

05/06/2024

Ruben Rouvière  
Arnaud Pruvost  
Robin Semene

Mathys Domergue  
Alexis Opolka  
Enzo Cadere

# Coordination MAE-RAR

## TL;DR: Architecture réseau

**Réseau : 172.16.1.0/24**

**Réseau VPN: 172.16.234.0/24**

**Réseau VMs communes: 172.16.3.0/24**

**Réseau interconnexion : 172.16.4.0/24**

**Réseau VMs MAE: 172.16.5.0/24**

**Réseau VMs RAR: 172.16.6.0/24**

- DNS: <http://172.16.6.51:5380/>

**Réseau coté salle:**

- 10.202.166.1 Proxmox MAE
- 10.202.166.2 Proxmox RAR
- 10.202.166.10 Routeur MAE
- 10.202.166.11 Routeur RAR

# Analyse sujet

## Réseau

- BGP Inter-équipes
- 1 routeur / VMs, qui annonce en OSPF les microservices hébergés par cette VM ?
  - OSPF vers l'hyperviseur et les autres VMs
  - Arista et frr-routing
  - => Implique que on a plusieurs VMs qui hébergent nos microservices

## Architecture 1: OSPF pur + BGP

OSPF entre chaque VM

- Containerlab sur chaque VM :(
  - Configuration manuelle des routes en /32 pour chaque microservice
- Containerlab sur les proxmox :)
  - Redistribuer en BGP
- Sauf que: vu que VXLAN entre les proxmox, on va avoir des adjacences entre les VMs des différents noeuds. -> Pas terrible côté BGP
- Intérêt quand même: loadbalancing intégré (route la plus proche)
- Conclusion: Pas convaincu: pas forcément utile...

## Architecture 2: BGP pure avec les autres équipes

VXLAN entre les nodes (shared L2), BGP entre les autres équipes (pas entre MAE et RAR)

- Pas d'OSPF, vu qu'on a VXLAN
- On annonce pas les VMs vu qu'on est sur le même L2
- Load-Balancing en VIP ou en Consul via HAProxy.
- Ca n'aurait pas de sens par contre de faire du BGP entre RAR et MAE vu que VXLAN
- Conclusion: Problématique d'un point de vue DHCP, vu qu'on partage un L2.

## Archi 3: Annonce BGP entre VMs et proxmox

- On retombe sur le problème de IPAM.
  - Enfaite il nous manquerait une solution de network mesh style K8s
- Pas de sens si on partage un L2 en VXLAN
- L'intérêt principal c'est pour une archi Top-Of-Rack où on termine le L3 au premier node de sortie.
- Conclusion: Pas de sens dans notre cas.

05/06/2024

Ruben Rouvière  
Arnaud Pruvost  
Robin Semene

Mathys Domergue  
Alexis Opolka  
Enzo Cadiere

## Architecture 4: OSPF entre les deux proxmoxs, BGP avec les autres équipes

- OSPF entre les deux proxmox (via VM bridgé sur le réseau ITCO).
- PAS de VXLAN, partager un L2 c'est pas pertinent.
- Chaque proxmox a son propre réseau pour ses VMs
- Conclusion: on part sur ça

## Services réseaux

### Communs MAE RAR

- DNS (Mathys):
  - Unbound
  - Ou Technitium (webUI et une gestion des utilisateurs)
- Consul (Aksel)
- Nautobot
- Equilibreur de charge commun (HAProxy: consul template) à toutes les équipes (lequel ??????????)
  - Avis ruben: Vive traefik

### Instance par équipe:

- Harbor (Mathys, xxxx côté RAR)
- Portainer (Mathys, xxxx côté RAR)
- Supervision (côté RAR: Uptime Kuma, côté MAE : Uptime Kuma et Wazuh)
- Wordpress IUT Béziers
- Nextcloud
- Kanban (Weakan)
- Tout en playbook ansible

## Services applicatifs cloud conteneurisés:

# Rappel du sujet

## Cahier des charges

### réseau

- Un réseau bgp pour vous connecter aux autres équipes et un réseau ospf interne qui permettra d'accéder à vos microservices. Ce réseau de routeurs containérisés sera implémenté à l'aide containerlab (<https://containerlab.dev/>). Il sera composé de deux types de routeurs containérisés : arista et fr-routing.
- Un infrastructure virtualisée avec la solution Cloud OpenNebula (<https://opennebula.io/>). Vous disposez d'un serveur pour deux personnes. Un stockage partagé NFS permettra de survivre à l'arrêt d'un serveur pour les containers redondés. Les serveurs dans l'idéal seront sur le même plan d'adressage mais reliés à l'aide du protocole vxlan ou genève.(ethernet dans udp)
- Votre infrastructure sera accessible via un vpn Wireguard (firezone..) et vous mettrez en place un bastion ssh (téléport..).

### **Vous devez donc implémenter à minima les services réseaux suivants:**

- Un DNS (unbound) en haute disponibilité derrière un équilibreur de charge.
- Un registry de service Consul (<https://www.consul.io/>)
- Un registry Harbor.
- Un système de supervision de vos réseaux et de vos microservices.
- Une source de vérité (nautobot) commune à tous les groupes.
- Un équilibreur de charge de type haproxy (avec consul template) pour la haute disponibilité commun à tous les groupes.

### **Services applicatifs cloud conteneurisés suivants à destination des usagers:**

- Un serveur web IUT à base d'un "Content" Management System" comme celui de l'IUT de Béziers. HA proxy assurera l'équilibrage de charge et la haute disponibilité.
- Un serveur Nextcloud.
- Un Kanban de votre choix. (wekan...) qui vous servira à suivre le projet.
- Les containers seront déployables à l'aide de playbook ansible.

Une solution de management (Portainer,rancher) devra être utilisé pour piloter vos containers. Un durcissement des containers est souhaité ( limits, rootless..).

Vous devrez aussi réaliser de l'automatisation par script ( Python, Ansible) par exemple pour alimenter Nautobot ou Consul ou produire des états.

Un compte-rendu écrit et un repos git par groupe sont obligatoires.

05/06/2024

Ruben Rouvière  
Arnaud Pruvost  
Robin Semene

Mathys Domergue  
Alexis Opolka  
Enzo Cadere

## **Critères d'évaluation de la SAE:**

### **Critères pour le groupe:**

- Conformité au CCTP.
- Clarté des schémas réseaux.
- Haute disponibilité de l'infrastructure.
- Sécurité de l'infrastructure.
- Organisation.
- Ecrits.
- Esprit et outils DevOps
- Soutenance orale.

### **Critères individualisables:**

- Communication.
- Quantité de travail.
- Evaluation par les pairs.
- Soutenance orale.