Vault

Implementation Foundations

Module 7 : Deployment Automation

What You Will Learn

Provisioning Infrastructure

- Installation
- Configuration As Code
- Vault Automation Process
- Pipeline Summary
- Routine Automation

Deployment Automation

Vault Automation Considerations

Provisioning Infrastructure

- Terraform
- Native tools (CF, GDM, ARM, VRA/VRo)

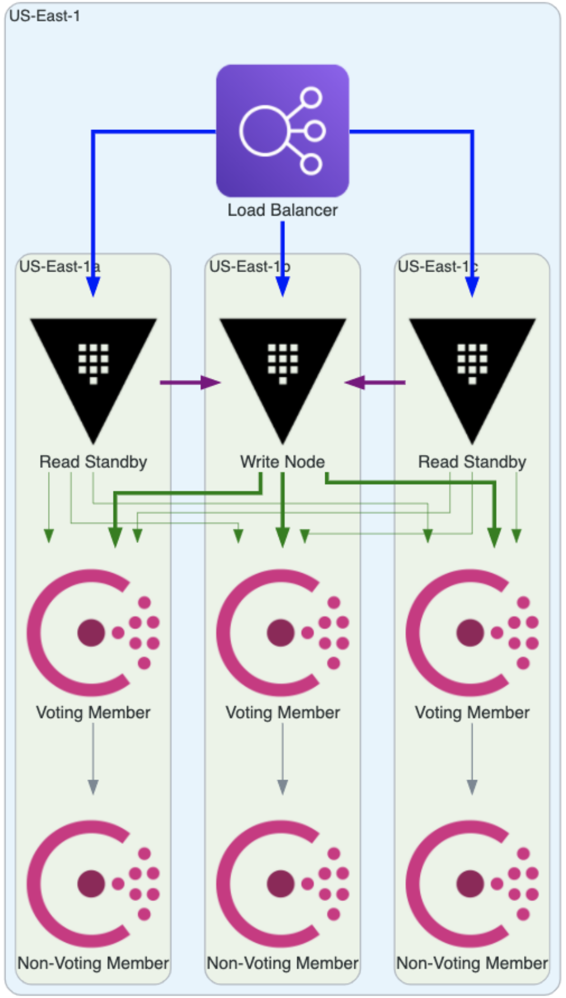
Installation

- Packer, Chef, Puppet, Ansible, SALT

Configuration as Code

- Vault TFE Provider
- Vault API

Provisioning Tasks

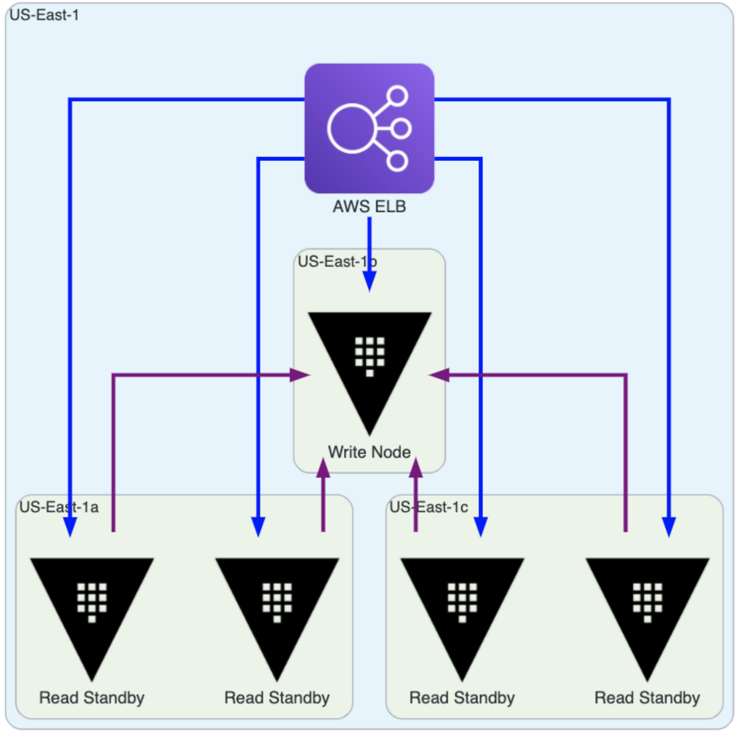


- Load Balancer
- Server Specifications
- Network Connectivity

Provisioning Check List (Consul)

