26
09/2025

HashiConf 2025 | Fort Mason, San Francisco

Lessons Learned from Deploying Vault at Scale

/ About me

Introduction

Leon Krass

Technical Leader
for HashiCorp Vault

Passionate about secrets management and (sometimes over-) engineering IT automation with a touch of Kubernetes, Terraform and/or Ansible magic.

HashiCorp Vault, Kubernetes, Ansible, Terraform

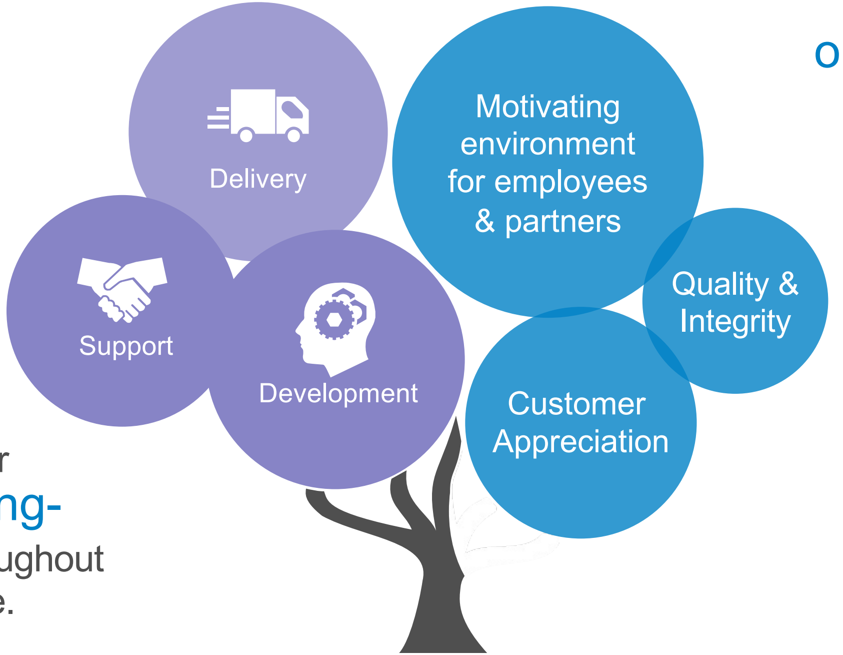
/ About us

Who is SVA?

Biggest owner-operated system integrator in Germany

Steady growth with more than 3.500 employees in Germany

We accompany our customers on a long-term basis throughout the project lifecycle.

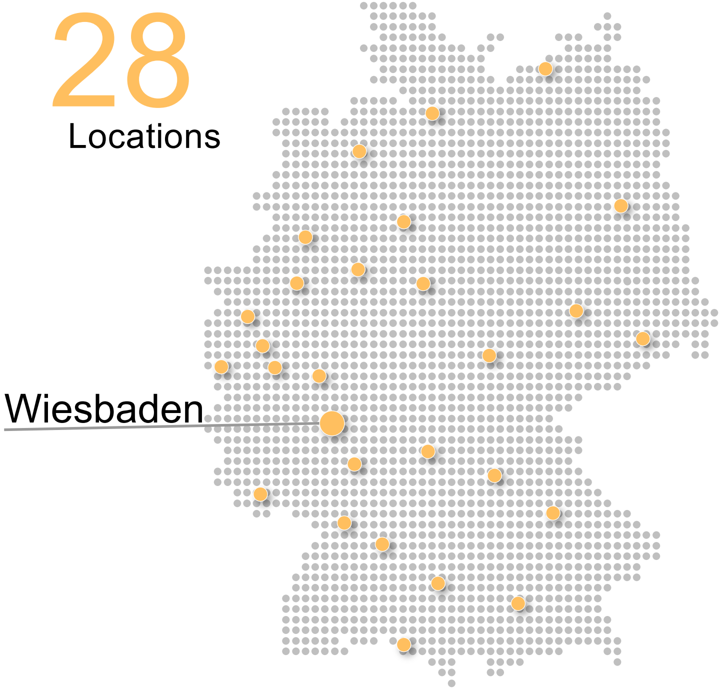


Company objectives

Who is SVA?

28

Locations



INDUSTRIES

such as

AUTOMOTIVE

RETAIL

PUBLIC

HEALTH CARE

MACHINARY & PLANT ENGINEERING

TELECOMMUNICATIONS

FINANCE & INSURANCE

/ About us

What brings a German integrator to the US?

