



# HCP Vault: Operationalizing for Production



# Agenda

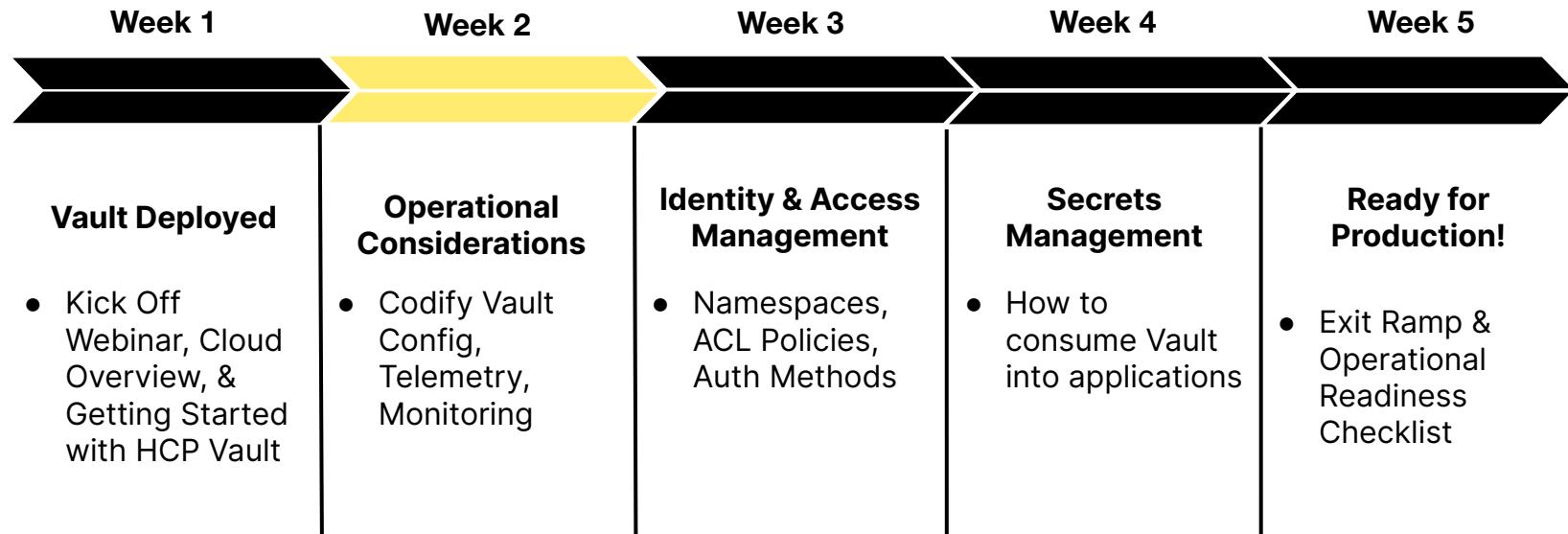
- 
- Automate HCP Control Plane 01
  - Automate Vault Configuration 02
  - Audit Log 03
  - Telemetry 04
- 



