

Cloud and Big Data Architecture

Capstone Project

Matthew DAVID – Maxence ROBICHON

Contents

Capstone Project – Requirements	2
Capstone Project – Theoretical Solution	3
Architecture	3
Capstone Project – AWS Solution	5
VPC	5
Subnets	6
Route Tables	8
Internet Gateway	10
Security Groups	11
EC2 Instances	12
IAM – Roles	13
Databases (RDS)	14
System Manager – Store parameters	16
Cloud IDE – AWS Cloud9	19
EC2 Console from Cloud9	20
Website	21
Capstone Project – Questions	26
Question: What actions are allowed for EC2 instances and S3 objects based on this policy? What specific resources are included?	26
Question: Under what condition does this policy allow access to VPC-related information? Which AWS region is specified?	26
Question: What actions are allowed on the "example-bucket" and its objects based on this policy? What specific prefixes are specified in the condition?	26
Question: What actions are allowed for IAM users based on this policy? How are the resource ARNs constructed?	26
Questions:	26
Questions:	27
Capstone Project – QuickSight	28
Conclusion	29

Capstone Project –Requirements

Example Social Research Organization is a (fictitious) nonprofit organization that provides a website for social science researchers to obtain global development statistics. For example, visitors to the site can look up various data, such as the life expectancy for any country in the world over the past 10 years.

Shirley Rodriguez, a researcher at the organization, developed the website. She thought it would be valuable to share the data that she had gathered with other researchers. Shirley stores the data in a MySQL database, and the data is available through a PHP website that she built. She initially published the site through a commercial hosting company that provides limited support for technical issues and security.

Over the past year, Shirley's website has grown in popularity. As a result of increased traffic, she started receiving complaints that the site is not as responsive as it used to be. She also experienced an attempted ransomware security breach. The security breach was unsuccessful, but her supervisor, Mateo Jackson, suggested that Shirley investigate new ways to host the website.

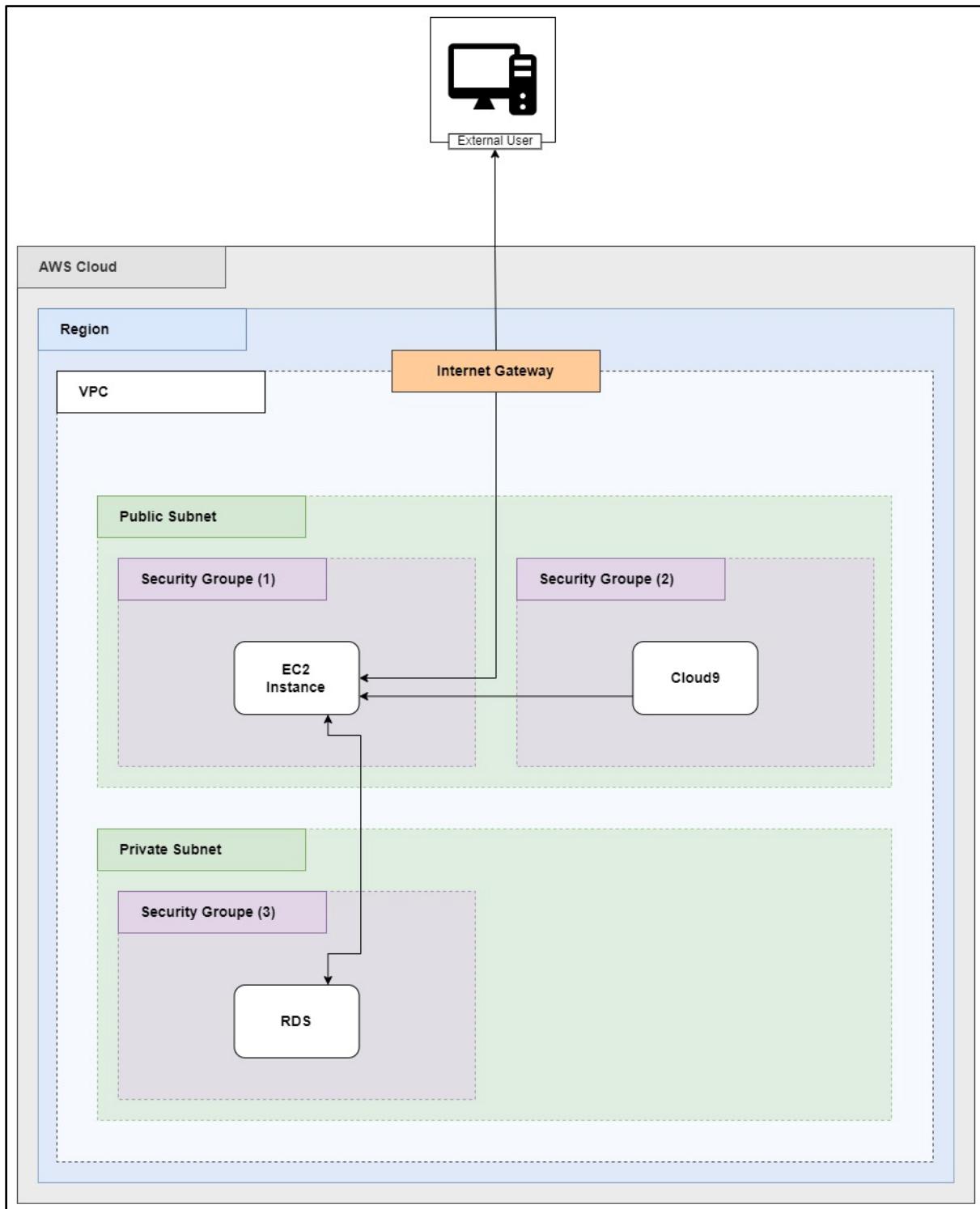
Shirley heard about Amazon Web Services (AWS), and initially moved her website and database to an EC2 instance that runs in a public subnet. She also runs an instance of MySQL on the same EC2 instance.

