OpenSearch passe en production sans gouvernance définie

Quelle gouvernance pour OpenSearch ? On n'a toujours pas la réponse. Sous cette marque, Amazon pousse un *fork* d'Elasticsearch et de Kibana, dans la continuité de son Open Distro. Voilà six mois qu'il a donné le coup d'envoi officiel du projet. Red Hat et SAP font partie des grands noms de l'IT qui s'y sont ralliés depuis.

Dans un premier temps, les travaux se sont faits exclusivement en interne. Ils ont d'abord consisté à éliminer tout code non place sous licence Apache 2.0. Cela a impliqué la suppression de près de 5 millions de lignes, essentiellement liées au fameux dossier x-pack. Lequel a accompagné le développement du modèle *open core* (cœur fonctionnel ouvert + modules additionnels prioritaires) sur la pile EKS (Elasticsearch et Kibana, ainsi que Beats et Logstash).

OpenSearch avait pris une dimension communautaire en avril, avec l'ouverture des dépôts au public. Sur le volet gouvernance, l'approche qui dominait alors au sein de la communauté était celle d'un comité de direction « d'amorçage » qui réunirait des représentants d'entreprises intéressées pour contribuer au projet. Que ce fût sur cette proposition ou sur celle du transfert à une fondation, Amazon n'avait pas tranché. Expliquant qu'il était trop tôt pour choisir un cap, il s'était positionné comme « coordinateur ». Dans la pratique, ses équipes valident toutes les contributions.

Aux dernières nouvelles, rien n'a changé. Et on ne nous offre pas davantage de perspectives. La *roadmap* technique, au contraire, est précise. Amazon se projette jusqu'à 2022, avec la v2.0 d'OpenSearch en ligne de mire. Pour le moment, on en est à la 1.0, publiée la semaine passée. Elle se fonde sur Elasticsearch et Kibana 7.10.2.

OpenSearch : SIEM et *machine learning* en fin d'année ?

Parmi les éléments ajoutés depuis l'ouverture aux contributions externes, on aura noté :

- Version Linux ARM64
- Streaming sur les visualisations
- Filtrage par attributs pour les fragments de traces
- Planification
- Prise en charge des locataires dans le *plug-in* Notebooks
- Support des transformations pour la gestion des index

La version 1.1, prévue pour fin août, doit notamment apporter :

- Paquets DEB, RPM et macOS pour x64 et ARM64 (et image Docker pour ARM64)
- Réplication entre clusters
- Centralisation des notifications
- Alertes au niveau des documents

- Gestion des requêtes d'indexation au niveau des *shards*
- Pour la détection d'anomalies, un *workflow* unique et des améliorations de la haute cardinalité (pagination, multiples champs catégoriques…)

Avec la version 1.2, prévue pour novembre, il est question d'intégrer une composante SIEM ouverte et un framework d'apprentissage automatique.

Amazon fournit des garanties pour la transition vers OpenSearch. En particulier le fait que toutes les *releases* 1.x seront compatibles avec Elasticsearch 7.10. Même si certaines API disparaîtront…

Photo d'illustration © agsandrew – Shutterstock