Conteneurs : AWS prend de la distance avec Docker

AWS Fargate et Docker Engine, c'est fini.

La nouvelle version (1.4) du moteur de calcul *serverless* associé aux offres ECS et EKS utilise Containerd pour l'exécution des conteneurs.

Il en va, affirme AWS, d'une simplification de l'architecture du plan de données de Fargate.

La démarche s'inscrit dans la lignée d'une prise de distance progressive avec les composantes de la pile Docker (schématisée ci-dessous).

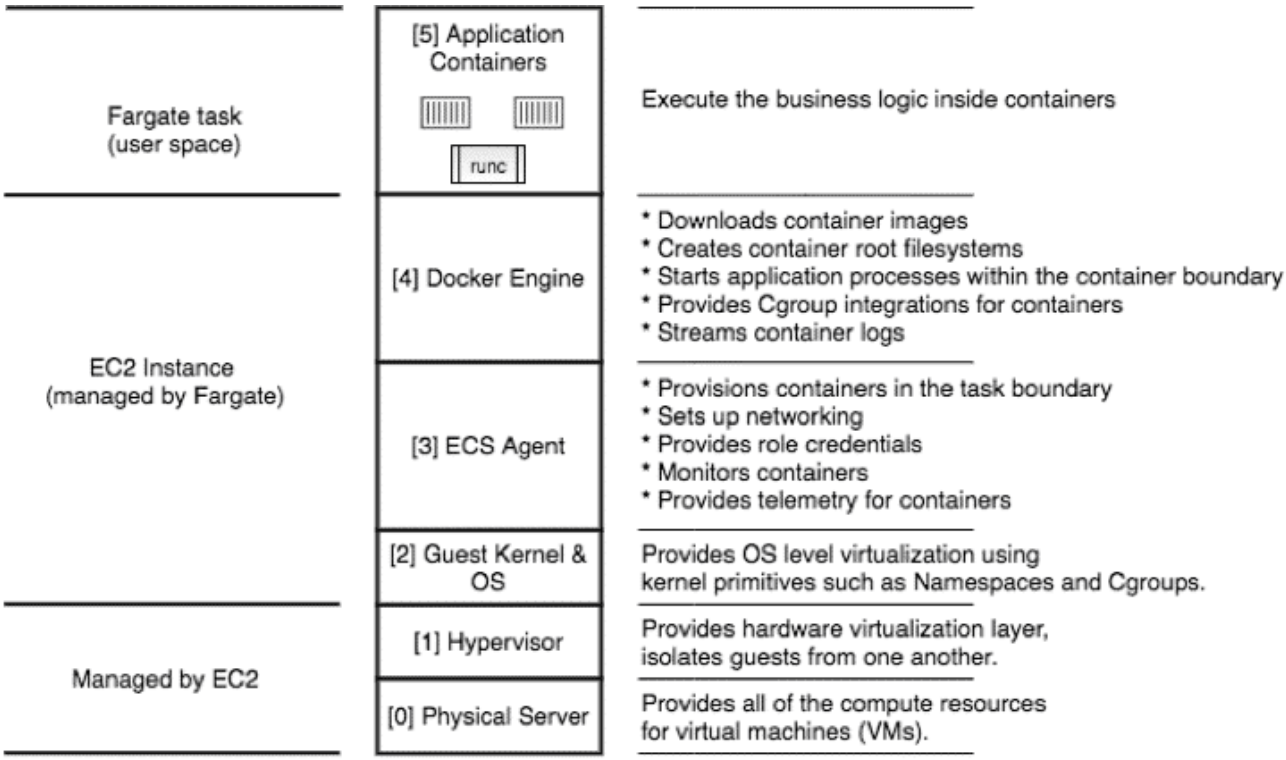


Figure 1: Fargate data plane stack with Docker Engine

Illustration sur la gestion du réseau. Aux fonctions natives de Docker Engine, AWS a substitué des *plug-in* qui apportent notamment la prise en charge des VPC dans les conteneurs.

Autre exemple : la journalisation. Pour en élargir les capacités, une jonction a été établie avec FireLens. Il en a résulté, entre autres, des options de filtrage à la source et de paramétrage de destinations multiples pour les logs.

De même, pour permettre le partage d'informations entre conteneurs dans une même tâche, AWS a choisi de passer par un point de terminaison HTTP local plutôt que d'appeler directement le moteur d'exécution.