Shirley approached your team to make sure that her current design follows best practices. She wants to make sure that she has a robust and secure website. One of your colleagues started the process of migrating to the site to a more secure implementation, but they were reassigned to another project. Your tasks are to complete the implementation, make sure that the website is secure, and confirm that the website returns data from the query page.

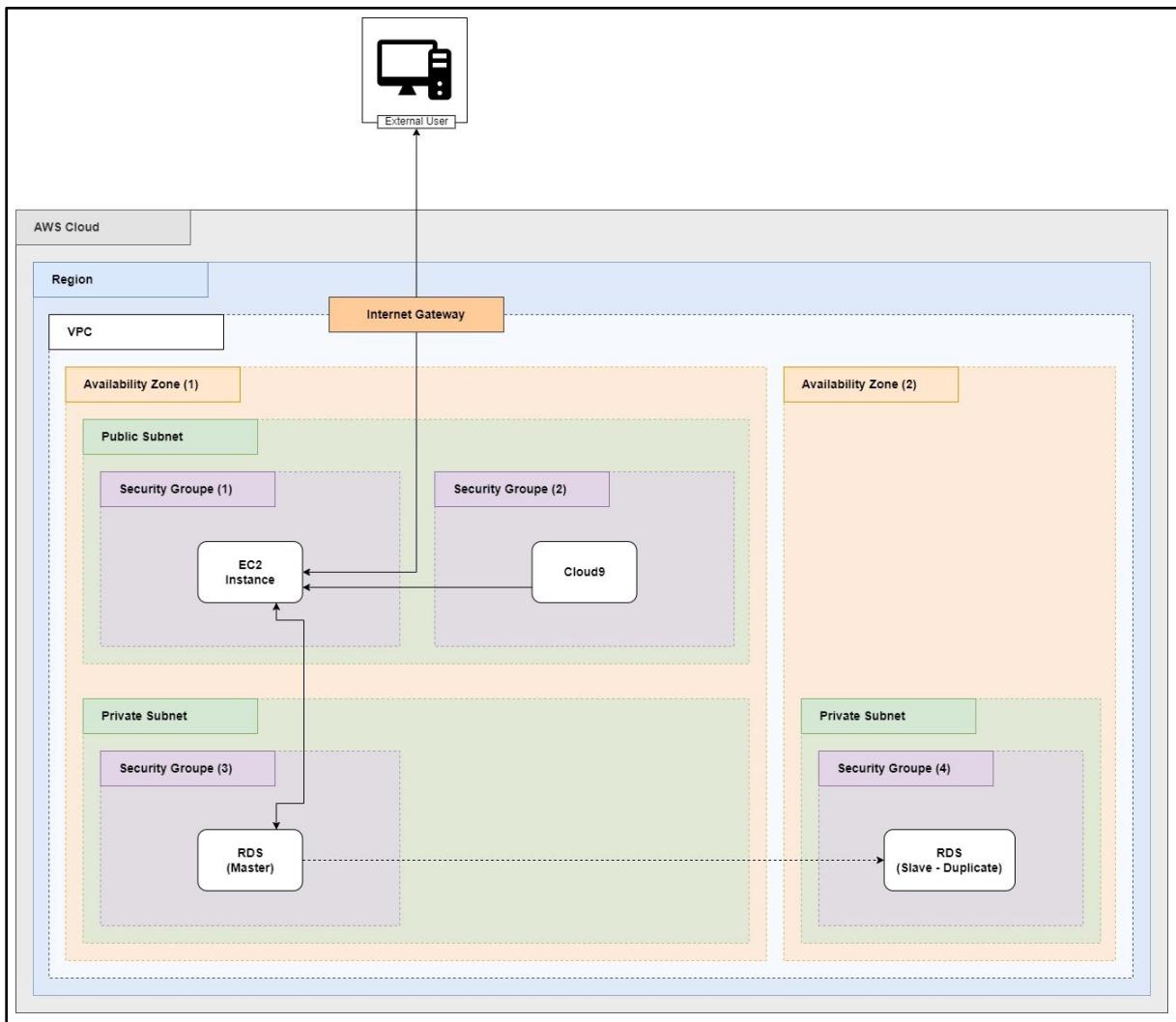
Capstone Project – Theoretical Solution

Architecture

We established the following architecture plan before starting to create the instances and components:



After completing the project, we realized that the RDS created backup of the database in multiple AZ, therefor we could represent the architecture like the following:



We still value the first schema more than the second one, since the second one is generated automatically by AWS for a highly available database principle.

Capstone Project – AWS Solution

VPC

The screenshot shows the AWS VPC console interface. The left sidebar navigation includes 'VPC dashboard', 'EC2 Global View', 'Filter by VPC', 'Virtual private cloud' (with 'Your VPCs' selected), 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', 'Endpoints', 'Endpoint services', 'NAT gateways', 'Peering connections', and 'Security'. The main content area displays 'Your VPCs (1/2) Info' with a table showing two VPCs: 'project-vpc' (VPC ID: vpc-00f000be44a6072f3, State: Available, IPv4 CIDR: 10.0.0.0/16, IPv6 CIDR: -, DHCP option set: dopt-03) and another unnamed VPC (VPC ID: vpc-0424100043b5aaa42, State: Available, IPv4 CIDR: 172.31.0.0/16, IPv6 CIDR: -, DHCP option set: dopt-03). Below the table, the details for 'vpc-00f000be44a6072f3 / project-vpc' are shown, including VPC ID (vpc-00f000be44a6072f3), State (Available), Tenant (Default), Default VPC (No), Network Address Usage metrics, and various configuration settings like DNS resolution, Main route table, IPv6 pool, and Owner ID.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP o
project-vpc	vpc-00f000be44a6072f3	Available	10.0.0.0/16	-	dopt-03
-	vpc-0424100043b5aaa42	Available	172.31.0.0/16	-	dopt-03

vpc-00f000be44a6072f3 / project-vpc

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

Details	
VPC ID vpc-00f000be44a6072f3	State Available
Tenancy Default	DHCP option set dopt-03596d64df70dd3ab
Default VPC No	IPv4 CIDR 10.0.0.0/16
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule
DNS hostnames Enabled	
Main route table rtb-0cd80ea0c00656520	
IPv6 pool -	
Owner ID	
DNS resolution Enabled	
Main network ACL acl-0fb3f54b7901ce943	
IPv6 CIDR (Network border group) -	

Subnets

Screenshot of the AWS VPC Subnets page showing 15 subnets listed in a table.

