

Task_Day_1

1- Create AWS account

2- Create 2 IAM Groups, Create 2 users one for each group with different permissions

The screenshot shows the AWS IAM User Groups page. A breadcrumb navigation bar at the top indicates: IAM > User groups > dev. The main title is "dev". On the right, there are "Delete" and "Edit" buttons. Below the title, a "Summary" section displays the following details:

User group name	Creation time	ARN
dev	March 15, 2022, 11:37 (UTC+03:00)	arn:aws:iam::663628946494:group/dev

Below the summary, there are three tabs: "Users" (selected), "Permissions", and "Access Advisor". The "Users" tab shows a table for "Users in this group (1)". The table has columns: "User name", "Groups", "Last activity", and "Creation time". One user, "bayader", is listed with 1 group, last activity at "None" (3 minutes ago), and creation time at "3 minutes ago". Action buttons for "Search", "Remove users", and "Add users" are located above the table.

The screenshot shows the AWS IAM User Groups page, identical to the one above, displaying the "dev" user group. The "Summary" section, tabs, and "Users" table are all present, showing the same information as the first screenshot.

IAM > User groups > ops

ops

Delete Edit

Summary

User group name ops	Creation time March 15, 2022, 11:38 (UTC+03:00)	ARN arn:aws:iam::663628946494:group/ops
------------------------	--	--

Users Permissions Access Advisor

Users in this group (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

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

Search Remove users Add users

IAM > User groups > ops

ops

Delete Edit

Summary

User group name ops	Creation time March 15, 2022, 11:38 (UTC+03:00)	ARN arn:aws:iam::663628946494:group/ops
------------------------	--	--

Users Permissions Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AWSDirectConnectReadOnlyAccess	AWS manag...	Provides read only access to AWS Direct Connect via the AWS Management ...

Filter policies by property or policy name and press enter Simulate Remove Add permissions

4- Create EC2 instance with the given script in user data and try to access it from web browser.

The screenshot shows the AWS EC2 Management Console. At the top, there's a search bar and a toolbar with buttons for 'Connect', 'Actions', and 'Launch Instances'. Below the toolbar is a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IP. One row is selected, showing 'i-0cf95b490842233b1' as the Instance ID, 'Running' as the Instance state, 't2.micro' as the Instance type, and 'us-east-1a' as the Availability Zone. The Public IP is listed as 'ec2-3-84-27-102.compute-1.amazonaws.com'. On the right side of the table, there are several small icons representing different services like S3, Lambda, and CloudWatch.

Instance: i-0cf95b490842233b1

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary

Instance ID i-0cf95b490842233b1	Public IPv4 address 3.84.27.102	Private IPv4 addresses 172.31.84.168
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-3-84-27-102.compute-1.amazonaws.com
Hostname type IP name: ip-172-31-84-168.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-84-168.ec2.internal	Answer private resource DNS name IPv4 (A)

The screenshot shows a browser window with the title 'Instances | EC2 Management Console'. The address bar shows the IP address '3.84.27.102'. The main content of the browser is a single line of text: "Hello World from ip-172-31-84-168.ec2.internal".

5- Connect to your EC2 in (task 4) and download your static website (from github or local device) then add it to root directory of the apache server then access your website from your browser.

The screenshot shows a browser window with the title 'Not Secure — 3.84.27.102'. The address bar shows the IP address '3.84.27.102'. The main content of the browser is the text "Hello bayader".

6- Create 3 SG:

- web_sg and allow http requests from all to be access publicly.

The screenshot shows the AWS EC2 Security Groups console. The top navigation bar includes 'EC2' and 'Security Groups'. Below it, the specific security group is identified as 'sg-0f2409848217376cd - web-sg'. On the right, there is an 'Actions' dropdown menu. The main area displays the 'Details' tab, which contains the following information:

Security group name web-sg	Security group ID sg-0f2409848217376cd	Description allows http traffic	VPC ID vpc-0fe101bdefe7a305e
Owner 663628946494	Inbound rules count 0 Permission entries	Outbound rules count 1 Permission entry	

Below the details, there are tabs for 'Inbound rules' (which is selected), 'Outbound rules', and 'Tags'. A message at the top of the 'Inbound rules' section says, 'You can now check network connectivity with Reachability Analyzer', with buttons for 'Run Reachability Analyzer' and 'X'. The 'Inbound rules' table has columns for Name, Security group rule..., IP version, Type, and Protocol. A search bar and a 'Manage tags' button are also present. The message 'No security group rules found' is displayed at the bottom of the table.

