AWS Certified Cloud Practitioner Exam Guide

Build your cloud computing knowledge and build your skills as an AWS Certified Cloud Practitioner (CLF-C01)

Rajesh Daswani

Chapter 1

Figures

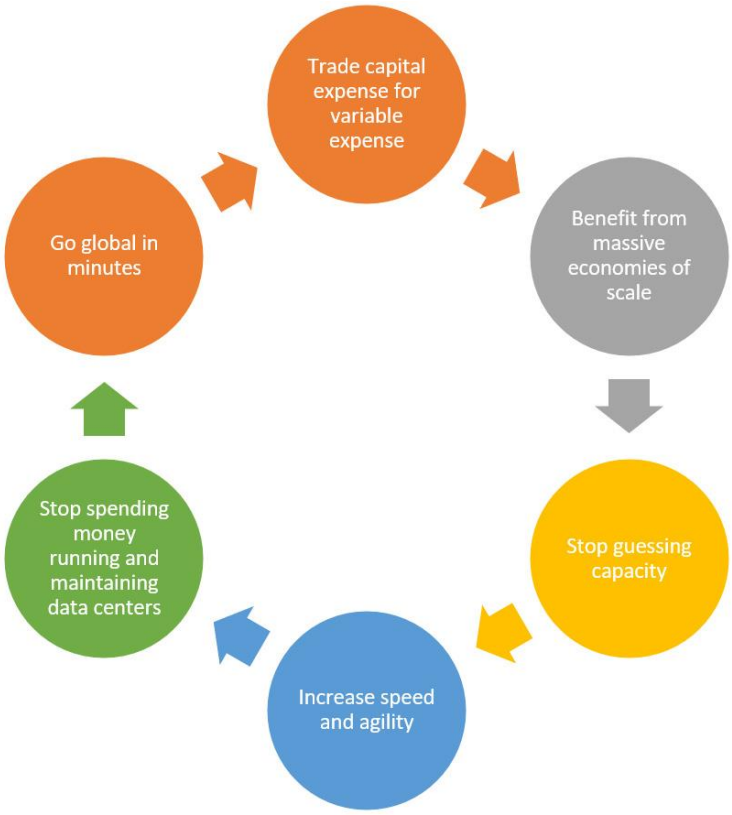

Figure 1.1 – The six advantages of cloud computing

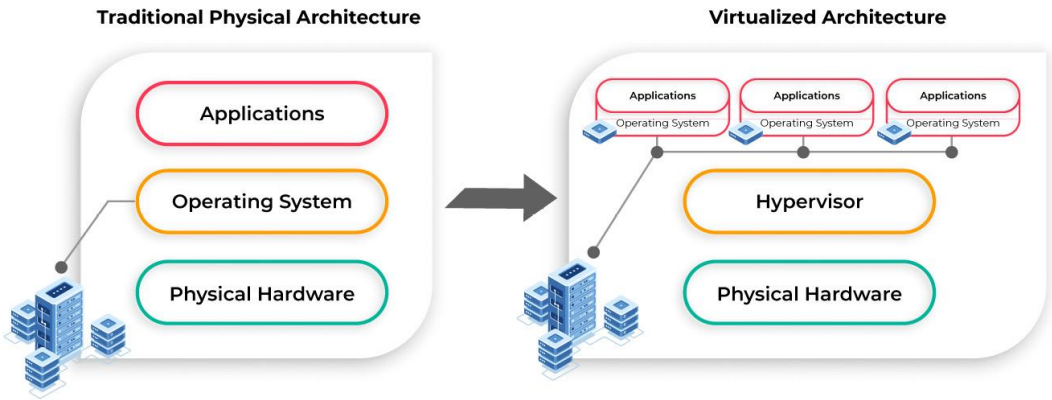

Figure 1.2 – Traditional physical architecture versus virtualized architecture

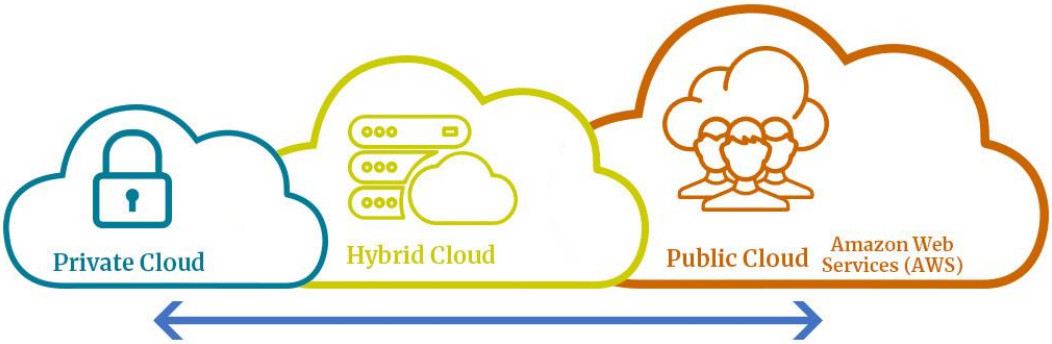

Figure 1.3 – Cloud deployment models

Links

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

Table

Cloud platform	Common examples
IaaS	Amazon Elastic Compute Cloud (EC2); Amazon Elastic Block Store (EBS); Amazon Elastic File System (EFS); Azure Virtual Machines (Azure VM)
PaaS	AWS Elastic Beanstalk; Azure Functions; Google App Engine
SaaS	Salesforce; GoToMeeting; Microsoft Office 365; Amazon Chime

Table 1.1 – Cloud computing models

Questions

Here are a few questions to test your knowledge:

1. Which of the following six advantages enables small start-up companies to immediately start consuming Eye-tee services from public cloud vendors such as AWS?

   A. Trade capital expense for variable expense

   B. Go global in minutes

   C. Stop guessing capacity

   D. Increase speed and agility

2. Which feature of cloud computing enables customers to deploy their resources in a matter of minutes using a self-service model?

   A. Access to cloud provider APIs

B. Access to cloud provider engineers to rack and stack servers

C. Scalability features

D. Multiple server options

3. What is a hypervisor?

A. Software that enables you to create and managed virtualized resources running on physical hardware, such as VMs

B. Software used to monitor the health of your Windows servers

C. Software used to create HA websites

D. Hardware that enables you to increase the performance of your physical servers

4. Which of the following are the primary benefits of server virtualization? (Select two answers.)

A. Efficient use of physical hardware resources

B. Ability to provision virtual servers in a matter of minutes

C. Enhanced encryption services

D. Ability to meet compliance requirements

5. Which of the following is a prime example of IaaS?

A. A service that gives you access to configure underlying virtual compute, storage, and network resources to host your application

B. A service that abstracts the underlying infrastructure, allowing you to focus on your application code deployment process

C. A service that hosts and delivers a complete application via a public network, with no access to any underlying infrastructure

D. A service that allows you to consume hardware resources for a short lease period and pay on a metered basis

6. Which of the following is a prime example of PaaS?

A. A platform that hosts and delivers a complete application via a public network, with no access to any underlying infrastructure

B. A service that gives you access to configure underlying virtual compute, storage, and network resources to host your application

C. A service that abstracts the underlying infrastructure, allowing you to focus on your application code deployment process

D. A service that allows you to build infrastructure using code for repeat deployments in different environments

7. Which of the following is a prime example of SaaS?

A. A service that gives you access to configure underlying virtual compute, storage, and network resources to host your application

B. A service that abstracts the underlying infrastructure, allowing you to focus on your application code deployment process

C. A service that hosts and delivers a complete application via a public network, with no access to any underlying infrastructure

D. A service that allows developers to adopt DevOps strategies for their software development life cycle

8. Which cloud deployment model enables you to connect your on-premises workloads with resources you have deployed with a public cloud provider such as AWS?

A. Private cloud

B. Public cloud

C. Hybrid cloud

D. Hyper cloud

Chapter 2

Figures

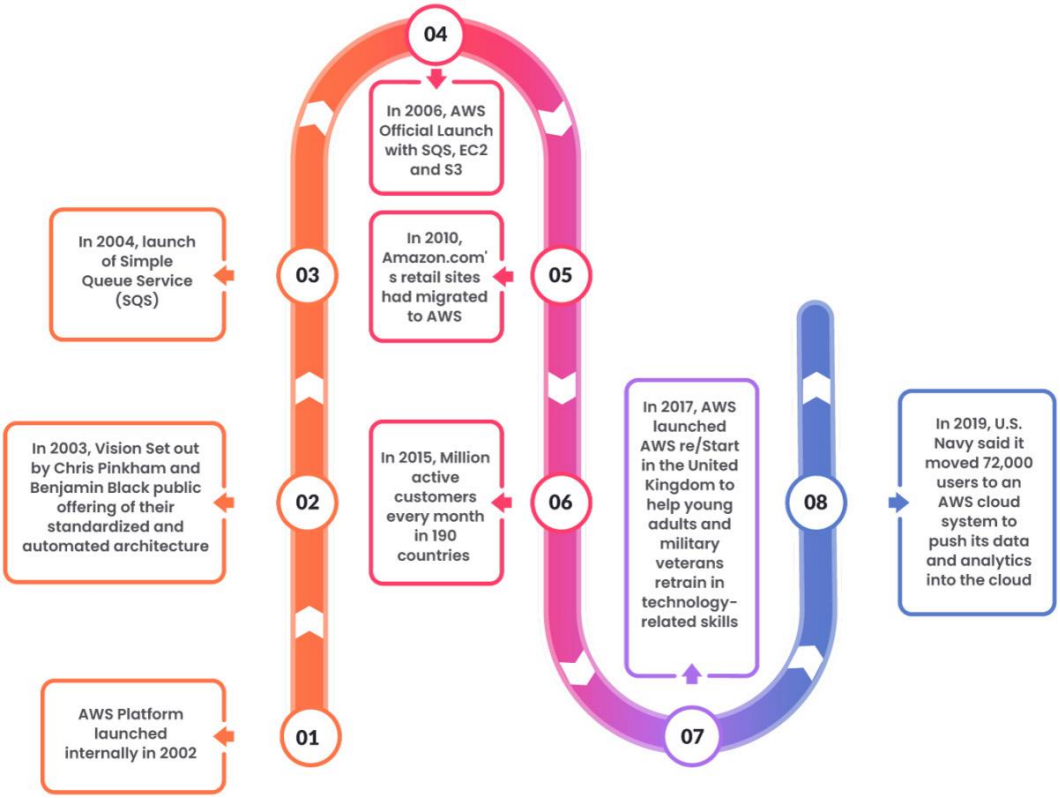

Figure 2.1 – AWS history: timeline

Figure 2.2 – AWS Global Infrastructure. Image courtesy of AWS (https://aws.amazon.com/about-aws/global-infrastructure/)

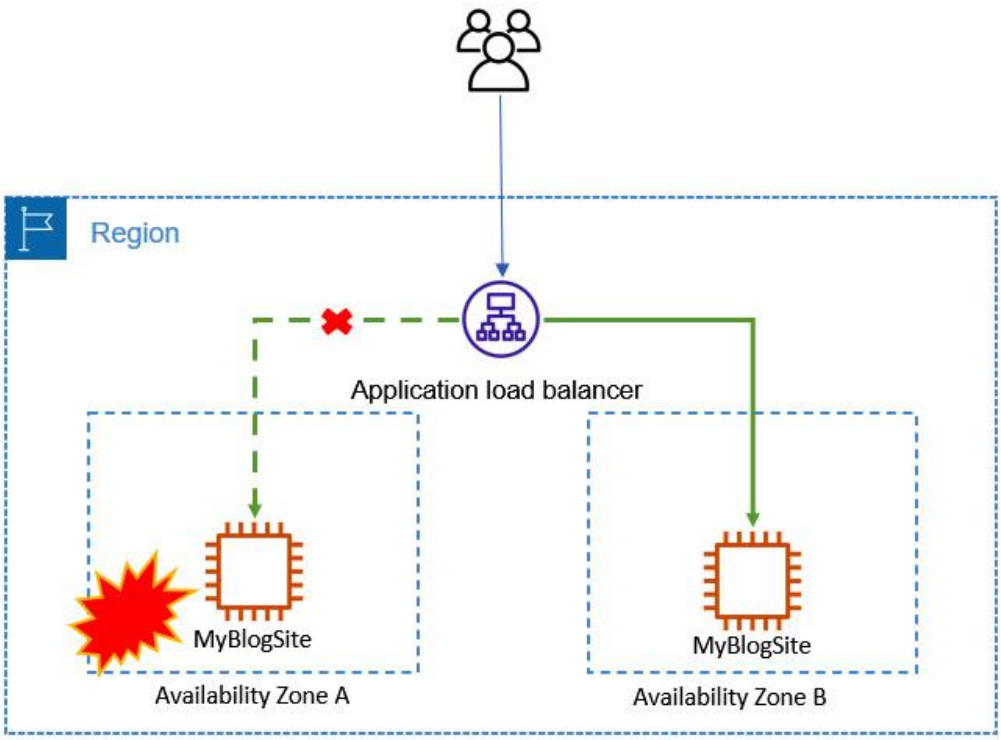

Figure 2.3 – User traffic is temporarily directed to only the server(s) in AZ B, until AZ A comes back online

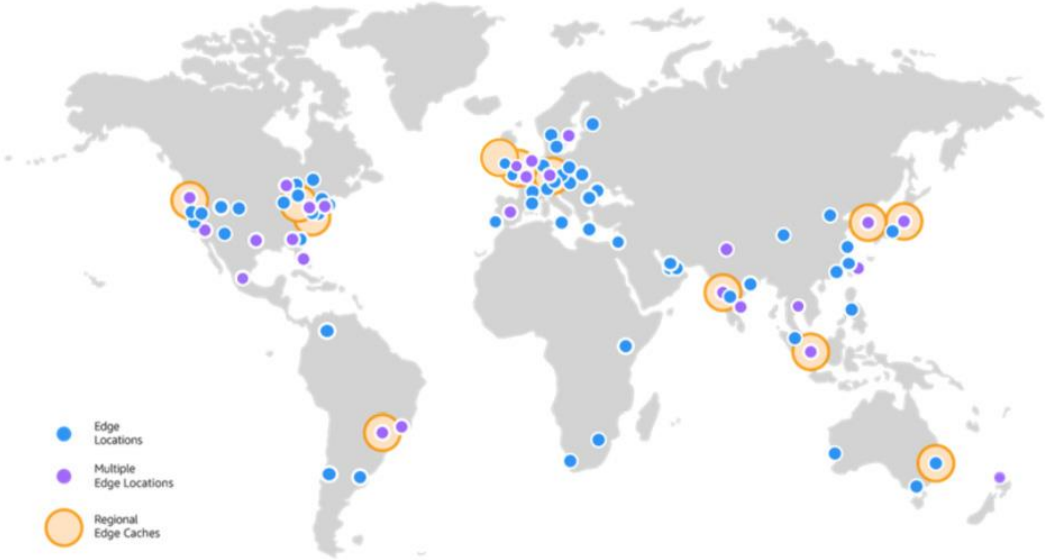

Figure 2.4 – Edge locations and regional edge caches across the globe. Image courtesy of AWS (https://aws.amazon.com/cloudfront/features/)

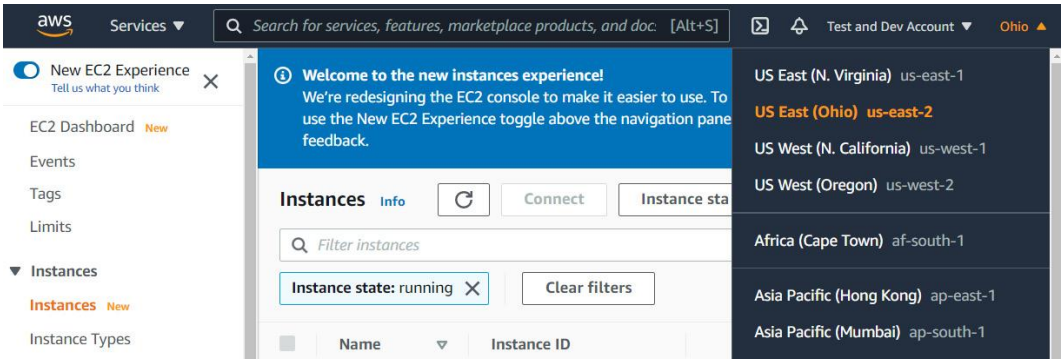

Figure 2.5 – Selecting a Region to access the EC2 instances (servers) deployed in that Region

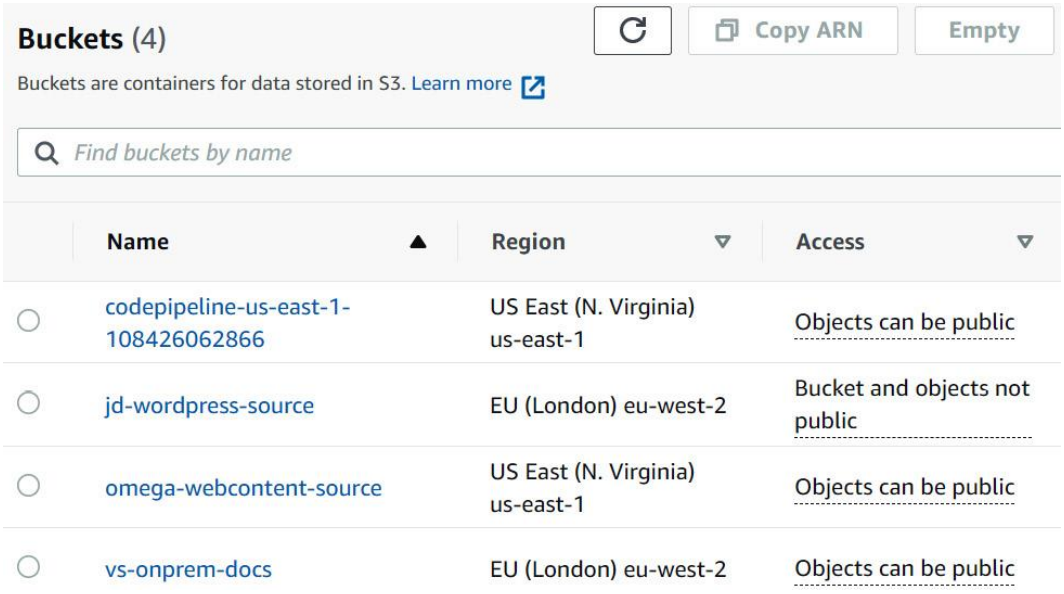

Figure 2.6 – Amazon S3, displaying all buckets in a specific AWS account across all Regions where they have been deployed

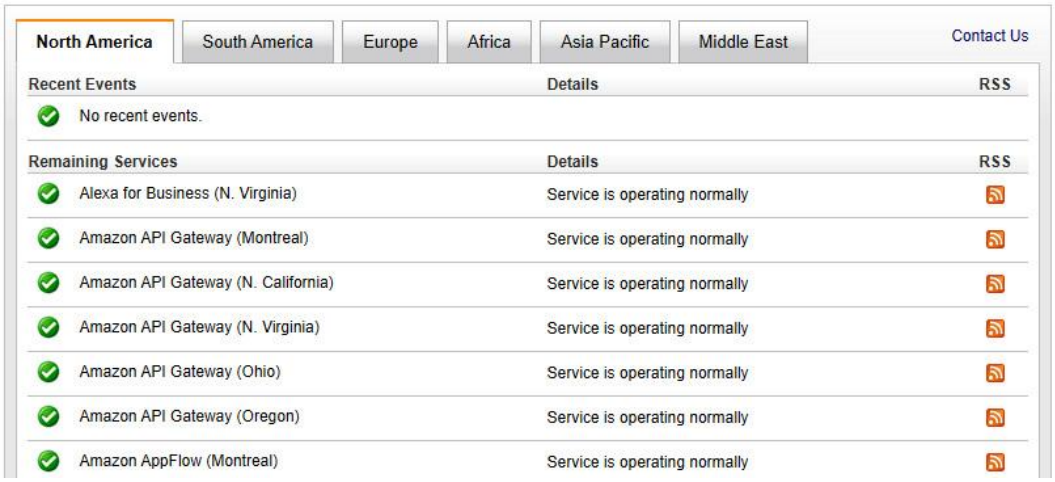

Figure 2.7 – AWS Service Health Dashboard. Image courtesy of AWS (https://status.aws.amazon.com/)

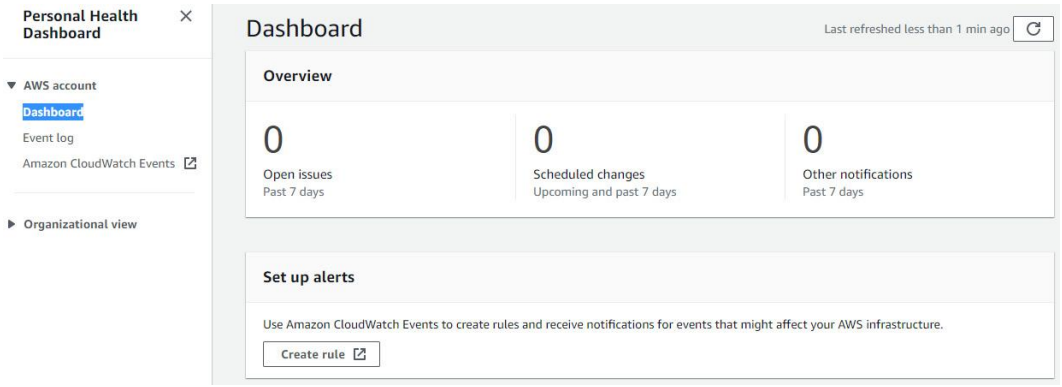

Figure 2.8 – AWS PHD

Table

Basic	Developer	Business	Enterprise
Offers only non-technical customer support	Technical support offered during business hours alone (8:00 a.m. to 6:00 p.m.—customer local time zone)	24/7 phone, email, and chat access to Cloud Support engineers	24/7 phone, email, and chat access to Cloud Support engineers
	General guidance offered within 24 business hours	General guidance offered within 24 hours	General guidance offered within 24 hours
	System impaired troubleshooting offered within 12 business hours	System impaired troubleshooting offered within 12 hours	System impaired-troubleshooting offered within 12 hours
		Production system-impaired support within 4 hours	Production system-impaired support within 4 hours
		Production system-down support within 1 hour	Production system-down support within 1 hour
			Business-critical-system down support within 15 minutes

Table 1.1:

Links

You can access a wide selection of analytical research reports at https://aws.amazon.com/resources/analyst-reports.

You can actually test your upload transfer rates using a tool provided by AWS which is available at https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html

Refer to https://aws.amazon.com/premiumsupport/plans/ for more information on Developer support plan.

You can find a full breakdown of each plan at https://aws.amazon.com/premiumsupport/plans/.

AWS offers SLAs for its various service offerings and you can get a full list of these at https://aws.amazon.com/legal/service-level-agreements/

Questions

Here are a few questions to test your knowledge:

1. Which of the following AWS support plans gives you access to all AWS Trusted Advisor reports? (Select two answers)

   E. Basic support plan

   F. Developer support plan

   G. Business support plan

   H. Enterprise support plan

   I. Global support plan

2. You have spent months developing a new application for your customers. You are now ready to go live and want to ensure that you have access to AWS technical support engineers if there are any issues with your application servers or backend database. Your organization is comfortable with 1-hour response times for production-system down issues. Which support plan is the most cost-effective option for you?

   A. Basic support plan

   B. Developer support plan

   C. Business support plan

   D. Enterprise support plan

3. Which AWS support plan gives you access to a technical account manager who will monitor your environment and provide guidance to optimize your workloads on the AWS platform?

   A. Basic support plan

   B. Developer support plan

   C. Business support plan

   D. Enterprise support plan

4. You are planning to build a test and development environment on AWS as a precursor to ultimately migrating your workloads to the platform. In the interim period, your developers require some basic technical support as they are new to cloud computing. Which AWS support plan offers cost-effective access to Cloud Support associates during business hours?

   A. Basic support plan

   B. Developer support plan

   C. Business support plan

   D. Enterprise support plan

5. Which of the following services is provided across all AWS support plans and allows support access 24/7 via telephone, chat, and email?

   A. Access to technical support via telephone and chat

   B. Access to customer support services to resolve any billing or account login issues

   C. Access to a technical account manager to help you manage your account

   D. Access to a full range of reports from the AWS Trusted Advisor

6. Which feature of the AWS Global Infrastructure enables you to launch applications and store data in a manner that is compliant with regulatory requirements?

   A. Regions

   B. AZs

   C. Edge location

   D. CloudFront

7. Which component of the AWS Global Infrastructure enables you to distribute your content to users across the globe such that cached versions of your digital assets are available locally to those users?

   A. Regions

   B. AZs

   C. Edge locations

   D. AWS RDS

8. Which component of the AWS Global Infrastructure enables you to architect your application solution to offer high-availability capabilities within a specific Region?

   A. Regions

   B. AZs

C. Edge locations

D. Regional edge caches

9. Which of the following services are considered global services on the AWS platform? (Select two answers)

A. AWS IAM

B. Amazon **Virtual Private Cloud** (**VPC**)

C. Amazon Snowball

D. AWS EC2

E. Amazon CloudFront

10. Which of the following services are designed to be set up, configured, and consumed on premises? (Select two answers)

A. AWS Outposts

B. Amazon Storage Gateway

C. Amazon DynamoDB

D. AWS **Simple Notification Service** (**SNS**)

E. AWS PHD

11. As part of the signup process, you are required to adhere to policy guidelines that describe prohibited activities. Which policy does this fall under?

A. Compliance policy

B. Password policy

C. AuP

D. Vulnerability testing guidelines

12. Which AWS service publishes up-to-the-minute information regarding any outages or issues with any service across all Regions of the AWS ecosystem?

A. PHD

B. Outage and issues dashboard

C. Service Health Dashboard

D. Amazon CloudWatch

Chapter 3

Figures

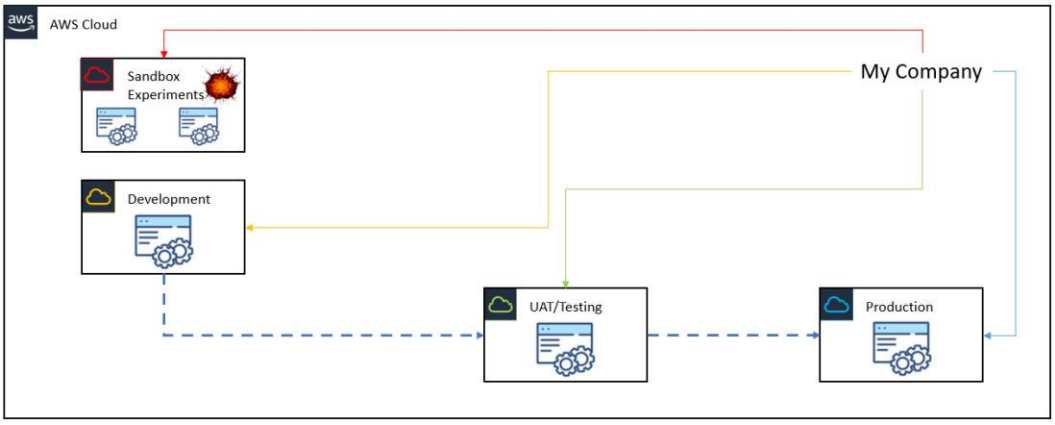

Figure 3.1 – Multiple accounts help to limit the blast radius of your workloads

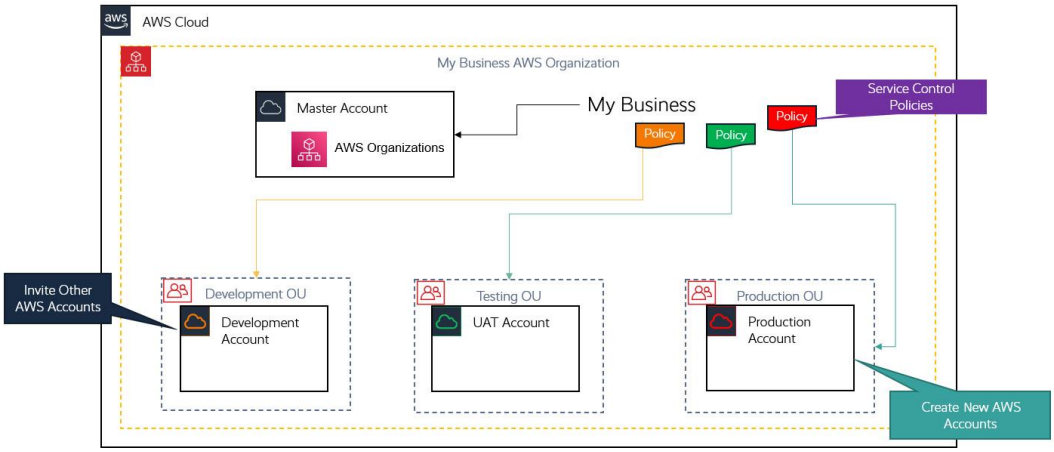

Figure 3.2 – AWS Organizations with multiple accounts

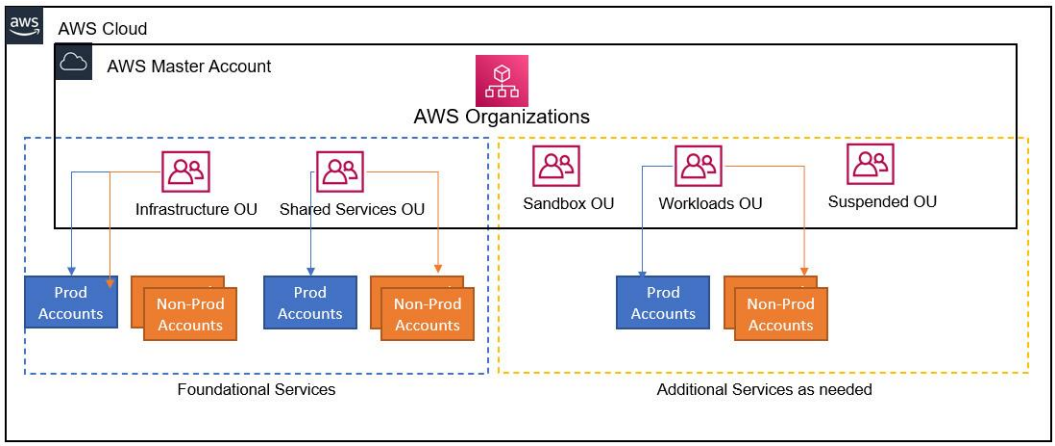

Figure 3.3 – AWS configured with core infrastructure as well as security and AWS Organizations additional OUs

Links

https://docs.aws.amazon.com/whitepapers/latest/organizing-your-aws-environment/recommended-ous.html

Exercise 3.1 – Setting up your first AWS Free Tier account

The following step-by-step process will show you how to set up your first AWS account. You will need the following to complete the setup process:

- Your personal details, name, physical address, and an email address.
- A mobile phone.
- A credit card. As far as possible, the labs in this training guide will fall under the free tier and your credit card will not be charged for those resources you deploy. A couple of labs, however, may go over the free tier threshold and if you choose to do those labs, there may be a small minimum charge. We will discuss this in more detail shortly.

Now that we know about the requirements, let's get started with creating our account:

1. In your favorite browser, search for the term `AWS Free Tier` and you should find a link to the Amazon Web Services Free Tier offering. Click on the second link, as shown in the following screenshot:

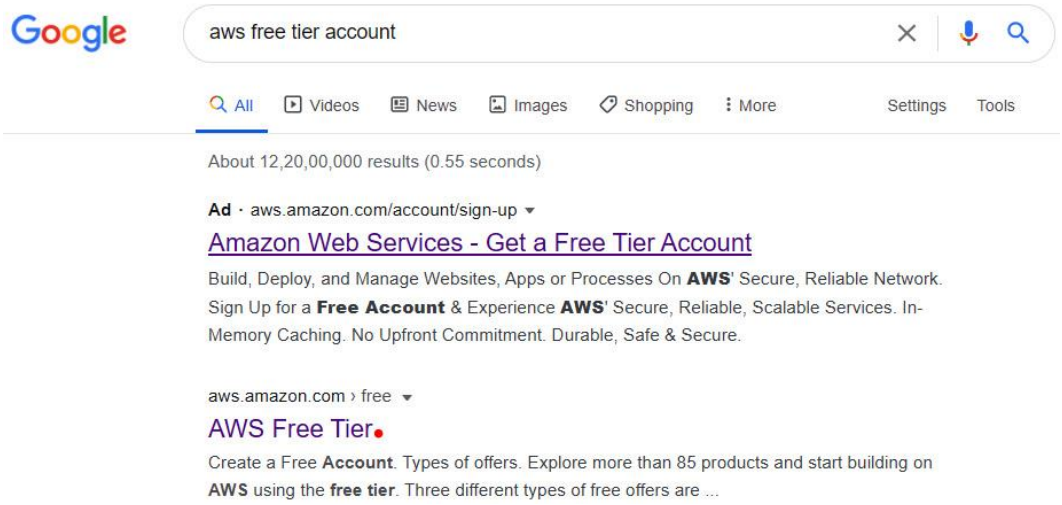

Figure 3.4 – AWS Free Tier link via Google Search

2. You will be taken to the AWS Free Tier home page. Next, click on **Create a Free Account**:

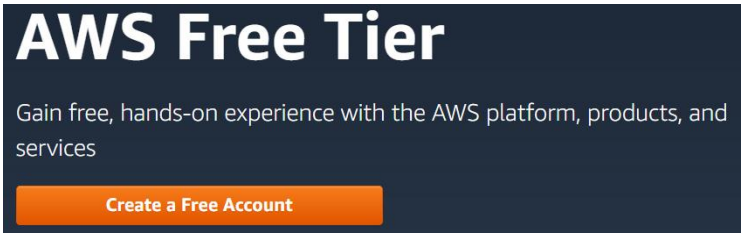

Figure 3.5 – Free account setup

3. At the AWS **Sign in** page, click, **Create a new AWS account**:

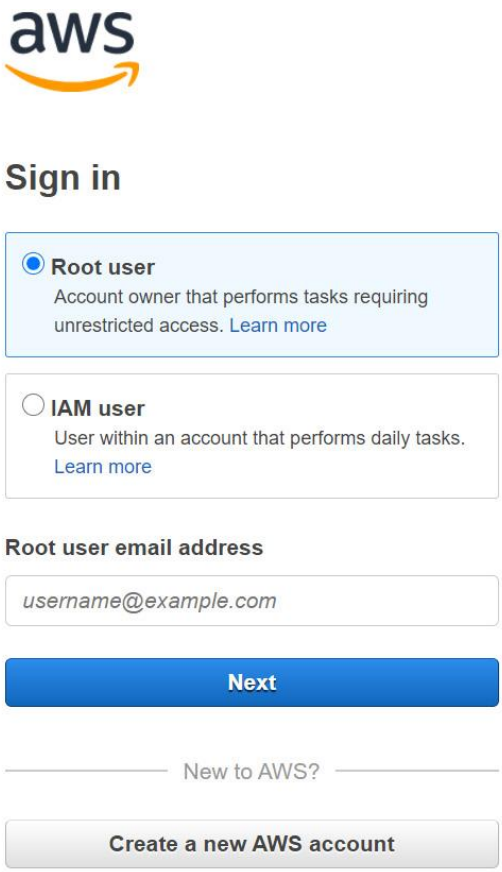

Figure 3.6 – Free account setup – creating a new AWS account

4. Next, provide an email address, choose a password, and choose an account name. The account name can be any name you like to use to identify the purpose of the account, for example, Dev or Prod:

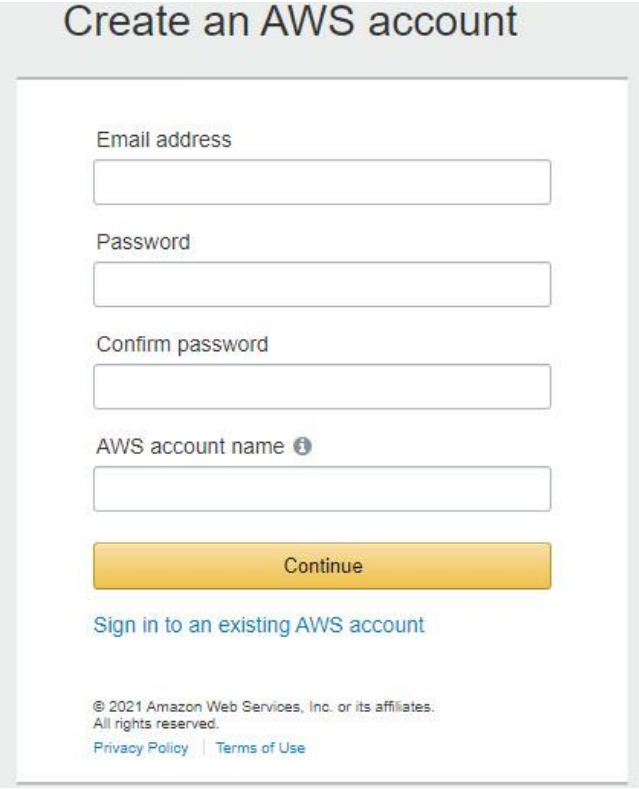

Figure 3.7 – Free account setup – providing an email address and an account name

5. Next, you may be asked to fill up a captcha form for security. Type the letters and numbers in the image into the textbox provided and click **Continue**:

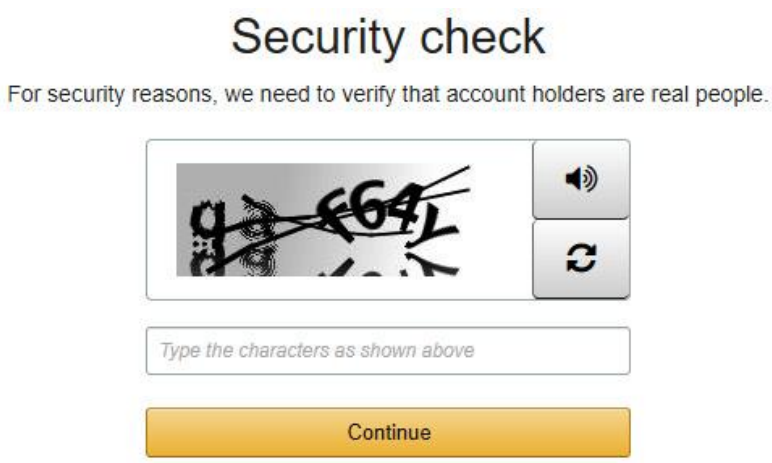

Figure 3.8 – Free account setup – security check screen

6. Next, you need to provide your full contact details and choose the type of account you want to create – Personal or Professional. Professional accounts allow you to get a full tax invoice and, in some countries, claim back certain types of tax, such as VAT or GST. Once you have completed the form, click **Create Account and Continue**:

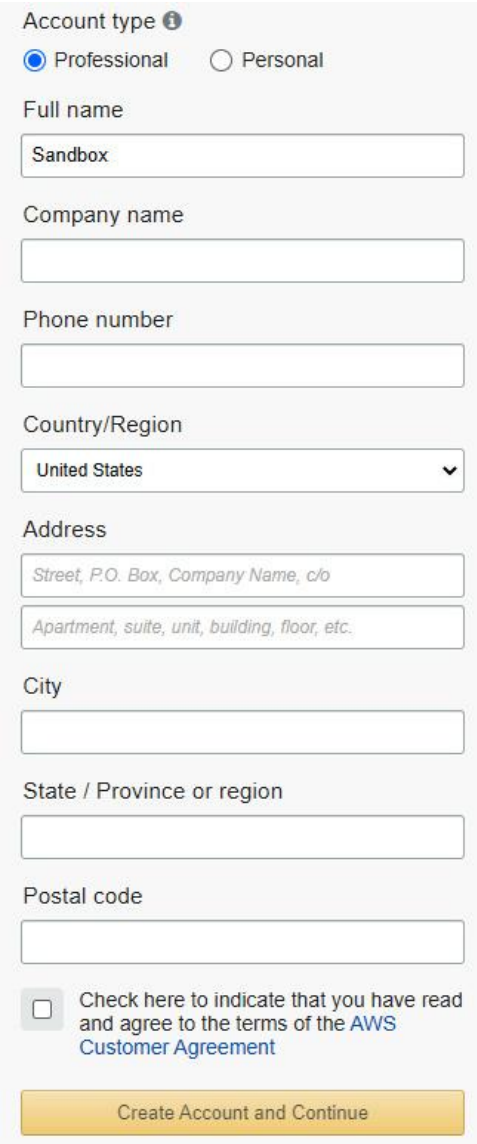

Figure 3.9 – Free account setup – providing contact details

7. Next, you need to provide your debit or credit card details, confirm your address, and click **Verify and Add**:

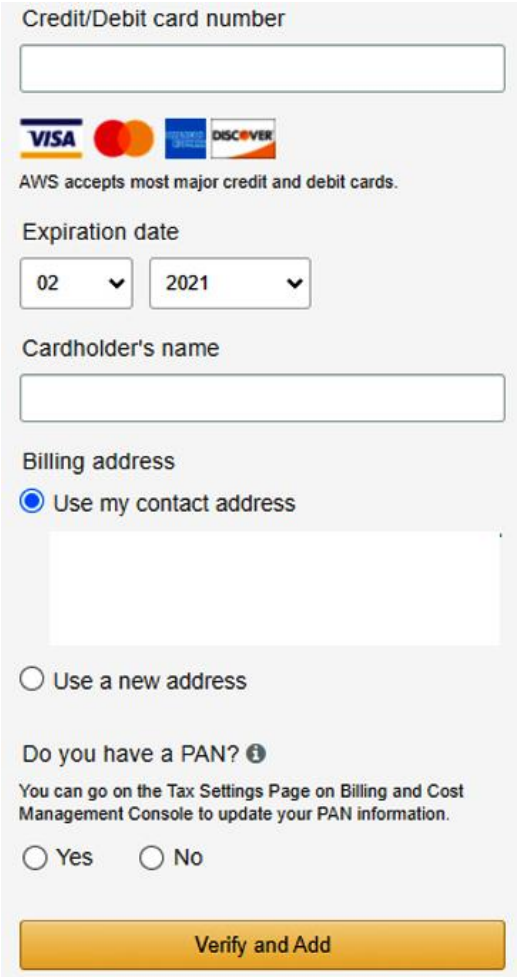

Figure 3.10 – Free account setup – providing credit card details

8. You may need to provide a one-time PIN that will be sent to your phone to verify the card. In some countries, you may be charged a very small amount, perhaps a few cents, to verify the card, but this amount will be refunded through the banking system.

9. After this, you will receive a **Confirm your identity** dialog box that requires you to provide a phone number using which you will be sent a verification code, either as an SMS text message or voice call, depending on your preference. You will also need to complete the security checkbox and then click on, for instance, the **Send SMS** option, as shown in the following screenshot:

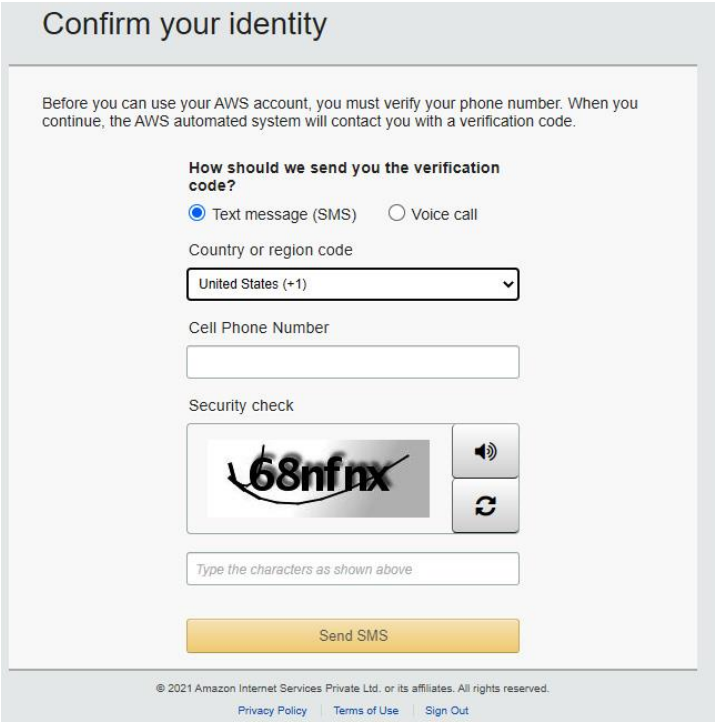

Figure 3.11 – Free account setup – providing a phone number for verification

10. You will then be taken to the following dialog box, which requires you to provide the verification code that has been sent to your phone:

Figure 3.12 – Free account setup – providing a verification code received on your mobile phone

11. Once you enter the code, your account will be verified, and you should get the following dialog box. Click **Continue**:

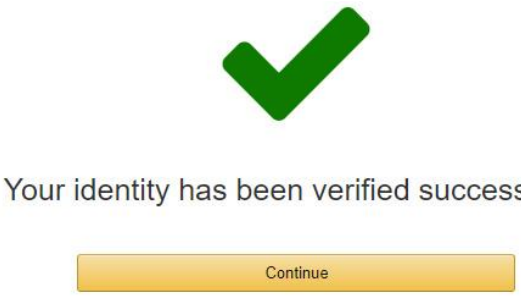

Figure 3.13 – Free account setup – completing the verification process

12. You will be taken to the **Select a Support Plan** screen, where you will have the option to select your support plan for this account. For the purpose of this account, go ahead and select **Basic Plan**:

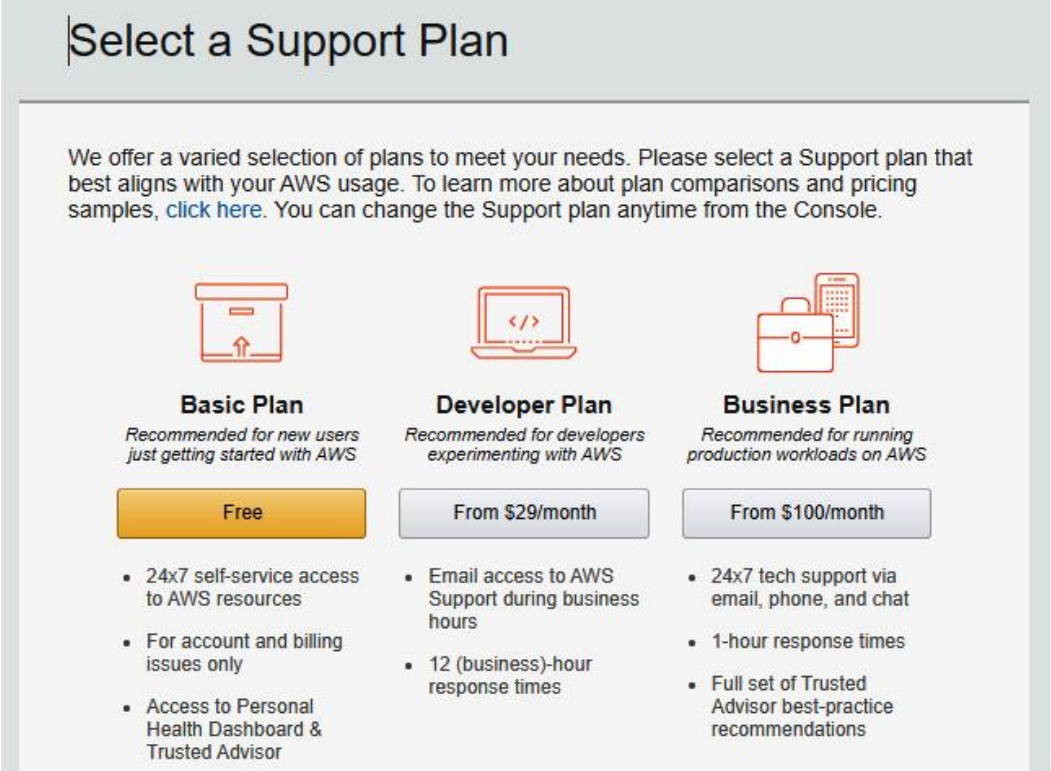

Figure 3.14 – Free account setup – selecting the basic support plan

13. You will now be taken to the **Welcome to Amazon Web Services** screen. Click the **Sign In to the Console** button:

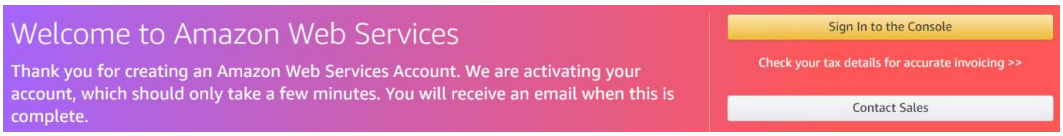

Figure 3.15 – Sign In to the Console

Ensure that you select **Root user** and provide the email address and password you used to create your new Free Tier account. This email address and password combination is also known as the **root user** of your AWS account and has complete control over your account:

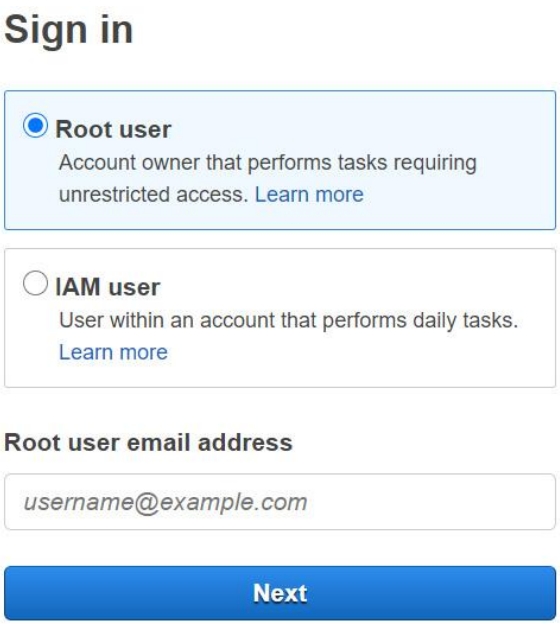

Figure 3.16 – Free account setup – signing in as the root user to test account setup

14. Once logged in, you will be presented with the **AWS Management Console** page:

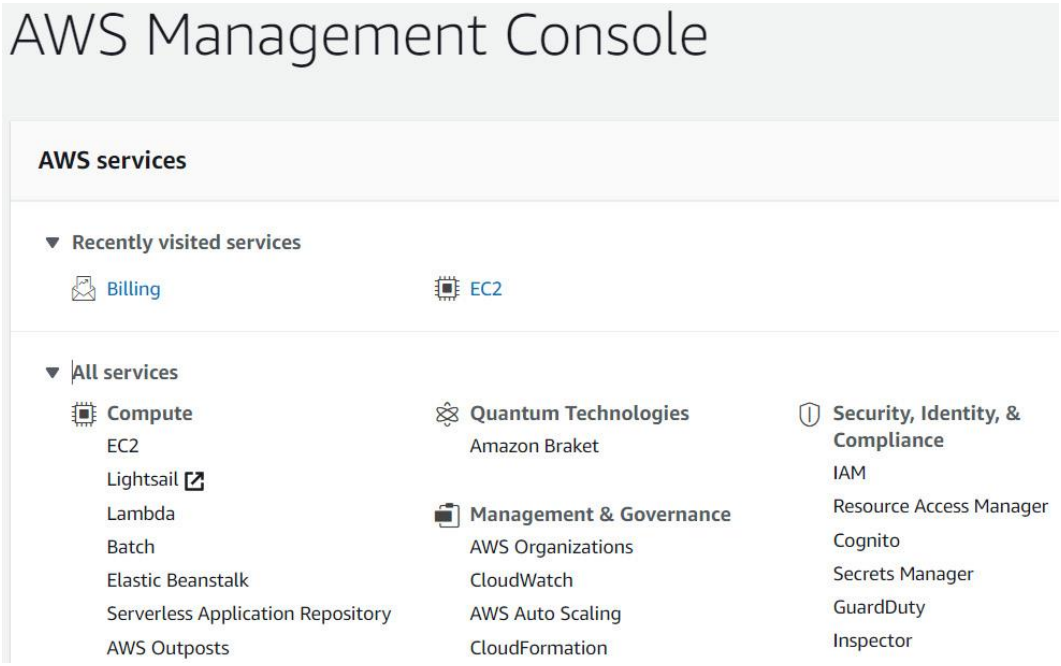

Figure 3.17 – Free account setup – accessing the AWS Management Console

In this section, you created your first AWS account, which will enable you to access all AWS services, across its global infrastructure. Using your AWS account, you can now set up and deploy a wide range of resources to support and host any application workload. In the next exercise, we look at how to set up your billing alarm.

To maximize your benefit from this training, you are encouraged to complete all of the exercises. This will help you to gain the necessary hands-on experience and the confidence to start building real-world solutions on AWS. While we ensure that most of the exercises fall within the Free Tier

thresholds, there are a few that will incur some costs. You will be notified of this as part of the exercise and you may choose to complete them if you wish.

In addition, you may deploy certain resources and forget to terminate them, resulting in crossing some of those Free Tier thresholds. By having a billing alarm, you can set yourself a small budget sufficient to complete all of the labs. With a billing alarm in place, you will be alerted if your total charges cross the budgeted thresholds.

We discuss how to set up your billing alarm in the next section.

Exercise 3.2 – Setting up a billing alarm

When you configure a billing alarm, you define a dollar amount as a threshold value as your maximum budget. If the total charges on your AWS account cross this value, you are alerted with a notification and can take remedial action.

As previously discussed, this training guide offers several hands-on labs and exercises to enable you to gain real-world hands-on experience in configuring various services to host your workloads in the cloud. Most of the labs will fall within the free tier, except for a few that may incur very minimal charges. We indicate the labs that may incur such charges. It is also important to terminate any labs you complete to ensure you do not forget about them.

To complete all exercises in this training guide, we recommend you set a billing alarm of USD 10, although you can choose any value you are comfortable with. Should you exceed this dollar amount, you will be alerted with a notification via email to take immediate action. You can then terminate any labs you no longer need.

So, let's now proceed with configuring your AWS billing alarm. We start by enabling the option to receive billing alerts. This is a prerequisite step and must be completed before configuring billing alarms:

1. Log in to your AWS Management Console using your root account credentials. This is the email address and password you will have configured at the time of account sign-up.
2. Access the **Billing and Cost Management** dashboard at https://console.aws.amazon.com/billing/.
3. In the left-hand navigation pane, click **Billing Preferences**.
4. Click on **Receive Billing Alerts** and then click **Save Preferences**.

The following screenshot illustrates enabling the billing alerts option:

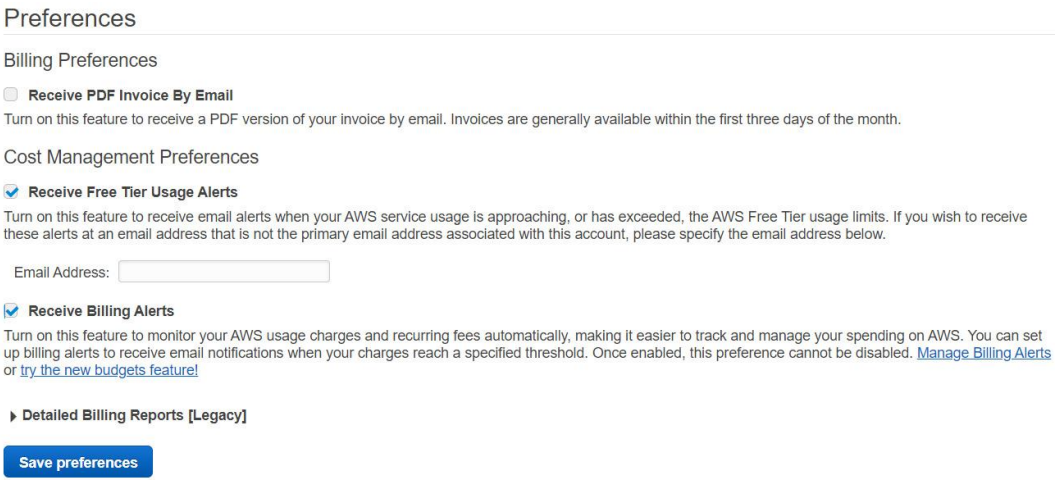

Figure 3.18 – Setting up billing alarms – enabling the option to receive billing alerts

Now that you have enabled the option to receive billing alerts, you can proceed with setting up your billing alarm. Note that once this setting has been enabled, it cannot be disabled.

In the following step-by-step process, you create an alarm that sends an email message when your estimated charges for your AWS account exceed a specified threshold:

5. Access the CloudWatch console at https://console.aws.amazon.com/cloudwatch/. Note that billing metric data is stored in the US-East-1 Region. From the top right-hand menu, ensure that you are in the N. Virginia (us-east-1) Region as per the following screenshot:

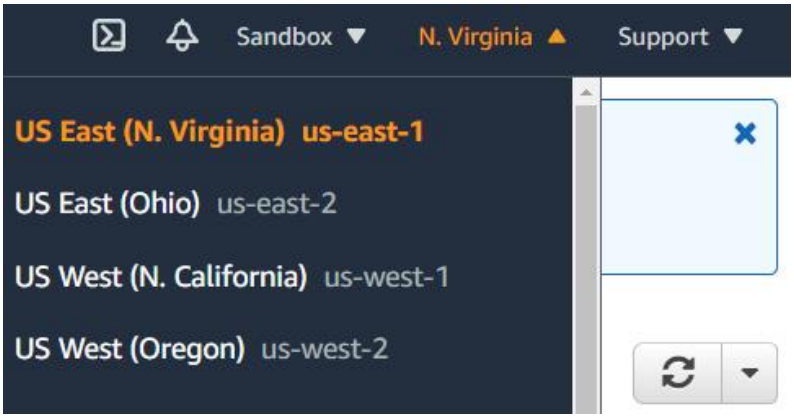

Figure 3.19 – Setting up billing alarms – navigating to the N. Virginia Region

6. In the left-hand navigation pane, select **Alarms** and then click **Create Alarm** in the far-right hand corner of the screen. You will be presented with the four-step **Create alarm** wizard:

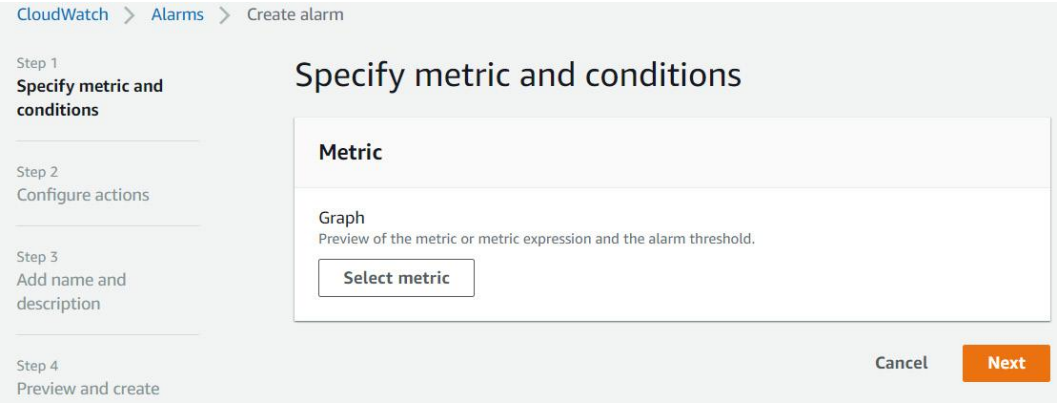

Figure 3.20 – Setting up billing alarms – setting up billing alarms in CloudWatch

7. Under **Step 1**, click **Select metric**.
8. Under **All metrics**, click on **Billing**.
9. Next, click on **Total Estimated Charge**:

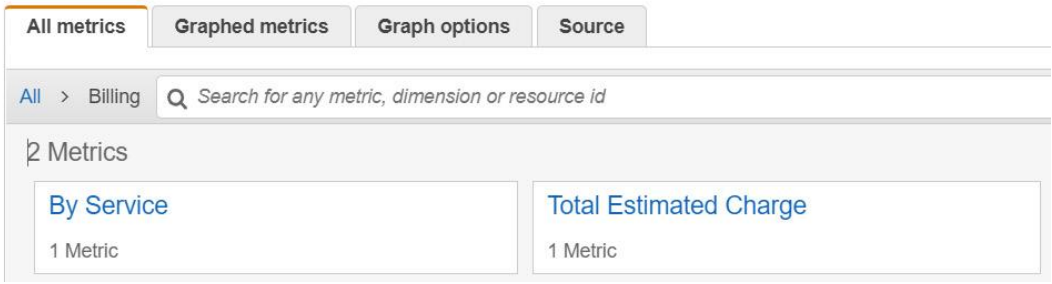

Figure 3.21 – Setting up billing alarms – defining metrics for Total Estimated Charge

10. Click the checkbox next to the **USD** currency for the metric name **EstimatedCharges**.
11. Click **Select metric**.
12. In the dialog box entitled **Specify metric and conditions**, scroll down and select **Static** as the threshold type, under **Conditions**.
13. Select **Greater > threshold**, under the heading **Whenever EstimatedCharges is...**.
14. Finally, set the dollar amount to **10** for USD under the **Define the threshold value** sub-heading, and then click **Next**, as per the following screenshot:

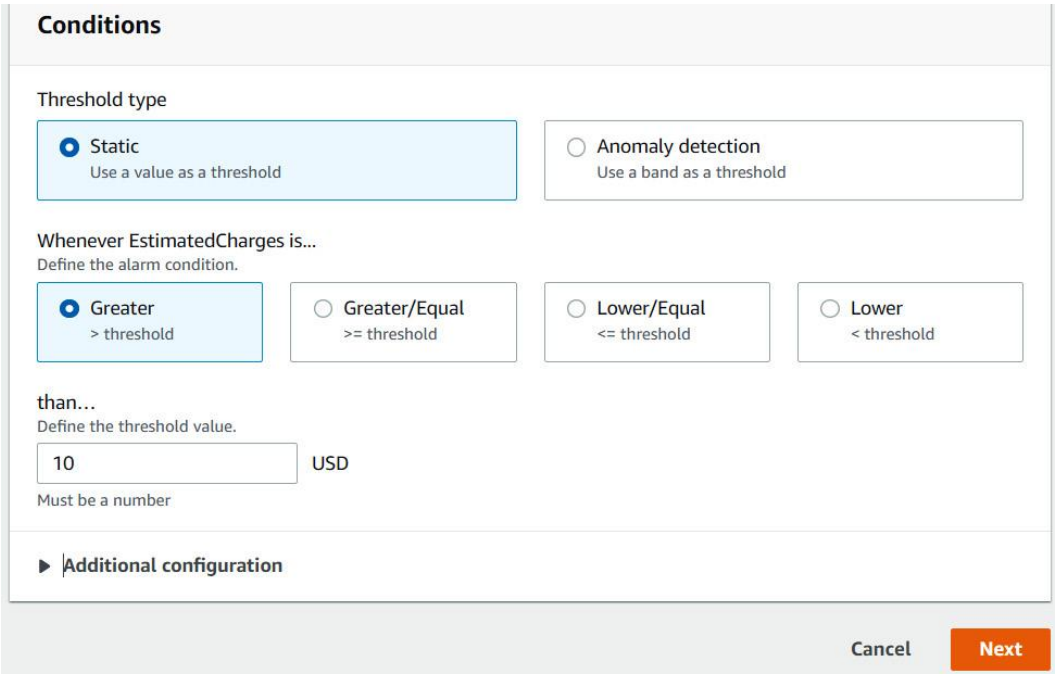

Figure 3.22 – Setting up billing alarms – setting up a billing alarm threshold value

15. In *Step 2*, you can now configure actions when the alarm breaches. For this, click the **Add notification** button:

Figure 3.23 – Setting up billing alarms – setup notification

16. Under the alarm state trigger, make sure that the **In alarm** state is selected.

17. Next, under **Select an SNS topic**, select the option for **Create new topic**. **SNS** stands for **Simple Notification Service** and is a push-based messaging service. You can configure an SNS topic to send you email alerts when the alarm is in the **In alarm** state. We discuss Amazon SNS in detail in *Chapter 10*, *Application Integration Services*.

18. Under the heading **Create a new topic…**, provide a topic name, for example, `MyBillingAlerts`.

19. Next, under the heading **Email endpoints that will receive the notification…**, provide an email address that you have access to where the alerts will be sent. You can use the same email address that you created your AWS account with.

20. Next, click **Create topic**:

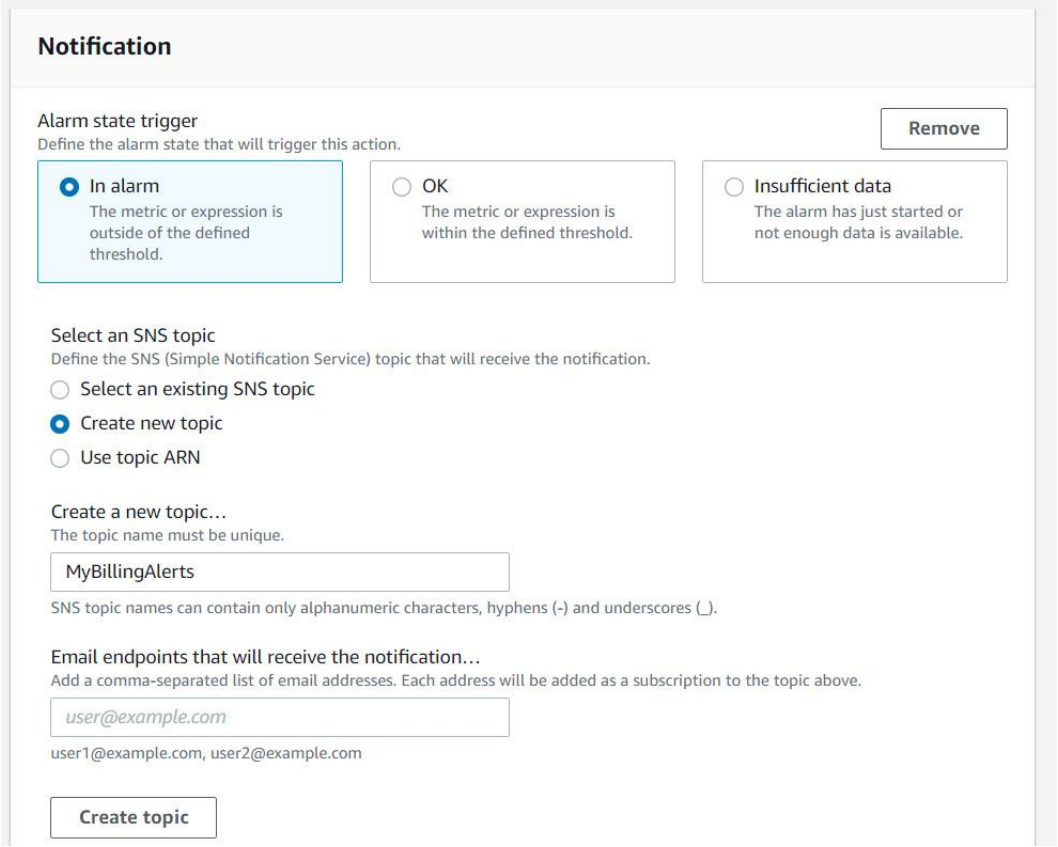

Figure 3.24 – Setting up billing alarms – defining SNS topics for notifications

21. Your SNS topic with the name you chose will be created and you will see the email address that notifications will be sent to.

22. Scroll toward the bottom of the screen and click on **Next**.

23. In *Step 3*, provide an appropriate name and description for the alarm and click **Next**:

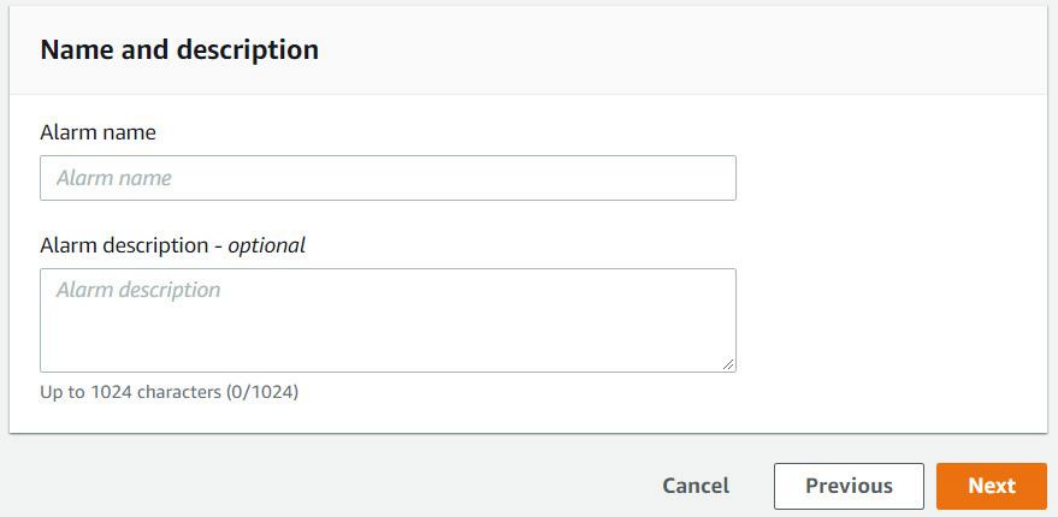

Figure 3.25 – Setting up billing alarms – alarm setup

24. In *Step 4*, you can review your settings and confirm by clicking on the **Create alarm** button.

25. You are then presented with the alarm configuration status in Amazon CloudWatch:

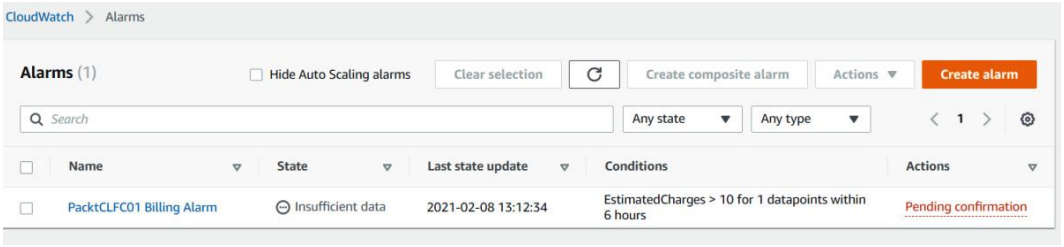

Figure 3.26 – Setting up billing alarms – verifying the Actions status

26. You will notice from the preceding screenshot that you have a **Pending confirmation** link highlighted in red. When you configure an SNS notification to send alerts to an email, you are, in effect, subscribing to the SNS topic you created earlier. For security purposes and to avoid rogue messages, you are required to log in to your email account and confirm the subscription.

27. Log in to your email account and you should find an email from Amazon asking you to confirm your subscription, as in the following screenshot:

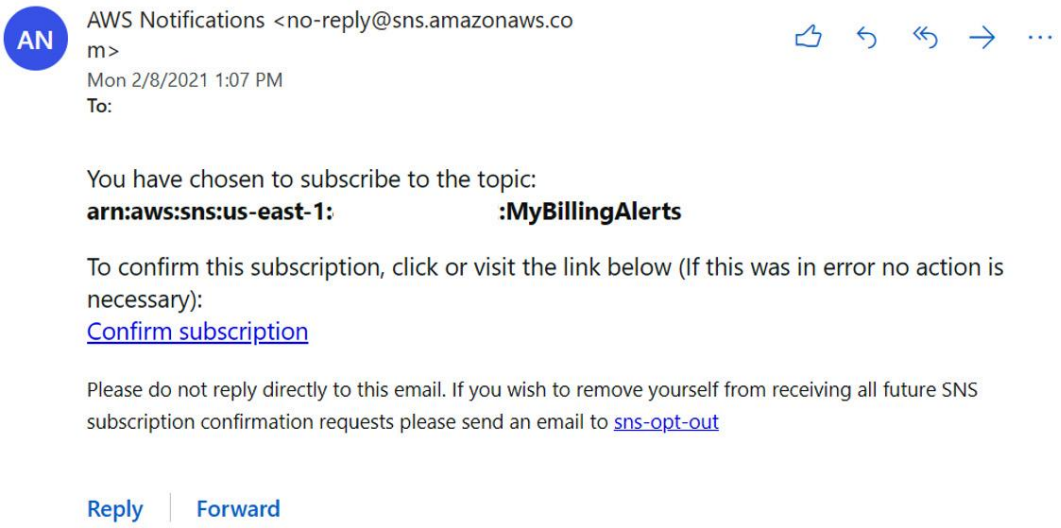

Figure 3.27 – Setting up billing alarms – confirming a notification subscription

28. Click on the **Confirm subscription** link so that your subscription can be activated. Should your monthly charges exceed the USD 10 threshold, an email notification will be sent to you and you can terminate any unwanted or forgotten labs.

29. If you now refresh your alarms by clicking on the circular arrow, you will see that the pending confirmation message disappears. Furthermore, as this is a brand-new account, you will not yet have incurred any charges and you will note that the alarm is in the **OK** state:

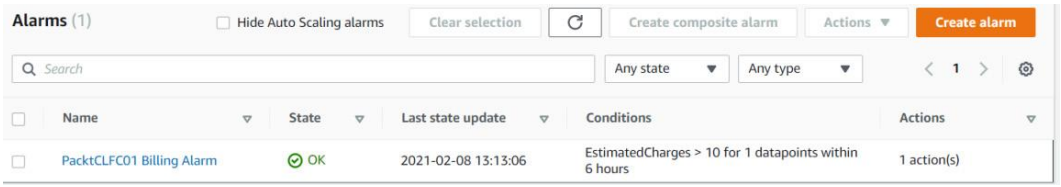

Figure 3.28 – Setting up billing alarms – verifying alarm status

Now that you have set up and configured your AWS billing alarms, you can be rest assured that you will be alerted if you exceed the threshold you selected previously. Alarms can be set for a wide range of services, enabling you to effectively monitor and maintain your workloads on AWS. Alarms are configured in Amazon CloudWatch, which we will discuss in detail in *Chapter 13, Management and Governance on AWS*.

Questions

Here are a few questions to test your knowledge:

1. Before setting up your billing alarms, which preference setting needs to be enabled first?

   A. Enable billing alerts

   B. Enable alarms

   C. Set up AWS Organizations

   D. Configure MFA

2. Which AWS service enables you to centrally manage multiple AWS accounts with SCPs to establish permission guardrails using which services can be enabled in those accounts?

   A. AWS Organizations

   B. AWS IAM

   C. AWS VPC

   D. AWS GuardDuty

3. Which of the following services are offered completely free by AWS? (Select two answers.)

   A. AWS Identity and Access Management (IAM)

   B. AWS Elastic Beanstalk

   C. Amazon Simple Storage Service (Amazon S3)

   D. Amazon Relational Database Service (Amazon RDS)

   E. AWS Simple Notification Service (SNS)

4. Which feature of AWS Organizations enables you to combine the costs of each member account to take advantage of any volume discounts on offer?

A. Consolidated billing

B. AWS EC2 savings plan

C. AWS Control Tower

D. AWS IAM

5. Which of the following is required when creating an AWS Free Tier account?

A. A credit card

B. A bank statement

C. A passport or driving license

D. An invitation letter from Amazon

6. Which AWS service enables you to automatically set up a new landing zone in accordance with best practices?

A. AWS Landing Zone

B. AWS Control Tower

C. AWS Organizations

D. AWS Free Tier Account

7. Which feature of the AWS Organizations service enables you to combine AWS accounts in a container that has common workloads and then apply a common set of policies to those accounts?

