

HCP Vault Onboarding Program Kickoff



Agenda

-
- Customer Success Overview 01
 - HCP Vault Onboarding Program 02
 - Customer Support 03
 - HashiCorp Cloud Platform Overview 04
 - HCP Vault Overview 05
 - Demo 06
-



Code of Conduct

HashiCorp is dedicated to providing a harassment-free experience for everyone, regardless of gender, gender identity, sexual orientation, disability, physical appearance, body size, race, national origin, or religion. We value your attendance and do not wish anyone to feel uncomfortable or threatened at any time.

The bottom line is that we do not tolerate harassment of conference participants in any form. Harassment includes but is not limited to offensive verbal comments related to gender, gender identity, sexual orientation, disability, physical appearance, body size, race, national origin, religion; sexual or inappropriate images in public spaces; deliberate intimidation; stalking; trolling; sustained disruption of talks or other events; and unwelcome sexual attention. Participants asked to stop any harassing behavior are expected to comply immediately. If you are being harassed, notice that someone else is being harassed, or have any other concerns, please let the HashiCorp event representative know immediately or email customer.success@hashicorp.com.





Noelle Dunn

Customer Success Manager
she/her



Justin Herreman

Solutions Architect Specialist
he/him



01



Customer Success Overview

Partnering Together

HashiCorp Customers

FINANCIAL SERVICES	ENTERTAINMENT & TELCO	MANUFACTURING & LOGISTICS	SOFTWARE & TECHNOLOGY	INSURANCE & HEALTH	
 Santander  KeyBank   SoftBank  RBC  wepay a CHASE company  Blackstone  Lincoln Financial Group®	 BNP PARIBAS  CREDICORP   ABN AMRO  Nationwide Building Society  STANDARD & POOR'S  ADB	 COMCAST  vodafone  NBCUniversal  UBISOFT  sky  RED VENTURES  DAZN  VINGROUP  ROBLOX	 gm  Lufthansa  BHP  OLD DOMINION FREIGHT LINE  AIRBUS  AirPlus INTERNATIONAL  WARE2GO  KPMG	 Booking.com  Grab  priceline.com®  cielo  shopify  SEAT GEEK  H&R BLOCK  ADT  Shipt  Q2	 PROGRESSIVE  co-operators  gsk  AXA  AstraZeneca  ellume Kansas City  athenahealth  GoodRx  surescripts



What You Can Expect from CS

Customer Success Manager (CSM)

Account & Success Management

- Providing a community-based onboarding program designed to get you up and running quickly
- Facilitating sessions to keep your team current with HashiCorp technology
- Joint discovery of objectives and success criteria
- Your customer advocate within HashiCorp

Solution Architecture Specialist (SA)

Technical Success & Advisory

- Technical resource for the onboarding process
- Providing product reference architecture information for better decision-making
- Thought leadership on best practices of product architecture and use-case patterns
- Timely education and enablement from a technical perspective



Other resources available to you

Our customer success pillars

So much goes into making you successful. Three core pillars are inform how we work to serve you.



Enablement

We educate, guide, and enable your teams to deploy and operate products according to proven best practices.



Adoption

We help you deliver against your top use cases, and ensure products are used properly to drive rapid ROI.



Value attainment

We connect product usage to business need and value-based outcomes to ensure you achieve measurable value.

Further information located at <http://hashicorp.com/customer-success>

02



HCP Vault Onboarding Program

How we engage

Customer Responsibilities

These are critical for your onboarding success

Training Consumption

Ensure team members attend workshops, training, office hours

Single Point of Contact

Main contact for decision making

Use Case Guidance

Provide timely information on your intended use cases during our success planning

Escalation Process

Understanding of escalation process

Project Team Participation

Inclusive of any stakeholder required for successful completion of your onboarding

Surveys Responses

Provide timely responses to surveys

Onboarding Checklist



Vault Deployed

- Create HCP Organization, deploy HVN and create a HCP Vault cluster
- Automate HCP Control plane & Vault Management
- Telemetry and Monitoring in place
- Performance replication in place (Plus tier)



Vault Operational

- First use case (team/service/application) onboarded & consuming secrets stored in Vault
- A roadmap created for onboarding additional teams & use cases (dynamic, PKI, etc).

