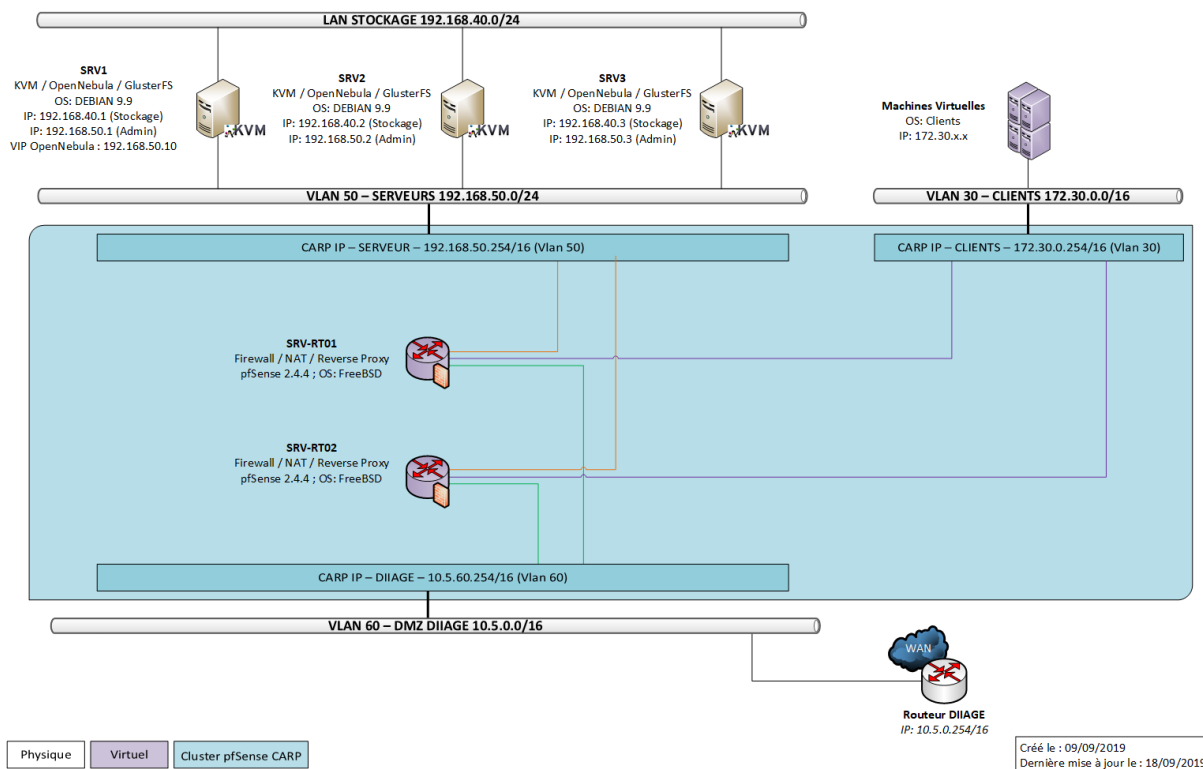




Département d'Ingénierie Informatique Appliquée

Projet CLOUD OpenNebula - Schéma Logique



UE C2-5 - Projet Cloud solution OpenNebula

Dossier d'Architecture Technique

Benoit LE CORRE

Florian LEAU

Léo ACQUISTAPACE

Thomas LAMY

DIIAGE 3 – Promotion 2019-2020

Table des matières

| | |
|--|----|
| Contexte | 3 |
| Les besoins fonctionnels | 4 |
| Les besoins non fonctionnels | 6 |
| Représentation fonctionnelle..... | 7 |
| Schéma des flux fonctionnels..... | 8 |
| Liste des environnements | 9 |
| Représentation applicative | 10 |
| Représentation de l'infrastructure | 11 |
| Axes d'améliorations : | 14 |

Contexte

Le Département d'Ingénierie Informatique Appliqué (DIIAGE) prépare en trois ans au titre d'Expert en Système Informatique. L'organisation actuelle est de deux sections d'étudiants, réseau et développement, avec 3 promotions par sections. Des formateurs externes interviennent pour dispenser des cours en lien avec le futur titre que souhaite obtenir les étudiants.