- Load Balancer
- 3 Vault Frontend Entities (Hardware, VM, Container)
- 5 Consul Backend Entities (Hardware, VM, Container)
- Network Configuration
  - Intra-cluster Requirements
  - Inbound Traffic Configuration
  - Replication Configuration

Provisioning Tasks (Integrated Storage)

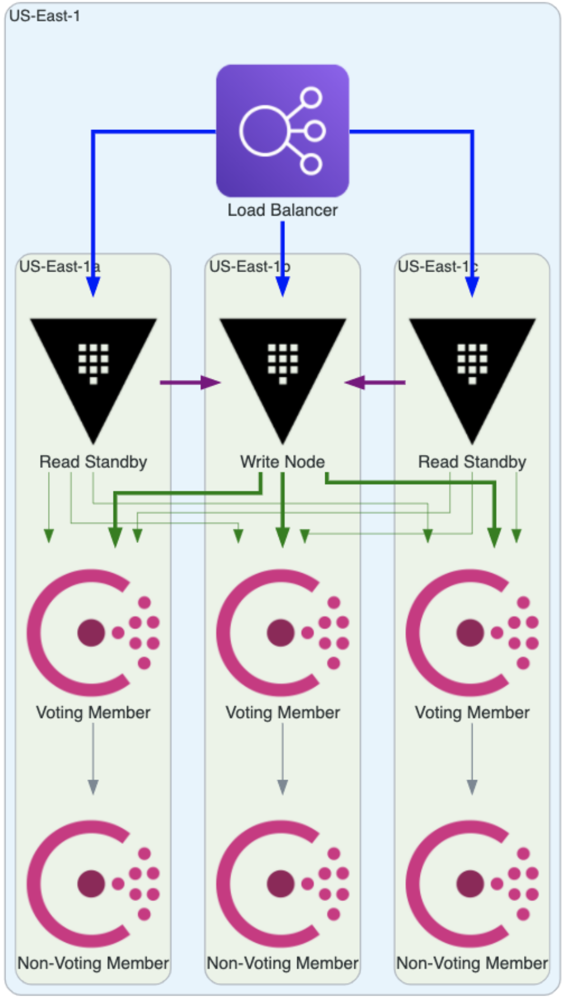


- Load Balancer
- Server Specifications
- Network Connectivity

Provisioning Check List (Integrated Storage)

- Load Balancer
- 5 Vault Entities (Hardware, VM, Container)
- Network Configuration
  - Intra-cluster Requirements
  - Inbound Traffic Configuration
  - Replication Configuration

Installation Tasks (Consul)



- Install Consul Server
- Install Consul Agent
- Install Vault

Install Check List (Consul)

- Download Vault to 3 Frontends
- Download Consul to all 8 Entities
- Install Consul on all 8 Entities
- Configure Consul
- Start Consul
- Install Vault on 3 Frontends
- Configure Vault
- Start Vault

Install Check List (Integrated Storage)

- Download Vault to 5 Servers
- Install Vault on 5 Servers
- Configure Vault
- Start Vault

Configuration Tasks - API

Once Vault is started and ready to be initialized all of Vault's capabilities are accessible via the HTTP API in addition to the CLI.

