Vault

Implementation Foundations

HashiCorp Enterprise Academy

Module 6 : Enterprise Replication

What You Will Learn

Vault Replication Overview

- Overview
- Terminology
- RTO, RPO and BCP
- Scoping Vault Deployments

Vault DR Replication

- Disaster Recovery Replication
- Steps for Disaster Recovery
- Post Disaster Recovery

Performance Replication

- Performance Recovery Topology
- Performance Recovery Specifications
- The Difference Between DR and PR

Inter-Cluster Replication Overview

Replication Design Parameters

Many organizations have infrastructure that spans multiple data centers, clouds and geographical regions.

Their design patterns rely on specific requirements around the availability and consistency of their services

They are typically measured on these requirements:

- **R**ecovery **P**oint **O**jective (**RPO**)
- **R**ecovery **T**ime **O**jective (**RTO**)
- **B**usiness **C**ontinuity **P**lan (**BCP**)

What Are RTO, RPO & BCP?

- **RTO:** The amount of time the business can be without the service, without incurring significant risks or significant losses.

- **RPO:** Maximum time period in which recent data may be permanently lost in the event of a major incident.

- **BCP:** The process of creating systems of prevention and recovery to deal with potential threats to a company.

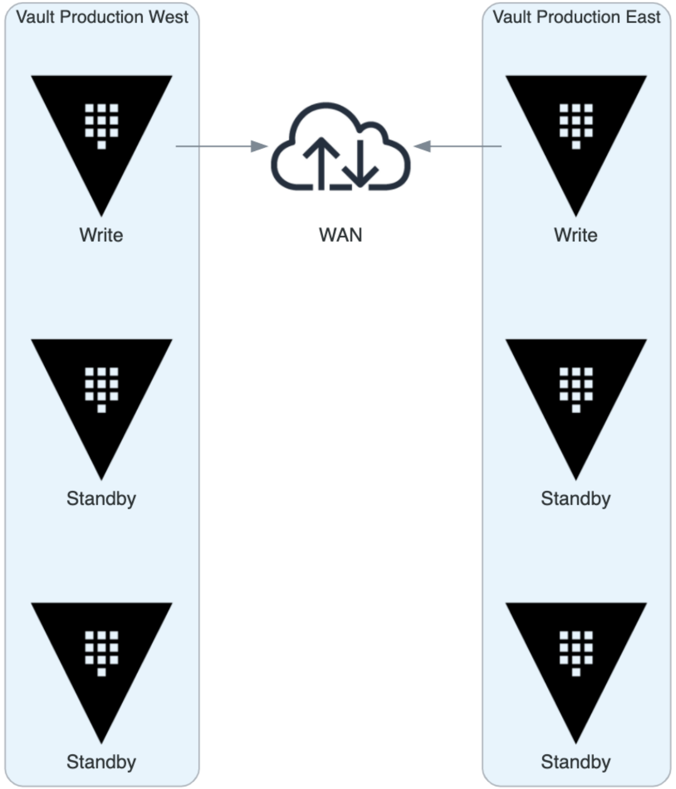
Vault Replication

- The purpose of Vault replication is to meet the RTO, RPO and BCP requirements of our customers.

- Vault replication addresses these needs in providing consistency, scalability, and highly-available disaster recovery.

