



HCP Vault Getting Started

5/18/2022

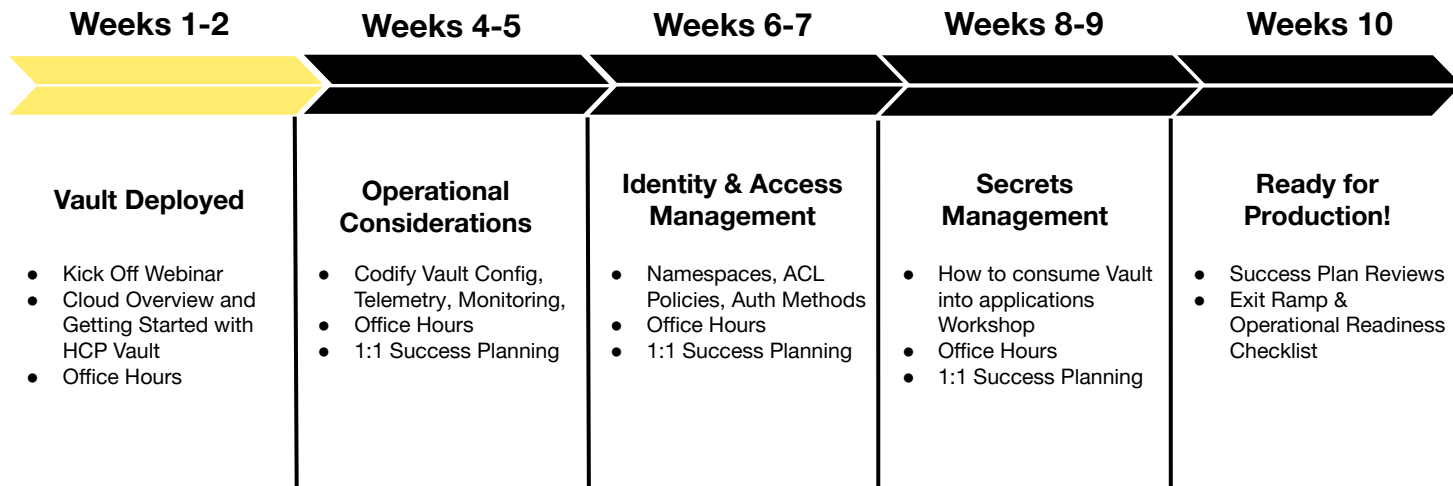
Copyright © 2021 HashiCorp



Agenda

- HashiCorp Cloud Platform Overview
- HCP Vault Overview
- Next Steps
- Q & A

HCP Vault Path to Production



The image features a dark background with decorative elements. In the top-left corner, there are several parallel, slanted lines in a light yellowish-green color, some of which are dotted. In the bottom-right corner, there is a rectangular area filled with a dense grid of small, light-colored dots.

