Une approche multicouche de la sécurité des conteneurs et de Kubernetes

Sécuriser les conteneurs, de la création à l'exécution

Table des matières

facebook.com/redhatinc
@RedHat_France
linkedin.com/company/red-hat

Introduction

Les conteneurs suscitent beaucoup d'intérêt grâce à leur capacité à regrouper les applications et leurs dépendances dans une seule image qui peut être promue d'un environnement d'exécution à un autre : développement, test, production. Ils simplifient la cohérence au sein des environnements et sur diverses cibles de déploiement, telles que les serveurs physiques, les machines virtuelles et les clouds publics et privés. Grâce aux conteneurs, les équipes peuvent développer et gérer plus facilement les applications qui assurent l'agilité de l'entreprise.

- **Applications :** les conteneurs permettent aux développeurs de simplifier la création et la promotion d'une application et de ses dépendances en tant qu'unité. Les conteneurs peuvent être déployés en quelques secondes seulement. Dans un environnement conteneurisé, le processus de création de logiciels est l'étape du cycle de vie où le code de l'application est intégré aux bibliothèques d'exécution nécessaires.
- **Infrastructure :** les conteneurs représentent des processus d'application en sandbox sur un noyau de système d'exploitation Linux® partagé. Ils sont plus compacts et légers que les machines virtuelles, et moins complexes. De plus, ils sont portables au sein de vos différents environnements, à savoir, sur site, sur les plateformes de cloud public, etc.

Kubernetes est la plateforme d'orchestration de conteneurs idéale pour les environnements d'entreprise. Aujourd'hui, de nombreuses entreprises exécutent des services essentiels sur les conteneurs. Il n'a donc jamais été aussi important de garantir leur sécurité. Ce document décrit les éléments clés de la sécurité des applications conteneurisées.

Sécurité complète des conteneurs et de Kubernetes : couches et cycle de vie

La sécurisation des conteneurs s'apparente à celle de n'importe quel processus Linux exécuté. Vous devez penser à sécuriser toutes les couches de la pile de la solution avant de déployer et d'exécuter votre conteneur, mais également à assurer la sécurité tout au long du cycle de vie de l'application et du conteneur. La sécurité doit être un processus continu, intégré tout au long du cycle de vie de l'environnement informatique, qui doit s'étendre pour englober les nouvelles menaces et solutions à mesure qu'elles apparaissent. La Figure 1 montre une approche complète de la sécurité des conteneurs.

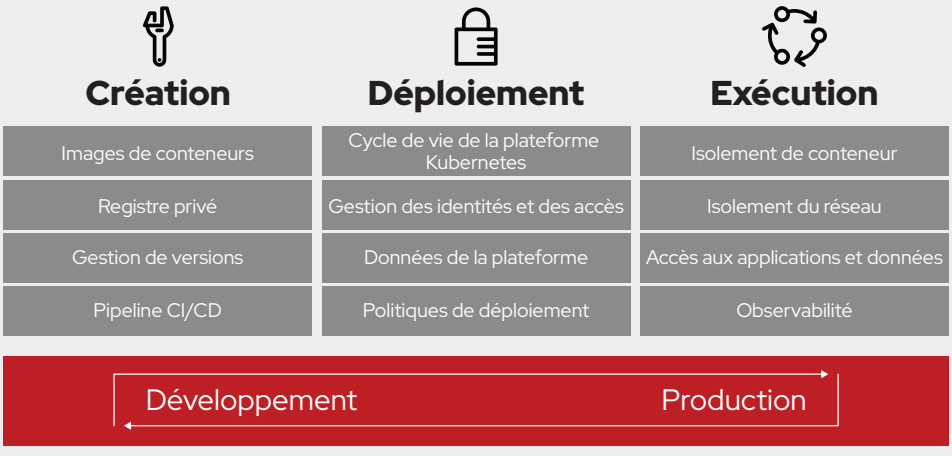

Figure 1. Pour sécuriser totalement un conteneur, il faut sécuriser la création, le déploiement et, si besoin, l'exécution à l'aide d'outils spécialisés.

Les conteneurs permettent aux développeurs de simplifier la création et la promotion d'une application et de ses dépendances en tant qu'unité. Ils vous aident également à valoriser au mieux vos serveurs en permettant le déploiement d'applications multi-clients sur un hôte partagé. Vous pouvez facilement déployer plusieurs applications sur un seul hôte en activant et en arrêtant des conteneurs individuels selon vos besoins. Avec les conteneurs, pas besoin d'hyperviseur pour gérer les systèmes d'exploitation invités sur chaque machine virtuelle, car ils virtualisent vos processus d'applications, pas votre matériel, ce qui n'est pas le cas avec la virtualisation traditionnelle.

Bien entendu, les applications sont rarement distribuées dans un seul conteneur. Même les applications simples ont généralement un front-end, un back-end et une base de données. Le déploiement des applications modernes basées sur des microservices dans des conteneurs implique de déployer plusieurs conteneurs, sur le même hôte ou répartis sur plusieurs hôtes ou nœuds, comme le montre la Figure 2.

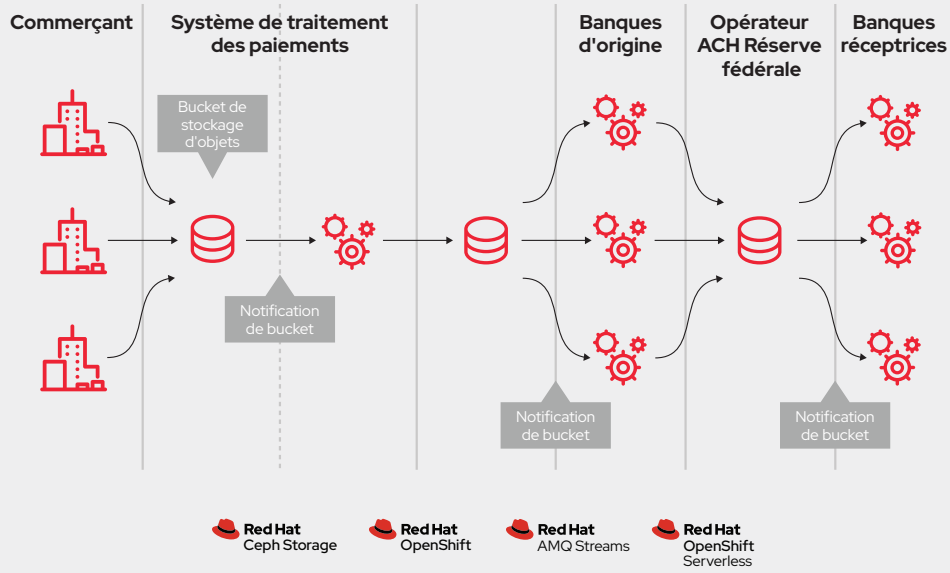

Figure 2. Les environnements de conteneurs peuvent être complexes et répartis sur plusieurs nœuds.

