Overview

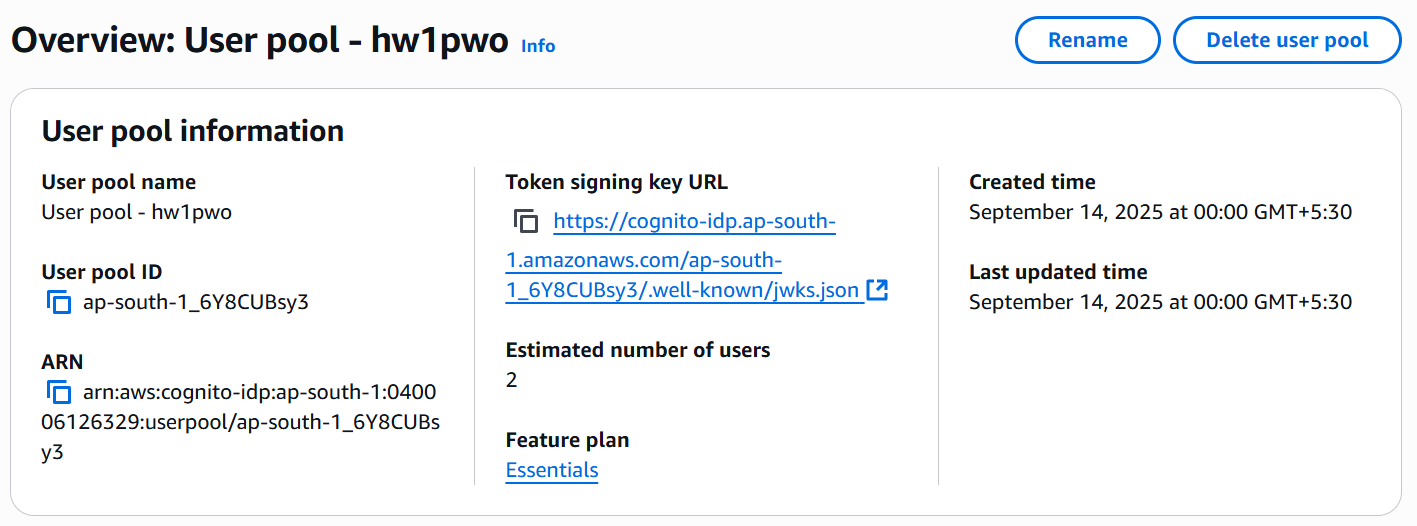
This API provides secure access to a resource using AWS Cognito for user authentication. Users must log in via Cognito to obtain a token, which is then used to authorize API requests.

