HashiCorp Vault

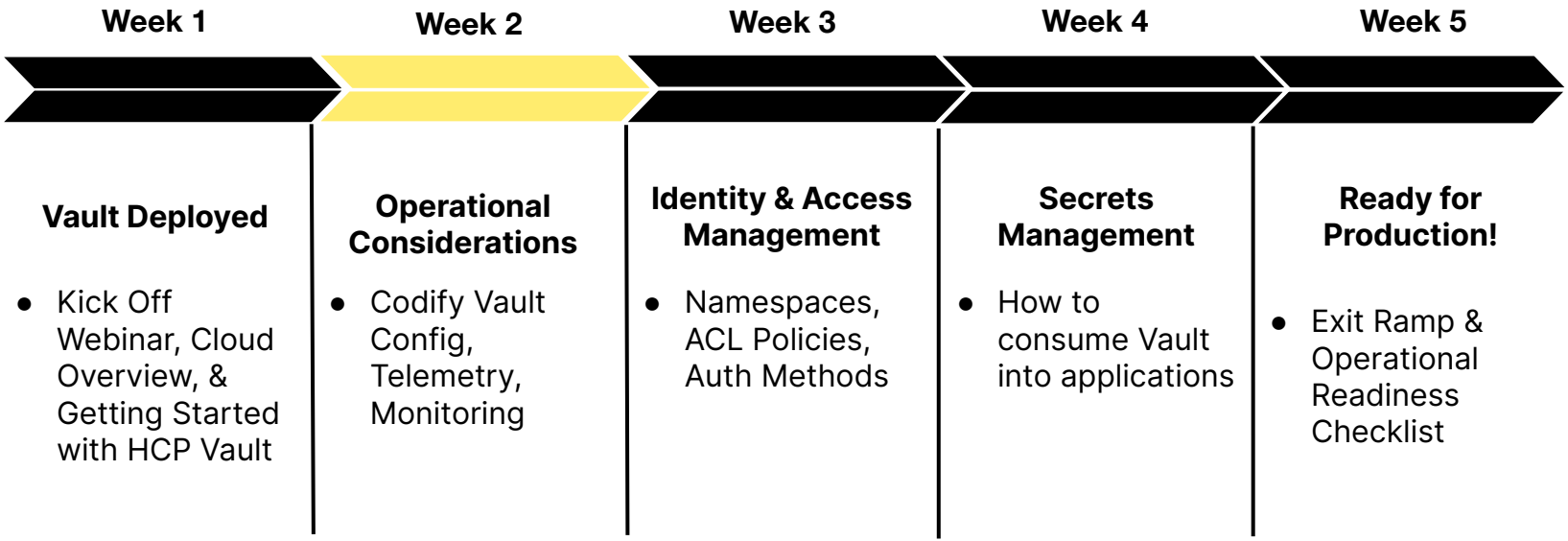
HCP Vault: Operationalizing for Production

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



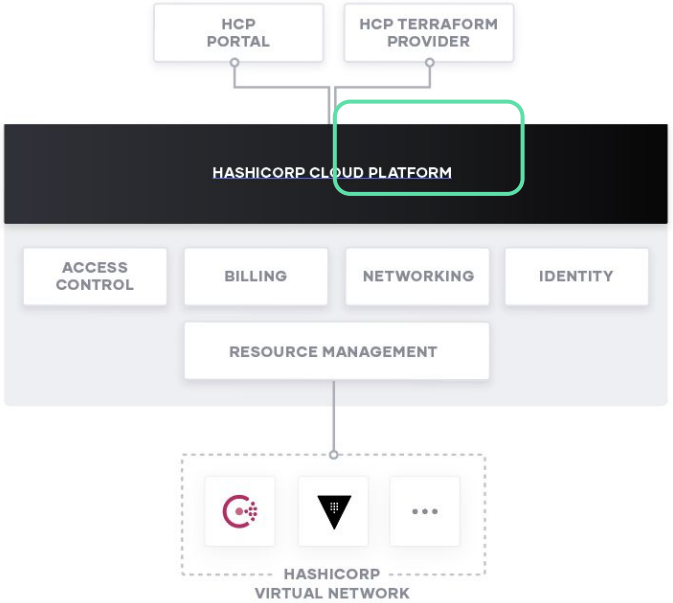
01

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

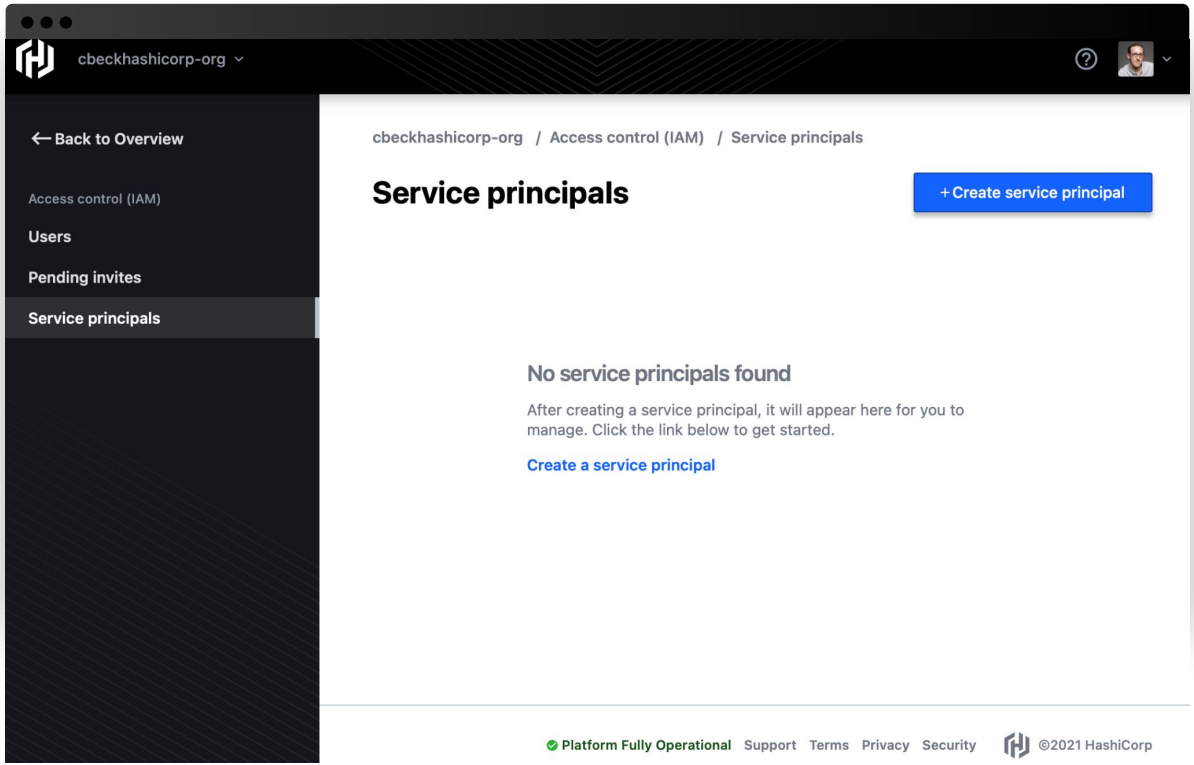
HashiCorp Cloud Platform allows you to grant access to both user and machines