Lorsque vous gérez des conteneurs à grande échelle, vous devez vous poser les questions suivantes :

- Quels conteneurs doivent être déployés ? Sur quels hôtes ?
- Quel hôte a la plus grande capacité ?
- Quels conteneurs doivent avoir accès les uns aux autres, et comment vont-ils se détecter ?
- Comment contrôler l'accès aux ressources partagées et leur gestion ? (Par exemple le réseau et le stockage)
- Comment surveiller l'intégrité des conteneurs ?
- Comment mettre à l'échelle automatiquement la capacité de l'application pour répondre à la demande ?
- Comment proposer le libre-service aux développeurs tout en répondant aux exigences de sécurité ?

Vous pouvez soit créer votre propre environnement de gestion des conteneurs, ce qui nécessite de passer du temps à intégrer et gérer les différents éléments, soit déployer une plateforme de conteneurs avec des fonctions de gestion et de sécurité intégrées. Cette deuxième approche permet à votre équipe de concentrer son énergie sur ce qui rapporte, c'est-à-dire vos applications, plutôt que de réinventer l'infrastructure.

La solution Red Hat® OpenShift® Container Platform constitue une plateforme Kubernetes d'entreprise hybride et cohérente, pour créer et mettre à l'échelle des applications conteneurisées. L'utilisation de Kubernetes à l'échelle de l'entreprise nécessite des mesures de protection supplémentaires qui vous aident à développer la sécurité au sein de vos applications, à automatiser les politiques qui gèrent la sécurité du déploiement des conteneurs et à protéger l'environnement d'exécution.

Intégrer la sécurité dans les applications

Pour le déploiement des applications cloud-native, il est essentiel que la sécurité soit intégrée. Voici comment procéder :

1. Utilisez un conteneur dont le contenu est fiable.
2. Utilisez un registre de conteneurs d'entreprise.
3. Contrôlez et automatisez la création des conteneurs.
4. Intégrez la sécurité au pipeline des applications.

1. Utilisez un conteneur dont le contenu est fiable

Pour bien gérer la sécurité d'un conteneur, vous devez vous intéresser à son contenu. Depuis un certain temps déjà, les applications et infrastructures sont constituées de composants préconçus. Nombre d'entre eux sont des paquets Open Source, tels que le système d'exploitation Linux, le serveur web Apache, la plateforme Red Hat JBoss® Enterprise Application Platform, PostgreSQL et Node.js. Des versions conteneurisées de ces paquets sont également disponibles pour que vous n'ayez pas à créer les vôtres. Toutefois, comme pour n'importe quel code que vous téléchargez à partir d'une source externe, vous devez chercher à connaître l'origine de ces paquets, leur créateur et les potentiels dangers qu'ils renferment. Posez-vous les questions suivantes :

- Le contenu du conteneur va-t-il compromettre mon infrastructure ?
- Existe-t-il des vulnérabilités connues dans la couche applicative ?
- Les couches d'exécution et du système d'exploitation dans le conteneur sont-elles à jour ?
- À quelle fréquence le conteneur est-il mis à jour et comment les mises à jour sont-elles signalées ?

Depuis des années, Red Hat met en paquet et distribue du contenu Linux de confiance sur la plateforme Red Hat Enterprise Linux et l'ensemble de nos produits. Aujourd'hui, Red Hat fournit ce même contenu fiable dans des conteneurs Linux. Avec les images de conteneurs universelles Red Hat, vous pouvez profiter de la fiabilité, de la sécurité et des performances des images de conteneurs Red Hat là où s'exécutent les conteneurs Linux conformes à l'Open Container Initiative (OCI). Cela signifie que vous pouvez créer une application conteneurisée sur une image de conteneurs universelle Red Hat, la transférer vers le registre de conteneurs de votre choix et la partager.

Red Hat fournit également un grand nombre d'images et d'opérateurs certifiés pour différents langages d'exécution, middlewares, bases de données, et plus encore via le catalogue Red Hat Ecosystem Catalog. Les conteneurs et opérateurs certifiés Red Hat s'exécutent partout où la plateforme Red Hat Enterprise Linux s'exécute : du serveur bare metal aux machines virtuelles en passant par le cloud. De plus, ils sont pris en charge par les logiciels de Red Hat et de ses partenaires.

Red Hat surveille en permanence l'intégrité des images fournies. L'indicateur Container Health Index montre la « note » de chaque image de conteneur et donne le détail sur la manière dont elles doivent être conservées, consommées et évaluées pour répondre aux besoins des systèmes de production. Un conteneur est noté en partie en fonction de l'âge et de l'impact des errata de sécurité non appliqués à tous ses composants. La note représente une évaluation globale de la sécurité de ce conteneur qui peut être comprise aussi bien par les spécialistes que par les non-spécialistes.

Au moment du lancement des mises à jour de sécurité (par exemple des correctifs pour runc CVE-2019-5736, MDS CVE-2019-11091 ou VHOST-NET CVE-2019-14835), Red Hat recrée également les images de conteneurs et les transfère vers le registre public. Les avis de sécurité Red Hat vous signalent tout problème détecté dans les images de conteneurs certifiés et vous dirigent vers l'image mise à jour afin qu'à votre tour, vous mettiez à jour toutes les applications qui utilisent cette image.

Si vous avez besoin d'un contenu que Red Hat ne fournit pas, utilisez des outils d'analyse des conteneurs qui s'appuient sur des bases de données de vulnérabilités mises à jour en continu. Ainsi, vous serez sûr de disposer des informations les plus récentes concernant les vulnérabilités connues lorsque vous utiliserez des images de conteneurs provenant d'autres sources. Attention : la liste des vulnérabilités connues évolue constamment. Aussi, en plus de vérifier le contenu de vos images de conteneurs au moment de les télécharger, vous devrez continuer à suivre l'état des vulnérabilités pour toutes vos images approuvées et déployées, comme Red Hat le fait pour ses images de conteneur.

2. Utilisez un registre de conteneurs d'entreprise pour un accès plus sécurisé aux images de conteneurs

Vos équipes créent des conteneurs qui ajoutent du contenu sur les images des conteneurs publics que vous téléchargez. Vous devez donc gérer l'accès aux images de conteneurs téléchargées et créées en interne (ainsi que leur promotion) de la même manière que vous gérez les autres types de binaires. Il existe un certain nombre de registres privés qui prennent en charge le stockage des images de conteneurs. Red Hat vous recommande de choisir un registre privé qui vous aide à automatiser les politiques d'utilisation des images de conteneurs stockées dans le registre.

La plateforme Red Hat OpenShift inclut un registre privé qui offre des fonctions de base pour gérer vos images de conteneurs. Ce registre fournit un contrôle d'accès basé sur les rôles qui vous permet de choisir les rôles autorisés à ajouter et extraire des images de conteneurs spécifiques. La plateforme Red Hat OpenShift prend également en charge l'intégration d'autres registres privés, tels que Artifactory et Sonatype Nexus de JFrog.

