# Vault

## Implementation Foundations

# Module : Vault Deployment Guidelines

# What You Will Learn

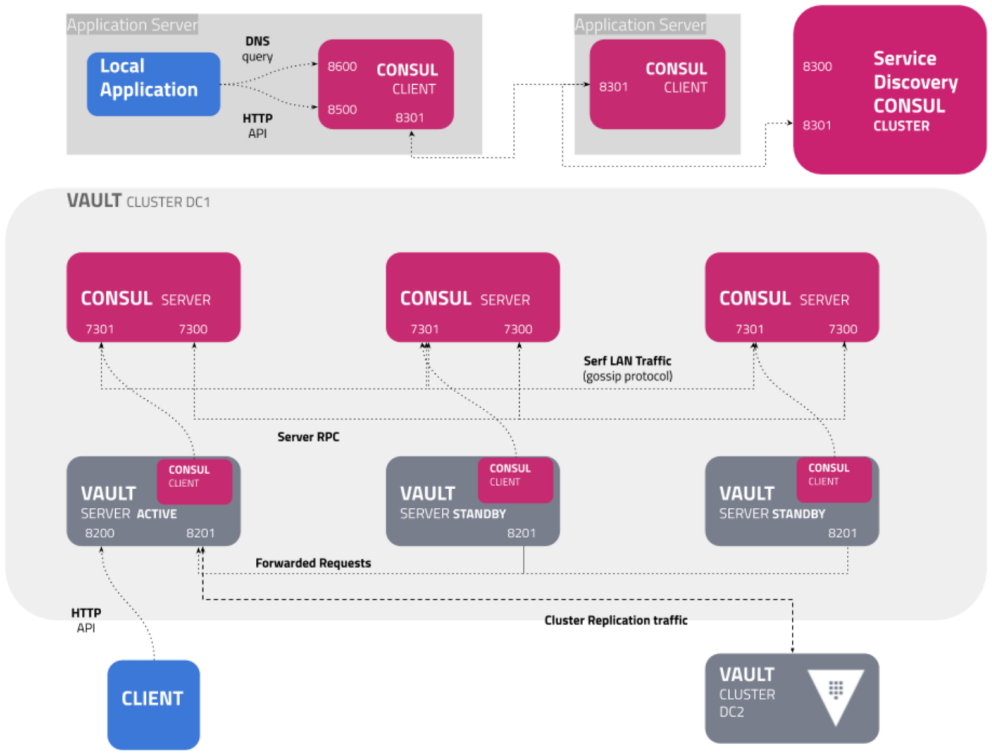
- Vault Production Deployment Best Practices
- Vault Deployment Considerations
- Vault Deployment Security Model
- Consul Storage Security Model

# Production Best Practices

# Things to Consider

| Location | Infrastructure | Security |
| --- | --- | --- |
| • Public vs. Private<br>• Availability Zone Strategy | • Physical vs. Virtual<br>• Platform Support<br>• Sizing Requirements<br>• Network Requirements | • Risk Assesment<br>• Security Model<br>• Production Hardening |

