CYBRARY

Study Guide

Amazon Web Services (AWS) Fundamentals

Shaun Balkum, Instructor

Created By:
Samuel Mitchell,
Teaching Assistant
July 2019

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

1

Module 1:
Introduction to AWS

CYBRARY

Lesson 1.1: Course Introduction

Skills Learned From This Lesson: AWS, Cloud Computing, AWS Certification, Course Overview

About the Instructor:

Shaun Balkum is an IT Consultant with nearly 20 years of IT experience and he currently holds 5 AWS certifications (Solutions Architect Associate, Certified Developer – Associate, Certified Developer – Associate, Solutions Architect – Professional and DevOps Engineer – Professional). The instructor's goal is to get you excited about AWS technologies and it's services.

This course will assist you in setting some of the foundational topics to advance in your AWS career.

This lesson introduces the following course objectives:

- Introduction to Amazon Web Services Fundamentals
- The AWS Management Console
- The AWS Core Services
- AWS Security - speaks to what aspect of security AWS is responsible for and what you will be expected to manage.
- AWS Technologies - Deeper Dive - explains how all the pieces are fitted together
- AWS Billing and Pricing - this area speaks to tracking and managing the cost of the AWS services and forecasting the future service expenses.
- Putting It All Together - this area you will utilize the various AWS technologies to understand how all the components work together.
- The Next step in your Cloud journey - the instructor will detailed his path to success in achieving his various AWS certifications.

The AWS has a free tier that can be leveraged to get familiar with the main AWS services in this course which can be access with the link below:
- https://aws.amazon.com/free/?nc2=h_ql_pr&all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc

Amazon has a certification Roadmap that can be accessed on the AWS certification website link below:
- https://aws.amazon.com/certification/?nav=tc&loc=3

Available AWS Certifications

aws certified
Updated May 2019

Professional

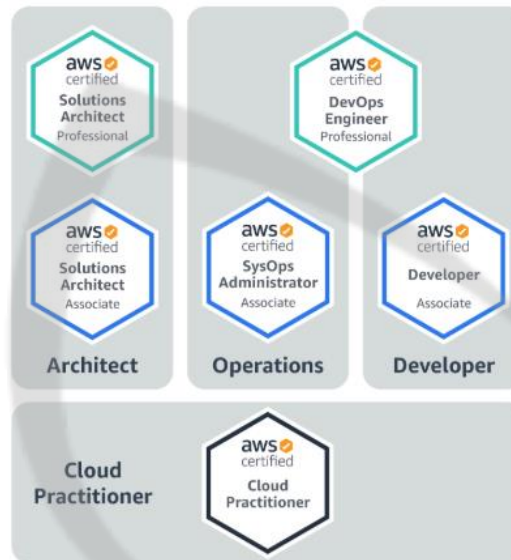**Two years** of comprehensive experience designing, operating, and troubleshooting solutions using the AWS Cloud

aws certified
Solutions Architect
Professional

aws certified
DevOps Engineer
Professional

Specialty

Technical AWS Cloud experience in the Specialty domain as specified in the **exam guide**

Associate

One year of experience solving problems and implementing solutions using the AWS Cloud

aws certified
Solutions Architect
Associate

aws certified
SysOps Administrator
Associate

aws certified
Developer
Associate

aws certified
Advanced Networking
Specialty

aws certified
Big Data
Specialty

AWS-Certification

Architect

Operations

Developer

aws certified
Security
Specialty

Foundational

Six months of fundamental AWS Cloud and industry knowledge

Cloud Practitioner

aws certified
Cloud Practitioner

aws certified
Machine Learning
Specialty

aws certified
Alexa Skill Builder
Specialty

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

4

Lesson 1.2: What is the Cloud?

Skills Learned From This Lesson: Cloud, Computing, Budget, IT Service Delivery, History, Administration

What is Cloud Computing?

