



« Virtual Lab as a Service »

Guide d'utilisation de l'outil « VLab Composer »

Date : 15 Novembre 2016-11-17

Version : 1.0



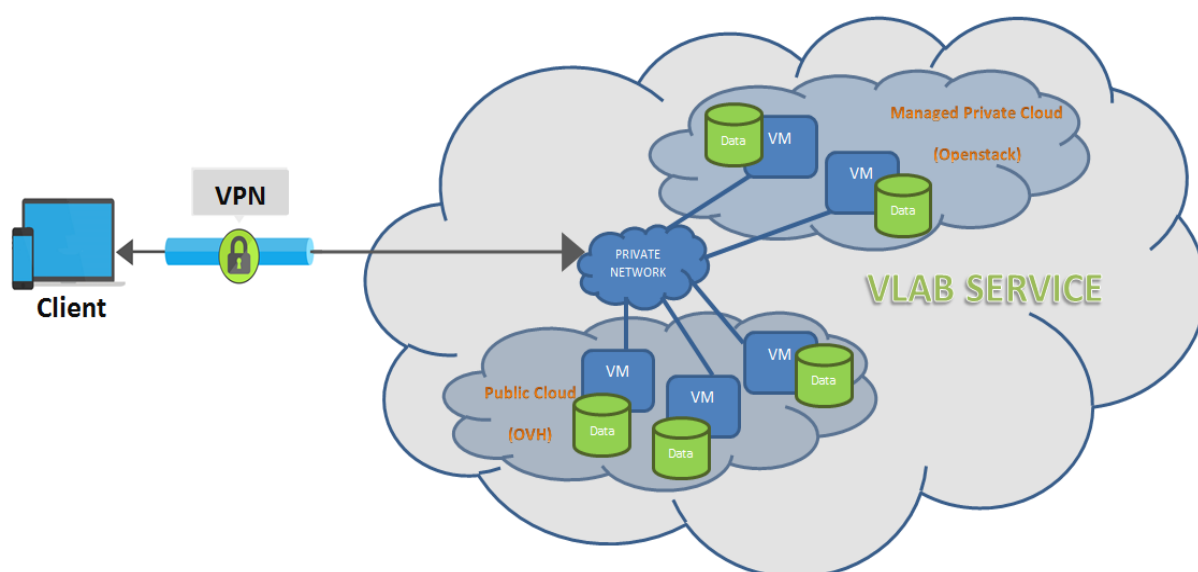
© COPYRIGHT PROCAN 2016

Préambule

L'objectif de ce guide est de montrer les différentes étapes nécessaires à la création d'un laboratoire virtuel en utilisant l'outil « vlab composer ». Cet outil permet de composer un cluster virtuel constitué d'un ou de plusieurs : machines virtuelles, volumes de stockage, réseaux virtuels dédiés, distributeurs de charge, etc...

Ce guide est structuré en deux parties. Partie A explique la création d'un laboratoire privé virtuel (Private Virtual Lab Service) hébergé sur le cloud vlab.tn (managed openstack based private cloud).

La deuxième partie B explique comment créer un laboratoire virtuel sur un cloud hybride entre le managed private cloud vlab.tn et le public cloud d'OVH (ovh.com/tn/cloud/). Votre laboratoire virtuel hybride (Hybrid Virtual Lab Service) vous offre l'élasticité nécessaire pour répondre aux pics d'activité et de charge et aux besoins de scalabilité pour vos projets ponctuels et temporaires. Parmi les originalités de ce service, les ressources offertes par le cloud public sont interconnectées à votre laboratoire virtuel d'une manière sécurisée et isolée via un VLAN. Vous aurez également le contrôle total du plan d'adressage des machines virtuelles d'OVH. Les ressources consommées sur le cloud public d'OVH sont facturées à l'heure.



A. Laboratoire virtuel Privé « Private Virtual Lab »

1. Accès au portail de vlab.tn:

Pour accéder au portail du frontal Vlab, taper dans un navigateur Web l'adresse suivante:
https://votre_domaine.vlab.tn

Une page d'authentification apparaîtra (Figure1). Taper le login et le mot de passe.

Remarque : si vous n'avez pas encore un compte sur le portail, cliquer sur le lien « create your account » pour l'inscription. Vous allez recevoir un email de confirmation contenant votre login et password.



Figure 1

Une fois authentifié, le tableau de bord (Dashboard) du portail s'affiche.

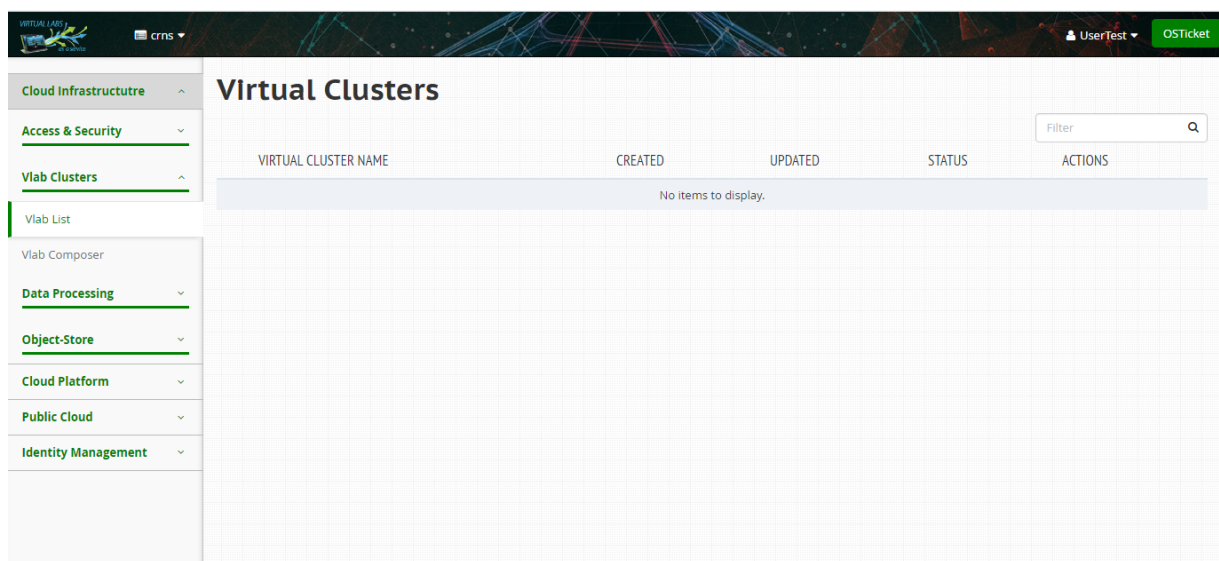


Figure 2

L'outil « vlab composer » se trouve sous le menu principal à gauche « Vlab Clusters ». Avant de lancer « vlab composer » pour créer votre cluster virtuel, vous aurez besoin de

- une clé de sécurité (**Obligatoire** pour accéder à vos VMs Linux)
- un réseau virtuel dédié –VLAN- (**Recommandé**) pour interconnecter vos ressources d’une manière sécurisée (environnement virtuel isolé).

La section 2 présente les différentes étapes pour créer une ou plusieurs clés de sécurité.

La section 3 présente les différentes étapes pour créer un ou plusieurs réseaux virtuels dédiés.

Si vous possédez déjà une clé et éventuellement un réseau privé, vous pouvez aller directement à la section 4 de ce guide pour lancer votre cluster virtuel.

2. Paire de clés :

Il s’agit ici de paires de clés SSH, permettant l’accès à un serveur distant via le protocole de communication SSH. Une paire de clés comprend une clé publique associée à une clé privée.

- La clé publique doit être copiée sur le serveur distant. Cette opération est réalisée par le biais d’OpenStack qui provisionne les clés d’accès aux instances à partir de celles qui lui ont été fournies (l’utilisateur doit uploader une ou plusieurs clé(s) publique(s) dans son compte Compute).
- La clé privée reste sur le poste client.

Pour générer une nouvelle paire de clés ou importer une paire de clés, cliquez sur « Access & Security » sous « Cloud Infrastructure » dans le menu principal à gauche puis cliquez sur l’onglet « Key Pairs » (Figure3).

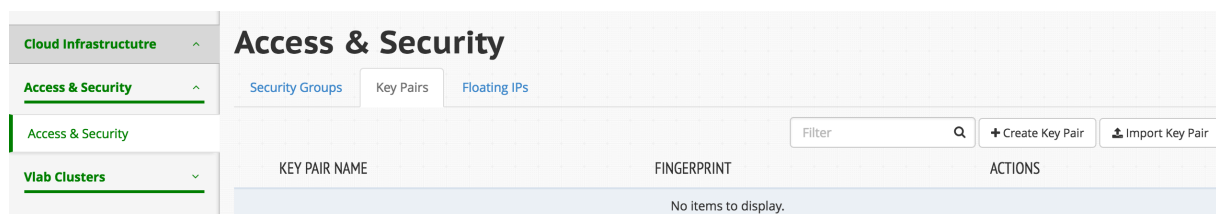


Figure 3

a. Générer une nouvelle paire de clés

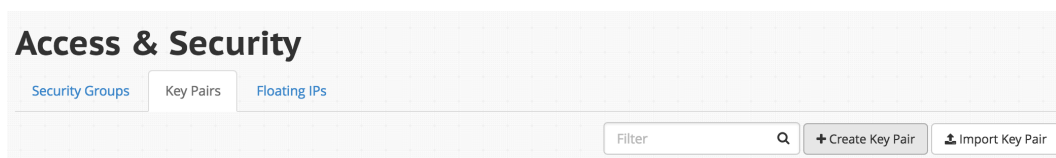
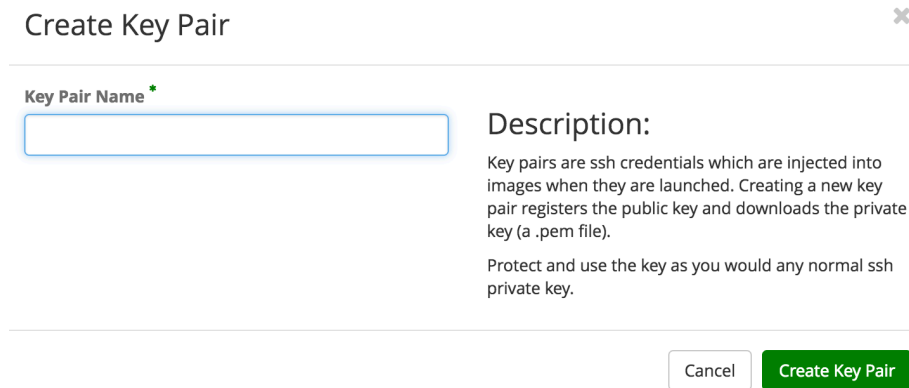


Figure 4

Pour générer une paire de clés (Figure 4):

- Rendez vous dans le menu “Access & Security”
- Cliquez sur l’onglet “Key Pairs” puis sur “Create Key Pair”

- Une fenêtre apparaîtra (Figure 5). Nommez votre paire de clés et cliquez sur “ **Create Key Pair**”
- Vous allez alors générer et télécharger la nouvelle paire de clés



Create Key Pair

Key Pair Name *

Description:

Key pairs are ssh credentials which are injected into images when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file).