- 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

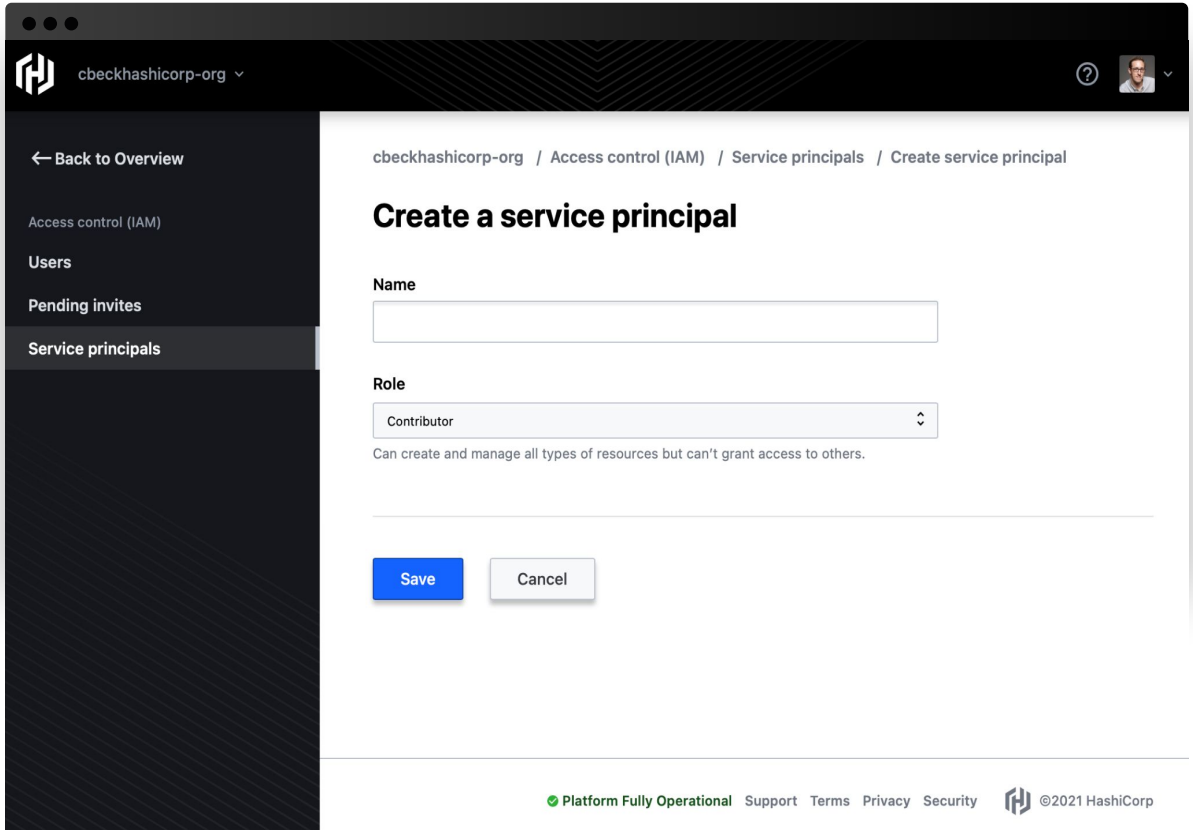
RBAC

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.

