HashiCorp Vault

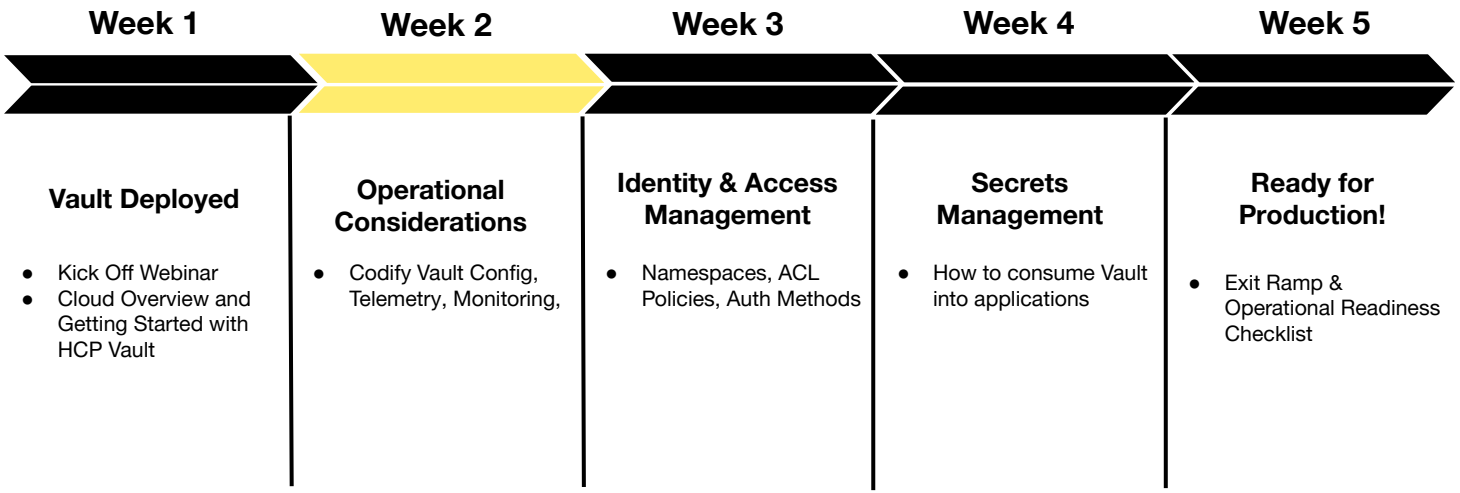
HCP Vault: Operationalizing for Production

October 2022

Agenda

1. Automate HCP Control Plane
2. Automate Vault Configuration
3. Audit Log
4. Telemetry

HCP Vault Path to Production



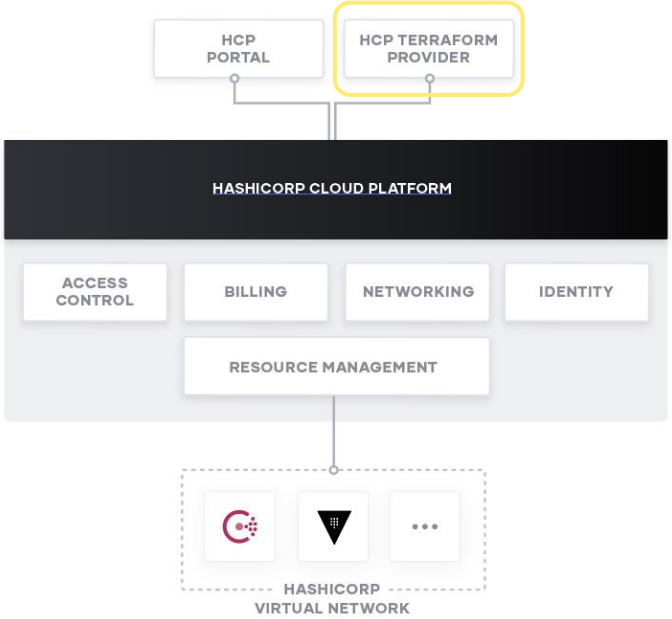
01

Automate HCP Control Plane

HashiCorp Cloud Platform

Overview

- The HashiCorp Cloud Platform (HCP) supports management of the platform via web interface
- HCP Management can be automated using Terraform coupled with the HCP and Vault Terraform providers