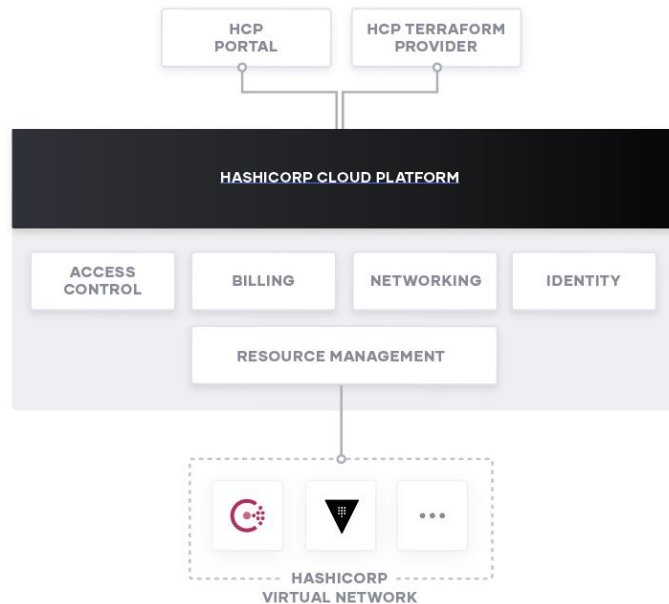
HashiCorp Cloud Platform Overview

HCP Architecture

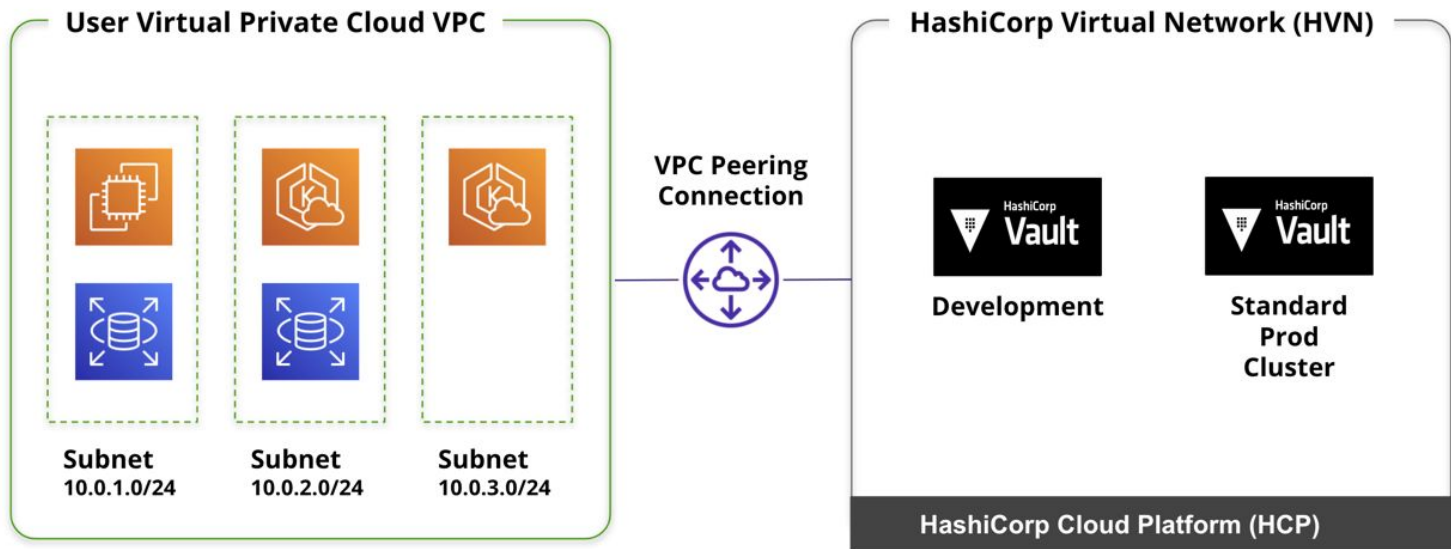


HCP consists of two main components, the control plane and data plane. The control plane is where you will manage your HCP Vault deployment.

The data plane contains all of your resources managed by HCP. Your HCP Vault clusters will be isolated into their own VPC managed in a HashiCorp Virtual Network.



HashiCorp Virtual Network (HVN)





Regions

Supported AWS Regions

Name	Identifier
US - Oregon	us-west-2
US - Virginia	us-east-1
Europe - Ireland	eu-west-1
Europe - London	eu-west-2
Europe - Frankfurt	eu-central-1
APAC - Singapore	ap-southeast-1
APAC - Sydney	ap-southeast-2

Access Controls HCP Platform



RBAC

The HCP console supports the capability to control permissions via RBAC roles.

MFA

When using the email based authentication, you can integrate with an MFA provider. This will increase the security of your HCP account and your companies data.

Add Users

Email based authentication allows you to invite additional users to join your organization. SSO integration is also available.

HCP RBAC Permissions



	Viewer	Contributor	Admin
Add and delete users			X
Manage user permissions			X
View users	X	X	X
Manage service principles			X
View current billing status	X	X	X
Create, edit, and delete HCP resources		X	X
View HCP resources	X	X	X



Single Sign-On

HCP supports federating identity from your trusted identity provider as an alternative to Github or email-based options. Currently, HCP supports Okta as an external IDP.

- Learn more about SSO at <https://cloud.hashicorp.com/docs/hcp/sso>



Automate HCP using Terraform

Automate through codification. The HCP provider for Terraform can manage the full lifecycle of your HCP resources. By managing your HCP infrastructure as code you will be able to build repeatable configurations that could be included as part of your build pipelines.



SLA

HashiCorp will use commercially reasonable efforts to maximize the availability of HashiCorp Cloud services, and provides uptime guarantees as detailed below. This Service Level Agreement (“SLA”) applies only to HashiCorp Cloud services at the Enterprise tier or above and does not apply to any other product offered by HashiCorp (Excludes development tier clusters).

