Intro

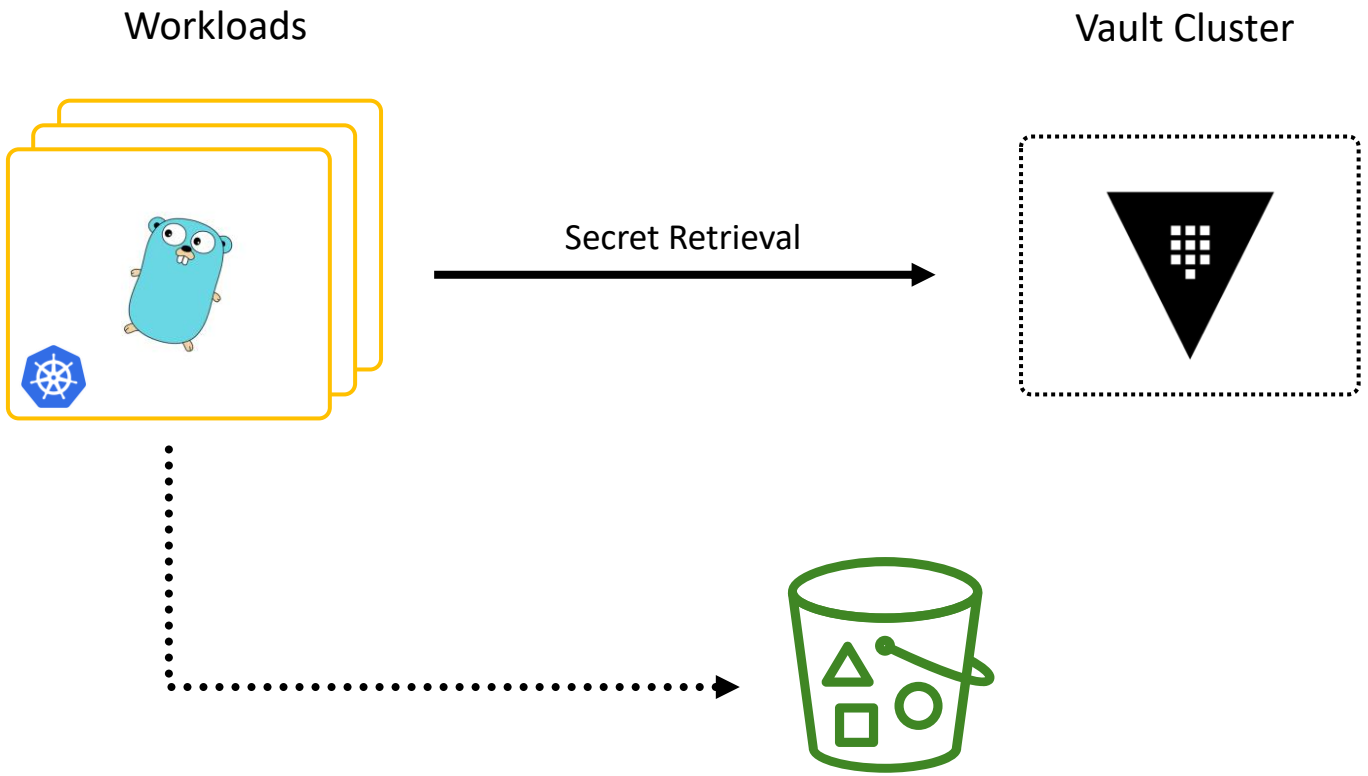
# Integrating with Amazon Web Services

# Introduction

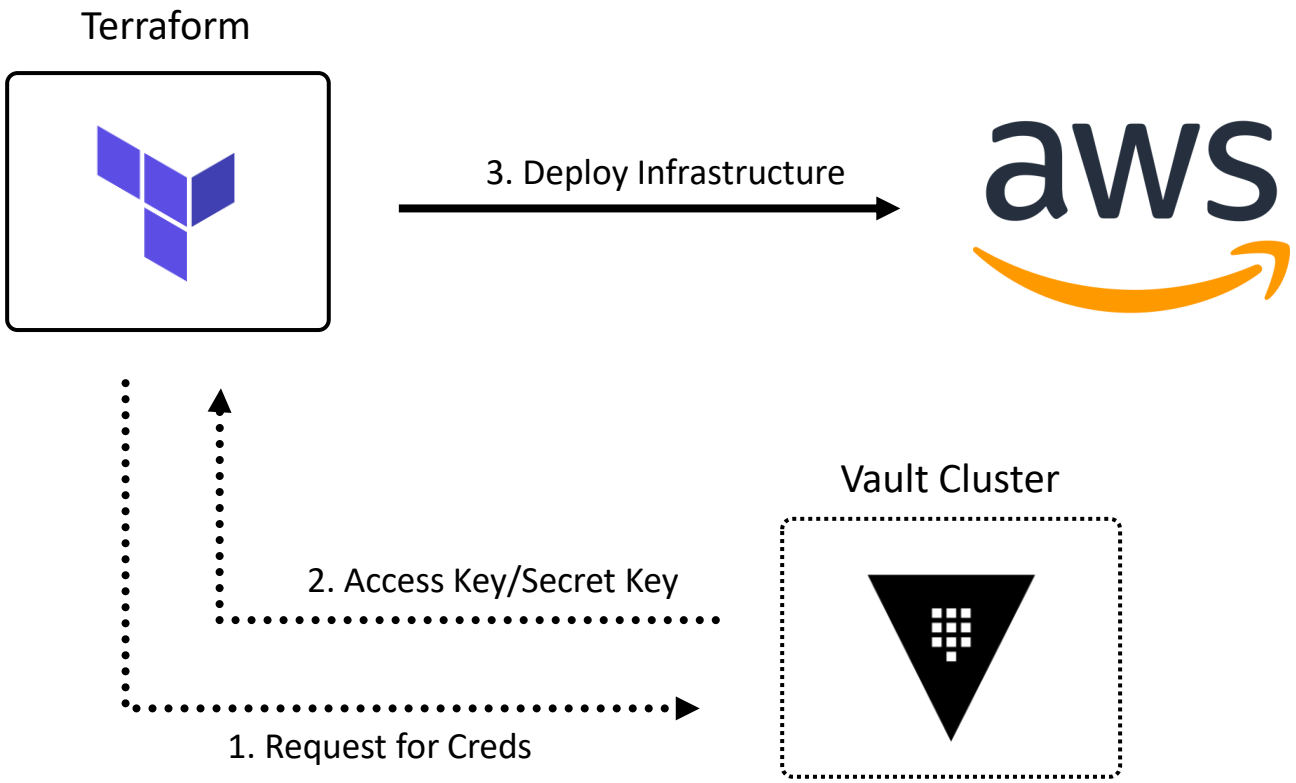
- AWS is the most popular public cloud provider today
- Vault provides quite a few native integrations with AWS
  - Auth Method
  - Secrets Engine
  - Database Secrets Engine for RDS

