Document de conception
SAE S4.Deploi.01

Tristan Petit, Nils Hubert, Toni Rey,
Majd El Sebeiti , Vianney Miquel

28 mars 2025

Table des matières

1 Introduction

En charge de l'IT pour l'entreprise PLETER, spécialisée dans l'animation 3D, un secteur fortement dépendant de l'informatique, il est essentiel de mettre en place une infrastructure réseau robuste et sécurisée, capable de répondre à tous les besoins de l'entreprise. Cette infrastructure doit également être conçue pour supporter l'ensemble des logiciels et systèmes d'exploitation nécessaires aux équipes créatives et de développement, afin de garantir une compatibilité optimale avec les outils utilisés (ex. : Blender, Adobe Creative Cloud, logiciels Autodesk, Unreal Engine, Cinema 4D, etc.).

Lors de la phase de réflexion du projet, nous avons décidé d'utiliser Proxmox afin de virtualiser nos machines. L'objectif initial était d'utiliser QEMU sur le serveur interne de notre IUT (ASSR) pour faire tourner une machine virtuelle disposant de suffisamment de ressources afin d'héberger notre infrastructure.

Avec Proxmox, comme nous avons des hyperviseurs réunis dans un cluster, nous améliorons les performances tout en complexifiant la tâche. En effet, les interfaces VLAN de Proxmox rendent la configuration des routeurs, qui permettent de connecter des VMs à travers les hyperviseurs, plus complexe. Nous avons les VxLAN de l'interface Proxmox, qui doivent inclure les hyperviseurs, mais sans relier directement les VMs, à l'exception de la VM routeur qui sera connectée à un hyperviseur Proxmox.

D'autres approches sont sans doute possibles, mais c'est la piste sur laquelle nous travaillons actuellement.

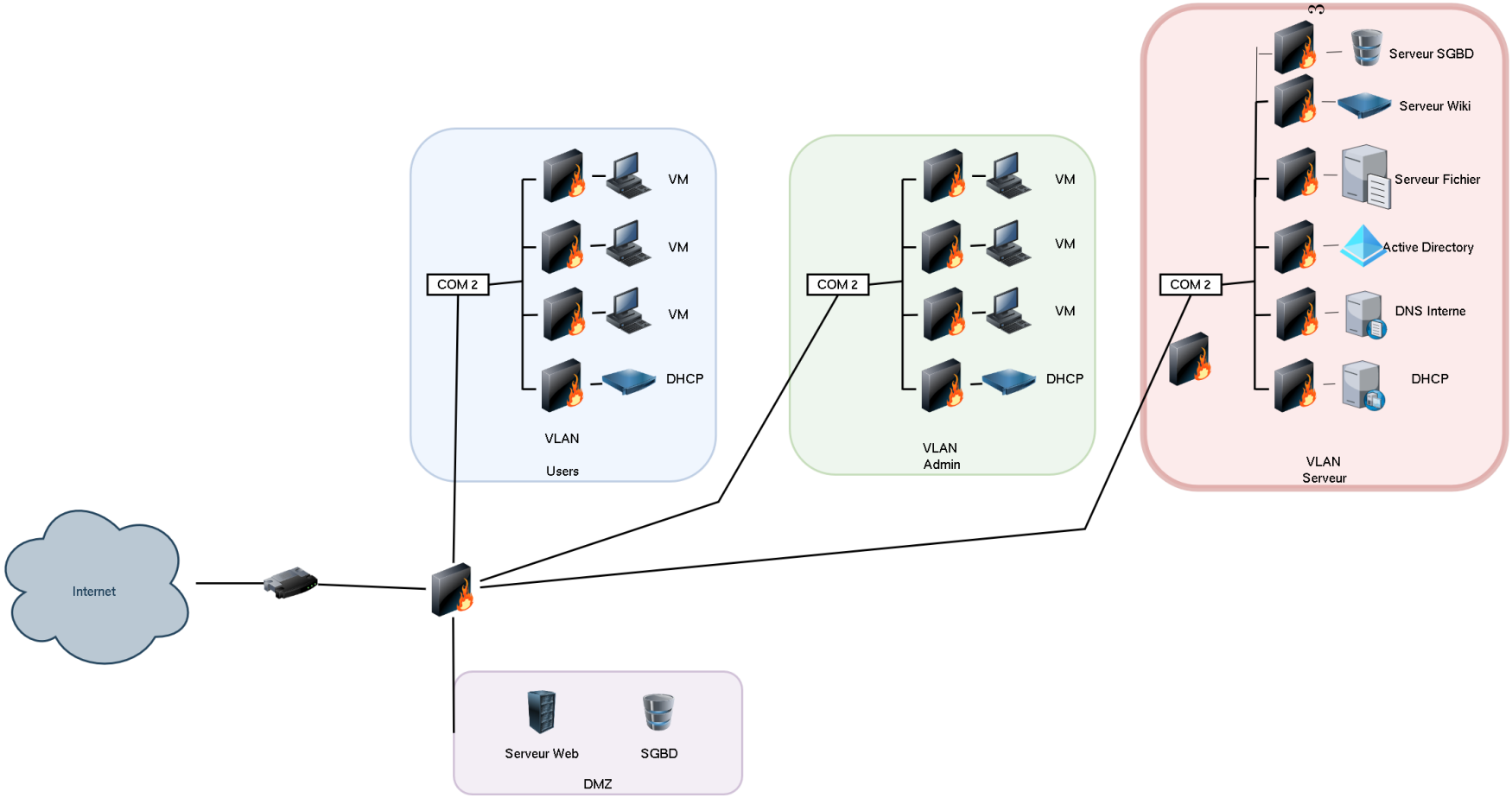
Afin de gagner du temps sur la partie réalisation, la plupart des tâches récurrentes, comme la configuration des serveurs DHCP qui alimenteront chaque sous-réseau, ont été automatisées. Les tests de connectivité permettent ainsi de valider le bon fonctionnement du réseau sans rencontrer de problèmes particuliers.

