





HashiCorp

# Vault AWS-KMS Auto Unseal

3



Role

KMS-Vault-role

create Role | AWS service | EC2 Service

Attach KMS Role policy

3.1

## Select trusted entity

### Trusted entity type

☒ AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

### Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

#### Common use cases

☒ EC2

Allows EC2 instances to call AWS services on your behalf.

☐ Lambda

Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

3.2

## Permissions policies (Selected 1/739)

Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter

< 1 2 3

	Policy name	Type	Description
<input checked="" type="checkbox"/>	KMS-role	Custom...	KMS-role

policy created in step 2



HashiCorp

Vault

# AWS-KMS Auto Unseal

AWS KMS Auto Unseal



AWS KMS

Aliases	Key ID	Status	Key spec	Key usage
mykey-vault-auto-unseal	0730e056-4d52-4131-89fb-0c4b15449463	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt



AWS Instance

allow port 8200 in security group

Attach role to EC2-Instance

```
ui = true
storage "file" {
  path = "/opt/vault/data"
}

listener "tcp" {
  address      = "0.0.0.0:8200"
  tls_cert_file = "/opt/vault/tls/tls.crt"
  tls_key_file  = "/opt/vault/tls/tls.key"
}

seal "awskms" {
  region = "us-east-1"
  kms_key_id = "0730e056-4d52-4131-89fb-0c4b15449463"
}
```

export VAULT\_SKIP\_VERIFY=true

```
ubuntu@ip-172-31-82-174:~$ vault status
Key          Value
---          -
Recovery Seal Type  awskms
Initialized         false
Sealed              true
Total Recovery Shares 0
Threshold            0
Unseal Progress      0/0
Unseal Nonce         n/a
Version              1.10.0
Storage Type         file
HA Enabled            false
```