HashiCorp | SUSE

Implement Kubernetes Security at Scale

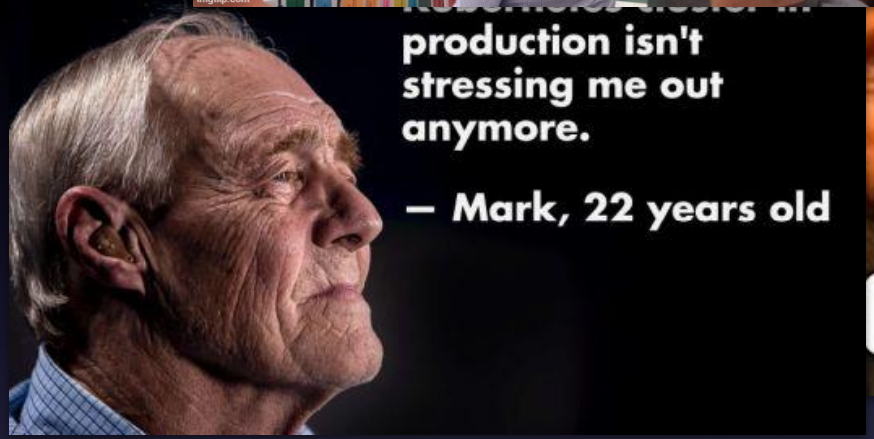
Carsten Duch
Senior Solution Engineer
HashiCorp

Claudio Serrano
Solution Architect
SUSE

Agenda

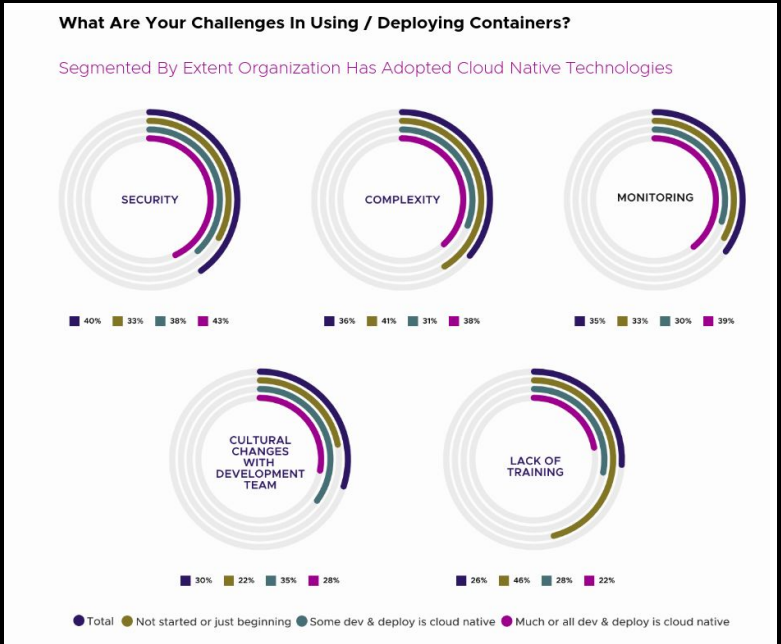
01

What is the challenge?



Kubernetes is a tool to orchestrate containers, it's not a turn-key platform.

Security is #1 challenge for production containers

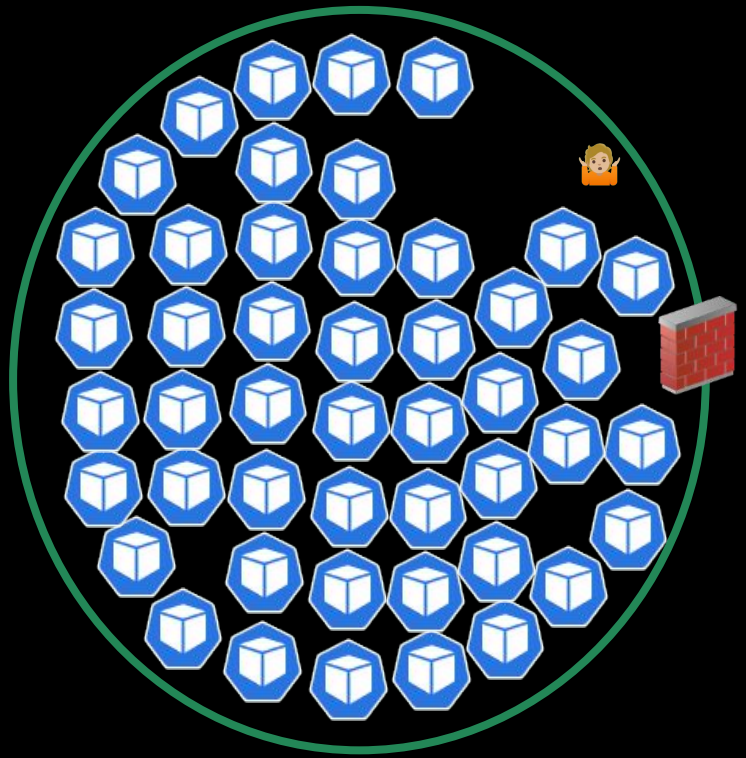


Extract from Cloud Native Computing Foundation Annual Survey 2023
(https://www.cncf.io/reports/cncf-annual-survey-2023/)

- Security is the top challenge for organizations running containers in production for two years in a row[1].
- Data breach average costs have been increasing 15% since 2020 reaching USD 4.45 million in 2023.[2]
- After the xz incident and others, securing the software supply chain continues to be one of the key challenges to prevent attacks.