Name	Subnet ID	State	VPC	IPv4 CIDR
RDS-Pvt-subnet-5	subnet-080e8bf3070b2af5d	Available	vpc-00f000be44a6072f3 proj...	10.0.18.0/25
RDS-Pvt-subnet-4	subnet-0ca5918c295ca1929	Available	vpc-00f000be44a6072f3 proj...	10.0.17.128/25
RDS-Pvt-subnet-3	subnet-0ecde4c5ecf4d3eea	Available	vpc-00f000be44a6072f3 proj...	10.0.17.0/25
RDS-Pvt-subnet-2	subnet-0010dd9521717a10	Available	vpc-00f000be44a6072f3 proj...	10.0.16.128/25
RDS-Pvt-subnet-1	subnet-080fb26f256d531af	Available	vpc-00f000be44a6072f3 proj...	10.0.16.0/25
project-subnet-public1-us-east-1a	subnet-0b5655fe2798b6fbe	Available	vpc-00f000be44a6072f3 proj...	10.0.0.0/20
project-subnet-private1-us-east-1a	subnet-03cfb21cb713973b1	Available	vpc-00f000be44a6072f3 proj...	10.0.128.0/20
-	subnet-061e54b6286c680f7	Available	vpc-0424100043b5aaa42	172.31.0.0/20
-	subnet-06c207ec595619cf	Available	vpc-0424100043b5aaa42	172.31.64.0/20
-	subnet-048fdbba81e499880	Available	vpc-0424100043b5aaa42	172.31.16.0/20
-	subnet-04fd41446f5889ffa	Available	vpc-0424100043b5aaa42	172.31.48.0/20
-	subnet-0cc242423fc82e344	Available	vpc-0424100043b5aaa42	172.31.32.0/20
-	subnet-0ee0df40d123d252d	Available	vpc-0424100043b5aaa42	172.31.80.0/20

Screenshot of the AWS VPC Subnets page showing 13 subnets listed in a table. A specific subnet (subnet-0b5655fe2798b6fbe) is selected and expanded.

Name	Subnet ID	State	VPC	IPv4 CIDR
RDS-Pvt-subnet-5	subnet-080e8bf3070b2af5d	Available	vpc-00f000be44a6072f3 proj...	10.0.18.0/25
RDS-Pvt-subnet-4	subnet-0ca5918c295ca1929	Available	vpc-00f000be44a6072f3 proj...	10.0.17.128/25

Selected Subnet Details:

Details	Value	Details	Value
Subnet ID	subnet-0b5655fe2798b6fbe	Subnet ARN	arn:aws:ec2:us-east-1:538795172629:subnet/subnet-0b5655fe2798b6fbe
Available IPv4 addresses	4090	State	Available
Network border group	us-east-1	IPv6 CIDR	-
VPC	vpc-00f000be44a6072f3 project-vpc	Route table	rtb-012ab948d29923250 project-rtb-public
Default subnet	No	Auto-assign IPv6 address	Auto-assign customer-owned IPv4 address

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#subnets;sort=desc;tagName

AWS Services Search [Alt+S] N. Virginia MaxenceRobichon

VPC dashboard EC2 VPC IAM

Subnets (1/13) Info

Find resources by attribute or tag

Name	Subnet ID	State	VPC	IPv4 CIDR
RDS-Pvt-subnet-5	subnet-080e8bf3070b2af5d	Available	vpc-00f000be44a6072f3 proje...	10.0.18.0/25
RDS-Pvt-subnet-4	subnet-0ca5918c295ca1929	Available	vpc-00f000be44a6072f3 proje...	10.0.17.128/25

Virtual private cloud Your VPCs New Subnets

Route tables Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections Security

CloudShell Feedback Language

Actions Create subnet

subnet-03cfb21cb713973b1 / project-subnet-private1-us-east-1a

Details Flow logs Route table Network ACL CIDR reservations Sharing Tags

Details

Subnet ID subnet-03cfb21cb713973b1	Subnet ARN arn:aws:ec2:us-east-1:538795172629:subnet/subnet-03cfb21cb713973b1	State Available	IPv4 CIDR 10.0.128.0/20
Available IPv4 addresses 4091	IPv6 CIDR -	Availability Zone us-east-1a	Availability Zone ID use1-az6
Network border group us-east-1	VPC vpc-00f000be44a6072f3 project-vpc	Route table rtb-069962209402e7bd project-rtb-private1-us-east-1a	Network ACL acl-0fb3f54b7901ce943
Default subnet No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Route Tables

Screenshot of the AWS VPC Route Tables page (us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables). The page shows a list of route tables:

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
RDS-Pvt-rt	rtb-01a0178bd7a04c095	5 subnets	-	No	vpc-00f000be44a6072f3
project-rtb-public	rtb-012ab948d29923250	subnet-0b5655fe2798b6...	-	No	vpc-00f000be44a6072f3
project-rtb-private1-us-east-1a	rtb-0699622209402e7bd	subnet-03cfb21cb71397...	-	No	vpc-00f000be44a6072f3

The selected route table is "rtb-012ab948d29923250 / project-rtb-public". The "Routes" tab is active, showing two routes:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-07c2742f8c63e0c9e	Active	No
10.0.0.0/16	local	Active	No

Screenshot of the AWS VPC Route Tables page (us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables). The page shows a list of route tables:

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
RDS-Pvt-rt	rtb-01a0178bd7a04c095	5 subnets	-	No	vpc-00f000be44a6072f3
project-rtb-public	rtb-012ab948d29923250	subnet-0b5655fe2798b6...	-	No	vpc-00f000be44a6072f3
project-rtb-private1-us-east-1a	rtb-0699622209402e7bd	subnet-03cfb21cb71397...	-	No	vpc-00f000be44a6072f3

The selected route table is "rtb-012ab948d29923250 / project-rtb-public". The "Subnet associations" tab is active, showing one explicit subnet association:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
project-subnet-public1-us-east-1a	subnet-0b5655fe2798b6fb	10.0.0.0/20	-

The "Subnets without explicit associations" section shows 0 subnets.