2 Rappel et évolution sur l'architecture

L'architecture que nous avons imaginée n'ayant pas encore été mise en place, nous n'avons, pour le moment, effectué aucune modification significative. Il nous reste à déterminer la méthode de configuration d'un routeur capable de connecter les machines virtuelles entre elles à travers les hyperviseurs, de manière transparente.

À ce jour, une seule modification a été réalisée : la configuration du routeur. Nous avons opté pour un routeur unique, chargé de relier les différents réseaux, qui sont représentés ici sous forme de VLANs. Chaque VLAN possède son propre serveur DHCP. Le routeur doit donc être configuré pour rediriger les requêtes DHCP des machines vers le serveur correspondant, et inversement.

Un service DNS sera également déployé dans la DMZ pour assurer la résolution des noms de domaine. Ce service sera constitué de deux serveurs DNS : l'un situé dans la DMZ pour résoudre les noms externes et l'autre dans l'intranet des serveurs, pour gérer les noms internes.


Internet
COM 2
VM
VM
VM
DHCP
VLAN
Users
COM 2
VM
VM
VM
DHCP
VLAN
Admin
COM 2
Serveur SGBD
Serveur Wiki
Serveur Fichier
Active Directory
DNS Interne
DHCP
VLAN
Serveur
Serveur Web
SGBD
DMZ

3 Scripte crée

Listing 1 – script test de l'ip

```
#!/bin/bash
shopt -s globstar nullglob

for element in "$(pwd)"/**;
  do
    if [[ -f $element ]]; then
        extension="${element##*.}"

        if [[ $extension == "aux" ]] || [[ $extension == "fls" ]] ||
        [[ $extension == "log" ]] || [[ $extension == "toc" ]] ||
        [[ $extension == "gz" ]]|| [[ $extension == "fdb_latexmk" ]]; then
            rm "$element"
        fi
      fi
  done
```

Listing 2 – Mon script Bash

```
    #!/bin/bash
shopt -s globstar nullglob

for element in "$(pwd)"/**;
  do
    if [[ -f $element ]]; then
        extension="${element##*.}"

        if [[ $extension == "aux" ]] || [[ $extension == "fls" ]] ||
        [[ $extension == "log" ]] || [[ $extension == "toc" ]] ||
        [[ $extension == "gz" ]]|| [[ $extension == "fdb_latexmk" ]]; then
            rm "$element"
        fi
      fi
  done
```

4 Ressources utilisées

Pour notre SAE, nous avons réuni les machines dans un cluster pour interconnecter nos hyperviseurs et mutualiser les ressources qui sont réparties à travers nos hyperviseurs.