If we do not achieve and maintain the Quarterly Uptime Percentages set forth in the table below, then you may be eligible for the following Service Credit(s).

Quarterly Uptime Percentage	Service Credit
< 99.9% but >= 99.5%	10%
< 99.5% but >= 99%	20%
< 99%	30%



Monitor HCP Status

status.hashicorp.com

<

>


Subscribe to HashiCorp Status updates via [Atom](#) or [RSS Feed](#) or contact [Support](#).

Subscribe via


Services

Incident History


Services

 HCP Portal

Operational

 HCP API

Operational

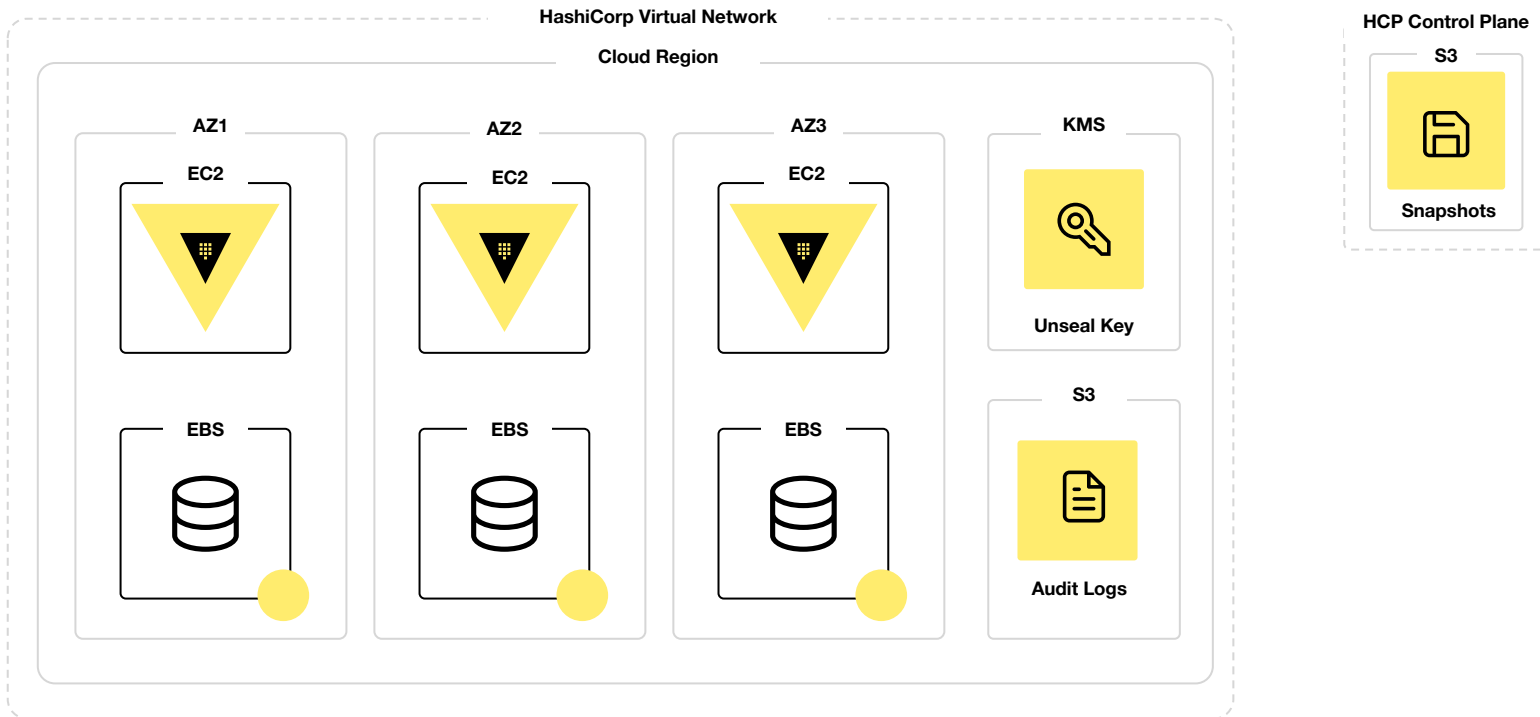
 HCP Packer

Operational

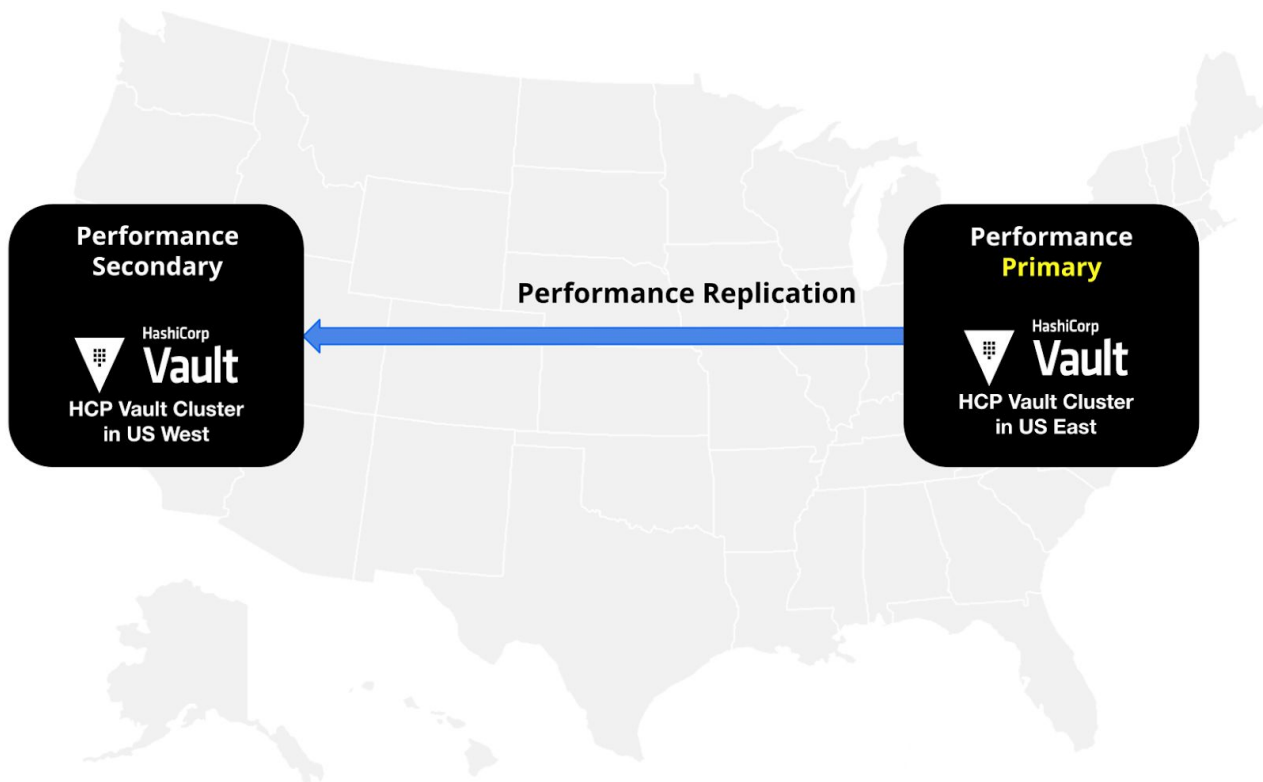
The image features a dark background with decorative elements. In the top-left corner, there are several parallel, slanted lines and a dotted pattern. In the bottom-right corner, there is a large, rectangular dotted pattern.

Getting Started with HCP Vault

HCP Vault Architecture



HCP Vault Plus Architecture



HCP Vault vs Self-managed



	Self-managed	HCP Vault
Infrastructure provisioning	Customer managed	HashiCorp managed
Infrastructure operations	Customer managed	HashiCorp managed
Vault updates	Customer managed	HashiCorp managed
Seal	Customer managed	HashiCorp managed
Auth Methods and Secrets Engines	All	Subset currently validated
Vault configuration	Customer managed	Customer managed

HCP Vault Tiers



Development

Designed to get started quickly for small projects, proof-of-concepts, non-production workloads.

1 Node Cluster

Extra Small

Starter

Designed as affordable, production-ready clusters with clients included to get started quickly.

Small

Standard

Clusters designed to scale with the demand of running production workloads.

3 Node Cluster Tiers

Small
Medium
Large

Plus

Designed for high availability replication of secrets and policies across multiple data centers.