Screenshot of the AWS VPC Route Tables page (us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:sort=desc:tag.Name).

The page shows a list of route tables:

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
RDS-Pvt-rt	rtb-01a0178bd7a04c095	5 subnets	-	No	vpc-00f000be44a6072f3
project-rtb-public	rtb-01ab948d29923250	subnet-0b5655fe2798b6...	-	No	vpc-00f000be44a6072f3
project-rtb-private1-us-east-1a	rtb-0699622209402e7bd	subnet-03cfb21cb71397...	-	No	vpc-00f000be44a6072f3

Details for the selected route table (rtb-0699622209402e7bd / project-rtb-private1-us-east-1a):

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Subnet associations (1)

Name	Subnet ID	IPv4 CIDR
project-subnet-private1-us-east-1a	subnet-03cfb21cb713973b1	10.0.128.0/20

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR

Screenshot of the AWS VPC Route Tables page (us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#RouteTables:sort=desc:tag.Name), showing the same route table configuration as the previous screenshot.

The page shows a list of route tables:

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
RDS-Pvt-rt	rtb-01a0178bd7a04c095	5 subnets	-	No	vpc-00f000be44a6072f3
project-rtb-public	rtb-01ab948d29923250	subnet-0b5655fe2798b6...	-	No	vpc-00f000be44a6072f3
project-rtb-private1-us-east-1a	rtb-0699622209402e7bd	subnet-03cfb21cb71397...	-	No	vpc-00f000be44a6072f3

Details for the selected route table (rtb-0699622209402e7bd / project-rtb-private1-us-east-1a):

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR
project-subnet-private1-us-east-1a	subnet-03cfb21cb713973b1	10.0.128.0/20

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR

A screenshot of a Windows desktop environment is overlaid on the bottom right of the browser window, showing a file explorer window and a taskbar with various icons.

Internet Gateway

The screenshot shows the AWS VPC Internet Gateways page. The left sidebar navigation includes 'VPC dashboard', 'EC2 Global View', 'Filter by VPC' (with a dropdown for 'Select a VPC'), 'Virtual private cloud' (with 'Your VPCs' and 'New' options), 'Subnets', 'Route tables', 'Internet gateways' (selected), 'Egress-only internet gateways', 'Carrier gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', 'Endpoints', 'Endpoint services', 'NAT gateways', 'Peering connections', and 'Security'. The main content area displays a table titled 'Internet gateways (1/2) Info' with two rows:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-04e51e16067e8a56c	Attached	vpc-0424100043b5aaa42	538795172629
project-igw	igw-07c2742f8c63e0c9e	Attached	vpc-00f000be44a6072f3 project-vpc	538795172629

Below the table, a section for 'igw-07c2742f8c63e0c9e / project-igw' shows the 'Details' tab selected, displaying the following information:

Internet gateway ID igw-07c2742f8c63e0c9e	State Attached	VPC ID vpc-00f000be44a6072f3 project-vpc	Owner 538795172629
--	-------------------	---	-----------------------

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

Security Groups

The screenshot shows the AWS VPC Security Groups page. The left sidebar includes options like Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security (Network ACLs, Security groups), DNS firewall (Rule groups, Domain lists), and Network Firewall (Firewalls). The main content area displays a table titled "Security Groups (1/6) Info" with columns: Name, Security group ID, Security group name, VPC ID, Description, and Owner. One row is selected, showing "aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b-InstanceSecurityGroup-P9NE68OALU5P" with "sg-0bf9f262c77f10bf2" as the ID, "aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b-InstanceSecurityGroup-P9NE68OALU5P" as the name, "vpc-00f000be44a6072f3" as the VPC ID, and "Security group for AWS Cloud9 environment aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b" as the description. The owner is listed as "538795172629". Below the table, there's a detailed view of the selected security group with fields: Security group name, Security group ID, Description, VPC ID, Owner, Inbound rules count, and Outbound rules count.

Name	Security group ID	Security group name	VPC ID	Description	Owner
aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b-InstanceSecurityGroup-P9NE68OALU5P	sg-0bf9f262c77f10bf2	aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b-InstanceSecurityGroup-P9NE68OALU5P	vpc-00f000be44a6072f3	Security group for AWS Cloud9 environment aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b	538795172629
-	sg-0eaaa0d0705a484999	ec2-rds-1	vpc-00f000be44a6072f3	Security group attached to ec2-rds-1	538795172629
-	sg-070c0844e5b4ccf71	default	vpc-00f000be44a6072f3	default VPC security group	538795172629
-	sg-0986be8f2436c3635	RDS-security-group	vpc-00f000be44a6072f3	Created by RDS manager	538795172629
-	sg-0538dab93d2be99a5	default	vpc-0424100043b5aaa42	default VPC security group	538795172629
-	sg-0165bafe09baa140e	rds-ec2-1	vpc-00f000be44a6072f3	Security group attached to rds-ec2-1	538795172629

Security group name: aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b-InstanceSecurityGroup-P9NE68OALU5P
Security group ID: sg-0bf9f262c77f10bf2
Description: Security group for AWS Cloud9 environment aws-cloud9-ProjectCloud-ef4e47514a0427cba5c5559c8c4726b
VPC ID: vpc-00f000be44a6072f3
Owner: 538795172629
Inbound rules count: 1 Permission entry
Outbound rules count: 1 Permission entry