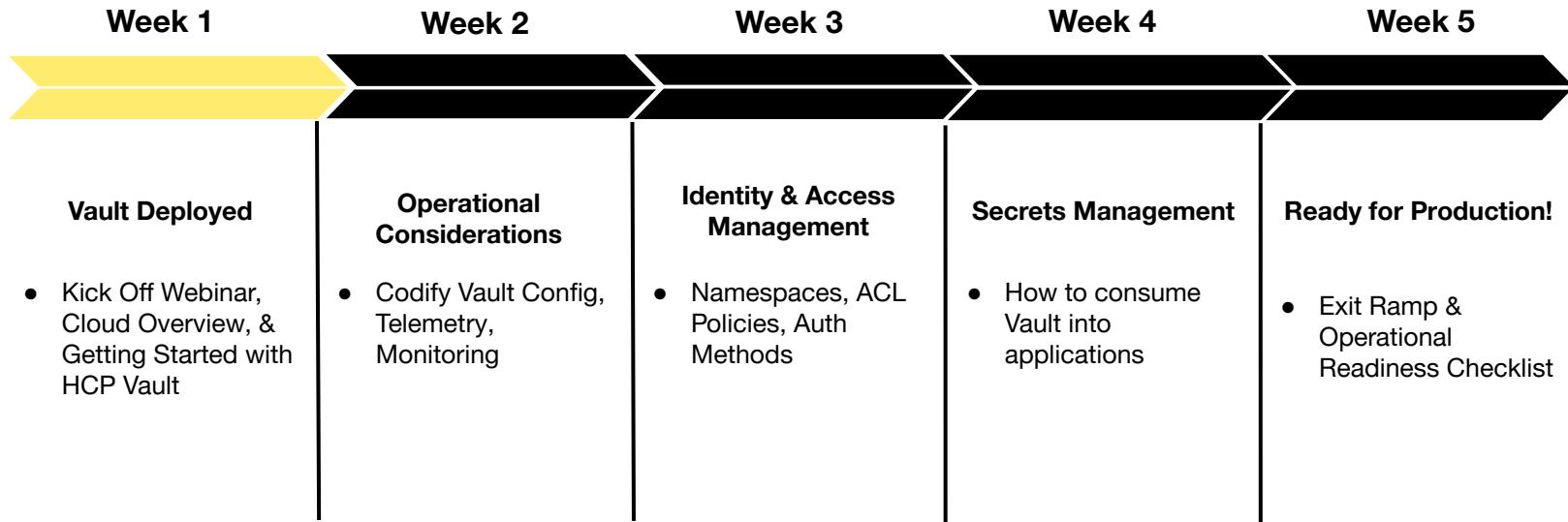


Completed within 60 days

HCP Vault Onboarding Program

A 5 week guided community environment

Assisting customers with onboarding and adoption



03



Customer Support

SLA, Contact Methods, Services, etc.

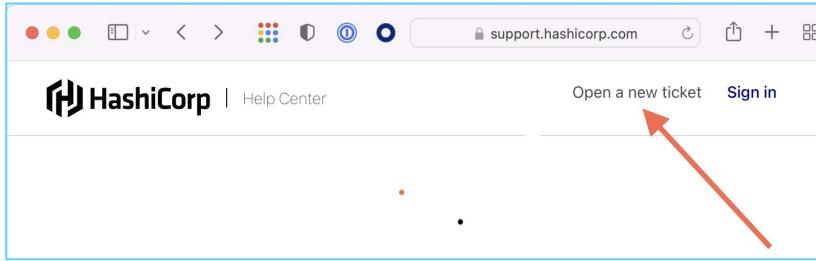
Contacting Support

There are two ways to contact our support team:

- **Support Portal:** Open a ticket through [our support portal](#)
 - Once customer access is setup, authorized users can submit a ticket using the email address they provided us
 - The portal provides faster routing via product and sub-product selection, the ability to send encrypted attachments, and set ticket priority
- **Email Support:** Send an email to support@hashicorp.com
 - All emailed support tickets default to “normal” priority - and cannot be changed
 - Don’t raise a SEV-1 over email, please use the support portal



Support Portal

A screenshot of the 'Submit a request' form on the HashiCorp Help Center. The form includes fields for 'Your email address*' (with 'person@company.com' entered), 'Product*' (with 'HashiCorp Cloud Platform' selected), and 'HCP Category*' (with 'HCP Vault' selected). There is also a 'Search' bar and a link to 'HashiCorp Help Center / Submit a request'.

