



HashiCorp

Vault Active Directory Secret Engine

1 Create the IAM user with administrator access in the AWS

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Users' highlighted under 'Access management'. A yellow box with the number '1' is placed over the 'Users' link. The main content area shows the 'Summary' page for a user named 'vijay', indicated by a yellow box with the number '2' over the user name. The 'Summary' section displays the following details:

- User ARN:** arn:aws:iam::974771016253:user/vijay
- Path:** /
- Creation time:** 2020-05-15 11:58 UTC+0100

A yellow box with the number '3' is placed over the 'Creation time' value. Below the summary, there are tabs for 'Permissions', 'Groups', 'Tags (1)', 'Security credentials', and 'Access Advisor'. The 'Security credentials' tab is selected. Under this tab, the 'Sign-in credentials' section is expanded, showing a table of credentials:

Sign-in credentials	
Summary	<ul style="list-style-type: none">Console sign-in link: https://vijayendra.signin.aws.amazon.com/consoleMFA is required when signing in. Learn more
Console password	Enabled (last signed in 221 days) Manage
Assigned MFA device	arn:aws:iam::974771016253:mfa/vijay (Virtual) Manage
Signing certificates	None



2

Create the Access Key for the users

if you need to rotate your secret key, you cannot rotate it in place, create a new access key and make the old key inactive. [Learn more](#)

Create access key

4

Access key ID	Created	Last used	Status
No results			

3

set the access key and key id

```
root@Vault-server-01 ~]# export AWS_ACCESS_KEY_ID=AKIA6F5HBKI6WKZ22O5J
root@Vault-server-01 ~]# export AWS_SECRET_ACCESS_KEY=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
```

4

configure the AWS secret Engine

```
[root@Vault-server-01 ~]# vault write aws/config/root \
> access_key=$AWS_ACCESS_KEY_ID \
> secret_key=$AWS_SECRET_ACCESS_KEY
Success! Data written to: aws/config/root
[root@Vault-server-01 ~]#
```



5

create the IAM role Using Vault

```
[root@Vault-server-01 ~]# vault write aws/roles/my-role \
credential_type=iam_user \
policy_document=<<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1426528957000",
      "Effect": "Allow",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
EOF
```

6

Secret key and Access key is automatically created using vault

```
[root@Vault-server-01 ~]# vault read aws/creds/my-role
Key          Value
----
lease_id     aws/creds/my-role/3mVt0FiYqv6cXgXQ0711je9R
lease_duration 768h
lease_renewable true
access_key    AKIA6F5HBKI626WNGQN3
secret_key    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
security_token <nil>
[root@Vault-server-01 ~]#
```

7

vault will create random user with associate with access key and mentioned IAM Policy

Find users by username or access key						
<input type="checkbox"/>	User name ▾	Groups	Access key age	Last activity	Creation time ▾	Group count
<input type="checkbox"/>	raj	None	None	221 days	2020-08-25 12:33 UTC+0100	0
<input type="checkbox"/>	rohit	None	None	247 days	2020-05-08 11:49 UTC+0100	0
<input type="checkbox"/>	vault-root-m...	None	✓ Today	None	2021-04-04 05:37 UTC+0100	0
<input type="checkbox"/>	vijay	None	✓ Today	221 days	2020-05-15 11:58 UTC+0100	0



8

once the lease is revoked the credential get deleted from aws

```
root@Vault-server-01 ~]# vault lease revoke aws/creds/my-role/3mVt0FiYqv6cXgXQ0711je9R
All revocation operations queued successfully!
root@Vault-server-01 ~]#
```

9

user deleted from aws console

<input type="checkbox"/>	User name ▾	Groups	Access key age	Password age	Last activity	MFA	Cred
<input type="checkbox"/>	raj	None	None	221 days	221 days	Not enabled	2020
<input type="checkbox"/>	rohit	None	None	247 days	247 days	Not enabled	2020
<input type="checkbox"/>	vijay	None	None	323 days	221 days	Virtual	2020