Service Principals

Access Controls

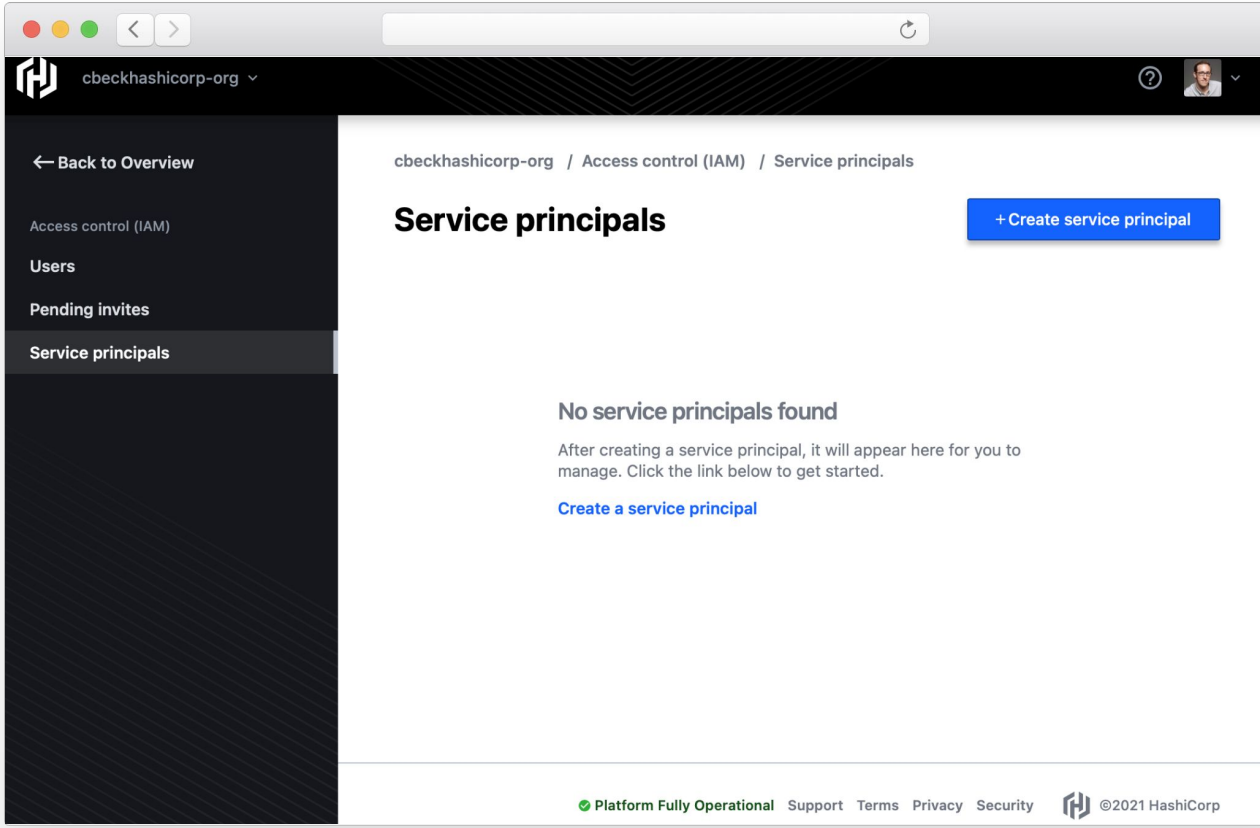
HashiCorp Cloud Platform allows you to grant access to both user and machines

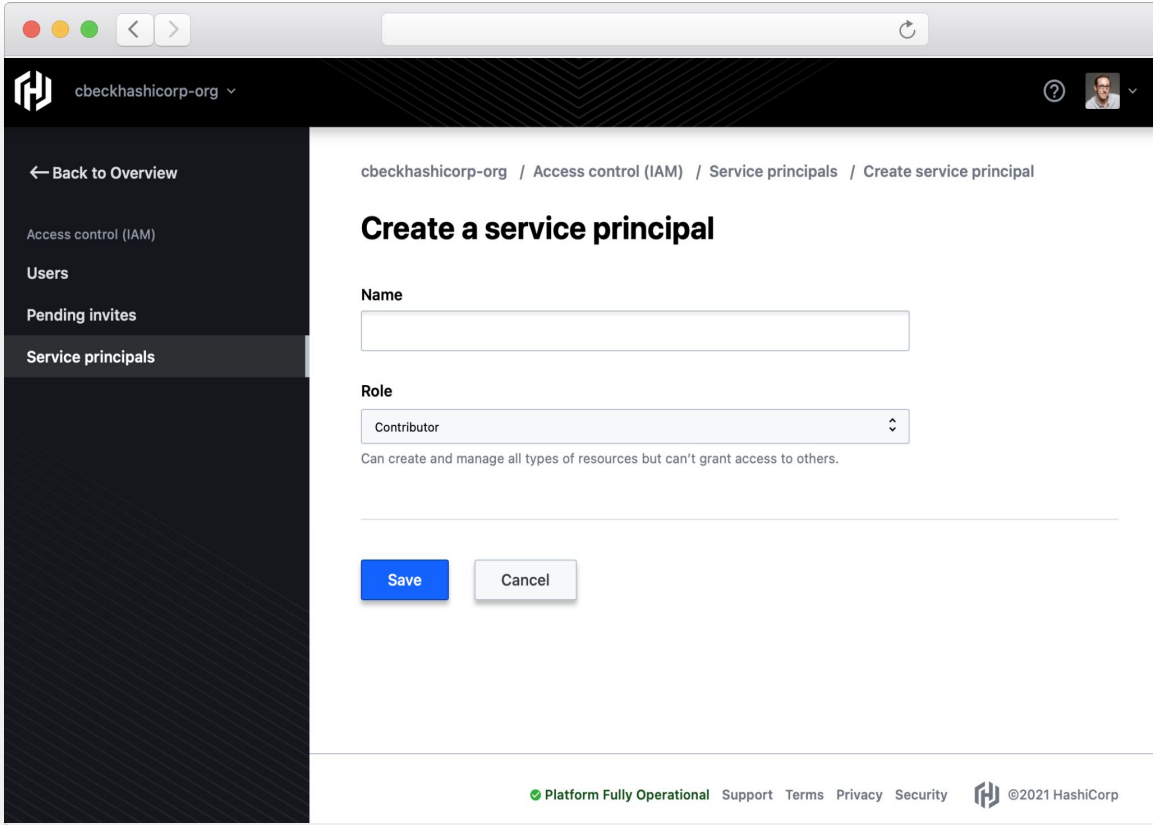
- User access is typically managed via user principal tied to identity
- Non-human clients or machine users need to be granted access using service principals