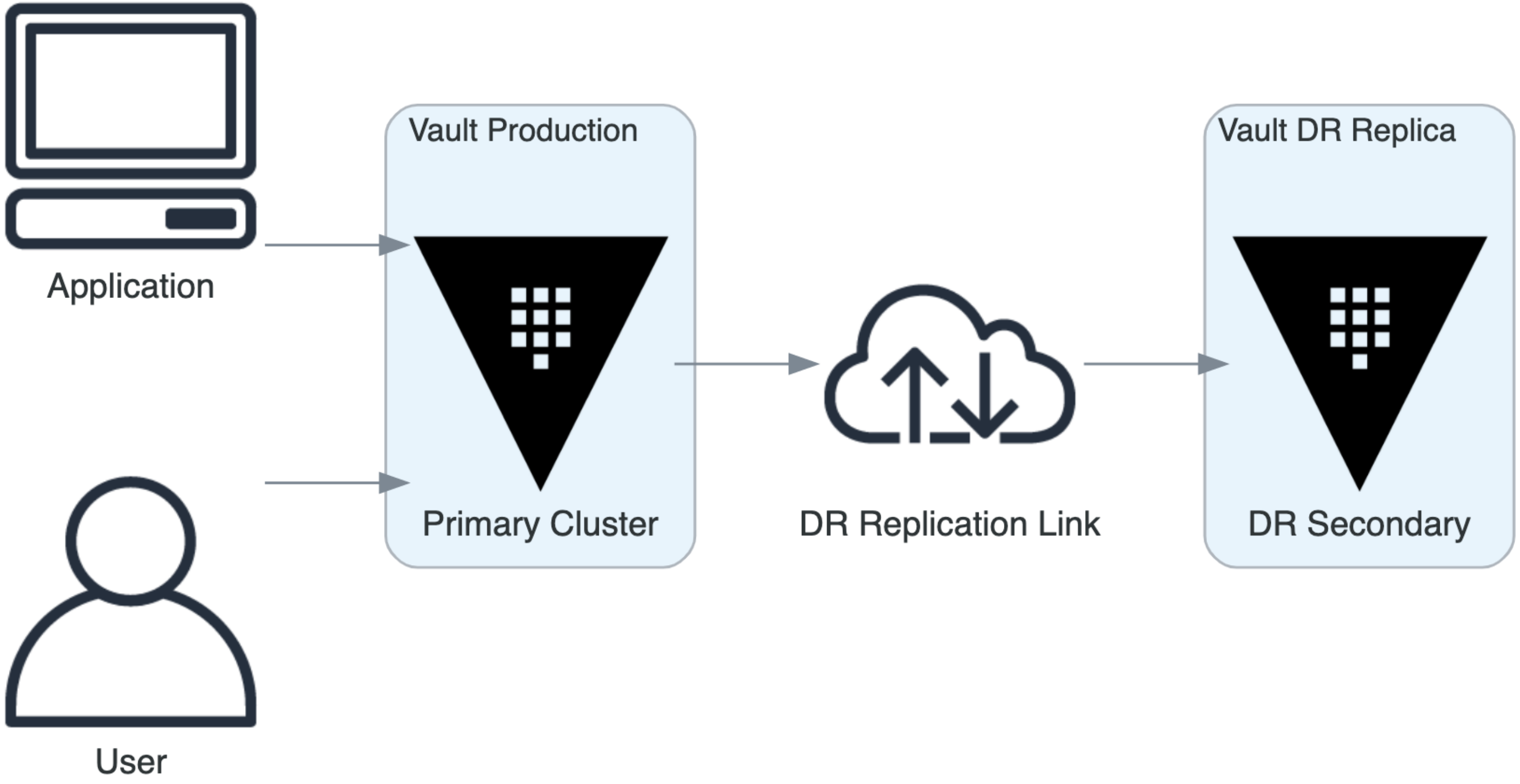
- There are two modes of replication in Vault that are commonly combined to provide end to end redundancy and support.

