

AWS Cloud & Big Data Architectures

Project

Mohammed Saber BELLAAZIRI

Bouthayna ATIK

SE1

Task 1 (App deployment)

Launch an EC2 instance using the AMI Cloud9AmazonLinux2-2023-06-22T17-21

The left screenshot shows the 'Amazon Machine Image (AMI)' selection step. The user has chosen 'Cloud9AmazonLinux2-2023-06-22T17-21' from the catalog. The right screenshot shows the 'Launch an instance' confirmation step, indicating a successful launch of instance i-05568ba81e5fc03fd.

Download the SQL dump file and move it to a suitable location on the EC2 instance.

```
https://aws.amazon.com/amazon-linux-2/
17 package(s) needed for security, out of 19 available
Run "sudo yum update" to apply all updates.
[root@ip-172-31-83-35 ~]# cd -
[root@ip-172-31-83-35 ~]# wget https://efrei-capstone.s3.amazonaws.com/Countrydatadump.sql
--2023-07-12 16:54:38-- https://efrei-capstone.s3.amazonaws.com/Countrydatadump.sql
Resolving efrei-capstone.s3.amazonaws.com (efrei-capstone.s3.amazonaws.com)... 54.231.73.11, 3.5.2.122, 3.5.27.169, ...
Connecting to efrei-capstone.s3.amazonaws.com (efrei-capstone.s3.amazonaws.com)|54.231.73.11|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15508 (15K) [binary/octet-stream]
Saving to: 'Countrydatadump.sql'

100%[=====] 15,508 --.-K/s   in 0s

2023-07-12 16:54:38 (93.7 MB/s) - 'Countrydatadump.sql' saved [15508/15508]

[root@ip-172-31-83-35 ~]# ls
Countrydatadump.sql
[root@ip-172-31-83-35 ~]# mv Countrydatadump.sql /home/ec2-user/
[root@ip-172-31-83-35 ~]# cd /home/ec2-user/
[root@ip-172-31-83-35 ec2-user]# ls
Countrydatadump.sql  environment  node_modules  package.json  package-lock.json
[root@ip-172-31-83-35 ec2-user]# 
```

i-05568ba81e5fc03fd (aws_project)
PublicIPs: 44.205.255.31 PrivateIPs: 172.31.83.35

The screenshot shows the AWS EC2 Instances page. On the left, a sidebar navigation includes 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Instances' (selected), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', and 'Capacity Reservations'. Under 'Images', it lists 'AMIs' and 'AMI Catalog'. Under 'Elastic Block Store', it lists 'Volumes' and 'Snapshots'. Under 'Network & Security', it lists 'Lifecycle Manager'. At the bottom of the sidebar are links for 'CloudShell', 'Feedback', and 'Language'. The main content area displays a table titled 'Instances (1/1) Info' with one row. The row details are: Name (aws_project), Instance ID (i-05568ba81e5fc03fd), Instance state (Pending), Instance type (t2.micro), Status check (-), Alarm status (No alarms), Availability Zone (us-east-1a), and Public IP (172.31.83.35). Below the table, a detailed view for 'Instance: i-05568ba81e5fc03fd (aws_project)' is shown with tabs for 'Details', 'Security', 'Networking', 'Storage', 'Status checks', 'Monitoring', and 'Tags'. The 'Details' tab is selected, showing fields like Instance ID, Public IPv4 address (44.205.255.31), Instance state (Pending), Hostname type (IP name: ip-172-31-83-35.ec2.internal), Private IP DNS name (ip-172-31-83-35.ec2.internal), Instance type (t2.micro), and Elastic IP addresses (172.31.83.35).

Create a custom Amazon VPC:

The screenshot shows the 'Create VPC' settings page. The 'VPC settings' section contains the following fields:

- Resources to create:** A radio button group with 'VPC only' selected (highlighted in blue) and 'VPC and more' unselected.
- Name tag - optional:** A text input field containing 'my-awsproject-vpc'.
- IPv4 CIDR block:** A dropdown menu with 'IPv4 CIDR manual input' selected (highlighted in blue) and 'IPAM-allocated IPv4 CIDR block' unselected.
- IPv4 CIDR:** A text input field containing '10.0.0.0/16'.
- IPv6 CIDR block:** A dropdown menu with 'No IPv6 CIDR block' selected (highlighted in blue) and three other options: 'IPAM-allocated IPv6 CIDR block', 'Amazon-provided IPv6 CIDR block', and 'IPv6 CIDR owned by me'.
- Tenancy:** A dropdown menu with 'Default' selected.

At the bottom of the page, there are links for 'CloudShell', 'Feedback', and 'Language', and a footer with copyright information: '© 2023, Amazon Web Services, Inc. or its affiliates.' and links for 'Privacy', 'Terms', and 'Cookie preferences'.

You successfully created **vpc-0b1e1d26ad4714f5e / my-awsproject-vpc**

Details **Info**

VPC ID vpc-0b1e1d26ad4714f5e	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-08c332ab351e666be	Main route table rtb-06b3bb8d97c42539c	Main network ACL acl-028287e34fcc82694
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 00233282585	

Resource map **New** | CIDRs | Flow logs | Tags

Resource map **Info**

- VPC **Show details** Your AWS virtual network my-awsproject-vpc
- Subnets (0) Subnets within this VPC
- Route tables (1) Route network traffic to resources rtb-06b3bb8d97c42539c

Create public and private subnets within the VPC:

Subnets (8) **Info**

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
-	subnet-0d468a7a4927377e3	Available	vpc-07e0cf812a795e9a	172.31.48.0/20	-
-	subnet-0250d694eab85f675	Available	vpc-07e0cf812a795e9a	172.31.0.0/20	-
-	subnet-0692c5e8bc8b0c4ef	Available	vpc-07e0cf812a795e9a	172.31.16.0/20	-
-	subnet-0f8dd6c2833013fe6	Available	vpc-07e0cf812a795e9a	172.31.80.0/20	-
my-private-project-...	subnet-063329c7a151d60b1	Available	vpc-0b1e1d26ad4714f5e my...	10.0.1.0/24	-
-	subnet-09f51e8b657fdfe01	Available	vpc-07e0cf812a795e9a	172.31.32.0/20	-
my-public-project-s...	subnet-06de92802dfb82050	Available	vpc-0b1e1d26ad4714f5e my...	10.0.0.0/24	-
-	subnet-09b10a06a06e8f247	Available	vpc-07e0cf812a795e9a	172.31.64.0/20	-

Select a subnet

The screenshot shows the AWS VPC Route Table creation page. A green success message at the top states: "Route table rtb-0c93a5803dd0182c9 | Public Subnet Route Table was created successfully." The main title is "rtb-0c93a5803dd0182c9 / Public Subnet Route Table". Below it, a message says "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button. The "Details" tab is selected, showing route table ID "rtb-0c93a5803dd0182c9", Main status "No", Owner ID "002332382585", and no explicit subnet or edge associations. The "Routes" tab is active, displaying one route: Destination "10.0.0.0/16", Target "local", Status "Active", and Propagated "No".

Associate the appropriate route tables with the subnets:

The screenshot shows the "Edit routes" page for route table "rtb-0c93a5803dd0182c9". It lists two routes: one for "10.0.0.0/16" targetting "local" (Status Active, Propagated No), and another for "0.0.0.0/0" targetting "igw-0c81de04f960cae97" (Status -, Propagated No). Buttons for "Add route", "Cancel", "Preview", and "Save changes" are visible.

Screenshot of the AWS VPC Route Table details page.

Route Table ID: rtb-0c93a5803dd0182c9

Main: No

VPC: [vpc-0b1e1d26ad4714f5e | my-awsproject-vpc](#)

Routes (2):

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0c81de04f960cae97	Active	No

Actions: Run Reachability Analyzer

Screenshot of the AWS VPC Route Tables list page.

Route tables (1/3):

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-06b3bb8d97c42539c	-	-	Yes	vpc-0b1e1d26ad4714f5e
-	rtb-009c08aff7524b0fc	-	-	Yes	vpc-07e0cfdb8
<input checked="" type="checkbox"/> Public Subnet Route Table	rtb-0c93a5803dd0182c9	subnet-06de92802dfb82...	-	No	vpc-0b1e1d26ad4714f5e

rtb-0c93a5803dd0182c9 / Public Subnet Route Table:

Details:

Route table ID: rtb-0c93a5803dd0182c9

Main: No

Explicit subnet associations: -

Edge associations: -

Actions: Run Reachability Analyzer

VPC > Route tables > rtb-0728ff1c9323312af > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)					
	Name	Subnet ID	IPV4 CIDR	IPV6 CIDR	Route table ID
<input checked="" type="checkbox"/>	my-private-project-subnet	subnet-063329c7a151d60b1	10.0.1.0/24	-	Main (rtb-06b3bb8d97c42539c)
<input type="checkbox"/>	my-public-project-subnet	subnet-06de92802dfb82050	10.0.0.0/24	-	rtb-0c93a5803dd0182c9 / Public Subnet

Selected subnets

- subnet-063329c7a151d60b1 / my-private-project-subnet

You have successfully updated subnet associations for rtb-0728ff1c9323312af / Private Subnet Route Table.