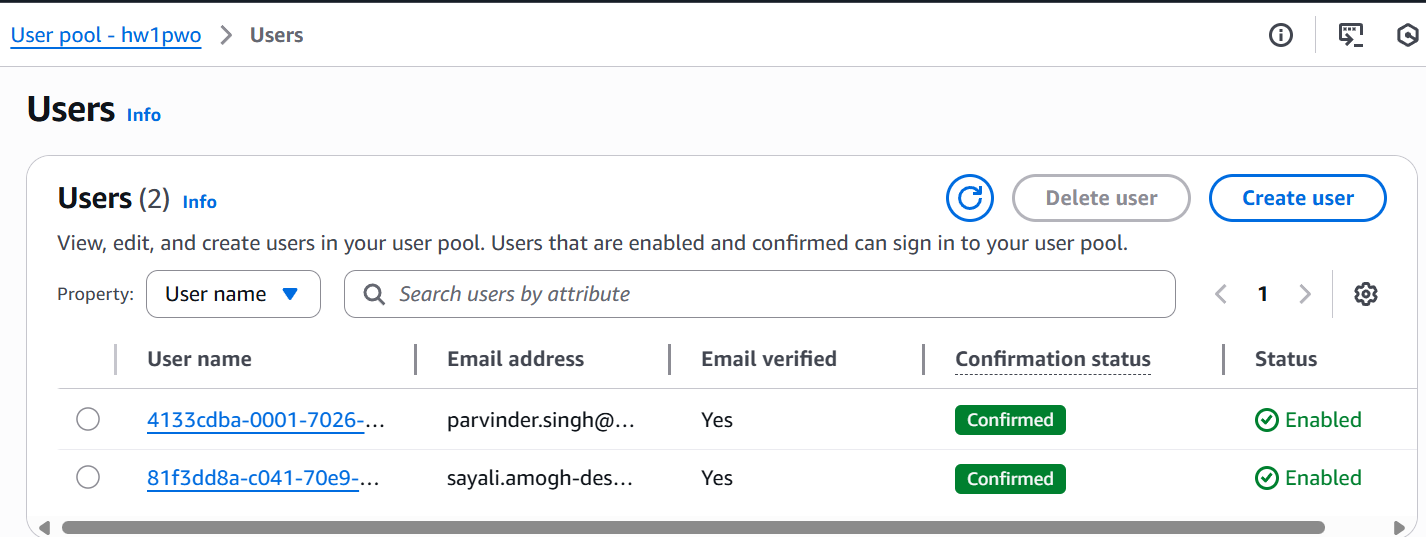
Endpoints

1. User Login

URL: <https://cognito-idp.ap-south-1.amazonaws.com/ap-south-1_6Y8CUBsy3/.well-known/jwks.json>

Description: Authenticates a user and retrieves a Cognito ID token.





2. API Gateway Lambda Function

Create a Lambda function to handle secure resource requests.

Python import json

def lambda\_handler(event, context):

# Extract token from Authorization header

token = event['headers'].get('Authorization', '').split(' ')[1]