EC2 Instances

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes). The main content area shows a table of instances with one row selected. The selected instance is named "aws-cloud9-Pr...", with the ID "i-03308bc817c5391a4". It is listed as "Running" with the instance type "t2.micro". The status check shows "2/2 checks passed" and no alarms. The availability zone is "us-east-1a" and the public IPv4 DNS is "ec2-18-206-241-21". Below the table, a detailed view for the selected instance is shown. The "Details" tab is active, displaying information such as Instance ID (i-03308bc817c5391a4), Public IPv4 address (18.206.241.236), Private IPv4 addresses (10.0.15.76), Instance state (Running), Private IP DNS name (ip-10-0-15-76.ec2.internal), Instance type (t2.micro), and Elastic IP addresses. Other tabs include Security, Networking, Storage, Status checks, Monitoring, and Tags.

This screenshot is identical to the one above, but the "Security" tab is now active in the detailed view. It shows the IAM Role assigned to the instance, which is "project_role", and the Owner ID, which is "538795172629". It also displays the launch time, which is "Fri Jul 21 2023 11:01:09 GMT+0200 (heure d'été d'Europe centrale)". Below this, the "Inbound rules" section is partially visible.

IAM – Roles

The screenshot shows the AWS IAM Roles page for a role named 'project_role'. The role allows EC2 instances to call AWS services on behalf of the user. It was created on July 21, 2023, at 12:02 (UTC+02:00). The last activity was 'None'. The maximum session duration is 1 hour. The ARN is arn:aws:iam::538795172629:role/project_role. An instance profile ARN is also listed: arn:aws:iam::538795172629:instance-profile/project_role.

Summary

Creation date	ARN
July 21, 2023, 12:02 (UTC+02:00)	arn:aws:iam::538795172629:role/project_role

Last activity	Maximum session duration
None	1 hour

Permissions

Permissions policies (1) Info
You can attach up to 10 managed policies.

Policy name	Type	Description
AmazonSSMReadOnlyAccess	AWS managed	Provides read only access to Amaz

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Databases (RDS)

The screenshot shows the Amazon RDS Databases console. On the left, a sidebar menu includes options like Dashboard, Databases (selected), Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Zero-ETL integrations, Events, and Event subscriptions. The main content area displays a table titled "Databases (1)". The table has columns for DB identifier, Status, Role, Engine, Region & AZ, Size, Actions, CPU, and Current activity. A single row is shown for "database-1", which is "Available", an "Instance", using "MySQL Community" engine, located in "us-east-1a", with "db.t3.micro" configuration, 2 Actions, 3.29% CPU usage, and 1 Co. The top of the page features a banner for "Introducing Aurora I/O-Optimized" and a note about minimizing downtime during upgrades.

The screenshot shows the Amazon RDS Connectivity & security console. The left sidebar is identical to the previous screenshot. The main content area is titled "Connectivity & security" and contains three sections: "Endpoint & port", "Networking", and "Security". Under "Endpoint & port", it shows the endpoint as "database-1.cpu6x25uobdy.us-east-1.rds.amazonaws.com" and the port as "3306". Under "Networking", it shows the availability zone as "us-east-1a", the VPC as "project-vpc (vpc-00f000be44a6072f3)", and the subnet group as "rds-ec2-db-subnet-group-1". Under "Security", it shows the VPC security groups as "RDS-security-group (sg-0966be8f2436c3635)" (Active) and "rds-ec2-1 (sg-0165bafe09baa140e)" (Active). It also indicates that the instance is publicly accessible. At the bottom, there is a section for "Security group rules (3)".

us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#database-id=database-1;is-cluster=false

Amazon RDS X

Services Search [Alt+S]

EC2 VPC IAM

Amazon RDS

Dashboard Databases

Query Editor Performance insights Snapshots Exports in Amazon S3 Automated backups Reserved instances Proxies

Subnet groups Parameter groups Option groups Custom engine versions Zero-ETL integrations Preview

Events Event subscriptions CloudShell Feedback Language

subnet-080fb26f256d531af
subnet-0010ddaa9521717a10
subnet-080e8bf3070b2af5d
subnet-0c5918c295ca1929
subnet-0ecd4c5ecf4d3eea

Certificate authority Info rds-ca-2019

Certificate authority date August 22, 2024, 19:08 (UTC+02:00)

Network type IPv4 DB instance certificate expiration date August 22, 2024, 19:08 (UTC+02:00)

Security group rules (3)

Filter by Security group rules

Security group	Type	Rule
rds-ec2-1 (sg-0165bafe09baa140e)	EC2 Security Group - Inbound	sg-0eaa40d705a484999
RDS-security-group (sg-0986be8f2436c3635)	CIDR/IP - Inbound	217.26.204.244/32
RDS-security-group (sg-0986be8f2436c3635)	CIDR/IP - Outbound	0.0.0.0/0

Replication (1)

Filter by Replication

DB identifier	Role	Region & AZ	Replication source	Replication state	Last error	Privacy	Terms	Cookie preferences
database-1	Instance	us-east-1a	-	-	-	-	-	-

© 2023, Amazon Web Services, Inc. or its affiliates.

us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#database-id=database-1;is-cluster=false

Amazon RDS X

Services Search [Alt+S]

EC2 VPC IAM

Amazon RDS

Dashboard Databases

Query Editor Performance insights Snapshots Exports in Amazon S3 Automated backups Reserved instances Proxies

Subnet groups Parameter groups Option groups Custom engine versions Zero-ETL integrations Preview

Events Event subscriptions CloudShell Feedback Language

database-1 Instance us-east-1a

Proxies (0)

Filter by proxies

Proxy identifier	Status	Engine family
No proxies	You don't have any proxies.	

