



# Namespaces, Authentication, and Policies

June 2022

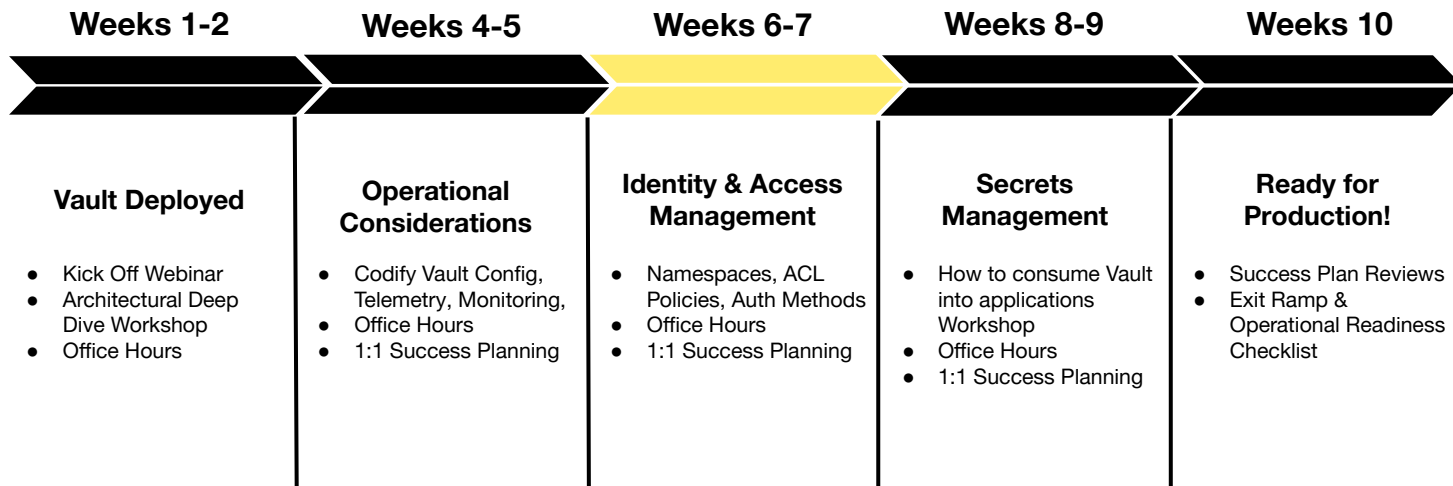
*Copyright © 2021 HashiCorp*



# Agenda

- Namespaces
- Authentication
- Policies
- Next Steps

# HCP Vault Path to Production



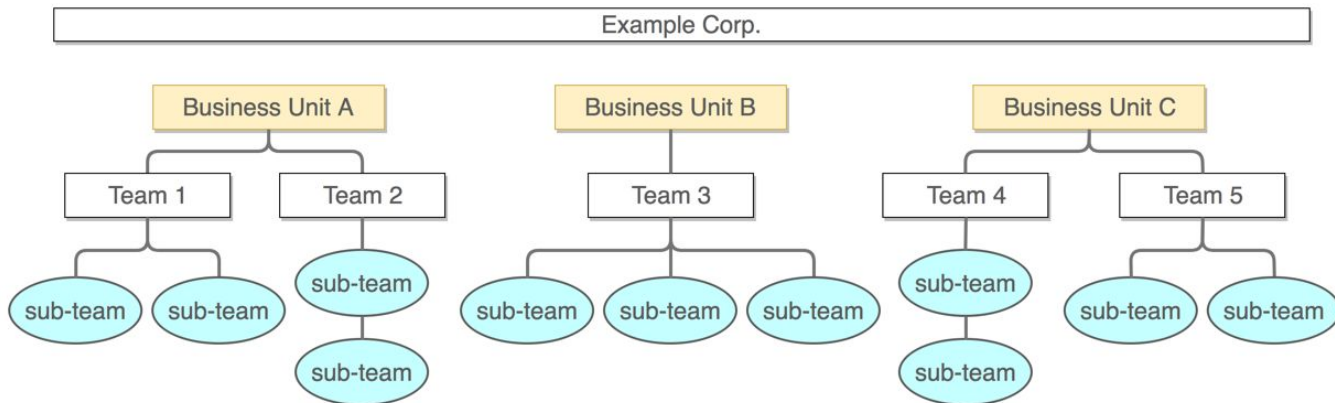
# Namespaces

# Namespaces



Namespaces create “Vaults within a Vault” that enables you to provide Vault as a service in your organization.

Each namespace will maintain its own path structure. This allows you to delegate administration of policies and secrets management to teams while controlling the blast radius by isolating control within their namespace



# Namespace Contents



Unique to each namespace

- Policies
- Secrets Engines
- Authentication Methods
- Tokens
- Identity Entities and Groups

# Considerations



Requirement	What to Consider
Organizational Structure	What is your organizational structure?
	What is the level of granularity across lines of businesses (LOBs), divisions, teams, services, apps that needs to be reflected in Vault's end-state design?
Self-Service Requirements	Given your organizational structure, what is the desired level of self-service required?
	How will Vault policies be managed?
	Will teams need to directly manage policies for their own scope of responsibility?
	Will they be interacting with Vault via some abstraction layer where policies and patterns will be templated? For example, configuration by code, Git flows, the Terraform Vault provider, custom onboarding layers, or some combination of these.

# Considerations



## Requirement

## What to Consider

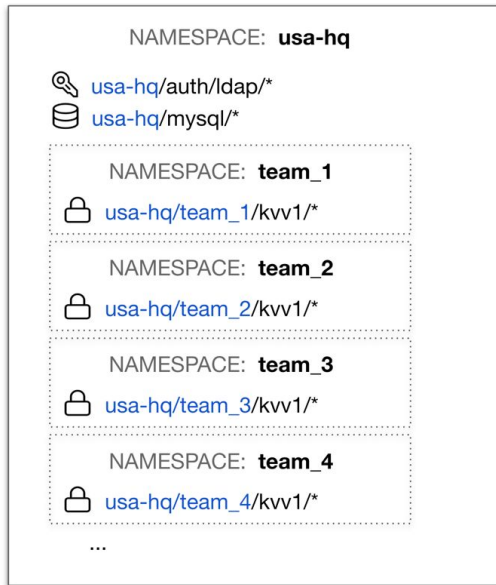
<b>Audit Requirements</b>	What are the requirements around auditing usage of Vault within your organization?
	Is there a need to regularly certify access to secrets?
	Is there a need to review and/or decommission stale secrets or auth roles?
	Is there a need to determine chargeback amounts to internal customers?
<b>Secrets Engine Requirements</b>	What types of secrets engines will you use (KV, database, AD, PKI, etc.)?



# When to use?



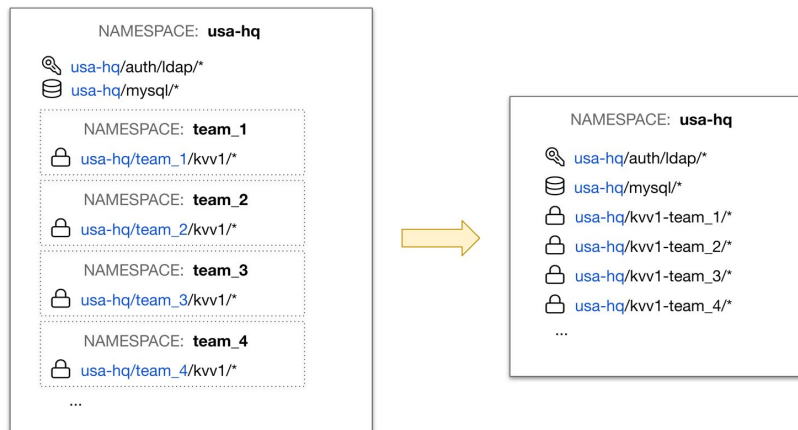
Namespaces should be leveraged sparingly and primarily to delineate administrative boundaries. However, when considering namespace structure often many unnecessary namespaces get created by trying to replicate organizational structure.



