Vault

Implementation Foundations

Module: Vault Configuration

What You Will Learn

Vault Configuration

- Overview
- Configuration Blocks
    - Listener
    - Storage
    - Secure Connections

Starting Vault

- Vault Initialization
- Vault Seal Keys
- Vault Root Token

Vault Configuration Overview

HashiCorp Vault Configuration

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

Base Vault Configuration

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

The storage stanza configures the durable storage backend

Configuration - Storage Stanza

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

Configuration - Storage Address

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

The IP/hostname of the storage

Configuration - Path

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

The Key-Value write path for the backend storage

Configuration - Listener

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

The listener stanza configures what address Vault should listen on

Configuration - Listener Address

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

The address and ports on which Vault will respond to requests

Configuration - TLS

```
storage "consul" {
  address = "127.0.0.1:8500"
  path    = "vault"
}

listener "tcp" {
  address     = "127.0.0.1:8200"
  tls_disable = "false"
}
```

Note: Vault assumes TLS is enabled by default

Example Listener Configuration

```
listener "tcp" {
  address            = "127.0.0.1:8200"
  tls_disable        = "false"
  tls_cert_file      = "/etc/tls/mycertfile"
  tls_key_file       = "/etc/tls/mykeyfile"
  tls_client_ca_file = "/etc/tls/my_client_ca"
}

api_addr = "https://10.0.0.5:8200"
cluster_addr = "https://10.0.0.5:8201"
```

Example Listener Configuration - Address

```
listener "tcp" {
  address            = "127.0.0.1:8200"
  tls_disable        = "false"
  tls_cert_file      = "/etc/tls/mycertfile"
  tls_key_file       = "/etc/tls/mykeyfile"
  tls_client_ca_file = "/etc/tls/my_client_ca"
}

api_addr = "https://10.0.0.5:8200"
cluster_addr = "https://10.0.0.5:8201"
```

Example Listener Configuration - TLS

```
listener "tcp" {
  address            = "127.0.0.1:8200"
  tls_disable        = "false"
  tls_cert_file      = "/etc/tls/mycertfile"
  tls_key_file       = "/etc/tls/mykeyfile"
  tls_client_ca_file = "/etc/tls/my_client_ca"
}

api_addr = "https://10.0.0.5:8200"
cluster_addr = "https://10.0.0.5:8201"
```

Remember: TLS is enabled by default

Example Listener Configuration - TLS Cert, Key, CA

```
listener "tcp" {
  address            = "127.0.0.1:8200"
  tls_disable        = "false"
  tls_cert_file      = "/etc/tls/mycertfile"
  tls_key_file       = "/etc/tls/mykeyfile"
  tls_client_ca_file = "/etc/tls/my_client_ca"
}

api_addr = "https://10.0.0.5:8200"
cluster_addr = "https://10.0.0.5:8201"
```

Used for checking the authenticity of client

Example Listener Configuration - API Address

```
listener "tcp" {
  address          = "127.0.0.1:8200"
  tls_disable      = "false"
  tls_cert_file    = "/etc/tls/mycertfile"
  tls_key_file     = "/etc/tls/mykeyfile"
  tls_client_ca_file = "/etc/tls/my_client_ca"
}

api_addr = "https://10.0.0.5:8200"
cluster_addr = "https://10.0.0.5:8201"
```

Specifies the address to advertise to other Vault servers in the cluster for client redirection