L'argument sécurité est évoqué non seulement sur ce dernier point, mais aussi de manière générale, l'architecture de la pile Containerd réduisant d'autant la quantité de code.

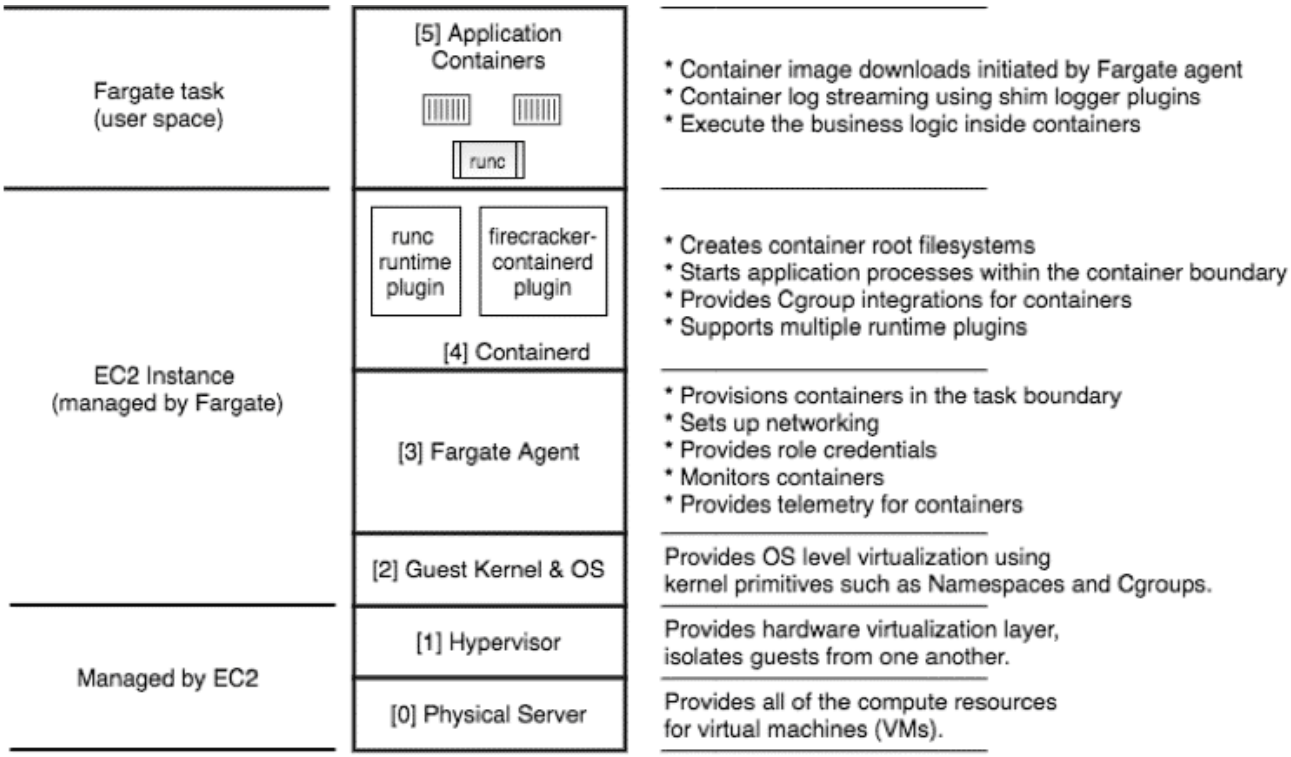
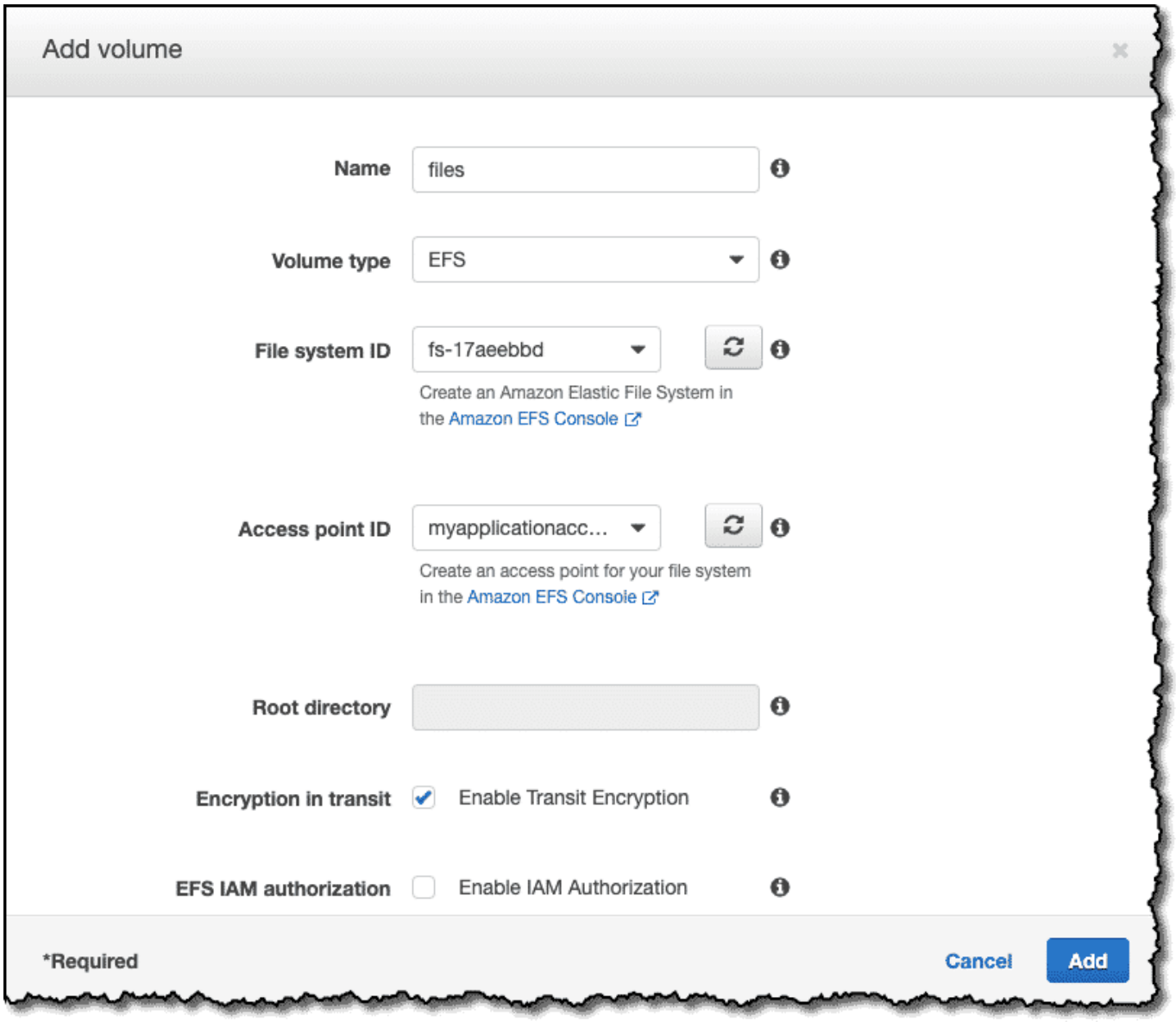