A. AWS Control Tower

B. AWS Landing Zone

C. **Organization Units** (**OUs**)

D. **Service Control Policies** (**SCPs**)

Chapter 4

Figures

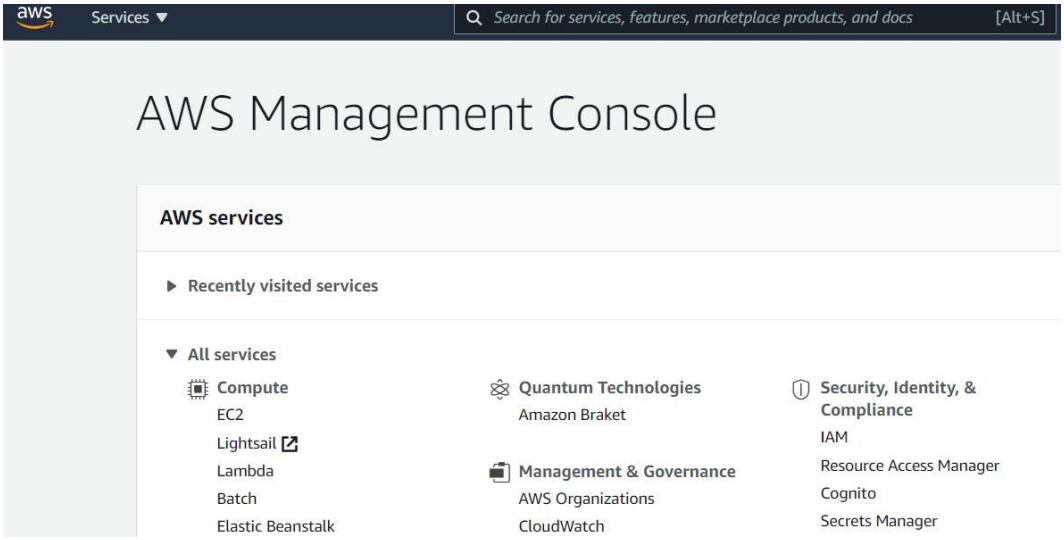

Figure 4.1 – AWS Management Console

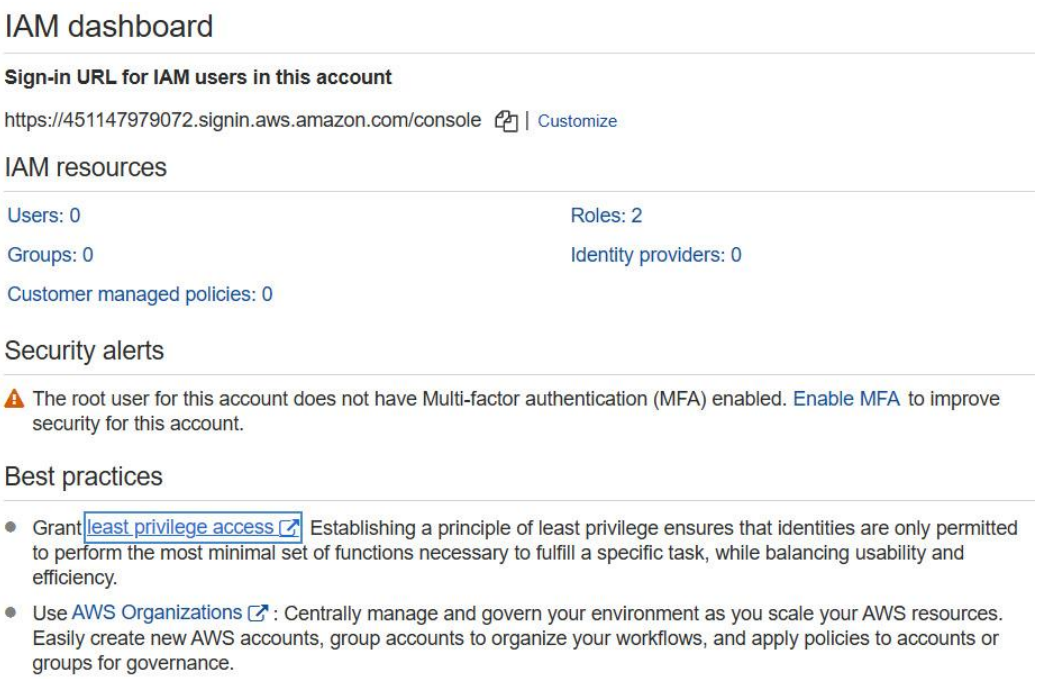

Figure 4.2 – IAM dashboard

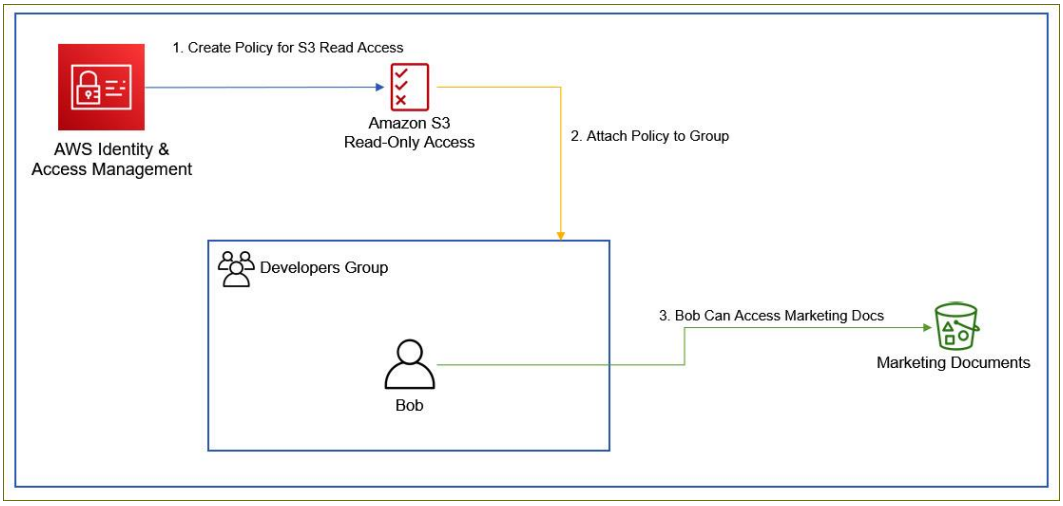

Figure 4.6 – Policy document attached to the developers group, granting Bob read access to the Marketing Documents bucket

Show Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Figure 4.7 – AWS managed policy: AmazonS3ReadOnlyAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::packt-marketing-docs"
        }
    ]
}
```

Figure 4.8 – Customer-managed policy restricting access to a single Amazon S3 bucket

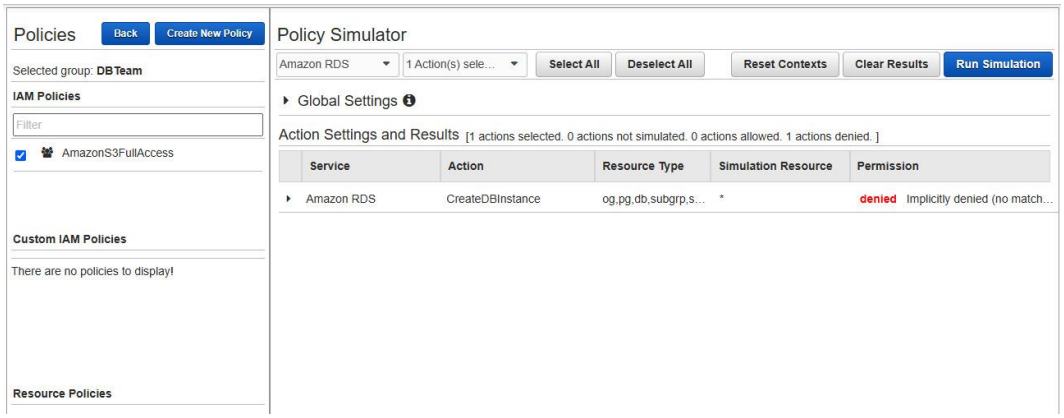

Figure 4.9 – Amazon policy simulator

Figure 4.13 – Links to download the appropriate AWS CLI installer for your operating system

Links

You can review the supported apps at https://aws.amazon.com/iam/features/mfa/.

Setting up MFA

Ensure that you have navigated to the IAM management console, then take the following steps:

1. On the IAM console, click on **Enable MFA**, under **Security alerts**:

Figure 4.3 – Security alerts

2. You are then presented with the **Security Credentials** page. Click on **Activate MFA.**

3. A pop-up dialog box is presented, and you need to select **Virtual MFA device**:

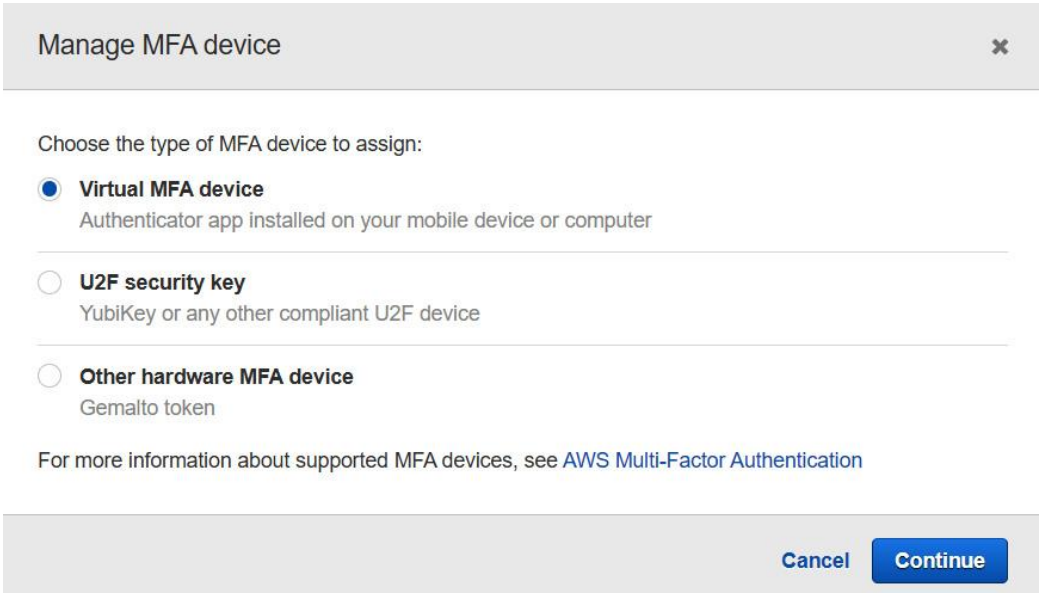

Figure 4.4 – Setting up a virtual MFA device

4. Click **Continue**.

5. You are then presented with the **Set up virtual MFA device** dialog box. You will have the option to scan a QR code to link your Google Authenticator app on your mobile phone with your AWS account. To get started, launch the Google Authenticator app on your phone and select the **Scan a QR code** option (you may have to tap the plus sign (**+**) first). This will activate your phone camera.

6. On the AWS console, in the **Set up virtual MFA device** dialog box, click **Show QR code** under list item number **2**:

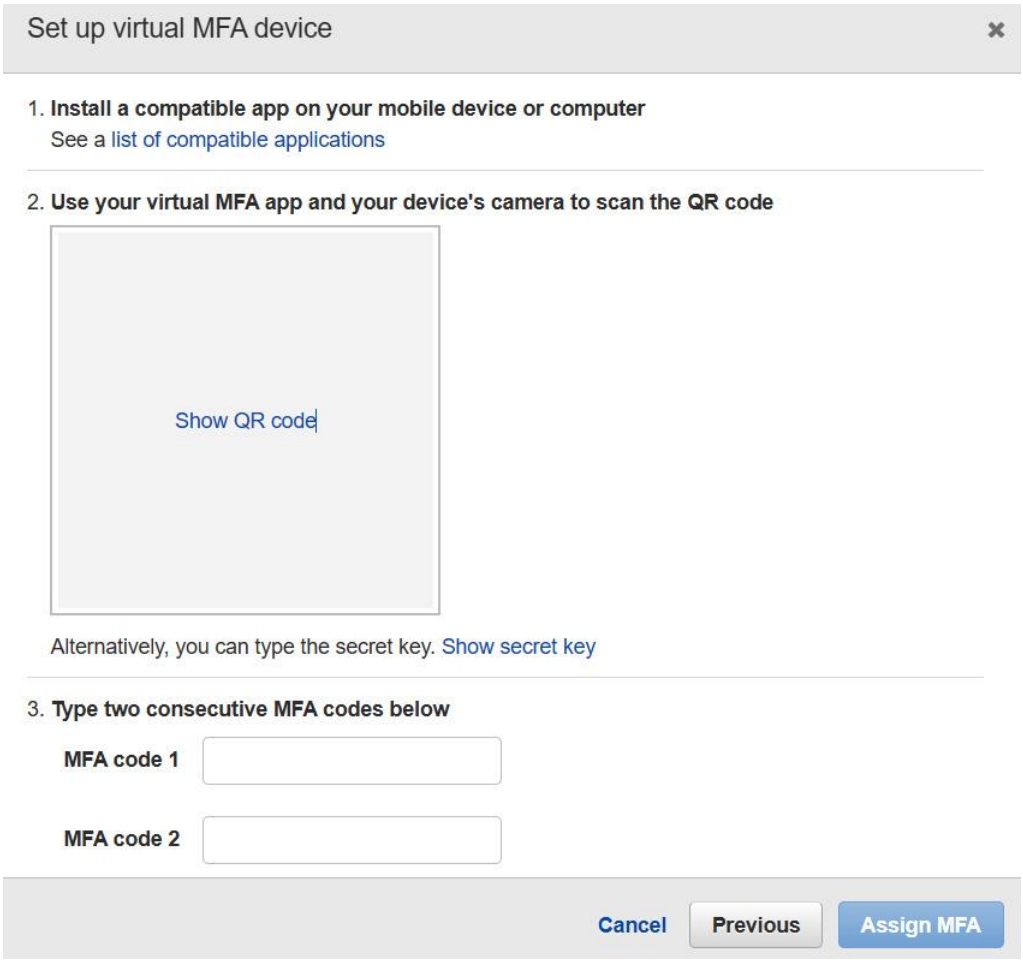

Figure 4.5 – Setting up a virtual MFA device

7. The QR code will be displayed. At this point, you need to position your phone camera so that it captures the QR code while in the Google Authenticator app.
8. Once the QR code is captured, you will be presented with an MFA code, which lasts for a few seconds. You will then need to type in the code in the textbox next to **MFA code 1**. Wait for the next code to be displayed and type that code into the textbox next to **MFA code 2**.
9. Finally, click **Assign MFA**.

Exercise 4.1 – creating an IAM group

In this exercise, you will create an IAM group for a development team that is going to require full access to Amazon S3:

1. Log in to your AWS account.
2. Click on the **IAM** link under the **Security, Identity, & Compliance** category on your **AWS Services** home page.
3. From the left-hand menu, click **Groups**.

4. Next, click on the **Create New Group** button.
5. You will then be presented with a step-by-step wizard. Provide a group name for your new group. For this exercise, type in `Developers`.
6. Click the **Next Step** button in the bottom right-hand corner of the screen.
7. You now need to attach a policy. You can create your own customer-managed policies but for the purposes of this exercise, type `S3` in the **Policy Type** filter search box. This will narrow down the available policies that relate to Amazon S3.
8. Tick the checkbox next to the **AmazonS3FullAccess** policy.
9. Click the **Next Step** button in the bottom right-hand corner of the screen.
10. Finally, click the **Create Group** button in the bottom right-hand corner of the screen.

You will now see that your group has been created and listed under **Group Name**. Now that you have created a group, you can proceed to create an IAM user and add it to the group. This allows you to manage multiple users more effectively. In the next exercise, we will create an IAM user and add it to the developers group.

Exercise 4.2 – creating an IAM user

Now that you have created a developers group, you can add your developers to this group. To illustrate this, we will create a new user, John. John is one of our senior developers at Packt and we would like to ensure that he is a member of the developers group, which will give him full access to Amazon S3:

1. In the IAM dashboard, click on **Users** from the left-hand menu.
2. Click the **Add user** button.
3. In the **User name** textbox, type in `john` (all lowercase).
4. Next, you need to select the type of access you want to grant John. John is a developer and will require both console access and programmatic access. This means that sometimes, John will use the web-based console to configure resources in Amazon S3, and at other times, he may use the CLI. For this exercise, tick both boxes – **Programmatic Access** and **AWS Management Console access**.
5. To access the AWS account via the console, you need to create a password for the user. For `john`, you can have AWS automatically generate a password for you or you can create a custom one yourself. Select **Custom password** and choose a complex password of your choice. Type that password in the textbox provided.
6. An additional setting, **Require password reset**, enables you to force your IAM users to change their password at the next login. That way, you will not know what their password is

when they change it and it is best practice to follow. For the purposes of this lab, disable this checkbox for now.

7. Click the **Next:Permissions** button in the bottom left-hand corner of the screen.

8. You now have the option to set permissions for the user. As we have already created a group with the right set of permissions attached to it, we simply need to make this user a member of the group. For this exercise, under **Add user to group**, tick the box next to the **Developers** group and click the **Next:Tags** button in the bottom right-hand corner of the screen.

9. Tags are key-value pairs that you can attach to any resource. You can attach up to 50 tags to each resource and they enable you to classify your resources better. You can then use tags to understand cost allocation and to identify and manage your resources. Tags can include user information, such as an email address, or can be descriptive, such as a job title. For this exercise, set a single tag, with the key set to `Name` and the value set to `John`.

10. Click the **Next:Review** button in the bottom right-hand corner of the screen.

11. You can now review all your settings for the user and once satisfied, go ahead and click the **Create user** button in the bottom right-hand corner of the screen.

12. You are now presented with a **Success** screen, which confirms that the user has been created. You are also informed of the option to download your access keys. Access keys are like usernames and passwords and comprise an access key ID (similar to the username) and the secret access key (similar to the password). Access keys are used to grant programmatic access via the AWS CLI or using the AWS SDKs. It is important that you download these keys now and keep them safe on your computer. If you move away from this screen, the secret access key (such as the password) is no longer visible, and you would need to recreate the keys. For this exercise, ensure that you download the keys by clicking on the **Download .csv** button. Store the `.csv` file.

13. You will also note that you have been provided with a special link to log in to your AWS Free Tier account using an IAM user account. The AWS account sign-in page for IAM users is slightly different from that of the root user. This is because when you sign in as an IAM user, you need to specify the AWS account ID you are trying to sign into. In our example, we have a link like this:

    ```
    Users with AWS Management Console access can sign-in
    at: https://111222333444.signin.aws.amazon.com/console
    ```

    The series of numbers just before `.signin` represents your AWS account ID.

14. Click the **Close** button in the bottom right-hand corner of the screen to exit from the user setup wizard.

We have now created a user who represents a developer in our organization and we have added the user to the developers group. In the next exercise, you will learn how to access your AWS account as the IAM user you created previously.

Exercise 4.3 – logging in to your AWS account as an IAM user

In this exercise, we log out of the AWS account as the root user and re-login as the IAM user you just created. If you did not make a note of the special sign-in link, you will need to know what your AWS account ID is. You can easily discover this by clicking on your account name in the top right-hand corner of your web-based management console and noting the account ID:

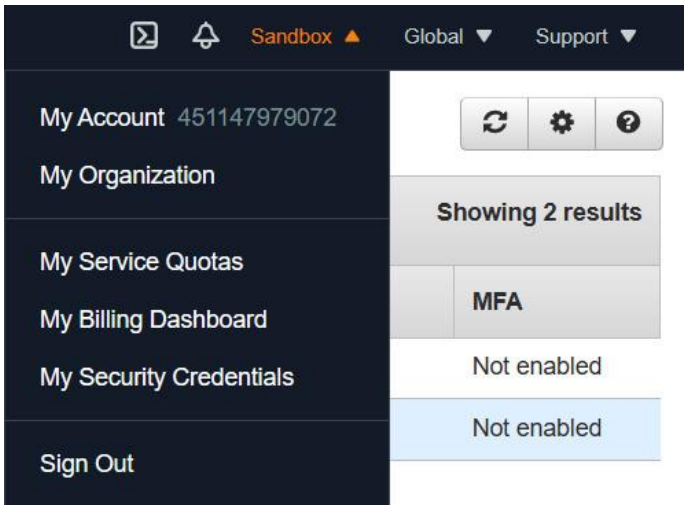

Figure 4.10 – Drop-down box when clicking on the account name to discover the account ID, which is shown after My Account

Now that you have the account ID (or you can make a note of the sign-in URL previously discussed), we can proceed to log in as the IAM user you created earlier:

1. Sign out of the AWS account (remember, you are currently signed in as the root user).
2. You will be taken to the AWS console home page where you can click the **Log back in** button or the **Sign in to the Console** button.
3. Clicking on either of these will take you to the AWS sign-in page.
4. Click on **IAM user** and provide the account ID in the available textbox:

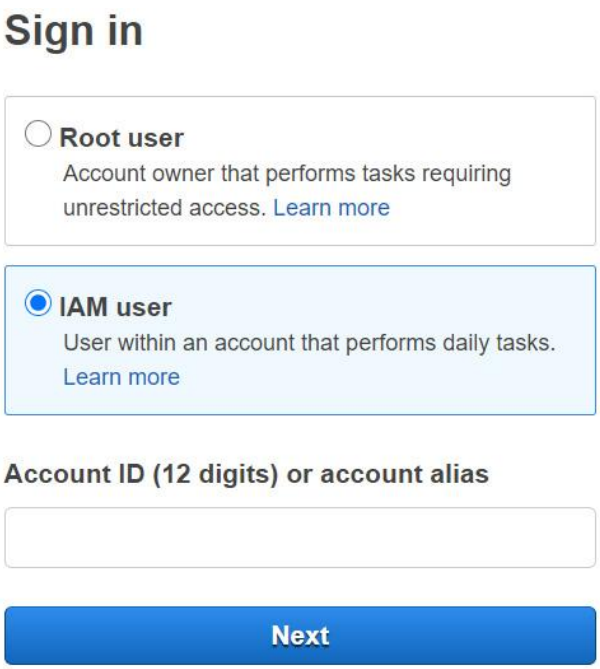

Figure 4.11 – AWS signing page

5. Once you have provided the account ID, click **Next**.
6. Now, provide your username, in this case, `john`, and the password you chose when you created the user.
7. You will now be logged in to the AWS Management Console as our developer, John. You will note that your username is displayed in the top right-hand corner of the screen:

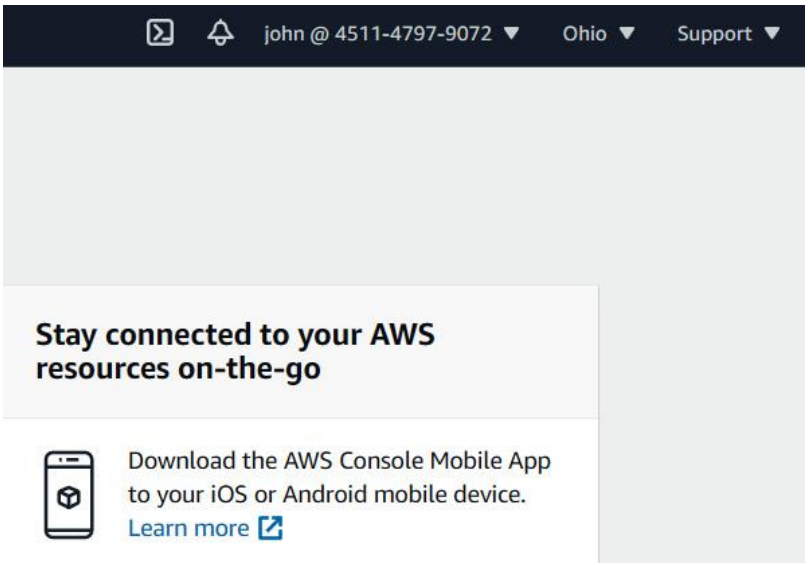

Figure 4.12 – IAM user John has successfully logged in to this AWS account

In this section, we completed a series of exercises using the AWS IAM service. We demonstrated how to create IAM groups and users and how to log in to the AWS Management Console as an IAM user.

In the next exercise, you will learn how to access the AWS platform using the Amazon CLI on a Windows computer.

Exercise 4.4 – accessing the AWS platform using the AWS CLI on a Windows computer

Once you have installed the AWS CLI tools on your Windows machine, the next step is to configure it to access your AWS account as the IAM user you created earlier:

1. Open the credentials file, which you downloaded earlier when you created the IAM user `john`. This file has the access keys for your user, which comprises the **access key ID** and the **secret access key**.
2. On your Windows desktop, click on the **Start** button and search for Command Prompt by typing in `CMD`:

Figure 4.14 – Command Prompt on a Windows computer

3. At the prompt, type in `AWS configure` to start the configuration process.
4. You will then be prompted to enter the **AWS access key ID**, followed by the **AWS secret access key**. These keys are in your credentials document that you downloaded earlier.
5. For **Default region name**, type in `us-east-1`.
6. For **Default output format**, leave this blank and press *Enter*:

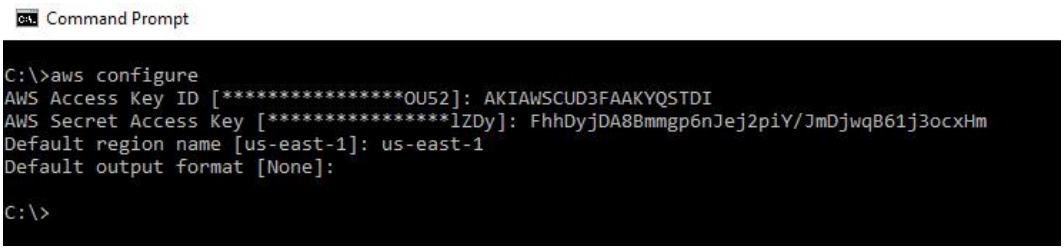

Figure 4.15 – Configuring the AWS CLI with access key ID and secret access keys

7. Your AWS CLI tool has now been configured with John's credentials.
8. You can try running a command such as `aws s3 ls`. This command lists out any Amazon S3 bucket you have in your account. If you have not created any buckets yet, you will just have the prompt return. In my case, I have already got one bucket in my account as you can see in the following screenshot:

Figure 4.16 – Configuring the AWS CLI with access key ID and secret access keys

In this section, we discussed the necessary steps required to configure your AWS CLI tool, so that you can access your AWS account as an IAM user using Command Prompt on a Windows machine. You can also use Terminal on a Mac or Linux computer to complete the same tasks. You would need to install the appropriate tool for your operating system.

Using the CLI can be very efficient, especially if you are trying to perform repeat tasks as you can also create scripts to automate the whole process.

You should try and avoid using the root account to perform any day-to-day operations in your AWS account. Instead, you must log in with an IAM user account that has only the necessary privileges to carry out the task at hand. This is known as following the principle of least privilege.

In the next exercise, you will create another IAM user account that you will use for all the exercises in the upcoming chapters.

Exercise 4.5 – creating an IAM user with administrative privileges

In this exercise, you will create another IAM user account that you will use to log in to your AWS account. This IAM user will be provided with full administrative access to help you work through the upcoming exercises easily, although in the real world, you would want to restrict permissions to only the job function of the users in question. By getting used to logging in as an IAM user, you will build a habit of avoiding the use of the root user credentials for your day-to-day tasks:

1. Ensure that you are logged in to your AWS account as the root user (the email address and password combination you used to create your AWS account).
2. Navigate to the IAM dashboard.
3. From the left-hand menu, click on **Users**. Next, from the right-hand pane, click **Add user**.

   You will be redirected to the **Add user** wizard page.
4. For the username, type in `Alice`. Throughout the rest of this guide, you will be logging in as `Alice` to carry out all upcoming exercises.
5. Under **Select AWS access type**, select both **Programmatic access** and **AWS Management Console access**.

6. For **Console password**, select the **Custom password** option and provide a complex password of your choice.
7. Uncheck the box next to **Require password reset** and click the **Next: Permissions** button.
8. In step 2, under **Set permissions**, select the **Attach existing policies directly** option. This will allow you to attach an inline policy to Alice's account alone.
9. From the list of policies provided, select the checkbox next to **AdministratorAccess** as per the following screenshot:

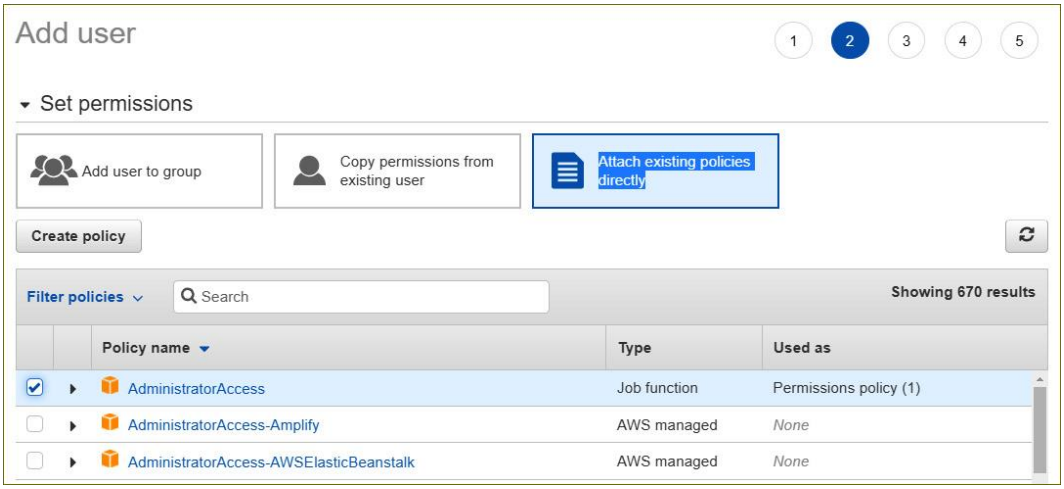

Figure 4.17 – IAM user (Alice) with administrator access permissions

10. Click the **Next: Tags** button at the bottom of the screen.
11. In step 3, under **Add tags (optional)**, provide a key-value pair where the key is set to `Name` and the value is set to `Alice`.
12. Click the **Next: Review** button.
13. Next, click the **Create user** button.
14. You will then be prompted to download the `.csv` file containing Alice's access keys and secret access keys. Download the file and ensure you keep it in a folder on your computer that you can easily access. Once downloaded, go ahead and click the **Close** button.
15. Your IAM user Alice is now ready to log in. Going forward, you will need to log in as the IAM user Alice for all upcoming exercises. Ensure you also make a note of either the special sign-in link for your AWS account or the AWS account ID, which you will need to log in as an IAM user.

In this exercise, you created an IAM user account that you will use to log in to your AWS account and perform all the upcoming exercises. In the next section, we'll review a summary of this chapter.

Questions

Here are a few questions to test your knowledge:

1. You wish to deploy a dev and test environment on AWS. You want to ensure that your developers can access your AWS account using a highly secure authentication process and follow best practices. Which of the following two configuration options will help ensure enhanced security? (Choose two answers)

   A. Configure your IAM accounts with MFA.

   B. Configure your IAM password policy with complexity rules.

   C. Ensure you encrypt your EBS volumes.

   D. Create RDS databases with Multi-AZ.

   E. Provide the root account credential details to your developers.

2. Your developer is working from home this weekend and needs to access your AWS account using the CLI to configure your RDS database from their local computer. Which type of IAM credentials would they need to configure the AWS CLI tool on their machine?

   A. IAM username and password

   B. Access key IDs and secret access keys

   C. Access keys and secret ID

   D. HTTPS

3. Which AWS service enables you to troubleshoot your IAM policies and identify the sets of permissions that may be denying access to a given AWS service?

   A. IAM policy simulator

   B. CloudWatch

   C. CloudTrail

   D. IAM policy manager

4. Which of the following AWS services is a better option to securely grant your application running on an EC2 instance access to a backend database running on Amazon RDS?

   A. Access keys

   B. IAM role

   C. IAM group

   D. Security group

5. Which format are IAM policy documents written in?

   A. JSON

   B. YAML

   C. XML

   D. JAVA

6. What best practice strategy should you follow when assigning permissions to IAM users and groups?

   A. Follow the principle of least privilege.

   B. Follow the principle of most privilege.

   C. Follow the ITIL principles.

   D. Follow the GDPR principle.

7. Which IAM service enables you to effectively manage users by creating a collection of them based on their job function and assigning them permissions according to their roles to the entire collective?

   A. IAM groups

   B. IAM policies

   C. IAM collection

   D. IAM roles

8. Which feature of IAM enables you to use your existing corporate Active Directory user credentials to log in to the AWS Management Console and therefore offer an SSO service?

   A. Identity federation

   B. IAM user database

   C. Active Directory users and computers

   D. MFA

9. Which AWS service enables you to generate and download a report that lists your IAM users and the state of their various credentials, including passwords, access keys, and MFA devices?

   A. AWS policies

   B. AWS Explorer

   C. Credentials report

D. User report

10. Which AWS service is responsible for assigning and managing temporary credentials to entities that assume an IAM role?

A. AWS Password Manager

B. AWS Security Token Service

C. AWS Credentials Manager

D. AWS Credentials Report

Chapter 5

Figures

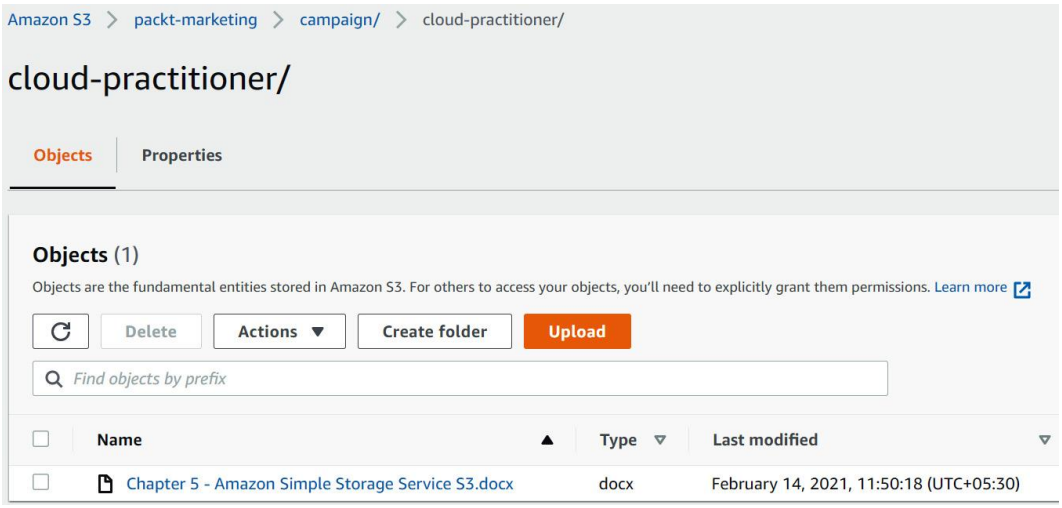

Figure 5.1 – Amazon S3 prefixes and delimiter example

```
{
  "Id": "Policy1613373871314",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1613373870082",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::packt-marketing/*",
      "Principal": "*"
    }
  ]
}
```

Figure 5.2 – Bucket policy example granting anonymous access to the contents of the 'packt-marketing' S3 bucket

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
              "arn:aws:s3:::packt-marketing",
        "arn:aws:s3:::packt-marketing/*"
      ],
      "Condition": {
         "NotIpAddress": {"aws:SourceIp": "w.x.y.z/c"}
      }
    }
  ]
}
```

Figure 5.3 – Bucket policy defined with a conditional statement

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA	S3 Glacier	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99.9%	99.9%

	S3 Standard	S3 Intelligent-Tiering	S3 Standard-IA	S3 One Zone-IA	S3 Glacier	S3 Glacier Deep Archive
Availability Zones	≥3	≥3	≥3	1	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128KB	128KB	40KB	40KB
Minimum storage duration charge	N/A	30 days	30 days	30 days	90 days	180 days
Retrieval fee	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	Milliseconds	milliseconds	milliseconds	select minutes or hours	select hours

Figure 5.4 – S3 storage class performance and key attributes

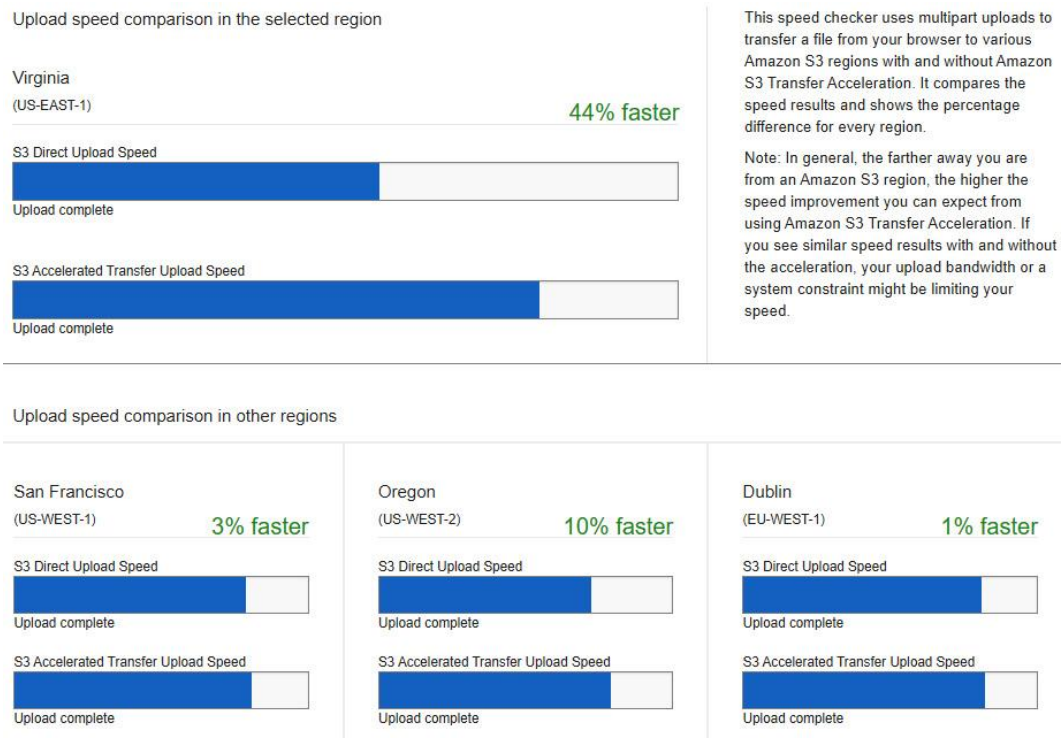

Figure 5.5 – Amazon S3TA speed test

Table

Storage class or tier	Expedited	Standard	Bulk
S3 Intelligent-Tiering Frequent and Infrequent Access tier	1–5 minutes	3–5 hours	5–12 hours
Intelligent-Tiering Archive and Deep Archive Access tier	Not available	Within 12 hours	Within 48 hours

Table 5.1 – Retrieval times for S3 Glacier, Deep Archive, and S3 Intelligent-Tiering archive classes

Links

You can review all **frequently asked questions** (**FAQs**) for Amazon S3 here: https://aws.amazon.com/s3/faqs/.

Virtual hosted-style endpoints: https://just-desserts.s3.amazonaws.com/blueberry-muffin.txt.

A) `s3-website` dash (-) Region—`http://bucket-name.s3-website-Region.amazonaws.com`. For example, our recipe will be available at http://just-desserts.s3-website-us-east-1.amazonaws.com/blueberry-muffin.txt.

B) `s3-website` dot (`.`) Region—`http://bucket-name.s3-website.Region.amazonaws.com`. For example, our recipe will be available at http://just-desserts.s3-website.us-east-1.amazonaws.com/blueberry-muffic.txt.

You can try out the speed test at https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html

Exercise 5.1 – Setting up an Amazon S3 bucket

In this exercise, we will create an Amazon S3 bucket and upload an object to it. More specifically, we will upload a single web page document and test access to it after the upload. Since we plan to later *use* this bucket to host a static website and make content accessible to anyone on the internet, you will need to disable the **Block Public Access** setting, as discussed in the access permissions settings earlier in this chapter. Proceed as follows:

1. On your computer, create a new file using a standard text editor of your choice (Notepad on Windows or TextEdit on Mac).

2. Add the following lines of code to the document:

```
<html>
<title>Blueberry Muffin Recipe</title>
<Body>
<h1>Blueberry Muffin Recipe</h1><p>
Bake the ultimate blueberry muffins for your guests and loved
ones. This recipe shows you how to create cafe-style blueberry
muffins in your own kitchen.</p>
<p><strong>Ingredients:</strong></p>
<ul><li>100g fresh <span style="color: rgb(85, 57,
130);"><strong>blueberries</strong></span></li>
<li>300g flour</li>
<li>150g granulated sugar</li>
<li>1 tsp. vanilla</li>
<li>60 ml vegetable oil</li>
<li>50g of butter</li>
</ul><p><br></p>
</body>
</html>
```

   The preceding code is also available in our GitHub repository for this book https://github.com/PacktPublishing/AWS-Certified-Cloud-Practitioner-Exam-Guide, and you can simply download the `index.html` file to your desktop as well.

3. Next, save it with a filename of `index` with a `.html` extension—so, the filename with the extension should be `index.html`. This will create a simple web page object for you. You

may need to set the **Save as type** option to **All Files**, as illustrated in the following screenshot:

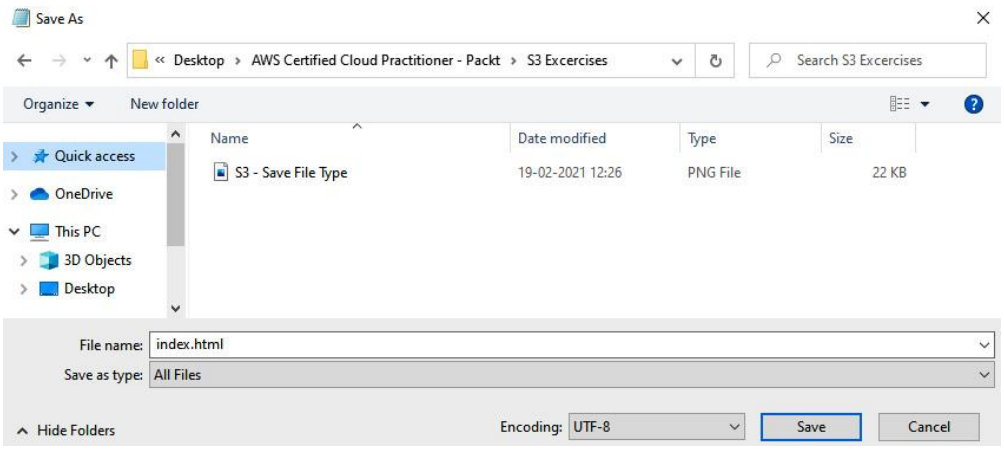

Figure 5.6 – Saving a file with a .html extension to create a web page

4. Next, log in to your AWS account as the IAM user, **Alice**.
5. Navigate to the Amazon S3 console.
6. Click **Create bucket**, as illustrated in the following screenshot:

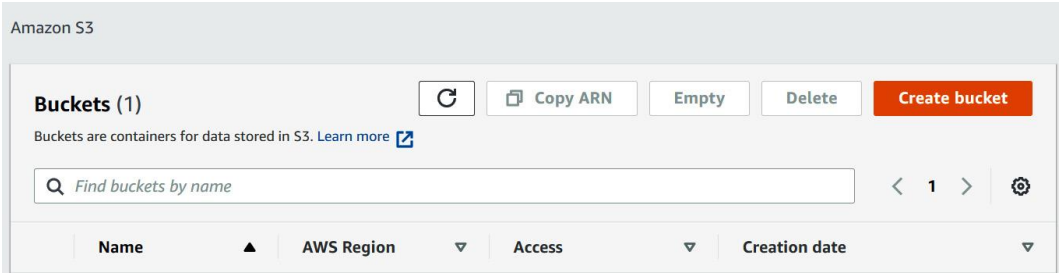

Figure 5.7 – List of buckets

7. For the name of the bucket, type in your name followed by a hyphen (-) and the word `webpage`. Make sure there are no spaces in the name and that all lowercase letters are used. Assuming that the name you have chosen has not already been taken by another customer of AWS, you should be able to use this bucket name. If you get an error when you create the bucket, stating that the name is not available, you will simply need to choose a different name.
8. For **AWS Region**, select `us-east-1`.
9. Next, under the **Block Public Access settings for bucket** sub-heading, uncheck he box for **Block all public access**. Note that for general use cases, you do not want to unblock public access unless your use case demands it, such as when trying to configure static website hosting, which we will look at later in *Exercise 5.4*. If you do not need anonymous access such as that from end users on the public internet, you must always correctly configure your

permissions using bucket policies, ACLs, or access point policies, to ensure you leverage the **principal of least privilege** (**PoLP**).

10. Next, check the box to state that you acknowledge that the preceding settings could make the bucket and its objects publicly accessible, as illustrated in the following screenshot:

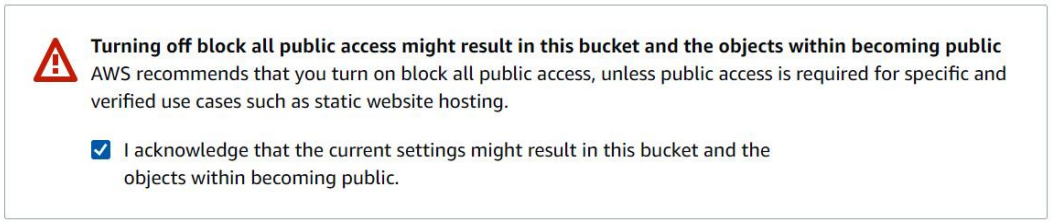

Figure 5.8 – Turning off block all public access on your bucket

11. Leave all other settings as default and click on the **Create bucket** button at the bottom of the screen. Your Amazon S3 bucket has now been created.

12. Next, in your list of buckets in the main S3 console, select the bucket you just created. This will take you to the current list of objects in the bucket. You will note that there will be none at present.

13. You will notice an **Upload** button. Click on this button and you will have the option to add files and folders, as per the following screenshot:

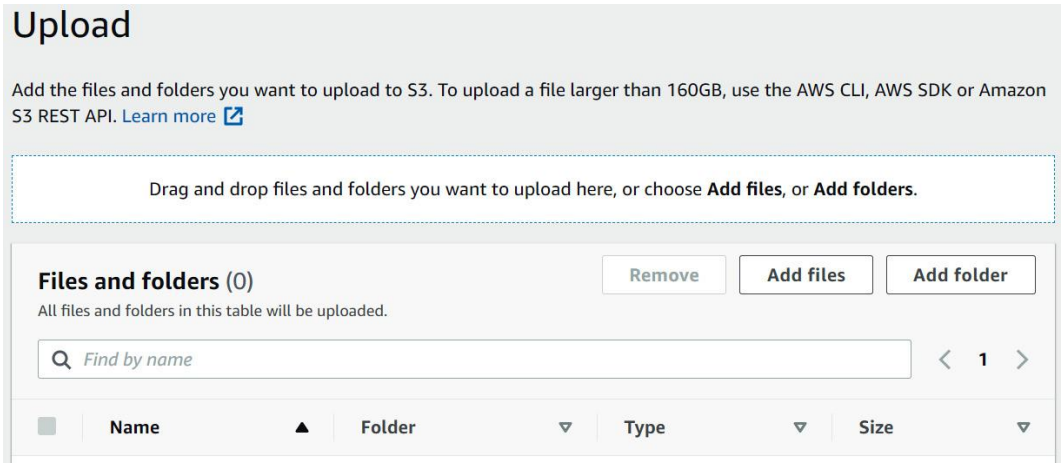

Figure 5.9 – Uploading object to your bucket

14. Add the `index.html` file you created/downloaded earlier.

15. Scroll toward the bottom of the screen and click the **Upload** button.

16. Your file will be uploaded.

17. You will note a green banner at the top of the screen to say that the upload has been successful. Now, go ahead and click **Exit**.

18. You are then presented with the contents of the bucket you just created.

19. You can now click on the `index.html` file in the **Objects** list, which will take you to the Amazon S3 properties page of the file itself.

20. Note that each object has its own URL accessible from the internet (as long as the permissions are correctly set), as we can see in the following screenshot:

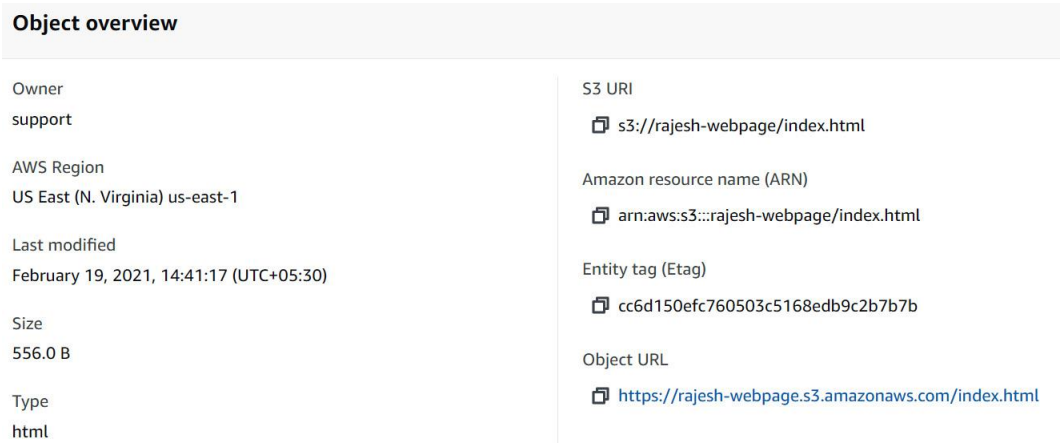

Figure 5.10 – Uploading the index.html object to your bucket

21. If you try to click on this object URL to open it up in another browser window, you will find that you cannot access it. Instead, you get an **Access Denied** error message. This is because access to an object via its URL has the same effect as trying to anonymously read the object over the public internet.

Although we disabled the **Block all public access** setting earlier, your buckets and objects still need an explicit `Allow` rule to grant access to them. You could click on the **Permissions** tab of the object itself and set up an ACL to enable public access for this object. However, as discussed previously, using bucket policies is a better option as these offer more features and granular control.

In the next exercise, we will set up a bucket policy to see how we can allow public access to this file.

Exercise 5.2 – Configuring public access to S3 buckets

In this exercise, we will configure the Amazon S3 bucket with a **bucket policy** (resource policy) that will allow users on the public internet to be able to access and read the `index.html` web page you created earlier.

Remember that you could choose to restrict access to only a set of known users—for example, if you wanted only IAM users in your AWS account to have access to the objects. You can also configure cross-account access, in which you define principals that belong to another AWS account and grant them specific levels of access.

In this exercise, we want to grant anonymous access to the `index.html` page because ultimately, we will be building out a static website hosting service using this bucket in later exercises. Proceed as follows:

1. Navigate back to the S3 console and click on the bucket you just created, as illustrated in the following screenshot:

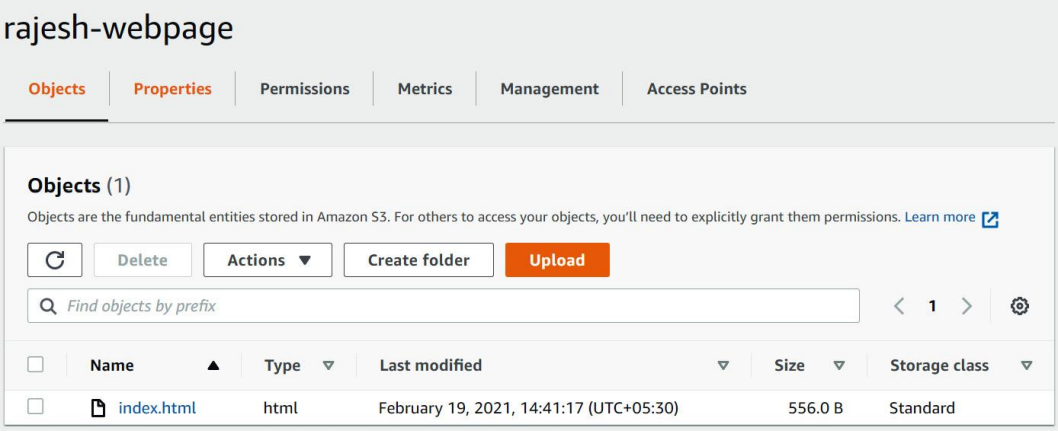

Figure 5.11 – Successful upload

2. Click on the **Permissions** tab.
3. You will note that the **Block public access** has been disabled and is in an **Off** state.
4. Scroll further down until you get to **Bucket Policies**, and then click **Edit**.
5. Add the following policy, replacing the values in the placeholder `Your-Bucket-Name` with the name of your S3 bucket:

```
{
  "Id": "Policy1613735718314",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1613735715412",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::Your-Bucket-Name/*",
      "Principal": "*"
    }
  ]
}
```

6. Click **Save Changes**. If you copied the policy correctly, the policy validator will not throw up any errors.

7. You should then get a confirmation that the policy has been saved and, more importantly, you will note that the bucket's contents are now publicly accessible, as illustrated in the following screenshot:

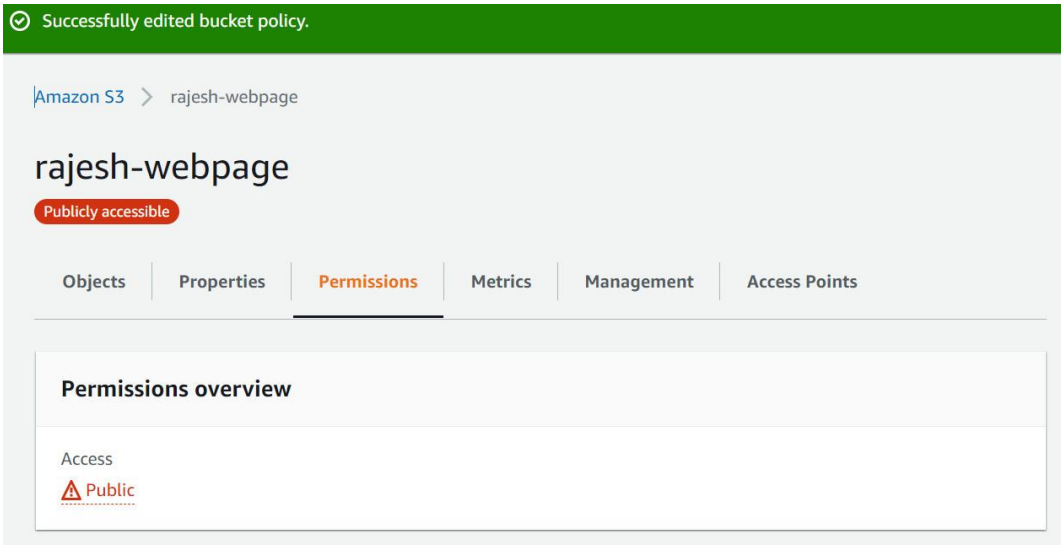

Figure 5.12 – S3 Bucket permissions tab

8. Next, click on the **Objects** tab again.
9. Click on the `index.html` file to open its **S3 Properties** pane.
10. Right-mouse click on the object URL and open it in a new browser tab.
11. You should find that the web page is now accessible from your browser, as illustrated in the following screenshot:

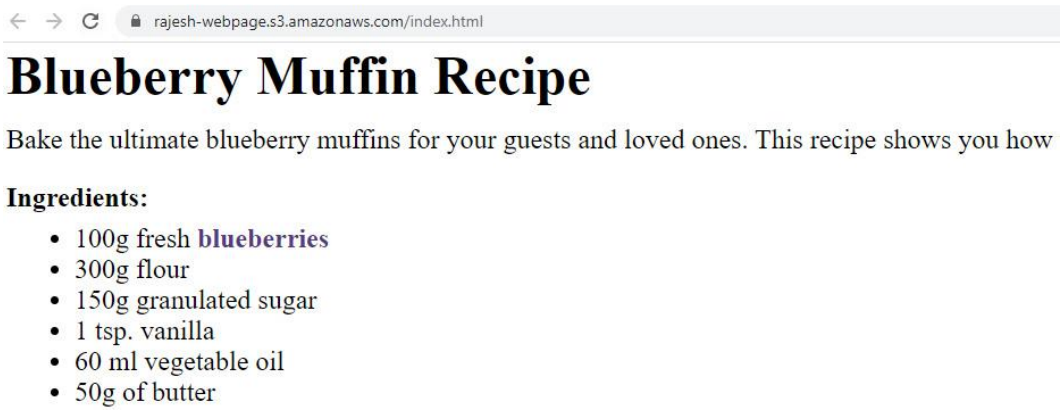

Figure 5.13 – Your index.html page in a browser window

So far, we have disabled block public access on this bucket as we will eventually be configuring it for static website hosting. In this exercise, we also uploaded the object, `index.html`, which is a recipe document written in HTML code.

In the next exercise, you will learn how to configure versioning on your bucket. Versioning will help you create previous copies of an object so that new uploads of updated content for the same object

are stored as new versions of the object. This will enable you to prevent against accidental changes to your objects by being able to restore a previous version, as we will see in the upcoming exercises.

Exercise 5.3 – Enabling versioning on your bucket

In this exercise, we will enable versioning on the Amazon S3 bucket. As you update existing objects with newer versions, you can rest assured that if you need to revert to an older version, those versions will still exist in your bucket. Obviously, if you try to delete a specific version of the object itself, then it will be purged from the S3 platform. However, enabling versioning can help prevent against accidental deletions and overwrites. Proceed as follows:

1. Navigate back to the S3 console.
2. Click on the bucket you created earlier in *Exercise 5.1*.
3. Click on the **Properties** tab.
4. You will see an **Edit the Bucket Versioning** option to edit the state. At present, the versioning will be set to **disabled**. Note that once again you can suspend versioning actions, but you will not be able to disable them.
5. Click **Edit** in the **Bucket Versioning** section.
6. Select **Enable**.
7. Click **Save Changes**.

Let's try to test the versioning feature next, as follows:

8. Navigate to the location where you saved the `index.html` web page on your computer. Open the file with your text editor using Notepad or TextEdit (for Mac).
9. Replace the word `Blueberry` in the existing `<H1>` tag within the document to `Chocolate`.
10. Save the file without changing the format or extension.
11. Navigate back to your Amazon S3 console in your AWS account and click on the bucket you created earlier.
12. Click on **Objects**, as illustrated in the following screenshot:

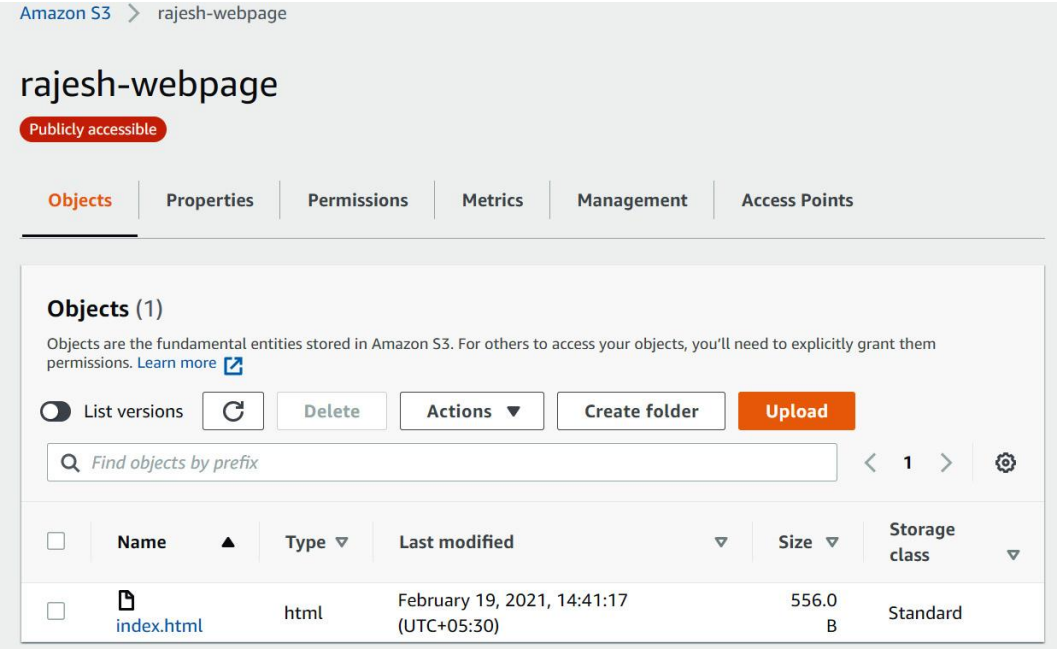

Figure 5.14 – List of objects in your Amazon S3 bucket

13. Click **Upload**.
14. Click **Add Files**.
15. Select the same `index.html` file you updated moments ago and click **Upload**.
16. Click **Exit**.
17. Click on the `index.html` fileagain to open up its **S3 Properties** window.
18. Under **Object URL**, right-mouse click on the URL and open in a new browser window.
19. You should find that the web page has been updated with the word **Chocolate**, as illustrated in the following screenshot:

Figure 5.15 – Your index.html page showcasing the recipe

20. In the Amazon S3 management console, click on the **Versions** tab, as illustrated in the following screenshot:

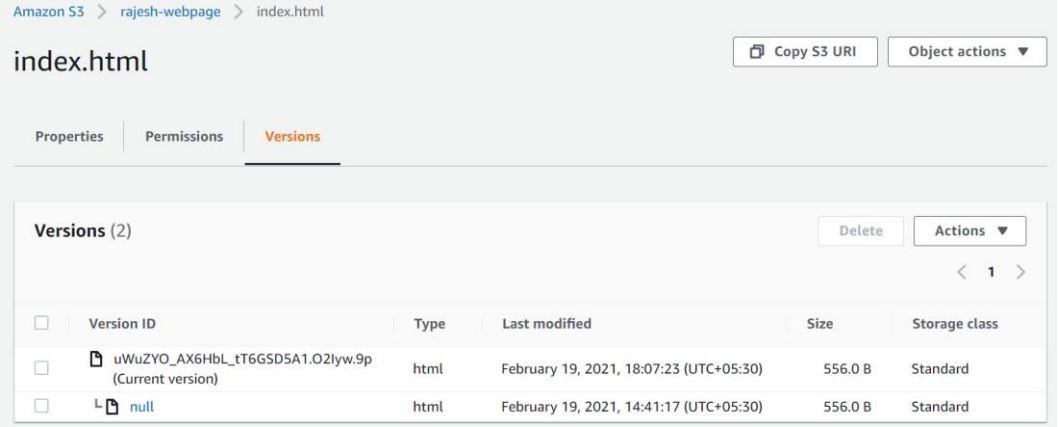

Figure 5.16 – Bucket version tab

21. Note that there are two versions—the original version, which has a version ID of `null`, and a newer version with a **string of letters and numbers**, called **Current version**. The reason why the first version has a version ID of `null` is because it was created/uploaded to the bucket before we enabled versioning. Going forward, all new updates to this file will be assigned a new version ID, allowing you to preserve older versions if you ever need to access them again.

In this exercise, you learned how to configure versioning on your bucket. You were able to upload and manage multiple versions of the same object, and you discovered how unversioned objects have a version ID of `null`, whereas versioned objects have a version ID comprised of a series of characters unique to that version. You also discovered how to display a list of available versions of your objects in a version-enabled bucket.

Exercise 5.4 – Setting up static website hosting

In this exercise, we will configure the bucket to host a static website. When configured with a static website hosting service, the bucket will be configured with a website endpoint that you can distribute to your users, who can then access all the pages (assuming they are linked) using the standard HTML protocol.

To configure your bucket for static website hosting, you need a minimum of two files— an `index.html` file and an `error.html` file. An error file is simply a file that the S3 static website hosting service will redirect to if there is a problem with the `index.html` file—for example, if it cannot find the `index.html` page. You could use the `error.html` file to broadcast the fact that perhaps the site is under maintenance. Proceed as follows:

1. Create a new HTML file using your text editor as before (either Notepad on Windows or TextEdit on a Mac). However, in this file, simply add a line of text along the lines of `This site is under maintenance`.

2. Save the file as `error.html`, making sure to set the file types to **All Types** if you are using a Windows machine.

3. Navigate back to the S3 console and click on your S3 bucket.

4. Click on **Properties** and then scroll toward the bottom of the page, until you find the **Static website hosting** section heading.
5. Click **Edit** and select the **Enable** option.
6. For **Hosting type**, select **Host a static website**.
7. Under the **Index document** sub-heading, type the name of your index file—in this case, `index.html`.
8. Under the **Error document** sub-heading, type the name of your new error file—in this case, `error.html`.
9. Leave all the remaining settings at their defaults and click **Save changes** at the bottom of the page.
10. Next, click on the **Objects** tab.
11. Click **Upload** and click **Add files**.
12. Select the `error.html` file and click **Upload**. You should then see a screen like this:

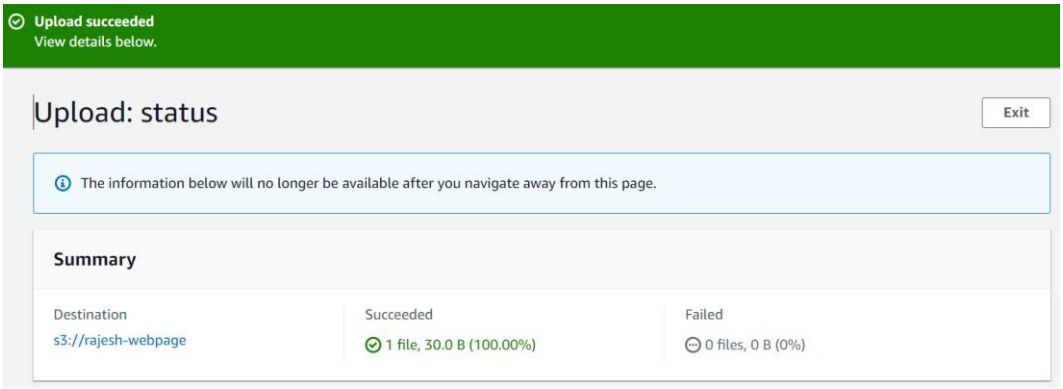

Figure 5.17 – Upload of updated index page to your bucket

13. Click **Exit**.
14. At this stage, your bucket has been configured for static website hosting. To test it, you need to access your website via the S3 website URL endpoint.
15. In the S3 console, while still viewing the contents of the buckets (under **Objects**), click on the **Properties** tab again.
16. Scroll down till you reach the **Static website hosting** section, and you will note the URL is provided under the **Bucket website endpoint** heading, as illustrated in the following screenshot:

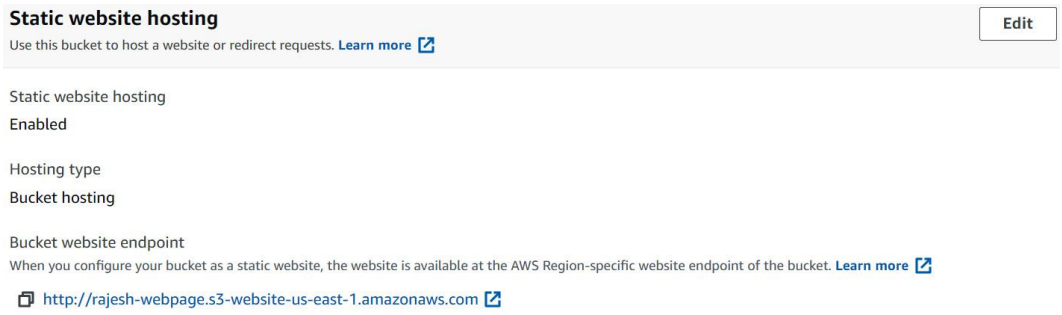

Figure 5.18 – Enabling static website hosting on your bucket

17. Navigate to the provided URL in a new browser window, and you should find that the website opens with the recipe web page, as illustrated in the following screenshot:

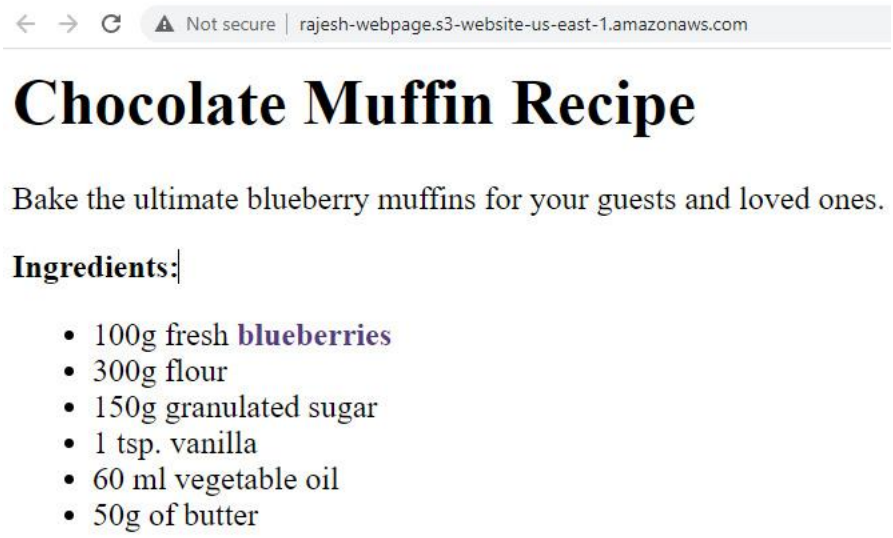

Figure 5.19 – Updated index.html page with the wrong heading (Chocolate)

18. As you will note, the recipe is for a blueberry muffin, but the heading has changed to **Chocolate**. Assuming that this was an error in the update, we can easily revert to the previous version of this web page because we have already configured the bucket for versioning.

19. Navigate back to the Amazon S3 bucket so that you are looking at the actual contents of the bucket under the **Objects** tab, as illustrated in the following screenshot:

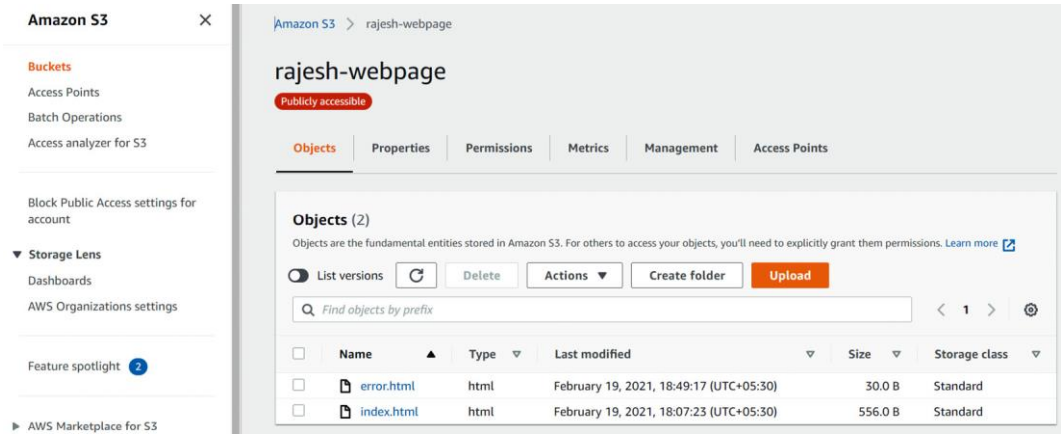

Figure 5.20 – List of updated objects in your bucket

20. Notice the **List versions** toggle just below the **Objects** sub-heading.

21. Click this toggle switch to list out all versions of all objects in your bucket, as illustrated in the following screenshot:

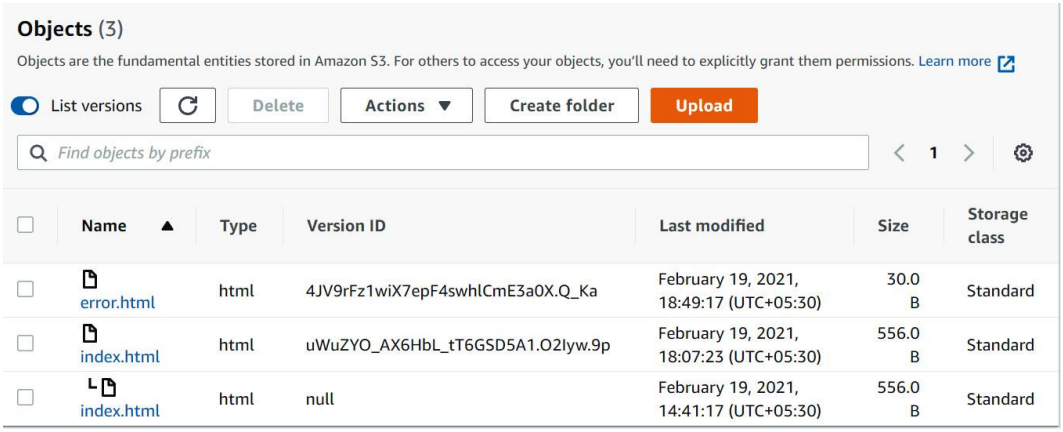

Figure 5.21 – List of objects and their individual versions.

22. As you will note, there are two versions of the `index.html` page. The latest version has got a version ID and contains an incorrect recipe heading.

23. Click on the checkbox to select this version and then click the **Delete** button.

24. You are then prompted to confirm your delete request by typing in the phrase `permanently delete` in the provided textbox, as illustrated in the following screenshot:

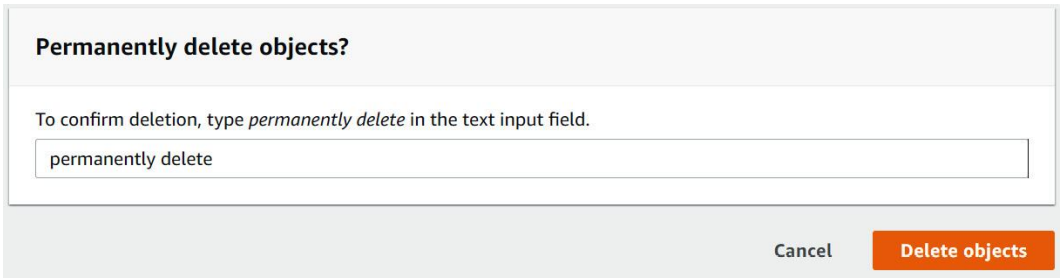

Figure 5.22 – Deleting incorrect version of the index.html page

25. Next, click **Delete objects**.
26. Click **Exit**, and you will note that the version has now been deleted.
27. Click on **Properties** again and then scroll down to the **Static website hosting** section. Open up the website URL in a new browser tab and you should see that the older, correct version of the web page is now displayed, as illustrated in the following screenshot:

Figure 5.23 – Previous recipe page with the correct heading (Blueberry)

In this exercise, you learned how to configure your bucket with static website hosting. You learned how, in this particular lab exercise, we made an error in the title of our web page and we were able to revert to an older versioning of the same document, thanks to having versioning enabled earlier.

Questions

Here are a few questions to test your knowledge:

1. Which of the following is true regarding Amazon S3? (Select 2 answers)
   A. Amazon S3 is object-based storage.
   B. Amazon S3 is an example of file storage.
   C. Amazon S3 is an example of block storage.
   D. The Amazon S3 One Zone-IA storage class offers 99.5% of availability. Amazon S3 can be configured as shared mount volumes for Linux-based EC2 instances.
2. You wish to enforce a policy on an S3 bucket that grants anonymous access to its content if users connect to the data from the corporate and branch offices as part of your security strategy. Which S3 configuration feature will enable you to define the IP ranges from where you will allow access to the data?
   A. Security groups

B. Bucket policy

C. NTFS permissions

D. **Network ACLs** (**NACLs**)

3. Which AWS service is the most cost-effective if you need to host static website content for an upcoming product launch?

A. Amazon EC2

B. Amazon EFS

C. Amazon S3

D. Azure ExpressRoute

4. Which Amazon S3 storage class enables you to optimize costs by automatically moving data to the most cost-effective access tier, while ensuring that frequently accessed data is made available immediately?

A. Amazon S3 Standard

B. Amazon S3 One-Zone IA

C. Amazon Snowball

D. Amazon S3 Intelligent-Tiering

5. Which Amazon S3 service can be configured to automatically migrate data from one storage class to another after a set number of days as a means of reducing your costs, especially where frequent instant access may not be required to that subset of data?

A. Static website hosting

B. Lifecycle management

C. Storage transition

D. S3 migration

6. When retrieving data from Amazon Glacier, what is the typical time taken by a Standard retrieval option to make the archive available for download?

A. 20 minutes

B. 24 hours

C. 3 to 5 hours

D. 90 seconds

7. Which feature of the Amazon S3 platform enables you to upload content to a centralized bucket from across any location via Amazon edge locations, ensuring faster transfer speeds and avoidance of public internet congestion?

   A. Amazon S3TA

   B. AWS S3 Storage Gateway

   C. Amazon VPC

   D. CloudFront

8. Your on-premises applications require access to a centrally managed cloud storage service. The application running on your servers need to be able to store and retrieve files as durable objects on Amazon S3 over standard NFS-based access with local caching. Which AWS service can help you deliver a solution to meet the aforementioned requirements?

   A. AWS Storage Gateway— Amazon S3File Gateway

   B. AWS EFS

   C. Amazon Redshift

   D. EBS volumes

9. You are looking to migrate your on-premises data to the cloud. As part of a one-time data migration effort, you need to transfer over 900 TB of data to Amazon S3 in a couple of weeks. Which is the most cost-effective strategy to transfer this amount of data to the cloud?