Small
Medium
Large

HCP Vault Tiers



		Max Clients	vCPU	Memory	Storage	High Availability	Rate Limit	Performance Replication	
Pre-Production Tiers	Development	25	2	1 GiB	Snapshots & audit logs not supported	1 node cluster	60 requests/sec	No	
Production Tiers	Starter		2	8 GiB	5 GB storage, 250 GB for snapshots & audit logs	3 node cluster	200 requests/sec	No	
	Standard / Plus Small	2	8 GiB	15 GB storage, 1 TB for snapshots & audit logs	400 requests/sec		Plus Only		
	Standard / Plus Medium	No Limit	4	16 GiB	30 GB storage, 5 TB for snapshots & audit logs			No Limit	
	Standard / Plus Large	8	32 GiB	50 GB storage, 10 TB for snapshots & audit logs					

HCP Vault Security



Cluster Hardening

HCP Vault clusters adhere to our production hardening guidelines. This ensures that each cluster has E2E TLS, firewall restrictions to only inbound TCP/8200, restricted storage access, and no clear text credentials. Refer to our [production hardening guide](#) for all hardening practices.

Root Tokens

During creation of an HCP Vault cluster, a root token is generated during the initialization process. This token is used to create the

- initial authentication methods
- define policies
- establish trust with the HCP control plane.

This token is revoked once setup is completed.

Vault Data

Vault's data is encrypted and stored in an account-specific Amazon Elastic Block Store (EBS) in the same region as the cluster.

Snapshots are stored in HashiCorp managed, encrypted Amazon S3 buckets in the US. When downloading, audit logs are sent to US to be concatenated for download.

Admin Token



Admin tokens are similar to root tokens and should only be used during initial setup of an HCP Vault cluster or in the event that you do not have access to the cluster. This token is highly privileged and can access all endpoints within your cluster. Once a token is generated it is only valid for 6 hours.


Quick actions

Cluster URLs

Private

Copy the address into your CLI or browser to access the cluster.

Admin token



+ Generate token

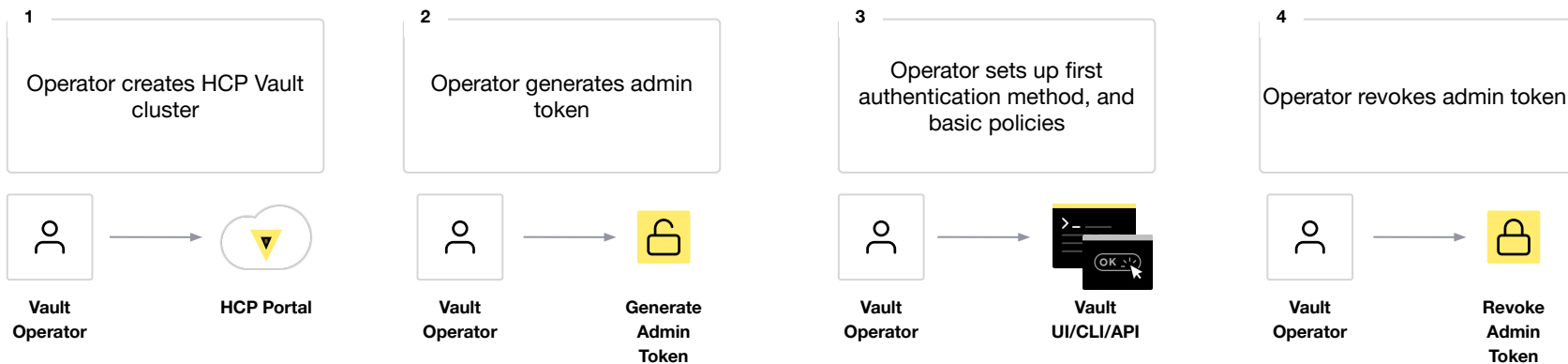
Admin token is used to sign into the cluster with unlimited privileges.

In case of emergency

Seal this cluster

Vault data can be locked if an intrusion is detected.

Initialization Process



Authentication Methods



Supported Authentication Methods

To date, HCP Vault has been validated to work with the listed authentication methods.

Additional authentication methods beyond the ones listed can be enabled, however operators may encounter limitations with configuration or functionality.