Le registre d'images Red Hat Quay est disponible en tant que registre d'entreprise autonome. Il offre de nombreuses fonctions supplémentaires pour les entreprises, telles que la réplication géographique et les déclencheurs de création d'images.

Le projet Clair est un moteur Open Source qui alimente l'outil d'analyse de sécurité du registre Red Hat Quay et lui permet de détecter les vulnérabilités de toutes les images qu'il contient. L'opérateur de sécurité des conteneurs de Red Hat OpenShift s'intègre à Red Hat Quay pour fournir une vue globale des vulnérabilités connues pour les images déployées dans la console OpenShift.

3. Contrôlez et automatisez la création des images de conteneurs

La gestion de ce processus de création est essentielle à la sécurisation de la pile logicielle. Avec la philosophie « créer une fois, déployer partout », le produit du processus de création correspond exactement à ce qui est déployé en production. Il est également important de garantir l'immuabilité des conteneurs, ce qui signifie qu'au lieu d'appliquer des correctifs aux conteneurs en cours d'exécution, vous devez les recréer et les redéployer.

La plateforme Red Hat OpenShift offre un certain nombre de possibilités pour automatiser les créations basées sur des événements externes afin d'améliorer la sécurité de vos images personnalisées.

- Les déclencheurs du registre Red Hat Quay ont un mécanisme qui génère la création de référentiel d'un Dockerfile à partir d'un événement externe tel qu'un push GitHub, BitBucket ou GitLab ou un webhook.
- Source-to-image (S2I) est un framework Open Source qui permet de combiner le code source et les images de base (Figure 3). Il aide vos équipes de développement et d'exploitation à collaborer facilement dans un environnement de création reproductible. Lorsqu'un développeur archive du code avec git sous S2I, la plateforme Red Hat OpenShift peut :
  - Déclencher l'assemblage automatique d'une nouvelle image à partir des artefacts disponibles, y compris l'image de base S2I, et du code nouvellement archivé (via des webhooks sur le référentiel de code ou un autre processus automatisé d'intégration continue)
  - Déployer automatiquement l'image créée pour la tester
  - Promouvoir l'image testée en production et la déployer automatiquement par le biais du processus d'intégration et de déploiement continus (CI/CD).

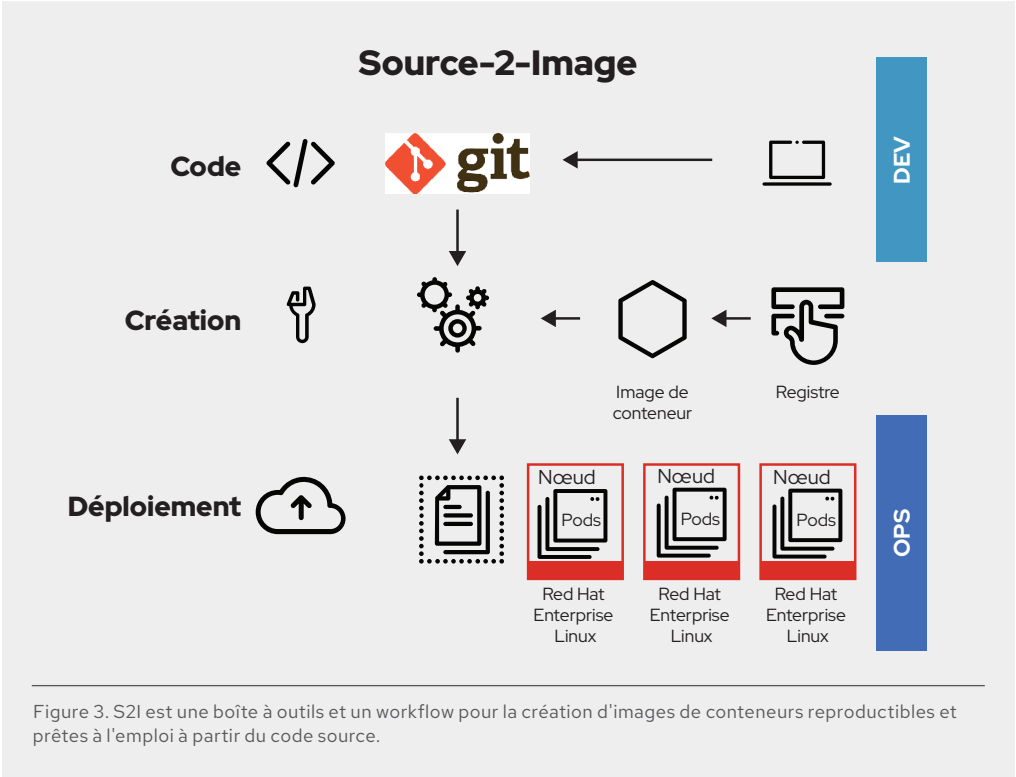

Figure 3. S2I est une boîte à outils et un workflow pour la création d'images de conteneurs reproductibles et prêtes à l'emploi à partir du code source.

- Les flux d'images Red Hat OpenShift peuvent servir à observer les changements apportés aux images externes déployées dans votre cluster. Les flux d'images fonctionnent avec toutes les ressources cloud-native disponibles sur la plateforme Red Hat OpenShift, notamment les créations ou les déploiements, les tâches, les contrôleurs de réplication ou les ensembles de réplicas. En surveillant un flux d'images, les créations et déploiements peuvent recevoir des notifications lors de l'ajout ou de la modification de nouvelles images et réagir en lançant automatiquement une tâche de création ou de déploiement, respectivement.

  Par exemple, prenons une application créée avec trois couches d'image de conteneur : la base, le middleware et la couche applicative. Un problème est détecté dans l'image de base et celle-ci est recréée par Red Hat, puis transférée vers le catalogue Red Hat Ecosystem Catalog. Lorsque les flux d'images sont activés, la plateforme Red Hat OpenShift détecte que l'image a changé. Pour les créations qui dépendent de cette image et qui disposent de déclencheurs, la plateforme recrée automatiquement l'image de l'application, en intégrant l'image de base réparée.

  Une fois la création terminée, l'image personnalisée mise à jour est transférée vers le registre interne de la plateforme OpenShift. Celle-ci détecte immédiatement les modifications apportées aux images dans son registre interne et, pour les applications avec déclencheurs, elle déploie automatiquement l'image mise à jour. Cette action garantit que le code exécuté en production est toujours identique à l'image la plus récente. Toutes ces capacités travaillent ensemble pour intégrer des capacités de sécurité dans votre processus et votre pipeline de CI/CD.

4. Intégrez la sécurité au pipeline des applications.

La plateforme Red Hat OpenShift intègre des instances de Jenkins pour l'intégration continue, et Tekton, un pipeline de CI/CD Kubernetes de nouvelle génération qui fonctionne pour les conteneurs (y compris sans serveur). Elle inclut aussi des API RESTful riches que vous pouvez utiliser pour intégrer vos propres outils de création ou de CI/CD, y compris un registre d'images privé.