Figure 2: Fargate data plane stack with Containerd

Pour orchestrer les conteneurs sur les instances Fargate, Containerd travaillera de concert avec un nouvel agent qui remplace celui d'ECS jusqu'alors utilisé.

Du *stateful* en *serverless*

Fargate 1.4, c'est aussi la prise en charge des volumes EFS. Et donc des applications *stateful*, qu'on ne pouvait jusqu'alors déployer faute d'un accès à la configuration des instances EC2 (la nature même du *serverless*).



Chaque tâche Fargate a désormais à sa disposition un volume de stockage temporaire de 20 Go. On peut consommer cette capacité de façon plus flexible qu'auparavant, où elle était divisée en deux volumes de taille fixe (4 et 10 Go). Ce changement s'applique aussi aux pods EKS exécutés sur Fargate.

Il y a également du nouveau sur le monitoring. En plus des indicateurs de performance CPU, mémoire et disque, on peut faire remonter vers CloudWatch Container Insights des données relatives au réseau.

Ces données peuvent aussi remonter vers des outils tiers *via* la dernière version (v4) de la fonction ECS Task Metadata Endpoint. Laquelle peut par ailleurs désormais récupérer la zone de disponibilité où sont déployées les tâches Fargate.

AWS ajoute aussi, sur toutes les versions de Fargate, une première capacité Linux : CAP_SYS_TRACE, pour le suivi de processus. La branche cloud d'Amazon avance doucement sur ces intégrations au nom du risque sécuritaire.

Illustrations © AWS