# When to use?

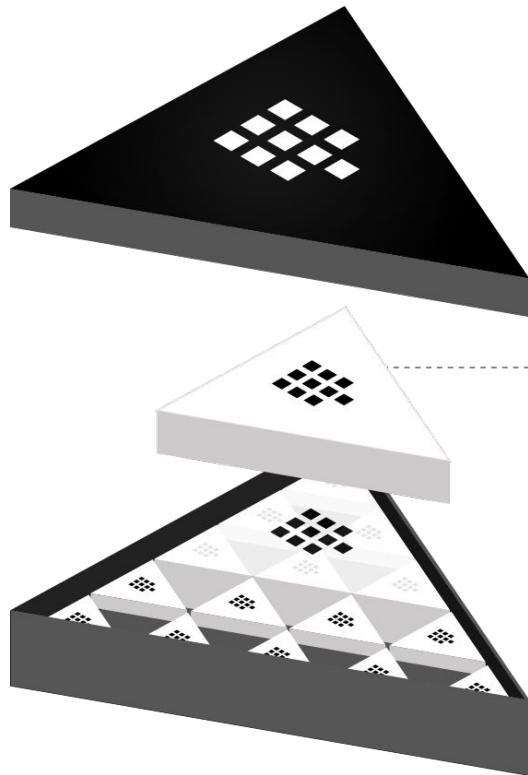


Instead of providing self-service by implementing many namespaces we recommend implementing an onboarding layer. We shift the administrative boundary from teams to the onboarding layer. This reduces the number of namespaces while enforcing a standard naming convention, secrets path structure, and templated policies.





# Namespaces for Teams and Groups



- **Engineering Org (Namespace)**

**Members:**

Security Team, Operations Teams, Engineering Manager

**Namespace Specific Configuration:**

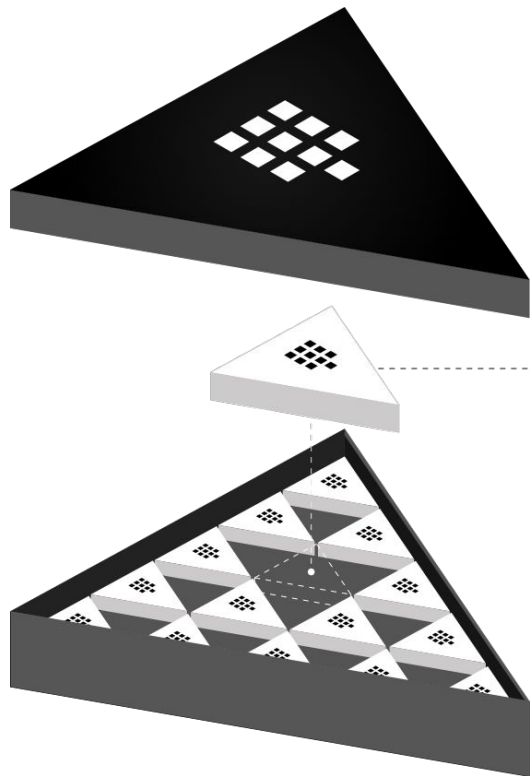
Defined engineering member access  
Defined engineering authentication mounts  
Defined engineering secrets engines



*Note: Vault supports namespaces within namespaces. By default there can always be a parent managed namespace that has rights to sub-namespaces, such as the Applications/User namespaces*



# Namespace per each Application



- **Application (Namespace)**

**Members:**

Alex Smith, Jennifer Johnson, Steve Stevens

**Namespace Specific Configuration:**

Defined member access

Defined authentication mounts for AWS, Azure, and GCP systems

Defined custom secrets engine





# Getting Started with Namespaces

CLI

```
TERMINAL

# Create namespace
> vault namespace create -namespace=admin/usa-hq

# Create child namespaces
> vault namespace create -namespace=admin/usa-hq/sales

# List namespaces from within admin namespace
> vault namespace list -namespace=admin

# List child namespaces for usa-hq namespace
> vault namespace list -namespace=admin/usa-hq

# Instead of CLI flag, environment variable can be used
> export VAULT_NAMESPACE="admin/usa-hq"
> vault namespace create sales
```



# Getting Started with Namespaces

CLI

```

/
/admin/
/admin/bu-a/
  - Secrets
  - Policy
  - Auth
  - Tokens
/admin/bu-b/
  - Secrets
  - Policy
  - Auth
  - Tokens
/admin/bu-b/team-a/
  - Secrets
  - Policy
  - Auth
  - Tokens

```



# Getting Started with Namespaces

API

```
TERMINAL

# Create namespace
> curl --header "X-Vault-Token: <TOKEN>" \
--request POST \
https://<vault_addr>/v1/sys/namespaces/admin/usa-hq

# Create child namespaces
> curl --header "X-Vault-Token: <TOKEN>" \
--header "X-Vault-Namespace: admin/usa-hq" --request POST \
https://<vault_addr>/v1/sys/namespaces/sales
```

# Authentication

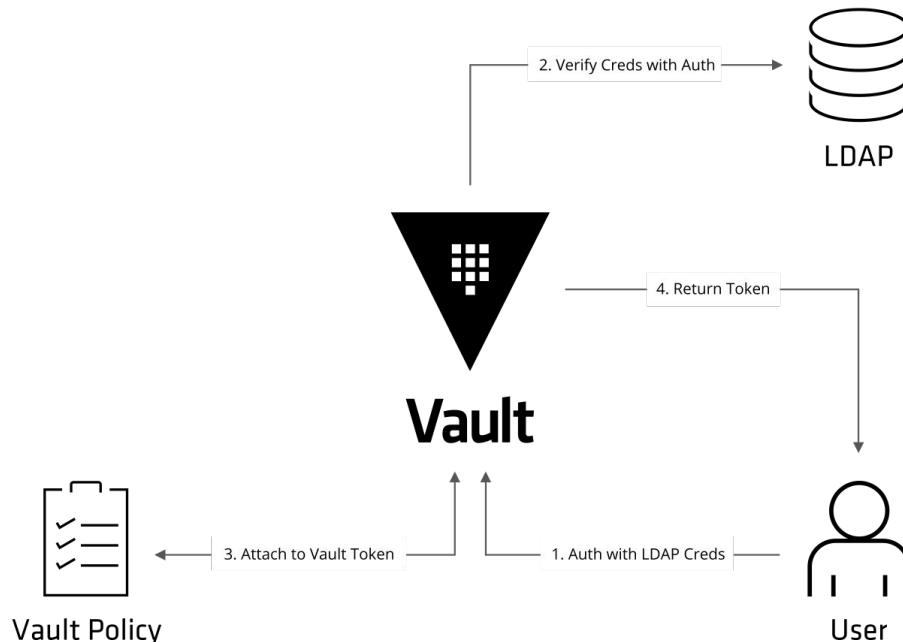


# Authentication in Vault



Vault supports integrating with trusted identity providers to validate user or machine supplied information to create a token tied to a pre-configured policy.