Helpful Hints

- Our ticketing system uses the email domain to associate with a company
- Select Cloud Platform-HCP Vault
- Always include reproduction steps and log files!

Support Levels

GOLD

SILVER

BRONZE

		24 X 7 (SEV-1 URGENT)	9-5, Monday - Friday US LOCAL TIME EUROPEAN CENTRAL TIME AUSTRALIA EASTERN TIME	N/A
SEVERITY 1	FIRST RESPONSE	60 minutes	4 business hours	N/A
	UPDATE FREQUENCY	4 hours	8 business hours	N/A
SEVERITY 2	FIRST RESPONSE	4 business hours	8 business hours	N/A
	UPDATE FREQUENCY	8 business hours	2 business days	N/A
SEVERITY 3	FIRST RESPONSE	8 business hours	24 business hours	N/A
	UPDATE FREQUENCY	3 business days	5 business days	N/A
SEVERITY 4	FIRST RESPONSE	24 business hours	24 business hours	24 business hours
	UPDATE FREQUENCY	Reasonable best effort	Reasonable best effort	Reasonable best effort
Technical contacts allowed		4	3	2

This info can also be accessed from our [Support SLA Page](#)



Severity Definitions

Sev-1 (Urgent)	A Sev-1 incident is an operational outage as defined below: Any error reported by customer where majority of the users for a particular part of the software are affected, the error has high visibility, there is no workaround , and it affects the customer's ability to perform its business .
Sev-2 (High)	Any error reported by customer where the majority of the users for a particular part of the software are affected, the error has high visibility, a workaround is available ; however, performance may be degraded or functions limited and it is affecting revenue .
Sev-3 (Normal)	Any error reported by customer where the majority of the users for a particular part of the software are affected, the error has high visibility, a workaround is available; however, performance may be degraded or functions limited and it is NOT affecting revenue.
Sev-4 (Low)	Any error reported by customer where a single user is severely affected or completely inoperable or a small percentage of users are moderately affected or partially inoperable and the error has limited business impact.

For reference only - Subject to Change

Current information available on the [Support SLA Page](#)



Suggested Resources

We strongly urge operations team members to subscribe to the HCP status web page at the following URL:

<https://status.hashicorp.com/>

We also recommend and hope you will participate in the active Hashicorp community, you can find more information at the following URL:

<https://www.hashicorp.com/community>



04

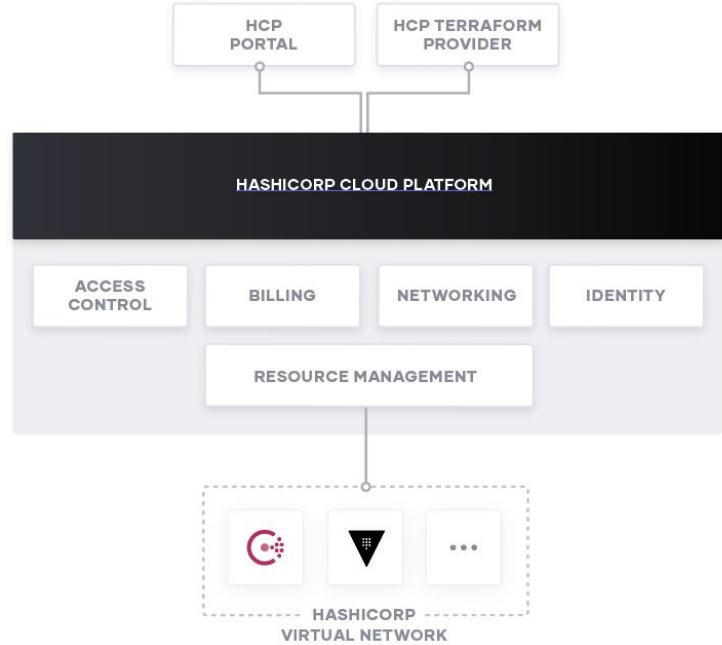


HashiCorp Cloud Platform Overview

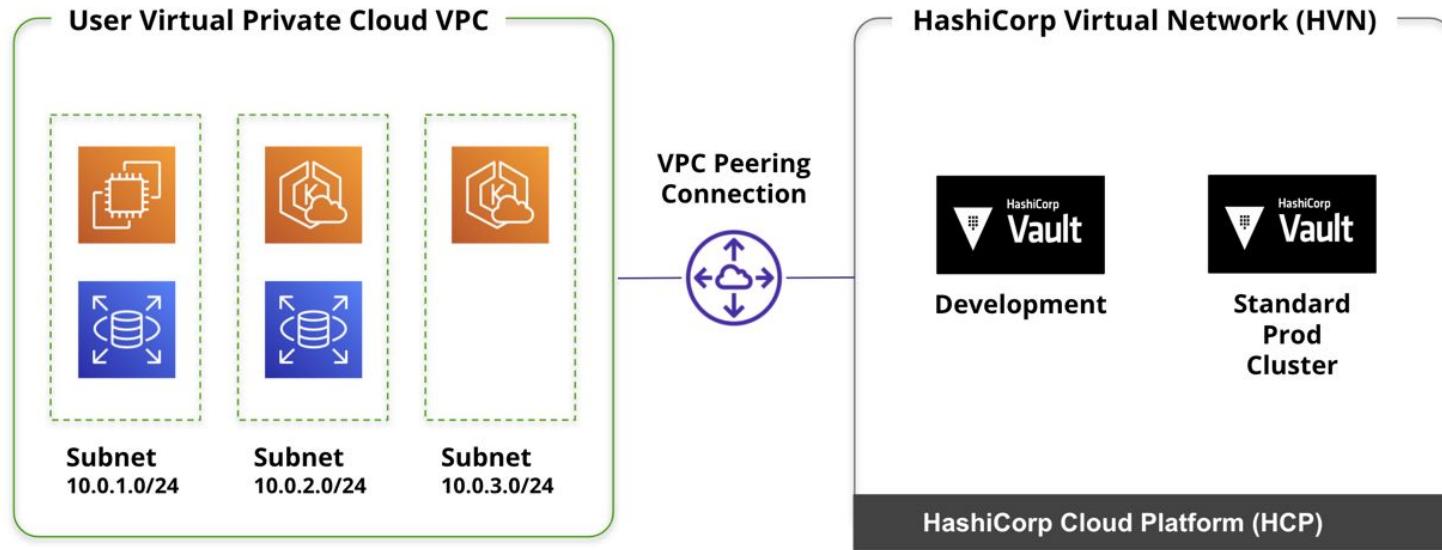
HCP Architecture

HCP consists of two main components, a control plane and a 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
US - Ohio	us-east-2
Canada - Central	ca-central-1
Europe - Ireland	eu-west-1
Europe - London	eu-west-2
Europe - Frankfurt	eu-central-1
APAC - Tokyo	ap-northeast-1
APAC - Singapore	ap-southeast-1
APAC - Sydney	ap-southeast-2



Regions

Supported Azure Regions

GA as of Feb 28, 2023

Name	Identifier
East US	eastus
East US 2	eastus2
West US 2	westus2
Central US	centralus
Canada Central	canadacentral
France Central	francecentral
North Europe	northeurope
West Europe	westeurope
UK South	uksouth
Australia Southeast	australiasoutheast
Japan East	japaneast
Southeast Asia	southeastasia



Access Controls HCP Platform

RBAC

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

MFA

When using the default email based authentication it is suggested to integrate with an MFA provider to increase the security of your HCP account and your company's data

Add Users

Users can be invited to join your organization via email or directly from the HCP console



Single Sign-On

Leverage GitHub or SAML 2.0 for federating identity with a trusted identity provider

- Organization owners and admins can configure [Single Sign-On](#)
- When SSO is enabled for an organization the user invitation feature is no longer offered, new users must be provisioned through the external IDP
- Existing accounts can still access the organization unless an admin removes them
- Current supported external IDP providers:
 - [Okta SAML](#)
 - [Azure Active Directory SAML](#)
 - [Okta OIDC](#)
 - [Azure Active Directory OIDC](#)



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

Automate HCP using Terraform

- The [HashiCorp Cloud Platform \(HCP\) Provider](#) for Terraform can manage the full lifecycle of HCP resources
- Managing HCP infrastructure as code enables creation of repeatable configurations that can be included in 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

The screenshot shows the HashiCorp Status page with the following details:

- Header:** Includes standard OS window controls (red, yellow, green buttons), back/forward navigation, a search bar, and a refresh button.
- Subscription Information:** A call-to-action to "Subscribe to HashiCorp Status updates via Atom or RSS Feed or contact Support." with a "Subscribe via" button.
- Navigation:** Tabs for "Services" (selected) and "Incident History".
- Section: Services**
 - HCP Portal:** Status is "Operational" (green checkmark).
 - HCP API:** Status is "Operational" (green checkmark).
 - HCP Packer:** Status is "Operational" (green checkmark).

