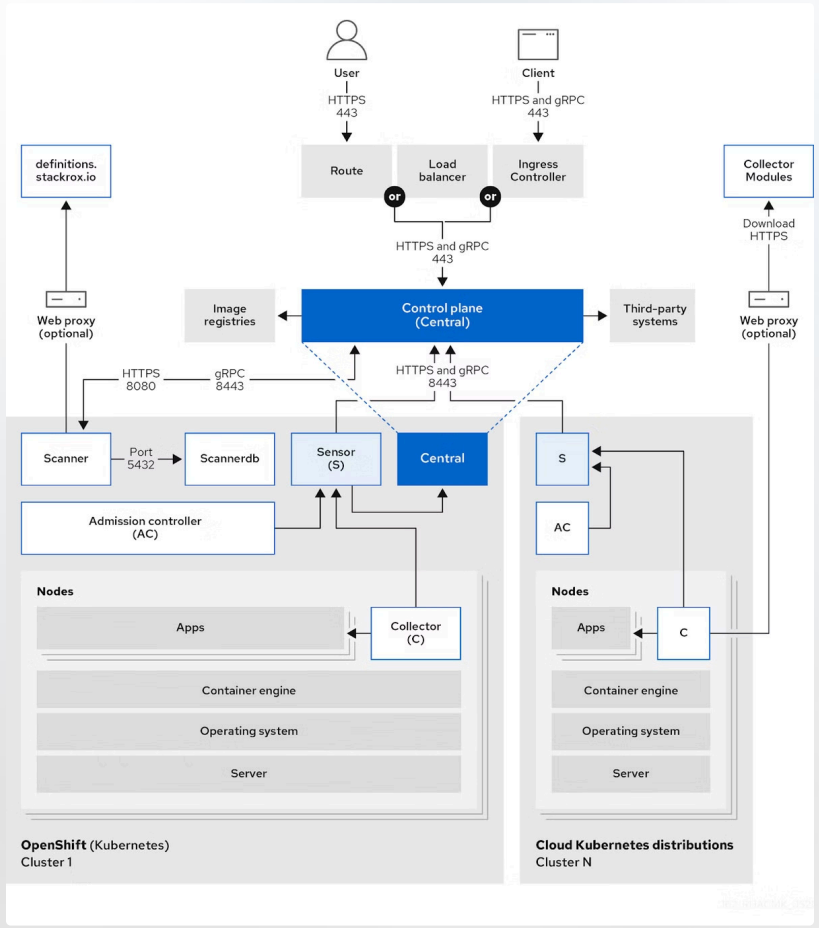
05 - Gestion de la Sécurité dans Kubernetes

La sécurité est un aspect essentiel de la gestion d'un cluster Kubernetes, en particulier dans un environnement de production où les applications sont exposées à divers risques.

par Tancrède SUARD

Code : KUB-A-1 (2024)



Contrôle d'Accès Basé sur les Rôles (RBAC)

Gestion des Permissions

RBAC permet de gérer les permissions et de restreindre les actions des utilisateurs ou des applications au sein d'un cluster Kubernetes.

Sécurité Renforcée

Grâce à RBAC, vous pouvez limiter les accès et les actions, augmentant ainsi la sécurité de votre environnement.

Contrôle Granulaire

RBAC offre un contrôle d'accès granulaire pour mieux sécuriser votre cluster Kubernetes.

Principes de RBAC

1. **Rôle**

   Définit les permissions pour des ressources spécifiques dans un namespace.

2. **ClusterRole**

   S'applique à l'ensemble du cluster, pas seulement à un namespace.

3. **RoleBinding et ClusterRoleBinding**

   Lient les rôles aux utilisateurs, groupes ou comptes de service.

Le contrôle d'accès basé sur les rôles (RBAC) repose sur ces trois concepts clés pour définir et attribuer les permissions dans un cluster Kubernetes.

Exemple de Configuration RBAC

Rôle de Lecture des Pods

Définit un rôle permettant la lecture des pods dans le namespace **dev**.

Affectation du Rôle

Utilise un **RoleBinding** pour attribuer le rôle **pod-reader** à l'utilisateur **user1**.

Politiques Réseau (Network Policies)

1 Contrôle du Trafic Réseau

Les Network Policies permettent de limiter la communication entre les pods et les segments de réseau externes.

2 Empêcher les Accès Non Autorisés

Elles empêchent les accès non autorisés en restreignant le trafic au sein du cluster Kubernetes.

3 Définition des Règles

Les Network Policies définissent des règles pour contrôler le trafic entrant et sortant des pods.

Principes des Network Policies

1

Pod Selector

Identifie les pods auxquels s'applique la règle de Network Policy.

2

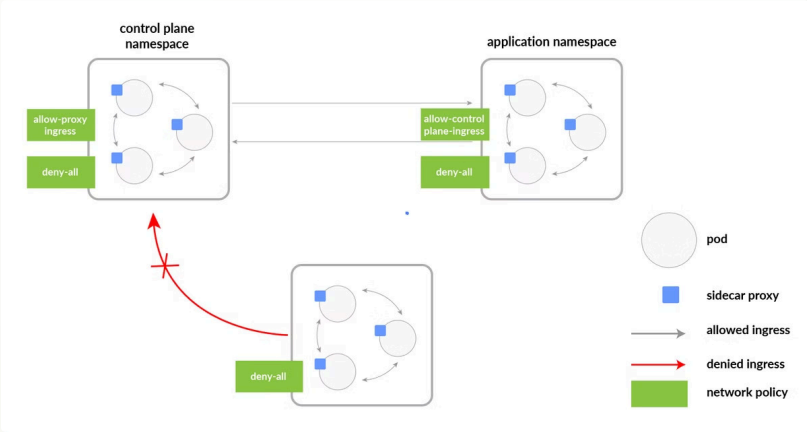
Policy Types

Précise si la règle s'applique au trafic entrant (Ingress) ou sortant (Egress).

