La Sécurité - Autolock dans Docker Swarm

Dans Docker Swarm, **autolock** est une fonctionnalité de sécurité qui permet de protéger les secrets de Docker Swarm en les verrouillant. Cela garantit que les secrets du cluster sont chiffrés de manière sécurisée, et seuls les administrateurs autorisés peuvent déverrouiller le gestionnaire de secrets du Swarm. Lorsque l'option **autolock** est activée, les gestionnaires de Swarm doivent être déverrouillés avant de pouvoir effectuer des opérations sensibles telles que la gestion des secrets.

Cette fonctionnalité est essentielle dans des environnements de production où la sécurité des informations sensibles (comme des mots de passe, des clés API ou des certificats) est critique.

---

1. Qu'est-ce que l'Option `autolock` ?

L'option `autolock` permet de chiffrer la clé de gestion du cluster Swarm. Cette clé de gestion est utilisée pour accéder aux secrets du Swarm, et **autolock** empêche les accès non autorisés en verrouillant cette clé de gestion.

Lorsque **autolock** est activé :

- Le Swarm est verrouillé par défaut après chaque redémarrage du gestionnaire.
- Vous devez fournir un mot de passe pour **déverrouiller** le gestionnaire et permettre des opérations sur les secrets.

Cela ajoute une couche de sécurité pour empêcher des accès non autorisés aux données sensibles, même si un attaquant obtient un accès physique à l'un des nœuds du cluster.

---

2. Activer l'Option `autolock` dans Docker Swarm

Pour activer **autolock**, vous devez être connecté à un **nœud manager** de Docker Swarm et exécuter la commande appropriée pour configurer le verrouillage automatique des secrets.

a. Initialiser ou Mettre à Jour un Cluster Swarm avec Autolock

Lorsque vous initialisez un cluster Swarm pour la première fois ou lorsque vous voulez activer **autolock** sur un cluster existant, vous pouvez activer **autolock** en utilisant la commande suivante.

Initialiser un Cluster Swarm avec `autolock` :

```
docker swarm init --autolock
```

Cela initialise le cluster Swarm et active automatiquement la fonctionnalité **autolock**.

b. Activer `autolock` sur un Cluster Existant

Si votre cluster Swarm est déjà initialisé, mais que vous souhaitez activer **autolock**, vous pouvez utiliser la commande suivante sur un nœud **manager** :

```
docker swarm update --autolock
```

Cela activera **autolock** sur le cluster existant.

---

3. Déverrouiller un Cluster Swarm avec `autolock`

Une fois **autolock** activé, le gestionnaire de Swarm sera verrouillé et ne pourra pas être utilisé pour effectuer des opérations sur les secrets tant qu'il n'est pas déverrouillé.

a. Déverrouiller le Gestionnaire de Swarm

Lorsque vous redémarrez un nœud manager ou après une interruption, vous devrez fournir une clé de déverrouillage pour permettre l'accès aux secrets. Vous pouvez déverrouiller le Swarm avec la commande suivante :

```
docker swarm unlock
```

Cela vous demandera de saisir un **mot de passe** ou une **clé de déverrouillage**. Si vous ne connaissez pas cette clé, vous ne pourrez pas accéder aux secrets du cluster.

b. Générer et Sauvegarder une Clé de Déverrouillage

Lorsque vous activez **autolock**, une clé de déverrouillage est générée. Vous devez enregistrer cette clé de manière sécurisée, car elle est nécessaire pour déverrouiller le Swarm. Vous pouvez la sauvegarder dans un gestionnaire de mots de passe ou tout autre emplacement sécurisé.

Exemple de sauvegarde de la clé de déverrouillage :
Lorsque vous activez **autolock**, Docker vous fournira une clé de déverrouillage. Conservez cette clé en sécurité, car elle est indispensable pour effectuer des opérations sur le Swarm après un redémarrage.

---

4. Vérifier l'État de `autolock`

Vous pouvez vérifier si l'option **autolock** est activée sur votre cluster Swarm à tout moment avec la commande suivante :

```
docker info | grep Swarm
```

Cela vous donnera un aperçu de l'état du Swarm, et vous pourrez voir si **autolock** est activé.

---

5. Rollback ou Désactivation de `autolock`

Si vous devez désactiver **autolock** pour une raison quelconque, vous pouvez le faire en exécutant la commande suivante sur un nœud manager :

```
docker swarm update --autolock=false
```

Cela désactivera le verrouillage automatique et reviendra à un état où les secrets ne sont pas verrouillés et peuvent être accessibles sans mot de passe.

---

6. Meilleures Pratiques pour `autolock`

- **Stocker la clé de déverrouillage en toute sécurité** : La clé de déverrouillage est cruciale pour accéder aux secrets du Swarm. Conservez-la dans un endroit sécurisé, comme un gestionnaire de mots de passe ou un coffre-fort matériel.
- **Activer `autolock` sur tous les nœuds manager** : Assurez-vous que l'option **autolock** est activée sur tous les nœuds manager de votre cluster Swarm pour garantir la sécurité des secrets à l'échelle du cluster.
- **Sauvegarder régulièrement la clé de déverrouillage** : Si vous perdez la clé de déverrouillage, vous ne pourrez pas accéder aux secrets et devrez peut-être réinitialiser le Swarm. Faites des copies de sauvegarde sécurisées.

Résumé des Commandes pour Configurer `autolock`

Action	Commande
Initialiser Swarm avec `autolock`	`docker swarm init --autolock`
Activer `autolock` sur un cluster existant	`docker swarm update --autolock`
Déverrouiller un nœud Swarm	`docker swarm unlock`
Vérifier l'état de `autolock`	`docker info | grep Swarm`
Désactiver `autolock`	`docker swarm update --autolock=false`

Conclusion

L'option **autolock** dans Docker Swarm offre une couche de sécurité supplémentaire pour protéger les secrets stockés dans votre cluster. En verrouillant l'accès aux secrets, vous vous assurez que seules les personnes disposant de la clé de déverrouillage peuvent y accéder, renforçant ainsi la sécurité de votre environnement Swarm. Assurez-vous de sauvegarder la clé de déverrouillage et de l'utiliser en cas de redémarrage du gestionnaire pour garantir la continuité de l'administration des secrets.