

---

## Table of Contents

1. Assignment Overview .....	5
2. Architecture Design.....	6
3. Security Design.....	9
4. Cost Considerations.....	13
5. Design Limitations.....	15
6. Implementation .....	16
7. Conclusions .....	32

---

## 1. Assignment Overview

### **Motivation**

After the implementation of the website on AWS cloud, Shops R' Us will have more options in fine tuning the website security. In addition, Shops R' Us do not need to purchase on-premise hardware since it will be handled by AWS. Lastly, when there is a significant increase in the website traffic, it is easier for Shop R' Us to scale up on cloud in comparison to when they host it on-premise. They will not get caught in the scenario for long lead time when ordering the hardware.

### **Objectives**

Shops R'Us would like to develop and deploy an online shopping website which is able to facilitate different customer events such placing a purchase, browsing products, create profiles and make payment. The website developed in this assignment is able to support placing a purchase only (which is used as an illustration since this is a cloud architecting course, but in real life the website should be able to handle multiple events).

### **Scopes**

The scope of this project includes :

- Database of the website will be hosted in MySQL format securely.
- All administrators will be able to access to AWS console securely.
- Other web users will be able to access the website anonymously.
- Administrators will also be able to use bastion host to securely access instances (especially private instances) via SSH.
- By using the Load Balancer which distributes incoming traffic to two Availability Zones.
- Auto-Scaling Group is used to scale-in or scale-out of web and app tier EC2 according to the traffic.
- Cloud Trail is used hence administrator is able to store and monitor activities performed by different users (AWS CloudTrail, 2023).

### **Assumptions**

- Only one EC2 is created for the web and app server, by assuming that Shop R' Us is a small medium enterprise when one EC2 (t2 micro size) is able to handle the website.
- 256 IP addresses per subnet are assigned for each public/private subnet, by assuming that 251 addresses (where the other five addresses are reserved for AWS) are sufficient for Shop R' Us.

---

## 2. Architecture Design

### Identify AWS Services

Requirement	AWS Service / Solution	Justification
Database (MySQL format)	RDS	To create relational databases as the storage (AWS RDS, 2023)
Network	VPC	To host all public subnets, private subnets and all associated instances (AWS VPC, 2023)
Activities Monitoring	Cloud Trail	To monitor activities performed by different users and store activities as logs (AWS CloudTrail, 2023)
Traffic Distribution	Elastic Load Balancer	To distribute traffics going into website into EC2 in different AZs (AWS ELB, 2023)
Server Capacities Adjustment	Auto-Scaling	To perform scaling-in or scaling-out of EC2 instances of web and application server according to traffic demand (AWS Auto-Scaling, 2023)
Compute	EC2	To cater computing resources to the web and application server (AWS EC2, 2023)
Software Development	Cloud9	To provide development environment which can be run and deployed on EC2 (AWS Cloud9, 2023)
Users Creation	IAM	To create roles, groups, users. Users can be assigned into groups (AWS IAM, 2023)

### Architecture Diagram

Architecture Diagram is provided in Appendix
--

### Network

VPC	Region	Purpose	No of Subnets	No of AZs	CIDR Range
myVPC	us-east-1 (N.Virginia)	To host all public subnets, private subnets and all associated instances (AWS VPC, 2023)	4 (with 2 subnets per AZ)	2	10.0.0.0/16

- NAT gateway is utilised to connect private subnet to internet
- Two AZs are created hence the website is highly available. Therefore, when 1 AZ is failed, there is a backup on the other AZ.

---

### Production Subnet Details

Subnet Name	VPC	Subnet Type (Public/Private)	AZ	Subnet Address
Public Subnet 1	1	Public	us-east-1a	10.0.0.0/24
Private Subnet 1	1	Private	us-east-1a	10.0.2.0/24
Public Subnet 2	1	Public	us-east-1b	10.0.1.0/24
Private Subnet 2	1	Private	us-east-1b	10.0.3.0/24

### Instance Details

Tier	Tag	OS	Type	Size	Justification	# of instances
web-app	key: <b>Name</b> value: <b>ShopAPP</b>	Amazon Linux	EC2	t2.micro (1vCPU, 1GiB RAM)	to cater computing and storage for web and app tier (AWS EC2, 2023)	Two for web-app (one instance per AZ)  One instance for bastion host in the first AZ
database	key: <b>Name</b> value: <b>DBTier</b>	N/A	RDS	200GiB	to cater relational database storage for the website (AWS RDS, 2023)	two (one instance per AZ)

The RDS created in the private subnet 2 acts as the secondary (backup) of the RDS created in Private Subnet 1

### Application Load Balancer:

Tier	Type	Group Name	Tag	VPC	Subnets	Security Group
web-app	Application Load Balancer	web-app-lb	key: <b>name</b> value: <b>web-app-elb</b>	myVPC	Public Subnet 1 & Public Subnet 2	web-app-lb-sg

---

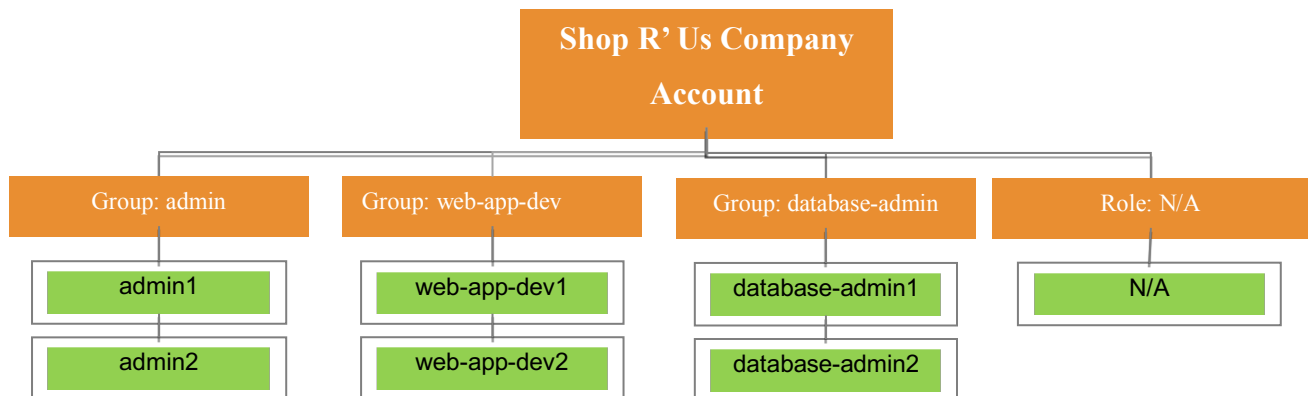
### Auto Scaling Group

Tier	Launch Config	Group Name	Group Size (min,max)	VPC	Subnets	ELB
web-app	after the website code is deployed on Cloud9, the EC2 created by Cloud9 is used to create AMI and afterwards used as Launch Config	web-app-asg	Desired capacity: 2 Min capacity: 1 Max capacity: 2	myVPC	Public Subnet 1 and Public Subnet 2	web-app-elb

The EC2 will scale out from 1 instance to 2 instances when the traffic is high.

---

### 3. Security Design



#### User Authentication

Group/Role	Group/Role name	Permissions
Group	admin	Admin is able to create, stop, start all instances. Admin is able to create new roles, user groups and users using IAM.
Group	web-app-dev	Web-app-dev user group is able to start, stop and view ELB, Auto-Scaling, EC2, Bastion Hosts. This group may only read RDS.
Group	database-admin	Database-admin is able to start, stop and view RDS instance. This group has only read access to ELB, Auto-Scaling, EC2, Bastion Hosts.

In addition, the following configurations will apply to all users:

- Passwords for all users by default follows the policy below, which have been applied when the users are created.