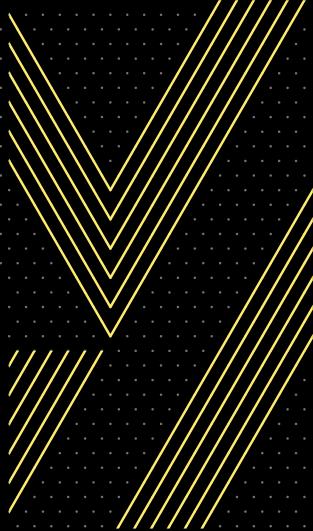
# HCP Vault Onboarding Program

A 5 week guided community environment

Assisting customers with onboarding and adoption



01

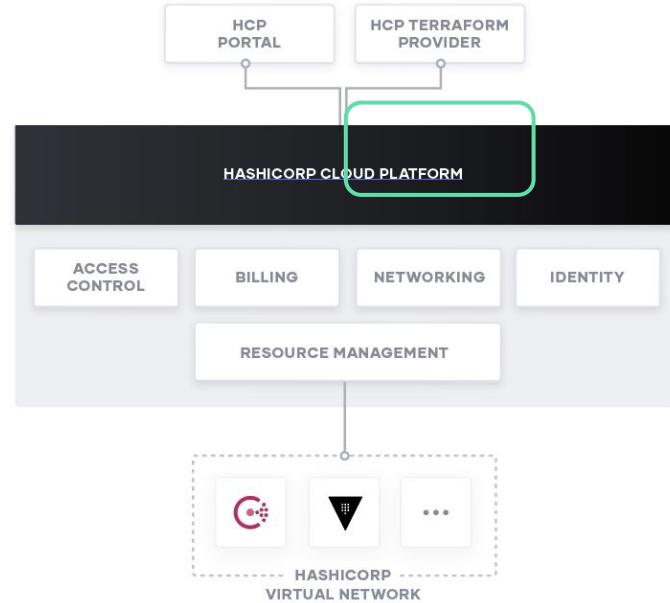


# Automate HCP Control Plane

# 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

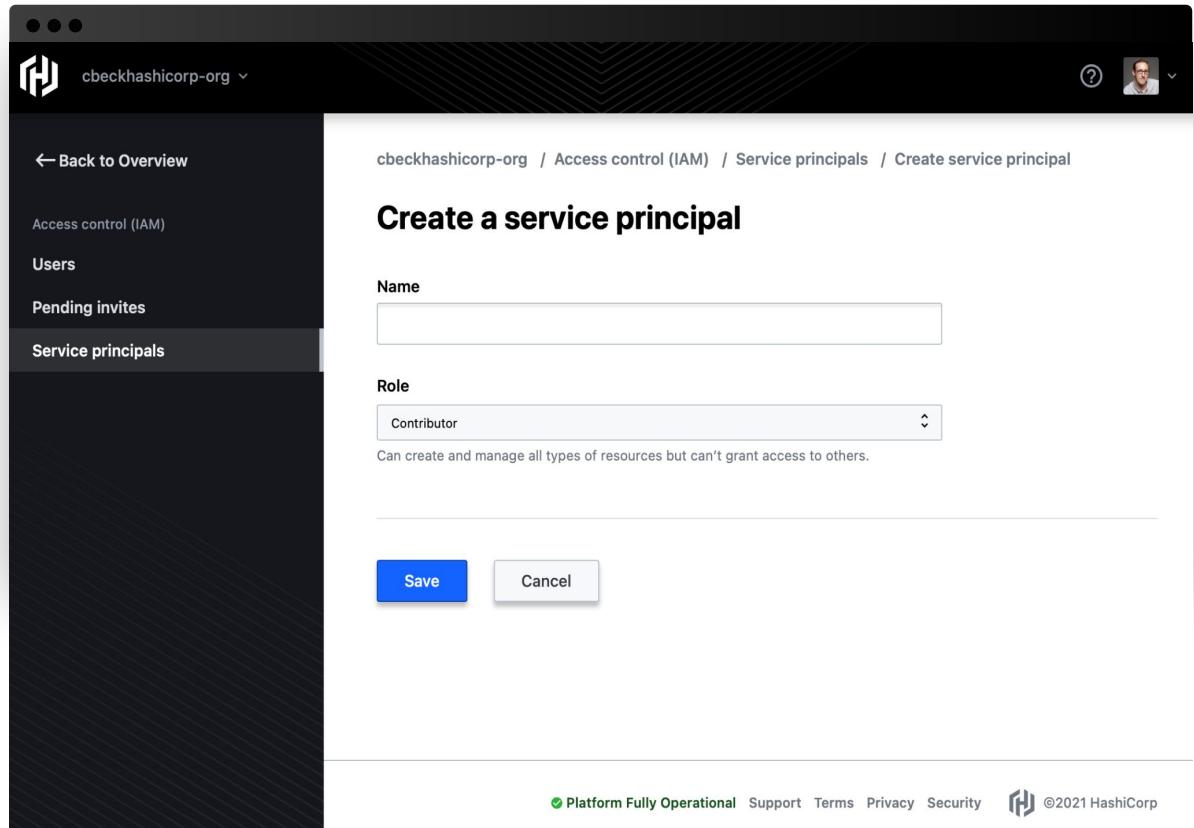
User principals and service principles can be assigned one of three roles (viewer, contributor, and admin) depending on the type of operations the user or service will need to perform.