- This is simply the on-demand delivery of compute power.
- This delivery could be in the form of databases, storage, networking, software, analytics, applications and other IT resources.
- It is delivered over the internet or "the cloud" as a pay-as-you-go pricing model.
- Cloud computing allows entities to provision precise services or resources needed on-demand without the upfront cost/capital expense.

A Brief History of Amazon Web Services (AWS)

There are many stories about how AWS started but the information that appears to be the most consistent was from interviews with Andy Jassy, the current CEO of Amazon Web Services. Mr Jassy explains that AWS was born roughly over a 3-year period between 2000 - 2003.

In 2000, AWS was attempting to launch a new e-commerce service over their existing e-commerce platform. This task was proven to be extremely difficult over their existing monstrous e-commerce platform. Amazon has been growing so rapidly between 1997 to 2000 that the company did not plan for such an exponential growth. Amazon did not have a truly independent development platform. Amazon just had a huge environment of inter-dependent platform systems.

To solve this problem, the Amazon software engineers introduced the concept of Decoupled services.

What are Decoupled services:

- It is services that does not depend on other services
- It involves the creation of well documented Application Programming Interfaces (API) which are communication protocols and subroutine definitions for building software tools

Unbundling FSI Value Chains

Monolithic Platforms   Decouple by Layering   Micro Services
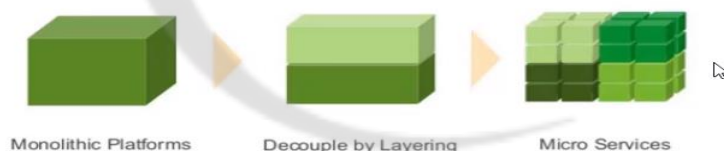
At first these APIs were only shared internally among Amazon developers. Teams will reuse other Amazon teams' APIs as building blocks for their own projects. At this point Amazon executives begin to understand that if their own teams can become far more efficient by sharing API, the thought came why not develop this concept into a business model. The idea was developed over a 3 years period.

In 2003, the executives at Amazon begin to envision an Operating System for the internet where a company can build products and services from scratch even from a college dorm or a kitchen table once the right tools are readily available. It is almost like a box of Legos.

In August 2006 Amazon Web Services (AWS) was launched with its first service offering being the Amazon Elastic Compute Cloud (EC2).

- EC2 is an online virtual machine used to allow developers to easily scale their web applications.

The idea was so new and swift that Amazon did not have a true competitor in the space until 2010 when Microsoft launched Project Red Dog which later became Microsoft Azure.

This is what helps to explains why Amazon continues to be the dominant player in cloud technologies.
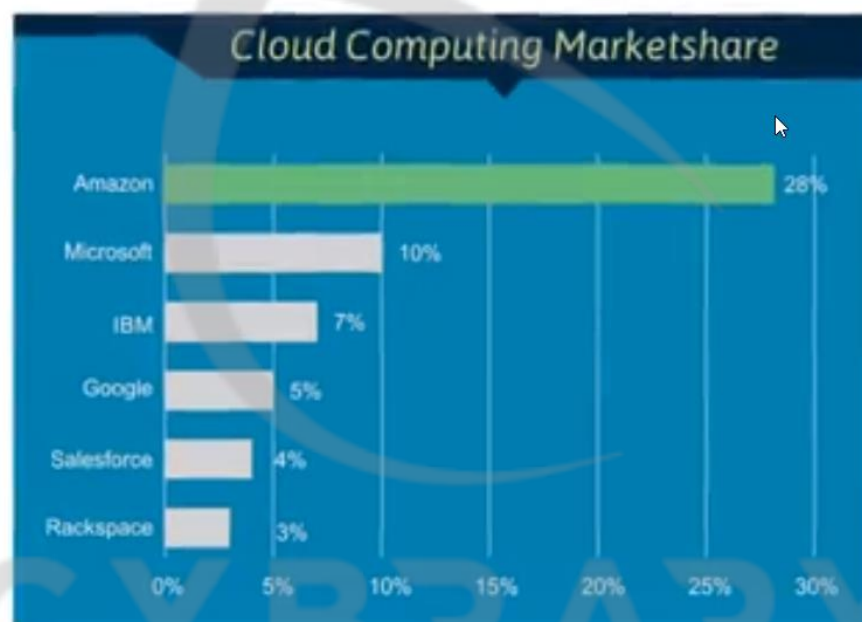
Type of Cloud Computing