<p>This AWS account uses the following default password policy:</p> <p>Password minimum length</p> <p>8 characters</p> <p>Password strength</p> <p>Include a minimum of three of the following mix of character types:</p> <ul style="list-style-type: none"><li>• Uppercase</li><li>• Lowercase</li><li>• Numbers</li><li>• Non-alphanumeric characters (!@#\$%^&amp;*()_+-=[]{} ')</li></ul>
--

(AWS Default, 2023)

- Passwords must be changed every 3 months and users are unable to use their previous 3 passwords. For each user, go to IAM and clicked on 'account setting' and choose 'edit password policy' :

Other requirements

☒ Turn on password expiration

Expire password in  day(s)

Needs to be between 1 and 1095 days.

☐ Password expiration requires administrator reset

☐ Allow users to change their own password

☒ Prevent password reuse

Remember  password(s)

Needs to be between 1 and 24.

(AWS Password, 2023)

- All the user groups mentioned above will have programmatic access, and this feature is enabled when each user is created as shown below:

Add user 1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type\* ☒ Access key - Programmatic access

Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

☐ Password - AWS Management Console access

Enables a password that allows users to sign-in to the AWS Management Console.

(AWS Programmatic, 2023)

- Multi-Factor Authentication will be used for all users where they are required an authentication code on their registered MFA device. This can be achieved by clicking on the created users and click on the 'Security Credential' tab, which is able to assign the MFA device, as shown below:

Permissions Groups Tags (1) **Security credentials** Access Advisor

Sign-in credentials

Summary • Console sign-in link: <https://790043767874.signin.aws.amazon.com/console>

Console password Enabled (never signed in) | [Manage](#)

Signing certificates None

Multi-factor authentication (MFA)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. You can assign a maximum of 8 MFA devices. [Learn more](#)

[Manage](#) [Assign MFA device](#)

(AWS MFA, 2023)

---

## Security Groups

Security Group (SG)	SG Name	Rule	Source
Bastion Security Group	bastion-sg	<b>Inbound Rule:</b> Type: SSH Protocol: TCP Port Range: 22  <b>Outbound Rule:</b> Type: All Traffic Protocol: All Port Range: All	<b>Inbound Rule:</b> Source: 0.0.0.0/0  <b>Outbound Rule:</b> Source: 0.0.0.0/0
Load Balancer Security Group	web-app-lb-sg	<b>Inbound Rule:</b> Type: HTTP Protocol: TCP Port Range: 80  <b>Inbound Rule:</b> Type: HTTPS Protocol: TCP Port Range: 443  <b>Outbound Rule:</b> Type: All Traffic Protocol: All Port Range: All	<b>Inbound Rule:</b> Source: 0.0.0.0/0  <b>Inbound Rule:</b> Source: 0.0.0.0/0  <b>Outbound Rule:</b> Source: 0.0.0.0/0
Web Application Security Group	web-app-server-sg	<b>Inbound Rule:</b> Type: SSH Protocol: TCP Port Range: 22  <b>Inbound Rule:</b> Type: HTTP Protocol: TCP Port Range: 80  <b>Outbound Rule:</b> Type: All Traffic Protocol: All Port Range: All	<b>Inbound Rule:</b> Source: bastion-sg (security group of bastion host)  <b>Inbound Rule:</b> Source: web-app-lb-sg (security group of load balancer)  <b>Outbound Rule:</b> Type: All Traffic Source: 0.0.0.0/0
Database Security Group	database-sg	<b>Inbound Rule:</b> Type: all TCP Protocol: TCP Port Range: 0-65535 <i>(by selecting all TCP is to allow connection of RDS to MySQL bench)</i>	<b>Inbound Rule:</b> Source: 0.0.0.0/0



---

		<b>Inbound Rule (alternative):</b> Type: MySQL/Aurora Protocol: TCP Port Range: 3306 <i>(This is the alternative more secure inbound rule to allow access from web-app tier only. However, by choosing this configuration, RDS is unable to connect to MySQL bench)</i>	<b>Inbound Rule (alternative):</b> Source: web-app-server-sg (security group Web-App-Tier)
		<b>Outbound Rule:</b> Type: All Traffic Protocol: All Port Range: All	<b>Outbound Rule:</b> Type: All Traffic Source: 0.0.0.0/0

#### Other Security Options

Other Security Options	Justifications
KMS Key	Encryption SDK key will be used to encrypt traffics flowing across AWS (AWS KMS, 2023)
SSL/TLS	An encrypted connection of network will be established in web browser when this feature is used (AWS SSL, 2023)

---

## Cost Considerations

In estimating the costs, Singapore is chosen as the region assuming that Shop R' Us headquarter is in Singapore.

The following assumptions are made when calculating the costs:

### VPC

- 4 subnets associations
- 22 working days per month
- 1 NAT Gateway
- Data processed per NAT Gateway: 20 GB per month
- Data transferred from internet: 20 GB (it is free)
- Outbound transfer: 20 GB

### Cloud Trail

Maximum 1000 write management of events per day, hence 30000 per month

### ELB

500 new connection per second, where maximum of 500 customers visit the website per second

### 3 EC2 instances (2 EC2 for web-app-tier and 1 EC2 for bastion host)

- Shared instances
- Linux operating system
- Workloads: constant usage
- t2.micro family
- EC2 Saving Instance Plans, reserve term 3 years and pay all upfront

### RDS for MySQL (2 instances)

- db.m1.small (1 vCPU and 1.7 GiB memory)
- General Purpose SSD (gp2)
- 200 GB storage

Summary of Price is as follow:

The screenshot displays the AWS Pricing Calculator interface. At the top, the 'Estimate summary' section shows the following costs:

Cost Type	Amount
Upfront cost	386.32 USD
Monthly cost	1,052.25 USD
<b>Total 12 months cost</b>	<b>13,013.32 USD</b>

The total cost includes the upfront cost. To the right, the 'Getting Started with AWS' section offers buttons for 'Get started for free' and 'Request a quote'.

The 'My Estimate' section features a search bar and a table of services:

Service Name	Upfront cost	Monthly cost	Description	Region	Config Summary
<input type="checkbox"/> AWS CloudTrail	0.00 USD	0.00 USD	sukarno-cloudtrail	Asia Pacific (Singapore)	Management ev...
<input type="checkbox"/> Elastic Load Balancing	0.00 USD	135.20 USD	sukarno-Elastic Load Balancing	Asia Pacific (Singapore)	Number of Appli...
<input type="checkbox"/> Amazon Virtual Private Cloud (VPC)	0.00 USD	759.65 USD	sukarno-VPC	Asia Pacific (Singapore)	Working days pe...
<input type="checkbox"/> Amazon EC2	386.32 USD	0.00 USD	sukarno-EC2	Asia Pacific (Singapore)	Tenancy (Shared...
<input type="checkbox"/> Amazon RDS for MySQL	0.00 USD	157.40 USD	sukarno-RDS	Asia Pacific (Singapore)	Storage for each...

At the bottom, an 'Acknowledgement' section states: 'AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. [Learn more](#)'.

The footer contains links for 'Privacy', 'Site terms', and 'Cookie preferences', along with the copyright notice: '© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.'

(AWS Pricing, 2023)

Shop R' Us can expect to pay USD 1052.25/month or USD 13,013.32/year.

---

## 4. Design Limitations

The login details of RDS is directly provided inside codes of the website. This is not the best practice since when the security of the website is compromised, the login details can be leaked easily. The login details include:

- Endpoint
- Username
- Password
- Database name

This can be improved by storing these parameters in AWS System Manager Parameter Store. Hence the website will retrieve these login details every time the website is loaded.

## 5. Implementation

### Step 1: Create a new VPC

A new VPC with the name “myVPC” is created, as follow:

The screenshot displays the AWS Management Console for a VPC named 'myVPC' (ID: vpc-074fa951464d9c6d6). The console shows various details and resource maps.

