Lab 06

COS20019

CLOUD COMPUTING ARCHITECTURE

Tran Thanh Minh

Step 1: Explore the users and groups

1. Effect says whether allow or deny the permissions, action specifies the API calls that can be made against an AWS service, resource defines the scope of entities covered by the policy ruleA screenshot of a computer

   Description automatically generated with medium confidence
2. S3-support group has the permission to access the amazon s3A screenshot of a computer

   Description automatically generated
3. Inline policy which is a policy assigned to just one user or groupA screenshot of a computer

   Description automatically generated

Task 2: add users to groups

1. Add user 1 to s3 support groupA screenshot of a computer

   Description automatically generated
2. Add user 2 to ec2-support groupA screenshot of a computer

   Description automatically generated with medium confidence
3. Add user 3 to ec2-admin groupA screenshot of a computer

   Description automatically generated

Task 3: sign in and test users

1. Get the URL for the IAM users signin linkA screenshot of a computer

   Description automatically generated
2. User-1 can’t access to ec2A screenshot of a computer

   Description automatically generated
3. User-2 can view the ec2 but can’t stop the ec2A screenshot of a computer

   Description automatically generated with medium confidence
4. User 2 don’t have permission to see the bucket A screenshot of a computer

   Description automatically generated
5. User 3 has permission to stop the instance A screenshot of a computer

   Description automatically generated