Aujourd'hui, le réseau du DIIAGE ne dispose d'aucune plateforme de virtualisation pour permettre aux formateurs de réaliser des démonstrations sur des produits, ou bien d'avoir une machine virtuelle de base accessible par les étudiants pour réaliser des tests. Les étudiants sont obligés de créer des machines virtuelles sur des stations de travail mutualisées avec les autres promotions. Ces machines peuvent donc être supprimées accidentellement par un autre étudiant.

Les besoins fonctionnels

Ce projet a pour objectif de déployer et de mettre à disposition de manière automatique des machines virtuelles à la suite d'une demande d'un utilisateur. C'est à travers un site web dédié que les utilisateurs (formateurs ou étudiants) peuvent choisir leur modèle et déployer leurs machines virtuelles.

Le projet de mise en place d'une infrastructure cloud interne au DIIAGE permettra d'avoir pour chaque élève la possibilité de disposer de machines virtuelles sans avoir besoin d'une machine performante personnelle. Il sera alors possible pour tous d'effectuer sur la même plateforme de virtualisation les manipulations pratiques liées aux cours ou aux projets.

Les principaux acteurs de ce projet sont :

- Le DIIAGE qui met à disposition des machines pour la mise en place du projet cloud privée permettant la virtualisation des machines virtuelles
- L'équipe projet qui est responsable de la mise en place technique du projet cloud et de la documentation pour permettre son exploitation
- Le product Owner qui a défini le sens du projet et qui a défini les finalités attendues pour ce projet

Les contraintes métiers liées à ce projet sont :

- matérielles. Le DIIAGE fournit pour ce projet 3 machines qui seront utilisées pour mettre en place l'infrastructure cloud de virtualisation
- techniques. Les connaissances sur la solution sont limitées pour les étudiants et les enseignants. Il est donc nécessaire pour eux de se documenter sur cette solution et de former les personnes amenées à travailler sur cette solution. Cela entraînera donc un coût en temps
- de temps accordé à la mise en place de l'infrastructure. La solution doit être opérationnelle et fonctionnelle en moins de deux semaines

L'infrastructure qui sera mise en place par les étudiants devra répondre aux besoins fonctionnelles principaux suivants :

- L'infrastructure à produire est une infrastructure cloud utilisant des solutions libres et open-source
- L'infrastructure devra être adaptée pour répondre aux besoins des étudiants des deux sections ainsi qu'aux enseignants et intervenants de la formation
- L'infrastructure réseau ainsi que les machines virtuelles devront être accessibles depuis l'extérieur via une adresse URL
- Chaque étudiant devra disposer d'un espace de virtualisation propre
- Des templates de machines virtuelles devront être disponibles pour l'ensemble des utilisateurs
- La solution d'infrastructure devra être facile d'utilisation pour les utilisateurs
- Un suivi de l'utilisation de la solution devra être accessible pour les utilisateurs

L'ensemble de ces besoins peuvent être complétés par des objectifs secondaires selon l'avancement de la mise en place de l'infrastructure :

- L'infrastructure cloud pourra être résiliente à la panne
- Mise en place d'un cluster entre les serveurs de la plateforme cloud
- Mise en place d'un cluster de stockage de données
- Mise en place de redondance matériels des actifs réseaux
- Mise en place de haute disponibilité au niveau des machines virtuelles
- L'automatisation du maintien à jour des templates de machines virtuelles

Les besoins non fonctionnels

Les besoins non fonctionnels sont définis dans le tableau suivant :

| Élément | Valeur | Commentaires |
|--------------------------------|---------------------|---|
| Emplacement des environnements | Sur place | Imposé |
| Editeur de Base de Données | MySQL | Imposé par la Solution |
| OS Hôte Principal | Debian 9.11 | Préféré à la version 10, pour stabilité et maîtrise |
| Active directory | Windows Server 2019 | Préféré pour stabilité et maîtrise |
| Nombre Utilisateurs Cibles | 90 | Nombre d'étudiants + intervenants maximum |

L'emplacement des environnements physiques et virtuelles n'est pas impactant sur la solution en elle-même mais est définis par l'utilisation du matériel fourni par le DIIAGE.