# Validate token (this is a simplified example)

if not token:

return {

"statusCode": 401,

"body": json.dumps({"message": "Unauthorized"})

}

# Return secure resource

return {

"statusCode": 200,

"body": json.dumps({

"message": "This is a secure resource",

"data": {"example": "value"}

})

}

3. Deploy API Gateway

Use AWS API Gateway to create a REST API.

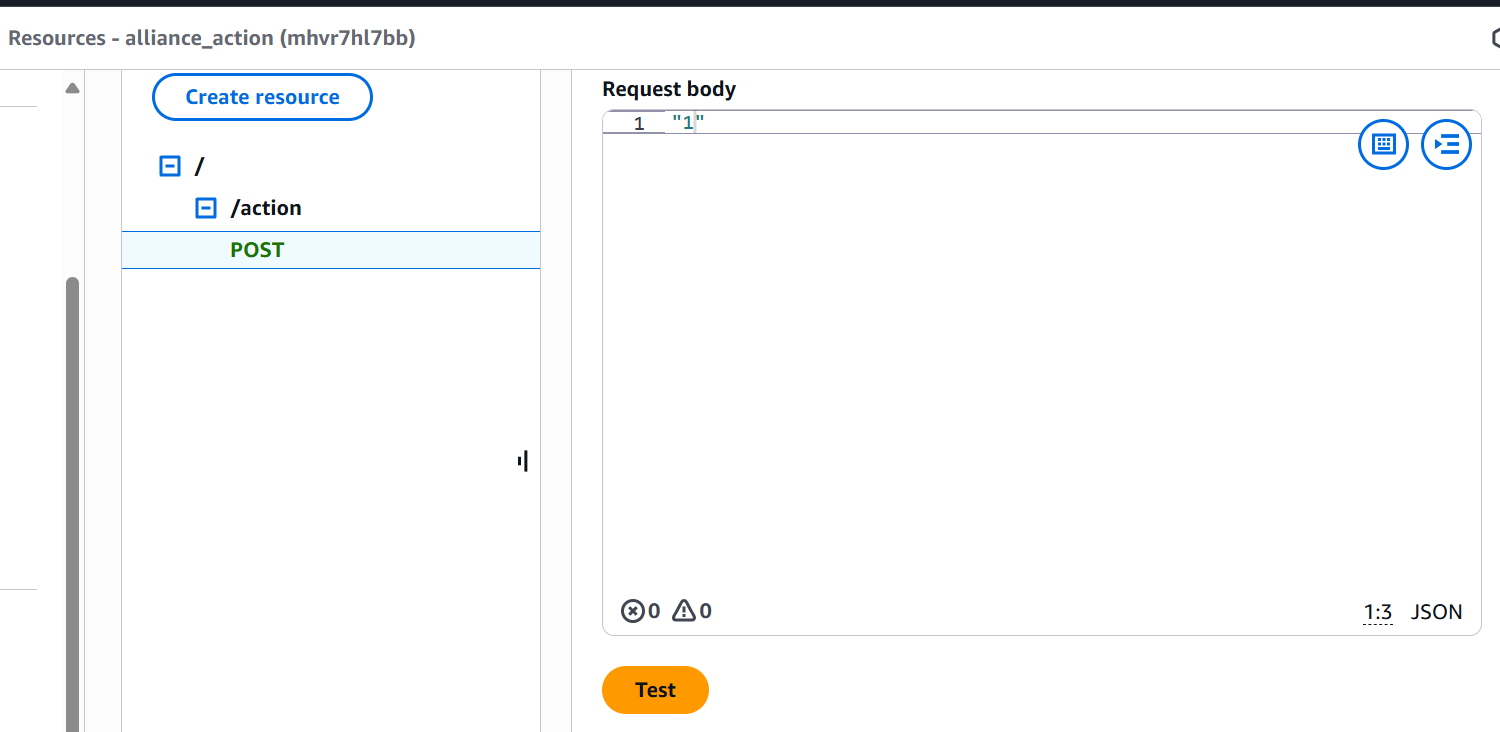
Configure Cognito User Pool Authorizer for the /secure-resource endpoint.