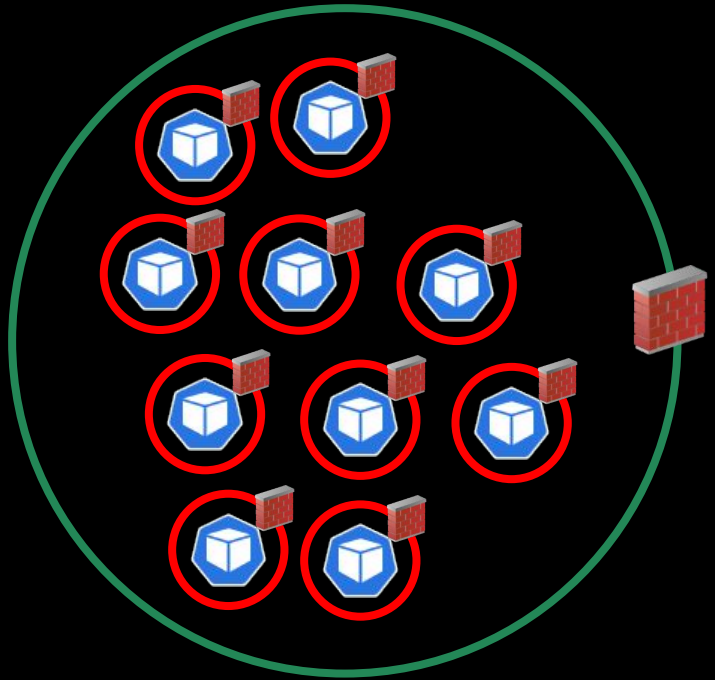
[1] Cloud Native Computing Foundation Annual Survey 2023 - (https://www.cncf.io/reports/cncf-annual-survey-2023/)
[2] Cost of a Data Breach Report 2023 - (https://www.ibm.com/security/data-breach)

Modern day challenges with container security



- Increasing in Popularity- more attractive for attackers
- Vulnerability & Compliance Management -PCI /NIST /GDPR / HIPAA
- Runtime Security / Zero Trust
- Supply Chain Security - Are the images secure and up to date? - Necessitates an automated approach
- Internal (East-West) security as much (if not more) of a concern than North-South traffic (Perimeter security).
- What is happening in the cluster / Who can communicate with whom
- Container Sprawl - Ephemeral environments / clusters / workloads
- Network is essentially flat *and a bit mysterious*

Modern day challenges with container security

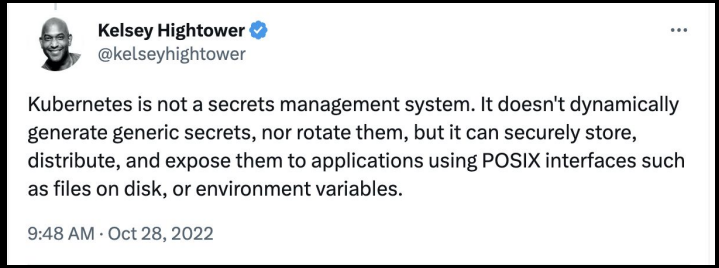


- Re-assign what we consider the security boundary
- Treat each container as its own security boundary
- Automate everything
- Zero-trust as default
- Layer 4 security is not enough
  - Layer 7 inspection/detection
- Falling back to a pure patching practice is not a strategy
  - Threat vs Risk Models
- Leverage abstractions
  - Grouping/Labelling/etc

Kubernetes is ...

... NOT a Secret Management System

- Secrets are stored unencrypted by default
- No secret rotation
- Secrets value must be base64-encoded
- Secrets are cluster + namespace scoped
- Adheres to K8s RBAC model (e.g if you can create a pod, you can see the value of the secret)
- no dynamic / short lived secrets
- Hard to audit secret access



Most breaches start with stolen credentials

380%

increase over the last 2 years of data theft breaches

74%

of breaches involved a human element

9/10

of web application breaches consisted of stolen credentials

62%

of system intrusions involved a supply chain

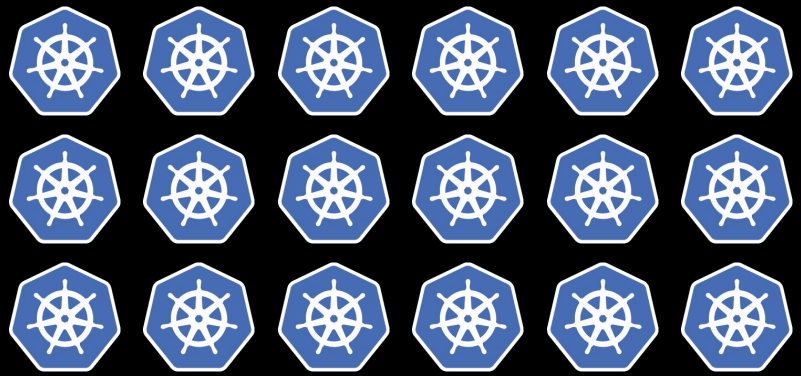
Source: Verizon 2023 Data Breach Investigations report

02

Solution Overview

Kubernetes clusters are great ...