L'utilisation de l'éditeur de base de données « MySQL » est fortement conseillée pour la mise en place de la solution OpenNebula et sera donc une contrainte à prendre en compte.

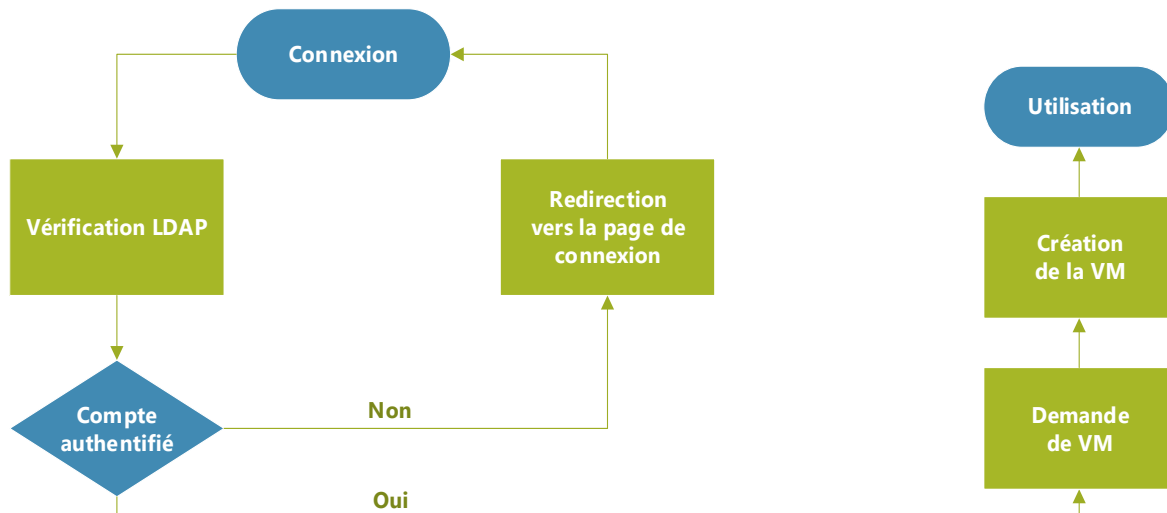
L'OS de l'hôte principal est un besoin non fonctionnel, en effet cela n'affecte en rien la solution et c'est un choix interne déterminé par les compétences de l'équipe chargée de l'implémentation de la solution.

La solution doit pouvoir gérer des comptes utilisateurs. Aucune solution n'est définie par le client. Nous avons donc choisi pour des raison interne d'utiliser un Active Directory qui sera l'annuaire de comptes utilisateurs.

Le nombre d'utilisateurs n'a pas d'impact sur la solution mais est une contrainte forte pour la mise en place et le dimensionnement de l'infrastructure.

Représentation fonctionnelle

Voici ci-dessous le processus d'utilisation basique pour un utilisateur final de l'infrastructure cloud :