Bold: Verified and supported

Italicized: Unverified auth method

Human	Machine
Azure AD	AWS EC2
Okta	AppRole
GCP (without G Suite option)	Kubernetes
<i>Github</i>	<i>JWT</i>
<i>OIDC</i>	<i>AWS IAM</i>
<i>LDAP</i>	
<i>User/Pass</i>	

Secrets Engines



Supported Secrets Engines

To date, HCP Vault has been validated to work with the listed secrets engines.

Additional secrets engines beyond the ones listed can be enabled, however operators may encounter limitations with configuration or functionality.

Secrets Engines

Key/Value (V1 & V2)

AWS

Transit

RDS PostgreSQL

Mongo Atlas

Snowflake DB



Constraints

Root Namespace

No access is granted to the root namespace. When you access an HCP Vault cluster you will be within the admin namespace.

Admin Token Policy

The admin policy used for admin tokens generated in the HCP portal is located in the admin namespace. It is viewable and editable by customers however it should not be edited.



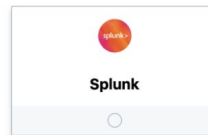
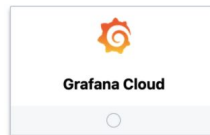
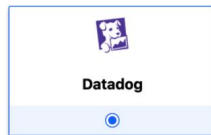
Cluster Deletion

Deletion of an HCP Vault cluster is a permanent, irreversible action

Currently, when deleting an HCP Vault cluster all data stored in the data plane is removed. This includes all snapshots and audit logs.

Audit logs can be exported in one hour increments from the HCP Portal. We recommend streaming audit logs to Datadog, Grafana, or Splunk for audit log retention.

Choose a provider



Performance Considerations



Profile Workloads

As you scale the adoption of Vault throughout your organization, you will have varying workloads access Vault. Telemetry monitoring should be leveraged to ensure proactive monitoring of Vault Cluster resources. Additionally, as you onboard new applications/services/teams/users to Vault, take time to profile the usage patterns to ensure optimal authentication and consumption patterns are used.

External Systems

Depending on the Authentication Methods and Secrets Engines used by your organization, you will likely have dependency on other external systems for Vault requests to be completed. Ensure telemetry is enabled on those services and proactively monitor for performance issues.

Next Steps

Next Steps



- Upcoming Schedule:

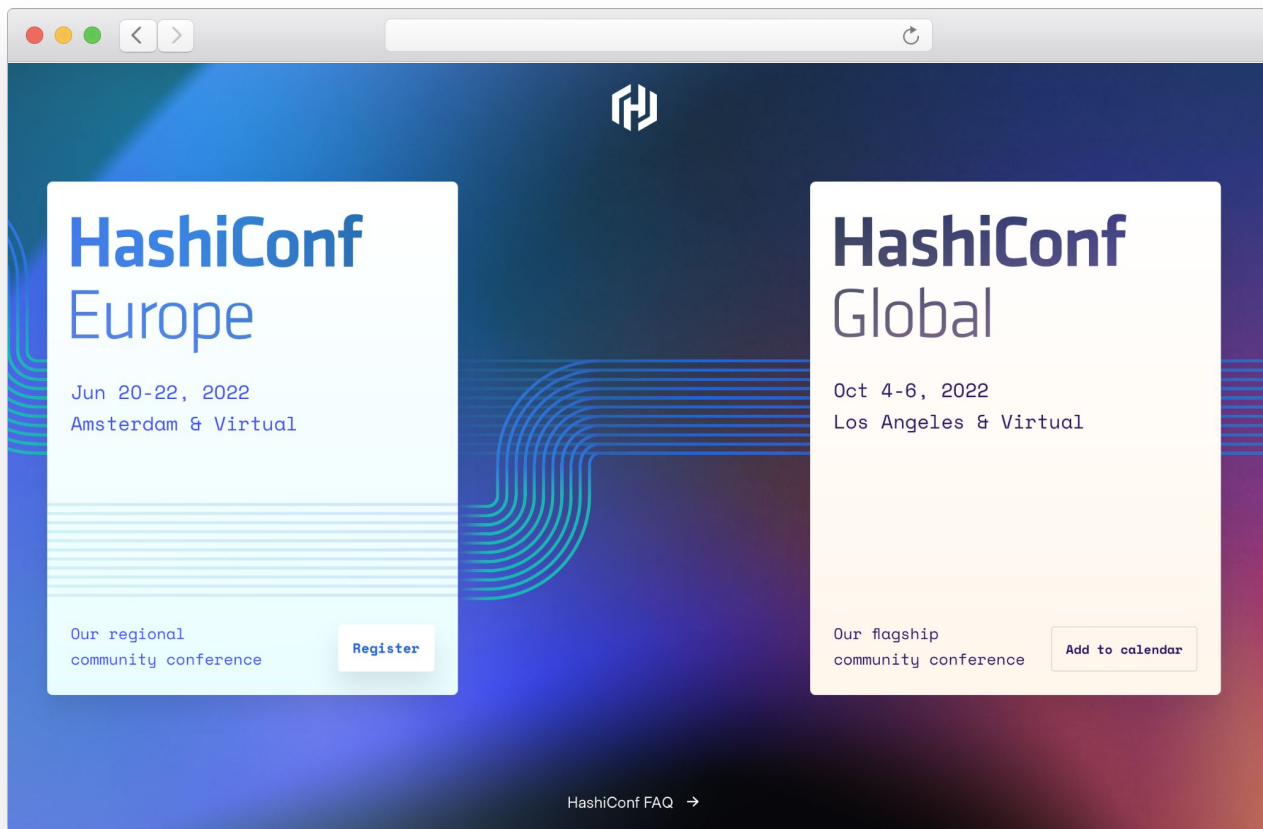
- ▼ Week 3 - HCP Vault - Operationalize your HCP Vault Clusters