Protect and use the key as you would any normal ssh private key.

Cancel Create Key Pair

Figure 5

Pour télécharger la clé privée, vous pouvez cliquer sur le lien « **Download Key Pairs** » (Figure 6)

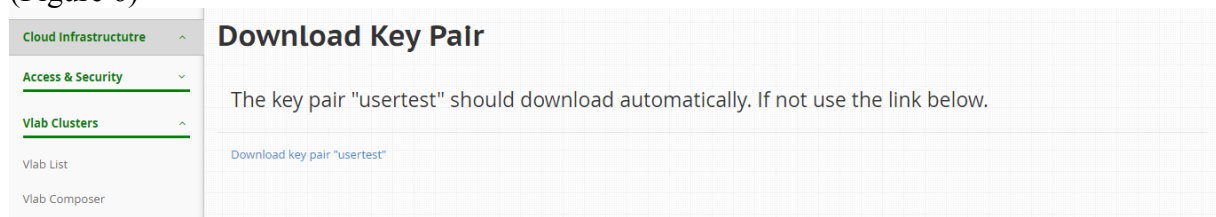


Figure 6

b. Importer une paire de clés

Cette section suppose que vous possédez déjà une paire de clés à importer dans le portail. **Pour plus d’information concernant la génération d’une paire de clés sous Linux, Windows et Mac, consultez l’annexe.**

Pour importer une paire de clés:

- Rendez vous dans le menu “ **Access & Security**”
- Cliquez sur l’onglet “ **Key Pairs** ” puis sur “ **Import Key Pair**”
- Choisissez un nom de paire de clés que vous reconnaîtrez et collez le contenu de votre clé publique SSH dans l’espace prévu (Figure 7, 8).
- Cliquez sur “ **Import Key Pair** ”

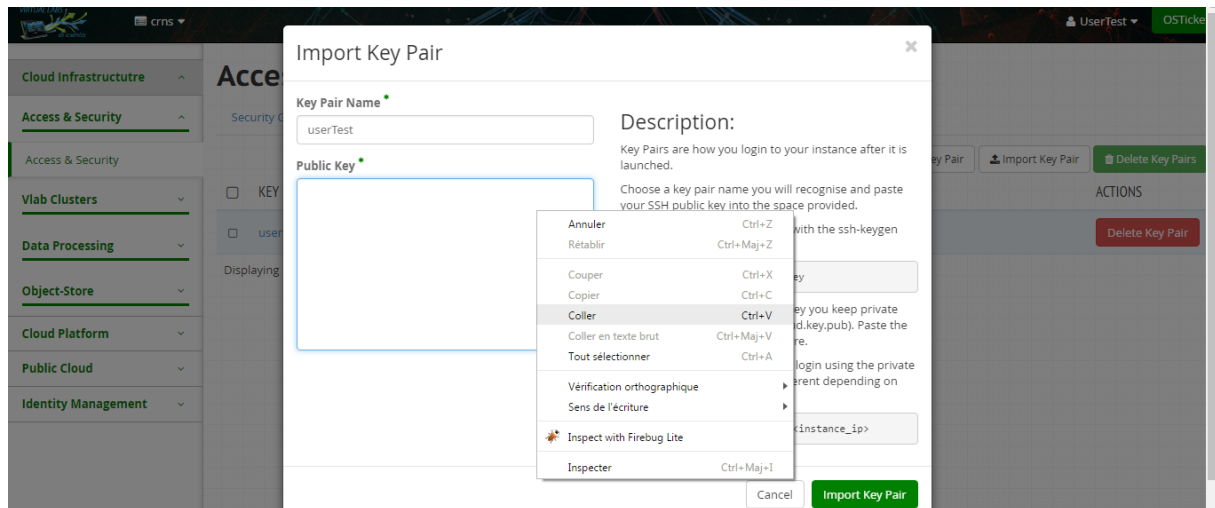


Figure 7

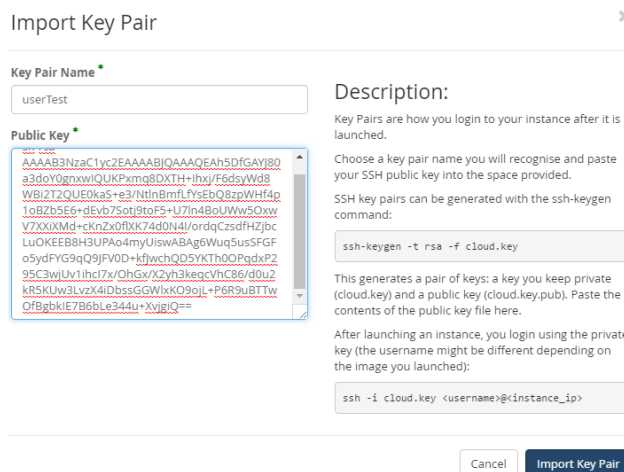


Figure 8

3. Créer un réseau privé :

Il est recommandé d'instancier un réseau privé VLAN pour interconnecter vos machines virtuelles d'une manière totalement isolé et sécurisé. Si vous ne souhaitez pas instancier un réseau virtuel dédié, vos ressources seront interconnecté par le réseau VLAN par défaut (partagé avec tous les membres du projet).

Pour créer un réseau privé, cliquez sur « **Advanced Management** » (figure 9) puis cliquez sur « **Networks** » dans le menu principal à gauche (figure 10).

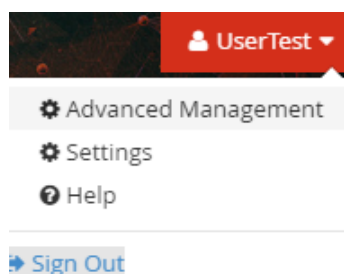


Figure 9

Cliquez sur « **Create Network** » (bouton à droite) (Figure 10).

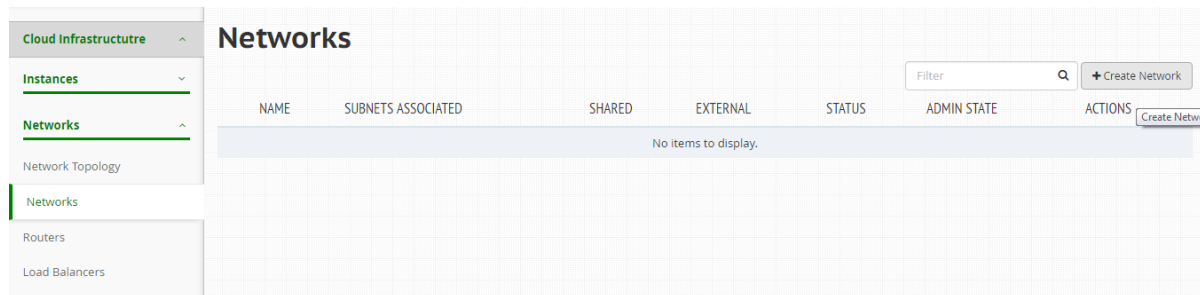


Figure 10

Tapez le nom du réseau à ajouter et cliquez sur « Next » (Figure 11).

Create Network

Network Subnet Subnet Details

Network Name
testNetwork

Create a new network. In addition, a subnet associated with the network can be created in the following steps of this wizard.

Admin State ?
UP

☐ Shared ?

☒ Create Subnet

Cancel < Back Next >

Figure 11

Tapez le nom du sous réseau, l'adresse du sous réseau ainsi que la passerelle (NB: la passerelle doit se terminer par '.1') puis cliquez sur « Next » (Figure 11).

Create Network

Network Subnet Subnet Details

Subnet Name
testsubnet

Creates a subnet associated with the network. You need to enter a valid "Network Address" and "Gateway IP". If you did not enter the "Gateway IP", the first value of a network will be assigned by default. If you do not want gateway please check the "Disable Gateway" checkbox. Advanced configuration is available by clicking on the "Subnet Details" tab.

Network Address ?
192.168.40.0/24

IP Version
IPv4

Gateway IP ?
192.168.40.1

☐ Disable Gateway

Cancel < Back Next >

Figure 11

Activez le dhcp en cochant « **Enable DHCP** », précisez la plage d'adresses du sous réseau dans le champ « **Allocation Pools** » (optionnel) ainsi que les serveurs DNS dans le champ DNS Name servers (Figure12).

L'exemple choisi dans ce guide montre la création d'un réseau privé avec la plage d'adresses 192.168.40.0/24 et la passerelle 192.168.40.1. Toutes les instances utilisent 8.8.8.8 pour la résolution DNS.

Si vous ne spécifiez rien dans le champ « allocation pools », le serveur DHCP attribue à chaque instance une adresse IP entre 192.168.40.2 et 192.168.40.254.