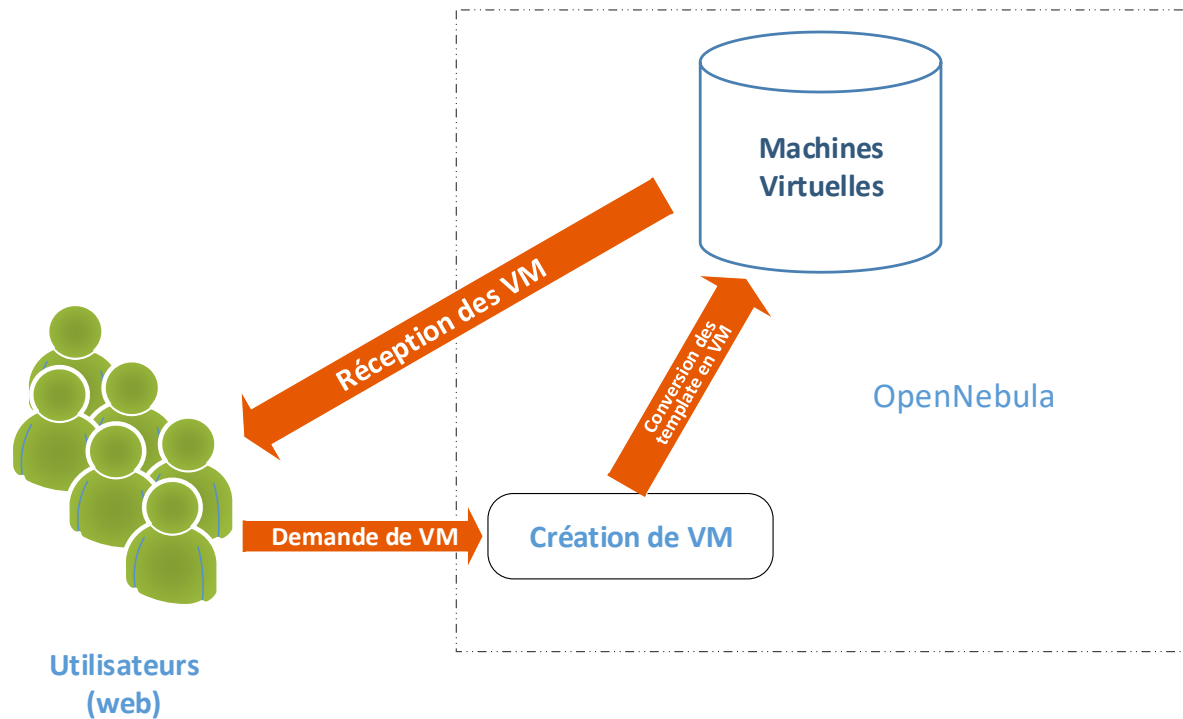
Le schéma de processus de l'utilisation basique de la solution pour l'utilisateur final ne comporte pas de complexité.

Lorsque l'utilisateur tente de se connecter, deux directions à cette connexion se dessine :

- L'authentification a réussi et l'utilisateur peut accéder à son interface, demander et utiliser des machines virtuelles (VM)
- L'authentification a échoué et l'utilisateur est amené à vérifier et ressaisir ses identifiants

Schéma des flux fonctionnels

Voici ci-dessous le schéma des flux fonctionnels d'utilisation basique pour un utilisateur final de l'infrastructure cloud :



