Your (container) secret’s safe with me

Liz Rice

@LizRice | @AquaSecTeam
se·cret

/ˈsɛkriːt/

noun

1. something that is kept or meant to be kept unknown or unseen by others.
Secrets

Secret store

Cluster
Desirable attributes for secrets management
Secrets

- Encrypted
  - At rest and in transit
  - Only decrypted in memory
Access control
- Only accessible by containers that need them
- And users
- Write-only access
Secrets

- Life-cycle
  - Risk of leak increases over time
  - Rotation, revocation, audit logging
Passing secrets to containers
Bad places for secrets

- Source code
- Dockerfiles / images
Environment variables

docker run -e VARNAME=secret ...

@LizRice | @AquaSecTeam
Environment variables

- `docker inspect`
- `docker exec`
- `/proc` directory
- Leaky logs
Mounted volume

docker run -v /hostsecrets:/secrets ...
Mounted volume

- `docker inspect`
- `docker exec`
- `/proc directory`
- `Leaky logs`
Orchestrator support for secrets
Docker

- Secrets support built in for Docker Swarm services
  - Not standalone containers

- Encrypted transmission with mutual authentication

- Secret accessible when exposed to service
  - Mounted to a temporary fs (not env vars)
  - RBAC in Enterprise Edition
Docker

- Encrypted in Raft log
  - Lock your Swarm!!
  - Shared to Swarm managers
- Audit log with events
- Rotation requires container restart & secret dance

Encrypted ✓  Access control ✓  Life-cycle ?
Kubernetes secrets

- Secret configured in pod YAML
  - Namespaced

- RBAC can be turned on
  --authorization-mode=RBAC

- Files and env vars
  - Files support updating secret values
  - Need to restart pod to get new env var value
Kubernetes secrets

- Stored in etcd
  - Make sure secrets are encrypted!
  - `--experimental-encryption-provider-config` on API Server

Encrypted?  Access control ✓  Life-cycle ✓
Kubernetes secrets

```yaml
kind: EncryptionConfig
apiVersion: v1
resources:
  - resources:
    - secrets
    providers:
    - aescbc:
      keys:
        - name: key1
          secret: bXlWZXJ5U2VjcmV0RW5jcnlwdGlvbktleQo=
        - identity: {}
```

@LizRice | @AquaSecTeam
Secrets all the way down

- EncryptionConfig holds a secret key...
DC/OS

- Enterprise DC/OS
  - Plug-ins for Mesos/Marathon
- Encrypted in ZooKeeper
- Env vars
- Access control by service path
- Restart service to update value

Encrypted ✓  Access control ✓  Life-cycle ?
Nomad

- Integrated with Vault
  - Use production mode
  - Encryption & security primitives
Nomad

- Secrets passed as files
- Nomad takes care of interactions with Vault
  - Tasks get tokens so they can retrieve values
  - Poll for changed values
- Access control
- Audit logging

Encrypted ✓  Access control ✓  Life-cycle ✓
Aqua secrets & external store

- Any orchestrator
- Secret storage in 3rd party backend
  - Hashicorp Vault, Amazon KMS, Azure Key Vault, CyberArk Vault...
Aqua secrets & external store

- File system & env var support
  - Update secrets without container restart
  - No env var leak through inspect or /proc
- Auditing of secret usage
- User & container access control

Encrypted ✓  Access control ✓  Life-cycle ✓
Summary
Access secrets at runtime
  Not built in
Rotate secrets
Your best option depends on
  Orchestrator
  Acceptable level of risk
RBAC can be turned on --authorization-mode=RBAC

```yaml
# This role binding allows "dave" to read secrets in the "development" namespace.
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: read-secrets
namespace: development # This only grants permissions within the "development" namespace.
subjects:
- kind: User
  name: dave
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: secret-reader
  apiGroup: rbac.authorization.k8s.io
```