When invoking the API, authentication is still required

Important API Endpoints

- **/sys/init** - used to initialize a new Vault.
- **/sys/unseal** - used unseal the Vault
- **/sys/license** - endpoint for license management
- **/sys/health** - health checking and status information for Vault
- **/sys/mounts** - used to manage all secret engines within Vault
- **/sys/policies** - used to manage all policies within Vault
- **/sys/replication** - for tuning, managing and changing replication topologies

Configuration Check List

- Initialize Vault
  - `vault operator init`
  - Specify encryption keys
  - Specify number of secret shares
  - Specify key qourum size
  - Specify recovery keys (shares, threshold)
- Unseal Vault - **Manual**
  - Does **NOT** require authentication

Key Management System Unseal

Vault supports opt-in automatic unsealing via KMS:

- AliCloud KMS

Key Management System Unseal

Vault supports opt-in automatic unsealing via KMS:

- AliCloud KMS
- Amazon KMS

Key Management System Unseal

Vault supports opt-in automatic unsealing via KMS:

- AliCloud KMS
- Amazon KMS
- Azure Key Vault

Key Management System Unseal

Vault supports opt-in automatic unsealing via KMS:

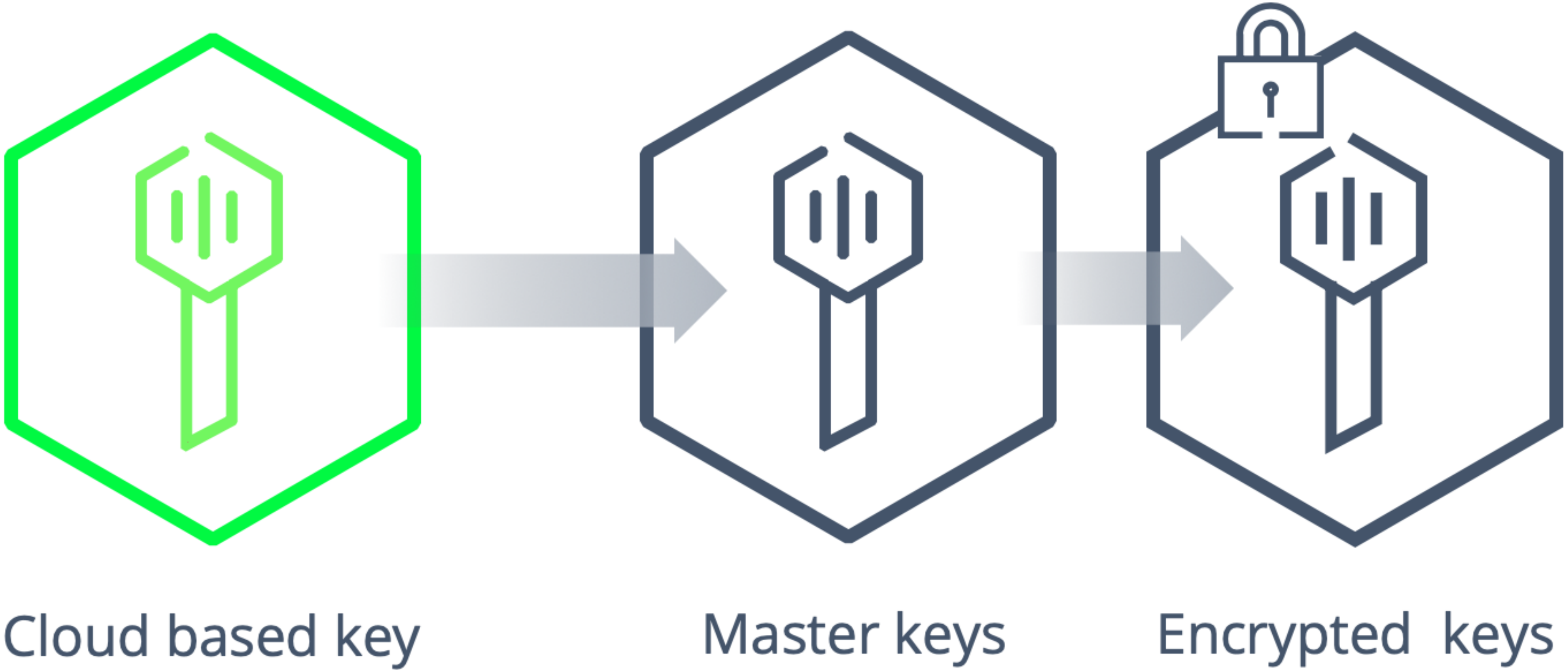
- AliCloud KMS
- Amazon KMS
- Azure Key Vault
- Google Cloud KMS

