'ubuntu 16.04 faisant tourner ssh.



Il récupère les informations générées par le job

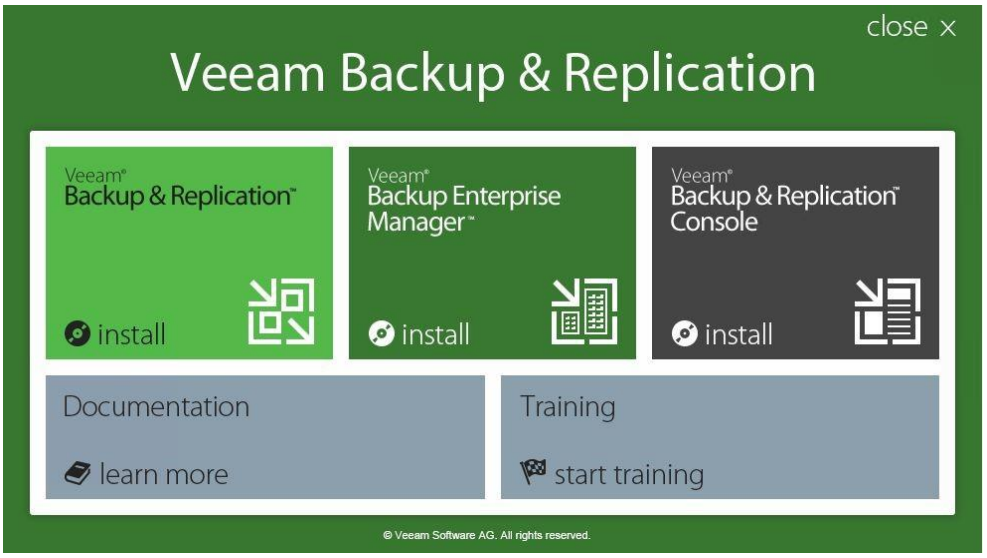


Il n'a plus qu'à se connecter en ssh



6. INFRASTRUCTURE DE SAUVEGARDE

6.1. VEEAMBACKUP REPLICATION



On ne peut pas avoir une infrastructure informatique virtualisée sans penser à une solution de backup fiable et performante qui nous permet de restaurer ou de garantir la disponibilité et l'intégrité de nos données. Veeam est l'un des meilleur logiciels qui en plus des fonctionnalités de sauvegardes, il permet aussi la déduplication des données, l'exclusion des blocs de disque virtuel, de fichiers et de volumes de disques inutiles.

Veeam est un des leaders de la sauvegarde de machines virtuelles. Elle propose entre autres les fonctionnalités suivantes :

- Sauvegarder, copier ou exporter une VM à chaud (sans interruption de service)
- Restaurer des fichiers de VM (disque virtuel, etc…) ou des fichiers contenus dans les OS (ex : fichiers Windows)
- Compatibilité VMware et Hyper-v
- Gestion des systèmes de stockage NAS/SAN et des librairies de bandes.
- Des outils comme Veeam Explorer : permet de naviguer au travers d'applications Windows (ex : Active Directory, Exchange) et de restaurer des objets uniques (ex: Comptes utilisateurs, groupes de sécurités, courriers électroniques, etc…).

- La migration à chaud d'une machine virtuel d'un hyperviseur vers un autre (Par exemple si la fonctionnalité vMotion n'est pas disponible)
- Dans notre situation, le logiciel Veeam Backup sera installé sur le serveur DC, pour ne pas utiliser plus de ressources concernant le reste du projet.

6.2. BACKUP EXEC

Pour la solution de sauvegarde nous avons choisie Backup Exec. Référence absolue en matière de protection des données Windows, Symantec Backup Exec pour Windows Servers assure des sauvegardes de disque à disque à bande certifiées et des restaurations rapides et efficaces. Grâce à la technologie de restauration granulaire en cours d'homologation et à la protection continue des données des applications stratégiques Microsoft, les données de l'entreprise sont protégées en permanence et facilement récupérables.

- Protection totale des données dans les environnements serveurs Windows
- Intégration multi-produits innovante avec des technologies de pointe
- La technologie de restauration granulaire en cours d'homologation permet de récupérer les données des applications critiques en quelques secondes
- La protection continue des données élimine la fenêtre de sauvegarde en protégeant les données au fur et à mesure qu'elles changent

7. ENVIRONNEMENT TECHNIQUE

Dans notre datacenter, nous allons louer une baie afin de pouvoir stocker notre materiels de virtualisation et de stockage.

Pour nos Esxi et notre vCenter nous allons utiliser un châssis qui possèdent les caractéristiques suivantes :

- Châssis Dell M1000e
- 3 x Lame : M620 150 Gb ram et 8 CPU - Liaison par ISCSI

Le stockage est assuré par deux serveurs de stockage avec les caractéristiques suivantes :

- Compellent : sc220

-2 Contrôleur

-PowerVault MD1400

Des Switches est dédié au réseau de stockage et au réseau pour les contrôleurs.
Quatre baies pour les serveurs, les switches, le serveur de stockage et le brassage.

7.1. ONDULEURS

Pour des raisons de stabilité, deux onduleurs supportant la salle serveur seront mis en place dans les deux sites.

En cas de coupure de l'alimentation générale et en attendant le relai du générateur électrique, l'activité doit continuer. Pour cela, des onduleurs seront placés.

7.2. STOCKAGE SAN/NAS

Pour le stockage ainsi que pour les serveurs de fichier nous avons choisi de centraliser avec un Compellent**.**

Un boîtier SAS 6 Gbit/s au format 2U prenant en charge jusqu'à 24 disques durs 2,5" ou des options « tout-Flash » ou Flash hybrides permettant un large choix d'options de stockage dans un seul châssis.

- Prise en charge de disques durs à 7 200, 10 000 et 15 000 tr/min et de disques SSD de 200 Go2, de 400 Go2 et de 1,6 To2.
- Modèle SC220 optimisé Flash avec micrologiciel Storage Center 6.4 pouvant hiérarchiser dans une seule solution des disques SSD équipés de cellules SLC à écriture intensive et de cellules MLC à lecture intensive hautes capacités (moins chères).
- Capacités maximales de 24 To2 par boîtier d'extension.

De plus pour ajouter plus de stockage, nous allons utiliser un DAS “Dell Storage MD1400” :

7.3. BAIE

Baie 42U 19’ 200 x 80 x 80

Baie standard pour serveur et réseau

8. PRA

Le Plan de Reprise d'Activité intervient seulement en cas de sinistre, comme par exemple un incendie dans un local contenant des routeurs, des serveurs …

Pour mettre en place un PRA, il faut répliquer tous les serveurs sur un site distant, pour pouvoir récupérer les configurations et les données dans des situations pareilles.

Pour permettre un Plan de Reprise d'Activité, notre choix s'est porté sur la solution suivante:

VMware vCenter Site Recovery Manager, il s'agit de créer un site distant de recours avec une automatisation de plan de reprise rapide et fiable et une limitation de perte de données.

9. VOLET FINANCIER

Désignation	Prix	Qte	Prix * Qte
Licence anti virus	1 050,00€	2	2 100,00€
Support /5 ans	1 500,00€	2	3 000,00€
Total : 5100,00€ H.T			
Total : 6120.00€			
Cœur de réseau :			
Désignation	Prix	Qte	Prix * Qte
Pfsense	0,00€	4	0,00€
Boitier	590,00€	4	2 360,00€
Support /5 ans	200,00€	2	4 000,00€
Total : 6360,00€ H.T			
Total : 7632.00€			
Antivirus :			
Désignation	Prix	Qte	Prix * Qte
Licence Serveur	0,00€	1	0,00€
Licence Utilisateur	40,00€	120	4 800,00€

Total : 4800,00€			
Switch :			
Désignation	Prix	Qte	Prix * Qte
Switch Cisco 2960-X 48	6 995,00€	8	55 960,00€
Cisco FlexStack plus Network stacking module	1 195,00€	8	9 560,00€
Stack T1 1M	200	8	1 600,00€
Support /5 ans	2 500,00€	8	20 000,00€
Total : 103392.00€			
FAI :			

Désignation	Prix	Qte	Prix * Qte
Lan to Lan 100Mo/mois	1 300,00€	8	10 400,00€
Sortie Internet 20Mo/mois	1 000,00€	4	4 000,00€
Total : 17280.00€			
Poste de travail :			
Désignation	Prix	Qte	Prix * Qte
Unité centrale (Avec OS intégré)	300,00€	800	320 000,00€

Ecran	125,00€	800	100 000,00€
Clavier, souris	50,00€	800	40 000,00€
Office Professional 2016	400,00€	800	200 000€
Total : 660000,00€			
Cables réseaux :			
Désignation	Prix	Qte	Prix * Qte
Câble RJ45 cat 6 3M	3,00€	800	2 400,00€
Câble RJ45 cat 6 5M	4,39€	100	439,00€
Câble RJ45 cat 6 10M	7,37€	25	184,25€
Cable RJ45 cat 6 20M	12,43€	25	310,75€
Total : 3333,00€			
Salle serveur :			
Désignation	Prix	Qte	Prix * Qte
Gros œuvre	33 000,00€	1	33 000,00€
Faux plancher	3 500,00€	1	3 500,00€
Courant forts	30 000,00€	1	30 000,00€
Alimentation sans interruption	7 840,00€	1	7 840,00€
Climatisation	32 000,00€	1	32 000,00€
Protection incendie	13 750,00€	1	13 750,00€

Baie et câblage	10 000 €	1	10 000,00€
Total : 130 090,00€ H.T			
Total : 156 108,00€			
Supervision :			

Désignation	Prix	Qte	Prix Total
Debian 7.8.0	0,00€	1	0,00€
Syslog	0,00€	1	0,00€
Apache 2.2.22	0,00€	1	0,00€
MySQL 14.14	0,00€	1	0,00€
ELK	0,00€	1	0,00€
Total : 0,00€			
OwnCloud :			

Désignation	Prix	Qte	Prix Total
OwnCloud (Serveur : 9.0 et Client : 2.2)	0,00€	1	0,00€
Apache 2.2.22	0,00€	1	0,00€
MySQL 14.14	0,00€	1	0,00€
Total : 0,00€			

Messagerie :			
Désignation	Prix	Qte	Prix Total
Licence Windows Server 2016 STD	776,00€	2	1 552,00€
Licence Exchange 2016 STD Server	171,00€	1	171,00€
Licence Exchange Standard User CAL	30,00€	120	3 600,00€
Certificat QuickSSL Premium chez GeoTrust	149,00€/an	3 ans	372,00€
Total : 5869,50€			
Coût infrastructure réseau sur 5 ans :			
Désignation	Prix		
Pfsense	3 816,00€		
Trend Micro Office	4 800,00€		
Switch	42 165,00€		
Orange	198 000,00€		
Poste de travail	136 680,00€		
Cablage	1 594,00€		
Salle serveur	156 108,00€		

Messagerie	6 000,00€		
Sous total réseau : 549 166,00€			
TOIP et SYSLOG :			
Désignation	Prix	Qte	Prix Total
Debian 9	0,00€	10	0,00€
Ossec	0,00€	1	0,00€
PRTG	2 580,00€	2000 Capteurs	2 580,00€
Serveur Syslog	0,00€	1	0,00€
Licence annuelle Splunk de 10 Gb/jour	1 035,71€	1	1 035,71€
Total : 3615,71€			
Désignation	Prix	Qte	Prix Total
Téléphones IP - Tiptel 3010	74,84€	800	59 872,00€
Pieuvres – Polycom IP 6000	459,51€	50	22 975.5€
Total : 82847,5€			
Virtualisation :			
Désignation	Prix	Qte	Prix Total
Licence Virtualisation : vSphere 6.5	26 421,00 €	1	26 421,00 €