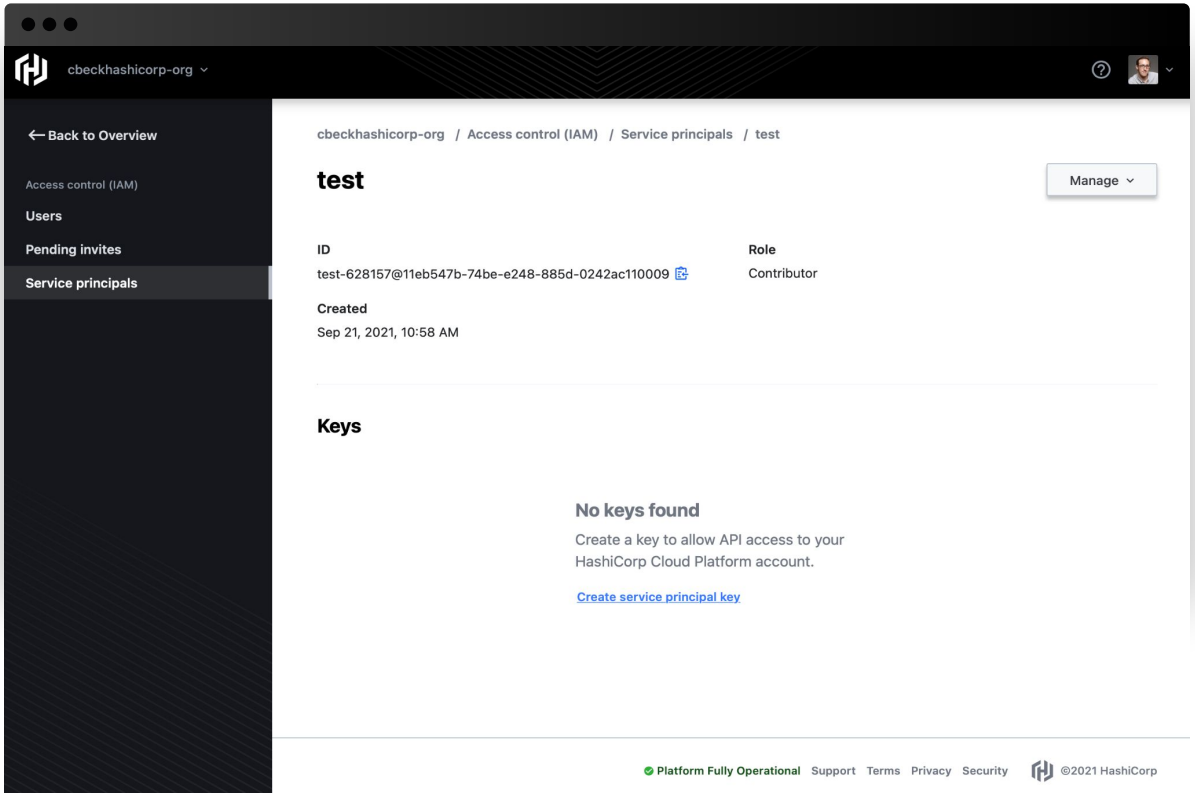
Creating Service Principals



Creating Service Principals

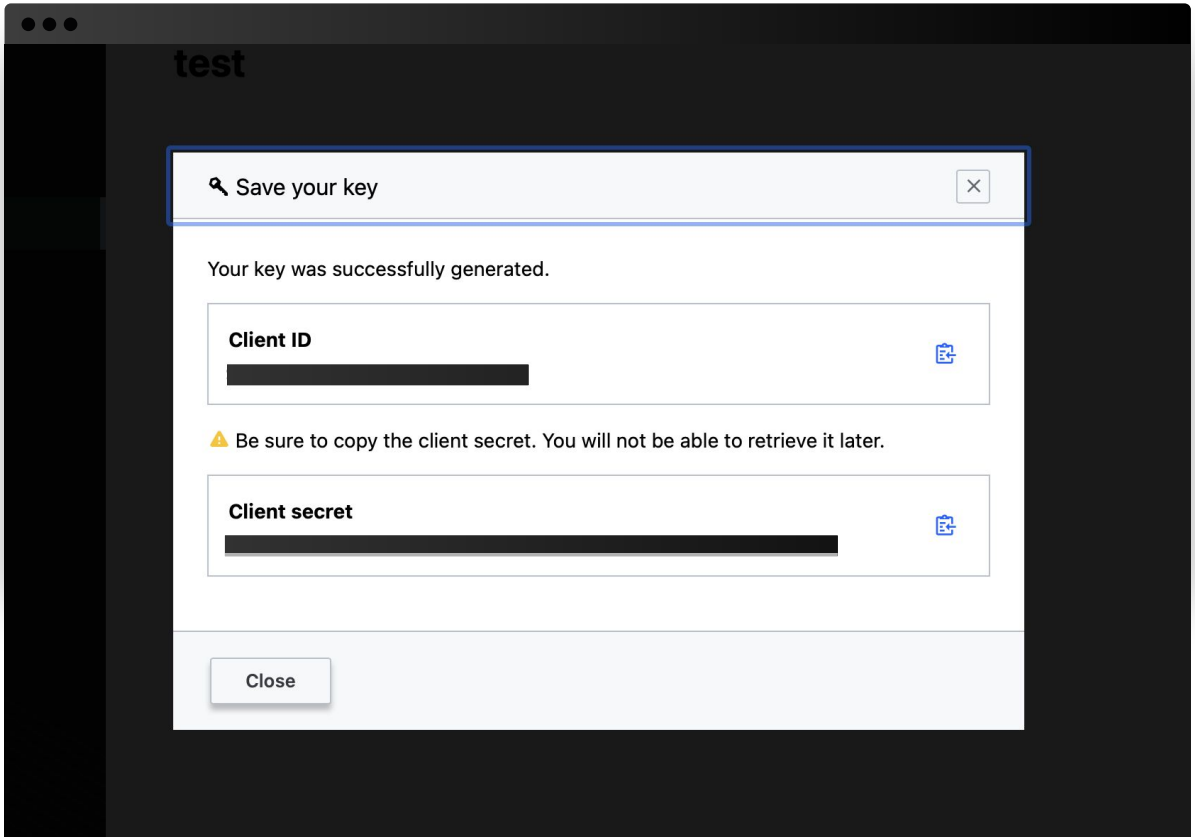


Creating Service Principal Key



Service Principal Key Secret

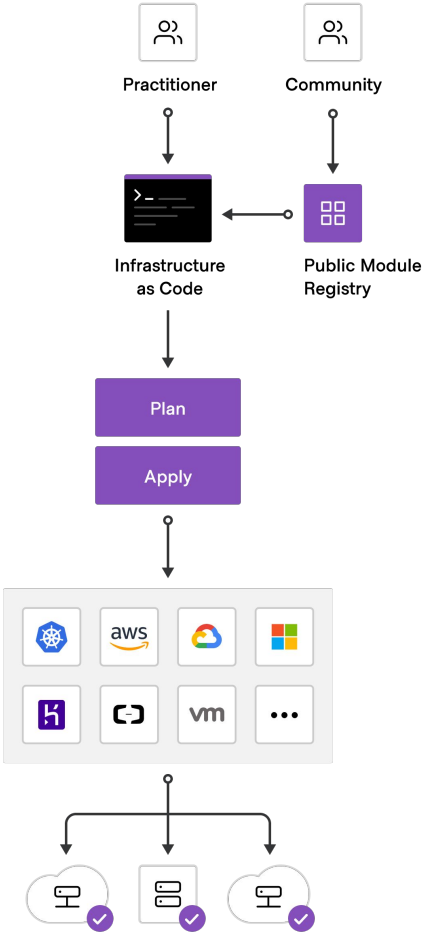
Client secret cannot be retrieved later