# Creating Service Principals

The screenshot shows the HashiCorp Vault interface. At the top, there's a dark header bar with the HashiCorp logo, the organization name "cbeckhashicorp-org", and a user profile icon. Below the header is a navigation sidebar on the left with options: "Back to Overview", "Access control (IAM)", "Users", "Pending invites", and "Service principals". The "Service principals" option is highlighted with a grey background. The main content area has a breadcrumb navigation: "cbeckhashicorp-org / Access control (IAM) / Service principals". The title "Service principals" is displayed prominently. A blue button labeled "+Create service principal" is located in the top right corner of this section. Below the title, a message states "No service principals found" and provides instructions: "After creating a service principal, it will appear here for you to manage. Click the link below to get started." A blue link labeled "Create a service principal" is provided. At the bottom of the page, there's a footer with links: "Platform Fully Operational" (green), "Support", "Terms", "Privacy", "Security", the HashiCorp logo, and the text "©2021 HashiCorp".

# Creating Service Principals



The screenshot shows the HashiCorp Platform interface for creating a service principal. The top navigation bar includes the HashiCorp logo, the organization name "cbeckhashicorp-org", a user profile icon, and a help icon. The left sidebar has a "Back to Overview" link and categories: "Access control (IAM)", "Users", "Pending invites", and "Service principals", with "Service principals" being the active tab. The main content area is titled "Create a service principal". It has fields for "Name" (an empty input field) and "Role" (a dropdown menu set to "Contributor"). A descriptive note below the role says: "Can create and manage all types of resources but can't grant access to others." At the bottom are "Save" and "Cancel" buttons. The footer contains links for "Platform Fully Operational", "Support", "Terms", "Privacy", "Security", and the HashiCorp logo with the text "©2021 HashiCorp".

cbeckhashicorp-org / Access control (IAM) / Service principals / Create service principal

## Create a service principal

Name

Role

Contributor

Can create and manage all types of resources but can't grant access to others.

Save Cancel

Platform Fully Operational Support Terms Privacy Security ©2021 HashiCorp

# Creating Service Principal Key

The screenshot shows the HashiCorp Cloud Platform interface for creating a service principal key. The left sidebar has a dark theme with navigation options: Back to Overview, Access control (IAM), Users, Pending invites, and Service principals (which is selected). The main content area shows a service principal named "test". The details for "test" include:

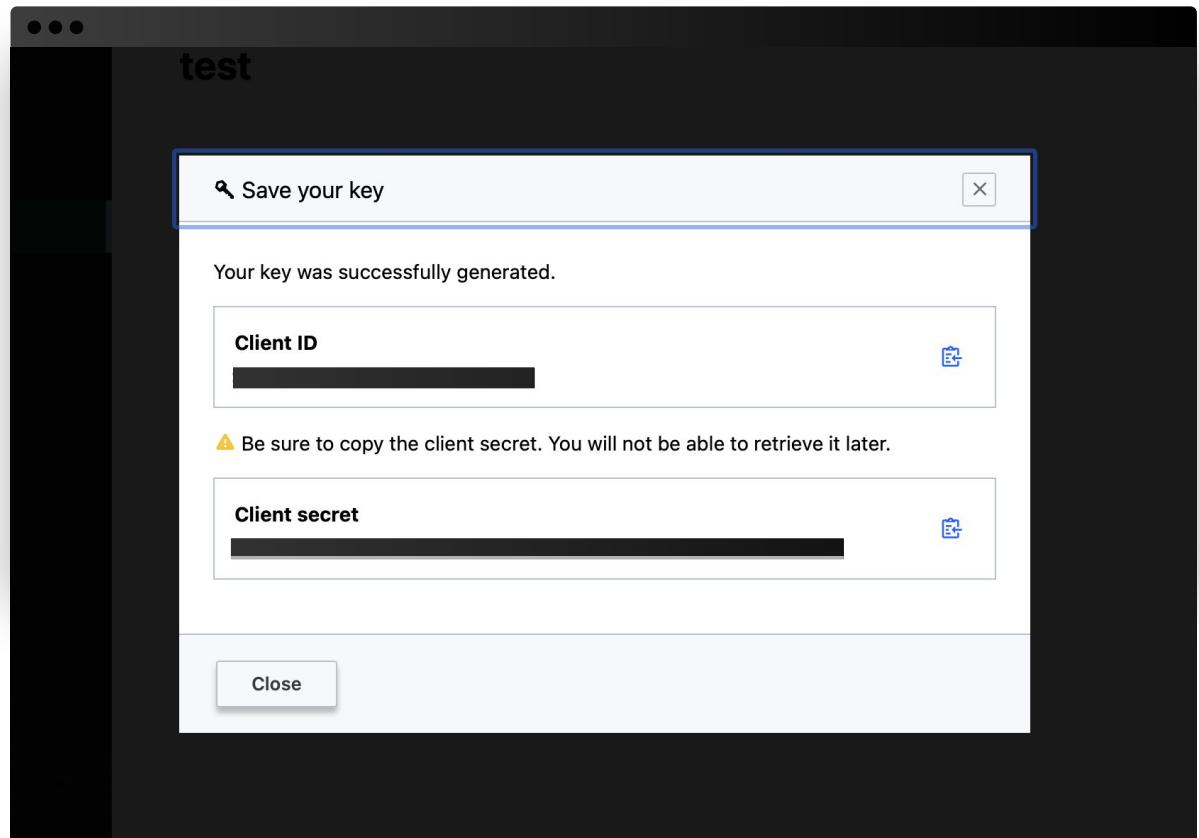
- ID: test-628157@11eb547b-74be-e248-885d-0242ac110009
- Role: Contributor
- Created: Sep 21, 2021, 10:58 AM