**Details:**

- VPC ID: vpc-074fa951464d9c6d6
- State: Available
- DNS hostnames: Enabled
- DNS resolution: Enabled
- Tenancy: Default
- DHCP option set: dopt-04e10dda15729a4b6
- Main route table: rtb-0dd723024613cc507
- Main network ACL: acl-09e7db8c44b84ba3d7
- Default VPC: No
- IPv4 CIDR: 10.0.0.0/16
- IPv6 pool: -
- Owner ID: 966576247265
- Network Address Usage metrics: Disabled
- Route 53 Resolver DNS Firewall rule groups: -

**Resource map:**

- VPC: myVPC-vpc
- Subnets (4): us-east-1a (myVPC-subnet-public1-us-east-1a, myVPC-subnet-private1-us-east-1a), us-east-1b (myVPC-subnet-public2-us-east-1b, myVPC-subnet-private2-us-east-1b)
- Route tables (4): myVPC-rtb-public, rtb-0dd723024613cc507, myVPC-rtb-private1-us-east-1a, myVPC-rtb-private2-us-east-1b
- Network connections (2): myVPC-igw, myVPC-vpc-s3

**CIDRs:**

Address type	CIDR	Network Border Group	Pool	Status
IPv4	10.0.0.0/16	-	-	Associated

The details of production subnets have been provided in Section 2.

Route Tables for Public Subnet, with internet gateway connected is shown below:

The screenshot displays the AWS Management Console for a Route Table named 'myVPC-rtb-public' (ID: rtb-0f437bbba7ed80e49). The console shows details and routes.

**Details:**

- Route table ID: rtb-0f437bbba7ed80e49
- Main: No
- Explicit subnet associations: 2 subnets
- Edge associations: -
- VPC: vpc-074fa951464d9c6d6 | myVPC-vpc
- Owner ID: 966576247265

**Routes (2):**

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f10b5940e9b36c87	Active	No
10.0.0.0/16	local	Active	No

Routes	Subnet associations	Edge associations	Route propagation	Tags
Explicit subnet associations (2)				
<input type="text" value="Find subnet association"/>				
Subnet ID	IPv4 CIDR			
subnet-0b03ee8c62ceec7cb / myVPC-subnet-public2-us-east-1b	10.0.1.0/24			
subnet-0130c846f2d7c5069 / myVPC-subnet-public1-us-east-1a	10.0.0.0/24			

Route table for Private Subnet 1 (where vpce is the VPC endpoint which is created as the alternative connection to private subnet without requiring internet gateway and NAT (AWS Endpoint, 2023)), is shown below:

VPC
>
Route tables
>
rtb-01c4c89319ddb1900

rtb-01c4c89319ddb1900 / myVPC-rtb-private1-us-east-1a

Actions

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Details

Info

Route table ID

rtb-01c4c89319ddb1900

Main

No

Explicit subnet associations

subnet-00290af27db13ac3 / myVPC-subnet-private1-us-east-1a

Edge associations

-

VPC

vpc-074fa951464d9c6d6 | myVPC-vpc

Owner ID

966576247265

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Both

Edit routes

Destination

Target

Status

Propagated

pl-63a5400a

vpce-00764d778364c17f2

Active

No

10.0.0.0/16

local

Active

No

Routes	Subnet associations	Edge associations	Route propagation	Tags
Explicit subnet associations (1)				
<input type="text" value="Find subnet association"/>				
Subnet ID	IPv4 CIDR			
subnet-00290af27db13ac3 / myVPC-subnet-private1-us-east-1a	10.0.2.0/24			

Route table for Private Subnet 2 is shown below:

VPC
>
Route tables
>
rtb-05d5c8b2a3c07cb24

rtb-05d5c8b2a3c07cb24 / myVPC-rtb-private2-us-east-1b

Actions

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Details

Info

Route table ID

rtb-05d5c8b2a3c07cb24

Main

No

Explicit subnet associations

subnet-0eda1a4ee69ced36 / myVPC-subnet-private2-us-east-1b

Edge associations

-

VPC

vpc-074fa951464d9c6d6 | myVPC-vpc

Owner ID

966576247265

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Filter routes

Both

Edit routes

Destination

Target

Status

Propagated

pl-63a5400a

vpce-00764d778364c17f2

Active

No

10.0.0.0/16

local

Active

No

Routes	Subnet associations	Edge associations	Route propagation	Tags
Explicit subnet associations (1)				
Find subnet association				
Subnet ID		IPv4 CIDR		
subnet-0eda1a4eef69ced36 / myVPC-subnet-private2-us-east-1b		10.0.3.0/24		

## Endpoint

→

↺

↻

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#EndpointDetailsvpcEndpointId=vpce-00764d778364c17f2

aws

Services

Search

[Alt+S]

📄

🔔

👤

N. Virginia

sukamo

VPC dashboard

✕

EC2 Global View

🔗

New

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

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

VPC > Endpoints > vpce-00764d778364c17f2

vpce-00764d778364c17f2 / myVPC-vpce-s3

Actions

Details

Endpoint ID

🔗 vpce-00764d778364c17f2

VPC ID

vpc-074fa951464d9c6d6 (myVPC-vpc)

Status

🟢 Available

Status message

-

Creation time

Wednesday, February 15, 2023 at 13:37:48 GMT+8

Service name

com.amazonaws.us-east-1.s3

Endpoint type

Gateway

Private DNS names enabled

No

Route tables

Policy

Tags

Route tables (2)

🔄

Manage route tables

Filter route tables

Name

▼

Route Table ID

▼

Main

▼

Associated Id

▼

myVPC-rtb-private1-us-east-1a

rtb-01c4c89319ddb1900 (myVPC-rtb-private1-us-east-1a)

No

subnet-00290a0f27db13ac3 (myVPC-subne...

myVPC-rtb-private2-us-east-1b

rtb-05d5c8b2a3c07cb24 (myVPC-rtb-private2-us-east-1b)

No

subnet-0eda1a4eef69ced36 (myVPC-subnet...

## Step 2: Developing Shop R' Us website using Cloud9

A simple website was cloned from github, which is developed by Nguyen (2018). The code was imported using Cloud9 and afterwards modified to suit the needs of Shop R' Us. The configuration of the Cloud9 environment is as follow:

←

→

us-east-1.console.aws.amazon.com/cloud9control/home?region=us-east-1#/environments/81653b9263df4952b20e2565b919b67e

AWS

Services

Search

[Alt+S]

N. Virginia

sukarno

AWS Cloud9

×

Environments

Documentation

AWS Cloud9

>

Environments

>

web-app-server3

web-app-server3

Delete

Open in Cloud9

Details

Edit

<div>Name</div> <div>web-app-server3</div>	<div>Owner ARN</div> <div>arn:aws:iam::966576247265:root</div>	<div>Status</div> <div>Ready</div>
<div>Description</div> <div>all php in one file</div>	<div>Number of members</div> <div>1</div>	<div>Lifecycle status</div> <div>Created</div>

EC2 instance

Network settings

Tags

EC2 instance

Manage EC2 instance

<div>ARN</div> <div>arn:aws:cloud9:us-east-1:966576247265:environment:81653b9263df4952b20e2565b919b67e</div>	<div>Instance type</div> <div>t2.micro (1 GiB RAM + 1 vCPU)</div>
<div>Platform</div> <div>Amazon Linux 2</div>	<div>Storage</div> <div>EBS only</div>

EC2 Instance   Network settings   Tags		
Connection and VPC		
Connection Secure Shell (SSH)	Amazon Virtual Private Cloud (VPC) vpc-074fa951464d9c6d6	Subnet subnet-0130c846f2d7c5069

The snapshot of the Cloud9 is shown below, while the snapshot of the entire code is provided in Appendix.

```

1 <?php
2 define('DB_SERVER', 'examplesq14.cwjk27xtjj.us-east-1.rds.amazonaws.com');
3 define('DB_USERNAME', 'postgres');
4 define('DB_PASSWORD', 'Post14567');
5 define('DB_DATABASE', 'examplesq14');
6
7 >>
8
9
10 <html><body>
11 <h1>Shop R' Us</h1>
12
13 </php>
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607

