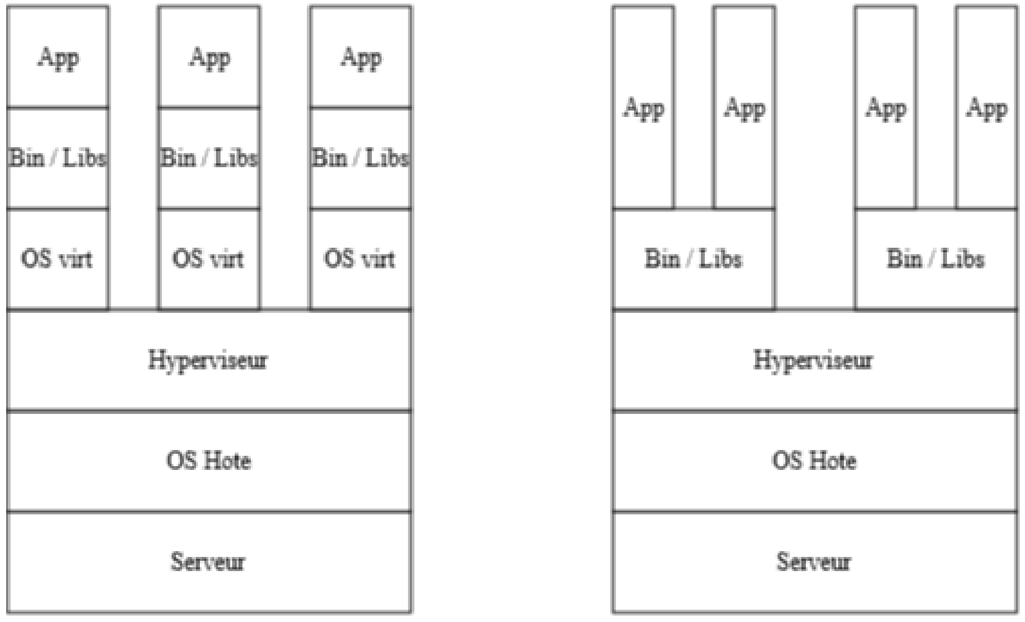
Docker en production : retour d'expérience au CDGP

Réunion X/stra - 19 octobre 2017

Thiébaut Mochel

Principe de virtualisation par conteneurs



Comparaison de solutions de conteneurisation

Solution Linux	Modification noyau Linux	Modification système de fichiers	Modifications réseaux
OpenVZ	o - noyau modifié	x	x
LXC	x - cgroups / namespaces	o - dir btrfs lvm overlayfs zfs	o - veth macvlan vlan phys
rkt (systemd-nspawn)	x - cgroups / namespaces	o - overlay fs	o - bridge
Docker	x - cgroups / namespaces	o - aufs, devicemapper, overlay2, overlay, zfs, vfs	o - libnetwork bridge, overlay, remote et plugins weave, calico, ...

Autres OS

OS	Conteneurs
FreeBSD	Jails
Solaris	Zones
Windows 10 ou Server 2016	Windows Container (avec Windows Server Core ou Nano Server)