Below this, the "Keys" section displays the message "No keys found" and a link to "Create service principal key".

At the bottom of the page, there is a footer bar with icons and text: "Platform Fully Operational" (green), Support, Terms, Privacy, Security, the HashiCorp logo, and the text "© 2021 HashiCorp".

# Service Principal Key Secret

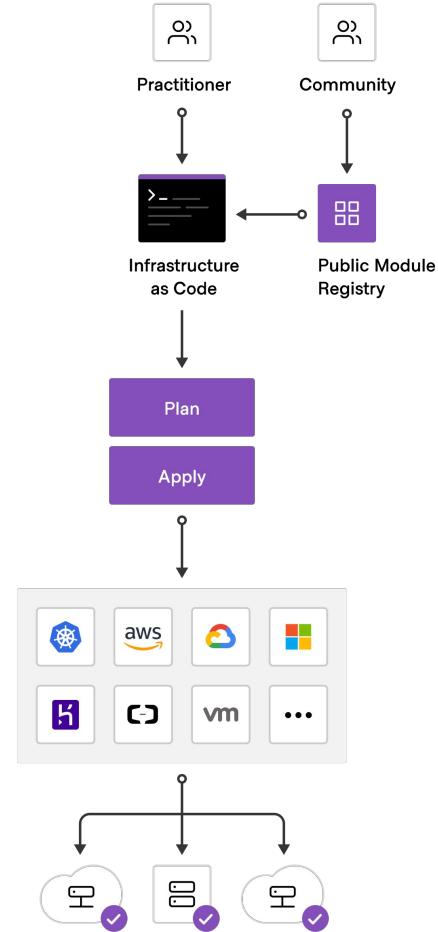
Client secret cannot be retrieved later



# 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 HC

The screenshot shows the HashiCorp Terraform Registry interface. At the top, there's a navigation bar with the HashiCorp logo, a search bar labeled "Search Providers and Modules", and dropdown menus for "Browse", "Publish", and user profile. Below the header, a breadcrumb navigation shows "Providers / hashicorp / hcp / Version 0.16.0" and a "Latest Version" button. The main content area features a provider icon, the name "hcp", an "Official" badge, and the publisher "HashiCorp". A "HashiCorp Platform" button is also present. To the right, there's a sidebar titled "HELPFUL LINKS" containing links to "Using Providers" and "Learn Terraform", and a "Report an issue" button. Below the provider details, a descriptive paragraph explains HCP as HashiCorp's first-party platform for hosting products as managed services. At the bottom, technical details are listed: "VERSION 0.16.0", "PUBLISHED 8 days ago", "INSTALLS 121.6K", and "SOURCE CODE hashicorp/terraform-provider-hcp".