Une bonne pratique de sécurisation des applications consiste à intégrer des tests de sécurité automatisés dans votre pipeline, y compris votre registre, votre environnement de développement intégré (IDE) et vos outils de CI/CD.

Registre : les images des conteneurs peuvent et doivent être analysées dans votre registre privé de conteneurs. Vous pouvez utiliser le registre Red Hat Quay avec l'outil d'analyse de sécurité Clair pour avertir les développeurs lorsque des vulnérabilités sont détectées. L'opérateur de sécurité des conteneurs d'OpenShift s'intègre à Red Hat Quay pour fournir une vue globale des vulnérabilités connues pour les images déployées dans la console OpenShift. Il existe également plusieurs solutions d'analyse de conteneurs tierces et certifiées dans le catalogue Red Hat Ecosystem Catalog.

IDE : les plug-ins de l'environnement de développement intégré Red Hat Dependency Analytics fournissent des alertes de vulnérabilité et des conseils de correction pour les dépendances du projet lorsque le code est introduit pour la première fois dans l'environnement.

CI/CD : les outils d'analyse peuvent être intégrés au processus d'intégration continue pour rechercher en temps réel les vulnérabilités répertoriées dans le catalogue dans les paquets Open Source de votre conteneur. Ils vous informent en cas de détection d'une vulnérabilité connue et vous préviennent lorsque de nouvelles vulnérabilités sont détectées dans les paquets précédemment analysés.

Par ailleurs, votre processus d'intégration continue doit inclure des politiques qui signalent les problèmes détectés lors des analyses de sécurité, afin que votre équipe puisse prendre les mesures nécessaires pour les régler le plus rapidement possible.

Enfin, nous vous recommandons de signer les conteneurs créés sur mesure afin de vous assurer qu'ils ne sont pas altérés entre le moment de leur création et leur déploiement.

Gestion de la configuration, sécurité et conformité de vos déploiements

Pour sécuriser efficacement vos déploiements, vous devez sécuriser la plateforme Kubernetes et automatiser les politiques de déploiement. La plateforme Red Hat OpenShift comprend les fonctions prêtes à l'emploi suivantes :

1. Configuration de la plateforme et gestion du cycle de vie
2. Gestion des identités et des accès
3. Sécurisation des données de la plateforme et du stockage associé
4. Politiques de déploiement

5. Configuration de la plateforme et gestion du cycle de vie

L'audit de sécurité Kubernetes de la fondation Cloud Native Computing Foundation (CNCF) publié durant l'été 2019 a conclu que la plus grande menace pour la sécurité de Kubernetes résidait dans la complexité de la configuration et du renforcement de ses composants. La solution Red Hat OpenShift résout ce problème grâce aux opérateurs Kubernetes.

Un opérateur est une méthode qui permet de mettre en paquet, déployer et gérer une application native pour Kubernetes. Il agit comme un contrôleur personnalisé qui peut étendre l'API Kubernetes avec la logique spécifique à l'application requise pour la gérer. Chaque composant de la plateforme Red Hat OpenShift est contenu dans un opérateur, ce qui permet d'automatiser la configuration, la surveillance et la gestion. Les opérateurs individuels configurent directement les composants tels que le serveur d'API et la mise en réseau logicielle, tandis qu'un opérateur de cluster gère plusieurs opérateurs sur la plateforme. Les opérateurs vous permettent d'automatiser la gestion des clusters, y compris les mises à jour, du noyau aux services situés plus haut dans la pile.

Les plateformes de conteneurs offrent aux développeurs un accès en libre-service, et c'est là l'un de leurs principaux avantages. Vos équipes de développement fournissent ainsi plus facilement et plus rapidement des applications créées sur des couches approuvées. Un portail en libre-service donne à vos équipes suffisamment de contrôle pour favoriser la collaboration tout en assurant la sécurité. L'opérateur Operator Lifecycle Manager fournit le framework qui permet aux utilisateurs du cluster Red Hat OpenShift de trouver et d'utiliser des opérateurs pour déployer les services nécessaires au fonctionnement de leurs applications. Avec cet outil, les utilisateurs peuvent installer, mettre à jour et attribuer un contrôle d'accès basé sur les rôles aux opérateurs disponibles.

Pour garantir la conformité, la plateforme Red Hat OpenShift fournit l'opérateur Compliance Operator qui permet d'automatiser la conformité de la plateforme avec les contrôles techniques requis par les frameworks de conformité. Avec cet opérateur, les administrateurs de Red Hat OpenShift peuvent décrire l'état de conformité souhaité d'un cluster et obtenir une vue d'ensemble des lacunes et des moyens de les corriger. Il évalue la conformité de toutes les couches de la plateforme, y compris des nœuds qui exécutent le cluster. Enfin, l'opérateur File Integrity Operator permet d'effectuer régulièrement des contrôles d'intégrité des fichiers sur les nœuds du cluster.

6. Gestion des identités et des accès

Étant donné l'étendue des fonctions de Kubernetes, tant pour les développeurs que pour les administrateurs, votre plateforme de conteneurs doit absolument offrir une gestion des identités et un contrôle d'accès basé sur les rôles solides. Les API Kubernetes sont essentielles pour automatiser la gestion des conteneurs à grande échelle. Elles servent notamment à envoyer et valider des requêtes, y compris pour configurer et déployer des pods et des services.

L'authentification et l'autorisation des API sont indispensables pour sécuriser votre plateforme de conteneurs. Le serveur d'API est un point d'accès central qui doit bénéficier du niveau de surveillance maximal. Sur le plan de contrôle de la plateforme Red Hat OpenShift, l'authentification est assurée par l'opérateur Cluster Authentication Operator. Pour s'authentifier

auprès de l'API, les développeurs, administrateurs et comptes de service doivent obtenir des jetons d'accès OAuth. Si vous êtes administrateur, vous pouvez configurer le fournisseur d'identité de votre choix pour le cluster afin que les utilisateurs puissent s'authentifier avant de recevoir un jeton. Neuf fournisseurs d'identité sont pris en charge, y compris les répertoires LDAP (Lightweight Directory Access Protocol).

L'option détaillée du contrôle d'accès basé sur les rôles est activée par défaut sur la plateforme Red Hat OpenShift. Les objets du contrôle d'accès basé sur les rôles déterminent si un utilisateur est autorisé à effectuer une action donnée au sein d'un groupe. Les administrateurs du cluster peuvent utiliser les rôles et les liens du cluster pour contrôler les niveaux d'accès au cluster OpenShift et aux projets au sein du cluster.

7. Sécurisation des données de la plateforme

Par défaut, la plateforme Red Hat OpenShift renforce Kubernetes pour assurer la sécurité des données en transit. Elle comprend également des options pour sécuriser les données au repos.