Vault Cluster



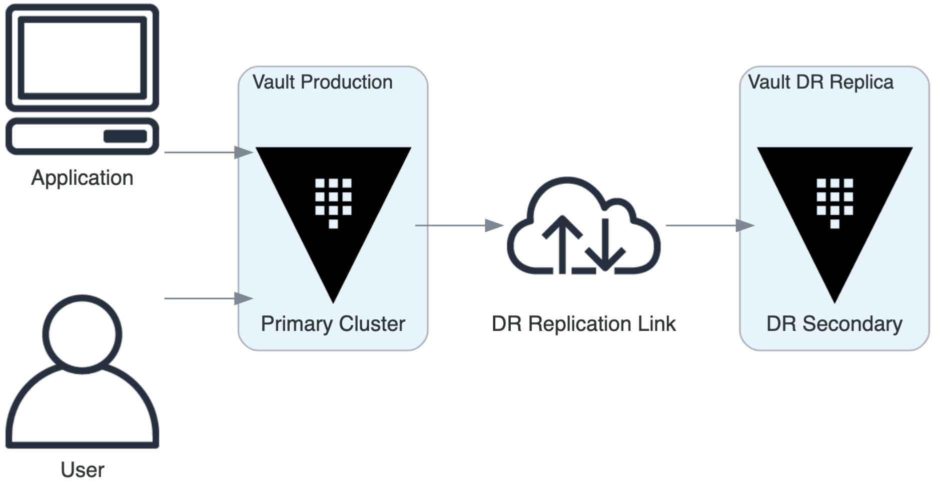
Clustered Replication Vault Service

Disaster Recovery Replication



Disaster Recovery Replication Vault Service

Disaster Recovery Replication (cont.)



- Consists of one active Vault cluster and one stand-by
- The DR secondary does not handle application requests
- Replication of all configuration, secrets and authentication tokens
- Failover consists of CLI/API/GUI promotion of the standby

Disaster Recovery Failover Process

- Verify Primary Vault Cluster is unreachable
- Generate a root token
- Initiate DR Root token creation
- Assemble DR seal key quorum
- Distribute `nonce` to the quorum
- Quorum authenticates with unseal keys
- Decode the DR Operation Token
- Finally promote the DR Secondary

Disaster Recovery Decisions

Once you've recovered from a DR Scenario:

- Depending on your DR setup you will either:
  - Recover back to your Vault Primary
  - Recover your former Primary to a Secondary
- Validate cluster health and data replication
  - Check the /v1/sys/health/ endpoint for both clusters
  - Check the /sys/replication/status endpoint for replication health