```



DetailsSecurityNetworkingStorageStatus checksMonitoringTags

▼ Instance details Info

Platform Linux/UNIX (Inferred)	AMI ID ami-07303e0c3f090f7bf	Monitoring disabled
Platform details Linux/UNIX	AMI name Cloud9AmazonLinux2-2023-02-09T12-11	Termination protection Disabled
Stop protection Disabled	Launch time Sat Feb 18 2023 09:56:01 GMT+0800 (Singapore Standard Time) (38 minutes)	AMI location amazon/Cloud9AmazonLinux2-2023-02-09T12-11
Instance auto-recovery Default	Lifecycle normal	Stop-hibernate behavior disabled
AMI Launch index 0	Key pair name -	State transition reason -
Credit specification standard	Kernel ID -	State transition message -
Usage operation RunInstances	RAM disk ID -	Owner 966576247265
ClassicLink -	Enclaves Support -	Boot mode -
Allow tags in instance metadata Disabled	Use RBN as guest OS hostname Disabled	Answer RBN DNS hostname IPv4 Disabled

▼ Host and placement group Info

Host ID -	Affinity -	Placement group -
Host resource group name -	Tenancy default	Placement group ID -
Virtualization type hvm	Reservation r-042e5ac92ceccca1a	Partition number -
Number of vCPUs 1		

▼ Capacity reservation Info

Capacity Reservation ID -	Capacity Reservation setting open	
------------------------------	--------------------------------------	--

▼ Accelerators Info

Elastic Graphics ID -	Elastic inference accelerator ID -	
--------------------------	---------------------------------------	--

DetailsSecurityNetworkingStorageStatus checksMonitoringTags

You can now check network connectivity with Reachability Analyzer.

Run Reachability Analyzer

▼ Networking details Info

Public IPv4 address 3.219.167.15   open address	Private IPv4 addresses 10.0.0.158	VPC ID vpc-074fa951464d9c6d6 (myVPC-vpc)
Public IPv4 DNS ec2-3-219-167-15.compute-1.amazonaws.com   open address	Private IP DNS name (IPv4 only) ip-10-0-0-158.ec2.internal	
Subnet ID subnet-0130c846f2d7c5069 (myVPC-subnet-public1-us-east-1a)	IPv6 addresses -	Secondary private IPv4 addresses -
Availability zone us-east-1a	Carrier IP addresses (ephemeral) -	Outpost ID -
Use RBN as guest OS hostname Disabled	Answer RBN DNS hostname IPv4 Disabled	

▼ Network Interfaces (1) Info

Filter network interfaces

Interface ID	Description	IPv4 Prefixes	IPv6 Prefixes	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6 addresses	Attachment time	Interface
eni-0806391182937d...	ENI for AWS Cloud9 e...	-	-	3.219.167.15	10.0.0.158	ip-10-0-0-158.ec2.internal	-	Wed Feb 15 2023 19:0...	96657624...

DetailsSecurityNetworkingStorageStatus checksMonitoringTags

▼ Root device details

Root device name /dev/xvda	Root device type EBS	EBS optimization disabled
-------------------------------	-------------------------	------------------------------

▼ Block devices

Filter block devices

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termination
vol-03597022aba00876a	/dev/xvda	10	Attached	Wed Feb 15 2023 19:00:46 G...	No	-	Yes

Security details have been provided in section 3 Security Design.

### Step 3: Create an Image using the EC2 spin off from Cloud9

In order to allow Auto-Scaling Group to scale-out identical EC2 when there is an increase in traffic, an AMI is created using the EC2 spin off from Cloud9 earlier, with the following configuration:

The screenshot displays the 'Image summary' page for the AMI 'ami-06c3fcccc79a3757'. The left sidebar shows the navigation menu with categories like Limits, Instances, Images, Elastic Block Store, and Network & Security. The main content area is titled 'Image summary for ami-06c3fcccc79a3757' and includes buttons for 'EC2 Image Builder', 'Actions', and 'Launch instance from AMI'. The summary is organized into a grid of key-value pairs:

Key	Value
AMI ID	ami-06c3fcccc79a3757
Image type	machine
Platform details	Linux/UNIX
Root device type	EBS
AMI name	web-app-ami
Owner account ID	966576247265
Architecture	x86_64
Usage operation	RunInstances
Root device name	/dev/xvda
Status	Available
Source	966576247265/web-app-ami
Virtualization type	hvm
Boot mode	-
State reason	-
Creation date	Wed Feb 15 2023 19:10:48 GMT+0800 (Singapore Standard Time)
Kernel ID	-
Block devices	/dev/xvda=snap-020658e697a8dfce2:10:true:gp2
Description	-
Product codes	-
RAM disk ID	-
Deprecation time	-
Last launched time	Sat Feb 18 2023 07:57:09 GMT+0800 (Singapore Standard Time)

Below the summary, there are tabs for 'Permissions', 'Storage', and 'Tags'. The 'Permissions' tab is currently selected, showing 'Image share permission' set to 'Private'.

The screenshot shows the 'Storage' tab for the AMI. It includes a section for 'Root device details' and a table for 'Block devices'. The 'Root device details' section shows the root device name as '/dev/xvda' and the root device type as 'EBS'. The 'Block devices' section contains a table with the following data:

Device ID	Device name	Volume size (GiB)	Volume type	Encrypted	Delete on termination	KMS key ID	Outpost ID
snap-020658e697a8dfce2	/dev/xvda	10	gp2	No	Yes	-	-

### Step 4: Create Launch Configuration using AMI created earlier

A launch configuration is created using the AMI created earlier with the following configuration:

The screenshot displays the 'Launch configurations' page in the AWS Management Console. At the top, there is a blue banner with a recommendation to migrate from launch configurations to launch templates. Below this, a table lists the launch configurations. The configuration 'web-app-lc3' is selected, and its details are shown in a sidebar.

Name	AMI ID	Instance type	Spot price	Creation time
web-app-lc3	ami-06c3fcccc79a3757	t2.micro	-	Wed Feb 15 2023 19:11:56 GMT+0800 (Singapore Standard Time)

The details for the 'web-app-lc3' launch configuration are as follows:

Key	Value
AMI ID	ami-06c3fcccc79a3757
Instance type	t2.micro
IAM instance profile	-
Kernel ID	-
Key name	key3
Monitoring	false
EBS optimized	false
Security groups	sg-0664f6df84f6e97a3
Spot price	-
Create time	Wed Feb 15 2023 19:11:56 GMT+0800 (Singapore Standard Time)
RAM disk ID	-
IP address type	Public
Metadata accessible	-
Token hop limit	-
Metadata version	-

### Step 5: Create Auto-Scaling Group

**AWS** Services Search [Alt+S]

Instance types  
Launch Templates  
Spot Requests  
Savings Plans  
Reserved Instances  
Dedicated Hosts  
Scheduled Instances  
Capacity Reservations

EC2 > Auto Scaling groups > web-app-asg

## web-app-asg

Details | Activity | Automatic scaling | Instance management | Monitoring | Instance refresh

### Group details

Auto Scaling group name <b>web-app-asg</b>	Desired capacity <b>2</b>	Status -	Amazon Resource Name (ARN) <b>arn:aws:autoscaling:us-east-1:966576247265:autoScalingGroup:d5664047-27ca-4a45-8853-8866945d172c:autoScalingGroupName/web-app-asg</b>
Date created <b>Wed Feb 15 2023 19:12:37 GMT+0800 (Singapore Standard Time)</b>	Minimum capacity <b>1</b>		
	Maximum capacity <b>2</b>		

### Launch configuration

Launch configuration <b>web-app-lc3</b>	AMI ID <b>ami-06c3fcccc79a3757</b>	Instance type <b>t2.micro</b>	Create time <b>Wed Feb 15 2023 19:11:56 GMT+0800 (Singapore Standard Time)</b>
Storage (volumes) <b>/dev/xvda</b>	Security groups <b>sg-0664fcdf84f6e97a3</b>	Key pair name <b>key3</b>	

[View details in the launch configuration console](#)

The minimum capacity is set to 1 and the maximum capacity is set to 2. Therefore, the number of EC2 will increase from 1 to 2 when there is an increase in website traffic. EC2 and ELB health check are performed every 300 seconds.

