Secrets

Unit 5.3.2

Secrets

Just like a ConfigMap, Secrets store arbitrary key/value pairs. These hold sensitive data like passwords or API keys and will get special treatment within your Kubernetes environment. They are base64-encoded to obfuscate their plaintext values when viewed by humans, but this provides a minimal amount of security.

Kubernetes does not encrypt secrets by default. Doing so requires additional configuration of the kube-apiserver component. The Rancher Hardening Guide shows how to encrypt secrets at rest, and detailed information about how to do it is included in the next level of certification.

Unlike ConfigMaps, Secrets can be assigned to a namespace or to a project. If assigned to a project, they are available to all namespaces within that project.

References

Secrets in Rancher - https://rancher.com/docs/rancher/v2.x/en/k8s-in-rancher/secrets/

Secret Configuration and Usage - https://kubernetes.io/docs/concepts/configuration/secret/

Rancher Hardening Guide - https://rancher.com/docs/rancher/v2.x/en/security/