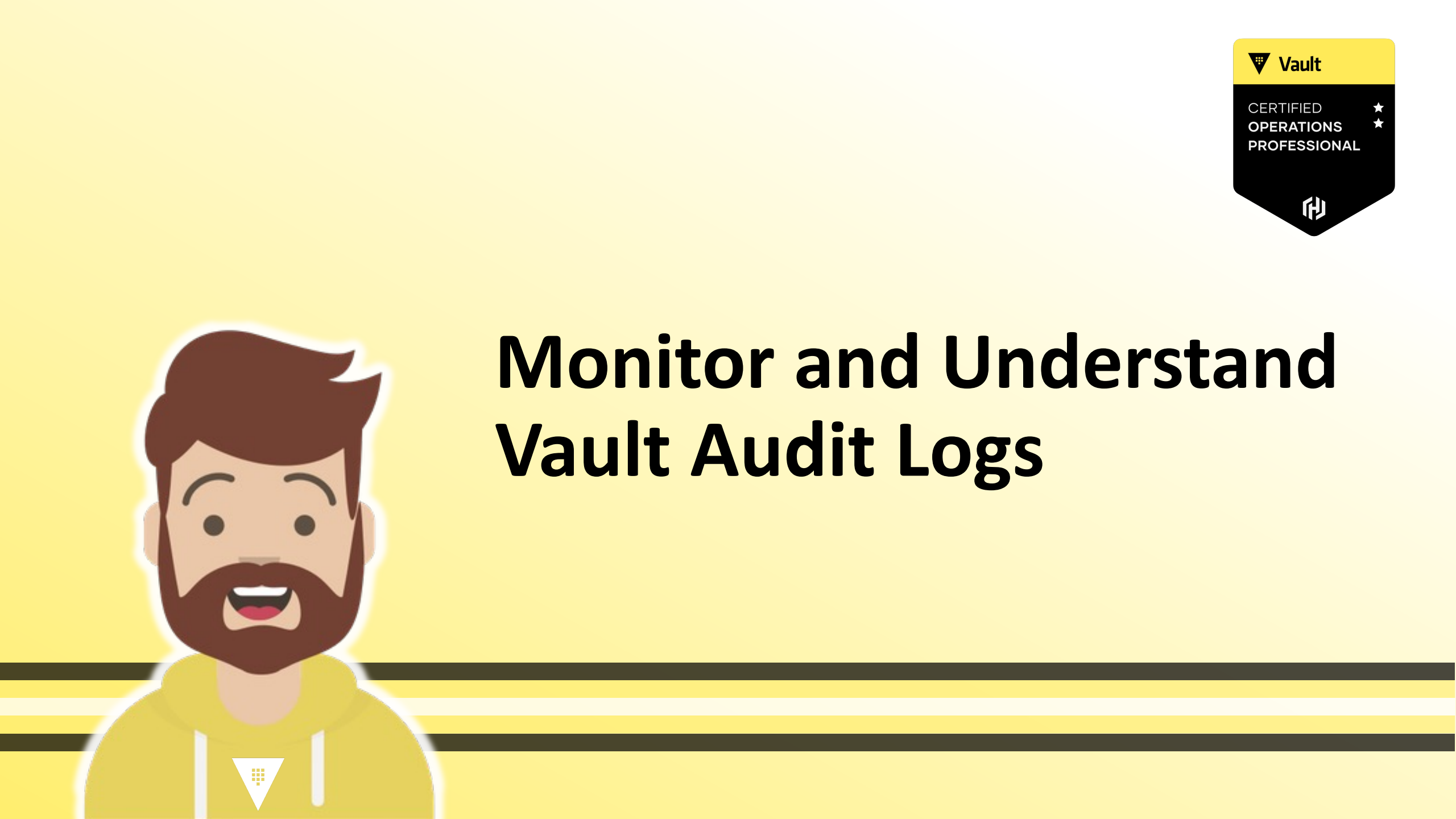


Monitor and Understand Vault Audit Logs

Introduction to Audit Devices

- Keep a detailed log of all authenticated requests and responses to Vault
- Audit log is formatted using JSON
- Sensitive information is hashed with a salt using HMAC-SHA256 to ensure secrets and tokens are never in plain text
- Log files should be protected as a user with permission can still check the value of those secrets via the /sts/audit-hash API and compare to the log file

What Audit Devices Does Vault Support?

File

- writes to a file – appends logs to the file
- does not assist with log rotation
- use fluentd or similar tool to send to collector