# Vault Single Region Deployment




Reference architecture of a single Vault cluster deployment with consul

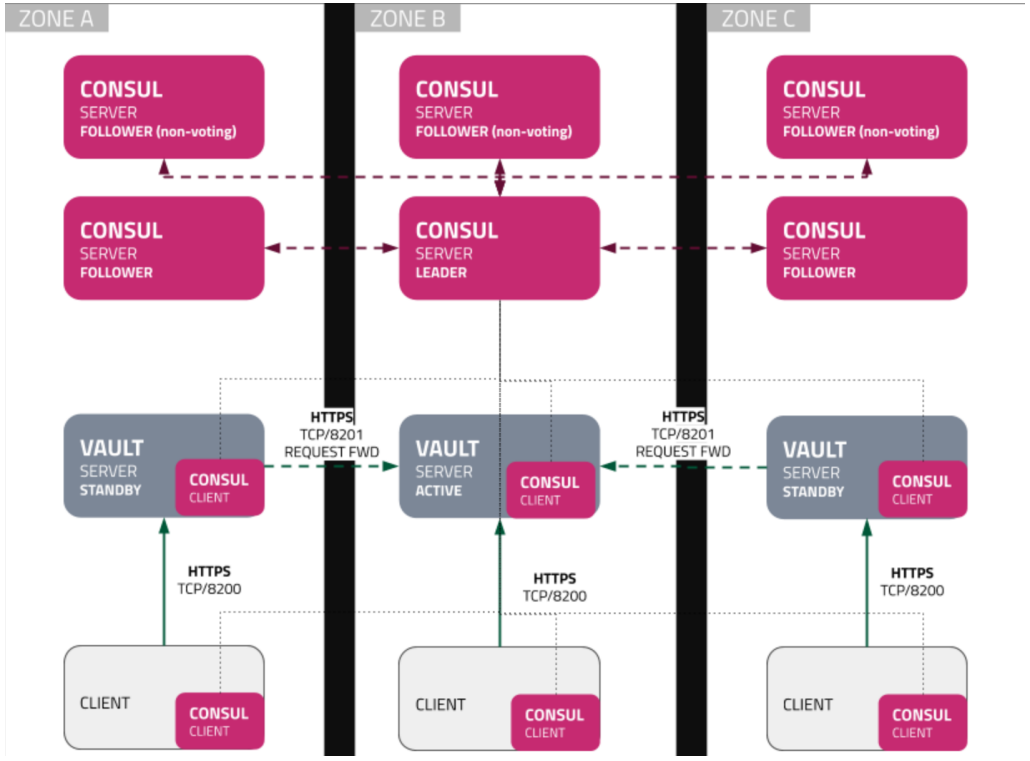
# Public vs Private Considerations

## Private

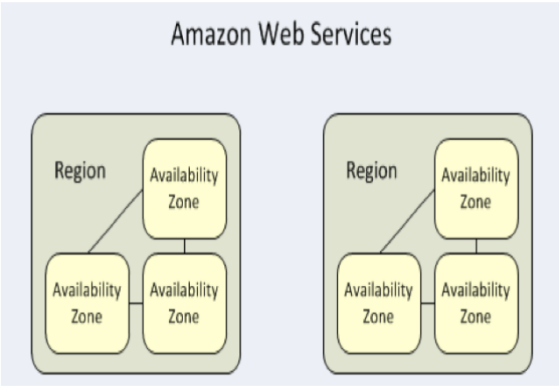
- vSphere Clustering

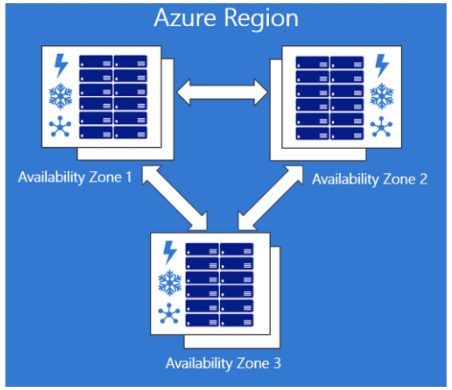
## Public

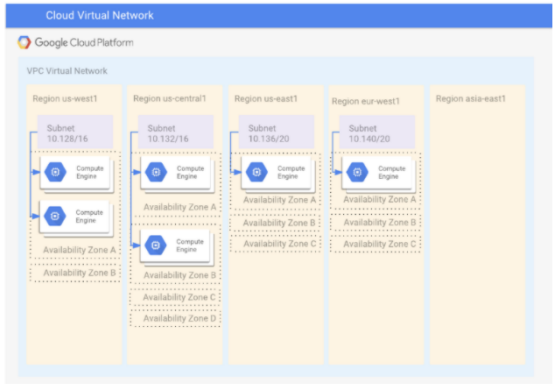
- Availability Zones
- Cross Region Connectivity
- Failure Topology