- If Vault is able to successfully validate the credentials, a Vault token will be returned that can then be used to access Vault.
- The token Vault returns is associated to a Vault policy that defines what access and capabilities the token can perform.



# Human vs. Machine Authentication



Vault provides authorization and not authentication of users so you will need to integrate with a trusted Identity provider to authenticate and verify the client before access to Vault is granted.

- Multiple authentication methods can and should be used
- Human users should authenticate using a method that leverages an external identity provider
- Machine users should authenticate using AppRole or auth type that uses instance metadata to authenticate the machine such as AWS or GCP.

Human Auth	Machine Auth
GitHub	AppRole
LDAP/AD	AWS
OIDC	Azure
Okta	Google Cloud
Cloud IAM	JWT
Username & Password	Kubernetes
	RADIUS
	TLS Certificates
	Cloud Foundry

# Vault Identity Recap



## Entities & Groups



**Group Name: Accounting**  
Group ID: 0bfed703-f07d-2965...  
Policies: **accounting**

A **group** can have multiple entities as its members



**Entity Name: Bob Smith**  
Entity ID: bf23f85c-4e26-b...  
Policies: **test**

### Aliases:

ID: 7b0788d6-a259-6eb7-9...  
Auth type: **LDAP**  
Name: "bsmith"  
Policies: test-admin, devops

ID: 7617592a-e737-2e9d-d...  
Auth type: **Userpass**  
Name: "bob"  
Policies: base

A Vault client can be mapped as an entity

An entity can have multiple aliases



**Entity Name: HCP Billing**  
Entity ID: lw23p85c-2e9-b...  
Policies: **billing**

### Aliases:

ID: 6713592a-e737-2e9d-d...  
Auth type: **AWS**  
Role Name: "hcp-billing"  
Policies: app



**Group Name: Payment**  
Group ID: l273k85c-2e9-b...  
Policies: **payment**

Also, a **group** can have subgroups

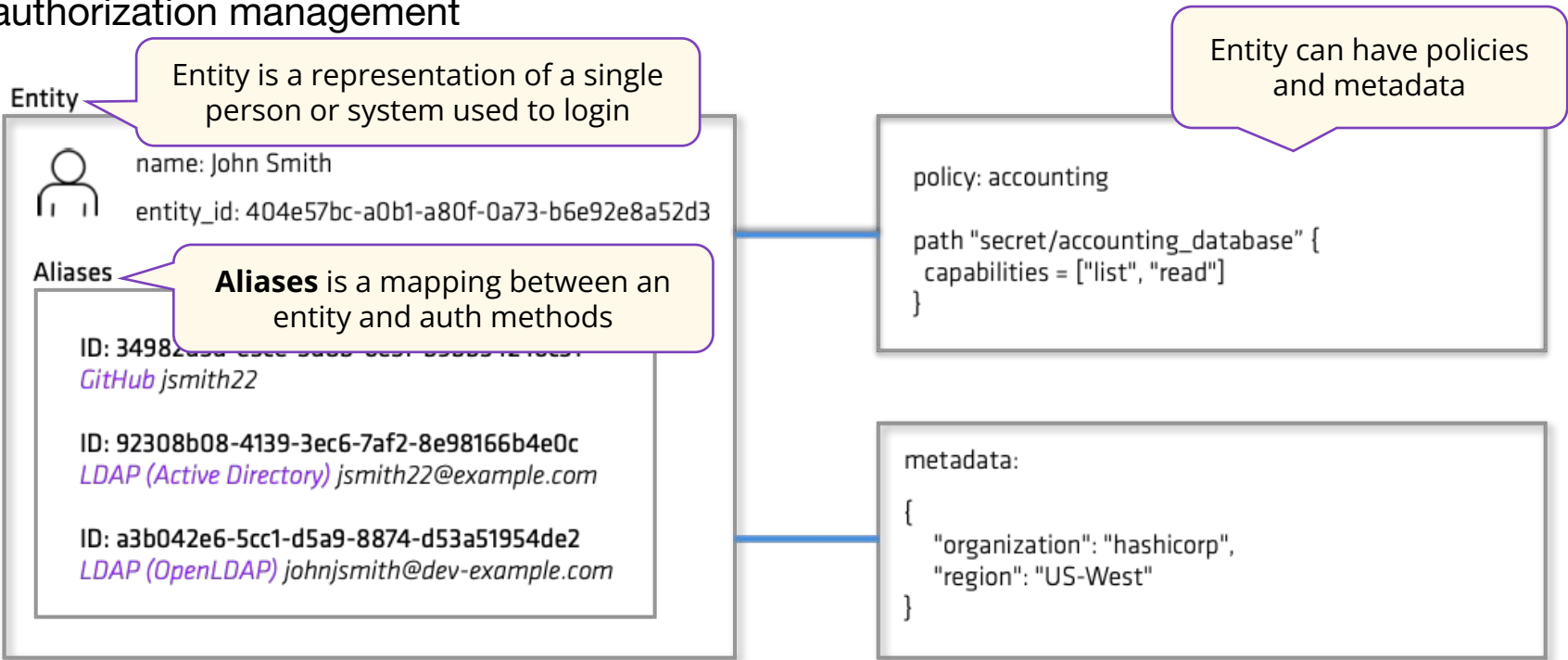
### Aliases:

ID: 6713592a-e737-2e9d-d...  
Auth type: **LDAP**  
Name: "payment"  
Policies: payment

# Entities and Aliases



Map multiple user authentication schemes to a single entity to provide for more efficient authorization management



# Token and Policies



Policies can be assigned to entities which will grant **additional** permissions



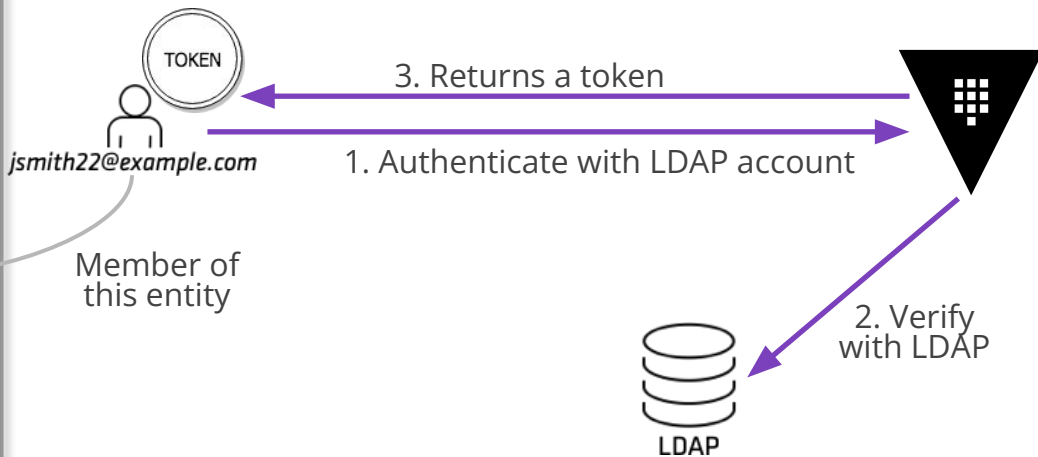
Token inherits **capabilities** granted by both policies