Route tables (1/4) Info

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
<input type="checkbox"/>	rtb-06b3bb8d97c42539c	-	-	Yes	vpc-0b1e1d26
<input type="checkbox"/>	rtb-009c08aff7524b0fc	-	-	Yes	vpc-07e0fd8
<input type="checkbox"/>	Public Subnet Route Table	subnet-06de92802dfb82...	-	No	vpc-0b1e1d26
<input checked="" type="checkbox"/>	Private Subnet Route Table	subnet-063329c7a151d6...	-	No	vpc-0b1e1d26

rtb-0728ff1c9323312af / Private Subnet Route Table

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

(1) You can now check network connectivity with Reachability Analyzer

Details

Route table ID rtb-0728ff1c9323312af	Main	Explicit subnet associations Edit	Edge associations Edit
---	------	--	---

Set up an Amazon RDS instance using the MariaDB engine and configure the database instance with the necessary specifications and security settings.

The screenshot shows the 'Create database' wizard on the AWS RDS console. In the 'Choose a database creation method' section, the 'Standard create' option is selected. Below it, the 'Engine options' section lists several engine types: Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), MySQL, MariaDB, PostgreSQL, and Oracle. The 'PostgreSQL' option is currently selected. At the bottom of the page, there are links for CloudShell, Feedback, Language, and cookie preferences.

The screenshot shows the 'Databases' page on the AWS RDS console. A green banner at the top indicates that 'Successfully created database database-1'. It also provides instructions for using settings from the database to simplify configuration of suggested database add-ons. Below the banner, a blue info box suggests creating a Blue/Green Deployment to minimize downtime during upgrades. The main table displays one database entry: 'database-1' (DB identifier), Status: 'Modifying', Instance: 'MariaDB', Region & AZ: 'us-east-1b', Engine: 'db.m6gd.large', and Maintenance: 'none'. Action buttons include 'Group resources', 'Modify', 'Actions', 'Restore from S3', and 'Create database'.

Screenshot of the AWS IAM console showing the creation of a new role named "my-iam-role".

Identity and Access Management (IAM)

Roles (6) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForEc2InstanceConnect	AWS Service: ec2-instance-connect (Service-Linked Role)	20 days ago
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	47 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
my-iam-role	AWS Service: ec2	-
rds-monitoring-role	AWS Service: monitoring.rds	22 minutes ago

Roles Anywhere Info
Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS **X.509 Standard** **Temporary credentials**

Actions

Create security groups for the EC2 instance and RDS database.

Screenshot of the AWS EC2 console showing the creation of a new security group named "EC2-SG".

EC2 Dashboard

Security group (sg-0f8345c0886e904f9 | EC2-SG) was created successfully

Details

Security group name	Security group ID	Description	VPC ID
EC2-SG	sg-0f8345c0886e904f9	security group for ec2 instance	vpc-0b1e1d26ad4714f5e
Owner	Inbound rules count	Outbound rules count	
002332382585	0 Permission entries	1 Permission entry	

Inbound rules **Outbound rules** **Tags**

Inbound rules

Actions

The screenshot shows the AWS EC2 Security Groups page. A success message at the top states: "Security group (sg-0e56aa78d05ab8dd1 | RDS-SG) was created successfully". The main content area displays the details of the new security group, including its name, ID, owner, and VPC ID. Below this, tabs for "Inbound rules", "Outbound rules", and "Tags" are visible. A note says "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button.

Configure inbound rules for the security groups to allow necessary access

The screenshot shows the "Edit inbound rules" page for a specific security group. It lists two existing rules: one for HTTP port 80 and another for MySQL/Aurora port 3306. Both rules have their source set to "Custom" and "0.0.0.0/0". A modal window is open over the second rule, showing the dropdown menu where "sg-0e56aa78d05ab8dd1" has been selected as the source. Buttons for "Add rule", "Cancel", "Preview changes", and "Save rules" are at the bottom.

Inbound security group rules successfully modified on security group (sg-0f8345c0886e904f9 | EC2-SG)

Security Groups (1/6) Info

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-033f28769568d4a40	launch-wizard-2	vpc-07e0cf812a795e9a	launch-wizard-2 create...	00233238
-	sg-0e56aa78d05ab8dd1	RDS-SG	vpc-0b1e1d26ad4714f5e	security group for rds	00233238
-	sg-0eaba17ab751bac78	launch-wizard-1	vpc-07e0cf812a795e9a	launch-wizard-1 create...	00233238
-	sg-03781d3887c94e50e	default	vpc-0b1e1d26ad4714f5e	default VPC security gr...	00233238
-	sg-0b57be9d91bfbb747	default	vpc-07e0cf812a795e9a	default VPC security gr...	00233238
<input checked="" type="checkbox"/>	sg-0f8345c0886e904f9	EC2-SG	vpc-0b1e1d26ad4714f5e	security group for ec2 i...	00233238

sg-0f8345c0886e904f9 - EC2-SG

Inbound rules (2)

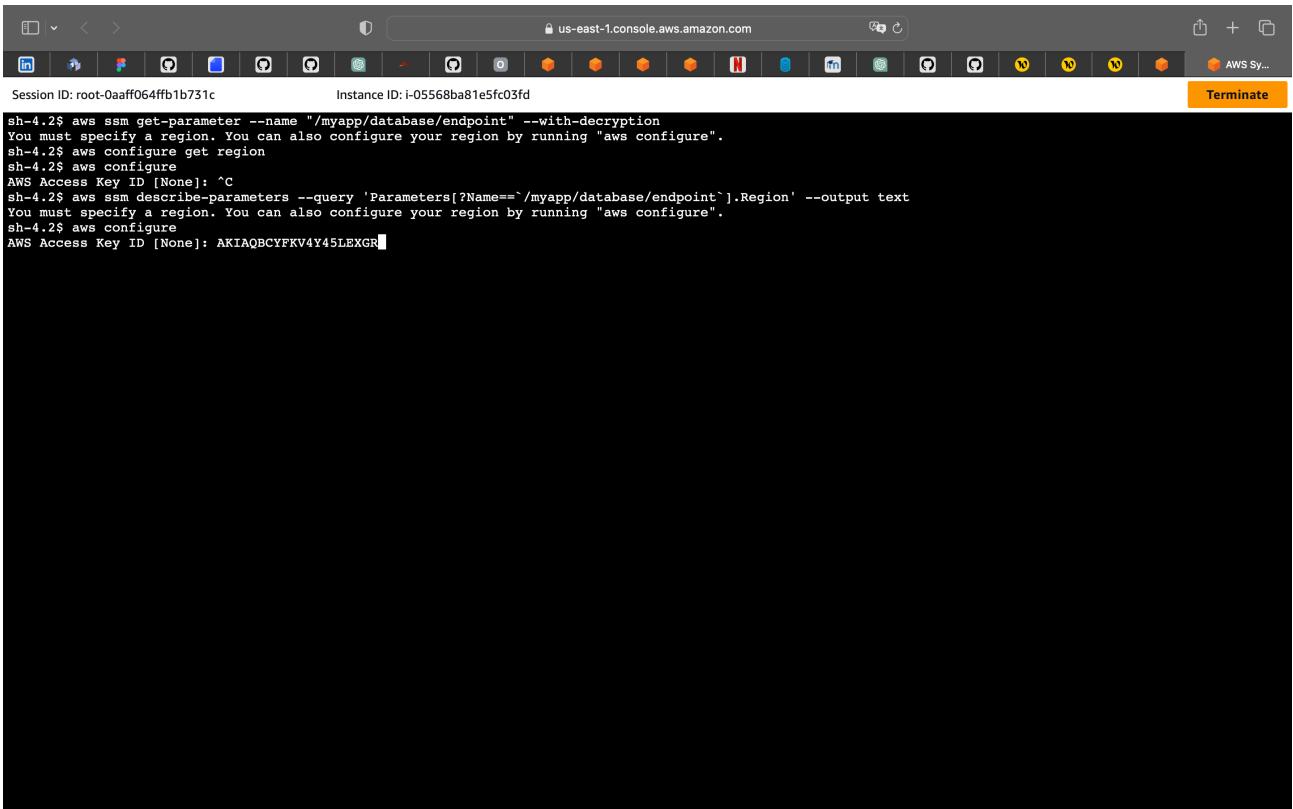
Store the database connection information (endpoint, username, password, database name) in AWS Systems Manager Parameter Store.

