

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 rule

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Access management' expanded and 'User groups' selected. The main content area shows the 'Permissions policies (1)' page. A table lists the policy 'AmazonEC2ReadOnlyAccess', which is 'AWS managed' and 'Provides read only access to Amazon ...'. Below the table, the policy's JSON definition is shown in a code editor. The JSON defines three statements, each with an 'Effect' of 'Allow' and specific actions on various AWS resources.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:Describe*",
7       "Resource": "*"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "elasticloadbalancing:Describe*",
12      "Resource": "*"
13    },
14    {
15      "Effect": "Allow",
16      "Action": [
17        "cloudwatch:ListMetrics",
18        "cloudwatch:GetMetricStatistics",
19        "cloudwatch:Describe*"
20      ],
21      "Resource": "*"
22    },
23    {
24      "Effect": "Allow",
25      "Action": "autoscaling:Describe*",
26      "Resource": "*"
27    }
28  ]
29 }
```

2. S3-support group has the permission to access the amazon s3

The screenshot shows the AWS IAM console for the 'S3-Support' user group. The 'Permissions' tab is selected, showing one attached policy: 'AmazonS3ReadOnlyAccess'. The policy is an AWS managed policy that provides read-only access to all buckets via the AWS Management Console. The JSON policy document is displayed below the policy name.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3:List*",
9         "s3-object-lambda:Get*",
10        "s3-object-lambda:List*"
11      ],
12       "Resource": "*"
13     }
14   ]
15 }
```