RBAC

User principals and service principles can be assigned one of three roles (viewer, contributor, and admin) depending on the type of operations the user or service will need to perform.

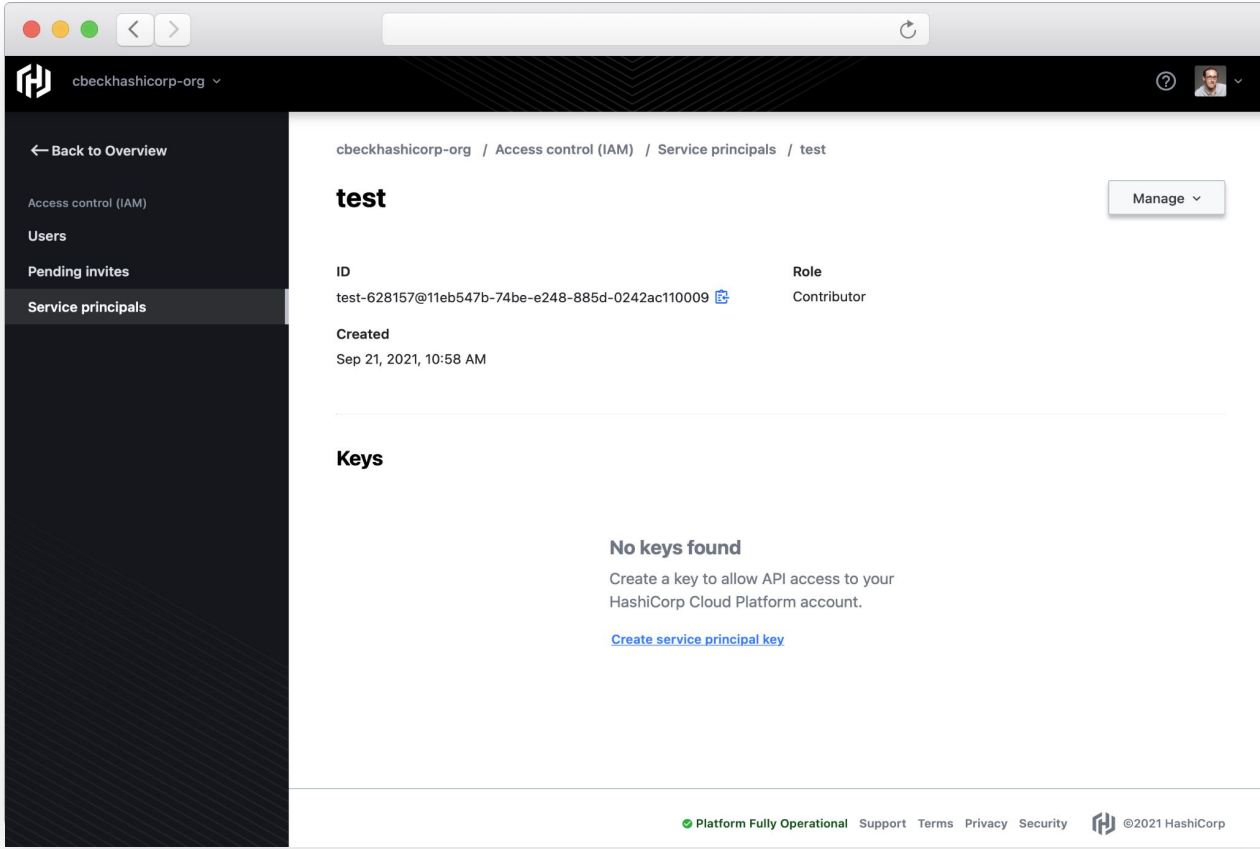