⇢ Partnership with HashiCorp to bring their products to the German market

⇢ Insights from deploying the products at our customers

⇢ Share lessons learned & contribute back to the community

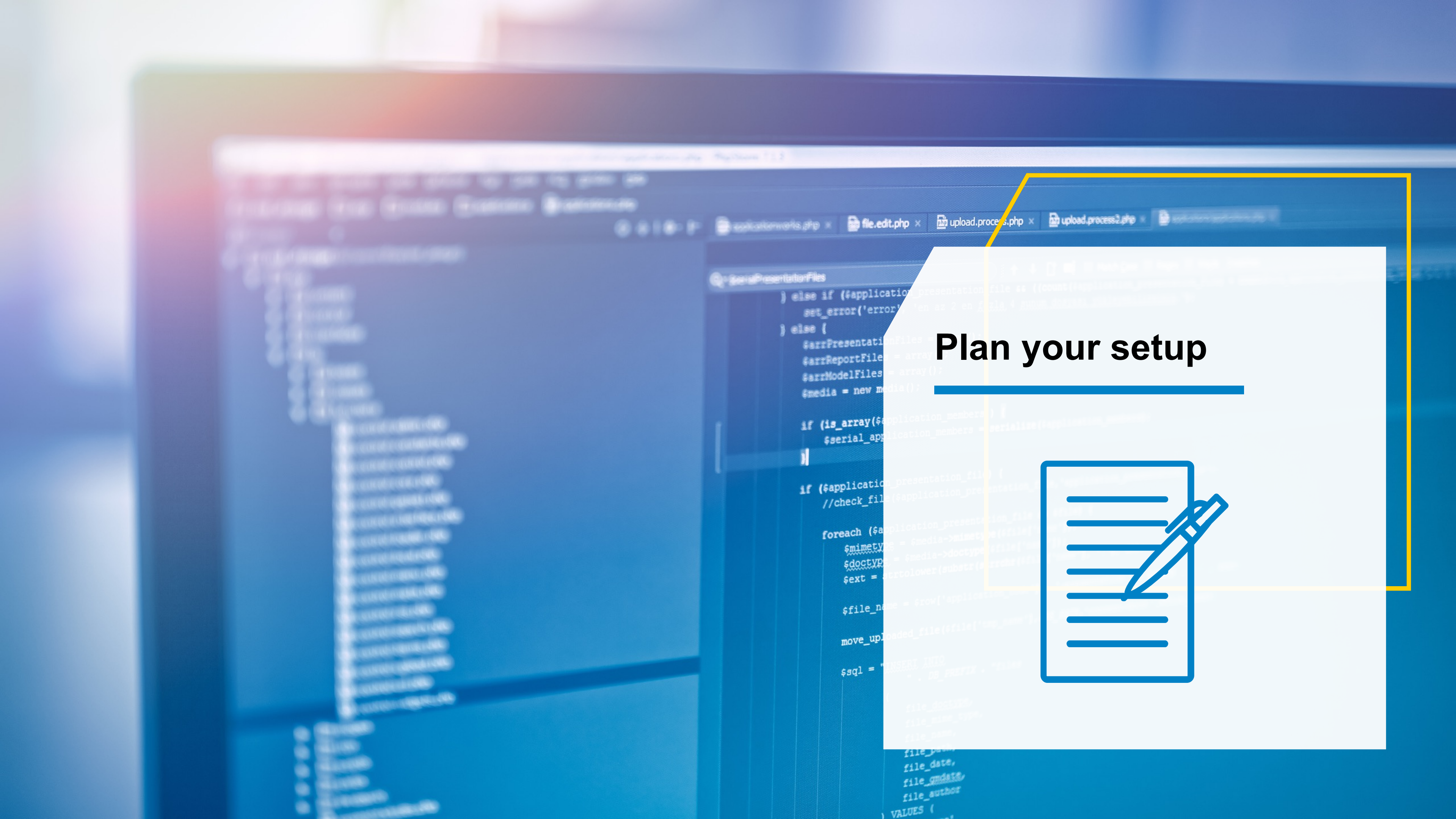
Lessons Learned from Deploying Vault at Scale

1 Plan your setup

2 Deploy your Vault

3 Configure and operate your Vault

4 Wrap-Up



Plan your setup

On Prem

/ Plan your setup

Where to run Vault?

Costs

Complexity

Attack Surface

…

On Prem

Where to run Vault?

	Bare-Metal
Costs	★☆☆
Complexity	★★☆
Attack Surface	★★★
…	

On Prem

Where to run Vault?