Remarque : Si vous souhaitez étendre plus tard votre cluster virtuel et y ajouter des ressources additionnelles du cloud public d'OVH, le remplissage du champ « Allocation Pools » devient obligatoire. Il faut spécifier une partie de la plage d'adresses pour le sous réseau du Vlab (exemple entre 192.168.40.2 -> 192.168.40.150) (Figure 12). La plage d'adresses 192.168.40.150 -> 192.168.40.254 sera attribuée plus tard pour le sous-réseau créé au niveau du cloud public OVH (voir partie B – Hybrid Vlab). Ceci pour ne pas avoir un conflit de réseau par la suite.

Create Network

Network Subnet Subnet Details

☒ Enable DHCP Specify additional attributes for the subnet.

Allocation Pools ⓘ

192.168.40.2,192.168.40.150

DNS Name Servers ⓘ

8.8.8.8

Host Routes ⓘ

Cancel « Back Create

Figure 12

Un message indique que le réseau a été ajouté avec succès (Figure20).

Cloud Infrastructure

Instances

Networks

Network Topology

Networks

Routers

Load Balancers

Networks

Filter

Success: Created network "testNetwork".

+ Create Network Delete Networks

<input type="checkbox"/>	NAME	SUBNETS ASSOCIATED	SHARED	EXTERNAL	STATUS	ADMIN STATE	ACTIONS
<input type="checkbox"/>	testNetwork	testsubnet 192.168.40.0/24	No	No	Active	UP	Edit Network

Displaying 1 item

Figure 13

Pour ajouter un routeur, cliquer sur « Routers » sous « Networks » dans le menu principal à gauche puis cliquer sur « Create Router » (Figure 14).

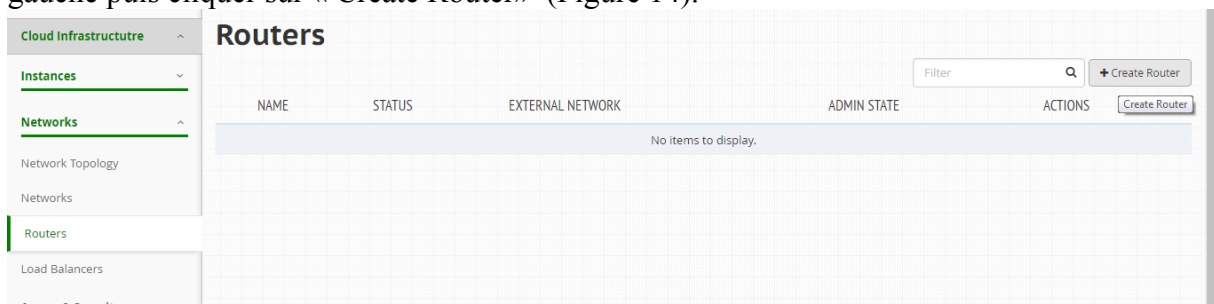


Figure 14

Taper le nom du routeur à ajouter, choisir le réseau "admin_floating_net" (le réseau public) comme un réseau externe puis cliquer sur « Create Router » (Figure 15).

Figure 15

Un message indique que le routeur a été ajouté avec succès (Figure 16).

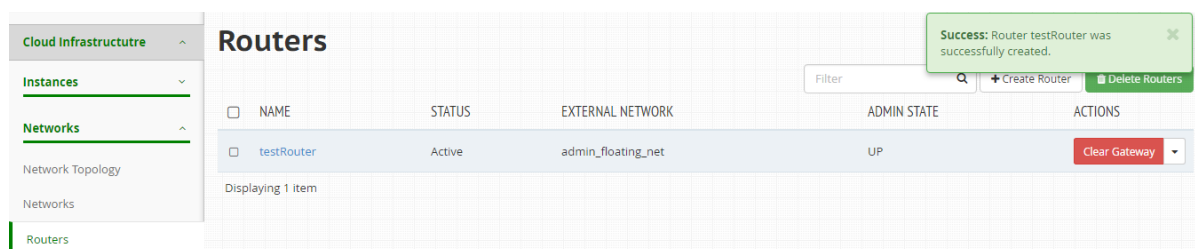


Figure 16

Cliquer sur le nom du nouveau routeur (lien en bleu) afin de créer des nouvelles interfaces. Cliquer sur l'onglet « Interfaces » puis sur le bouton à droite « Add Interface » (figure 17).

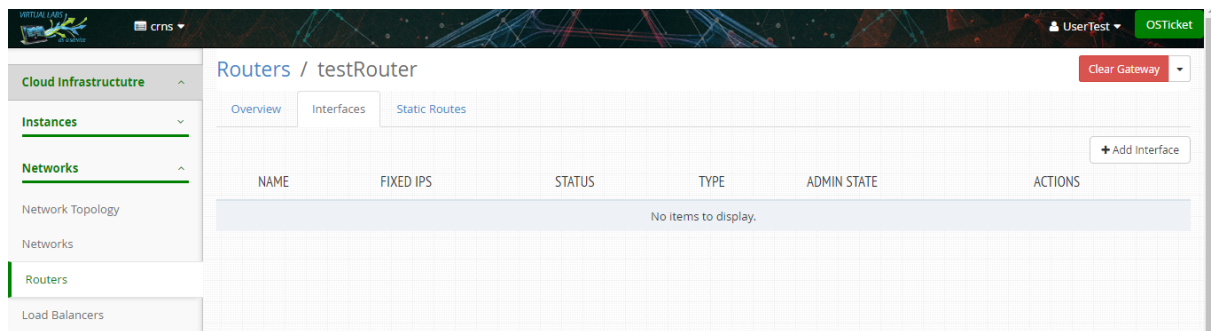


Figure 17

Choisissez le sous réseau ajouté auparavant puis cliquer sur « Submit» (figure 18).

The 'Add Interface' dialog box is shown. It contains the following fields and values:

- Subnet:** testNetwork: 192.168.40.0/24 (testsubnet)
- IP Address (optional):** (empty field)
- Router Name:** testRouter
- Router ID:** 92b2e4bd-67e9-4c14-bfb7-c1328a0ad3cf

The 'Description' text on the right states: 'You can connect a specified subnet to the router. The default IP address of the interface created is a gateway of the selected subnet. You can specify another IP address of the interface here. You must select a subnet to which the specified IP address belongs to from the above list.'

At the bottom right, there are 'Cancel' and 'Submit' buttons. The 'Submit' button is highlighted in blue.

Figure 18

Un message indique que l'interface a été ajoutée avec succès (Figure 19).

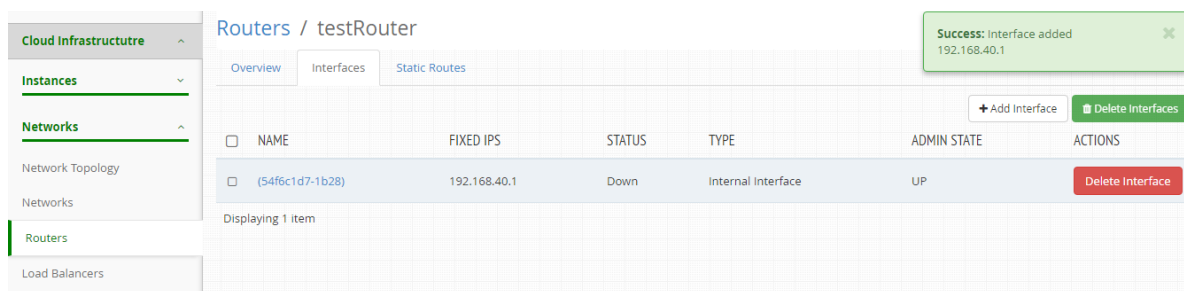


Figure 19

4. Créer un cluster (laboratoire) virtuel

Pour ajouter un cluster (vlab) virtuel, cliquez sur « Vlab Composer » sous « Vlab Clusters » dans le menu principal à gauche (Figure 20). Une interface vous demande de saisir de nouveau votre password.

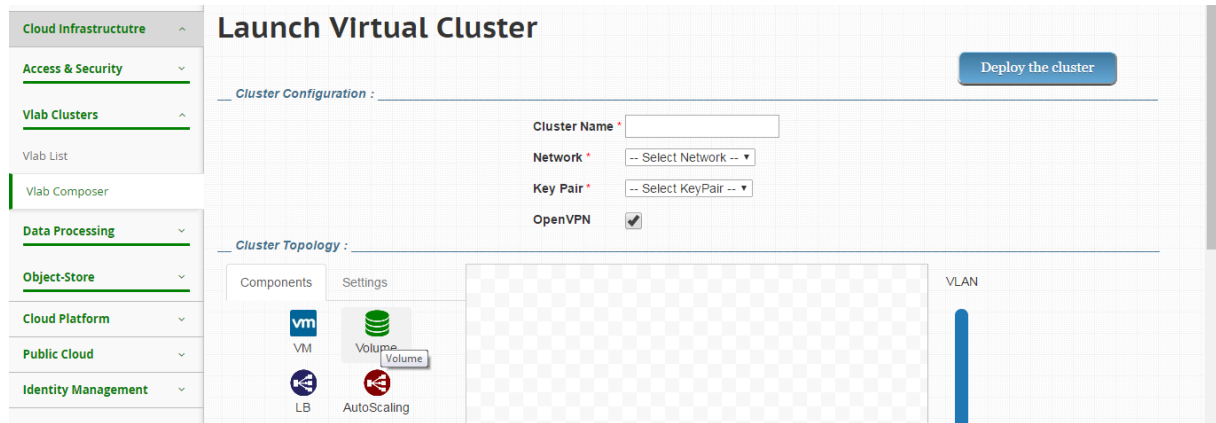


Figure 20

Dans la partie « **Cluster Configuration** », tapez le nom du cluster à ajouter puis sélectionnez le réseau privé ainsi que le nom de la clé (Figure 21).

NB: Pour avoir un accès sécurisé à votre vlab via un tunnel VPN, veuillez cocher la case « OpenVPN ».