... but hard to manage, especially many of them!



- Different environments
- Different teams
- Different hardware
- Different locations
- Edge devices

Rancher Prime

Open/ Interoperable Container Management

- Simple, consistent operations from data center to Edge
- Trusted, secure delivery
- Complete lifecycle management
- Industry leading container security, storage, VM management, and Linux OS
- Access to broad ecosystem of open source technologies

SUSE

Everything you need to deploy, run, and manage all of your containerized workloads

Full-lifecycle cluster management

RANCHER PRIME

Virtual machine management

HARVESTER

Distributed storage

LONGHORN

Full-lifecycle container security

NeuVector PRIME

Operating system management

ELEMENTAL

Infrastructure & Application Monitoring

StackState

Certified OS

SUSE Linux Enterprise Server

What do you get with Rancher Prime?

Security

SUSE NeuVector

- Vulnerability & Compliance Scanning
- Pipeline Security Automation
- Zero-Trust Controls & File Protection
- Vulnerability (CVE) investigation, triage assistance
- Best practices, hardening assistance
- Run-time threat rules configuration, optimization

Platform Services

Rancher Prime Manager

- App Catalog
- Observability
- Storage
- Service Mesh
- Policy Enforcement
- Governance
- Virtual Machine & OS Management
- Cluster Provisioning & LCM

Rancher Prime Hosted

Developer Tools

- App Deployment
- Local Dev Tooling
- Container Images

Trusted Registry

Infrastructure Services

On-prem

Any Certified Kubernetes Distribution

Any Enterprise Linux & VMware

Servers | Containers | VM

Cloud

Full Cluster Lifecycle Support for EKS, AKS, & GKE

IaaS | CaaS

Edge

Lightweight Kubernetes Distribution

Lightweight Linux OS & HCI

Servers | Devices | VM

Up to 24/7/365 Support & Professional Services

Why Rancher Prime

50,000+

Rancher active users

35,000+

Active Downloads Per Month

10 million+

K3s monthly downloads

Lead

Contributors to 3x CNCF Projects

Trusted by

15,000+ organization worldwide

SUSE

SUSE provided Kubernetes Distributions

RKE

RKE 2

K3S

Rancher Kubernetes Engine

- 100% Upstream Kubernetes
- CNCF certified
- Easy installation
- Zero-downtime upgrades
- Backup & Disaster Recovery
- Air gapped installation support

NeuVector

SUSE NeuVector Container Security

Why SUSE NeuVector?