HashiCorp Terraform Registry

Search Providers and Modules

Browse ▾ Publish ▾

Providers / hashicorp / hcp / Version 0.16.0 ▾ Latest Version

hcp Official by: HashiCorp

HashiCorp Platform

HELPFUL LINKS

Using Providers

Learn Terraform

Report an issue

HashiCorp Cloud Platform (HCP) is HashiCorp's first-party platform for hosting our products as managed services. HCP includes shared platform functionality like login, access control, and billing, and can be managed via web portal interface or Terraform provider. It primarily serves to enable easily launching and running services like Consul and Vault, which will be deployed into HashiCorp Virtual Networks (HVNs) and connected to your infrastructure resources.

VERSION 0.16.0 PUBLISHED 8 days ago INSTALLS 121.6K SOURCE CODE hashicorp/terraform-provider-hcp



# Module

[Code on GitHub](#)

The screenshot shows a GitHub repository interface. At the top, there are navigation buttons for 'main' (with a dropdown arrow), '1 branch' (with a dropdown arrow), '0 tags' (with a dropdown arrow), 'Go to file', 'Add file', and 'Code' (with a dropdown arrow). On the right side, there's an 'About' section with the message 'No description, website, or topics provided.' Below it are icons for 'Readme' (document icon), '0 stars' (star icon), '1 watching' (eye icon), and '0 forks' (fork icon). Further down are sections for 'Releases' (with a note 'No releases published' and a link 'Create a new release') and 'Packages' (with a note 'No packages published' and a link 'Publish your first package'). The main content area displays a list of commits from 'cbeckhashicorp' (fbfd629) made 4 hours ago, showing updates to various files like '.gitignore', 'awsvpc.tf', 'hcp.tf', etc. Below the commits is a preview of the 'readme.md' file, which contains the title 'COBRA - HCP Vault Onboarding Train' and a section 'Week 5 - Operationalizing HCP Vault'. A note below states: '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'.

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

The screenshot shows the Hashicorp Vault provider page on the Terraform Registry. The URL is [https://registry.terraform.io/providers/hashicorp/vault/2.24.0](#). The page has a dark header with three dots on the left. Below it is a light-colored navigation bar with links for Providers, hashicorp, vault, Version 2.24.0, and Latest Version. The main content area has a title "vault" with a yellow lock icon. To the right are tabs for Overview (which is selected), Documentation, and a "USE PROVIDER" button with a globe icon. The "Overview" tab contains a provider icon (a black triangle with a white grid), the provider name "vault", a "Official" badge, and the developer "HashiCorp". A "HashiCorp Platform" badge is also present. A brief description states: "Allows Terraform to read from, write to, and configure Hashicorp Vault." Below this are details: VERSION 2.24.0, PUBLISHED 8 days ago, INSTALLS 34.5M, and SOURCE CODE linking to [hashicorp/terraform-provider-vault](#). To the right, a box titled "How to use this provider" contains instructions: "To install this provider, copy and paste this code into your Terraform configuration. Then, run `terraform init`". It also lists "Terraform 0.13+" and shows a snippet of Terraform code:

```
terraform {  
  required_providers {  
    vault = {  
      source = "hashicorp/vault"  
      version = "2.24.0"  
    }  
  }  
  
provider "vault" {  
  # Configuration options  
}
```



# Access HCP Vault using Terraform

```
...
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"
}
```

# Namespace & Provider Alias

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

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

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

...
```

# Create Policy

Create auth method  
for OIDC provider

```
...
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

```
...
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"
    }
}
```

# Create Auth Role

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

```
...
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"]
}
```