- Other AWS Integrations that can be used:
  - TOTP for IAM & root accounts
  - Deployment of Vault on the AWS platform
  - Use of VPC endpoints

# AWS Auth Method

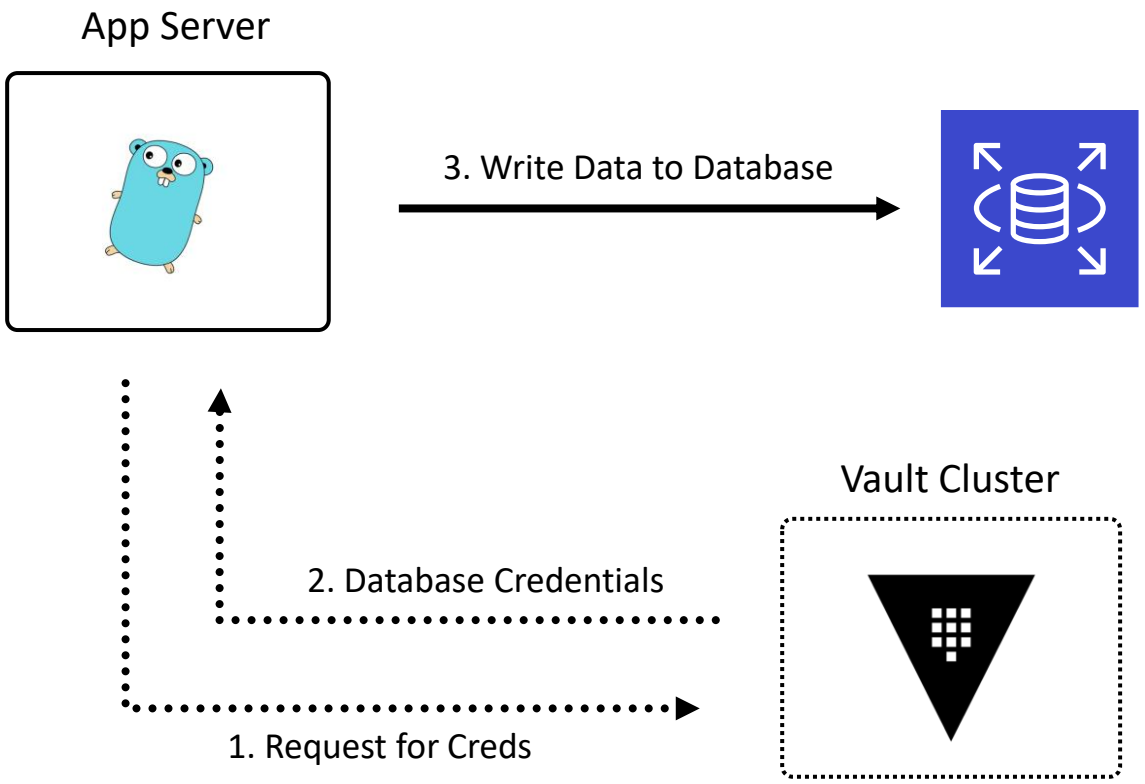


# AWS Secrets Engine

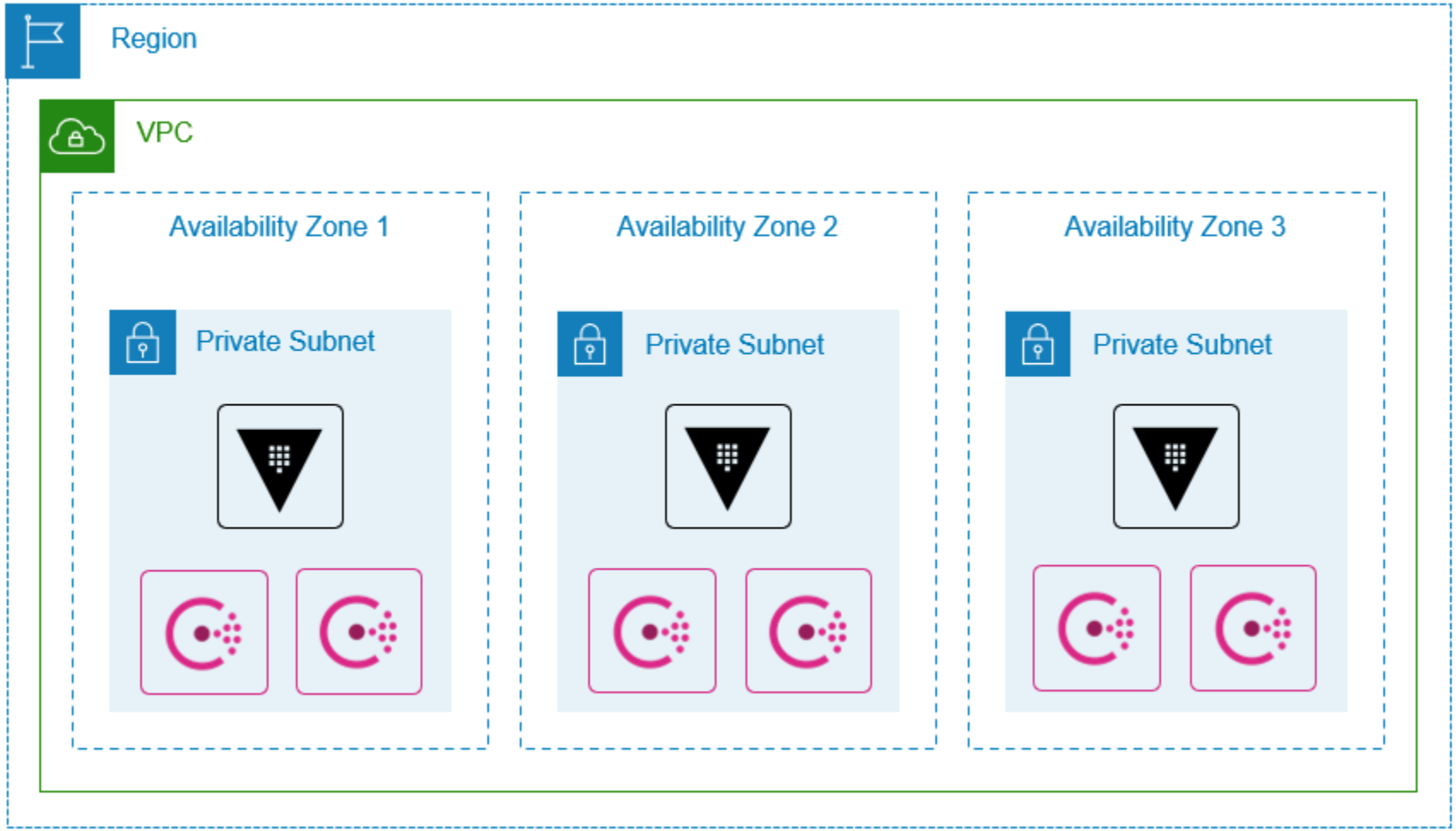


# Database Secrets Engine

Accessing Amazon RDS