	Bare-Metal	VM
Costs	★☆☆	★★⯪
Complexity	★★☆	★★⯪
Attack Surface	★★★	★★☆
…		

On Prem

Where to run Vault?

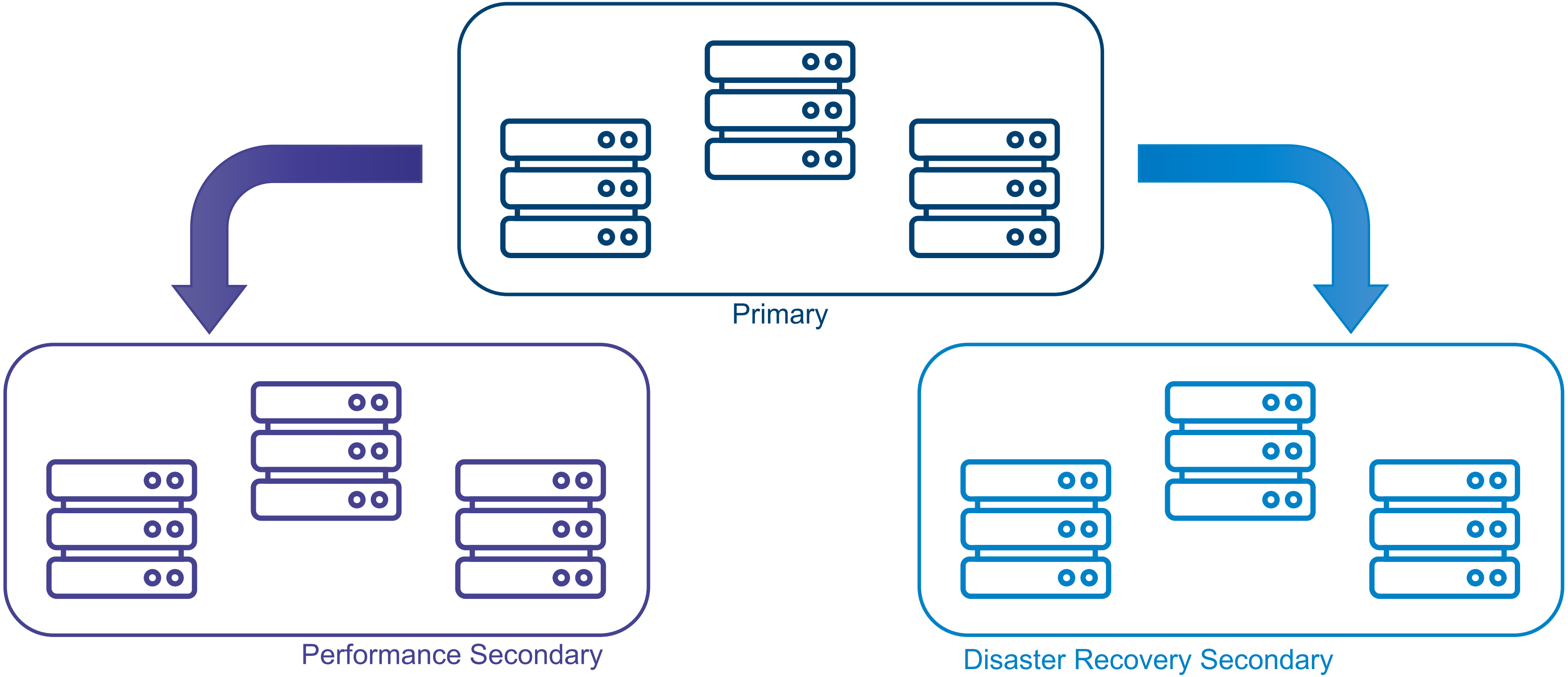
	Bare-Metal	VM	Kubernetes
Costs	★☆☆	★★⯨	★★★
Complexity	★★☆	★★⯨	★☆☆
Attack Surface	★★★	★★☆	★☆☆
…			

Where to run Vault?