   A. Use the Amazon RDS service

   B. Use the Amazon Snowball service

   C. Use the Amazon VPN connection between your on-premises network and AWS

   D. Use AWS Rain

Chapter 6

Figures

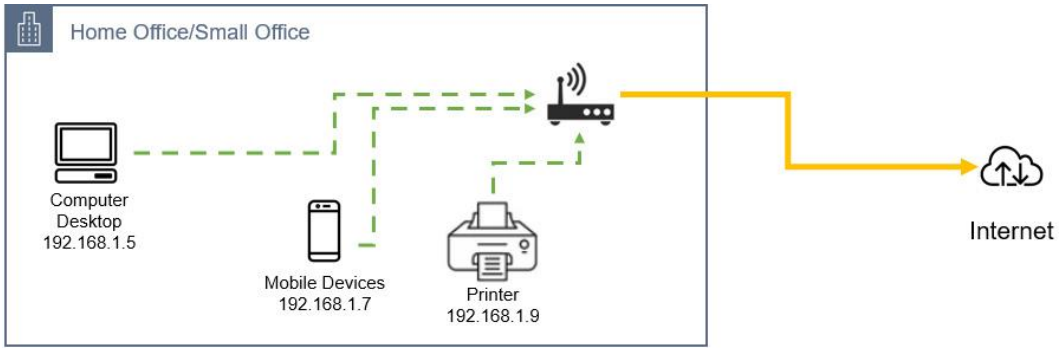

Figure 6.1 – Home network components

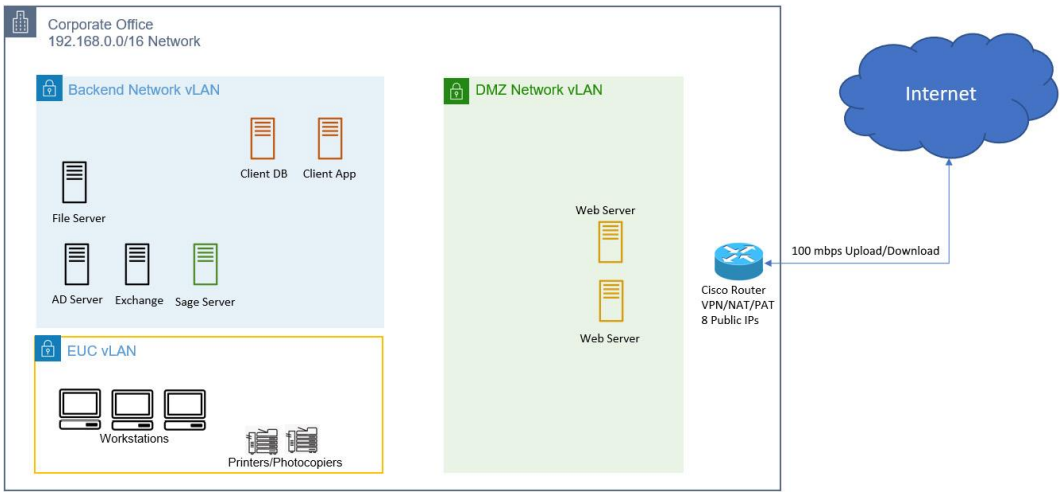

Figure 6.2 – Basic office network

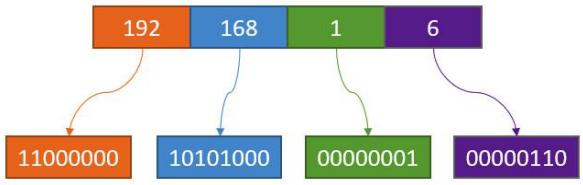

Figure 6.3 – IP address to binary conversion

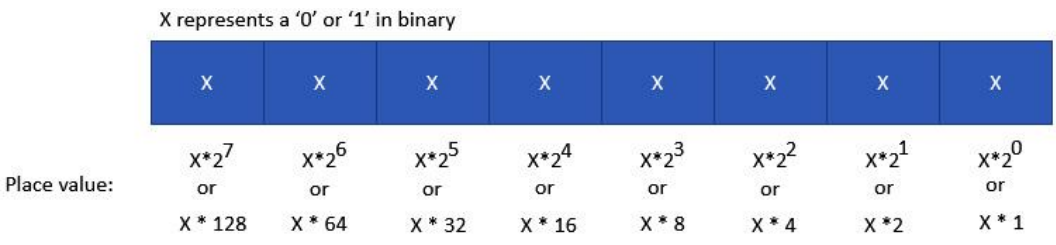

Figure 6.4 – IP address place values

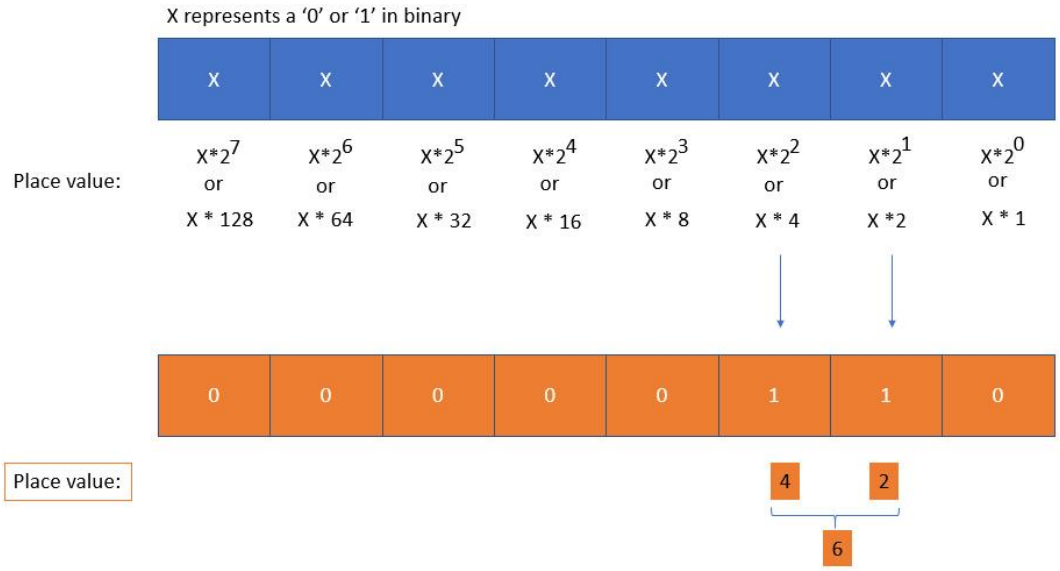

Figure 6.5 – Converting an IP address to its equivalent binary representation

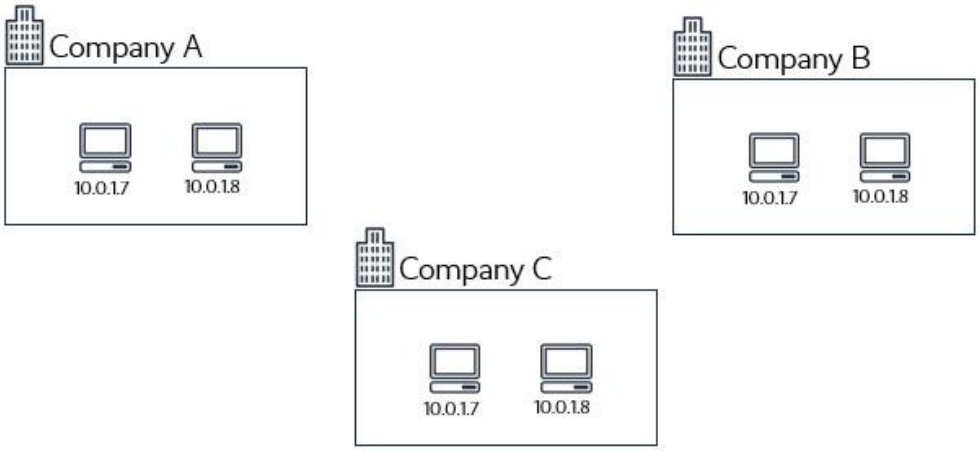

Figure 6.6 – Private IP address ranges used by businesses

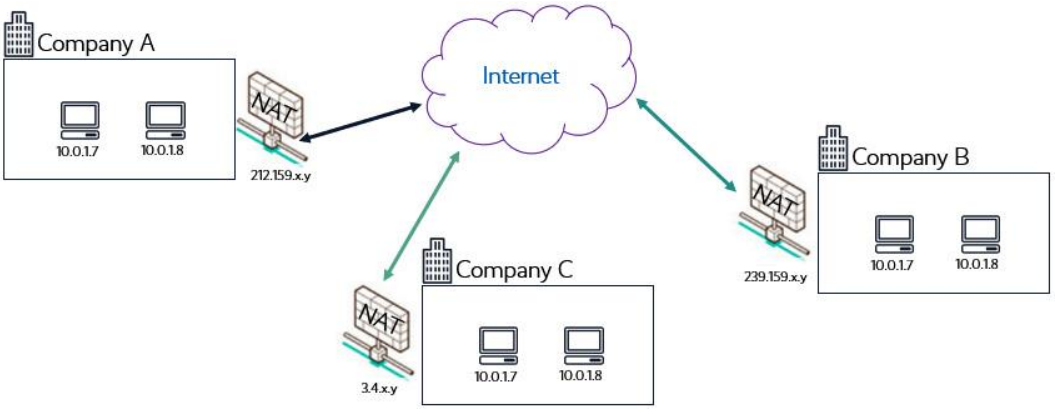

Figure 6.7 – Private IP address ranges used by businesses with internet via NAT services

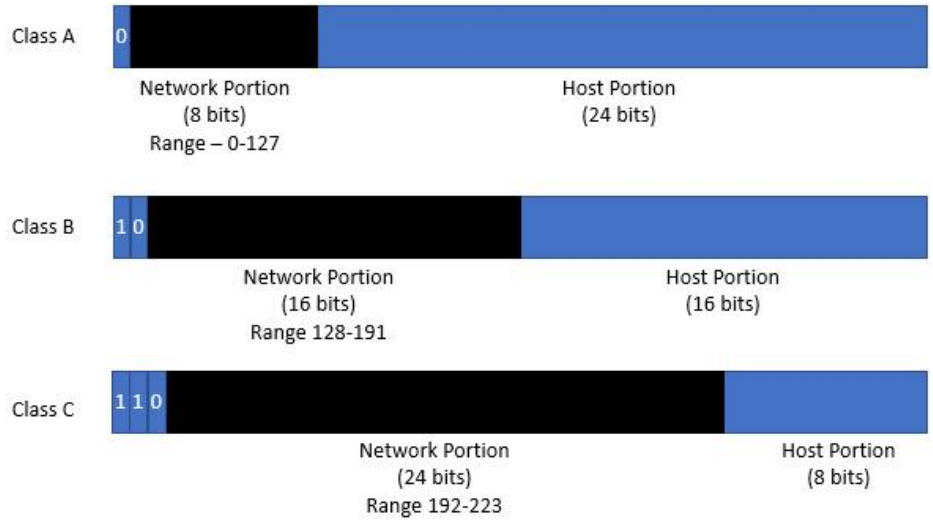

Figure 6.8 – IP address classes

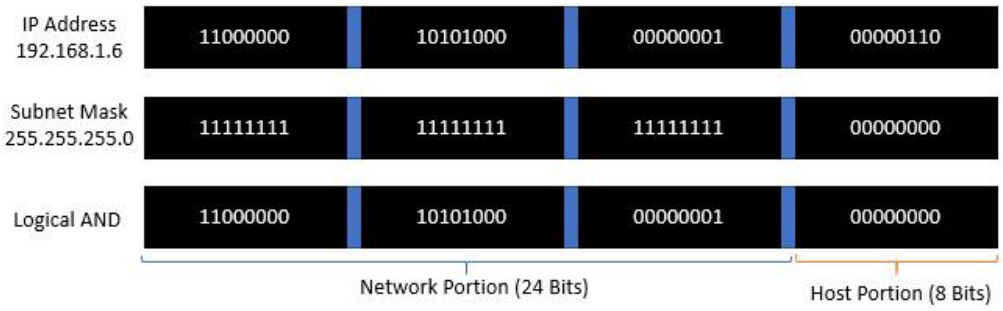

Figure 6.9 – IP address and subnet mask conversion for 192.168.1.6

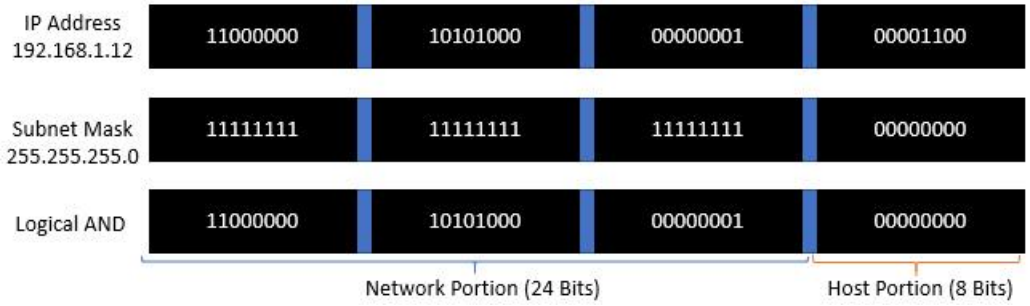

Figure 6.10 – IP address and subnet mask conversion for 192.168.1.12

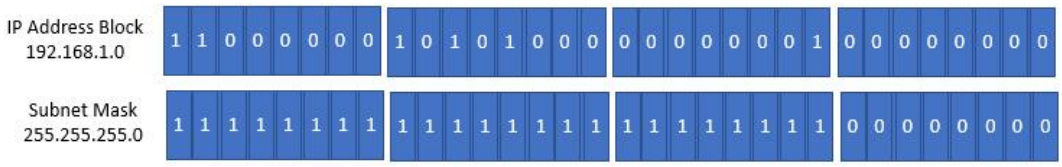

Figure 6.11 – IP class C network

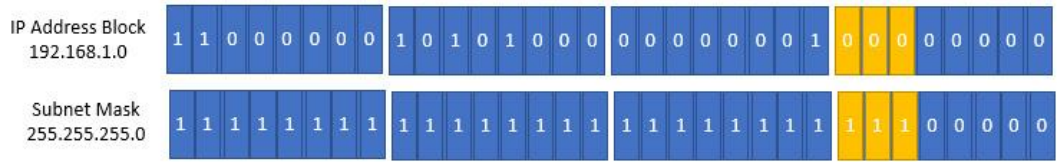

Figure 6.12 – Creating subnets by borrowing bits from the host portion of the IP address

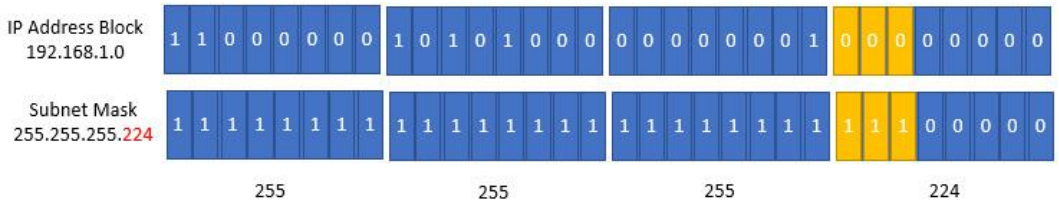

Figure 6.13 – Creating subnets resulting in a new subnet mask

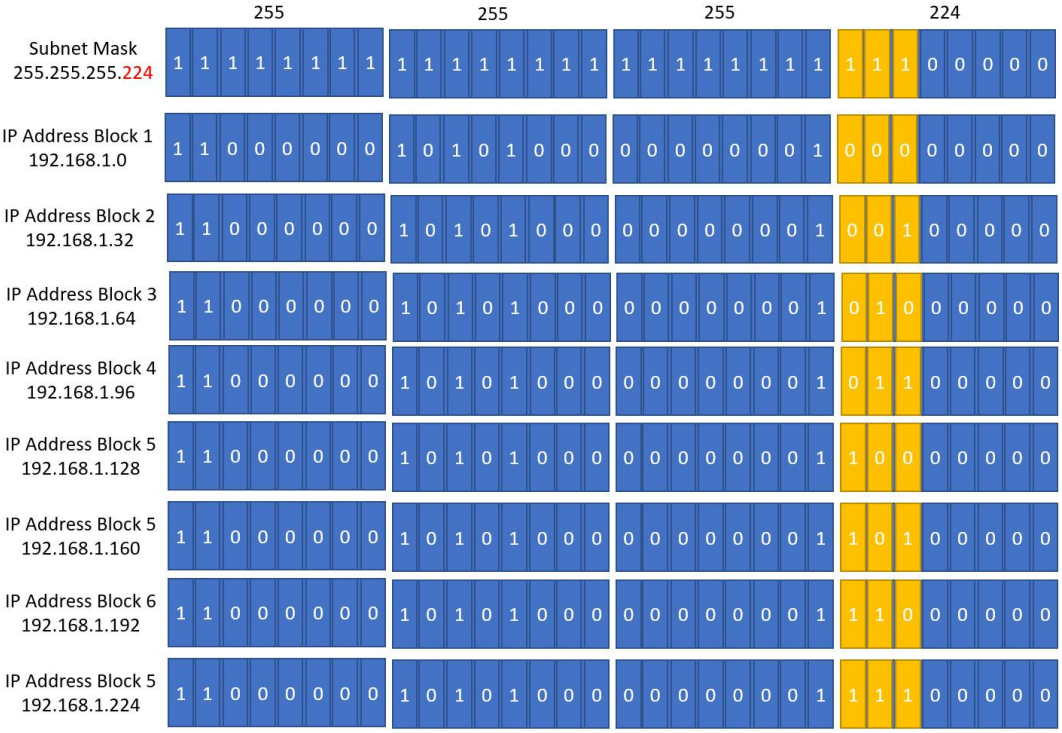

Figure 6.14 – Creation of eight subnetworks

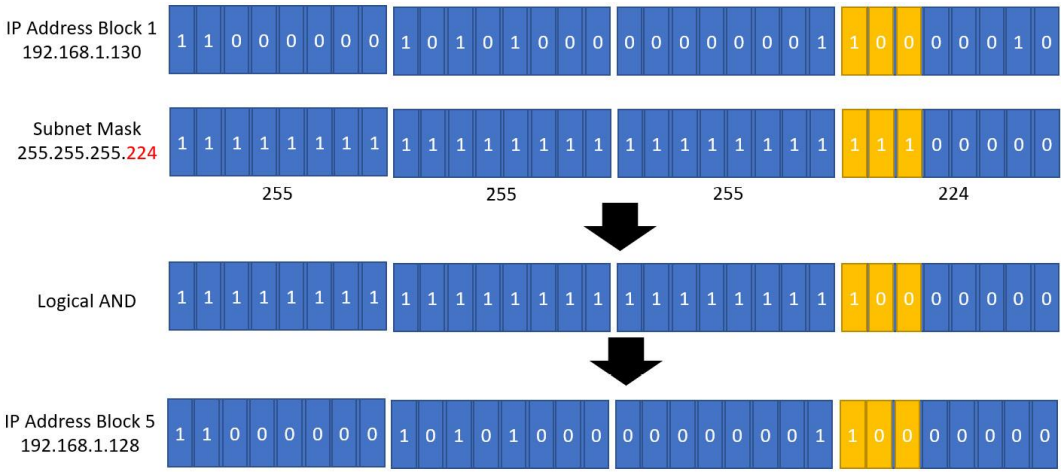

Figure 6.15 – Illustrating how IP addresses fall in a given subnetwork range

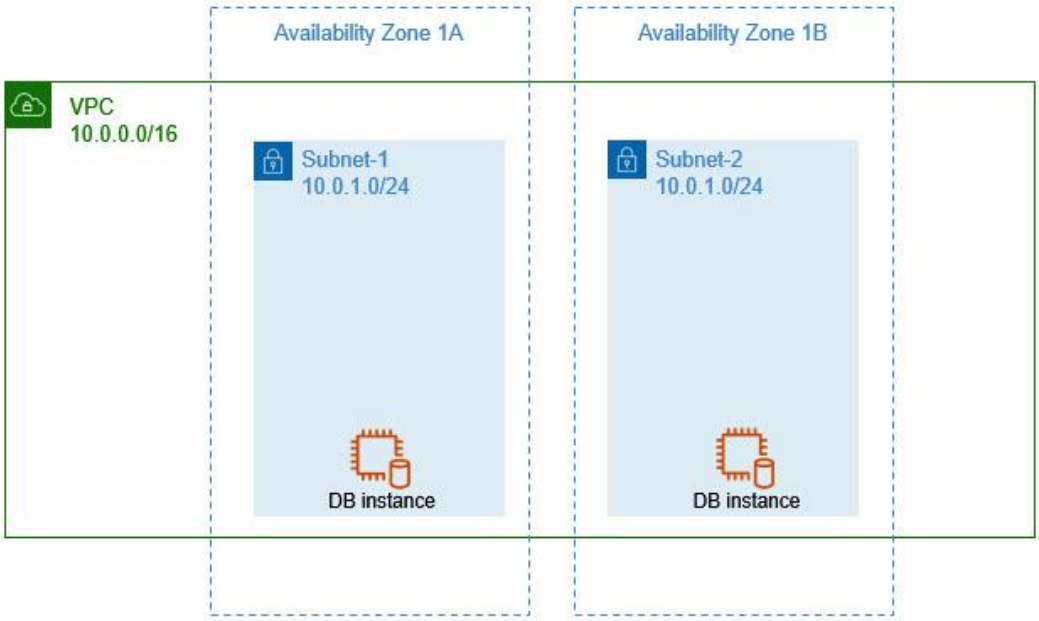

Figure 6.16 – VPCs and subnets with non-overlapping IP addresses

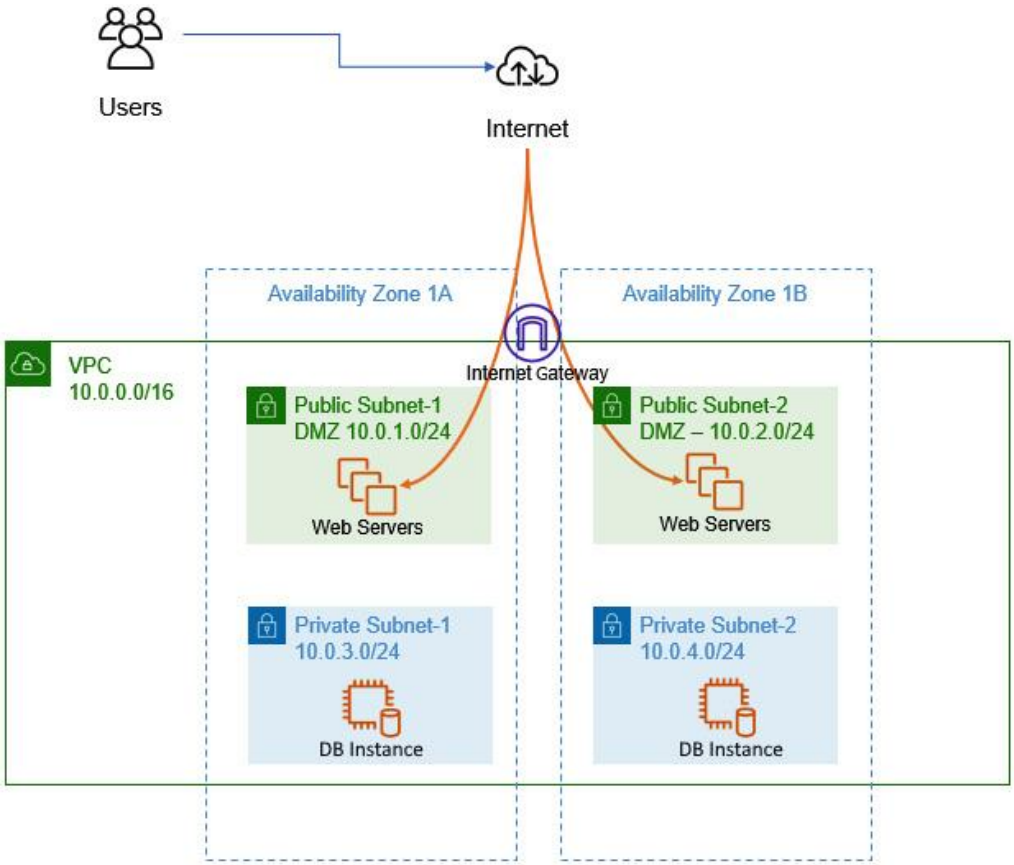

Figure 6.17 – VPCs and public and private subnets

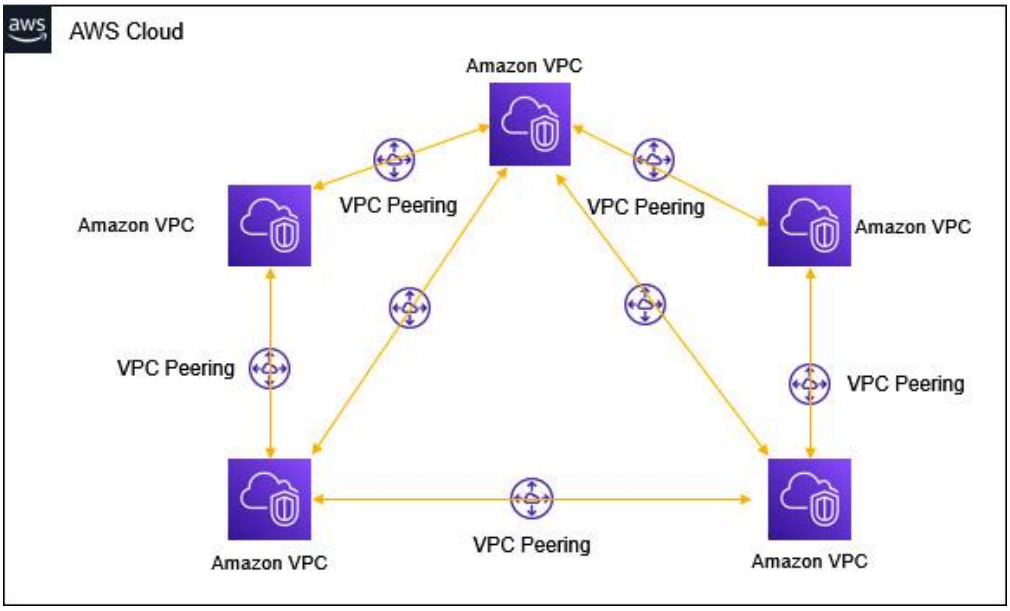

Figure 6.18 – Multiple VPC peering connections

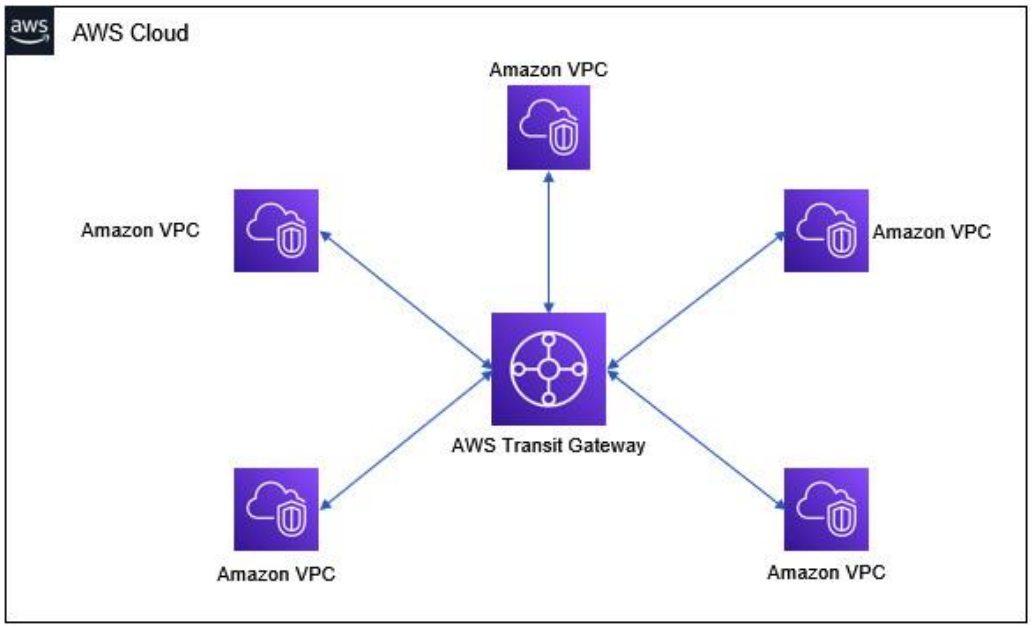

Figure 6.19 – AWS Transit Gateway

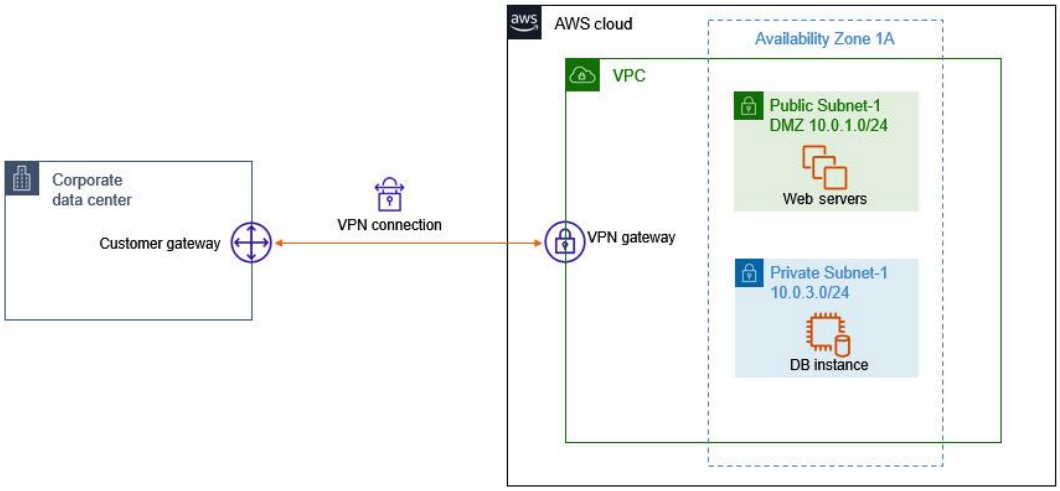

Figure 6.20 – Amazon VPNs

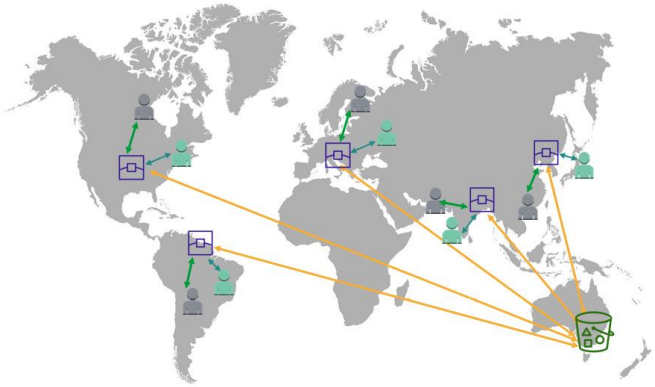

Figure 6.21 – A typical CloudFront distribution

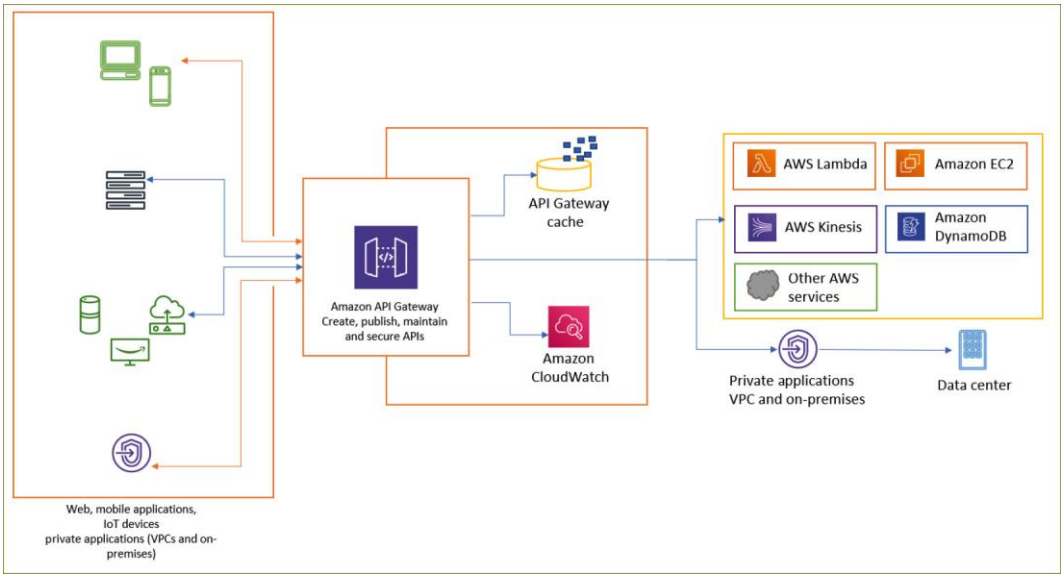

Figure 6.22 – Amazon API Gateway

Table

Name	Type	Value	Description
Iaasacademy.com	A - IPv4 Address	92.204.222.124	Points to server or load balancer hosting the website
Iaasacademy.com	MX-Mail exchange	iaasacademy-com.mail.protection.outlook.com	Points to email server/ service provider
Portal.Iaasacademy.com	CNAME	iaasacademy.com	Canonical name to map one domain name to another

Table 6.1 – Example resource records for iaasacademy.com

Code

- **Private DNS hostnames** – These resolve to the private IPv4 address of the instance. The DNS hostname can take one of the following two forms, depending on the Region:

```
ip-private-ipv4-address.ec2.internal for the us-east-1 Region

ip-private-ipv4-address.region.compute.internal for other Region
```

Note

`private-ipv4-address` is the reverse lookup IP address.

- **Public DNS hostnames** – These resolve a public DNS hostname to the public IPv4 address of the instance outside the network of the instance, and to the private IPv4 address of the

instance from within the network of the instance. The DNS hostname can take one of the following two forms, depending on the Region:

```
ec2-public-ipv4-address.compute-1.amazonaws.com for the us-east-1

ec2-public-ipv4-address.region.compute.amazonaws.com for other Regions.Exercise
```

6.1 – setting up a public subnet VPC

In this exercise, you will create your own custom VPC that will contain a public subnet. In later chapters, you will expand this VPC to add private subnets for different use case:

1. Log in to your AWS account as the IAM user `Alice` you created in *Chapter 4*, *Identity and Access Management*.
2. On the main AWS Management Console, search for `VPC` in the search box.

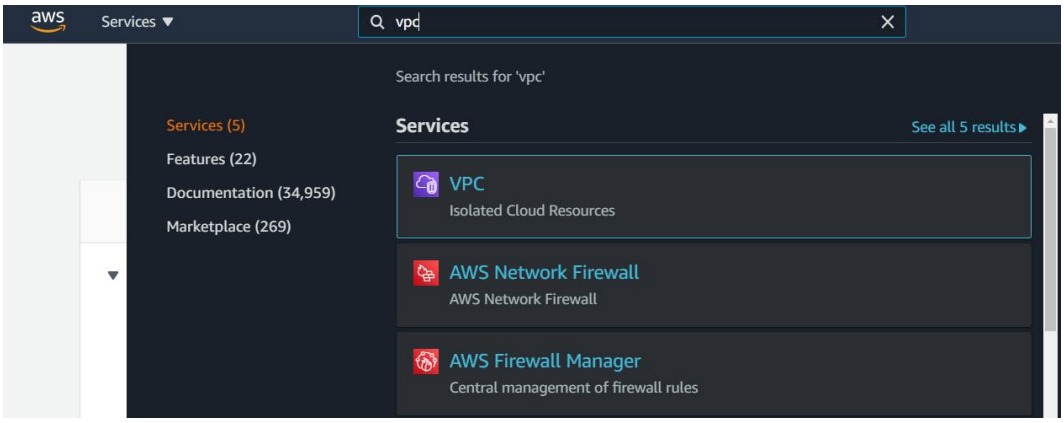

Figure 6.23 – Configuring a new VPC

3. Select **VPC** from the filtered list.
4. VPCs are Region-specific, so make sure you select the US-East-1 Region from the top right-hand corner of the screen.
5. On the main VPC console screen, click on the **Launch VPC Wizard** button. This will launch the VPC wizard.
6. Next, select the first option, **VPC with a Single Public Subnet.**
7. In *Step 2*, provide the following details for your VPC.

   For **IPv4 CIDR block**, enter the IP block of `10.0.0.0/16`. This IP block represents your VPC network.

   For **VPC name**, enter the name `ProductionVPC`.

The wizard gets you to create a single public subnet. Later, you will expand this VPC for future use, but for now, set the **Public subnet's IPv4 CIDR** field to `10.0.1.0/24`.

For **Availability Zone**, select **us-east-1a** from the drop-down list. Remember that while VPCs span the entire Region, each subnet you create spans a single Availability Zone. In this case, we are creating a single public subnet in **us-east-1a.**

Next, rename the subnet name to **Public Subnet One**.

Next, click the **Create VPC** button in the bottom right-hand corner of the screen. Review the following screenshot for the preceding steps:

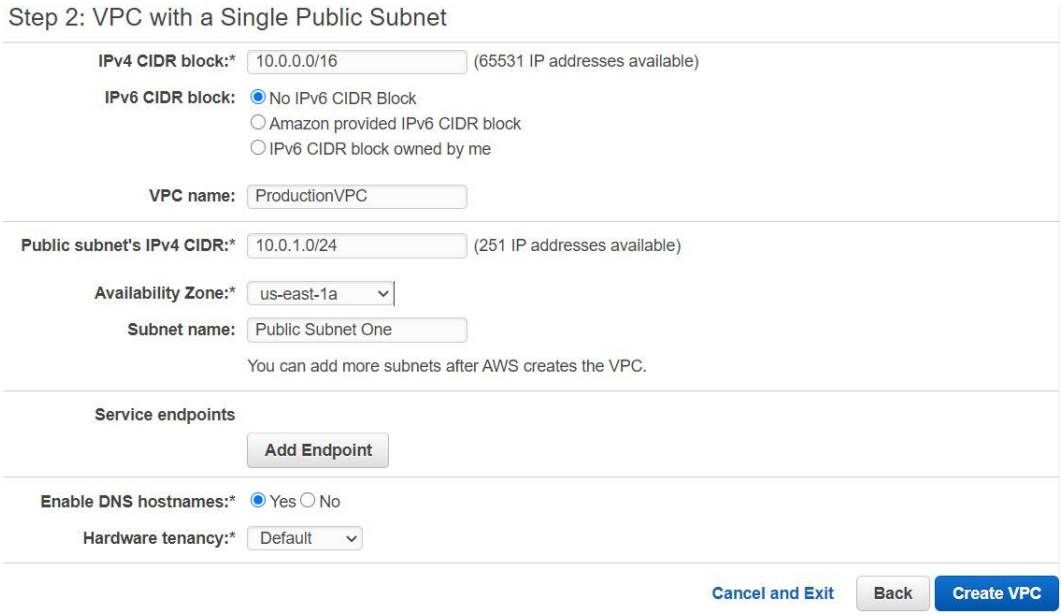

Figure 6.24 – VPC with public subnet configuration page

8. The wizard runs through the parameters you specified and creates your first VPC.
9. Click **OK** on the **VPC Successfully Created** status page.
10. In the list of VPCs, you will note that your newly created **ProductionVPC** has been successfully created:

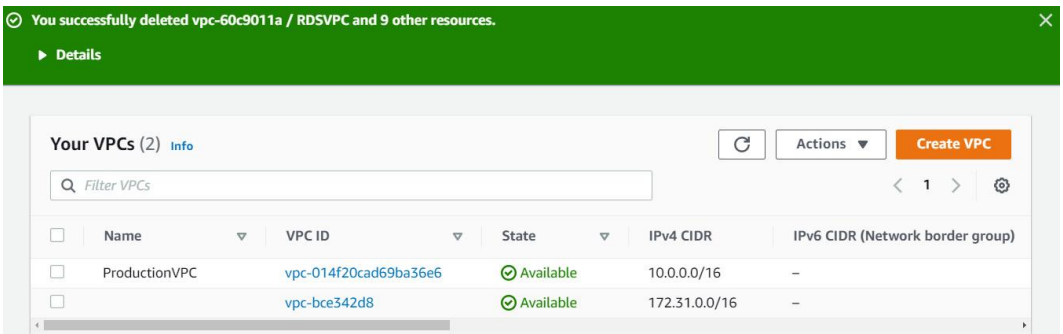

Figure 6.25 – Newly created ProductionVPC

In this section, we demonstrated how to create your first public subnet VPC using the AWS VPC wizard. Later in the training guide, you will expand the VPC to include private subnets and deploy servers within our VPCs.

Questions

1. Which VPC component enables to you grant internet access to servers in the public subnet deployed in the VPC?

   A. NAT gateway

   B. Internet gateway

   C. VPC peering

   D. Security group

2. Which of the following statements are true?

   A. NACLs protect entire subnets, whereas security groups protect the individual instance.

   B. NACLs protect the individual instance, whereas security groups protect the entire subnet.

   C. NACLs enable instances in the private subnet to access the internet and act as a NAT device, whereas security groups are used to assign IAM policies to servers that need access to S3 buckets.

   D. NACLs enable instances in the private subnet to access the internet and act as a NAT device, whereas security groups are used to assign IAM policies to servers that need access to S3 buckets.

3. Which AWS service enables you to purchase and register new domain names that can be used to publish your website on the internet?

   A. Route53

   B. VPC

   C. RDS

   D. Elastic Beanstalk

4. Which AWS service enables you to distribute your digital assets such that it is cached locally to users who attempt to access this content for a time to live, and thus helps to reduce network latency?

   A. AWS CloudFront

   B. AWS CloudTrail

   C. AWS CloudWatch

D. AWS CloudScape

5. Your organization hosts multiple AWS accounts with multiple VPCs. You would like to connect these VPCs together and centrally manage connectivity policies. Which AWS service enables you to connect multiple VPCs configured as a hub that controls how traffic is routed among all the connected networks, which act like spokes?

   A. AWS Transit Gateway

   B. AWS Global Accelerator

   C. AWS VPC Peering

   D. AWS Virtual Private Gateway

6. Which AWS service enables you to grant internet access to EC2 instances configured with IPv4, and located in the private subnet of your VPC?

   A. Egress-only internet gateway

   B. NAT gateway

   C. VPC endpoint

   D. VPN tunnel

7. You company has a primary production website in the US and a DR site in Sydney. You need to configure DNS such that if your primary site becomes unavailable, you can fail DNS over to the secondary site. Which DNS routing policy can you configure to achieve this?

   A. Weighted Routing

   B. Geolocation Routing

   C. Latency Routing

   D. Failover Routing

8. You plan to set up DNS failover using Amazon Route53. Which feature of Route53 can you use to test your web application's availability and reachability?

   A. Private DNS

   B. CloudWatch

   C. Health checks

   D. DNS ping

9. Which VPC firewall solution enables you to deny inbound traffic from a specific IP address, which can be used to prevent malicious attacks?

   A. AWS Firewall

B. AWS Security Groups

C. AWS **Network Access Control Lists** (**NACLs**)

D. AWS CloudFront

10. Which AWS service enables you to connect your private data center to your Amazon VPC with up to 100 Gbps network connectivity?

A. Snowball

B. Direct Connect

C. **Virtual Private Network** (**VPN**)

D. **Virtual Satellite Network** (**VSN**)

Chapter 7

Figures

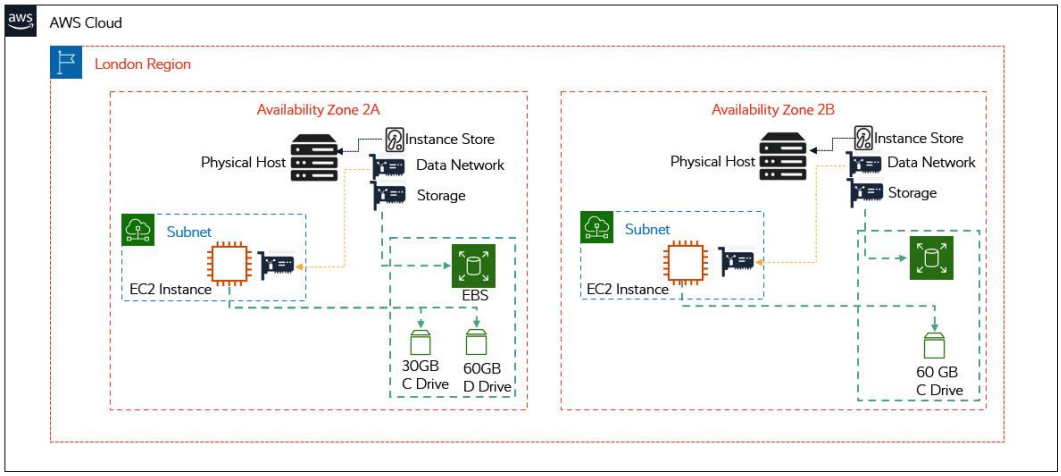

Figure 7.1 – EC2 instance components

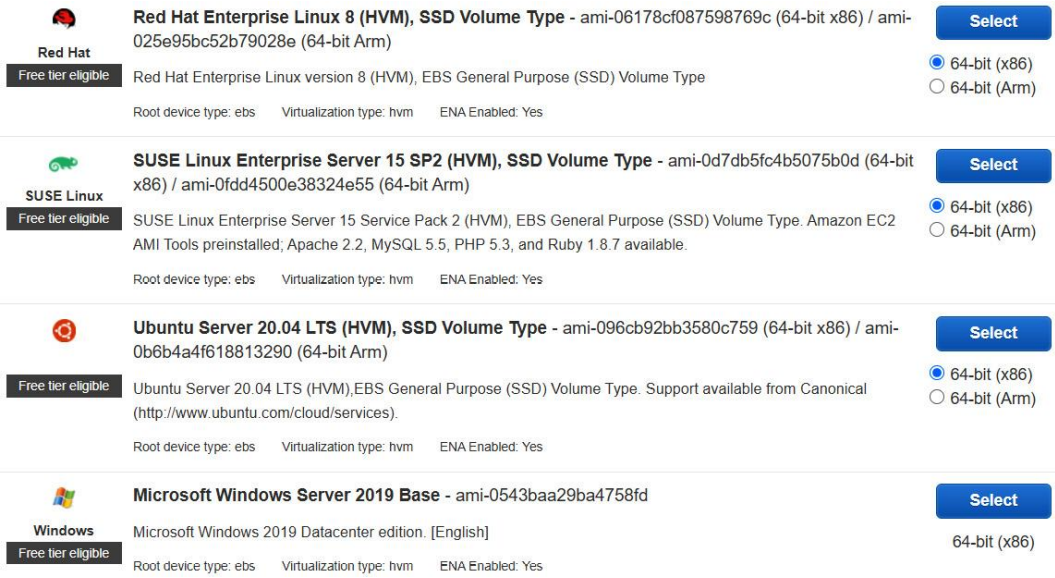

Figure 7.2 – AMIs

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750

Figure 7.3 – Sample selection of M5 instance sizes

t2.micro

STANDARD 1-YEAR TERM					
Payment Option	Upfront	Monthly*	Effective Hourly**	Savings over On-Demand	On-Demand Hourly
No Upfront	$0	$5.26	$0.007	38%	$0.0116
Partial Upfront	$30	$2.48	$0.007	41%	
All Upfront	$59	$0.00	$0.007	42%	

Figure 7.4 – t.2micro Reserved Instance Pricing Option in N. Virginia Region, standard 1-year term

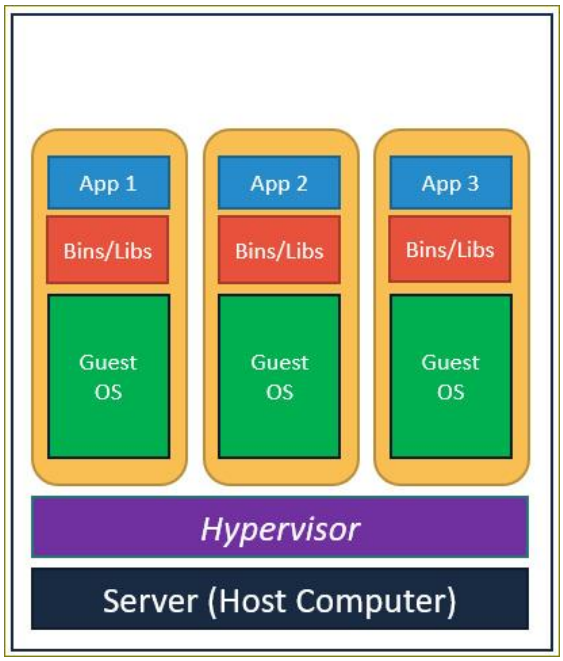

Figure 7.5 – Hypervisor architecture hosting VMs

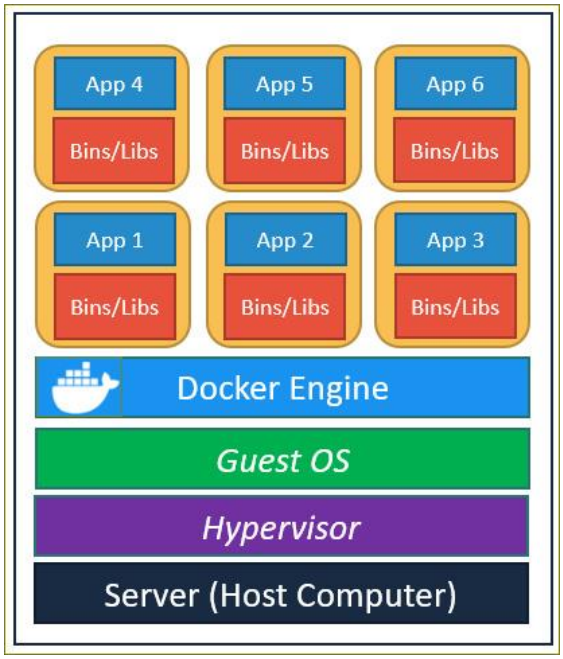

Figure 7.6 – Docker concepts

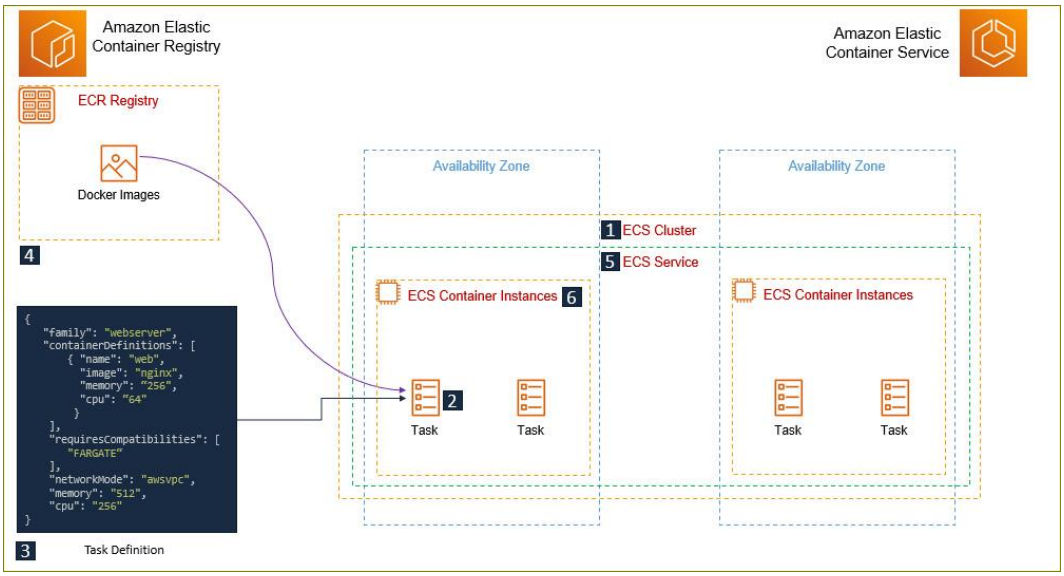

Figure 7.7 – Amazon ECS architecture

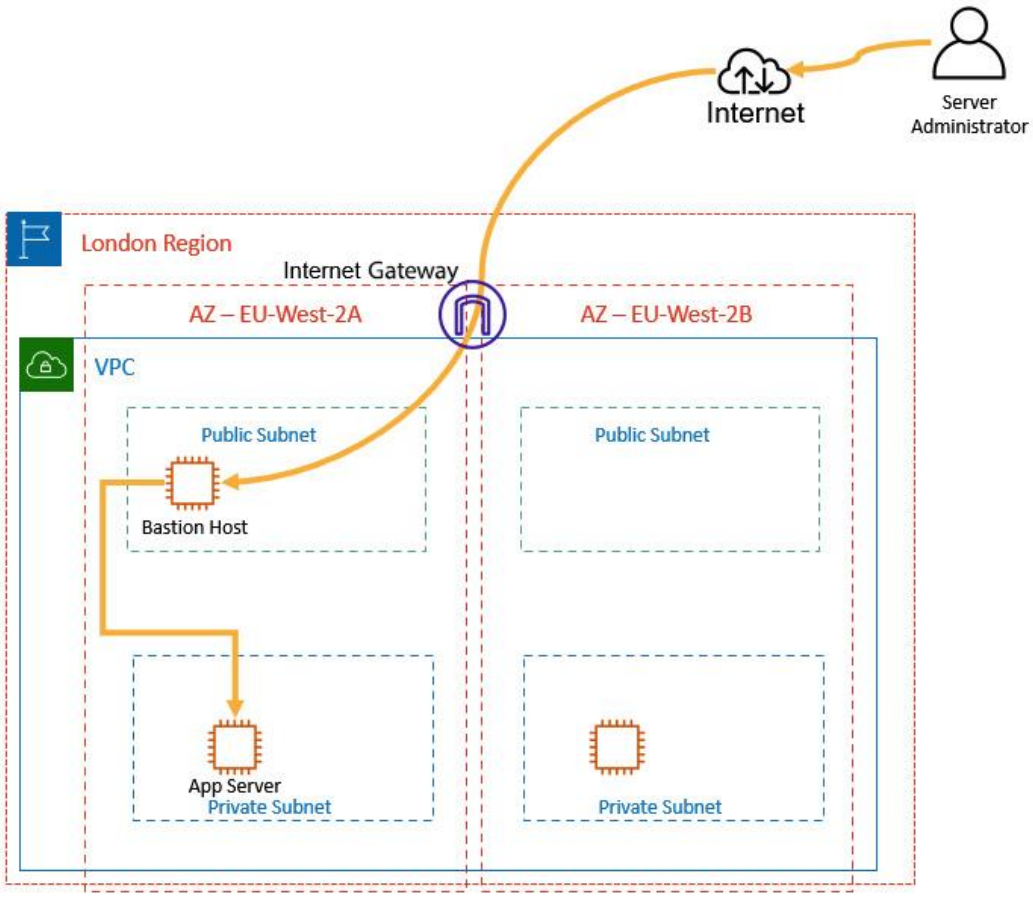

Figure 7.8 – Securing access to your VPC using bastion hosts

Links

For more details on how to create and copy AMIs, refer to the Amazon documentation at https://aws.amazon.com/premiumsupport/knowledge-center/copy-ami-region/

You can review the AWS Marketplace offering at https://aws.amazon.com/marketplace.

Exercise 7.1 – Expanding ProductionVPC so that it includes two public subnets and two private subnets

In this exercise, we will expand the architecture of **ProductionVPC** that we built in the previous chapter so that it includes an additional public subnet in another Availability Zone and two private subnets – one in each Availability Zone. This will enable us to design an architecture that can offer high availability in case of a single Availability Zone outage.

We will be extending the VPC to fulfill our design specifications, as shown in the following diagram:

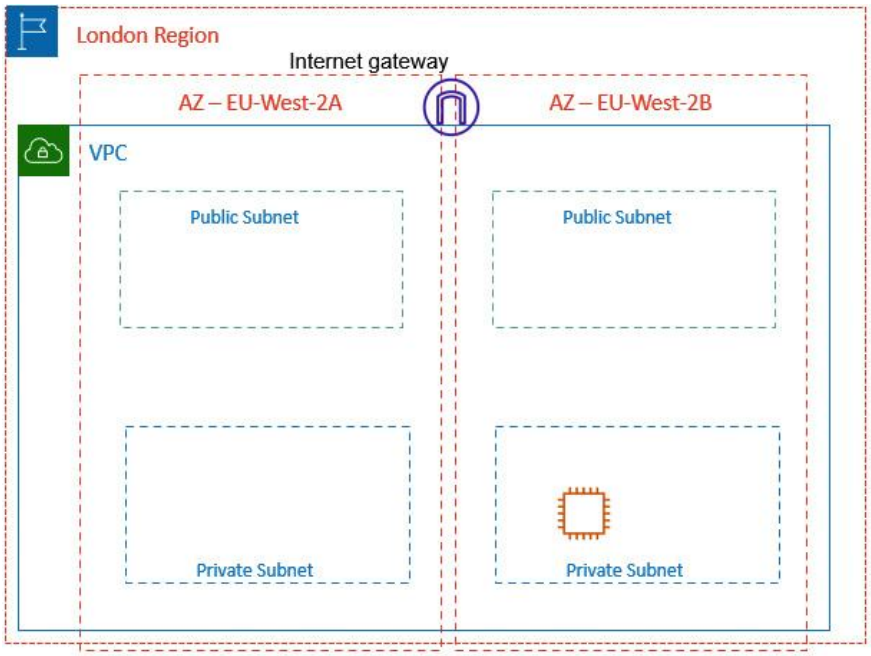

Figure 7.9 – VPC with public and private subnets across two Availability Zones

Log in to your AWS account as the root user and on the main AWS Management Console, search for `VPC` in the search box. Click on the `VPC` link to open the VPC Console. Once in the console, ensure that you are in the us-east-1 Region, where you created **ProductionVPC** in the previous chapter. If necessary, navigate to the us-east-1 Region by selecting it from the drop-down list.

Review your current VPC:

1. On the left-hand menu in **VPC console**, click on **Subnets**. You will see that there is one **Public Subnet One** that is associated with ProductionVPC, which you created in the previous chapter. You will also see other subnets, but these are associated with the default VPC in the us-east-1 Region, as per the following screenshot:

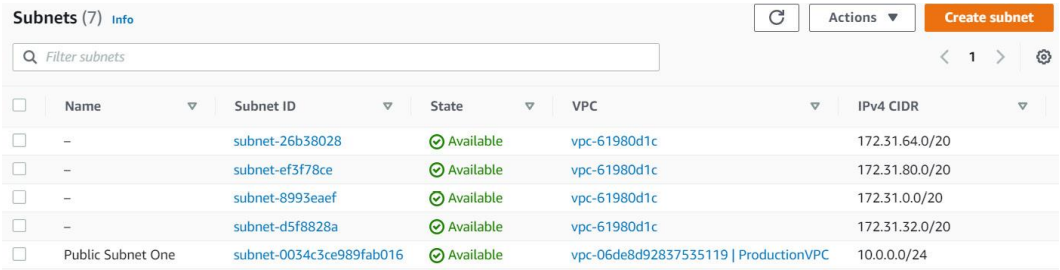

Figure 7.10 – ProductionVPC with a single public subnet

2. Next, click on the **Route Tables** link from the left-hand menu. Using the VPC Wizard, your ProductionVPC has been configured with a main route table and a public route table. From the following screenshot, you can see that the main route table associated with the ProductionVPC has a route table ID of **rtb-0d6fb017c417d8e1b**. You can tell it is the main route table because this is indicated in the **Main** column with a **Yes**. This main route table is designed to be associated with all private subnets in your VPC.

If you click on the **Main Route Table ID** link in the console, the bottom pane will provide additional information about the route table. Furthermore, if you click on the **Routes** tab of the bottom pane, you will note that currently, there is only one route: the **local route**. This local route is designed for traffic to flow within the VPC. The main route table does not offer any direct access to the internet now. This is a best practice because, for subnets that need direct access to the internet, you should ideally create a separate **public route table** and attach any *public subnets* to it:

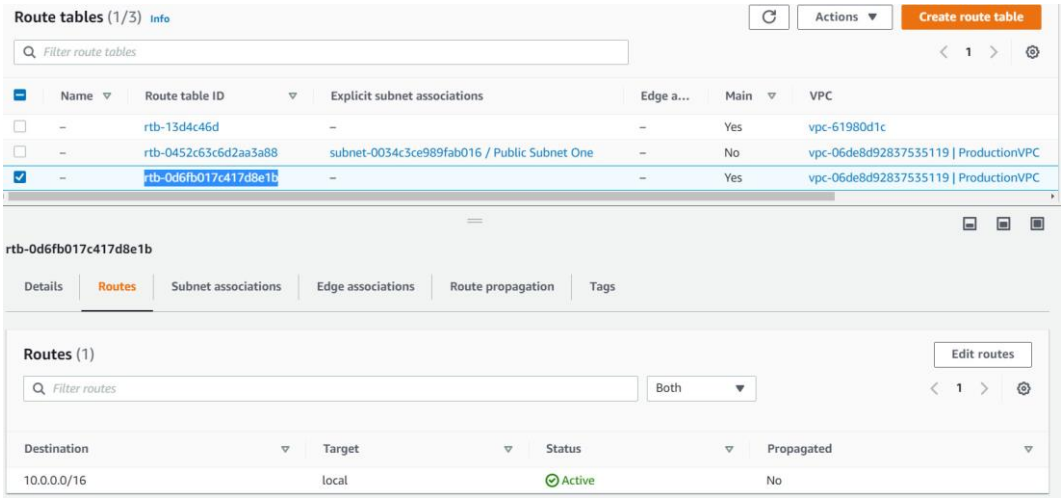

Figure 7.11 – ProductionVPC main route table configuration

3. Next, in the top pane, you will notice that the wizard has already created a public route table (with a **Route table ID** of **rtb-0452c63c6d2aa3a88**). We know this is the public route table because, in the preceding screenshot, you can see a **No** in the **Main** column. It also has one subnet associated with it: **Public Subnet One**.

4. If you click on the **Route Table ID** link of the public route table, the bottom pane will offer additional information, as per the following screenshot. Specifically, if you click on the **Routes** tab of the public route table, you will see two routes: one local route and a route to the internet. Routes to the internet are denoted with a destination of **0.0.0.0/0**. In this case, the route to the internet has a target, which is the **internet gateway**. This internet gateway gives the subnet direct access to send traffic to the internet and receive traffic from the internet if the security groups and/or **Network Access Control Lists** (**NACLs**) permit the traffic:

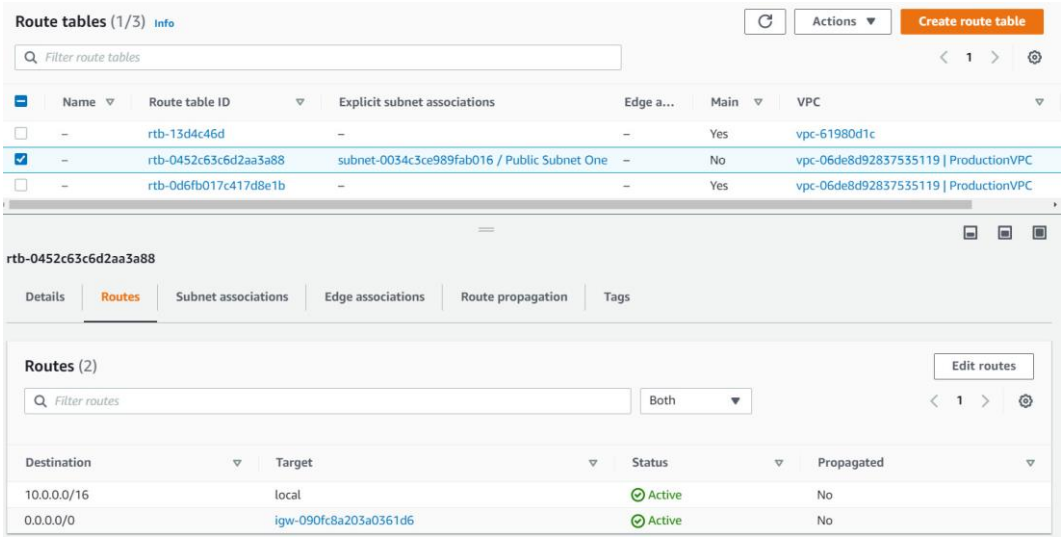

Figure 7.12 – ProductionVPC with public route table configuration

You will also notice that AWS does not create a name tag for your route tables by default. This can sometimes make it difficult to identify your resources. You can easily add name tags to make resources easy to identify. Using your mouse, simply hover over the area in the **Name** column next to the **Public Route** table until you notice an edit icon. Click on this edit icon and in the **Edit Name** text box that appears, type in `Public Route Table`. Perform the same action for the main route table, making sure to tag the route table with the name **Main Route Table**. This will make it easy to identify your route tables, as per the following screenshot:

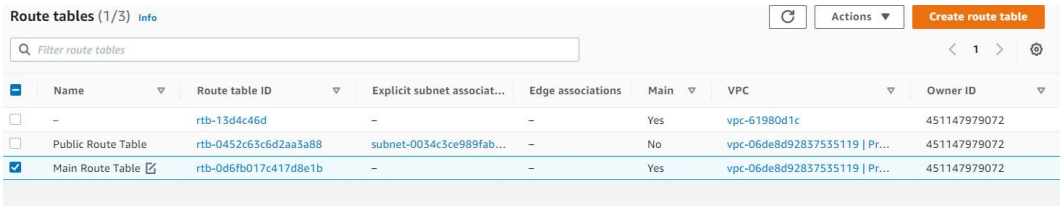

Figure 7.13 – Tagging your route tables

When you create new subnets, they are automatically associated with the main route table. This technically makes them private subnets. If you need to create a public subnet, you need to remember to disassociate the subnet from the main route table and attach it to a route table that offers public internet access via the internet gateway.

While you can configure a direct route to the internet in the main route table that sends traffic via the internet gateway, this is not advisable. You want to ensure that some subnets offer only internal private access without direct exposure to the internet. Since EC2 instances deployed as backend services require internet access to download software updates, for example, you can set up NAT gateways in the public subnets to facilitate this requirement. You would then need to configure the **Main Route** table with a route to the internet via this NAT gateway, which acts as a proxy for any internet requests from your backend EC2 instances. These backend EC2 instances do not require public IP addresses and can still communicate with the internet via the NAT gateway.

Setting up additional subnets

In this part of the exercise, we will be expanding our VPC to include multiple public and private subnets. We wish to host two public subnets and two private subnets across two Availability Zones. We wish to do this because we want to offer high availability so that if one Availability Zone fails or is offline, we can access duplicate copies of our resources in the other Availability Zone.

You already have one public subnet in your VPC. This has been configured with a name of **Public Subnet One** and has been placed in the **us-east-1a** Availability Zone as per the following screenshot:

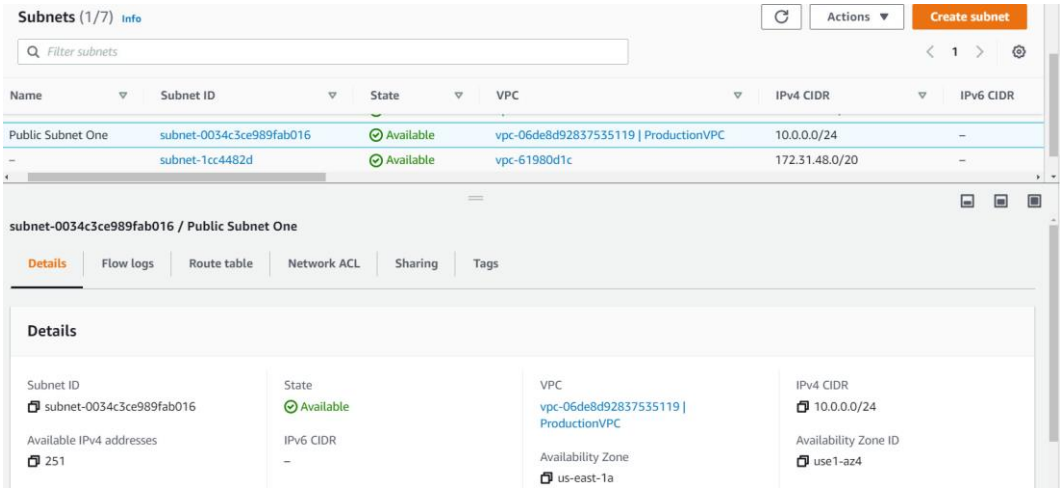

Figure 7.14 – Public Subnet One in the us-east-1a Availability Zone

As part of this exercise, we will create another public subnet in the **us-east-1b** Availability Zone:

1. From the left-hand menu in your VPC console, click on **Subnets**.
2. Click on the **Create subnet** button in the top right-hand corner.
3. In the **Create subnet** wizard that appears, choose **ProductionVPC** from the list of VPCs available.
4. Under **Subnet settings**, provide a subnet name such as `Public Subnet Two`.
5. Next, under **Availability Zone**, ensure you select **us-east-1b**. This is because we want the second public subnet to be placed in a different Availability Zone from the first public subnet.
6. For the IPv4 CIDR block, provide a block address of `10.0.2.0/24`. This CIDR block is on a separate range from the CIDR block of the first public subnet but is still a subset of the VPC's CIDR range.
7. Finally, as per the following screenshot, click on **Create subnet**:

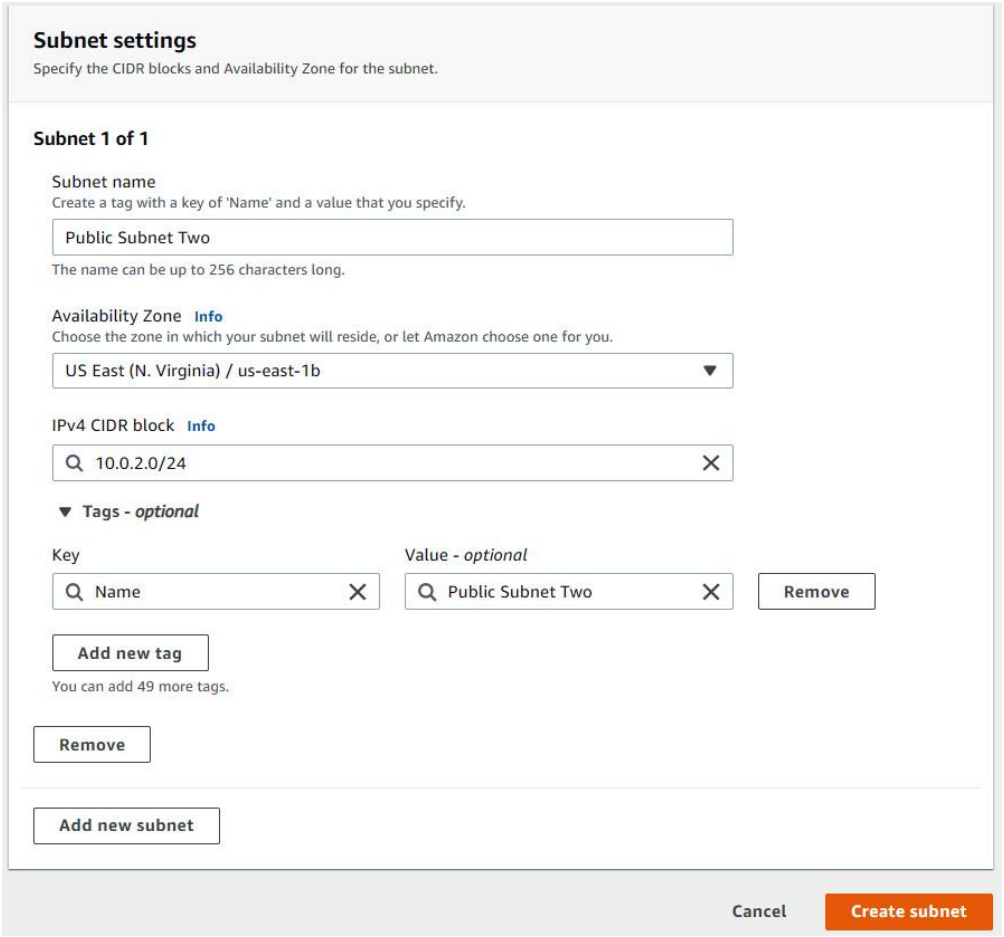

Figure 7.15 – Creating Public Subnet Two

The wizard will create the subnet and display a successful creation message.

If you click on the checkbox next to the newly created subnet, the bottom pane will provide information about the subnet. Click on the **Route table** tab. You will notice that this newly created subnet has been automatically associated with **main route table**, as shown in the following screenshot:

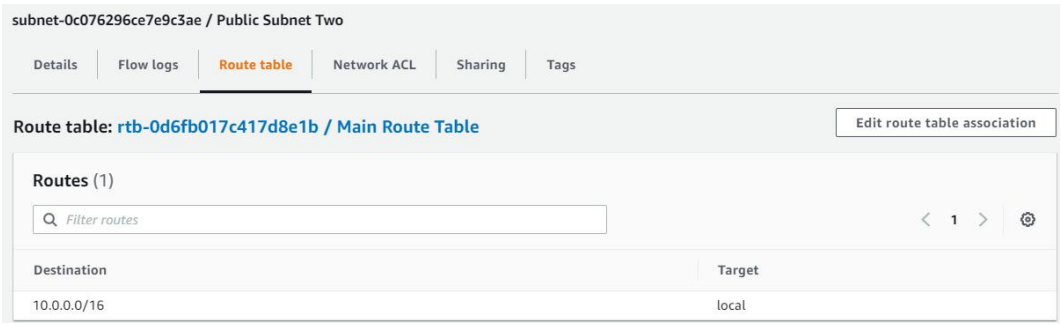

Figure 7.16 – Newly created subnet associated with main route table

Because we want this subnet to be a public subnet, we need to change its association from the main route table to the public route table, as follows:

8. Click on the **Edit route table association** button, as shown in the preceding screenshot.

9. In the **Edit route table association** dialog box that appears, select **Public Route Table** from the **Route table ID** drop-down list, as shown in the following screenshot:

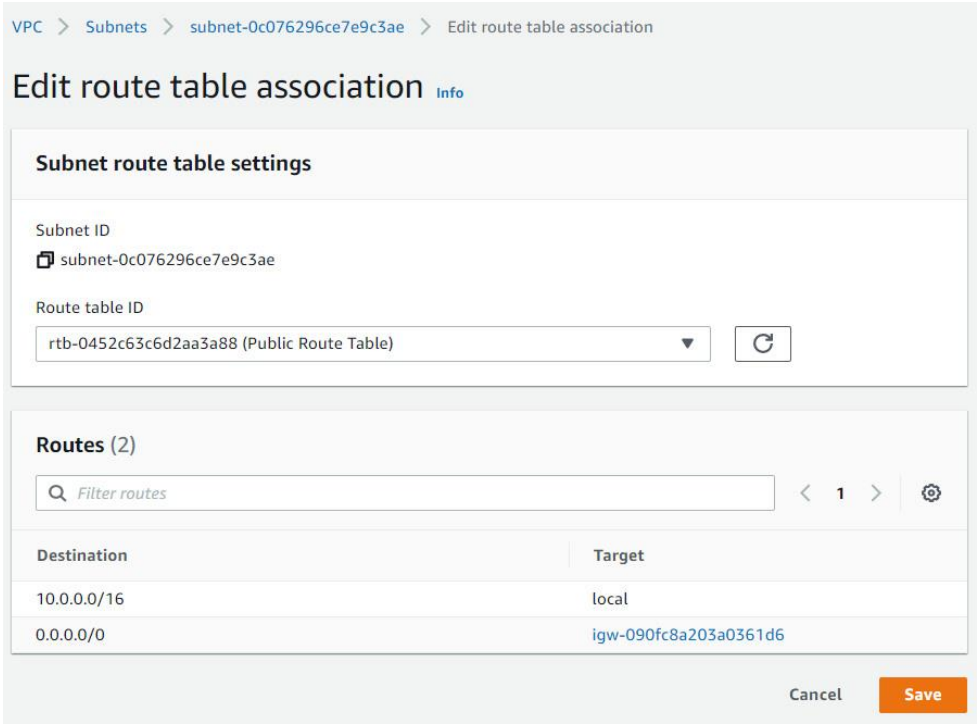

Figure 7.17 – Edit route table association

10. Click **Save**.

At this point, both public subnets have been correctly configured. Next, we'll create two private subnets, one in **us-east-1a** and the other in **us-east-1b**.

Creating private subnets

Follow these steps to create the aforementioned private subnets:

1. While still in the VPC console, click on the **Subnets** link from the left-hand menu.
2. In the **Create subnet** dialog box that appears, select **ProductionVPC** from the **VPC ID** drop-down list.
3. Next, in the **Subnet settings** section, type `Private Subnet One` in the **Subnet name** text box.
4. Under **Availability Zone**, select **us-east-1a** – this is the same zone where we placed **Public Subnet One**. This way, any frontend web resources in **Public Subnet One** can access any backend resources in **Private Subnet One**, allowing those resources to be in the same Availability Zone.
5. For the IPv4 CIDR block, provide the IP CIDR range of `10.0.3.0/24` – this CIDR block does not conflict with any of the other subnets and is still a subset range of the main VPC's IP range.

6. Finally, click the **Create subnet** button at the bottom of the page, as per the following screenshot:

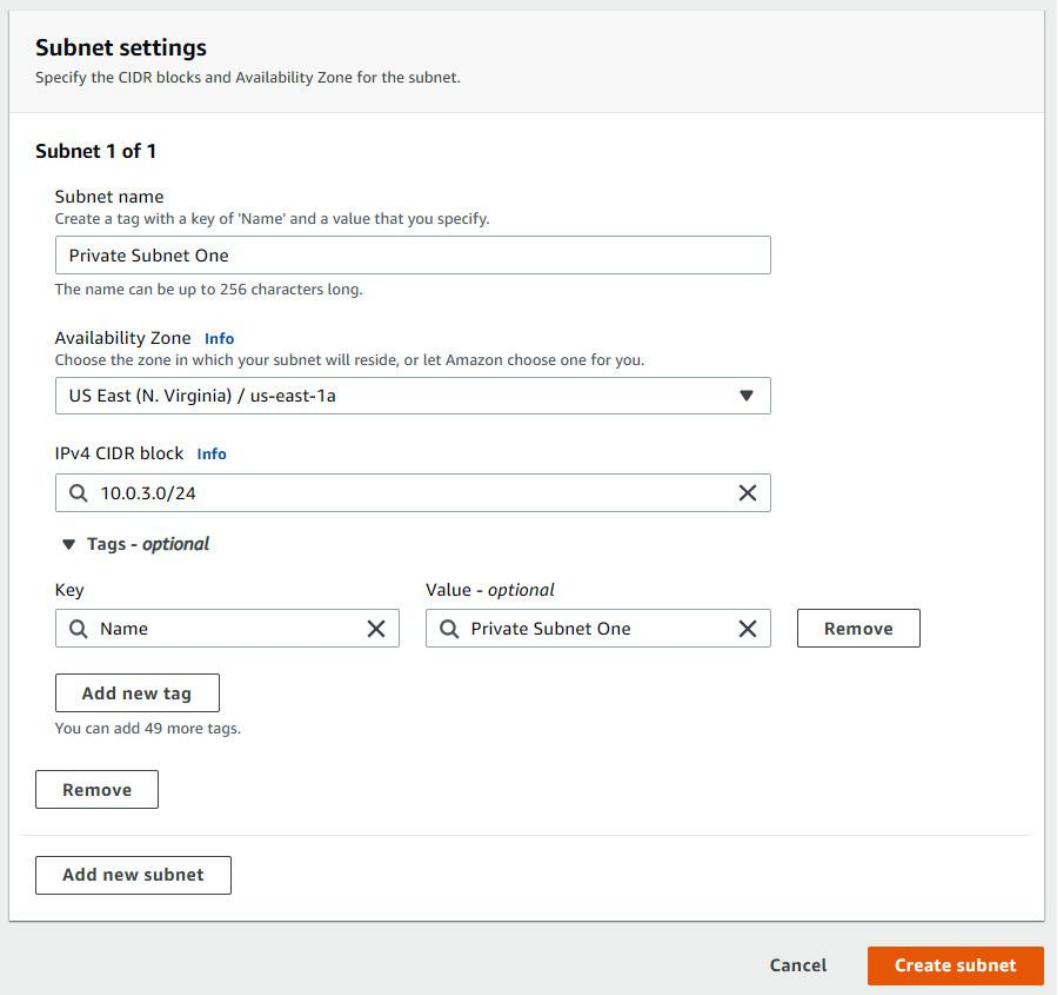

Figure 7.18 – Private Subnet One settings

You will receive a success message. Next, we will perform the same steps we did previously, but this time to create the second private subnet in **us-east-1b**:

1. Click **Create subnet**.
2. Select **ProductionVPC** from the VPC ID drop-down list.
3. For the subnet name, type in `Private Subnet Two`.
4. Under **Availability Zone**, select **us-east-1b**.
5. For the IPv4 CIDR block, type in `10.0.4.0/24` as the CIDR block range for this subnet.
6. Click the **Create subnet** button at the bottom of the page.

At this point, you have a VPC configured with two public subnets and two private subnets.

Note

You do not need to associate the two private subnets to the main route tables manually, as this is done for you by default.

To check this, perform the following steps:

1. Select **Route Tables** from the left-hand menu.
2. From the top pane, click on the checkbox next to the main route table.
3. In the bottom pane, you will notice that both private subnets are associated with the main route table (not explicitly) but by default instead, as shown in the following screenshot:

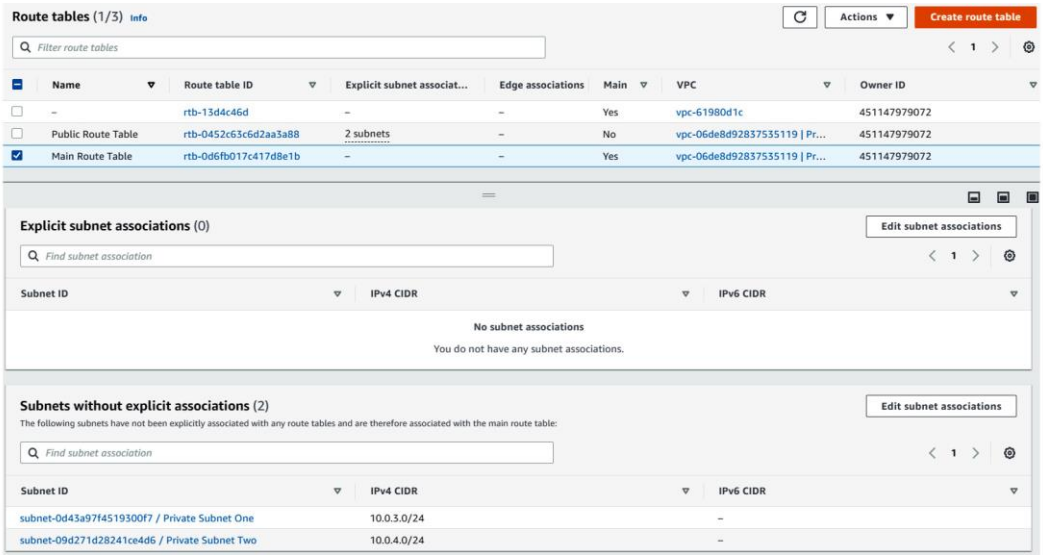

Figure 7.19 – Private subnet route table associations

In this exercise, we expanded our **ProductionVPC** to include two public subnets and two private subnets across two Availability Zones. This will enable us to deploy duplicate workloads in each Availability Zone to design for high availability.

In the next exercise, we will deploy our first custom security group in **ProductionVPC**. This security group will be used to define what types of traffic we will allow inbound to an EC2 instance that will be deployed in the third exercise.

Exercise 7.2 – Creating a Bastion Host security group

In this exercise, we will create a custom security group that will be used by an EC2 instance. This will act as a Bastion Host, as previously discussed in this chapter. Let's get started:

1. Log in to your AWS account and navigate to the VPC console. Ensure you are in the **us-east-1** Region. From the left-hand menu, confirm that **ProductionVPC** is available in this Region.
2. Select the **Security Groups** link from the left-hand menu, which is located under the **Security** category, as shown in the following screenshot:

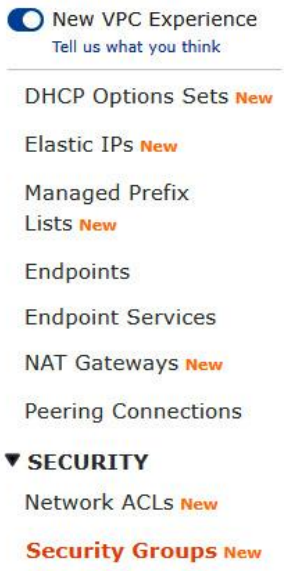

Figure 7.20 – Selecting Security Groups from the VPC console

3. Click on the **Create security group** button on the top right-hand corner of the screen.
4. Under **Basic details**, provide a name for your security group; for example, `BastionHost-SG`.
5. Next, provide an appropriate description, such as `Allow Remote Access to Bastion Host Server`.
6. Under **VPC**, make sure your select **ProductionVPC** from the drop-down list.
7. Next, under the **Inbound rules** section, click the **Add rule** button.
8. Select **RDP** for the type of rule. **RDP** is a remote access protocol that's used to connect to Microsoft Windows servers and desktops. RDP uses the TCP (6) protocol and operates on port `3389`.
9. Under the **Source** column, ensure that **Custom** is selected and in the text box, type in `0.0.0.0/0`. This IP block represents all external networks, including the internet.
10. Next, click on the **Create security group** button on the bottom right-hand corner of the page.

You will receive a successful creation message to confirm that the security group has now been created. We will use this security group in the next exercise to ensure that we can connect to our EC2 instance over the **Remote Desktop Protocol** (RDP), which operates on port `3389`.