# Deploying Vault on AWS



# Deploying Vault on AWS

Deployment methodologies include:

- Manual installation
- CloudFormation
- Terraform
- AWS Quick Start for Vault (EKS)
- AWS Quick Start for EC2 (EC2)

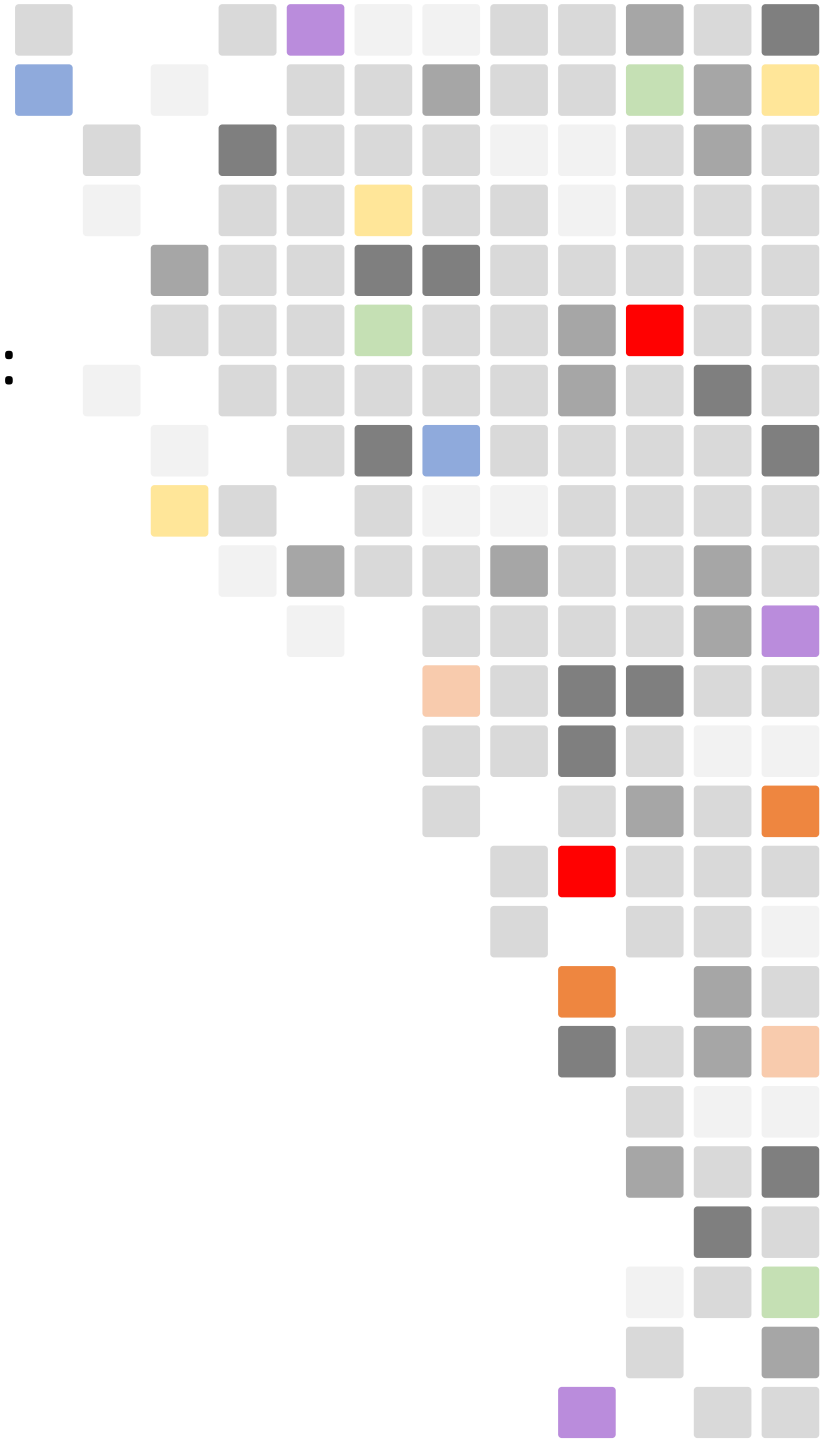
https://aws-quickstart.s3.amazonaws.com/quickstart-hashicorp-vault/doc/hashicorp-vault-on-the-aws-cloud.pdf