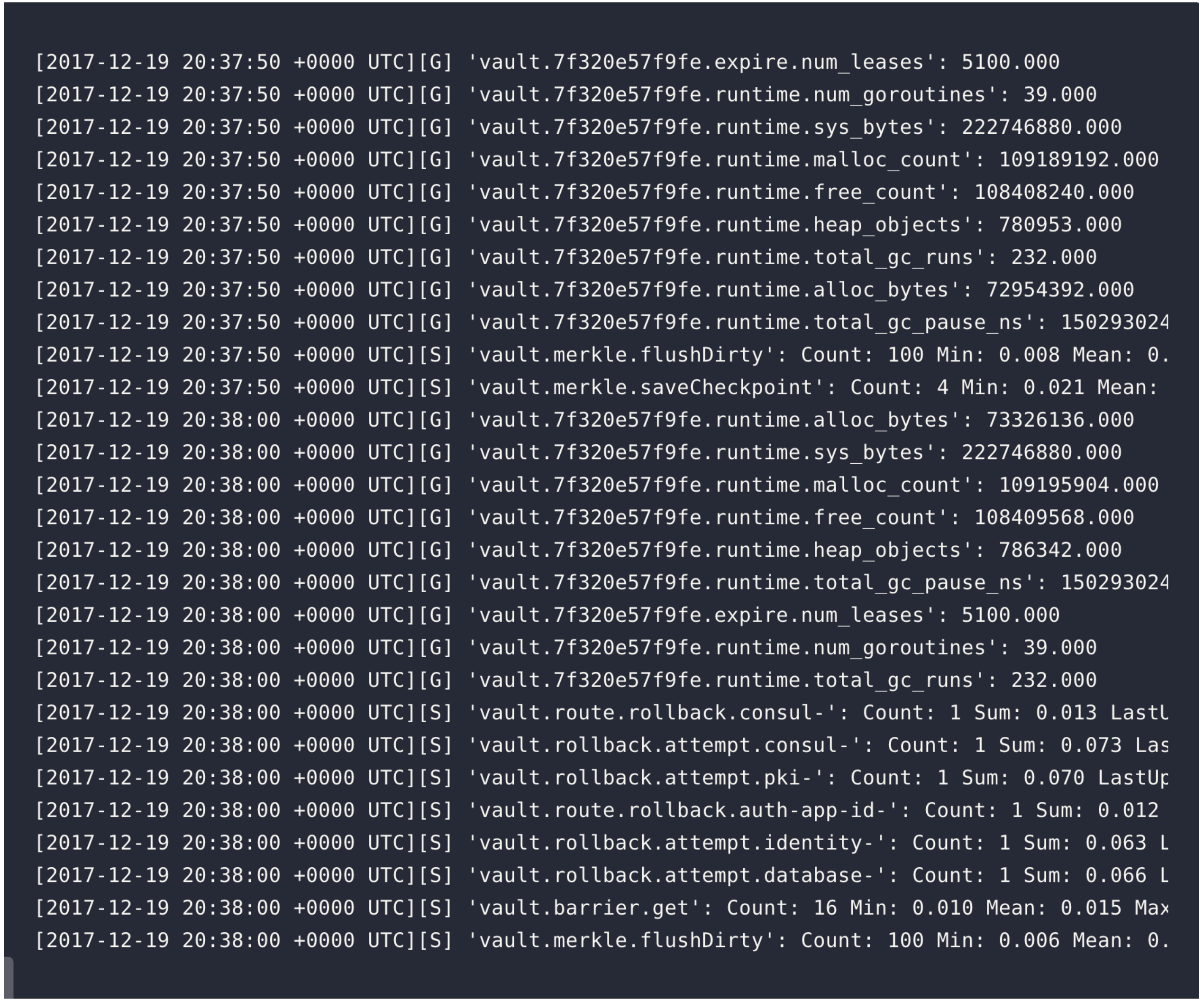
Example Listener Configuration - Cluster Address

```
listener "tcp" {
  address            = "127.0.0.1:8200"
  tls_disable        = "false"
  tls_cert_file      = "/etc/tls/mycertfile"
  tls_key_file       = "/etc/tls/mykeyfile"
  tls_client_ca_file = "/etc/tls/my_client_ca"
}

api_addr = "https://10.0.0.5:8200"
cluster_addr = "https://10.0.0.5:8201"
```

Specifies the address to advertise to other Vault servers in the cluster for request forwarding

Vault Telemetry



```
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.expire.num_leases': 5100.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.num_goroutines': 39.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.sys_bytes': 222746880.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.malloc_count': 109189192.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.free_count': 108408240.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.heap_objects': 780953.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.total_gc_runs': 232.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.alloc_bytes': 72954392.000
[2017-12-19 20:37:50 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.total_gc_pause_ns': 150293024
[2017-12-19 20:37:50 +0000 UTC][S] 'vault.merkle.flushDirty': Count: 100 Min: 0.008 Mean: 0.
[2017-12-19 20:37:50 +0000 UTC][S] 'vault.merkle.saveCheckpoint': Count: 4 Min: 0.021 Mean:
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.alloc_bytes': 73326136.000
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.sys_bytes': 222746880.000
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.malloc_count': 109195904.000
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.free_count': 108409568.000
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.heap_objects': 786342.000
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.total_gc_pause_ns': 150293024
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.expire.num_leases': 5100.000
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.num_goroutines': 39.000
[2017-12-19 20:38:00 +0000 UTC][G] 'vault.7f320e57f9fe.runtime.total_gc_runs': 232.000
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.route.rollback.consul-': Count: 1 Sum: 0.013 LastU
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.rollback.attempt.consul-': Count: 1 Sum: 0.073 Las
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.rollback.attempt.pki-': Count: 1 Sum: 0.070 LastUp
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.route.rollback.auth-app-id-': Count: 1 Sum: 0.012
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.rollback.attempt.identity-': Count: 1 Sum: 0.063 L
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.rollback.attempt.database-': Count: 1 Sum: 0.066 L
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.barrier.get': Count: 16 Min: 0.010 Mean: 0.015 Max
[2017-12-19 20:38:00 +0000 UTC][S] 'vault.merkle.flushDirty': Count: 100 Min: 0.006 Mean: 0.
```