Windows Server 2016 Datacenter	3 700,00 €	5	18 500,00 €
M1000e	8 441,00€	2	24 918,00 €
Lames M620	8 340,00€	4	33 360,00€
Total : 103 199,00€			
Stockage :			
Désignation	Prix	Qte	Prix Total
Compellent SC220	1 503,00€	2	3 006,00€
MD1400	8 890€	2	17 780€
Total : 20 786,00€			
Sauvegarde :			
Désignation	Prix	Qte	Prix Total
Backup Exec	3 277,00€	6	19 662,00 €
VeeamBackup Entreprise	1 900 €	1	1 900,00 €
Total : 21 562,00 €			
Autres :			
Désignation	Prix	Qte	Prix Total
Baie 42U 200x80x80	750,00€	4	3 000,00 €
Onduleurs 450 VA	9 000,00 €	2	18 0000,00 €
Total : 21 000,00 €			

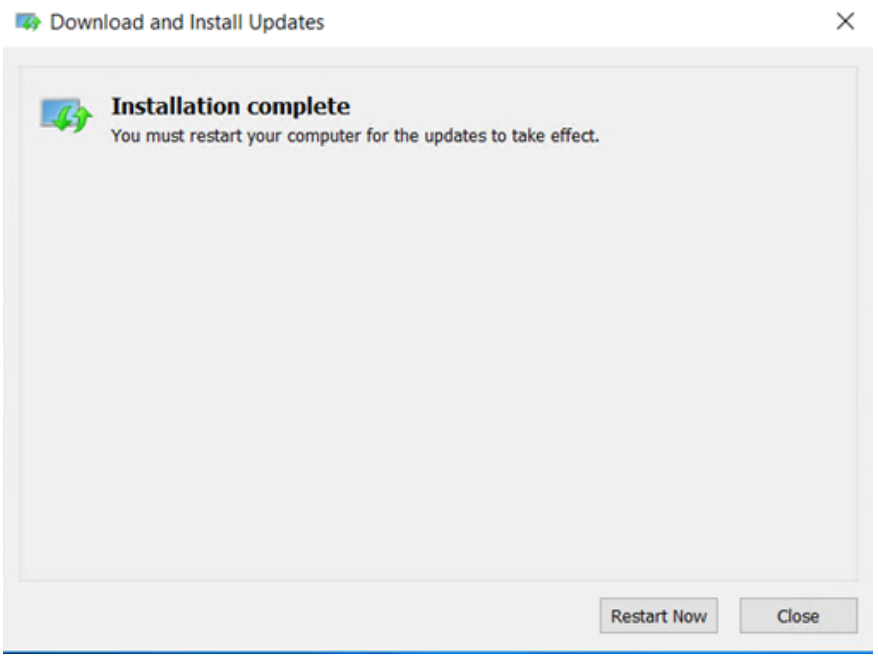
10. ANNEXES

10.1. Mise en place du serveur Exchange

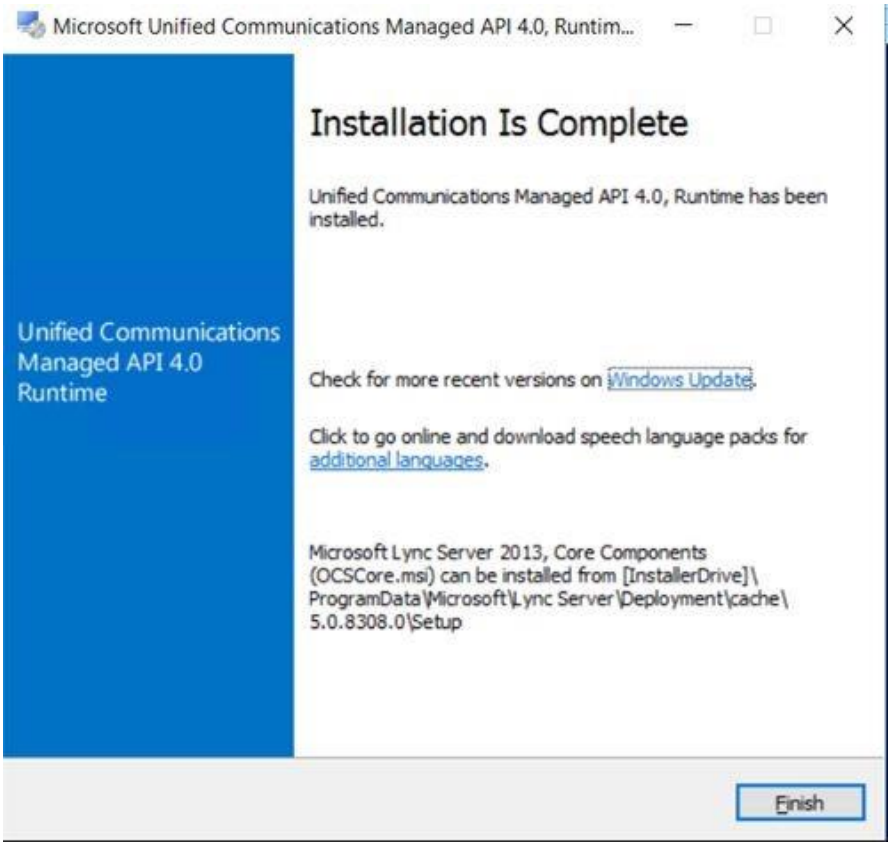
Prérequis :
- 8 Go de RAM
- 10 Go d'espace libre sur le disque dur
- Mise à jour KB3206632
- Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit
- ISO Exchange 2016

Installation :

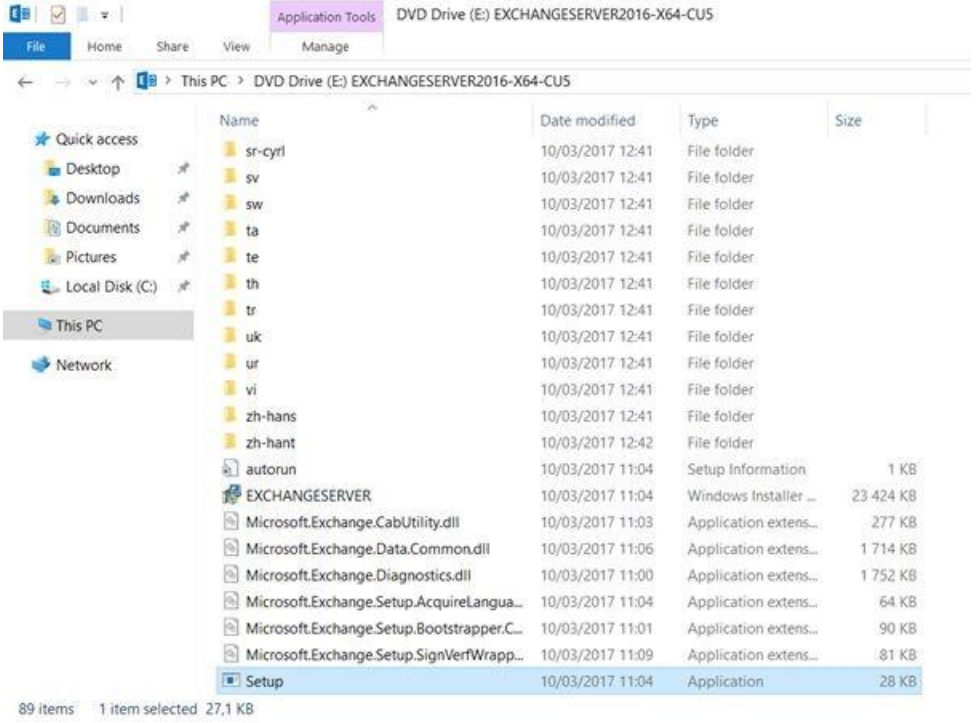
On se connecte en VPN sur l'infrastructure via OpenVPN, puis on lance le bureau à distance sur le 172.16.1.12 avec l'identifiant et mot de passe administrateur du domaine. On commence par installer la mise à jour KB3206632 avec le setup (téléchargé depuis le catalogue Windows):

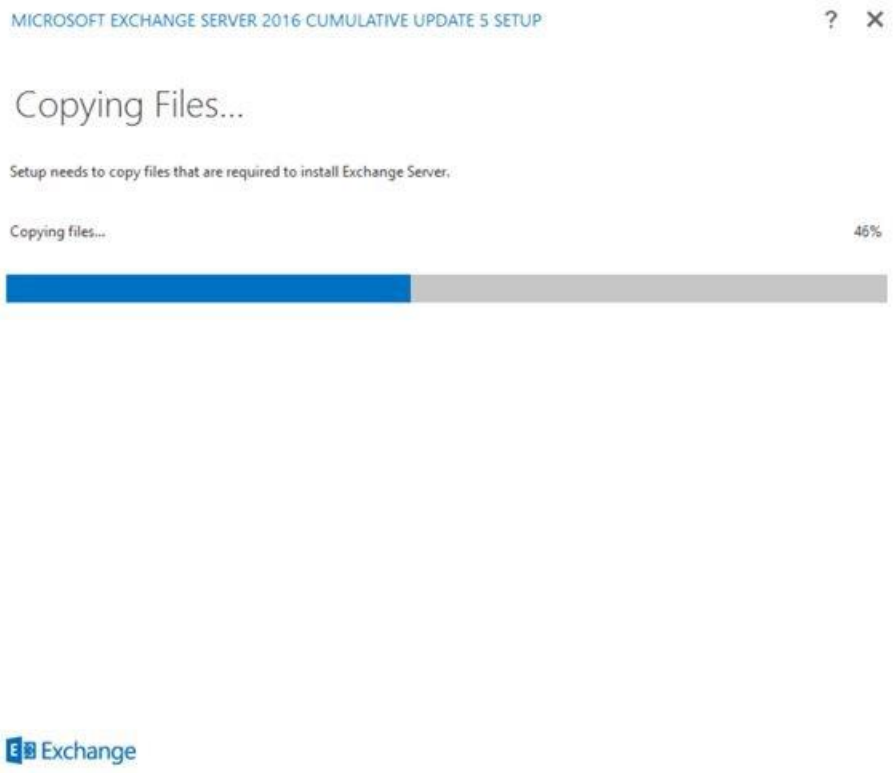


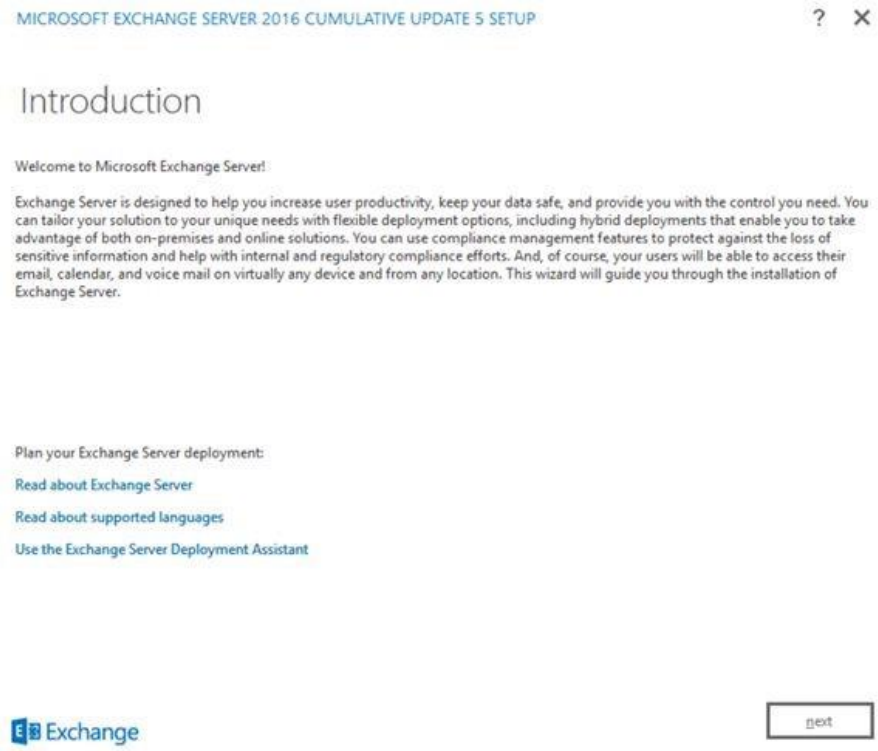
Une fois la mise à jour KB3206632 installée et le serveur redémarré, on lance l'installation de MUCM API 4.0 via le setup (téléchargé sur le site Windows) :

