GABRIELE ROMANATO

Gestione dei secrets in Docker

Quando si gestiscono applicazioni containerizzate, uno degli aspetti più critici è la protezione delle informazioni sensibili, come password, token API e certificati. Docker fornisce un meccanismo nativo per la gestione sicura di questi dati: i **Docker secrets**.

Cosa sono i Docker secrets?

I Docker secrets sono un modo sicuro per gestire dati sensibili all'interno di un ambiente Docker Swarm. I secrets vengono memorizzati in modo criptato e montati nei container solo quando necessario, minimizzando l'esposizione delle informazioni.

Prerequisiti

Per utilizzare i Docker secrets, è necessario lavorare in un **Docker Swarm**. Questo significa che il cluster deve essere inizializzato con il comando:

```
docker swarm init
```

Creazione di un secret

Per creare un secret, si utilizza il comando `docker secret create`. Ad esempio:

```
echo "mypassword" | docker secret create db_password -
```

Questo comando crea un secret chiamato `db_password` con il contenuto "mypassword".

Utilizzo dei secrets in un servizio

Una volta creato il secret, è possibile utilizzarlo all'interno di un servizio Docker:

```
docker service create \
  --name my_service \
  --secret db_password \
  my_image
```

Il secret sarà disponibile nel container all'interno del path `/run/secrets/db_password`.

Accesso al secret dal container

Nel container, è possibile leggere il secret semplicemente accedendo al file:

```
cat /run/secrets/db_password
```

Rimozione di un secret

Per rimuovere un secret non più necessario:

```
docker secret rm db_password
```

Considerazioni di sicurezza

- I secrets sono criptati in transito e a riposo.
- Solo i servizi che esplicitamente richiedono un secret possono accedervi.
- I secrets non sono disponibili in container standalone, ma solo in servizi Swarm.

Conclusione

Docker secrets fornisce un metodo sicuro e scalabile per la gestione delle credenziali in ambienti containerizzati. Utilizzandoli in combinazione con le best practice di sicurezza, è possibile ridurre significativamente i rischi associati alla gestione dei dati sensibili.