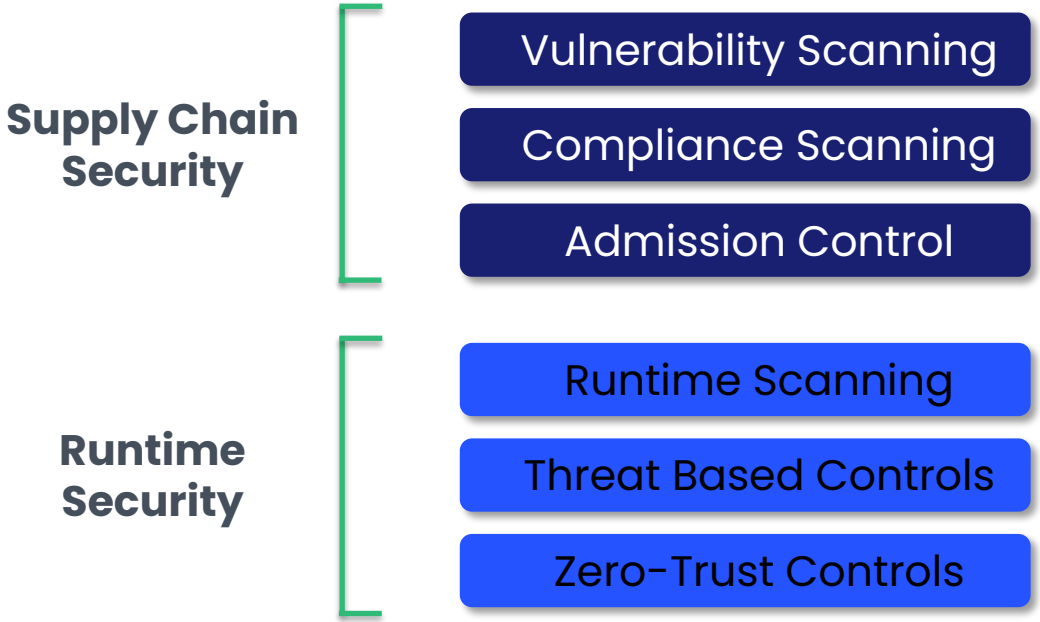
Automate Security Policies

Network Visibility in Production

Zero-Trust Protections – Network, Process & File Access

Data Loss Prevention for Compliance

LAYERED SECURITY: DEFENSE IN DEPTH

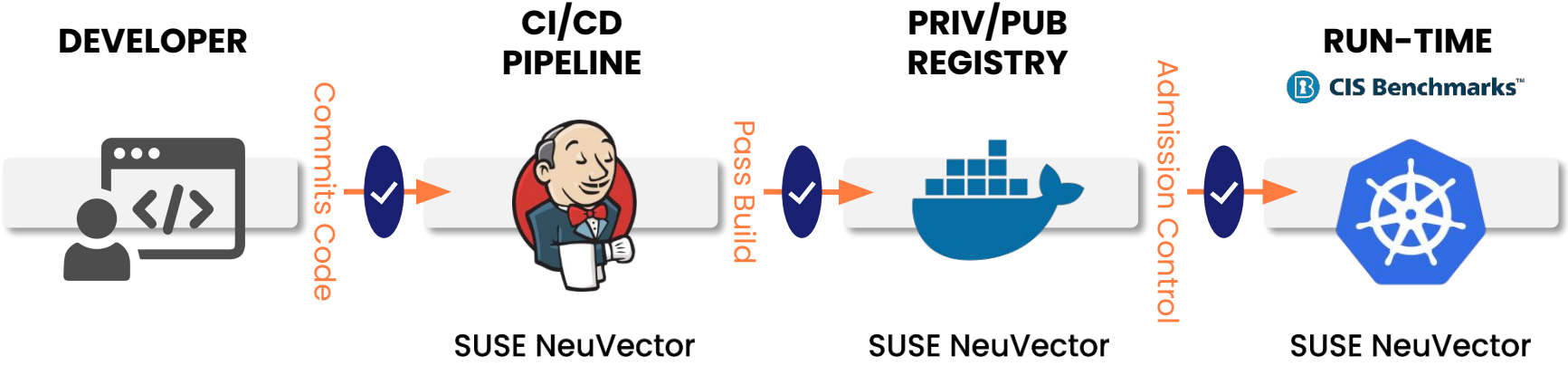


CVE Database Sources

Source	URL
nvd and Mitre	https://nvd.nist.gov/feeds/
SUSE SLE/SLES	https://ftp.suse.com/pub/projects/security/oval/
Rancher OS	https://rancher.com/docs/os/v1.x/en/about/security/
Alpine	https://github.com/alpinelinux/alpine-secdb
Ubuntu	https://launchpad.net/ubuntu-cve-tracker
Debian	https://security-tracker.debian.org/tracker/data/json
RedHat	https://www.redhat.com/security/data/oval/
Amazon	https://alas.aws.amazon.com/
Busybox	https://www.cvedetails.com/vulnerability-list/
NGINX	http://nginx.org/en/security_advisories.html
NodeJS	https://www.npmjs.com/advisories/
Ruby	https://github.com/rubysec/ruby-advisory-db
OpenSSL	https://www.openssl.org/news/vulnerabilities.html
Apache	https://www.cvedetails.com/vendor/45/Apache.html
Java	https://openjdk.java.net/groups/vulnerability/advisories/
Python	https://github.com/pyupio/safety-db
Microsoft Mariner	https://github.com/microsoft/CBL-MarinerVulnerabilityData