Liste des environnements

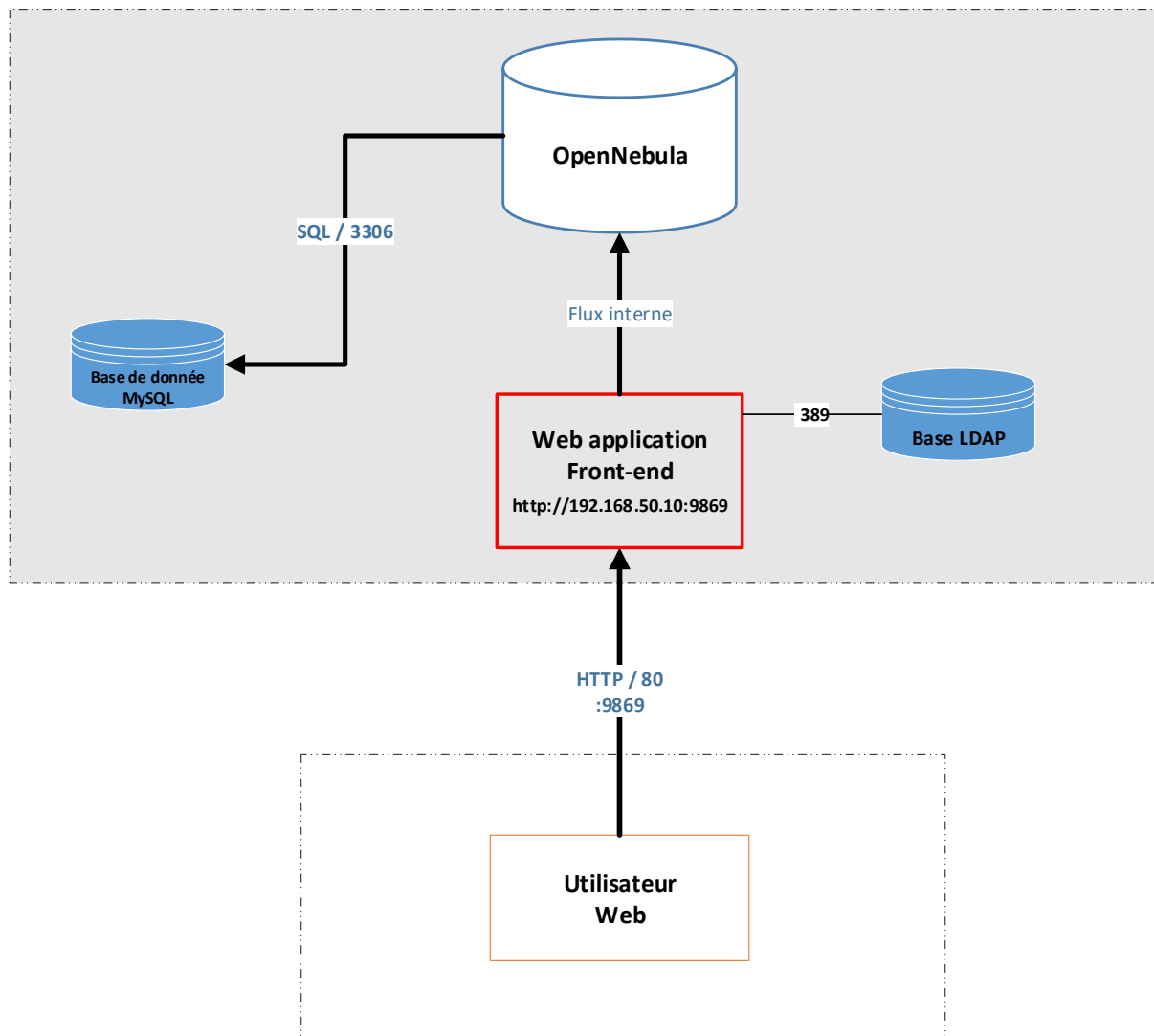
Voici ci-dessous la liste des environnements de l'infrastructure cloud :

| Environnement | Nom | Type de machine | Système d'exploitation | vCPU | RAM (en Go) | Stockage (en Go) | Réseau(x) | Rôle(s) |
|---------------|----------|-----------------|------------------------|------|-------------|------------------|-----------------------|----------------------------|
| PRODUCTION | SRV-AD01 | VM | Windows Server 2019 | 1 | 4 | 40 | Serveur | Annuaire ActiveDirectory |
| PRODUCTION | SRV1 | Physique | Debian 9.11 | N/A | 16 | 240 / 480 / 1024 | Serveur/Diage/Clients | KVM, OpenNebula, GlusterFS |
| PRODUCTION | SRV2 | Physique | Debian 9.11 | N/A | 16 | 241 / 480 / 1024 | Serveur/Diage/Clients | KVM, OpenNebula, GlusterFS |
| PRODUCTION | SRV3 | Physique | Debian 9.11 | N/A | 16 | 242 / 480 / 1024 | Serveur/Diage/Clients | KVM, OpenNebula, GlusterFS |
| PRODUCTION | SWI1 | Physique | Cisco 15.0(2)SE6 | N/A | N/A | N/A | Serveur/Diage/Clients | Commutateur réseau |
| PRODUCTION | SWI2 | Physique | Cisco 15.0(2)SE6 | N/A | N/A | N/A | Serveur/Diage/Clients | Commutateur réseau |
| PRODUCTION | pfSense1 | VM | FreeBSD | 1 | 4 | 20 | Serveur/Diage/Clients | Routeur, Firewall |
| PRODUCTION | pfSense2 | VM | FreeBSD | 1 | 4 | 20 | Serveur/Diage/Clients | Routeur, Firewall |

Dans le contexte actuel pour la mise en place de cette infrastructure, nous n'avons pas d'environnement de préproduction ni de plateforme de développement. Nous avons donc réalisé différentes maquettes de chaque brique sur lesquelles se reposent notre infrastructure.

