Migrating HashiCorp Vault Secrets and Certificates to AWS Services

1. Cost Comparison

HashiCorp Vault (Self-Hosted Enterprise):

- Enterprise licensing costs can exceed $2M/year, excluding infrastructure and operational overhead.
- Infrastructure, storage, backups, and personnel increase costs.

AWS Services:

- Secrets Manager (SM): ~$0.40 per secret per month, ~$0.05 per 10,000 API calls.
- AWS Certificate Manager (ACM): Free for public certs, imported certs are free.
- AWS Private Certificate Authority (PCA): ~$400/month per CA + ~$0.75 per certificate.
- AWS eliminates operational burden with managed services.

2. Best Practices for Security and Compliance

- IAM Policies: Enforce least privilege with specific roles for secret access.
- Encryption: Secrets encrypted with AWS KMS, both at rest and in transit.
- Secret Rotation: Leverage AWS Lambda to automate rotation.
- Audit Logging: Enable CloudTrail for detailed logs of secret access.
- Secure Migration: Isolate migration environment, ensure no secrets are logged.
- Compliance: Use correct AWS regions and services to meet data residency and compliance needs.

3. Automation Tools and Techniques

Vault Sync:

- Vault Enterprise feature to sync secrets to AWS Secrets Manager.
- Allows near real-time replication and phased migration.

Terraform:

- Use Vault and AWS providers to extract secrets and provision them in AWS.
- Manage infrastructure as code and ensure idempotency.

boto3 + hvac (Python):

- Direct migration script using Vault's API (hvac) and AWS SDK (boto3).

- Customizable, flexible, and automatable for large-scale migrations.

4. Real-World Case Studies

- AWS Security Blog Series on migrating secrets with prescriptive guidance.
- Community experiences shared on Reddit highlighting costs, practices, and hybrid patterns.
- HashiCorp's Vault Sync used by enterprises to bridge Vault and AWS before full migration.
- AWS PCA adoption to replace internal PKI systems.

5. Migration Strategy (Non-Hybrid Approach)

Step 1: Preparation

- Inventory all Vault secrets and certificates.
- Communicate with stakeholders and set freeze periods.
- Define secret mappings and migration tools.

Step 2: AWS Environment Setup

- Configure IAM roles, KMS keys, Secrets Manager, PCA, and ACM.
- Ensure logging (CloudTrail) and monitoring (CloudWatch) are enabled.

Step 3: Test Migration

- Perform dry-run with development secrets.
- Validate secret retrieval by applications.

Step 4: Production Migration

- Bulk migrate secrets using Vault Sync, Terraform, or scripts.
- Import certificates into ACM/PCA.

Step 5: Cutover

- Update applications to retrieve secrets from AWS.
- Switch certificates on services to ACM/PCA managed ones.

Step 6: Post-Cutover Validation

- Monitor secrets and certificate usage.
- Enable rotation and compliance audits.

- Verify all applications are functioning.

Step 7: Decommission Vault

- Backup Vault data.
- Shutdown servers and revoke tokens.
- Clean up Vault artifacts and permissions.

Rollback Plan:

- Maintain Vault in read-only mode temporarily.
- Roll back apps by redirecting to Vault if critical issues occur.

Monitoring Strategy:

- CloudWatch alarms for secret access anomalies.
- AWS Config and Security Hub for compliance checks.
- Routine IAM policy audits to avoid privilege creep.

This structured approach ensures a smooth transition from HashiCorp Vault to AWS Secrets Manager, ACM, and PCA, reducing operational costs, improving security posture, and leveraging AWS-managed services for scalability and reliability.

For more references, visit:

- AWS Secrets Manager Pricing
- AWS Private CA Pricing
- HashiCorp Vault Secrets Sync Documentation
- AWS Security Blog: Migrating Secrets to AWS
- Community discussions and case studies from Reddit and re:Invent