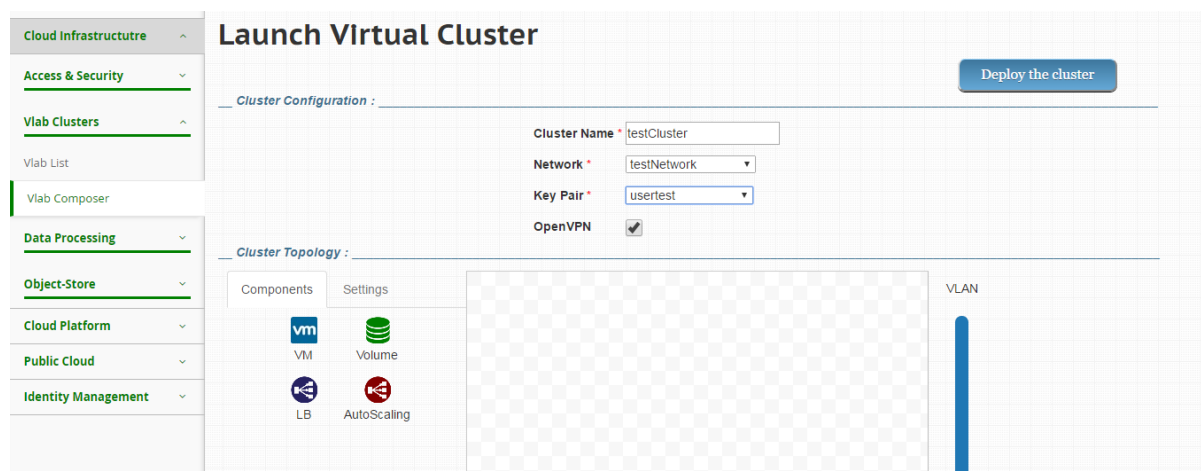







Figure 21

Dans la partie « **Cluster Topology** », sous l'onglet « **Components** », quatre composants sont offerts pour constituer votre vlab:

- Machine virtuelle ()
- Volume ()
- Répartiteur de charge – Load Balancer ()
- Auto-Elasticité ()

4.1. Machine Virtuelle :

Glisser l'icône «  » vers le rectangle situé au milieu afin d'ajouter une machine virtuelle à votre cluster (Figure 22).

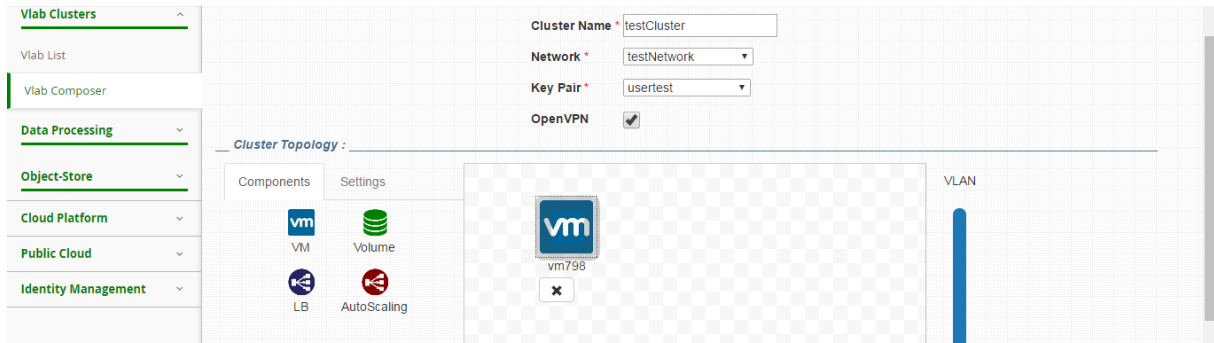


Figure 22

Cliquez deux fois sur l'icône en bleu de la VM ajoutée afin de la configurer (Figure 23). L'onglet « **settings** » s'active (sous la zone « **cluster Topology** »).

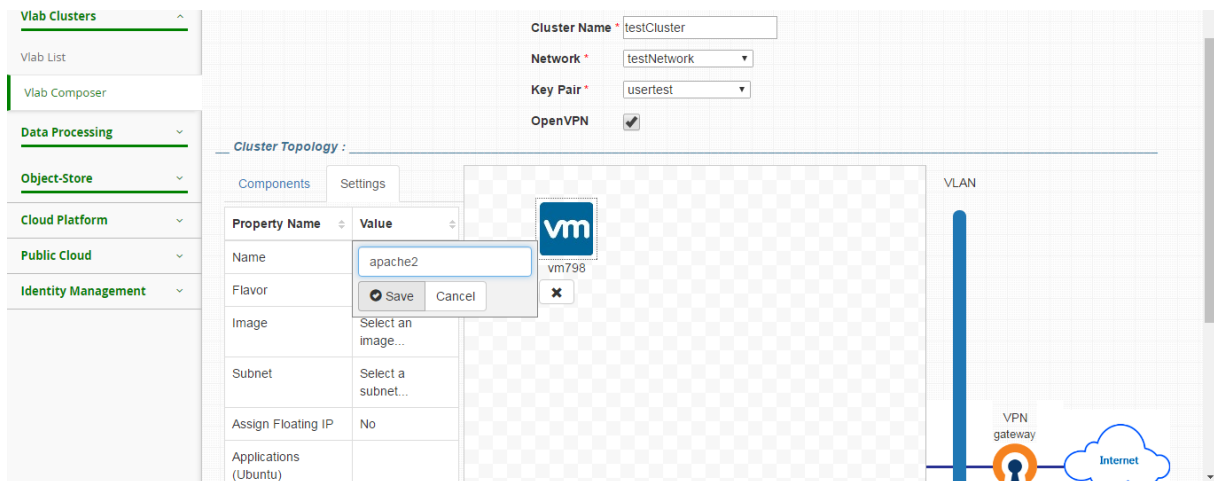


Figure 23

Il faut ensuite définir la valeur de chaque paramètre de configurations :

- *Name* : Nom de la machine virtuelle
- *Flavor* (Gabarit) : définit les paramètres de la VM: nombre de vCPU, quantité de mémoire vRAM, taille du disque système.
- *Image* : Spécifier l'image à partir de laquelle vous souhaitez créer l'instance (exemple ubuntu-server-12.04, windows-server-2012-r2,).
- *Subnet* : le sous réseau à attacher à la VM
- *Assign Floating IP* : associer une adresse IP publique à la VM.
- *Applications (Ubuntu)* : ce champ est spécifique pour les OS ubuntu. Actuellement, quatre applications sont disponibles (Apache2, Tomcat, Ngnix, MySQL...) (Figure 24). Sélectionnez l'application à installer automatiquement sur la VM après instanciation.

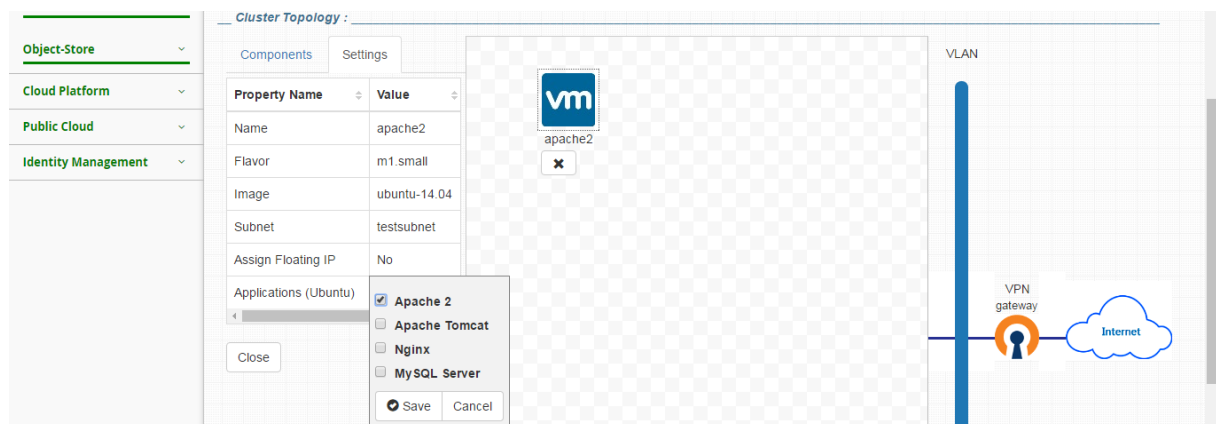



Figure 24

Remarque: Pour supprimer un composant (exemple une VM), cliquez sur la croix située juste au dessous du composant.



4.2. Volume :

Vous pouvez associer un volume supplémentaire à votre VM (optionnelle). Glisser «  » vers le rectangle situé au milieu afin d'ajouter un volume au cluster (Figure 25).

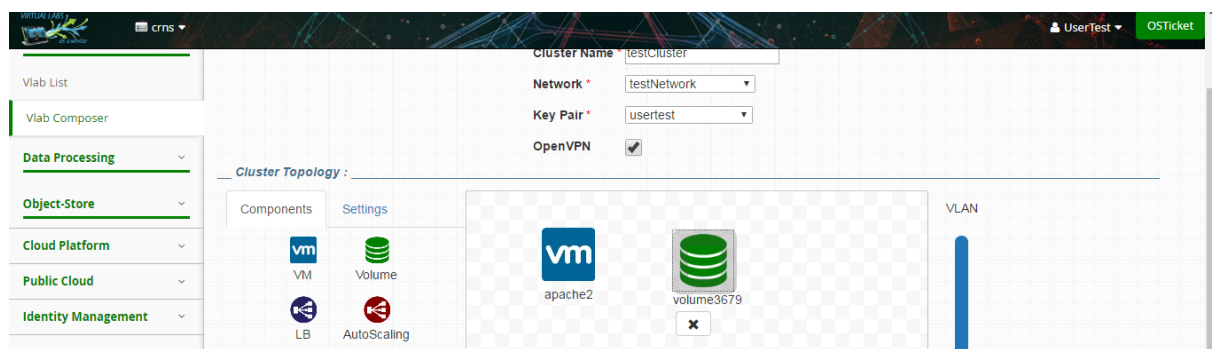


Figure 25

Cliquez deux fois sur le volume ajouté afin de le configurer. Puis, tapez le nom et choisissez la taille du volume en Go (Figure 26).