https://aws.amazon.com/quickstart/architecture/eks-vault/

# Integrating Vault with AWS Services

AWS Services used to increase security and availability:

- Auto Scaling
- IAM Roles (EC2 Service Role)
- VPC Endpoints
- Amazon Load Balancing
- Security Groups
- EC2 Metadata
- TOTP for IAM and root accounts

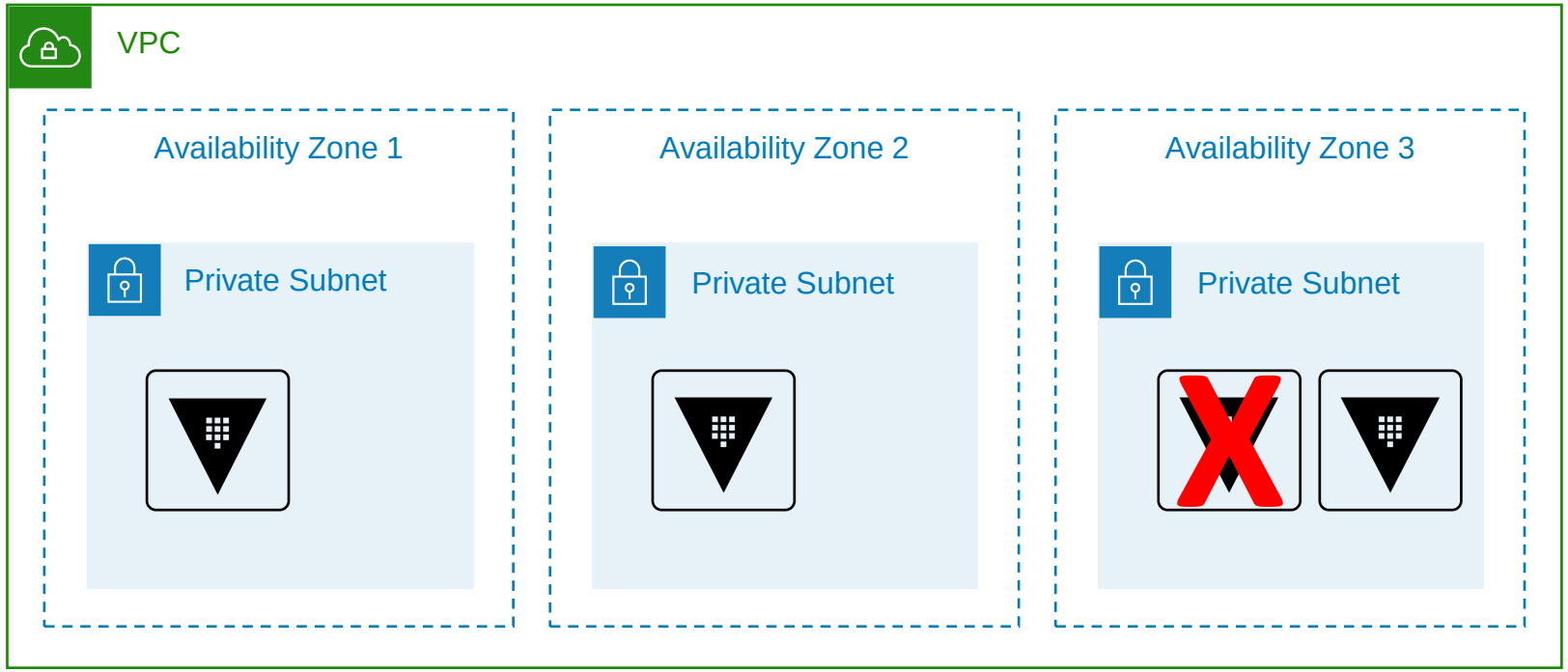


# Using Auto Scaling

Requires complete automation of Vault deployment using userdata or an AMI:

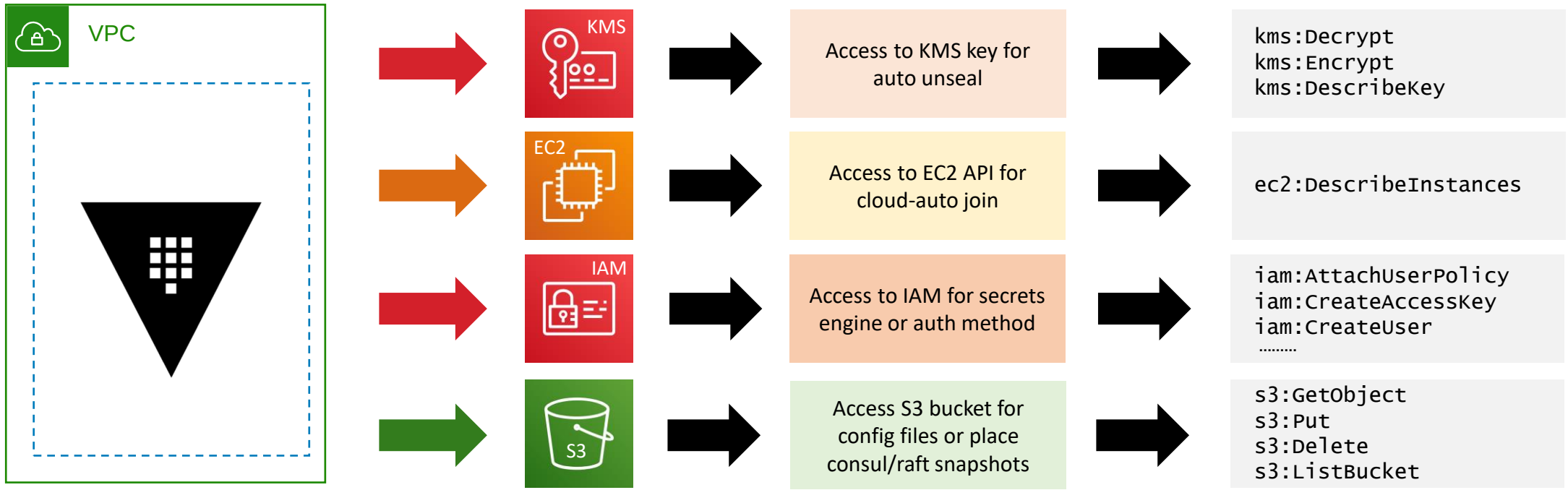
Auto Scaling Group:

- Max: 3
- Min: 3
- Desired: 3

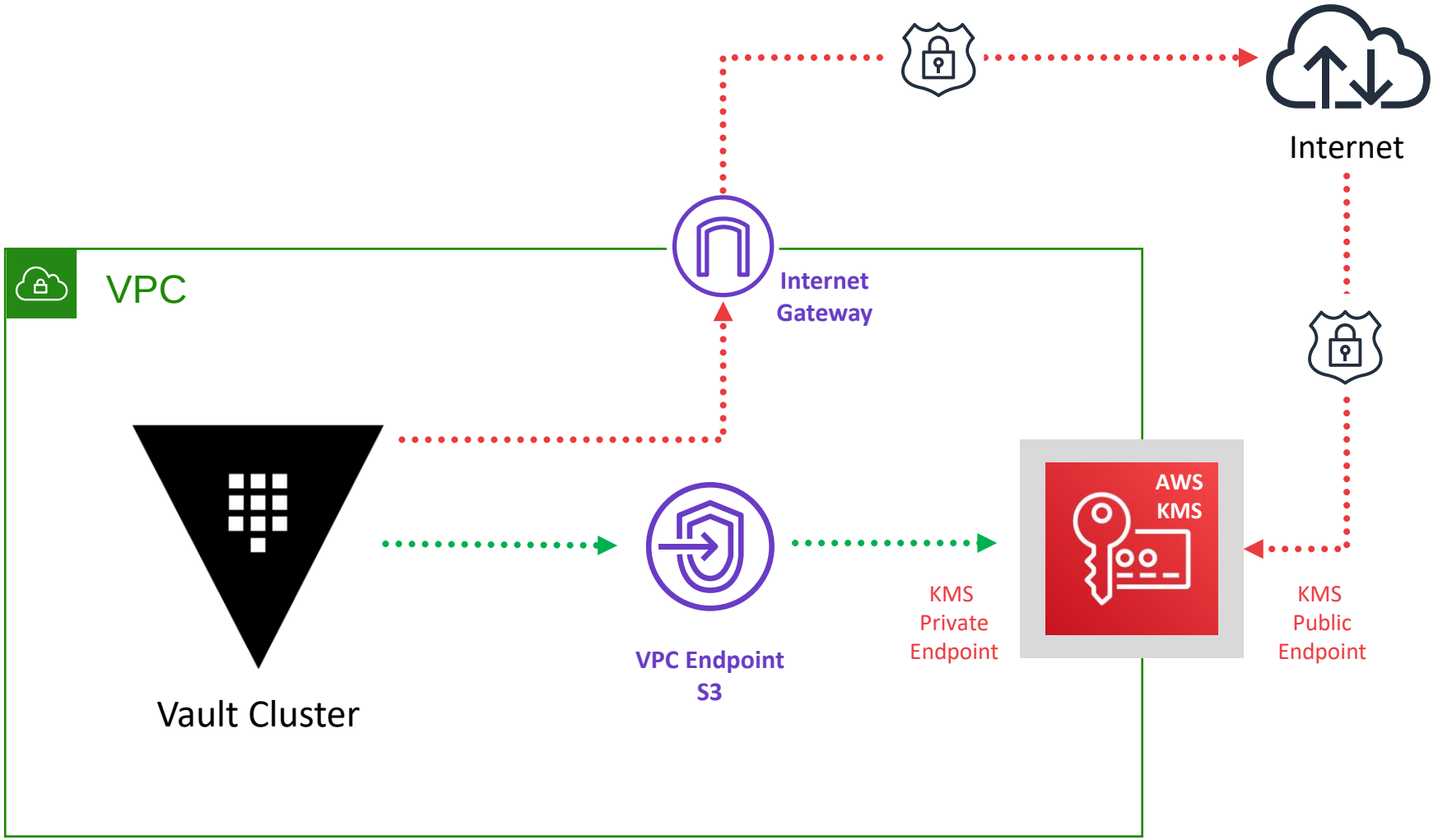


# Using IAM Roles

- Enables access to AWS services *without providing credentials to Vault*
- Common AWS services accessed include KMS, EC2, IAM, S3

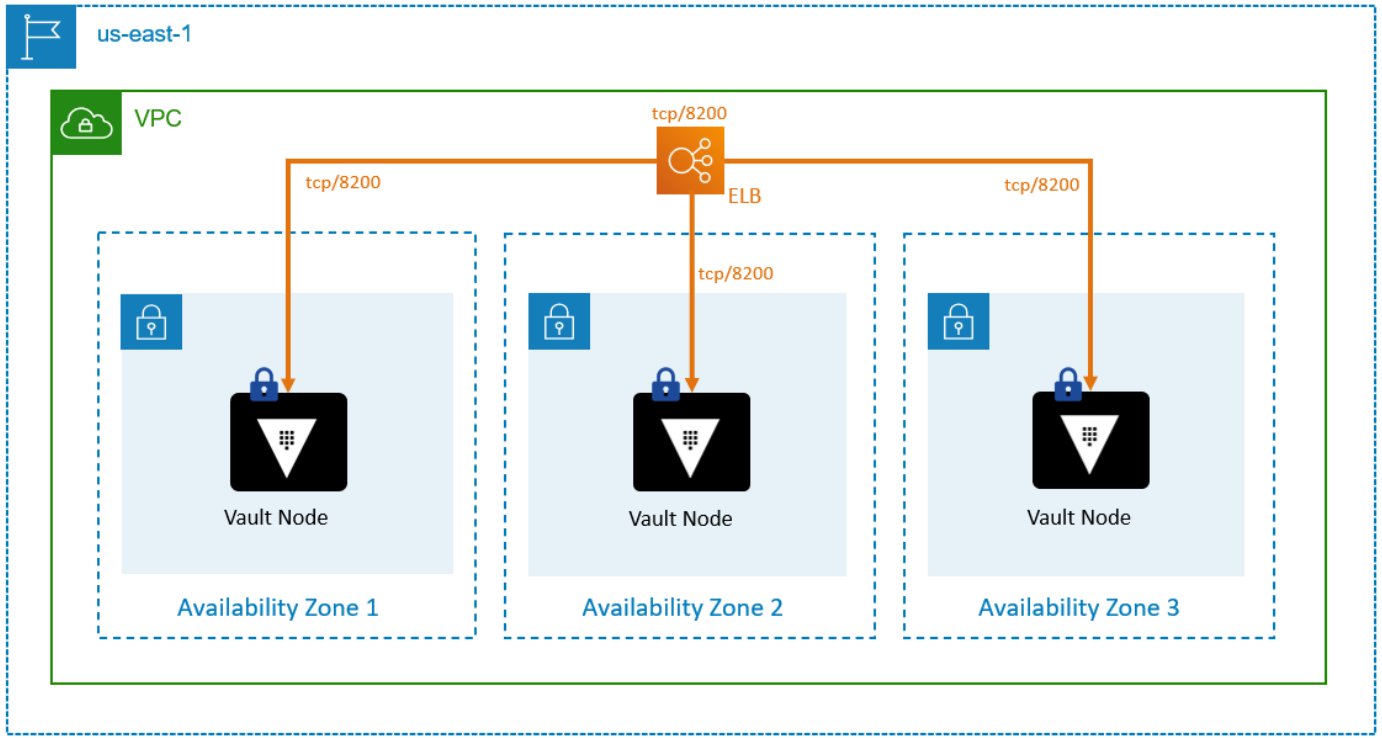


# Using a VPC Endpoint



# Use Amazon Load Balancing

- Provides front-end access to Vault cluster
- Use health checks to determine the Active node vs. standby nodes
  - Configure load balancer to check against **/v1/sys/health** endpoint




| Return Code | Node Status |
|---|---|
| 200 | Initialized, Unsealed, and Active |
| 429 | Unsealed and standby |
| 472 | DR replica and active |
| 473 | Performance Standby |
| 501 | Not Initialized |
| 503 | Sealed node |