Create parameter request succeeded

AWS Systems Manager > Parameter Store

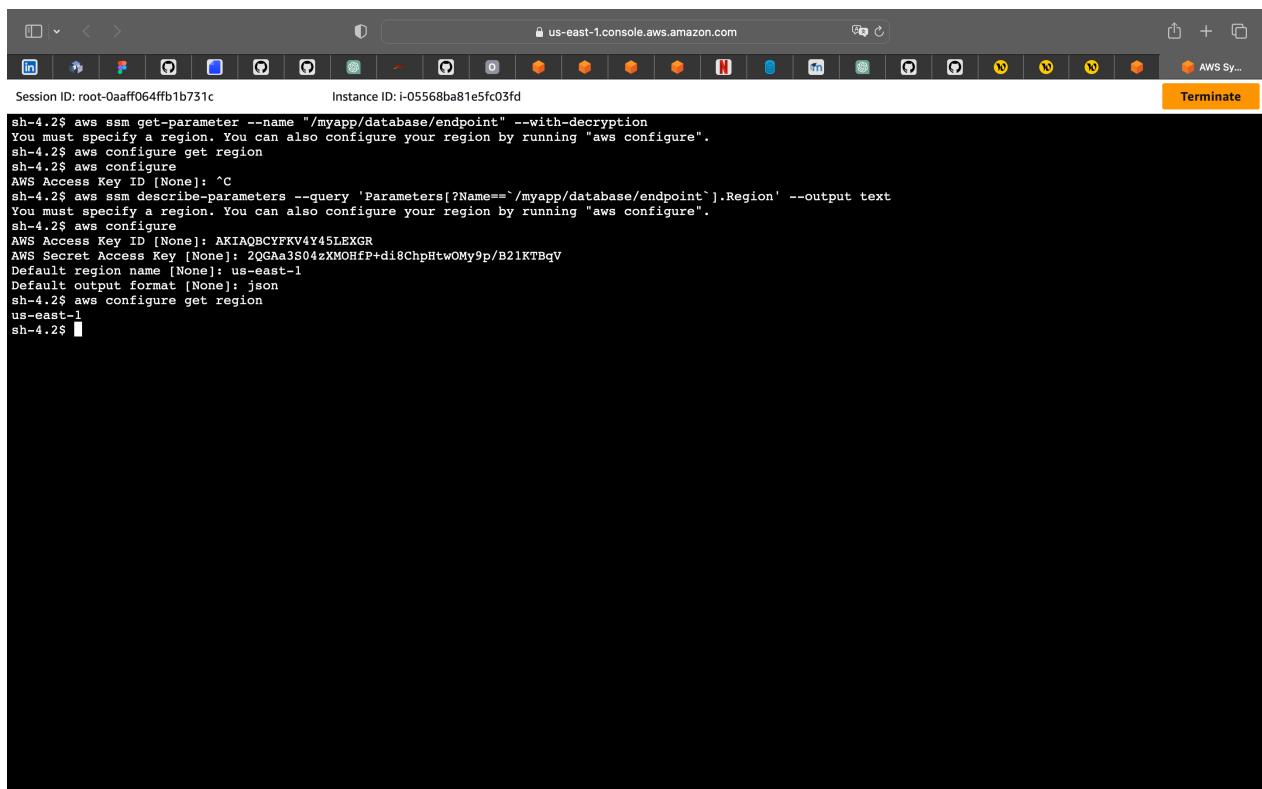
My parameters

Name	Tier	Type	Last modified
/myapp/database/database	Standard	String	Thu, 20 Jul 2023 03:55:04 GMT
/myapp/database/endpoint	Standard	String	Thu, 20 Jul 2023 03:52:56 GMT
/myapp/database/password	Standard	String	Thu, 20 Jul 2023 03:54:37 GMT
/myapp/database/username	Standard	String	Thu, 20 Jul 2023 03:53:32 GMT



Session ID: root-0aaff064ffb1b731c Instance ID: i-05568ba81e5fc03fd

```
sh-4.2$ aws ssm get-parameter --name "/myapp/database/endpoint" --with-decryption
You must specify a region. You can also configure your region by running "aws configure".
sh-4.2$ aws configure get region
sh-4.2$ aws configure
AWS Access Key ID [None]: `C
sh-4.2$ aws ssm describe-parameters --query 'Parameters[?Name==`/myapp/database/endpoint`].Region' --output text
You must specify a region. You can also configure your region by running "aws configure".
sh-4.2$ aws configure
AWS Access Key ID [None]: AKIAQBCYFKV4Y45LEXGR
```



Session ID: root-0aaff064ffb1b731c Instance ID: i-05568ba81e5fc03fd

```
sh-4.2$ aws ssm get-parameter --name "/myapp/database/endpoint" --with-decryption
You must specify a region. You can also configure your region by running "aws configure".
sh-4.2$ aws configure get region
sh-4.2$ aws configure
AWS Access Key ID [None]: `C
sh-4.2$ aws ssm describe-parameters --query 'Parameters[?Name==`/myapp/database/endpoint`].Region' --output text
You must specify a region. You can also configure your region by running "aws configure".
sh-4.2$ aws configure
AWS Access Key ID [None]: AKIAQBCYFKV4Y45LEXGR
AWS Secret Access Key [None]: ZQGAa3S04zXMOHfP+di8ChpHtwOMy9p/B2lKTBqV
Default region name [None]: us-east-1
Default output format [None]: json
sh-4.2$ aws configure get region
us-east-1
sh-4.2$
```

```

Session ID: root-Oaff064ff1b731c           Instance ID: i-05568ba81e5fc03fd
You must specify a region. You can also configure your region by running "aws configure".
sh-4.2$ aws configure
AWS Access Key ID [None]: AKIAQBCYFKV4Y45LEXGR
AWS Secret Access Key [None]: 2QGAa3S04zXMOHfP+di8ChpHtwOMy9p/B2lKTBqV
Default region name [None]: us-east-1
Default output format [None]: json
sh-4.2$ aws configure get region
us-east-1
sh-4.2$ aws ssm get-parameter --name "/myapp/database/endpoint" --with-decryption
{
    "Parameter": {
        "Name": "/myapp/database/endpoint",
        "DataType": "text",
        "LastModifiedDate": 1689825176.765,
        "Value": "{\"endpoint\":\"mydatabase.c2fnz0afbxq8.us-east-1.rds.amazonaws.com\"}",
        "Version": 2,
        "Type": "String",
        "ARN": "arn:aws:ssm:us-east-1:002332382585:parameter/myapp/database/endpoint"
    }
}
sh-4.2$ aws ssm get-parameter --name "/myapp/database/password" --with-decryption
{
    "Parameter": {
        "Name": "/myapp/database/password",
        "DataType": "text",
        "LastModifiedDate": 1689825277.05,
        "Value": "{\"password\":\"nykmir-5gygge-fywNyw\"}\n",
        "Version": 1,
        "Type": "String",
        "ARN": "arn:aws:ssm:us-east-1:002332382585:parameter/myapp/database/password"
    }
}
sh-4.2$ aws ssm get-parameter --name "/myapp/database/database" --with-decryption
{
    "Parameter": {
        "Name": "/myapp/database/database",
        "DataType": "text",
        "LastModifiedDate": 1689825304.848,
        "Value": "{\"database\":\"myawsdatabase\"}\n",
        "Version": 1,
        "Type": "String",
        "ARN": "arn:aws:ssm:us-east-1:002332382585:parameter/myapp/database/database"
    }
}
sh-4.2$ 

```

Modify the PHP application files to use the stored parameter values for database connection

```

[root@ip-172-31-83-35 ~]# wget https://efrei-capstone.s3.amazonaws.com/Example.zip
--2023-07-12 16:57:31-- https://efrei-capstone.s3.amazonaws.com/Example.zip
Resolving efrei-capstone.s3.amazonaws.com (efrei-capstone.s3.amazonaws.com)... 52.216.41.113, 52.216.206.83, 52.217.160.9, ...
Connecting to efrei-capstone.s3.amazonaws.com (efrei-capstone.s3.amazonaws.com)|52.216.41.113|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6359580 (6.1M) [application/zip]
Saving to: 'Example.zip'

100%[=====] 6,359,580  ---K/s in 0.09s

2023-07-12 16:57:31 (69.4 MB/s) - 'Example.zip' saved [6359580/6359580]

[root@ip-172-31-83-35 ~]# ls
Example.zip
[root@ip-172-31-83-35 ~]# unzip Example.zip -d /var/www/html/
Archive: Example.zip
  inflating: /var/www/html/index.php
  inflating: /var/www/html/gdp.php
  inflating: /var/www/html/Shirley.jpeg
  inflating: /var/www/html/query2.php
  inflating: /var/www/html/query3.php
  inflating: /var/www/html/population.php
  inflating: /var/www/html/lifeexpectancy.php
  inflating: /var/www/html/get-parameters.php
  inflating: /var/www/html/aws.phar
  inflating: /var/www/html/mortality.php
  inflating: /var/www/html/menu.php
  inflating: /var/www/html/Logo.png
  extracting: /var/www/html/style.css
  inflating: /var/www/html/mobile.php
  inflating: /var/www/html/query.php
[root@ip-172-31-83-35 ~]# ls /var/www/html/
aws.phar          index.php      Logo.png   mobile.php   population.php  query3.php  Shirley.jpeg
Example.zip        get-parameters.php lifeexpectancy.php menu.php   mortality.php  query2.php  style.css
[root@ip-172-31-83-35 ~]# 

i-05568ba81e5fc03fd (aws_project)
PublicIPs: 44.205.255.31 PrivateIPs: 172.31.83.35

```

Restricted Mode is intended for safe code browsing. Trust this window to enable all features. [Manage](#) [Learn More](#)

get-parameters.php

```

1 <?php
2 # Retrieve settings from Parameter Store
3 error_log('Retrieving settings');
4 require 'aws.phar';
5 session_start();
6
7 $az = file_get_contents('http://169.254.169.254/latest/meta-data/placement/availability-zone');
8 $region = substr($az, 0, -1);
9 $ssm_client = new Aws\Ssm\SsmClient([
10     'version' => 'latest',
11     'region'  => $region
12 ]);
13
14 try {
15     # Retrieve individual parameters
16     $result = $ssm_client->GetParametersByPath([Path => '/myapp/database', 'WithDecryption' => true]);
17
18     # Extract individual parameters
19     foreach($result['Parameters'] as $p) {
20         $values[$p['Name']] = $p['Value'];
21     }
22
23     $_SESSION['ep'] = $values['/myapp/database/endpoint'];
24     $_SESSION['un'] = $values['/myapp/database/username'];
25     $_SESSION['pw'] = $values['/myapp/database/password'];
26     $_SESSION['db'] = $values['/myapp/database/database'];
27 }
28 catch (Exception $e) {
29     $_SESSION['ep'] = '';
30     $_SESSION['un'] = '';
31     $_SESSION['pw'] = '';
32     $_SESSION['db'] = '';
33 }
34
35 >
36

```

You have Docker installed on your system. Do you want to [Install](#) the recommended 'Docker' extension from Microsoft for it?