Creating Service Principals

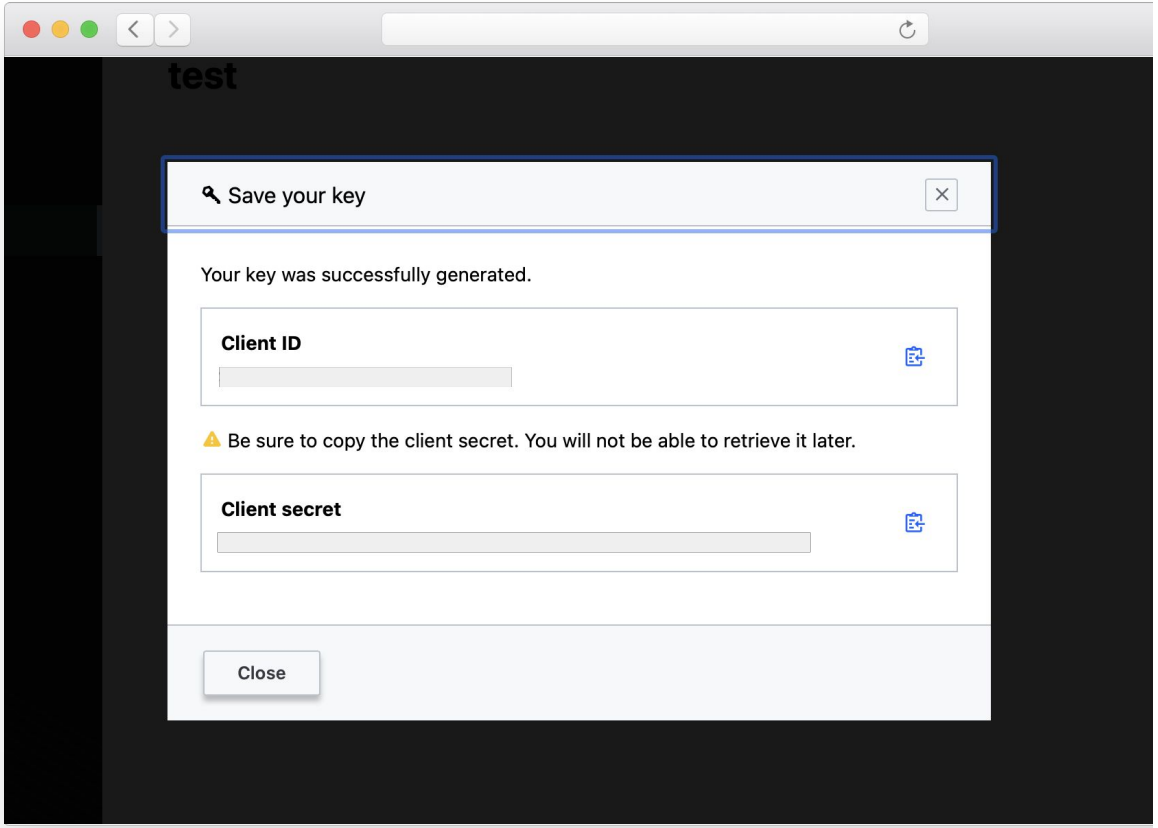




Service Principal Role Selection

Creating Service Principal Key





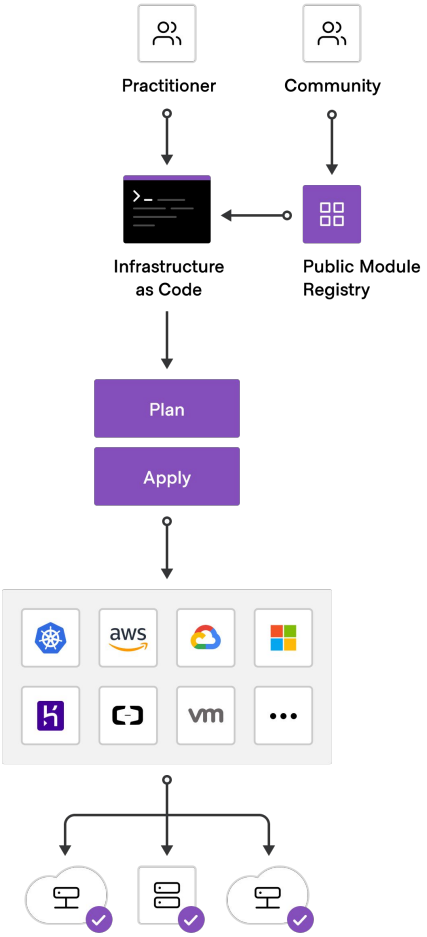
Service Principal Key Secret

Client secret cannot be retrieved later.