expense



acct-manager



# Basic Workflow



**Step 1: Enable auth methods**



**Step 2: Configure each auth method**



**Step 3: Create an Entity**



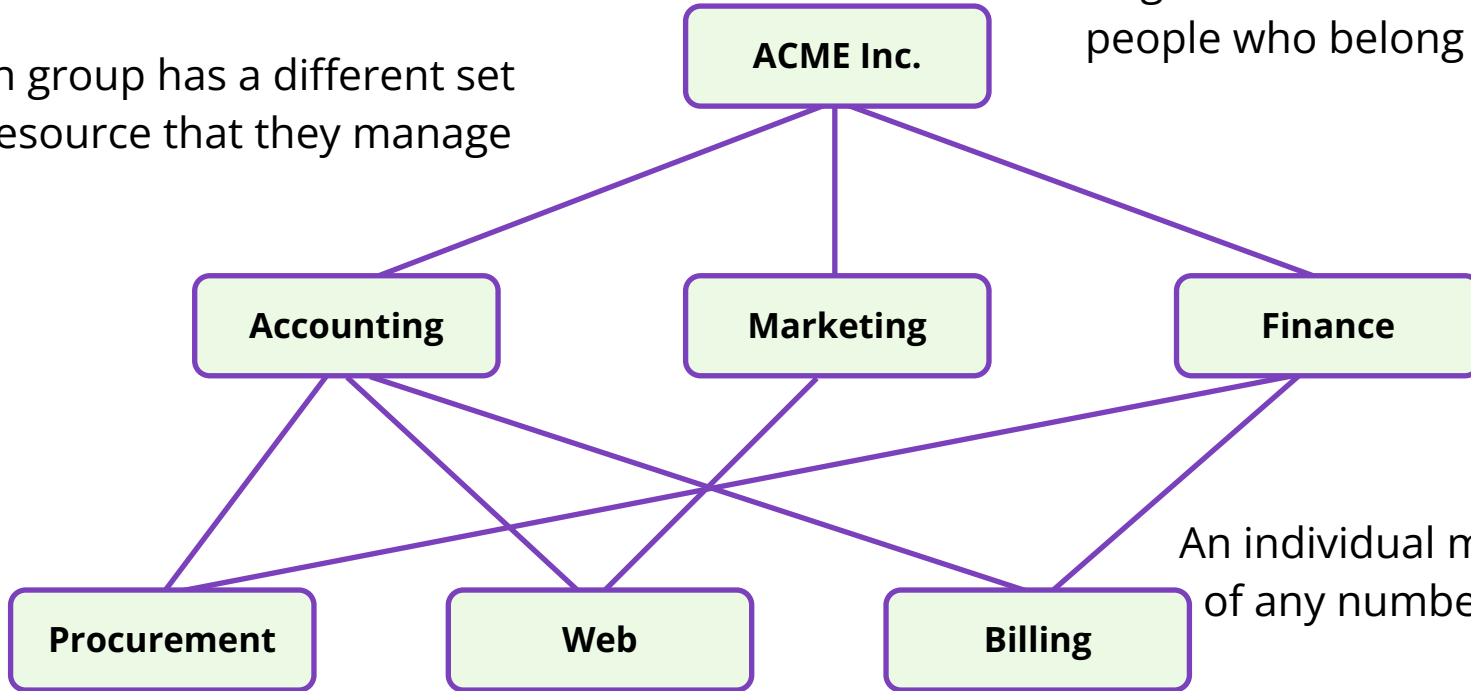
**Step 4: Create the Entity Aliases**

# Organizational Structure



Each group has a different set of resource that they manage

Organization is composed of people who belong in groups



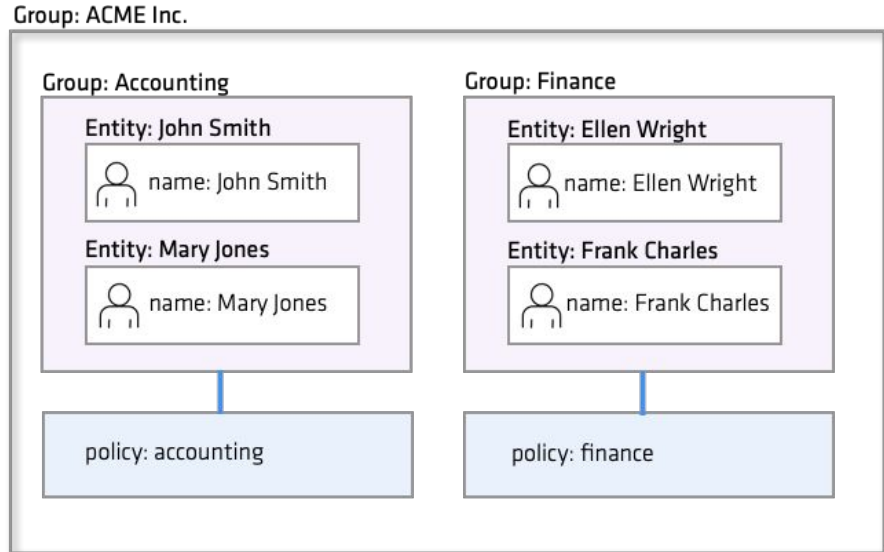
An individual may be a part of any number of groups

# Identity Groups



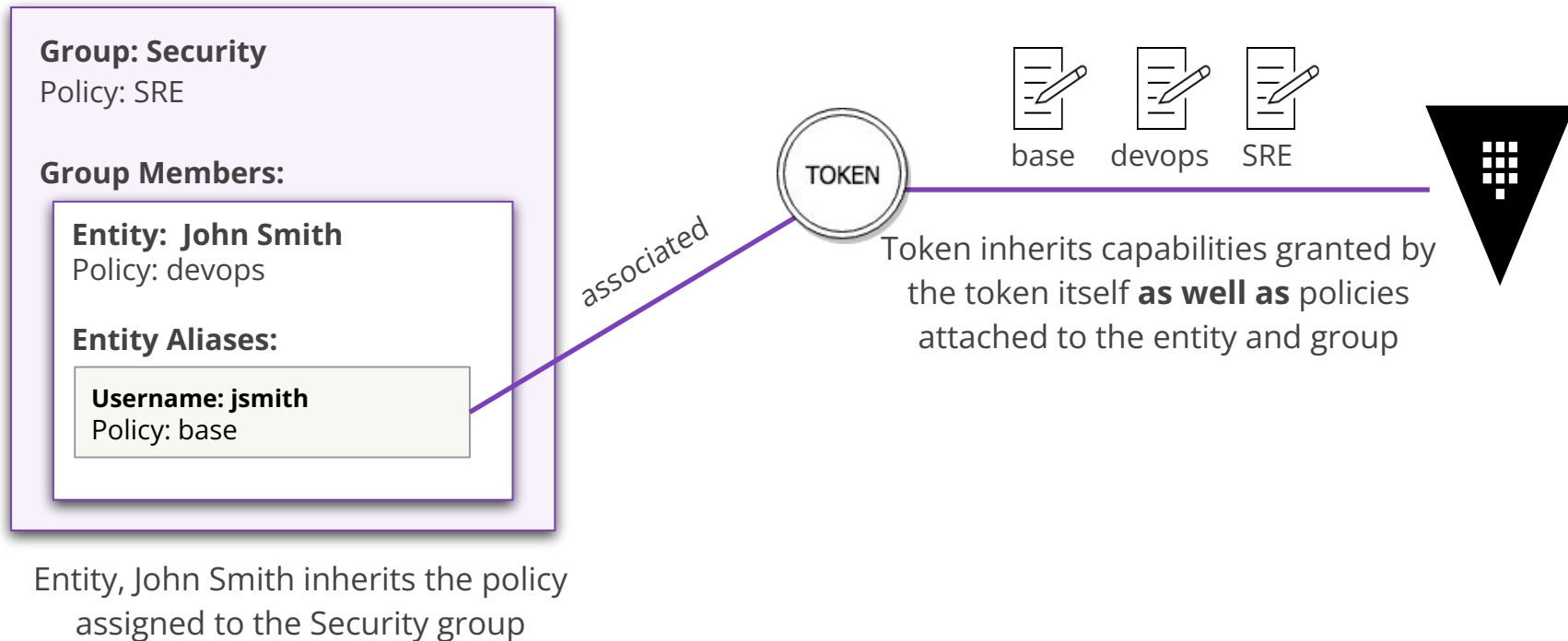
Identity group maps multiple user entities to a group for authorization management at scale.