Ln 16, Col 75 Spaces: 2 UTF-8 LF PHP ⌂ ↻

```

[msaber@Sabers-MacBook-Air ~ % scp -i saber69.pem ~/Downloads/ExampleToReplace.zip ec2-user@44.207.6.232:/var/www/html
ExampleToReplace.zip
msaber@Sabers-MacBook-Air ~ % ]
100% 6221KB 3.9MB/s 00:01

```

Session ID: root-04ffef483cc7e3b82 Instance ID: i-05568ba81e5fc03fd [Terminate](#)

```

checkdir error: cannot create __MACOSX
Permission denied
unable to process __MACOSX/Example/_mobile.php.

checkdir error: cannot create Example
Permission denied
unable to process Example/query.php.

checkdir error: cannot create __MACOSX
Permission denied
unable to process __MACOSX/Example/_query.php.

sh-4.2$ sudo unzip ExampleToReplace.zip -d /var/www/html/
Archive: ExampleToReplace.zip
  creating: /var/www/html/_Example/
  inflating: /var/www/html/_MACOSX/._Example
  inflating: /var/www/html/_MACOSX/Example/.index.php
  inflating: /var/www/html/_MACOSX/Example/.index.php
  inflating: /var/www/html/_Example/gdp.php
  inflating: /var/www/html/_MACOSX/Example/.gdp.php
  inflating: /var/www/html/_Example/Shirley.jpeg
  inflating: /var/www/html/_MACOSX/Example/.Shirley.jpeg
  inflating: /var/www/html/_Example/query2.php
  inflating: /var/www/html/_MACOSX/Example/.query2.php
  inflating: /var/www/html/_Example/query3.php
  inflating: /var/www/html/_MACOSX/Example/.query3.php
  inflating: /var/www/html/_Example/population.php
  inflating: /var/www/html/_MACOSX/Example/.population.php
  inflating: /var/www/html/_Example/lifeexpectancy.php
  inflating: /var/www/html/_MACOSX/Example/.lifeexpectancy.php
  inflating: /var/www/html/_Example/get-parameters.php
  inflating: /var/www/html/_MACOSX/Example/.get-parameters.php
  inflating: /var/www/html/_Example/aws.phar
  inflating: /var/www/html/_MACOSX/Example/.aws.phar
  inflating: /var/www/html/_Example/mortality.php
  inflating: /var/www/html/_MACOSX/Example/.mortality.php
  inflating: /var/www/html/_Example/menu.php
  inflating: /var/www/html/_MACOSX/Example/.menu.php
  inflating: /var/www/html/_Example/Logo.png
  inflating: /var/www/html/_MACOSX/Example/.Logo.png
  inflating: /var/www/html/_Example/style.css
  inflating: /var/www/html/_MACOSX/Example/.style.css
  inflating: /var/www/html/_Example/mobile.php
  inflating: /var/www/html/_MACOSX/Example/_mobile.php
  inflating: /var/www/html/_Example/query.php
  inflating: /var/www/html/_MACOSX/Example/_query.php

sh-4.2$ ls
aws.phar ExampleToReplace.zip gdp.php index.php Logo.png menu.php mortality.php query2.php query.php style.css
Example Example.zip get-parameters.php lifeexpectancy.php _MACOSX mobile.php population.php query3.php Shirley.jpeg
sh-4.2$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
sh-4.2$ pwd
/var/www/html
sh-4.2$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf
     Active: active (running) since Thu 2023-07-20 04:58:19 UTC; 2min 26s ago
       Docs: man:httpd.service(8)
    Main PID: 17019 (httpd)
      Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
      Tasks: 47
     Memory: 13.6M
      CGroup: /system.slice/httpd.service
              ├─17019 /usr/sbin/httpd -DFOREGROUND
              ├─17059 /usr/sbin/httpd -DFOREGROUND
              ├─17061 /usr/sbin/httpd -DFOREGROUND
              ├─17062 /usr/sbin/httpd -DFOREGROUND
              ├─17063 /usr/sbin/httpd -DFOREGROUND
              └─17064 /usr/sbin/httpd -DFOREGROUND

Jul 20 04:58:19 ip-172-31-83-35.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Jul 20 04:58:19 ip-172-31-83-35.ec2.internal systemd[1]: Started The Apache HTTP Server.
sh-4.2$ 
```

Session ID: root-04ffef483cc7e3b82 Instance ID: i-05568ba81e5fc03fd [Terminate](#)

```

inflating: /var/www/html/_Example/get-parameters.php
inflating: /var/www/html/_MACOSX/Example/.get-parameters.php
inflating: /var/www/html/_Example/aws.phar
inflating: /var/www/html/_MACOSX/Example/.aws.phar
inflating: /var/www/html/_Example/mortality.php
inflating: /var/www/html/_MACOSX/Example/.mortality.php
inflating: /var/www/html/_Example/menu.php
inflating: /var/www/html/_MACOSX/Example/.menu.php
inflating: /var/www/html/_Example/Logo.png
inflating: /var/www/html/_MACOSX/Example/.Logo.png
inflating: /var/www/html/_Example/style.css
inflating: /var/www/html/_MACOSX/Example/.style.css
inflating: /var/www/html/_Example/mobile.php
inflating: /var/www/html/_MACOSX/Example/_mobile.php
inflating: /var/www/html/_Example/query.php
inflating: /var/www/html/_MACOSX/Example/_query.php

sh-4.2$ ls
aws.phar ExampleToReplace.zip gdp.php index.php Logo.png menu.php mortality.php query2.php query.php style.css
Example Example.zip get-parameters.php lifeexpectancy.php _MACOSX mobile.php population.php query3.php Shirley.jpeg
sh-4.2$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
sh-4.2$ pwd
/var/www/html
sh-4.2$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf
     Active: active (running) since Thu 2023-07-20 04:58:19 UTC; 2min 26s ago
       Docs: man:httpd.service(8)
    Main PID: 17019 (httpd)
      Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
      Tasks: 47
     Memory: 13.6M
      CGroup: /system.slice/httpd.service
              ├─17019 /usr/sbin/httpd -DFOREGROUND
              ├─17059 /usr/sbin/httpd -DFOREGROUND
              ├─17061 /usr/sbin/httpd -DFOREGROUND
              ├─17062 /usr/sbin/httpd -DFOREGROUND
              ├─17063 /usr/sbin/httpd -DFOREGROUND
              └─17064 /usr/sbin/httpd -DFOREGROUND

Jul 20 04:58:19 ip-172-31-83-35.ec2.internal systemd[1]: Starting The Apache HTTP Server...
Jul 20 04:58:19 ip-172-31-83-35.ec2.internal systemd[1]: Started The Apache HTTP Server.
sh-4.2$ 
```

AWS Quicksight

Loading the data from Kaggle as csv file

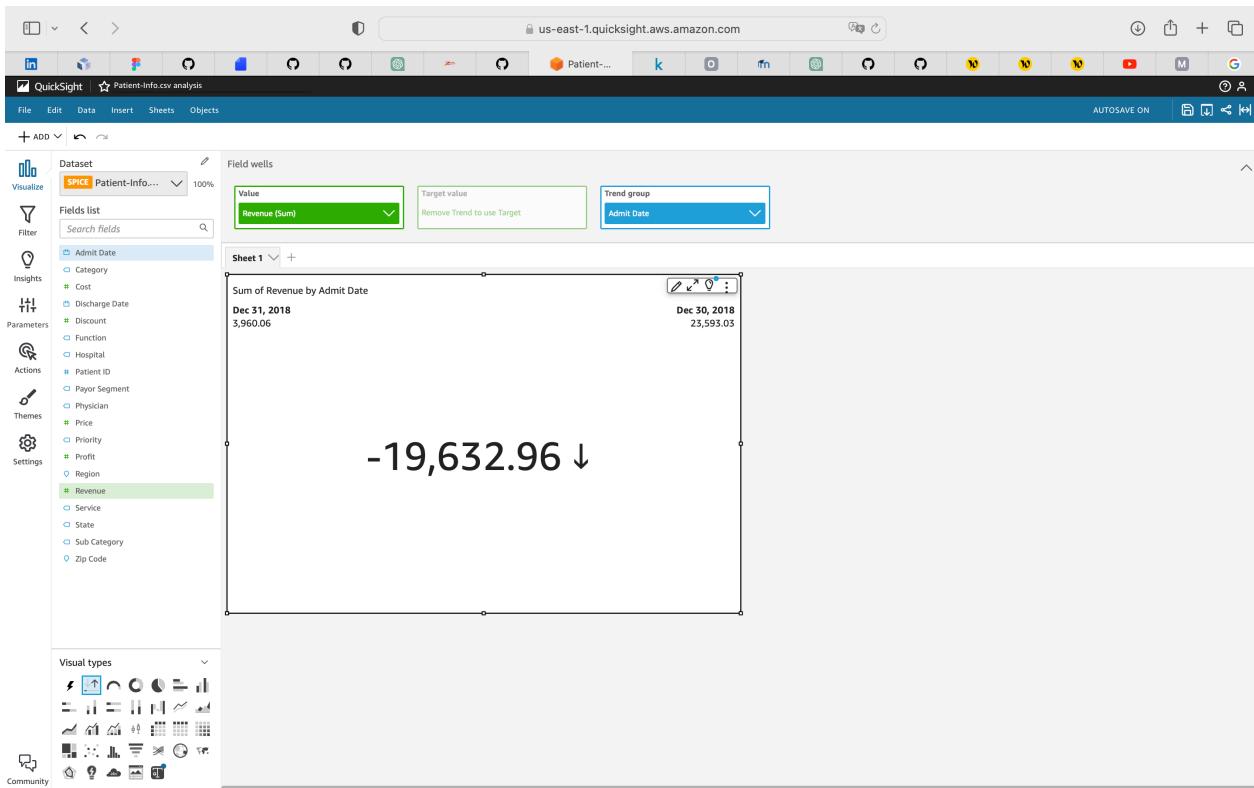
The screenshot shows the AWS Quicksight interface with a data sheet titled "Sheet 1". The sheet displays a CSV file named "Patient-Info.csv" containing 194 rows of medical data. The columns include Patient ID, Admit Date, Discharge Date, Priority, Hospital, Profit, Price, Cost, Revenue, Discount, Payor Segment, Category, and Sub Category. The data spans from 2014 to 2018 across various hospitals and categories.