Terraform Overview

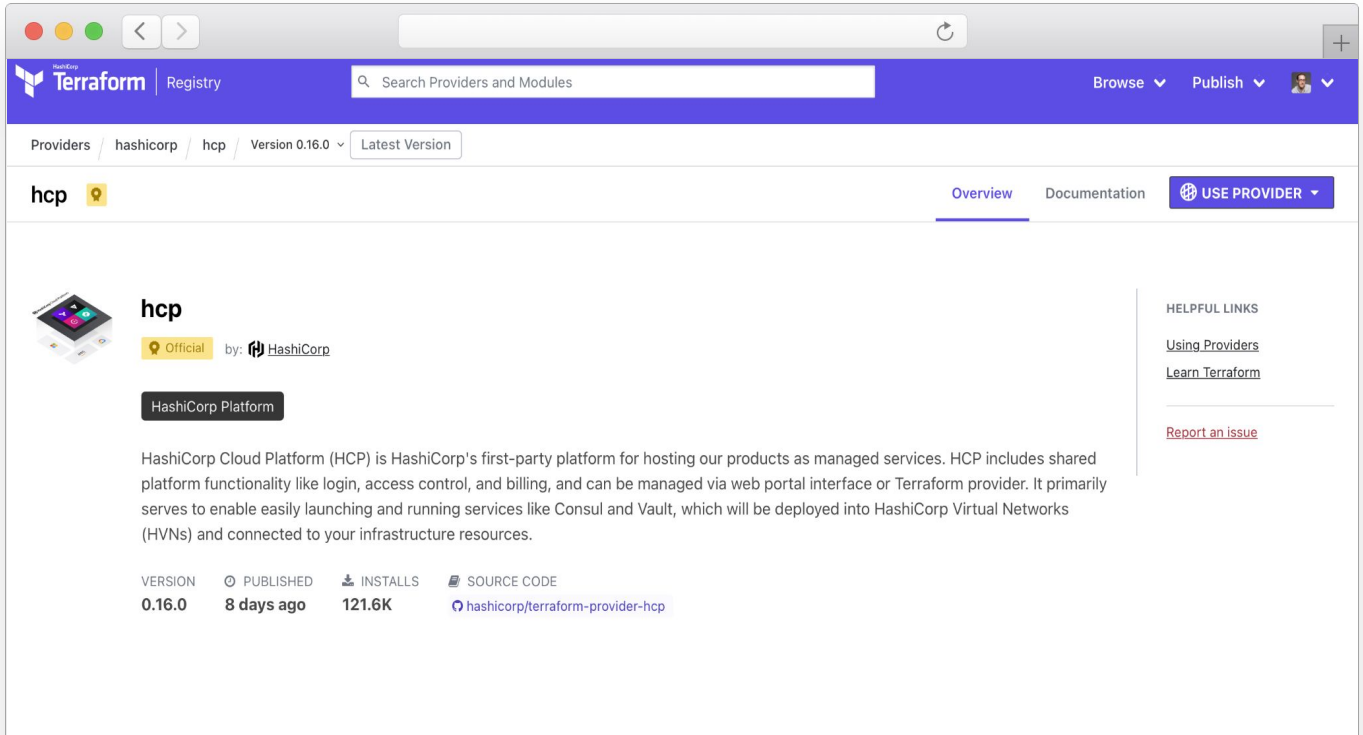
Cloud Infrastructure Automation

- Terraform enables cloud infrastructure automation by codifying your infrastructure as code
- Infrastructure and services from any provider can be provisioned in a codified, secure, and automated fashion



HCP Provider

Provision and manage control plane resources in HCP



Module

[Code on GitHub]

main | 1 branch | 0 tags | Go to file | Add file | Code

cbeckhashicorp Update readme — fbfd629 4 hours ago — 37 commits

.gitignore	update gitignore	20 days ago
awsvpc.tf	update	19 days ago
hcp.tf	update	19 days ago
instances.tf	subnet	20 days ago
outputs.tf	update	19 days ago
provider.tf	cloud	20 days ago
readme.md	Update readme	4 hours ago
variables.tf	variable	20 days ago
vault.tf	update	20 days ago

readme.md

COBRA - HCP Vault Onboarding Train

Week 5 - Operationalizing HCP Vault

This repository contains example code for configuration of the HCP control plane and deployment of an HCP Vault cluster.

THe code includes deployment and configuration of the required AWS components including VPC, Transit

About

No description, website, or topics provided.

Readme
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Languages

HCL 100.0%

02

Automate Vault Configuration

Vault Provider

Provision namespaces, policies, secrets engines, & auth methods

Providers / hashicorp / vault / Version 2.24.0 Latest Version

vault

Overview Documentation USE PROVIDER

vault

Official by: HashiCorp

HashiCorp Platform

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

VERSION	PUBLISHED	INSTALLS	SOURCE CODE
2.24.0	8 days ago	34.5M	hashicorp/terraform-provider-vault

How to use this provider

To install this provider, copy and paste this code into your Terraform configuration. Then, run `terraform init`.

Terraform 0.13+

```
terraform {
  required_providers {
    vault = {
      source = "hashicorp/vault"
      version = "2.24.0"
    }
  }
}

provider "vault" {
  # Configuration options
```

Access HCP Vault using Terraform

CODE EDITOR

```
data "hcp_vault_cluster" "dev" {
      cluster_id = var.cluster_id
}

resource "hcp_vault_cluster_admin_token" "token" {
      cluster_id = var.cluster_id
}

provider "vault" {
      address     = data.hcp_vault_cluster.dev.vault.private_endpoint_url
      token       = hcp_vault_cluster_admin_token.token.token
      namespace   = “admin”
}
```

CODE EDITOR

```
resource "vault_namespace" "infosec" {
  path = "infosec"
}

provider vault {
  alias     = "infosec"
  namespace = vault_namespace.infosec.path
}

resource "vault_policy" "example" {
  provider = vault.infosec
  …
}
```

Namespace & Provider Alias

Create Policy

Create auth method for OIDC provider

CODE EDITOR

```
data "vault_policy_document" "dev_user_policy" {
    rule {
        path         = "secret/data/development/*"
        capabilities = ["create", "read", "update",
"delete", "list"]
    }
}

resource "vault_policy" "devusers" {
    name   = "dev-policy"
    policy = "${data.vault_policy_document.hcl}"
}
```