Choix de la distribution de linux

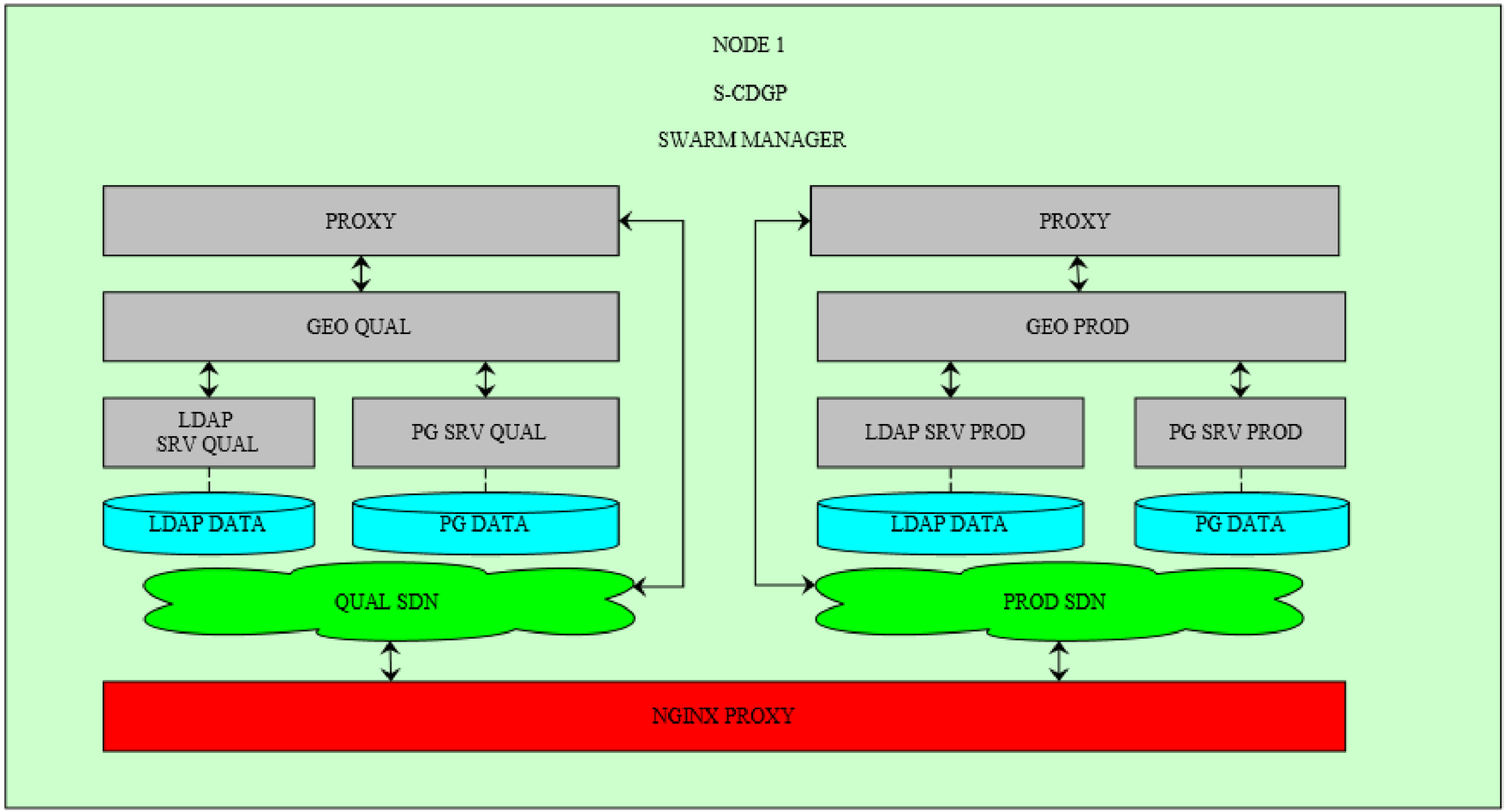
OS	Exemples	Avantages	Inconvénients
Multi-usages	Debian Ubuntu Centos OpenSuse	Choix des packages	Performances des conteneurs
Spécifiques conteneurs	RancherOS Redhat Atomic Mesosphere DC/OS open-source	Tâches séparées	Compatibilité matérielle Extensibilité hôte limitée

Sources de codes ou données

Compilation de l'image

Méthode	Language	Avantages	Inconvénients
Dockerfile	Shell + Instructions docker	Inclus dans docker	Maintenance complexe (bash)
Ansible-container	Ansible YAML	Portable multi-distributions Ansible-galaxy Inclus démarrage des conteneurs	Fonctionnalités récentes non disponibles
Packer	JSON (Builder, Provisionner, Post-processor)	Multi-formats (sources identique pour image Docker, LXC, Virtualbox, ...)	Développement plus long

Cluster docker swarm



Méthode de déploiement des conteneurs

Méthode	Format	Commentaire
docker-compose	YAML	Compatible systemd
ansible-container	YAML	Limité à Ansible-container

Planification des tâches

Méthode	Options	Commentaires
Service docker	Restart : unless-stopped, on-failure, always	Les conteneurs liés sont également redémarrés
Systemd	docker run, compose ou stack	Ordre des conteneurs et process hors docker Systemd timer possible

Sécurité

Filtrage IPtables :

Utilisation d'iptables-persistent avec plage d'IPs des réseaux overlays
Utilisation de DOCKER-USER pour le filtrage INPUT

Niveau applicatif

Multi-process dans un conteneur docker avec supervisord
Utilisation d'un ou plusieurs conteneurs proxy - Apache ou Nginx / Openresty

Supervision des conteneurs et traitement des logs

Supervision en mode texte (console) : dry
Supervision mode web : Shipyard (prévu)
Logging : Logstach (prévu)
Supervision complète : Prometheus (prévu)

Conclusion : perspectives

Backup et snapshot des conteneurs
Implémentation d'un plug-in volume (Convoy, Portworx, ...)