- app_sg and allow http requests only from SGs (web_app and db_app).

sg-0662df88755b7e2c1 - app-sg				Actions ▾
Details				
Security group name app-sg	Security group ID sg-0662df88755b7e2c1	Description allow http requests only from SGs (web_app and db_app)	VPC ID vpc-0fe101bdefe7a305e	
Owner 663628946494	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry		

[Inbound rules](#) [Outbound rules](#) [Tags](#)

ⓘ You can now check network connectivity with Reachability Analyzer

[Run Reachability Analyzer](#)

X

Inbound rules (2)

C

Manage tags

Edit inbound rules

Filter security group rules

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-001568bf2556ee0f6	-	Custom TCP	TCP
<input type="checkbox"/>	-	sgr-0723fab32302e2539	-	Custom TCP	TCP

- db_sg and allow http requests only from SG(web_app) on port 3306.

sg-0b169b8ce25ac98f1 - db-sg

Actions ▾

Details

Security group name db-sg	Security group ID sg-0b169b8ce25ac98f1	Description allow http requests only from SG(web_app)	VPC ID vpc-0fe101bdefe7a305e
Owner 663628946494	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

[Inbound rules](#) [Outbound rules](#) [Tags](#)

ⓘ You can now check network connectivity with Reachability Analyzer

[Run Reachability Analyzer](#)

X

Inbound rules (1/1)

C

Manage tags

Edit inbound rules

Filter security group rules

< 1 >

⚙

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input checked="" type="checkbox"/>	-	sgr-0accbb6c7de4211b7	-	MySQL/Aurora	TCP

7- Create 3 EC2 with one tag (Name) for each one (web_server, app_server, db_server) and attached each server with its respective SG.

The screenshot shows the AWS EC2 Instances page with three instances listed:

- Instance 1:** web_server (i-Oee6526a774d439d4) - Running, t2.micro, No alarms. Security group sg-Of2409848217376cd (web-sg).
- Instance 2:** app_server (i-0c3a031f7d11e6719) - Running, t2.micro, No alarms. Security group sg-0662df88755b7e2c1 (app-sg).
- Instance 3:** db_server (i-0cf95b490842233b1) - Running, t2.micro, 2/2 checks passed, Initializing. Security group -.

Details for the web_server instance:

Security details	
IAM Role	Owner ID
-	663628946494
Security groups	Launch time
sg-Of2409848217376cd (web-sg)	Tue Mar 15 2022 15:48:23 GMT+0300 (+03)

Details for the app_server instance:

Security details	
IAM Role	Owner ID
-	663628946494
Security groups	Launch time
sg-0662df88755b7e2c1 (app-sg)	Tue Mar 15 2022 15:55:55 GMT+0300 (+03)

Instances (1/4) [Info](#)

[⟳](#) [Connect](#) [Instance state ▾](#) [Actions ▾](#)

[Search](#)

-	Name ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alar
<input type="checkbox"/>	-	i-0cf95b490842233b1	Running ⊕ ⊖	t2.micro	2/2 checks passed	No a
<input type="checkbox"/>	web_server	i-0ee6526a774d439d4	Running ⊕ ⊖	t2.micro	2/2 checks passed	No a
<input type="checkbox"/>	app_server	i-0c3a031f7d11e6719	Running ⊕ ⊖	t2.micro	Initializing	No a
<input checked="" type="checkbox"/>	db_server	i-0f78d678233592fad	Running ⊕ ⊖	t2.micro	-	No a

Instance: i-0f78d678233592fad (db_server)

[Details](#) | **Security** | [Networking](#) | [Storage](#) | [Status checks](#) | [Monitoring](#) | [Tags](#)

▼ Security details

IAM Role -	Owner ID 663628946494	Launch time Tue Mar 15 2022 15:5
Security groups sg-0b169b8ce25ac98f1 (db-sg)		

▼ Inbound rules