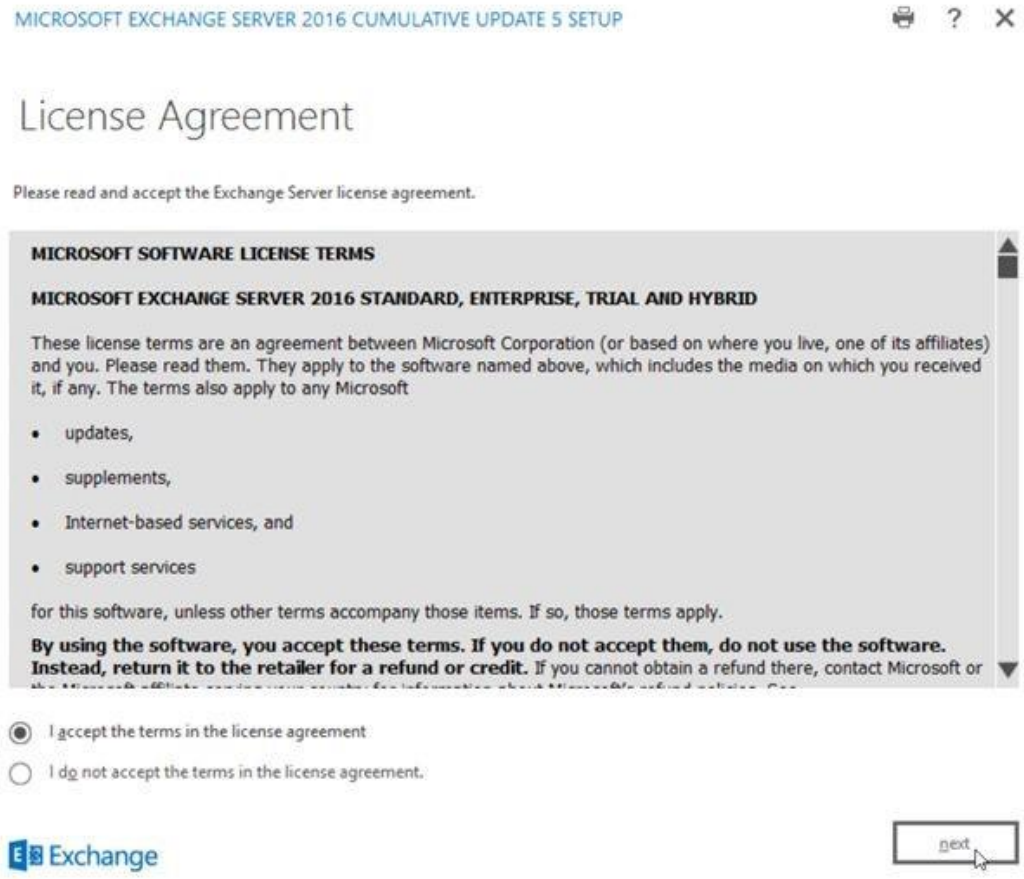


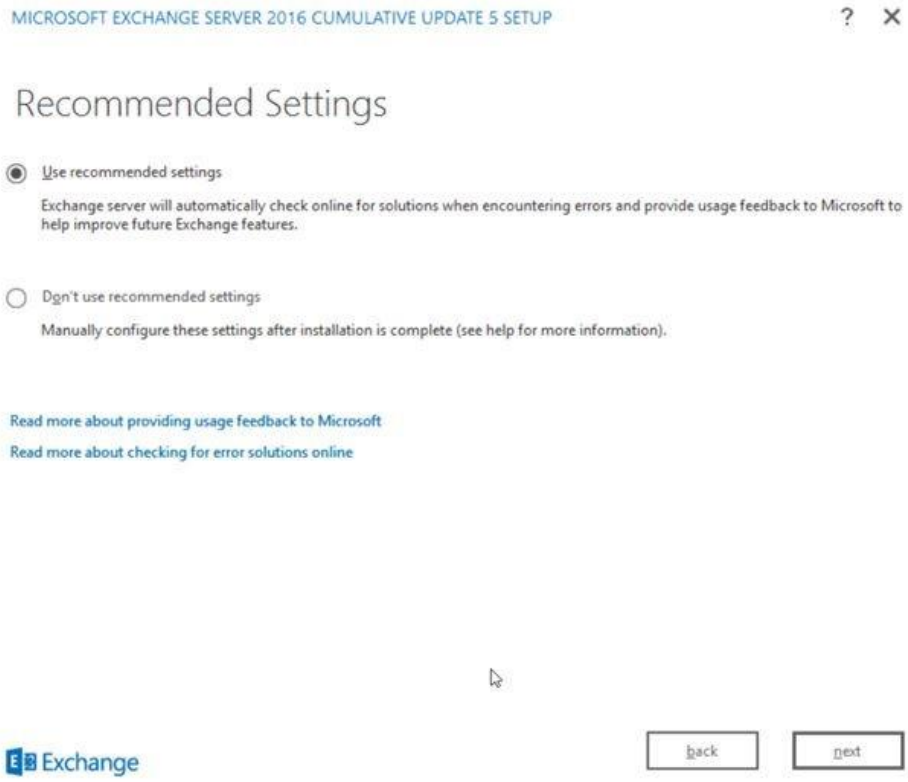
Une fois cette installation effectuée, on va dans l'ISO Exchange 2016 pour lancer le Setup :

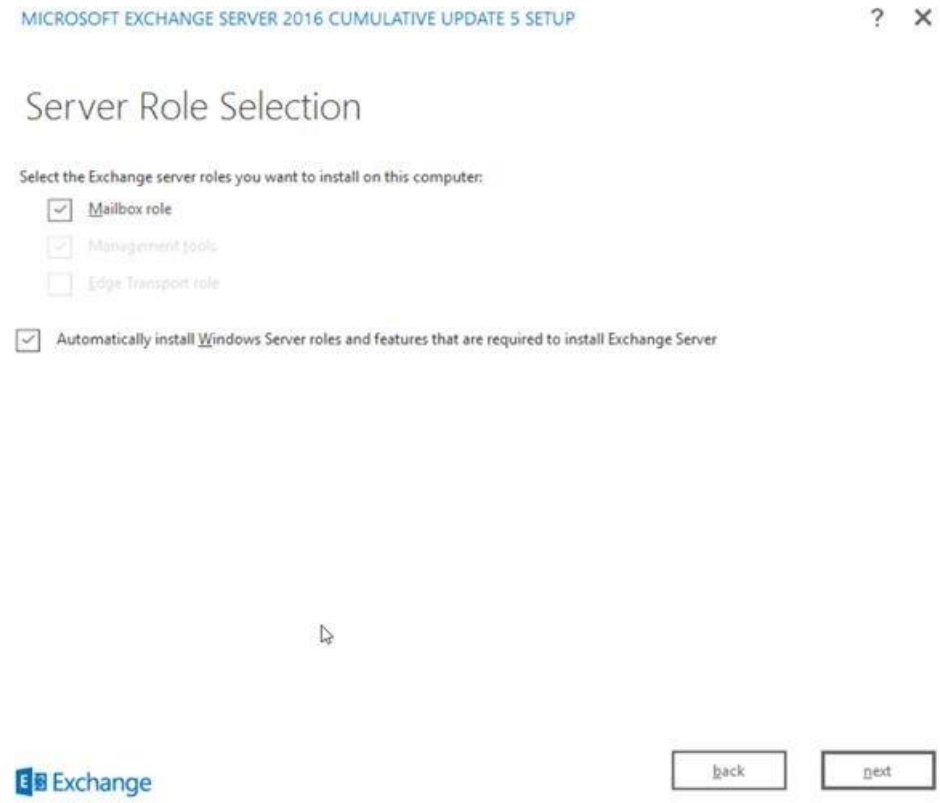


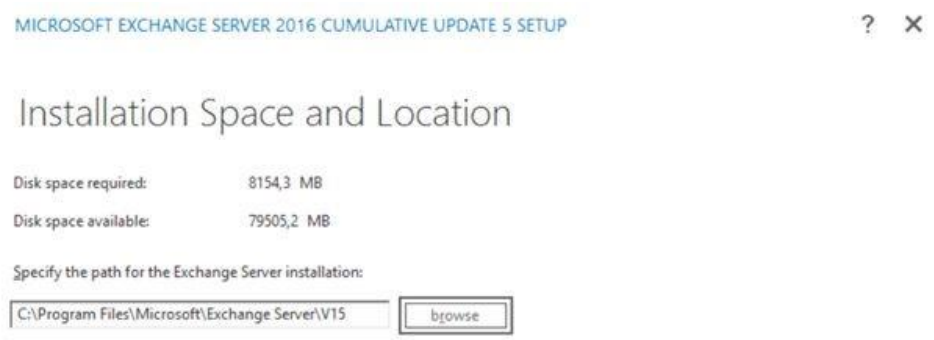

MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Copying Files...
Setup needs to copy files that are required to install Exchange Server.
Copying files...
46%
Exchange


MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Introduction
Welcome to Microsoft Exchange Server!
Exchange Server is designed to help you increase user productivity, keep your data safe, and provide you with the control you need. You can tailor your solution to your unique needs with flexible deployment options, including hybrid deployments that enable you to take advantage of both on-premises and online solutions. You can use compliance management features to protect against the loss of sensitive information and help with internal and regulatory compliance efforts. And, of course, your users will be able to access their email, calendar, and voice mail on virtually any device and from any location. This wizard will guide you through the installation of Exchange Server.
Plan your Exchange Server deployment:
Read about Exchange Server
Read about supported languages
Use the Exchange Server Deployment Assistant
Exchange
next