# Security with Security Groups

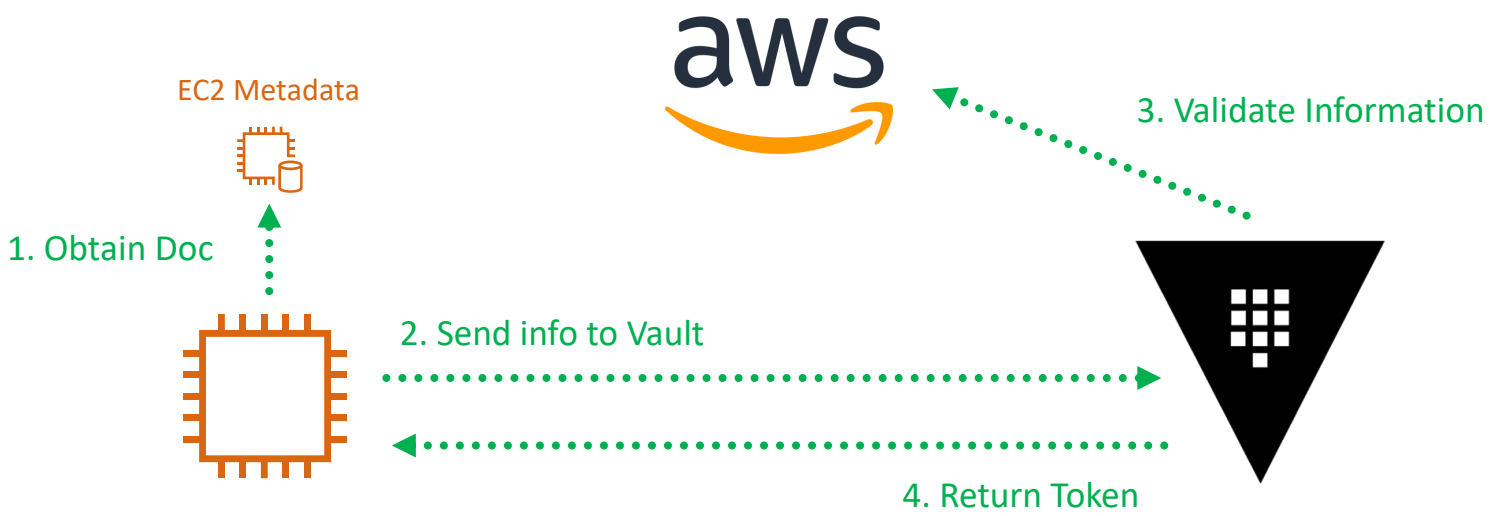
- Provides firewalling capabilities at the ENI level (micro segmentation)
- Easily permit traffic between nodes while only allowing Vault traffic from the load balancer
- Also need to permit management connectivity (SSH, syslog forwarding, log collection, Consul connectivity)

## Vault Cluster – backed by Consul

| Source | Target | Port | Protocol | Direction | Description |
|---|---|---|---|---|---|
| **Vault Clients** | Vault Load Balancer | 8200 | tcp | ingress | Vault Interface (API) |
| **Vault Load Balancer** | Vault Nodes | 8200 | tcp | ingress | Vault Interface (API) |
| **Vault Nodes** | Vault Nodes | 8201 | tcp | bidirectional | Request Forwarding |
| **Vault Nodes** | Vault Nodes | 8301 | tcp/udp | bidirectional | LAN Gossip Communication |
| **Vault Nodes** | Consul Nodes | 8301 | tcp/udp | bidirectional | LAN Gossip Communication |
| **Consul Nodes** | Consul Nodes | 8300 | tcp/udp | bidirectional | Server RPC |
| **Consul Nodes** | Consul Nodes | 8301 | tcp/udp | bidirectional | LAN Gossip Communication |
| **Vault Nodes** | Consul Nodes | 8500 | tcp | ingress | Consul Interface (API) |
| **Secondary Cluster** | Vault Primary Cluster LB | 8200 | tcp | bidirectional | Unwrap Secondary Token |
| **Vault Primary Cluster** | Secondary Cluster | 8201 | tcp | bidirectional | Vault Replication |

