
SPRING FRAMEWORK
GURU

Docker Secrets

Using Docker Secrets

Docker Secrets

- Docker Secrets are designed to protect sensitive configuration data.
- Only available to Docker Swarm Services
- Use Secrets to protect things such as:
  - Usernames / Passwords
  - TLS Certificates
  - SSH Keys
  - Any other sensitive data

Why Use Docker Secrets?

- Typically you will need to use Docker Secrets in the enterprise for regulatory compliance.
- Regulations such as PCI, SOX, SAS-70 prohibit free text passwords
- Sensitive data is required to be encrypted in flight and at rest.

How Docker Secrets Work

- Secrets can be strings or binary content up to 500 kb in size.
- Secrets are stored in the Raft log, which is encrypted by default in version 1.13 and later.
  - WARNING: Raft is not encrypted prior to Docker 1.13.
- Secrets are made available inside containers via a file system mount at /run/secrets/<secret_name>
- Nodes can only access secrets which it has been granted to.

Docker Secrets Commands

- `docker secret create`
- `docker secret inspect`
- `docker secret ls`
- `docker secret rm`
- Example: `docker service create –secret=“my_secret” redis:alpine`


SPRING FRAMEWORK
GURU