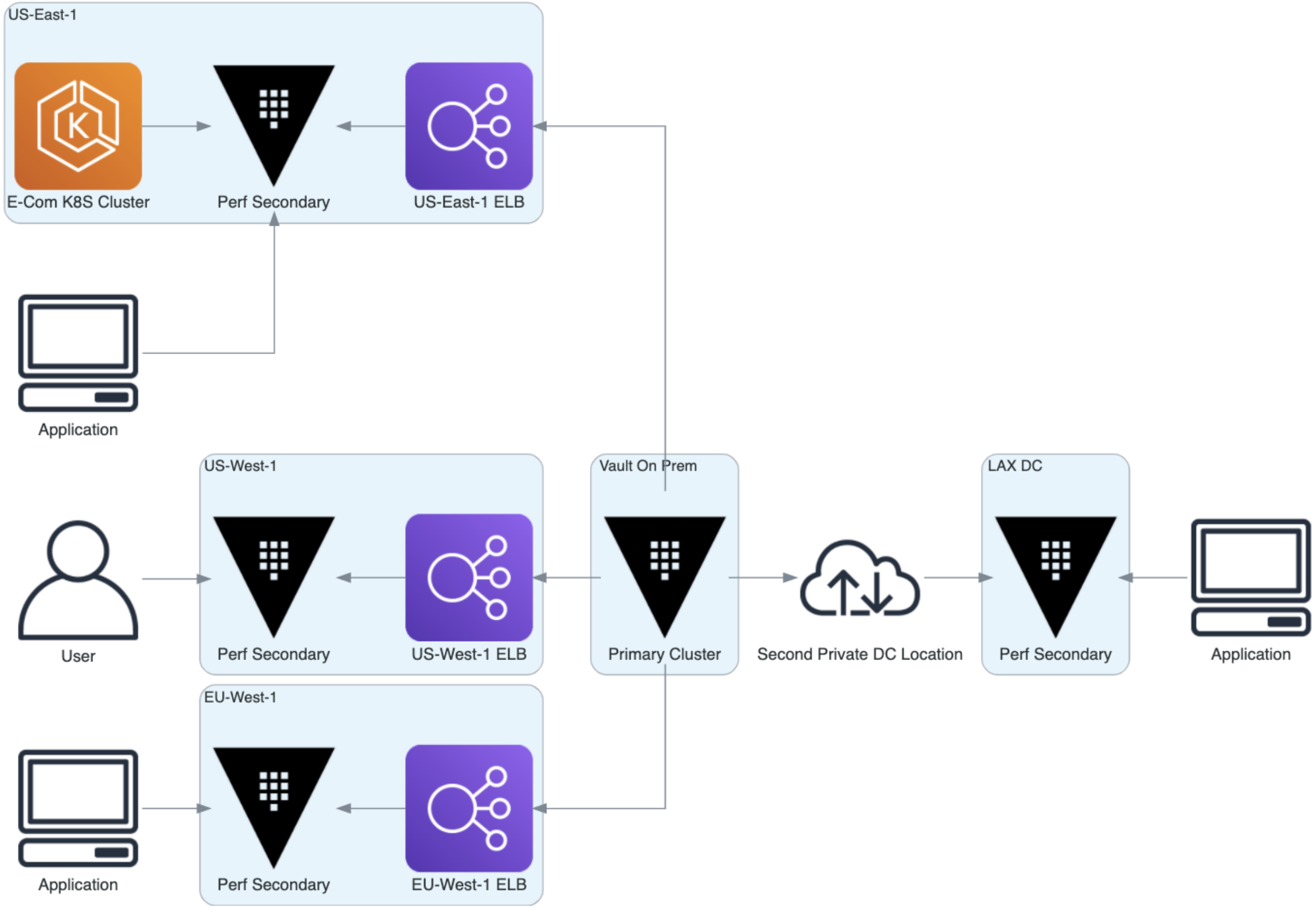
Disaster Recovery Summary

Have a good strategy for a quick recovery

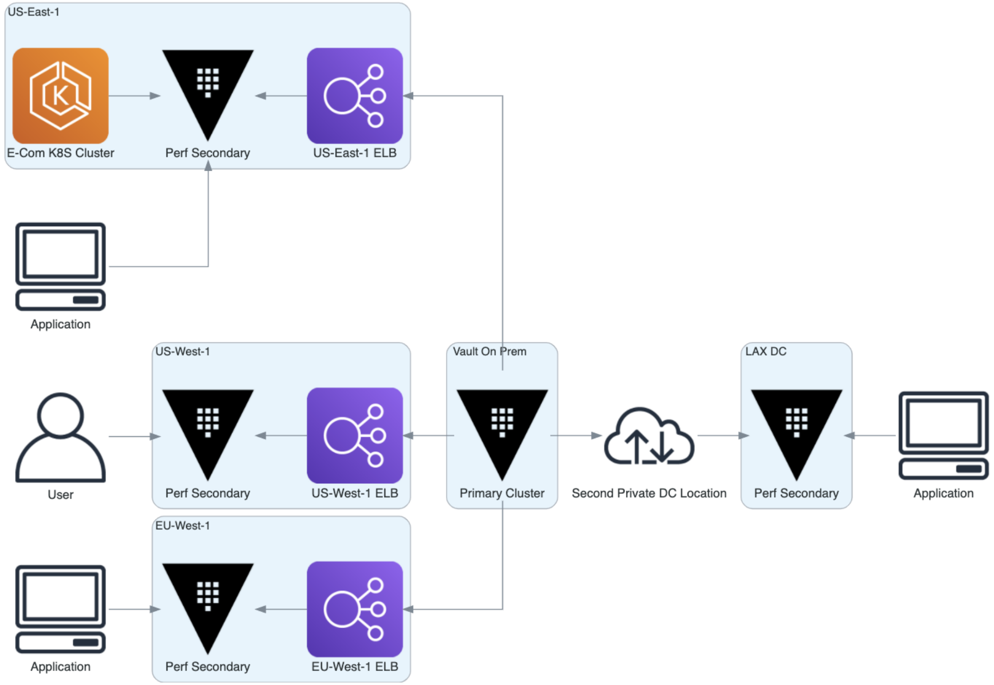
- Know who the recovery key holders are to generate a root token
- If you already have a root token stored know how to access it
- Practice DR Failover