	Cloud
Costs	★★☆
Complexity	★★★
Attack Surface	★★★
…	

Architecture

On Prem



Auto unseal

On Prem

2nd Vault

- Keys are stored in Transit Engine of 2nd Vault
- Can be managed locally
- Simple to setup, but maintenance overhead

On Prem

Auto unseal

2nd Vault

- Keys are stored in Transit Engine of 2nd Vault
- Can be managed locally
- Simple to setup, but maintenance overhead

Cloud KMS

- Keys are stored in external public cloud
- Needs internet access
- Simple to setup, but keys in non sovereign environment

On Prem

/ Plan your setup

Auto unseal

2nd Vault

- Keys are stored in Transit Engine of 2nd Vault
- Can be managed locally
- Simple to setup, but maintenance overhead

Cloud KMS

- Keys are stored in external public cloud
- Needs internet access
- Simple to setup, but keys in non sovereign environment

HSM

- Keys are stored on hardware
- Local access only
- Expensive and complex, but most secure

On Prem

/ Plan your setup

TLS

⇢ Get your Certificates right!

⇢ Automate renewals

⇢ Use e2e TLS

⇢ Let Vault manage its own certificates

⇢ Hard to bootstrap, but worth it

Storage

Use Vaults integrated Raft storage!

except...

- ⇢ … you run dev mode
- ⇢ … you have a single node cluster
- ⇢ … need more performance (→ Consul)

Load Balancing

On Prem

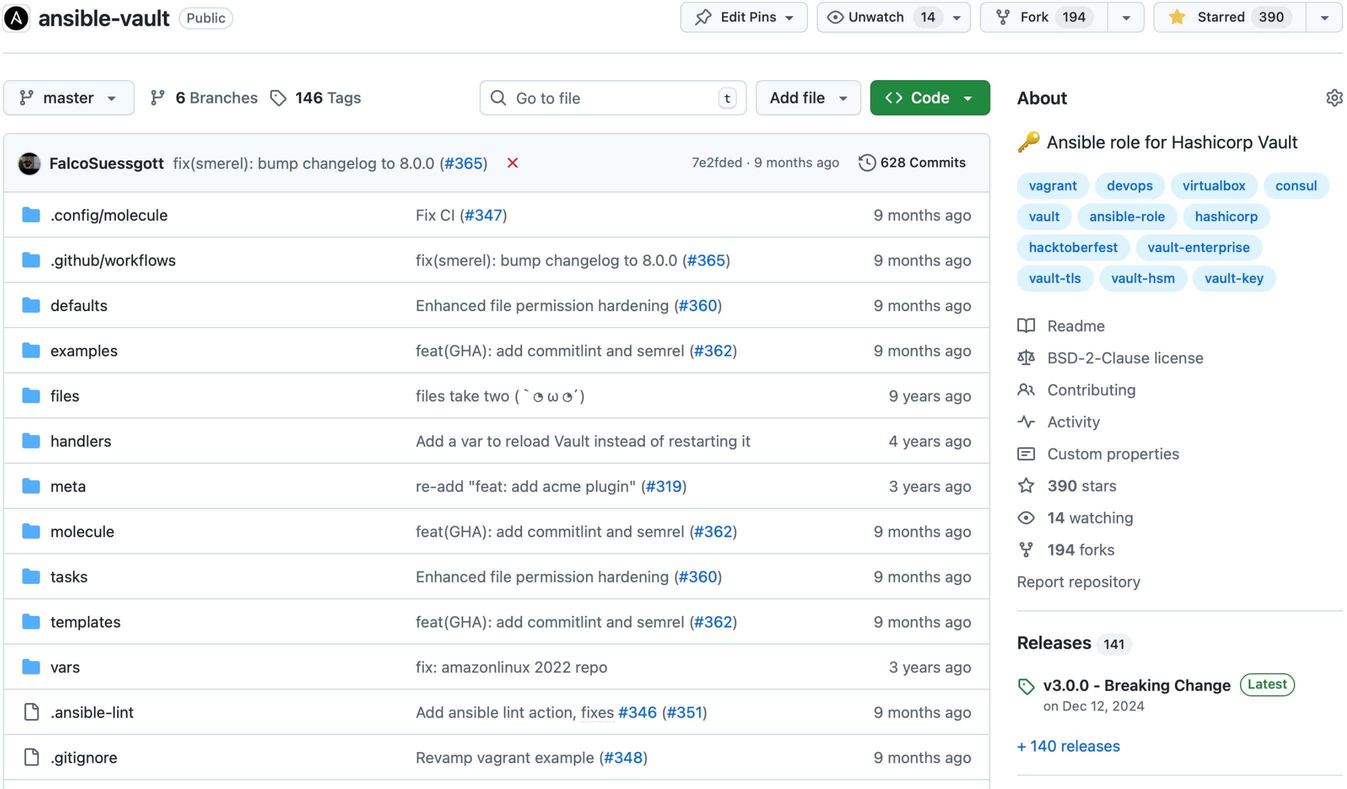
- Use Performance Standbys
- Use a proper balancer (Nginx, F5, HAProxy, …)
- Be aware of Vaults health check return codes
- Virtual IPs also work