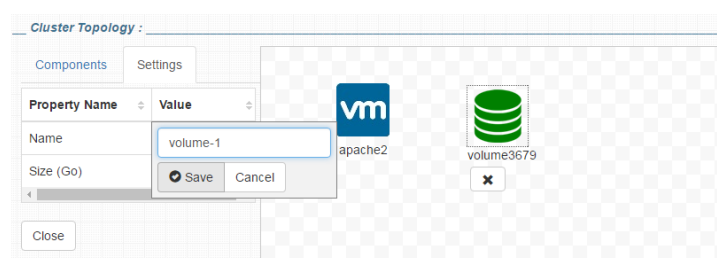


Figure 7

Afin d'attacher le volume au VM, ajouter un connecteur entre les deux composants (Figure 27). Cliquez sur le contour en gris de l'icône du premier composant et déplacez le pointeur de la souris vers l'autre contour gris du deuxième composant. Vous pouvez renommer le connecteur.

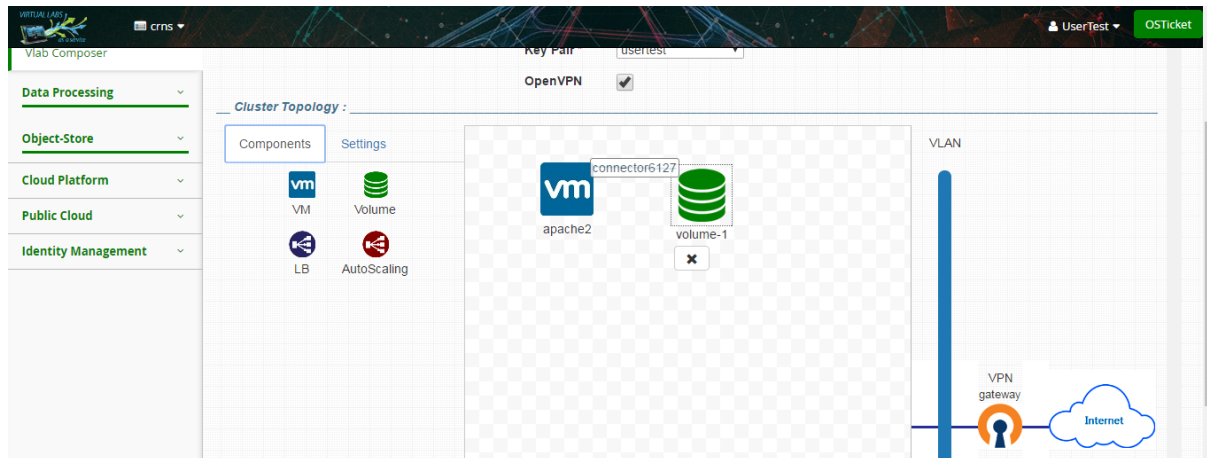


Figure 8

Pour ajouter d'autres machines virtuelles, d'autres volumes et d'autres connecteurs, répétez les mêmes étapes déclarées ci-dessus (Figure 28 et Figure 29).

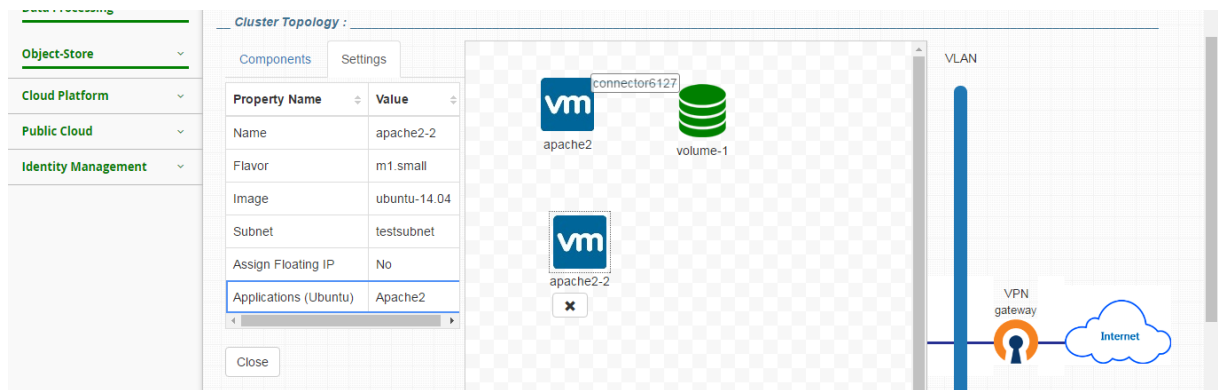


Figure 9

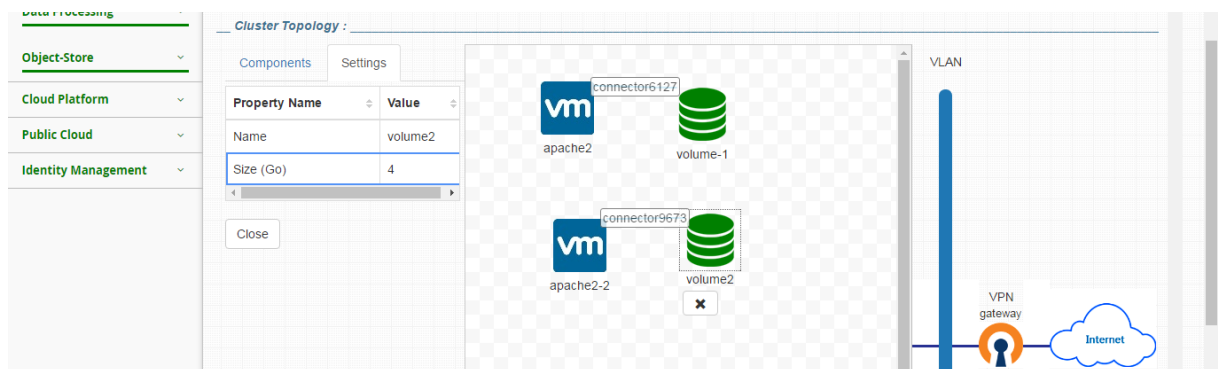



Figure 29

4.3. Répartiteur de charge:

La répartition de charge permet de distribuer une charge de travail entre différentes VMs et de gérer la résilience d'un service. Cela permet également de réduire l'indisponibilité potentielle de ce service lors des pannes.

Glisser «  » vers le rectangle situé au milieu afin d'ajouter un LB (Load Balancing) au cluster (Figure 30).

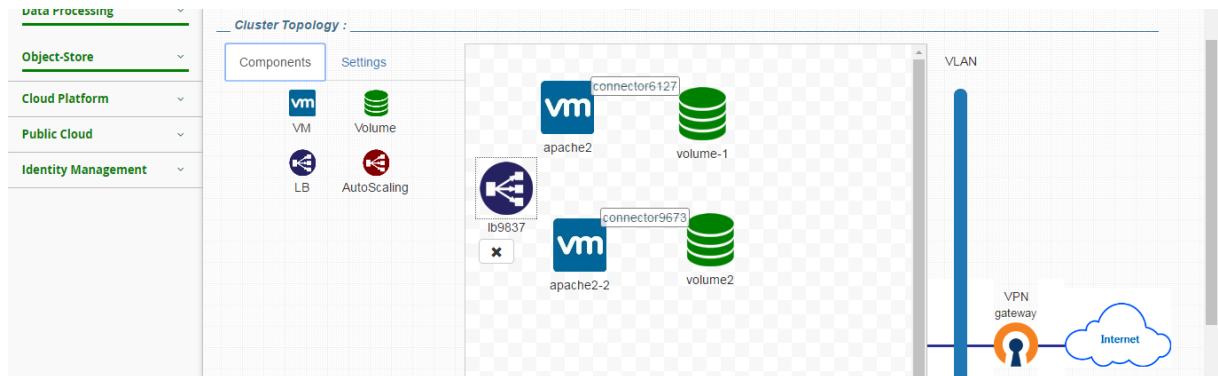


Figure 30

Taper le nom du LB, le port et le sous réseau du VIP (Virtual IP) (Figure 31).

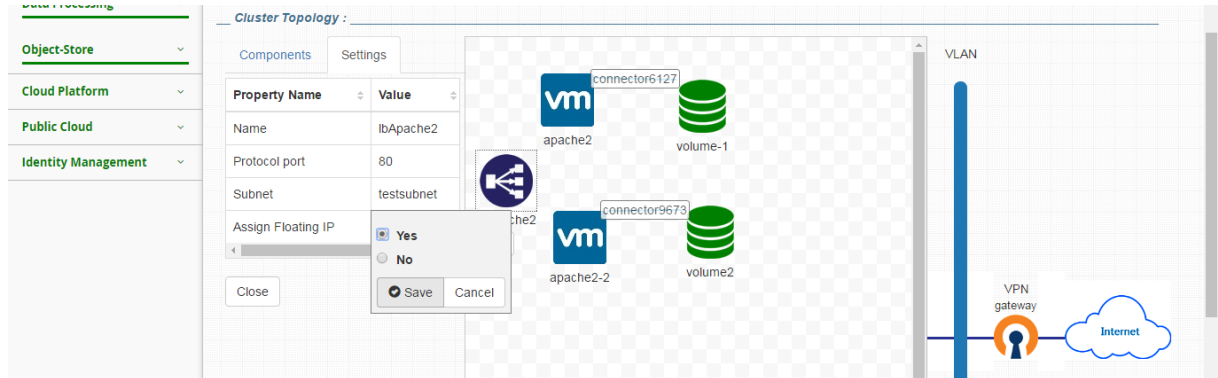


Figure 31

Ajouter des liaisons entre le LB et les machines virtuelles (Figure 32).