Performance Replication

Performance Replication Overview



Performance Replication



- Consists of one Primary with many Secondaries
- Secondaries must be connected to the primary
- "Hub and Spoke" replication
- Primary may be connected to a secondary **and** disaster recovery cluster
- Replication of all configuration, secrets (except active leases)
- Authentication Tokens are not replicated

Replication Comparison

Capability	DR Replication	Performance Replication
Configuration Mirroring	Yes	Yes
Secrets Configuration	Yes	Yes
Static Secrets	Yes	Yes
Dynamic Secrets	Yes	No
Token Replication	Yes	No
Secondaries Handle Requests	No	Yes

Replication Comparison (cont.)

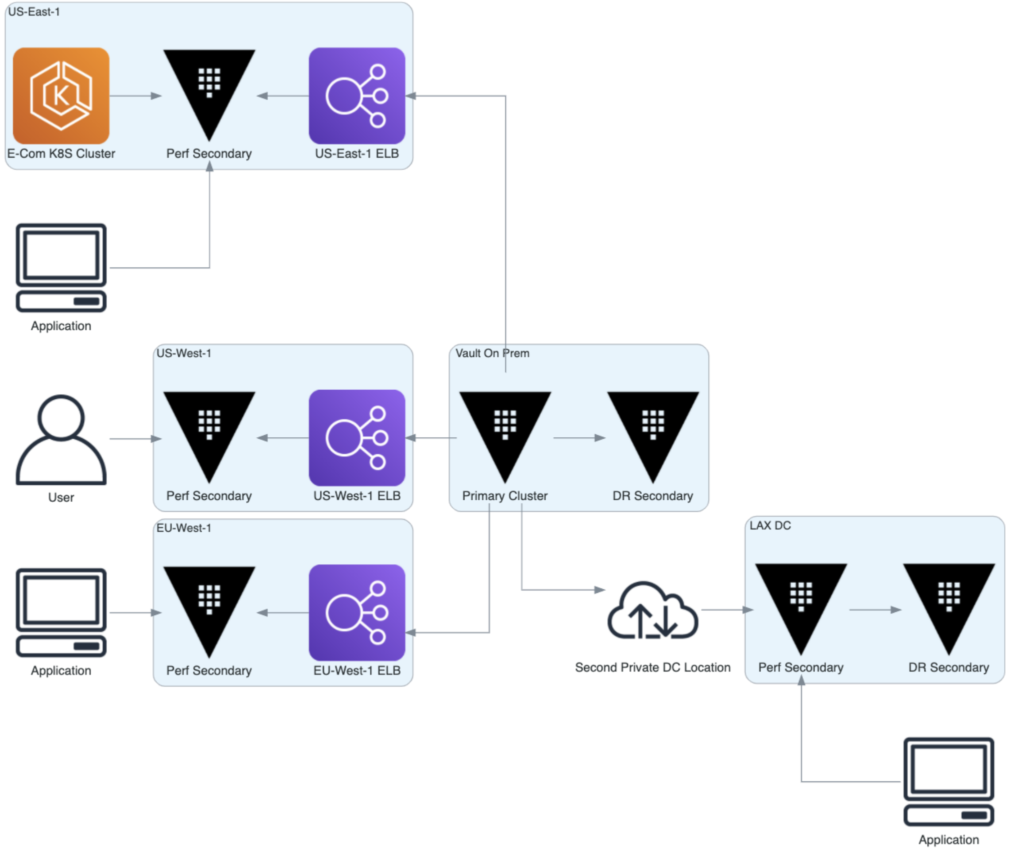
Performance Replication

- Applications support a multi-zone topology
- Multiple Cloud Regions
- Multiple Clouds (AWS, Azure, GCP, On-Premise)
- Private to Cloud migration