3

Définition des Règles

Les Network Policies permettent de définir des règles de trafic entrant et sortant pour un groupe de pods sélectionné.



Principes des Network Policies

Contrôle du Trafic Réseau

Les Network Policies permettent de définir des règles pour contrôler le trafic réseau entrant et sortant des pods.

Sécurité Granulaire

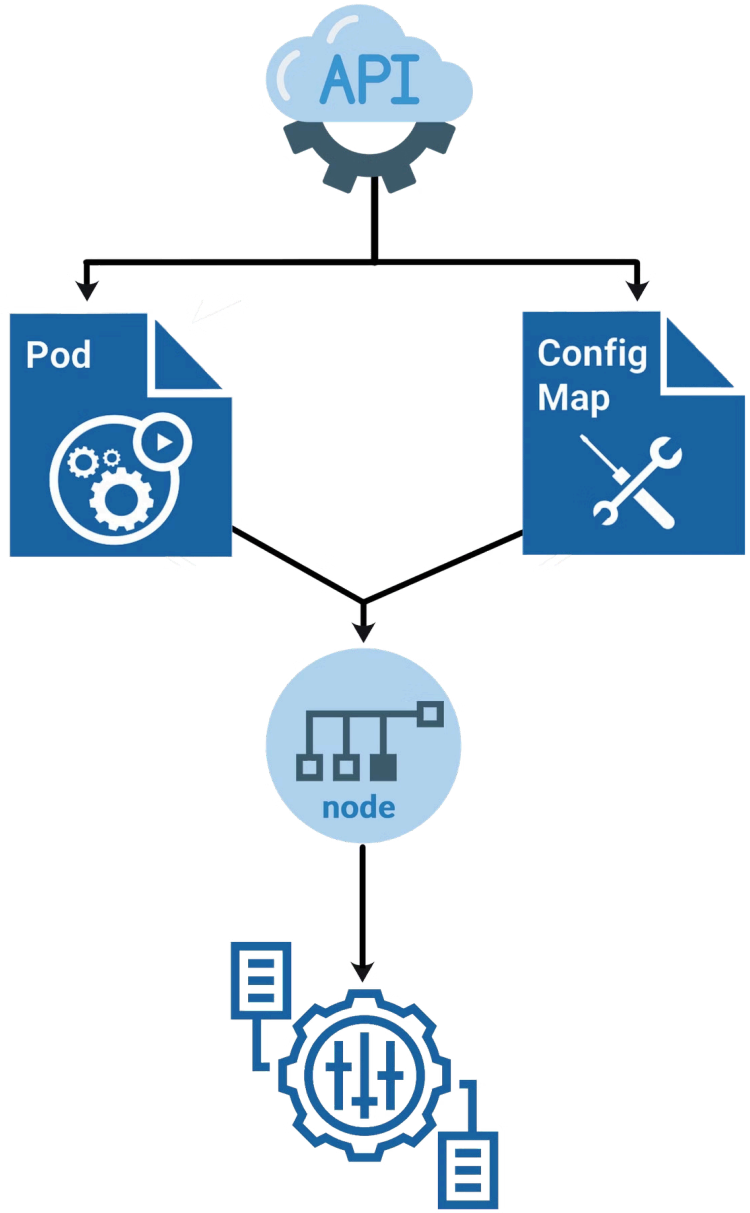
Elles offrent une sécurité granulaire en autorisant ou en bloquant le trafic en fonction des labels des pods.

Isolation des Namespaces

Les Network Policies peuvent être appliquées au niveau des namespaces pour isoler le trafic entre différents environnements.

Gestion des Secrets et ConfigMaps

Les **Secrets** permettent de gérer les informations sensibles comme les mots de passe et les clés d'API. Les **ConfigMaps** stockent les données de configuration des applications sans les inclure dans le code des conteneurs.



Création et Utilisation des Secrets

1 Sécurité des Secrets

Les Secrets sont encodés en base64 pour une protection de base des informations.

2 Création de Secrets

Les Secrets peuvent être créés manuellement ou à partir de fichiers existants.

3 Utilisation des Secrets

Les Secrets peuvent être injectés comme variables d'environnement ou montés comme fichiers.

Création et Utilisation des Secrets et ConfigMaps

1 Créer un ConfigMap

À partir de lignes de commande ou de fichiers YAML.

2 Lier un ConfigMap

Utiliser comme variable d'environnement ou monter comme volume.

3 Créer un Secret

Stocker des données sensibles de manière sécurisée.

Les ConfigMaps permettent de stocker des configurations non sensibles, tandis que les Secrets servent à sécuriser les données sensibles dans Kubernetes.

Bonnes Pratiques pour la Sécurité dans Kubernetes

Quotas de Ressources

Limitez les ressources attribuées aux pods pour prévenir les surcharges.

Audit Activé

Configurez l'audit de Kubernetes pour enregistrer et surveiller les actions.

Isolation des Environnements

Utilisez les namespaces pour séparer les environnements (dev, test, prod).

Contrôle Réseau

Configurez des Network Policies pour restreindre les communications.

Gestion des Secrets

Utilisez des outils externes pour stocker et contrôler l'accès aux informations sensibles.

Permissions Restreintes

Appliquez le principe de moindre privilège pour les rôles et permissions.