Exercise 7.3 – Launching an EC2 instance

In this exercise, we will launch a Windows-based EC2 instance in **Public Subnet One** of our **ProductionVPC**. We will use this EC2 instance as a Bastion Host, allowing us to configure other EC2 instances in the VPC:

1. Log in to your AWS account and from the **Services** drop-down list, select **EC2** under the **Compute** category, as shown in the following screenshot:

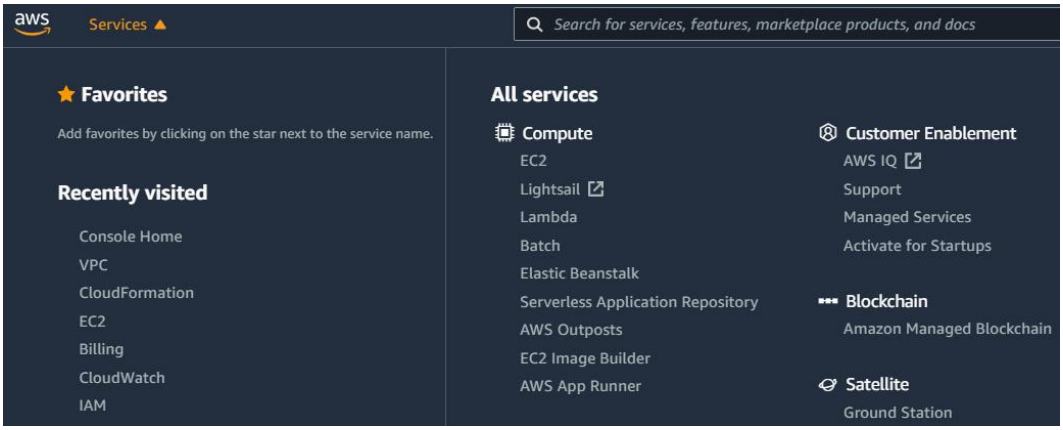

Figure 7.21 – Accessing the EC2 console

2. From the **Regions** list in the top right-hand corner, ensure that you are in the **US East N.Virgina (us-east-1)** Region.

3. On the **EC2** dashboard, you will note that there are 0 Instances in the running state.

4. Click on the **Instances (running)** link, as shown in the following screenshot. This will bring up the **Instances** console:

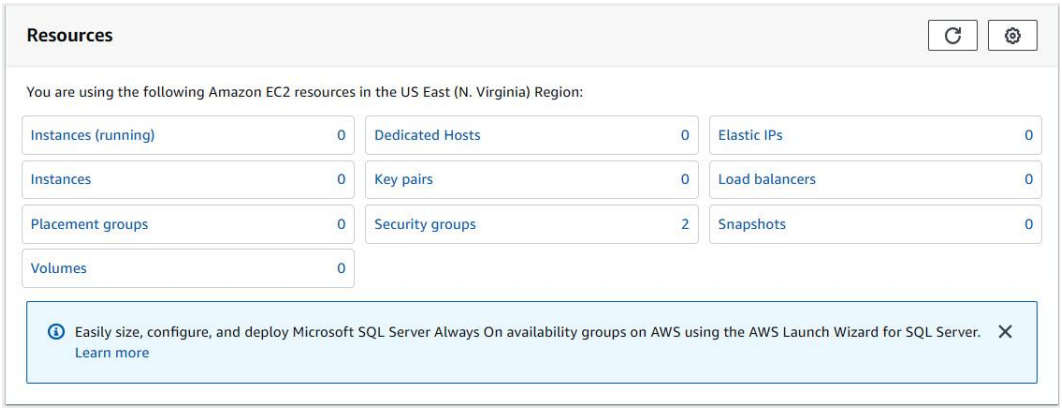

Figure 7.22 – EC2 dashboard

5. From the **Instances** console, select the **Launch instances** button from the top right-hand corner of the screen.

6. You will now be presented with **Step 1: Choose an Amazon Machine Image (AMI)**. From the list of available AMIs, select **Microsoft Windows Server 2016 Base - ami-05ce3abcaf51f14b2**.

7. In **Step 2: Choose an Instance Type**, ensure that the checkbox next to the **t2.micro** instance is selected. This instance type is available as part of your Free Tier offering.

8. Next, click the **Next: Configure Instance Details** button in the bottom right-hand corner of the screen.

9. In **Step 3: Configure Instance Details**, choose the following options:

    - For Network, select ProductionVPC.
    - For Subnet, select the Public Subnet One subnet.
    - For Auto-assign Public IP, select Enable.
    - Leave all the remaining settings as their default values and click the Next: Add Storage button in the bottom right-hand corner of the screen.

10. In **Step 4: Add Storage**, accept the default root volume size and click on the **Next: Add Tags** button in the bottom right-hand corner of the screen.

11. In **Step 5: Add Tags**, provide a key-value combination to tag the EC2 instance with a name, as shown in the following screenshot. For **Key**, type in `Name`, and for **Value**, type in `Windows-BastionSrv`:

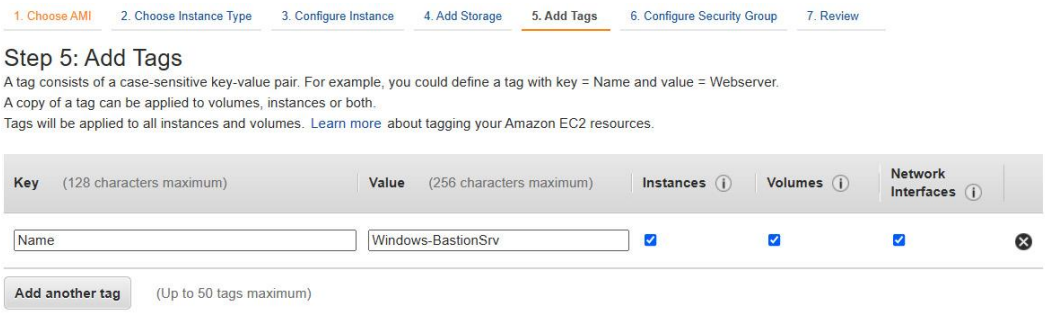

Figure 7.23 – Step 5: Add Tags

12. Next, click the **Next: Configure Security Group** button in the bottom right-hand corner of the screen.

13. In **Step 6: Configure Security Group**, click on the **Select an existing security group** option under the **Assign a security group** heading.

14. Next, from the list in the **Security Group ID** column, select the security group ID that corresponds to the newly created **BastionHost-SG**, which we set up in the previous exercise.

15. Finally, click on the **Review and Launch** button in the bottom right-hand corner of the screen.

16. You will then be presented with **Step 7: Review Instance Launch**. Review the settings you have defined and then click on the **Launch** button in the bottom right-hand corner of the screen.

17. At this point, you will be presented with another dialog box, requesting you to either select an existing EC2 key pair or create a new key pair.

Key pairs are cryptographically encrypted public/private keys that are used to encrypt the credentials required to authenticate against the EC2 instance operating system so that you can remotely access them.

For Microsoft Windows-based EC2 instances, the public key of the keys pair is used to encrypt the *Administrator* password. You then use the private key to decrypt the password to remotely access the Windows machine. For Linux-based EC2 instances, the private key can be used to establish a **Secure Socket Shell** (**SSH**) connection. Establishing SSH connections to your Linux-based EC2 instance allows you to work on the server remotely using the Linux shell interface. Let's take a look:

1. In the **Select an existing key pair or create a new key pair** dialog box, select the option to **Create a new key pair**, from the drop-down list.
2. Next, provide a key pair name. For example, I am naming my key `USEC2Keys`.
3. Click on the **Download Key Pair** button, which will download the private key in `.pem` format into your load `Downloads` folder. Make sure that you copy and save the keys in a safe location or on the desktop for easy access.
4. Next, click on the **Launch Instances** button to launch your EC2 instance.
5. On the **Launch Status** page, click on the **View Instances** button at the bottom right-hand corner of the page.

At this point, you will be redirected to the instances console and will be able to see your EC2 instance, as per the following screenshot:

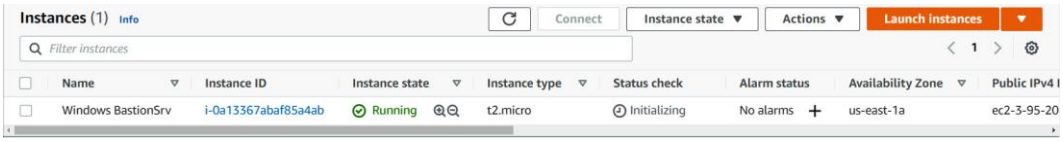

Figure 7.24 – Successfully launched the Windows BastionSRV EC2 instance

It will take a few minutes for the server to fully launch and become accessible. Look out for the **Status Check** column, as per the preceding screenshot, and ensure that AWS has completed all its checks; you will receive a **2/2 checks passed** message in the **Status check** column.

You can now remotely connect to the Windows Server using the Microsoft Remote Desktop client. If you are performing these labs from a laptop or desktop using Microsoft Windows, then the **remote desktop client** will already be installed on your machine. Simply click the **Start** button and search for the `Remote Desktop Connection` app. If you are performing these labs on a macOS-based computer, you will need to download the Microsoft Remote Desktop client from the Apple Play Store.

To connect to your new Windows Bastion Host server, follow these steps:

1. From the EC2 instances console, click on the checkbox next to the EC2 instance you have just launched.
2. In the bottom pane, make a note of the EC2 instance's public IP address.

3. Next, with the EC2 instance still selected, click on the **Actions** menu from the top right-hand corner of the screen, and then on the **Security** sub-menu. From here, select the **Get Windows password** link, as per the following screenshot:

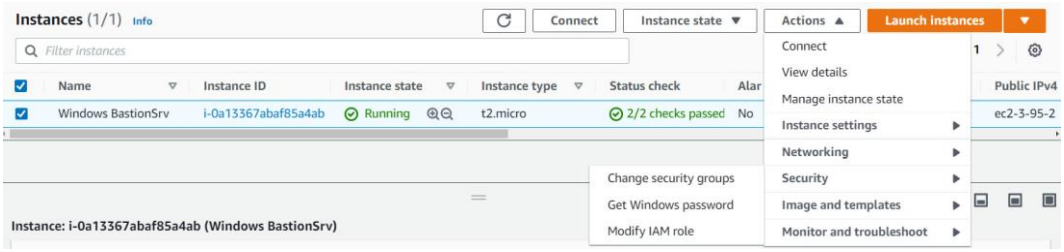

Figure 7.25 – The Get Windows password option for your EC2 instance

4. You will be presented with the **Get Windows password** page. Here, you need to browse for the EC2 key pairs you previously downloaded using the **Browse** button. Select the key pair from the location where you stored a copy of it; you should also find that it is still in the `Downloads` folder.

5. Upon selecting the key, you will note that the text box below the **Browse** button gets populated with the encrypted key, as per the following screenshot:

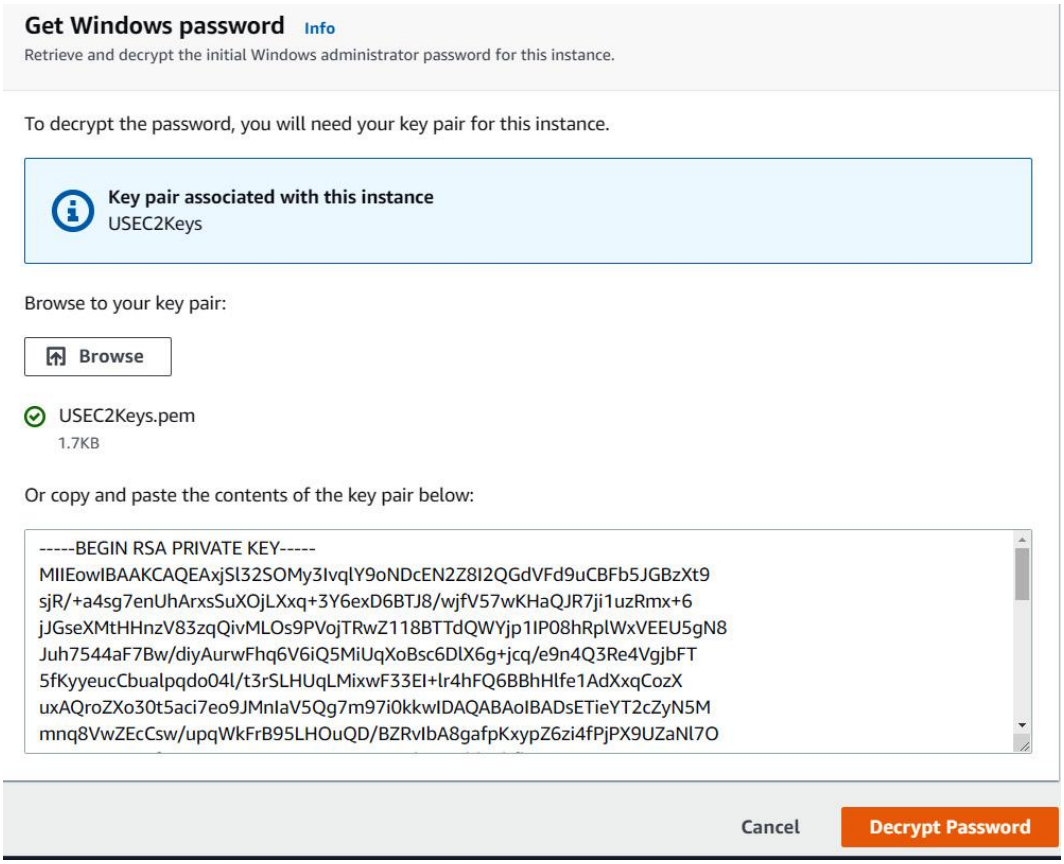

Figure 7.26 – Decrypting your key pairs

6. Click on the **Decrypt Password** button in the bottom right-hand corner of the screen; you will be provided with the Windows Administrator password. Make a note of this password.

7. Next, launch your **Remote Desktop Connection** application.

8. In the **Remote Desktop Connection** app, type in the public IP address of your Windows Bastion Server in the text box, next to the **Computer:** field, as per the following screenshot:

Figure 7.27 – Remote Desktop Connection client

9. Click the **Connect** button.

10. You will be prompted to provide your security credentials in the Windows Security dialog box, as per the following screenshot:

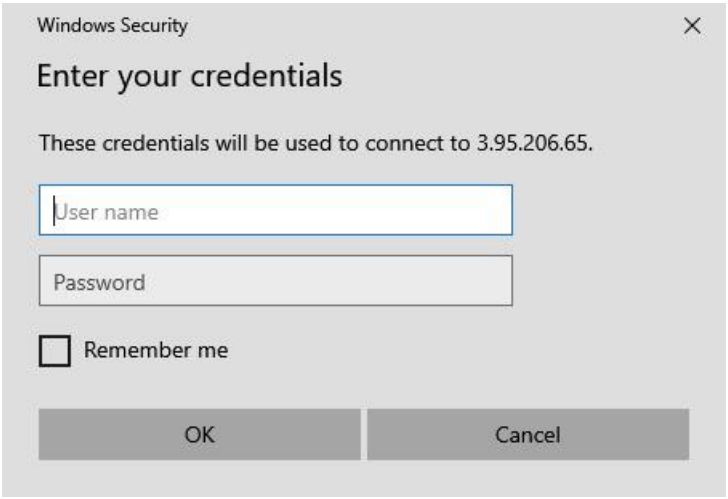

Figure 7.28 – Windows Security – Enter your credentials

11. For **Username**, type in `Administrator`.

12. For **Password**, type in the password you decrypted earlier, and then click **OK**.

13. If the password has been correctly typed in, you will be prompted with a **Remote Desktop Connection** security prompt, informing you that the connection to the remote computer cannot be authenticated due to its security certificate. This warning message can be ignored and you can proceed to log in to the server, as per the following screenshot:

Figure 7.29 – RDP certificate warning dialog box

14. Click on the **Yes** button to proceed with the remote connection.

15. The Remote Desktop client should now connect you to the remote Windows Server, as per the following screenshot:

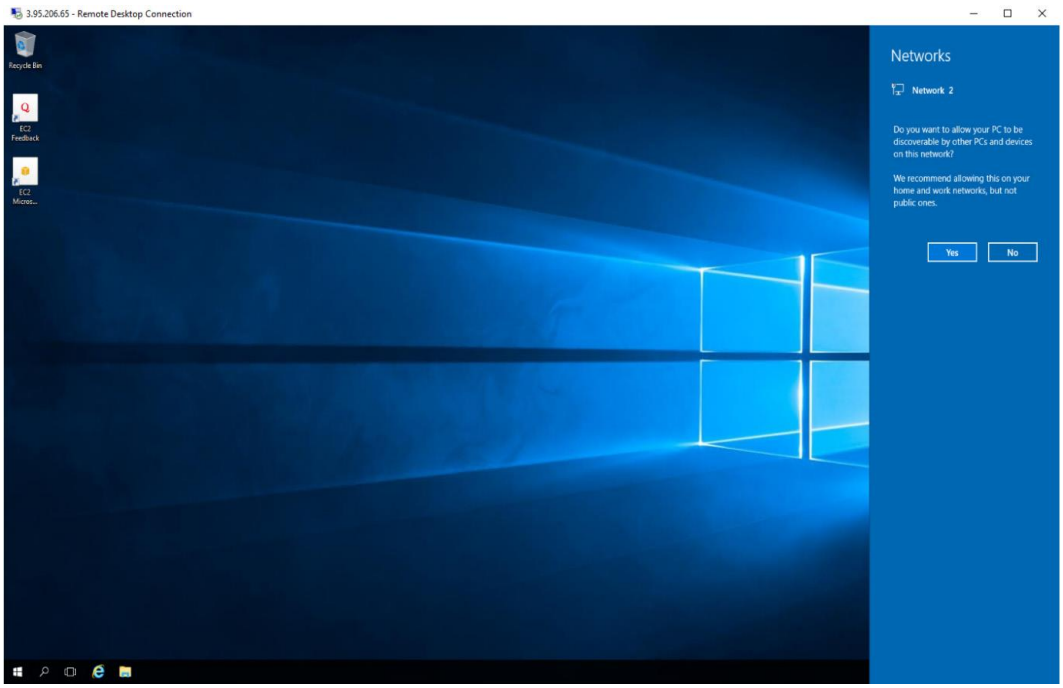

Figure 7.30 – Remote Bastion Host Server

In this exercise, you were able to launch a new EC2 instance that will act as our Bastion Host server. You will be able to remotely connect to the Windows EC2 instance using the RPD client and can now perform any operation, as required, on this server.

Important Note

As part of ending this exercise, you should terminate your EC2 instances to ensure you do not go over the billing alarm threshold you configured in *Chapter 4*, *Identity and Access Management*. To terminate your EC2 instances, from the EC2 dashboard, click on **Instances** from the left-hand menu. Next, select the checkbox next to the **Windows BastionSrv** EC2 instance you launched. Then, from the top right-hand menu, click on the **Instance state** drop-down menu and select **Terminate instance**. You will be prompted to confirm that you wish to terminate your EC2 instances. Go ahead and click the **Terminate** button.

In the next exercise, we will demonstrate the Amazon ECS service while focusing on the Fargate launch type with a simple example.

Exercise 7.4 – Launching an application on Amazon Fargate

In this exercise, you will launch a task on ECS, which is essentially a Docker container:

1. Log in to your AWS account as **Alice** and in the top search bar in the AWS Management Console, type in `ECS`.
2. From the search results, select **Elastic Container Service**.
3. You will be presented with the ECS splash screen, as per the following screenshot:

Figure 7.31 – Amazon ECS

4. From the left-hand menu, select **Clusters**.
5. In the right-hand pane, click the **Create cluster** button.
6. You will be prompted to select the cluster template. You will be deploying a Fargate cluster, so go ahead and select the **Network only** option design for use with either AWS Fargate or an external instance capacity.
7. Click the **Next step** button at the bottom of the page.
8. On the next screen, name your cluster `MyCluster`.

9. Next, click the **Create** button at the bottom of the page.
10. You will see a notification once the cluster has been created. Click the **View Cluster** button.
11. Next, from the left-hand menu, click on **Task Definition**.
12. In the right-hand pane, click the **Create new Task Definition** button.
13. You will then be prompted to select the launch type's compatibility, as per the following screenshot:

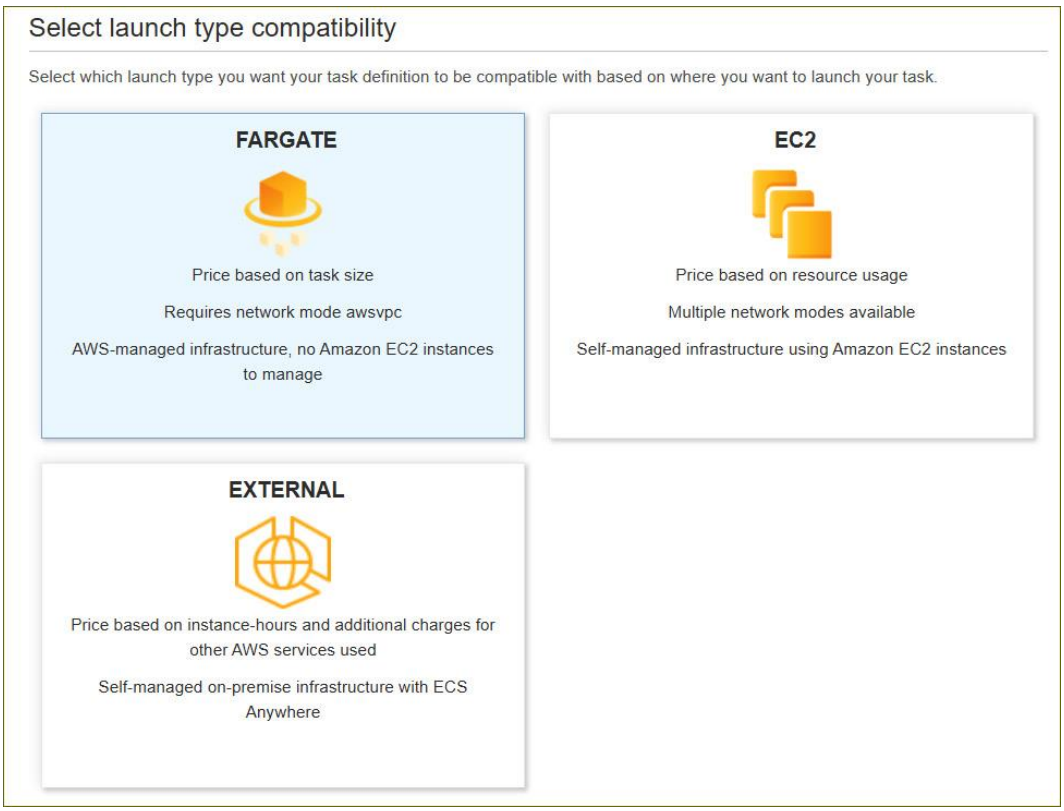

Figure 7.32 – ECS task definition

14. Select the Fargate type and click the **Next step** button at the bottom of the page.
15. Provide a name for your task definition; for example, `fargate-task`.
16. Scroll further down and under **Task size**, set **Task memory (GB)** to **1GB**.
17. Next, set **Task CPU (vCPU)** to **0.5 vCPU**.
18. Next, under **Container Definitions**, click the **Add container** button.
19. You will be selecting an existing container here, so in the **Add container** dialog box, for **Container name**, type in `nginx`.
20. Similarly, for **Image**, ensure you type in `nginx`, as per the following screenshot:

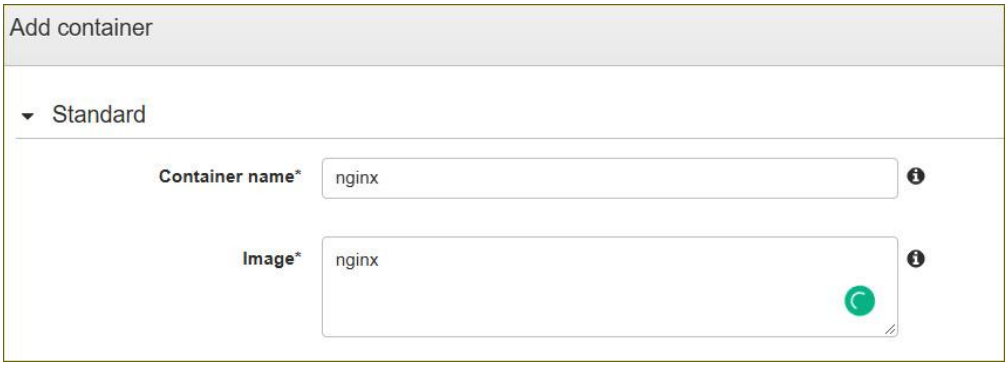

Figure 7.33 – Fargate launch container

21. Next, for **Port mappings**, type in `80` for the **Container** port.
22. Scroll toward the bottom and click the **Add** button. This will take you back to the **Create new Task Definition** page. Scroll toward the bottom and click on the **Create** button.
23. After a few seconds, you should find that your task definition has been created.
24. Click on the **View task definition** button. This will take you back to the ECS dashboard.
25. Next, click on the **Clusters** link from the left-hand menu. You will see that your **MyCluster** cluster is now available. Click on the **MyCluster** link.
26. Next, click on the **Task** tab.
27. Click the **Run new Task** button.
28. On the **Run Task** page, ensure that **Launch type** is set to **Fargate**.
29. You will find that the task definition has been pre-populated with your task. If not, select it from the drop-down arrow.
30. For **Number of tasks**, ensure that only `1` is set as we will only run one task.
31. Under **VPC and security groups**, select **ProductionVPC**.
32. For **Subnets**, select **Public Subnet One**.
33. For **Security groups**, click the **Edit** button next to the provided security group name.
34. You will be prompted to create a new security group, as per the following screenshot:

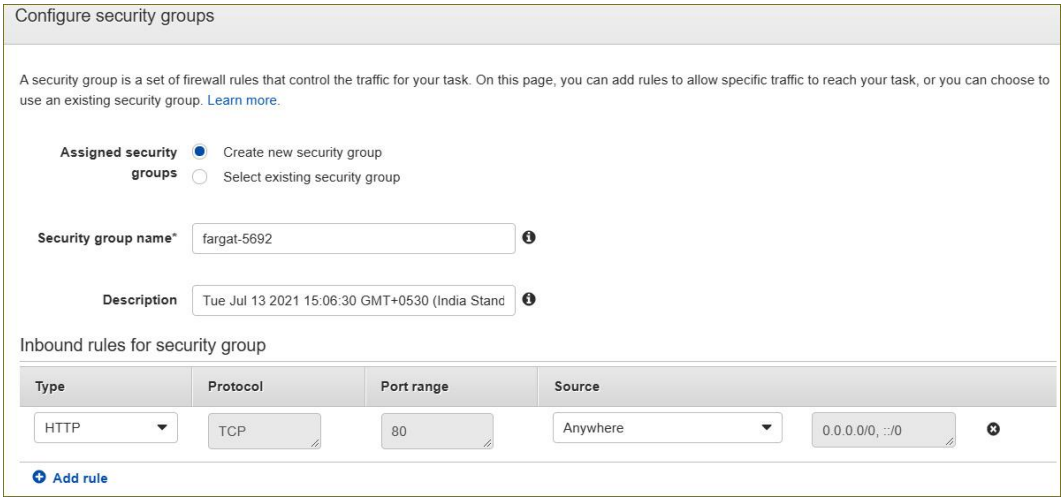

Figure 7.34 – Fargate task security group

35. Accept the default to create an inbound rule that allows port `80` from the internet. Click the **Save** button at the bottom of the page.

36. Next, ensure that **Auto-assign public IP** is set to **ENABLED**.

37. Click the **Run Task** button at the bottom of the page.

38. You will be taken back to the ECS dashboard.

39. Within a few seconds, you should find that your task is now in the **RUNNING** status, as per the following screenshot:

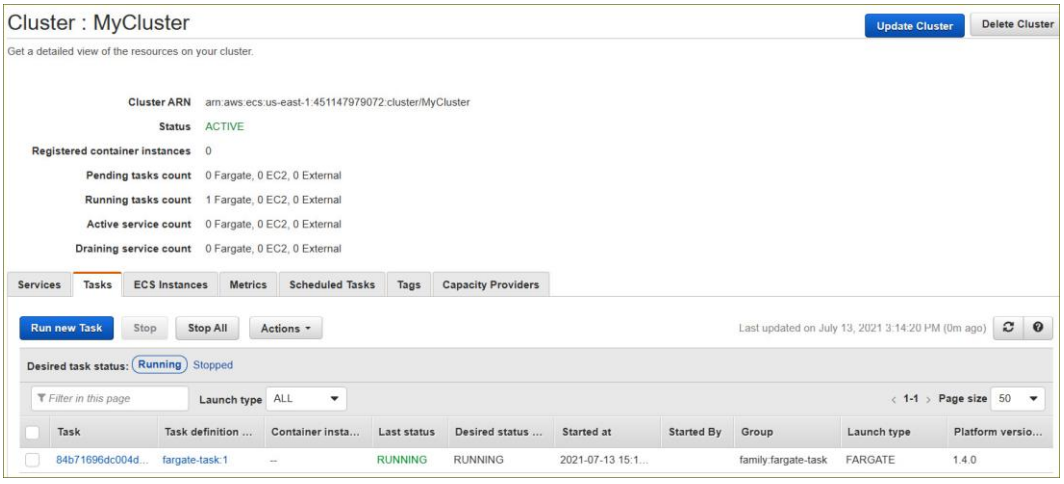

Figure 7.35 – Fargate running task

40. Next, under **Task**, click on the task ID link. This will bring up the **Details** page of the task.

41. Make a note of the **Public IP** address and copy and paste it into a new browser tab.

42. You should then find that you can connect to the `nginx` web page, as per the following screenshot:

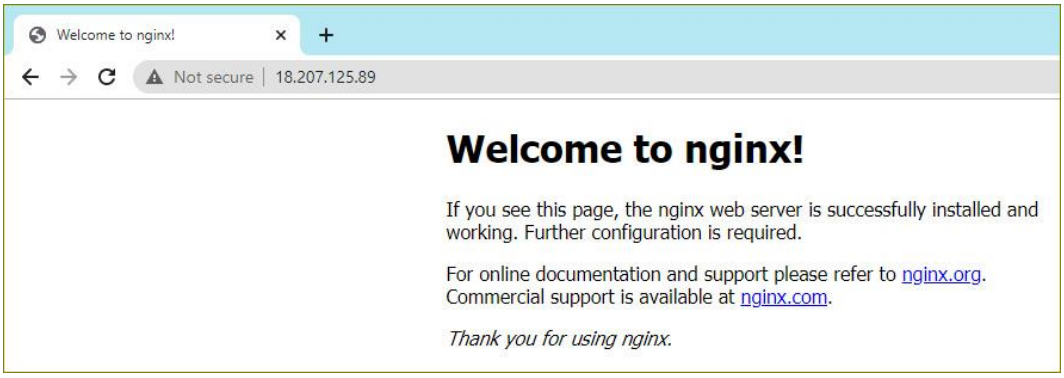

Figure 7.36 – nginx application running on Fargate

43. You have just deployed your first Fargate task!
44. To clean up, go back to your ECS dashboard. From the left-hand menu, click the **Clusters** link.
45. In the right-hand pane, click the **MyCluster** link.
46. Next, from the **Task** tab, select the checkbox next to your task.
47. Finally, click on the **Stop** button. You will be prompted to confirm your action. Click the **Stop** button in the dialog box that appears.
48. This will stop your task. You will also receive a notification, stating that the task was successfully stopped. You do not need to worry about the cluster as you only pay for the tasks on Fargate.

In this exercise, we demonstrated how you can launch a simple nginx Docker container on ECS using the Fargate launch type. Next, we will summarize this chapter.

Questions

1. Which AWS EC2 pricing option can help you reduce costs by allowing you to use your existing server-bound software licenses?
   A. On-Demand
   B. Reserved
   C. Spot
   D. Dedicated Hosts
2. Which AWS EC2 pricing option enables you to take advantage of unused EC2 capacity in the AWS cloud and can offer up to a 90% discount compared to On-Demand prices?
   A. Spot Instances
   B. Reserved Instances

C. On-Demand Instance

D. Dedicated Hosts

3. Which of the following is true with regards to the benefits of purchasing a Convertible EC2 Reserved Instance? (Choose 2 answers)

   A. You can exchange a Convertible Reserved Instance for a Convertible Reserved Instance in a different Region.

   B. You can exchange one or more Convertible Reserved Instances at a time for both Convertible and Standard Reserved Instances.

   C. To benefit from better pricing, you can exchange a No Upfront Convertible Reserved Instance for an All Upfront or Partial Upfront Convertible Reserved Instance.

   D. You can exchange All Upfront and Partial Upfront Convertible Reserved Instances for No Upfront Convertible Reserved Instances.

   E. You can exchange one or more Convertible Reserved Instances for another Convertible Reserved Instance with a different configuration, including instance family, operating system, and tenancy.

4. Which feature of the AWS EC2 service helps prevent accidentally terminating an EC2 instance by preventing the user from issuing a termination command either from the console or CLI?

   A. Enable "termination protection"

   B. Enable "termination protect"

   C. Enable "prevent termination"

   D. Enable "protect EC2"

5. Which storage solution enables you to share a common filesystem across multiple Linux-based EC2 instances that can be used to support applications that require access to data with very low latency connectivity?

   A. EFS

   B. EBS

   C. S3

   D. NTFS

6. Which type of IP address offering from AWS gives you a static, publicly routable address that will not change, even if you stop and restart an EC2 instance that it is associated with?

   A. Public IP address

B. Private IP address

C. Elastic IP address

D. Regional IP address

7. Which AWS service enables you to configure multiple Windows-based EC2 instances to share and access a common storage solution that is based on using the industry-standard SMB protocol and eliminate the administrative overhead of managing Windows file servers?

A. Amazon FSx for Windows File Server

B. Amazon Elastic File System

C. Amazon Elastic Block Store

D. Amazon DFS Volumes for Windows File Server

8. Which of the following types of EBS volumes can be used as boot volumes for your EC2 instances? (Select 2 answers)

A. General Purpose SSD (gp2)

B. Provisioned IOPS SSD (io1)

C. Throughput Optimized HDD (st1)

D. Cold HDD (sc1)

E. FSx for Windows

9. Which of the following AWS services enables you to quickly launch a web server with a pre-configured WordPress installation pack, offers predictable monthly pricing, comes with integrated certificate management, and provides free SSL/TLS certificates?

A. AWS Lightsail

B. AWS EC2

C. AWS RDS

D. AWS Elastic Beanstalk

10. Which AWS service can be used to run a piece of code that can create thumbnails of images uploaded to one Amazon S3 bucket and copy them to another S3 bucket?

A. AWS SNS

B. AWS Lambda

C. AWS RDS

D. AWS Snowball

Chapter 8

Figures

Primary Key

Customer-ID	First Name	Last Name	Flat/House	Street	Town
Cust001	Penny	Smith	11	Hoxton Grove	Richmond
Cust002	Mark	Edwards	18	Cavendish Ave	Harrow
Cust003	Luke	Skywalker	33	Hazelwood Ave	Morden
Cust004	Jean Luke	Picard	22	Delta Drive	Knightsbridge

Figure 8.1 – Customer contact table

Primary Key

Customer-ID	Order-ID	Order Date	Order Amount
Cust002	Omega001	12 April 2019	$200.75
Cust002	Omega002	15 June 2019	$250.99
Cust002	Omega003	17 August 2019	$330.99

Figure 8.2 – Customer order table

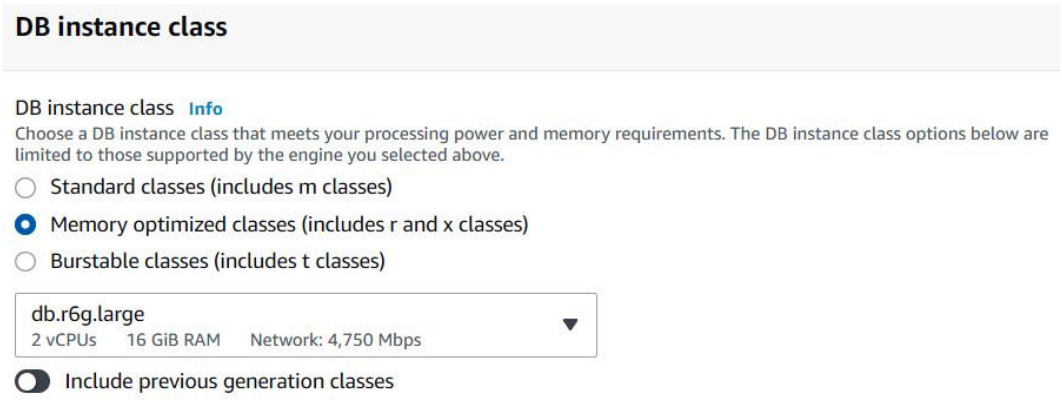

Figure 8.3 – Database instance class options

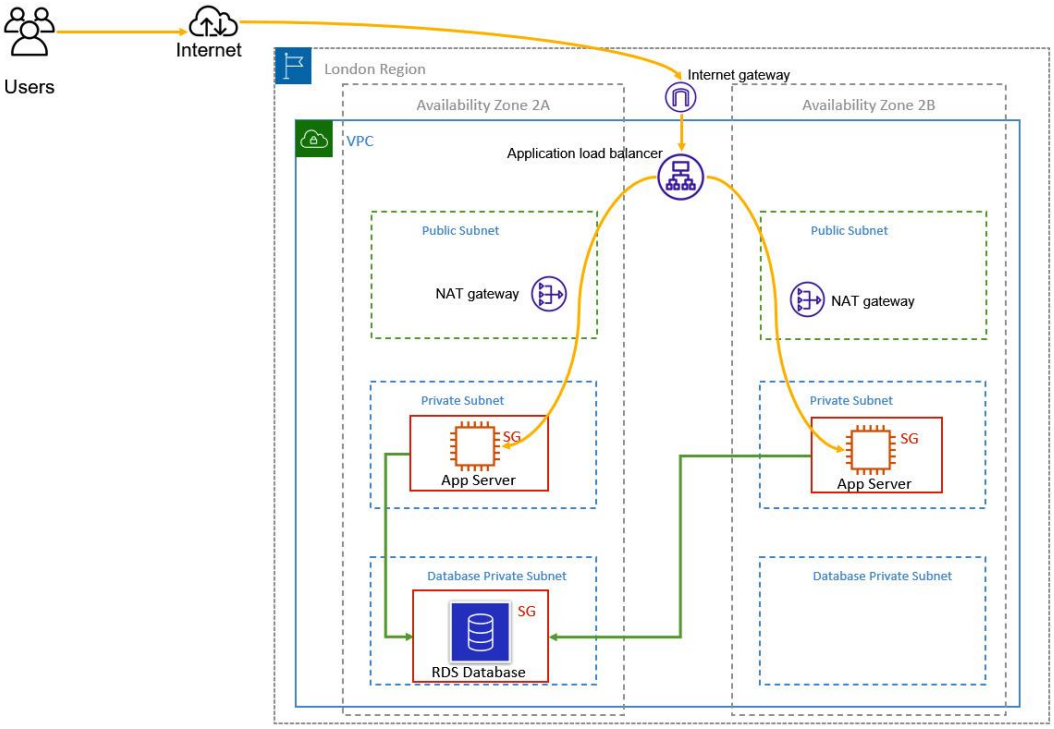

Figure 8.4 – Amazon RDS deployed in a VPC in private subnets

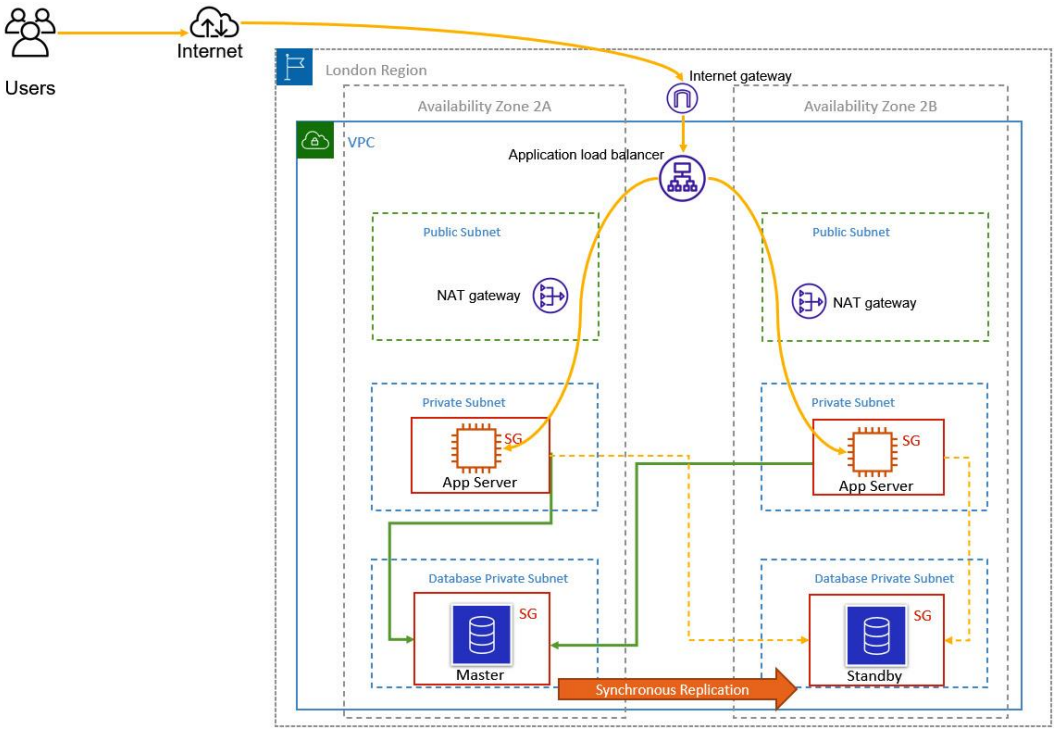

Figure 8.5 – Amazon RDS configured with Multi-AZ

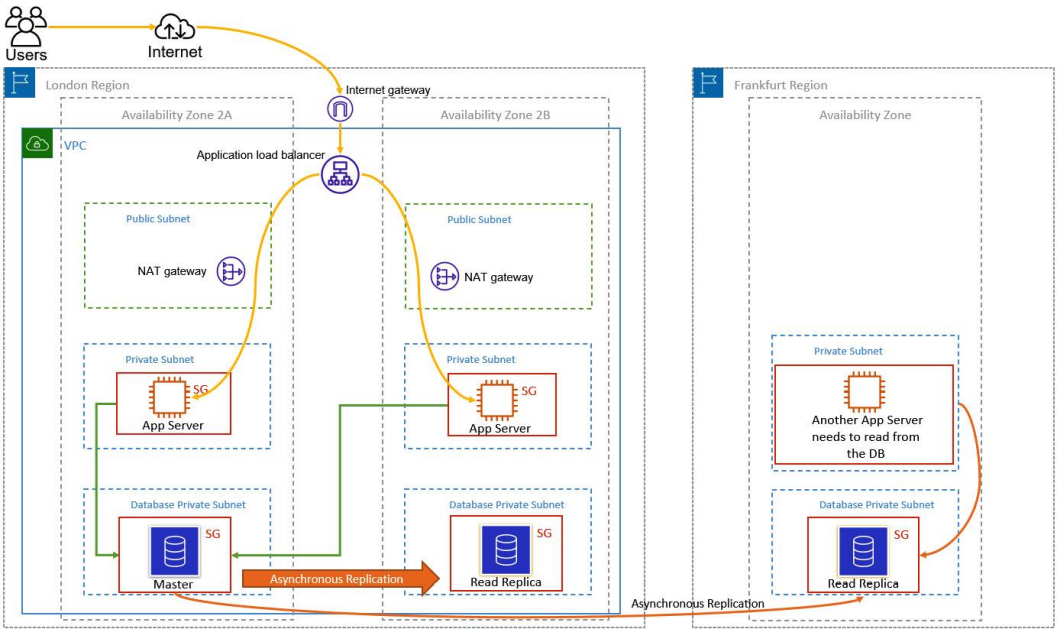

Figure 8.6 – AWS RDS with read replicas

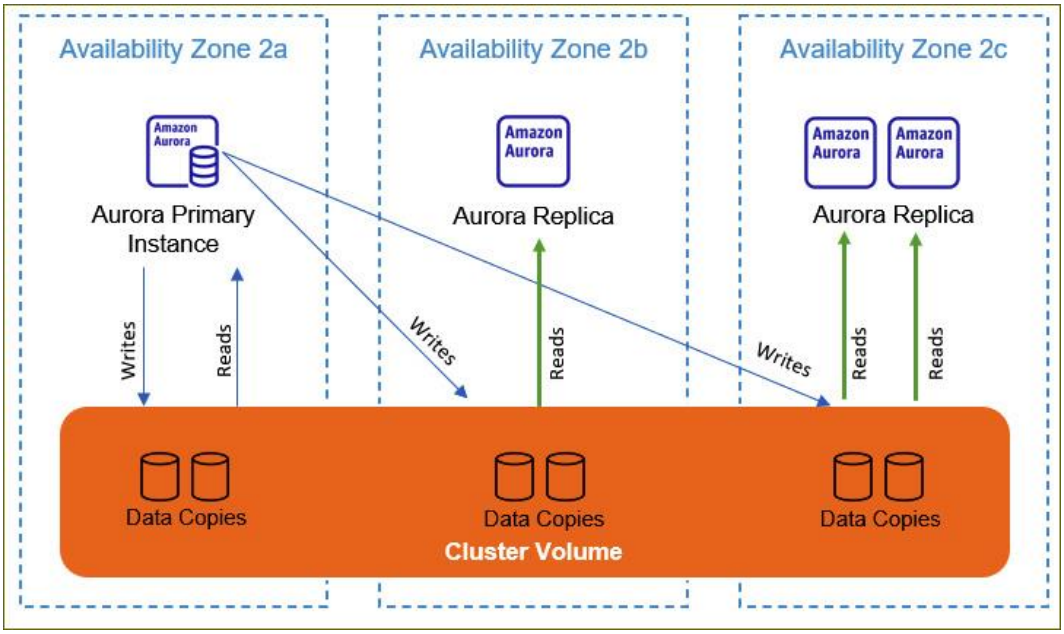

Figure 8.7 – Amazon Aurora DB cluster architecture

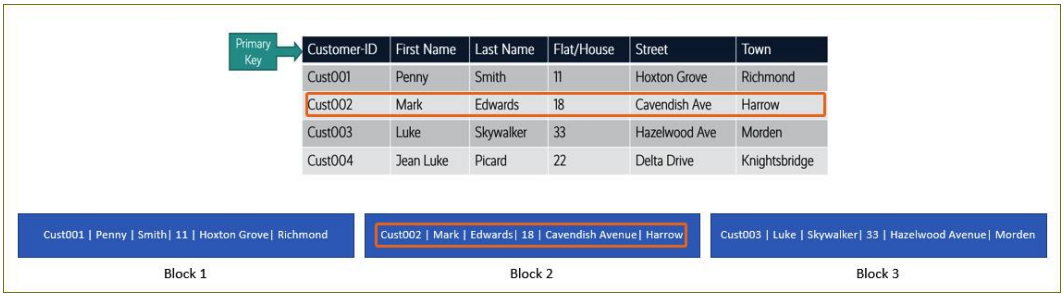

Figure 8.8 – Data stored in blocks on disk

Figure 8.9 – Data stored on Amazon Redshift

Exercise 8.1 – Extending your VPC to host database subnets

In *Chapter 7*, *AWS Compute Services*, you expanded your VPC to include both private subnets and public subnets. Generally, you would only host services in a public subnet that would need direct exposure on the internet. Examples include the bastion host server we deployed earlier in *Chapter 7*, *AWS Compute Services* (which we will discuss in the next chapter).

Most applications are deployed across tiers – so, for example, you can have a web tier, an application tier, and a database tier. These different tiers are designed to separate different components of your application stack, allowing you to create a degree of isolation, as well as benefit from a layered security model. In *Chapter 7*, *AWS Compute Services* , as part of *Exercise 7.1 – Expanding ProductionVPC so that it includes two public subnets and two private subnets*, you also configured two private subnets across two Availability Zones to host your application servers. In this example, the application tier and web tier are the same. However, in many real-world scenarios, they would be separate.

In this exercise, you will be extending your VPC to add an additional tier, known as the database tier, within which you will be able to launch an Amazon RDS database. Like EC2 instances, Amazon RDS needs to be deployed in a VPC.

In the following diagram, you can see that your VPC now has three tiers – a public (DMZ) tier to host bastion host servers, NAT gateways, and Elastic Load Balancers, an application tier comprised of the **Private Subnet One – App** and **Private Subnet Two – App** subnets, and finally, a database tier comprised of the **Private Subnet Three – Data** and **Private Subnet Four – Data** subnets. Note that the subnets are spread across two Availability Zones to enable you to offer high availability of services in the event of an Availability Zone failure. We will discuss high availability in more detail in the next chapter:

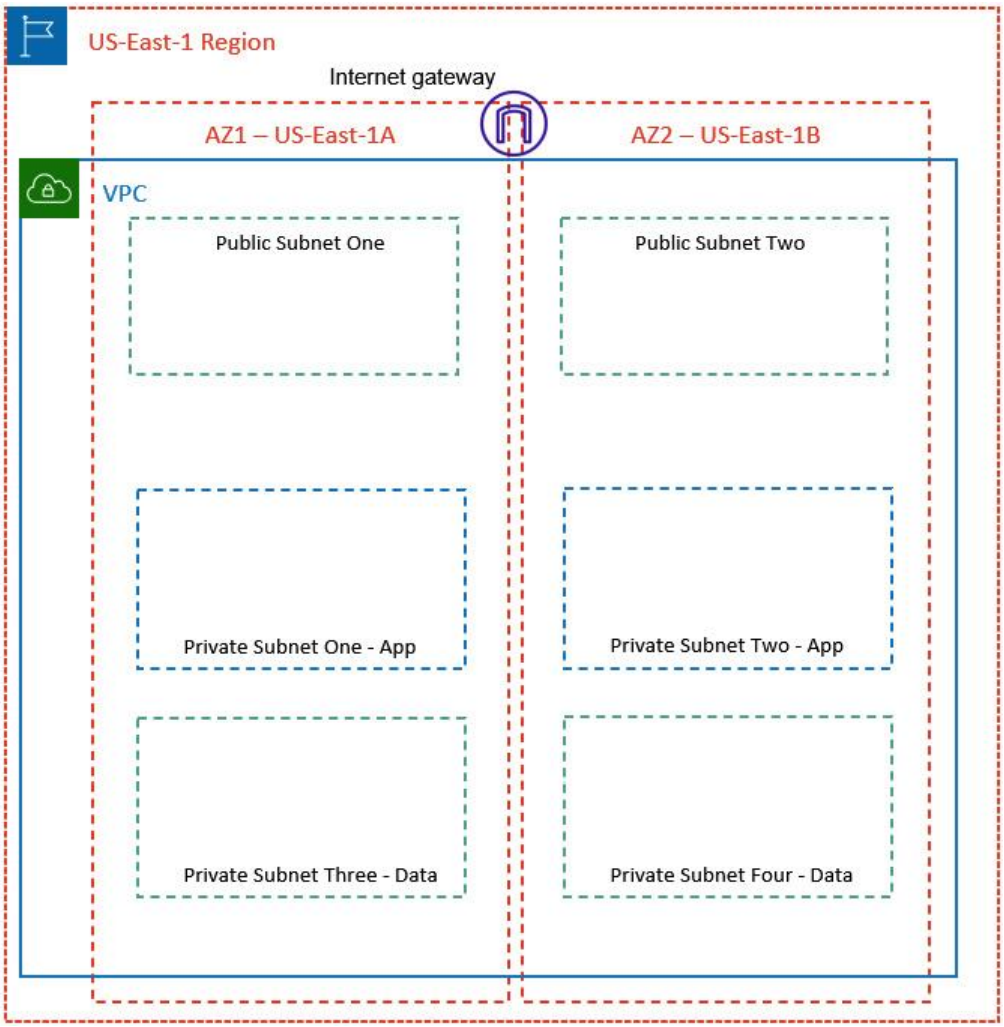

Figure 8.10 – Extending the VPC to include a database tier

Let's start by extending your VPC so that it includes our database tier:

1. Log back into your AWS account as our administrator, **Alice**.
2. Navigate to the **VPC** dashboard and ensure you are in the **US-East-1** Region.
3. In the left-hand menu, click on **Subnets**.
4. Next, click the **Create subnet** button in the top right-hand corner of the screen.
5. You will be presented with the **Create subnet** wizard page.
6. Under **VPC ID**, select **ProductionVPC** from the drop-down menu.
7. In the **Subnet settings** section, under **Subnet 1 of 1**, provide a name for your first database subnet. For this exercise, name your subnet **Private Subnet Three – Data**.
8. Under **Availability Zone**, select the **us-east-1a** Availability Zone.
9. Next, for **IPv4 CIDR block**, type in `10.0.5.0/24`.

10. Next, rather than create this subnet and repeat the wizard to create the second database subnet, simply click on the **Add new subnet** button, as per the following screenshot:

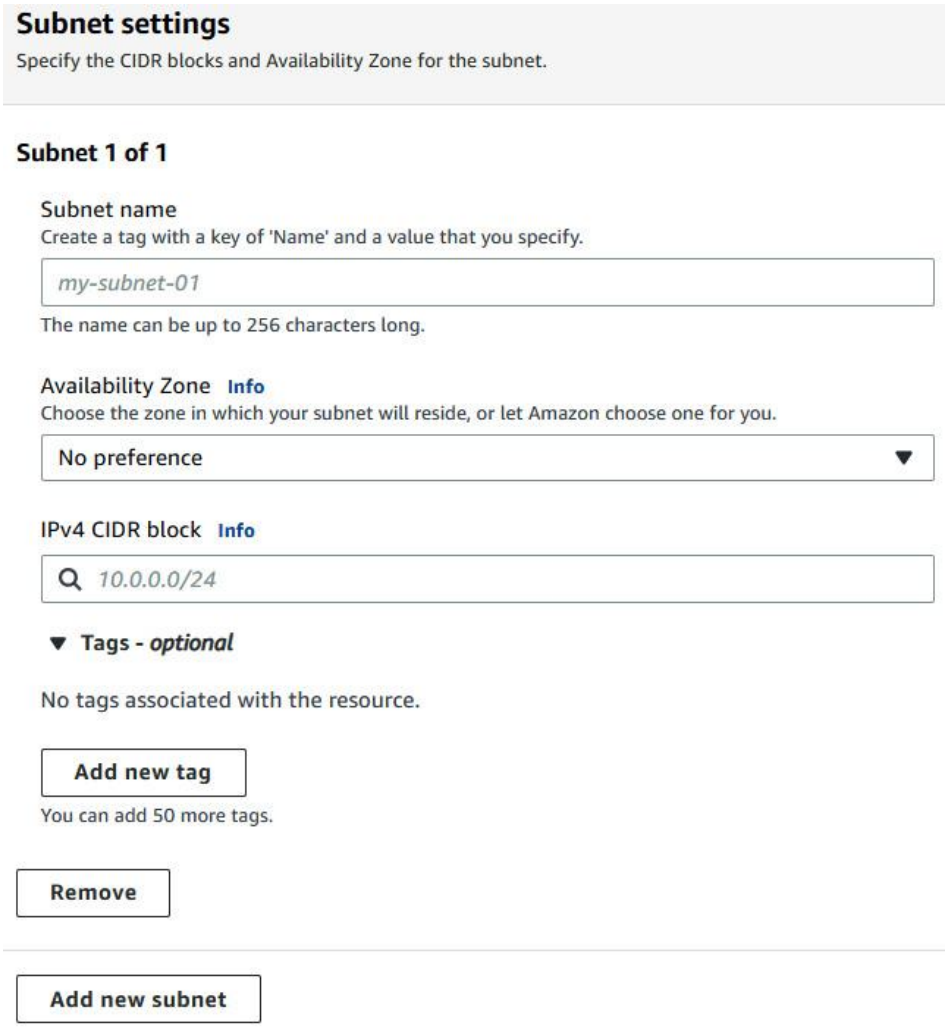

Figure 8.11 – Creating multiple subnets

11. A new subsection, **Subnet 2 of 2**, will appear, allowing you to create an additional subnet in the same wizard. Under **Subnet name**, type in **Private Subnet Four – Data**.
12. For **Availability Zone**, select the **us-east-1b** Availability Zone from the drop-down list.
13. For **IPv4 CIDR block**, type in `10.0.6.0/24`.
14. Click the **Create subnet** button at the bottom of this page.

AWS will successfully create two new subnets, which you will use to host your Amazon RDS database. In the right-hand menu, click on **Subnets** to view all the subnets now associated with your **ProductionVPC**, as per the following screenshot:

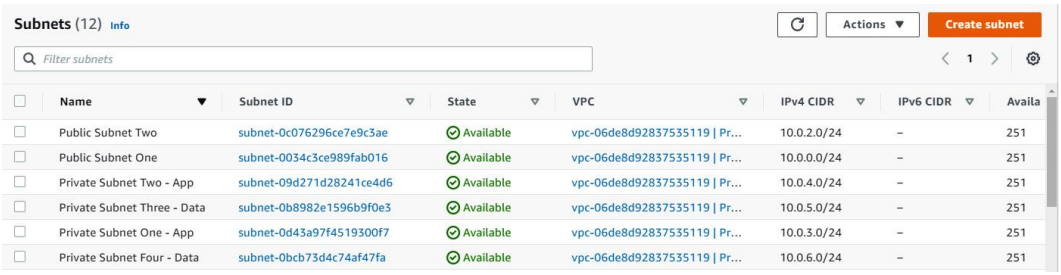

Figure 8.12 – Subnets in ProductionVPC

Now that you have created an additional two subnets for your **ProductionVPC**, you can proceed with the next part of this exercise. Like EC2 instances, Amazon RDS databases require you to configure the necessary security groups that will permit traffic to the database instances.

In our layered security model, we wish to ensure that only our application servers will be able to communicate with the databases in the backend. In this part of the exercise, you will create a new security group that will be configured to allow database-relevant traffic from any application servers you deploy later. To do this, you must configure an inbound rule on the new database security group to accept traffic on port `3306` for MySQL traffic from the security group of the application servers, specifically from the **AppServers-SG** security group. Let's get started:

15. Ensure you are currently in the **VPC** dashboard. Then, from the left-hand menu, click on **Security Groups**.
16. Click the **Create security group** button in the top right-hand corner of the screen.
17. For **Security group name**, type in `Database-SG`. Under description, type in `Allow MYSQL traffic from AppServer-SG`.
18. Under **VPC**, ensure you select **ProductionVPC** from the drop-down list.
19. Next, in the **Inbound rules** section, click on the **Add rule** button.
20. Under **Type**, select **MySQL/Aurora**.
21. Ensure that **Source** is set to **Custom**, and in the search box, start typing `sg-`. You should see that a list of all security groups shows up in a list. Select the **AppServers-SG** security group.
22. Provide an optional description if required.
23. Click on the **Create security group** button in the bottom right-hand corner of the screen.

AWS will now confirm that the security group has been created successfully.

In this exercise, you extended your VPC to host two additional private subnets that we will use to host our Amazon RDS database. You also created a new security group, **Database-SG**, which will be associated with our Amazon RDS database instance. It will also allow MySQL/Aurora traffic on port `3306` from any EC2 instance that is associated with the **AppServer-SG** security group.

In the next exercise, we will configure an Amazon RDS database subnet group that will be used to inform Amazon RDS of which subnets it can deploy our databases to.

Exercise 8.2 – Creating a database subnet group

Before you can launch an RDS database in your VPC, you need to define a DB subnet group. A **DB subnet group** is a collection of two or more subnets within the VPC where you want to deploy your database instance. When creating your DB subnet group, at least two subnets must be selected in the VPC that are associated with two separate Availability Zones in a Region. Amazon RDS uses the subnet group's IP address CIDR block to assign your RDS database instance(s) with an IP address.

Amazon RDS can then deploy the database instance on one of your chosen subnets that is part of the group. In the case of a Multi-AZ deployment, the master copy will be deployed in one subnet in a particular Availability Zone, while the standby copy will be deployed in another subnet that is hosted within another Availability Zone.

Note that the subnets in a DB subnet group are either public or private, but they cannot be a mix of both public and private subnets. Ideally, you want to configure private subnets as part of your subnet group because you want to deploy any backend databases in the private subnets of your VPC. Your databases should only be accessible from web/application servers and not directly from the internet.

To set up the DB subnet group, follow these steps:

1. Ensure that you are logged into your **AWS Management Console** as the IAM user **Alice**.
2. From the top left-hand menu, click on the **Services** drop-down arrow and select **RDS** located under the **Database** category. This will take you to the Amazon RDS dashboard.
3. Ensure that you are in the **us-east-1** Region and from the left-hand menu, click on **Subnet groups**.
4. Next, in the main pane of the screen, click the **Create DB Subnet Group** button.
5. On the page that appears, you will need to define your DB subnet group details:

- Provide a name for your DB subnet group; for example, `ProductionVPC-DBSubnet`.
- For the description, type in `DB Subnet Group to host RDS Database in Production VPC`.
- Under **VPC**, select **ProductionVPC** from the drop-down menu.
- Next, under **Availability Zone**, choose the Availability Zones that include the subnets you want to add. For this exercise, select the checkboxes next to **us-east-1a** and **us-east-1b**.

6. Next, under **Subnets**, select the subnets you created earlier for your RDS database. When you click on the drop-down list next to **Subnets**, you will notice that the subnet names are not visible; instead, the subnets are identified by their subnet IDs. You can determine the correct subnets by cross-referencing the subnet ID against the subnets you created in the VPC dashboard, which you can access in another browser window. Alternatively, you can ensure you select the correct subnets by comparing their relative IPv4 CIDR blocks. So, in our example, the private DB subnets are in the `10.0.5.0/24` and `10.0.6.0/24` Ipv4 CIDR blocks, as per the following screenshot:

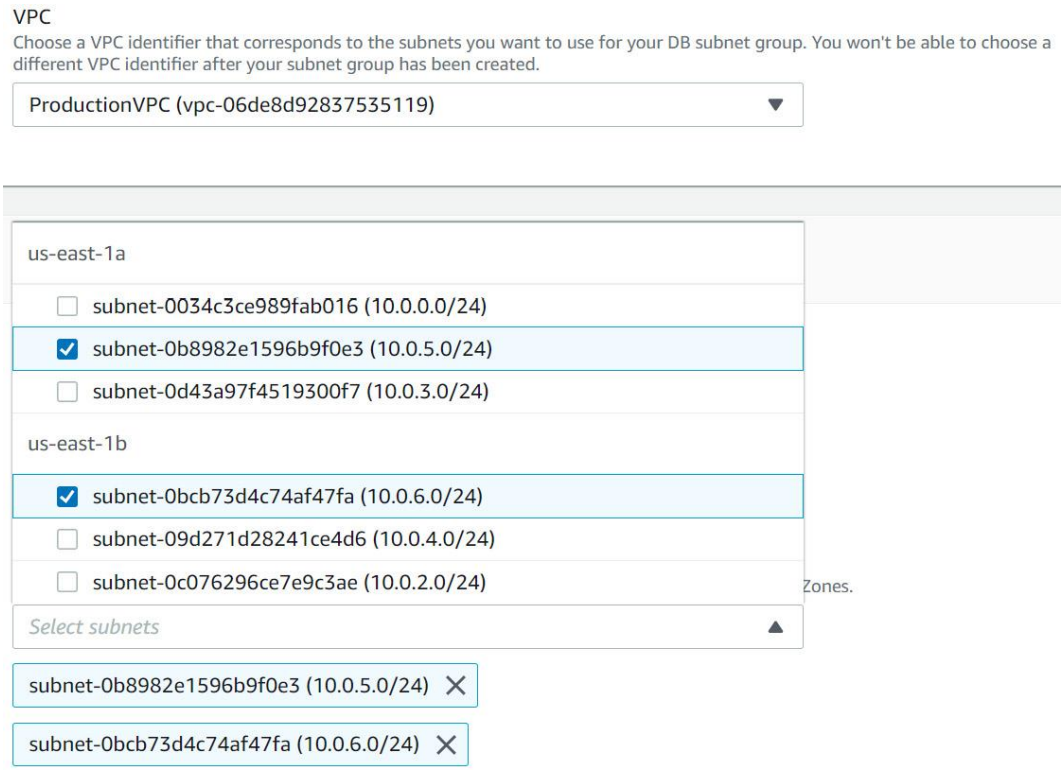

Figure 8.13 – Creating database subnet groups

7. Next, click the **Create** button at the bottom right-hand corner of the screen.

AWS will create your DB subnet group using the details you provided, as per the following screenshot:

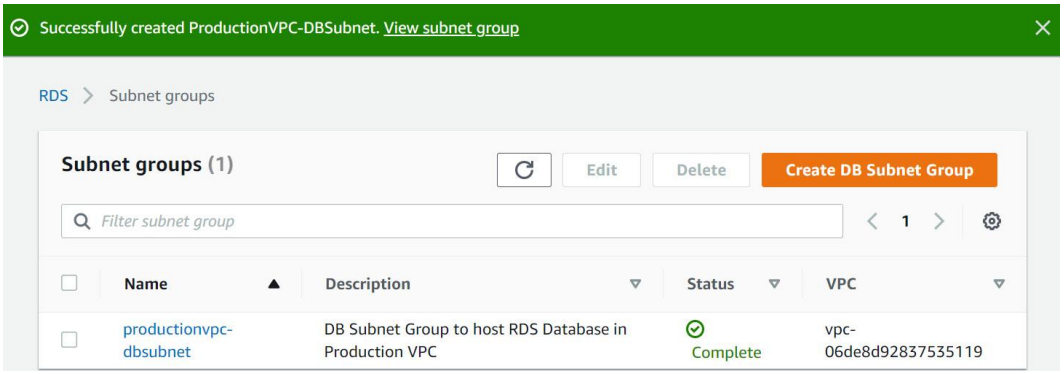

Figure 8.14 – Successfully creating a database subnet group

In this exercise, you learned about RDS DB subnet groups, which allow you to define a minimum of two subnets across two Availability Zones, where Amazon RDS can deploy your RDS DB instance when you choose to launch your database.

In the next exercise, we will launch our RDS database in **ProductionVPC**. We will also use this database to host the backend data of our web application, which we will then deploy in the fourth exercise of this next chapter.

Exercise 8.3 – Launching your Amazon RDS database in ProductionVPC

In this exercise, you will launch an Amazon RDS MySQL database in the DB subnet group of **ProductionVPC**. Let's get started:

1. Ensure that you are logged into your AWS account as the IAM user **Alice**.
2. Navigate to the Amazon RDS dashboard.
3. From the left-hand menu, select **Databases**.
4. On the right-hand side of the pane, click the **Create database** button.
5. Next, you will be presented with the **Create database** wizard, where you will need to define various parameters of your VPC. Amazon offers the `t2.micro` database instance running the MySQL engine as part of the Free Tier offering, which comes with the following features for up to 12 months:

- 750 hours of Amazon RDS in a Single-AZ db.t2.micro instance.
- 20 GB of General Purpose storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB snapshots.

6. For **Choose a database creation method**, select the option next to **Standard create**.
7. Next, for the database engine option, select **MySQL**.
8. Leave the **Edition** and **Version** settings as-is.
9. Under **Templates**, select the **Free Tier** option.
10. Next, you need to provide some settings:

- For the DB instance identifier, type in `productiondb`.
- Under **Credential Settings**, leave the **Master** username set to **admin** and provide a password of your choice. Make sure that you note this password down; otherwise, you will not be able to connect to the database.

11. Under **Database instance class**, leave the settings as-is.
12. Under **Storage**, leave the settings as-is except for **Storage autoscaling**, where you should *disable* the option for **Enable storage autoscaling**.
13. Under **Availability & durability**, you will note that the option to enable **Multi-AZ** is grayed out. This is because Multi-AZ is not available in the Free Tier.
14. Next, under **Connectivity**, do the following:

- Ensure that you select **ProductionVPC** from the drop-down list under **Virtual private cloud (VPC)**.
- Note that the subnet group has been pre-populated with the DB subnet group we created earlier, which in this case is `productionvpc-dbsubnet`.
- Under **Public Access**, select **No**.
- Next, under **VPC Security Group**, ensure that **Choose Existing** is selected. Then, from the drop-down list under **Existing VPC security groups**, select the **Database-SG** security group you created earlier.
- Next, under **Availability Zone**, you can select an AZ of your choice or leave it as the **No preference** option.
- Next, expand the **Additional configuration** option and ensure that the database port is set to `3306`.

15. Under **Database authentication options**, ensure that **Password authentication** is enabled.
16. Under **Additional configuration**, do the following:

- Type in the same database name as you did earlier for **DB instances identifier**. In our example, the name will be `productiondb`.
- Leave **DB parameters group** and **Options group** as-is.
- Under **Backups**, ensure that **Enable automatic backups** is enabled and then set **Backup retention period** to **1 Day**.
- Under **Backup window**, select the **No preference** option. For real-world applications, you may wish to set the backup window to a period outside of normal business hours.
- Under the **Maintenance** subheading, leave the settings as-is.
- Finally, click the **Create database** button at the bottom right-hand corner of the screen.

Your RDS database will take a few minutes to launch. As part of the launch process, an initial backup will also be performed. Once the database has been successfully launched and ready to use, you will see that its **Status** will be set to **Available**, as per the following screenshot:

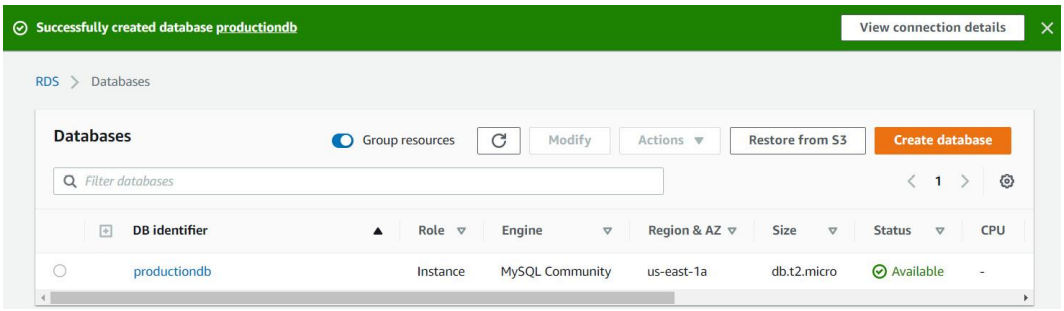

Figure 8.15 – RDS database created successfully notification

In the next exercise, you will learn how to deploy a DynamoDB table.

Exercise 8.4 – Deploying an Amazon DynamoDB table

In this exercise, you will deploy a very simple DynamoDB table. Let's get started:

1. Ensure that you are logged into your AWS account as the IAM user known as **Alice**.
2. Next, navigate to the DynamoDB dashboard. You can search for `DynamoDB` from the top search box of **AWS Management Console**.
3. If this is the first time you have visited the **DynamoDB console** page, you will be presented with a splash screen.
4. Click the **Create table** button.
5. Provide a name for your table in the text box next to **Table name**; for example, `Recipes`.
6. In the **Primary key** field, enter `RecipeName` and ensure that the type is set to **String**.
7. Under **Table settings**, uncheck the box next to **Use default settings**.
8. In the **Read/write capacity mode** section, select the **On-demand** option.
9. Click the **Create** button at the bottom of the page. DynamoDB will create a new table for you in a few seconds, as per the following screenshot:

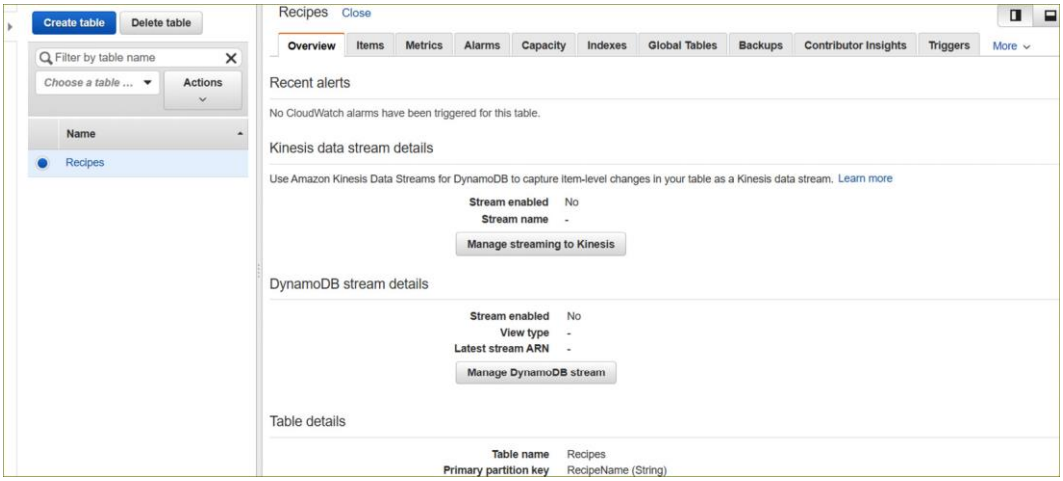

Figure 8.16 – DynamoDB table – Recipes

10. Click on the **Items** tab.
11. You can start adding items in the **Items** tab. Click the **Create item** button.
12. You will see a dialog box in which you can add a new item (record) to your database.
13. In the text box next to **RecipeName String**, enter `Vegan Sausage Rolls`.
14. Click on the **Save** button.

15. Note that the new item has been added and that the value of the primary key for this item is the name of the recipe, `Vegan Sausage Rolls`.

16. Click the **Create item** button again.

17. In the text box next to **RecipeName String**, enter `Vegan Peri Peri Burger`.

18. Click on the *plus* sign and select the **Append** drop-down list. From the list of options provided, select the **StringSet** type. A new field will be created for you. In the **field** box, enter an attribute (field name); for example, `Ingredients`. You will also notice that an additional entry appears below this **StringSet**, which is where you would input the values for the field you just created. Click on the *plus* sign next to the *empty array* line and select **Append**.

19. In the **Value** box, type in the following words, followed by pressing *Enter* on your keyboard after each word – `Lettuce` `Tomato` `Cucumber`. Click on a different part of the screen to update the values, as per the following screenshot:

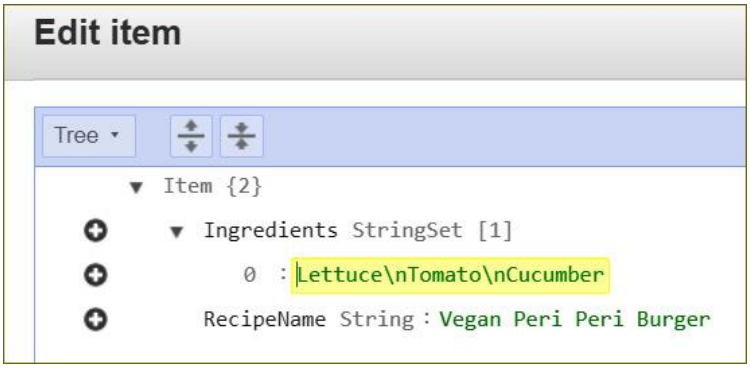

Figure 8.17 – DymanoDB item entry

20. Click on the **Save** button.

21. At this point, your table has been updated with a new record. You will see the two items in your table. The **Vegan Sausage Roll** item only has one field with a value in it, namely the primary key. The **Vegan Peri Peri Burger** item has two fields associated with it, which are the primary key and an attribute called **Ingredients**. Review the following screenshot for reference:

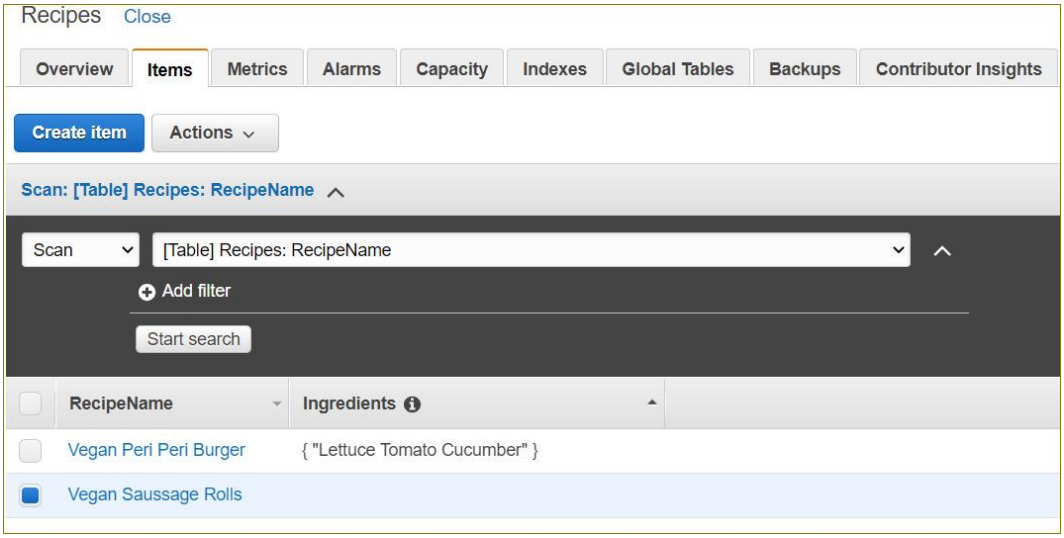

Figure 8.18 – DynamoDB Recipes table

As you can see, DynamoDB offers lots of flexibility in not requiring a rigid schema definition before inputting data.

Next, we will conclude by summarizing this chapter.

Questions

1. A company plans to migrate its on-premises MySQL database to Amazon RDS. Which AWS service should they use for this task?

   A. Amazon Snowball

   B. AWS Database Migration Service (AWS DMS)

   C. AWS VM Import/Export

   D. AWS Server Migration Service

2. Which of the following is the primary benefit of using an Amazon RDS database instead of installing a MySQL-compatible database on your EC2 instance?

   A. Managing the database, including patching and backups, is taken care of by Amazon.

   B. Managing the database, including patching and backups, is taken care of by the customer.

   C. You have full access to the operating system layer that the RDS database runs on.

   D. You can choose which drive and partition to install the RDS database on.

3. AWS RDS supports six database engines. From the following list, choose *three* engines supported by Amazon RDS.

A. Microsoft SQL

B. Oracle

C. MySQL

D. FoxPro

E. Db2

4. You are building an application for a wealth asset management company that will be used to store portfolio data and transactions of stocks, mutual funds, and forex purchased. To that end, you need a backend database solution that will ensure a ledger-like functionality because they want to maintain an accurate history of their applications' data, for example, tracking the history of credits and debits for its customers. Which AWS database solution would you recommend for this business requirement?

   A. Amazon RDS

   B. Amazon DynamoDB

   C. Amazon QLDB

   D. Amazon Redshift

5. Which AWS database solution enables you to build a complete data warehousing solution, capable of handling complex analytic queries against petabytes of structured data using standard SQL and industry-recognized business intelligence tools?

   A. AWS DynamoDB

   B. AWS Redshift

   C. AWS Neptune

   D. AWS Pluto

6. You are looking to host a production-grade enterprise relational database solution that offers high-end features such as self-healing storage systems that are capable of scaling up to 128 TB per database instance. Which of the following AWS database solutions fulfills the requirement?

   A. Amazon DynamoDB

   B. Amazon Aurora

   C. Amazon Redshift

   D. Amazon Neptune

7. Which AWS feature of Amazon Redshift enables you to run SQL queries against data stored directly on Amazon S3 buckets?