Patient ID	Admit Date	Discharge Date	Priority	Hospital	Profit	Price	Cost	Revenue	Discount	Payor Segment	Category	Sub Category
3	10/14/16	10/21/16	Low	North Hospital	-213.25	38.94	35	326.925	0.04	Personal Cost	Labor & Delivery	Labor & Deepak
6	2/20/18	2/21/18	Not Specified	North Hospital	-4.64	2.08	2.56	8.6625	0.01	Medicaid	Critical Care	Critical Care
32	7/15/17	7/16/17	High	North Hospital	-128.38	8.46	8.99	175.7	0.04	Medicaid	NICU	Inpatient
32	7/15/17	7/16/17	High	South Hospital	-1748.56	70.89	89.3	2201.75	0.09	Medicaid	Surgical	Abdominal
32	7/15/17	7/17/17	High	North Hospital	-85.129	7.99	5.03	200.291875	0.04	Medicaid	Step Down	Medical
32	7/15/17	7/17/17	High	North Hospital	1054.82	107.53	5.81	3510.1	0.07	Medicaid	Surgical	Inpatient
35	10/22/17	10/23/17	Not Specified	North Hospital	60.72	9.11	2.25	360.7	0.03	Medicaid	Surgical	Gyne Oncology
35	10/22/17	10/24/17	Not Specified	North Hospital	48.967	155.99	8.99	2366.06	0.01	Medicaid	Psychology	Psychology
36	11/2/17	11/2/17	Urgent	North Hospital	657.477	65.99	4.2	3105.931875	0.1	Corporate Insurance	Ante/Post Partum	Inpatient
65	3/17/17	3/18/17	Urgent	North Hospital	1470.3	115.79	1.99	4765.9125	0.02	Medicaid	Critical Care	Critical Care
66	1/20/15	1/20/15	Low	North Hospital	7.57	2.88	0.7	135.1875	0.09	Medicare	Critical Care	Critical Care
640	1/23/16	1/24/16	High	North Hospital	29.42	18.97	9.54	580.9625	0.01	Medicare	Medical	Cardiology
69	6/4/15	6/6/15	Not Specified	Downtown Hospital	0.35	1.68	0.7	64.4125	0.03	Medicaid	Step Down	Step Down
70	12/18/16	12/23/16	Low	North Hospital	2057.166	205.99	5.99	9755.6625	0.05	Corporate Insurance	Step Down	Thoracic
70	12/18/16	12/23/16	Low	North Hospital	-107	1.86	2.58	112.5625	0.03	Corporate Insurance	Step Down	Down
96	4/17/15	4/19/15	High	North Hospital	1228.887	125.99	8.99	5197.654375	0.01	Corporate Insurance	Surgical	Orthopedic
1344	4/16/18	4/23/18	Low	North Hospital	-11.682	65.99	5.26	1043.63	0.06	Medicaid	Medical	Cardiology
1637	2/8/17	2/8/17	Not Specified	Downtown Hospital	-1191.13	35.48	35	1531.9	0.1	Medicaid	Medical	Cardiology
130	5/8/18	5/9/18	High	North Hospital	71.75	18.97	9.03	718.8875	0.02	Medicaid	BMT	BMT Oncology
130	5/8/18	5/10/18	High	Downtown Hospital	-356.12	150.98	13.99	577.3625	0.05	Medicaid	Ante/Post Partum	Ante/Post Partum
1792	11/9/16	11/14/16	Low	North Hospital	-5.45	13.48	4.51	463.1	0.04	Medicare	Medical	Cardiology
1831	12/2/16	12/3/16	Urgent	South Hospital	619.71	370.98	99	15732.7375	0	Corporate Insurance	Medical	Cardiology
2752	11/19/16	11/19/16	High	North Hospital	15.77	34.76	8.22	457.025	0.03	Personal Cost	Medical	Cardiology
2978	5/2/17	5/3/17	Urgent	North Hospital	1312.038	205.99	19.99	7830.231875	0.01	Medicaid	Medical	Cardiology
135	10/20/17	10/22/17	Not Specified	North Hospital	-89.25	4.98	4.62	157.3125	0.09	Medicare	Surgical	Abdominal
166	9/11/17	9/13/17	High	Downtown Hospital	-126.093	65.99	8.99	709.92	0.02	Medicare	Step Down	Surg
193	8/8/16	8/10/16	Urgent	North Hospital	-37.04	12.44	6.27	218.6125	0.06	Medicare	Ante/Post Partum	Ante/Post Partum
194	4/5/18	4/7/18	Medium	North Hospital	-197.25	7.28	7.98	411.2875	0.1	Medicaid	Step Down	Step Down
194	4/5/18	4/7/18	Medium	North Hospital	-13.44	3.14	1.92	25.2375	0.04	Medicaid	Step Down	Step Down

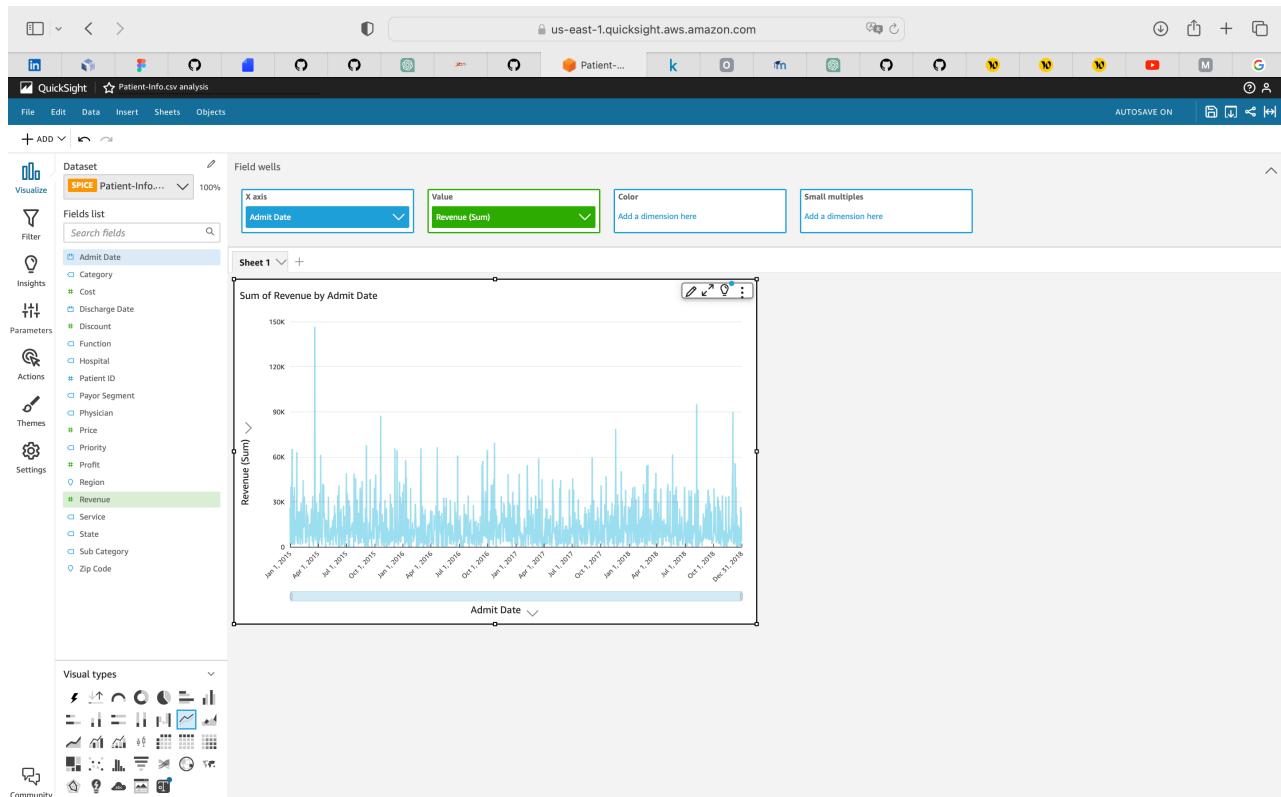
Upload the data file in QuickSight

The screenshot shows the AWS Quicksight "Create a Dataset" wizard. The current step is "Confirm file upload settings". The user has selected "csv file, Patient-Info.csv" and chosen "Patient ID" as the primary key. A preview of the data is shown, and the user can adjust settings like file type, encoding, and separator. The next step is "Edit settings and prepare data".

