Python script to migrate secrets from AWS Secrets Manager to HashiCorp Vault using GitHub OIDC authentication for both services.

**Setup Instructions**

**1. AWS Configuration**

In your AWS account, create an IAM role for GitHub Actions with OIDC:

{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Federated": "arn:aws:iam::YOUR\_ACCOUNT\_ID:oidc-provider/token.actions.githubusercontent.com" }, "Action": "sts:AssumeRoleWithWebIdentity", "Condition": { "StringEquals": { "token.actions.githubusercontent.com:aud": "sts.amazonaws.com", "token.actions.githubusercontent.com:sub": "repo:YOUR\_ORG/YOUR\_REPO:ref:refs/heads/main" } } } ] }

Attach this policy to the role:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"secretsmanager:ListSecrets",

"secretsmanager:GetSecretValue",

"secretsmanager:DescribeSecret"

],

"Resource": "\*"

}

]

}

**2. Vault Configuration**

Enable JWT auth method in your Vault namespace:

bash

vault auth enable jwt

vault write auth/jwt/config \

oidc\_discovery\_url="https://token.actions.githubusercontent.com" \

bound\_issuer="https://token.actions.githubusercontent.com"

vault write auth/jwt/role/github-actions \

role\_type="jwt" \

bound\_audiences="https://github.com/YOUR\_ORG" \

bound\_subject="repo:YOUR\_ORG/YOUR\_REPO:ref:refs/heads/main" \

user\_claim="actor" \

policies="secret-writer" \

ttl=1h

**3. GitHub Secrets**

Add these secrets to your GitHub repository:

* AWS\_ROLE\_ARN: ARN of the AWS IAM role
* VAULT\_ADDR: Vault server address (e.g., https://vault.example.com)
* VAULT\_NAMESPACE: Your Vault namespace
* VAULT\_ROLE: The Vault role name (e.g., github-actions)

**4. Usage**

1. Place the Python script in your repo as migrate\_secrets.py
2. Place the workflow file in .github/workflows/migrate-secrets.yml
3. Run the workflow from GitHub Actions UI with appropriate parameters
4. Start with dry\_run: true to test without making changes

The script will:

* ✅ Authenticate to AWS using OIDC
* ✅ Authenticate to Vault using GitHub OIDC token
* ✅ Support Vault namespaces
* ✅ List and retrieve all secrets from AWS Secrets Manager
* ✅ Migrate them to Vault KV v2 engine
* ✅ Provide detailed logging and error handling

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"secretsmanager:ListSecrets"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": [

"secretsmanager:GetSecretValue",

"secretsmanager:UpdateSecret"

],

"Resource": [

"arn:aws:secretsmanager:ca-central-1:497241180797:secret:\*"

]

}

]

}