A. Redshift DaX

B. Athena

C. Redshift Spectrum

D. Redshift Cache

8. Which AWS service enables you to migrate an on-premises MySQL database to an Amazon RDS database running the Oracle Engine?

A. AWS Cross-Region Replication

B. AWS SMS

C. AWS DMS

D. AWS EFS

9. You are running a single RDS DB instance. Which configuration would you recommend so that you can avoid I/O suspension issues when performing backups?

A. Configure RDS read replicas.

B. Configure RDS Multi-AZ.

C. Configure RDS Cross Region Backup.

D. Configure DynamoDB DaX.

Chapter 9

Figures

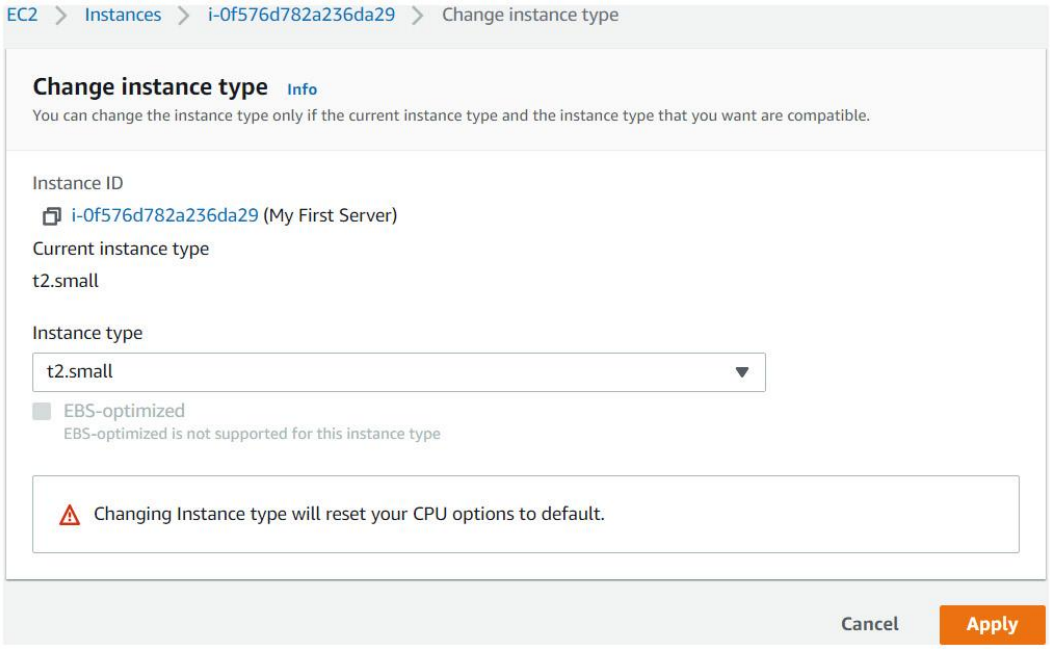

Figure 9.1 – Changing EC2 instance type: vertical scaling

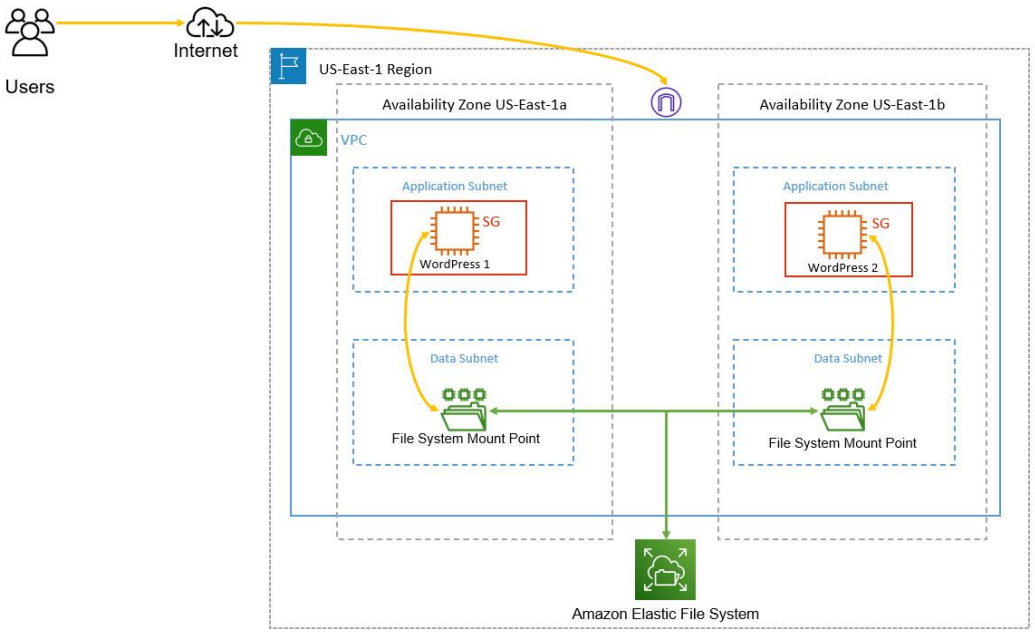

Figure 9.2 – Enabling horizontal scaling at the application layer

Figure 9.3 – OSI model

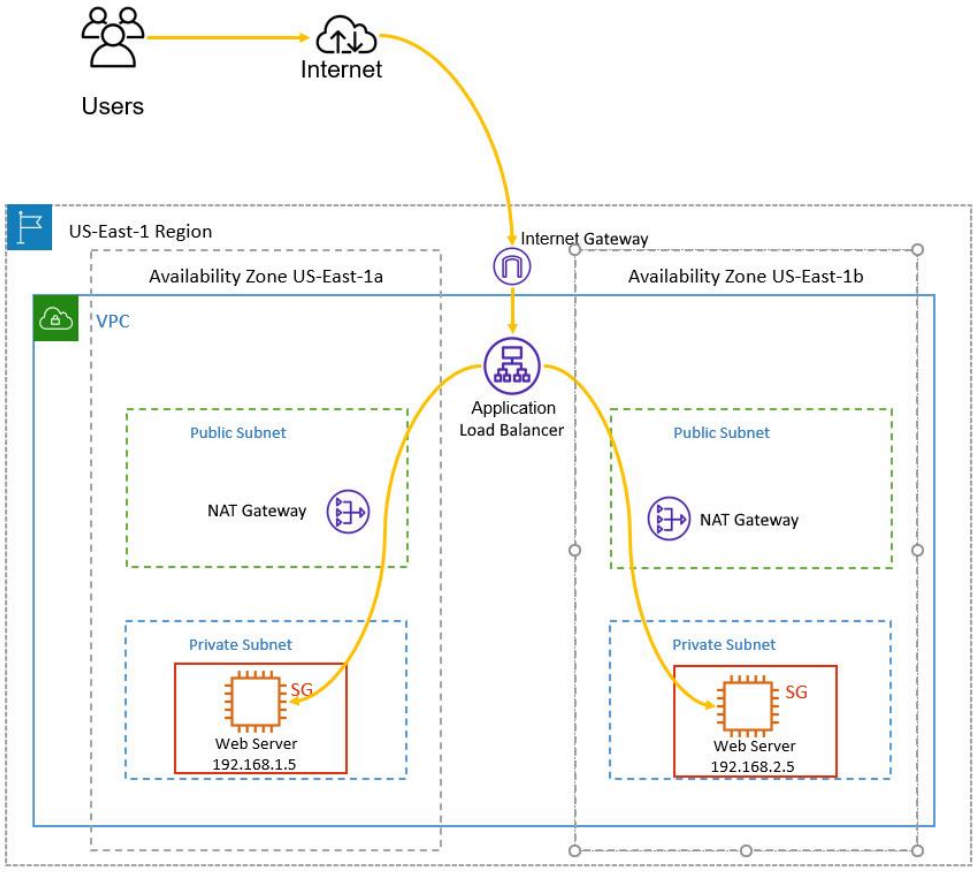

Figure 9.4 – Amazon ELB VPC configuration

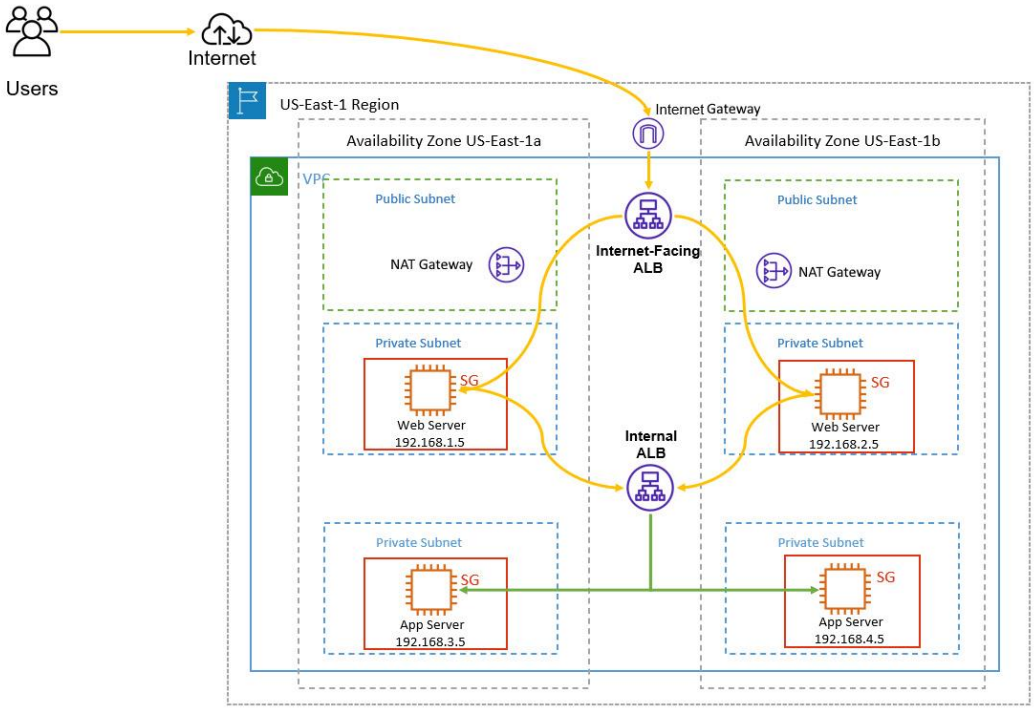

Figure 9.5 – Internal versus internet-facing ELBs

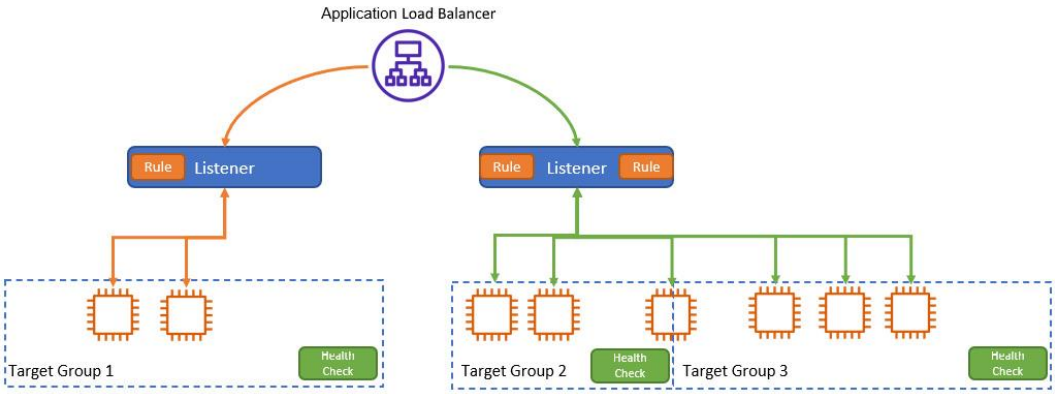

Figure 9.6 – AWS ALB with multiple listener rules

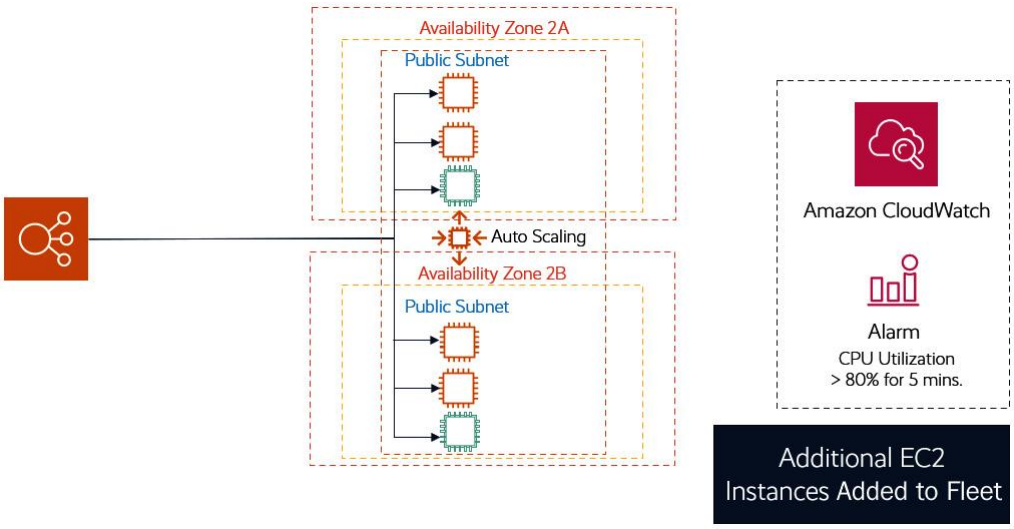

Figure 9.7 – Auto Scaling service example

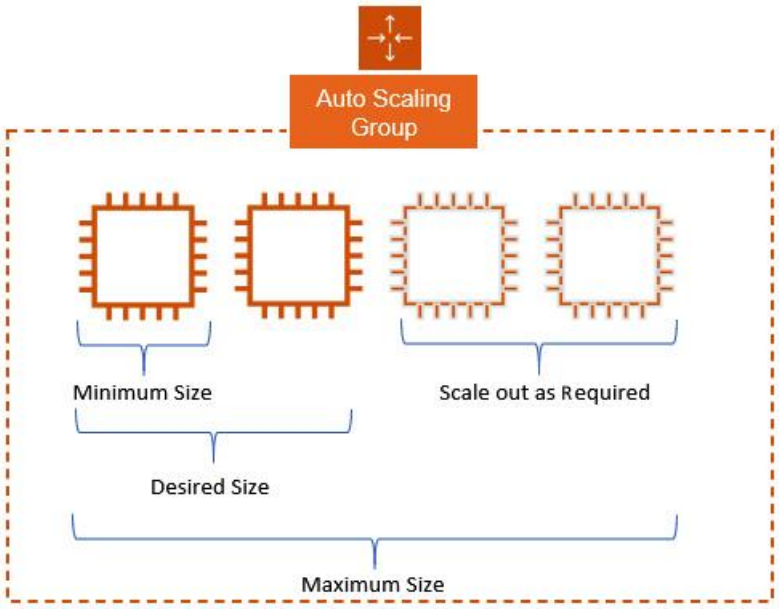

Figure 9.8 – Auto Scaling groups

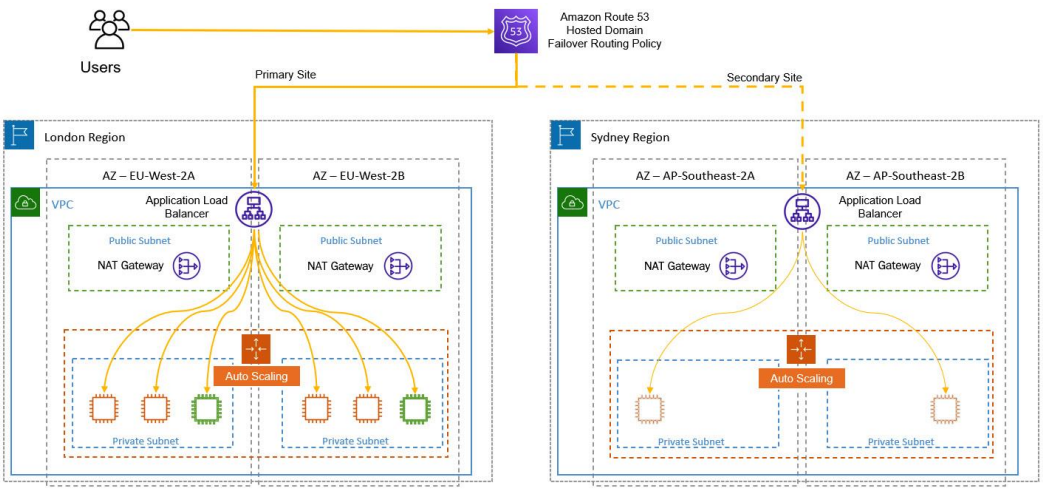

Figure 9.9 – Route 53 configured with failover routing policy, enabling an active/passive solution for application architecture

Links

For additional information on EBS, refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html.

Furthermore, to complete the exercise, you will need to access the source code files of the application, which are available at the *Packt Publishing* GitHub repository: https://github.com/PacktPublishing/AWS-Certified-Cloud-Practitioner-Exam-Guide

Extended exercises – setting the scene

The upcoming exercises are based on the following scenario. You work for a fictitious company called **The Vegan Studio**. The company is in the hospitality industry. Specifically, the company runs a chain of cafes and restaurants across the **United States** (**US**), serving only vegan dishes for those looking to indulge in meat-free cuisine. The company employs over 4,000 employees across its business, and keeping everyone engaged and feeling part of a large family is something the business takes great pride in.

Every year, they run several contests for their employees to participate in. This year, they are running a *My Good Deed for the Month* contest. A web application has been designed by one of the developers, which you need to now deploy in a highly available and scalable manner on AWS in the `us-east-1` Region. The contest will run for a month and all employees are encouraged to submit a statement of any good deeds they carried out. Five winners will be chosen from a list of entries and awarded a special hamper prize. Participants must back up their good deeds with evidence if requested (just to be sure no one is fooling around)!

Next, we will walk you through a series of exercises to deploy the application designed by your developer with HA and scalability features.

Important Note

Some AWS services, such as ELBs and **Network Address Translation** (**NAT**) gateways, are chargeable. We suggest you complete all the exercises in reasonably quick succession and then perform the cleanup exercise at the end. Overall, the cost should not be more than $5. To ensure costs are kept to a minimum, we will not be configuring the RDS database you deployed in the previous chapter with Multi-AZ.

The following exercises will make use of a multi-tier application design that will be deployed in the **production VPC** that you already built in the previous chapters. Recall that the VPC comprises both public and private subnets, spanning across two AZs. From the previous chapters, you have already built a foundation architecture as per the following diagram:

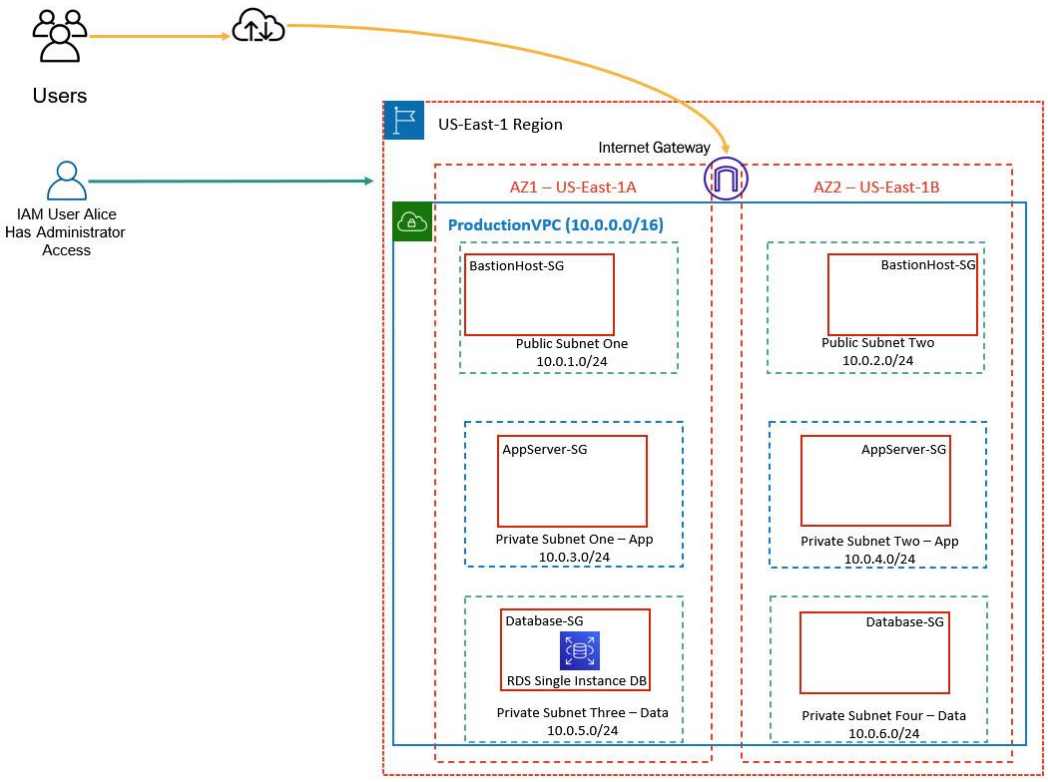

Figure 9.10 – Production VPC architecture prior to deploying the "Good Deed of the Month" contest application

As per the previous diagram, your current architecture is comprised of the following key AWS services and resources:

- A VPC created in the `us-east-1` Region with public and private subnets across two AZs. The private subnets have been designed to support a two-tier application solution comprising a web/application tier and a database tier.
- The public subnets will normally be used to deploy bastion hosts for remote administration and NAT gateways. For the upcoming series of exercises, we will not be deploying any bastion hosts as this is not required for the labs in these exercises. However, we will amend the bastion host security group to allow inbound **Secure Shell** (**SSH**) connections if you wish to later deploy bastion hosts. Furthermore, because we will be deploying Linux servers, remote administration requires SSH access on port `22`.
- The application tier private subnets do not currently have any EC2 instances deployed.
- The database tier private subnets currently host a single instance MySQL RDS database in the `us-east-1a` AZ.

Through the upcoming exercises in this chapter, we will build on the architecture to design a fully functional application solution with HA and scalability features.

Exercise 9.1 – setting up an Amazon S3 bucket to host source files

In this exercise, you will first create an Amazon S3 bucket that will be used to host your source files for your application. You need to first download the source file, which is available in a ZIP folder format, and extract its contents into a new folder or onto the desktop of your computer for easy access.

The first step is to prepare your source code files. Your source code files contain a database connection file that will need to be amended to the specific RDS database you configured in the previous chapter. Follow these next steps:

10. Once you unzip the downloaded folder, you can see the contents of the main `vegan-php-files` folder, as per the following screenshot:

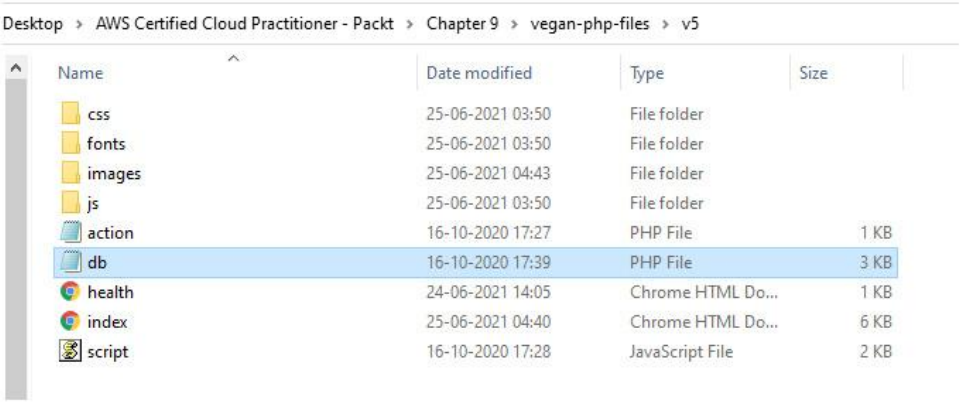

Figure 9.11 – vegan-php-files source code

11. You will note that in the `v5` directory, there is a file called `db` that is a **PHP: Hypertext Preprocessor** (**PHP**) file. This file contains default database connection string details that you will first need to amend before you upload the source code to your S3 bucket. Specifically, you will need to provide the RDS database connection details, which include the RDS endpoint DNS name, master username, password, and database name. *Recall that you made a note of these values in the last chapter*.

12. In a notepad or text editor tool, open the `db.php` file from the `v5` folder.

13. Within the PHP file, you will need to edit the values of the placeholders with the appropriate database connection values. In the following screenshot, you will see the placeholders:

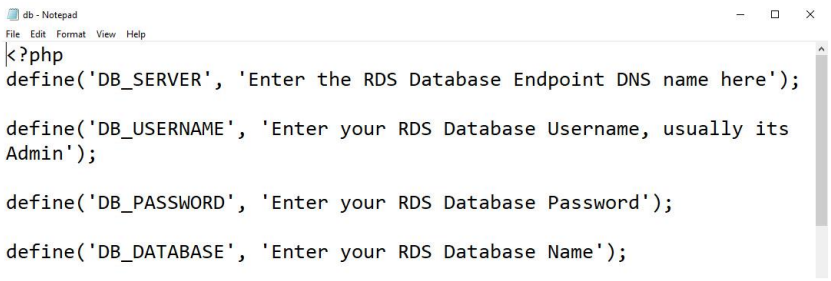

Figure 9.12 – db.php file

14. You will need to replace the placeholders with the connection details to your database, making sure to place all the values within single quotation marks. Do not make any other changes to the code. Here is a screenshot of where you can obtain these values after you create your database. The database endpoint is visible on the main **Connectivity & security** tab, and you will find the username and database name in the **Configuration** tab. Note that the password is not visible, as you should have made a note of it when launching the database instance:

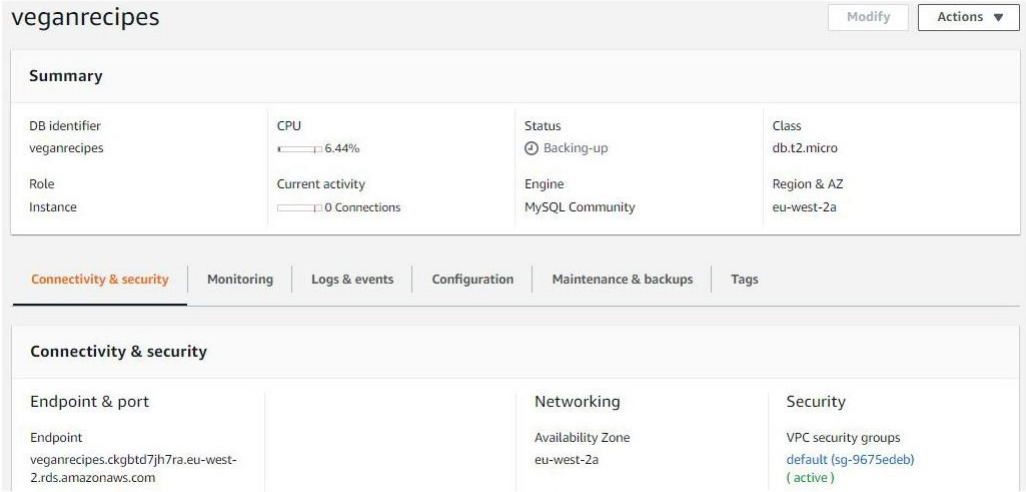

Figure 9.13 – Amazon RDS database settings

15. Save the file in its original location.
16. Log in to your AWS Management Console and navigate to the Amazon S3 dashboard.
17. In the left-hand menu, click **Buckets**.
18. Click **Create bucket** in the right-hand pane of the dashboard.
19. For the **Bucket name** field, provide any name of choice. You will need to choose a unique name as bucket names are obtained on a first-come, first-served basis. For example, my bucket name is `vegan-good-deed`. Ensure that the Region selected is the `us-east-1` Region.
20. Scroll to the bottom of the page, leaving all settings at their default values, and click the **Create bucket** button. Your Amazon S3 bucket will be created, and you will be redirected back to the list of available buckets.
21. Click on the bucket you just created, and you will be redirected to the **Objects** listing page, where you will note that there are currently no objects, as per the following screenshot:

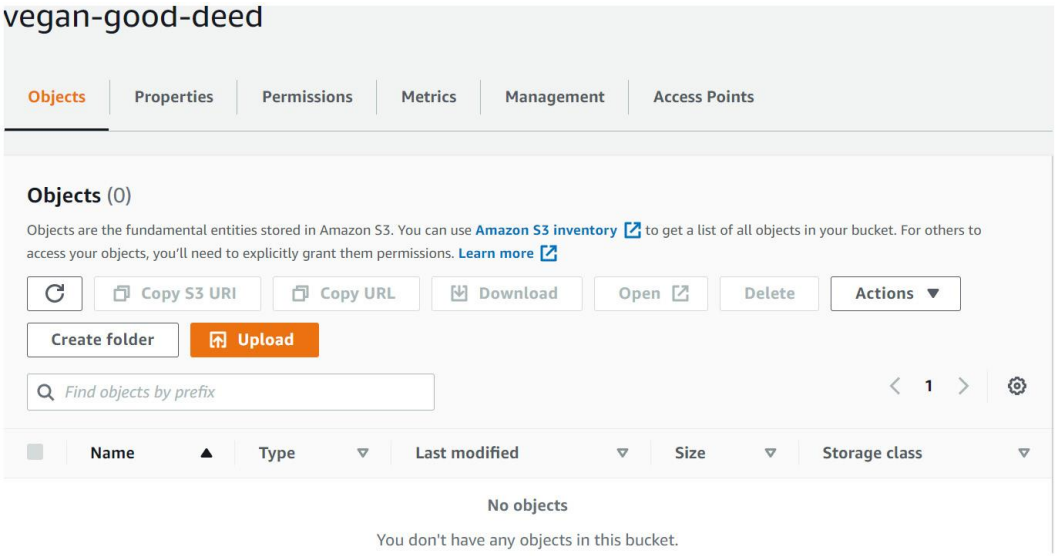

Figure 9.14 – New bucket creation

22. Click the **Upload** button.

23. Next, you want to try to resize your browser page with the S3 bucket **Upload** page visible, and next to it resize the `vegan-php-files` folder so that you can easily drag and drop all the folders and files into the S3 bucket's **Object** area, as per the following screenshot. You need to ensure that the folder hierarchy is maintained for the application to work:

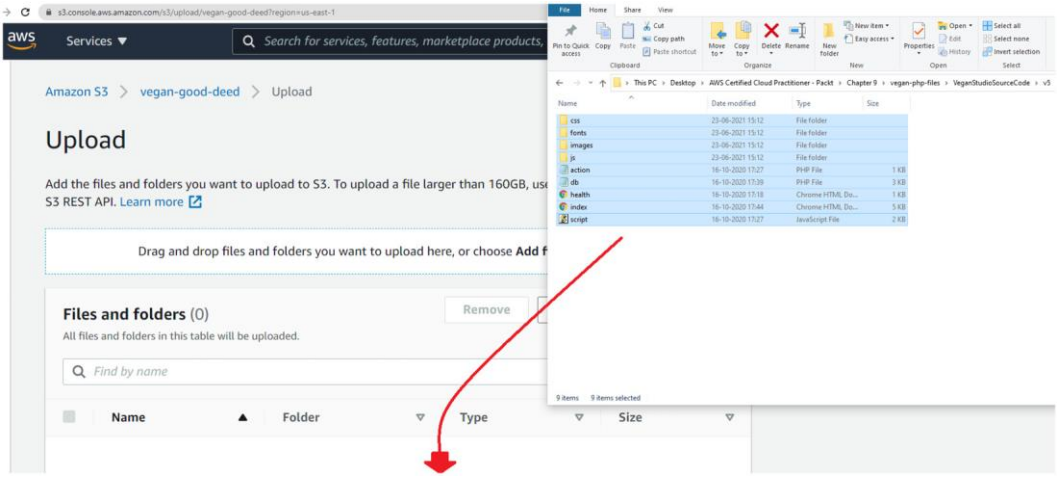

Figure 9.15 – Copying files and folders to the S3 bucket

24. Your Amazon S3 **Upload** page will provide a summary of files and folders to be uploaded. You will need to then click on the **Upload** button at the bottom of the page.

25. Once all the files and folders have been uploaded, you receive an **Upload succeeded** message.

Now that your source code and files for your application have been uploaded, we will move on to the next exercise. As part of this series of exercises, you will need to configure your EC2 instances to download the source code files for the application. Using Bash scripts at the time of launching your

EC2 instances, you will download the source code from the Amazon S3 bucket and place it in the appropriate folders within the EC2 instances to serve the application.

Because your EC2 instance would need to have permissions to access the previous S3 bucket we created and download the source code, we need to configure an IAM role that your EC2 instance will use to authenticate to Amazon S3.

Exercise 9.2 – creating an IAM role

In this exercise, you will create an IAM role that your EC2 instances will use to authenticate and access the source code files in your Amazon S3 bucket. Proceed as follows:

26. Ensure that you are logged in to your AWS account and navigate to the IAM dashboard.
27. Click on **Roles** from the left-hand menu.
28. Click **Create role**, as per the following screenshot:

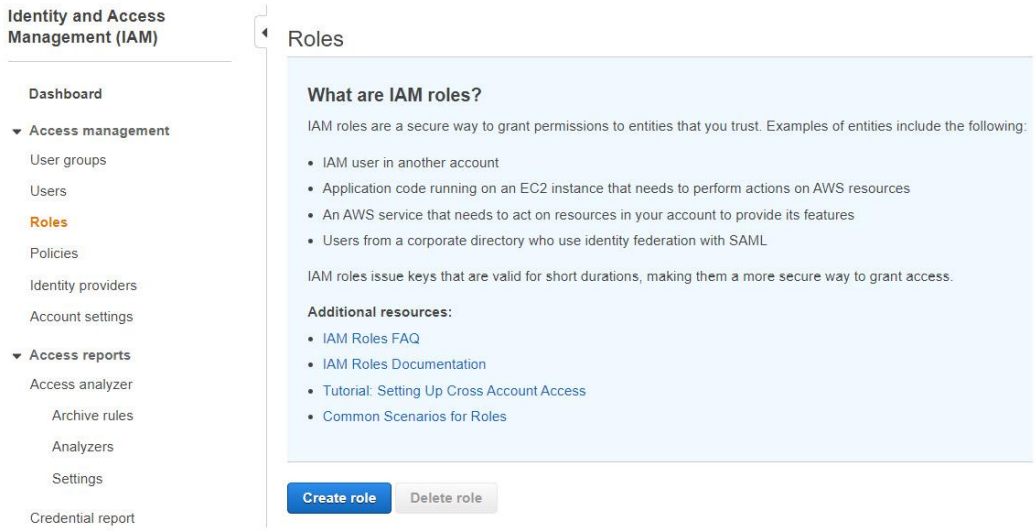

Figure 9.16 – Creating an IAM role

29. In the **Select type of trusted entity** field, click the **AWS services** option, and under **Choose a use case**, select **EC2** under **Common use cases**.
30. Click the **Next: Permissions** button at the bottom of the page.
31. On the **Attach permissions policies** page, filter the list by searching for `S3`. Next, select the `AmazonS3ReadOnlyAccess` policy and click the **Next: Tags** button, as per the following screenshot:

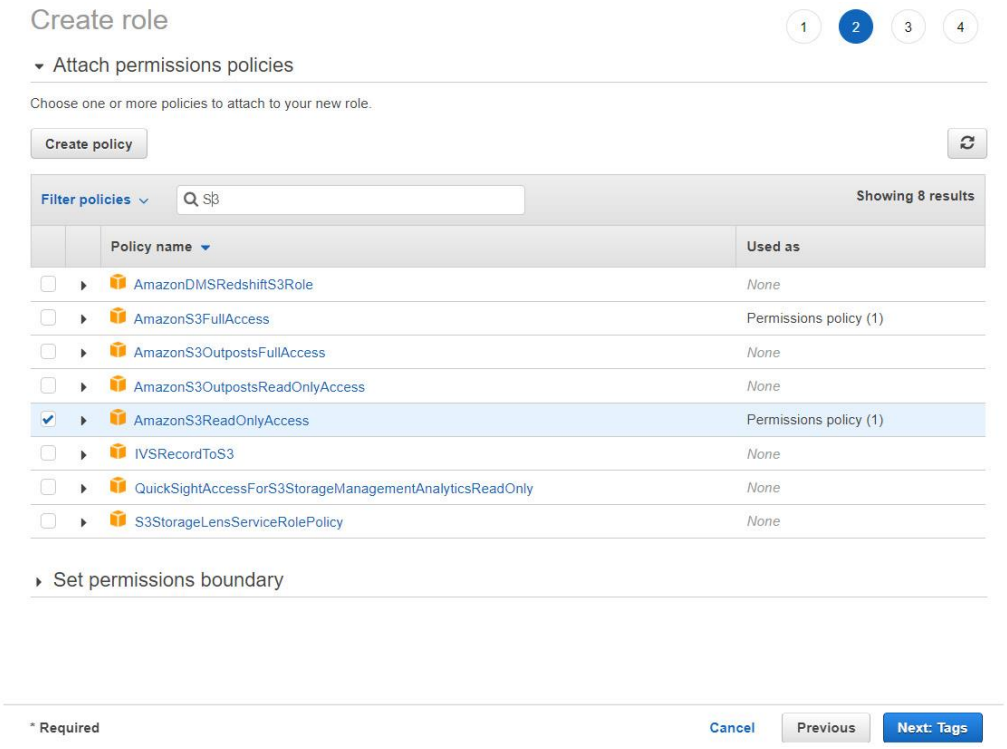

Figure 9.17 – Creating an IAM role (continued)

32. Set a key-value pair to tag your role with a key of **Name** and a value of `EC2-to-S3-Read-Access`. This allows us to easily identify the role. Click the **Next: Review** button on the bottom right-hand corner of the page.

33. In the **Review** section, provide a name for your role, such as `EC2-to-S3-Read-Access`, and a description.

34. Finally, click the **Create role** button.

AWS will now create your IAM role, and you will need to reference this role when we launch our EC2 instances in a later chapter.

At this stage, you have the following AWS services configured:

- An Amazon VPC with public and private subnets across two AZs. You have a public subnet to host bastion hosts and NAT gateways, and four private subnets—two for your web/application servers located in the **web/application tier** and another two for your **database tier**.
- An RDS database that will store all data such as the *good deeds of the month* that the employees of The Vegan Studio will submit.
- An Amazon S3 bucket with the source code files configured to point to the RDS database.
- An IAM role to allow your EC2 instances to download the source code files from the S3 bucket.

When you deploy your application, you will install Apache Web Services and host your application files on EC2 instances. Specifically, you will be deploying two EC2 instances that will be placed across two AZs. To distribute traffic across those EC2 instances, you will need to configure an ALB that will be configured to accept inbound HTTP (port `80`) traffic from the internet and distribute them to your EC2 instances. In the next exercise, you will need to configure your ALB.

Exercise 9.3 – configuring an ALB

In this exercise, you will be configuring an ALB that will be used to accept inbound traffic from your users on the internet and distribute them across the EC2 instances you deploy later in this chapter.

ALBs, as discussed earlier in this chapter, can be used to distribute web and application traffic using HTTP and HTTPS protocols. You will configure an internet-facing load balancer so that you can accept inbound requests from the internet.

CLBs and ALBs require you to also configure a security group within which you define which traffic would be permitted inbound to those load balancers. Therefore, the first step is to revisit the VPC dashboard and create a new security group for your ALB, as follows:

35. Navigate to the VPC dashboard and ensure you are still in the `us-east-1` Region.
36. From the left-hand menu, click on **Security Groups**.
37. Click the **Create security group** button in the top right-hand corner of the screen.
38. Provide the security group with a name such as `ALB-SG` and a description such as `Allow inbound HTTP traffic from Internet`.
39. Ensure that you select **ProductionVPC** from the VPC drop-down list.
40. Click the **Add rule** button under **Inbound rules**.
41. For **Type**, select **HTTP** from the drop-down list, and set the source to **Custom**, with a **classless inter-domain routing** (**CIDR**) block of `0.0.0.0/0`. This source denotes the public internet.
42. Provide an optional description and then click on the **Create security group** button on the bottom right-hand corner of the screen.

AWS will now create your security group, which we will use to configure our ALB.

Important Note

ELBs do not fall under the Free Tier offering from AWS, and you must ensure you delete them once you have completed all the labs.

Now that we have configured a security group, we can move on to configuring our load balancing service. However, your ALB requires a **target group** to send traffic to. The target group will be used to register the EC2 instances that will accept traffic from the ALB. So, the first step is to create your target group, as follows:

43. Navigate to the EC2 dashboard and ensure that you are in the `us-east-1` Region.
44. From the left-hand menu, click on **Target Groups**, under the **Load Balancing** menu.
45. From the right-hand pane, click on **Create target group**.
46. Next, you are presented with a two-step wizard. In *Step 1*, select **Instances** and then scroll further down to provide a **Target group name** value. I have named my target group `Production-TG`.
47. Under **Protocol**, ensure that **HTTP** is selected and the port is set to `80`.
48. Next, under **VPC**, ensure you select `Production-VPC`.
49. Scroll further down till you reach the **Health checks** section.
50. Next, set the **Health check protocol** to **HTTP**.
51. For the **Health check path** field, type in `/health.html` as per the following screenshot:

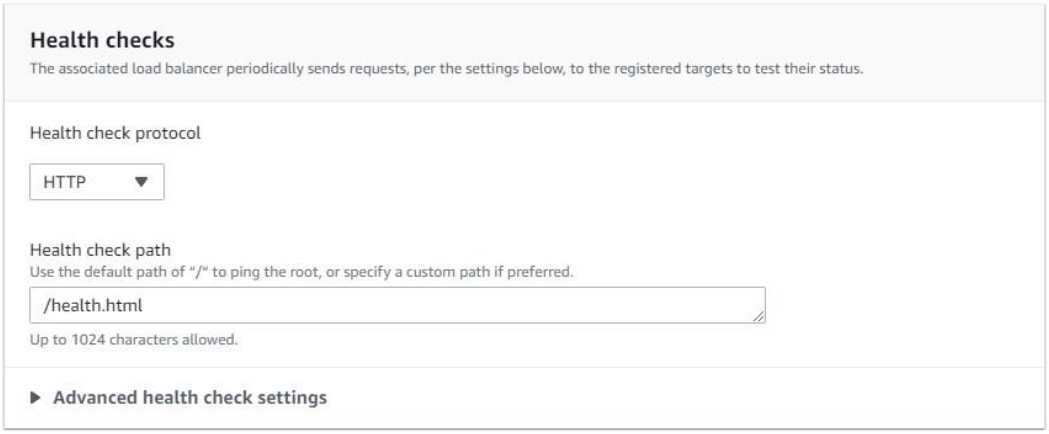

Figure 9.18 – Load balancer target group health checks

52. Next, expand the **Advanced health check settings** field.
53. Set the **Port** value to **Traffic Port**.
54. Set the **Healthy threshold** value to `3`.
55. Set the **Unhealthy threshold** value to `2`.
56. Next, set the **Timeout** value to `2`.
57. Finally, set the **Interval** value to `10` seconds.
58. Click the **Next** button at the bottom of the page.
59. This will take you to *Step 2*, where you would normally register any EC2 instances. However, as we have not launched any EC2 instances yet, you can ignore this step and simply click on the **Create target group** button at the bottom of the page.

Next, now that we have the **target group** configured, we can launch our ALB. ELBs are configured in the EC2 management console or via the **command-line interface** (**CLI**).

60. From the left-hand menu, click on **Load Balancers** under the **Load Balancing** category.
61. Next, click on the **Create Load Balancer** button at the top of the screen in the right-hand pane.
62. Click on the **Create** button in the **Application Load Balancer** section of the page, as per the following screenshot:

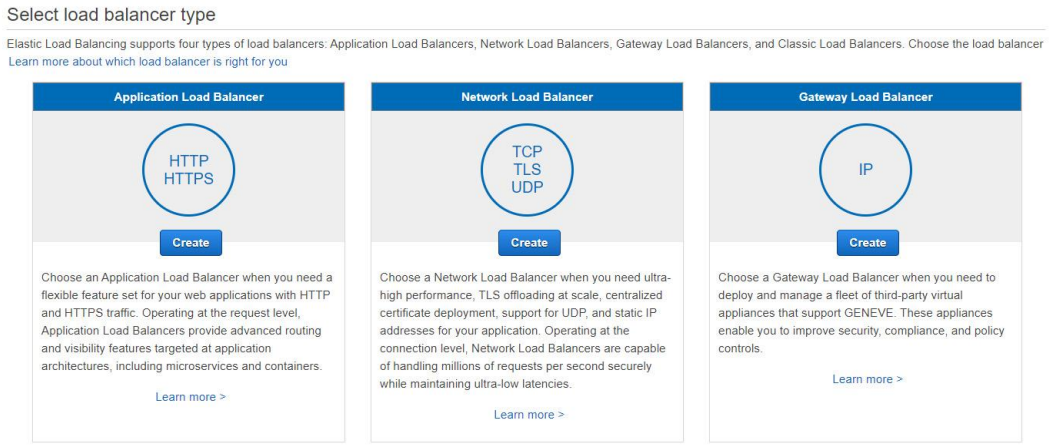

Figure 9.19 – Selecting Application Load Balancer as load balancer type

63. In **Step 1: Configure Load Balancer**, proceed as follows:
64. Set the name of the load balancer to `Production-ALB`.
65. Ensure that the **Scheme** field is set to **Internet facing** and that **IP address type** is set to **ipv4**.
66. Next, under **Network mapping**, select `Production-VPC` under the **VPC** heading.
67. Under **Mappings**, you need to select which AZs will be enabled for the ALB.
68. Select the checkboxes next to both the `us-east-1a` and `us-east-1b` AZs.
69. In the **Subnet** drop-down list for the `us-east-1a` AZ, select the **Public Subnet One** subnet.
70. Next, in the **Subnet** drop-down list for the `us-east-1b` AZ, select the **Public Subnet Two** subnet.

    AWS will then deploy the ALB *nodes* in these public subnets, routing incoming traffic from the internet to the EC2 instances in the private subnets that we registered as targets for the load balancer. Internet-facing load balancers should be created in subnets that have been configured with an internet gateway such as in this case: the public subnets of your VPC.
71. Next, under **Security Groups**, select the `ALB-SG` security group from the drop-down list. You can also delete the **default** security group that was pre-selected by clicking on the **X** sign

next to the group. This is because we only want to associate the load balancer with the `ALB-SG` security group.

72. In the **Listener** section, ensure that the **Protocol** field is set to **HTTP** and the **Port** field is set to `80`. Next, under **Default Action**, select the `Production-TG` target group you created earlier from the drop-down list.

73. Finally, scroll further down and click on the **Create load balancer** button.

74. You will receive a confirmation message stating that the load balancer has been created successfully. Click on **View load balancers**, which will take you back to the list of load balancers deployed, and you should find your `Production-ALB` load balancer in the list. After a few moments, the status of the load balancer should change from **Provisioning** to **Active**.

At this point, we have now configured our ALB. Let's go ahead and look at our architectural diagram to see how our configuration is coming along:

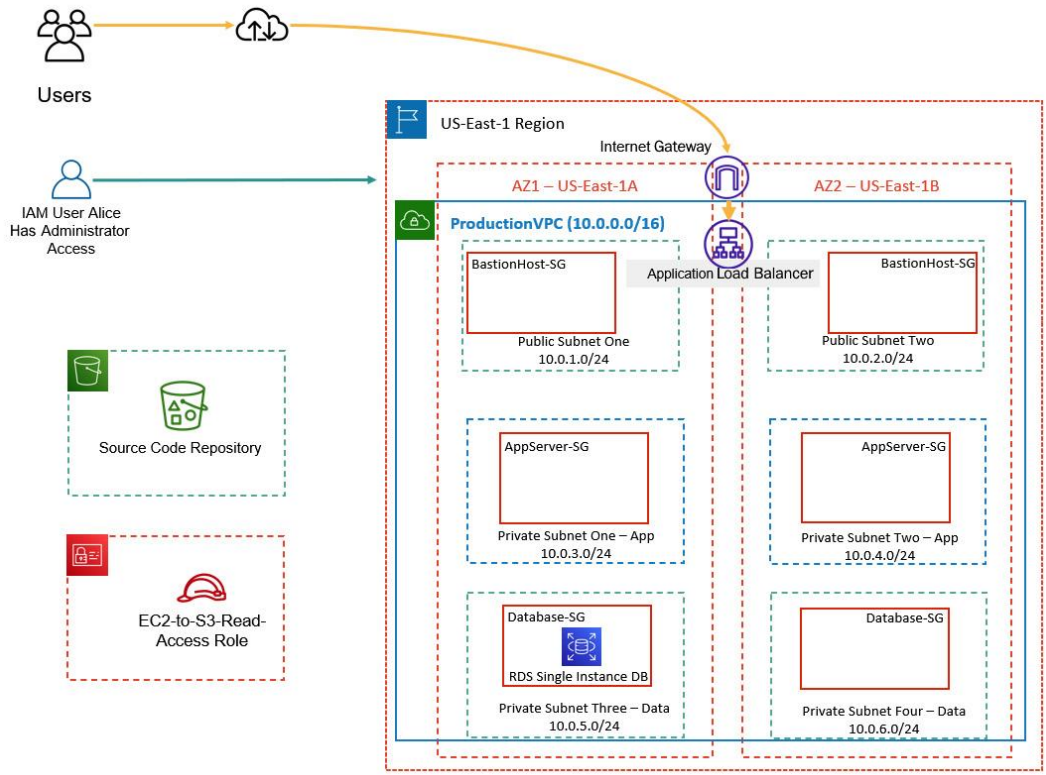

Figure 9.20 – Production VPC architecture after configuring S3 bucket, IAM role, and ALB

For traffic to be allowed inbound to the application servers, we need to ensure that the security groups associated with those servers have been correctly configured. Specifically, the `AppServers-SG` security group must allow traffic on the HTTP protocol (port `80`) from the ALB we deployed in the previous exercise.

Furthermore, in *Chapter 7*, *AWS Compute Services*, you configured the `AppServers-SG` security group to accept traffic from the `BastionHost-SG` security group. This was to enable inbound traffic on **Remote Desktop Protocol** (**RDP**) (port `3389`), which enables the Windows

Remote Desktop client to perform remote access operations. Although we will not be deploying any bastion hosts in the remaining exercises in this chapter, we will amend the inbound rule on the `AppServers-SG` security group such that the protocol and port used to accept traffic from the `BastionHost-SG` security group will be set to the SSH protocol on port `22`. This is because we will be deploying Linux EC2 instances to host our application, and any remote management of Linux servers requires you to configure SSH access.

Exercise 9.4 – amending the Production-VPC security group

In this exercise, we will amend the RDP inbound rule in the `AppServers-SG` security group such that it is configured to accept traffic on the SSH protocol (port `22`) from the `BastionHost-SG` security group. Next, we will add a new rule to accept traffic on the HTTP protocol (port `80`) from the ALB's security group, `ALB-SG`. Finally, we will amend the `BastionHost-SG` security group such that it is configured to accept traffic on the SSH protocol (port `22`) from the internet. This is useful if you later wish to perform any remote administration of your Linux servers.

Amend the `BastionHost-SG` security group, as follows:

75. Navigate to the VPC dashboard and ensure that you are in the `us-east-1` Region.
76. From the left-hand menu, click on **Security Groups**.
77. In the middle pane, select the checkbox next to the **Security group ID** value associated with the `BastionHost-SG` security group.
78. In the pane below, click on **Inbound rules** and then click on the **Edit inbound rules** button.
79. Next, delete the existing **RDP** rule by clicking on the **Delete** button on the far right of the page.
80. Click the **Add rule** button.
81. For the type, select **SSH** from the drop-down list. Next, ensure that the **Custom** option is selected in the **Source** column, and in the search box next to it, type in `0.0.0.0/0`.
82. Finally, click on the **Save rules** button in the bottom right-hand corner of the page.

    Amend the `AppServers-SG` security group.

83. Click on the **Security Groups** link from the left-hand menu again to see all your security groups in the VPC.
84. In the middle pane, select the checkbox next to the **Security group ID** value associated with the `AppServers-SG` security group.
85. In the pane below, click on **Inbound rules** and then click on the **Edit inbound rules** button.
86. Next, delete the existing **RDP** rule by clicking on the **Delete** button on the far right of the page.
87. Click the **Add rule** button.

88. For the type, select **SSH** from the drop-down list. Next, ensure that the **Custom** option is selected in the **Source** column, and in the search box next to it, start by typing in `sg-`. You will notice that a list of your security groups will become visible. Select the `BastionHost-SG` security group from this list.

89. Next, click the **Add rule** button again.

90. For the type, select **HTTP** from the drop-down list. Next, ensure that the **Custom** option is selected in the **Source** column, and in the search box next to it, start by typing in `sg-`. You will notice that a list of your security groups will become visible. This time, select the `ALB-SG` security group from the list.

91. Finally, click on the **Save rules** button in the bottom right-hand corner of the page.

We will not need to amend the `Database-SG` security group because this has already been configured to only accept traffic from the `AppServers-SG` security group using the MySQL port `3306`.

Recall from the architectural diagram in *Figure 9.20* that the web/application EC2 instances are going to be placed in a private subnet. Our The Vegan Studio employees will be able to access the *Good Deed of the Month* contest application on those EC2 instances via the ALB. However, the EC2 instances will need access to the internet to download updates as well as the source code files stored on the Amazon S3 bucket.

Remember that, unlike the public subnet, the private subnet does not grant direct access to the internet. Any EC2 instance in the private subnet would need to direct internet-bound traffic via an AWS NAT gateway, as discussed in *Chapter 6*, *AWS Networking Services – VPCs, Route53, and CloudFront*.

In the next exercise, we will deploy a NAT gateway.

Exercise 9.5 – deploying a NAT gateway

In this exercise, we will deploy a NAT gateway in the **Public Subnet One** subnet of our production VPC. Ideally, you want to deploy multiple NAT gateways in each public subnet across the AZs you have resources in to avoid a **single point of failure** (**SPOF**). However, for the purposes of this lab, we will use a single NAT gateway.

In addition, you will need to configure your **main route table** with a new route that will allow outbound traffic to the internet via this NAT gateway.

We will start this exercise by first allocating an elastic IP address for our AWS account, which is a requirement to configure a NAT gateway. To do this, follow these steps:

92. Navigate to your VPC dashboard and ensure that you are in the `us-east-1` Region.

93. NAT gateways require an elastic IP address, and so you will need to allocate one first to your AWS account. From the left-hand menu, click on **Elastic IPs**. In the right-hand pane, click the **Allocate Elastic IP address** button.

94. You will be presented with the **Allocate Elastic IP address** page. Ensure that **Amazon's pool of IPv4 addresses** is selected and then click the **Allocate** button.

AWS will allocate an elastic IP address from its pool of available addresses for your AWS account. Next, you will need to set up your NAT gateway, as follows:

95. From the left-hand menu, click on **NAT Gateways**.
96. In the right-hand pane, click the **Create NAT gateway** button.
97. On the **Create NAT gateway** page, proceed as follows:
98. Provide a name for your NAT gateway—for example, `Production-NAT`.
99. Next, from the **Subnet** drop-down list, select the **Public Subnet One** subnet.
100. Next, from the drop-down list under **Elastic IP allocation ID**, select the elastic IP you allocated to your account moments ago.
101. Finally, click the **Create NAT gateway** button at the bottom of the page.

The NAT gateway will take a couple of minutes to be provisioned. Once ready, the NAT gateway state will be set to **Available**, as per the following screenshot:

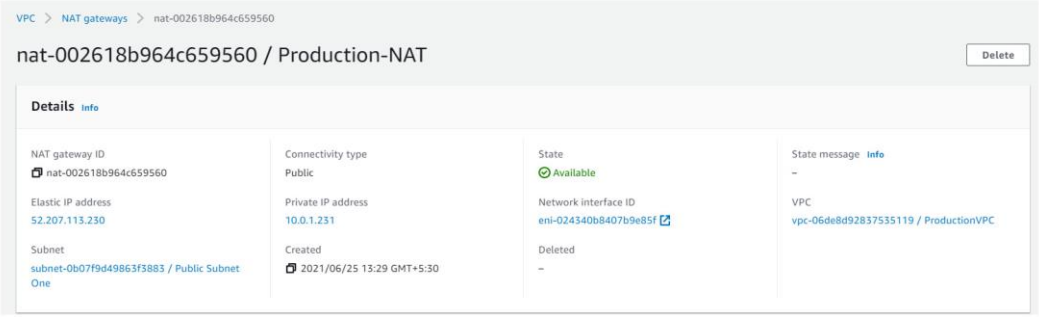

Figure 9.21 – NAT gateway

Now that you have deployed your NAT gateway, you will need to configure your main route table with a route to the internet that uses the NAT gateway, as follows:

102. From the left-hand menu in the VPC dashboard, select **Route Tables**.
103. Click on the checkbox next to **Main Route Table**.
104. In the bottom pane, click on the **Routes** tab.
105. Next, click the **Edit routes** button on the far right-hand side of the page.
106. You will be presented with the **Edit routes** page. Click the **Add route** button.
107. Under the **Destination** column, provide the destination as `0.0.0.0/0`.
108. Next, click on the **Target** search box to open up a list of potential targets. Select the **NAT Gateway** target, and AWS will display available NAT gateways associated with this VPC. You should find the `Production-NAT` NAT gateway in the list. Go ahead and select this.

109. Finally, click on the **Save changes** button.

Your main route table has now been configured with a route to the internet that will use the NAT gateway.

Now that you have configured your NAT gateway and the main route table correctly, we can proceed with deploying our EC2 instances that will host the *Good Deed of the Month* application in the next exercise.

Exercise 9.6 – deploying your application servers with Amazon Auto Scaling

In this exercise, we will configure the Amazon Auto Scaling service to define a **Launch Configuration** for our deployment, which will include a script to configure our EC2 instances with the Apache web service and download the application source files from the Amazon S3 bucket. As part of the exercise, you will also create an EC2 instance profile that will be used to contain the IAM role you created earlier and allow the EC2 instance to assume that role.

The EC2 instances will also be provisioned as targets in the `Production-TG` target group we created earlier in the ALB exercise. The `Production-ALB` ALB will then be able to distribute inbound traffic from our The Vegan Studio employees on the internet to those EC2 instances, enabling them to submit any good deeds they carried out for review by our panel.

In addition, we will configure Auto Scaling policies to always ensure that we always have two running EC2 instances, one in each private subnet, across the two AZs, `us-east-1a` and `us-east-1b`. In terms of health checks, these will be performed both at the EC2 level and via the ALBs using the health check parameters you defined in *Exercise 9.3* earlier.

Creating an Auto Scaling Launch Configuration

As part of this exercise, you will need access to a Bash script that we have included in the GitHub repository https://github.com/PacktPublishing/AWS-Certified-Cloud-Practitioner-Exam-Guide. In the `vegan-php-files.zip` file you downloaded earlier, which you unzipped, you will find a file called `userdata-script` in the top-level folder. You will need to amend this script to match your configuration. Open the script file in a notepad or text editor application and change the last line of the script, replacing `[Source Bucket]` with the actual name of your bucket. So, for example, if your bucket name is `vegan-good-deed`, then the last line should be changed from `aws s3 cp s3://[Source Bucket] /var/www/html –recursive` to `aws s3 cp s3://vegan-good-deed /var/www/html –recursive`. Make sure to save the file.

Next, we look at the steps required to set up our AWS Auto Scaling Launch Configuration, as follows:

110. Navigate to the EC2 dashboard and ensure that you are in the `us-east-1` Region.

111. From the left-hand menu, select **Launch Configurations** from the **Auto Scaling** category.

112. In the right-hand pane, click on the **Create Launch Configuration** button.

113. You will be presented with the **Create Launch Configuration** page.

114. Provide a name for your Launch Configuration—for example, `Production-LC`.

115. Next, you need to search for the Amazon Linux 2 AMI. It might be difficult to find the AMI in the new **user interface** (**UI**). To identify the AMI ID, open another browser window to access your AWS account and navigate to the EC2 dashboard. Click on **Instances** from the left-hand menu and then click on the **Launch instances** button in the far right-hand corner of the screen. You will find a list of quickstart AMIs. From this page, *make a note of the AMI ID for the Amazon Linux 2 instance*. Ensure that the AMI ID is for the `64-bit x86` architecture, which I have highlighted as per the following screenshot:

Figure 9.22 – AMI ID for Amazon Linux 2 instance

116. Back in the previous browser window where you are configuring your Auto Scaling Launch Configuration, click on the drop-down arrow under **AMI** and paste in the AMI ID you copied previously in the search box. You should then be able to find the relevant AMI to use. Make sure you select this AMI.

117. Next, under **Instance type**, click on the **Choose instance type** button, and in the search box, type in `t2.micro`. You can then select the `t2.micro` instance type from the filtered list. Go ahead and click the **Choose** button.

118. Next, under the **Additional configuration** option, click the drop-down arrow under **IAM instance profile** and select the `EC2-to-S3-Read-Access` instance profile that contains the IAM role you created earlier.

119. Next, expand the **Advanced details** section.

120. Under **User Data**, ensure that **As Text** is the selected option and, in the textbox provided, go ahead and paste in a copy of the Bash script file you amended a few moments ago.

121. Next, under **IP address type**, ensure that you select **Do not assign a public IP address to any instances**. This is because the EC2 instances are going to be launched in the private subnets and will not require a public IP address.

122. Leave the settings in the **Storage (volumes)** field at their default values.

123. Next, under **Security groups**, click on the **Select an existing security group** option, and from the list of available security groups, select the security group ID associated with the `AppServers-SG` security group.

124. In the **Key pair (login)** section, select **Choose an existing key pair** from the **Key pair options** drop-down list.

125. In the drop-down list under **Existing key pair**, ensure that you select the key pair you created earlier. In my example, this is the `USEC2Keys` key pair.

126. Next, tick the box to acknowledge that you have access to the private key file that you downloaded earlier in *Chapter 7*, *AWS Compute Services*.

127. Finally, click on the **Create Launch Configuration** button at the bottom of the screen.

At this point, you have successfully created your first Auto Scaling Launch Configuration, as per the following screenshot:

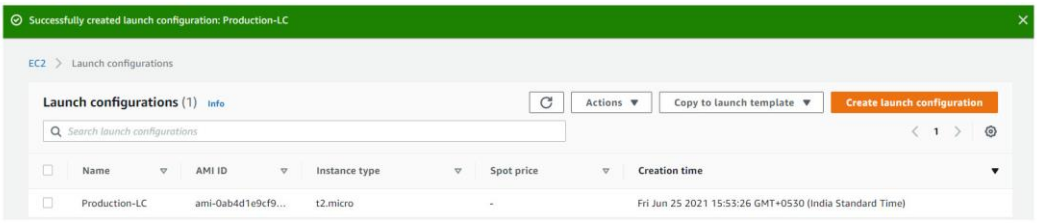

Figure 9.23 – Amazon Auto Scaling Launch Configuration

Now that you have created your Launch Configuration, you can proceed to configure your Auto Scaling groups.

Configuring Auto Scaling groups

As part of creating your Auto Scaling groups, you can define Auto Scaling policies. Because we will not be performing any real load testing on our application servers, we will simply configure our Auto Scaling policy to ensure that we always have a minimum of two EC2 instances across the two AZs. Proceed as follows:

128. From the left-hand menu of the EC2 dashboard, click on the **Auto Scaling Groups** link under **Auto Scaling**.

129. Click the **Create an Auto Scaling group** button in the right-hand pane of the screen.

130. In **Step 1, Choose Launch Template or configuration**, provide a name to identify your Auto Scaling group—for example, `Production-ASG`.

131. In the next section of the screen, you will have an option to select a Launch Template from a drop-down list. However, instead of a Launch Template, we have configured a Launch Configuration. To access your Launch Configuration, click on the **Switch to Launch Configuration** link on the far right-hand side of the screen.

132. Next, under **Launch Configuration**, select the `Production-LC` Launch Configuration you created earlier.

133. Click the **Next** button to move on to *Step 2*.

134. In **Step 2, Configure settings**, select `Production-VPC` from the **VPC** drop-down list.

135. In the drop-down list under **Subnets**, ensure that you select both the **Private Subnet One - App** and **Private Subnet Two - App** subnets, as per the following screenshot:

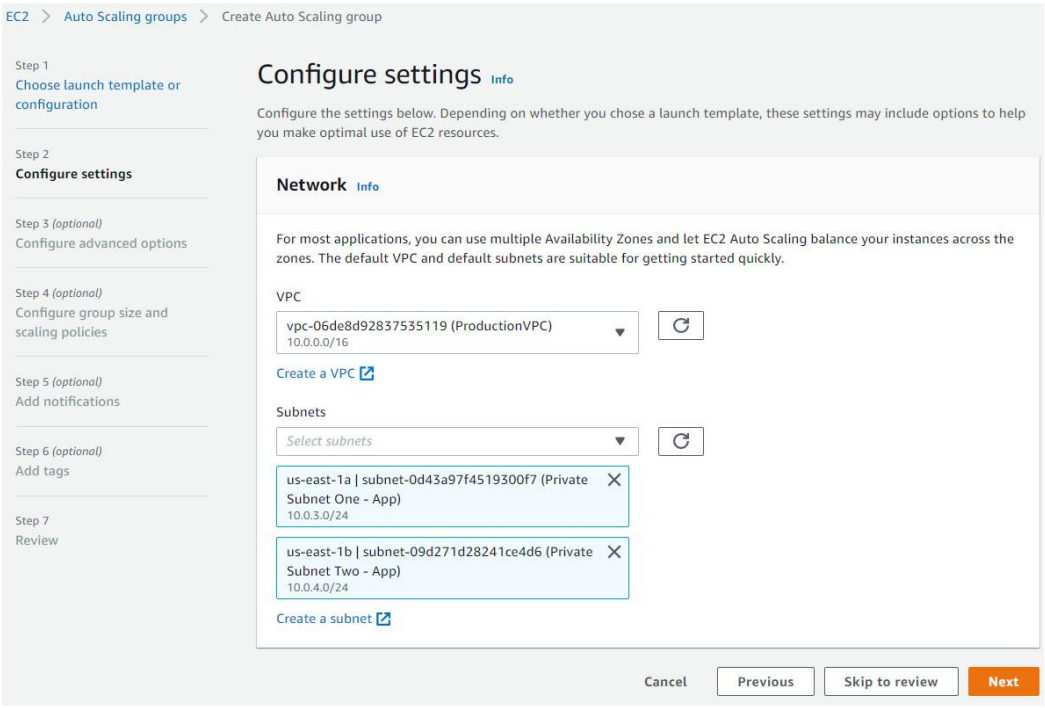

Figure 9.24 – Auto Scaling group subnet selection

136. Click the **Next** button.

137. In **Step 3, Load balancing – optional**, we will be using the ALB you created earlier. Select the **Attach to an existing load balancer** option.

138. Next, ensure that **Choose from your load balancer target groups** is selected under the **Attach to an existing load balancer** section.

139. From the drop-down list under **Existing load balancer target groups**, select the `Production-TG` target group that is associated with the `Production-ALB` ALB.

140. Next, under the **Health checks – optional** section, select the **ELB** checkbox. This is to enable ELB health checks in addition to the EC2 health checks.

141. Click the **Next** button at the bottom of the screen.

142. In **Step 4, Configure group size and scaling policies**, under **Group size**, set the **Desired**, **Minimum**, and **Maximum** capacity values to `2` each. We want to always maintain two EC2 instances in our fleet.

143. Under **Scaling policies – optional**, ensure that **None** is selected, and then click the **Next** button.

144. In **Step 5, Add notifications**, do not add any notifications and click on the **Next** button.

145. In **Step 6, Add tags**, click the **Add tag** button. Specify a key-value pair to set the name of the servers you launch such that the **Key** field is set to `Name` and the **Value** field is set to `Production-Servers`.

146. Click the **Next** button to continue.

147. You are then presented with a **Review** page. Review the configuration settings that you have defined to make sure you followed the preceding series of steps correctly. When you are satisfied, go ahead and click the **Create Auto Scaling group** button at the bottom of the page.

AWS will then start configuring your Auto Scaling group and proceed to launch two EC2 instances based on the parameters of the groups. The EC2 instances will be configured as per the configuration you defined in the Launch Configuration earlier.

Once Auto Scaling has completed the deployment of your EC2 instances, you will be able to see the details of your deployment, as per the following screenshot:

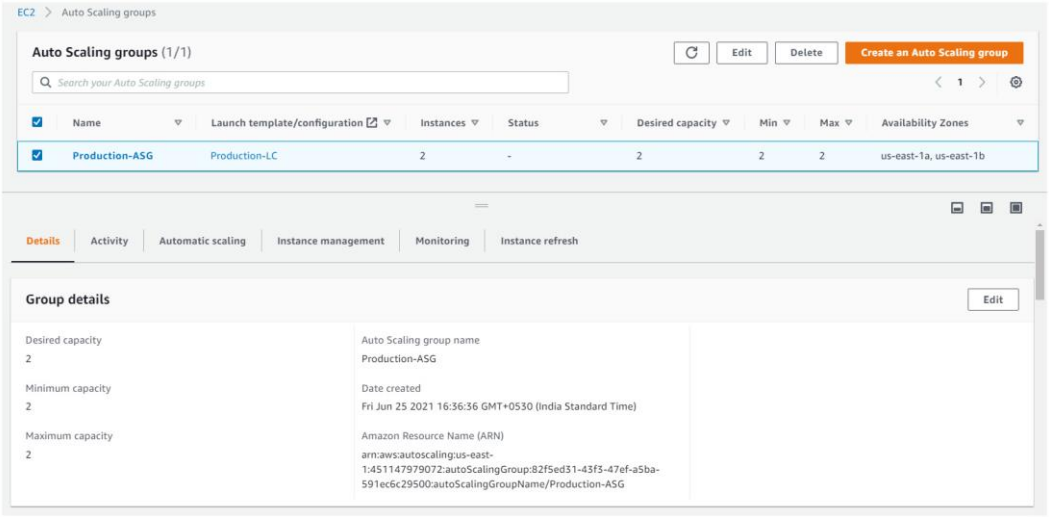

Figure 9.25 – Auto Scaling group deployment completed

At this point, your application has now been deployed across two EC2 instances. If you click on the **Activity** tab, you will see the AWS Auto Scaling service launched two EC2 instances in response to the fact that the minimum and desired capacity were not met before the launch of those EC2 instances. The Auto Scaling service will always try to ensure you have the desired number of EC2 instances in your fleet. Next, we will review the deployment and access the application.

Reviewing your deployment and accessing your application

You can check whether the Auto Scaling service has correctly deployed your application. Specifically, you can check whether two EC2 instances have been deployed and registered with your ALB. Furthermore, you can also check whether the ALB has marked those EC2 instances as healthy, indicating that the health checks have passed as well.

Here are the steps to perform these checks and then access the application:

148. In the EC2 dashboard, click on the **Target Groups** link from the left-hand menu under **Load Balancing**.

149. In the right-hand pane, click on the `Production-TG` target group that you created earlier.

150. On the details page of the `Production-TG` target group, you will note that two EC2 instances have been launched and both are in a **healthy** state, as per the following screenshot:

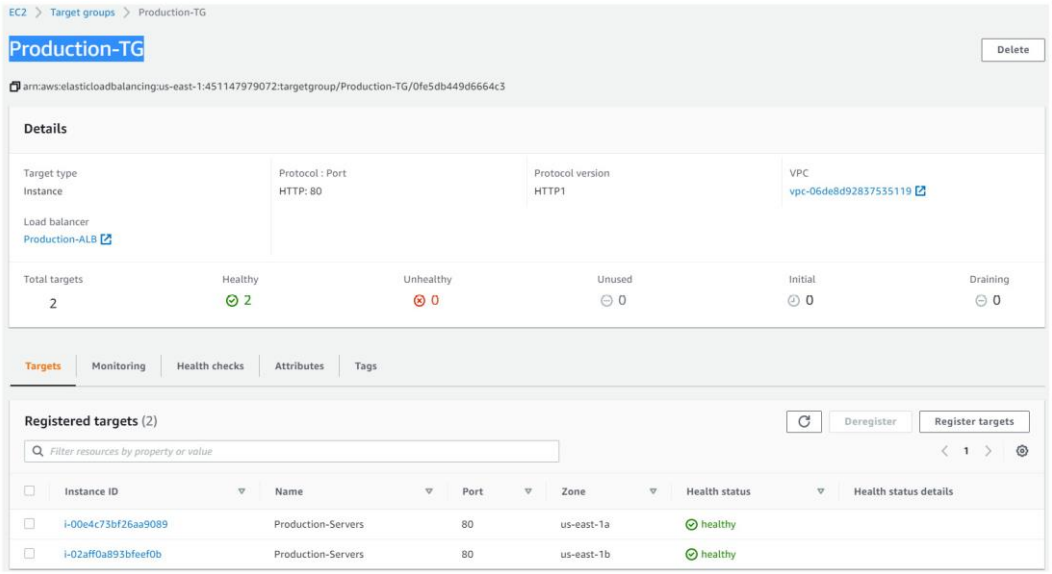

Figure 9.26 – Healthy EC2 instances registered to load balancer target group

151. Next, click on the **Instances** link from the left-hand menu.

152. You will notice that two instances with the name `Production-Servers` have been launched, with one EC2 instance in the `us-east-1a` AZ and the other in the `us-east-1b` AZ, as per the following screenshot:

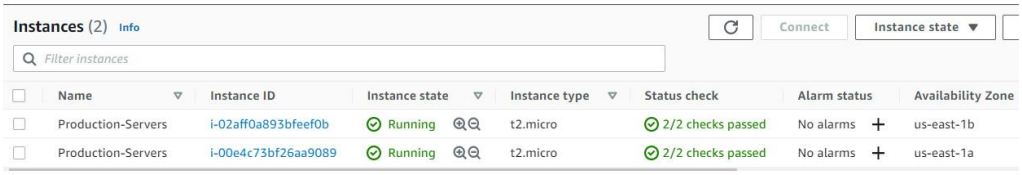

Figure 9.27 – Auto Scaling group successfully launched two EC2 instances

153. Next, we can access our application. From the left-hand menu, click on the **Load Balancers** link under **Load Balancing**.

154. In the right-hand pane, you will find your ALB details, as per the following screenshot:

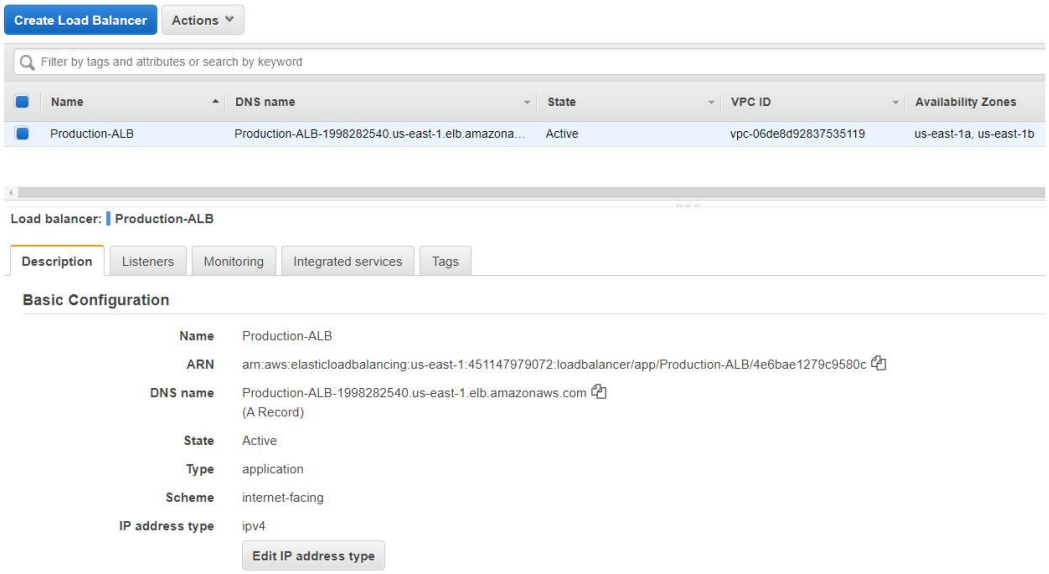

Figure 9.28 – ALB details for Production-ALB

155. In the bottom pane, you will find a **DNS name** link for your ALB. Copy this URL and paste it into a new browser window. If you have successfully completed all of the previous exercises, you will be able to access the **Good Deed of the Month Contest** web application, as per the following screenshot:

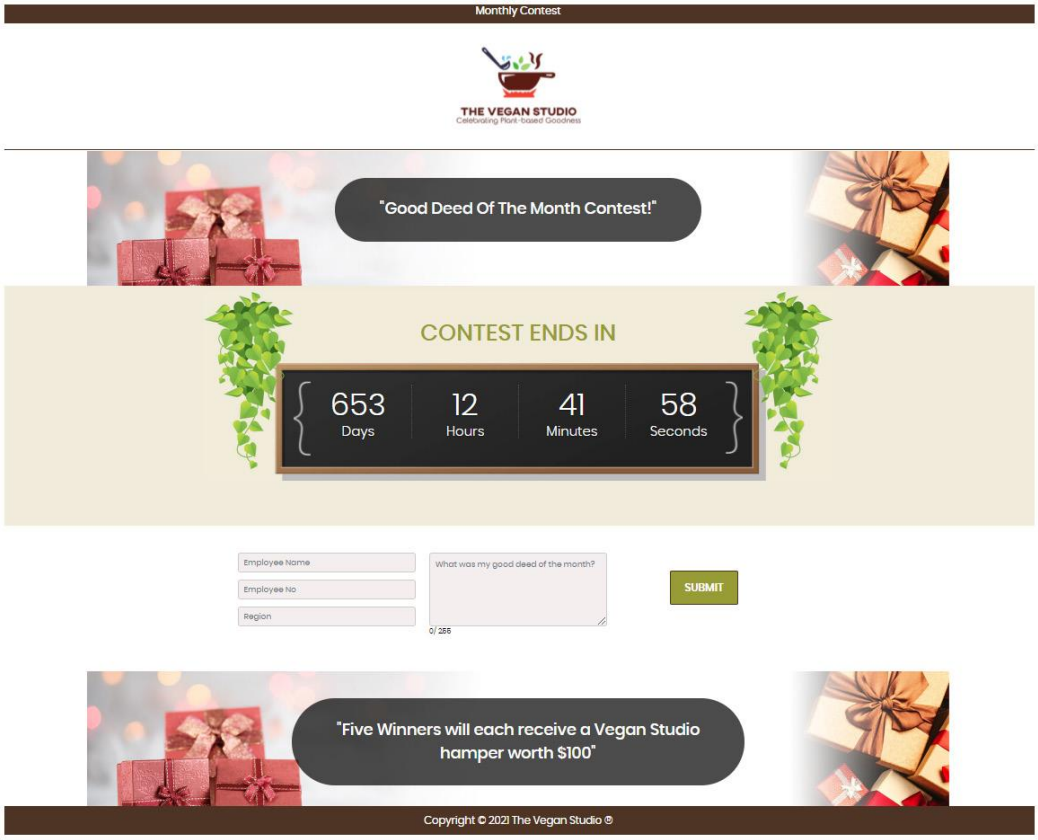

Figure 9.29 – Good Deed of the Month Contest web application

156. You can test your application by entering details of some potential good deeds you have done yourself. Once you have filled in the form in the middle of the web page, click the **SUBMIT** button.