Create proxy

Connected compute resources (1) [Info](#)

Connections to compute resources that were created automatically by RDS are shown here. Connections to compute resources that were created manually aren't shown.

Filter by compute resources

Resource identifier	Resource type	Availability zone	RDS security group	Compute resource security group
i-03308bc817c5391a4	EC2 instance	us-east-1a	rds-ec2-1	ec2-rds-1

© 2023, Amazon Web Services, Inc. or its affiliates.

System Manager – Store parameters

The screenshot shows the AWS Systems Manager Parameter Store interface. At the top, there's a search bar and navigation links for EC2, VPC, and IAM. Below that, the AWS Systems Manager logo and 'Parameter Store' are visible. A breadcrumb trail shows 'My parameters'. On the left, a sidebar has 'My parameters' selected. The main area displays a table of parameters:

Name	Tier	Type	Last modified
/example/database	Standard	String	Fri, 21 Jul 2023 10:00:37 GMT
/example/endpoint	Standard	String	Fri, 21 Jul 2023 09:59:48 GMT
/example/password	Standard	String	Fri, 21 Jul 2023 10:00:20 GMT
/example/username	Standard	String	Fri, 21 Jul 2023 10:00:06 GMT

At the bottom right of the table are buttons for 'View details', 'Edit', 'Delete', and 'Create parameter'. The footer includes links for CloudShell, Feedback, Language, and copyright information.

This screenshot shows the detailed view for the '/example/database' parameter. The URL in the address bar is 'us-east-1.console.aws.amazon.com/systems-manager/parameters/example/database?region=us-east-1&tab=Table'. The page title is 'AWS Systems Manager > Parameter Store > /example/database > Overview'. The parameter name is '/example/database'. The 'Overview' tab is selected, with 'History' and 'Tags' also available.

Name	/example/database	Description	-
Tier	Standard	Data type	text
Type	String	Last modified user	arn:aws:iam::538795172629:root
Last modified date	Fri, 21 Jul 2023 10:00:37 GMT	Version	1
Value	project		

At the bottom right are 'Edit' and 'Delete' buttons. The footer includes links for CloudShell, Feedback, Language, and copyright information.

The screenshot shows the AWS Systems Manager Parameter Store Overview page for a parameter named `/example/endpoint`. The parameter is of type String and has a value of `database-1.cpu6x23uobdy.us-east-1.rds.amazonaws.com`. It was last modified on Fri, 21 Jul 2023 09:59:48 GMT by the user arn:aws:iam::538795172629:root.

Attribute	Value
Name	<code>/example/endpoint</code>
Tier	Standard
Type	String
Last modified date	Fri, 21 Jul 2023 09:59:48 GMT
Value	<code>database-1.cpu6x23uobdy.us-east-1.rds.amazonaws.com</code>
Description	-
Data type	text
Last modified user	arn:aws:iam::538795172629:root
Version	1

The screenshot shows the AWS Systems Manager Parameter Store Overview page for a parameter named `/example/password`. The parameter is of type String and has a value of `admin1234`. It was last modified on Fri, 21 Jul 2023 10:00:20 GMT by the user arn:aws:iam::538795172629:root.

Attribute	Value
Name	<code>/example/password</code>
Tier	Standard
Type	String
Last modified date	Fri, 21 Jul 2023 10:00:20 GMT
Value	<code>admin1234</code>
Description	-
Data type	text
Last modified user	arn:aws:iam::538795172629:root
Version	1

us-east-1.console.aws.amazon.com/systems-manager/parameters/example/username?region=us-east-1&tab=Table

aws Services Search [Alt+S]

EC2 VPC IAM

AWS Systems Manager > Parameter Store > /example/username > Overview

/example/username

Edit Delete

Overview History Tags

Name	Description
/example/username	-
Tier	Data type
Standard	text
Type	Last modified user
String	arn:aws:iam::538795172629:root
Last modified date	Version
Fri, 21 Jul 2023 10:00:06 GMT	1
Value	
admin	

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Cloud IDE – AWS Cloud9

The screenshot shows the AWS Cloud9 interface. The left sidebar has 'Environments' selected. The main content area shows a table titled 'Environments (1)'. The table has columns: Name, Cloud9 IDE, Environment type, Connection, Permission, and Owner ARN. One row is listed: 'ProjectCloud' (Cloud9 IDE), 'Open' (Environment type), 'EC2 instance' (Connection), 'AWS Systems Manager (SSM)' (Permission), and 'Owner' (Owner ARN). A 'Create environment' button is at the top right of the table.

Name	Cloud9 IDE	Environment type	Connection	Permission	Owner ARN
ProjectCloud	Open	EC2 instance	AWS Systems Manager (SSM)	Owner	arn:aws:iam::538795172629:root

EC2 Console from Cloud9

The screenshot shows the AWS Cloud9 IDE interface with the MySQL command:

```
MySQL [project]> select * from countrydata_final
```

The output displays data for various countries across several columns:

name	GDP	mobilephones	mortalityunder5	healthexpenditurepercapita	healthexpenditurepercentGDP	population	populationurban	birthrate	lifeexpectancy
Afghanistan	2491666315	0	158	11	9	26697430	5771984	50	46
Albania	3686640387	29791	29	75	6	3071856	1288964	17	74
Algeria	54790505957	86000	49	63	3	30533827	18259229	21	70
American Samoa	0	1992	0	0	0	57625	51171	0	0
Andorra	113644295	23543	5	1289	8	64634	59722	11	0
Angola	191180361	25806	200	15	2	13926373	6823923	50	46
Antigua and Barbuda	802526781	22000	15	411	5	77656	24928	21	0
Argentina	284204000000	6487950	20	689	9	36938709	33274569	19	74
Armenia	1911563665	17486	33	41	7	3076098	2802540	13	71
Aruba	1858659293	15000	0	0	0	96271	42157	14	74
Australia	18562000	8562000	6	1728	8	19153000	16701416	13	88
Austria	192071800000	6117000	6	2361	10	8011566	5271610	18	78
Azerbaijan	5272617196	428400	67	30	5	80485000	4120883	15	67
Bahamas, The	6327552000	31524	17	1072	6	297651	244074	18	72
Bahrain	797069894	205727	12	488	4	638193	564163	22	74
Bangladesh	1	279000	86	9	3	129592275	30583777	27	65