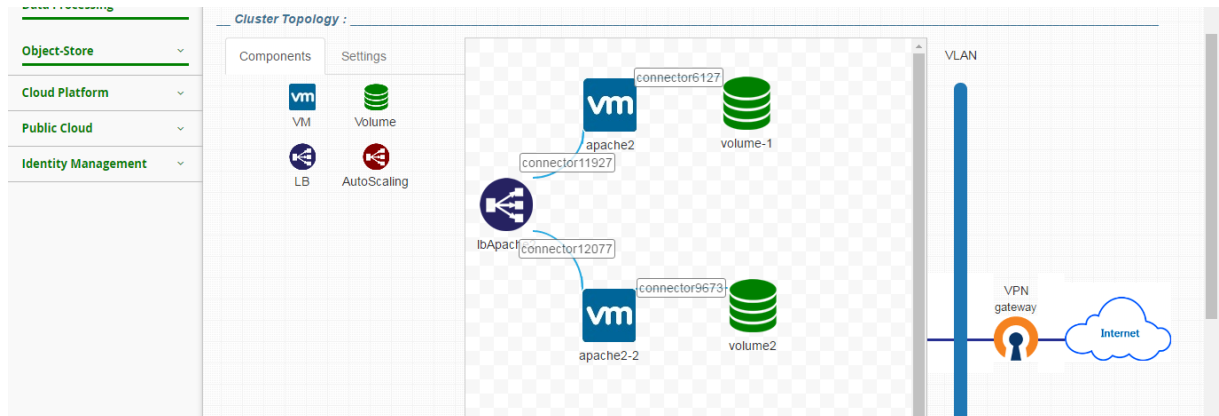


Figure 32

4.4. Auto-Elasticité

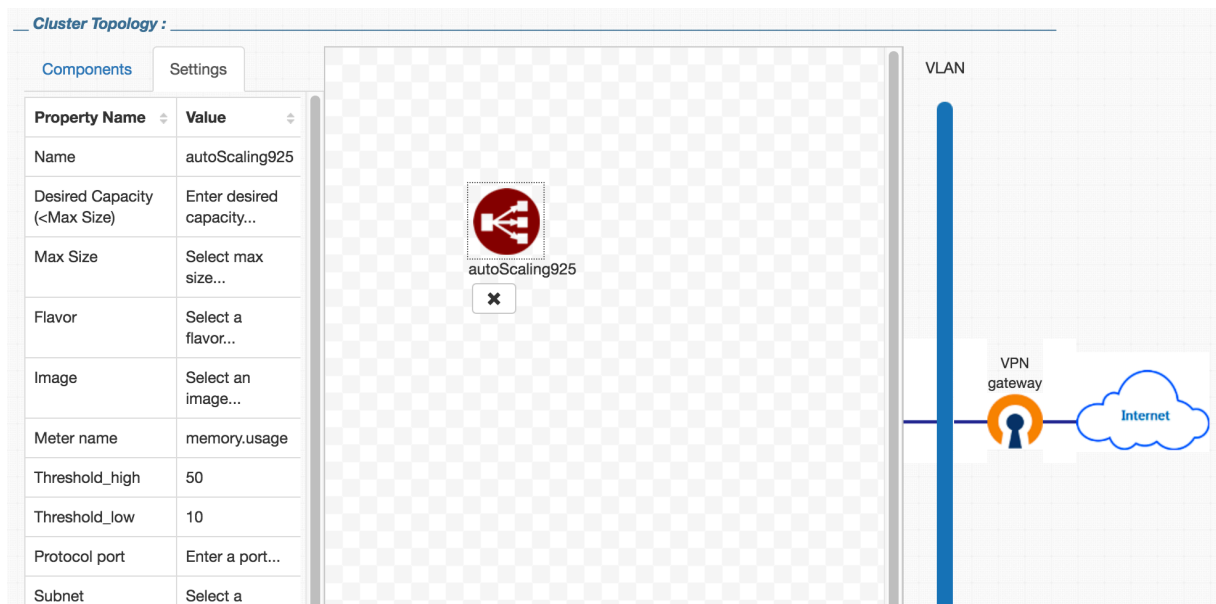


Figure 33

4.5. Déploiement

Après l'ajout des composants, cliquez sur « Deploy the Cluster » afin de créer le cluster virtuel (Figure 34).

Launch Virtual Cluster

Cluster Configuration :

Cluster Name: testCluster

Network: testNetwork

Key Pair: usertest

OpenVPN: ☒

Cluster Topology :

Components: Settings

VLAN

Figure 34

Pour vérifier l'état du nouveau cluster ou pour lister les clusters déjà créés, cliquez sur « *Vlab List* » sous « *Vlab Clusters* » dans le menu principal à gauche (Figure 35). Le champ « *Status* » vous indique l'état de déploiement.

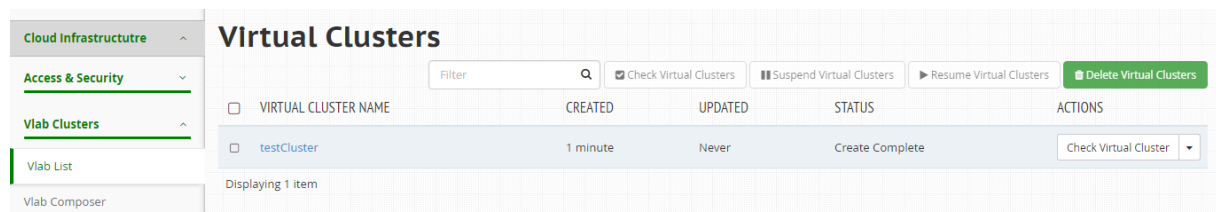


Figure 35

Si le cluster est bien déployé (l'état « Create Complete »), un email vous sera envoyé comme le montre l'exemple de la Figure 36.

```
The Cluster testCluster has been created successfully.

Follow these instructions to install OpenVPN client :
On Ubuntu:

# sudo apt-get install openvpn

Retrieve the client configuration file:

# scp -i usertest.pem ubuntu@178.33.18.122:/home/ubuntu/vpnaccess.tar.bz2 .

(If you get an error message saying this file does not exist, please wait a few minutes 'after' the cluster to have fully
completed, indeed, certain commands (e.g.: the Diffie Hellman generation) take a certain time after the cluster completed)

Copy this vpnaccess.tar.bz2 to the /etc/openvpn/ directory of your client:

# sudo cp /home/ubuntu/vpnaccess.tar.bz2 /etc/openvpn

Extract the archive and launch the client:

# sudo su -
# cd /etc/openvpn
# tar -xvzf vpnaccess.tar.bz2
# service openvpn restart

Check the vpn connection

You can now access through ssh to your VMs directly with their internal IPs.
IPs Address :
lbApache2_Floating_IP = 178.33.18.123
apache2_private_ip = 192.168.40.13
apache2-2_private_ip = 192.168.40.11
openvpn_Floating_IP = 178.33.18.122
```

Figure 36

Si vous avez coché l'option OpenVPN, un tunnel VPN est établi avec votre cluster. La première partie de l'email de configuration reçu fournit les étapes d'installation d' OpenVPN pour les clients Linux (voir section suivante).

A la fin de l'email, vous trouverez les adresses IP publique (floating_IP) et/ou privée (private_IP) des machines virtuelles, le Virtual IP du répartiteur de charge et l'adresse ip publique du gateway OpenVPN.

Figure 36 montre l'exemple d'un cluster composé d'un répartiteur de charge (@IP publique : 178.33.18.123), de deux VMs (@IP privés 192.168.40.11 et 192.168.40.13). L'adresse IP du gateway VPN est 178.33.18.122.

```
You can now access through ssh to your VMs directly with their internal IPs.
IPs Address :
lbApache2_Floating_IP = 178.33.18.123
apache2_private_ip = 192.168.40.13
apache2-2_private_ip = 192.168.40.11
openvpn_Floating_IP = 178.33.18.122
```

Figure 37

Pour vérifier que le LB est bien configuré, ouvrez le navigateur et tapez l'adresse IP du répartiteur en précisant le port du service apache2 – ici port 80 - (Figure 38).

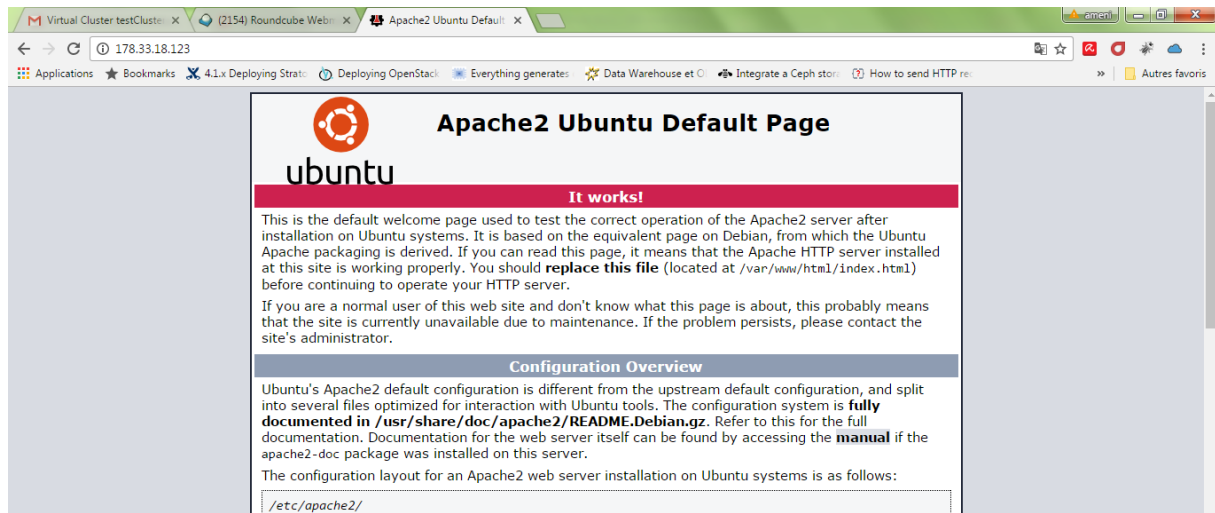


Figure 38

5. Installer et configurer le client OpenVPN :

Si le système d'exploitation du client est Linux, suivez les étapes d'installation d'OpenVPN qui sont déclarées dans l'email de configuration reçu.

```
# sudo apt-get install openvpn
```

Retrieve the client configuration file:

```
# scp -i userTest.pem ubuntu@178.33.18.122:/home/ubuntu/vpnaccess.tar.bz2 .
```

Copy this vpnaccess.tar.bz2 to the /etc/openvpn/ directory of your client:

```
# sudo cp /home/ubuntu/vpnaccess.tar.bz2 /etc/openvpn
```

Extract the archive and launch the client:

```
# sudo su -  
# cd /etc/openvpn  
# tar -xvjp vpnaccess.tar.bz2  
# service openvpn restart
```

Si le système d'exploitation du client est Windows, suivez les étapes suivantes:

- 1- Téléchargez le logiciel « pscp.exe ».
- 2- Installez le logiciel « OpenVPN GUI ».
- 3- Ouvrez le « cmd » afin de copier les fichiers de configuration d'OpenVPN vpnaccess.tar.bz2 dans un dossier local (Figure 39).