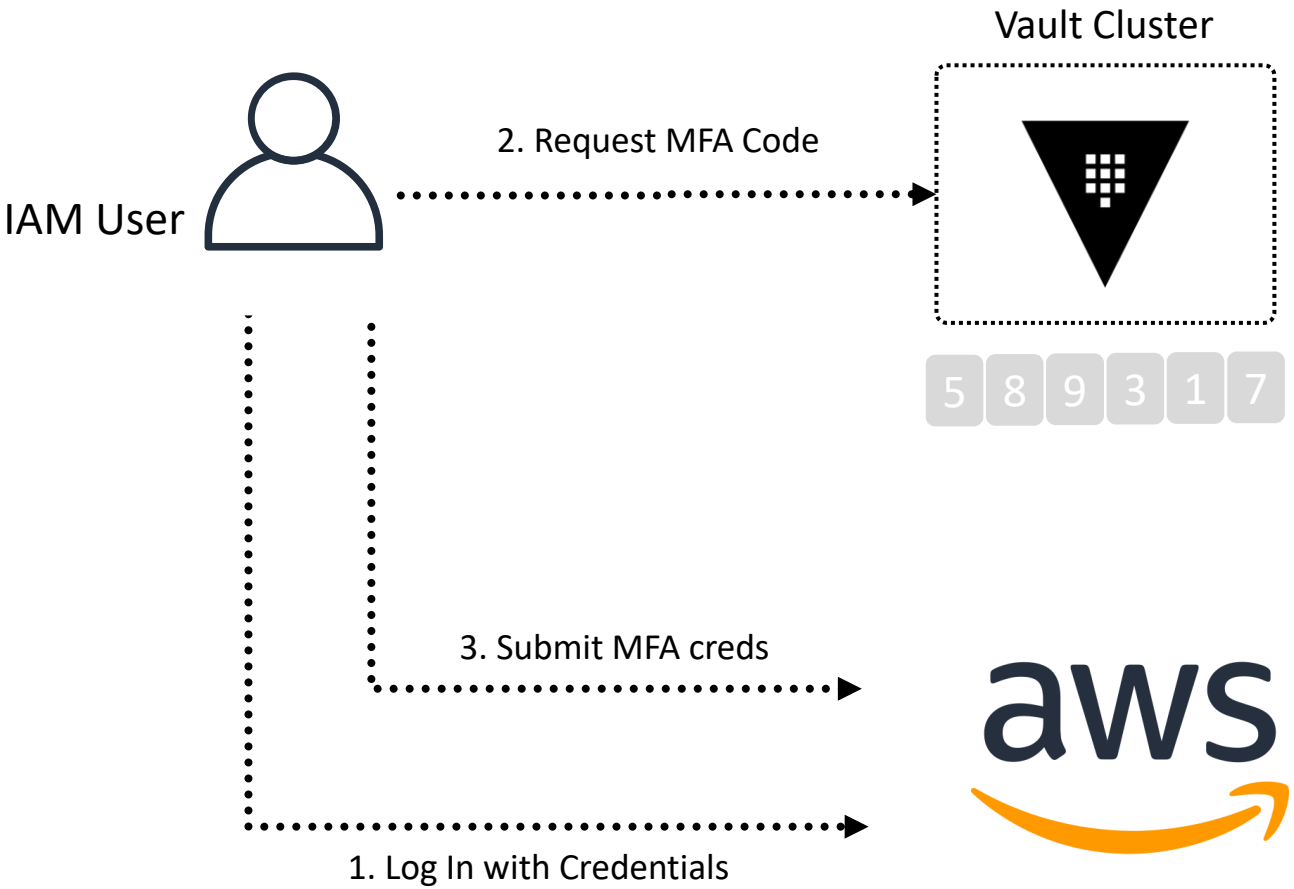
# How Vault uses EC2 Metadata

- AWS auth method can use the EC2 method or the IAM method
- EC2 method will obtain Instance identity document from EC2 metadata and send to Vault when authenticating
- Vault will verify information with AWS
- If valid, Vault issues a token to the EC2 based on the policies configured



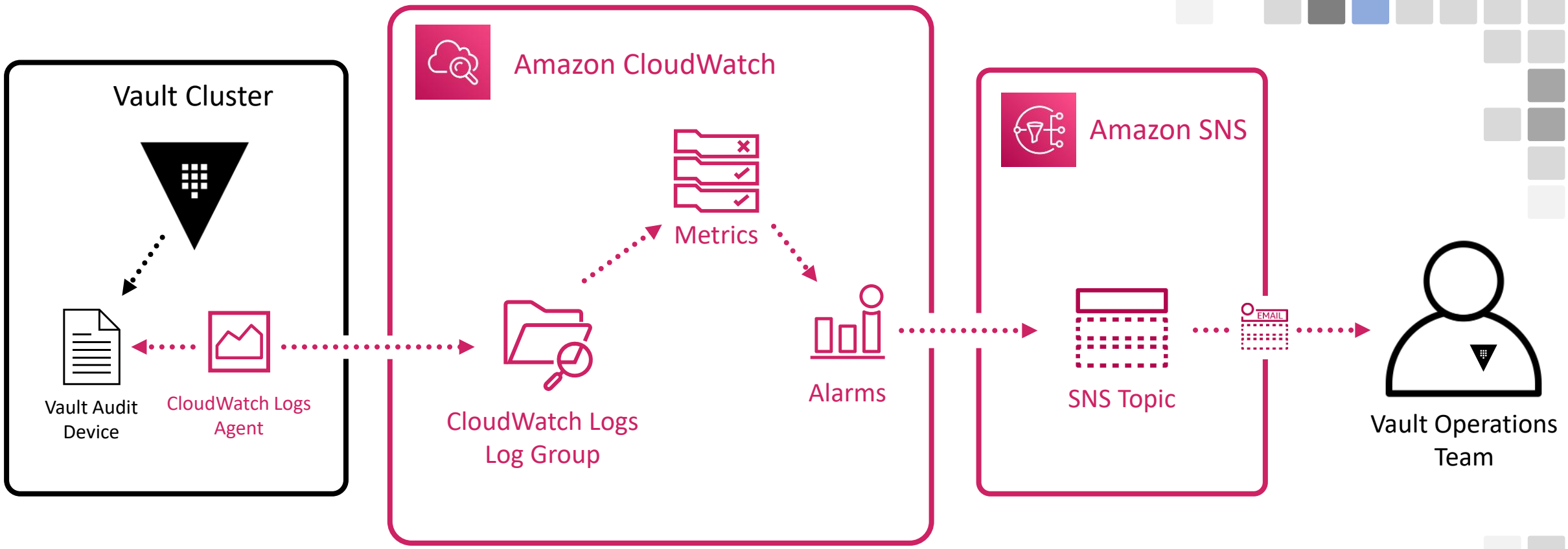
# Securing Accounts

Using the TOTP Secrets Engine



# Logging and Alerting

Using CloudWatch Logs for Audit Logs



# Logging and Alerting

Configure Rules and Alarms for Vault actions

- ❑ Use of a root token
- ❑ Creation of a new root token
- ❑ Vault policy modification
- ❑ Enabling a new auth method
- ❑ Modification of an auth method role
- ❑ Creation of a new auth method role
- ❑ Permission denied (403) responses
- ❑ Use of Vault by human-related accounts outside of regular business hours
- ❑ Vault requests originating from unrecognized subnets
- ❑ Transit Minimum Decryption Version Config
- ❑ Seal Status of Vault
- ❑ Audit Log Failures
- ❑ Resource Quota Violations
- ❑ Updates to Vault Policies
- ❑ Transit Key Deletion
- ❑ Cloud-based resource changes