# Enable Secrets Engines

```
...
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

03



# 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](https://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 third 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

### Configure HCP Vault Audit Logs Streaming to Grafana

2min

### Configure HCP Vault Metrics Streaming to Splunk

# Audit Log Access

Audit Logs appear under Vault configuration on the cluster page

The screenshot shows the HashiCorp Vault cluster configuration interface. At the top, there's a banner for configuring a HashiCorp Virtual Network (hvn) with a peering connection or transit gateway attachment. Below this, a note says "This cluster's IP address configuration has been set to public. It is not recommended to use this configuration in production." On the left, a sidebar lists "Learn more about integration & scaling" with links to various Vault documentation pages. The main area is titled "Usage" and shows "Current clients: 0", "0 entity tokens", and "0 non-entity tokens". To the right, under "Vault configuration", it shows the "State" as "Running", "Version" as "v1.8.1", "Namespace" as "admin", and "Cluster URLs" with options for "Private" and "Public". There are also sections for "Configuration" (set to "Default") and "Generate admin token" (with a button to "+ Generate token"). At the bottom, there's a link to "Access audit logs". A footer at the very bottom reads "In case of emergency".

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**

- [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**

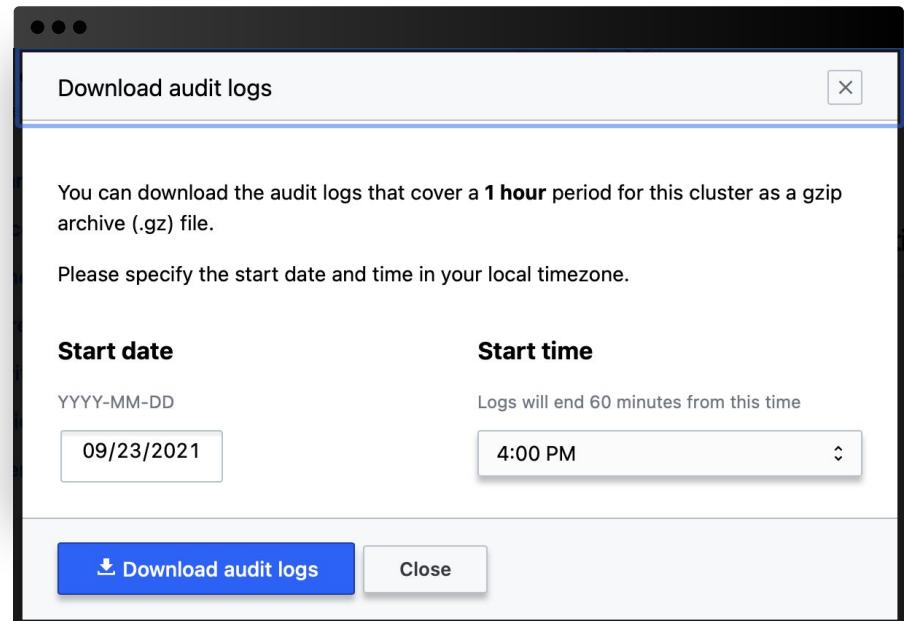
State	<span>Running</span>
Version	v1.8.1
Namespace	admin
Cluster URLs	<span>Private</span> <span>Public</span>
Configuration	Default
Generate admin token	<a href="#">+ Generate token</a>
Audit logs	<a href="#">Access audit logs</a>

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



04