Attach the Lambda function to the /secure-resource endpoint.

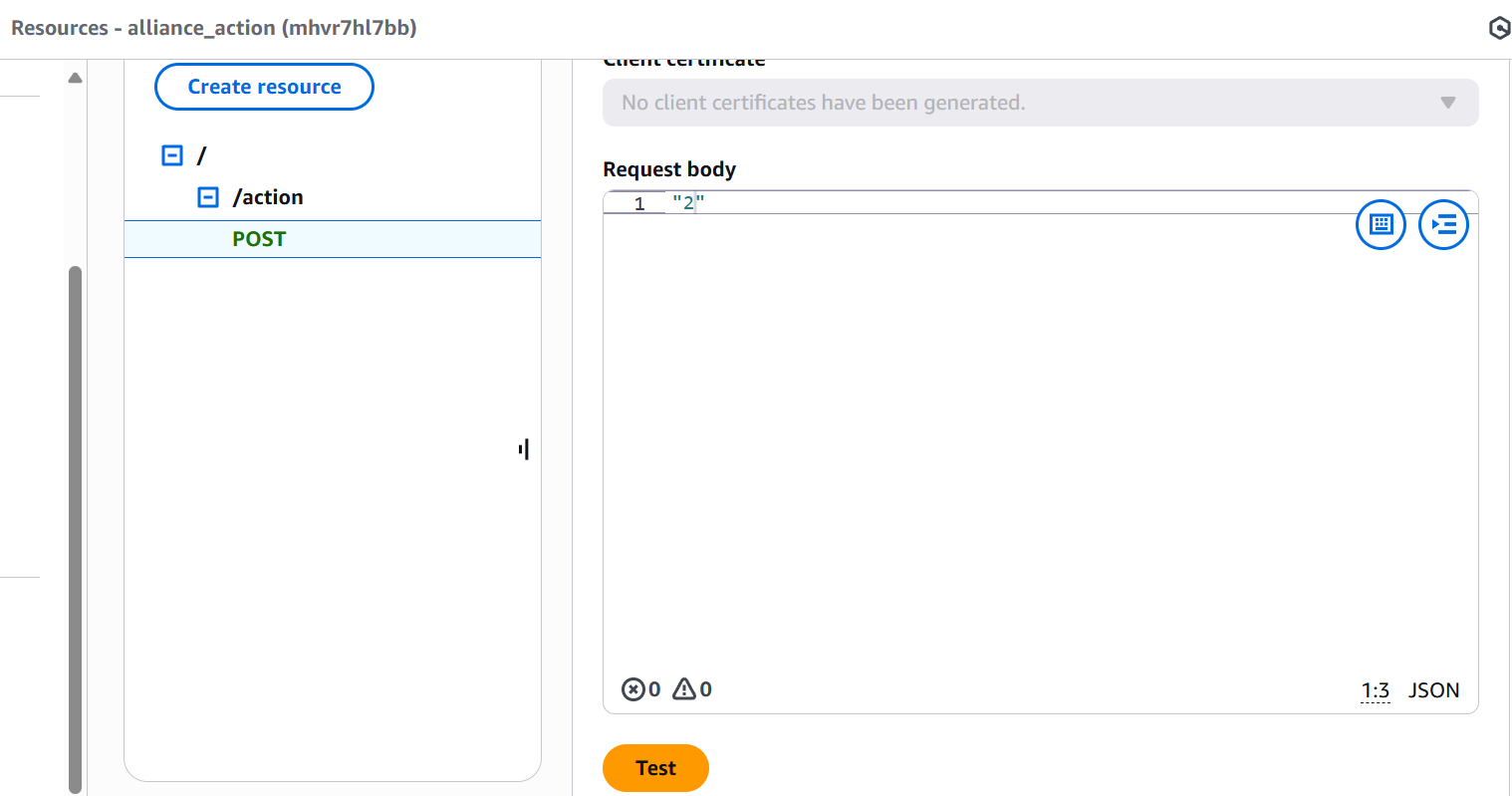
This method will not require separate lambda authorizer and validates user using cognito authorizer.