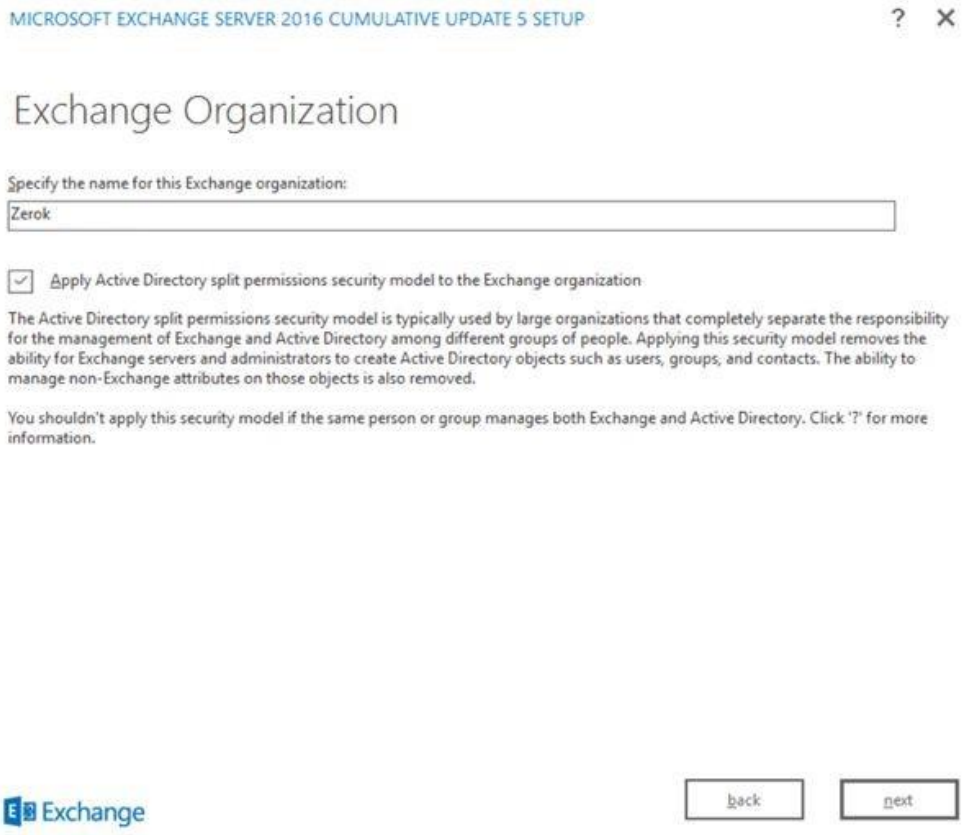

MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
License Agreement
Please read and accept the Exchange Server license agreement.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT EXCHANGE SERVER 2016 STANDARD, ENTERPRISE, TRIAL AND HYBRID
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
updates,
supplements,
Internet-based services, and
support services
for this software, unless other terms accompany those items. If so, those terms apply.
By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or
I accept the terms in the license agreement
I do not accept the terms in the license agreement.
Exchange
next

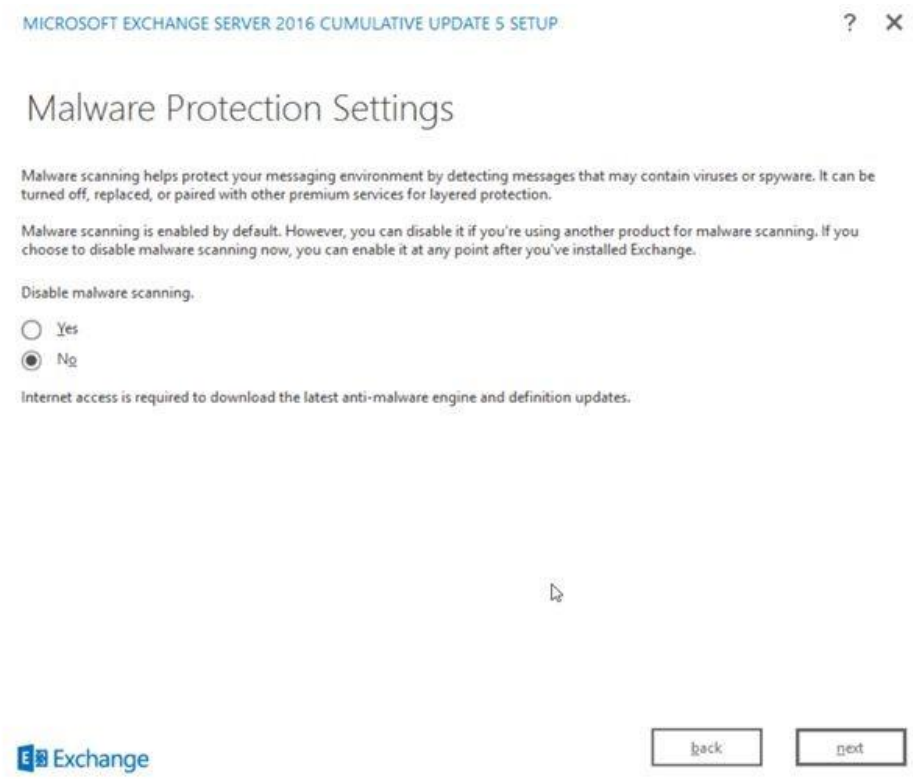

MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Recommended Settings
Use recommended settings
Exchange server will automatically check online for solutions when encountering errors and provide usage feedback to Microsoft to help improve future Exchange features.
Don't use recommended settings
Manually configure these settings after installation is complete (see help for more information).
Read more about providing usage feedback to Microsoft
Read more about checking for error solutions online
Exchange
back
next

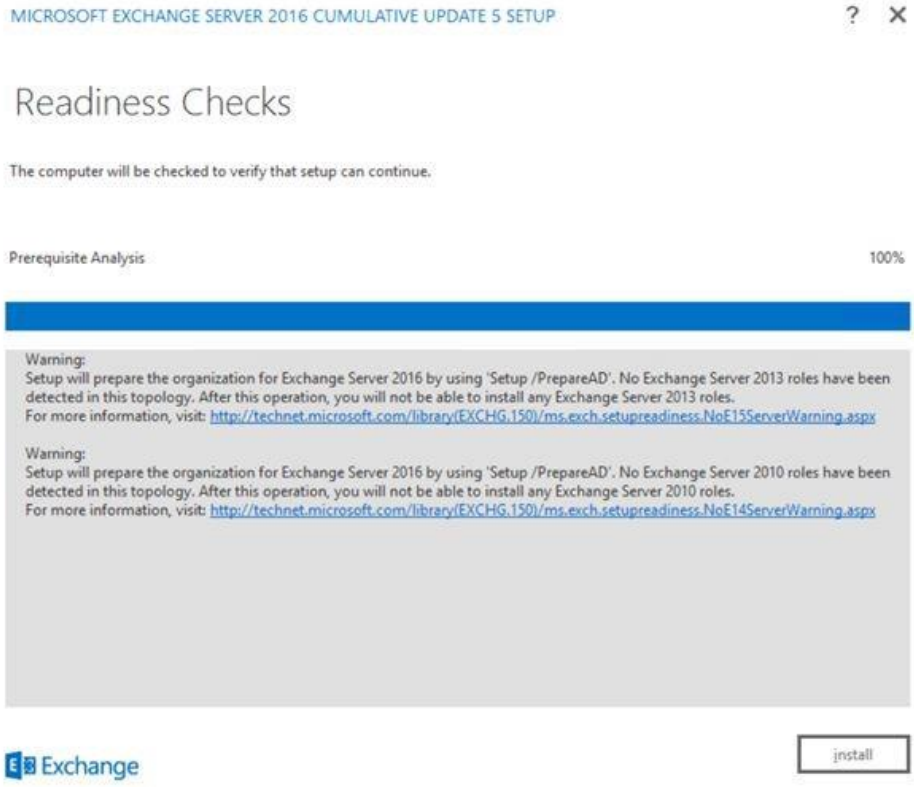

MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Server Role Selection
Select the Exchange server roles you want to install on this computer:
Mailbox role
Management tools
Edge Transport role
Automatically install Windows Server roles and features that are required to install Exchange Server
Exchange
back
next

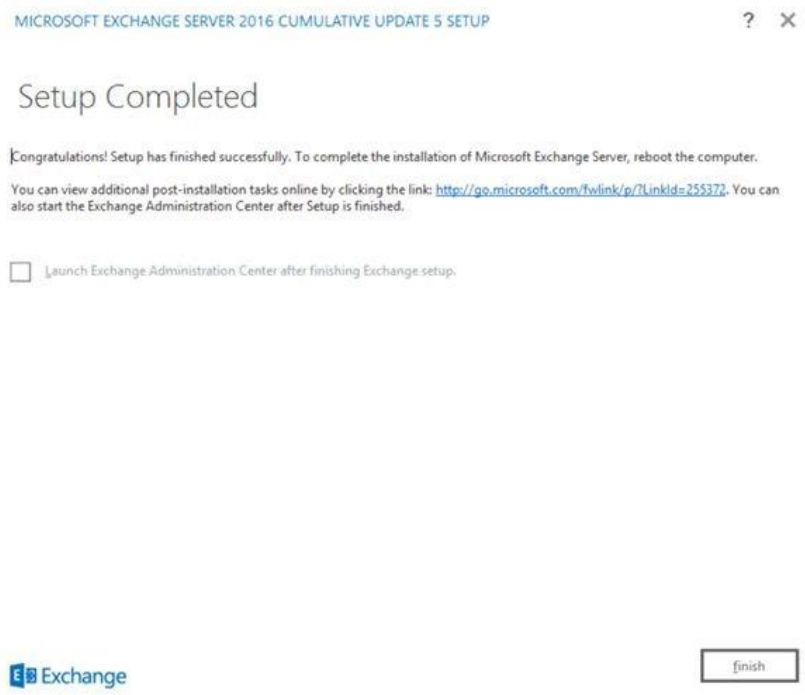

MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Installation Space and Location
Disk space required: 8154,3 MB
Disk space available: 79505,2 MB
Specify the path for the Exchange Server installation:
C:\Program Files\Microsoft\Exchange Server\V15
browse


Exchange
back
next

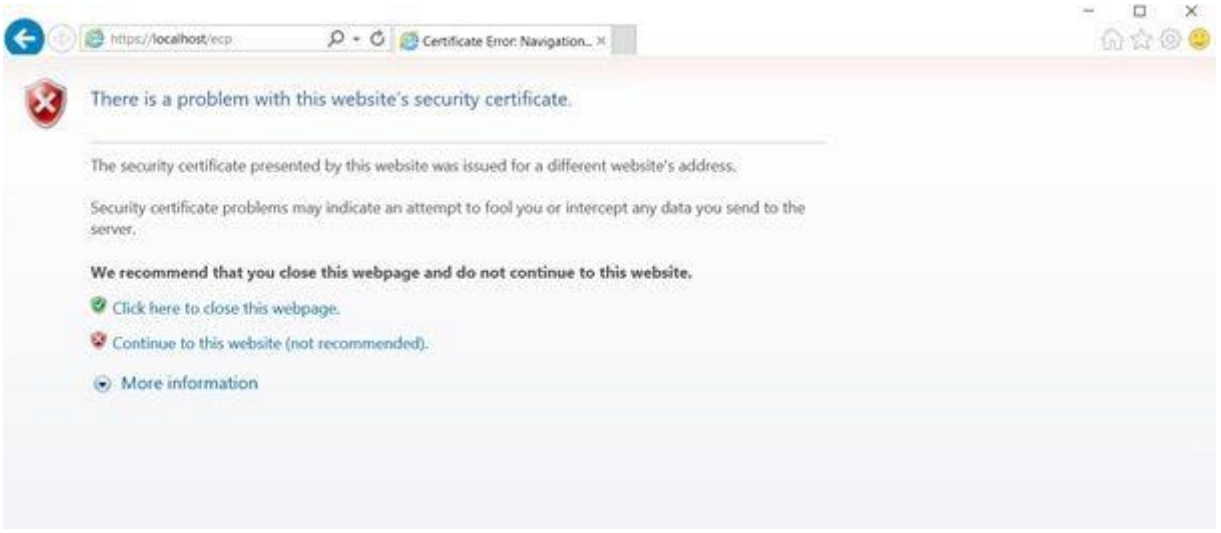

MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Exchange Organization
Specify the name for this Exchange organization:
Zerok
Apply Active Directory split permissions security model to the Exchange organization
The Active Directory split permissions security model is typically used by large organizations that completely separate the responsibility for the management of Exchange and Active Directory among different groups of people. Applying this security model removes the ability for Exchange servers and administrators to create Active Directory objects such as users, groups, and contacts. The ability to manage non-Exchange attributes on those objects is also removed.
You shouldn't apply this security model if the same person or group manages both Exchange and Active Directory. Click '?' for more information.
Exchange
back
next


MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Malware Protection Settings
Malware scanning helps protect your messaging environment by detecting messages that may contain viruses or spyware. It can be turned off, replaced, or paired with other premium services for layered protection.
Malware scanning is enabled by default. However, you can disable it if you're using another product for malware scanning. If you choose to disable malware scanning now, you can enable it at any point after you've installed Exchange.
Disable malware scanning.
Yes
No
Internet access is required to download the latest anti-malware engine and definition updates.
Exchange
back
next

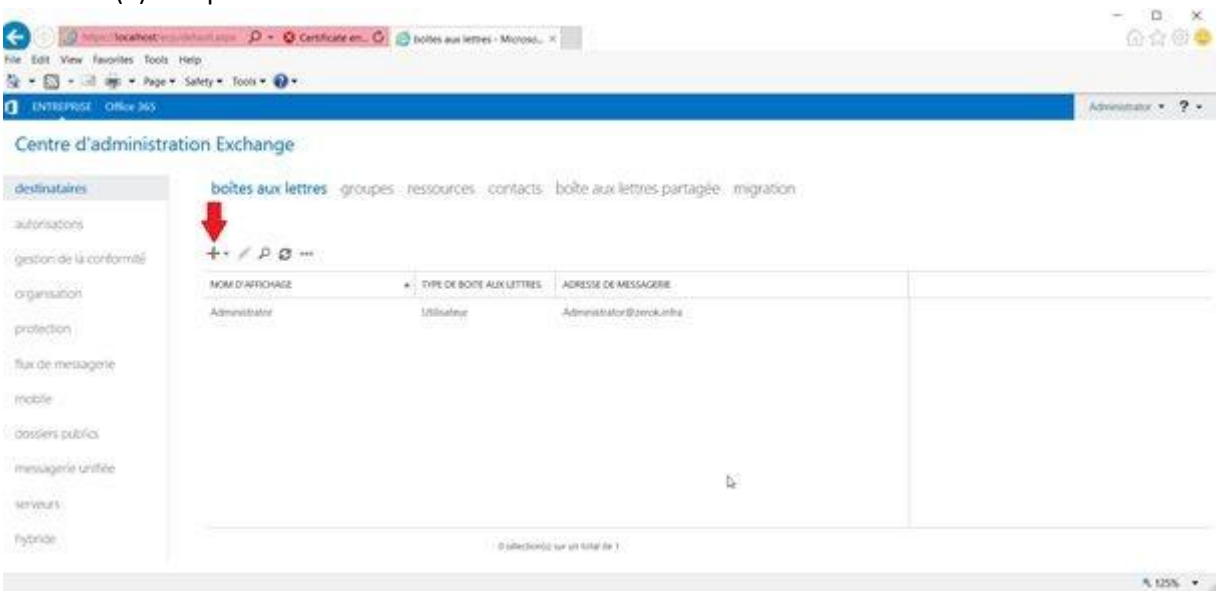

MICROSOFT EXCHANGE SERVER 2016 CUMULATIVE UPDATE 5 SETUP
Readiness Checks
The computer will be checked to verify that setup can continue.
Prerequisite Analysis
100%
Warning:
Setup will prepare the organization for Exchange Server 2016 by using 'Setup /PrepareAD'. No Exchange Server 2013 roles have been detected in this topology. After this operation, you will not be able to install any Exchange Server 2013 roles.
For more information, visit: http://technet.microsoft.com/library(EXCHG.150)/ms.exch.setupreadiness.NoE15ServerWarning.aspx
Warning:
Setup will prepare the organization for Exchange Server 2016 by using 'Setup /PrepareAD'. No Exchange Server 2010 roles have been detected in this topology. After this operation, you will not be able to install any Exchange Server 2010 roles.
For more information, visit: http://technet.microsoft.com/library(EXCHG.150)/ms.exch.setupreadiness.NoE14ServerWarning.aspx
Exchange
install

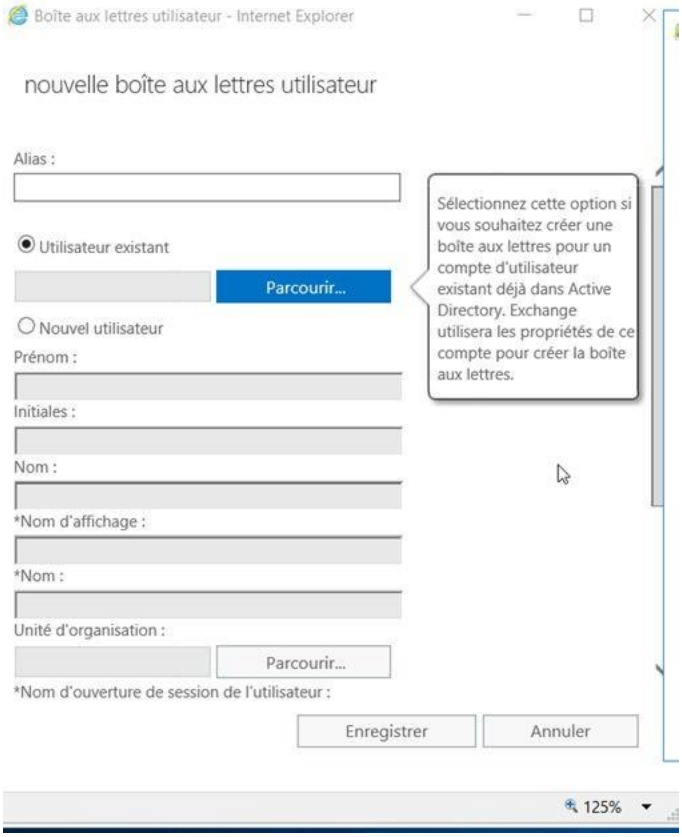


Une fois l'installation terminé, on redémarre le serveur et on démarre les services exchange (via le gestionnaire de serveur si cela n'est pas déjà fait) puis l'on se connecte sur notre interface d'administration exchange via le navigateur web



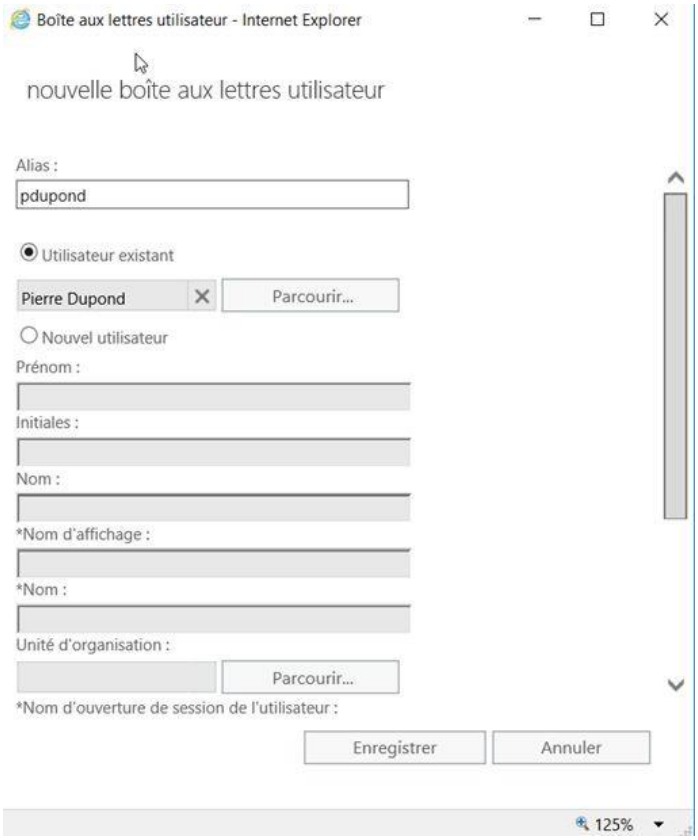
Une fois la connexion effectuée et la page d'accueil chargé, nous allons configurer un utilisateur de l'AD via l'icône (+) indiquée ci-dessous