- Identity groups can have multiple entities as its members as well as subgroups
- Entities can be direct member of groups
- Inherits the policies of the groups they belong to
- Entities can be indirect member of groups
- Groups can have a set of policies and metadata inherited from the member entity or subgroups





# Group Hierarchical Permissions



# Identity Groups Aliases



- **Internal groups** are those groups manually created by the operators via API
- **External groups** are the groups which Vault infers and creates based on the group associations coming from the auth methods
- Identity **group alias** is a mapping between identity groups and groups in an third party authentication provider
  - If a user is a part of an external group (LDAP group), automatically adds the user to the identity group inheriting the policies and metadata

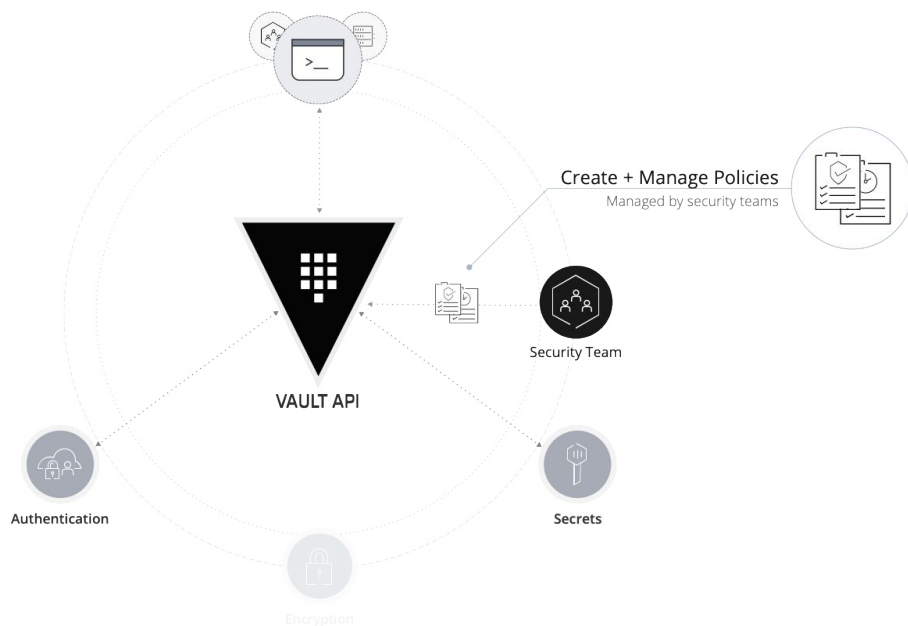


# Policies

# Vault Policies

## Role-Based Access Control

- Use policies to govern the behavior of the Vault clients
- Instrument Role-Based Access Control (RBAC)
- **Safeguard access** and secret distribution to apps

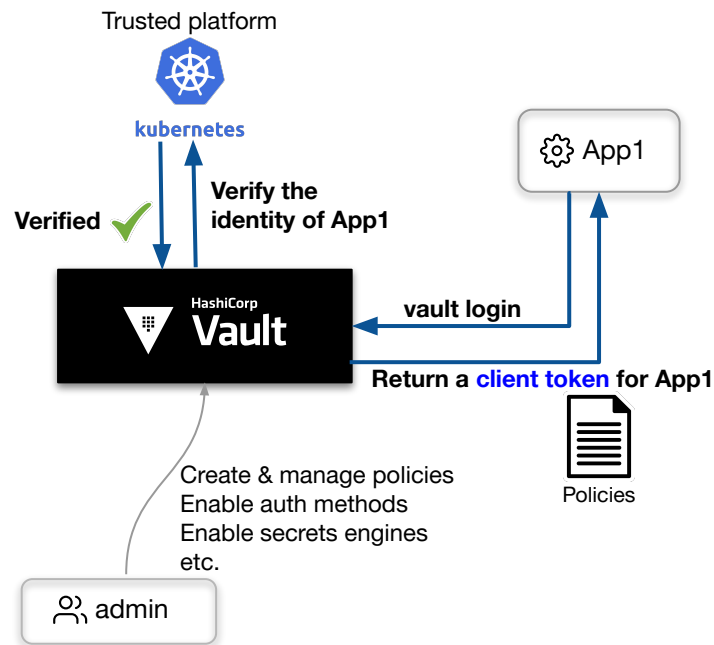


# Vault Policies and Client Tokens



## How it all fit together

- Every Vault client must authenticate with Vault to acquire a **client token**
- The client token has **policies attached**
- Use the client token to invoke Vault operations (e.g. read secrets)



# Language of policies



- Policies are written in **HashiCorp Configuration Language (HCL)**
- Everything is **path**-based and corresponds to Vault API endpoints
  - Policies grant or deny access to certain **paths** and operations
- Empty policy grants **no permission**

Vault is **deny by default**

No policy = No authorization



# Policies

## path

```
TERMINAL
path "<PATH>" {
  capabilities = [ <LIST> ]
}
```

### Example path

http://VAULT\_ADDR:8200/v1/auth/userpass/users/apps



# Policies

path

capabilities

```

path "<PATH>" {
  capabilities = [ <LIST> ]
}

```

## capabilities

create

read

update

delete

list

sudo

deny

## HTTP Verbs

POST/PUT

GET

POST/PUT

DELETE

LIST





# Root protected paths

The **sudo** capability must be provided for those root protected paths

Refer to the [Learn tutorial](#)

Jump to section ▾ Show terminal

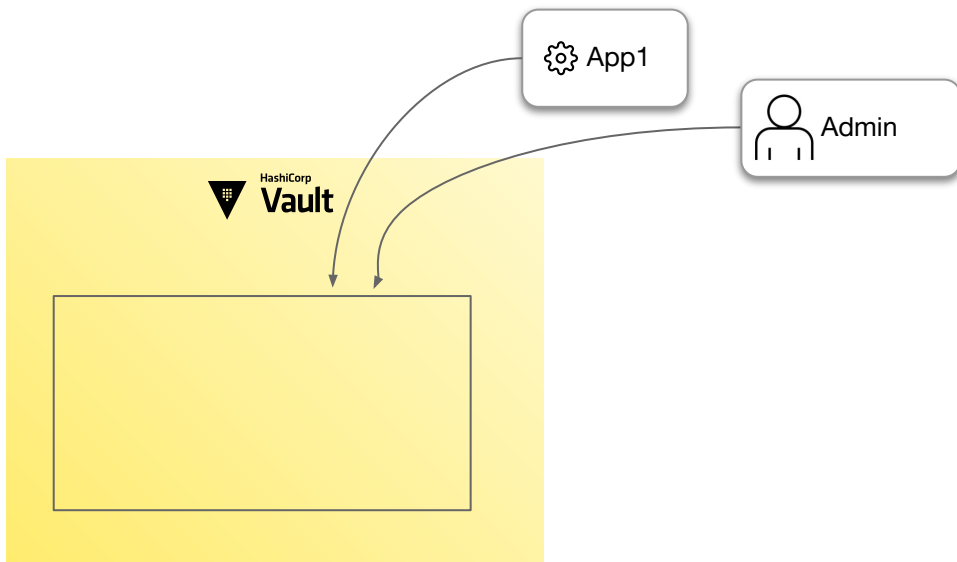
Docs Forum Bookmark

## Root protected API endpoints

The following paths requires a root token or `sudo` capability in the policy:

