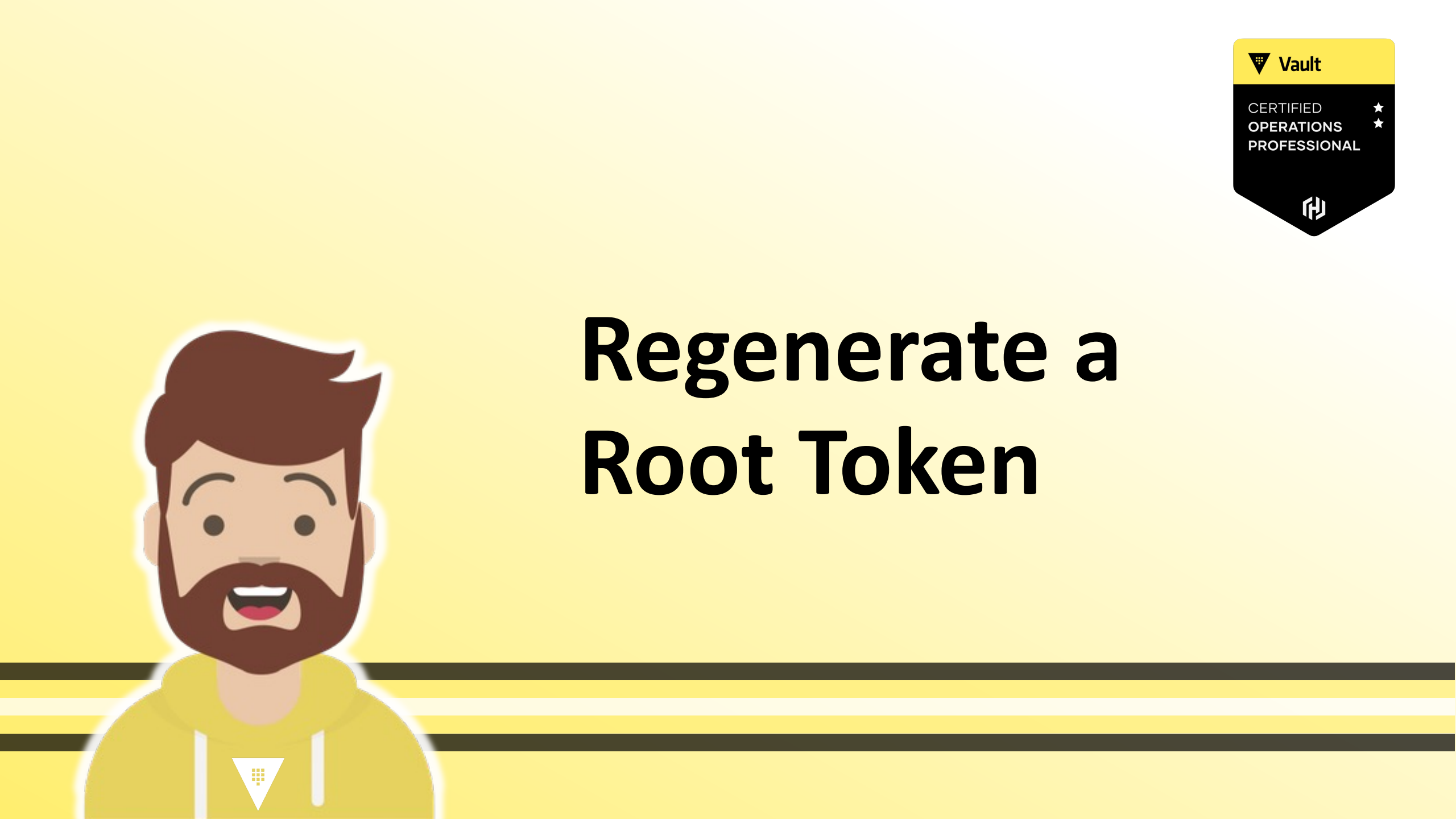


Regenerate a Root Token

About Root Tokens

Root token is a superuser that has unlimited access to Vault

- It does NOT have a TTL – meaning it does not expire
- Attached to the root policy
- Note: Root tokens can create other root tokens that DO have a TTL

Root tokens should NOT be used on a day-to-day basis

- In fact, rarely should a root token even exist
- Once you have used the root token, it should be revoked

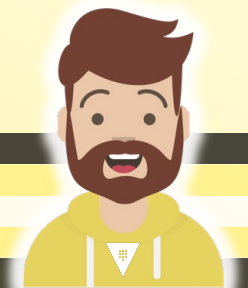
My First Root Token!