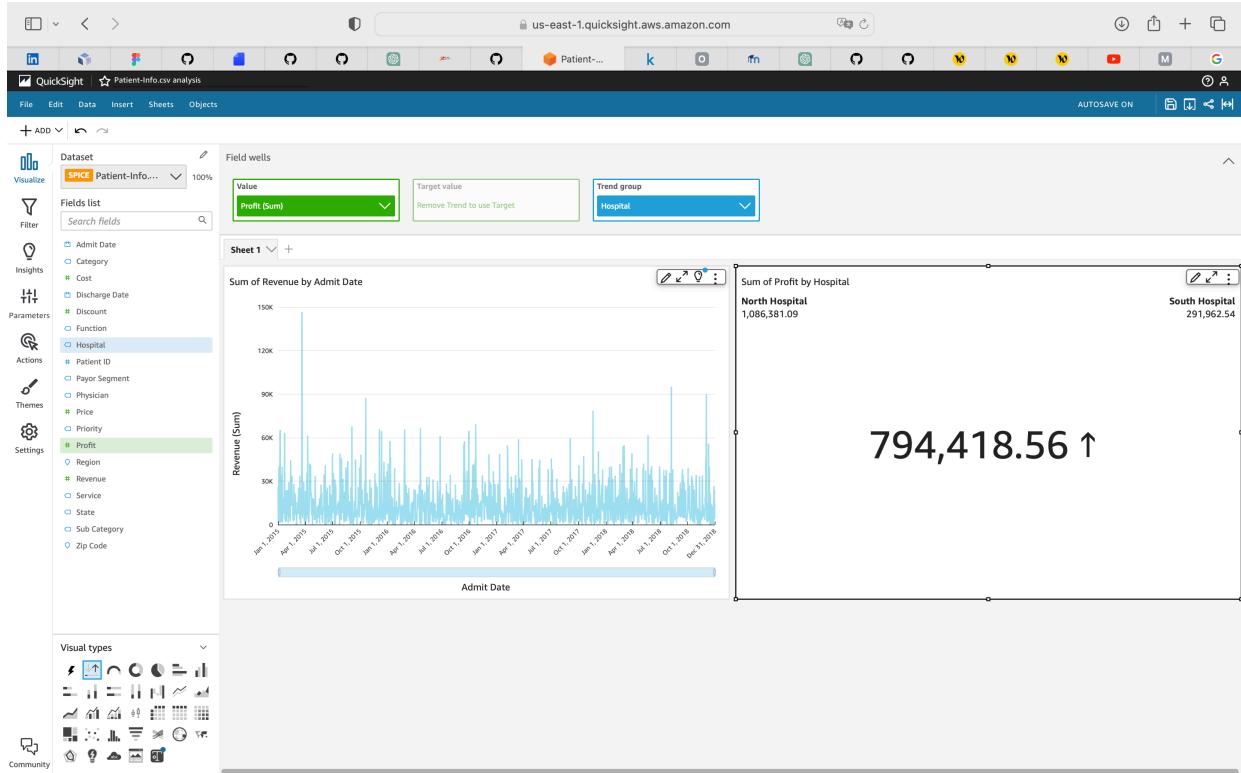
Choosing the first column to display as value and by which category (Sum of Revenue by Admit Date)



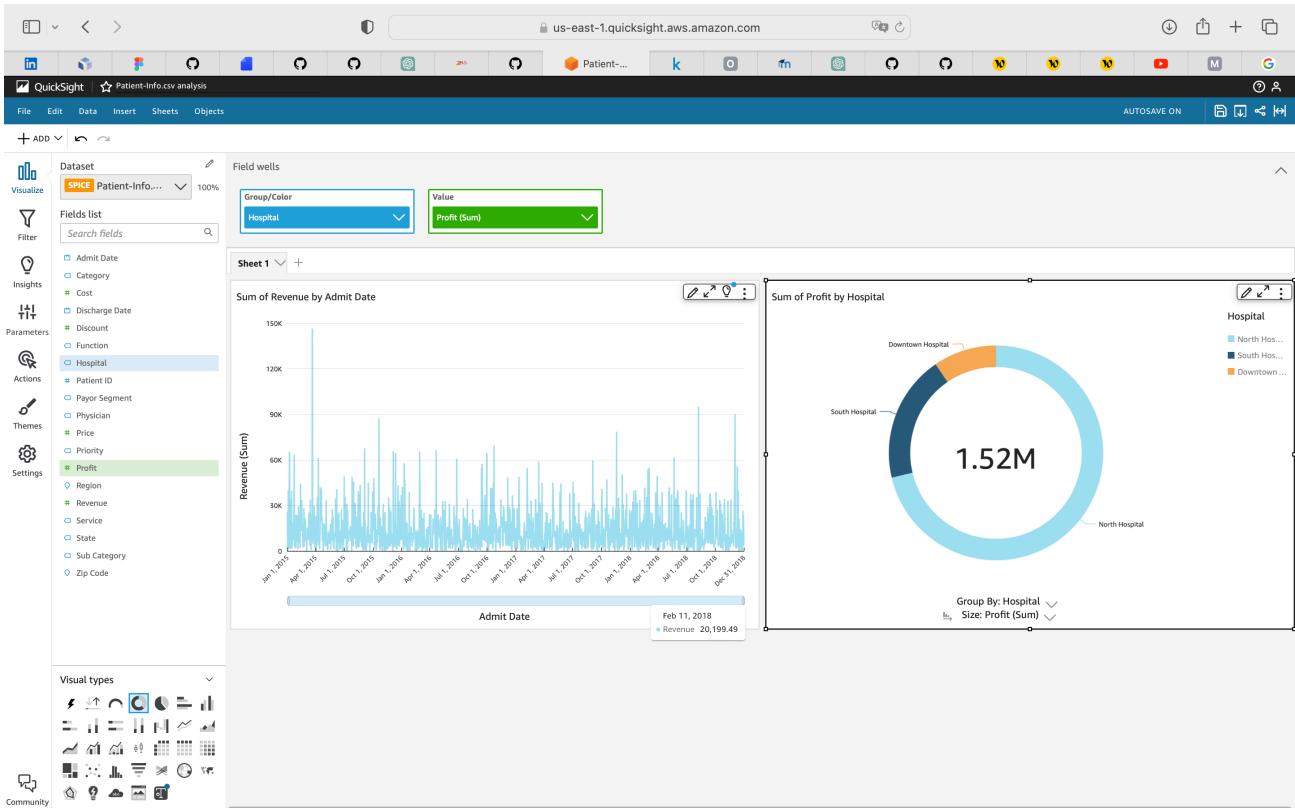
Choose the visual type desired (Line chart)



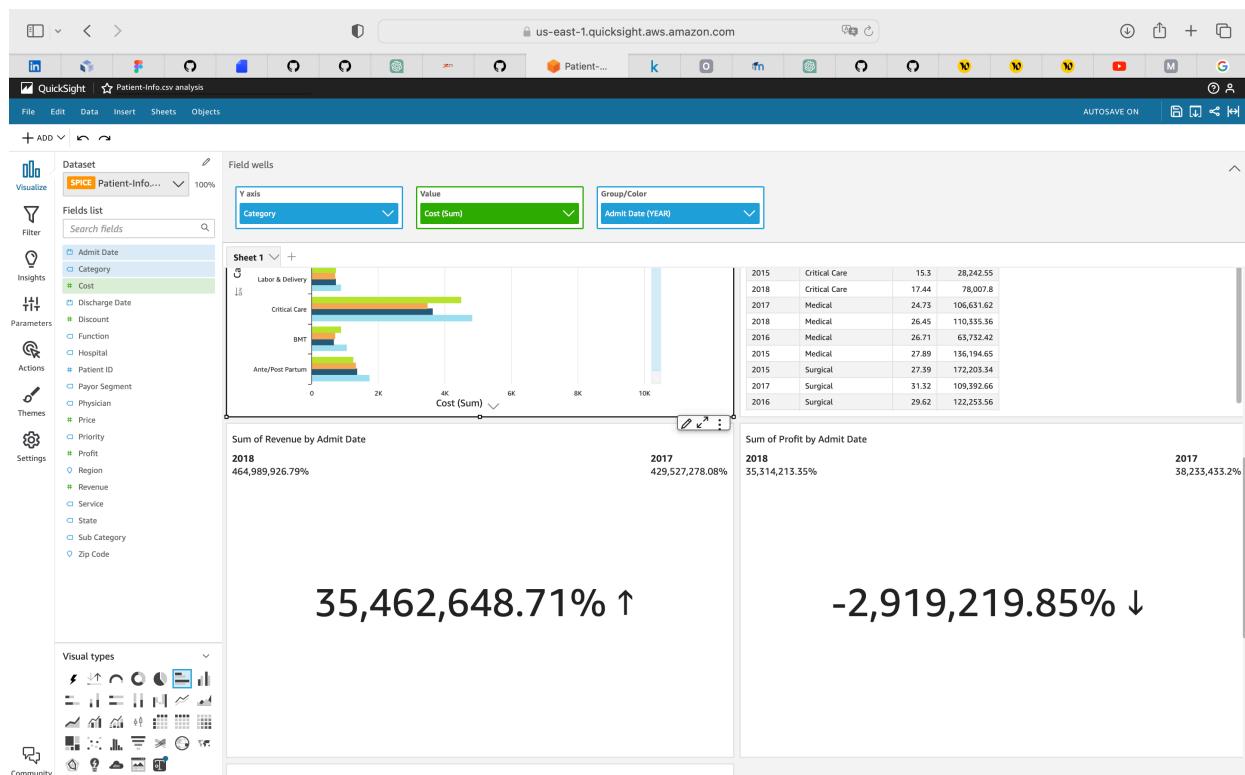
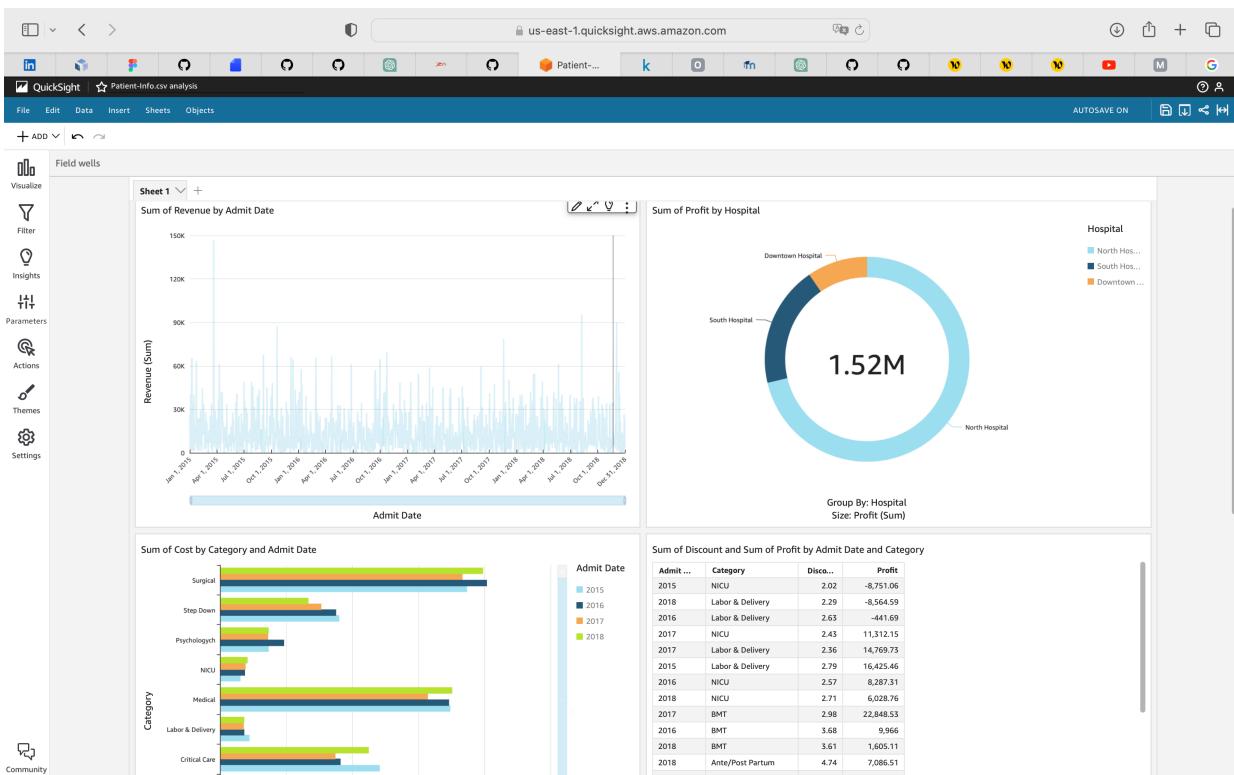
Follow the same steps with the other columns to display (Sum of Profit by Hospital)