Enable User Authentication Method

Create auth method for OIDC provider

CODE EDITOR

```
resource "vault_jwt_auth_backend" "oidcauth" {
    description         = "Auth0 OIDC"
    path                = "oidc"
    type                = "oidc"
    oidc_discovery_url  = "https://myco.auth0.com/"
    oidc_client_id      = "1234567890"
    oidc_client_secret  = "secret123456"
    bound_issuer        = "https://myco.auth0.com/"
    tune {
        listing_visibility = "unauth"
    }
}
```

CODE EDITOR

```
resource "vault_jwt_auth_backend_role" "example" {
  backend         = vault_jwt_auth_backend.oidc.path
  role_name       = "test-role"
  token_policies  = ["default", "dev", "prod"]

  user_claim            = "https://vault/user"
  role_type             = "oidc"
  allowed_redirect_uris =
["http://localhost:8200/ui/vault/auth/oidc/oidc/callback"]
}
```

Create Auth Role

Role will define the user claim to authenticate a user and which policy assignments they have in Vault.

Enable Secrets Engines

CODE EDITOR

```
resource "vault_mount" "kvv2-infosec" {
  path                          = "infosec"
  type                          = "kv-v2"
}

resource "vault_mount" "pki-dev" {
  path                          = "pki-dev"
  type                          = "pki"
  default_lease_ttl_seconds     = 3600
  max_lease_ttl_seconds         = 86400
}
```

Best Practices

Protect State

- Terraform, by default, stores state in the working directory where Terraform CLI is executed
- Remote State should be used and encrypted
- Access to state should be limited by following practice of least privilege

Manage as Code

- Treat Terraform configuration files as code
- Store in a VCS like Github and practice least privilege for access and who can commit changes
- Integrate into CI process and ensure code is tested in dev before pushing to production

Sensitive Values

- Do not put any secrets in code
- Pass any secrets, such as credentials or Vault token by using environment variables
- Sensitive values may appear in state if not handled correctly

04

Audit Log

Audit Log

Overview

- HCP Vault includes auditing capabilities for all production tier clusters
- Logs are written locally and stored in an encrypted S3 bucket
- Audit log retention period varies based on the cluster tier as each tier has different storage capabilities

Streaming

- Audit logs can be streamed from any production tier cluster to supported third party logging providers
- Log streaming to Datadog, Grafana Cloud, and Splunk is currently supported

Setup Guides

developer.hashicorp.com

Developer / Vault / Tutorials / HCP Vault Monitoring

HCP Vault Monitoring

Learn how to monitor and audit your HCP Vault clusters.

Create an account to track your progress.

Start | 7 tutorials

10min
HCP Vault Metrics Guide
Learn how to stream HCP Vault cluster telemetry metrics into thrid party tools.

2min
Configure HCP Vault Metrics Streaming to Datadog
Learn how to stream HCP Vault cluster telemetry metrics into Datadog.

2min
Configure HCP Vault Audit Logs Streaming to Datadog
Learn how to stream HCP Vault cluster audit logs into Datadog.

2min
Configure HCP Vault Metrics Streaming to Grafana Cloud
Learn how to stream HCP Vault cluster telemetry metrics into Grafana Cloud.

2min

2min

Audit Log Access

Audit Logs appear under Vault configuration on the cluster page

Cluster

Configure your HashiCorp Virtual Network, **hvn**, with a peering connection or transit gateway attachment to access your cluster.

View network

This cluster's IP address configuration has been set to public. It is not recommended to use this configuration in production.

Learn more about integration & scaling

Ready to learn more about using Vault and security best practices? Start with our Learn and Docs sites.

- Running Commands with the Vault CLI
- Managing access & policies
- Enabling authentication methods
- Enabling secrets engines
- Integrating with your applications
- Optimizing clients for Vault Cloud
- Vault documentation