Key Management System Unseal

Vault supports opt-in automatic unsealing via KMS:

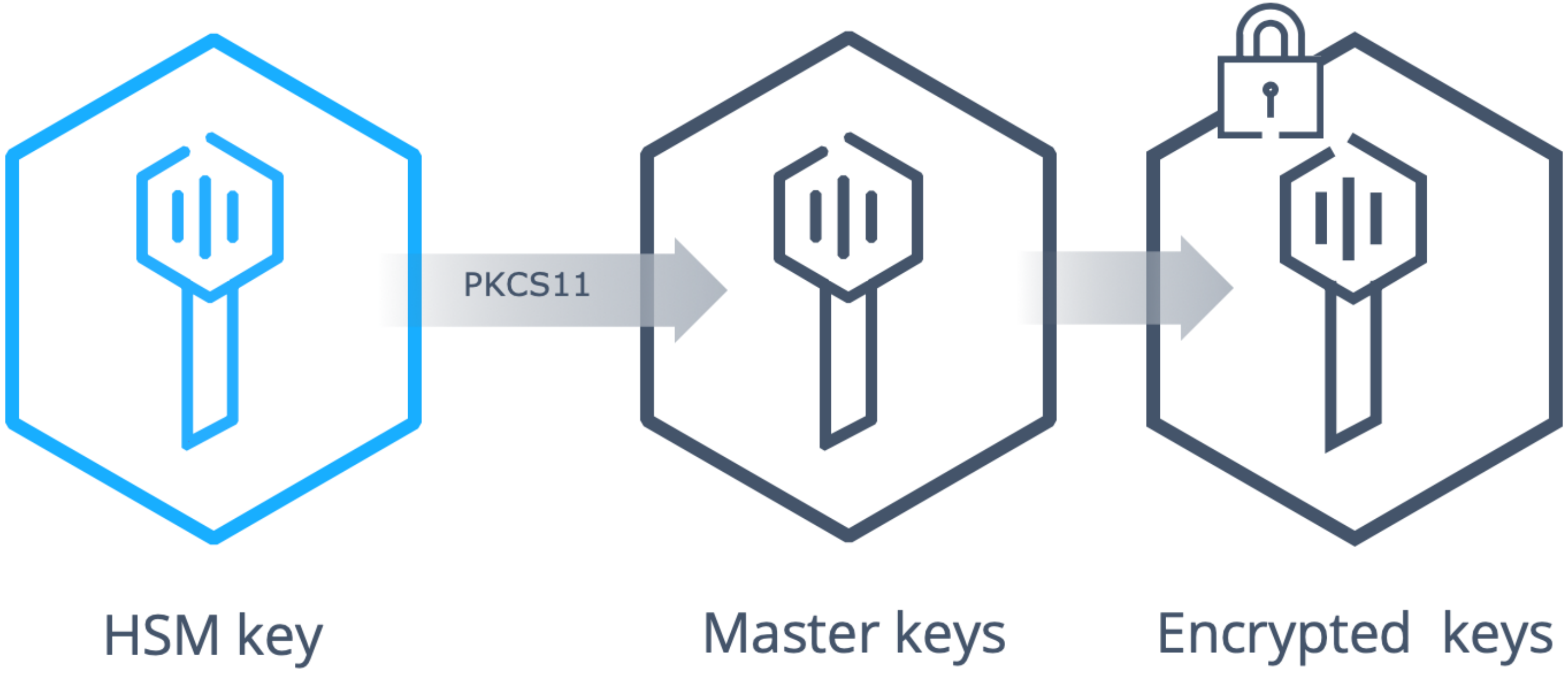
- AliCloud KMS
- Amazon KMS
- Azure Key Vault
- Google Cloud KMS
- Vault Transit Unseal

Key Management System Diagram



HSM Unseal

Vault stores its HSM-wrapped master key in storage, allowing for automatic unsealing



Turning On Audit

Audit devices are the components in Vault that keep a detailed log of all requests and response to Vault

Audit Devices:

- File
- Syslog
- Socket

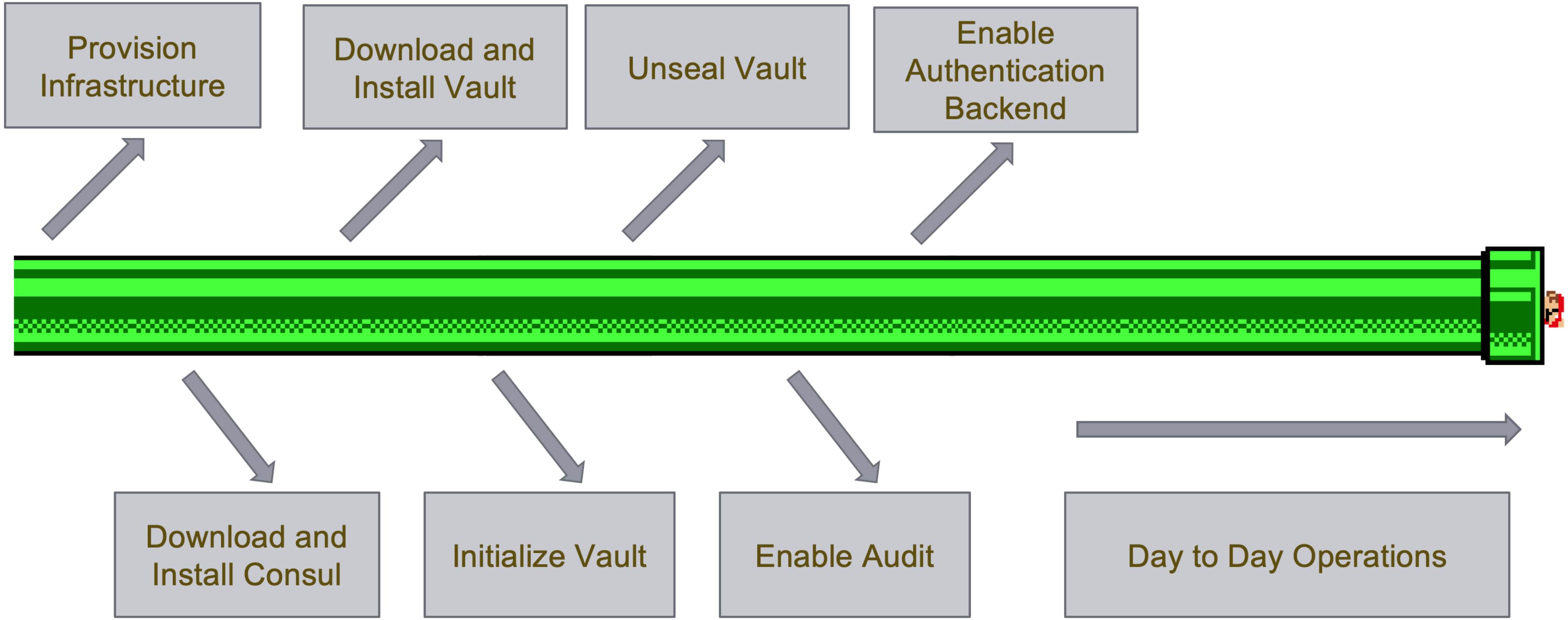
Enabling Authentication Backend

Commonly considered the final **setup** step for a Vault Cluster this step may be considered optional.

Authentication Methods:

- LDAP
- Cloud IAM
- Github
- Okta
- MORE!

Pipeline Overview



Provision Infrastructure

Download and Install Consul

Download and Install Vault

Initialize Vault

Unseal Vault

Enable Audit

Enable Authentication Backend

Day to Day Operations

Chapter Summary

- Identify all of the components to automate with Vault:
  - Infrastructure
  - Components
  - Configuration
  - Services
- One time events:
  - Initialization
  - Unseal
  - Enable Auth
  - Enable Audit devices
- API Capabilities

Reference links

- Vault API Documentation
- Using the API
- Auth API
- Sys API Endpoint

Vault Deployment Automation Module Complete!