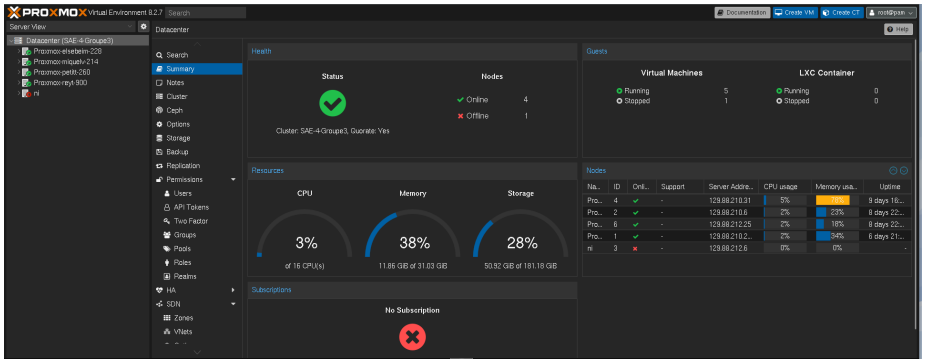


FIGURE 2 – Ressource utilisée pour la SAE sous proxmox

L'avantage de cette configuration par rapport à celle présente sur ASSR, c'est que nous n'avons pas de machines virtuelles imbriquées, ce qui permet d'améliorer de manière significative les performances.
Le CPU est la ressource qui pose le moins de problème dans notre cas, il en est tout autre pour la RAM. Celle-ci devra être gérée de manière équitable entre les hyperviseurs pour éviter une surcharge. Le stockage ne devrait pas poser de problème majeur, mais pourrait le devenir si nous étions dans l'obligation d'ajouter de nouvelles machines.

5 Documentation Technique

5.1 DNS Interne

Ce réseau abrite un contrôleur de domaine Active Directory responsable de la gestion du domaine **local.pleter.ovh**. Afin d'assurer un fonctionnement optimal du domaine, il est recommandé que la gestion des domaines soit confiée au serveur DNS de Windows Server. Toutefois, pour éviter toute surcharge du serveur principal et garantir la redondance, un autre serveur DNS sera déployés pour l'ensemble de l'infrastructure. Un mécanisme de transfert de zone DNS sera mis en place via IXFR et sécurisé par TSIG. Ainsi, le serveur DNS intégré de Windows Server agira en tant que serveur principal, tandis qu'un serveur DNS Bind9 sera configuré en tant que serveur esclave. Le serveur DNS Bind9 assurera principalement la résolution DNS pour l'infrastructure, mais le serveur DNS Windows Server restera accessible comme serveur secondaire. Pour renforcer la sécurité des requêtes DNS, le protocole DoH (DNS over HTTPS) sera implémenté sur les deux serveurs DNS. Ces serveurs fonctionneront également en tant que résolveurs DNS récursifs et garantiront l'authenticité des réponses grâce à DNSSEC.

5.2 DNS Externe

L'infrastructure comprend une DMZ avec plusieurs serveurs de PLETER. Afin de garantir un accès fluide à ces serveurs depuis Internet via un nom de domaine, un serveur DNS Bind9 sera déployé dans la DMZ pour gérer la résolution des noms ***.pleter.ovh**. Il ne couvrira toutefois pas le sous-domaine interne **local.pleter.ovh**. Pour assurer l'intégrité des réponses, ce serveur mettra en œuvre DNSSEC sur sa zone, tout en proposant les services DoH et DoT (DNS over TLS) pour sécuriser les communications.