Syslog

- writes audit logs to a syslog
- sends to a local agent only

Socket

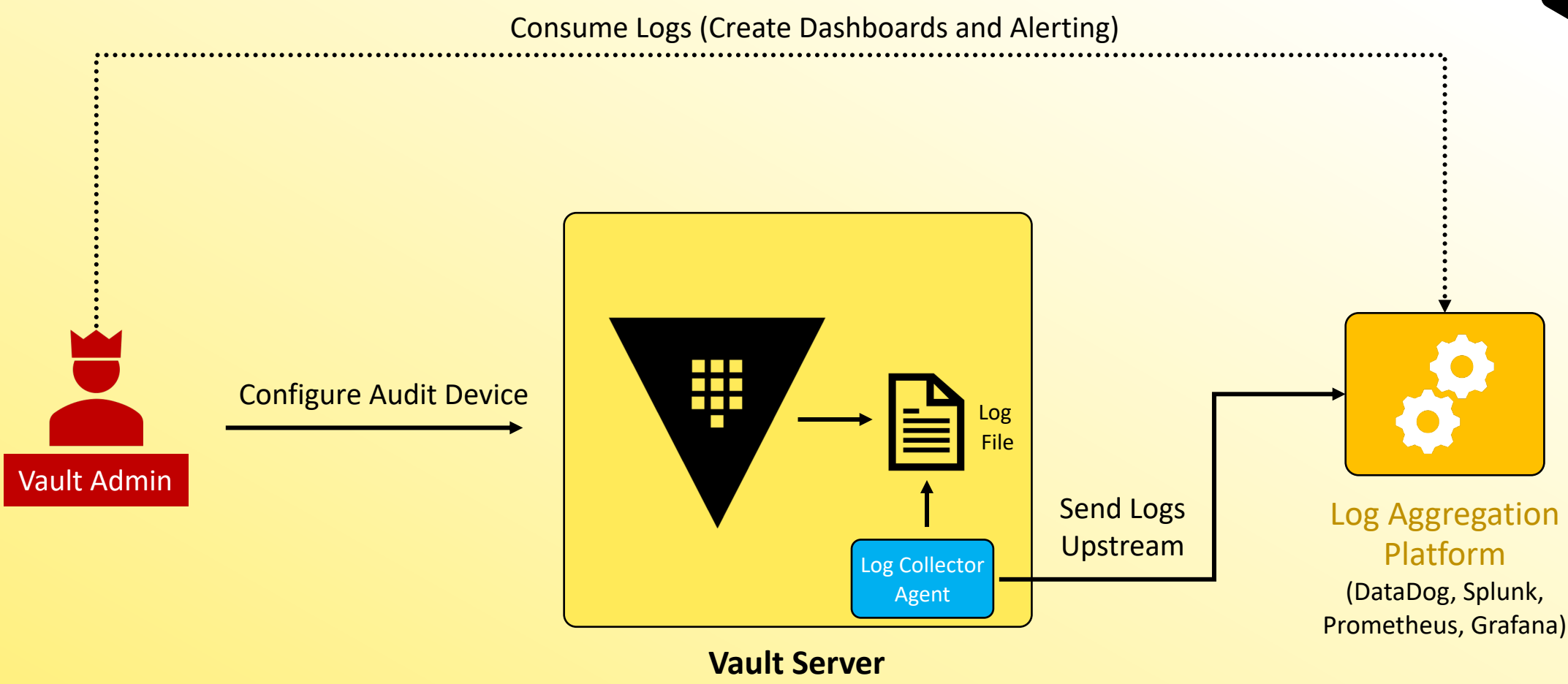
- writes to a tcp, udp, or unix socket
- TCP should be used where strong guarantees are required

Important Info about Audit Devices

- Can and should have more than one audit device enabled
- If there are any audit devices enabled, Vault requires that it can write to the log before completing the client request.
  - Prioritizes safety over availability
- If Vault cannot write to a persistent log, it will stop responding to client requests – which means Vault is down!

Vault requires at least one audit device to write the log before completing the Vault request – if enabled

Audit Log Workflow



Enabling an Audit Device

Use the `vault audit` command

Terminal

```
# Enable file audit device at default path
$ vault audit enable file file_path="/var/log/vault_audit.log
Success! Enabled the file audit device at: file/


#Enable file audit device at custom path of "logs"
$ vault audit enable -path=logs file \
   file_path="/var/log/audit.log"
Success! Enabled the file audit device at: logs/
```

Enabling an Audit Device

Use the `vault audit` command

Terminal

```
# View the audit devices currently enabled
$ vault audit list
Path     Type     Description
----     ----     -----------
file/    file     n/a
syslog/  syslog   n/a


# Disable an Audit Device
$ vault audit disable syslog/
Success! Disabled audit device (if it was enabled) at: syslog/
```

Reading an Audit Log

Terminal

```
$ cat vault_audit.log | jq

{
  "time": "2022-12-25T21:20:12.40607Z",
  "type": "response",
  "auth": {
    "client_token": "hmac-sha256:c134d4c72a6cd891102c654b0b897f3b747a3366e88b6b2fc25247bd977ec949",
    "accessor": "hmac-sha256:e307f9f20d81fc513904534d74f5dab2348a612543271f0c2f3aa1eafe951576",
    "display_name": "root",
    "policies": [
      "root"
    ],
    "token_policies": [
      "root"
    ],
    "token_type": "service",
    "token_issue_time": "2022-12-25T11:07:35-04:00"
  },
  "request": {
    "id": "96801004-f2a5-a994-bc7a-0b15e3739db9",
    "operation": "update",
```

Permissions Needed for Audit Devices

If you need to work with an Audit Device, you need a root token or `sudo` privileges (plus the capabilities you need for the action) on the specific path

Terminal

```
# Required Permissions for interacting with the file audit device
at the default path of file/
path "sys/audit/file" {
  capabilities = ["read","create","list","update","delete","sudo"]
}
```