Path	HTTP verb	Description
<a href="#">auth/token/accessors</a>	LIST	List token accessor
<a href="#">auth/token/create-orphan</a>	POST	Create an orphan token (the same as <code>no_parent</code> option)
<a href="#">auth/token</a>	POST	Create a periodic or an orphan token ( <code>period</code> or <code>no_parent</code> ) option
<a href="#">pki/root</a>	DELETE	Delete the current CA key ( <a href="#">pki secrets engine</a> )
<a href="#">pki/root/sign-self-issued</a>	POST	Use the configured CA certificate to sign a self-issued certificate ( <a href="#">pki secrets engine</a> )
<a href="#">sys/audit</a>	GET	List enabled audit devices
<a href="#">sys/audit/:path</a>	PUT, DELETE	Enable or remove an audit device
<a href="#">sys/auth/:path</a>	GET, POST, DELETE	Manage the auth methods (enable, read, delete, and tune)
<a href="#">sys/config/auditing/request-headers</a>	GET	List the request headers that are configured to be audited
<a href="#">sys/config/auditing/request-headers:name</a>	GET, PUT, DELETE	Manage the auditing headers (create, update, read and delete)

# Policy Authoring Workflow



Discover the policy:

- gather secret requirements
- perform operations with Vault
- discovering the paths and the capabilities required
- define a policy
- test the policy



# Three discovery techniques

- API documentation
- -output-curl-string
- Vault's audit logs



# API docs

```
path "transit/encrypt/app1" {  
  capabilities = [ "update" ]  
}
```

## Encrypt Data

This endpoint encrypts the provided plaintext using the named key.

This path supports the `create` and `update` policy capabilities as



context parameter is empty or not). If the user only has `update` capability and the key does not exist, an error will be returned.

Method	Path
POST	/transit/encrypt/:name

app1

update capability



# CLI command flag

`-output-curl-string`

```
path "sys/policies/acl/test" {  
  capabilities = [ "read" ]  
}
```

TERMINAL

```
$ vault policy read -output-curl-string test
```

default HTTP verb is GET

👁 `curl -H "X-Vault-Request: true" -H "X-Vault-Token:`  
`$(vault print token) "`

👁 `http://127.0.0.1:8200/v1/sys/policies/acl/test`

path



# Audit Log

A detailed log of every authenticated interaction.

- Time
- Requestor
- Request
- Response

```
$ cat log/vault_audit.log | jq -s "[-1]"
```

```
$ cat log/vault_audit.log | jq -s "[-1].request"
{
```

```
  "id": "70419a8b-d904-542b-fe48-61d8f869a0b7",
```

```
  "operation": "update",
```

```
  "mount_type": "transit"
```

```
  ...
```

```
  "path": "transit/keys/app-auth",
```

```
  "remote_address": "127.0.0.1"
```

```
}
```

operation maps to capability

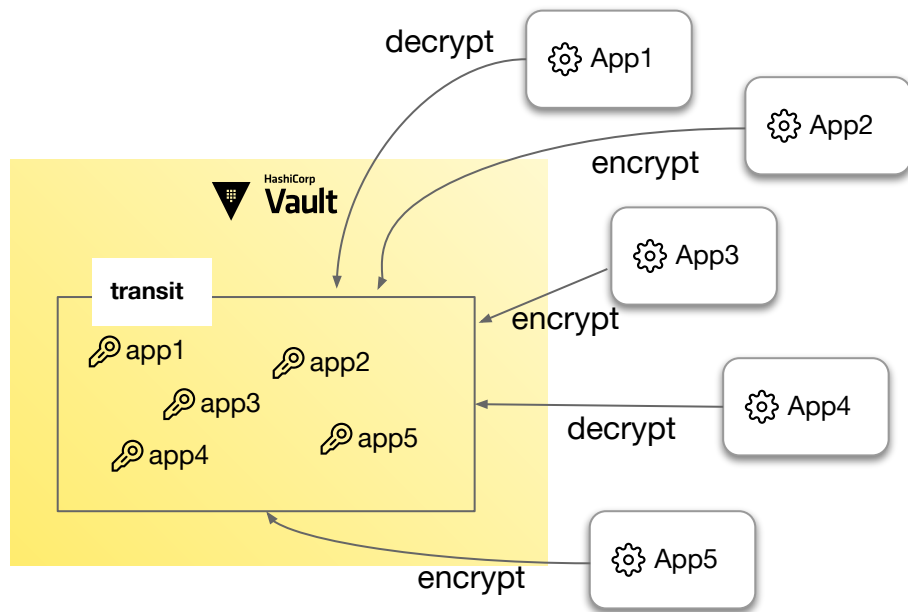
path

```
path "transit/keys/app-auth" {
  capabilities = [ "update" ]
}
```

# Example Scenario



## Using transit secrets engine for data encryption/decryption



- Each application has its own encryption key
- Challenge:
  - The number of applications will grow
  - You cannot foresee the name of future applications to be developed

# Policy Solutions



## Using transit secrets engine for data encryption/decryption

Solution 1

```
path "transit/encrypt/*" {  
  capabilities = [ "update" ]  
}  
  
path "transit/decrypt/*" {  
  capabilities = [ "update" ]  
}
```

Is it good enough?

- Trouble points:

The policy is **too open**. App1 can access app4 encryption key.

Solution 2

```
path "transit/encrypt/app1" {  
  capabilities = [ "update" ]  
}  
  
path "transit/decrypt/app1" {  
  capabilities = [ "update" ]  
}
```

Is this easy to scale and maintain?

- Trouble points:

You have to write policies for each app.



# ACL Templating



```
CODE EDITOR

path "secret/data/{{identity.entity.id}}/*" {
    capabilities = ["create", "update", "read", "delete"]
}

path "secret/metadata/{{identity.entity.id}}/*" {
    capabilities = ["list"]
}
```

- Use variable replacement in some policy strings with values available to the token
- Define policy paths containing double curly braces: **{{<parameter>}}**

# Available Templating Parameters (1 of 2)



Parameter	Description
<code>identity.entity.id</code>	The entity's ID
<code>identity.entity.name</code>	The entity's name
<code>identity.entity.metadata.&lt;&lt;metadata key&gt;&gt;</code>	Metadata associated with the entity for the given key
<code>identity.entity.aliases.&lt;&lt;mount accessor&gt;&gt;.id</code>	Entity alias ID for the given mount
<code>identity.entity.aliases.&lt;&lt;mount accessor&gt;&gt;.name</code>	Entity alias name for the given mount
<code>identity.entity.aliases.&lt;&lt;mount accessor&gt;&gt;.metadata.&lt;&lt;metadata key&gt;&gt;</code>	Metadata associated with the alias for the given mount and metadata key