Usage

Current clients	0
	0 entity tokens
	0 non-entity tokens

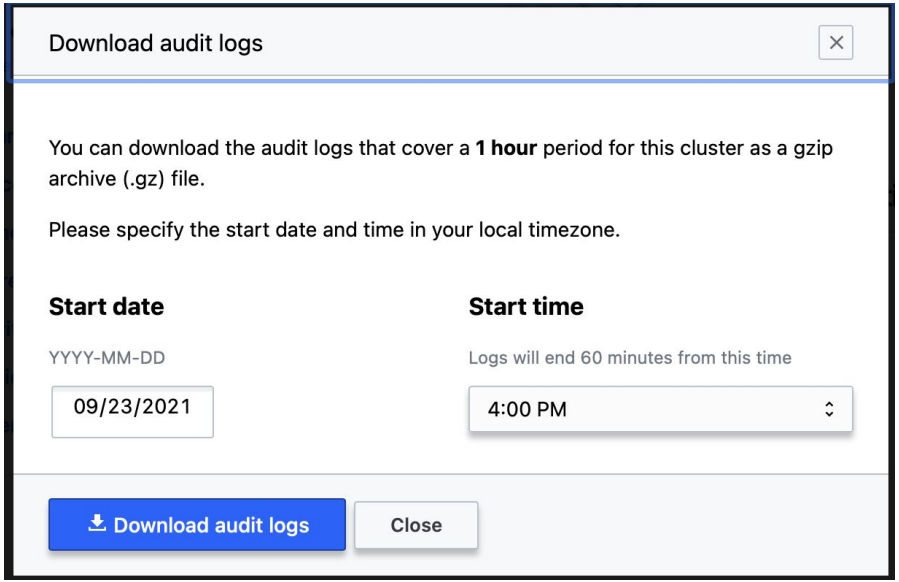
Vault configuration

State	Running
Version	v1.8.1
Namespace	admin
Cluster URLs	Private
	Public
Configuration	Default
Generate admin token	+ Generate token
Audit logs	Access audit logs

In case of emergency

Download Audit Logs

- Audit logs can be downloaded in 1 hour increments
- Once audit log are downloaded they can be imported into monitoring solutions for analysis



05

Telemetry

Vault Telemetry

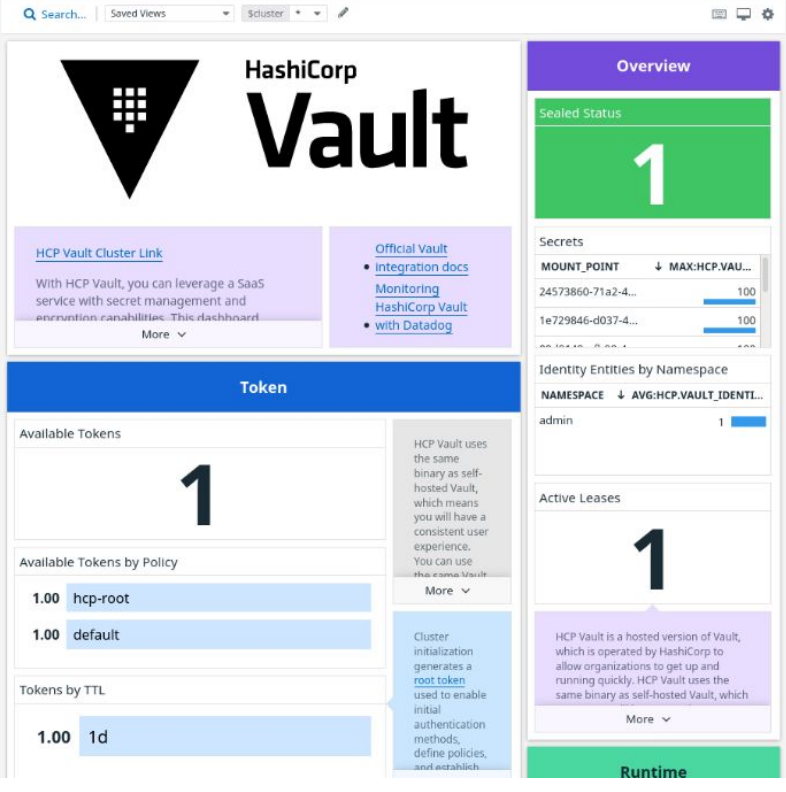
Overview

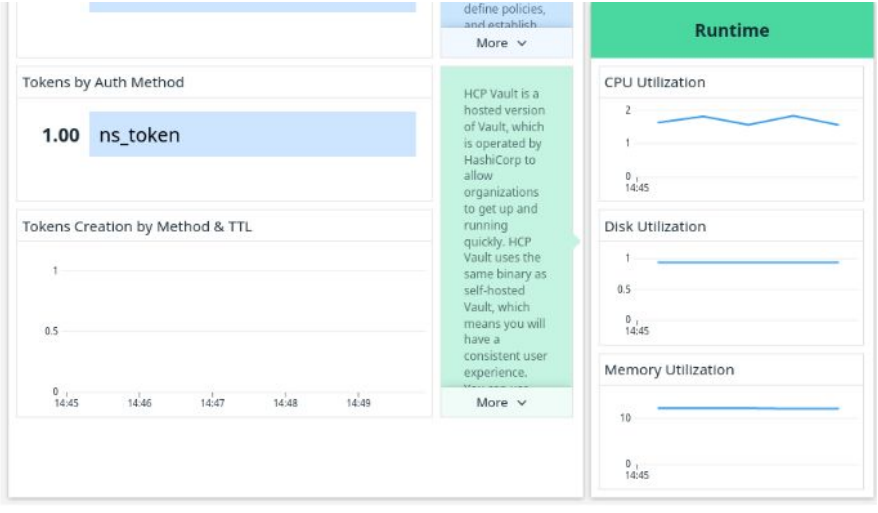
- HCP Vault supports telemetry monitoring to better understand the metrics and usage of your HCP Vault implementation
- Metrics can be streamed to Datadog, Grafana Cloud, and Splunk

Considerations

- Metrics streaming is currently supported with the three providers listed above
- If you are using an additional provider that is not currently supported, please contact us with more information so we can investigate support in future releases
- Metrics streaming is not supported with development tier clusters

Example DataDog Dashboard





Monitoring Patterns

Organizations that have successfully adopted Vault at scale typically classify Vault as a tier 0 application as it is typically a dependency for their most critical applications.