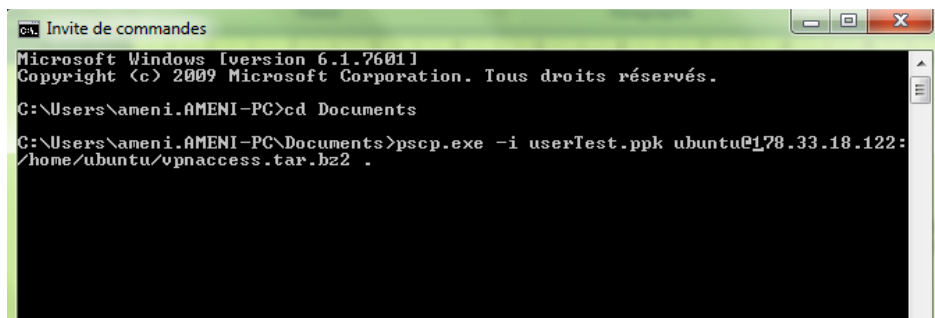


Figure 39

- 4- Tapez « y » pour confirmer le transfert (Figure 40).

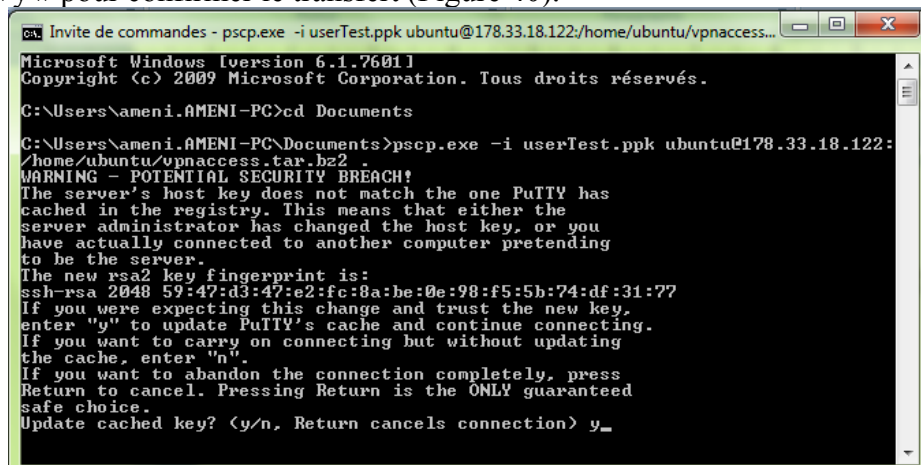


Figure 40

- 5- Vérifiez que les fichiers de configuration d'OpenVPN sont bien copiés (Figure 41).

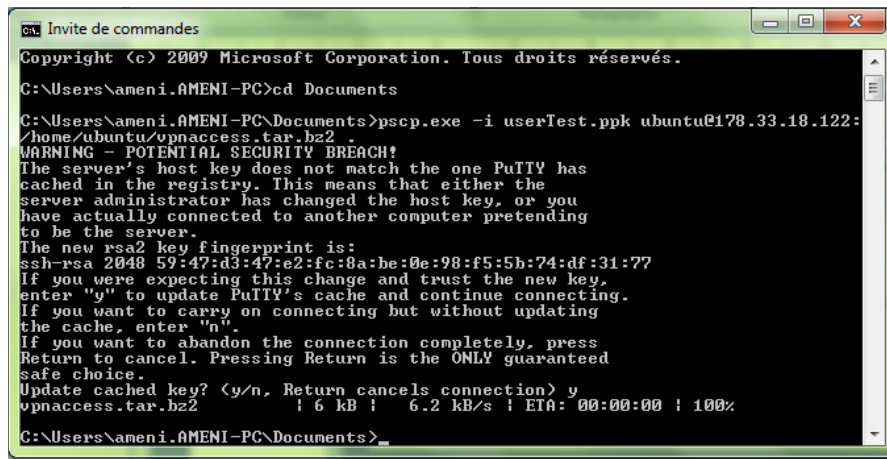


Figure 41

6- Accédez au dossier contenant « vpnaccess.tar.bz2 » puis décompressez le (Figure 42). Vous obtenez un nouveau dossier « vpnaccess ».

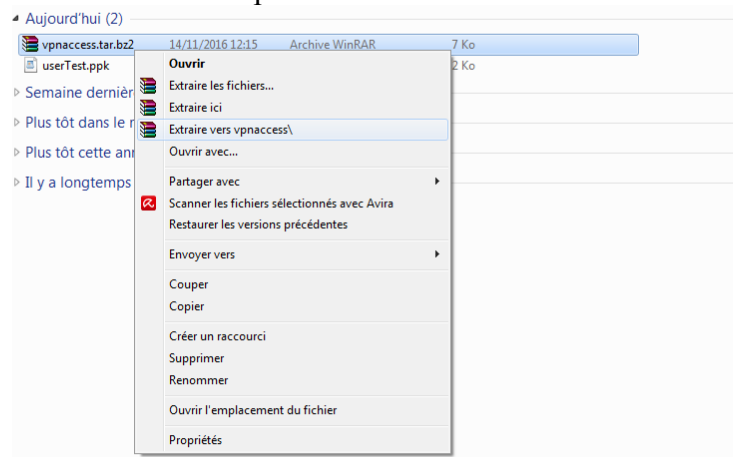


Figure 42

7- Ouvrez le nouveau dossier « vpnaccess » contenant les fichiers de configuration du client OpenVPN (Figure 43) : fichier client.conf et le dossier Keys.

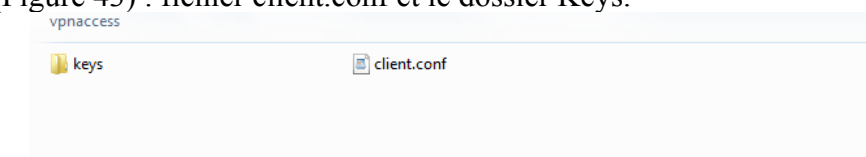


Figure 410

8- Modifiez l'extension du fichier « client.conf » en « client.ovpn » (Figure 44).



Figure 44

9- Sous le dossier « C:\Program Files\OpenVPN\config », remplacez le fichier « client.ovpn » et le dossier « keys » par ceux placés dans le dossier « vpnaccess » (Figure 45).

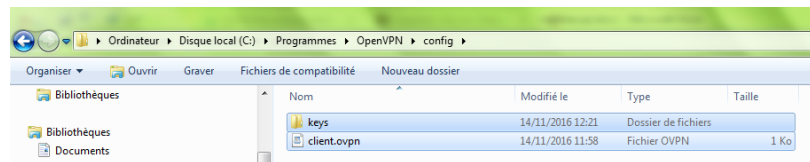


Figure 45

11- Ouvrir le logiciel « OpenVPN GUI » (Figure 46).

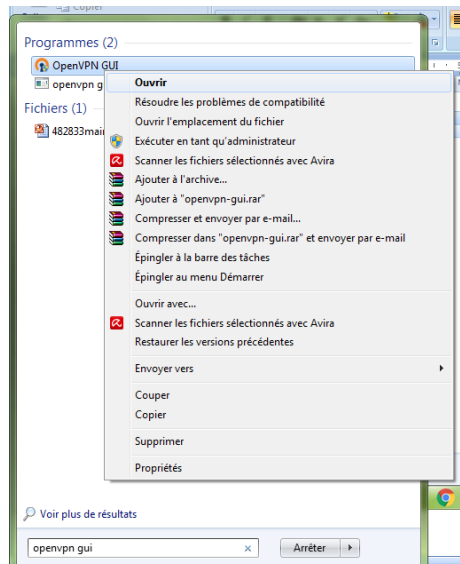
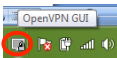


Figure 46

12- Cliquez sur «  » puis sur « Connecter » (Figure 47).

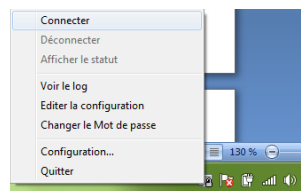


Figure 47

13- Une nouvelle fenêtre s'affiche afin d'établir un tunnel vers le cluster (Figure 48).

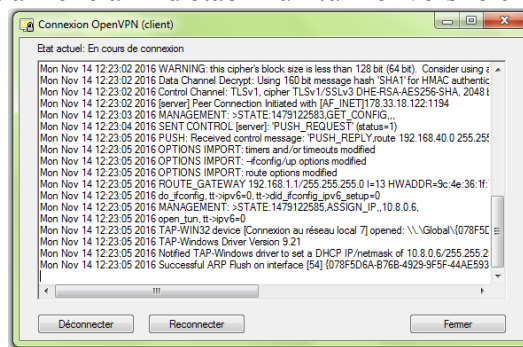


Figure 48

14- Un message indique que le tunnel a été établi avec succès (Figure 49).



Figure 49

6. Tester le client OpenVPN :

Pour tester la bonne installation d'OpenVPN (client linux ou windows), accédez à l'email reçu et copiez l'adresse privée de la machine virtuelle contenant par exemple le service apache. Collez l'adresse dans un navigateur web pour voir le résultat (Figure 50).