# Selecting Your Deployment Region




AWS

Azure

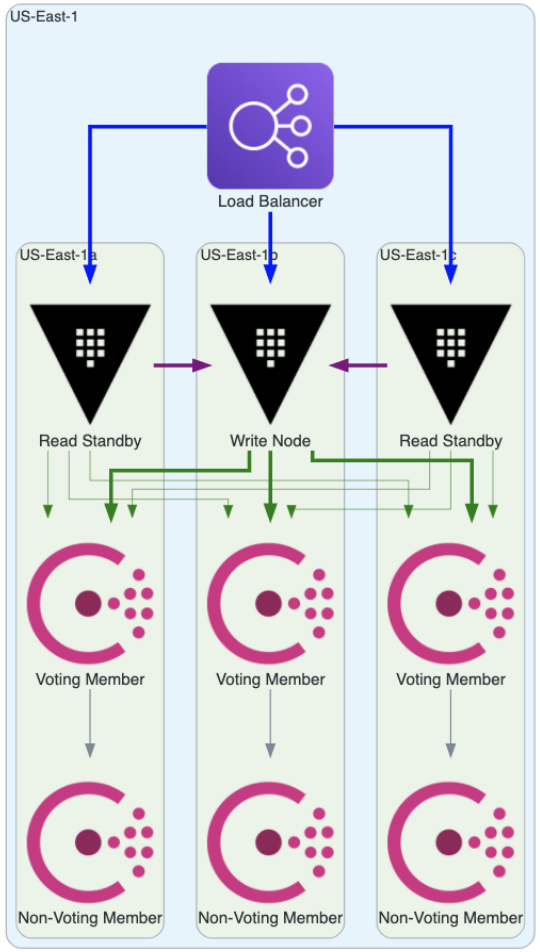
GCP

# Redundant Deployment - Consensus

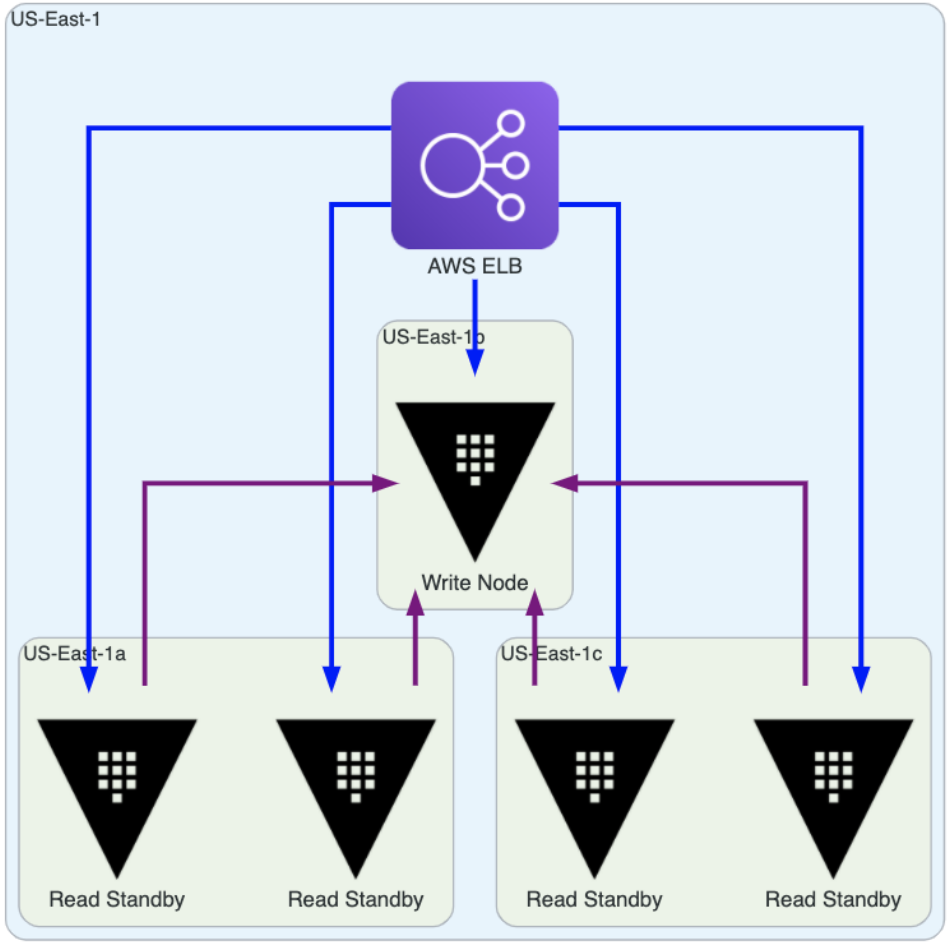
| Servers | Quarum Size | Failure Tolerance |
|---|---|---|
| 1 | 1 | 0 |
| 2 | 2 | 0 |
| 3 | 2 | 0 |
| 4 | 3 | 1 |
| 5 | 3 | 2 |
| 6 | 4 | 2 |
| 7 | 4 | 3 |