Telemetry Setup

```
telemetry {
  statsd_address = "statsd.company.local:8125"
}
```

Once a telemetry block has been configured Vault will begin to stream out data

Telemetry - Common Values

- `usage_gauge_period = "10m"`
- `maximum_gauge_cardinality = 500`
- `disable_hostname = false`
- `enable_hostname_label = false`
- `lease_metrics_epsilon = "1hr"`
- `num_lease_metrics_buckets = 168`
- `add_lease_metrics_namespace_labels = false`
- `filter_default = true`
- `prefix_filter = ["+vault.token", "-vault.expire"]`

Initializing Vault

Installing Vault

1. Download and Install Vault
2. Configure Vault
3. Configure systemd/upstart/windows service
4. Start Vault
5. Vault Init
6. Unseal Vault

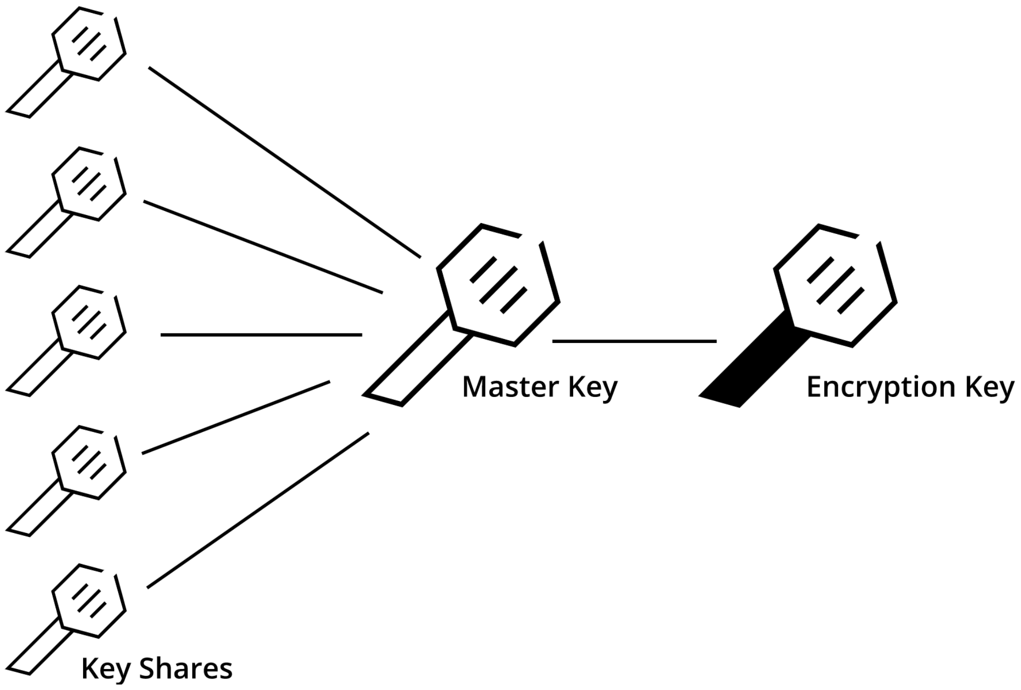
Operator init Command

- The `init` command initializes a Vault server
- Generates in-memory master key
- Generates a seal key
- Generates a root token

Seal Overview

- Vault starts in a sealed state
- Data is encrypted at rest
  - When sealed Vault knows where the data is
  - But doesn't know how to decrypt any of it

Shamir's Secret Sharing Algorithm



The default unseal method for Vault is Shamir's Secret Sharing Algorithm

Chapter Summary

- Vault's storage configuration operations
- Tuning Vault with various listener configs
- Common tunable options that are important
- Getting started commands

Reference links

- Getting Start with Vault
- Starting the Vault
- Telemetry Data

Vault Configuration Module Complete!