Further considerations

- Network
- Update Strategy
- Identity Management
- On- & Offboarding
- …

Deploy your Vault

Use automation



FalcoSuessgott fix(smerel): bump changelog to 8.0.0 (#365) ✕ 7e2fded · 9 months ago 628 Commits

.config/molecule	Fix CI (#347)	9 months ago
.github/workflows	fix(smerel): bump changelog to 8.0.0 (#365)	9 months ago
defaults	Enhanced file permission hardening (#360)	9 months ago
examples	feat(GHA): add commitlint and semrel (#362)	9 months ago
files	files take two (ˋ ◔ ω ◔ ˊ)	9 years ago
handlers	Add a var to reload Vault instead of restarting it	4 years ago
meta	re-add "feat: add acme plugin" (#319)	3 years ago
molecule	feat(GHA): add commitlint and semrel (#362)	9 months ago
tasks	Enhanced file permission hardening (#360)	9 months ago
templates	feat(GHA): add commitlint and semrel (#362)	9 months ago
vars	fix: amazonlinux 2022 repo	3 years ago
.ansible-lint	Add ansible lint action, fixes #346 (#351)	9 months ago
.gitignore	Revamp vagrant example (#348)	9 months ago

About

🔑 Ansible role for Hashicorp Vault

vagrant devops virtualbox consul vault ansible-role hashicorp hacktoberfest vault-enterprise vault-tls vault-hsm vault-key

- Readme
- BSD-2-Clause license
- Contributing
- Activity
- Custom properties
- 390 stars
- 14 watching
- 194 forks