The screenshot shows the AWS Cloud9 IDE interface with the MySQL command:

```
MySQL [project]> select * from countrydata_final
```

The output displays data for various countries across several columns:

name	GDP	mobilephones	mortalityunder5	healthexpenditurepercapita	healthexpenditurepercentGDP	population	populationurban	birthrate	lifeexpectancy
United States	15	989880000000	109478031	9	4703	13	282162411	223190467	1
Uruguay	16	77	410787	17	773	11	3300847	3013674	1
Uzbekistan	21	75	22823255806	53128	63	32	24650400	9194599	1
Vanuatu	33	67	13760374488	365	23	48	185074	40161	1
Venezuela, RB	23	68	272014693	5447172	25	273	24311000	21886567	1
Vietnam	17	73	117148000000	788559	35	22	77630900	18864309	1
Virgin Islands (U.S.)	14	72	31172517272	35000	0	0	108639	100600	1
West Bank and Gaza	41	78	0	7076	31	0	3064150	2147967	1
Yemen, Rep.	41	71	4113261233	32842	100	25	17723186	4661198	1
Zambia	45	60	9636342275	98853	157	18	10281562	3550144	1
Zimbabwe	30	42	3237716325	266441	115	59	12569477	4228203	1

Below the table, the command:

```
MySQL [project]> show tables;
```

Shows the following tables:

Tables_in_project	countrydata_final
Tables_in_project	countrydata_final

Website

Number of mobile phone providers	
Afghanistan	0
Albania	29791
Algeria	86000
American Samoa	1992
Andorra	23543
Angola	25806
Antigua and Barbuda	22000
Argentina	6487950
Armenia	17486
Aruba	15000
Australia	8562000
Austria	6117000
Azerbaijan	420400
Bahamas, The	31524
Bahrain	205727
Bangladesh	279000
Barbados	28467
Belarus	49353
Belgium	5629000
Belize	16812
Benin	55476
Bermuda	13000
Bhutan	0
Bolivia	582620
Bosnia and Herzegovina	93386
Botswana	222190
Brazil	23188171
Brunei Darussalam	95000
Bulgaria	738000
Burkina Faso	25245
Burundi	16320
Cambodia	130547

Non sécurisé | 18.206.241.236/index.php

Example Social Research Organization

[About Us](#) [Contact Us](#) [Query](#)

Welcome to our data query site. You can get data from countries all over the world to use in your research.

We provide data for a variety of areas including basic demographics and development statistics.

About Us



Shirley Rodriguez

Our site got started when Shirley Rodriguez found that she was frequently looking up data from a variety of databases. Shirley decided to start sharing some of this data with other social researchers.

Non sécurisé | 18.206.241.236/index.php#contactUs



Shirley Rodriguez

Our site got started when Shirley Rodriguez found that she was frequently looking up data from a variety of databases. Shirley decided to start sharing some of this data with other social researchers.

Contact Us

**ESRI
DATA FOR
SOCIAL RESEARCH**

123 Any Street
Any Town, USA

Hours

Weekdays: 6:00am - 6:00pm
Saturday: 7:00am - 7:00pm
Closed on Sundays

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Outil Capture d'écran

Capture d'écran copiée dans le Presse-papiers et enregistrée

Sélectionner ici pour annoter et partager l'image

Non sécurisé | 18.206.241.236/query2.php

Pick another query

This is a Country Name

	Gross Domestic Product
Afghanistan	2461666315
Albania	3686649387
Algeria	54790058957
American Samoa	0
Andorra	1133644295
Angola	9129180361
Antigua and Barbuda	802526701
Argentina	284204000000
Armenia	1911563665
Aruba	1858659293
Australia	416888000000
Austria	192071000000
Azerbaijan	5272617196
Bahamas, The	6327552000
Bahrain	7970690894
Bangladesh	47124925462
Barbados	2558850048
Belarus	12736856485
Belgium	232673000000
Belize	832072465
Benin	2254838685
Bermuda	3480219000
Bhutan	427808817
Bolivia	8397858206
Bosnia and Herzegovina	5505984456
Botswana	5632391130
Brazil	644702000000
Brunei Darussalam	6001153318
Bulgaria	12903546576
Burkina Faso	2610945549
Burundi	835334807
Cambodia	3654031716

[Pick another query](#)

Country Name	Population	Urban Population
Afghanistan	26697430	5771984
Albania	3071856	1280964
Algeria	30533827	18259229
American Samoa	57625	51171
Andorra	64634	59722
Angola	13926373	6823923
Antigua and Barbuda	77656	24928
Argentina	36930709	33274569
Armenia	3076098	2002540
Aruba	90271	42157
Australia	19153000	1670416
Austria	8011566	5271610
Azerbaijan	8048600	4120883
Bahamas, The	297651	244074
Bahrain	638193	564163
Bangladesh	129592275	30583777
Barbados	267511	97106
Belarus	10005000	6993495
Belgium	10251250	9953964
Belize	249800	119404
Benin	6517810	2496321
Bermuda	62100	62100
Bhutan	571262	145101
Bolivia	8307248	5133879
Bosnia and Herzegovina	3693698	1595678
Botswana	1757925	935216
Brazil	174425387	141633414
Brunei Darussalam	327036	232523
Bulgaria	8170172	5629249
Burkina Faso	12294012	2040806
Burundi	6374347	529071
Cambodia	12446949	2103534

[Pick another query](#)

Country Name	Birth Rate	Life Expectancy
Afghanistan	50	46
Albania	17	74
Algeria	21	70
American Samoa	0	0
Andorra	11	0
Angola	50	46
Antigua and Barbuda	21	0
Argentina	19	74
Armenia	13	71
Aruba	14	74
Australia	13	80
Austria	10	78
Azerbaijan	15	67
Bahamas, The	18	72
Bahrain	22	74
Bangladesh	27	65
Barbados	12	76
Belarus	9	69
Belgium	11	78
Belize	30	74
Benin	43	53
Bermuda	14	78
Bhutan	27	62
Bolivia	31	63
Bosnia and Herzegovina	11	75
Botswana	27	51
Brazil	21	70
Brunei Darussalam	23	77
Bulgaria	9	72
Burkina Faso	45	50
Burundi	38	46
Cambodia	27	58

← → C Non sécurisé | 18.206.241.236/query2.php

Pick another query.