NeuVector CVE Database is Updated via 17 Security Sources Nightly

VULNERABILITY & COMPLIANCE MANAGEMENT



Run Time Security: Defense in Depth

Threat (Signature) Based Controls

- CVEs
- DLP
- Network Attacks
- OWASP Top 10
- Admission Control

NeuVector Zero-Trust Controls

- Automated Learning
- Network
- Process
- File Access
- Security as Code


HashiCorp
Vault

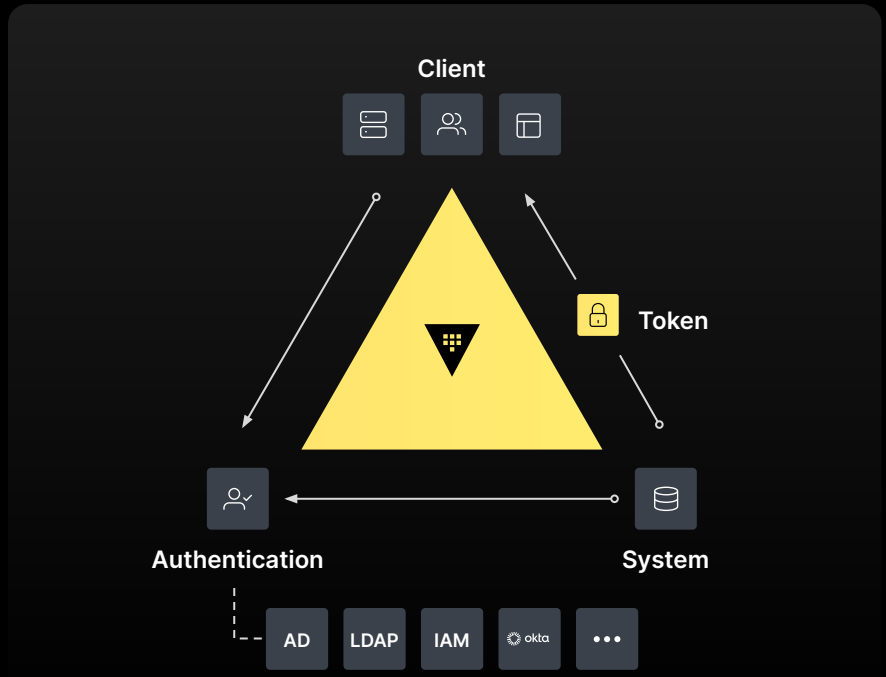
Authenticate and authorize every access request

In dynamic cloud infrastructure, security starts with identity.

Identity-based security uses trusted identities to automate access to secrets, data, and applications

Security system of record to centrally store and protect secrets across clouds and applications

Lifecycle management of your credentials to ensure proper oversight, rotation, and expiry



Vault

Automate **secure access** and **lifecycle management** for credentials and sensitive data

Identity-based security

Secrets	Certificates	Keys	Data Protection
Static	PKI	KMS	Encryption
Rotated	Managed Keys	KMIP	Signatures
Dynamic		HSM	Tokenization
Database			

Choose your delivery model

HCP Vault

For small and medium size businesses with cloud-native architectures

- **HCP Vault Secrets** for secret lifecycle management
- **HCP Vault Radar** for secret scanning

Cloud | Managed | Self-managed

Choose your delivery model

HCP Vault Dedicated

For large businesses that require a single tenant cloud environment

- Secrets Management
- Key Management
- Certificate Management
- Advanced Data Protection

Cloud | **Managed** | Self-managed

Choose your delivery model

Vault Enterprise

For large businesses with strict compliance and security requirements

- Secrets Management
- Key Management
- Certificate Management
- Advanced Data Protection

Cloud | Managed | **Self-managed**

Kubernetes secrets

Kubernetes

In the DevOps world, some CI/CD pipelines require the ability to manage applications running on a Kubernetes cluster.

Kubernetes Secrets are, by default, stored unencrypted in the API server's underlying data store (etcd). Anyone with API access can retrieve or modify a Secret, and so can anyone with access to etcd.

Kubernetes secrets

Kubernetes

The Kubernetes Secrets Engine for Vault generates Kubernetes service account tokens, and optionally service accounts, role bindings, and roles. The created service account tokens have a configurable TTL and any objects created are automatically deleted when the Vault lease expires.

Kubernetes secrets

Sidecar containers

Enable access to Vault secrets by Kubernetes applications that don't have native Vault logic built-in.

- Allow automatic injection of secrets into the pod file system
- Allow applications to only concern themselves with finding a secret at a filesystem path, rather than managing the auth tokens and other mechanisms

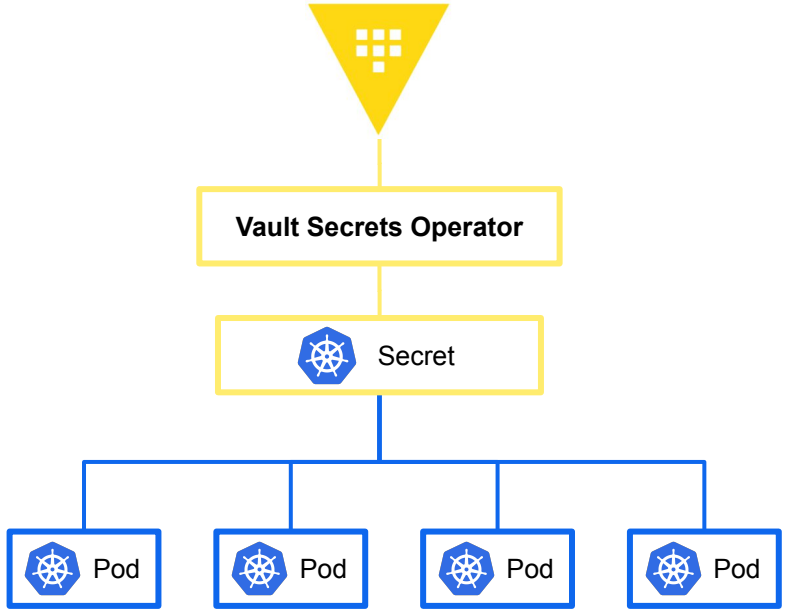
Kubernetes secrets

Vault Secrets Operator for Kubernetes

Using controller-runtime and custom resource definitions to allow application developers to consume Vault Secrets directly from Kubernetes. The Operator ensures Vault Secrets remain synchronized in the cluster.