## Step 6: Create Target Group

After the EC2 is spin-off using Auto-Scaling Group, they are registered inside the target group with the configuration below:

The screenshot shows the AWS Management Console for the 'web-app-target-group'. The 'Details' tab is selected, showing the following information:

- Target type:** Instance
- Protocol - Port:** HTTP: 80
- Protocol version:** HTTP1
- VPC:** vpc-074fa95146489c6d6
- IP address type:** IPv4
- Load balancer:** web-app-elb

Below the details, a summary shows:

- Total targets:** 2
- Healthy:** 0
- Unhealthy:** 0
- Unused:** 0
- Initial:** 2
- Draining:** 0

The 'Targets' tab is also visible, showing a table of registered targets:

Instance ID	Name	Port	Zone	Health status	Health status details
i-035d6b736835625		80	us-east-1b	Initial	Target registration is in progress
i-04112a0324a505964		80	us-east-1a	Initial	Target registration is in progress

## Step 7: Create Elastic Load Balancer

Now configure the ELB using the target group created earlier:

The screenshot shows the AWS Management Console for the 'web-app-elb'. The 'Details' tab is selected, showing the following information:

- Load balancer type:** Application
- DNS name:** web-app-elb-107820152.us-east-1.elb.amazonaws.com
- Status:** Active
- VPC:** vpc-074fa95146489c6d6
- IP address type:** IPv4
- Scheme:** Internet-facing
- Availability Zones:** subnet-0b03ee8b632ee7cb (us-east-1b), subnet-0130c846f2c7c5069 (us-east-1a)
- Hosted zone:** Z55XDDOTRQ7K7K
- Date created:** February 15, 2023, 19:22 (UTC+08:00)

The 'Listeners' tab is also visible, showing a table of listeners:

Protocol/Port	ARN	Security policy	Default SSL cert	Default routing rule	Rules	Tags
HTTP:80	ARN	Not applicable	Not applicable	1. Forward to web-app-target-group (100%)	1	0

The ELB is configured to distribute traffic to both public subnets:

Listeners

Network mapping

Security

Monitoring

Integrations

Attributes

Tags

Network mapping

Info

Targets in the listed zones and subnets are available for traffic from the load balancer using the IP addresses shown.

VPC

vpc-074fa951464d9c6d6

IPv4: 10.0.0.0/16

IPv6: -

IP address type

IPv4

Mappings

Selecting two or more Availability Zones and corresponding subnets increases the fault tolerance of your applications.

Zone	Subnet	IPv4 address	Private IPv4 address	IPv6 address
us-east-1b (use1-az2)	subnet-0b03ee8c62ceec7cb	Assigned by AWS	Assigned from CIDR 10.0.1.0/24	Not applicable
us-east-1a (use1-az1)	subnet-0130c846f2d7c5069	Assigned by AWS	Assigned from CIDR 10.0.0.0/24	Not applicable

## Step 8: Create RDS instance

The configuration is as follow:

Amazon RDS

RDS > Databases > examplesql4

examplesql4

Modify

Actions

Summary

DB identifier examplesql4

CPU 2.29%

Status Available

Class db.t3.micro

Role Instance

Current activity 2 Connections

Engine MySQL Community

Region & AZ us-east-1b

Connectivity & security

Monitoring

Logs & events

Configuration

Maintenance & backups

Tags

Connectivity & security

Endpoint & port

Endpoint examplesql4.cnjw427t1tj.us-east-1.rds.amazonaws.com

Port 3306

Networking

Availability Zone us-east-1b

VPC myVPC-vpc (vpc-074fa951464d9c6d6)

Subnet group default-vpc-074fa951464d9c6d6

Subnets subnet-0130c846f2d7c5069 subnet-0b03ee8c62ceec7cb subnet-00290a0f27db13ac3 subnet-0eda1a4ee69ced56

Network type IPv4

Security

VPC security groups db-test (sg-02f860d6f6397f6a)

Publicly accessible Yes

Certificate authority rds-ca-2019

Certificate authority date August 23, 2024, 01:08 (UTC+08:00)

DB instance certificate expiration date August 23, 2024, 01:08 (UTC+08:00)

Connectivity & securityMonitoringLogs & eventsConfigurationMaintenance & backupsTags

Instance

Configuration

DB instance ID  
examplesql4

Engine version  
8.0.28

DB name  
examplesql4

License model  
General Public License

Option groups  
default:mysql-8-0 In sync

Amazon Resource Name (ARN)  
arn:aws:rds:us-east-1:966576247265:db:examplesql4

Resource ID  
db-yk1z2c4vg5j0wqtc424u1lgyou

Created time  
February 16, 2023, 13:53 (UTC+08:00)

DB instance parameter group  
default:mysql8.0 In sync

Deletion protection  
Disabled

Instance class

Instance class  
db.t3.micro

vCPU  
2

RAM  
1 GB

Availability

Master username  
postgres

Master password  
\*\*\*\*\*

IAM DB authentication  
Not enabled

Multi-AZ  
No

Secondary Zone  
-

Storage

Encryption  
Enabled

AWS KMS key  
[aws/rds](#)

Storage type  
General Purpose SSD (gp2)

Storage  
20 GiB

Provisioned IOPS  
-

Storage throughput  
-

Storage autoscaling  
Disabled

Performance Insights

Performance Insights enabled  
Turned off

Db.t3.micro is selected because AWS Free Tier is used to create this project. In reality the instance class is db.m1.small.  
The security details are provided in Section 4.

Step 9: Test run the website using ELB Public DNS Address

← → ↻ ⚠ Not secure | web-app-elb-107820152.us-east-1.elb.amazonaws.com/index.php

Shop R' Us

ITEM

QUANTITY

Add Data

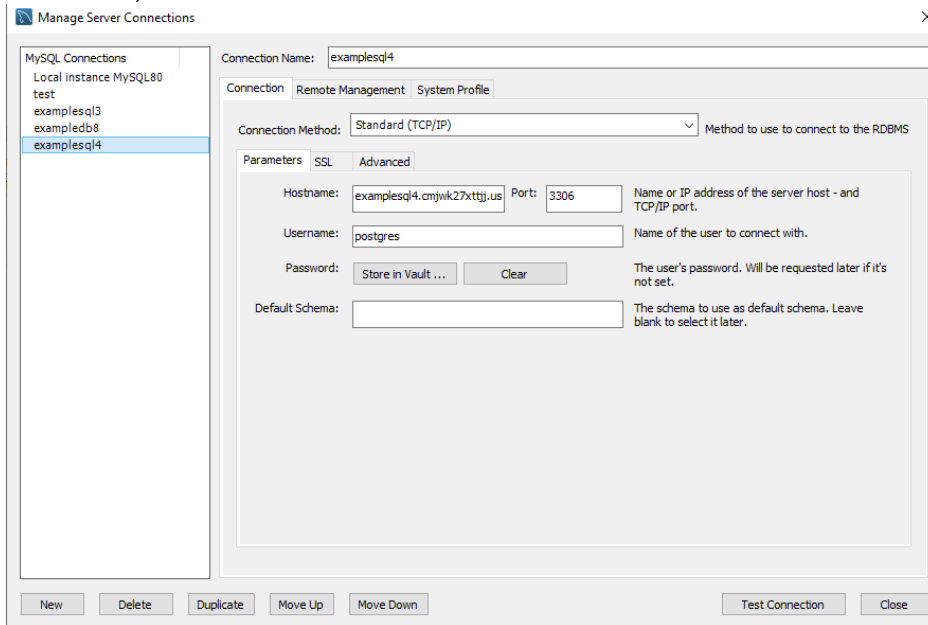
ID	ITEM	QUANTITY
1	Volley Ball	1
2	Pyjamas	2
3	Baskets	5

(Nguyen, 2018)

As an illustration, the shoppers are able to add items and their quantities they wish to buy.