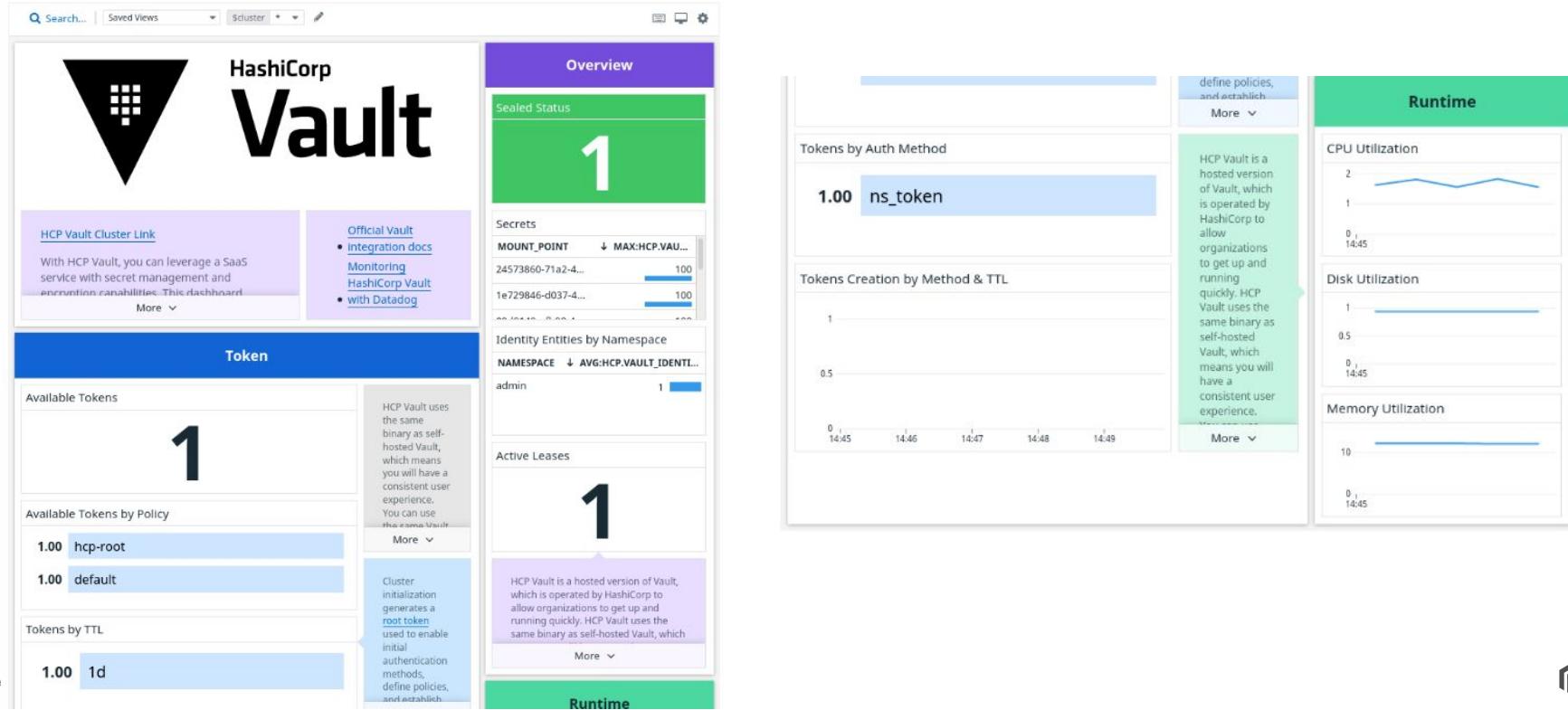
# Telemetry

# 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
- 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	



# Setup Guides

[developer.hashicorp.com](https://developer.hashicorp.com)

The screenshot shows a web browser displaying a tutorial page titled "HCP Vault Monitoring". The URL in the address bar is "Developer / Vault / Tutorials / HCP Vault Monitoring". The page features a "Start" button and a "7 tutorials" link. Below these, there are five cards, each representing a different tutorial:

- HCP Vault Metrics Guide** (10min): Learn how to stream HCP Vault cluster telemetry metrics into third party tools.
- Configure HCP Vault Metrics Streaming to Datadog** (2min): Learn how to stream HCP Vault cluster telemetry metrics into Datadog.
- Configure HCP Vault Audit Logs Streaming to Datadog** (2min): Learn how to stream HCP Vault cluster audit logs into Datadog.
- Configure HCP Vault Metrics Streaming to Grafana Cloud** (2min): Learn how to stream HCP Vault cluster telemetry metrics into Grafana Cloud.
- Configure HCP Vault Audit Logs Streaming to Grafana** (2min): Learn how to stream HCP Vault cluster audit logs into Grafana.
- Configure HCP Vault Metrics Streaming to Splunk** (2min): Learn how to stream HCP Vault cluster telemetry metrics into Splunk.

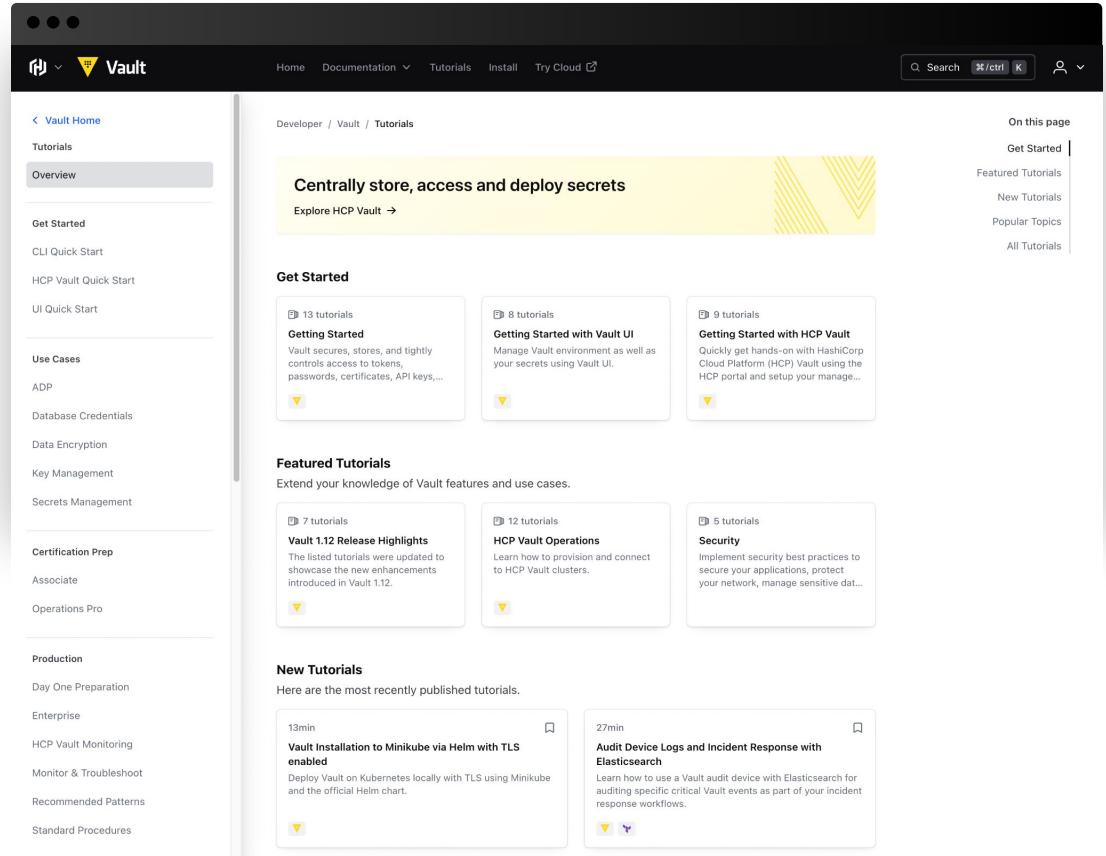


# Next Steps



# Tutorials

Step-by-step guides to accelerate deployment of Vault



The screenshot shows the HashiCorp Vault Tutorials page. At the top, there's a navigation bar with links for Home, Documentation, Tutorials, Install, Try Cloud, and a search bar. On the left, a sidebar lists various tutorial categories: 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, Operations Pro), Production (Day One Preparation, Enterprise, HCP Vault Monitoring, Monitor & Troubleshoot, Recommended Patterns, Standard Procedures). The main content area features a yellow banner