OpenShift 4.3 : sécurité renforcée sur la voie du cloud hybride

Déployer des clusters avec des équilibreurs de charge isolés du réseau Internet ? OpenShift le permet désormais sur AWS, Azure et GCP.

La dernière version (4.3) de la plate-forme de conteneurs, basée sur Kubernetes 1.16, apporte d'autres avancées dans le domaine du cloud hybride. Notamment la possibilité de mettre en place, sur ces trois mêmes plates-formes, des clusters au sein de VPN et de VPC existants (ainsi que sur leurs sous-réseaux).

Ces nouveautés s'accompagnent d'un renforcement de la sécurité. Avec en particulier :

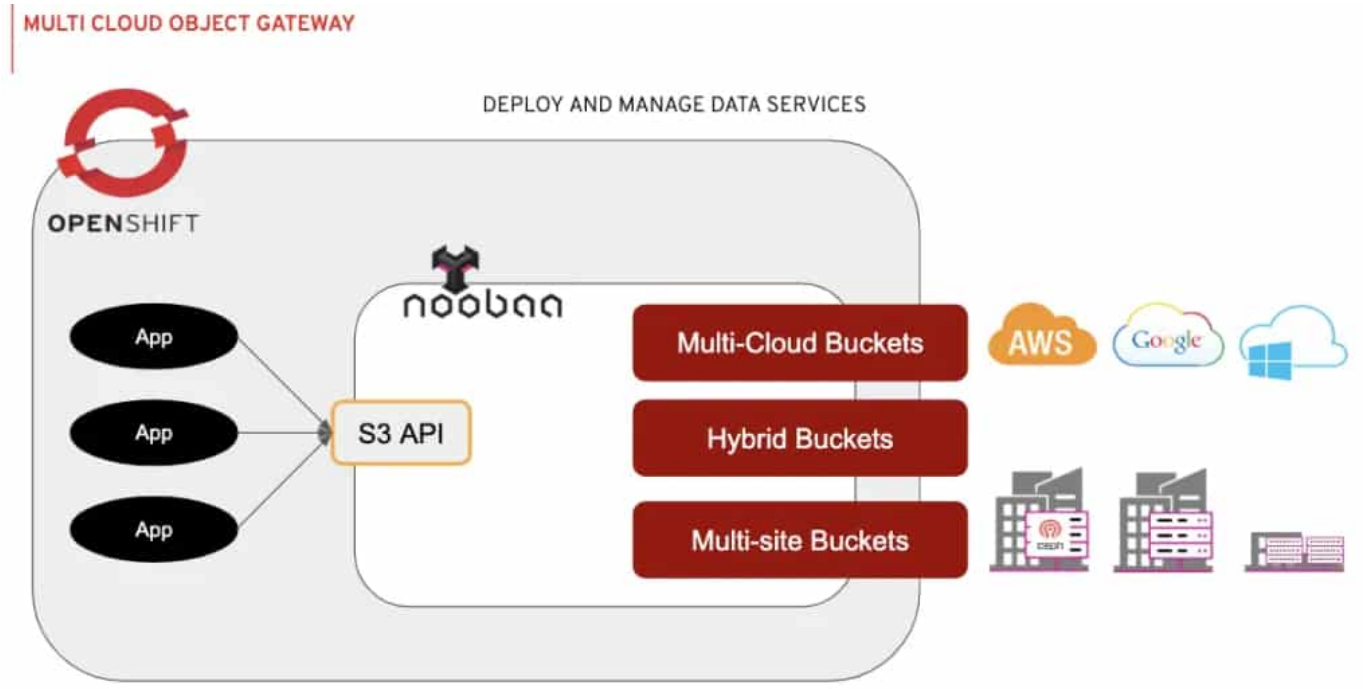
- Intégration du chiffrement FIPS 140-2 niveau 1
  Le paquet go-toolset permettait déjà, depuis quelques mois, de faire appel à une bibliothèque FIPS sur Red Hat Enterprise Linux. Cette fonctionnalité est maintenant intégrée à OpenShift.
- Prise en charge du chiffrement d'etcd, la base de données clé-valeur utilisable comme mémoire de sauvegarde pour les clusters.
- Possibilité d'utiliser NBDE (chiffrement de disques sur machines virtuelles et physiques sans avoir à entrer un mot de passe à chaque démarrage). Et ainsi, entre autres, d'automatiser l'activation à distance des volumes LUKS.

Le cloud hybride avec NooBaa

Parallèlement à OpenShift 4.3, Red Hat rend disponible la v4 de son système de stockage logiciel OpenShift Container Storage.

Il y intègre la technologie de l'entreprise israélienne NooBaa, acquise fin 2018.

Sous le nom Multi-Cloud Object Gateway, la technologie en question apporte une couche d'abstraction destinée à favoriser la portabilité des données entre clouds.



OpenShift Container Storage 4 progresse par ailleurs sur la rapidité de création de volumes persistants.

Red Hat fait la jonction avec Rook pour l'orchestration de ces voumes et avec Quay pour faciliter la recherche de vulnérabilités dans les images de conteneurs.

Photo d'illustration © Red Hat