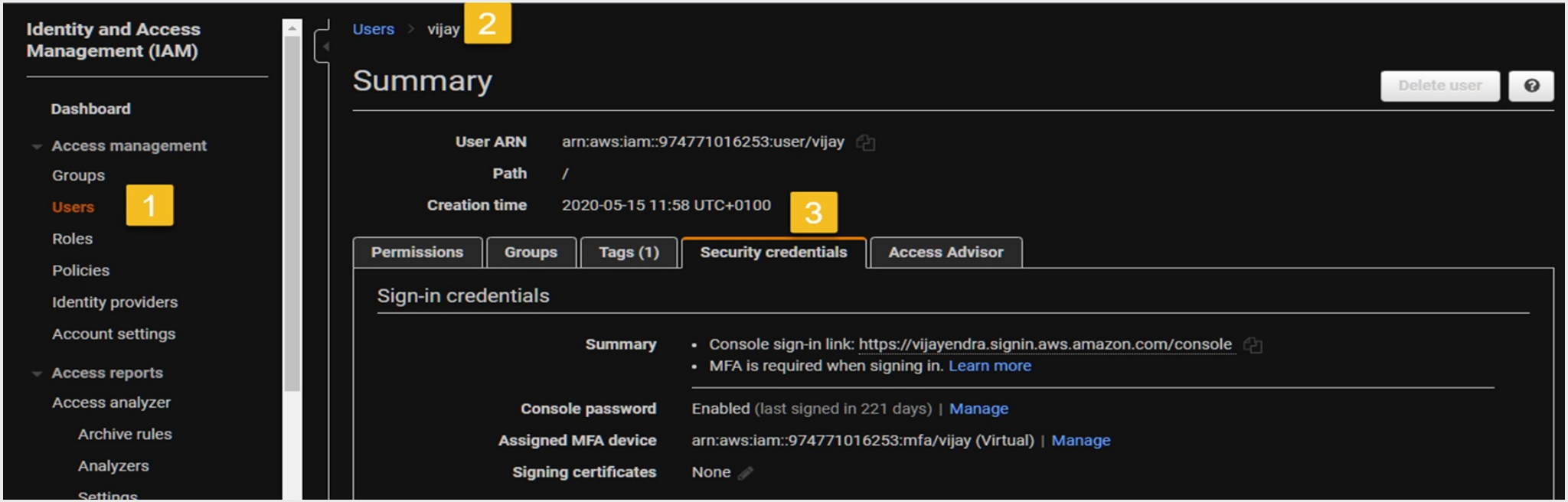
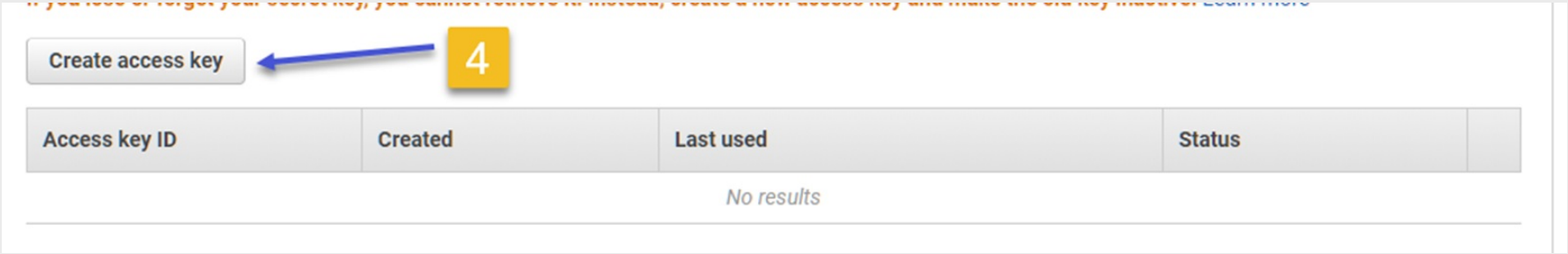
HashiCorp Vault Active Directory Secret Engine

1 Create the IAM user with administrator access in the AWS



HashiCorp Vault Active Directory Secret Engine

2 Create the Access Key for the users



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 ~]#
```

HashiCorp Vault Active Directory Secret Engine

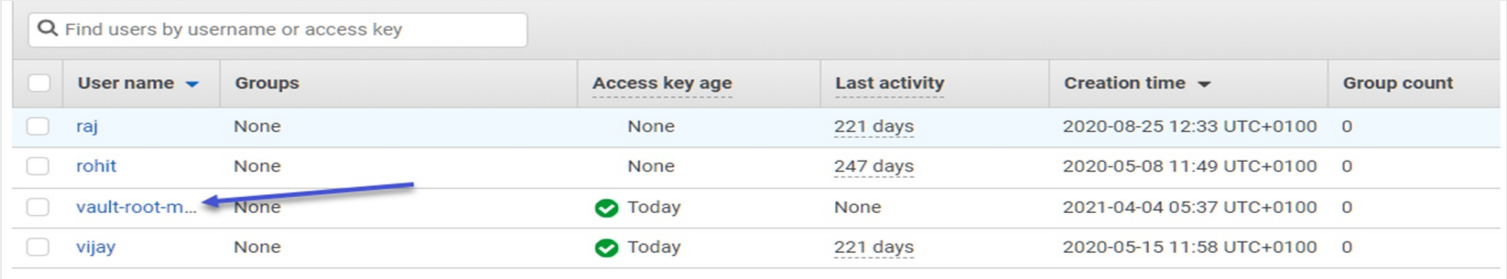
5 create the IAM role Using Vault

```
[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/3mVtOFiYqv6cXgXQ0711je9R
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



HashiCorp Vault Active Directory Secret Engine

8 once the lease is revoked the credential get deleted from aws

```
root@Vault-server-01 ~]#
root@Vault-server-01 ~]# vault lease revoke aws/creds/my-role/3mVtOFiYqv6cXgXQO711je9R
ll revocation operations queued successfully!
root@Vault-server-01 ~]#
```

9 user deleted from aws console

User name	Groups	Access key age	Password age	Last activity	MFA	Crea
raj	None	None	221 days	221 days	Not enabled	202(
rohit	None	None	247 days	247 days	Not enabled	202(
vijay	None	None	323 days	221 days	Virtual	202(