Représentation applicative

Voici ci-dessous la liste des environnements de l'infrastructure cloud :



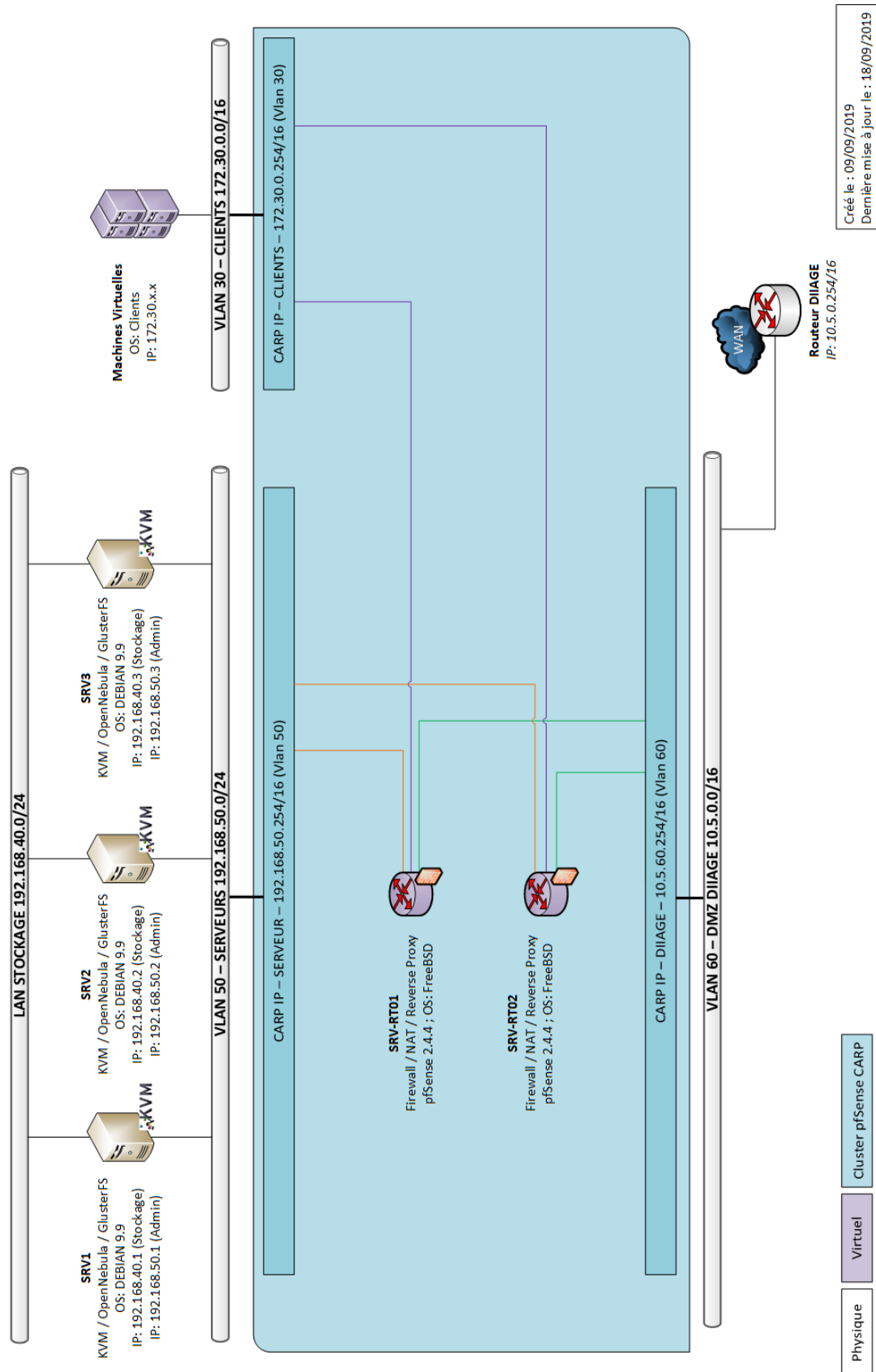
Pour pouvoir synthétiser les flux principaux entre les éléments nous avons établie une matrice de flux :