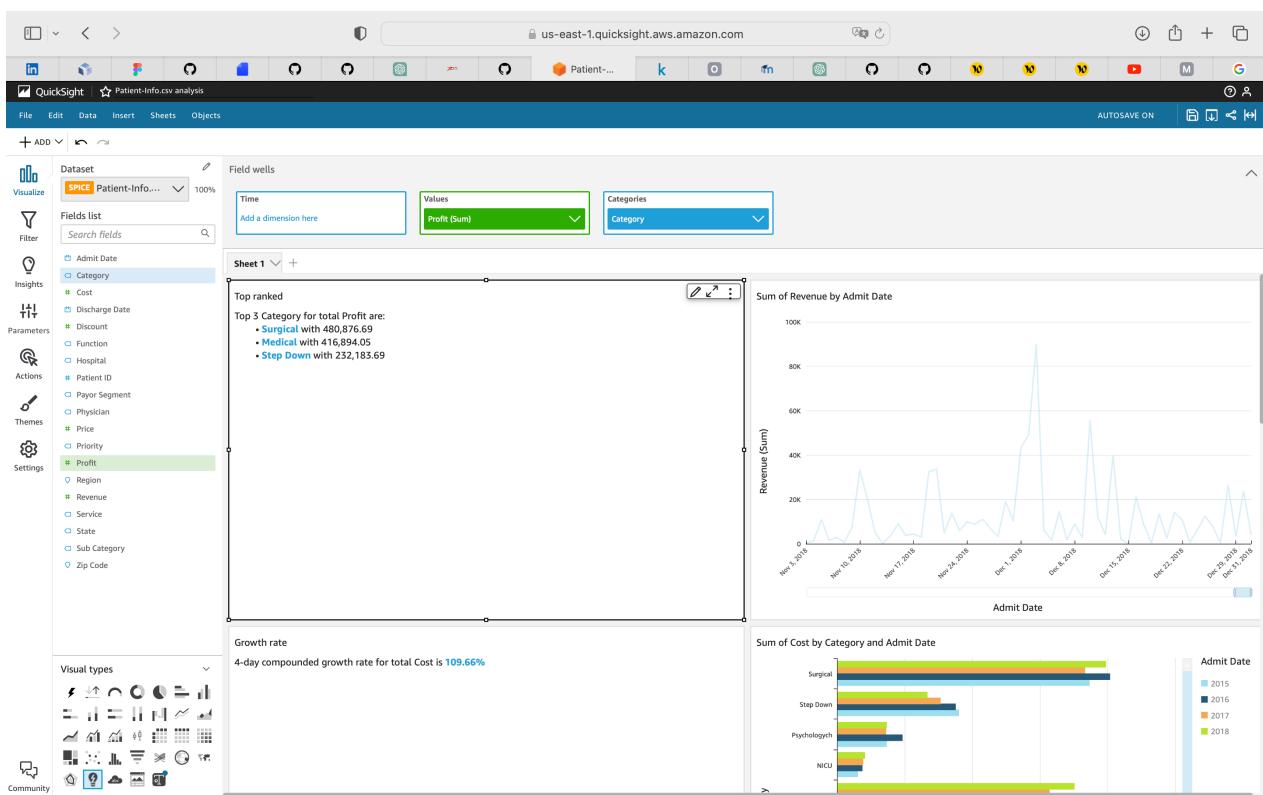
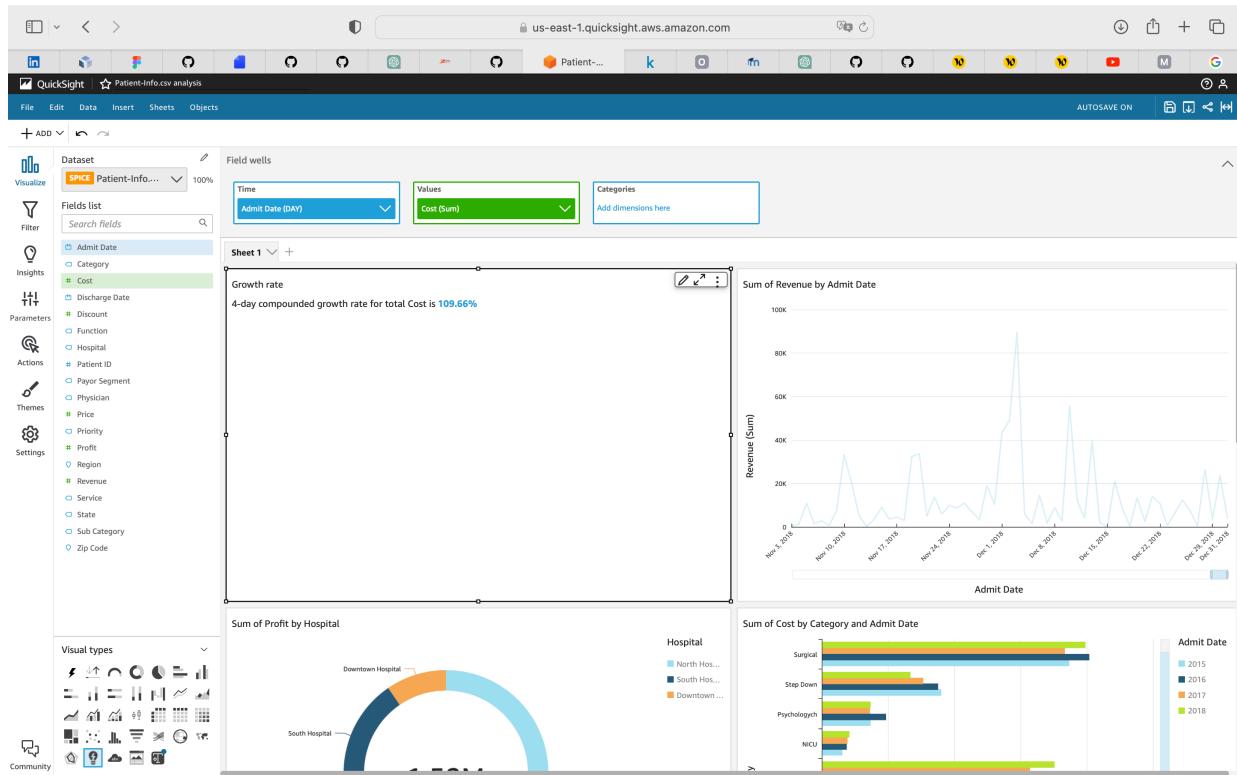
Then the visual type desired (Donut chart)



Follow the same steps



The use of insights in order to produce the Period over period and the Top 3 visual



Iam Quiz

Which statement describes AWS Identity and Access Management (IAM) users?

- IAM users are used to control access to a specific AWS resource.
- IAM user names can represent a collection of individuals.
- Every IAM user for an account must have a unique name.
- Every IAM user name is unique across all AWS accounts.