Supports synchronizing all classes of Vault secrets:

- Dynamic: database credentials, cloud credentials, etc.
- PKI: TLS certificates
- Static: Key/Value
- Google auth for Workload Identity on GKE
- OpenShift OLM



How to Consume Vault Secrets in Kubernetes

- Vault Secrets Operator (VSO): Sync secrets from Vault into k8s “secret”-ressource
  - https://developer.hashicorp.com/vault/tutorials/kubernetes/vault-secrets-operator
- Vault Agent Injector (VAI): Inject secret from Vault directly into a Pod
  - https://developer.hashicorp.com/vault/tutorials/kubernetes/kubernetes-sidecar

Alternative Options:

- CSI: Mount Secret through Container Storage Interface (CSI)
  - https://developer.hashicorp.com/vault/tutorials/kubernetes/kubernetes-secret-store-driver
- API: Applications can use Vault API Library’s to consume Secrets from Vault
  - https://developer.hashicorp.com/vault/api-docs/libraries

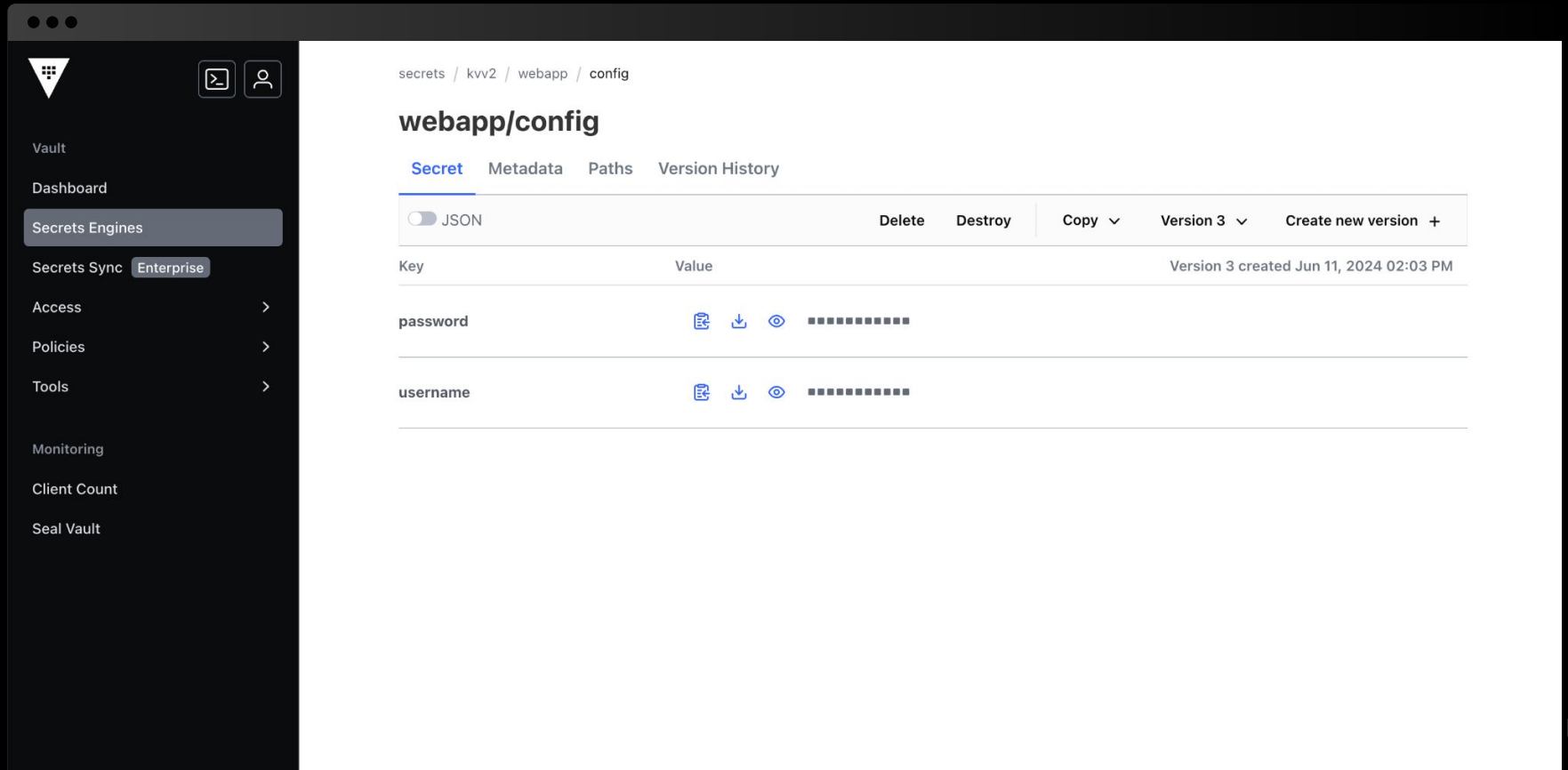
Blogpost:
https://www.hashicorp.com/blog/kubernetes-vault-integration-via-sidecar-agent-injector-vs-csi-provider