Three patterns that should be adopted for monitoring the health of Vault include:

1. Time-series telemetry data
2. Log Analytics
3. Active Health Checks

Metric Types

[C] Counter

Cumulative metrics that increment when an event occurs and are reset at the end of the reporting interval.

[G] Gauge

Provides measurements of current values

[S] Summary

Provide sample observations of values. Commonly used to measure timing duration of discrete events in the reporting interval.

Contributing Factors in Performance

- Know the expected workload
- Vault System Resources (CPU, MEM, Disk)
- Complexity of Vault Policies
- Audit Logging
- Network for all the things

Key System Metrics

Metric	Description	What to look for?
vault.core.unsealed	Status of Vault seal 1 unsealed. 0 sealed	Unexpected changes to 0
host_cpu_seconds_total	Total CPU time	Heavy
Host_cpu_seconds_total (idle mode)	Time CPU in idle state	Look for heavy CPU usage or unexpected periods of idle, may indicate incorrect sizing.
host_cpu_seconds_total	Total CPU time	
host_memory_total_bytes	Physical RAM available to server	Look for high memory usage or under utilized physical RAM to ensure correct system sizing.
host_memory_available_bytes	Unused physical RAM on the server	

Key Usage Metrics

Metric	Description
vault.token.creation	A new service or batch token was created
vault.token.count	Number of service tokens available for use.
vault.token.count.by_auth	Number of existing tokens broken down by the auth method used to create them.
vault.token.count.by_policy	Number of existing tokens, counted in each policy assigned.
vault.token.count.by_ttl	Number of existing tokens, aggregated by their TTL at creation.
vault.secret.kv.count	Count of secrets in key-value stores.
vault.secret.lease.creation	Count of leases created by a secret engine (excluding leases created internally for token expiration.)

Setup Guides

developer.hashicorp.com

Developer / Vault / Tutorials / HCP Vault Monitoring

HCP Vault Monitoring

Learn how to monitor and audit your HCP Vault clusters.

Create an account to track your progress.

Start | 7 tutorials

10min
HCP Vault Metrics Guide
Learn how to stream HCP Vault cluster telemetry metrics into thrid party tools.

2min
Configure HCP Vault Metrics Streaming to Datadog
Learn how to stream HCP Vault cluster telemetry metrics into Datadog.

2min
Configure HCP Vault Audit Logs Streaming to Datadog
Learn how to stream HCP Vault cluster audit logs into Datadog.

2min
Configure HCP Vault Metrics Streaming to Grafana Cloud
Learn how to stream HCP Vault cluster telemetry metrics into Grafana Cloud.

2min

2min

06

Next Steps

Tutorials

https://developer.hashicorp.com/vault/tutorials

Step-by-step guides to accelerate deployment of Vault

Vault

Home | Documentation | Tutorials | Install | Try Cloud

Search ⌘/ctrl K

Vault Home

Tutorials

Overview

Get Started

CLI Quick Start

HCP Vault Quick Start

UI Quick Start

Use Cases

ADP

Database Credentials

Data Encryption

Key Management

Secrets Management

Certification Prep

Associate

Developer / Vault / Tutorials

Centrally store, access and deploy secrets

Explore HCP Vault →

Get Started

13 tutorials

Getting Started

Vault secures, stores, and tightly controls access to tokens, passwords, certificates, API keys,...

8 tutorials

Getting Started with Vault UI

Manage Vault environment as well as your secrets using Vault UI.

9 tutorials

Getting Started with HCP Vault

Quickly get hands-on with HashiCorp Cloud Platform (HCP) Vault using the HCP portal and setup your manage...

Featured Tutorials

Extend your knowledge of Vault features and use cases.

7 tutorials

Vault 1.12 Release Highlights

The listed tutorials were updated to showcase the new enhancements

12 tutorials

HCP Vault Operations

Learn how to provision and connect to HCP Vault clusters.

5 tutorials

Security

Implement security best practices to secure your applications, protect

On this page

- Get Started
- Featured Tutorials
- New Tutorials
- Popular Topics
- All Tutorials

Resources

- HashiCorp Cloud Platform (HCP) Provider
- Sample Terraform Deployment Code
- Vault Provider
- HCP Vault Telemetry & Monitoring

Need Additional Help?

Customer Success

Contact our Customer Success Management team with any questions. We will help coordinate the right resources for you to get your questions answered.

customer.success@hashicorp.com

Technical Support

Something not working quite right? Engage with HashiCorp Technical Support by opening a ticket for your issue at support.hashicorp.com.

Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

discuss.hashicorp.com

Next Steps

- Upcoming Schedule:
  - Week 3 - Namespaces, Authentication, and Policies Webinar - Learn how to implement identity and access management in HCP Vault
  - Week 4 - Consuming HCP Vault webinar - Learn how to consume secrets from Vault in your apps and services
  - Week 5 - HCP Vault train closing session

Q & A

Thank You

customer.success@hashicorp.com
www.hashicorp.com