Terraform Overview

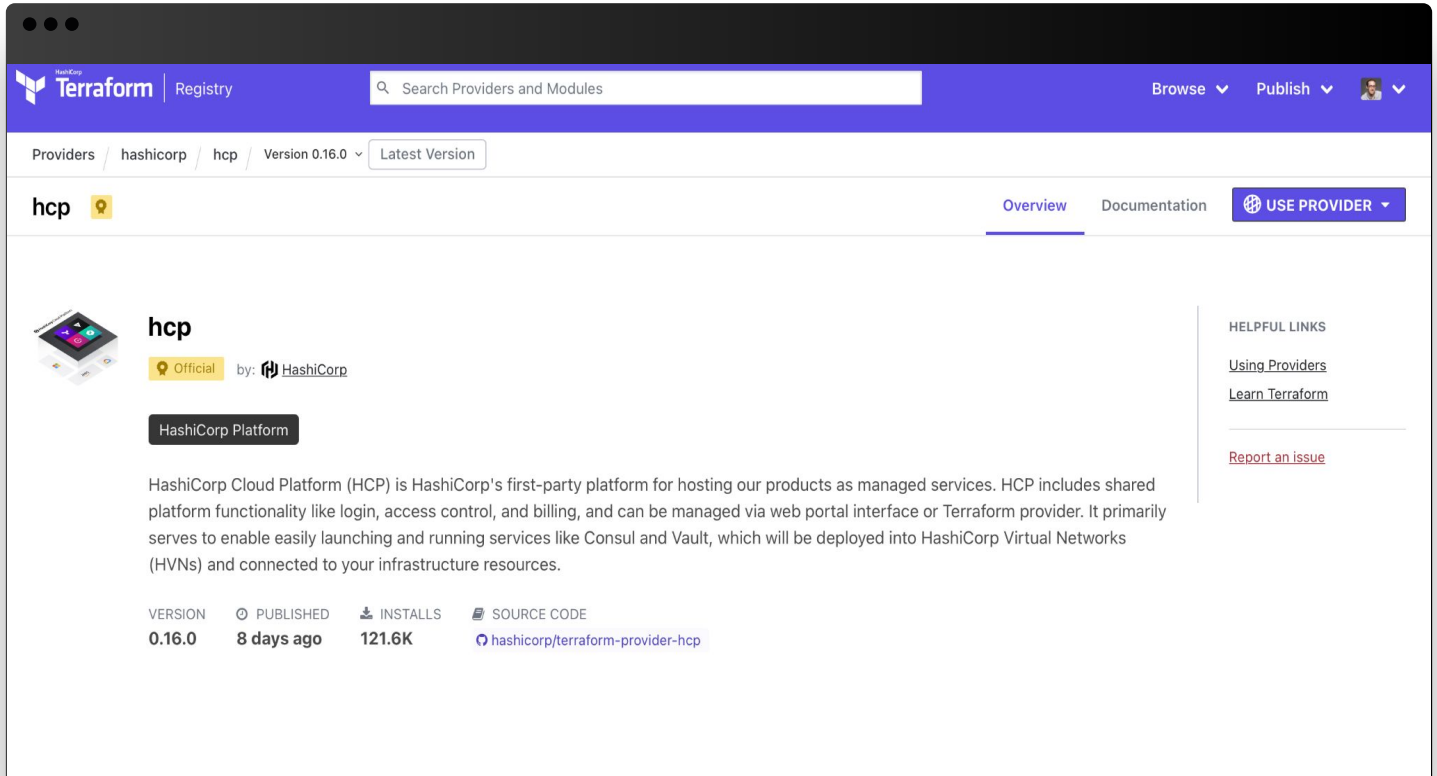
Cloud Infrastructure Automation

- 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



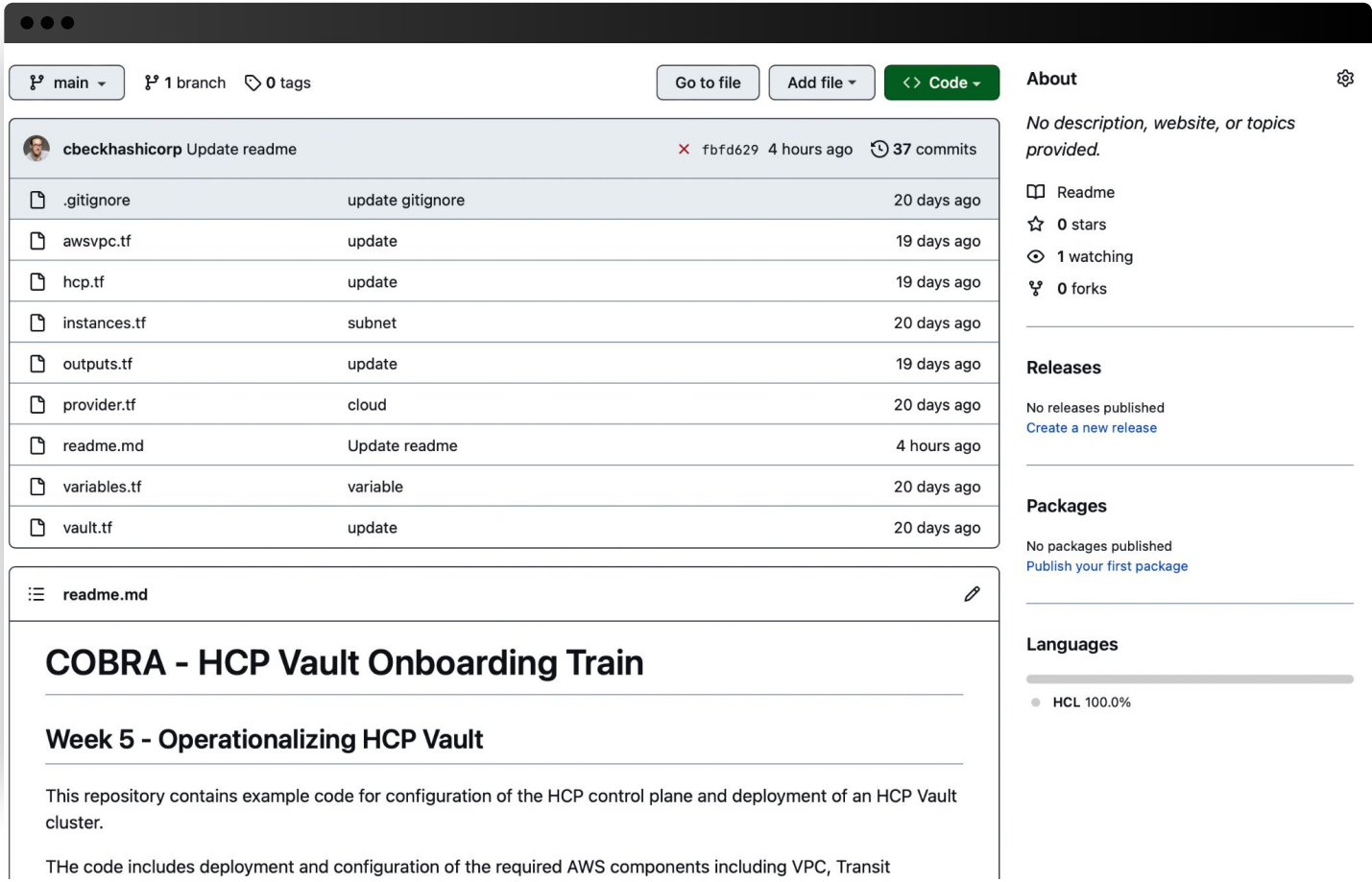
HCP Provider

Provision and manage control plane resources in HC



Module

[Code on GitHub]