157. You will note that when the web page reloads after you click on the **Submit** button, your *good deed of the month* is read back from the MySQL RDS database and presented on the page. If you submit more entries, these are also reported back. This demonstrates how the application can write to and read from the backend RDS database.

Let's take another look at the application architectural diagram to see how you have built this multi-tier solution:

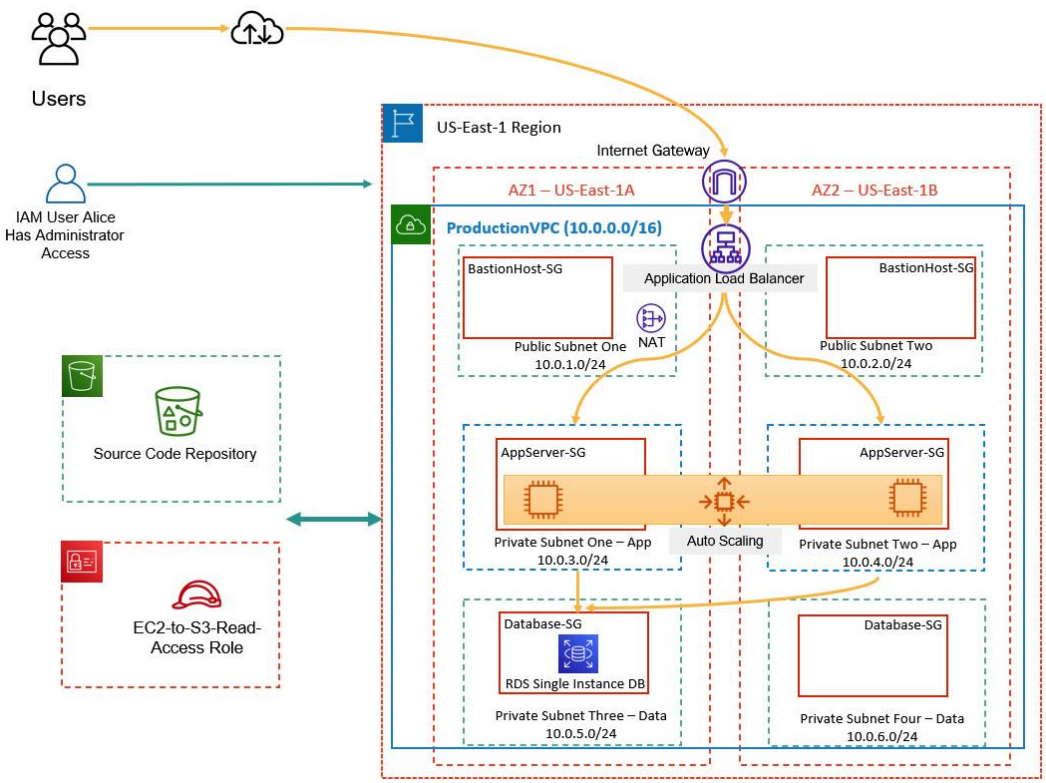

Figure 9.30 – Multi-tier application architecture

The key components of your architecture include the following:

- A VPC in the `us-east-1` Region that consists of public and private subnets across the `us-east-1a` and `us-east-1b` AZs. The VPC consists of six subnets in total: two public subnets to host your ALB nodes and NAT gateway, two private subnets to host your application tier, and another two private subnets to host the database tier.
- You also have an Amazon S3 bucket to host all the application source code and files.
- An IAM role that will allow your EC2 instances to gain authorization to read and download the application source code from the S3 bucket.
- An RDS database deployed in the `us-east-1a` AZ as a single database instance. Ideally, you would want to configure your database with Multi-AZ for HA.

- Two EC2 instances deployed using an Auto Scaling group and Launch Configuration. The Launch Configuration contains the necessary **bootstrapping** script to set up and configure the EC2 instances as web servers and automatically serve the application to your users. Furthermore, the Auto Scaling group automatically registers any EC2 instances deployed to the ALB target group. The target group runs health checks against the EC2 instances, marking them as healthy or unhealthy based on the health checks defined.
- Finally, the application code has the necessary database connection to access the backend RDS database and store any application data. Note that storing database connection details within the application is not considered best practice, and AWS offers several options such as the **AWS Systems Manager Parameter Store** or **AWS Secrets Manager** to manage such pieces of sensitive data. To keep this lab simple, we stored the database connection details within the application code.

Next, we look at how to test the AWS Auto Scaling service by simulating a failure of an EC2 instance.

Testing the Auto Scaling service

In this part of the exercise, you will stop an EC2 instance to simulate failure. When the EC2 instance is in a stopped state, it will not respond to the load balancer health checks. The load balancer will then mark the EC2 instances as unavailable. This will send a notification to the Auto Scaling group, confirming that there are fewer than two EC2 instances in the group, which is less than the desired capacity. Auto Scaling should then replace the instance and new server. Let's proceed with simulating this failure of an EC2 instance, as follows:

158. In the EC2 dashboard, click on the **Instances** link from the left-hand menu.

159. Next, in the right-hand pane of the screen, you will note that you have two EC2 instances running. Select the instance that is in the `us-east-1b` AZ, as per the following screenshot:

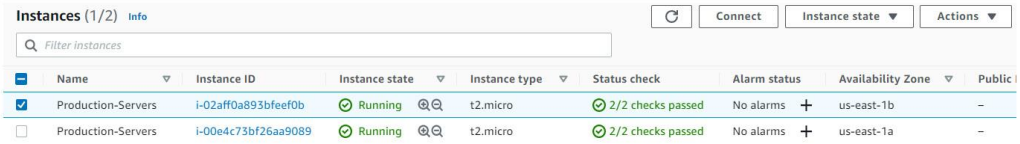

Figure 9.31 – EC2 instances in Running state

160. From the **Instance state** drop-down list at the top right-hand corner of the screen, select **Stop instance** while ensuring the EC2 instance in the `us-east-1b` AZ is selected.

161. You will be prompted with a dialog box to confirm whether you want to stop the selected instance. Go ahead and click the **Stop** button.

162. AWS will then perform a shutdown of your EC2 instance, which will take a couple of minutes. Wait until the EC2 instance is in a **Stopped** state, and then proceed to click on the **Auto Scaling Group** link under the **Auto Scaling** category from the left-hand menu.

163. Next, in the right-hand pane, click the `Production-ASG` Auto Scaling group.

164. Next, click on the **Activity** tab.

165. You will find additional activities that clearly show that the Auto Scaling service terminated the stopped EC2 instance. This is because, in a stopped state, it cannot respond to health checks. This is then followed by the launch of a new EC2 instance to replace the one that got terminated (see the following screenshot), in order to maintain our desired capacity at two instances as per the Auto Scaling group configuration. You will note that the Auto Scaling service will not try to restart the stopped instance. The Auto Scaling group will use the same Launch Configuration to configure the server with the application and register it to the ALB's target group, as illustrated here:

Figure 9.32 – Auto Scaling activity history

166. Now that the Auto Scaling service has replaced your EC2 instance, you can visit your application via the ALB URL to confirm that your application is still functioning as expected. Note that when one of the EC2 instances was stopped, the application was still accessible via the ALB URL because traffic would have been forwarded onto the other EC2 instance that was still running in the `us-east-1a` AZ.

Congratulations! Well done on completing the series of exercises to get to this stage. You have now learned how to design and architect a multi-tier application solution using a combination of AWS services to help you build an HA and scalable application.

In the next exercise, you will perform a cleanup operation to terminate unwanted resources so that you do not incur any further charges.

Exercise 9.7 – cleanup

In this exercise, you will terminate the various resources you deployed in the previous exercises. The first step is to delete the Auto Scaling group, which will terminate your EC2 instances. If you try terminating the EC2 instances manually, then the Auto Scaling group will simply launch new ones. Proceed as follows:

167. From the EC2 dashboard, click on **Auto Scaling Group** from the left-hand menu under **Auto Scaling**.

168. From the right-hand pane, select the `Production-ASG` Auto Scaling group. Click the **Delete** button and confirm the delete request by typing in `delete` in the textbox and clicking the **Delete** button.

169. Next, click on **Launch Configuration** from the left-hand menu under the **Auto Scaling** service.

170. Next, select the `Production-LC` Launch Configuration, and from the **Actions** menu, click **Delete Launch Configuration**. Confirm the delete request.

171. Next, click **Load Balancers** under the **Load Balancing** menu.

172. From the right-hand pane, select the `Production-ALB` load balancer, and from the **Actions** drop-down list, click **Delete**.

173. Next, click on **Target Groups** under **Load Balancing** in the left-hand menu. In the right-hand pane, select the `Production-TG` target group, and from the **Actions** drop-down list, click **Delete** and delete the target group.

Your load balancer and the Auto Scaling group have been removed from your account. Next, navigate to the Amazon RDS console, as follows:

174. From the left-hand menu, click on **Databases**.

175. In the right-hand pane, select the database that you created earlier in *Chapter 8*, *AWS Databases Services*.

176. From the **Actions** drop-down list, click **Delete**.

177. Uncheck the **Create final snapshot?** box and click the acknowledgment box that states that upon deletion, automated backups, including system snapshots and **point-in-time recovery** (**PITR**), will no longer be available. Next, type `delete me` in the confirmation textbox and click the **Delete** button. Your Amazon RDS database will now be deleted.

178. Next, we should also remove the database subnet group created previously. From the left-hand menu, click on **Subnet groups**.

179. In the right-hand pane, select the database subnet group you created previously and click the **Delete** button.

    Now that your database has also been deleted, we can delete the VPC. Navigate to the VPC console.

180. Before we can delete the VPC, you need to delete the NAT gateway. From the left-hand menu, click on **NAT Gateways**. In the right-hand pane, select the `Production-NAT` NAT gateway, and from the **Actions** drop-down list, click **Delete NAT gateway**. You will then be presented with a dialog box to confirm the deletion. Type `delete` in the confirmation box and click the **Delete** button.

181. Next, you need to check whether there are any network interfaces still attached to your VPC. Usually, you will find that the Amazon RDS network interface (`RDSNetworkInterface`) may still be attached to the `Database-SG` security group. If

that is the case, you will first need to delete this interface before you can delete the VPC, as follows:

182. Navigate to the EC2 console and select **Network Interfaces** from the left-hand menu.

183. Check whether there are any interfaces still attached to your VPC by cross-referencing the VPC ID with your `Production-VPC` security group ID. Select the network interface and then, from the **Actions** menu, click the **Delete** button. The following screenshot shows the attached network interface:

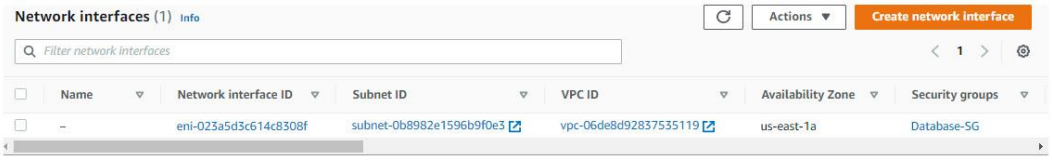

Figure 9.33 – Network interfaces attached to your VPC

184. Navigate back to the VPC console. Next, from the left-hand menu, click on **Your VPCs**.

185. From the right-hand pane, select the `Production-VPC` security group, and then, from the **Actions** drop-down list, select **Delete VPC**.

186. You will be presented with a list of all components of your VPC that will be deleted. Confirm your delete request by typing `delete` into the confirmation textbox and then clicking the **Delete** button.

Your VPC should now get deleted. Within the VPC console, there is still one more component you need to delete, and that is the elastic IP address you allocated to your AWS account. This is because elastic IP addresses are only free if they are associated with running instances (or in our case, the NAT gateway). Proceed as follows:

187. From the left-hand menu, click on **Elastic IPs**.

188. In the right-hand pane, select the IP address you allocated to your AWS account, and from the **Actions** drop-down list, click the **Release Elastic IP addresses** link. Next, in the **Release Elastic IP addresses** dialog box, click the **Release** button.

At this point, your elastic IP address has been released back to AWS. You will not incur any charges on unused elastic IP addresses in your account.

This completes your cleanup exercise for this chapter, and you can now rest assured that you will not incur any further costs associated with this lab.

Important Note

You still have an Amazon S3 bucket that hosts all the source code for the application you deployed in this chapter. While you could delete that resource, we advise you to keep the bucket as we will be using it for the exercises in the next chapter.

Next, we provide a summary of this chapter and the key concepts to remember for the exam.

Questions

1. You are planning on developing a website in multiple languages such that you have one fleet of EC2 instances that serves the English version of your site and another fleet that serves the Spanish version of your site. For each language version, you will be configuring URLs with different paths such that the English version of your site will contain `/en/` in the path and the Spanish version will contain `/es/`.

   Which type of load balancer would you use to route traffic to ensure users connect to the site in their desired language?

   A. CLB

   B. NLB

   C. ALB

   D. Path-based load balancer

2. You are building a multi-tier architecture with web servers placed in the public subnet and application servers placed in the private subnet of your VPC. You need to deploy ELBs to distribute traffic to both the web server farm and the application server farm. Which type of load balancer would you choose to distribute traffic to your application servers?

   A. Internet-facing

   B. Internal load balancer

   C. Dynamic load balancer

   D. Static load balancer

3. Which ELB is ideal for handling volatile workloads and can scale to millions of requests per second?

   A. ALB

   B. NLB

   C. CLB

   D. Premium load balancer

4. Which configuration feature of the AWS Auto Scaling service enables you to define a maximum number of EC2 instances that can be launched in your fleet?

   A. Auto Scaling group

   B. Auto Scaling Launch Configuration

C. Auto Scaling max fleet size

D. Auto Scaling policy

5. When an ELB detects an unhealthy EC2 instance, which action does it perform regarding distributing incoming traffic?

A. It continues to send traffic to the failed instance.

B. It terminates the failed instance so that it is not part of the ELB target group.

C. It only sends traffic to the remaining healthy instances.

D. It restarts the unhealthy EC2 instance.

6. Which service does an AWS ALB integrate with to protect your applications from common web attacks?

A. WAF

B. Shield

C. Inspector

D. Key Management Service (KMS)

Chapter 10

Figures

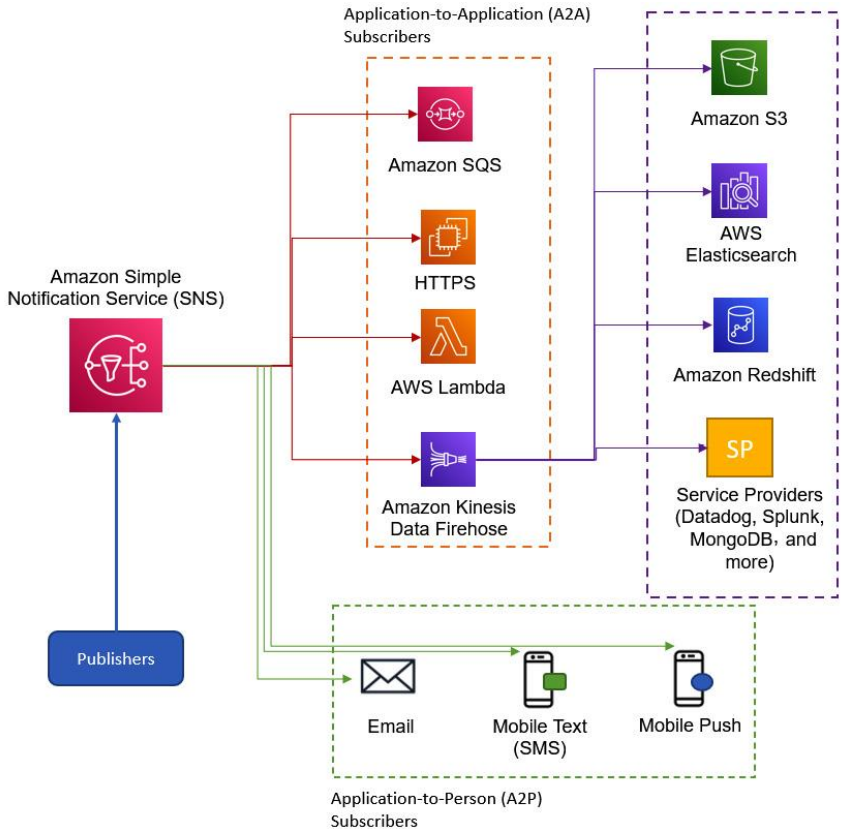

Figure 10.1 – Amazon SNS subscriber endpoints

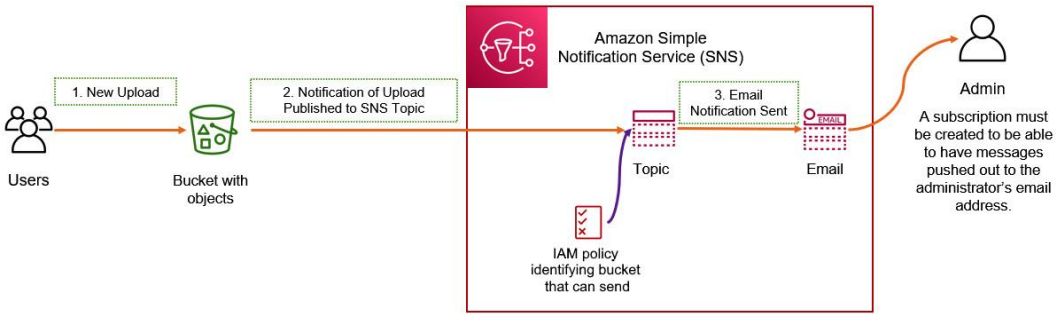

Figure 10.2 – Example – configuring an SNS notification for an S3 event notification

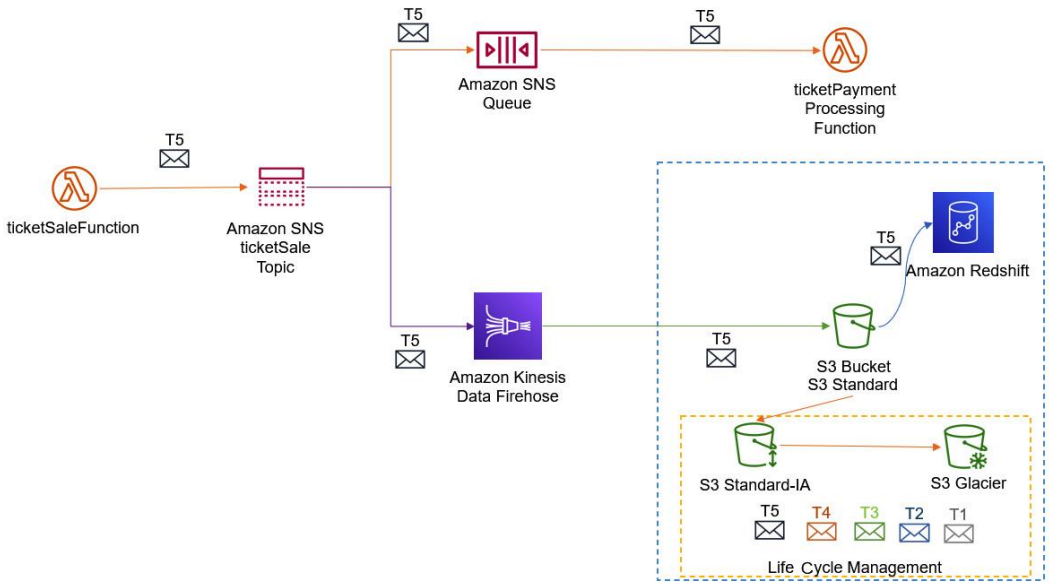

Figure 10.3 – Example of an Amazon SNS Fanout scenario

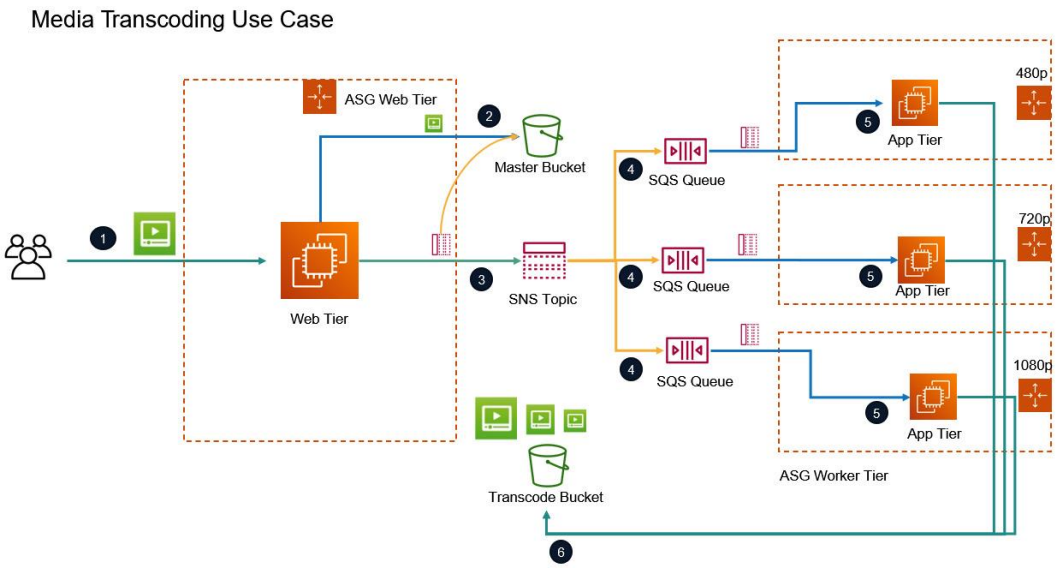

Figure 10.4 – Amazon SQS use case example

Figure 10.5 – Amazon SQS standard queue

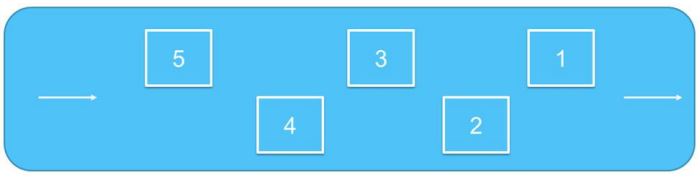

Figure 10.6 – Amazon SQS FIFO queue

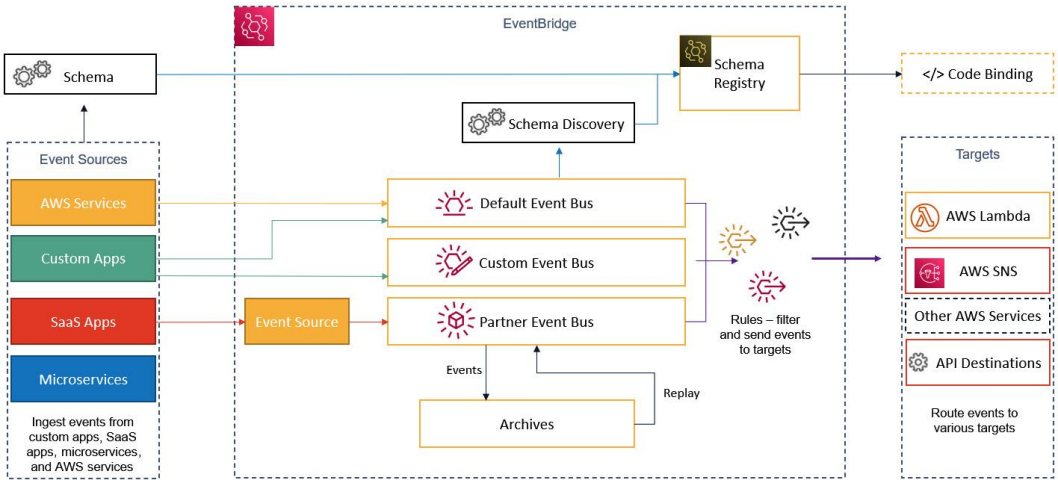

Figure 10.7 – How EventBridge works

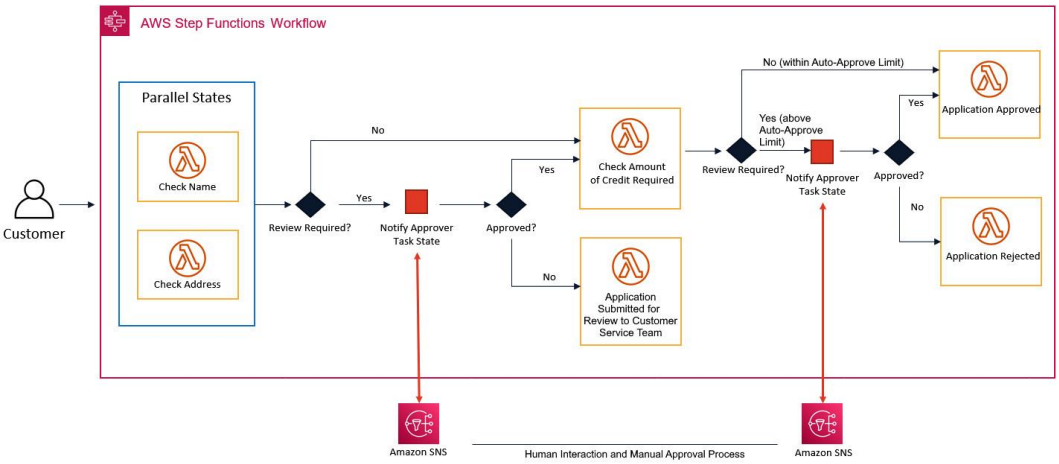

Figure 10.8 – Example of a credit card application workflow

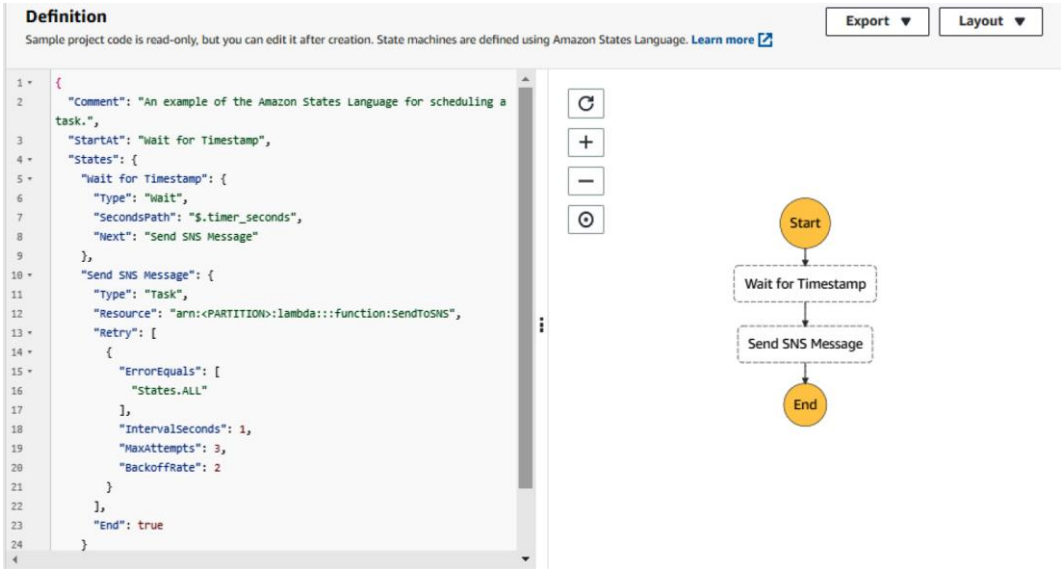

Figure 10.9 – AWS Step Functions task timer example

Code

Example of ARN:

So, for example, an SNS topic called `new-recipe-upload-alert`, created in the London Region, with an AWS account ID of `123456789789` will have an ARN of `arn:aws:sns:eu-west-2:1234567890123789: new-recipe-upload-alert`.

Exercise 10.1 – Amazon S3 event notification using Amazon SNS

In the previous chapter, you designed, architected, and deployed a complete web application using several AWS services. One such service was the Amazon S3 service, where you created a bucket to host your application source code repository. The source code was comprised of multiple files that helped you build your web application.

Maintaining this source code is of paramount importance and any changes that are made to the code need to be monitored. There are several best practice strategies you can use to manage your source code, including using DevOps principles. In this exercise, your senior administrator, **Alice**, would like to know whenever a new file (object) gets uploaded to this source code repository, which is stored in the Amazon S3 bucket.

Amazon S3 comes with a feature known as event notifications. This feature enables you to receive notifications when certain events occur in your S3 bucket, such as an object being created or deleted. The service can be configured to send out such notifications to an Amazon SNS topic, which an administrator can subscribe to using an email as the endpoint. Let's configure an Amazon S3 notification to send email alerts to **Alice** whenever a new file is uploaded (that is, created) to the S3 bucket that hosts the source code repository.

This exercise is divided into four main steps, as described in the following sub-sections.

Step 1 – creating an SNS topic and subscribing to the topic

The first step is to create an SNS topic that will be used as the logical access point that Alice will subscribe to. Messages sent to this topic will then be emailed to Alice:

1. From the AWS Management Console, search for `SNS` in the top search box and select the service to be taken to the Amazon SNS dashboard.
2. If you have never created an SNS topic before, you should see the Amazon SNS splash screen.
3. Click on the far left-hand menu icon, denoted by the three lines, to expand the sidebar.
4. Next, click on the **Topics** link from the menu.
5. Click the **Create topic** button in the right-hand pane of the screen.
6. On the **Create topic** page, in the **Details** section, select the **Standard** type under **Type**.

7. Enter a name for the topic; for example, `source-code-changes`. Next, enter a display name for the topic; for example, `Source Code Changes Alert`.
8. Leave all the remaining settings as their default values and click the **Create topic** button.
9. Once the topic has been created, you will be redirected to the topic page. Make a note of the topic's ARN, as per the following screenshot:

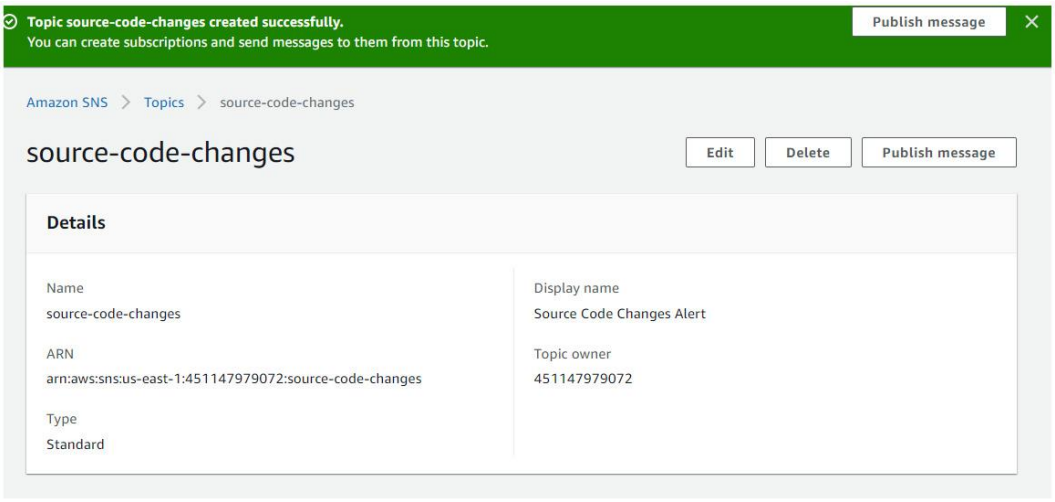

Figure 10.10 – Amazon SNS topic

10. Now that you have created a topic, you can create a subscription for it. We will be using email as the endpoint for notifications, and you can use your email address to receive the notifications.
11. In the bottom pane of the topics page, as per the previous screenshot, you will find a section to create subscriptions. Click on the **Create subscription** button.
12. On the **Create subscription** page, you will note that the topic ARN is already selected. If not, ensure that you paste the topic ARN that you made a note of earlier.
13. Next, under **Protocol**, select **Email** from the drop-down list.
14. In the text box under **Endpoint**, provide your email address.
15. Click the **Create subscription** button at the bottom of the page.
16. You will get a confirmation statement to say that your subscription has been created. However, its status will be set to **Pending confirmation**. AWS will have sent you a confirmation request to your email account. You will need to log into your email account and confirm the subscription to activate it. I have just logged into my email account to do the same, as per the following screenshot of my Gmail account:

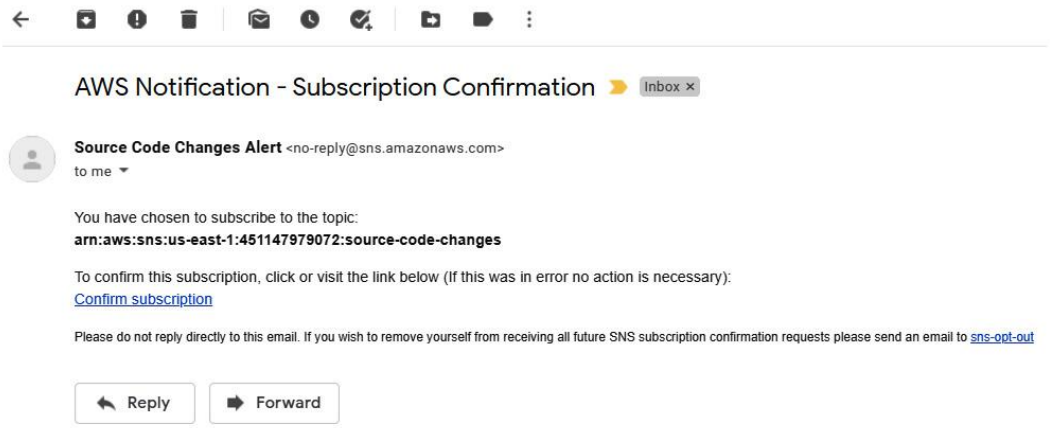

Figure 10.11 – Email subscription request for topic subscription

17. Once you confirm your subscription, return to the Amazon SNS dashboard and click on the **Topics** link from the left-hand menu.

Now that you have confirmed your subscription to the topic, you can configure an access policy that will grant the Amazon S3 service the permissions to send notifications to the topic.

Step 2 – configuring your SNS topic policy

For Amazon S3 to send notifications to the SNS topic you just created, you will need to configure an **access policy**. An access policy defines who or what can access your topic and publish messages to it. We have provided a sample policy document in the GitHub repository for this study guide that you will need to amend https://github.com/PacktPublishing/AWS-Certified-Cloud-Practitioner-Exam-Guide. You will need to have the following information before editing the policy:

- The ARN of the SNS topic, which you made a note of earlier.
- The Amazon ARN of the S3 bucket, which you created in the previous chapter. You can find the bucket ARN by clicking on the **Properties** tab on the bucket details page within your Amazon S3 dashboard.
- The AWS account ID (which you can obtain by clicking on your account name in the top right-hand corner of the screen and making a note of the 12-digit number next to **My Account**).

Open the sample access policy document in Notepad or a text editor of your choice, as per the following screenshot:

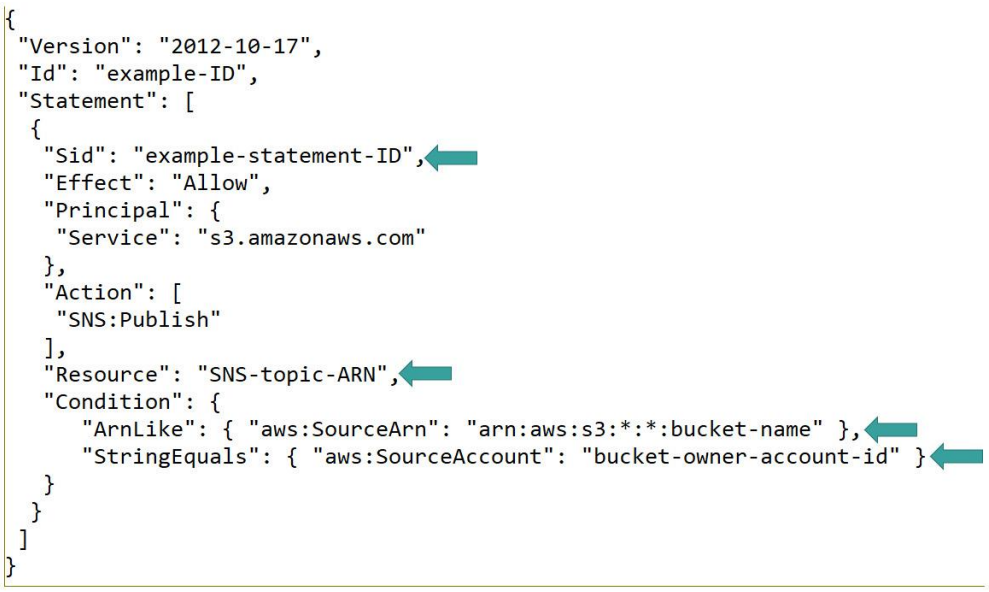

Figure 10.12 – Sample access policy

Replace the values in the policy, as highlighted by the arrows in the preceding screenshot, with the following:

- For `Sid`, change `example-statement-ID` to any relevant information you would like to use; for example, `source-code-change-policy`.
- For `Resource`, change `SNS-topic-ARN` to the ARN of your topic, making sure to place the ARN in double quotes.
- For `ArnLike`, change `arn:aws:s3:*:*:bucket-name` to the ARN of your bucket name.
- For `StringEquals`, change `bucket-owner-account-id` to your AWS account ID.

Save the file and keep it handy for the next step of steps:

1. Navigate back to the Amazon SNS dashboard and from the left-hand menu, click ron **Topics**.
2. Click on your SNS topic in the middle pane, which will redirect you to the topic's details page, as per the following screenshot:

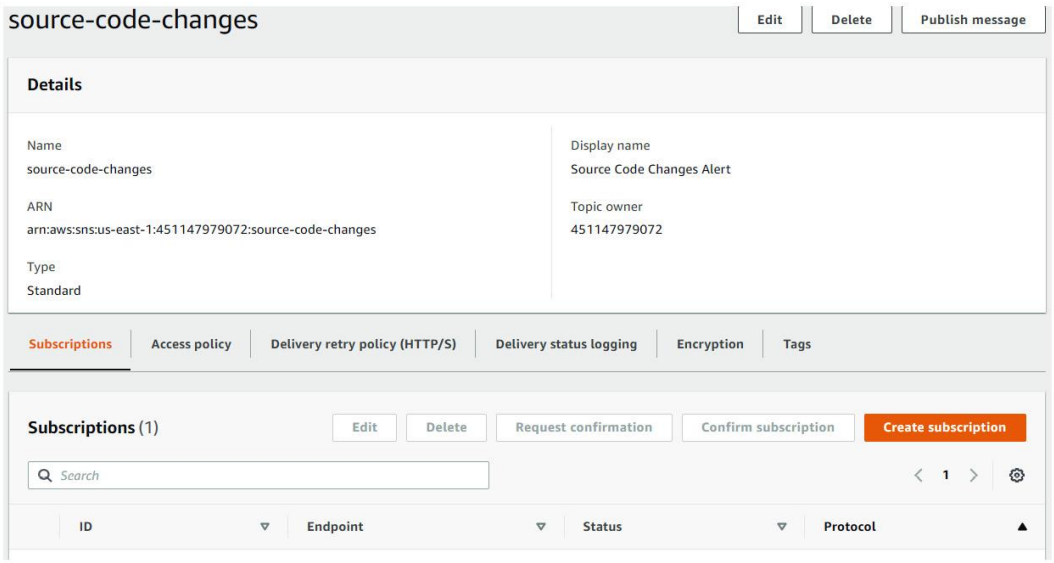

Figure 10.13 – SNS topic details page

3. Click on the **Access policy** tab in the bottom section of the pane.
4. You will find a default access policy that allows only the topic owner to publish to the topic.
5. In the top half of the pane, click on the **Edit** button.
6. Next, expand the **Access policy – optional** section.
7. Next, highlight and delete the existing policy that is in the JSON editor, and paste in a copy of your amended access policy instead.
8. Finally, click the **Save changes** button at the bottom of the page.

Now that you have set up the SNS topic and an appropriate access policy, it is time to set the Amazon S3 event notification service.

Step 3 – setting up the Amazon S3 event notification service

In this step, you will configure the event notification service on your Amazon S3 source code bucket, which hosts your application repository to send out alerts every time a new file is uploaded to the bucket:

1. Navigate to the Amazon S3 dashboard and click on the **Buckets** link from the left-hand menu.
2. From the right-hand pane, click on the Amazon S3 bucket that you created in the previous chapter to host your source code files.
3. Next, click on the **Properties** tab and scroll down until you reach the **Event Notifications** section.
4. Click the **Create event notification** button.

5. Enter a name for your event, such as `New files added alert`.
6. In the **Event types** section, tick the box that states **All object create events**.
7. Scroll further down until you reach the **Destination** section.
8. Select **SNS topic** from the **Destination** options.
9. Under **Specify SNS topic**, select the SNS topic that you created earlier in *Step 1* from the **SNS topic** drop-down list.
10. Finally, click the **Save changes** button.

Now that you have configured S3 to send event notifications to your SNS topic, it is time to test the configuration.

Step 4 – testing the configuration

In this step, we will test out the configuration of our Amazon S3 event notification service:

1. In the Amazon S3 dashboard, from the left-hand menu, select **Buckets**.
2. From the right-hand pane, select your Amazon S3 bucket, which will contain the source code files.
3. Next, click on the **Upload** button.
4. Go ahead and upload any random file you have access to. Alternatively, you can create a text file, save it, and then upload that text file instead. You can either use the **Add files** button to browse for a file on your computer or simply drag and drop a file from another file explorer window into the upload area.
5. Upload your file to the Amazon S3 bucket by clicking on the **Upload** button at the bottom of the page.
6. Once the upload has succeeded, click the **Close** button. Your object should be visible in the list of objects in the bucket.
7. Access your email account once again and check whether you have received a notification from AWS, alerting you to the fact that a new object has been uploaded. Refer to the following screenshot as an example:

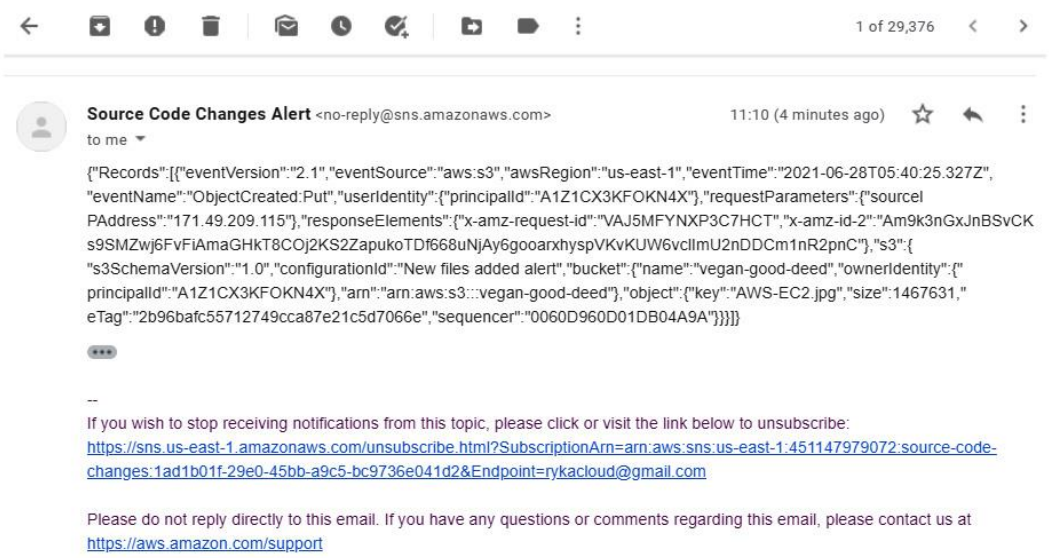

Figure 10.14 – Amazon S3 event notification alert email

As you can see, AWS has sent me an email, alerting me to the fact that an object was uploaded (created) in my Amazon S3 bucket. The email contains lots of information, including the time of the event, the alert's name, the bucket in question, the name of the object that was uploaded, as well as its size. As you can appreciate, this can be very useful for auditing purposes.

Amazon S3 event notifications can use other destinations too, such as an SQS queue or a Lambda function. In this exercise, you learned how Amazon SNS can be used to push out notification messages to an email address.

In the next exercise, you will perform a cleanup to remove any resources that are no longer required from our AWS account.

Exercise 10.2 – cleaning up

In this exercise, you will delete the resources that you created in the previous exercise as part of the cleanup process:

1. Navigate back to the Amazon SNS console.
2. From the left-hand menu, select **Topics**.
3. Next, from the right-hand pane, select the **source-code-changes** topic. Click the **Delete** button.
4. You will be prompted to confirm the delete request with a dialog box. Type `delete me` in the confirmation text box and then click the **Delete** button. The topic will be deleted.

Now that you have deleted the Amazon SNS topic, you can also delete the Amazon S3 bucket as we no longer require it:

1. Navigate to the Amazon S3 console.
2. From the left-hand menu, click on **Buckets**.

3. From the right-hand pane, select the bucket that you uploaded your source code to earlier.
4. You can only delete buckets if they are empty. This means that you have to delete the objects in your bucket first. With the bucket selected, click the **Empty** button.
5. Next, you will be prompted to confirm that you wish to delete the objects by typing `permanently delete` in the confirmation text box. Then, you can click on the **Delete** button to empty the bucket.
6. Now that the bucket has been emptied, you can delete it.
7. Click the **Exit** button to go back to the list of buckets. With the bucket still selected, click the **Delete** button. Next, in the confirmation text box, type in the name of the bucket to confirm that you wish to delete it and click the **Delete bucket** button.

Your Amazon S3 bucket will be successfully deleted.

Next, we will provide a summary of this chapter and the key concepts that you learned.

Questions

Answer the following questions to test your knowledge of this chapter:

1. Which AWS services does Amazon CloudWatch use to send out email alerts to administrators when alarms are triggered and enter the `Alarm` state?
   A. Amazon SNS
   B. Amazon SES
   C. Amazon CloudTrail
   D. Amazon Email
2. Which feature of Amazon CloudWatch enables you to create a visualization of metrics by resource type and service?
   A. CloudWatch Events
   B. CloudWatch Logs
   C. CloudWatch Alarms
   D. CloudWatch dashboards
3. Which AWS application integration service can be configured to offer A2P communication using mobile SMS to send out text alerts?
   A. Amazon SQS
   B. Amazon SNS

C. Amazon Amplify

D. Amazon Workspaces

4. You need to configure your Amazon SNS topic to push out messages of newly uploaded videos to an Amazon S3 bucket, across three different SQS queues. Each queue is designed to encode the raw video into a different resolution. Which feature of Amazon SNS enables you to push out such notifications in parallel?

   A. Amazon SNS standard topic

   B. Amazon SNS FIFO topic

   C. Fanout scenario

   D. Amazon EventBridge

5. Which Amazon SQS queue type offers maximum throughput, best-effort ordering, and at least one delivery?

   A. SQS standard queue

   B. SQS power queue

   C. SQS FIFO queue

   D. SQS LIFO queue

6. Which AWS service is designed to help you build a decoupled application architecture where incoming web requests can be held in a queue until a backend application can retrieve and process the request?

   A. Amazon SQS

   B. Amazon SWF

   C. Amazon SNS

   D. Amazon Step Functions

7. You are required to configure an SQS queue for your application where the order of messages needs to be preserved for the application to function correctly. Which type of queue do you need to configure?

   A. SQS standard queue

   B. SQS power queue

   C. SQS FIFO queue

   D. SQS LIFO queue

8. To reduce costs, you have been asked to automate the shutdown of a fleet of UAT test servers every weekday at 7 P.M. and then restart them the following weekday at 8 A.M. The servers should remain in the shutdown state at weekends.

   Which AWS service can help you achieve the preceding requirements?

   A. Amazon SQS

   B. Amazon Athena

   C. Amazon EventBridge

   D. Amazon SNS

9. Which AWS service enables you to manage application workflows as state machines by breaking them into multiple steps, adding flow logic, and tracking the inputs and outputs between the steps?

   A. Amazon Step Functions

   B. Amazon SQS

   C. Amazon SNS

   D. Amazon SWF

10. Which AWS service offers an orchestration service to coordinate work across application components that make use of decider programs to determine the latest state of each task and use it to initiate subsequent tasks?

    A. Amazon SNS

    B. Amazon EventBridge

    C. Amazon SQS

    D. Amazon SWF

Chapter 11

Figures

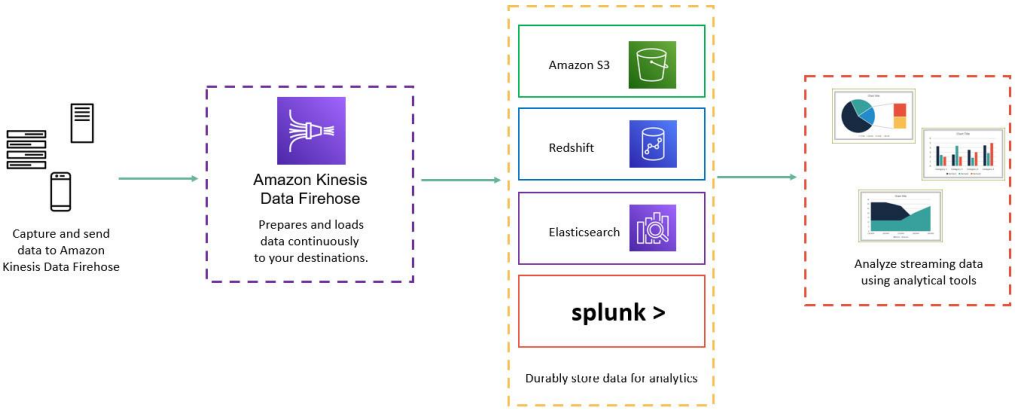

Figure 11.1 – Kinesis Firehose

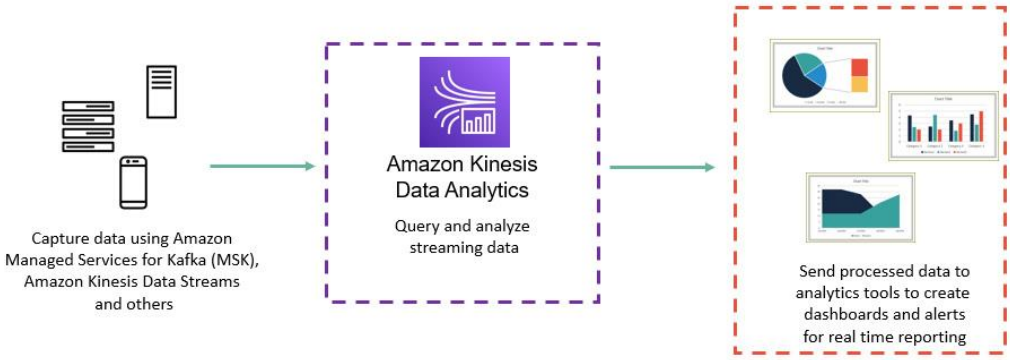

Figure 11.2 – Amazon Kinesis Data Analytics

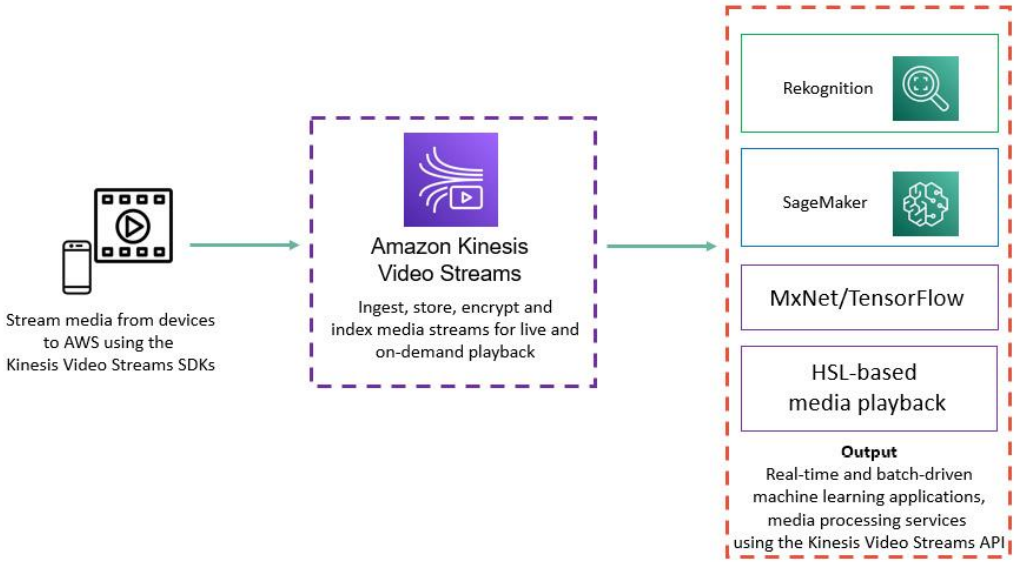

Figure 11.3 – Amazon Kinesis Video Streams

Links

You can view the pricing overview of quicksight at aws.amazon.com/quicksight/pricing/.

Exercise 11.1 – analyzing your sales report with Amazon Athena and AWS Glue

In this exercise, you will need to download a sample CSV file, which is available in the Packt GitHub repository for this chapter https://github.com/PacktPublishing/AWS-Certified-Cloud-Practitioner-Exam-Guide. This is a simple CSV file that contains some sales data for the Vegan Studio, the fictitious company that you have been carrying out a series of exercises for in the previous chapters.

You will need to store this CSV file in an Amazon S3 bucket and then use Amazon Athena to run queries against the data. Ensure that you have downloaded the CSV file and stored it on your computer before you start this exercise.

Step 1 – Amazon S3

1. Log into your AWS account using the IAM user ID of our senior administrator, **Alice**.
2. Navigate to the Amazon S3 dashboard.
3. Create two new buckets with appropriate names. For example, I have named my buckets `vegan-sales-report` (to store the CSV file) and `vegan-query-results` (to store the Athena query results). Since I have taken these names, you will not be able to use them since bucket names must be unique in the AWS ecosystem. Ensure that the buckets are created in the `us-east-1 (N.Virginia)` Region.

4. Next, upload your CSV file to the bucket that will be used to host the data. Recall the steps required from the previous chapters to complete the upload. (Tip: try to do this from memory as this will help you build your confidence.)

Step 2 – Amazon Athena and Amazon Glue

1. Navigate to the Amazon Athena dashboard. You can search for the Athena service from the top search bar in your AWS Management Console.

2. If this is the first time you are accessing Amazon Athena, you should see a splash screen. Click **Get Started**. If you do not see the **Get Started** option, this is because you are using the new user interface. AWS is notorious for making changes to the UI. If you do see the new console, then you will need to click on the **Explore the query editor** button. For this lab, we suggest that you use the old console for now. To access the old console, click on the ellipsis (three dashes) in the top far left of the console and switch the toggle to disable the **New Athena experience** option. This will take you back to the old console interface:

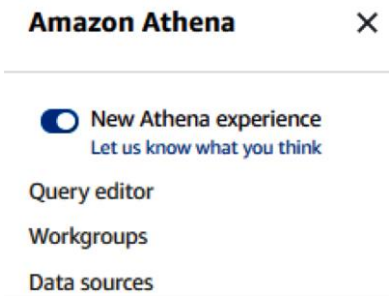

Figure 11.4 – Disabling the New Athena experience toggle switch

3. From the top right-hand corner, click on the **Settings** link. You will be presented with the following dialog box. You will need to provide the S3 bucket details to store your query results. The format should be `s3://bucket-name`. You can also store your queries in a sub-folder and choose to encrypt your query results:

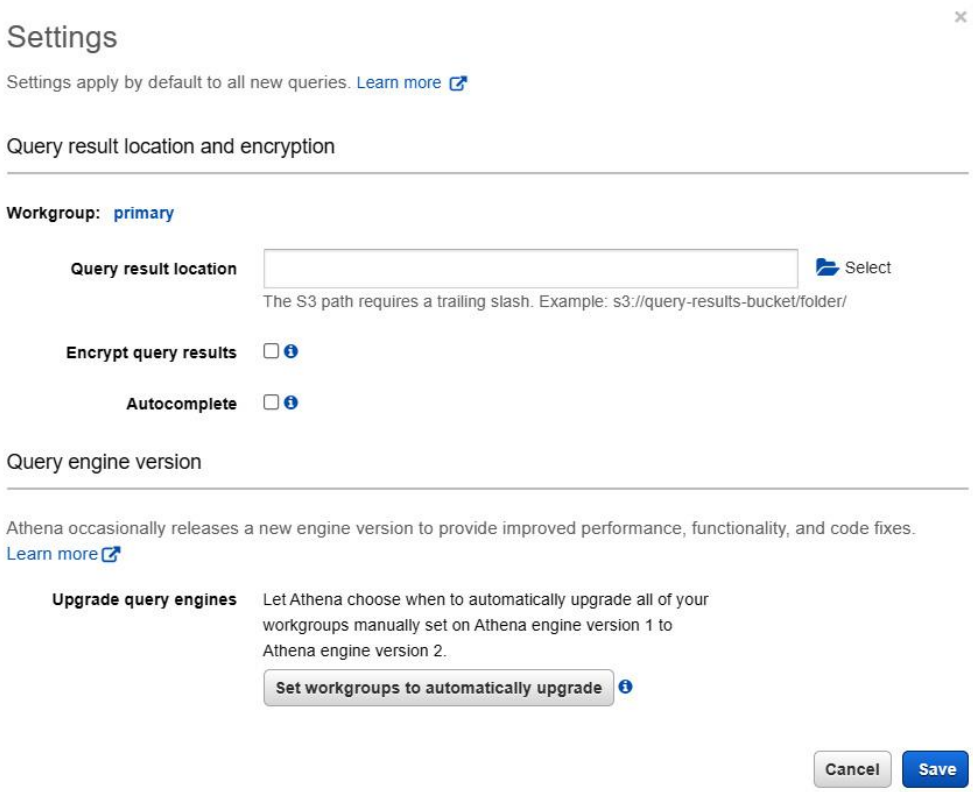

Figure 11.5 – Amazon Athena – Settings

4. Next, click the **Save** button.
5. Next, from the left-hand menu, click on **Connect data source**, as per the following screenshot:

Figure 11.6 – Amazon Athena – Connect data source

6. Under **Choose where your data is located**, ensure that **Query data in Amazon S3** is selected.
7. Under **Choose a metadata catalog**, ensure that **AWS Glue Data Catalog** is selected. For this exercise, you will use AWS Glue to crawl your data and create a schema. There is a slight charge to this, but it is very minimum, and you will only need to do this once.
8. Click the **Next** button on the right-hand pane of the page.

9. Under **Connection details**, ensure that **AWS Glue Data Catalog in this account** is selected. Then, under **Choose a way to create a table**, select **Create a crawler in AWS Glue**.
10. Click the **Connect to AWS Glue** button. This will launch **AWS Glue** in a new browser tab. Switch over to this tab to configure Amazon Glue. Do not close the Amazon Athena browser tab as we will return to this later.
11. If you see the splash screen, click the **Get started** button.
12. From the left-hand menu, click **Crawlers**.
13. From the right-hand pane, click the **Add crawler** button. You will be presented with the **Add crawler** wizard:
14. Provide a name for the crawler. Click **Next**.
15. On the **Specify crawler source type** page, ensure that the **Data stores** and **Craw all folders** options are selected.
16. Click **Next**.
17. On the **Choose a data store** page, ensure that **S3** is selected as your chosen data store.
18. Next, under **Craw data in**, select the **Specified path in my account** option. For **Include path**, provide the S3 bucket URL of your S3 bucket that hosts the sales report. In this case, the URL is in the format of `s3://bucket-name.` Note that at the end of the path defined for your S3 bucket, ensure that you add another slash (`/`). **For example, my bucket path reads** `s3://vegan-sales-report/`.
19. Click **Next**.
20. On the **Add another data store** page, click **No** and then **Next**.
21. Next, on the **Choose an IAM Role** page, select the **Create an IAM role** option and type a name in the text box next to **AWSGlueServiceRole-**. This will form the path of your IAM **role** name. For example, I have typed in `VeganSalesRole` so that it is self-explanatory. Click **Next**.
22. On the **Create a schedule for this crawler** page, set **Frequency** to **Run on demand**. Click **Next**.
23. On the **Configure the crawler's output** page, click the **Add database** button.
24. In the **Add database** dialog box that appears, provide a name for your database, such as `vegansalesdb`. Click **Create**.
25. You will be taken back to the **Configure the crawler's output** page, with your newly created database name shown in the **Database** text box. Click **Next**.
26. On the **Review all steps** page, click **Finish**.

27. You will be redirected to the **Crawlers** page. Here, you will be able to see that your crawler has been created. Click on the checkbox next to your crawler and click the **Run crawler** button, as per the following screenshot:

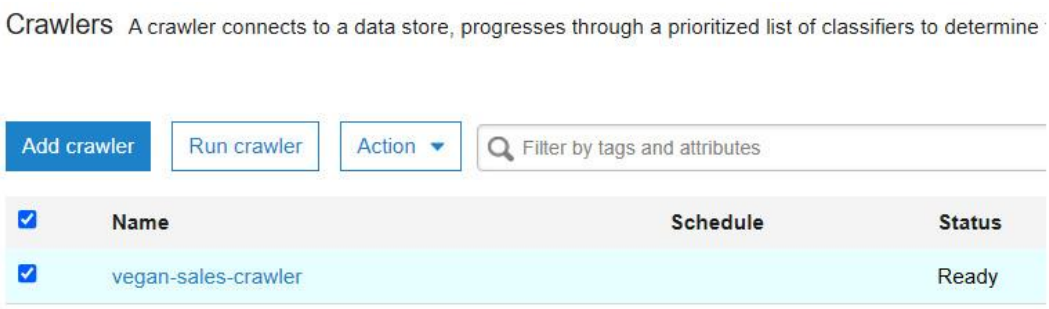

Figure 11.7 – Amazon Glue – Run crawler

28. After a minute or two, you should find that its **Status** is set to **Ready** and that the crawler has successfully run. You will see that a table has been added, as per the following screenshot:

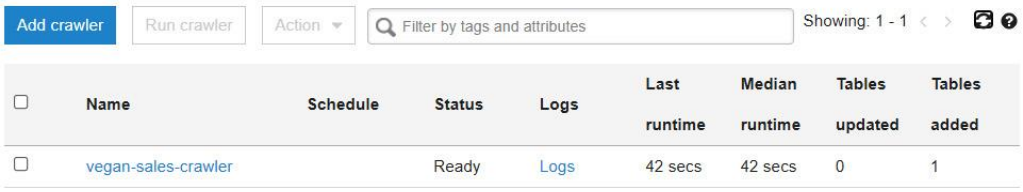

Figure 11.8 – Amazon Glue – Crawl complete

29. Now that the crawl is complete, we can return to the Amazon Athena browser tab.

Step 3 – Amazon Athena

1. Back in the Athena browser tab, go ahead and click on the **cancel** button at the bottom right-hand corner of the page. This will take you back to the main **Amazon Athena Data sources** page, where you will see that your recently created Glue Catalog is listed under **Data sources**, as per the following screenshot:

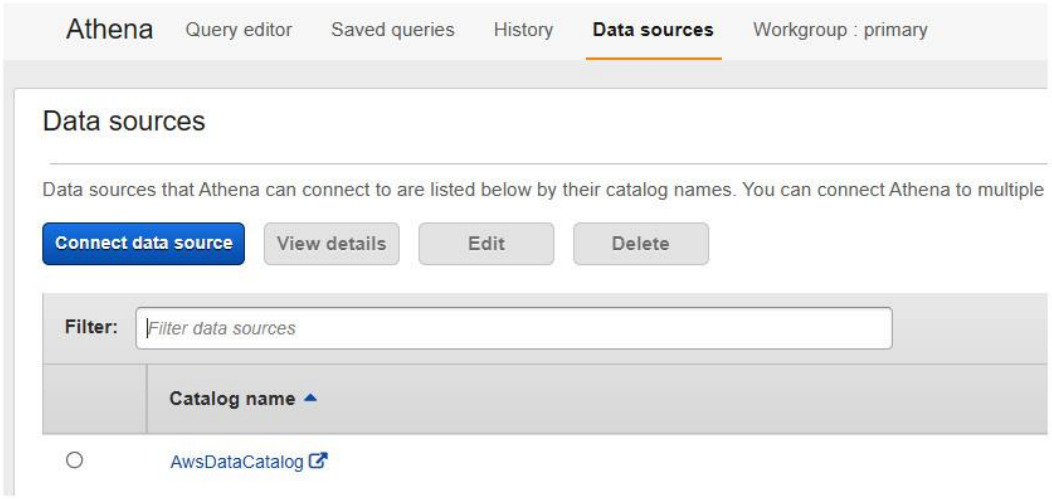

Figure 11.9 – Amazon Athena – Data sources

2. Next, click on the **Query editor** tab.

3. From the left-hand menu, select the database you created earlier in *Step 2*, which will also reveal the table that you created within the database, as per the following screenshot:

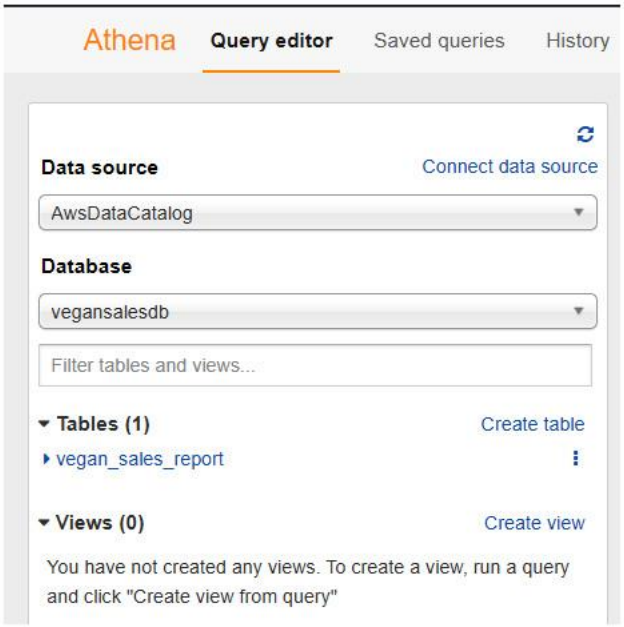

Figure 11.10 – Amazon Athena – Query editor

4. Now, you can easily preview the data held in Amazon S3 by clicking on the ellipsis (the three dots next to your table name) and then clicking on **Preview table** from the context menu that appears. This will run a SQL query and retrieve the sample data from your table, as per the following screenshot:

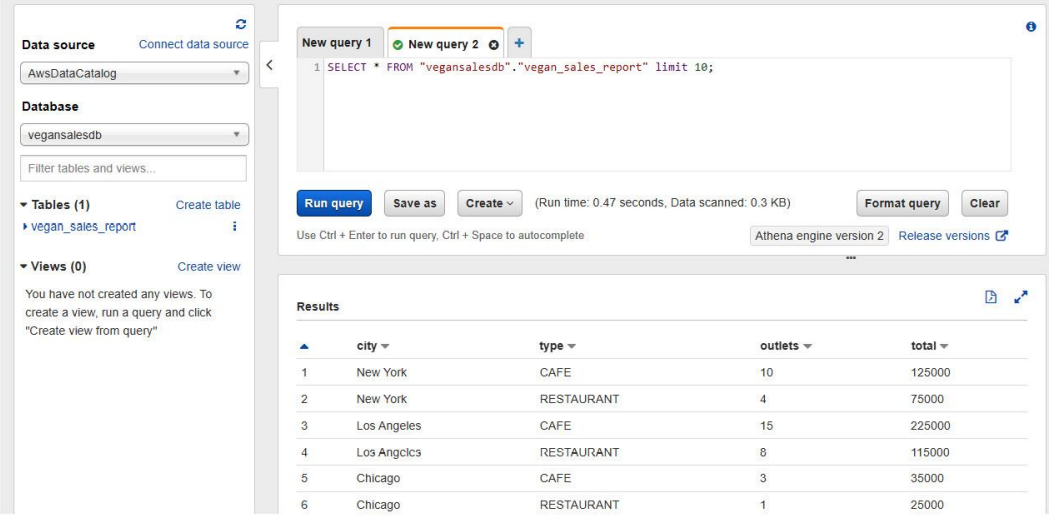

Figure 11.11 – Amazon Athena – Sample query

5. You can run additional queries. For example, you can replace the SQL statement in the top half of the pane with the following:

```
SELECT * FROM "vegansalesdb"."vegan_sales_report" WHERE total >=100000;
```

The preceding statement will showcase all the cities where the sales that were achieved were equal to or above $100,000, as per the following screenshot:

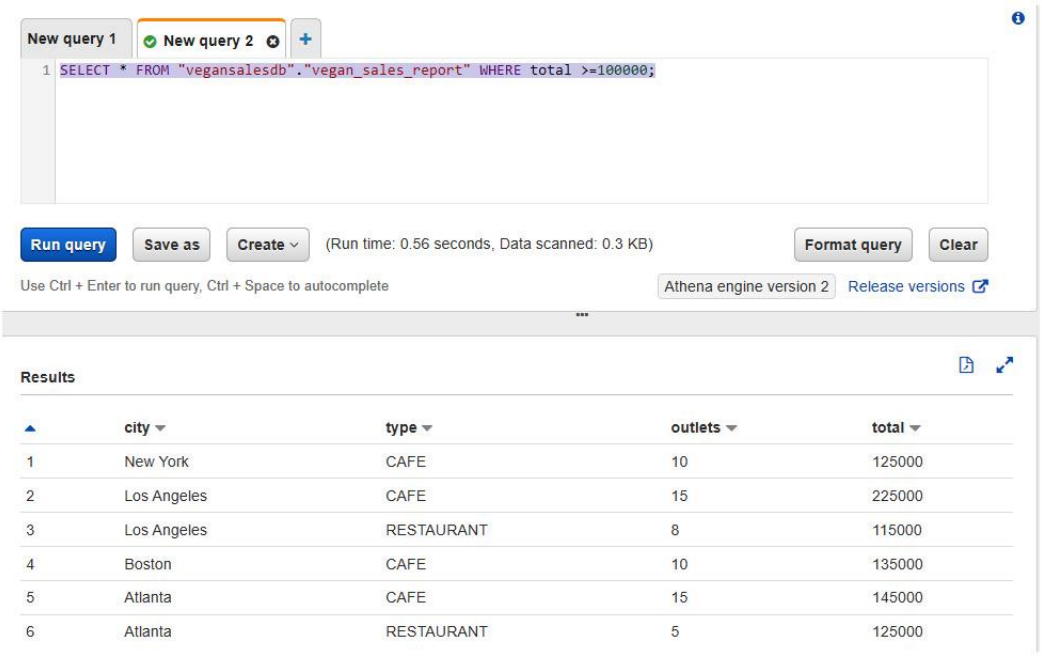

Figure 11.12 – Amazon Athena – Query to identify those cities where sales were greater than or equal to $100,000

As you can see, Amazon Athena is extremely powerful in being able to access and query your raw data in Amazon S3. You do not need to set up and deploy servers or run expensive databases for such ad hoc analysis of your data.

Now, we will perform a cleanup exercise to remove unwanted resources from our AWS account.

Exercise 11.2 – cleaning up

In this exercise, you will delete the resources you created in the previous exercise to ensure that there are no unwanted costs:

1. Navigate to the Amazon Glue console.
2. From the left-hand menu, click the **Crawlers** link. In the right-hand pane, select **vegan-sales-crawler**. From the **Actions** drop-down list, click the **Delete Crawler** option and then confirm the delete operation.
3. Next, from the left-hand menu, click **Databases**. In the right-hand pane, select the **vegansalesdb** database. Then, from the **Actions** drop-down list, click the **Delete database** option.
4. Click the **Delete** button in the **Delete Database** confirmation dialog box that appears.

Next, you will need to delete the Amazon S3 buckets as they are no longer required:

1. Navigate to the Amazon S3 console. From the left-hand menu, click on **Buckets**.
2. In the right-hand pane, select the **vegan-query-results** bucket and then click the **Empty** button. Confirm that you want to empty the bucket by typing `permanently delete` in the confirmation text box. Next, click the **Empty** button. You will get a confirmation message, stating that the bucket has been successfully emptied. Click the **Exit** button.
3. Next, with the **vegan-query-results** bucket still highlighted, click the **Delete** button.
4. Confirm the delete operation by typing the bucket's name in the confirmation text box and then clicking on the **Delete bucket** button.
5. Repeat *Steps 1* to *4* for the **vegan-sales-report** bucket.

Now that you have completed the cleanup exercise, we will summarize this chapter.

Questions

Answer the following questions to test your knowledge of this chapter:

1. Which AWS service can help you ingest and deliver massive amounts of streaming data into Amazon Redshift for near real-time analytics?

   A. Amazon Athena

   B. Amazon Kinesis Firehose

   C. Amazon Kinesis Video Streams

D. Amazon RDS

2. Which AWS service can help you query streaming data using standard SQL queries in real time?

   A. Amazon Kinesis Data Streams

   B. Amazon Kinesis Data Analytics

   C. Amazon Glue

   D. Amazon QuickSight

3. You are planning on building an application that will capture video streams from speed cameras on country roads for analysis. You need to be able to capture all the vehicles that break the speed limit and identify the offending drivers via the vehicles' license plates. Which two services on AWS can help you achieve these requirements? (Choose 2 answers.)

   A. Amazon Athena

   B. Amazon Kinesis Data Analytics

   C. Amazon Kinesis Video Streams

   D. Amazon Elasticsearch

   E. Amazon Rekognition

4. Which AWS service enables you to index all types of content, offers integration with **Kibana**, and helps you build data visualization tools to analyze large datasets?

   A. Amazon Elasticsearch

   B. Amazon Glue

   C. Amazon Athena

   D. Amazon Kinesis Firehose

5. You store several network log files (in CSV format) in an Amazon S3 bucket. You have been asked to analyze the contents of a specific file for possible malicious attacks. Which AWS service can help you analyze raw data in Amazon S3 and perform the necessary ad hoc analysis?

   A. Amazon Glue

   B. Amazon QuickSight

   C. Amazon Athena

   D. Amazon Data Pipeline

6. Which AWS service can be used to perform serverless ETL functions to discover, prepare, enrich, clean, and transform your data from various sources for analysis?

   A. AWS Glue

   B. AWS Athena

   C. AWS QuickSight

   D. AWS Rekognition

7. Which AWS service enables you to create and publish interactive BI dashboards for your business data to provide access to meaningful information for your business to make decisions?

   A. AWS Kinesis Data Analytics

   B. AWS Glue

   C. AWS QuickSight

   D. AWS Kinesis Firehose

Chapter 12

Figures

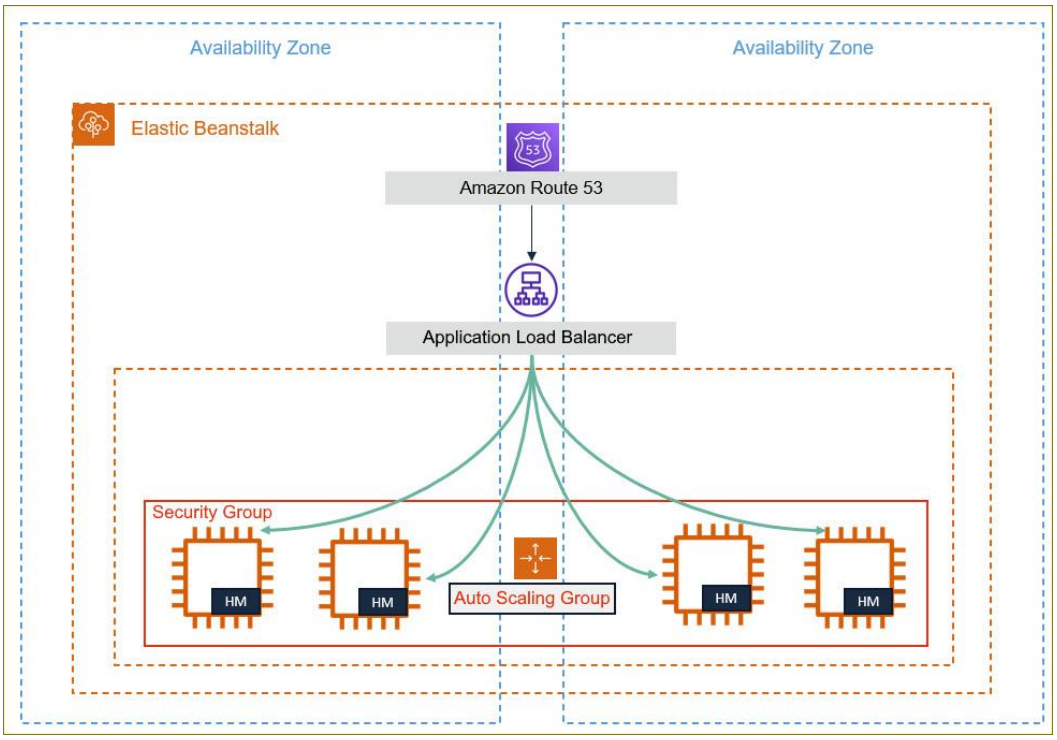

Figure 12.1 – AWS Elastic Beanstalk – web server environment tier

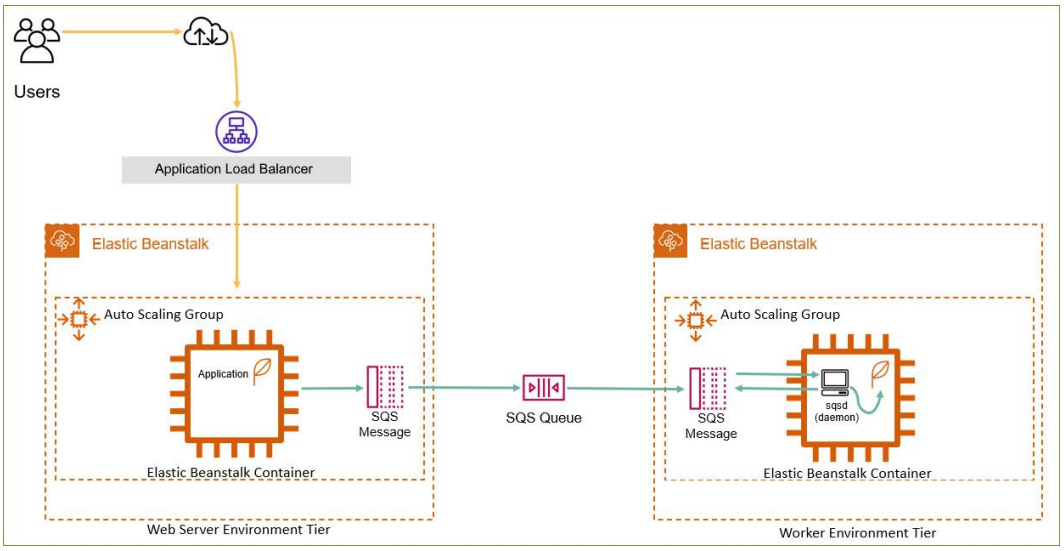

Figure 12.2 – AWS Elastic Beanstalk – worker environment tier

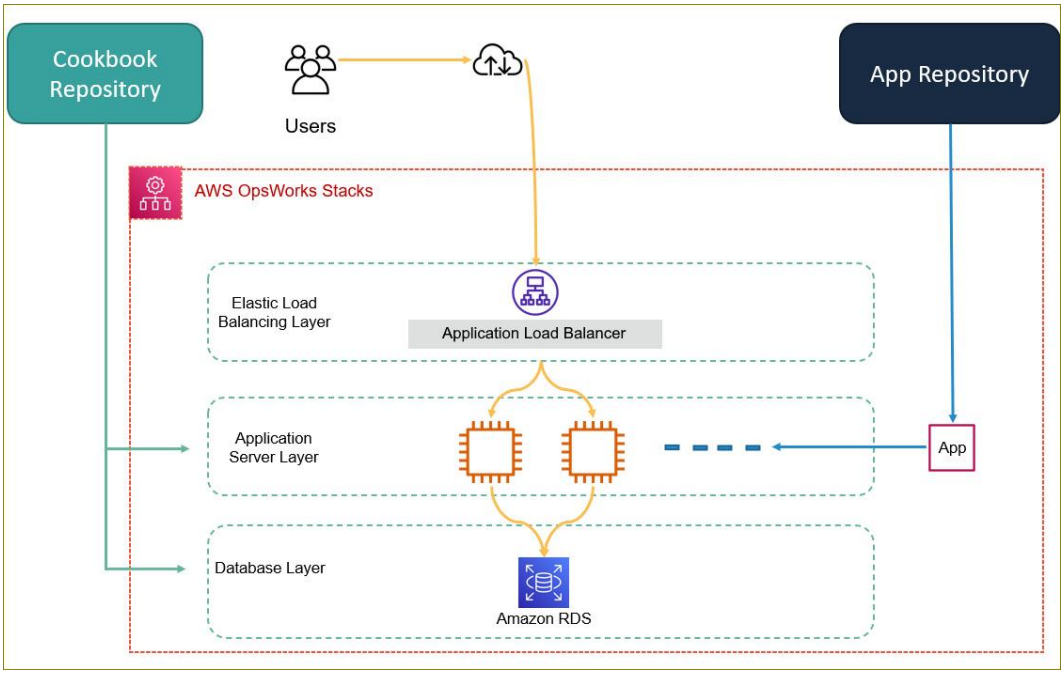

Figure 12.3 – AWS OpsWorks stacks

Exercise 12.1 – stopping and starting EC2 instances at regular intervals using AWS Lambda

Imagine a scenario where you need to run a fleet of on-demand EC2 test servers that your **user acceptance testing** (**UAT**) team needs to perform multiple functional and technical tests on for an upcoming application that you are developing. Your UAT team only works from Monday to Friday, 9 A.M. to 5 P.M. The UAT team only needs access to the fleet of test servers during this time. Rather than have a technician manually start up all the servers in the morning and shut them down again at the end of the business day, you could automate the process using AWS Lambda. You would not want to have your on-demand EC2 instances running when they are not needed because you are charged for every hour that those servers are running.

