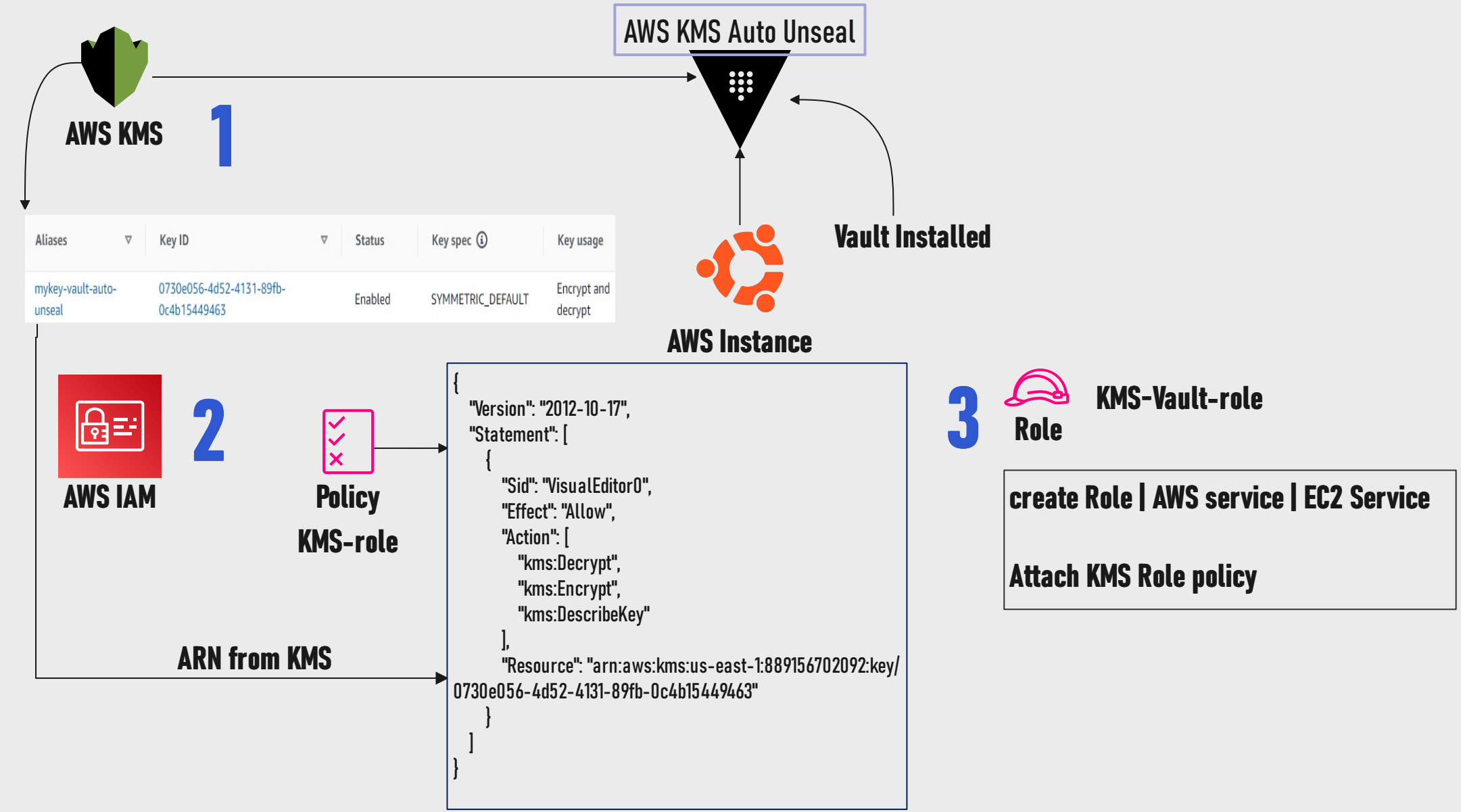
HashiCorp Vault AWS-KMS Auto Unseal



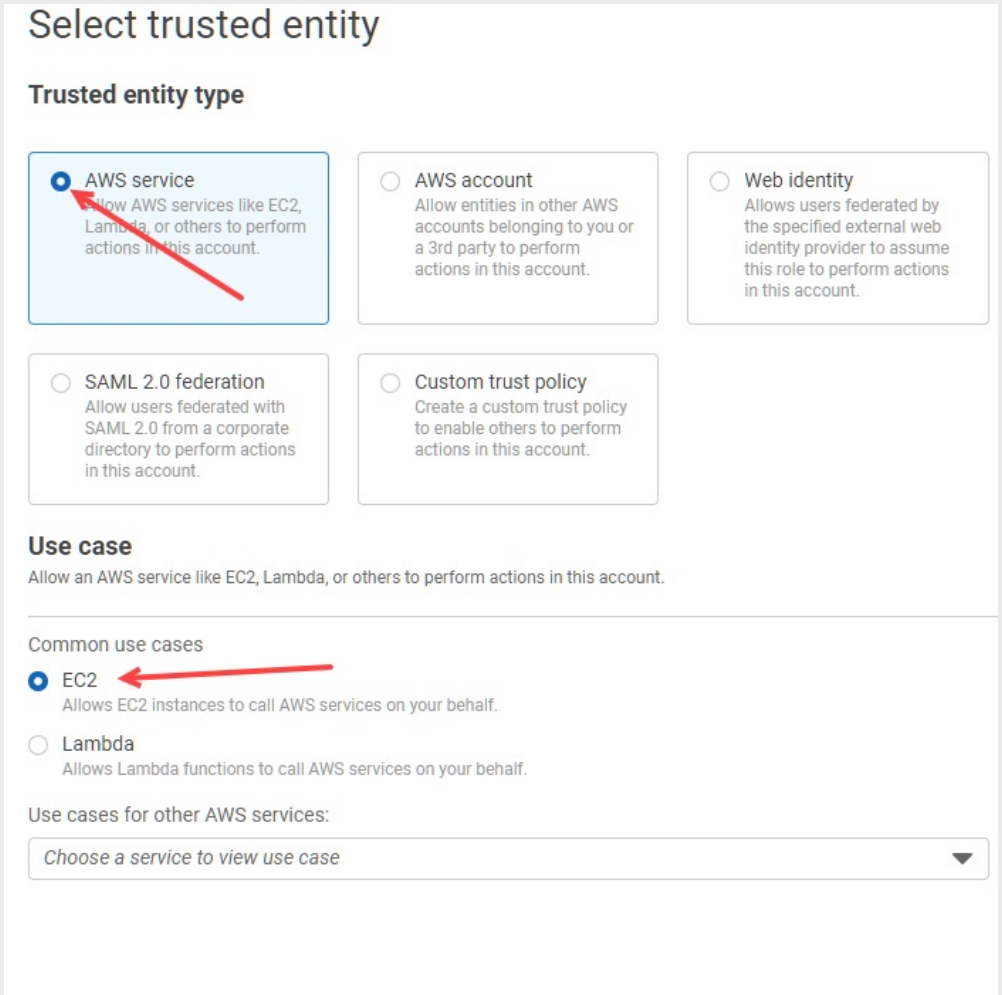
HashiCorp Vault AWS-KMS Auto Unseal

3 Role KMS-Vault-role

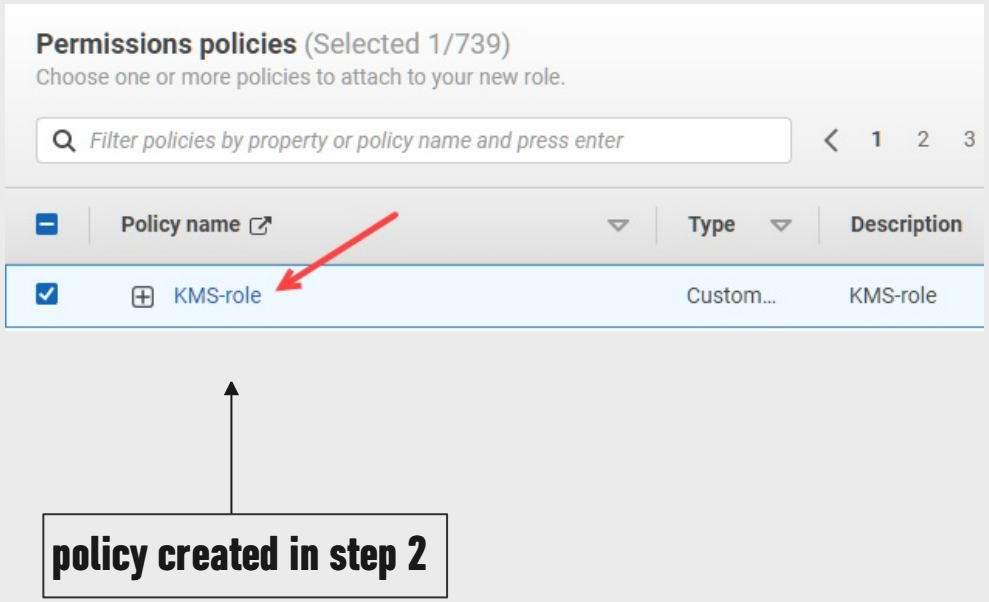
create Role | AWS service | EC2 Service

Attach KMS Role policy

3.1



3.2



policy created in step 2

HashiCorp Vault AWS-KMS Auto Unseal

AWS KMS

AWS KMS Auto Unseal

allow port 8200 in security group

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

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
```