# Available Templating Parameters (2 of 2)



Parameter	Description
<code>identity.groups.ids.&lt;&lt;group id&gt;&gt;.name</code>	The group name for the given group ID
<code>identity.groups.names.&lt;&lt;group name&gt;&gt;.id</code>	The group ID for the given group name
<code>identity.groups.names.&lt;&lt;group id&gt;&gt;.metadata.&lt;&lt;metadata key&gt;&gt;</code>	Metadata associated with the group for the given key
<code>identity.groups.names.&lt;&lt;group name&gt;&gt;.metadata.&lt;&lt;metadata key&gt;&gt;</code>	Metadata associated with the group for the given key



# Token policies & Identity Policies

```
$ vault token lookup
```

Key	Value
---	-----
accessor	yOMHJzMZ5Krz7BSrOtF2ZzC2
creation_time	1622087787
creation_ttl	768h
display_name	userpass-bob
entity_id	bf3ea189-61a1-d7...snip...
expire_time	2021-06-28T<time_stamp>
explicit_max_ttl	0s
external_namespace_policies	map[]
id	s.UYkAjU6ak70qwQ4OCmLP3uyT
<b>identity_policies</b>	<b>[base]</b>
issue_time	2021-05-27T<time_stamp>
<b>meta</b>	<b>map[username:bob]</b>
num_uses	0
orphan	true
path	auth/userpass/login/bob
<b>policies</b>	<b>[default test]</b>
...snip...	



# ACL Templating with Identity Entity Names

```
CODE EDITOR

path "transit/encrypt/{{identity.entity.name}}" {
    capabilities = [ "update" ]
}

path "transit/decrypt/{{identity.entity.name}}" {
    capabilities = [ "update" ]
}
```

If the app name and key name do not match, you can store the key name as a metadata → `{{identity.entity.metadata.key_name}}`

# ACL Templating with Identity Groups



```
CODE EDITOR

path "auth/ldap/groups/{{identity.groups.ids.fb036ebc-2f62-4124-9503.name}}" {
    capabilities = [ "update", "read" ]
}

path
"secret/data/groups/{{identity.groups.names.education.metadata.product}}/*" {
    capabilities = [ "create", "update", "read", "delete" ]
}
```

- Identity **groups** are not directly attached to a token and an **entity** can be associated with multiple groups
- To reference a group, the **group ID** or **group name** must be provided



# CLI

## vault

```
TERMINAL

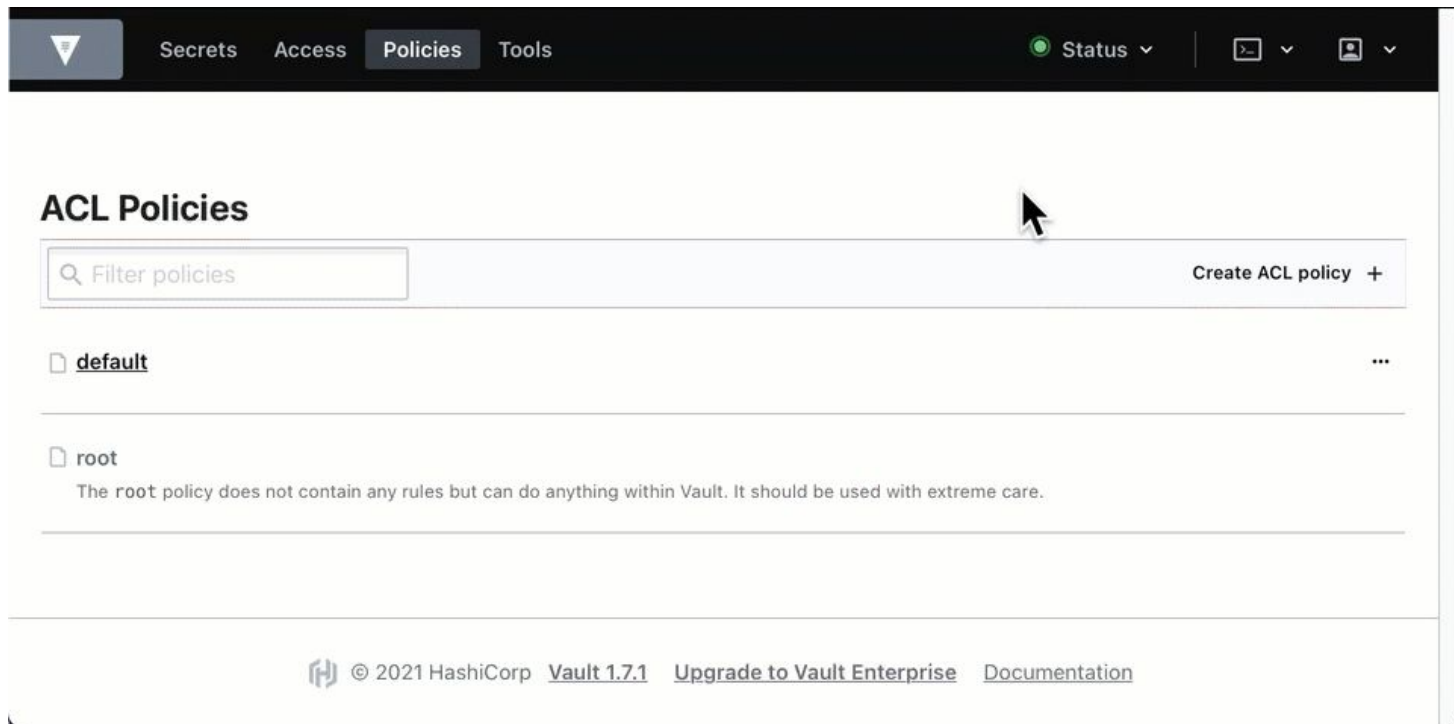
$ vault policy --help

$ vault policy list
default
root
list all policies

$ vault policy read default
...
show policy

$ vault policy write apps-policy apps-policy.hcl
create or
update policy
```

# Vault UI



The screenshot shows the Vault UI interface. At the top is a dark navigation bar with a dropdown menu icon on the left, followed by tabs for 'Secrets', 'Access', 'Policies' (which is selected), and 'Tools'. On the right side of the bar are a 'Status' indicator with a green dot and a dropdown arrow, a terminal icon with a dropdown arrow, and a user profile icon with a dropdown arrow. Below the navigation bar, the main content area is titled 'ACL Policies'. It features a search bar with the placeholder text 'Filter policies' and a 'Create ACL policy +' button. A list of policies is shown below, including 'default' and 'root'. The 'root' policy has a descriptive note: 'The root policy does not contain any rules but can do anything within Vault. It should be used with extreme care.' At the bottom of the page is a footer containing the HashiCorp logo, copyright information '© 2021 HashiCorp', and links for 'Vault 1.7.1', 'Upgrade to Vault Enterprise', and 'Documentation'.

**ACL Policies**

Filter policies

Create ACL policy +

**default** ...

**root**

The root policy does not contain any rules but can do anything within Vault. It should be used with extreme care.

© 2021 HashiCorp [Vault 1.7.1](#) [Upgrade to Vault Enterprise](#) [Documentation](#)





# hcp-root policies

- **hcp-root** policy is the policy used for the admin token generated in the HCP control panel and used to access admin namespace.
- Admin tokens with the **hcp-root** policy are not the same as root tokens with the **root** policy



# Associate policies

Upon successful authentication, the generated token will have the policies attached

A terminal window with a dark background. The title bar on the right says 'TERMINAL'. It contains two lines of text: a comment in yellow and a command in white. The command is partially enclosed by a green box.

```
# LDAP group, "sre" has "dev" & "ops" policies attached
$ vault write auth/ldap/groups/sre policies="dev, ops"
```


# Next Steps


# Next Steps



- Upcoming Schedule:

 Week 7 - Community Office Hours - Bring your questions to this week!

