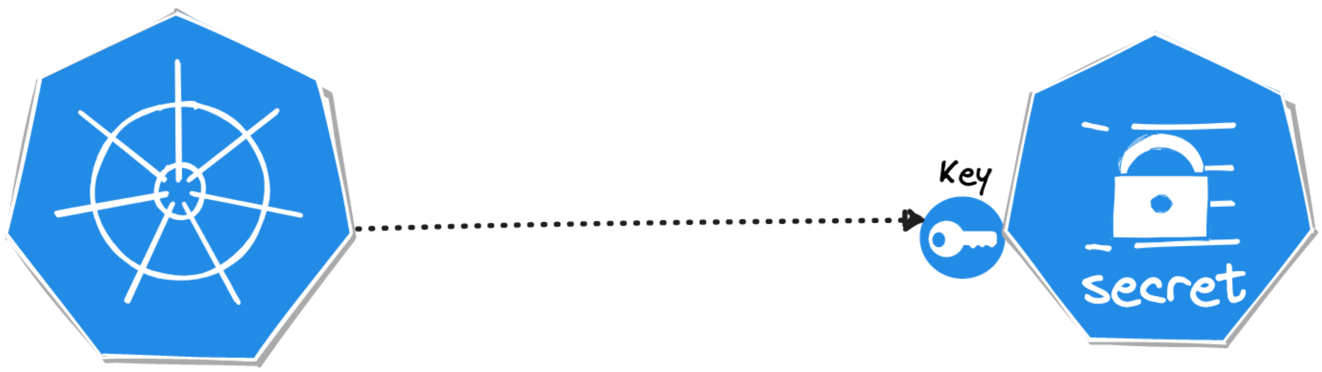
Securing Secrets in Kubernetes



Do not Print this page. This is property of the Securitydojo. Powered by Virtual Cybertron.

Kubernetes uses secret objects called as Secrets, to store the secret data. Kubernetes Secrets allows confidential data separated from the application code by creating it separately from pods. This segmentation lowers the likelihood that the Secret will be exposed while interacting with pods, enhancing security.

While Kubernetes Secrets are helpful for preventing accidental data exposure, they may not secure the cluster data against malicious entity having access to the cluster.

- Storing data in a Secret does not automatically make it secure, as Secrets are encoded in Base64, which is equivalent to plaintext.
- Secrets provide more control over access and usage of sensitive data, and they can be mounted separately or saved as environment variables for pods.
- The built-in Secrets mechanism in Kubernetes offers basic security features such as encryption at rest, authorization policies, and whitelisting access to specific containers.

Third-Party Secret Management Tools

- Third party tools adds primary value as they provide a centralized, robust mechanism for encrypting secrets and granting access to secrets. All these tools support Kubernetes, but they are not purpose-built for container workloads.

- Cloud provider tools: including AWS Secrets Manager, Google Cloud Platform KMS and Azure Key Vault

- Open source tools: Hashicorp Vault

Limitations of Secret Management in a Container Environment There is no doubt that secrets management tools can provide value for Kubernetes projects. However, even when you are armed with a secret management solution, you will still be limited in your ability to manage and monitor secrets.

Limitation of Default Secrets management systems

- Managing containers having access to secrets
- Retrieving secrets from the vault
- Store secrets in the containers securely
- Pushing updated secrets directly to containers

Do not print this page. This is property of the Securitydojo Powered by Virtual Cybertron.