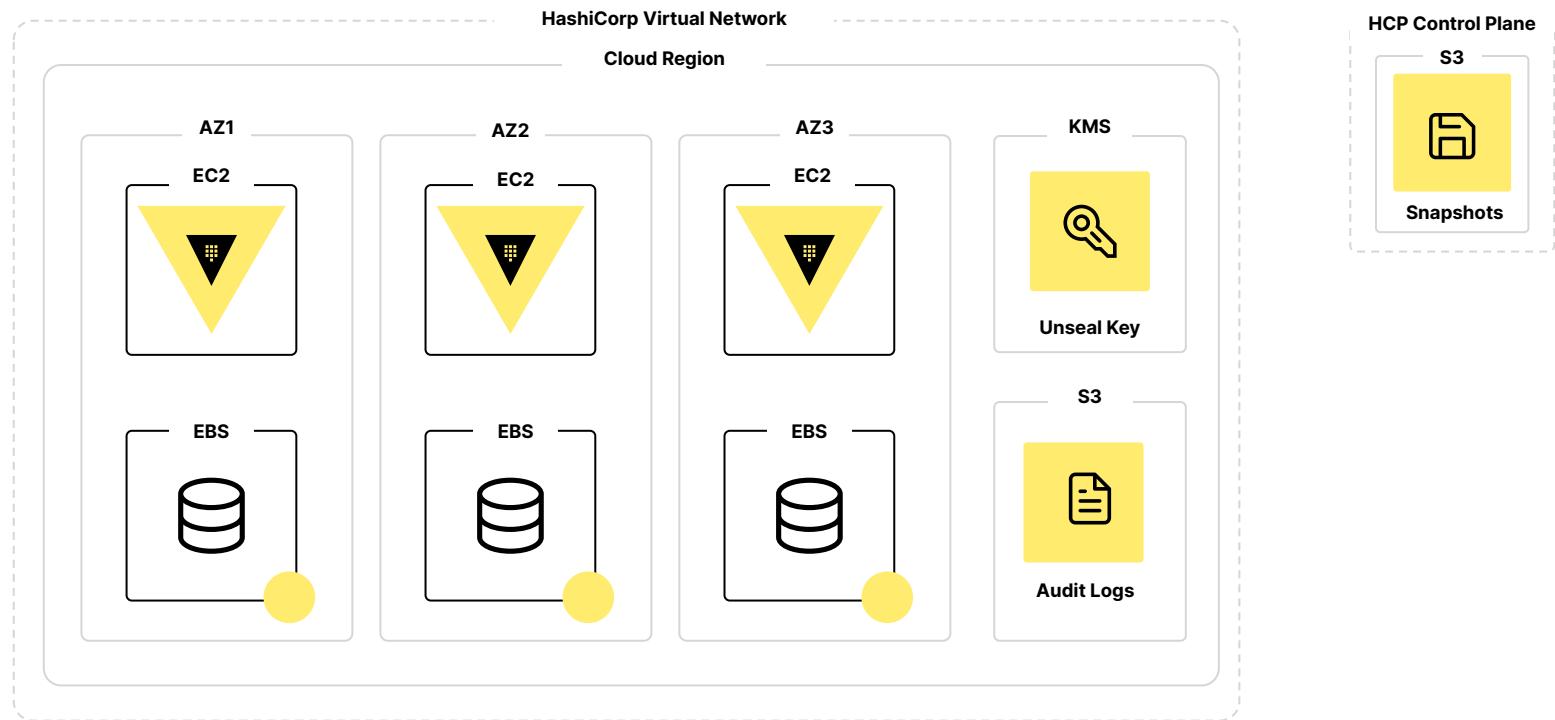


05

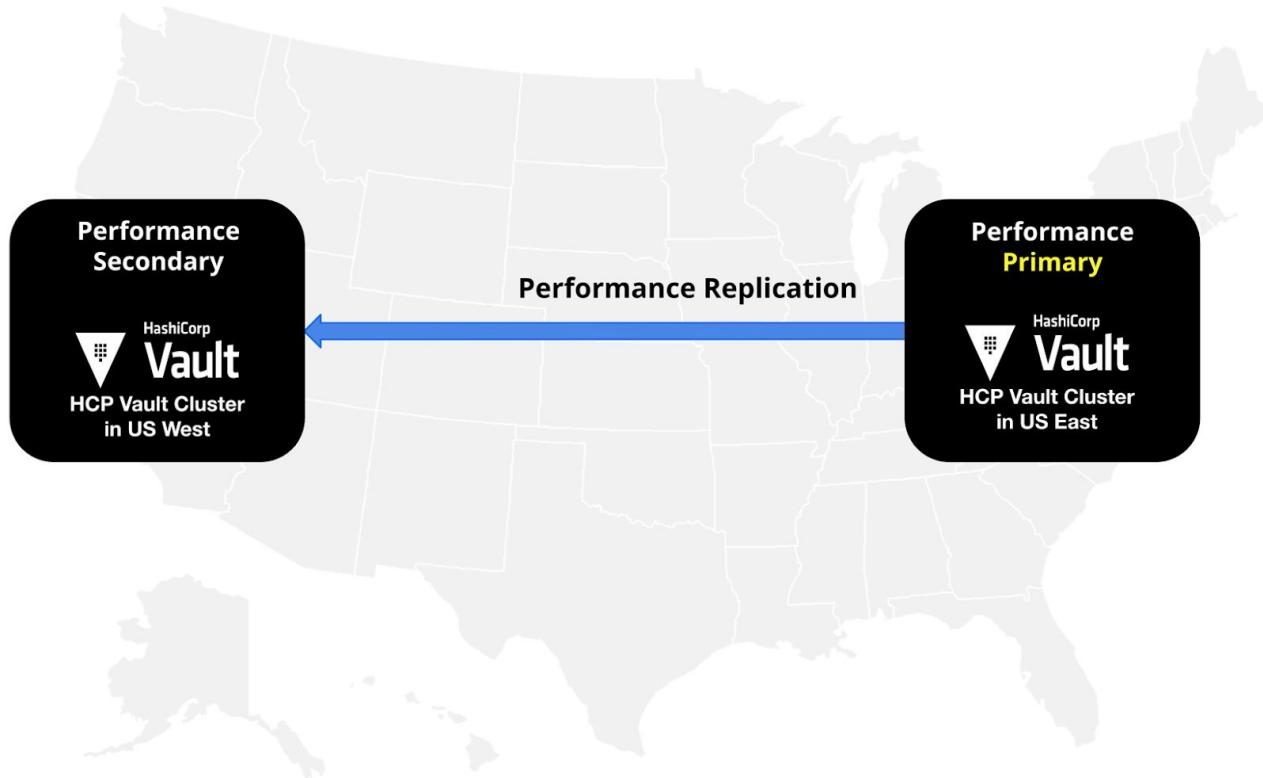


HCP Vault Overview

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	Starter	Standard	Plus
Designed to get started quickly for small projects, proof-of-concepts, non-production workloads.	Designed as affordable, production-ready clusters with clients included to get started quickly	Clusters designed to scale with the demand of running production workloads.	Designed for high availability replication of secrets and policies across multiple data centers
1 Node Cluster	3 Node Cluster Tiers		
Extra Small	Small	Small Medium Large	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
	Starter		2	8 GiB	5 GB storage, 250 GB for snapshots & audit logs			
	Standard / Plus Small		2	8 GiB	15 GB storage, 1 TB for snapshots & audit logs			
Production Tiers	Standard / Plus Medium	No Limit	4	16 GiB	30 GB storage, 5 TB for snapshots & audit logs	3 node cluster	400 requests/sec	Plus Only
	Standard / Plus Large		8	32 GiB	50 GB storage, 10 TB for snapshots & audit logs			



HCP Vault Security

Cluster Hardening

Clusters adhere to the published
[Vault production hardening guidelines](#)

Each cluster has:

- End-to-End TLS
- Firewall restrictions to only inbound TCP/8200
- Restricted storage access
- No clear text credentials

[HCP Vault cluster hardening details](#)

Root Tokens

At cluster creation, a root token is generated during the initialization process

Token is used for creation of:

- Initial authentication methods
- Initial policies
- Trust establishment with the HCP control plane