Disaster Replication

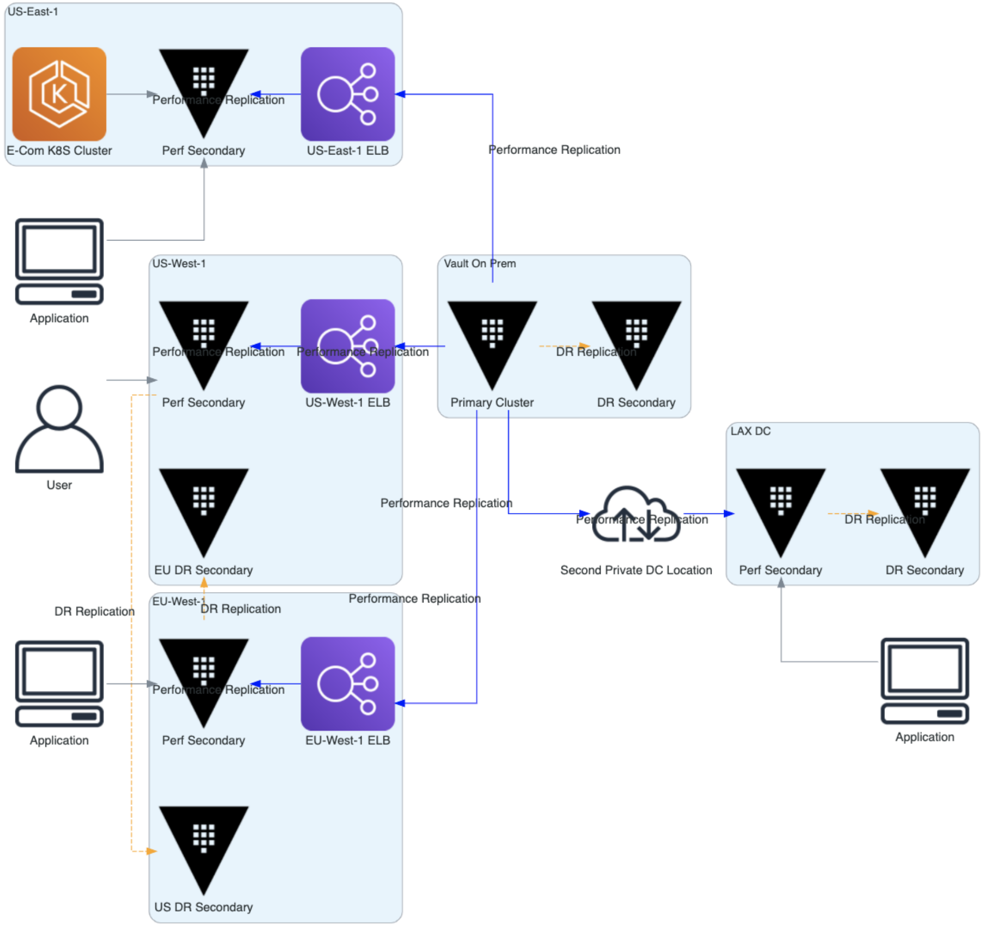
- For in-region recovery of a failed cluster
- For cross-region recovery of a failed zone/region

In-Region Disaster Recovery



Performance & DR Replication

Cross-Region Disaster Recovery



Performance & Cross DR Replication

Scoping Considerations For RTO/RPO/BCP

- How many regions do you want to support with Vault? What are they?
- On-premise datacenters, cloud regions, etc
- Where do you have applications?
- What is your application failover topology?
- What are your business' RTO/RPO requirements?

Chapter Summary

- Performance Replication enables active-active service
- Disaster Recovery Replication considerations
  - In-region
  - Cross-region
- Achieving RTO, RPO, BCP

Reference links

- Vault Enterprise Replication
- Learn Performance Replication
- Setting up Configuration

Vault Enterprise Replication Module Complete!