The initial root token comes from Vault cluster initialization

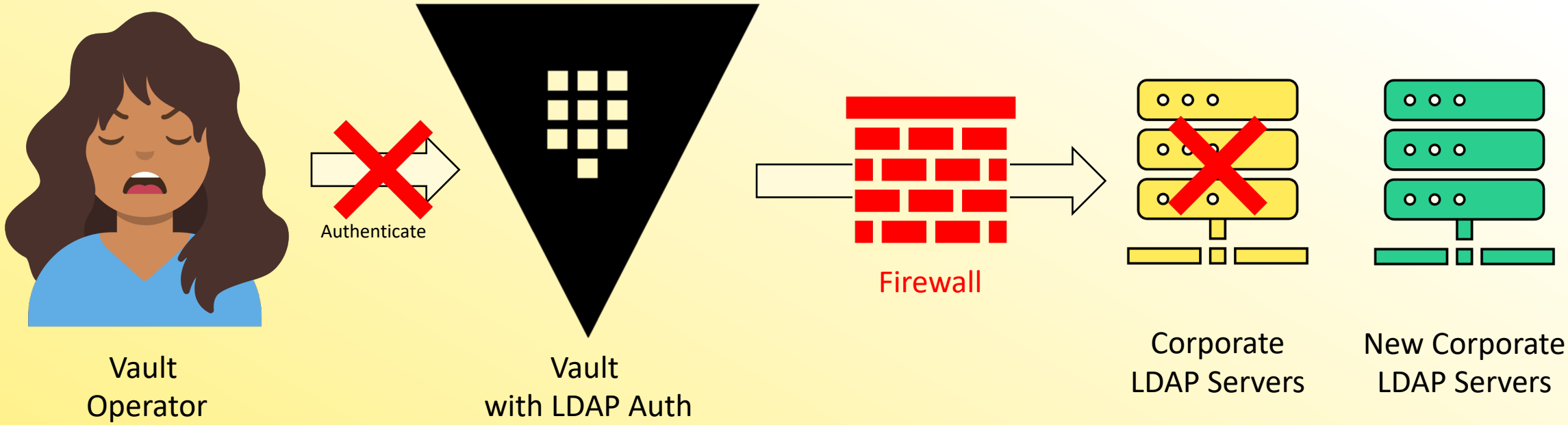
- Only method of authentication when first deploying Vault
- Used for initial configuration – such as auth methods or audit devices
- Once your new auth method is configured and tested, the root token should be revoked

Terminal

```
$ vault token revoke s.dhtIk8VsE3Mj61PuGP3ZfFrg
Success! Revoked token (if it existed)
```



A Broken Auth Workflow…



What happens if we do not have a working auth method to fix?

Regenerate a Root Token

Create a root token using unseal/recovery keys

- Helpful if you need to generate a root token in an emergency or a root token is needed for a particular task
- A quorum of key holders can generate a new root token
  - Enforces the "no single person has complete access to Vault"

Step 1

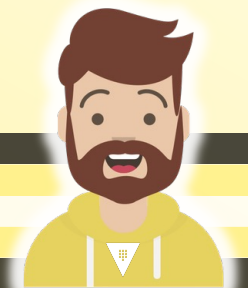
Initialize the root generation

Step 2

Each key holder runs 'generate root' with their unseal key

Step 3

Decode the generated root token



Vault Initialization

To perform the task, use the `vault operator generate-root` command

Command Options	Description
-generate-otp	Generate and print high-entropy one-time-password
-init	Start a root token generation
-decode=<string>	Decode and output the generated root token
-otp=<string>	OTP code to use with –decode or –init
-status	Print the status of the current attempt
-cancel	Cancel the current attempt

Generating a Root Token

Step 1 – Initialize the Process

Terminal

```
$ vault operator generate-root -init
A One-Time-Password has been generated for you and is shown in the OTP field.
You will need this value to decode the resulting root token, so keep it safe.

Nonce            5b6e3831-2a45-4695-7757-5810074d36c8
Started          true
Progress         0/1
Complete         false
OTP              E87jF6ZeJo8NjJwvytl7mvKLEr
OTP Length       26
```

One-Time-Password (OTP) gets generated

Generating a Root Token

Step 2 – Provide the Keys

Terminal

```
$ vault operator generate-root
Root generation operation nonce: f8579a51-5138-c31...
Unseal Key (will be hidden):
Nonce       f8579a51-5138-c319-445d-2d3640119f87
Started     true
Progress    1/3
Complete    false
```

Key holders each provide their key until you meet the threshold

Generating a Root Token

Step 3 – Receive Encrypted Token

Terminal

```
$ vault operator generate-root
Root generation operation nonce: f8579a51-5138-c319...
Unseal Key (will be hidden):
Nonce            f8579a51-5138-c319-445d-2d3640119f87
Started          true
Progress         3/3
Complete         true
Encoded Token    G2NeKUZgXTsYYxILAC9ZFBguPw9ZXBovFAs
```

Encrypted Root Token

Generating a Root Token

Step 4 – Decode the Newly Generated Root Token

Terminal

```
$ vault operator generate-root \
      -otp="hM9q24nNiZfnYIiNvhnGo4UFc3" \
      -decode="G2NeKUZgXTsYYxILAC9ZFBguPw9ZXBovFAs"

Root token: hvs.gXtT3uq9teYf0ZnFQH6hOiw8
```

We Got A Root Token!!!