This applies to both consul and vault native storage options

# Multi-AZ Deployment - Consul Storage



# Multi-AZ Deployment - Integrated Raft



# Hardware vs Virtual vs Container

| Hardware | Virtual | Container |
| --- | --- | --- |
| • Best level of security<br>• Limits to on premise resources or expensive cloud options | • Universal Standard<br>• Cost Optimization<br>• Supported Automation Methods | • Service Management<br>• Supported Automation Methods |

# Vault Backend Storage Model

## HashiCorp Consul

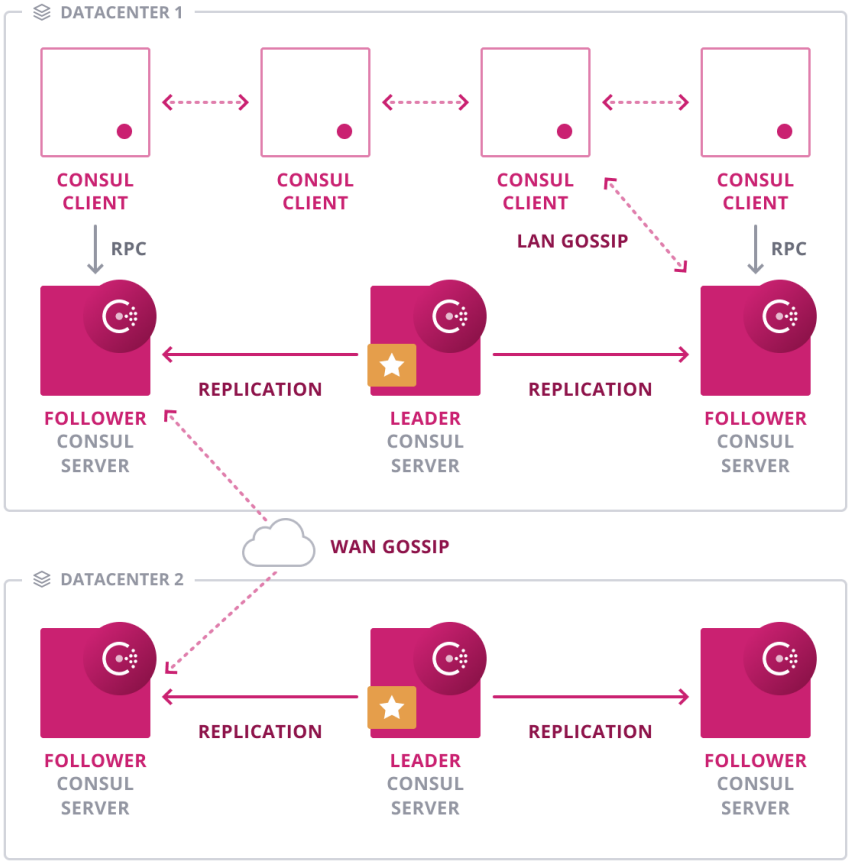
- Supports high availability
- Robust distributed storage engine
- Supports multiple data centers

## Vault Native Storage

- Available in Vault 1.4 and higher
- Reduces operational surface area
- Reference architecture pending
- Based on Consul storage engine

# Vault Security Model

# Vault Storage - Security Model




Consul Storage

- All agent communication is done via the Gossip Protocol
- This traffic is handed by Serf which uses symmetric keys for encrypting communications between agents
- The RPC system uses TLS for end-to-end encryption between Consul client and server

# Vault Storage - Consul ACL

- Consul provides a robust ACL system to authenticate and authorize access
- Vault servers use an ACL token to access the storage backend
- Vault encrypts the data before it writes it to the KV store
- Protects against accidental or malicious data corruption or deletion
- Best practice is to have ACLs in place before standing up the vault servers