- ▼ Week 4 - HCP Vault - Identity and Access Management Strategy



HashiConf

<https://hashiconf.com>



<


>

HashiCorp | Discuss

Sign in





Q

≡



Information on HashiCorp Cloud Platform (HCP) use cases, Q&A, and best practices discussions. Please note that offerings may be in various release lifecycles. Categorize your question or comment under [HCP Consul](#) or [HCP Vault](#) subcategories. If your question or comment relates to networking, access control, or billing, post in this category. For support requests, please [open a ticket](#).

HashiCorp Cloud Platform (HCP) ▾ All ▾ Tags ▾ | Latest Top

Topic	Replies	Views	Activity
About the HashiCorp Cloud Platform (HCP) category			
<div>HashiCorp Cloud Platform (HCP)</div> <div>Information on HashiCorp Cloud Platform (HCP) use cases, Q&A, and best practices discussions. Please note that offerings may be in various release lifecycles. Categorize your question or comment under HCP Consul or HCP V... read more</div>	 1	387	May 24
<div>HCP Vault “per-client” pricing</div> <div>HCP Vault</div>	 0	39	9d
<div>Failing to use HCP Consul as my terraform backend</div> <div>HashiCorp Cloud Platform (HCP)</div>	 1	72	12d
<div>Does HCP support Automation APIs in AWS</div> <div>HashiCorp Cloud Platform (HCP) vault</div>	 0	73	27d



Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers.

discuss.hashicorp.com

Learn

Step-by-step guides to implement features in HCP and HCP Vault



HashiCorp Learn [Browse tutorials](#)

Search

[Sign in](#)

HCP Vault Week 1

- Week 1 - Welcome to HCP Vault
- HCP Vault Introduction
- Create a Vault Cluster on HCP
- Multi-tenancy with Namespaces
- Your First Secret
- Create Vault Policies
- Manage Authentication Methods
- Vault Operation Tasks
- Week 1 Wrap-up

HCP Vault Onboarding Week 1

🕒 1 HR 9 MIN 📄 9 TUTORIALS

Get off to a strong start with HCP Vault in week 1 of your onboarding journey.

15 MIN

Week 1 - Welcome to HCP Vault

• Welcome to week 1 with HashiCorp Cloud Platform (HCP) Vault. Watch a quickstart demo and learn more about the internals of Vault.