 Week 8 - Consuming HCP Vault webinar - Learn how to consume secrets from Vault in your apps and services

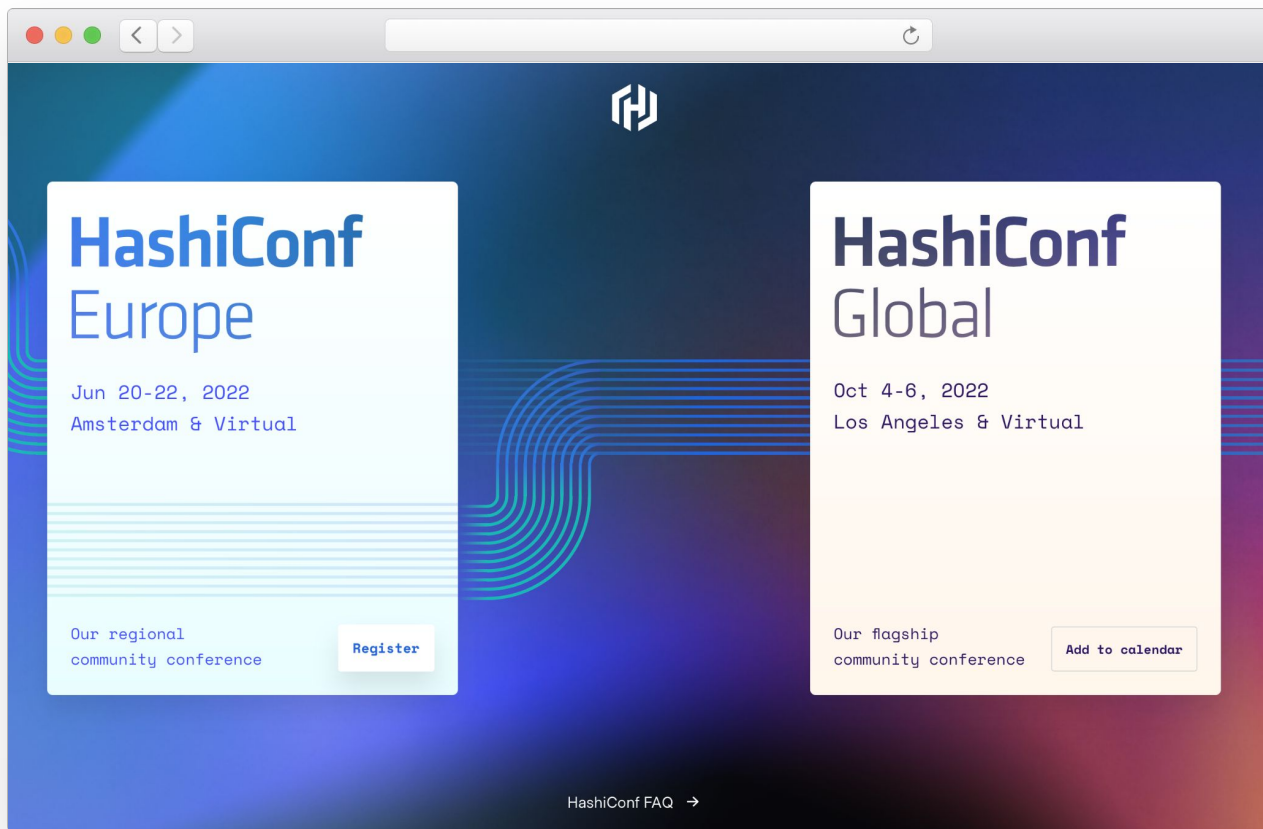
 Week 9 - HCP Vault roadmap overview and Q&A with James Bayer, EVP of Secure Product & Engineering

 Week 10 - HCP Vault train closing session



# 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
<b>About the HashiCorp Cloud Platform (HCP) category</b>			
<div>HashiCorp Cloud Platform (HCP)</div> <div>Information on HashiCorp Cloud Platform (HCP) use cases, Q&amp;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](https://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.

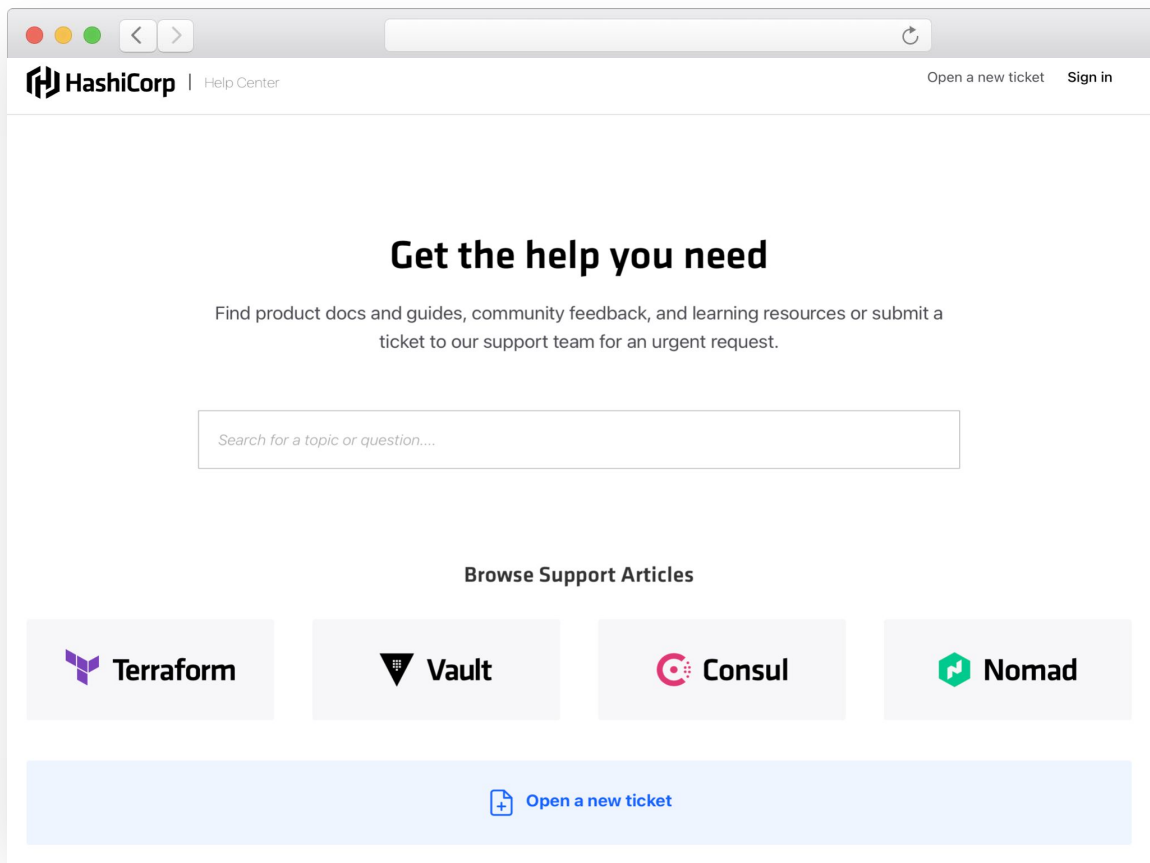
▼ ▶

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](mailto: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](#).



# Thank You

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

[www.hashicorp.com](http://www.hashicorp.com)