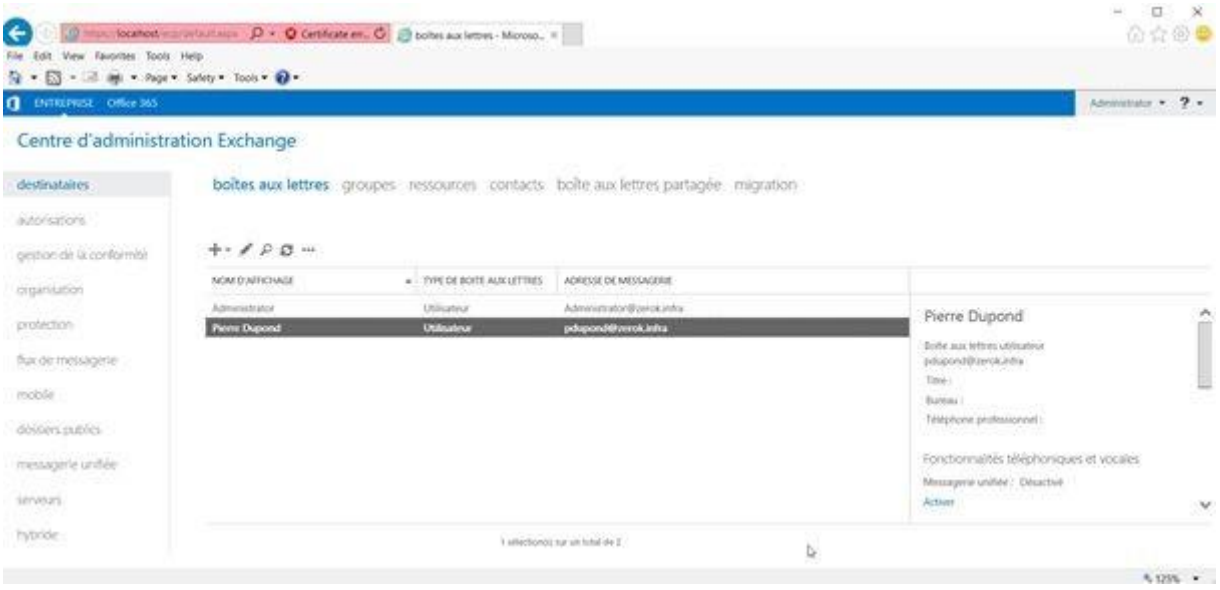




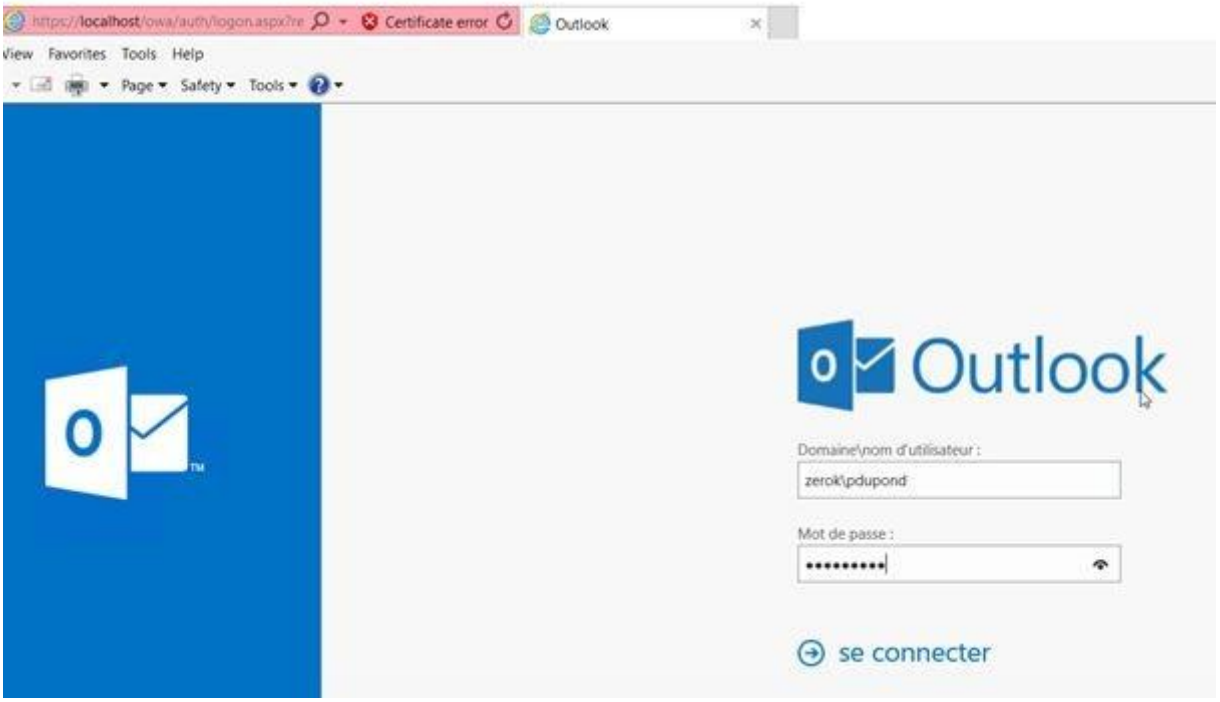
On clique sur **« Parcourir »**

Voici notre utilisateur présent dans l'AD

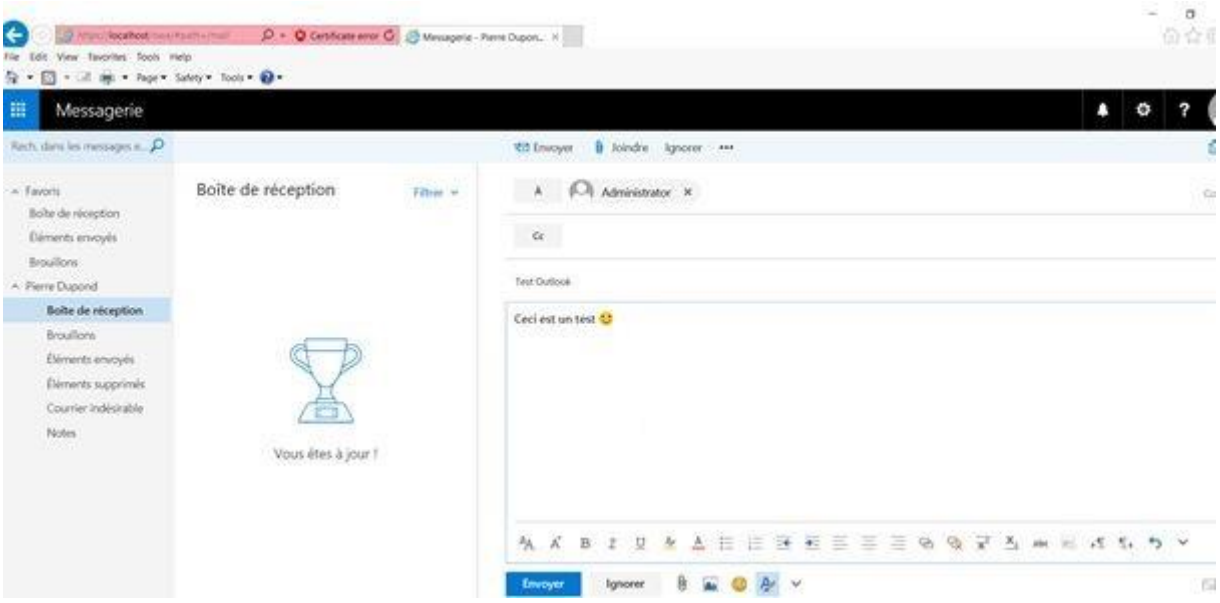


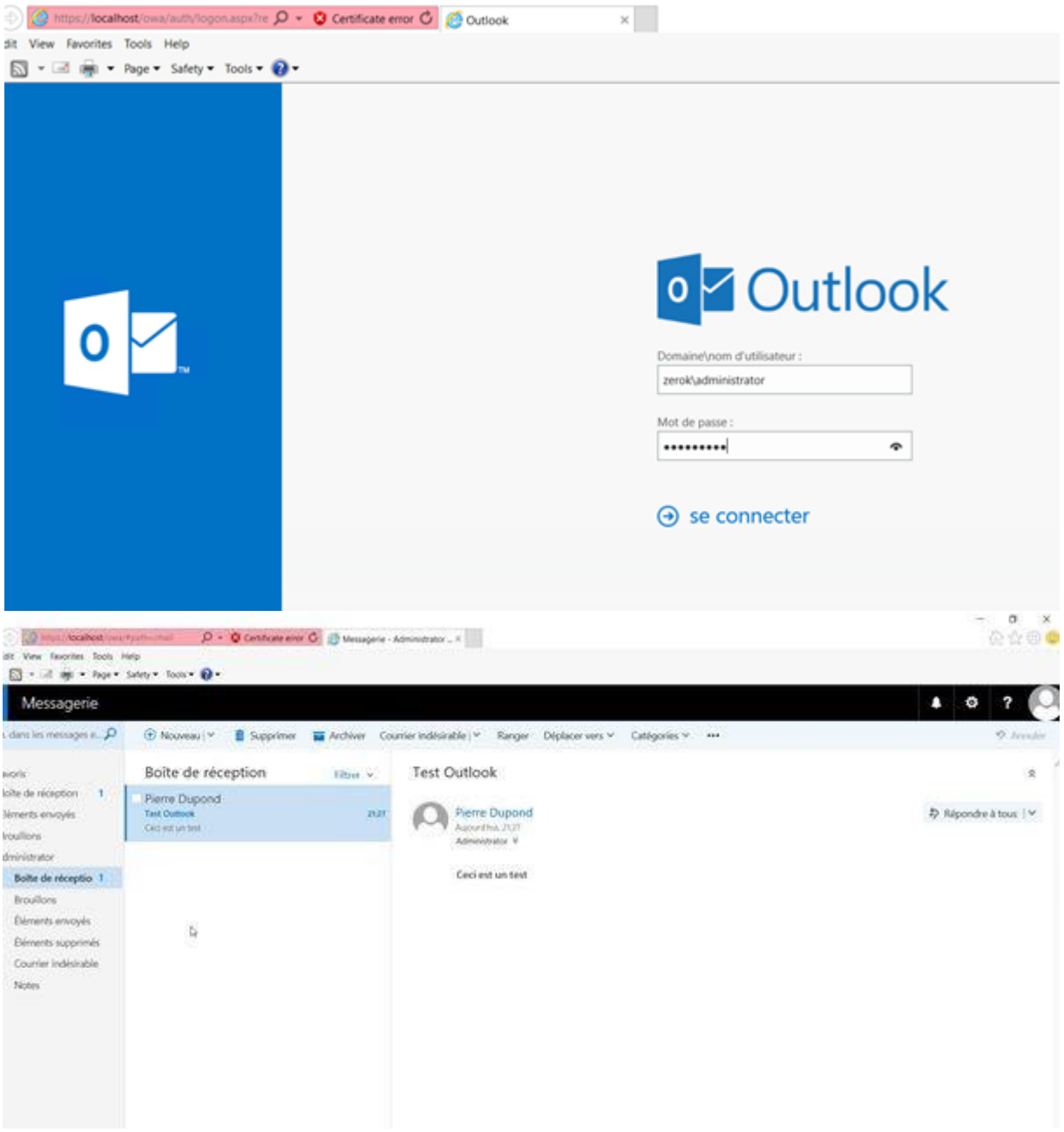


Voici Pierre Dupond qui apparaît, afin d'effectuer un test on va se déconnecter de l'interface administrateur pour se reconnecter avec Pierre Dupond (via l'URL https://localhost/ et non https://localhost/ecp) :

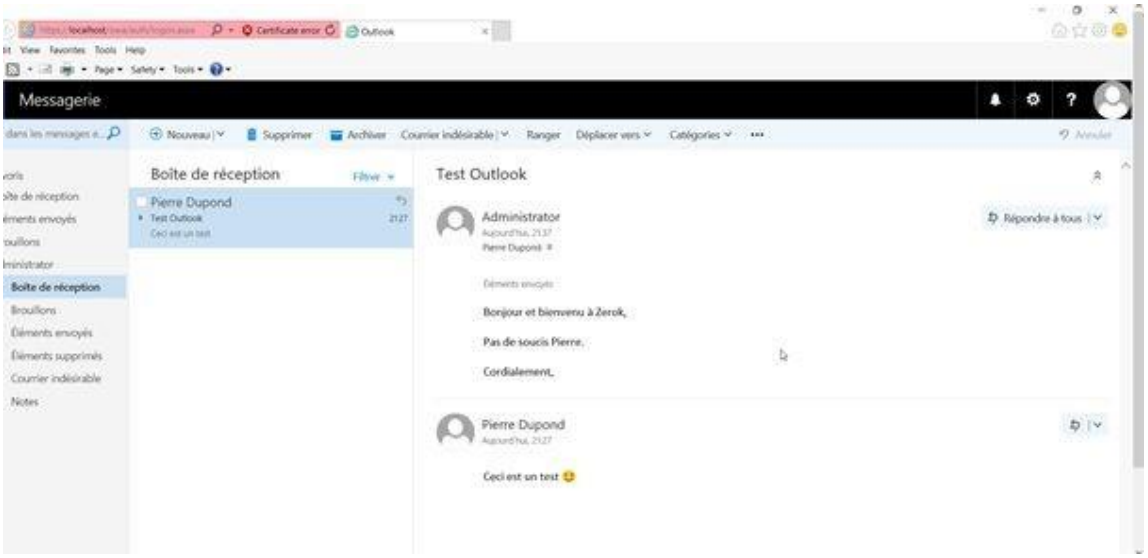


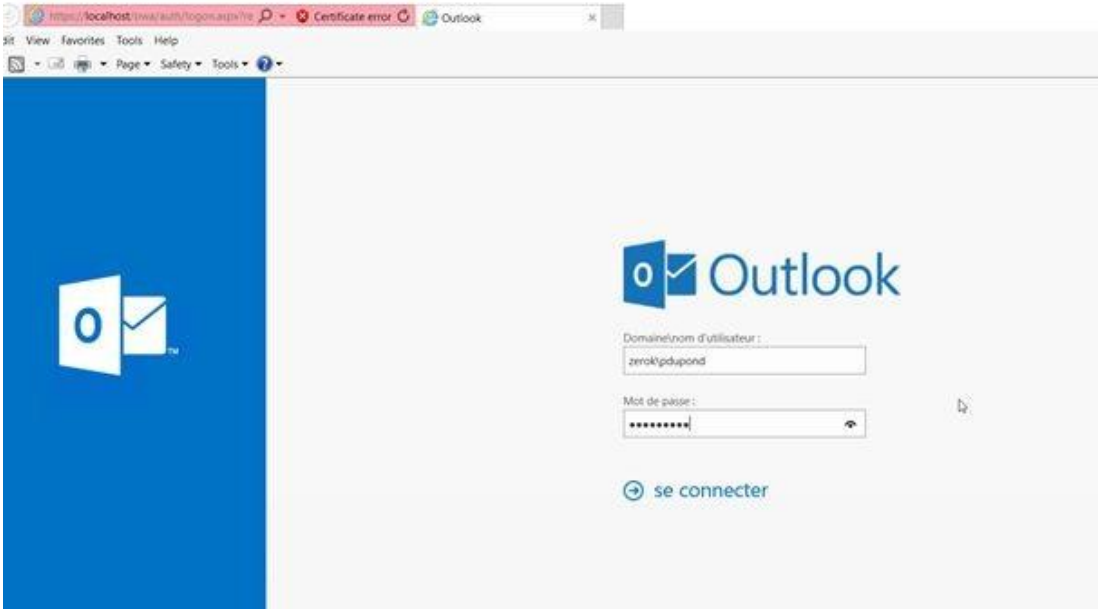
Une fois connecté, nous allons voir si nous arrivons à joindre l'administrateur par mail :