In this exercise, we will look at how to configure AWS Lambda to automatically stop and then start your EC2 instances at defined schedules.

To complete the exercises in this chapter, you will need to download the sample IAM policy from this book's Packt GitHub repository at: https://github.com/PacktPublishing/AWS-Certified-Cloud-Practitioner-Exam-Guide

Step 1 - Launching an EC2 instance

To complete this excercise, you will need to deploy an EC2 Instance running the Linux 2 AMI:

1. Log into the AWS Management Console as the IAM user called **Alice**.
2. Navigate to the EC2 dashboard. Ensure that you are in the **us-east-1 (N. Virginia)** Region.
3. Click on **Instances** from the left-hand menu and then click on the **Launch instances** button.

4. For **Step 1: Choose an Amazon Machine Image (AMI)**, select the **Amazon Linux 2** AMI.
5. For **Step 2: Choose an Instance Type**, select the **t2.micro** instance type and click the **Next: Configure Instance Details** button.
6. For **Step 3: Configure Instance Details**, provide the following key details:
    - For **Network**, select the default VPC.
    - For **Subnet**, select the subnet ID that represents the default subnet in **us-east-1a**.
    - In the text box next to **Auto-assign Public IP**, ensure that **Enable** is selected.
    - Leave all the remaining options as their default values and click the **Next: Add Storage** button at the bottom of the page.
7. For **Step 4: Add Storage**, leave all the options as their default values and click the **Next: Add Tags** button at the bottom of the page.
8. For **Step 5: Add Tags**, click the **Add Tag** button and provide a key-value name for your EC2 instance. For example, for **Key**, type in `Name`, and for **Value**, type in `UAT-Server-01`.
9. Next, click on the **Next: Configure Security Group** button at the bottom of the page.
10. For **Step 6: Configure Security Group**, ensure that the **Create a new security group** option is selected and set **Security group name** to **UAT-SG**. This will represent the security group of our UAT test server(s).
11. Next, you need to configure the inbound rules. You should already have a pre-configured inbound rule defined that allows SSH traffic inbound from the internet, as per the following screenshot:

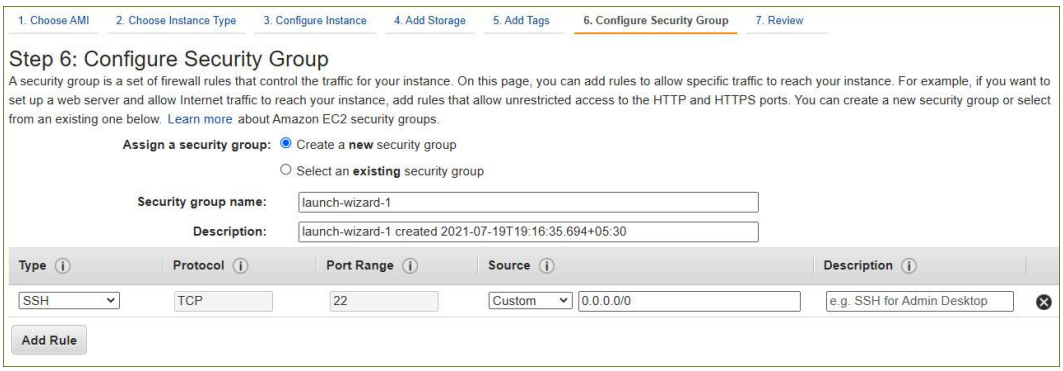

Figure 12.4 – Configure Security Group

12. Click the **Review and Launch** button at the bottom of the page.
13. On the next page, review your configuration and then click the **Launch** button at the bottom of the page.
14. You will be prompted to choose an existing key pair or create a new one. You can use the existing key pair you created for the previous exercise. You will need to click on the checkbox

to acknowledge that you have access to this key pair and then click on the **Launch instances** button.

15. Finally, click on the **View Instances** button to be taken back to the EC2 dashboard, where you can see the instance you just launched.

Because we will be stopping and starting these EC2 instances using a Lambda function, you will need to make a note of the EC2 instance ID, as per the following screenshot. Note that your EC2 instance ID will be different from the one shown in this screenshot:

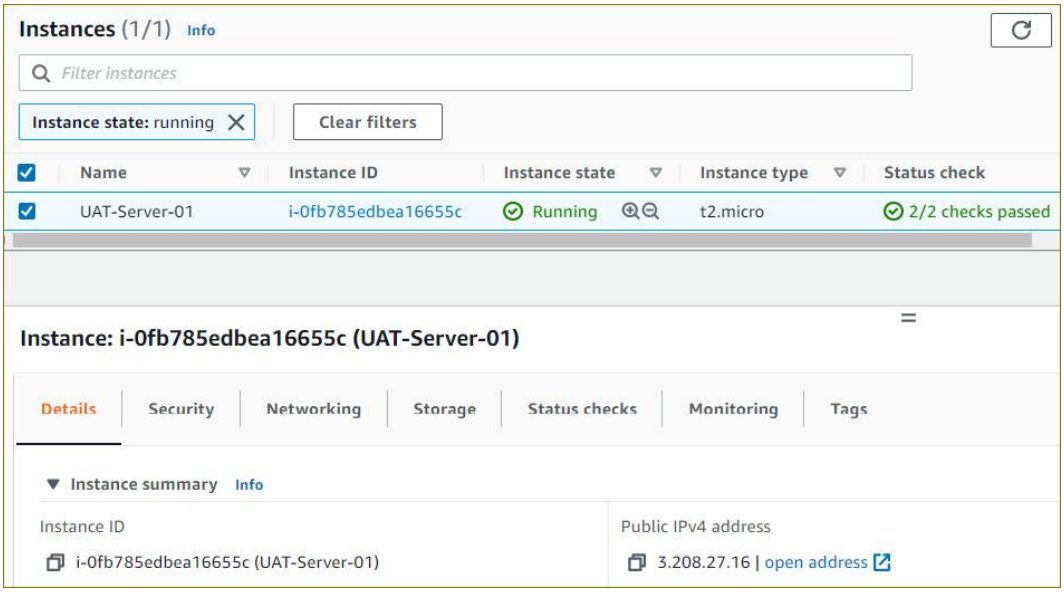

Figure 12.5 – EC2 instance ID

Once your instance is up and running, we can start creating the necessary IAM policy and IAM role to enable our Lambda functions to start and stop our EC2 instance.

Step 2 - Creating an IAM policy and execution role for your Lambda function

For your Lambda function to be able to start and stop your EC2 instances, it needs to have the necessary permissions. In this step, you will configure an IAM policy and an IAM role to enable your Lambda function to perform the start and stop operations on your EC2 instances:

1. Navigate to the IAM dashboard.
2. From the left-hand menu, click on **Policies**.
3. Click the **Create Policy** button from the right-hand pane.
4. Select the **JSON** tab and delete the default JSON text in the editor tool.
5. Next, copy and paste the following JSON policy document into the policy editor (you can also download this policy from the Packt GitHub repository for this book https://github.com/PacktPublishing/AWS-Certified-Cloud-Practitioner-Exam-Guide):

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Start*",
        "ec2:Stop*"
      ],
      "Resource": "*"
    }
  ]
}
```

6. Click the **Next: Tags** button at the bottom of the page.
7. On the **Add tags (Optional)** page, click the **Add tag** button to provide a tag name for your policy. For example, for **Key**, type in `Name`, and for **Value**, type in `Lambda-EC2-Access-Policy`.
8. Click **Next: Review**.
9. On the **Review Policy** page, type in a name for your policy; for example,`Lambda-EC2-Access-Policy`.
10. Click the **Create policy** button at the bottom of the page. You will receive a notification that your policy has been created.
11. Next, you will need to create an IAM role for Lambda. From the left-hand menu, click on **Roles**.
12. Click **Create role** from the right-hand pane.

13. On the **Create role** page, ensure that the **AWS service** option is selected under **Select type of trusted entity**.
14. Next, under **Choose a use case**, select **Lambda**.
15. Click the **Next: Permissions** button at the bottom of the page.
16. On the **Attach permissions policies** page, search for the policy you just created in the search box next to **Filter policies**. In the search box, start by typing in `Lambda-EC2`, which should filter the list down to the policy you just created. Select this policy and click on the **Next: Tags** button at the bottom of the page.
17. On the **Add tags (Optional)** page, click the **Add tag** button and provide a tag name for your policy. For example, for **Key**, type in `Name`, and for **Value**, type in `Lambda-EC2-Start-Stop-IAM-Role`.
18. Click the **Next: Review** button and set **Role name** to `Lambda-EC2-Start-Stop-IAM-Role`.
19. Click the **Create role** button at the bottom of the page.
20. You will get a notification, stating that the IAM role has been created.

Now that your role has been created, you can create Lambda functions to stop and start your EC2 instances.

Step 3 - Creating Lambda functions that stop and start your EC2 instances

Now, let's create a Lambda function to stop and start your EC2 instance at a predefined schedule:

1. From the **Services** drop-down list at the top of the AWS Management Console page, select **Lambda**, which is located under the **Compute** category.
2. From the left-hand menu, click on **Functions**.
3. Click the **Create function** button in the right-hand pane.
4. Select the **Author from scratch** option.
5. Under **Basic information**, provide the following details:
    - For **Function name**, provide a name that represents the purpose of the function. For example, if you are creating the Stop EC2 instance function first, in the name field, type in `StopEC2Instances`.
    - For **Runtime**, select **Python 3.8**
    - Next, under **Permissions**, expand **Change default execution role**.
    - Under **Execution role**, select **Use an existing role**. Next, from the **Existing role** drop-down list, select the IAM role you created earlier.

6. Click the **Create function** button.
7. You will be redirected to the **StopEC2Instances** function page.
8. Next, in the **Code source** section, in the **Code** tab, you will be able to add your function code. From the left-hand **Environment** menu, expand the `StopEC2Instance` folder and double-click on the `lambda_function.py` file. In the right-hand pane, you will notice some sample code.
9. Delete the sample code and replace it with the following code:

```
import boto3
region = 'us-west-1'
instances = ['i-12345cb6de4f78g9h', 'i-08ce9b2d7eccf6d26']
ec2 = boto3.client('ec2', region_name=region)
def lambda_handler(event, context):
    ec2.stop_instances(InstanceIds=instances)
    print('stopped your instances: ' + str(instances))
```

Important Note

You will need to amend the code as follows.

For the Region, replace the `us-west-1` Region with the Region your EC2 instance is in. In our example, the Region would be `us-east-1`.

10. Next, you will notice that the sample code refers to two EC2 instances. Replace this with the instance ID of the server you deployed in *Step 1 - Launching an EC2 instance* of this exercise, ensuring that the instance ID is placed within single quotes.
11. Next, click on the **Configuration** tab.
12. Click the **Edit** button from the **General configuration** pane.
13. Next, set the timeout value to 10 seconds.
14. Click the **Save** button. This will take you back to the **Function** page. Click the **Code** tab.
15. Recheck your Lambda code and ensure that you have made all the preceding changes. Next, click on the **Deploy** button.
16. If necessary, click on the ellipsis icon in the far left-hand pane to bring up the main menu and click on the **Function** link.
17. You should now see a list of your functions, which will include the `StopEC2Instances` function you just created.

18. Repeat *Steps 1* to *15* to create another function. This time, you will be creating a function to start your EC2 instances. For *Step 5*, enter a different function name than the one you used before; for example, **StartEC2Instances**.

19. For *Step 9*, copy and paste the following code into the editor pane, remembering to delete the sample code that is already there:

```
import boto3
region = 'us-west-1'
instances = ['i-12345cb6de4f78g9h', 'i-08ce9b2d7eccf6d26']
ec2 = boto3.client('ec2', region_name=region)
def lambda_handler(event, context):
    ec2.start_instances(InstanceIds=instances)
    print('started your instances: ' + str(instances))
```

20. Remember to also change the Region to `us-east-1` and amend the instance ID to the ID of your EC2 instance.

21. Once you have deployed your function, go back to the list of functions by clicking on the link from the left-hand menu (if necessary, by first clicking on the ellipsis icon).

You should now have two functions that will be used to stop and start your EC2 instances, as per the following screenshot:

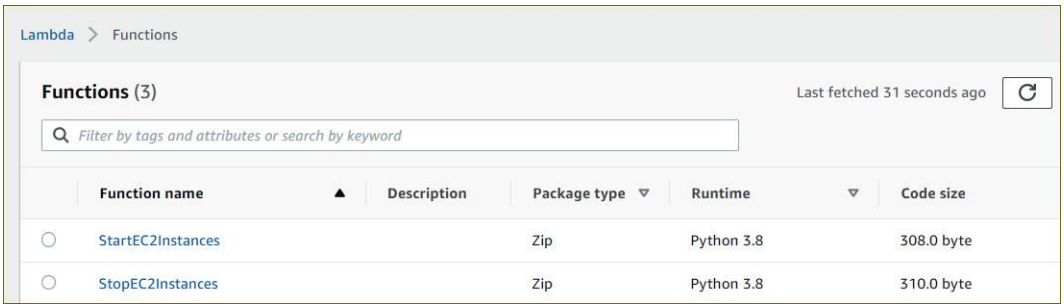

Figure 12.6 – Functions

Next, you will create CloudWatch event rules to help you execute the Lambda functions at scheduled times. We discussed CloudWatch events briefly in *Chapter 13, Management and Governance on AWS*. We will look at CloudWatch in more detail in the next chapter.

Step 4 - Creating CloudWatch event rules to trigger your Lambda functions

In this step, you will learn how to create CloudWatch event rules to trigger your Lambda functions at a given schedule:

1. Navigate to the CloudWatch dashboard. You can either search for CloudWatch from the top search bar of the AWS Management Console page or click the **CloudWatch** link from the **Management & Governance** category in the list of services.

2. From the left-hand menu, click on **Rules**, under **Events**.
3. Click the **Create rule** button.
4. For **Step 1: Create rule**, select **Schedule** under **Event Pattern**.
5. Next, select **Cron expression**. A CRON expression is a string comprised of six fields separated by white spaces that represent a set of times. These can be used as a schedule to execute a particular task regularly.
6. In the text field next to **Cron expression**, you will need to type in an expression that tells Lambda when to stop your instances. To learn more about how to define your expressions, visit https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/ScheduledEvents.html.
7. For this exercise, we wish to stop our EC2 instances at 6 P.M. Our UAT testers normally leave work at 5 P.M., but just in case anyone decides to work a bit late, we can execute the Lambda Stop function at 6 P.M.
8. The cron expression that you can use to execute the Lambda Stop function is **0 18 ? * MON-FRI ***. This will also display the next 10 triggers and their time of execution, as per the following screenshot:

Figure 12.7 – AWS CloudWatch event rule cron expression

9. Next, click on the **Add target** button under **Targets**.
10. From the drop-down list that appears, select **Lambda function**.

11. In the drop-down list next to **Function**, select the **StopEC2Instances** function. As you may recall, this is a Lambda function that will stop your EC2 instance.
12. Next, click on the **Configuration details** button.
13. For **Step 2: Configure rule details**, type an appropriate name in the **Name** field under **Rule definition**. For example, you can type in `StopUATInstances`.
14. In the **Description** field, type `Stops UAT instances at 6 PM Monday to Friday`.
15. Next, click the **Create rule** button.
16. Repeat *Steps 3* to *15* to start your EC2 instances. For this rule, ensure that, in *Step 6*, for **Cron expression**, you provide an expression that defines a start time of 8 A.M. Monday to Friday. Here, again, our UAT engineers will start work at 9 A.M. but some may come in a bit early. You can refer to https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/ScheduledEvents.html to help you build the cron expression. For this particular exercise, the cron expression that's required is **0 8 ? * MON-FRI ***. Furthermore, in *Step 11*, for **Function**, select the **StartEC2Instances** function. Also, in *Step 13*, enter `StartUATInstances` for the name and for the description, `Starts UAT instances at 8 AM Monday to Friday`.
17. At this point, you have ensured that your scheduled events automatically trigger the relevant Lambda functions, as per the following screenshot:

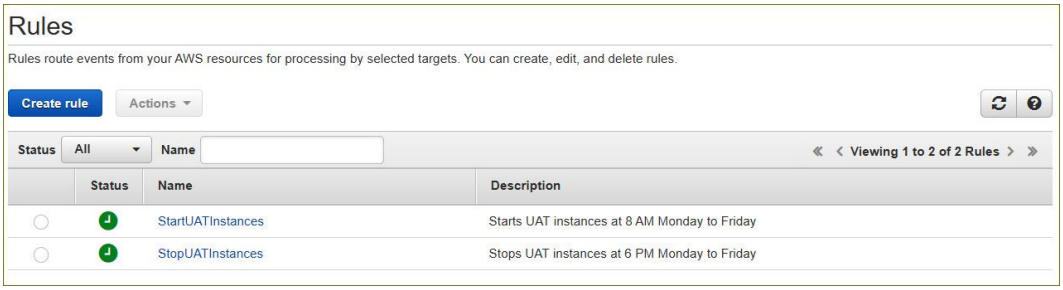

Figure 12.8 – CloudWatch event rules

You can wait for the designated times to check whether your EC2 instance has been stopped and then restarted. Alternatively, you can just test your Lambda function, which is what we will be doing next.

Step 5 - Testing your Lambda function

We can test our Lambda function rather than waiting for the scheduled times to see whether the functions work:

1. Navigate back to the Lambda dashboard.
2. From the left-hand menu, select **Functions**. Then, from the right-hand pane, select the **StopEC2Instances** function.

3. Next, from the **Actions** drop-down list, select **Test**.
4. For **StopEC2Instances**, click on the **Test** button in the **Test event** pane.
5. If the function has been configured correctly, you should see the **Execution result: succeeded** message and an option to expand the **Details** pane. This will provide details of the execution, as per the following screenshot:

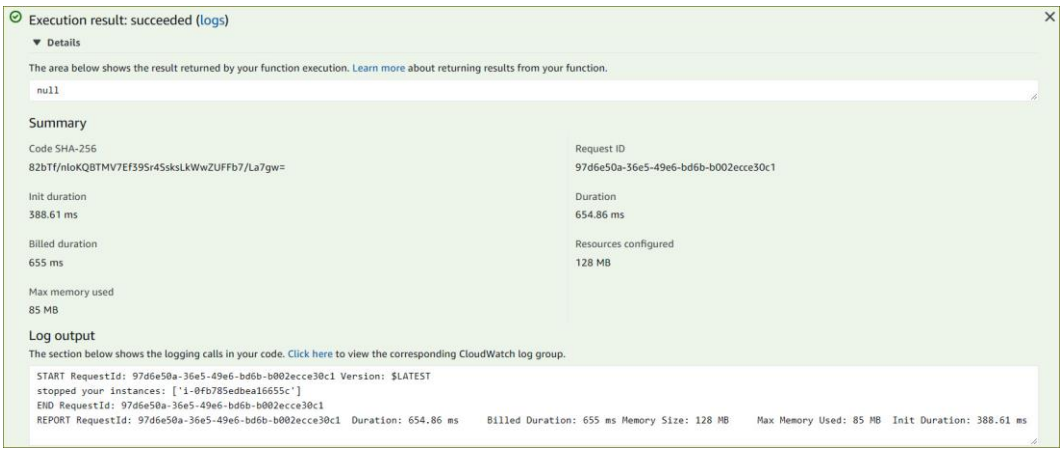

Figure 12.9 – The Lambda function's execution details

6. In another browser window, navigate to your EC2 dashboard. Here, you should find that your EC2 instance has been stopped.
7. Return to the AWS Lambda browser tab and click on **Functions** from the far left-hand menu.
8. Repeat *Steps 2* to 5, this time selecting the **StartEC2Instances** function.
9. Within a few seconds, you should find that the function was executed successfully, and you can cross-reference this with the EC2 dashboard. You should find that your EC2 instance has started again.

In this exercise, you learned how to create Lambda functions that can be used to perform repetitive IT tasks for your organization and help automate various processes. You also learned how to schedule those repetitive tasks using AWS CloudWatch event rules and cron expressions.

Exercise 12.2 – cleaning up

In this exercise, you will terminate your EC2 instance and delete your Lambda functions to avoid any unnecessary charges to your AWS account:

1. Navigate to the EC2 dashboard and ensure that you are in the **us-east-1** (North Virginia) Region.
2. Click on **Instances** from the left-hand menu.

3. In the right-hand pane, under **Instances**, select the EC2 instance you launched earlier. Then, from the **Instance state** drop-down menu, click **Terminate instance**. Confirm that you wish to terminate the instance; AWS will terminate it.
4. Next, navigate to the Lambda dashboard.
5. Click on **Functions** from the left-hand menu. In the right-hand pane, for each function, select the function. Then, from the **Actions** drop-down list, click **Delete**. Click the **Delete** button in the pop-up dialog box to delete the function.
6. Next, navigate to the CloudWatch management console.
7. From the left-hand menu, click on **Rules**, under **Events**.
8. For each rule, select the rule. Then, from the **Actions** drop-down list, click **Delete**. Click the **Delete** button in the pop-up dialog box to delete the rule.

Your resources have now been removed from your AWS accounts. In the next section, we will provide a summary of this chapter.

Questions

Answer the following questions to test your knowledge of this chapter:

1. Which AWS service automatically provisions the necessary infrastructure (for example, load balancing, auto-scaling, and health monitoring) and enables developers to automatically deploy an application's built-in supported languages such as Node.js, PHP, and Python?
    A. AWS CloudFormation
    B. AWS Lambda
    C. AWS Elastic Beanstalk
    D. AWS Deployer
2. You work for a web application development company and have been asked to design an infrastructure solution that can be repeatedly created using scripted templates. This will allow you to create individual sandbox environments for your developers to use. Some infrastructure components will include the setup and configuration of a VPC, EC2 instances, S3 buckets, and more. Which AWS service enables you to design an infrastructure template that can be deployed to create repeatable infrastructure for your developers to use as a sandbox environment?
    A. AWS Systems Manager
    B. AWS CloudFormation
    C. AWS Config

D. AWS FSx for Lustre

3. Which two file formats are used when creating CloudFormation templates? (Choose 2.)

   A. JSON

   B. YAML

   C. XML

   D. HTML

   E. Java

4. Which AWS service provides integration with Chef recipes to start new application instances, configure application server software, and deploy the application?

   A. Amazon CloudFormation

   B. Amazon Elastic Beanstalk

   C. Amazon OpsWorks

   D. Amazon Cookbook.

5. Which type of environment do you need to configure for an Elastic Beanstalk deployment to host backend application layer services?

   A. Web server environment tier

   B. Worker environment tier

   C. Backend environment tier

   D. Hybrid environment

6. Which feature of the Amazon CloudFormation service enables you to review any proposed changes you wish to make to an environment and identify how those changes will impact your environment?

   A. Drift detection

   B. Change sets

   C. Stack sets

   D. Change management

Chapter 13

Figures

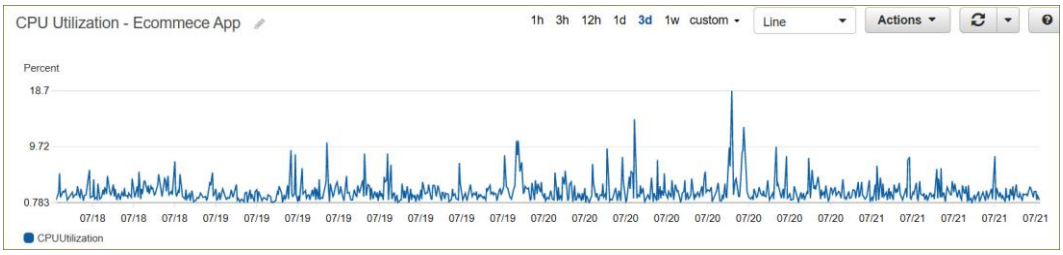

Figure 13.1 – CPU utilization metrics for an EC2 instance running an e-commerce application

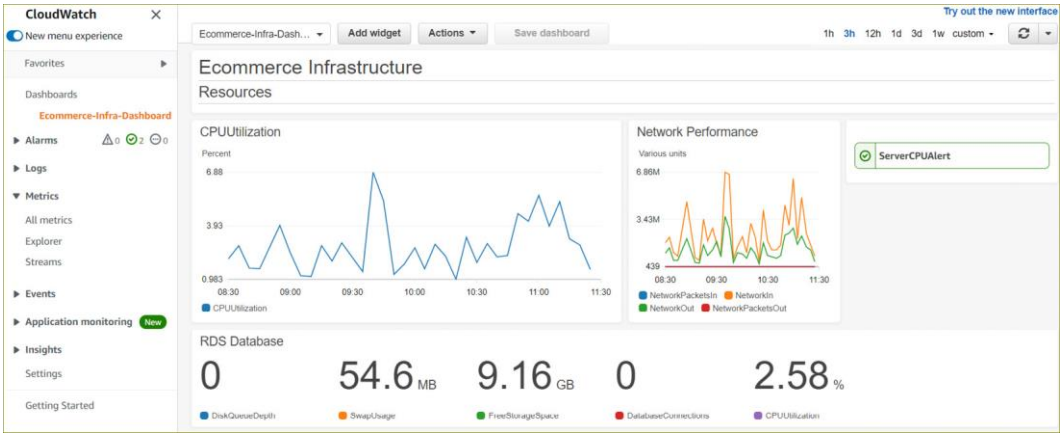

Figure 13.2 – A CloudWatch dashboard

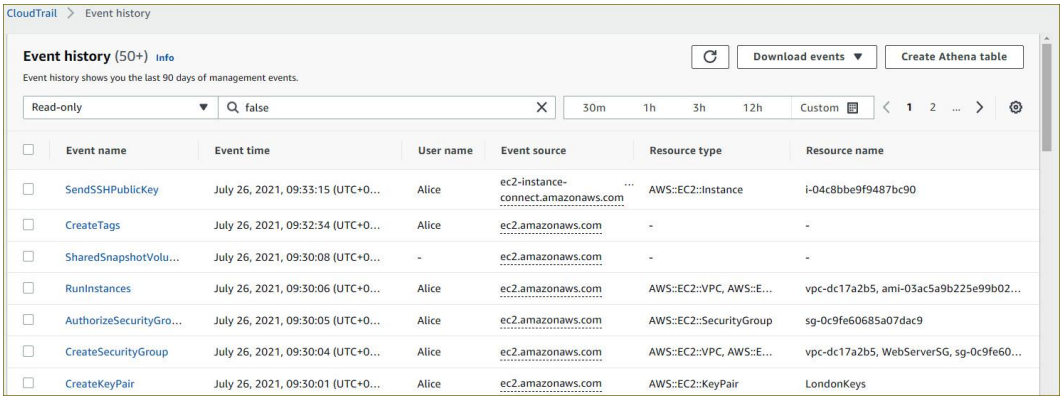

Figure 13.3 – AWS CloudTrail

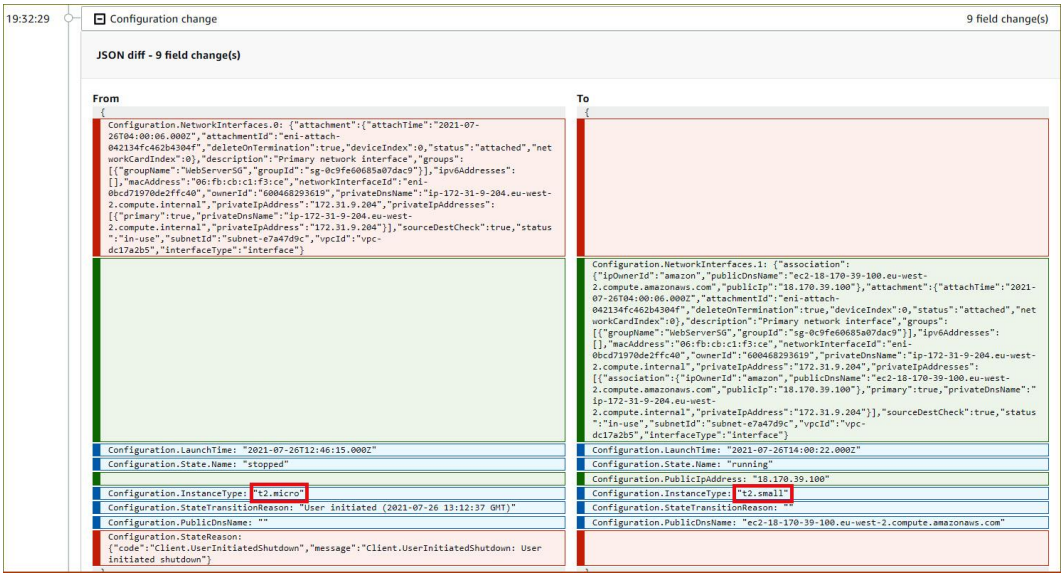

Figure 13.4 – AWS Config JSON showing a configuration change for an EC2 instance

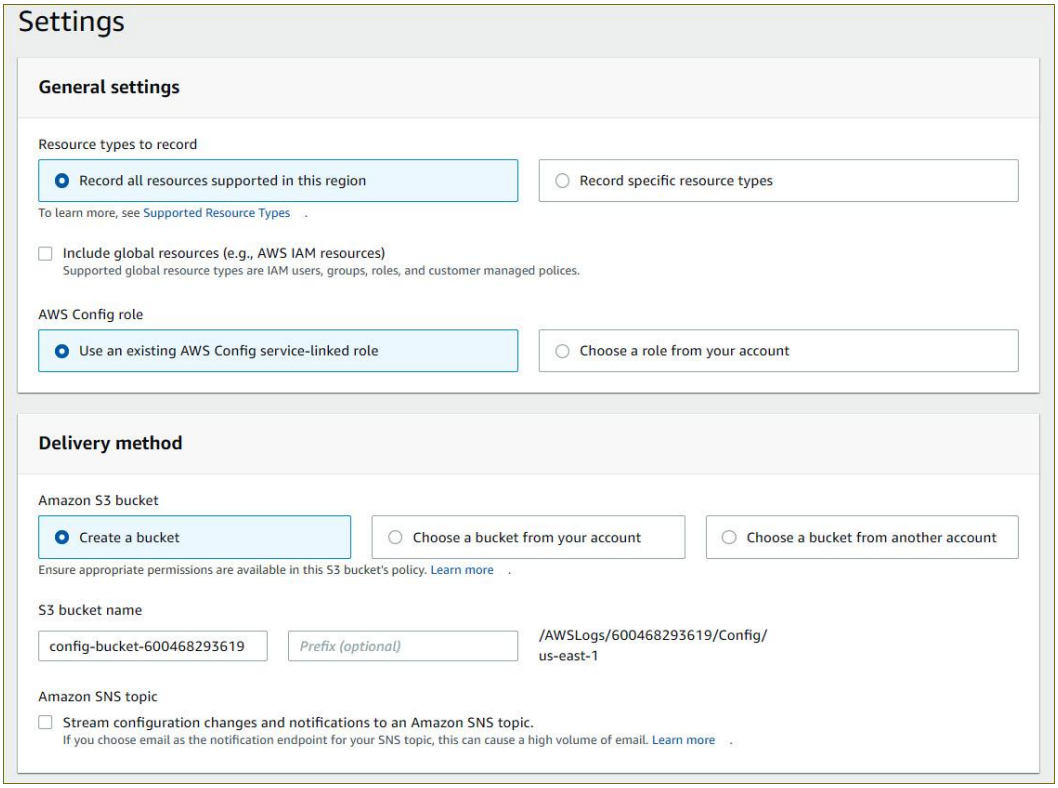

Figure 13.5 – AWS Config settings

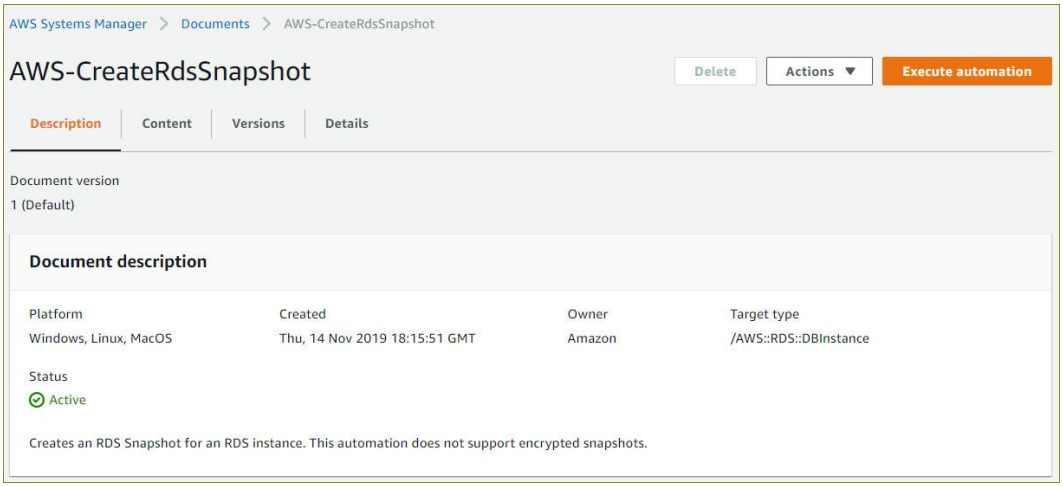

Figure 13.6 – AWS Systems Manager predefined documents

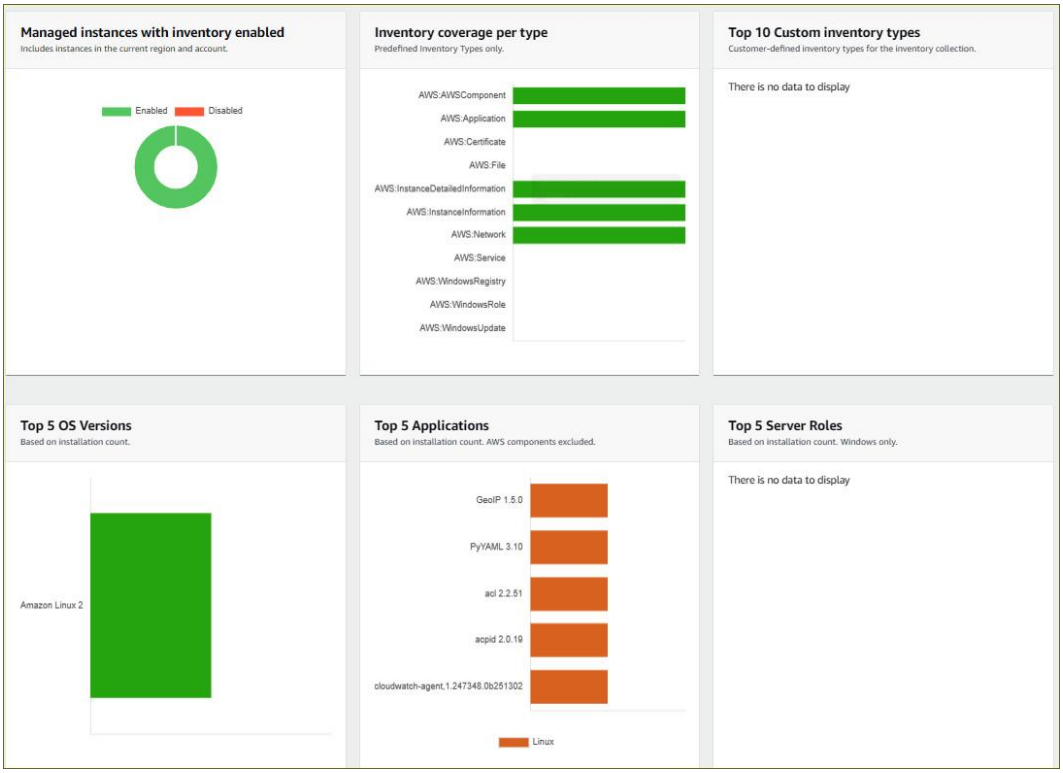

Figure 13.7 – AWS Systems Manager Inventory

Exercise 13.1 – Reviewing the Trusted Advisor reports in your AWS account

In this exercise, you will log into your AWS account and review the Trusted Advisor service:

1. Log in to your AWS Management Console as the IAM user **Alice**.

2. Navigate to the **Trusted Advisor** console, which is located under the **Management & Governance** category in your list of services.
3. You will be redirected to the Trusted Advisor dashboard.
4. Because you may only have subscribed to the Basic Support plan, you will note that only a few checks are visible. From the main dashboard, note the **Checks Summary** section on the main pane of the dashboard.
5. From the right-hand pane, click on the **Security** category.
6. In the right-hand pane, you will note various checks, such as the one for MFA being enabled on your root account.
7. Expand the check labeled **Security Groups - Specific Ports Unrestricted**. This check analyzes how your security groups have been configured, highlighting specific ports that should provide restricted access. For example, the number 22 port that enables **SSH** remote connections should not be opened to the internet. Ideally, you should restrict access to this port to a specific IP range, such as the IP block of your corporate on-premises network. In our previous exercises, we created inbound rules on this port from the entire internet and, therefore, AWS Trusted Advisor will highlight it as a potential security issue.

   In the following screenshot, you will note that we have three security groups that have been configured to allow inbound traffic on the number 22 port from the internet unrestricted:

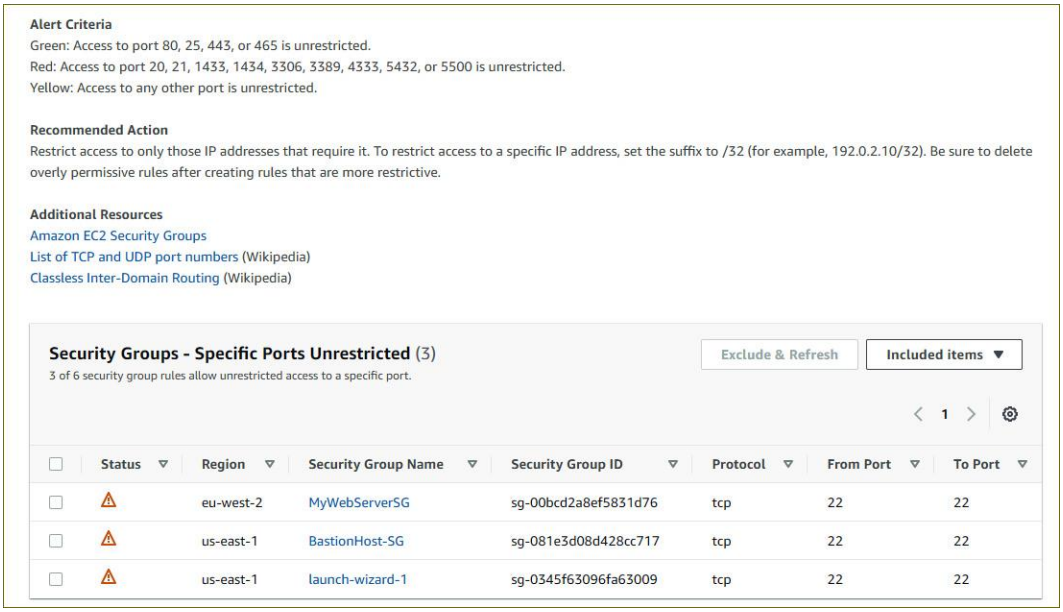

Figure 13.8 – AWS Trusted Advisor dashboard

From this exercise, you should've learned how to review the AWS Trusted Advisor dashboard. You were able to identify some security alerts based on your configuration of security groups from earlier exercises that did not adhere to best practices. You can then use this report to identify which security groups need to be amended to increase security.

Questions

1. Which AWS service enables you to track all API activity in your AWS account, regardless of whether the activity was performed using the AWS Management Console of the CLI?

   A. AWS CloudTrail

   B. AWS Config

   C. AWS Trusted Advisor

   D. Application load balancer logs

2. As part of implementing change management, which AWS service can be used to assess, audit, and evaluate change configurations of your AWS resources, enabling you to identify whether a change was the cause of an incident?

   A. AWS Config

   B. AWS CloudTrail

   C. Amazon CloudWatch

   D. AWS Outposts

3. Which AWS service can be used to monitor your company's fleet of EC2 instances, which can be used to identify performance issues related to CPU utilization or memory consumptions?

   A. Amazon CloudWatch

   B. AWS Cloud Monitor

   C. AWS EC2 Monitor

   D. AWS CloudTrail

4. Which AWS service helps you identify potential unused resources, such as Elastic IP addresses, that are not attached to a running instance and thus highlight opportunities to save on costs?

   A. AWS Cost Explorer

   B. AWS Trusted Advisor

   C. AWS Resource Manager

   D. AWS Budgets

5. Which capability of the AWS Systems Manager service enables you to remotely connect to your Linux EC2 instances without having to use bastion hosts in your VPC?

   A. Session Manager

B. Parameter Store

C. Run Command

D. Incident Manager

Chapter 14

Figures

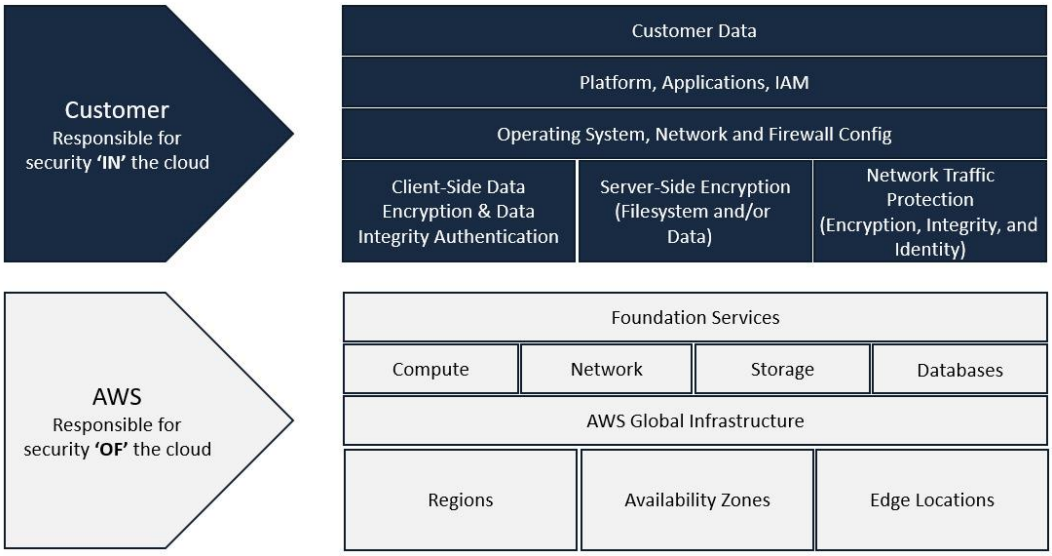

Figure 14.1 – AWS Shared Responsibility Model

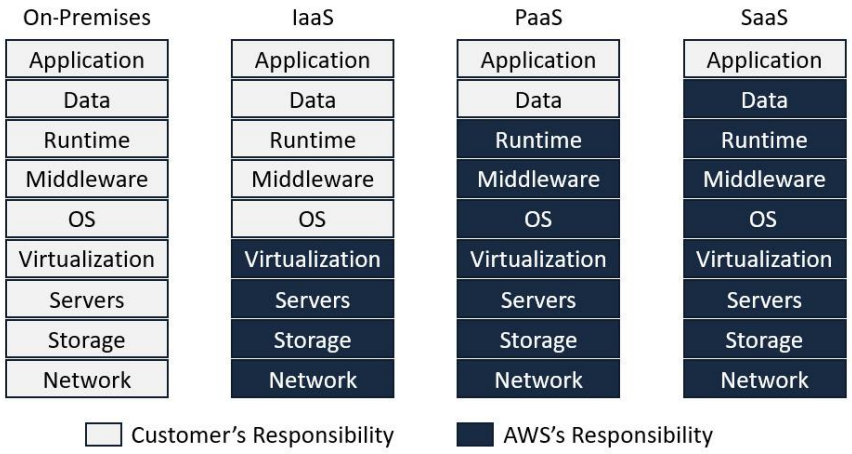

Figure 14.2 – The customer's responsibility varies, depending on the type of cloud computing model

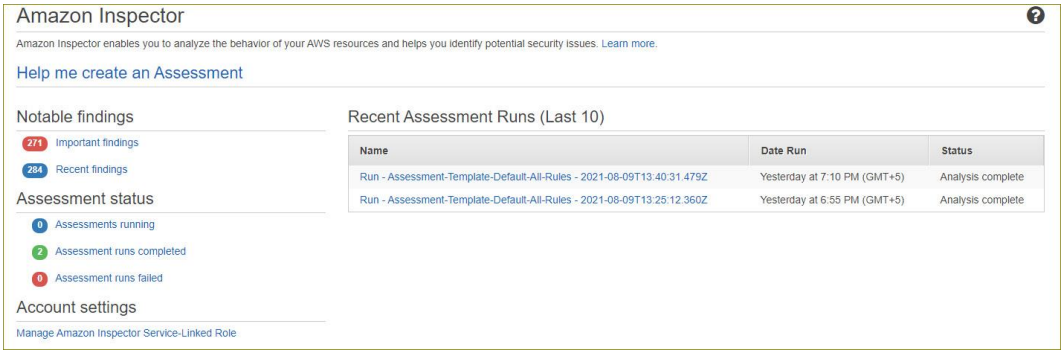

Figure 14.3 – AWS Inspector dashboard

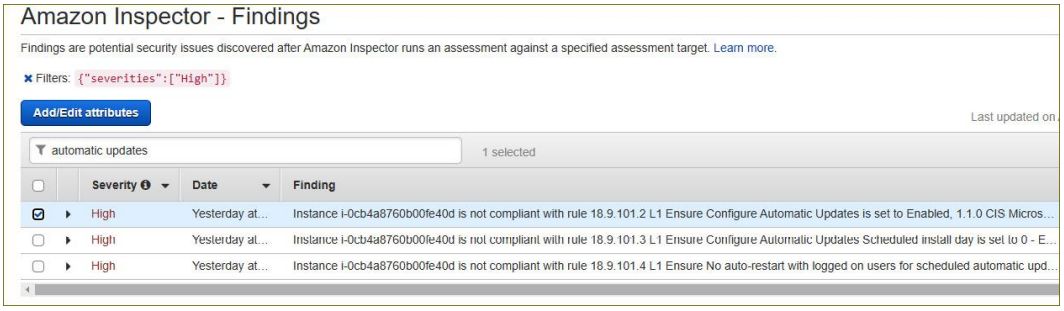

Figure 14.4 – AWS Inspector – Findings

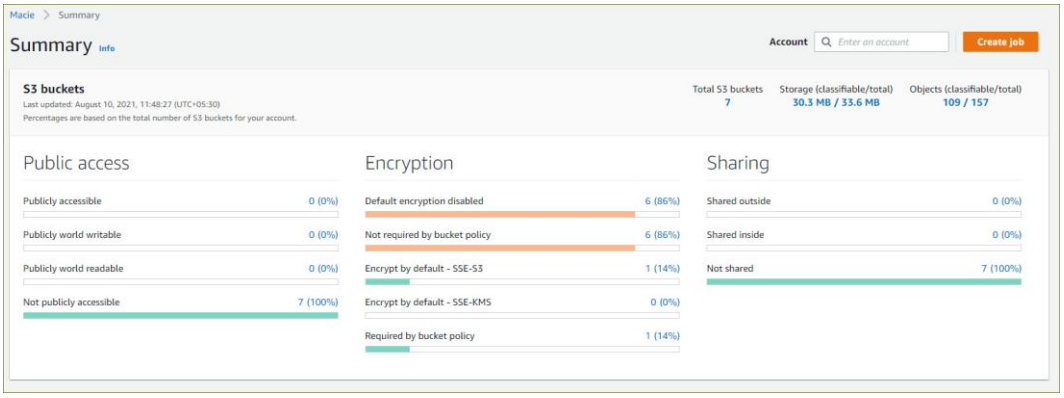

Figure 14.5 – Amazon Macie – Summary

Table

Permitted Services	Prohibited Activities
Amazon EC2 instances, NAT gateways, and elastic load balancers	DNS zone walking via Amazon Route 53 hosted zones
Amazon RDS	DoS, DDoS, simulated DoS, and simulated DDoS
Amazon CloudFront	Port flooding
Amazon Aurora	Protocol flooding
Amazon API Gateway	Request flooding
AWS Lambda and Lambda@Edge functions	
Amazon Lightsail resources	
Amazon Elastic Beanstalk environments	

Table 14.1 – AWS permitted services and prohibitive activities for penetration testing

Exercise 14.1 – preventing data leaks with Amazon Macie

In this exercise, you will use Amazon Macie to monitor a single Amazon S3 bucket and identify whether any PII was stored in the bucket. Imagine a scenario where a user in your organization has uploaded a sensitive file to the wrong Amazon S3 bucket. In our example, we have a *product details* bucket, which would contain product information that can be accessed by the marketing team.

However, because of poorly configured access policies, a member of the HR team has uploaded sensitive employee information into this bucket.

This could result in data leaks. While you want to ensure that users are restricted to which buckets they can access, sometimes, accidents do happen. Amazon Macie can detect content that's uploaded to S3 buckets and identify specific types of sensitive data. You can then take the appropriate action.

Step 1 – creating a new Amazon S3 bucket

1. Navigate to Amazon S3 and click on the **Buckets** link from the left-hand menu.
2. In the right-hand pane, click the **Create bucket** button.
3. Provide a bucket name and select the **us-east-1** Region to create your bucket in. I have named my bucket **justdessertsproducts**, so you will need to select a different name that is unique to your bucket. We are going to assume that someone has accidentally uploaded sensitive PII to this bucket.
4. Click the **Create bucket** button at the bottom of the page.
5. Next, create a simple CSV file using Excel or Google Sheets and upload it to the S3 bucket. Ensure that the CSV file contains some data that you can classify as PII. For example, in the following screenshot, you will note that I have added some dummy data that contains sensitive employee information. In this example, **EmployeeID** can be used to identify a specific employee and their salary information:

	A	B	C	D
1	EmployeeID	Name	Department	Salary
2	JD-8976	Richard	IT	$110,000.00
3	JD-9899	Mark	Sales	$120,000.00
4	JD-1212	Fernando	Sales	$120,000.00
5	JD-2343	Chekov	Catering	$90,000.00
6				

Figure 14.6 – Salary information of employees

When using Amazon Macie to identify information that may be PII-related, you would need to be able to identify the format of the data so that Amazon Macie knows what to look for. Note that the format of the `EmployeeID` data, as per the preceding screenshot, is *two characters* (*capital letters*), followed by a *hyphen* (-) and then *four numbers*.

Step 2 – configuring Amazon Macie to identify sensitive employee data

1. From the AWS Management Console, search for Amazon Macie in the top search bar and click on the service from the filtered search results.
2. If this is the first time you have navigated to the Amazon Macie console, you will see a splash screen, as shown in the following screenshot:

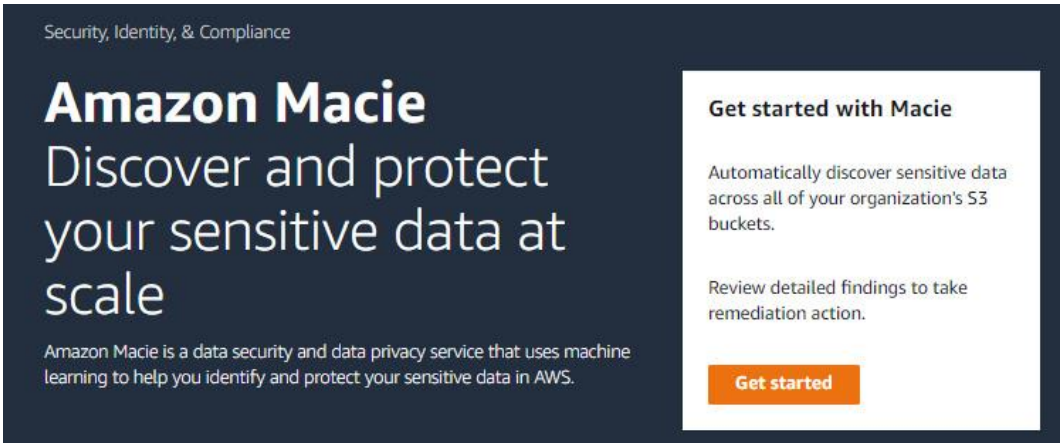

Figure 14.7 – Amazon Macie

3. Click the **Get started** button.

4. Amazon Macie requires permission to access information about the data that you store in Amazon S3. You will be provided with the option to enable Amazon Macie with the necessary access, which will create an IAM role.

5. Go ahead and click the **Enable Macie** button, as per the following screenshot:

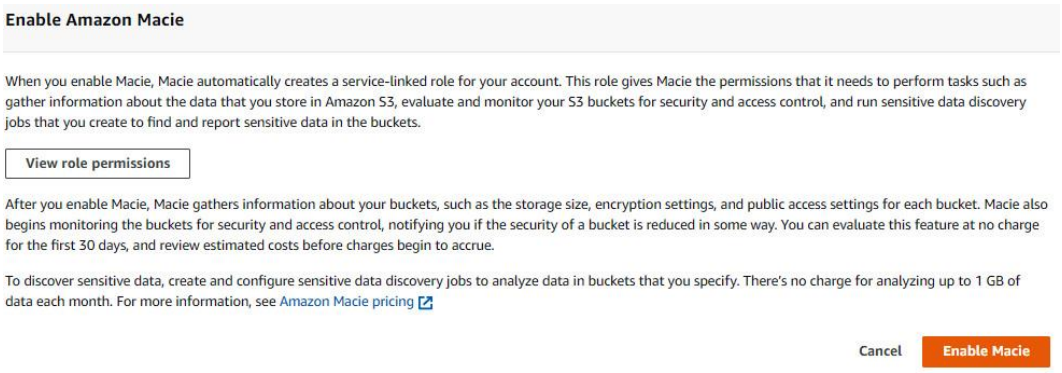

Figure 14.8 – Enable Macie

6. Once enabled, Amazon Macie will analyze your environment and, after a short time, provide a dashboard, as shown in the following screenshot:

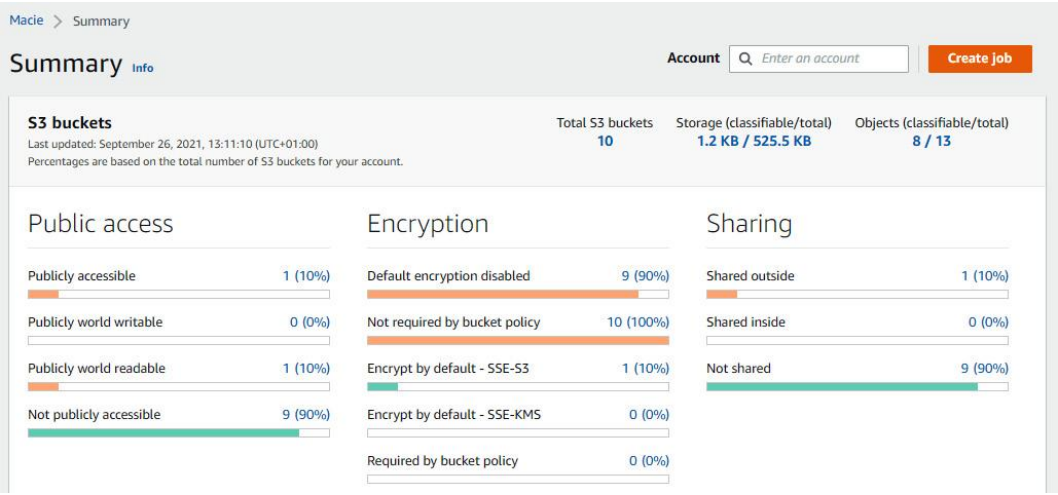

Figure 14.9 – Amazon Macie – Summary

7. While several items from the preceding summary need to be examined, for this exercise, we are primarily interested in ensuring that PII is not uploaded to the specific bucket we configured earlier. For this, we need to create an **Amazon Macie job**.
8. From the left-hand menu, select the **Jobs** link.
9. From the right-hand pane, click the **Create job** button. This will launch the job creation wizard, which you will need to complete as follows:
    I. For **Step 1**, select the bucket you created to upload the CSV file to. In my case, it is the **justdessertsproducts** bucket.
    II. Click **Next**.
    III. For **Step 2**, confirm that the correct bucket has been selected and click **Next**.
    IV. For **Step 3, Refine Scope**, select the **One-time job** option and then click **Next**. Normally, you would set a schedule to perform the discovery daily, but for this exercise, we are only going to perform the discovery once.
    V. Under **Additional settings**, select **File name extensions** under **Object criteria**.
    VI. In the text box below, type in `csv` and then click the **Include** button.
    VII. Click **Next**.
    VIII. For **Step 4, Select managed data identifiers**, select **None** and then click **Next**.
    IX. For **Step 5, Select custom data identifiers**, click on the **Manage custom identifiers** link to open the **Custom data identifiers** web page in another browser tab, as per the following screenshot:

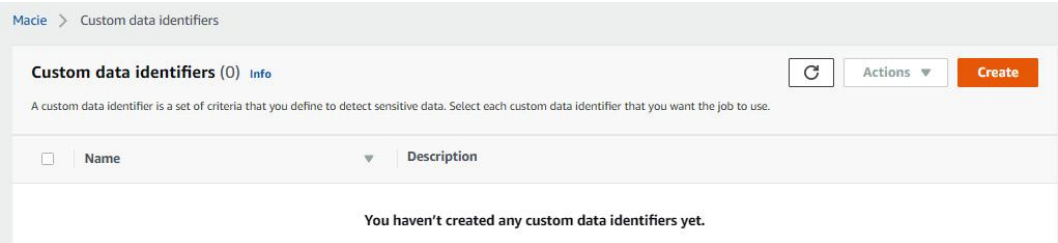

Figure 14.10 – Creating custom data identifiers

X. Click the **Create** button.

XI. Give the identifier a name and an optional description.

XII. Next, you will need to provide a **regex** pattern that matches your `EmployeeID` format. Regex is short for *regular expression*, which is a sequence of characters that specifies a search pattern. Often, you can use regex patterns to search for specific types of data or to validate data. For this exercise, your regex pattern will be *[A-Z]{2}-[0-9]{4}*. Input this pattern into the **Regular expression** text box.

XIII. Next, click the **Submit** button, which will create the custom data identifier for this exercise.

XIV. Navigate back to the **Job creation** wizard, which should still be visible in the previous browser tab. You should still be in **Step 5**. Click on the refresh icon to access the **EmployeeID** custom data identifier, as per the following screenshot:

Figure 14.11 – Select custom data identifiers

XV. Select the **EmployeeID** custom data identifier and click the **Next** button.

XVI. For **Step 6**, provide a name for the job and then click on the **Next** button.

XVII. For **Step 7**, review the configuration settings and then click the **Submit** button at the bottom of the page.

10. Your job has now been created and will be in the **Active (Running)** state, as per the following screenshot:

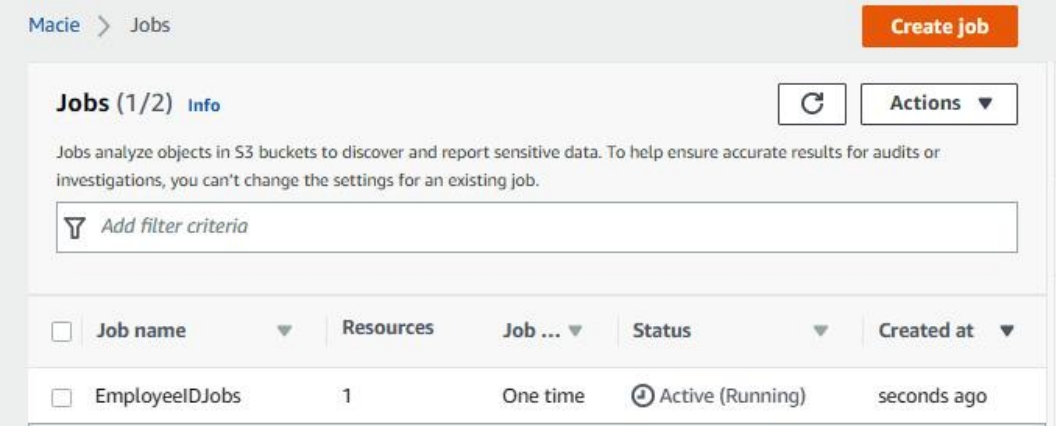

Figure 14.12 – Amazon Macie S3 job created

11. The job will take a few minutes to complete. Once the job completes, click on the **Show results** drop-down arrow and select **Show findings**. You will see that it has found the CSV file we uploaded earlier, as per the following screenshot:

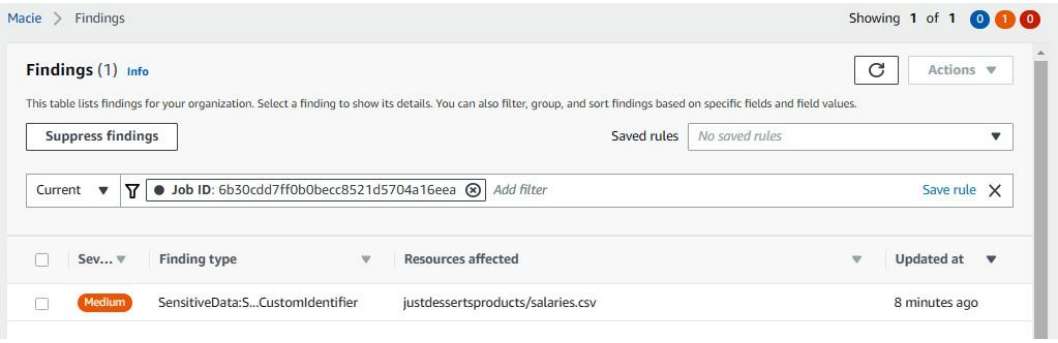

Figure 14.13 – Macie findings

12. Select the findings. Then, from the **Actions** drop-down list, select **Export (JSON)**.

13. You will be able to review the JSON file, which clearly shows that it identified four counts of PII data, as per the following screenshot:

Figure 14.14 – Amazon Macie job findings

14. The JSON will also highlight the columns and rows where the PII data was identified.

As you can see, Amazon Macie is an extremely powerful tool that can help you understand your data access patterns and alert you of potential data breaches.

In the next exercise, you will clean up the resources you created.

Exercise 14.2 – cleaning up

In this exercise, you will clean up the resources you created in this chapter:

1. Navigate to the Amazon Macie console.
2. From the left-hand menu, select **Settings**.
3. Next, from the right-hand pane, click on the **Disable Macie** button. Amazon Macie will permanently delete all your existing findings, classification jobs, and other Macie resources.
4. In the dialog box that appears, type **Disable** in the text box and click the **Disable** button.
5. Next, from the Amazon S3 console, you will need to empty the S3 bucket you created and then delete the bucket, as you did previously.

Next, we will provide a summary of this chapter.

Questions

Answer the following questions to test your knowledge of the topics covered in this chapter:

1. Which of the following is part of the customers' responsibility regarding the Shared Security Model? (Choose 2.)
   A. Patch Windows EC2 instances with the latest security patches.
   B. Configure NACL to only allow inbound ports `80` and `443` to Linux web servers from the internet.
   C. Update the network cabling in the `us-east-1` data centers.
   D. Upgrade the underlying infrastructure support for the Lambda service.
   E. Upgrade the biometric readers in the London Region.
2. Which service in AWS protects your virtual network and resources from common DDoS attacks?
   A. AWS WAF
   B. AWS Shield
   C. AWS Detective

D. Amazon Macie

3. Which of the following AWS Security tools can protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources?

   A. AWS WAF

   B. AWS GuardDuty

   C. AWS Shield

   D. AWS NACL

4. Which AWS service uses machine learning to classify sensitive information stored in your Amazon S3 buckets and monitor access patterns for anomalies that indicate risks or suspicious behavior, such as large quantities of source code being downloaded?

   A. Amazon Macie

   B. Amazon X-Ray

   C. AWS Shield

   D. AWS WAF

5. Which AWS service enables companies looking to migrate to the AWS cloud to obtain copies of various compliance documents such as ISO certifications, **PCI, and SOC** reports?

   A. AWS Artifact

   B. AWS Config

   C. AWS CloudWatch

   D. AWS security reports

6. To fulfill strict compliance requirements, you need to create and manage your encryption keys using FIPS 140-2 Level 3-validated HSM devices. Which type of encryption service would you recommend?

   A. AWS KMS

   B. AWS CloudHSM

   C. Certificate Manager

   D. BitLocker

Chapter 15

Figures

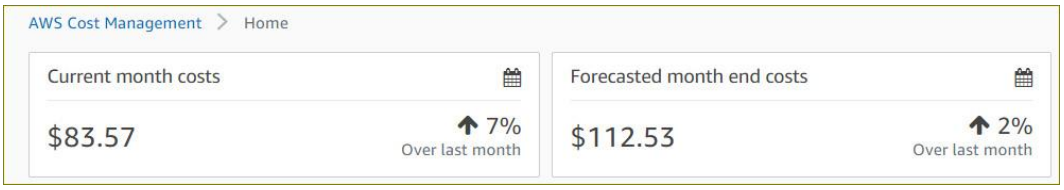

Figure 15.1 – Cost Explorer home page

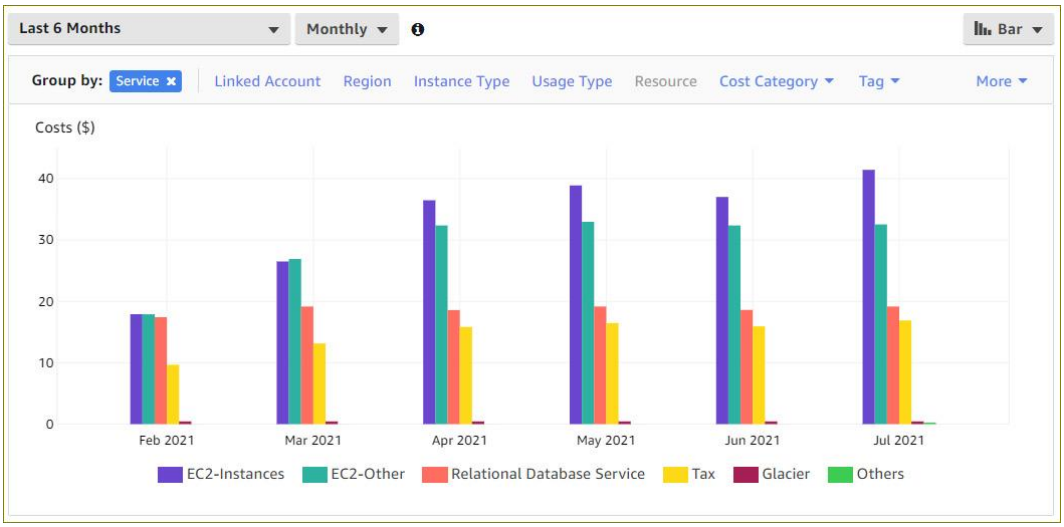

Figure 15.2 – Cost Explorer – monthly cost by service report

Figure 15.3 – Cost Explorer RI recommendations

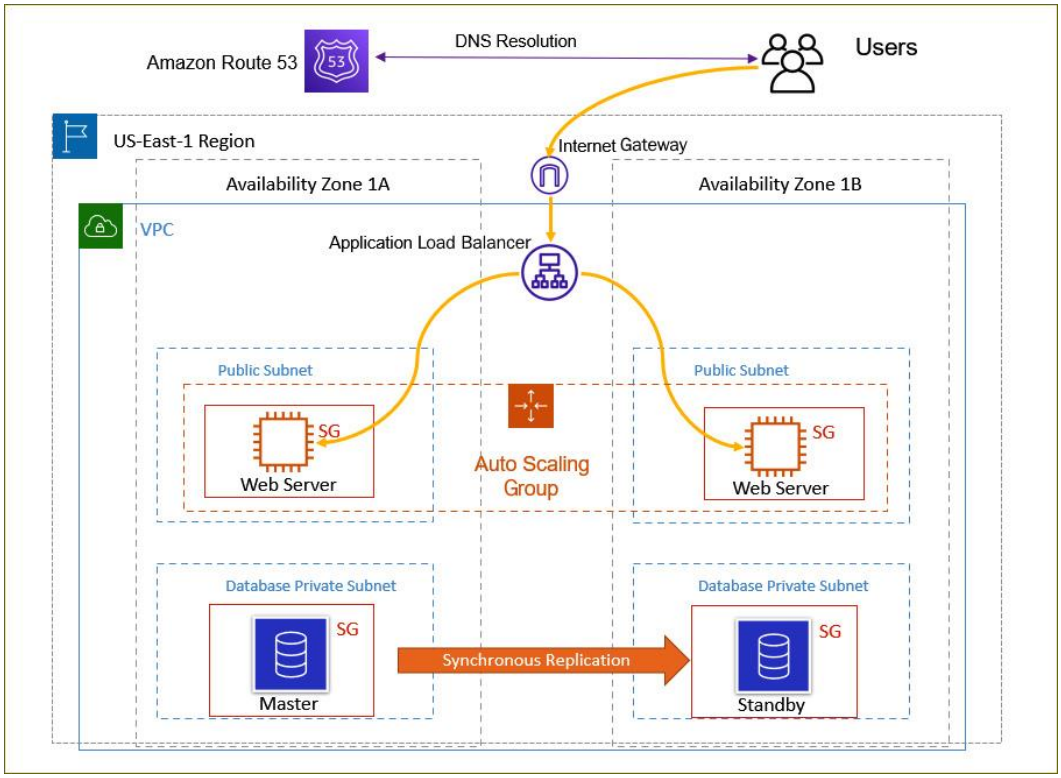

Figure 15.4 – AWS Pricing Calculator example – application architecture

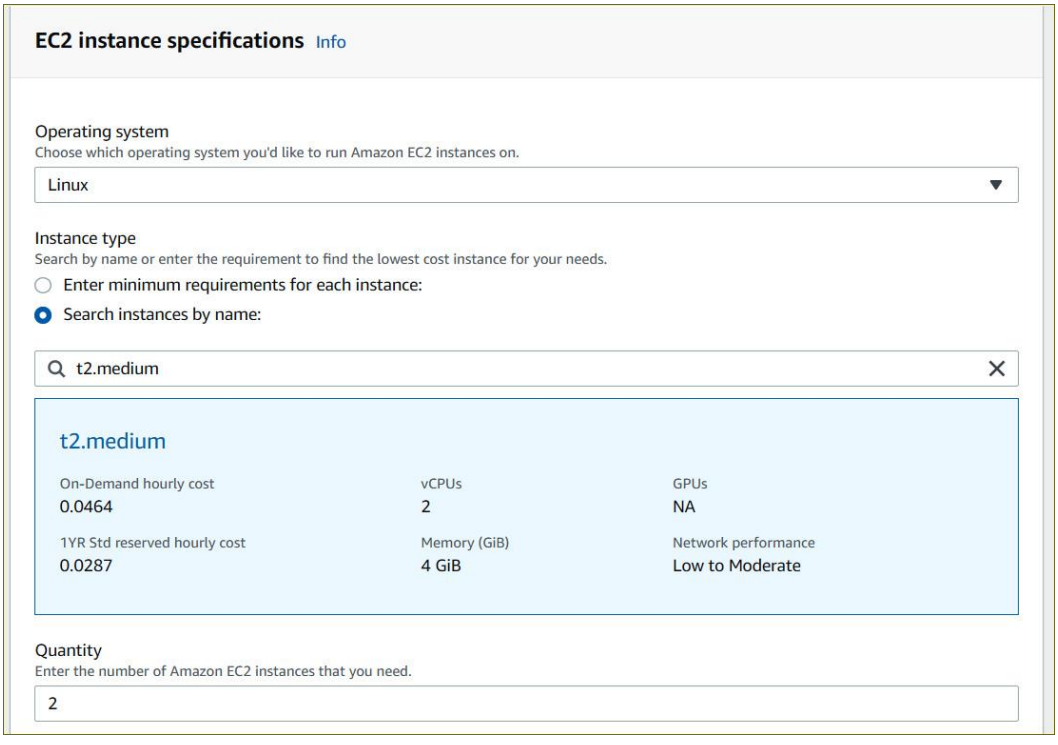

Figure 15.5 – AWS Pricing Calculator – EC2 instance specifications

Table

Characteristic	Estimated Usage	Description
Utilization	100%	All infrastructure components run 24 hours per day, 7 days per week
Instance	t2.medium	4 GB memory, 2 vCPUs. On-demand pricing option
Storage	Amazon EBS SSD gp2	1 EBS volume per instance with 30 GB of storage per volume
Data backup	Daily EBS snapshots	1 EBS volume per instance with 30 GB of storage per volume, 50 MB change per snapshot
Data transfer	Data in 1 TB/month Data out: 1 TB/month	10% incremental change per day
Instance scale	2	There are 2 EC2 instances running in the fleet and for Auto Scaling, we will maintain the fleet size to 2
Load balancing	10 GB/Hour	Elastic load balancing is used 24 hours per day, 7 days per week. It processes a total of 10 GB/Hour (data in + data out)
Database	MySQL, db.m5.large instance with 8 GB memory, 2 vCPUs, 200 GB storage	Multi-AZ deployment with synchronous standby replica in separate Availability Zone

Table 15.1 – AWS Pricing Calculator example architecture

Service	Monthly	Annual	Configuration summary
Amazon Virtual Private Cloud (VPC)	$92.07	$1,104.84	DT Inbound: Internet (1 TB per month), DT Outbound: Internet (1 TB per month), DT Intra-Region: (0 TB per month), Data transfer cost (92.07)
Application Load Balancer	$74.83	$897.96	Number of Application Load Balancers (1)

Service	Monthly	Annual	Configuration summary
Amazon EC2	$47.90	$574.80	Operating system (Linux), Quantity (2), Pricing strategy (EC2 Instance Savings Plans 1 Year No Upfront), Storage amount (30 GB), Instance type (t2.medium)
Amazon Elastic Block Store (EBS)	$9.37	$112.44	Number of instances (2), Average duration each instance runs (730 hours per month), Storage amount (30 GB), Snapshot Frequency (Daily), Amount charged per snapshot (250 MB)
Amazon RDS for MySQL	$295.66	$3,547.92	Storage for each RDS instance (General Purpose SSD (gp2)), Storage amount (200 GB), Quantity (1), Instance type (db.m5.large), Deployment option (Multi-AZ), Pricing strategy (OnDemand)
Amazon Route 53	$0.50	$6.00	Hosted Zones (1), Basic Checks Within AWS (1)
Total Project Costs	$520.33	$6,243.96	

Table 15.2 – AWS Pricing Calculator – estimated costs

Exercise 15.1 – setting up cost budgets on AWS

In this exercise, you will create a total monthly cost budget for your workloads. This will allow you to monitor your spending and avoid unintentional cost overruns:

1. Log in to the AWS Management Console using the credentials of the IAM user *Alice*.
2. Search for `AWS Budgets` from the top search bar on the console screen, and navigate to the AWS Budgets console page.
3. From the right-hand pane, click on the **Create a budget** button.
4. Next, from the list of **Budget types**, select **Cost budget – Recommended**.
5. Click the **Next** button in the bottom-right corner of the page.
6. In the **Set budget amount** pane, configure the following:
7. Set the period to **Monthly**.
8. Select **Recurring budget**.
9. Set the start month of your choice.
10. Select the **Fixed** option under **Choose how to budget**.
11. Next, enter your budget amount. I have set mine to $20 as per the following screenshot:

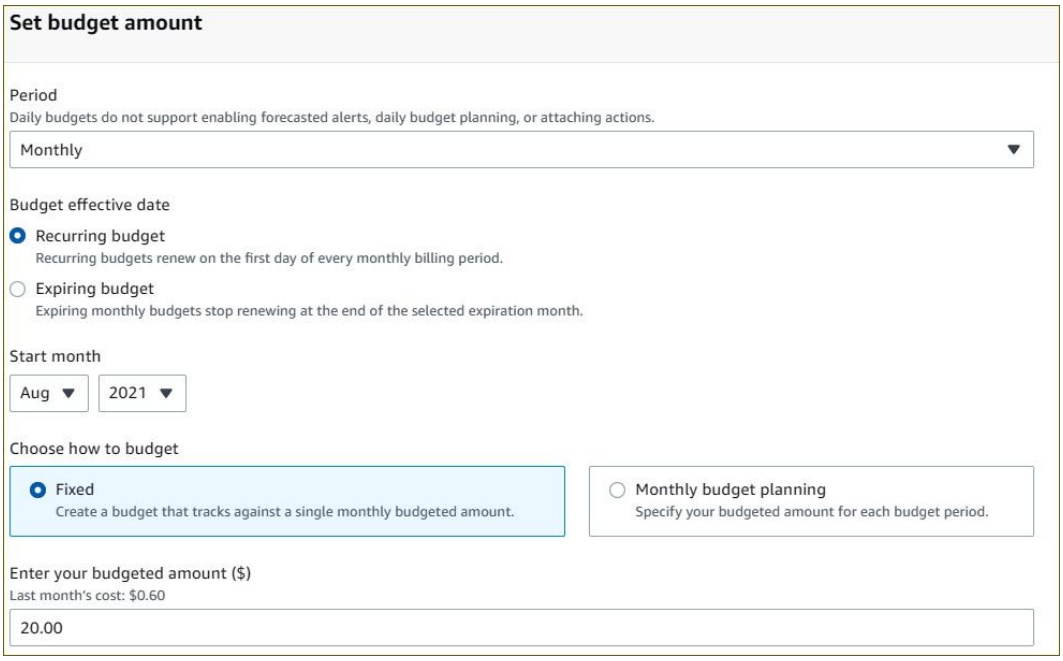

Figure 15.6 – AWS Budgets – setting up monthly cost budgets

12. Scroll further down to review your **Budget scoping** pane. Here, you will see whether your monthly cost budget is reasonable based on historic costs. As you will note from the

following screenshot, for my AWS account, the budget of $20 is acceptable because, since February 2021, I have been spending less than $15, which is within my budget:

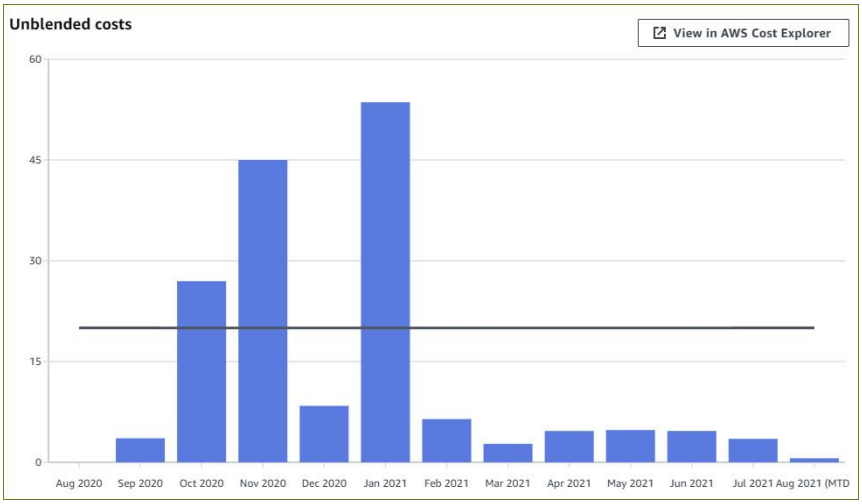

Figure 15.7 – AWS Budgets – budget scoping

13. Finally, provide a name for your budget and click **Next**.
14. Next, you can configure an alerts threshold, where you can be notified if you cross the threshold. Click on the **Add an alert threshold** button.
15. Under **Set alert threshold**, specify a threshold of 80% of the budgeted amount and set the trigger to **Actual** as per the following screenshot:

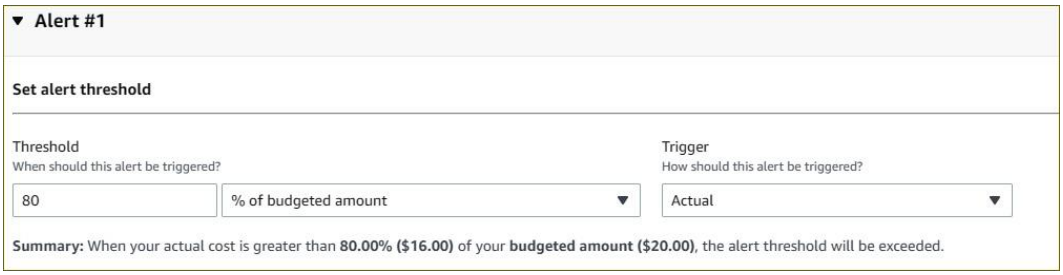

Figure 15.8 – Setting alert threshold

16. Next, under **Email recipients**, specify an email address to send the alerts to.
17. You can also set Amazon SNS alerts and Amazon Chatbot alerts.
18. Click on the **Next** button in the bottom-right corner of the page.
19. You can also define **Actions** to take when the threshold is crossed, for which you will need to configure appropriate IAM roles. For now, just click on the **Next** button.
20. Review your settings and click the **Create budget** button in the bottom right-hand corner of the page.
21. Your cost budget will be created, and you will be able to view it in the **Overview** console as per the following screenshot:

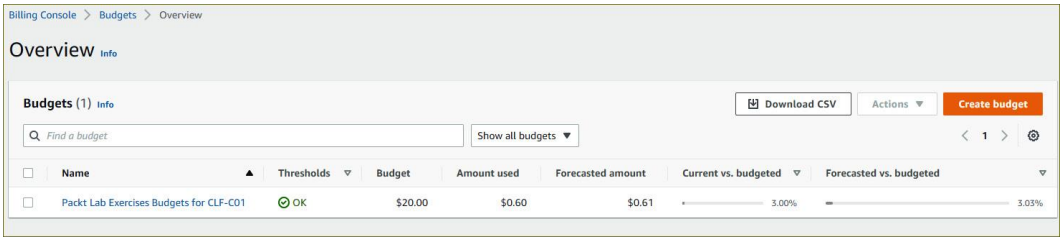

Figure 15.9 – AWS Budgets – Overview console

Note that you can set up five additional alerts for your budgets, such as the following:

- When current monthly costs exceed the budgeted amount
- When current monthly costs exceed 80% of the budgeted amount
- When forecasted monthly costs exceed the budgeted amount

In this section exercise, you learned how to create monthly cost budgets for your AWS account. Setting custom budgets can alert you if you are crossing specific threshold values or even forecasted costs in the future.

Next, we provide a summary of this chapter.

Questions

1. Which AWS service enables you to specify a monthly cost amount for your AWS account and send out an alert if the actual or forecast spending is likely to cross the budgeted threshold values?

   A. AWS Budgets

   B. AWS Cost Explorer

   C. AWS Config

   D. AWS Pricing Calculator

2. Which AWS service enables you to access 12 months of usage and spending data as well as forecasting what your future costs will be for the next 12 months?

   A. AWS Cost Explorer

   B. AWS Billing alarms

   C. AWS Config

   D. AWS annual report

3. The finance department would like to get a report on the total monthly spending for all AWS resources broken down by business unit/project name. The purpose of which is to understand how much each business unit/project costs. Which feature of the AWS Billing and Cost Management services enables you to achieve this requirement?

A. Cost allocation tags

B. Cost and usage report

C. AWS Budgets

D. AWS CloudWatch

4. Which AWS service can analyze your monthly compute usage and offer recommendations for purchasing EC2 **RI** for your existing on-demand workloads?

A. AWS CloudTrail

B. AWS Budgets

C. AWS Cost Explorer

D. AWS Migration Evaluator

5. You are planning on architecting and building a three-tier application solution, comprising EC2 instances, load balancers, the Auto Scaling service, and a backend database. Which AWS service can you use to produce an estimated monthly cost for your proposal?

A. AWS Cost Explorer

B. AWS Pricing Calculator

C. AWS Cost Optimization Analyzer

D. AWS SNS

Chapter 16: Mock Tests

The AWS Certified Cloud Practitioner exam is a 90-minute, multi-choice, and multi-answer-style exam. AWS charges USD 100 to enroll for the exam, which can be booked via their website at https://www.aws.training/certification. The exams are delivered at test centers located across several cities in many countries or can be taken online at home.

In this chapter, we will offer you two complete exam-style mock tests that you can use to gauge your readiness for the official AWS Certified Cloud Practitioner exam.

These tests comprise 65 questions each with full answer explanations available at the end of this chapter. To effectively use these tests, ensure you follow these steps:

- Set aside 90 minutes for each test, where you will not be disturbed. You can use your phone to set an alarm.
- Grab some paper and a pen and for each question, jot down the question's number and the Correct answer.
- Ensure that if you have time left over when you complete the test, you review your answers once more.
- At the end of the 90 minutes, review your answers and compare them with the answer explanation section at the end of this chapter.

You want to be able to answer all the questions correctly before you enter the exam room. You should use these tests to identify any questions that you did not answer correctly and then go back and review the chapter that covers the concepts examined in the question. This way, you will fill any gaps in your knowledge and be in a better position to get a high score on the official exam.

Mock test 1

1. Which type of cloud service model is most like an on-premises environment, where you configure virtual infrastructure components such as compute, network, and storage services that you can host your applications on?

   A. Software as a Service (SaaS)

   B. Platform as a Service (PaaS)

   C. Infrastructure as a Service (IaaS)

   D. Function as a Service (FaaS)

2. Your company is looking to move all its applications and services to the cloud but would like to migrate workloads in stages. This would require you to ensure that there is connectivity between the on-premises infrastructure and the applications you deploy on AWS for a while. What cloud deployment model would you need to establish?

A. Private cloud

B. Public cloud

C. Hybrid cloud

D. Multi-cloud

3. Which of the following statements are valid reasons for choosing a specific AWS Region to deploy your applications in? (Choose two)

A. Your organization would choose a specific AWS Region that enables you to ensure that your applications are closer to your end users, thereby reducing any latency.

B. If your organization has specific compliance or data residency laws to follow, then your choice of an AWS Region will be dictated by this requirement.

C. Your organization would choose a Region closer to its location since your IT staff will need to visit the AWS data centers to set up servers and networking equipment.

D. Your organization would choose a Region-based location where your business has an established legal presence. This is because you cannot access other Regions unless you have a legal establishment in that Region.

E. Your organization would select an AWS Region that offered higher variable costs but lower upfront costs.

4. Which component of the AWS Global Infrastructure enables you to cache content (videos, images, and documents) and offer low-latency access when your users try to download them?

A. AWS Regions

B. Availability Zones

C. Edge locations

D. Local Zones

5. Which of the following AWS services can help you design a hybrid cloud architecture and enable your on-premises applications to get access to Amazon S3 cloud storage?

A. Amazon Snowball Edge

B. AWS Storage Gateway

C. Amazon Elastic Block Store

D. Amazon CloudFront

6. You are planning on using AWS services to host an application that is still under development, and you need to decide which AWS support plan you should subscribe to. You

do not need production-level support currently and are happy with a 12-hour response time for any system-impaired issues. Which is the most cost-effective support plan you should subscribe to?

A. Basic Support plan

B. Developer Support plan

C. Business Support plan

D. Enterprise Support plan

7. Which of the following are regarded as global services on AWS? (Choose two)

A. AWS IAM

B. Amazon Route53

C. Amazon EC2

D. Amazon EFS

E. Amazon RDS

8. Which of the following statements closely relates to the advantage of cloud computing that discusses the ability to *go global in minutes*?

A. The ability to trade capital expenses for variable expenses and thus avoid huge CAPEX.

B. The ability to provision resources just in time for when you need them using tools such as Auto Scaling.

C. The ability to deploy your applications across multiple Regions with just a few mouse clicks.

D. The ability to focus on experimentation and the development of your applications rather than infrastructure builds, management, and maintenance.

9. Which AWS service can you configure to send out an alert to an email address if your total expenditure crosses a predefined monthly cost?

A. Set up a billing alarm in Amazon CloudWatch

B. Set up a billing alarm in Amazon CloudTrail

C. Set up a billing alarm in Amazon Config

D. Set up a billing blarm in Amazon Trusted Advisor

10. Which of the following resource types is tied to the Availability Zone that it was launched in?

A. Elastic Block Store (EBS)

B. Elastic File Store (EFS)

C. Amazon Route53 Hosted Zones

D. Amazon DynamoDB

11. As part of enhancing the security of your AWS account, you need to ensure that all IAM users use complex passwords comprising of at least one capital letter, a number, a symbol, and a minimum of 9 characters. Which AWS IAM feature can you use to configure these requirements?

A. Password policies

B. Permission boundaries

C. Service Control Policies (SCPs)

D. Resource policies

12. As a recommended best practice, what additional authentication security measure can you implement for your root user and IAM users?

A. Implement MFA.

B. Implement LastPass.

C. Implement AWS WAF.

D. Implement AWS Shield.

13. What is the easiest way to assign permissions to many IAM users who share a common job function?

A. Create a customer-managed IAM policy and attach the same policies to all IAM users who share a common job function.

B. Create an IAM Group, add IAM users who share the common job function to that group, and apply an IAM policy to the group with the necessary permissions.

C. Create an SCP to restrict users who share a common job function for specific permissions.

D. Create an IAM role with the necessary permissions and assign the role to all IAM users who share the common job function.

14. You have outsourced the development of your application to a third-party provider. This provider will require temporary access to your AWS account to set up the necessary infrastructure and deploy the application. What type of identity should you configure for the provider to use to gain access?

A. IAM User

B. IAM Group

C. IAM role

D. Root user

E. Which tool on AWS can be used to estimate your monthly costs?

F. AWS Pricing Calculator

G. AWS TCO Calculator

H. AWS Free Tier Calculator

I. AWS Monthly Calculator

15. You need to differentiate the cost of running different workloads in your AWS account by business unit and department. How you can identify your resources, as well as their owners, in the billing reports generated by AWS?

A. Designate specific tags as cost allocation tags in the AWS Billing and Cost Management Console.

B. Set up an SNS alert for each department.

C. Create a billing alarm.

D. Configure consolidated billing in AWS Organizations.

16. Which AWS tool enables you to view your **Reserved Instance** (**RI**) utilization?

A. AWS Cost Explorer

B. AWS Config

C. AWS CloudTrail

D. AWS Personal Health Dashboard

17. Which set of credentials do you need to configure for IAM users who need to access your AWS account via the **command-line interface** (**CLI**)?

A. IAM username and password

B. IAM access key ID and secret access key

C. IAM MFA

D. IAM key pairs

18. An application is to be deployed on EC2 instances that will need to access an Amazon S3 bucket to upload any artifacts that are created. Which security option is considered a best

practice to grant the application running on the EC2 instances the necessary permissions to upload files to the Amazon S3 bucket?

A. Create an IAM user account with a set of access keys and assign the required level of permissions using an IAM policy. Hardcode the application with the access keys.

B. Create an IAM user account with a username and password and assign the required level of permissions using an IAM policy. Hardcode the application with the username and password.

C. Create an IAM role with the required level of permissions using an IAM policy. Attach the role to the application running on the EC2 instance.

D. Create an IAM role with the required level of permissions using an IAM policy. Attach the role to the EC2 instances that will host the application.

19. Which AWS service enables you to troubleshoot IAM policies by identifying which set of permissions are allowed and which are denied?

A. AWS Policy Simulator

B. AWS Policy Manager

C. AWS CloudTrail

D. AWS **SCPs**

20. As part of your regular compliance processes, you are required to regularly audit the list of your IAM users and review information such as if they have been configured with passwords and access keys, as well as if MFA has been enabled on those accounts. Which AWS IAM service enables you to produce regular reports containing the preceding information?

A. IAM Credentials Report

B. IAM MFA Report

C. AWS CloudWatch

D. AWS Config

21. Which type of AWS policy enables you to define boundaries against what an IAM user or IAM role can be permitted to do in your AWS account?

A. IAM policies

B. Resource-based policies

C. **SCPs**

D. Permission boundaries

22. Which type of AWS policy enables you to control the maximum set of permissions that can be defined for AWS member accounts of an organization?

    A. IAM policies

    B. Resource-based policies

    C. **SCPs**

    D. Permission boundaries

23. Which of the following Amazon S3 storage classes can help you reduce the cost of storage for objects that are infrequently accessed, and yet still give you instant access when you need it?

    A. Amazon S3 Standard-IA

    B. Amazon S3 Glacier

    C. Amazon S3 Glacier Deep Archive

    D. Amazon S3 Standard

24. You are hosting an Amazon S3 bucket that contains important documents, and you want to enhance security whereby IAM users who try to access the objects can only do so from within the corporate office network. How would you configure your S3 bucket to fulfill this requirement?

    A. Create a resource policy granting the necessary level of access with a condition statement that defines and specifies the corporate office IP block.

    B. Create a resource policy granting the necessary level of access with a condition statement that specifies your corporate IAM users' accounts.

    C. Create an SCP granting access with a condition statement that specifies the corporate office IP block.

    D. Create an Amazon S3 **Access Control List** (**ACL**) with a condition statement that specifies your corporate IAM users' accounts.

25. Which type of Amazon S3 Storage class is cost-effective where you are unsure of your access patterns for the data contained within the S3 bucket?

    A. Amazon S3 Standard storage class

    B. Amazon S3 Standard-IA storage class

    C. Amazon S3 One-Zone IA

    D. Amazon S3 Intelligent Tiering

26. Your junior colleague accidentally deleted some financial data that was stored in an Amazon S3 bucket. How can you prevent such accidental deletions of data in Amazon S3?

    A. Do not give junior administrators access to Amazon S3.

    B. Set up Amazon S3 Versioning on your S3 bucket.

    C. Set up Amazon S3 Lifecycle Management.

    D. Set up Amazon S3 Termination Protection.

27. Which feature of Amazon S3 enables you to create a secondary copy of your objects in a given S3 bucket that will be stored in a different Region for compliance purposes?

    A. Amazon S3 Cross-Region Replication (CRR)

    B. Amazon S3 Same Region Replication

    C. Amazon S3 Versioning

    D. Amazon S3 Multi-Copy

28. Company policy dictates that objects stored in Amazon S3 must be encrypted at rest. It is also mandated that your choice of encryption should offer an auditing feature that shows when your **Customer Master Key** (**CMK**) was used and by whom. Which type of Amazon S3 encryption option will you need to configure to fulfill the requirements?

    A. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

    B. Client-Side Encryption

    C. Server-Side Encryption with KMS keys stored in AWS Key Management Service (SSE-KMS) Bitlocker

29. You need to retrieve a small subset of some archive data urgently to resolve a pending investigation. The data is stored in the Amazon S3 Glacier storage class. Which retrieval option can use to access the data urgently?

    A. Standard retrieval option

    B. Expedited retrieval option

    C. Bulk retrieval option

    D. Power retrieval option

30. You have a team of remote workers who need to upload research documents and videos to your Amazon S3 bucket hosted in the us-east-1 Region. You would like to ensure that your remote staff can upload research material with low latency access. What can you do to reduce speed variability for uploads, which are often experienced due to the architecture of the public internet?

A. Enable Amazon S3 Transfer Acceleration (S3TA) for your bucket.

B. Configure an IPSec site-to-site VPN connection between your remote workers and the VPC in the us-east-1 Region.

C. Use the Amazon Storage Gateway service.

D. Set up Amazon Express Route.

31. You need to transfer large amounts of data from your on-premises network to the Amazon S3 platform. The total data capacity is around 400 TB. You have decided to opt for the Amazon Snowball Edge service to complete the transfer. No data compute or processing is required. Which *flavor* of the Amazon Snowball Edge service would you recommend?

A. Snowball Edge Compute Optimized

B. Snowball Edge Storage Optimized

C. Snowball Edge Data Optimized

D. Snowball Edge Function Optimized

32. You host several Microsoft Windows applications on-premises that need low latency access to large amounts of storage. You would like to use the Amazon Storage Gateway service to host all application-level data. Which gateway option would you recommend?

A. Amazon S3 File Gateway

B. Amazon FSx File Gateway

C. Volume Gateway Cached Mode

D. Tape Gateway

33. Following best practices, you have deployed your application servers within the private subnets of a VPC. However, these servers require internet access to download updates and security patches. Which type of resource can enable you to grant internet access to EC2 instances in private subnets without having to assign public IP addresses to those instances?

A. Internet gateway

B. NAT gateway

C. Subnet

D. Route table

34. Which of the following statements is true about security groups?

A. Security groups are stateful and you need to configure both inbound and the corresponding outbound rules for traffic to flow bidirectionally.

B. Security groups are stateless and you do not need to configure both inbound and the corresponding outbound rules for traffic to flow bidirectionally.

C. Security groups can be used to explicitly deny inbound traffic from a specific IP address range.

D. Security groups are used to limit what actions IAM users that are members of the group can perform.

35. Which feature of the AWS VPC service enables you to connect multiple VPCs so that traffic between those VPCs can be sent using private IP address space?

A. VPC peering

B. VPC Flow Logs

C. Subnets

D. VPC endpoints

36. Which service enables you to reduce the complexity associated with establishing multiple VPC peering connections?

A. AWS Transit Gateway

B. AWS VPC Manager

C. AWS Direct Connect

D. IPSec VPN Tunnel

37. Which AWS service enables you to connect your on-premises network to your AWS account using a dedicated private connection that bypasses the internet altogether?

A. IPSec VPN

B. Express Route

C. Direct Connect

D. Snowball

38. Which AWS feature can help you establish connectivity between your on-premises network and your AWS VPC using an IPSec tunnel?

A. Direct Connect

B. **Virtual Private Network** (**VPN**)

C. AWS Outposts

D. Amazon SNS

39. You are about to publish your web application using an **Application Load Balancer** (**ALB**) and would like to use a friendly domain name to advertise the site to your users rather than the ALB's DNS name. Which AWS service can you use to configure the alias's name so that when users type in the friendly domain name into the browser, they are directed to the ALB's DNS URL?

    A. Amazon Route53

    B. Amazon CloudFront

    C. Amazon S3

    D. Amazon Direct Connect

40. Which AWS service enables you to purchase and register new domain names that can be used to publish your website on the internet?

    A. Route53

    B. VPC

    C. RDS

    D. Elastic Beanstalk

41. You have developed a web application that you want to offer redundancy and resilience for. Which feature of the Amazon Route53 service can help you design your web application with a primary site where all users' traffic is directed to, by default, and if the primary site is offline, then users are redirected to a secondary site located in a different Region.

    A. Simple routing policy

    B. Weighted routing policy

    C. Failover routing policy

    D. Geolocation routing policy

42. You plan to host a new Amazon S3 static website through which you will offer free recipe guides. The site is going to be accessed by users across the globe. The site contains lots of videos and images about the recipes you offer. Which AWS service can help you cache your digital assets locally to where users are located and thus reduce latency when your users access content on your website?

    A. Amazon Route53

    B. Amazon VPC

    C. Amazon CloudFront

    D. Amazon Cloud9

43. You have created an EC2 AMI that contains the base operating system and all necessary corporate settings/configurations. Your colleagues in another Region are trying to launch new EC2 instances but they are unable to access your AMI. What do you need to do so that your colleagues can use the new image?

    A. Copy the AMI to other Regions.

    B. Set up a VPC endpoint between the Regions to allow your colleagues to download the AMI.

    C. Copy the AMI to an S3 bucket.

    D. Use the Amazon Snowball service to send a copy of the AMI to your colleagues.

44. Which EC2 instance type is designed for floating-point number calculations, graphics processing, or data pattern matching?

    A. General Purpose

    B. Memory-Optimized

    C. Compute Optimized

    D. Accelerated Computing

45. You need to deploy a certain third-party application on an EC2 instance where the licensing term is based on a per-CPU core/socket basis. Which EC2 pricing option do you need to use for this requirement?

    A. On-Demand

    B. Reserved Instance

    C. Spot Instance

    D. Dedicated Host

46. You are currently running a test phase for a new application that is being developed in-house. Your UAT testers will need to access test servers for 3 hours a day, three times a week. The test phase is supposed to last 5 weeks. You cannot afford any interruptions to the application while the tests are being run. Which EC2 pricing option will be the most cost-effective?

    A. On-Demand

    B. Reserved

    C. Spot

    D. Dedicated Host

47. Which EBS volume type is designed for critical, I/O-intensive databases and application workloads?

    A. `gp2`

    B. `st1`

    C. `sc1`

    D. `io1`

48. Which of the following payment options will help you achieve the maximum discount for your RIs?

    A. A 1-year commitment with payment made using the **Partial Upfront** option.

    B. A 1-year commitment with payment made using the **All Upfront** option.

    C. A 1-year commitment with payment made using the **No Upfront** option.

    D. A 3-year commitment with payment made using the **All Upfront** option.

49. Which AWS service enables you to quickly deploy a **Virtual Private Server** (**VPS**) that comes preconfigured with common application stacks, SSD storage, and fixed IP addresses for a fixed monthly fee based on the configuration of the server?

    A. Amazon EC2

    B. Amazon Lightsail

    C. Amazon ECS

    D. Amazon ECR

50. You are planning on deploying a Docker application on AWS. You wish to deploy your Docker image without having to manage EC2 instances such as provisioning and scaling clusters, or patching and updating virtual servers yourself. Which service enables you to fulfill this requirement?

    A. Amazon ECS deployed using the EC2 Launch Type

    B. Amazon ECS deployed using the Fargate Launch Type

    C. Amazon ECS deployed using ECR

    D. Amazon ECS deployed with Lambda functions to manage your servers

51. Which of the following services is part of the AWS serverless offering that allows you to run code in response to a trigger or event?

    A. Amazon ECS

    B. AWS Lambda

C. Amazon EC2

D. AWS CloudFront

52. Which AWS storage option is designed to offer file sharing capabilities for Windows-aware applications and offers options for integration with Microsoft Active Directory?

A. AWS FSx for Lustre

B. Amazon FSx for Windows File Server

C. AWS Elastic File Syste

D. AWS instance store volumes

53. You are planning on deploying 10 EC2 instances across two Availability Zones that will host the new line of business applications. All the servers will need to share common files and will run the Amazon Linux 2 operating system. Which storage architecture would you recommend to host the shared files for your application servers?

A. Amazon Elastic File System (EFS)

B. Amazon FSx Lustre

C. Amazon S3

D. Amazon EBS

54. You have just launched a Windows EC2 instance. How can you obtain the Windows local administrator password?

A. Raise a support request with Amazon to obtain the password.

B. The password is sent to you automatically via email.

C. The password is sent to you via an SMS text message to your registered mobile.

D. Use the key pair to decrypt the password.

55. Which AWS service enables you to configure a hybrid solution by extending AWS Infrastructure so that EC2 and EBS services can be hosted in your on-premise data center?

A. AWS RDS

B. AWS Direct Connect

C. AWS Outposts

D. AWS Route53

56. Your company provides spread betting services. You wish to run an end of day analysis against the day's transaction costs and carry out the necessary market analysis. Which AWS

service dynamically provisions the necessary compute services that will scale based on the volume and resource requirements of your submitted jobs?

A. AWS Batch

B. AWS CloudFront

C. AWS Lambda

D. AWS Blockchain

57. Which AWS service can help you deploy, manage, and scale containerized applications using Kubernetes on AWS?

A. Amazon ECS

B. Amazon EKS

C. Amazon MFA

D. Amazon EC2

58. Which of the following statements is an example of an advantage of using Amazon RDS over databases installed on EC2 instances?

A. Amazon RDS is a fully managed database where AWS manages the underlying compute and storage architecture, as well as patching and updates.

B. Amazon RDS grants you access to the operating system, allowing you to fine-tune the database for the operating system it is running.

C. Amazon RDS is faster than running the Microsoft SQL Server database on EC2 instances.

D. Amazon RDS automatically enables encryption of the data in Amazon RDS.

59. Which feature of Amazon RDS enables you to create a standby copy of the database and offer failover capabilities if the master copy fails?

A. Read Replicas

B. Multi-AZ

C. Failover policy

D. Snapshots

60. Your company is planning to migrate its on-premises MySQL database to Amazon RDS. Which service will enable you to perform the migration?

A. Amazon Server Migration Service (SMS)

B. Amazon Database Migration Service (DMS)

C. Amazon VM Import Export

D. Amazon Redshift Migration Utility

61. Which feature of AWS Redshift allows you to perform SQL queries against data stored directly on Amazon S3 buckets?

A. Redshift leader node

B. Redshift Spectrum

C. Redshift Copy

D. Redshift Streams

62. Which Amazon RDS engine offers high resilience with copies of the database placed across a minimum of three Availability Zones?

A. MySQL

B. PostgreSQL

C. Microsoft SQL Server

D. Amazon Aurora

63. Which AWS-managed database service enables you to store data using complex structures with options for nested attributes, such as a JSON-style document?

A. Amazon RDS

B. Amazon Redshift

C. Amazon DynamoDB

D. Amazon Aurora

64. Which AWS database service is designed to store sensitive data that is immutable and where the transactional logs are cryptographically verifiable?

A. AWS QLDB

B. Amazon Neptune

C. Amazon Aurora

D. Amazon RDS

Mock test 2

1. You are currently performing a manual snapshot of your single instance MySQL Amazon RDS database every 4 hours. Some users have complained that the application that connects to

the database experiences a brief outage when the backup process initializes. What can you do to resolve this issue?

A. Configure your Amazon RDS database with Read Replicas.

B. Configure your Amazon RDS database with Multi-AZ.

C. Configure an AWS backup to perform the RDS database backups.

D. Use the DMS service to migrate the MySQL database to Microsoft SQL Server.

2. Your organization is in a healthcare industry based in New York. You are planning on using an in-memory caching engine to alleviate the load on your Amazon RDS database for frequently used queries. Which AWS in-memory caching engine offers Multi-AZ capabilities, encryption of data, and compliance with the **Health Insurance Portability and Accountability Act** (**HIPAA**)?

   A. Amazon Elasticache for Redis

   B. Amazon Elasticache for Memcached

   C. Amazon CloudFront

   D. Amazon DynamoDB DAX

3. Which AWS service offers a fully managed data warehousing capability and enables you to analyze large datasets using standard SQL and **Business Intelligence** (**BI**) tools?

   A. Amazon RDS

   B. Amazon QLDB

   C. Amazon Redshift

   D. Amazon Aurora

4. Which of the following services further increase your EC2 instances' costs? (Choose two)

   A. Detailed monitoring

   B. Use of Elastic Load Balancers

   C. S3 buckets that you connect to

   D. DynamoDB tables that you query

   E. Setting up multiple key pairs

5. Your developer team needs to deploy an Elastic Load Balancer that will direct traffic to your web servers based on the URL path and over the HTTPS protocol. Which Elastic Load Balancer would you recommend?

   A. Network Load Balancer

B. ALB

C. Gateway Load Balancer

D. Classic Load Balancer

6. Which feature of the Elastic Load Balancer service is suitable for **Transmission Control Protocol** (**TCP**), **User Datagram Protocol** (**UDP**), and **Transport Layer Security** (**TLS**) type traffic and operates at layer 4 of the **Open Systems Interconnection** (**OSI**) model?

   A. Network Load Balancer

   B. ALB

   C. Gateway Load Balancer

   D. Classic Load Balancer

7. Which of the following statements is true about Elastic Load Balancers?

   A. Elastic Load Balancers act as firewalls to protect the application running on your EC2 instances.

   B. Elastic Load Balancers enable you to achieve high availability across multiple Regions by distributing incoming web traffic to targets located in multiple Regions.

   C. Elastic Load Balancers enable you to achieve high availability within a single Region by distributing incoming web traffic to targets located in multiple Availability Zones.

   D. Elastic Load Balancers enable you to scale horizontally by provisioning or terminating EC2 instances based on the demand of your resources.

8. Which component of an Elastic Load Balancer do you need to configure to ensure you accept traffic on a designated port and forward that traffic on a specific port to your EC2 instances behind the load balancer?

   A. Port forwarder

   B. NAT Gateway

   C. Listener

   D. Echo

9. You are building a multi-tier architecture with web servers placed in the public subnet and application servers placed in the private subnet of your VPC. Which type of load balancer would you choose to distribute traffic to your application servers?

   A. Internet-facing

   B. Internal load balancers

C. Dynamic load balancers

D. Static load balancers

10. Which configuration feature of the AWS Auto Scaling service enables you to define a maximum number of EC2 instances that can be launched in your fleet?

A. Auto Scaling group

B. Auto Scaling Launch Configuration

C. Auto Scaling MaxFleet Size

D. Auto Scaling policy

11. Which AWS service can help you provision only the necessary number of EC2 instances required to meet application demand, thus saving on costs usually associated with overprovisioning resources?

A. Elastic Load Balancer

B. Auto Scaling

C. Cost Explorer

D. EC2 Launcher

12. You have recently launched a new *free coupon* web application across a fleet of EC2 instances configured in an Auto Scaling group. Traffic has increased dramatically before the Black Friday sale and you have noticed that your Auto Scaling service is not launching any more EC2 instances, even though the threshold metrics have been crossed in CloudWatch. Your colleague tells you that you may have crossed a quota or limit on the number of EC2 instances you can launch. Which AWS service can offer you a quick look to determine this is the case?

A. Personal Health Dashboard

B. AWS Systems Manager

C. AWS Config

D. AWS Trusted Advisor

13. Which firewall protection service does the ALB offer to help protect against common web exploits such as cross-site scripting and SQL injection?

A. AWS WAF

B. AWS Shield

C. Amazon Guard Duty

D. **Network Access Control Lists** (**NACLs**)

14. Which dynamic scaling policy offered by the Amazon Auto Scaling service can help you launch or terminate EC2 instances in the fleet based on the target value of a specific metric?

A. Target tracking scaling policy

B. Step scaling policy

C. Simple scaling policy

D. Predictable scaling policy

15. You plan to use Amazon CloudWatch to send out alerts whenever the CPU utilization on your production EC2 instances is more than 80% for 15 minutes. Which AWS service can you use to send out this alert notification?

A. Amazon SES

B. Amazon SNS

C. Amazon SQS

D. Amazon MQ

16. Which feature of the Amazon SNS service enables you to push notification messages to multiple endpoints in parallel?

A. You can use the SNS Fanout scenario to help you push notifications to multiple endpoints.

B. You can use SNS FIFO topics to help you push notifications to multiple endpoints.

C. You can change the timeout period to ensure that notifications are sent to multiple endpoints.

D. To send out notifications to multiple endpoints, you will need to configure Amazon SQS to integrate with Amazon SNS.

17. Which AWS service enables you to design your application architecture by decoupling its components into distributed systems and facilitating the design and architecture of microservices?

A. Amazon SNS

B. Amazon Simple Queue Service (SQS)

C. Amazon MQ

D. Amazon Redshift

18. You plan to use Amazon SQS to help decouple your application components. Which queue type will help you ensure that the message order from one component to another is preserved?

    A. Configure Amazon SQS with a standard queue.

    B. Configure Amazon SQS with a FIFO queue.

    C. Configure Amazon SQS with a LIFO queue.

    D. Configure Amazon SQS with a DLQ.

19. You are planning on migrating an application to the cloud. Which message brokering service will enable you to continue to use Apache ActiveMQ and facilitate communications between application components?

    A. Amazon SQS

    B. Amazon MQ

    C. Amazon SNS

    D. Amazon SES

20. Which AWS service can help you trigger a Lambda function based on an event such as an object being deleted from an Amazon S3 bucket?

    A. AWS ECS

    B. AWS Batch

    C. AWS EventBridge

    D. Amazon CloudTrail

21. Your application architecture for an insurance claim solution has a workflow process that can take up to 30 days to complete and requires human intervention in the form of manual approval processes to follow. Which AWS service would you recommend for architecting the workflow process?

    A. Amazon SQS

    B. Amazon Step Functions

    C. AWS CloudFormation

    D. AWS Lambda

22. You plan to configure a Lambda function that will be used to automatically start and stop EC2 instances at the start and close of the business day, respectively. How can you automate the start and stop of EC2 instances according to a specified schedule?

A. Configure Amazon SNS to send out an alert trigger to the Lambda function.

B. Configure Amazon CloudTrail to trigger the Lambda function at the designated schedule.

C. Configure Amazon CloudWatch Events with a rule to trigger the Lambda function at the designated schedule.

D. Configure the Amazon Scheduler service.

23. You need to run certain SQL queries to analyze data from a streaming source and conduct analysis. Which of the following services can you use to analyze stream data in real time?

A. Amazon SQS

B. Amazon Kinesis Data Streams

C. Amazon Kinesis Analytics

D. Amazon Athena

24. You are required to run ad hoc test queries against weekly reports that are stored in Amazon S3. Which AWS service can you use to query raw data in Amazon S3 using standard SQL?

A. Amazon Athena

B. Amazon Kinesis

C. Amazon RDS

D. Amazon Redshift

25. Which AWS service can be used to load a massive amount of streaming data into your Redshift data warehousing solution in near real time?

A. Amazon Kinesis Data Streams

B. Amazon Kinesis Firehose

C. Amazon Kinesis Video Streams

D. Amazon Athena

26. Which AWS service can be used to create and publish interactive BI dashboards that can be embedded into your applications, websites, and portals using Amazon-provided APIs and SDKs?

A. Amazon Athena

B. Amazon QuickSight

C. Amazon Config

D. Amazon Glue

27. Which AWS service offers a serverless **Extract, Transform, and Load** (**ETL**) solution that's used to discover and extract data from various sources and perform any cleaning or normalization on data warehouses and data lakes, before loading them into databases?

    A. AWS QuickSight

    B. Amazon Athena

    C. Amazon Glue

    D. Amazon CloudTrail

28. As part of your migration to the cloud, you need to re-host an application that uses Apache Spark to process vast amounts of data for a big data project. Which service on AWS can you use to help with data transformation and perform ETL jobs such as sort, aggregate, and join on large datasets?

    A. AWS QuickSight

    B. Amazon EFS

    C. Amazon EMR

    D. Amazon S3

29. You need to regularly build test environments for new applications currently under development. Which AWS service can you use to automate the infrastructure build of your test environment and thus reduce the time taken to provision the infrastructure required?

    A. Amazon Elastic Beanstalk

    B. Amazon CloudFormation

    C. AWS OpsWorks

    D. AWS Systems Manager

30. Which service can be used to orchestrate and configure environments to deploy applications using the Chef and Puppet enterprise tools?

    A. Amazon CloudFormation

    B. AWS OpsWorks

    C. Amazon Elastic Beanstalk

    D. Amazon Cloud9

31. Which service enables developers to upload code to AWS and have the necessary infrastructure provisioned and managed to support that application?

    A. Amazon Elastic Beanstalk

B. Amazon CloudFormation

C. Amazon Cloud9

D. AWS OpsWorks

32. Which of the following environment tiers within the Elastic Beanstalk architecture is designed to support backend operations?

A. Web services tier

B. Worker tier

C. Backend tier

D. Database tier

33. Which of the following formats are CloudFormation templates written in? (Choose two)

A. YAML

B. XML

C. CSV

D. JSON

E. JAVA

34. Which of the following is an example of a custom CloudWatch metric?

A. CPU utilization

B. Disk read in

C. Network bytes in

D. Memory

35. Which feature of CloudWatch can help send you notification alerts via Amazon SNS whenever a particular threshold is breached for a specified period?

A. Dashboards

B. Alarms

C. Logs

D. Events

36. You plan to use CloudWatch Logs to monitor network traffic that enters the AWS environment that's been specifically destined for an EC2 instance. You would like to record all inbound network traffic on port 80 that was accepted. What service can you configure to help you achieve this requirement?

A. ALB access logs

B. VPC Flow Logs

C. CloudTrail Logs

D. Config logs

37. Which AWS service enables you to track user activity and API usage in your AWS account for auditing purposes?

A. AWS Config

B. AWS CloudWatch

C. AWS CloudTrail

D. AWS Trusted Advisor

38. Which AWS service can be used to see how resources are interrelated to each other, how they were configured in the past, and view historical changes to those resources over time?

A. AWS Trusted Advisor

B. AWS Systems Manager

C. AWS Config

D. AWS IAM

39. Which feature of the AWS System Manager service enables you to roll out security patches across EC2 instances and on-premises servers?

A. Patch Manager

B. Microsoft WSUS

C. AWS Config

D. SCCM

40. You are planning on deploying a three-tier application architecture that is comprised of a database backend. Your application has been hardcoded with the database connection strings and secrets such as username and password. The company's security policy dictates that this approach is unacceptable and they would like you to manage the secrets information more securely. What would you recommend?

A. Store the configuration information in the SSM Parameter Store and reference the parameter name from your code to dynamically retrieve the connection information.

B. Store the configuration information in Amazon Redshift and reference the connection details from your code to dynamically retrieve the connection information.

C. Store the configuration information in Amazon S3 and reference the connection details from your code dynamically.

D. Store the configuration information on an EBS volume and reference the connection details from your code dynamically.

41. Which AWS service can be used to manage and resolve incidents that affect their AWS-hosted applications?

A. AWS Systems Manager Incident Manager

B. AWS Systems Manager Event Manager

C. Amazon EventBridge

D. AWS **Personal Health Dashboard** (**PHD**)

42. Which AWS service can be used to identify resources that have not been configured by following security best practices?

A. AWS CloudWatch

B. AWS Trusted Advisor

C. AWS IAM

D. AWS CloudTrail

43. You are trying to review the AWS Trusted Advisor service to analyze potential cost savings opportunities for various workloads you have deployed on AWS. However, you have noticed that the Cost Optimization category is grayed out and there are no reports on current configuration states. What could be preventing you from viewing the Cost Optimization report?

A. You do not have enough permissions to access the Cost Optimization category on AWS Trusted Advisor.

B. You have not subscribed to either the business or enterprise support plans.

C. You have logged in with an IAM account and only the root user can access pricing and cost information.

D. The AWS account does not have an active debit/credit card associated with it.

44. Which Well-Architected Framework pillar suggests that replacing failed resources is often better than trying to figure out why the failure occurred? Identifying the reason for failure can be done later, but focusing on replacing the failed resource will help you get up and running quickly.

A. Cost Optimization

B. Fault Tolerance

C. Reliability

D. Performance

45. Which of the following services can help fulfill the guidelines provided in the performance pillar concerning ensuring low latency access to video content hosted in a single S3 bucket globally?

A. Use AWS CloudFront to cache the video content closer to end users.

B. Use AWS DynamoDB DAX to cache the video content closer to end users.

C. Use Amazon Elasticache to cache the video content closer to end users.

D. Use Amazon Kinesis to cache the video content closer to end users.

46. Which pillar of the Well-Architected Framework refers to selecting the appropriate pricing options that allow you to adopt a consumption model for provisioning various resources?

A. Performance pillar

B. Reliability pillar

C. Fault Tolerance pillar

D. Cost Optimization pillar

47. Regarding the AWS Shared Responsibility Model, who is responsible for patching Amazon RDS database instances?

A. AWS

B. Customer

C. Database engine vendor

D. Both the customer and AWS

48. Which AWS service gives customers access to various compliance reports that confirm if the services offered by AWS meet specific requirements and regulatory requirements?

A. AWS CloudTrail

B. AWS **Acceptable Usage Policy** (**AUP**)

C. AWS Artifacts

D. AWS Compliance Programs

49. AWS allows customers to run vulnerability scans and perform penetration testing. However, certain types of testing are not permitted. Which of the following actions is the customer prohibited from performing?

    A. Brute-force attacks by trying to guess your Amazon RDS database passwords.

    B. Running malware detection programs on your EC2 instances.

    C. Attempting to perform cross-site scripting or SQL injection tests via your ALB.

    D. Performing simulated **Distributed Denial of Service** (**DDoS**) attacks.

50. Which AWS service enables you to encrypt data stored in your Amazon S3 buckets with a **CMK** and offers auditing capabilities?

    A. Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

    B. Server-Side Encryption with CMKs Stored in AWS KMS (SSE-KMS)

    C. Server-Side Encryption with Customer-Provided Keys (SSE-C)

    D. Client-Side Encryption with Amazon-Managed Keys

51. To meet strict compliance and regulatory requirements, you are required to encrypt the application data stored on your EC2 instances using dedicated FIPS 140-2 Level 3 validated devices. Which AWS service can you use to fulfill this requirement?

    A. AWS KMS

    B. AWS CloudHSM

    C. AWS TPM Hardware Modules

    D. AWS Certificate Manager

52. Which AWS security solution offers protection against **DDoS** attacks and features an AWS **Shield Response Team** (**SRT**) 24/7 to assist you in handling such attacks?

    A. AWS WAF

    B. AWS X-Ray

    C. AWS Detective

    D. AWS Shield Advanced

53. Which type of firewall solution integrates with Amazon CloudFront and ALBs to offer protection against common web exploits such as cross-site scripting and SQL injection?

    A. AWS WAF

    B. AWS Shield

C. AWS X-Ray

D. AWS Firewall Manager

54. You are planning lots of data on Amazon S3 and you would like to monitor how your data is accessed, particularly highlighting any sensitive information such as **personally identifiable information** (**PII**). Which AWS service can help you meet this requirement?

A. Amazon Macie

B. AWS GuardDuty

C. AWS Detective

D. AWS X-Ray

55. You are building a mobile application that will be publicly accessible and you would like to integrate a third-party identity provider for authentication purposes, such as Facebook or Google. Which AWS service can be used to set up identity and access control solutions for your web and mobile applications?

A. AWS Cognito

B. AWS IAM

C. Active Directory

D. AWS Certificate Manager

56. Which AWS service can help detect malicious activities by analyzing data from your CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs?

A. AWS Shield

B. AWS Detective

C. AWS GuardDuty

D. Amazon Macie

57. Which AWS service can help you determine the root cause of security issues by extracting time-based events such as logins, network traffic from Amazon VPC Flow Logs, and data ingested from GuardDuty findings?

A. AWS Shield

B. AWS WAF

C. AWS Detective

D. Amazon Macie

58. You are planning on migrating your on-premises workloads and applications to the cloud. Which AWS service enables you to capture millions of real-time data points related to your IT environment and review recommendations for right sizing and appropriately costing workloads on AWS?

    A. AWS Pricing Calculator

    B. AWS Migration Evaluator

    C. AWS Hybrid Calculator

    D. AWS Cost Explorer

59. Which EC2 instance pricing model can offer up to a 90% discount off the on-demand price and be used in scenarios where interruptions to your instances will not impact the application workflow?

    A. Reserved Instances

    B. Spot Instances

    C. Dedicated Instances

    D. Dedicated Hosts

60. Which Amazon S3 storage class enables you to host 48 TB or 96 TB as part of the S3 storage capacity and provides the option to create a maximum of 100 S3 buckets on-premises?

    A. Standard storage class

    B. Standard One-Zone (IA)

    C. Glacier

    D. Amazon S3 on Outposts

61. Which type of policy can you create to grant anonymous access to the objects stored in an S3 bucket that can be used to host website assets?

    A. IAM policy

    B. IAM permission boundaries

    C. Resource policy

    D. SNS policy

62. Which AWS service enables you to register new domain names for your corporate business requirements?

    A. AWS DNS

    B. AWS Route53

C. AWS VPC

D. Amazon Macie

63. Which AWS service offers image and video analysis that can be used to identify objects, people, text, scenes, and other activities?

A. Amazon Rekognition

B. Amazon Kinesis Video Streams

C. Amazon Prime

D. Amazon Athena

64. Which AWS service offers text search and analytics capabilities that can store, analyze, and perform search functions against big data volumes in near real time?

A. Amazon Redshift

B. Amazon ElastiCache

C. Amazon Elastisearch

D. Amazon Search

65. You plan to migrate your entire on-premises network to the cloud and have also decided to move away from physical desktops and workstations to a complete VDI solution. Which service on AWS enables you to provision virtual desktops in the cloud, accessible via a web browser?

A. Amazon EC2

B. Amazon Lightsail

C. Amazon WorkSpaces

D. Amazon EKS

Answers

Chapter 1

1. D
2. A
3. A
4. A and B
5. A
6. C
7. C
8. C

Chapter 2

1. C and D
2. C
3. D
4. B
5. B
6. A
7. C
8. B
9. A and E
10. A and B
11. C
12. C

Chapter 3

1. A
2. A
3. A and B
4. A
5. A
6. B
7. B

Chapter 4

1. A and B
2. B
3. A
4. B
5. A
6. A
7. A
8. A
9. C
10. B

Chapter 5

1. A and D
2. B
3. C
4. D
5. B
6. C

7. A
8. A
9. B

Chapter 6

1. B
2. A
3. A
4. A
5. A
6. B
7. D
8. C
9. C
10. B

Chapter 7

1. D
2. A
3. C and E
4. A
5. A
6. C
7. A
8. A and B
9. A
10. B

Chapter 8

1. B
2. A
3. A, B, and C
4. C
5. B
6. B
7. C
8. C
9. B

Chapter 9

1. C
2. B
3. B
4. A
5. C
6. A

Chapter 10

1. A
2. D
3. B
4. C
5. A
6. A
7. B
8. C

9. A
10. D

Chapter 11

1. B
2. B
3. C and E
4. A
5. C
6. A
7. C

Chapter 12

1. C
2. B
3. A and B
4. C
5. B
6. B

Chapter 13

1. A
2. A
3. A
4. B
5. A

Chapter 14

1. A and B

2. B
3. A
4. A
5. A
6. B

Chapter 15

1. A
2. A
3. A
4. C
5. B

Chapter 16

Mock Test 1

1. C

   Infrastructure as a Service (**IaaS**) is a cloud service model that gives you access to virtualized infrastructure components comprising computing, network, and storage services. This is very similar to hosting your own VMware or Hyper-V virtualized platforms, where you deploy servers, attach storage volumes, and configure network connectivity services. However, the primary difference is that you do not have access to the underlying hypervisor platform with cloud-hosted IaaS solutions. IaaS offerings give the greatest amount of control over how the virtual components of your infrastructure are configured and also require you to take responsibility for managing, maintaining, and enforcing security measures for those components.

2. C

   Companies who wish to move their entire suite of applications to the cloud would normally carry out a series of migration projects over time. During this migration phase, connectivity between the on-premises environment and the AWS cloud would be required to facilitate the migration. Many companies may also require a more permanent hybrid design architecture. This could be because certain types of applications need to be in much closer proximity to the on-premises infrastructure where users are based, such as your corporate office network, ultimately ensuring low-latency access, data residency requirements, or even

unique local data processing requirements. AWS offers several services to build hybrid clouds from VPN technologies and Direct Connect services to offering on-premises services such as AWS Storage Gateway and AWS Outposts.

3. A and B

   There are several reasons why you would choose a specific AWS Region to deploy your applications in, including the need for closer proximity to your end users and thus to reduce latency, data residence laws, regulatory requirements, the choice of services available, and costs.

4. C

   Edge locations are AWS infrastructure facilities located across the globe that help cache content for Amazon CloudFront. Any content that is accessed from the origin is cached locally at one or more edge locations closer to users to access that content for a particular **time to live** (**TTL**). This way, repeated access to the same content is delivered over a low latency connection.

5. B

   AWS Storage Gateway enables you to build hybrid cloud solutions by giving access to the Amazon S3 and Glacier environments from your on-premises network. You install and configure the gateway appliance at your on-premises location and can use any one of four gateway types to access unlimited storage in the cloud. These gateway types are Amazon S3 File Gateway, Amazon FSx File Gateway, Tape Gateway, and Volume Gateway.

6. B

   The Developer Support plan gives you access to technical support via email and chats only. This support plan is cheaper than the Business and Enterprise Support plans and is recommended for experimenting with or testing applications on AWS.

7. A and B

   Several services are configured from a global perspective on AWS. For example, with IAM, every IAM user in your AWS account is unique across the entire AWS Global Infrastructure. The same applies to Amazon Route53, where domain names configured in host zones have a global presence across all Regions on AWS. Another global service on AWS is Amazon CloudFront.

8. C

   One of the six advantages of cloud computing is the ability to **go global in minutes**. This is made possible because, as an AWS customer, you have access to all Regions and Availability Zones where you can provision the resources required to host your application in a matter of minutes.

9. A

   Amazon CloudWatch enables you to set up alarms that can be triggered when a particular threshold is crossed. You can set up an alarm for billing alerts that monitors when your total spend crosses a specified dollar amount. This alarm can be configured to send out an alert to an email address that uses the Amazon SNS service.

10. A

    Amazon EBS is like the virtual hard disks (volumes) that you attach to EC2 instances. They need to be provisioned in the same availability where the EC2 instance has been launched to be attached to that EC2 instance. Furthermore, you cannot attach an EBS volume to an EC2 instance in another Availability Zone. You could take a snapshot of the EBS volume and launch a new volume in another Availability Zone from that snapshot if required.

11. A

    AWS IAM Password Policies enable you to define custom policies on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. This ensures that IAM user accounts are created with complex, hard-to-crack passwords.

12. A

    Multi-Factor Authentication (**MFA**) is a recommended best practice authentication security measure. It requires you to authenticate with a username and password, as well as a security token generated by a physical or virtual device you own. Used together, these factors provide increased security for your AWS account settings and resources.

13. B

    An IAM Group can be used to club users who share common job functions. You can then assign the necessary permissions to the IAM Group, which will filter down to the IAM users that are members of the group.

    Where possible, entities that need access to services and resources on AWS ought to be granted access via IAM roles using temporary security credentials. For example, users who need to access resources in another AWS account can be granted permission to assume a role rather than having to create IAM accounts for them in the other account. This is considered best practice and AWS highly recommends this approach.

14. C

    An IAM role enables you to grant external users access to resources in your AWS account using temporary credentials that are managed by the AWS **Security Token Service** (**STS**). An IAM role will also have an IAM policy attached to it that specifies the exact set of permissions the role will grant to the external user(s).

15. A

    AWS Pricing Calculator can help you estimate the monthly costs of the resources you wish to provision on AWS. In addition to specifying the expected usage for the month, to calculate the cost of the resources, you can provide additional details such as the amount of data transferred in and out of the AWS Region and cross-Region to get a complete estimate.

16. A

    You can use cost allocation tags to identify your resource costs on your cost allocation report and track your AWS costs by resources and who owns them. AWS provides two types of cost allocation tags: AWS-generated tags and user-defined tags.

17. A

    AWS Cost Explorer enables you to view 12 months of usage and spending data, as well as a forecast of what your future costs will be for the next 12 months. Cost Explorer can also provide information on how much of your RI you have utilized, as well as the savings that have been made from using RIs over on-demand options for EC2 Amazon Redshift, Amazon RDS, and more.

18. B

    To access an AWS account as an IAM user, you need to create a set of access keys, which is a combination of an access key ID and a secret access key. Note these keys are considered long-term access keys. One set of keys is associated with a specific IAM user.

19. D

    You can create an IAM role with the necessary permissions to upload objects to a specific Amazon S3 bucket. You should then deploy your EC2 instances with this role attached (this involves creating an instance profile associated with the role). The IAM role will enable the application running on the EC2 instance to access the Amazon S3 bucket. Using an IAM role, the EC2 instance will obtain temporary credentials from the **Security Token Service** (**STS**).

20. A

    AWS Policy Simulator can help you identify which set of policies are allowed and which are denied against specific identities, groups of identities, and IAM roles. You can obtain granular visibility into specific permissions that have been allowed and denied, helping you troubleshoot access issues.

21. A

    The IAM Credentials Report enables you to review IAM user accounts created in your AWS account. You can identify if an IAM user has been configured with a username and password, as well as access keys. You can also identify IAM users that may not have accessed resources in your AWS accounts recently, which may indicate that those accounts may not

be required anymore. Regularly deleting unwanted IAM user accounts is part of the security best practice.

22. D

    Permission boundaries enable you to define the maximum set of permissions that can be granted by an identity-based policy for an IAM user or IAM role.

23. C

    SCPs is a feature of the AWS Organization service that enables you to set the maximum set of permissions that can be defined for member accounts. You can also set policies to prevent the root users of member accounts from removing the membership to an organization management account once the invitation to become a member account has been accepted.

24. A

    Amazon S3 Standard-IA can be used to store objects that you are not going to frequently access, but at the same time, you have instant access to the data when you need it.

25. A

    You can create a resource policy with a condition statement that allows you to restrict the application of the policy based on a predefined condition, such as the corporate office network IP block.

26. D

    Amazon S3 Intelligent Tiering is ideal if you are unsure of what your object access patterns might be. Objects are automatically transitioned across four different tiers, two of which are latency access tiers, which are designed to move objects between frequently accessed and infrequently accessed tiers, while the other two are optional archive access tiers. For the infrequent access tier, if you do not access your objects for 30 days, then it transitions to the Amazon S3 Standard-IA storage class, which is cheaper. If you need to access the same objects again later, they are transitioned back to the Amazon S3 Standard storage class.

27. B

    To protect against accidental deletions or overwriting, Amazon S3 Versioning can be enabled. This service ensures that if someone tries to perform a delete request on an object without specifying the version ID, it will not be deleted. Instead, a delete marker will be added and the object will be hidden from view. You can then delete this marker to reenable access to the object. You should also consider setting a bucket policy so that not all users can perform delete requests.

28. A

    Amazon S3 **CRR** is used to asynchronously copy objects across AWS buckets in different AWS Regions. This feature can be used to fulfill compliance and regulatory requirements, which

may require you to store copies of data thousands of kilometers away for **Disaster Recovery** (**DR**) purposes.

29. C

    With SSE-KMS, you can encrypt your objects in Amazon S3. You can create and manage your **CMKs**, as well as benefit from the auditing feature, which shows when your CMK was used and by whom. This service integrates with Amazon CloudTrail to offer full auditing features.

30. B

    If you need urgent access to just a subset of your archives, you can opt for the Expedited retrieval option. Expedited retrievals are made available within 1 to 5 minutes for archives of up to 250 **megabytes** (**MB**).

31. A

    S3TA reduces this speed variability that is often experienced due to the architecture of the public internet. S3TA routes your uploads via Amazon CloudFront's globally distributed edge locations and AWS backbone networks. This, in turn, gives faster speeds and consistently low latency for your data transfers.

32. B

    The Amazon Snowball Edge Storage Optimized device offers a larger storage capacity and is ideal for data migration tasks. With 80 TB of HDD and 1 TB of **serial advanced technology attachment** (**SATA**) SDD volumes, you can start moving large volumes of data to the cloud. The device also comes with 40 vCPUs and 80 GB of memory.

33. B

    Amazon FSx File Gateway enables you to connect your on-premises Windows applications that need large amounts of storage to the cloud-hosted Amazon FSx service for Windows File Server with low latency connectivity. Amazon FSx File Gateway also supports integration with **Active Directory** (**AD**) and the ability to configure access controls using **ACLs**.

34. B

    NAT gateways help relay outbound requests to the internet on behalf of EC2 instances configured to use them. The NAT gateway replaces the source IPv4 address of your EC2 instances with the private IP address of the NAT gateway, thus acting as a proxy. Response traffic is then redirected by the NAT gateway back to the private IP address of the EC2 instance that made the original request.

35. B

    Security groups are stateful. This means that even if you have not configured any inbound rules, response traffic to any outbound requests will be permitted inbound by the Security

Group. Similarly, if you configured any inbound rules, outbound response traffic to any inbound traffic is permitted, without you having to explicitly create those outbound rules.

36. A

    A VPC peering connection is a private network connection between two VPCs. The service allows you to connect multiple VPCs so that instances in one VPC can access resources in another VPC over a private IP address space.

37. A

    The problem with VPC peering, when you're configuring multiple VPC to connect, is that every VPC must establish a one-to-one connection with its peer. This can quickly create complex connections that are difficult to manage. Route tables for each VPC also need to be configured for every peering connection.

    AWS Transit Gateway allows you to connect your VPCs via the gateway in a hub-and-spoke model, greatly reducing this complexity as each VPC only needs to connect to the Gateway to access other VPCs.

38. C

    Direct Connect is a service that enables you to connect your corporate data center to your VPC and the public services offered by AWS, such as Amazon S3, via a dedicated private connection that bypasses the internet altogether. The service enables you to achieve bandwidth connectivity of up to 100 Gbps.

39. B

    You can set up a **VPN** connection between your on-premises network and your VPC. This is a secure encrypted site-to-site tunnel that's established between two endpoints over the public internet. It offers AES 128 or 256-bit **IPsec** encryption, which means that you can transfer data between the two endpoints securely.

40. A

    Amazon Route53 can help you create alias records so that when a user types in a corporate domain-friendly name into the browser, it will direct the traffic to an AWS service, such as an ALB, giving access to the web application.

41. A

    Amazon Route 53 offers domain name registration. You can purchase and manage domain names such as `example.com` and Amazon Route 53 will automatically configure the DNS settings for your domains.

42. C

To offer high availability of your web application, you can host two copies of your resources ideally across different Regions. One set of resources will be designated as your primary resource and the other as a secondary resource. If the primary resource is offline, then users' requests are redirected to the secondary resource.

43. C

Amazon CloudFront is a **Content Delivery Network** (**CDN**) that helps you distribute your static and dynamic content globally over low latency connections. The service caches content at edge locations closer to where your users are accessing the website.

44. A

To launch an EC2 instance with a custom AMI that you have built in another Region, you need to ensure that you copy the AMI to that Region.

45. D

Accelerated Computing EC2 instance types are designed with hardware accelerators, or co-processors, to perform complex functions. They are best for processing complex graphics, number crunching, and machine learning.

46. D

A Dedicated Host is a physical host dedicated for your use alone and gives you additional control and management capability over how instances are placed on a physical server. In addition, dedicated hosts can help address certain third-party licensing terms that are based on a per-CPU core/socket basis.

47. A

On-Demand is ideal for users who need the flexibility to consume compute resources when required and without any long-term commitment. They are ideal for test/dev environments or for applications that have short spiky or unpredictable workloads.

48. D

Provisioned IOPS SSDs offering high-performance EBS storage is ideal for critical, I/O-intensive databases and application workloads.

49. D

Using an **All Upfront** payment option for your RIs means paying for the entire term of the RI upfront at the beginning of the contract. You do not get a monthly/hourly bill and you benefit from the maximum available discount. Furthermore, a 3-year commitment will offer a bigger discount than a 1-year one.

50. B

Amazon Lightsail is a VPS solution that comes pre-configured with common application stacks such as WordPress, Drupal, Plesk, LAMP, and your chosen operating system. You choose the size of the server and it comes preconfigured with SSD storage, an IP address, and more. The best part about Lightsail is that you have a fixed monthly fee based on the instance type and the associated operating system and applications that have been deployed.

51. B

The ECS Fargate Launch Type enables you to set up your ECS environment without having to spin up EC2 instances, provision and scale clusters, or patch and update virtual servers yourself. AWS will manage how the ECS tasks are placed on the cluster, scale them as required, and fully manage the entire environment for you.

52. B

Amazon Lambda is a serverless offering from AWS that allows you to run code and perform some tasks. Amazon Lambda is known as a **Function as a Service** (**FaaS**) solution that can be used to build an entirely serverless architecture comprised of storage, databases, and network capabilities where you do not manage any underlying servers.

53. B

Microsoft Windows-aware applications that need to share files can easily use FSx for Windows File Share, which offers support for the SMB protocol and Windows NTFS, **AD** integration, and **Distributed File System** (**DFS**).

54. A

Amazon EFS can be used by Linux-based EC2 instances as a centralized file storage solution. This is particularly useful when you have applications deployed across multiple EC2 instances that need to share common files. Amazon EFS can also be accessed from on-premises servers over a VPN or Direct Connect service.

55. D

When you launch a server (Windows or Linux), you must configure it to be associated with a key pair. This is an encrypted key where you will be able to use your private key to log in to Linux-based servers or decrypt the Windows administrator password using the AWS Management Console.

56. C

AWS Outposts is ideal when you want to run AWS resources with very low latency connections to your on-premises application or if you require local data processing due to any compliance and regulatory requirements. You can get AWS Outposts delivered to your local on-premises location as a 42U rack and can scale from 1 rack to 96 racks to create pools of compute and storage capacity.

57. A

AWS Batch can be used to run thousands of batch computing jobs on AWS for performing various types of analysis. AWS Batch will set up and provision the necessary compute resources to fulfill your batch requests. There is no need to deploy server clusters as AWS takes care of this for you.

58. B

Amazon EKS is designed to help you deploy, manage, and scale containerized applications using Kubernetes on AWS.

59. A

The primary advantage of using Amazon RDS over installing databases on EC2 is the fact that AWS manages all the compute and storage provisioning, as well as performing all management tasks on the database. This frees you up to focus on your application and the infrastructure components that host the database.

60. B

Amazon RDS offers a feature known as Multi-AZ where the primary (master) copy of your database is deployed in one Availability Zone and a secondary (standby) copy is deployed in another Availability Zone. Data is then synchronously replicated from the master copy to the standby copy continuously. If the master copy fails, AWS will promote the standby copy to become the new master and perform a failover.

61. B

Amazon offers a **Database Migration Service** (**DMS**) that can be used to migrate the data from one database to another. This migration can be performed from your on-premises network to the AWS cloud over a VPN connection or a Direct Connect connection. AWS DMS offers support for both homogeneous migrations, such as from MySQL to MySQL or Oracle to Oracle, as well as heterogenous migrations between engines such as Oracle to Microsoft SQL Server or Amazon Aurora.

62. B

Redshift Spectrum allows you to perform SQL queries against data stored directly on Amazon S3 Buckets. This is particularly useful if, for instance, you store frequently accessed data in Redshift and some infrequently accessed data in Amazon S3.

63. D

Amazon Aurora is an AWS proprietary database that maintains copies of the database placed across a minimum of three Availability Zones. Amazon Aurora is also five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases.

It also offers self-healing storage capabilities that can scale up to 128 TB per database instance.

64. C

    DynamoDB supports both key-value and document data models such as JSON. DynamoDB is a NoSQL database solution that offers a flexible schema and offers single digit millisecond performance at any scale.

65. A

    Amazon QLDB is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log owned by a central trusted authority. Amazon QLDB can maintain a history of all data changes.

Mock test 2

1. B

   In scenarios where you have a single RDS database instance deployed, your users are likely to experience a brief I/O suspension when your backup process initializes. By configuring your Amazon RDS database with Multi-AZ, the backup is taken from the standby copy of the database instead of the master. This will ensure that users do not experience any brief outages when trying to access the database.

2. A

   Amazon Elasticache for Redis is designed for complex data types, offers Multi-AZ capabilities, encryption of data, and compliance with FedRAMP, HIPAA, PCI-DSS, as well as high availability and automatic failover options.

3. C

   Amazon Redshift is AWS's data warehousing solution that is designed for analytics and is optimized for scanning many rows of data for one or multiple columns. Instead of organizing data as rows, Redshift transparently organizes data by columns. You can use standard SQL to query the database and use it with your existing BI tools.

4. A and B

   Detailed monitoring and use of Elastic Load Balancers will increase your EC2 instances' costs. This is because Elastic Load Balancers are not part of the free tier and you are charged based on each hour or partial hour that a load balancer is running and the number of **Load Balancer Capacity Units** (**LCUs**) used per hour. Furthermore, whereas basic monitoring is offered free of charge, detailed monitoring is a chargeable service.

5. B

ALBs are designed to distribute traffic at the application layer (using HTTP and HTTPS). Furthermore, with ALBs, you can have multiple target groups, allowing you to define complex routing rules based on the different application components. You can configure path-based routing, host-based routing, and much more. You can also configure Lambda functions as targets for your load balancer.

6. A

   Network Load Balancers are designed to operate at the fourth layer of the OSI model and can handle millions of requests per second. Network Load Balancers are designed for load balancing both TCP and UDP traffic and maintaining ultra-low latencies.

7. C

   Using a load balancer, you can direct incoming traffic to multiple registered EC2 instances across multiple Availability Zones within a given Region. This enables you to offer high availability in case any of the EC2 instances fails or even if an entire Availability Zone goes offline.

8. C

   You need to configure listeners to specific ports that you will accept incoming traffic on and the ports you will use to forward traffic to the EC2 instances.

9. B

   The nodes of an internal load balancer only have private IP addresses and allow communication between the web layer and the internal application layer. The DNS name of an internal load balancer can be publicly resolved to the private IP addresses of the nodes. Therefore, internal load balancers can only route requests from clients with access to the VPC for the load balancer.

10. A

    When configuring your Auto Scaling group, you can define the minimum and maximum size of your group. You can also choose to keep the size of the group to an initial size that does not expand the group size but ensures that you always have the exact number of EC2 instances running.

11. B

    Amazon Auto Scaling can help you provision new EC2 instances based on CloudWatch metrics that change according to the load on your instances. Similarly, when demand drops, you can configure Auto Scaling to terminate unwanted resources and thus save on costs.

12. D

    AWS Trusted Advisor is an online tool that can offer guidance on AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas. The service

quota (service limits) category of Trusted Advisor can notify you if you use more than 80% of a service quota for a specific service. You can then follow recommendations to delete resources or request a quota increase.

13. A

    The AWS ALB service provides integration with **Web Application Firewall** (**WAF**), which helps protect against common web exploits such as SQL injection and cross-site scripting.

14. A

    With the target tracking scaling policy, Auto Scaling will launch or terminate EC2 instances in the fleet based on the target value of a specific metric. The target tracking policy tracks the metric value and attempts to ensure the correct number of EC2 instances are running to meet that target value.

15. B

    Amazon **Simple Notification Service** (**SNS**) is a push-based messaging and notification system that can be used to allow one application component to send messages to another application component or directly to end users. So, Amazon SNS can be used to send out alerts when a particular CloudWatch metric crosses a threshold for a period and triggers an alarm.

16. A

    The Fanout scenario enables you to publish messages to an SNS topic for parallel asynchronous processing. You send the notifications to supported endpoints such as Kinesis Data Firehose delivery streams, Amazon SQS queues, HTTP(S) endpoints, and Lambda functions.

17. B

    Amazon **SQS** is a fully managed message queuing solution that enables you to decouple your application components into distributed systems and facilitates the design and architecture of microservices. A queueing system such as Amazon SQS can help different components of your application work independently. Queues can hold messages in the form of requests/tasks until capacity is available.

18. B

    FIFO stands for **First-In-First-Out** and its queues are designed to preserve the order of your messages, as well as ensure only one-time delivery with no duplicates.

    With FIFO queues, you can get a throughput at a rate of 300 transactions per second. If you use batching, you can get up to 3,000 transactions per second, per API method (`SendMessageBatch`, `ReceiveMessage`, or `DeleteMessageBatch`).

19. B

Amazon recommends using Amazon MQ for migrating applications from existing message brokers where compatibility with APIs such as JMS or protocols such as AMQP 0-9-1, AMQP 1.0, MQTT, OpenWire, and STOMP are required.

20. C

Amazon EventBridge is a serverless *event bus service* that allows you to stream real-time events from your applications to support targets such as Lambda functions, which can then be triggered to take some form of action. In the preceding example, EventBridge can trigger a Lambda function if someone tries to delete an object in your S3 bucket and some action can be taken in response to the event.

21. B

Amazon Step Functions enables you to define these workflows as a series of state machines that contain states that make up the workflow. These states make decisions based on input, perform some action, and produce an output to other states. Step Functions also allow you to integrate human interaction, particularly where manual intervention is required, and can run for up to 1 year.

22. C

You can configure CloudWatch Events with a rule to trigger a Lambda function at a defined schedule. You would need to create the Lambda function and then, in the rule settings for CloudWatch events, specify the Lambda function as a target to be triggered at the designated schedule.

23. C

Kinesis Data Analytics lets you query and analyze stream data in real time. You can use standard programming and database query languages such as Java, Python, and SQL to query streaming data as it is being ingested.

24. A

Amazon Athena is an interactive query service that can be used to analyze data in Amazon S3 using standard SQL. To set up the service, you need to specify the source S3 bucket and define a schema.

25. B

Amazon Kinesis Firehose is designed to capture, transform, and deliver streaming data to several AWS services, including Amazon S3 and Redshift in near real time. The service can also batch, compress, transform, and encrypt your data streams, thereby reducing storage usage and increasing security.

26. B

Amazon QuickSight is a serverless **Business Intelligence** (**BI**) service that can help you build interactive dashboards and embedded visualizations into your applications and web portals.

27. C

    AWS Glue is a fully managed ETL service that makes it easy for customers to prepare and load their data for analytics.

28. C

    Amazon EMR is a managed Hadoop framework that allows you to process vast amounts of big data. You can use open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto.

29. B

    Amazon CloudFormation is a solution that can help you design, build, and deploy your infrastructure using code. You can create templates that use a declarative approach to instruct CloudFormation to build a precise infrastructure repeatedly, as required, by your testing team. CloudFormation templates can also be configured to accept input parameters for environment-specific configurations and variations required in the build.

30. B

    AWS OpsWorks is a configuration management and orchestration service that enables you to provision resources such as servers both in the cloud and on-premises using Chef and Puppet. With OpsWorks, you can define service layers for your application stack such as the database layer, load balancer layer, and more.

31. A

    Amazon Elastic Beanstalk is a service that enables you to deploy your application without having to manually configure the underlying infrastructure that will support the application. You upload your code in a supported language and environment and AWS will provision the underlying infrastructure, such as the compute, storage, and network components, to support the application. Amazon ElasticBeanstalk will also enable you to specify how the underlying infrastructure components will be deployed – for example, you can specify the EC2 instance type and size that is deployed or enforce that a set minimum number of EC2 instances are deployed as part of an Auto Scaling group.

32. B

    In a multi-tier application architecture, backend operations such as application, middleware, or database operations are performed by the worker tier of your Elastic Beanstalk configuration. AWS Elastic Beanstalk will also provision an Amazon SQS queue to facilitate communication between the web services tier and the worker tier.

33. A and D

CloudFormation templates can be written in both JSON and YAML format. These are declarative markup languages that can help CloudFormaton provision infrastructure in your AWS account.

34. D

Memory is a custom metric because memory metrics are at the OS level and cannot be monitored by default. To ingest custom metrics, you need to use the CloudWatch agent or the **PutMetricData** API action to publish them to CloudWatch.

35. B

You can configure CloudWatch alarms to monitor a given resource metric, such as the average CPU utilization of an EC2 instance. If the metric crosses a specific threshold for a specified period, then the alarm can be triggered to take a certain action. The alarm only triggers if the threshold has been breached for a specified period.

36. B

VPC Flow Logs can capture information about the IP traffic going to and from network interfaces in your VPC. You can configure VPC Flow Logs to capture all traffic to the VPC, a specific subnet, or a specific network interface of an EC2 instance.

37. C

AWS CloudTrail stores event history from within the CloudTrail dashboard for every activity that occurs in your AWS account. You can create trails to store specific management events or data events and if you require more than 90 days' worth of event history.

38. C

AWS Config is a service that allows you to gain visibility into how your AWS resources are configured and deployed in your AWS account. This includes configuration information, as well as changes to those configurations over time. You can also use AWS Config to enforce specific configurations rules and ensure that you follow internal guidelines that fulfill compliance requirements.

39. A

AWS Systems Manager's Patch Manager enables you to automatically patch your EC2 instances that are comprised of security and application updates. Note that updates for applications on Windows servers are limited to those released by Microsoft.

40. A

AWS Systems Manager's Parameter Store enables you to provide sensitive information such as passwords and database strings as parameter values. These values can be stored or encrypted, and your application can be configured to securely retrieve these values as they are needed from the Parameter Store.

41. A

    The AWS Systems Manager Incident Manager service offers a management console to track all your incidents and notify responders of the impact, identify data that can help with troubleshooting, and help you get services back up and running.

42. B

    AWS Trusted Advisor analyzes your resources and how they have been configured and compares those configurations against security practices to identify opportunities to save money, improve system availability and performance, or address security concerns.

43. B

    The AWS Trusted Advisor service offers different levels of checks based on the AWS support plan that you have subscribed to. To access the full range of checks across all categories, you must be subscribed to either the Business or Enterprise Support plan. With either of these plans, you can also use Amazon CloudWatch Events to monitor the status of Trusted Advisor checks.

44. C

    The Reliability pillar also focuses on how quickly you can recover from failure based on your architectural design. This is because failures are bound to happen and your architecture must be able to recover from these failures swiftly. One key concept that you should also consider is that replacing failed resources is often better than trying to figure out why the failure occurred and then attempting to resolve the issue that caused the failure.

45. A

    When architecting solutions for the cloud, you must select the resource types and sizes based on your performance needs, while monitoring your resources consistently to ensure you maintain those levels of performance as per demand. Amazon CloudFront can help you improve performance by reducing the latency associated with accessing large amounts of content across the globe. It does this by caching content locally at edge locations as they are being accessed.

46. D

    The Cost Optimization pillar focuses on ensuring that you architect and build solutions in a manner that avoids unnecessary costs. At the same time, you want to be able to ensure that your applications are highly performant, reliable, operationally efficient, and secure. To achieve cost optimization, you should understand your spending patterns and analyze where the money is going.

47. A

Amazon RDS is a managed database service. The customer can provision databases and select the instance type and size to power the database. However, the customer cannot manage the instance itself as this is taken care of by AWS, which includes patching and installing database updates. In contrast, patching EC2 instances is the customer's responsibility as EC2 is not a fully managed service.

48. C

Compliance reports and agreements are available via a portal on AWS known as **AWS Artifact**. These reports include AWS **Service Organization Control** (**SOC**) reports, **Payment Card Industry** (**PCI**) reports, and certifications from accreditation bodies across different Regions.

49. D

As a customer, you need to follow the service policy for penetration testing, which includes permitted services and prohibited activities. Such prohibited activities are **Denial of Service** (**DoS**), **DDoS**, simulated DoS, and simulated DDoS.

50. B

With SSE-KMS, you create and manage **CMKs**, and you use these keys to encrypt data keys and your data. SS3-KMS offers additional features such as auditing capabilities and integrates with CloudTrail.

51. B

AWS CloudHSM is a dedicated **Hardware Security Module** (**HSM**) that allows you to generate and manage your encryption keys in the cloud. You are provided with dedicated FIPS 140-2 Level 3 validated HSM devices, placed in your VPC, that are fully managed for you by AWS.

52. D

AWS Shield is a fully managed service offering protection against DDoS attacks. AWS Shield Advanced offers additional protection against attacks on your EC2 instances, ELBs, CloudFront, Global Accelerator, and Route53 resources. The service also offers a dedicated AWS **Shield Response Team** (**SRT**) 24/7 to assist you in handling such attacks.

53. A

AWS WAF can help protect applications at layer 7 of the **OSI** model, which helps you monitor and protect traffic over HTTP and HTTPS. This allows you to protect your content from common web exploits, such as SQL injection and cross-site scripting.

54. A

Amazon Macie uses machine learning and pattern matching techniques to detect and alert on any sensitive data, such as **PII**, stored in Amazon S3.

55. A

Amazon Cognito enables you to set up identity and access control solutions for your web and mobile applications using standards such as OAuth 2.0, SAML 2.0, and OpenID Connect. With Amazon Cognito, you can create user pools and identity pools.

56. C

AWS GuardDuty is a threat detection service that can analyze and detect malicious activity against your AWS accounts and application workloads. The service can detect the use of exposed credentials, any communication with malicious IP addresses and domains, as well as irregular activities carried out in your AWS account.

57. C

Amazon Detective can extract time-based events such as logins, network traffic from AWS CloudTrail and Amazon VPC Flow Logs, as well as ingest your GuardDuty findings to determine the root cause of those security findings.

58. B

With the Migration Evaluator service, you can use the AWS Application Discovery service, the TSO Logic agentless collector, or third-party tools to discover and gain insights into your current compute, storage, and total cost of ownership. The agentless collector tool can analyze any on-premises resources that just require read-only access to your VMware, Hyper-V, Windows, Linux, Active Directory, and SQL Server infrastructure.

59. B

Spot EC2 instances are ideal for applications that are fault-tolerant, scalable, or flexible, and where your application can tolerate interruptions. Spot Instances can save you up to 90% on On-Demand prices and there is no upfront commitment.

60. D

Amazon S3 on Outposts offers durability and redundancy by storing data across multiple devices and servers hosted on your outposts. It is ideal for low-latency access, while also enabling you to meet strict data residency requirements.

61. C

Resource policies are designed to enable access to resources such as objects in an Amazon S3 bucket. This policy enables you to identify a principal that you grant access to. With resource-based policies, you can configure the principal as a wildcard (*), which denotes anyone, and enables you to grant anonymous access.

62. B

Amazon Route53 offers complete domain name registration services. When you choose a name to register, you do so under a **top-level domain** (**TLD**) such as `.com`, `.co.uk`, `.org`, or `.net`. If the name of choice under a particular TLD is not available, you could try a different TLD.

63. A

Amazon Rekognition is a service that uses machine learning to identify objects, people, text, scenes, and activities in images and videos, as well as to detect any inappropriate content. Amazon Rekognition can be used for various application solutions such as identifying people, or sensitive data such as **PII** in images and videos.

64. C

Elasticsearch is an open source full-text search and analytics engine that can analyze all types of data such as textual, numerical, geospatial, structured, and unstructured data. Amazon Elasticsearch offers integration with Kibana, which is a data visualization tool, and Logstash, which is an open source, server-side data processing pipeline.

65. C

Amazon WorkSpaces is an end user computing service that enables you to deploy virtual Linux and Windows desktops in the cloud. AWS manages these virtual desktops, including security patching and managing the operating system. With Amazon WorkSpaces, you can consider migrating away from your on-premises desktop infrastructure to a **Virtual Desktop Infrastructure** (**VDI**) solution.