Pour protéger ses données en transit, la plateforme Red Hat OpenShift recourt aux mécanismes suivants :

- Chiffrement des données en transit via le protocole HTTPS pour tous les composants de la plateforme de conteneurs qui communiquent entre eux
- Envoi de toutes les communications avec le plan de contrôle via le protocole TLS (Transport Layer Security)
- Vérification des certificats X.509 ou des jetons pour l'accès au serveur d'API
- Utilisation de quotas de projets pour limiter les dommages que pourrait causer un jeton non autorisé
- Configuration du magasin etcd avec sa propre autorité de certification (CA) et ses propres certificats (dans Kubernetes, etcd stocke l'état persistant du maître, tandis que les autres composants surveillent les modifications apportées dans etcd pour adapter leur état en conséquence)
- Rotation automatique des certificats de plateforme

Pour protéger ses données au repos, la plateforme Red Hat OpenShift recourt aux mécanismes suivants :

- Chiffrement facultatif des disques Red Hat Enterprise Linux CoreOS et du magasin de données etcd pour renforcer la sécurité
- Respect des normes FIPS (Federal Information Processing Standards) pour Red Hat OpenShift : FIPS 140-2 est une norme de sécurité développée par le gouvernement des États-Unis, utilisée pour approuver les modules de chiffrement. Lorsque Red Hat Enterprise Linux CoreOS est lancé en mode FIPS, les composants de la plateforme Red Hat OpenShift appellent les modules de chiffrement de Red Hat Enterprise Linux.

Les conteneurs sont utiles à la fois pour les applications à état et sans état. La plateforme Red Hat OpenShift prend en charge le stockage éphémère et persistant. La protection du stockage associé est un élément clé de la sécurisation des services à état. La plateforme Red Hat OpenShift prend en charge plusieurs types de stockage, notamment le NFS (Network File System), les Elastic Block Stores (EBS) d'Amazon Web Services (AWS), Persistent Disk de Google Compute Engine, Azure Disk, iSCSI et Cinder.

En outre, Red Hat OpenShift Container Storage est un système de stockage logiciel persistant, intégré et optimisé pour la plateforme Red Hat OpenShift Container Platform. Hautement évolutif et persistant, il stocke les applications cloud-native qui nécessitent des fonctions telles que le chiffrement et la réplication ainsi qu'une disponibilité élevée dans le multicloud hybride.

- Les options de montage d'un **volume persistant** sur un hôte dépendent du fournisseur de ressources. Les fournisseurs offrent des capacités différentes et les modes d'accès de chaque volume persistant sont réglés sur les modes spécifiques pris en charge par chaque volume particulier. Par exemple, le système NFS peut prendre en charge plusieurs clients en lecture/écriture, toutefois certains volumes persistants NFS ne peuvent être exportés sur le serveur qu'en lecture seule. Chaque volume persistant reçoit son propre ensemble de modes d'accès qui décrit ses capacités spécifiques, notamment ReadWriteOnce, ReadOnlyMany et ReadWriteMany.
- Pour le **stockage partagé** (par exemple NFS, Ceph, Gluster), il faut que l'identifiant de groupe du volume persistant de stockage partagé soit enregistré sous la forme d'une annotation dans la ressource du volume persistant. Ainsi, lorsque le pod revendique ce volume, son identifiant de groupe est ajouté aux groupes supplémentaires du pod et lui donne accès au contenu du stockage partagé.
- Pour le **stockage en mode bloc** (par exemple EBS, GCE Persistent Disk, iSCSI), les plateformes de conteneurs peuvent utiliser les capacités du module SELinux pour sécuriser la racine du volume monté pour les pods non privilégiés. Ainsi, le volume monté est détenu, et visible, seulement par le conteneur auquel il est associé.

N'hésitez pas non plus à tirer parti des fonctions de sécurité disponibles dans la solution de stockage que vous avez choisie.

8. Automatisation du déploiement basé sur les politiques

Afin de garantir un niveau de sécurité élevé, vous aurez besoin de politiques automatisées pour gérer le déploiement des conteneurs et des clusters.

- Déploiement de conteneurs basé sur des politiques

Les clusters Red Hat OpenShift peuvent être configurés pour autoriser ou non l'extraction d'images spécifiques d'un registre. En production, la meilleure pratique consiste à n'autoriser le déploiement d'images qu'à partir de votre registre privé.

Le plug-in du contrôleur d'admission des contraintes de contexte de sécurité de la plateforme Red Hat OpenShift définit un ensemble de conditions qu'un pod doit respecter pour être accepté dans le système. Les **contraintes de contexte de sécurité** vous permettent d'abandonner des privilèges par défaut. Elles constituent d'ailleurs la meilleure pratique et il est important de les utiliser. Les contraintes de contexte de sécurité de Red Hat OpenShift garantissent que, par défaut, aucun conteneur privilégié n'est exécuté sur les nœuds de calcul OpenShift. L'accès aux identifiants du réseau hôte et du processus hôte est refusé par défaut.

Toutefois, les utilisateurs qui disposent des autorisations requises peuvent, s'ils le souhaitent, assouplir les politiques par défaut de ces contraintes.

La solution Red Had Advanced Cluster Management for Kubernetes fournit des fonctions de **gestion avancée du cycle de vie des applications** en utilisant des normes ouvertes pour déployer des applications grâce à des politiques de placement intégrées dans les pipelines CI/CD et contrôles de gouvernance existants.

- Gestion de plusieurs clusters basée sur des politiques

Le déploiement de plusieurs clusters peut être utile pour fournir des applications hautement disponibles dans plusieurs zones de disponibilité, ou des fonctionnalités de gestion commune des déploiements ou migrations entre plusieurs fournisseurs de cloud, tels qu'Amazon Web Services (AWS), Google Cloud et Microsoft Azure. Lorsque vous gérez plusieurs clusters, vos outils d'orchestration doivent fournir le niveau de sécurité dont vous avez besoin sur les différentes instances déployées. Comme toujours, la configuration, l'authentification et l'autorisation sont essentielles, tout comme la gestion des politiques d'application dans les clusters et la capacité à transmettre des données en toute sécurité à vos applications, quel que soit leur environnement d'exécution. La solution Red Had Advanced Cluster Management for Kubernetes fournit les capacités suivantes :

- **La gestion du cycle de vie de plusieurs clusters** : permet de créer, mettre à jour et détruire des clusters Kubernetes de manière fiable et cohérente à grande échelle
- **La gouvernance axée sur les risques et la conformité** : utilise des politiques pour configurer et garantir automatiquement la cohérence des contrôles de sécurité conformément aux normes des entreprises du secteur. Vous pouvez également spécifier une politique de conformité à appliquer dans un ou plusieurs clusters gérés.