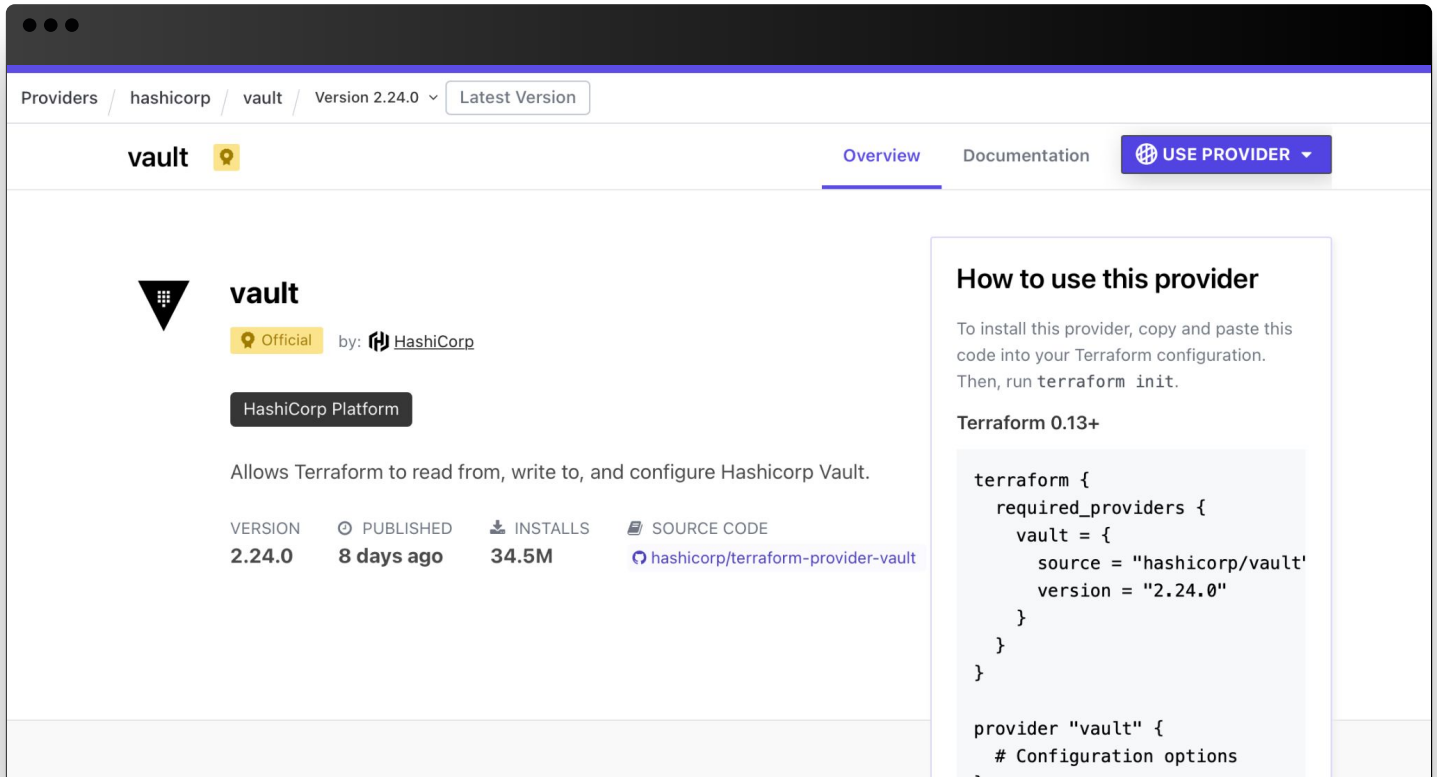


02

Automate Vault Configuration

Vault Provider

Provision namespaces, policies, secrets engines, & auth methods



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

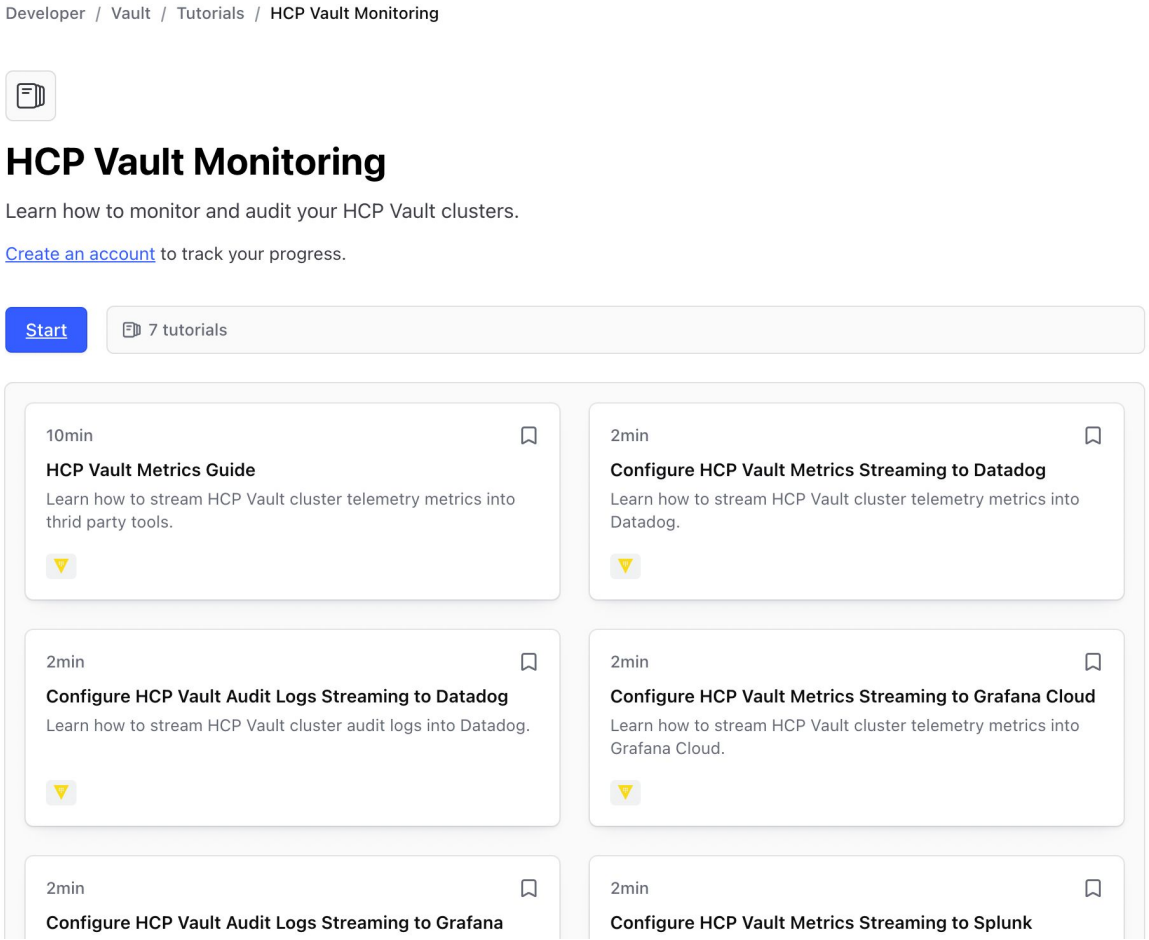
- HCP Vault includes auditing capabilities for all production tier clusters
- Logs are written locally and stored in an encrypted S3 bucket
- Audit log retention period varies based on the cluster tier as each tier has different storage capabilities