03

Demo


HashiCorp
Vault

Setup Static Secret in Vault



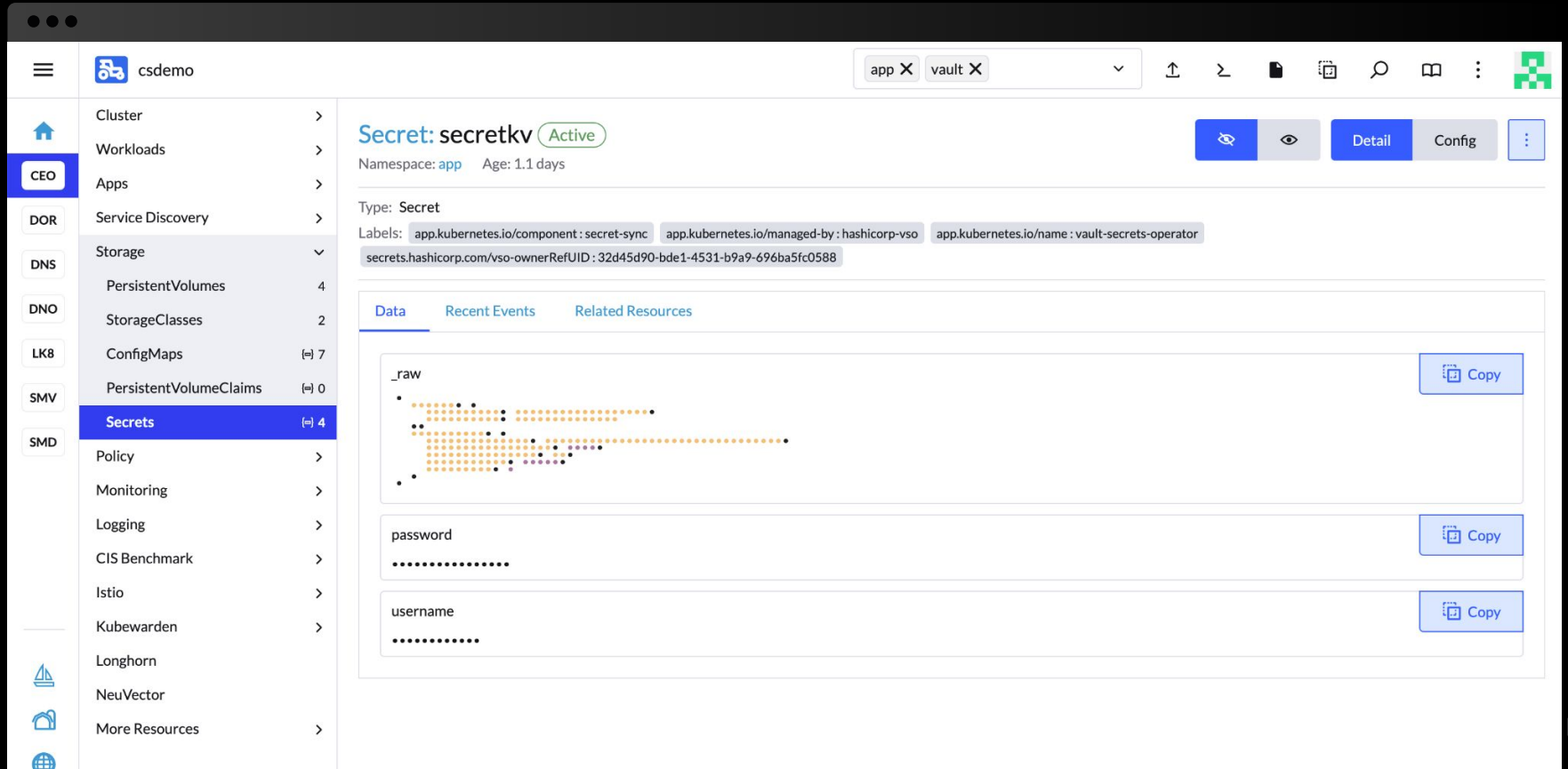
VSO: Configure Secret Sync via CRD

static-secret.yaml

Users > cduch > Documents > git > hashicorp-education > learn-vault-secrets-operator > vault > static-secret.yaml

```yaml
apiVersion: secrets.hashicorp.com/v1beta1
kind: VaultStaticSecret
metadata:
  name: vault-kv-app
  namespace: app
spec:
  type: kv-v2

  # mount path
  mount: kvv2

  # path of the secret
  path: webapp/config

  # dest k8s secret
  destination:
    name: secretkv
    create: true

  # static secret refresh interval
  refreshAfter: 30s

  # Name of the CRD to authenticate to Vault
  vaultAuthRef: static-auth
```