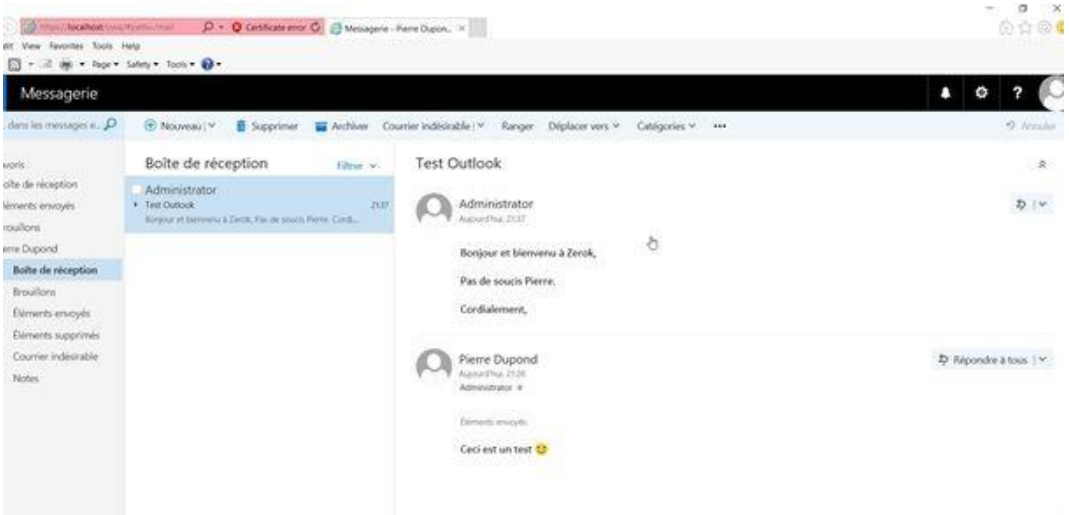




Le message arrive bien à destination ! Voyons désormais si l'inverse est possible lorsque l'administrateur répond :


Messagerie
Boîte de réception
Test Outlook
Pierre Dupond
Test Outlook
Administrator
Répondre à tous
Bonjour et bienvenu à Zerok,
Pas de soucis Pierre.
Cordialement,
Pierre Dupond
Ceci est un test
Boîte de réception
Brouillons
Éléments envoyés
Éléments supprimés
Courrier indésirable
Notes


Outlook
Domaine\nom d'utilisateur :
zerok\pdupond
Mot de passe :
se connecter


Messagerie
Boîte de réception
Test Outlook
Administrator
Bonjour et bienvenu à Zerok,
Pas de soucis Pierre.
Cordialement,
Pierre Dupond
Répondre à tous
Ceci est un test

Effectivement le message parvient à destination ! Notre serveur exchange est donc opérationnel !

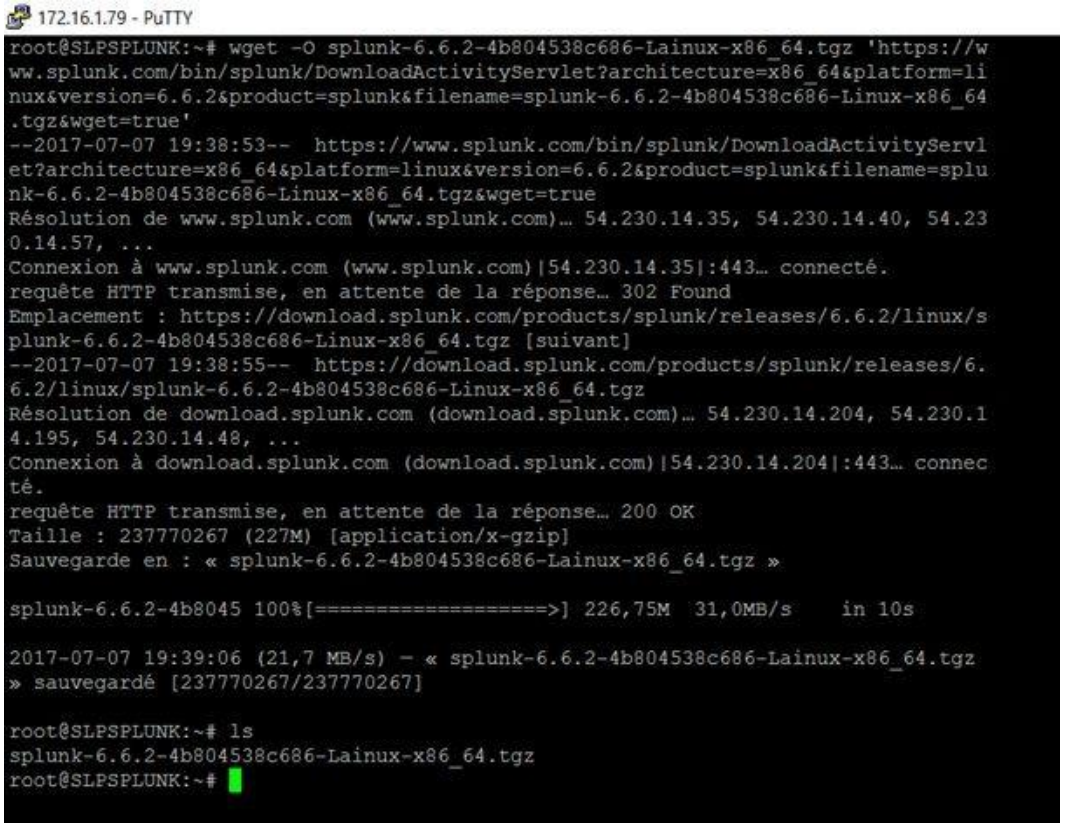
10.2. Mise en place du serveur Splunk

Prérequis :
- Machine virtuelle sous Debian
- Compte Splunk

Il faut au préalable créer un compte sur le site web de Splunk, une fois cette étape réalisée, nous pouvons installer Splunk :
On se connecte sur notre infrastructure avec OpenVPN, puis on lance Putty pour se connecter sur la machine virtuelle faisant office de serveur Splunk (172.16.1.79) en SSH

On fait un **wget -O splunk-6.6.2-4b804538c686-Lainux-x86_64.tgz**

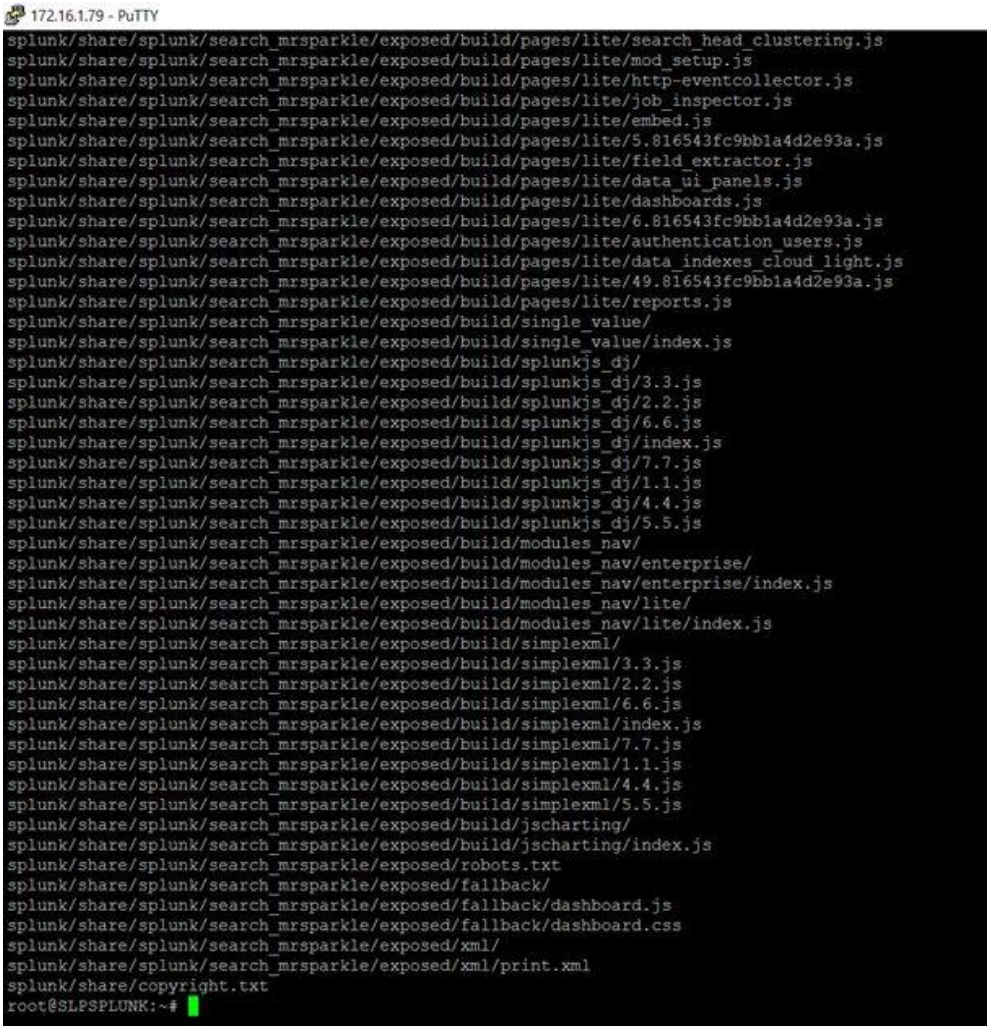
'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=6.6.2&product=splunk&filename=splunk-6.6.2-4b804538c686-Linux-x86_64.tgz&wget=true'



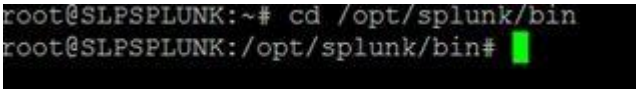
Si on fait un **ls** on voit bien le fichier **.tgz** à décompresser

On tape ensuite la commande : **tar xvzf splunk-6.6.2-4b804538c686-Lainux-x86_64.tgz -C /opt**

Une fois l'installation terminé on obtient cela :



On tape par la suite : **cd /opt/splunk/bin** pour nous rendre dans le dossier d'installation