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

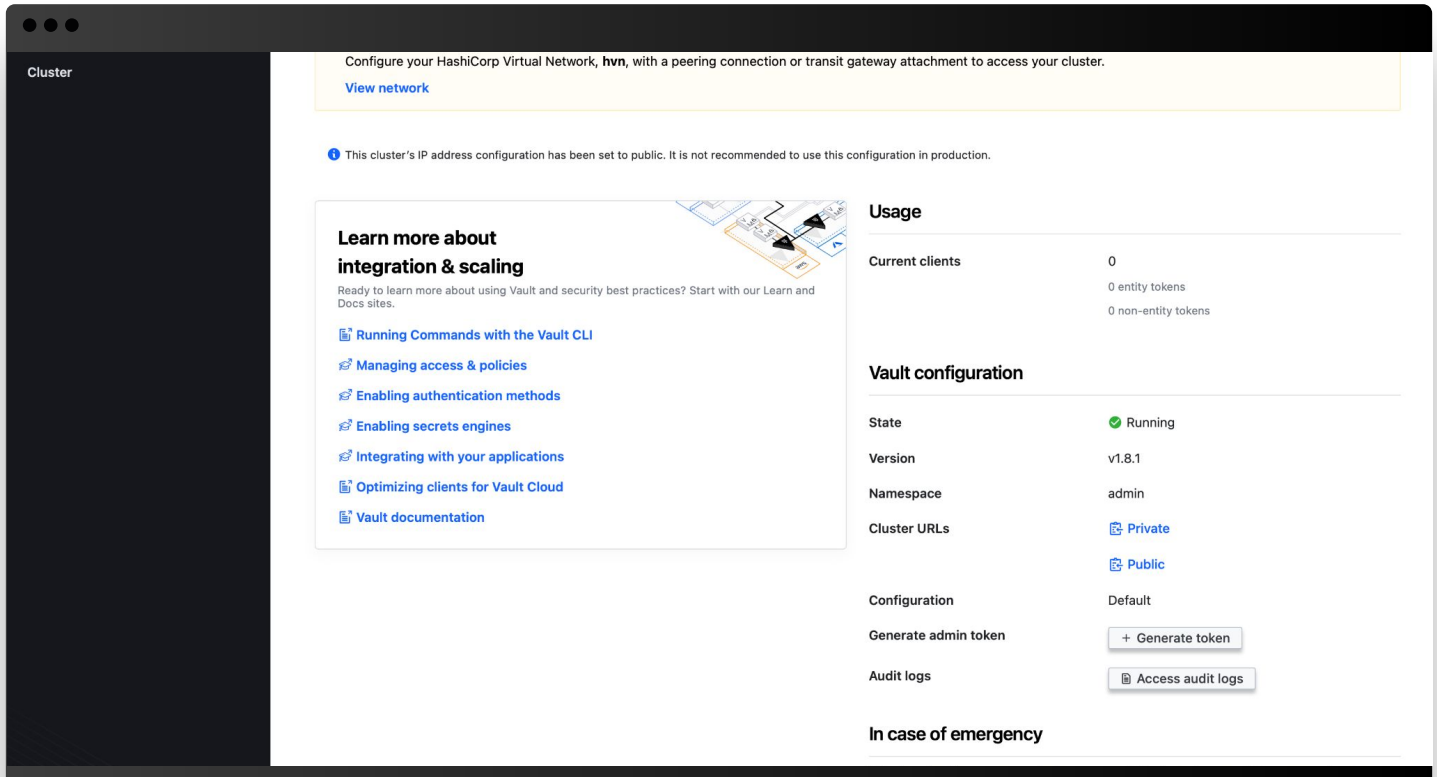
Setup Guides

developer.hashicorp.com



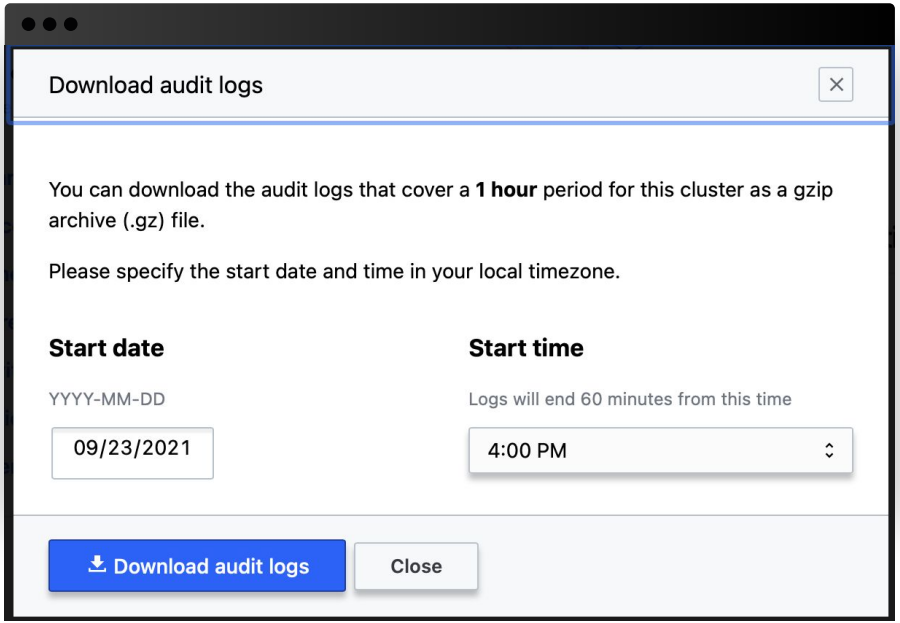
Audit Log Access

Audit Logs appear under Vault configuration on the cluster page



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

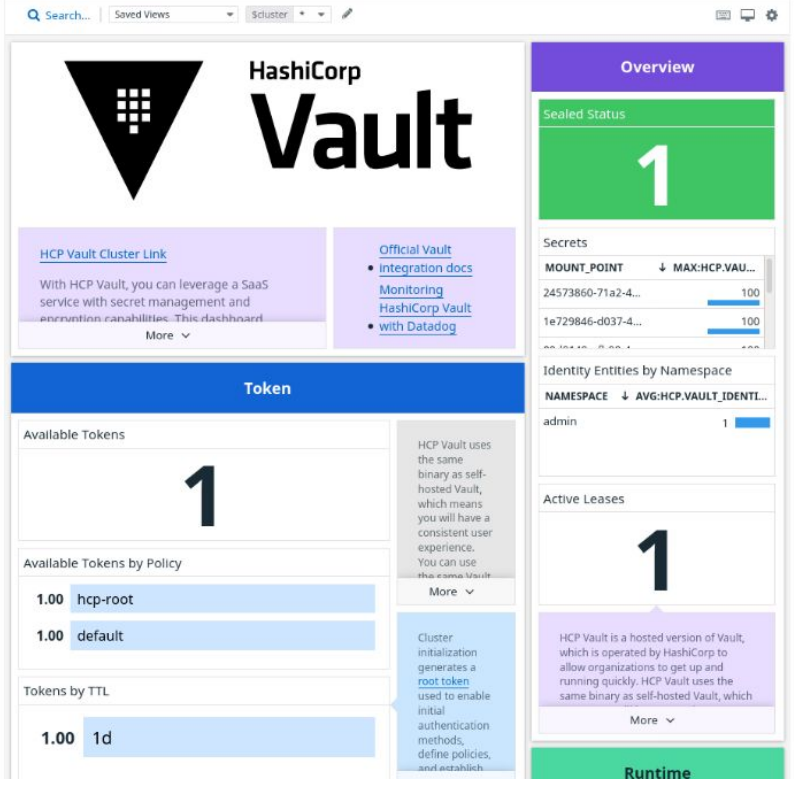
Telemetry