VSO: Access Synced Secret in Kubernetes



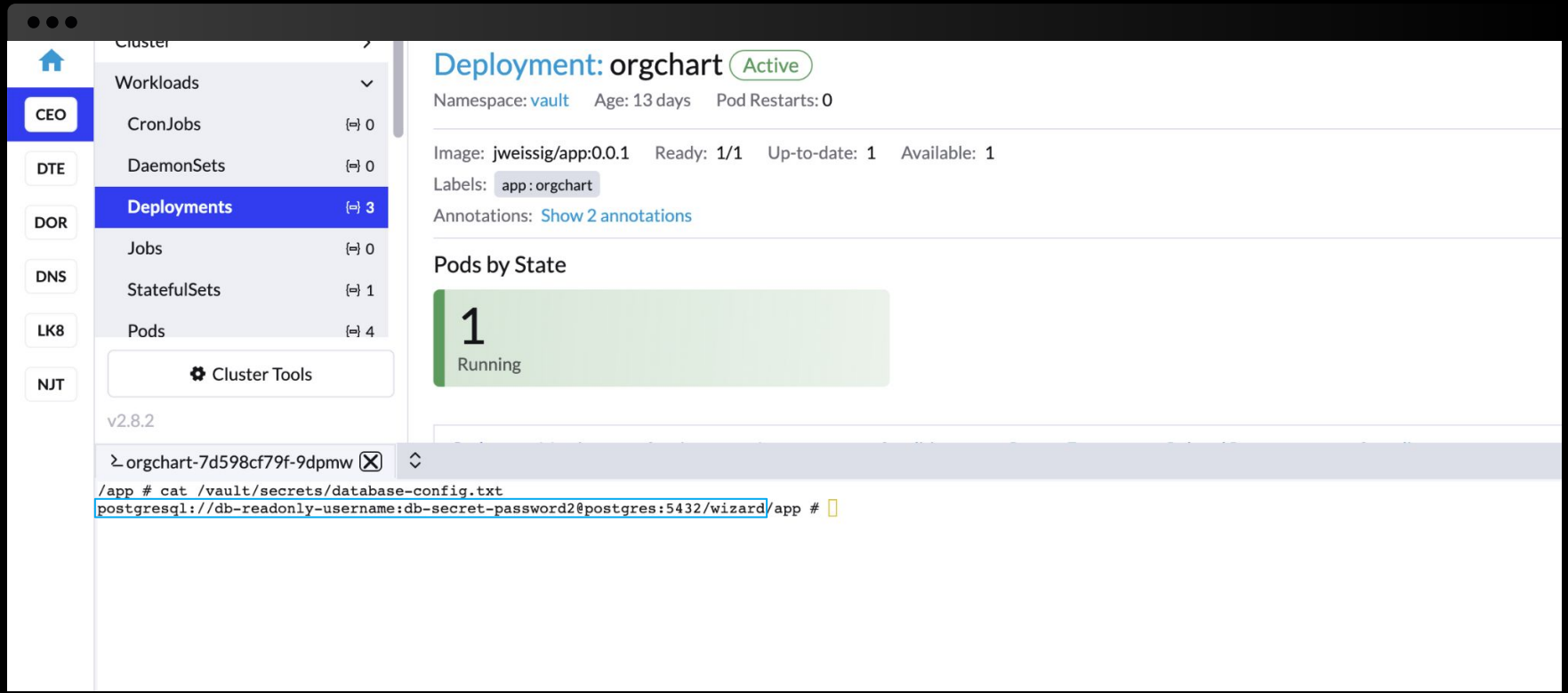
VAI: Inject Secret with Template into Pod

patch-inject-secrets-as-template.yaml M

patch-inject-secrets-as-template.yaml

```yaml
spec:
  template:
    metadata:
      annotations:
        vault.hashicorp.com/agent-inject: "true"
        vault.hashicorp.com/auth-path: "auth/demo-auth-mount"
        vault.hashicorp.com/agent-inject-status: "update"
        vault.hashicorp.com/role: "internal-app"
        vault.hashicorp.com/agent-inject-secret-database-config.txt: "internal/data/database/config"
        vault.hashicorp.com/agent-inject-template-database-config.txt: |
          {{- with secret "internal/data/database/config" -}}
          postgresql://{{ .Data.data.username }}:{{ .Data.data.password }}@postgres:5432/wizard
          {{- end -}}
```

VAI: Show Injected Secret In Pod



04

Conclusion & QA

Conclusion - SUSE & HashiCorp: Better Together!

SUSE Rancher Prime

Streamlines cluster deployment, offering centralized authentication, access control and observability across your deployments anywhere.

SUSE Neuvector Prime

Providing end-to-end vulnerability management for the full container lifecycle for your Kubernetes environments.

HashiCorp Vault

Providing identity-based security to automatically authenticate and authorize access to secrets and other sensitive data for Kubernetes Applications.

Events

HashiConf 2024

October 14-16, 2024 | Boston

HashiConf is HashiCorp's global cloud conference. Join us for 2+ days of conversations on the future of cloud automation with product announcements, technical sessions, hands-on labs, certifications, social events, and more.

https://www.hashicorp.com/conferences/hashiconf

SUSE Rancher and SUSE Neuvector Rodeos:

https://www.suse.com/events/?event_type=rodeos

Thank you

hello@hashicorp.com