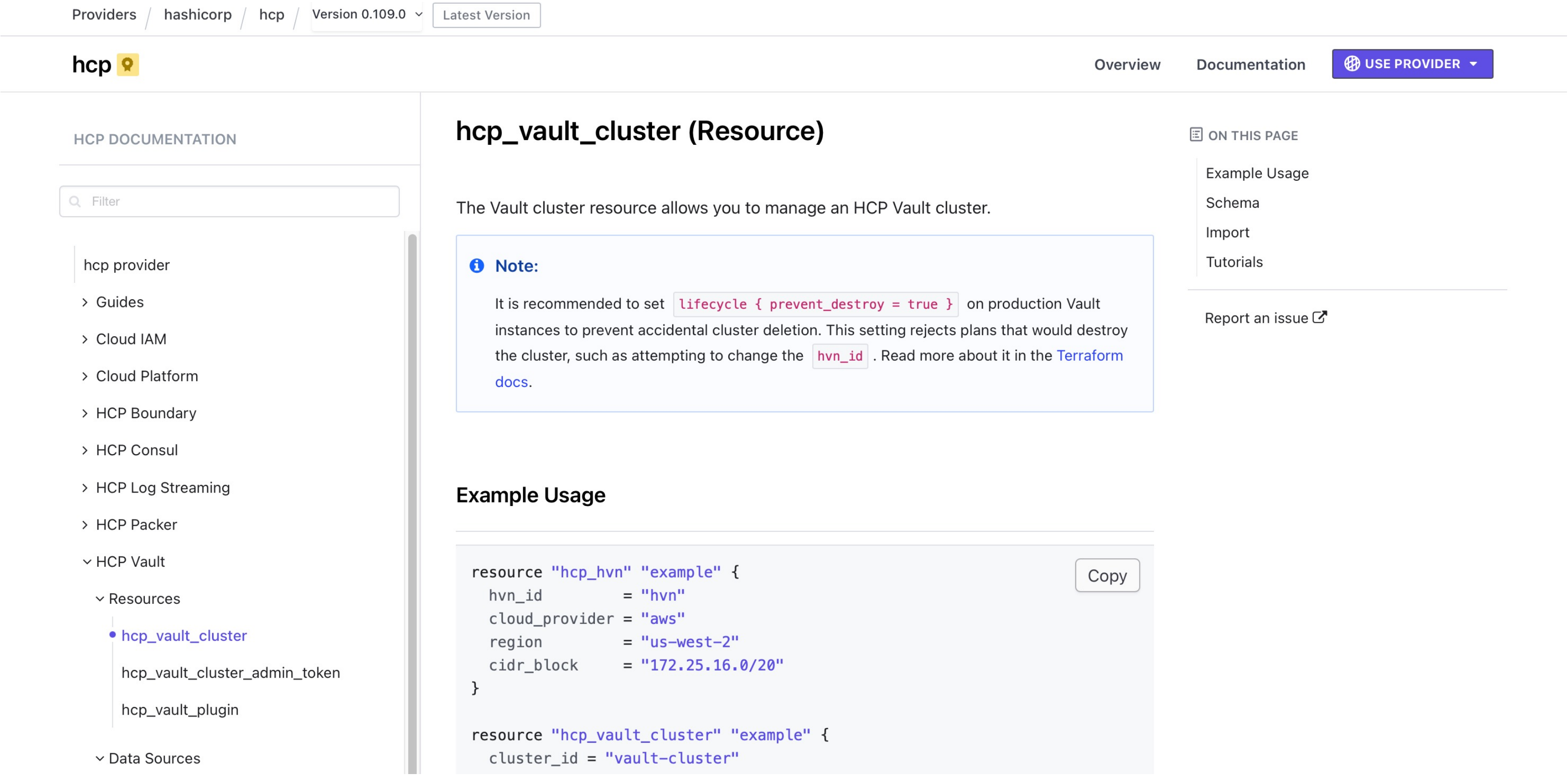
Report repository

Releases 141

v3.0.0 - Breaking Change Latest
on Dec 12, 2024

+ 140 releases

Use automation



hcp_vault_cluster (Resource)

The Vault cluster resource allows you to manage an HCP Vault cluster.

Note:

It is recommended to set `lifecycle { prevent_destroy = true }` on production Vault instances to prevent accidental cluster deletion. This setting rejects plans that would destroy the cluster, such as attempting to change the `hvn_id`. Read more about it in the Terraform docs.

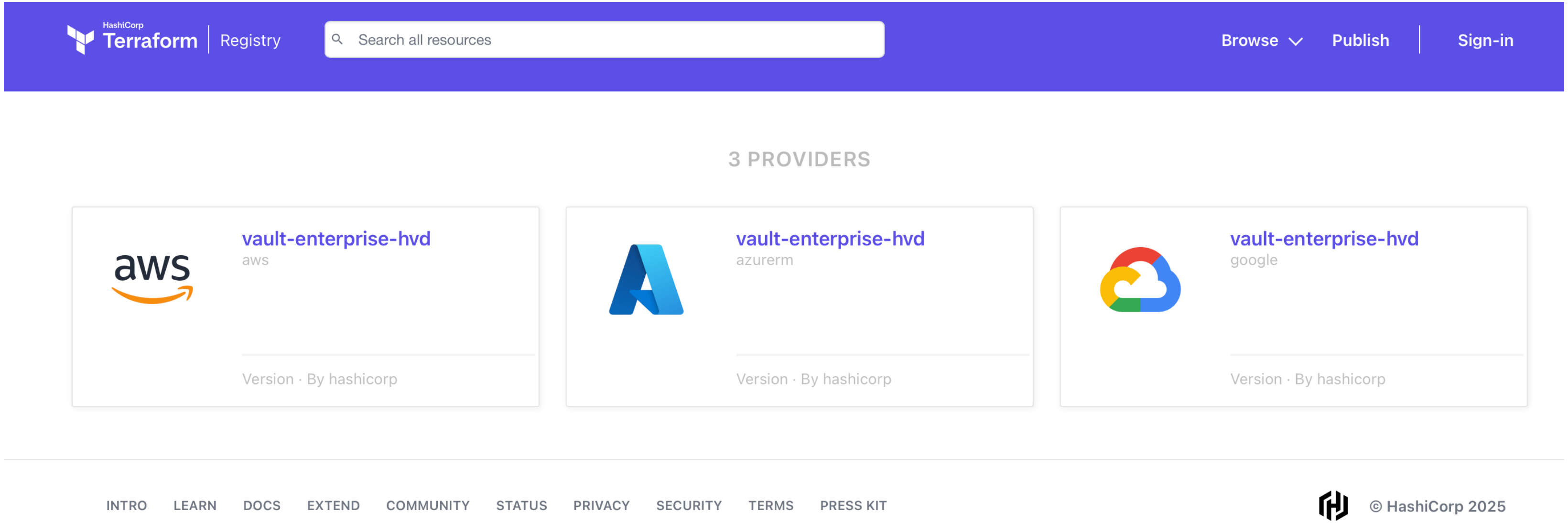
Example Usage

```
resource "hcp_hvn" "example" {
  hvn_id         = "hvn"
  cloud_provider = "aws"
  region         = "us-west-2"
  cidr_block     = "172.25.16.0/20"
}

resource "hcp_vault_cluster" "example" {
  cluster_id = "vault-cluster"
```