Testing the API

For AWS we can send action event as “1” for create and start instance and “2” for stop and delete instance.



If testing from console Auth token is called internally from cognito if authorizer is attached or we need to write separate lambda authorizer.



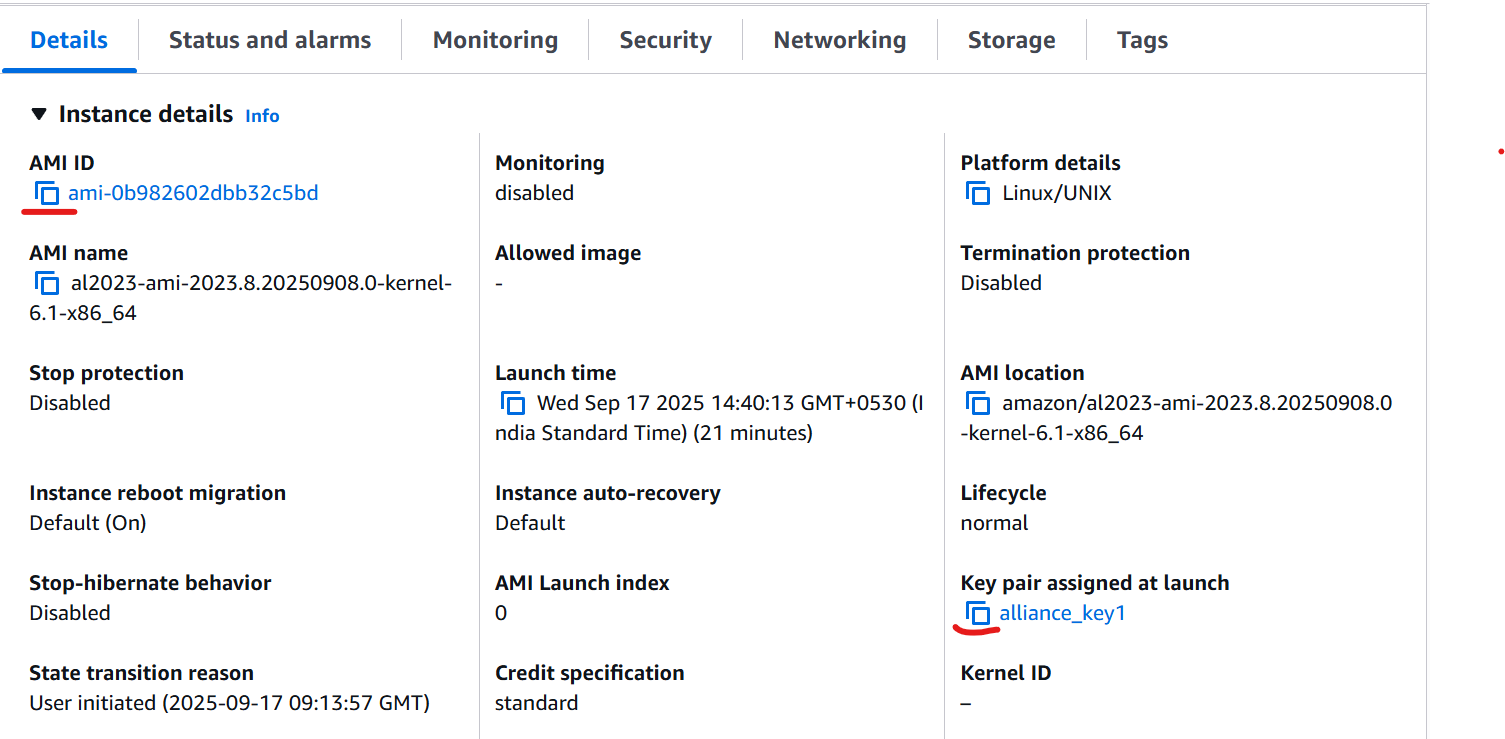
Login: Send a POST request to /login with valid credentials to retrieve the id\_token.

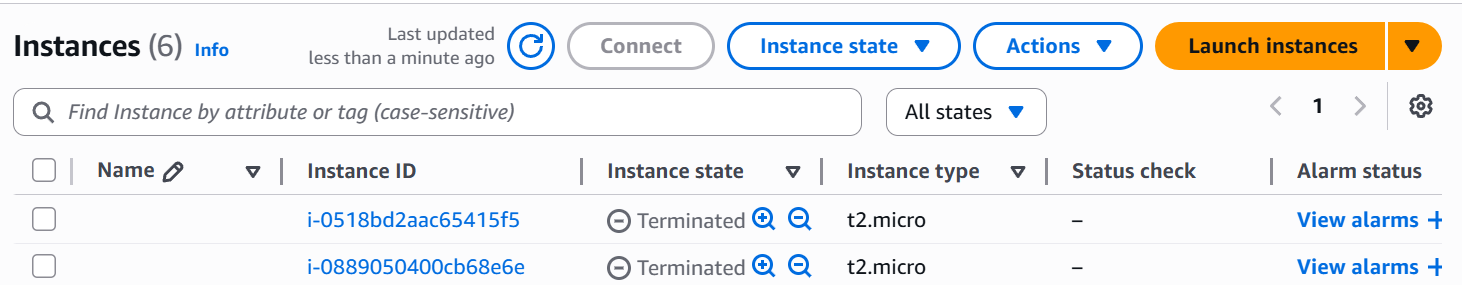
Access Secure Resource:

Use the id\_token in the Authorization header to access /secure-resource.

This setup ensures that only authenticated users can access the secure resource, leveraging AWS Cognito for robust user management and authentication.

We can see instances created and terminated in EC2 console with instance details.





Cloudwatch Logs:

We can see logs generated with key details, instance id, ip address and ssh command.

User must be asked to store this key with keyname mentioned in ssh command or can be asked to choose key name and lambda function can be modified accordingly.

In Current code key pair is generated using random numbers as id with fix header.