Protection des applications en cours d'exécution

Au-delà de l'infrastructure, il est essentiel d'assurer le bon fonctionnement de la sécurité des applications. Pour sécuriser vos applications conteneurisées, il faut :

1. Isoler les conteneurs
2. Isoler les applications et les réseaux
3. Sécuriser l'accès aux applications
4. Assurer l'observabilité

9. Isoler les conteneurs

Pour tirer pleinement parti des technologies de mise en paquet et d'orchestration des conteneurs, l'équipe d'exploitation a besoin d'un environnement adapté aux conteneurs. Il leur faut un système d'exploitation capable de sécuriser les conteneurs aux frontières, qui protège le noyau hôte contre les fuites de conteneurs et protège les conteneurs les uns des autres.

Les conteneurs sont des processus Linux qui isolent et confinent les ressources, ce qui permet d'exécuter des applications en sandbox sur un noyau hôte partagé. Pour sécuriser les conteneurs, vous devez adopter la même approche que pour les autres processus exécutés sous Linux.

Le document NIST special publication 800-190 du National Institute of Standards and Technology recommande l'utilisation d'un système d'exploitation optimisé pour les conteneurs afin de renforcer la sécurité. Red Hat Enterprise Linux CoreOS, le système d'exploitation de base de la plateforme Red Hat OpenShift, réduit la surface d'attaque en minimisant l'environnement hôte et en l'adaptant aux conteneurs. Il ne contient que les paquets nécessaires à l'exécution de Red Hat OpenShift et son espace utilisateur est en lecture seule. La plateforme est testée, versionnée et expédiée avec Red Hat OpenShift, et elle est gérée par le cluster. L'installation et la mise à jour de Red Hat Enterprise Linux CoreOS sont automatisées et toujours compatibles avec le cluster. Elle prend également en charge l'infrastructure de votre choix, héritant de la majeure partie de l'écosystème Red Hat Enterprise Linux.

Chaque conteneur Linux qui s'exécute sur une plateforme Red Hat OpenShift est protégé par de puissantes fonctions de sécurité Red Hat Enterprise Linux intégrées dans les nœuds Red Hat OpenShift. Les espaces de noms Linux, SELinux, cgroups, les capacités de Linux et la fonctionnalité de sécurité seccomp sont utilisés pour sécuriser les conteneurs exécutés sur Red Hat Enterprise Linux.

- Les espaces de noms Linux fournissent les bases pour l'isolement des conteneurs. Un espace de noms fait croire à ses processus qu'ils disposent de leur propre instance des ressources globales. Il s'agit d'un espace abstrait qui leur donne l'impression de s'exécuter sur leur propre système d'exploitation à l'intérieur d'un conteneur.
- SELinux fournit une couche de sécurité supplémentaire pour maintenir les conteneurs isolés les uns des autres et de l'hôte. Il permet aux administrateurs d'appliquer des contrôles d'accès obligatoires pour chaque utilisateur, application, processus et fichier. SELinux agit comme un mur de briques qui vous arrête si vous parvenez à sortir de l'espace de noms (accidentellement ou volontairement). Il atténue les vulnérabilités des environnements d'exécution des conteneurs. De bonnes configurations SELinux peuvent empêcher les processus des conteneurs d'échapper à leur confinement.

- cgroups (abréviation de « groupes de contrôle ») est une fonctionnalité qui limite, compte et isole l'utilisation des ressources (CPU, mémoire, E/S disque, réseau, etc.) d'un ensemble de processus. Ces groupes de contrôle permettent d'éviter que les ressources d'un conteneur soient consommées par un autre conteneur hébergé sur le même hôte. Ils servent également à contrôler les pseudo-terminaux, qui sont des vecteurs d'attaque répandus.
- Les capacités de Linux peuvent être utilisées pour verrouiller les privilèges dans un conteneur. Ces capacités sont des unités de privilège distinctes qui peuvent être activées ou désactivées de manière indépendante. Elles permettent par exemple d'envoyer des paquets de protocoles Internet bruts ou de se lier à des ports inférieurs à 1024. Lorsque vous exécutez des conteneurs, vous pouvez désactiver plusieurs capacités sans que cela n'ait d'incidence sur la grande majorité des applications conteneurisées.
- Enfin, un profil seccomp peut être associé à un conteneur pour limiter les appels système disponibles.

10. Isoler les applications et les réseaux

La sécurité de l'architecture multi-client est essentielle pour utiliser Kubernetes à l'échelle de l'entreprise. Une architecture multi-client permet à différentes équipes d'utiliser le même cluster tout en empêchant qu'elles accèdent aux environnements qui ne les concernent pas. La plateforme Red Hat OpenShift prend en charge les architectures multi-clients grâce à une combinaison d'espaces de noms de noyau, de SELinux, de contrôles d'accès basé sur les rôles, d'espaces de noms Kubernetes (projet) et de politiques de réseau.

- **Les « projets » Red Hat OpenShift** sont des espaces de noms Kubernetes avec des annotations SELinux. Ces projets isolent les applications entre les équipes, les groupes et les services. L'accès aux différents projets est contrôlé par des rôles et les liens locaux.
- **Les contraintes de contexte de sécurité** vous permettent d'abandonner des privilèges par défaut. Elles constituent d'ailleurs la meilleure pratique et il est important de les utiliser. Les contraintes de contexte de sécurité de Red Hat OpenShift garantissent que, par défaut, aucun conteneur privilégié n'est exécuté sur les nœuds de calcul OpenShift. L'accès aux identifiants du réseau hôte et du processus hôte est refusé par défaut.

Le déploiement des applications modernes basées sur des microservices dans des conteneurs implique souvent de déployer plusieurs conteneurs répartis sur plusieurs nœuds. Ces microservices ont besoin de se découvrir et de communiquer les uns avec les autres. Pour défendre votre réseau, vous avez besoin d'une plateforme de conteneurs qui vous permette de segmenter le trafic de chaque cluster afin d'isoler les différents utilisateurs, équipes, applications et environnements. Vous avez également besoin d'outils pour gérer l'accès au cluster depuis l'extérieur ainsi que l'accès aux composants externes depuis les services du cluster. Voici les principaux éléments requis pour isoler le réseau :

- **Contrôle du trafic entrant.** La plateforme Red Hat OpenShift inclut le serveur CoreDNS qui fournit aux pods un service de résolution de noms. Le routeur Red Hat OpenShift (HAProxy) prend en charge les Ingress et routes pour fournir un accès externe aux services exécutés dans le cluster. Les deux prennent en charge les politiques « re-encrypt » et « passthrough ». La première permet de déchiffrer et de re-chiffrer le trafic HTTP lors de sa transmission, tandis que la seconde fait passer le trafic sans terminaison TLS.
- **Espaces de noms de réseaux.** Les espaces de noms de réseau constituent la première ligne de défense des réseaux. Chaque ensemble de conteneurs (« pod ») reçoit sa propre adresse IP et une plage de ports auxquels il peut s'associer, ce qui permet d'isoler les réseaux de pods les uns des autres sur le nœud. Les adresses IP des pods sont indépendantes du réseau physique auquel les nœuds de la plateforme Red Hat OpenShift sont connectés.