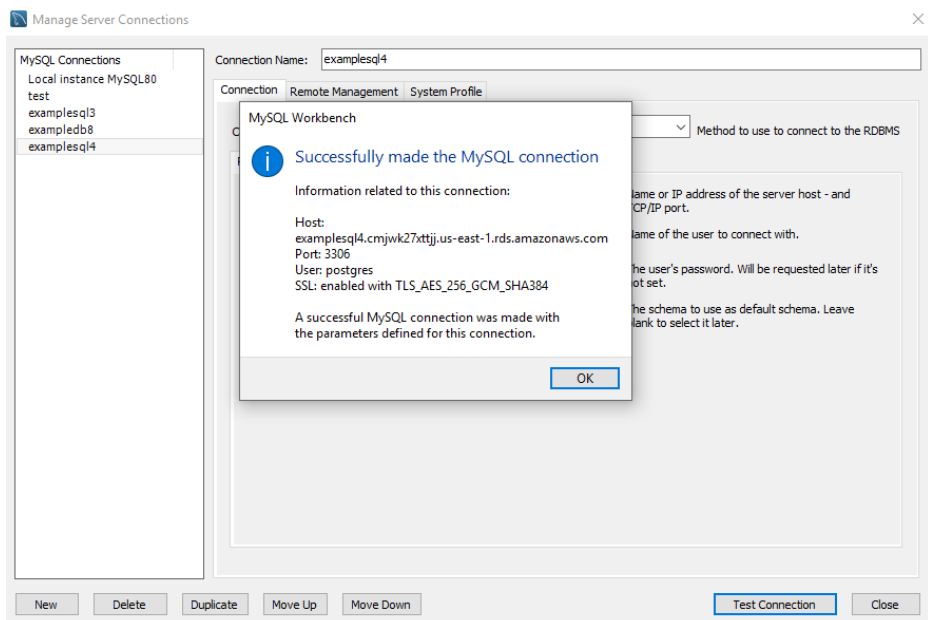
## Step 10: Connect MySQL bench to RDS

MySQL workbench (in local machine) is connected to RDS using RDS endpoint, as shown below. Therefore, clients are able to view the data inside RDS.



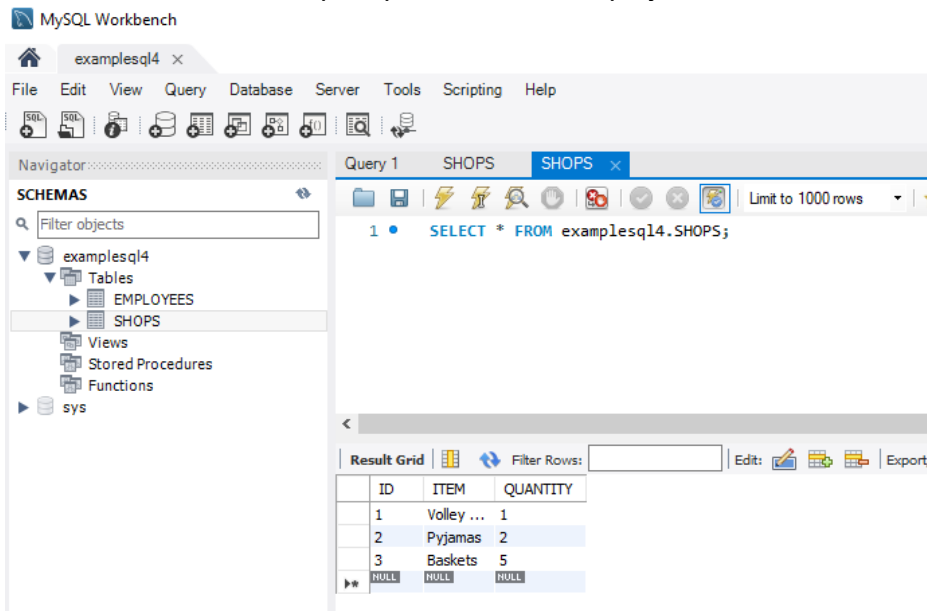
(MySQL, 2023)

## Test the connection



(MySQL, 2023)

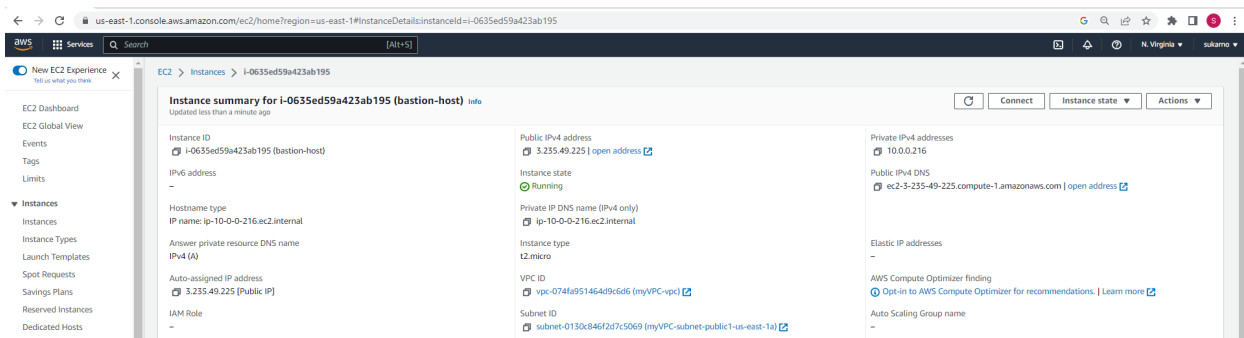
Use 'Select \* from examplesql4.SHOPS' to display all data.



(MySQL, 2023)

### Step 11: Add Bastion Host

Bastion Host is added to allow local terminal to use SSH (secure shell) to access to EC2 and RDS instance, with the configuration as follow:





DetailsSecurityNetworkingStorageStatus checksMonitoringTags

▼ Instance details info

Platform

Amazon Linux (Inferred)

Platform details

Linux/UNIX

Stop protection

Disabled

Instance auto-recovery

Default

AMI Launch index

0

Credit specification

standard

Usage operation

RunInstances

ClassicLink

-

Allow tags in instance metadata

Disabled

AMI ID

ami-0dfcb1ef8550277af

AMI name

amzn2-ami-kernel-5.10-hvm-2.0.20230207.0-x86\_64-gp2

Launch time

Sat Feb 18 2023 12:39:30 GMT+0800 (Singapore Standard Time) (1 minute)

Lifecycle

normal

Key pair name

key3

Kernel ID

-

RAM disk ID

-

Enclaves Support

-

Use RBN as guest OS hostname

Disabled

Monitoring

disabled

Termination protection

Disabled

AMI location

amazon/amzn2-ami-kernel-5.10-hvm-2.0.20230207.0-x86\_64-gp2

Stop-hibernate behavior

disabled

State transition reason

-

State transition message

Client.UserInitiatedShutdown: User initiated shutdown

Owner

966576247265

Boot mode

-

Answer RBN DNS hostname IPv4

Enabled

▼ Host and placement group info

Host ID

-

Host resource group name

-

Virtualization type

hvm

Number of vCPUs

1

Affinity

-

Tenancy

default

Reservation

r-03228104cf41e574

Placement group

-

Placement group ID

-

Partition number

-

▼ Capacity reservation info

Capacity Reservation ID

-

Capacity Reservation setting

open

▼ Accelerators info

Elastic Graphics ID

-

Elastic inference accelerator ID

-

DetailsSecurityNetworkingStorageStatus checksMonitoringTags

🔗 You can now check network connectivity with Reachability Analyzer.

Run Reachability Analyzer

▼ Networking details info

Public IPv4 address

3.235.49.225 | open address

Public IPv4 DNS

ec2-3-235-49-225.compute-1.amazonaws.com | open address

Subnet ID

subnet-0130c846f2d7c5069 (myVPC-subnet-public1-us-east-1a)

Availability zone

us-east-1a

Use RBN as guest OS hostname

Disabled

Private IPv4 addresses

10.0.0.216

Private IP DNS name (IPv4 only)

ip-10-0-0-216.ec2.internal

IPv6 addresses

-

Carrier IP addresses (ephemeral)

-

Answer RBN DNS hostname IPv4

Enabled

VPC ID

vpc-074fa951464d9c6d6 (myVPC-vpc)

Secondary private IPv4 addresses

-

Outpost ID

-

▼ Network Interfaces (1) info

Filter network interfaces

Interface ID	Description	IPv4 Prefixes	IPv6 Prefixes	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6 address	Attachment time	Interface owner	Attachment status
eni-0c6074094fc508...	-	-	-	3.235.49.225	10.0.0.216	ip-10-0-0-216.ec2.int...	-	Thu Feb 16 2023 14:4...	966576247265	attached

## Step 12: Test Bastion Host

- Download the PEM key (key3.pem) from AWS.
- Connect to bastion host using key3.pem and bastion endpoint.