Token is revoked upon setup completion

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
- During download, audit logs are sent to the US for concatenation



Admin Token

- Admin tokens are similar to root tokens
- Should only be used during initial setup of a cluster or if an operator does not have cluster access
- Admin tokens are highly privileged and can access all endpoints within a cluster
- Tokens have a 6 hour TTL and cannot be renewed

Quick actions

[Access web UI](#)
Public Private

[New admin token](#)
[Generate token](#)

[Read a secret](#)
[Tutorial](#)

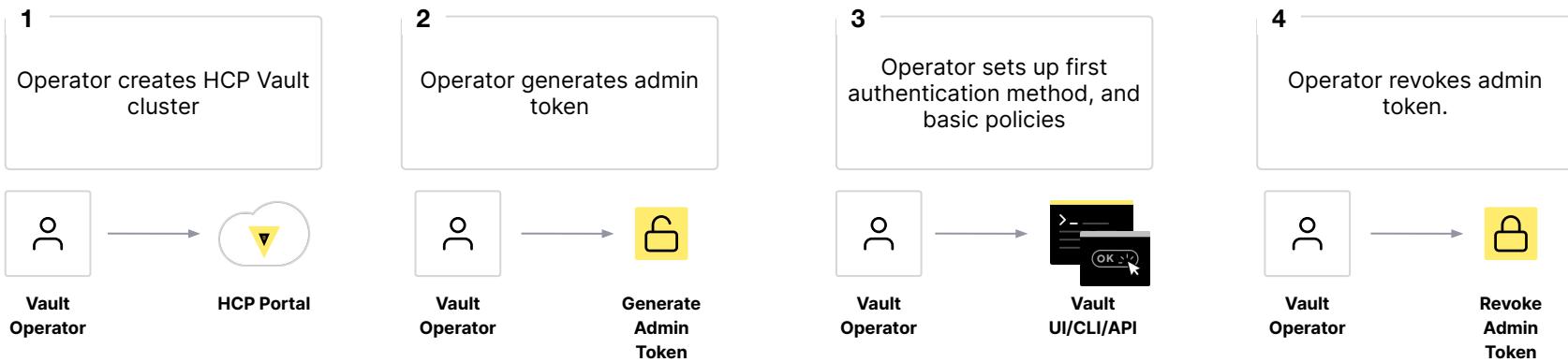
Cluster URLs
Copy the address into your CLI or browser to access the cluster.
 Private
 Public

In case of emergency
Vault data can be locked if an intrusion is detected.
 API Lock

Revoke all admin tokens
Admin tokens can be revoked before their expiration.
 Revoke



Initialization Process



Authentication Methods

Supported Authentication Methods

- HCP Vault has been validated to work with the listed authentication methods
- Additional authentication methods can be enabled, however limitations with configuration or functionality may be encountered

Human	Machine
Azure AD	AWS EC2
Okta	AppRole
GCP (without G Suite option)	Kubernetes
Github	JWT/OIDC
OIDC	AWS IAM
LDAP	GCP
Userpass	Azure
RADIUS	
Token	
MFA Duo	
MFA PingID	
MFA Okta	
MFA TOTP	



Secrets Engines

Supported Secrets Engines

- HCP Vault has been validated to work with the listed secrets engines
- Additional secrets engines can be enabled, however limitations with configuration or functionality may be encountered

[Validated Secrets Engines & Auth Methods](#)

Secrets Engines	Database Secrets Engines
Key/Value (V1 & V2)	Snowflake DB
AWS	MongoDB Atlas
GCP	RDS PostgreSQL
Consul, Consul Tokens	Elasticsearch
Transit	MySQL/MariaDB
Terraform Cloud Secrets	Cassandra
PKI (Certificates)	MSSQL
Cubbyhole	Redshift
TOTP	HandDB
OIDC Identity Provider (TP)	InfluxDB
OpenLDAP	Couchbase
RabbitMQ	
SSH	
Identity	
Azure	
Active Directory	
Nomad	



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,
including **all snapshots** and audit logs

- Audit logs can be exported in one hour increments from the HCP Portal
- Streaming audit logs to Datadog, Grafana, or Splunk for audit log retention is recommended



Performance Considerations

Profile Workloads

As organizations scale up the adoption of Vault, varying workloads access the Vault instance

- Telemetry should be leveraged to ensure proactive monitoring of Vault Cluster resources
- As new applications/services/teams/users are onboarded, it is suggested to profile the usage patterns to ensure optimal authentication and consumption patterns are used

External Systems

- Multiple Vault Authentication Methods and Secrets Engines have dependency on external systems for Vault requests to be completed
- Ensure telemetry is enabled on those services and proactively monitor for performance issues.