with the text "Centrally store, access and deploy secrets" and a link to "Explore HCP Vault". Below this, there are three sections: "Get Started" (with 13 tutorials), "Featured Tutorials" (with 7, 12, and 5 tutorials for Vault 1.12 Release Highlights, HCP Vault Operations, and Security), and "New Tutorials" (with two entries: "Vault Installation to Minikube via Helm with TLS enabled" and "Audit Device Logs and Incident Response with Elasticsearch"). A sidebar on the right titled "On this page" includes links for Get Started, Featured Tutorials, New Tutorials, Popular Topics, and All Tutorials.

<https://developer.hashicorp.com/vault/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](mailto: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](https://support.hashicorp.com)

## Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

[discuss.hashicorp.com](https://discuss.hashicorp.com)



# Upcoming Webinars

## Namespaces, Authentication & Policies

Learn best practices for deploying and managing Namespaces, Auth Methods, and Vault policy

## Consuming Secrets from HCP Vault

The webinar covers how Vault works with trusted platforms to manage Identity and best practices and patterns for leveraging Vault for secrets management

## Program Closing

Asynchronous content sent to your inbox that includes some useful resources to validate production readiness and ensure operational best practices for your HCP Vault clusters



# Action Items

- Share to [customer.success@hashicorp.com](mailto:customer.success@hashicorp.com)
  - Authorized technical contacts for support
  - Stakeholders contact information (name and email addresses)
- Provision and configure an HCP Vault cluster
- Plan and begin deployment of your telemetry and monitoring solution



# Q&A





# Thank you

[customer.success@hashicorp.com](mailto:customer.success@hashicorp.com)

[www.hashicorp.com/customer-success](http://www.hashicorp.com/customer-success)