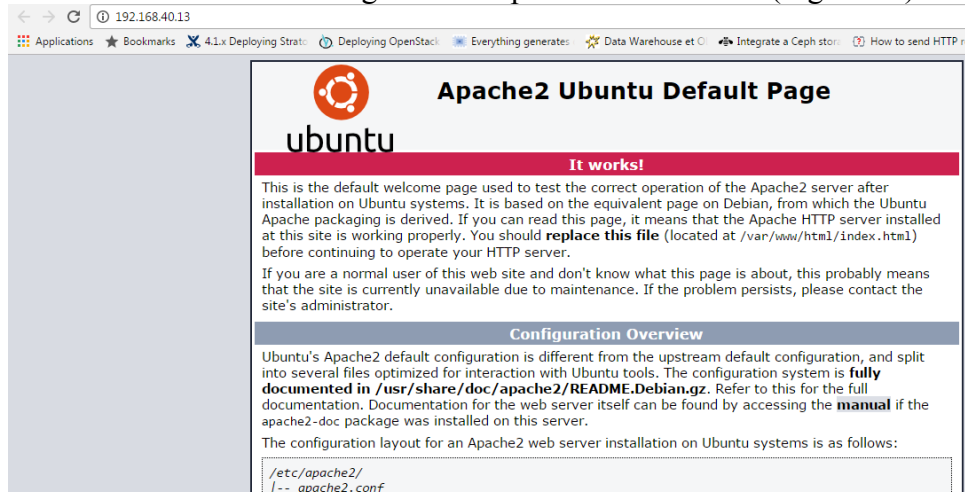


Figure 50

B. Laboratoire virtuel hybride « Hybrid Virtual Lab »

To be done

Annexe 1 : Création de la paire de clés

Préambule

Pour se connecter de manière sécurisée, il faudra donc configurer une clé SSH. Cela permet notamment de se connecter :

- sans avoir à retenir de mot de passe
- avec une sécurité supérieure que celle proposée par les mots de passe

Ce guide vous explique les étapes à suivre afin de configurer votre clé.

1. Sous Linux & Mac

a. Création de la clé

D'abord, il vous faut installer le client openSSH:

```
~$ sudo apt-get update
```

```
~$ sudo apt-get install openssh-client
```

Taper la commande suivante qui permettra de générer une clé SSH:

```
~$ ssh-keygen -b 4096
```

On obtient le résultat suivant, la commande vous propose de modifier l'emplacement de la clé privée:

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/home/user/.ssh/id_rsa):
```

L'étape suivante consiste à configurer une passphrase pour votre clé SSH :

```
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
```

Remarque: Il est recommandé de définir une passphrase afin de protéger la clé, n'hésitez pas à mettre un mot de passe.

```
Your identification has been saved in /home/user/.ssh/id_rsa.
```

```
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
```

```
The key fingerprint is:
```

```
0a:3a:a4:ac:d1:40:6d:63:6d:fd:d9:fa:d6:b2:e0:36 user@host
```

```
The key's randomart image is:
```

```
+---[RSA 4096]-----+
```

```
|  .      |
```

```
|      |
```

```
| .      |
```

```
|...     |
```

```
|..=.o .S. |
```

```
|=o.o. ..  |
```

```
|o+ . . o .. |
```

```
|.. . oEoo . |
```

```
|o. . .o+oo |
```

```
+-----+
```

Afficher la clé publique grâce a la commande suivante :

```
~$ cat /chemin/vers/cle/publique
```

b. Connexion en SSH sur la machine virtuelle

Lors de la création de la machine virtuelle dans Vlab, La **clé publique** va être **copiée sur la nouvelle machine virtuelle** dans ~/.ssh/authorized_keys. La clé privée reste sur votre poste client. Pour accéder à votre machine, tapez la commande suivante:

```
~$ ssh -i /chemin/vers/cle/privée user@IP_VM
```

2. Sous Windows

c. Création de la clé

Télécharger le logiciel **puttygen** permettant de générer la clé puis l'exécuter.
Au niveau de **Number of bits in a generated key**, indiquer la valeur 4096 (Figure 1).

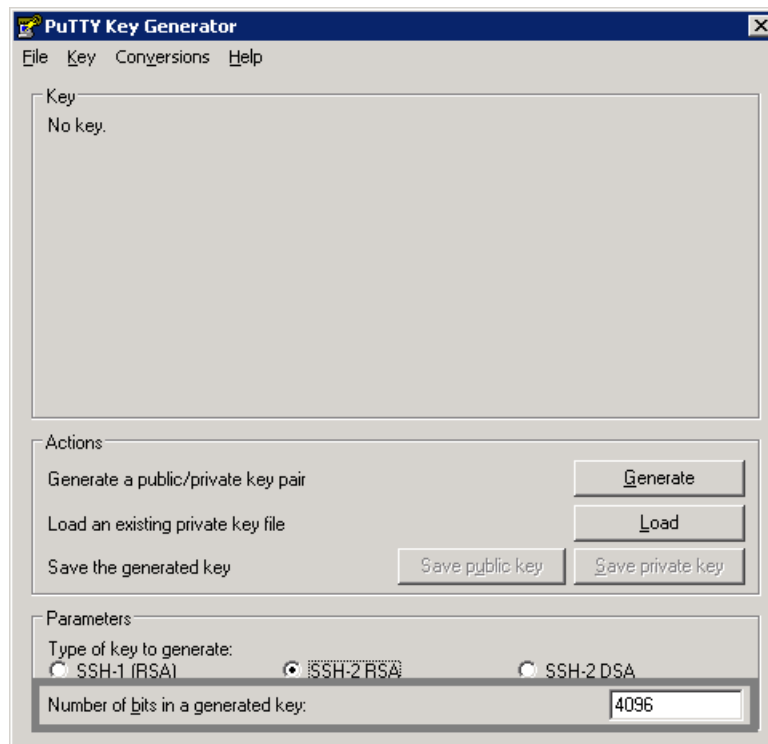


Figure 11

Cliquer sur **Generate** (déplacer la souris dans le cadre gris pendant l'opération), indiquer une passphrase pour protéger la clé par un mot de passe, enregistrer la clé privée **Save private key**, donner un nom à ce fichier puis copier la clé publique affichée dans le cadre (Figure 2).

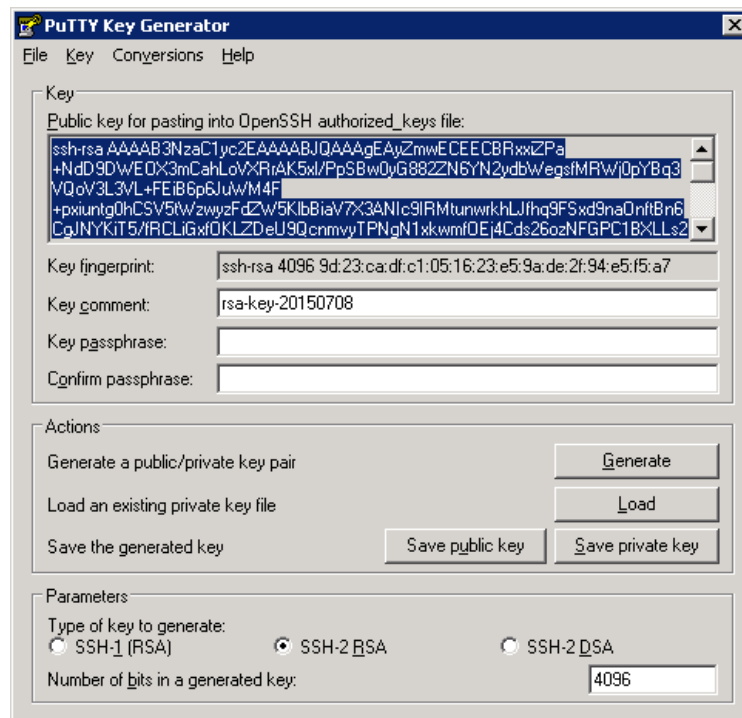


Figure 12

d. Connexion en SSH sur la machine virtuelle

<ftp://ftp.chiark.greenend.org.uk/users/sgtatham/putty-latest/x86/putty.exe> Démarrer **Putty** (Putty est le client SSH le plus répandu pour Windows).

Entrer l'adresse de la machine ainsi que le port ssh.

Dans la liste sur la gauche, cliquer sur **Connection** puis **SSH**, puis **Auth**. A la ligne **Private key file for authentication**, cliquer sur **Browse**, sélectionner la clé privée, valider (Figure 3).

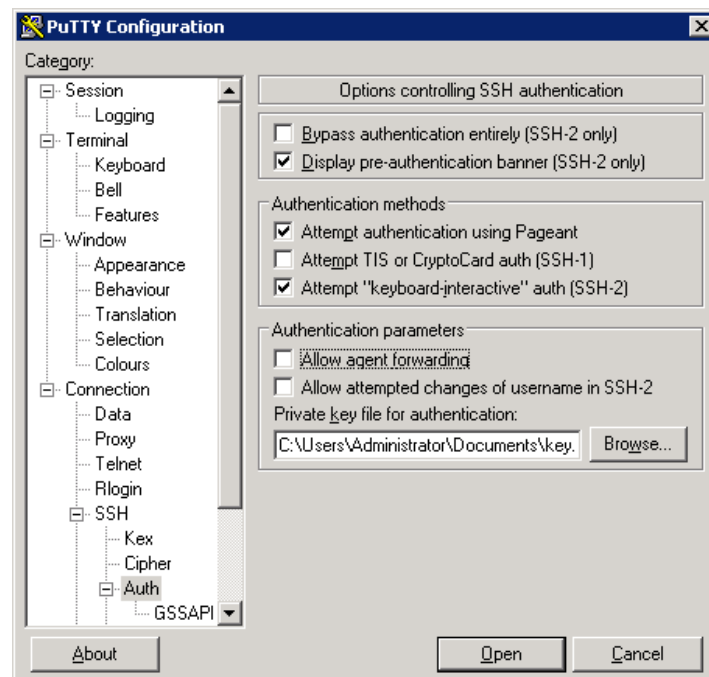


Figure 13