/ Deploy your Vault

Use automation



HashiCorp Terraform | Registry

Search all resources

Browse Publish Sign-in

3 PROVIDERS

vault-enterprise-hvd
aws
Version · By hashicorp

vault-enterprise-hvd
azurerm
Version · By hashicorp

vault-enterprise-hvd
google
Version · By hashicorp

INTRO LEARN DOCS EXTEND COMMUNITY STATUS PRIVACY SECURITY TERMS PRESS KIT

© HashiCorp 2025

Use automation

registry.terraform.io

Production Hardening

- Minimal privileges
- Single Tenancy
- e2e TLS
- No swap or core dumps
- Updates
- No root tokens
- Synchronized Clocks
- Audit Logs
- …

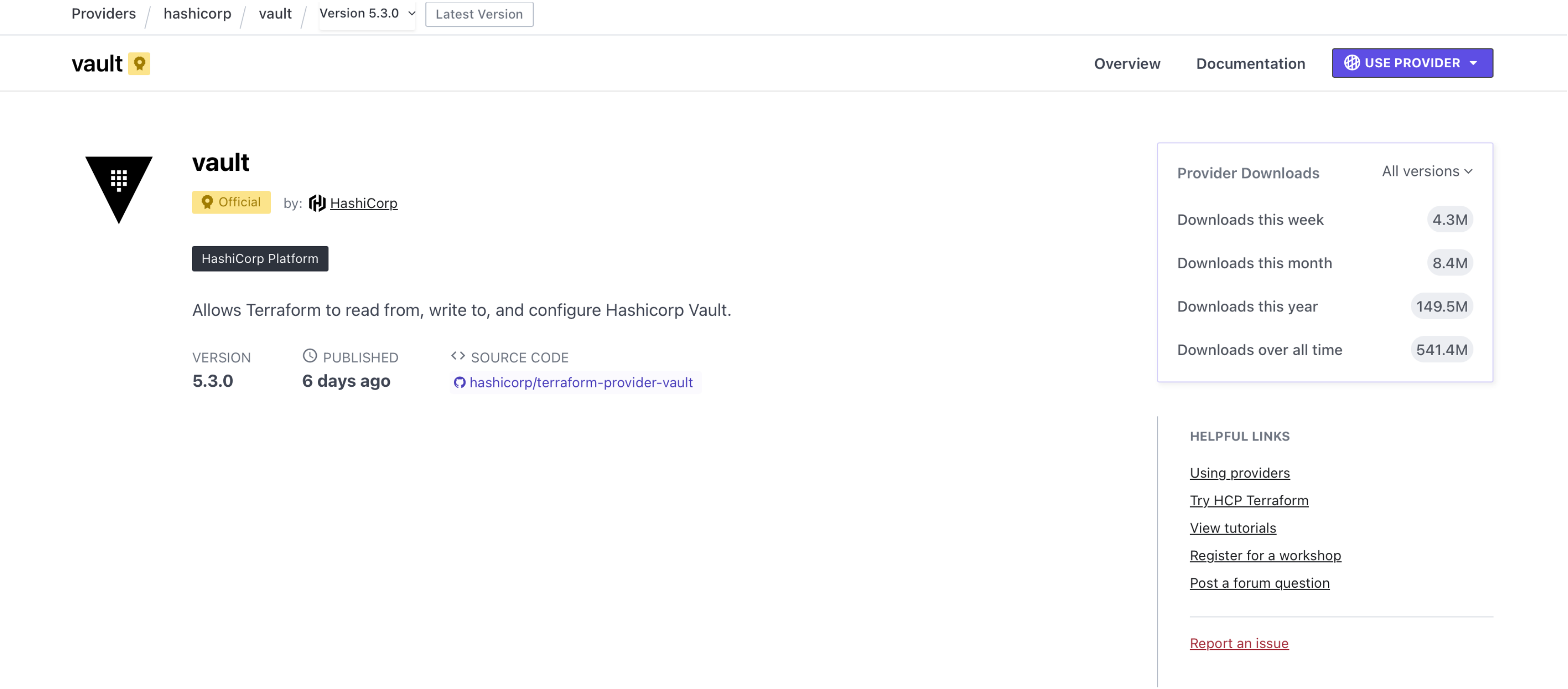
Production Hardening

developer.hashicorp.com

Configure and operate your Vault

/ Configure and operate your Vault

Infrastructure as code



Providers / hashicorp / vault / Version 5.3.0 Latest Version

vault

vault

Official by: HashiCorp

HashiCorp Platform

Allows Terraform to read from, write to, and configure Hashicorp Vault.