Option 3

How can you grant the same level of permissions to multiple users within an account?

- Apply an AWS Identity and Access Management (IAM) policy to an IAM group.
- Apply an AWS Identity and Access Management (IAM) policy to an IAM role.
- Create a resource-based policy.
- Create an organization in AWS Organizations.

Option 1

Which statements describe AWS Identity and Access Management (IAM) roles? (Select TWO.)

- They are uniquely associated to an individual.
- They can only be used by accounts associated to the person who creates the role.
- They can be assumed by individuals, applications, and services.
- They provide temporary security credentials.
- They provide permanent security credentials.

Options 3 & 4

Which statement describes a resource-based policy?

- It can be applied to any AWS resource.
- It can be an AWS managed policy.
- It is attached to a user or group.
- It is always an inline policy.

Option 1

How does AWS Identity and Access Management (IAM) evaluate a policy?

- It checks for explicit allow statements before it checks for explicit deny statements.
- It checks for explicit deny statements before it checks for explicit allow statements.
- If there is no explicit deny statement or explicit allow statement, users will have access by default.
- An explicit deny statement does not override an explicit allow statement.

Option 2

A team of developers needs access to several services and resources in a virtual private cloud (VPC) for 9 months. How can you use AWS Identity and Access Management (IAM) to enable access for them?

- Create a single IAM user for the developer team and attach the required IAM policies.
- Create an IAM user for each developer, and attach the required IAM policies to each IAM user.
- Create an IAM user for each developer, put them all in an IAM group, and attach the required IAM policies to the IAM group.
- Create a single IAM user for the developer team, place it in an IAM group, and attach the required IAM policies to the IAM group.

Option 3

How does identity federation increase security for an application that is built in Amazon Web Services (AWS)?

- Users can use single sign-on (SSO) to access the application through an existing authenticated identity.
- The application can synchronize users' user names and passwords in AWS Identity and Access Management (IAM) with their social media accounts.
- The browser can establish a trust relationship with the application to bypass the need for multi-factor authentication (MFA).
- Users can use their AWS Identity and Access Management (IAM) accounts to log in to on-premises systems.

Option 1

Network Quiz

Which definition describes a virtual private cloud (VPC)?

- A virtual private network (VPN) in the AWS Cloud
- An extension of an on-premises network into Amazon Web Services (AWS)
- A logically isolated virtual network that you define in the AWS Cloud
- A fully managed service that extends the AWS Cloud to customer premises

Option 3

A company's VPC has the CIDR block 172.16.0.0/21 (2048 addresses). It has two subnets (A and B). Each subnet must support 100 usable addresses now, but this number is expected to rise to at most 254 usable addresses soon. Which subnet addressing scheme meets the requirements and follows AWS best practices?

- Subnet A: 172.16.0.0/25 (128 addresses) Subnet B: 172.16.0.128/25 (1024 addresses)
- Subnet A: 172.16.0.0/25 (128 addresses) Subnet B: 172.16.0.128/25 (128 addresses)
- Subnet A: 172.16.0.0/23 (512 addresses) Subnet B: 172.16.2.0/23 (512 addresses)
- Subnet A: 172.16.0.0/22 (1024 addresses) Subnet B: 172.16.4.0/22 (128 addresses)

Option 4

Which combination of actions enables direct internet access for IPv4 hosts in a virtual private cloud (VPC)? (Select THREE.)

- Creating a route for 0.0.0.0/0 that points to the internet gateway
- Enabling Domain Name System (DNS) resolution for the VPC
- Configuring hosts to have or obtain an internet-routable address
- Configuring the VPC domain name in a Dynamic Host Configuration Protocol (DHCP) options set
- Creating a default route that points to the virtual private gateway
- Configuring security groups and network access control lists (network ACLs) to permit internet traffic

Option 1 & 3 & 6

Several EC2 instances launch in a virtual private cloud (VPC) that has internet access. These instances should not be accessible from the internet, but they must be able to download updates from the internet. How should the instances launch?

- With Elastic IP addresses, in a subnet with a default route to an internet gateway
- With public IP addresses, in a subnet with a default route to an internet gateway
- Without public IP addresses, in a subnet with a default route to an internet gateway
- Without public IP addresses, in a subnet with a default route to a network address translation (NAT) gateway

Option 4

Policies evaluation

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowEC2AndS3",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances",  
                "ec2:TerminateInstances",  
                "s3:GetObject",  
                "s3:PutObject"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1:123456789012:instance/*",  
                "arn:aws:s3:::example-bucket/*"  
            ]  
        }  
    ]  
}
```

Version: Specifies the version of the IAM policy language used, which is "2012-10-17" in this case.

Statement: Contains an array of policy statements. In this policy, there's only one statement.

Sid: A unique identifier for the statement, used for clarity in the policy. In this case, it is "AllowEC2AndS3".

Effect: Specifies the effect of the policy, which can be either "Allow" or "Deny". In this policy, the effect is set to "Allow," meaning the actions specified in the statement are permitted.

Action: Lists the AWS actions (API operations) that are allowed by the policy. The allowed actions in this policy are:

ec2:RunInstances: Allowing the IAM entity to launch EC2 instances.

ec2:TerminateInstances: Allowing the IAM entity to terminate EC2 instances.

s3:GetObject: Allowing the IAM entity to retrieve (read) objects from the S3 bucket.

s3:PutObject: Allowing the IAM entity to upload (write) objects to the S3 bucket.

Resource: Specifies the resources (e.g., ARNs - Amazon Resource Names) to which the actions apply. The resources allowed in this policy are:

All EC2 instances in the "us-east-1" region belonging to the AWS account with ID "123456789012". The * at the end of the ARN indicates that it applies to all instances within that region.

All objects (files) in the S3 bucket named "example-bucket".

Question: What actions are allowed for EC2 instances and S3 objects based on this policy? What specific resources are included?

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowVPCAccess",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeVpcs",  
                "ec2:DescribeSubnets",  
                "ec2:DescribeSecurityGroups"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestedRegion": "us-west-2"  
                }  
            }  
        }  
    ]  
}
```

Based on this IAM policy, the specific actions allowed for EC2 instances are limited to viewing information about VPCs, Subnets, and Security Groups. The policy applies to all resources (EC2 instances, VPCs, Subnets, and Security Groups) in any region, but the condition restricts these actions to only be allowed when the API request is made from the "us-west-2" region. S3 objects are not mentioned or granted any permissions in this policy.

Question: Under what condition does this policy allow access to VPC-related information? Which AWS region is specified?

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowS3ReadWrite",  
            "Effect": "Allow",  
            "Action": ["s3:GetObject", "s3:PutObject", "s3>ListBucket"],  
            "Resource": [  
                "arn:aws:s3:::example-bucket",  
                "arn:aws:s3:::example-bucket/*"  
            ],  
            "Condition": {  
                "StringLike": {  
                    "s3:prefix": ["documents/*", "images/*"]  
                }  
            }  
        }  
    ]  
}
```

The condition allows access only when the IAM entity tries to access objects in the "example-bucket" that have the prefix "documents/" or "images/". The StringLike condition with s3:prefix ensures that the IAM entity can read and write objects with keys (object names) starting with "documents/" or "images/" in the "example-bucket". This policy does not provide access to VPC-related information, and no AWS region is specified for VPC actions.

Question: What actions are allowed on the "example-bucket" and its objects based on this policy? What specific prefixes are specified in the condition?

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowIAMUserCreation",  
      "Effect": "Allow",  
      "Action": "iam:CreateUser",  
      "Resource": "arn:aws:iam::123456789012:user/${aws:username}"  
    },  
    {  
      "Sid": "AllowIAMUserDeletion",  
      "Effect": "Allow",  
      "Action": "iam:DeleteUser",  
      "Resource": "arn:aws:iam::123456789012:user/${aws:username}"  
    }  
  ]  
}
```

Based on the provided IAM policy, the actions allowed are related to IAM user creation and deletion, not actions on the "example-bucket" or its objects.

There is no reference to "example-bucket" or its objects in this policy, and there are no specific prefixes specified in the conditions. This policy only grants permissions related to IAM user creation and deletion for the AWS account with the ID "123456789012".

Question: What actions are allowed for IAM users based on this policy? How are the resource ARNs constructed?

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": ["iam:Get*", "iam>List*"],  
         "Resource": "*"  
     }  
}
```

IAM users are allowed to perform certain read-only actions related to IAM resources.

Questions:

- Which AWS service does this policy grant you access to?
- Does it allow you to create an IAM user, group, policy, or role?
- Go to <https://docs.aws.amazon.com/IAM/latest/UserGuide/> and in the left navigation expand Reference > Policy Reference > Actions, Resources, and Condition Keys. Choose Identity And Access Management. Scroll to the Actions Defined by Identity And Access Management list. Name at least three specific actions that the iam:Get* action allows.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Condition": {  
                "StringEquals": {  
                    "ec2:InstanceType": ["t2.micro", "t2.small"]  
                }  
            },  
            "Resource": "arn:aws:ec2:*::instance/*",  
            "Action": ["ec2:RunInstances", "ec2:StartInstances"],  
            "Effect": "Deny"  
        }  
    ]  
}
```

The policy grants access to the Amazon EC2 service. More specifically, it controls the permissions for actions related to EC2 instances.

The policy does not include any explicit permissions to create IAM users, groups, policies, or roles. It focuses on EC2 instance-related actions.

iam:GetUser: Allows getting information about an IAM user, including user details and attached policies.

iam:GetGroup: Allows getting information about an IAM group, including group details and attached policies.

iam:GetRole: Allows getting information about an IAM role, including role details, attached policies, and trust policy.