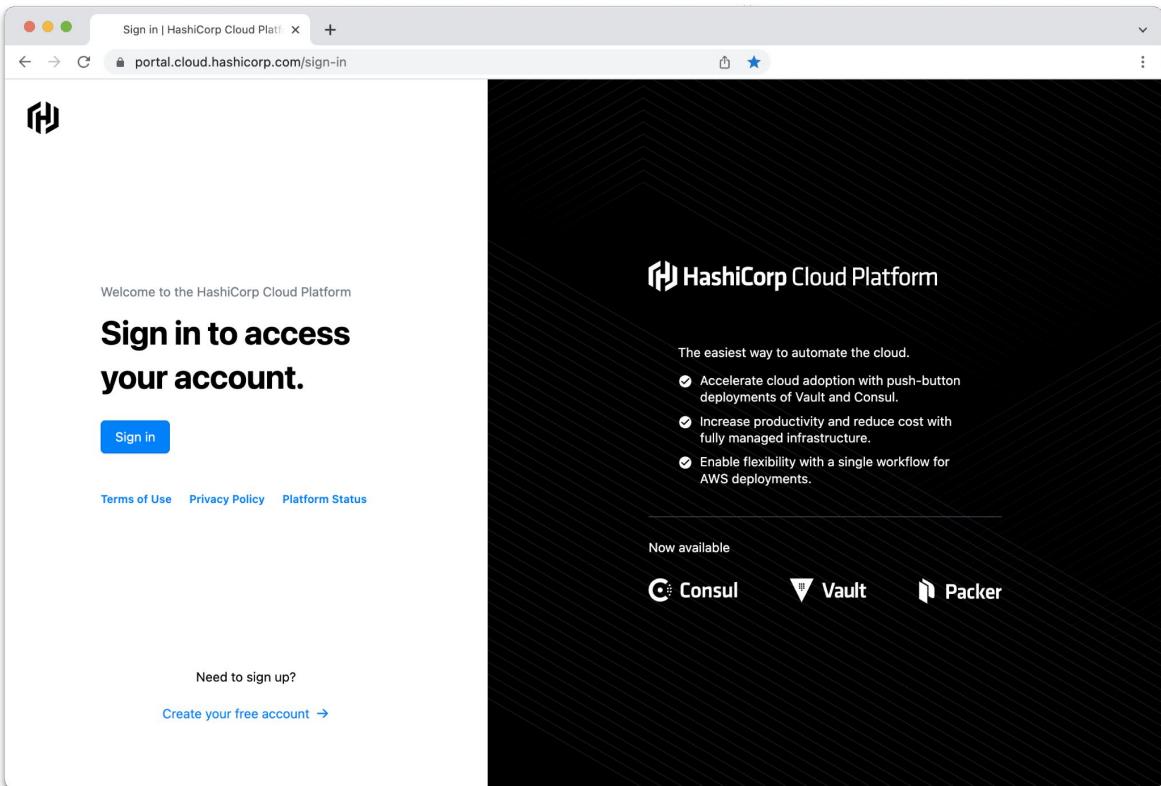


06

Demo



HCP Portal Login



<https://portal.cloud.hashicorp.com>

Demo

Accessing HashiCorp Cloud Platform (HCP)

Navigating HCP Portal

Create a HashiCorp Virtual Network

Create a HCP Vault Cluster

Create a Vault Operator policy

Enable initial authentication method for Vault Operator

Create a Vault Namespace

Enable KV Secrets engine and write a secret



Upcoming Webinars



Vault

Operationalizing for Production

Learn best practices for automating configuration of the HCP Control Plane & Vault along with Telemetry, Monitoring, and Audit Logging

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

Action Items



- Share to customer.success@hashicorp.com
 - Authorized technical contacts for support
 - Stakeholders contact information (name and email addresses)
- Email your CSM with a brief summary of HCP Vault use case(s), goals, and project milestones
- Activate your HCP Account and create an Administrative user



Thank you