

✔ You successfully stored the secret key. To show it in the list, choose Refresh.
Use the sample code to update your applications to retrieve this secret.

key

Secret details

Encryption key

custom_key

Secret name

key

Secret ARN

arn:aws:secretsmanager:us-east-1:122627526984:secret:key-ivZC4u

Overview

Rotation

Versions

Replication

Tags

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

AWS CloudHSM key stores

External key stores

7e8e0dea-4ea7-444f-a7a9-17ddadfc2951

General configuration

Alias
custom_key

Status
Enabled

ARN
arn:aws:kms:us-east-1:122627526984:key/7e8e0dea-4ea7-444f-a7a9-17ddadfc2951

Description
-

Key policy

Cryptographic configuration

Tags

Key rotation

Aliases

Key policy

Key administrators (0)

Choose the IAM users and roles who can administer this key through the KMS API. You might need to add

Search Key administrators

Name

Path

aws

Search

[Alt+S]

IAM > Policies > secret_policy

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

Policy secret_policy updated.

secret_policy

Policy details

Type

Customer managed

Creation time

May 03, 2025, 14:05 (UTC+03:00)

Edited time

May 03, 2025, 14:16 (UT

Permissions

Entities attached

Tags

Policy versions

Last Accessed

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group,

Search

Allow (2 of 439 services)

| Service | Access level | Resource | Request condition |
|-----------------|----------------|--|-------------------|
| KMS | Limited: Write | KeyID string like [7e8e0dea-4ea7-444f-a7a9-17ddadfc2951, region string like [us-east-1 | None |
| Secrets Manager | Limited: Read | region string like [us-east-1 | None |

aws

Search

[Alt+S]

IAM > Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users groups

Policy secret_policy updated.

Roles (5)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities tha

Search

| Role name | Trusted entities | Last activity |
|--------------------|------------------|----------------|
| access_for_secrets | AWS Service: ec2 | 11 minutes ago |

Successfully attached access_for_secrets to instance i-0ce9c2bb964e84045

Instances (1/1)

Find Instance by attribute or tag (case-sensitive)

All states

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|------------------|---------------------|----------------|---------------|-------------------|--------------|
| Bastion instance | i-0ce9c2bb964e84045 | Running | t2.micro | 2/2 checks passec | View alarms |

aws

Search

[Alt+S]

IAM > Roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users groups

Policy secret_policy updated.

Roles (5)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities tha

Search

| Role name | Trusted entities | Last activity |
|--------------------|------------------|----------------|
| access_for_secrets | AWS Service: ec2 | 11 minutes ago |

Successfully attached access_for_secrets to instance i-0ce9c2bb964e84045

Instances (1/1)

Find Instance by attribute or tag (case-sensitive)

All states

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|------------------|---------------------|----------------|---------------|-------------------|--------------|
| Bastion instance | i-0ce9c2bb964e84045 | Running | t2.micro | 2/2 checks passec | View alarms |

i-0ce9c2bb964e84045 (Bastion instance)

Answer private resource DNS name

Auto-assigned IP address

98.80.224.156 [Public IP]

IAM Role

access_for_secrets

Instance type

t2.micro

VPC ID

vpc-08cae3cb9c6ce67d8 (terraform_vpc)

Subnet ID

subnet-0724411d4bb5f49ab (public-subnet)

```

ubuntu@ip-10-0-1-236:~$ aws secretsmanager get-secret-value --secret-id key
{
  "ARN": "arn:aws:secretsmanager:us-east-1:122627526984:secret:key-ivZC4u",
  "Name": "key",
  "VersionId": "a263ffdd-7ca8-4149-99ec-8fd6b432ec49",
  "SecretString": "{\"key\":\"secret\"}",
  "VersionStages": [
    "AWSCURRENT"
  ],
  "CreateDate": "2025-05-03T10:45:58.798000+00:00"
}

ubuntu@ip-10-0-1-236:~$ aws secretsmanager get-secret-value --secret-id key --qu
ery SecretString --output text
{"key":"secret"}
ubuntu@ip-10-0-1-236:~$ aws secretsmanager get-secret-value --secret-id key --qu
ery SecretString --output text | jq
{
  "key": "secret"
}

ubuntu@ip-10-0-1-236:~$ aws secretsmanager describe-secret --secret-id key
{
  "ARN": "arn:aws:secretsmanager:us-east-1:122627526984:secret:key-ivZC4u",
  "Name": "key",
  "KmsKeyId": "arn:aws:kms:us-east-1:122627526984:key/7e8e0dea-4ea7-444f-a7a9-
17ddadfc2951",
  "LastChangedDate": "2025-05-03T10:45:58.804000+00:00",
  "LastAccessedDate": "2025-05-03T00:00:00+00:00",
  "Tags": [],
  "VersionIdsToStages": {
    "a263ffdd-7ca8-4149-99ec-8fd6b432ec49": [
      "AWSCURRENT"
    ]
  },
  "CreateDate": "2025-05-03T10:45:58.744000+00:00"
}

```