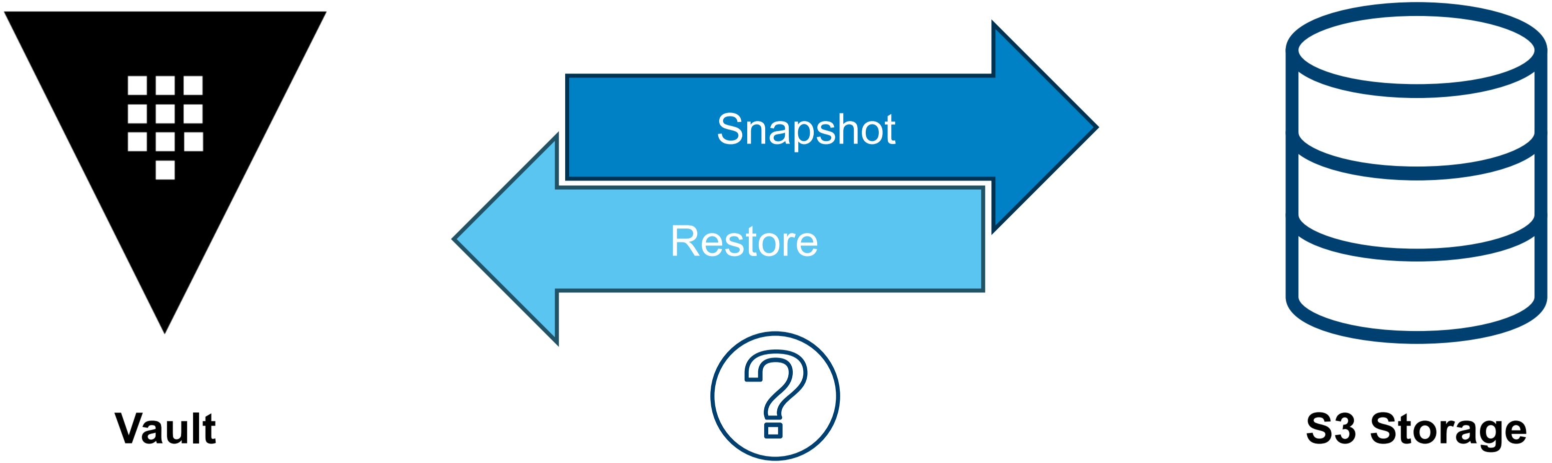
VERSION	PUBLISHED	SOURCE CODE
5.3.0	6 days ago	hashicorp/terraform-provider-vault

Provider Downloads — All versions

Downloads this week	4.3M
Downloads this month	8.4M
Downloads this year	149.5M
Downloads over all time	541.4M

HELPFUL LINKS

Backup & Restore



Observability

Logs

- Operational Logs
- Audit Logs
- Use log aggregation system and/or SIEM

Observability

Logs

- Operational Logs
- Audit Logs
- Use log aggregation system and/or SIEM

Metrics

- Configure the telemetry stanza
- Collect and aggregate your metrics in a proper backend
- Enable alerting on key metrics

Observability

Logs

- Operational Logs
- Audit Logs
- Use log aggregation system and/or SIEM

Metrics

- Configure the telemetry stanza
- Collect and aggregate your metrics in a proper backend
- Enable alerting on key metrics

Synthetic Monitoring

- Write automated tests for your standard workflows
- Run tests continuously
- Keep track of results and execution time

Observability

hashicorp.com/blog

Troubleshooting

Unseal / Recovery Keys

Logs & Log Level

(Physical) Access

Wrap-Up

/ Grab your copy!

Slides

/ Got questions?

Contact

Leon Krass

Technical Leader HashiCorp Vault

+49 151 53882677
leon.krass@sva.de
www.sva.de

SVA System Vertrieb Alexander GmbH
Location Hamburg
Große Elbstraße 273
22767 Hamburg

26
09/2025

HashiConf 2025 | Fort Mason, San Francisco

Lessons Learned from Deploying Vault at Scale