- **Politiques de réseau.** La mise en réseau logicielle de la plateforme Red Hat OpenShift utilise des politiques de réseau pour assurer un contrôle précis des communications entre les pods. Le trafic du réseau peut être contrôlé depuis et vers n'importe quel pod, sur des ports et dans des directions spécifiques. Lorsque les politiques de réseau sont configurées en mode multi-client, chaque projet obtient son propre identifiant de réseau virtuel, ce qui permet d'isoler les réseaux des projets les uns des autres sur le nœud. En mode multi-client (par défaut), les pods d'un même projet peuvent communiquer entre eux, mais ceux de différents espaces de noms ne peuvent pas envoyer de paquets aux pods ou aux services d'un autre projet, ni en recevoir.
- **Contrôle du trafic sortant.** La plateforme Red Hat OpenShift offre également la possibilité de contrôler le trafic sortant des services exécutés dans le cluster en utilisant soit un routeur, soit un pare-feu. Vous pouvez par exemple utiliser une liste blanche d'adresses IP pour donner accès à une base de données externe.

11. Sécuriser l'accès aux applications

La sécurisation des applications comprend la gestion de l'authentification et de l'autorisation des utilisateurs et des API.

- **Contrôler les accès utilisateur**

Les fonctions d'authentification unique et unifiée (SSO) sur le Web sont un élément clé des applications modernes. Les plateformes de conteneurs peuvent inclure un certain nombre de services conteneurisés pour la création des applications. Red Hat Single Sign-On est un service de fédération et d'authentification unique et unifiée sur le Web prêt à l'emploi, basé sur le projet Keycloak en amont. Ses fonctionnalités s'appuient sur le standard SAML 2.0 ou sur OpenID Connect. Ce service propose des adaptateurs clients pour les plateformes Red Hat Fuse et Red Hat JBoss Enterprise Application Platform. Il permet l'authentification et l'authentification unique et unifiée sur le Web pour les applications Node.js et peut être intégré aux services d'annuaire basés sur le protocole LDAP, notamment Microsoft Active Directory et Red Hat Enterprise Linux Identity Management Le service s'intègre également aux fournisseurs d'identifiants de réseaux sociaux tels que Facebook, Google et Twitter.

- **Contrôler l'accès à l'API**

Les API sont essentielles aux applications composées de microservices. Ces applications disposent de multiples services d'API indépendants, ce qui entraîne une prolifération des points de terminaison de services dont la gouvernance nécessite des outils supplémentaires. Aussi, nous vous recommandons d'utiliser un outil de gestion des API. Red Hat 3scale API Management est un outil qui vous offre une grande variété d'options standard pour l'authentification et la sécurité des API. Ces options sont utilisables seules ou combinables pour fournir des identifiants et contrôler l'accès.

Les fonctions de contrôle d'accès disponibles dans l'outil Red Hat 3scale API Management vont au-delà de la sécurité et de l'authentification de base. En effet, les plans d'application et de compte vous permettent de restreindre l'accès à certains points de terminaison, méthodes et services spécifiques, et d'appliquer des politiques d'accès à des groupes d'utilisateurs. Les plans d'application vous permettent également de fixer des limites de débit pour l'utilisation des API et de contrôler le flux de trafic des groupes de développeurs. Vous pouvez fixer des limites par période pour les appels d'API entrants afin de protéger votre infrastructure et de maintenir la fluidité du trafic. Vous pouvez également déclencher automatiquement des alertes de dépassement pour les demandes qui atteignent ou dépassent les limites de débit, et définir le comportement des applications qui dépassent ces limites.

Sécuriser le trafic des applications

La sécurisation du trafic des applications à l'aide des options d'entrée et de sortie des clusters est détaillée dans la section 10 de ce document. Pour les applications basées sur les microservices, il est tout aussi important de sécuriser le trafic entre les services du cluster. Vous pouvez recourir à un Service Mesh pour cette couche de gestion. Le terme « Service mesh » décrit le réseau de microservices qui compose les applications dans une architecture de microservices distribuée, ainsi que les interactions entre ces microservices.

Basé sur le projet Open Source Istio, le service Red Hat OpenShift Service Mesh ajoute une couche transparente sur les applications distribuées pour gérer la communication entre les services, sans avoir besoin de modifier le code du service. Red Hat OpenShift Service Mesh utilise un opérateur multi-client pour gérer le cycle de vie du plan de contrôle, ce qui vous permet de l'utiliser indépendamment sur plusieurs projets. De plus, il ne nécessite pas de ressources de contrôle d'accès basé sur les rôles en cluster.

Le service Red Hat OpenShift Service Mesh fournit des fonctions de découverte, d'équilibrage de charge et surtout d'authentification et de chiffrement de service à service. La récupération en cas de défaillance, des indicateurs de mesures et des fonctions de surveillance sont également disponibles.

L'adaptateur 3scale Istio Adapter est facultatif et vous permet d'étiqueter un service exécuté dans Red Hat OpenShift Service Mesh.

12. Assurer l'observabilité

La surveillance et l'audit des clusters Red Hat OpenShift sont des aspects importants d'une bonne stratégie de protection du cluster et de ses utilisateurs contre une utilisation inappropriée. C'est pourquoi la plateforme Red Hat OpenShift intègre des fonctionnalités de surveillance et d'audit ainsi qu'une pile de journalisation optionnelle.

Les services d'Openshift Container Platform se connectent à la solution de surveillance intégrée composée de Prometheus et de son écosystème. Les alertes s'affichent sur un tableau de bord. Les administrateurs des clusters peuvent choisir d'activer, ou non, la surveillance des projets définis par les utilisateurs. Les applications déployées sur la plateforme Red Hat OpenShift peuvent être configurées pour tirer profit des composants de surveillance des clusters.

L'audit des événements est une meilleure pratique en matière de sécurité et il est généralement requis pour se conformer aux cadres réglementaires. L'audit Red Hat OpenShift a été conçu selon une approche cloud-native pour assurer à la fois la centralisation et la résilience. Sur la plateforme Red Hat OpenShift, l'audit des hôtes et l'audit des événements sont activés par défaut sur tous les nœuds. Cette plateforme offre une flexibilité extraordinaire pour configurer la gestion et l'accès aux données d'audit. Vous pouvez contrôler la quantité d'informations qui sont consignées dans les journaux d'audit du serveur de l'API en choisissant le profil de politique de journal d'audit à utiliser.

Les données de surveillance, d'audit et de journal sont protégées par le contrôle d'accès basé sur les rôles. Les administrateurs du projet peuvent accéder aux données du projet et les administrateurs du cluster aux données du cluster.