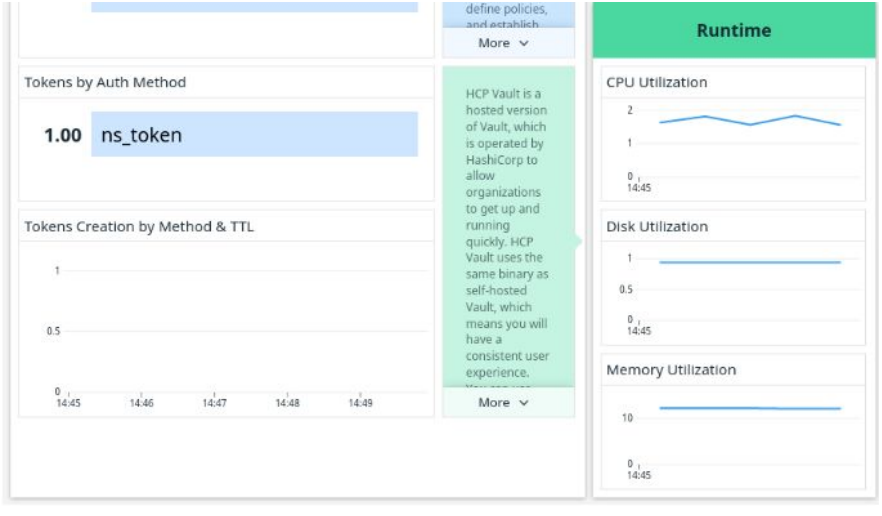
Vault Telemetry

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

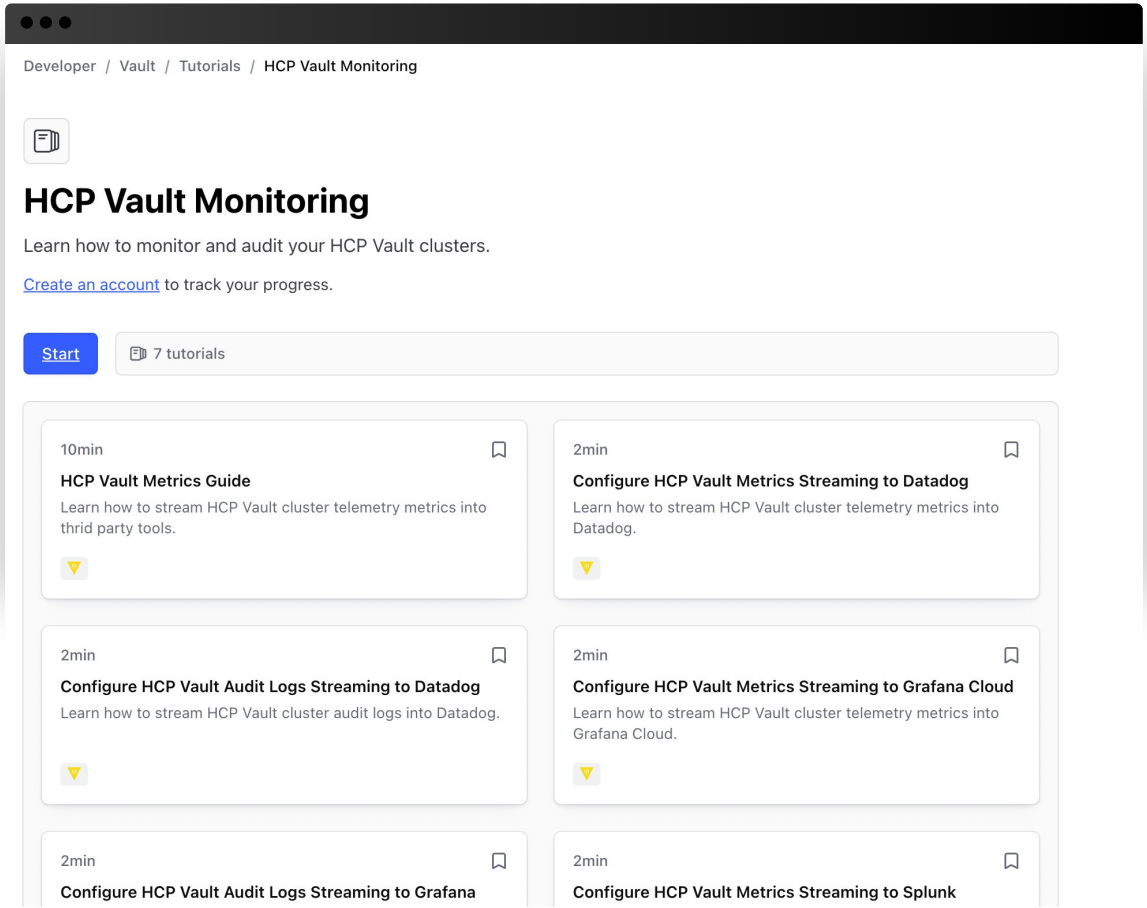
- Know the expected workload
- Vault System Resources (CPU, MEM, Disk)
- Complexity of Vault Policies
- Audit Logging
- Network for all the things

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

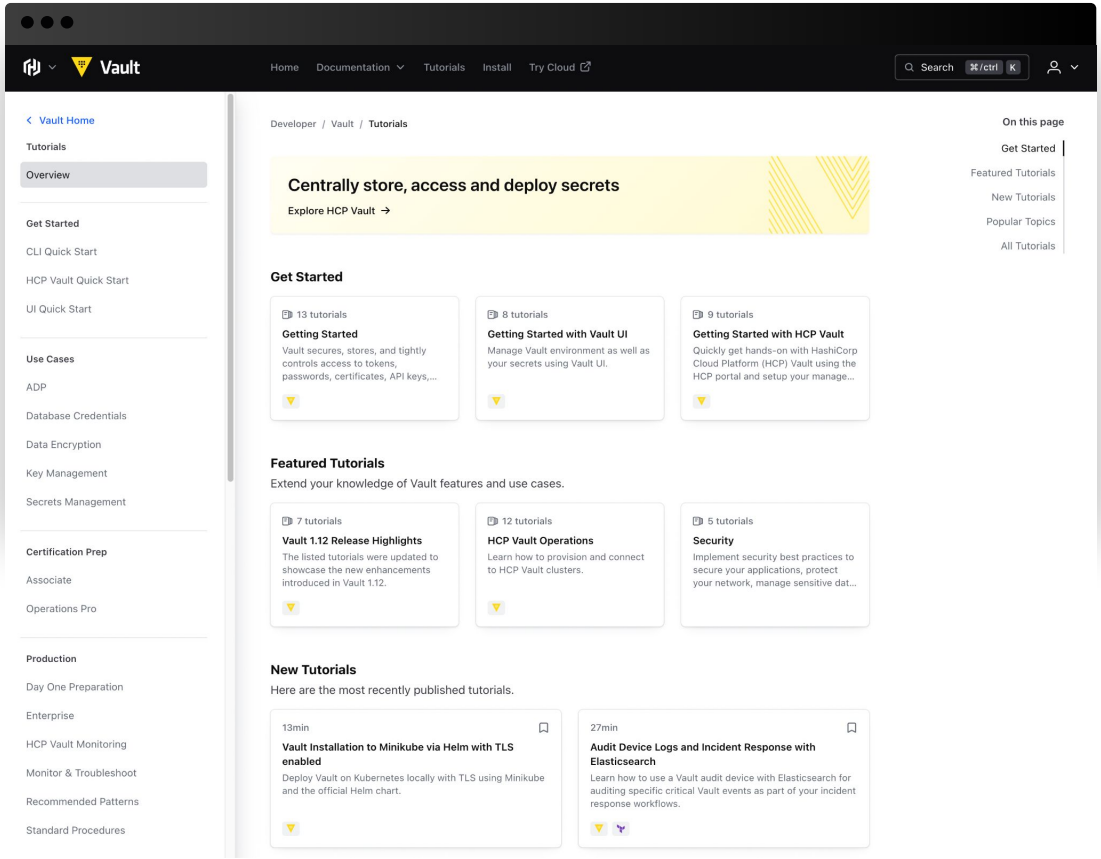
developer.hashicorp.com



Next Steps

Tutorials

Step-by-step guides to accelerate deployment of Vault



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

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

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
  - 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

www.hashicorp.com/customer-success