# Consul Best Practices

- ACLs should be enabled with a default Deny All policy
- Encryption should be enabled
  - TLS should be used for agent to server communication
  - The `verify_outgoing` flag should be enabled and each server should have a unique TLS certificate
  - The `verify_incoming_rpc` flag should be enabled and each server should have a unique TLS certificate
- This combination of ACLs and TLS provides a robust security model for consul

# Vault Production Hardening

- End-to-End TLS
- Single Tenancy
- Firewall Traffic
- Disable SSH (RDP)
- Enable memory locking (mlock)
- Disable Swap
- Don't Run as root
- Turn core dumps off
- Immutable Upgrades
- Good Root Token management

# Platform Optimization

## Vault Officially Supported Platforms

- AWS Marketplace
- Terraform Provider
- Docker container
- Helm Chart

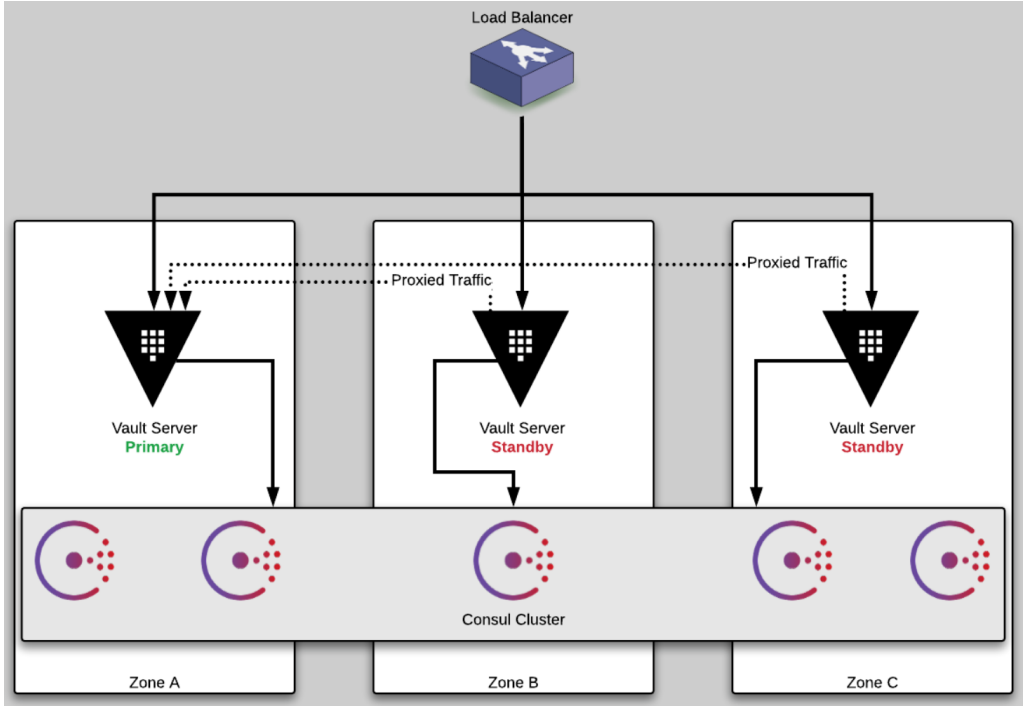
## Vault Community Supported Platforms

- Chef/Puppet/Ansible/Salt
- Openshift/Openstack

# Vault Load Balancing - Consul

- Consul can provide load balancing capabilities
- Achieved through native integration with Consul service discovery
- It requires that any Vault clients are Consul aware
- Example Access via URL:
  - `http://active.vault.service.consul:8200`

# External Load Balancing




Note:

- Poll the sys/health endpoint to detect active node
- Prefer L4 over L7 load balancing
- If L7 required, must terminate TLS on Vault

# Chapter Summary

- What to Think About when Deploying Vault
  - Deployment Location
  - Hardware, Virtual, Container
  - Load Balancer Management
- The Various Security Considerations
- Platform Native Support Capabilities

# Reference Links

- Vault Security Models
- Vault Architecture
- Vault Reference Architecture
- Vault Deployment Guide
- Consul Security Model

# Vault Deployment Guide Module Complete!