Country Name	Childhood Mortality
Afghanistan	150
Albania	29
Algeria	49
American Samoa	0
Andorra	5
Angola	200
Antigua and Barbuda	15
Argentina	20
Armenia	33
Aruba	0
Australia	6
Austria	6
Azerbaijan	67
Bahamas, The	17
Bahrain	12
Bangladesh	86
Barbados	17
Belarus	14
Belgium	6
Belize	27
Benin	143
Bermuda	0
Bhutan	89
Bolivia	82
Bosnia and Herzegovina	10
Botswana	96
Brazil	36
Brunei Darussalam	9
Bulgaria	21
Burkina Faso	191
Burundi	164
Cambodia	103

Quizz

IAM part

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

A

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

A

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

C,D

Which statement describes a resource-based policy?

A

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

B

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?

C

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

A

Network part

Which definition describes a virtual private cloud (VPC)?

C

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?

C

Which combination of actions enables direct access for IPv4 hosts in a virtual private cloud (VPC)? (select three)

A,D,F

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?

D

Capstone Project – Questions

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

The given IAM policy allows a user to perform the following actions:

1. On EC2 instances in the "us-east-1" region for a specific AWS account (account number: 123456789012):
 - o Launch instances (ec2:RunInstances).
 - o Terminate instances (ec2:TerminateInstances).
2. On S3 objects in the "example-bucket" S3 bucket:
 - o Get (read) objects (s3:GetObject).
 - o Put (write) objects (s3:PutObject).

The policy is set to "Allow" for these actions.

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

This policy allows access to VPC-related information only if the request is made from a specific region. The region from which the request is done must be "us-west-2".

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

The provided IAM policy permits users to read and write the "example-bucket" S3 bucket and all its related objects, symbolized with the (*). The specific prefixes which are specified in the condition are "documents/*" and "images/*"

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

The provided IAM policy allows users to create and delete IAM users, but only for their own user path in IAM.

Questions:

Which AWS service does this policy grant you access to?

The provided IAM policy allows IAM users to perform read-only actions (Get) and list operations (List) on all IAM resources within the AWS account. The policy's resource field is set to "*", meaning it applies to all IAM resources without restrictions.

Does it allow you to create an IAM user, group, policy, or role?

This policy does not allow the creation of IAM users, groups, policies, or roles because it is not explicitly defined.

Name at least three specific actions that the iam:Get* action allows.

The iam:Get* action is a wildcard that grants IAM users the ability to perform multiple read-only operations on various IAM resources. It includes specific actions such as:

1. iam:GetUser: Allows IAM users to fetch information about an IAM user, such as the user's name, path, unique ID, and access keys.
2. iam:GetGroup: Allows IAM users to retrieve information about an IAM group, including the group's name, path, unique ID, and its members.
3. iam:GetPolicy: Enables IAM users to obtain details about an IAM policy, including its name, path, and the policy document.

Questions:

What actions does the policy allow?

This policy targets EC2 instances with instance types "t2.micro" and "t2.small" and applies a "Deny" effect on the actions `ec2:RunInstances` and `ec2:StartInstances`. The Deny effect will prevent users from running or starting instances with those specific instance types in the AWS account.

How would the policy restrict the access granted to you by this additional statement?

The "Allow" statement permits all actions for the "t2.micro" and "t2.small" EC2 instances but because "Deny" statements take precedence over "Allow" statements in case of conflicts between the two, the "t2.micro" and "t2.small" EC2 instances are still not able to run and start instances with those specific instance types in the AWS account.

If the policy included both the statement on the left and the statement in question 2, could you terminate an m3.xlarge instance that existed in the account?

Given these two policies, if there is an m3.xlarge instance, attempting to terminate that specific instance with the "t2.micro" and "t2.small" EC2 instances will be denied. The "Deny" statement takes precedence over the "Allow" statement, so the "Deny" effect will prevent the termination of the specified instance, despite the "Allow" statement allowing all other EC2 actions.

Capstone Project – QuickSight

Screenshot of the QuickSight analysis titled "Patient-Info analysis".

The interface includes a top navigation bar with back, forward, search, and other browser controls, and a right sidebar with user information (Username: 538795172629, Account name: quicksight-projet-cloud) and account management links.

The main area shows the following components:

- Dataset:** SPICE Patient-Info
- Sheet 1:** Sum of Revenue by Admit Date (Line chart showing revenue peaks around Dec 1-4, 2018).
- Sum of Discount and Sum of Profit by Admit Date and Category:** A table showing data for Ante/Post Partum admissions across various categories.
- Sum of Profit by Hospital:** A donut chart showing hospital profits, with the total value labeled as 1.52M.
- Sum of Cost by Category and Admit Date:** A stacked bar chart comparing costs for different categories (Surgical, Medical, Critical Care) between 2017 and 2018.

A message in the top-left corner states: "Total Cost for 2018 increased by 13.53% (2,306.01) from 17,045.85 to 19,351.86."

The sidebar also lists various parameters, actions, themes, and settings.

Conclusion

The project is now functional and running. We closed the instances and shut down our website.