Dans ce domaine, la meilleure pratique consiste à configurer votre cluster pour qu'il transmette tous les événements d'audit et de journalisation à un système de gestion des informations et des événements de sécurité (SIEM) pour la gestion, la conservation et l'analyse de l'intégrité. Les administrateurs du cluster peuvent déployer la journalisation du cluster pour centraliser tous les journaux du cluster Red Hat OpenShift, tels que les journaux d'audit des hôtes et des API, ainsi que les journaux des conteneurs d'applications et de l'infrastructure. La journalisation du cluster permet de regrouper ces journaux issus de tous les nœuds du cluster et de les stocker dans un magasin de journaux par défaut. Il existe plusieurs options pour transmettre les journaux au système SIEM de votre choix.

Un écosystème robuste pour étendre la sécurité

Pour renforcer davantage la sécurité de vos conteneurs et de Kubernetes ou pour respecter vos politiques, vous pouvez intégrer des outils de sécurité tiers. Le vaste écosystème de partenaires certifiés de Red Hat offre des solutions telles que :

- La gestion des accès privilégiés
- Des autorités de certification externes
- Des coffres-forts externes et des solutions de gestion de clés
- Des outils d'analyse du contenu des conteneurs et les outils de gestion des vulnérabilités
- Des outils d'analyse de l'exécution des conteneurs
- Un système SIEM

Conclusion

Le déploiement d'applications et de microservices basés sur des conteneurs n'est pas seulement une question de sécurité. Votre plateforme de conteneurs doit offrir une expérience fonctionnelle à vos développeurs et à votre équipe d'exploitation. Votre plateforme d'applications doit s'étendre à toute l'entreprise, être axée sur la sécurité et basée sur des conteneurs pour simplifier la vie des développeurs et des opérateurs sans compromettre les fonctions nécessaires à chaque équipe, le tout, en améliorant l'efficacité opérationnelle et l'utilisation des infrastructures.

La plateforme Red Hat OpenShift est construite sur une base de conteneurs Linux standard et portables qui offrent, notamment, les fonctions de sécurité intégrées suivantes :

- Outils intégrés de création et de CI/CD pour les pratiques DevOps de sécurité
- Version renforcée de Kubernetes pour les entreprises, avec des fonctions intégrées de configuration, de conformité et de gestion du cycle de vie de la plateforme
- Contrôle d'accès basé sur les rôles renforcé avec des intégrations aux systèmes d'authentification des entreprises
- Options de gestion des entrées et sorties des clusters
- Mise en réseau logicielle intégrée et Service Mesh avec prise en charge de la microsegmentation du réseau
- Prise en charge de la sécurisation des volumes de stockage à distance
- Red Hat Enterprise Linux CoreOS, optimisé pour l'exécution de conteneurs isolés à grande échelle
- Politiques de déploiement pour automatiser la sécurisation de l'exécution
- Fonctionnalités de surveillance, d'audit et de journalisation intégrées

La plateforme Red Hat OpenShift fournit également la plus grande collection de langages de programmation, de frameworks et de services (Figure 4). Le service Red Hat Advanced Cluster Management for Kubernetes assure la gestion étroitement intégrée de plusieurs clusters.

Red Hat OpenShift peut s'exécuter sur OpenStack, VMware, des serveurs bare metal, AWS, Google Cloud Platform (GCP), Azure, IBM Cloud et toute plateforme qui prend en charge Red Hat Enterprise Linux. Red Hat fournit également le service de cloud public Red Hat OpenShift Dedicated sur AWS et GCP. La solution Azure Red Hat OpenShift est proposée conjointement par Red Hat et Microsoft, tandis que Red Hat OpenShift Service on AWS est fournit par Red Hat et Amazon.

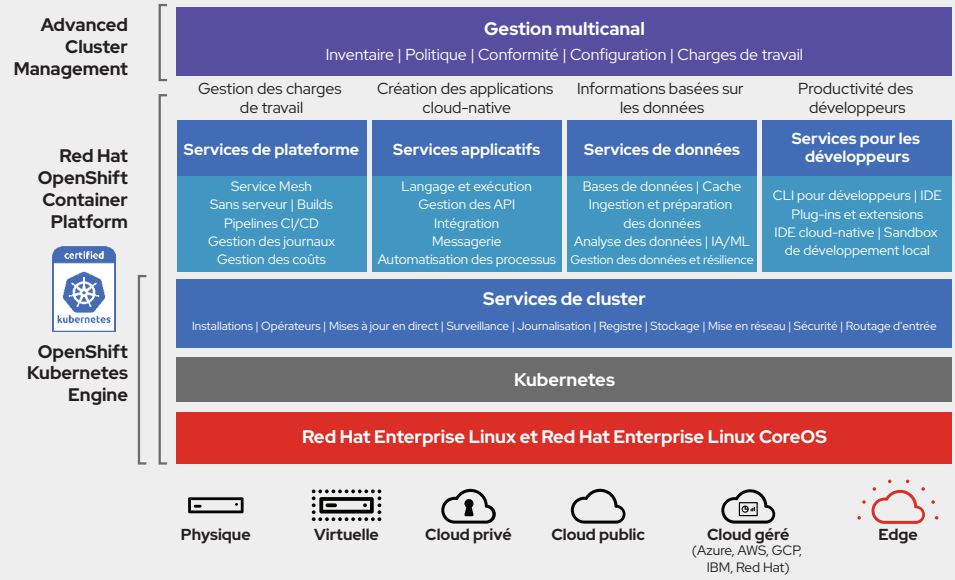

Figure 4. Red Hat OpenShift fournit une pile technologique complète pour les clouds physiques, virtuels, privés et publics.

Principal éditeur de solutions Open Source fiables pour les entreprises depuis plus de 20 ans, Red Hat intègre ce même niveau de fiabilité et de sécurité aux conteneurs grâce à des solutions telles que Red Hat OpenShift Container Platform, Red Hat Advanced Cluster Management for Kubernetes, et à sa gamme de produits Red Hat pour les conteneurs.

À PROPOS DE RED HAT

Premier éditeur mondial de solutions logicielles Open Source pour les entreprises, Red Hat s'appuie sur une approche communautaire pour proposer des technologies Linux, de cloud hybride, de conteneur et Kubernetes fiables et performantes. Red Hat aide ses clients à intégrer des applications nouvelles et existantes, à développer des applications natives pour le cloud, à standardiser leur environnement sur son système d'exploitation leader sur le marché ainsi qu'à automatiser, sécuriser et gérer des environnements complexes. Red Hat propose également des services d'assistance, de formation et de certification primés qui lui ont valu le titre de conseiller de confiance auprès des entreprises du Fortune 500. Partenaire stratégique des prestataires de cloud, intégrateurs système, fournisseurs d'applications, clients et communautés Open Source, Red Hat aide les entreprises à se préparer à un avenir toujours plus numérique.

facebook.com/redhatinc
@RedHat_France
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 4191 2323
fr.redhat.com

fr.redhat.com
#F26463_1220