3. Inline policy which is a policy assigned to just one user or group

The screenshot shows the AWS IAM console for the 'EC2-Admin' user group. The 'Permissions' tab is selected, showing one attached policy: 'EC2-Admin-Policy'. The policy is a customer inline policy that allows actions on EC2 instances. The JSON policy document is displayed below the policy name.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "ec2:Describe*",
7         "ec2:StartInstances",
8         "ec2:StopInstances"
9       ],
10      "Resource": [
11        "*"
12      ],
13      "Effect": "Allow"
14    }
15   ]
16 }
```

Task 2: add users to groups

1. Add user 1 to s3 support group

The screenshot shows the AWS IAM console interface. At the top, a green banner indicates "Users added to this group." The breadcrumb navigation shows "IAM > User groups > S3-Support". The main heading is "S3-Support" with "Delete" and "Edit" buttons. Below is a "Summary" section with a table containing the following data:

User group name	Creation time	ARN
S3-Support	June 22, 2023, 22:34 (UTC+07:00)	arn:aws:iam::161847276488:group/spl66/S3-Support

Below the summary are tabs for "Users", "Permissions", and "Access Advisor". The "Users" tab is active, showing "Users in this group (1)". A search bar and pagination controls are present. The table below lists the users in the group:

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	user-1	1	None	12 minutes ago

2. Add user 2 to ec2-support group

The screenshot shows the AWS IAM console interface. At the top, a green banner indicates "Users added to this group." The breadcrumb navigation shows "IAM > User groups > EC2-Support". The main heading is "EC2-Support" with "Delete" and "Edit" buttons. Below is a "Summary" section with a table containing the following data:

User group name	Creation time	ARN
EC2-Support	June 22, 2023, 22:34 (UTC+07:00)	arn:aws:iam::161847276488:group/spl66/EC2-Support

Below the summary are tabs for "Users", "Permissions", and "Access Advisor". The "Users" tab is active, showing "Users in this group (1)". A search bar and pagination controls are present. The table below lists the users in the group:

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	user-2	1	None	13 minutes ago

3. Add user 3 to ec2-admin group

The screenshot shows the AWS IAM console interface. At the top, a green banner indicates "Users added to this group." Below this, the breadcrumb navigation shows "IAM > User groups > EC2-Admin". The main heading is "EC2-Admin" with "Delete" and "Edit" buttons. Under the "Summary" tab, the following details are listed:

User group name	Creation time	ARN
EC2-Admin	June 22, 2023, 22:34 (UTC+07:00)	arn:aws:iam::161847276488:group/spl66/EC2-Admin

Below the summary, there are tabs for "Users", "Permissions", and "Access Advisor". The "Users" tab is active, showing "Users in this group (1)". A search bar and pagination controls are present. The table below lists the users in the group:

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	user-3	1	None	14 minutes ago

Task 3: sign in and test users

1. Get the URL for the IAM users signin link

The screenshot shows the AWS IAM dashboard. The "Security recommendations" section has a red alert icon and the text "Add MFA for root user". The "IAM resources" section displays a summary of resources:

User groups	Users	Roles	Policies	Identity providers
3	4	14	1	0

The "What's new" section lists updates for features in IAM. On the right, the "AWS Account" section displays account information:

- Account ID: 161847276488
- Account Alias: 161847276488
- Sign-in URL for IAM users in this account: <https://161847276488.signin.aws.amazon.com/console>

The "Tools" section includes links to the "Policy simulator" and "Web identity federation playground".

2. User-1 can't access ec2

The screenshot shows the AWS Management Console interface for the "Instances" page. The breadcrumb navigation shows "Instances > Info". The main heading is "Instances" with "Connect", "Instance state", "Actions", and "Launch instances" buttons. A search bar is present. Below the search bar, a table header is visible with columns: "Name", "Instance ID", "Instance state", "Instance type", "Status check", and "Alarm status". A message in the center of the page states: "You are not authorized to perform this operation." At the bottom, there is a "Select an instance" button.

3. User-2 can view the ec2 but can't stop the ec2

The screenshot shows the AWS Management Console interface for User-2. A red error banner at the top states: "Failed to stop the instance i-04c33944656f51a0d. You are not authorized to perform this operation. Encoded authorization failure message: ZcUJwc5RLZmk2suSzkVuDYump-VSzsVKCB6G4ko9GHqj7KoyQnkX5KSyoNOAUjspe_z9JtdYqefZfMry8sKkEhmQnS3w-rQxF1EDm_TftRPqE0dTdKmSXyVTOybdOFIjmWbSJsB9s_Volh2tTSF16QJ70U9LEcZtwDleqf2LS9uoUX8xYgVUcqBG-7a5mkqISNZInt48169o64NDw5P3a9rVwcOHqrbqO1iqKwLYbOywYibVzPAeyWvMCTFCTuG585tk_miOYPM8fblPpM6SoqgFC771zQ8kc3RuFixKk0i4Fx4-10M_JVzclloWfuHYHM0VXNZULSqv3n42hXJzCp_E8VARlmafkaZefz_zCT4GHf6a2arqy3VaU-_vH6R2fi306tkVoA5FOsolvM34bu4ao6r3n_uat1ZP1RxilgVGsWN2OCawmYxOSZarY0zBMzdumRf1JFC3F197UDJkAFsijSRlZUu9gvYxsuy9mA-sJ0Lwu71m5Ea26LfjWTrxcy_C8biTkwz-YE_Ov5sJFvKmi5Yne3Da4-A71NzXOWwzot2cvqZ8yUGWfftdc0PRf9NTXBnDuWsmQmwaaitM2Cyc07i30tbZrMOy0VoJfhk1Ud32_nkO6iaDaOxvLbSezKpRzzG1N0pGRwlnLRcWgNVldnN5w-mf3thTuVBnYmaSM7zsayk3WnpKkALecHP6Jn5NBzGopAioTgtwtQWbGh4kmF-1O-ia6mWdUOLJ9HlzkOiuqtO-ivw3c6c39TNQ5x_PVd_8-VBxKWIOlgkzgzpi7PIFwS6YF5hRLh5CqbR4E5wCO8qfMxOC1T9JRd2UMdviHpg9Un4EUymykhjSF7diCsjFLhDCB_SFCS4eucWbUoxmIOaRezjmL6_9HjhMBgcz20sx7sOpqsdUgdSvohcEW-MfkLqXooyFLDepW35TXFS-zkKbZO2URd6ZF-I5V8EfgeMLMajCGh1uXYOP3iINNBXeni_JuQ475eDw". Below the error, the details for instance i-04c33944656f51a0d (LabHost) are visible, showing it is in a "Running" state.

4. User 2 don't have permission to see the bucket

The screenshot shows the AWS Management Console interface for User-2. A red error banner at the top states: "You don't have permissions to list buckets. After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3". Below the error, the "Buckets" section is visible, showing a search bar and a table with columns: Name, AWS Region, Access, and Creation date.

5. User 3 has permission to stop the instance

The screenshot shows the AWS Management Console interface for User-3. A green success banner at the top states: "Successfully stopped i-04c33944656f51a0d". Below the banner, the "Instances (1/2)" section is visible, showing a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 D. The table lists two instances: "Bastion Host" (i-0bd9798cd7bee0c0d) in "Running" state and "LabHost" (i-04c33944656f51a0d) in "Stopping" state. Below the table, the details for instance i-04c33944656f51a0d (LabHost) are visible, showing it is in a "Stopping" state.