| Source | IP (source) | Réseau | Destination | Réseau dest | protocole | Port |
|--------------------|----------------|---------|----------------------|-------------|-----------|------|
| SRV-AD01 | 192.168.50.11 | Serveur | SRV1 / SRV2 / SRV3 / | Serveur | LDAP | 389 |
| SRV1 | 192.168.50.1 | Serveur | SRV1 / SRV2 / SRV3 / | Serveur | SSH | 22 |
| SRV2 | 192.168.50.2 | Serveur | SRV1 / SRV2 / SRV3 / | Serveur | SSH | 22 |
| SRV3 | 192.168.50.3 | Serveur | SRV1 / SRV2 / SRV3 / | Serveur | SSH | 22 |
| pfSense1 | 192.168.50.201 | Serveur | 192.168.50.10:9869 | Serveur | HTTP | 80 |
| pfSense2 | 192.168.50.202 | Serveur | 192.168.50.10:9869 | Serveur | HTTP | 80 |
| 192.168.50.10:9869 | 192.168.50.10 | Serveur | pfSense1 / pfSense2 | Serveur | HTTP | 80 |

Représentation de l'infrastructure

Afin de répondre au mieux aux besoins des utilisateurs et fournir une infrastructure résiliente, nous avons établi le schéma logique suivant :

Projet CLOUD OpenNebula - Schéma Logique



Le schéma précédant montre les spécificités de notre infrastructure. Nous avons une redondance logicielle concernant la solution OpenNebula.

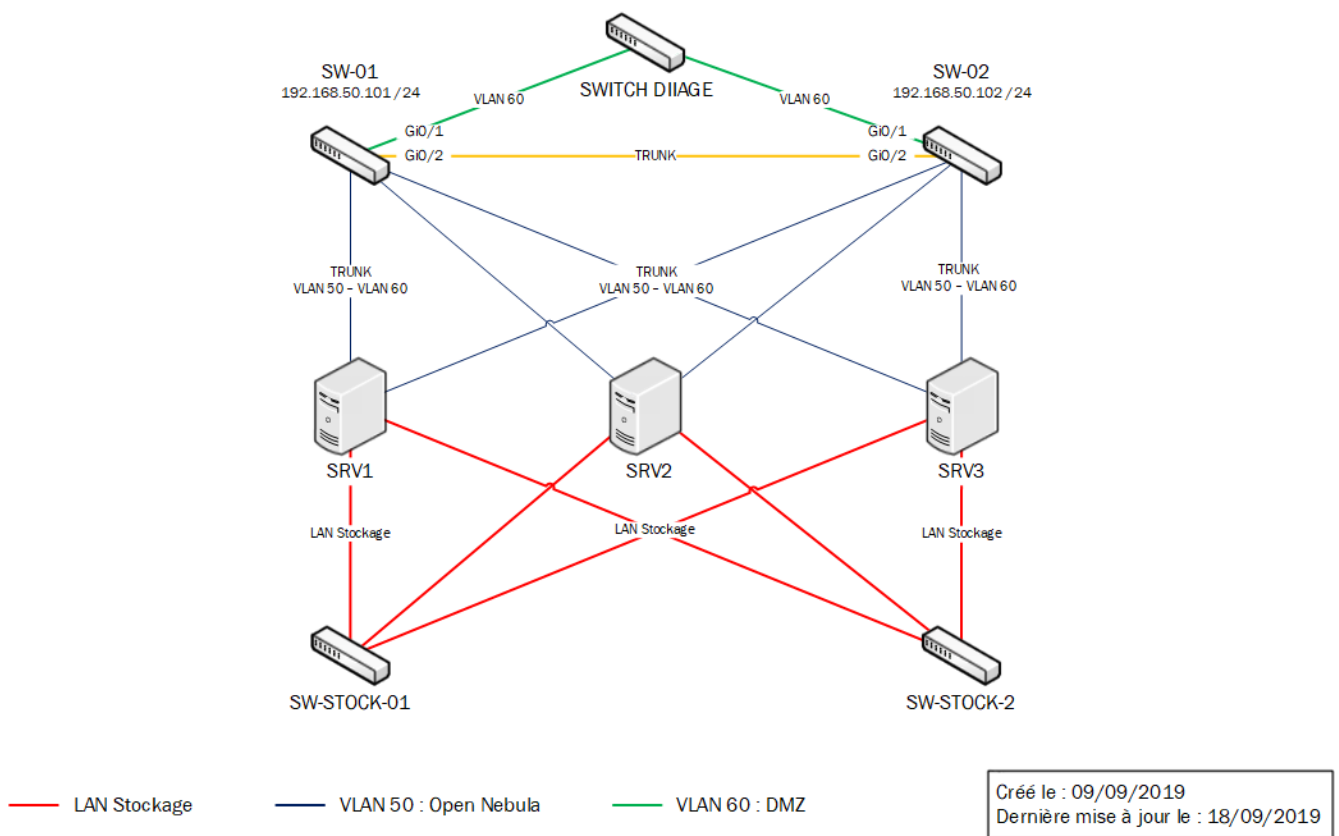
Concernant la partie web de la plateforme, le frontend est un cluster constitué de trois nœuds. L'interface web sera donc toujours disponible à partir d'une seule et même adresse IP et lien URL.

