



CLOUD COMPUTING APPLICATIONS

Docker Configs and Secrets
Prof. Reza Farivar

Docker Secrets

- A secret is a blob of data
 - E.g. password, SSH private key, SSL certificate
- Should not be transmitted over a network or stored unencrypted in a Dockerfile or in your application's source code
- use Docker *secrets* to centrally manage
- Docker secrets are only available to swarm services, not to standalone containers

Docker Secrets CLI

- `docker secret create`
- `docker secret inspect`
- `docker secret ls`
- `docker secret rm`
- `--secret` **flag for** docker service create
- `--secret-add` **and** `--secret-rm` **flags for** docker service update

Docker Secrets

- When you grant a newly-created or running service access to a secret, the ***decrypted*** secret is mounted into the container in an in-memory filesystem
- Location of the mount point within the container defaults to:
 - /run/secrets/<secret_name> in Linux containers
 - C:\ProgramData\Docker\secrets in Windows containers

Docker Configs

- Docker secrets are only available to swarm services, not to standalone containers
- Docker configs are only available to swarm services, not to standalone containers
- Configs operate in a similar way to secrets, except that they are not encrypted at rest and are mounted directly into the container's filesystem without the use of RAM disks.

Docker Config CLI

- `docker config create`
- `docker config inspect`
- `docker config ls`
- `docker config rm`

Cloud Computing Applications
Copyright R.Farivar
All Rights Reserved