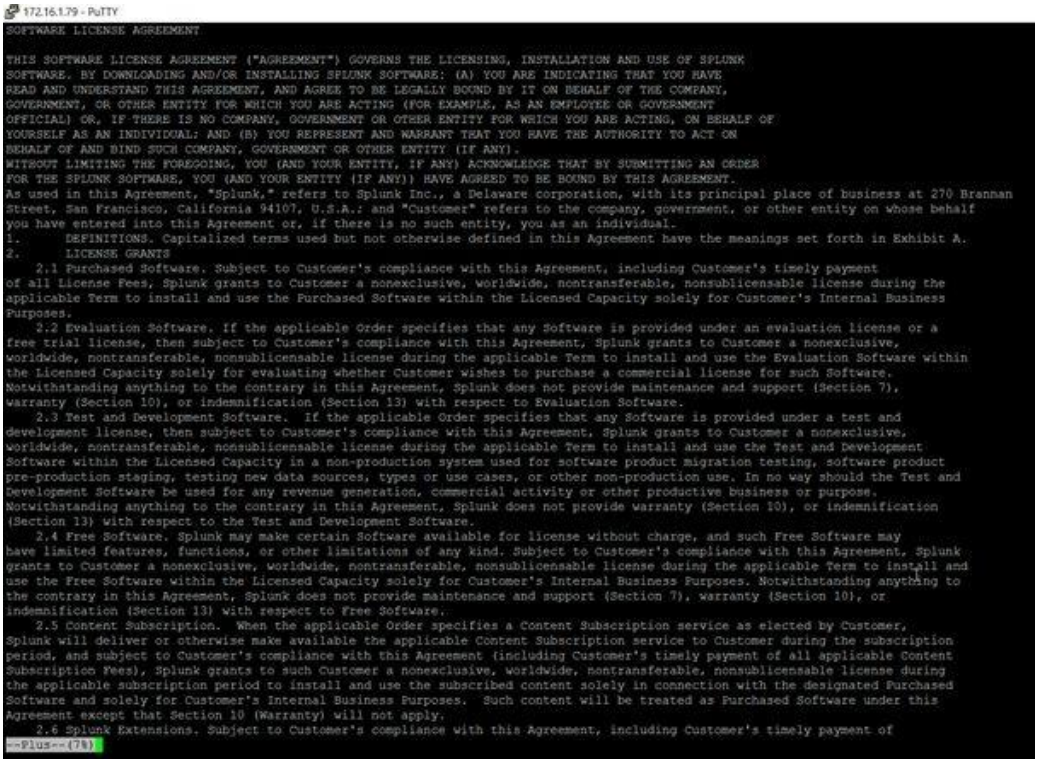


Voici les trois commandes principales pour lancer ou arrêter Splunk :

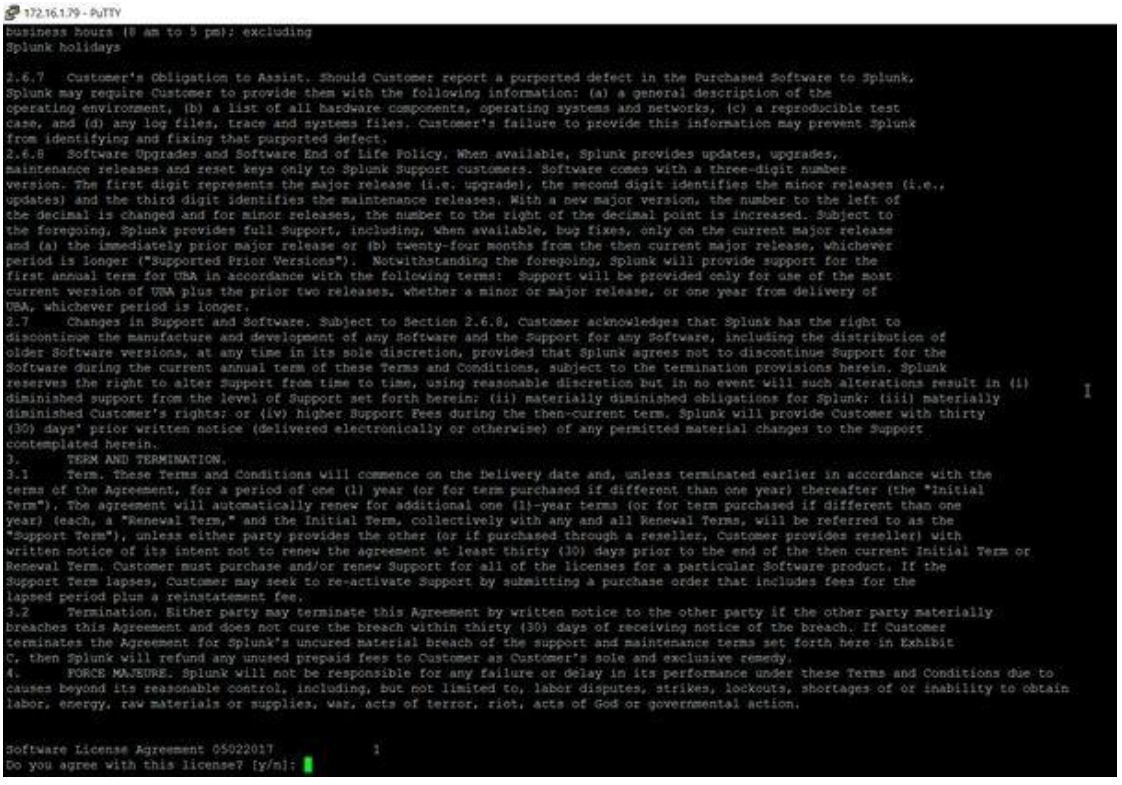
- **./splunk start**
- **./splunk stop**
- **./splunk restart**

Ou encore : **./splunk help** pour obtenir de l'aide

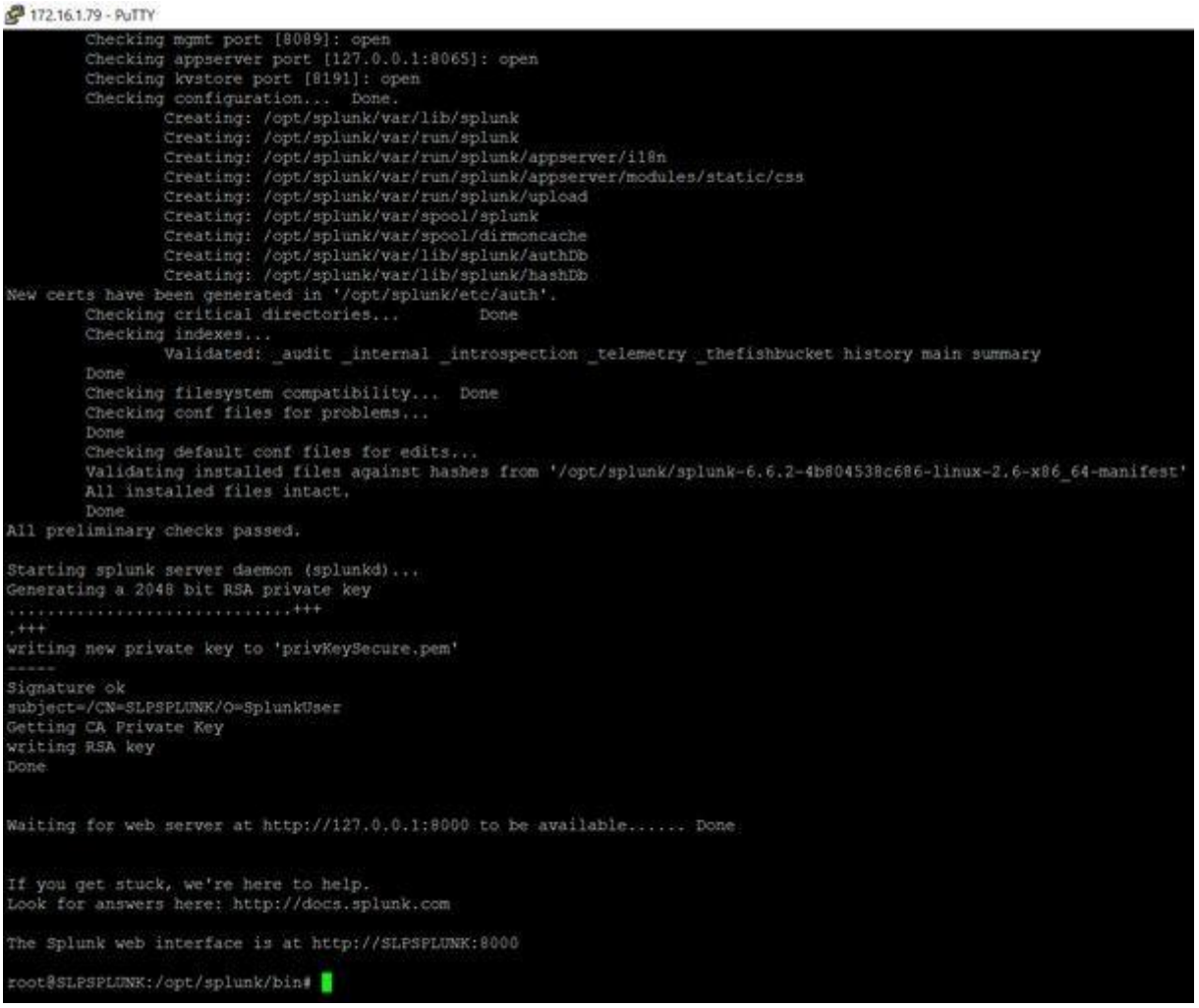
On lance splunk en tapant **./splunk start**



Splunk nous demande d'accepter les conditions d'utilisation, pour ce faire on descend à l'aide de la touche **« Entrée »** ou la **« Barre d'espace ».**

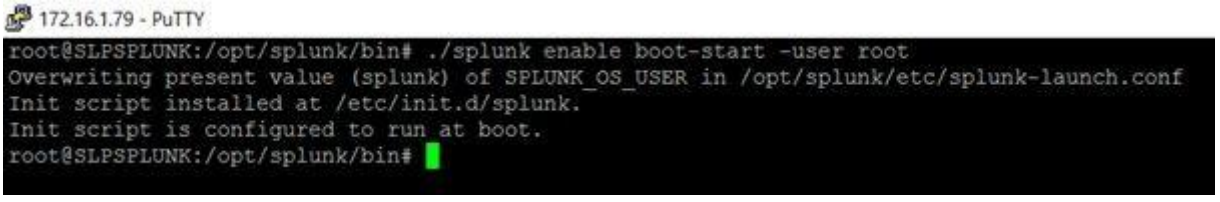


Une fois en bas de la page on tape **« y »** puis **« Entrée »** pour accepter les conditions d'utilisation.



Une fois l'initialisation terminé, Splunk nous affiche notre page d'interface web à l'adresse IP ou nom de domaine DNS donné.

On tape la commande : **./splunk enable boot-start -user root**

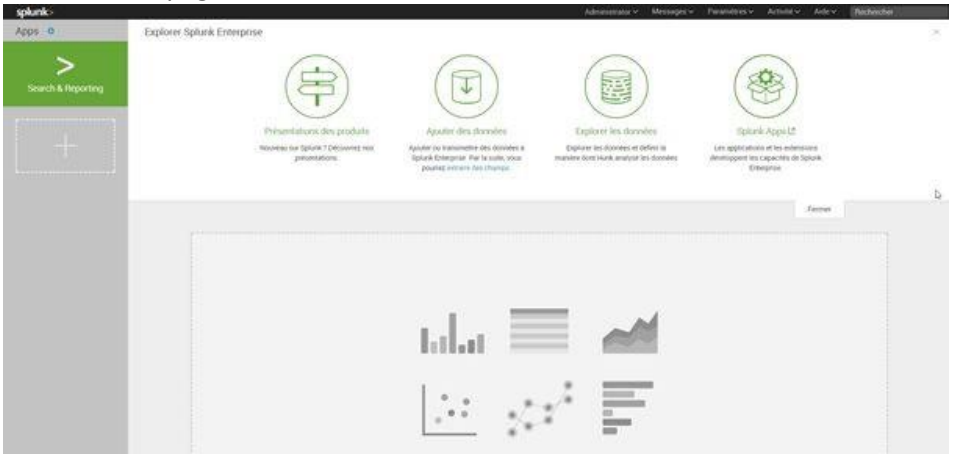


On se rend ensuite sur notre interface web (ici http://172.16.1.79:8000) à l'aide de notre navigateur :

Comme indiqué, il s'agit bien d'une première connexion donc on tape les identifiants :

Username : admin | **Password :** changeme On entre le nouveau mot de passe :

Nous voici connecté sur la page d'accueil :



Nous pouvons désormais monitorer et ajouter nos données.