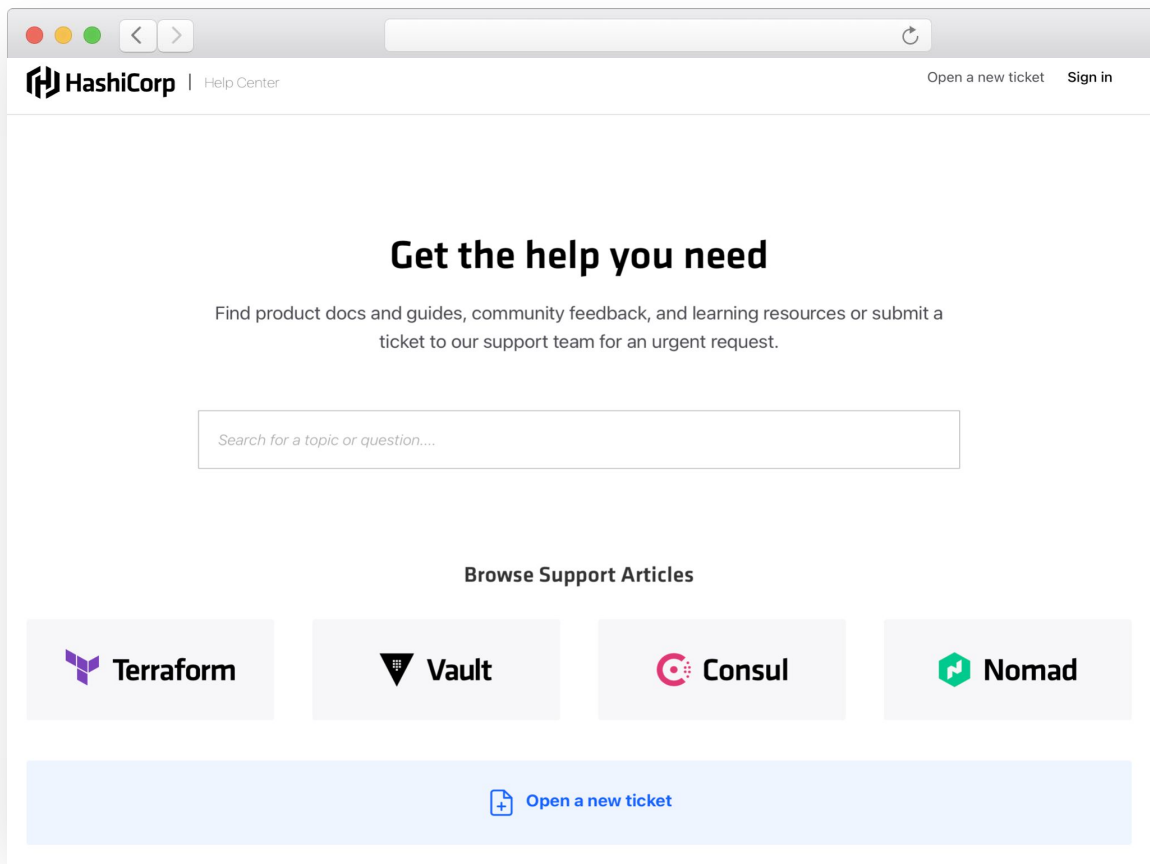
▼ ▶

5 MIN

HCP Vault Introduction

• HashiCorp Cloud Platform (HCP) Vault enables you to deploy a managed Vault service on AWS.

▼ ▶



Support

<https://support.hashicorp.com>

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

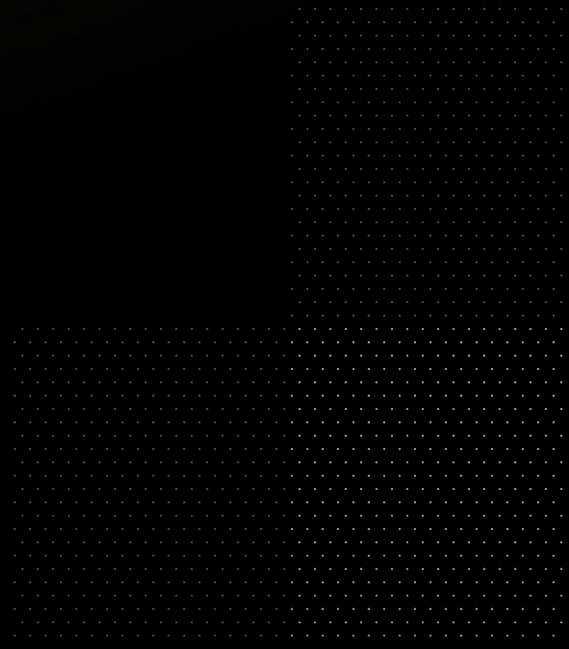
Technical Support

Something not working quite right?

Engage with HashiCorp Technical Support by opening a new ticket for your issue at [Hashicorp Support](#).



Q & A





Thank You

customer.success@hashicorp.com

www.hashicorp.com