Run chmod 400 beforehand to allow access of pem key.

```
[(base) sukarno.zhanggmail.com@Sukarnos-MacBook-Pro rp % chmod 400 key3.pem  
[(base) sukarno.zhanggmail.com@Sukarnos-MacBook-Pro rp % ssh -i key3.pem ec2-user@ec2-44-192-89-145.compute-1.amazonaws.com
```

```
__|  __|_  )  
_| (  /  
---|\---|  
Amazon Linux 2 AMI
```

```
https://aws.amazon.com/amazon-linux-2/  
~bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory  
[ec2-user@ip-10-0-0-216 ~]$ █
```

- Create a new pem key called "new.pem", the contents are identical to key3.pem.  
Upload new.pem to bastion host using bastion endpoint

```
[(base) sukarno.zhanggmail.com@Sukarnos-MacBook-Pro rp % scp -i key3.pem new.pem ec2-user@ec2-44-192-89-145.compute-1.amazonaws.com:  
/etc/profile.d/lang.sh: line 19: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory  
new.pem 100% 1674 5.1KB/s 00:00  
[(base) sukarno.zhanggmail.com@Sukarnos-MacBook-Pro rp % █
```

- Use new.pem and web-app EC2 endpoint to connect to web-app EC2 from bastion host

```
[ec2-user@ip-10-0-0-216 ~]$ ssh -i new.pem ec2-user@ec2-3-86-97-47.compute-1.amazonaws.com  
The authenticity of host 'ec2-3-86-97-47.compute-1.amazonaws.com (10.0.1.80)' can't be established.  
ECDSA key fingerprint is SHA256:tbDsVct7n6ob/yk4Scjer65nIBI5NNvHLrWkYZDjLdQ.  
ECDSA key fingerprint is MD5:f7:f2:81:07:ac:b4:e1:50:94:b7:30:8b:98:04:5f:14.  
[Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'ec2-3-86-97-47.compute-1.amazonaws.com,10.0.1.80' (ECDSA) to the list of known hosts.
```

```
[  __|  __|_  )  
  _| (  /  
  ---|\---|  
  Amazon Linux 2 AMI  
[  
https://aws.amazon.com/amazon-linux-2/  
No packages needed for security; 1 packages available  
Run "sudo yum update" to apply all updates.  
manpath: can't set the locale; make sure $LC_* and $LANG are correct  
:~ $ █
```

- Inside web-app tier, CD into /var/www/html/ and check if the php file is inside

```
[:~ $ ls  
environment node_modules package-lock.json package.json  
[:~ $ cd /var/www/html  
[:/var/www/html $ ls  
index.php  
:/var/www/html $ █
```

***index.php file developed earlier was found inside /var/www/html/***

- Connect to RDS using RDS endpoint  

```
~ $ mysql -u postgres -p --host examplesql4.cmjwk27xttjj.us-east-1.rds.amazonaws.com
```

Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MySQL connection id is 65  
Server version: 8.0.28 Source distribution  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MySQL [(none)]> █
- Show the databases  

```
MySQL [(none)]> show databases;
```

Database
examplesql4
information_schema
mysql
performance_schema
sys
- Finally, display the contents inside the SHOPS table  

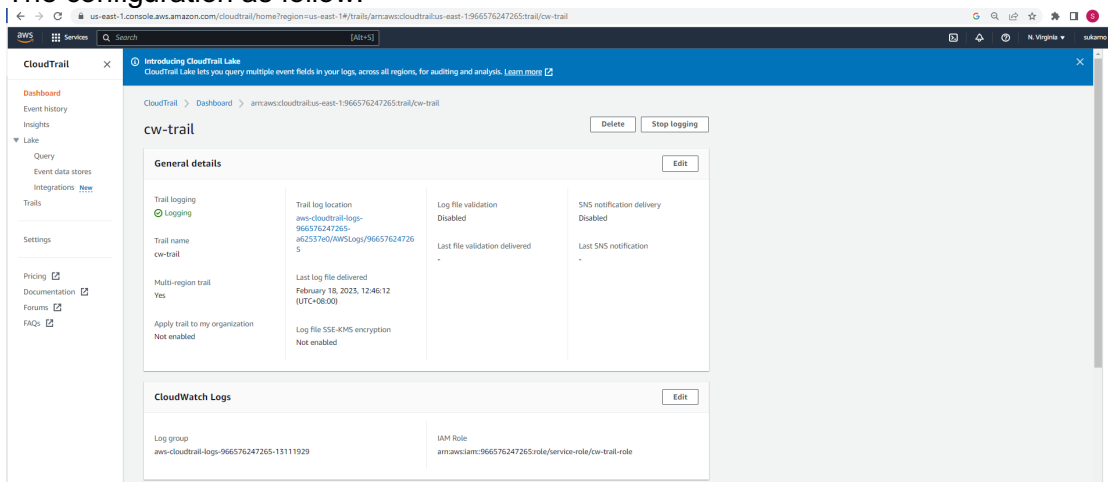
```
MySQL [examplesql4]> select * from SHOPS;
```

ID	ITEM	QUANTITY
1	Monitor	1

1 row in set (0.00 sec)

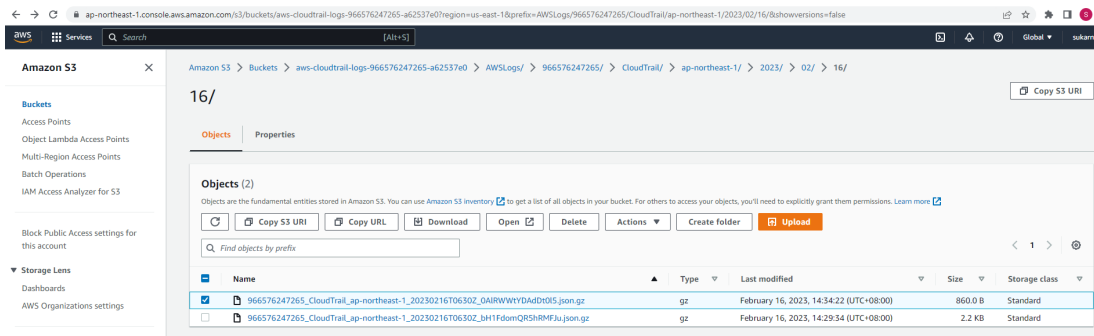
### Step 13: Add Cloud Trail

The configuration as follow:

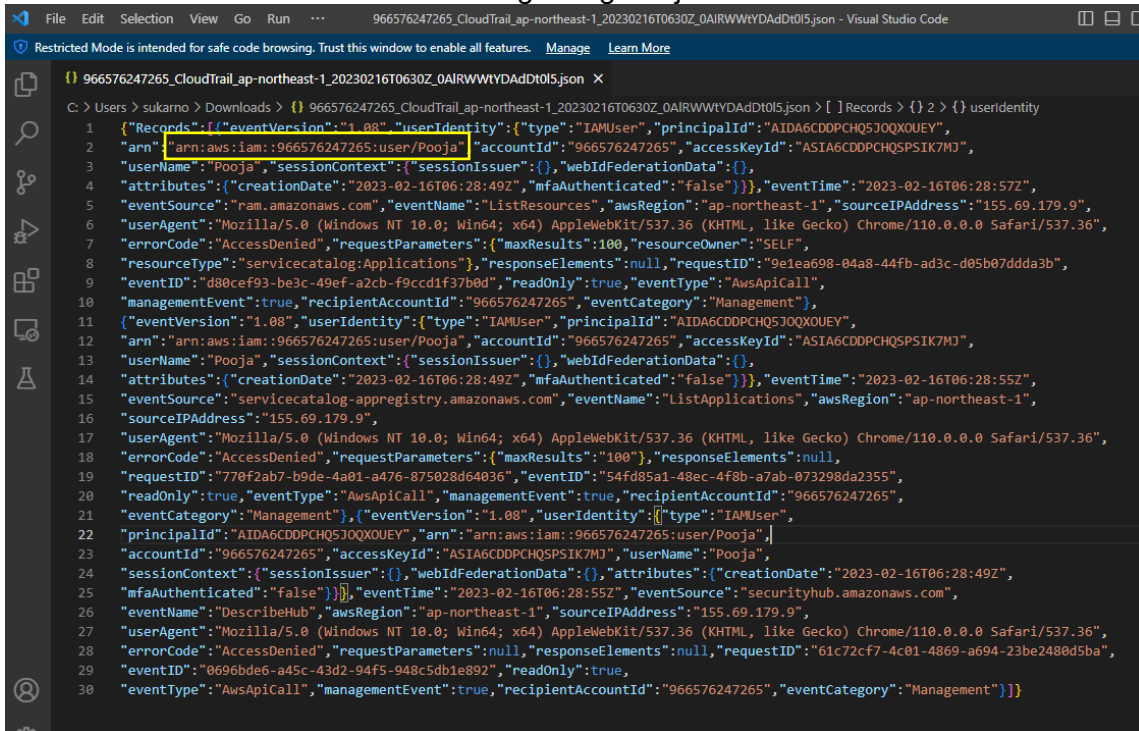


## Step 14: Test Cloud Trail

When the user “Pooja” created in IAM do a login into AWS console, a new logging details are provided in the S3 bucket.



The details of the file is shown below regarding Pooja's activities:



---

## 6. Conclusions

To host website for Shop R' Us, a single VPC was created. Two Availability Zones (AZs) are built in the VPC hence the website is highly available. In another word, when one AZ is down, there will be a back up in another AZ. In each AZ, there is a public and private subnet. The public subnet hosts the web and application server in general, while database is hosted in the private subnet to enhance security. There is an elastic load balancer to distribute traffic into 2 AZs, while the Auto-Scaling is used to scale-in or scale out web-app EC2 accordingly. In addition, bastion host is added to allow admin to access to EC2 and RDS securely from local terminal using SSH (secure shell). Finally, AWS CloudTrail is added to monitor activities of different users.

Since this is an open-ended assignment, an overall high-level understanding of the AWS Cloud Architecting teaching materials and labs are required to successfully complete this project. Hence a revision of learning materials and labs are required when I encountered configurations error on AWS console. Due to the number of restrictions implemented in AWS Leaner environment, AWS Free Tier is used to complete this assignment instead. Therefore, an extra caution is required to avoid exorbitant costs. However, this has also honed my skills in budget planning when designing and configuring the instances on AWS Free Tier console.

---

## References

- AWS Default. (2023). *AWS IAM*. AWS. Retrieved February 17, 2023, from [https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/account\\_settings](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/account_settings)
- AWS Password. (2023). *AWS IAM*. AWS. Retrieved February 17, 2023, from [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_passwords\\_account-policy.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html)
- AWS Project 1. (202). *AWS Project 1 – Designing a Cloud Solution*. AWS. Retrieved February 17, 2023
- AWS Pragmatic. (2023). *AWS IAM*. AWS. Retrieved February 17, 2023, from [https://us-east-1.console.aws.amazon.com/iam/home#/users\\$new?step=details](https://us-east-1.console.aws.amazon.com/iam/home#/users$new?step=details)
- AWS MFA. (2023). *AWS IAM*. AWS. Retrieved February 17, 2023, from [https://us-east-1.console.aws.amazon.com/iam/home#/users/user-1?section=security\\_credentials](https://us-east-1.console.aws.amazon.com/iam/home#/users/user-1?section=security_credentials)
- AWS Cloud Trail. (2023). *CRR Monitor* AWS. Retrieved February 17, 2023, from <https://docs.aws.amazon.com/solutions/latest/crr-monitor/architecture.html>
- AWS ELB Security. (2023). *AWS EC2*. AWS. Retrieved February 17, 2023, from <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateLaunchConfiguration:>
- AWS VPC. (2023). *What is Amazon VPC*. AWS. Retrieved February 17, 2023, from <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>
- AWS EC2. (2023). *EC2*. AWS. Retrieved February 17, 2023, from <https://aws.amazon.com/ec2/>
- AWS RDS. (2023). *RDS*. AWS. Retrieved February 17, 2023, from [https://aws.amazon.com/free/database/?trk=fc551e06-56b0-418c-9ddd-5c9dba18569b&sc\\_channel=ps&s\\_kwcid=AL!4422!3!548908918497!e!!g!!amazon%20relational%20database%20service&ef\\_id=EA!a!QobChMIg5Lg6f2J\\_AIVCB4rCh3caAwzEAAYASAAEgl9RvD\\_BwE:G:s&s\\_kwcid=AL!4422!3!548908918497!e!!g!!amazon%20relational%20database%20service](https://aws.amazon.com/free/database/?trk=fc551e06-56b0-418c-9ddd-5c9dba18569b&sc_channel=ps&s_kwcid=AL!4422!3!548908918497!e!!g!!amazon%20relational%20database%20service&ef_id=EA!a!QobChMIg5Lg6f2J_AIVCB4rCh3caAwzEAAYASAAEgl9RvD_BwE:G:s&s_kwcid=AL!4422!3!548908918497!e!!g!!amazon%20relational%20database%20service)
- AWS ELB. (2023). *AWS ELB*. AWS. Retrieved February 17, 2023, from <https://aws.amazon.com/elasticloadbalancing/>
- AWS Auto Scaling. (2023). *AWS Auto Scaling*. AWS. Retrieved February 17, 2023, from <https://aws.amazon.com/autoscaling/>
- AWS Security. (2023). *AWS Security*. AWS. Retrieved February 17, 2023, from <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html>
- AWS S3. (2023). *AWS S3*. AWS. Retrieved February 17, 2023, from

- 
- <https://aws.amazon.com/s3/>
- AWS Networking. (2023). *AWS S3*. AWS. Retrieved February 17, 2023, from <https://aws.amazon.com/blogs/apn/aws-networking-for-developers/>
- AWS ELB. (2023). *AWS ELB*. AWS. Retrieved February 17, 2023, from <https://aws.amazon.com/elasticloadbalancing/features/#compare>
- AWS Capstone. (2023). *AWS Capstone*. AWS. Retrieved February 17, 2023
- AWS CloudTrail. (2023). *AWS CloudTrail*. AWS. Retrieved February 17, 2023 <https://aws.amazon.com/cloudtrail/>
- AWS System Manager. (2023). *Session Manager Getting Started Instance Profile*. Retrieved February 17, 2023 <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-getting-started-instance-profile.html>
- AWS KMS. (2023). *Key Management Service*. Retrieved February 18, 2023 <https://aws.amazon.com/kms/>
- AWS SSL. (2023). *SSL/TLS Certificate*. Retrieved February 18, 2023 <https://aws.amazon.com/what-is/ssl-certificate/#:~:text=SSL%2FTLS%20stands%20for%20secure,using%20the%20SSL%2FTLS%20protocol.>
- AWS Cloud9. (2023). *Cloud9*. Retrieved February 18, 2023 <https://aws.amazon.com/cloud9/>
- AWS Endpoint. (2023). *VPC Endpoint*. Retrieved February 18, 2023 <https://wa.aws.amazon.com/wellarchitected/2020-07-02T19-33-23/wat.concept.vpc-endpoint.en.html#:~:text=A%20VPC%20endpoint%20enables%20you,or%20AWS%20Direct%20Connect%20connection.>
- Nguyen, T. (2018). *Sample PHP*. Retrieved February 18, 2023 <https://gist.github.com/thosuperman/cbf1eeb9fe62c4840db96d90398230cf>
- MySQL. (2023). *MySQL Bench*. Retrieved February 18, 2023 <https://www.mysql.com/products/workbench/>
- AWS Pricing. (2023). *AWS Pricing Calculator*. Retrieved February 18, 2023 <https://calculator.aws/#/>