La solution de virtualisation KVM est elle aussi en cluster, cela permet la migration à chaud des machines virtuelles entre les nœuds et la répartition de ces machines entre les nœuds selon leurs ressources systèmes disponible.

Afin d'assurer une infrastructure logicielle la plus résiliente possible, nous avons décidé de mettre en place deux serveurs pfSense virtualisés eux aussi en cluster pour assurer les rôles de routeur et de pare-feu entre nos différents réseaux.

Pour visualiser l'aspect physique de notre infrastructure cloud, nous avons établi le schéma physique suivant :

Projet CLOUD OpenNebula - Schéma physique



Nous avons conceptualisé ce schéma physique avec pour objectif premier de rendre notre l'infrastructure physique tolérante à la panne.

Tous les liens et matériels réseaux étant doublés, cela permet en cas de défaillance d'un matériel physique de ne pas interrompre la production. Cela restera donc transparent pour l'utilisateur qui n'aura qu'une perte de connectivité réseau de quelques secondes.

Chaque serveur a un lien connecté aux deux switchs et ces switchs sont reliés entre eux ce qui permet d'avoir dans tous les cas une continuité de réseau.

Grâce à toutes ces dispositions, notre infrastructure ne peut être impactée seulement si les deux commutateurs réseaux tombent en panne en même temps.

Le point de panne le plus probable serait une coupure électrique. Le matériel n'étant pas ondulé et redondé électriquement, nous ne pouvons pas assurer une reprise d'activité dans un délai donné.

Axes d'améliorations :

Parmi tous les besoins auxquels nous avons pu répondre grâce à notre infrastructure, nous avons pu identifier plusieurs axes d'amélioration afin de la rendre encore plus résiliente :

- Mise en place d'onduleurs pour les matériels physiques
- Mise en place d'une redondance électrique avec deux sources d'électricité différentes
- Mise en place d'une haute disponibilité pour les machines virtuelles
- L'automatisation du maintien à jour des templates de machines virtuelles
- Industrialisation de la plateforme
- Utilisation de serveurs ReverseProxy plus robuste (tel que HAProxy)
- Solution de sauvegarde de données
- Solution de sauvegarde des machines virtuelles