There are several types of cloud models that have evolved to assist developers and IT departments to select the right solution for their needs. The different models offer varying levels of management, flexibility and control:

- **Infrastructure as a Service[1] (IaaS)**

- ○ It is a standardized, highly automated offering where compute, storage and network resources and capabilities are owned and hosted by a service provider
- ○ Offered to customers on-demand
  - ■ Customers are able to self-provision this infrastructure using a web console that serves as the IT operations management console for the environment.
  - ■ API access to the infrastructure can be offered as an option.

- **Platform as a Service (PaaS)**[1]
  - ○ It is a broad collection of application infrastructure (middleware) services (including application platform, integration, business process management and database services).

- **Software as a Service (SaaS)**[2]
  - ○ it is a model for the distribution of software where customers access software over the internet.
  - ○ A service provider hosts the application at its data center and a customer accesses it via a standard web browser.
  - ○ The SaaS vendor apply updates automatically without customer intervention.
  - ○ The service is purchased on a subscription basis.
  - ○ No hardware is required to be installed by the customer.

Type of Cloud Computing Deployment Model

- **Cloud**
  - ○ The entire application and supporting infrastructure is run in the cloud.
- **Hybrid**
  - ○ The applications are shared and run between cloud based and on-premise resources.
- **Private**
  - ○ Cloud computing resources are utilized primarily by a single business or organization.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

8

○ The resources may be located on the premises of the organization's data center or perhaps in a third-party co-location facility.

Methods of accessing the AWS services

- AWS Management Console
- Command Line Interface
- Software Development Kit (SDK)

Here is a quick preview of some of AWS Management Console services:

Compute services:
- Amazon EC2
- Elastic Block Store (EBS)
- Amazon Elastic Beanstack

Storage services:
- Amazon S3
- Amazon Elastic File System (EFS)
- Amazon Storage Gateway

Database services:
- Amazon Aurora
- Amazon RDS
- Amazon DynamoDB
- Amazon ElasticCache

Networking and Content Delivery services:
- VPC (Virtual Private Cloud)
  ○ This is one of the most important service offerings by Amazon. This is where you can build your own private segment of AWS cloud and launch your own AWS elements in a private virtual network that you create and manage.
- CloudFront
- Route 53
- Direct Connect

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

9

- Elastic Load-Balancing

Security Identity and Compliance services:
- These services allow you to create policies to secure access to your AWS resources, manage users and groups, provide key management services and Web Application Firewall)

Among the other services offered by Amazon are:
- Migration Tools
- Development and Management
- Analytics
- Artificial Intelligence (AI)
- Mobile
- Messaging
- Internet of Things (IoT)
- Desktop and App Streaming
- Gaming Development

Amazon service offerings are amazing and just continues to grow.

References:
1. *Gartner IT Glossary*
2. *Techopedia*

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

10

Lesson 1.3: Value of learning AWS

Skills Learned From This Lesson: AWS, Cloud Computing, Regions, Availability Zones

The AWS Cloud Value Proposition

- Amazon makes access to resources very easy via CLI, API and web interface
- The network and hardware is owned by the service provider

Benefits of AWS Cloud computing

- **Cost Savings**
  - AWS helps to reduce the capital cost of startups.
- **Global services**
  - The AWS services are available in multiple regions across the world.
- **Productivity**
  - It eliminates the following:
    - Staging a data center would typically require tons of manual labor such as racking and stacking hardware and cabling.
    - It will also require waiting on hardware shipping delivery and vendor support to commission some of this hardware before use.
  - It allows you time to focus on the most important task of development of products and services
- **Speed and Agility**
  - AWS can provide infrastructure in minutes
- **Security**
  - Amazon is responsible for the physical security of the Data center
    - They have built large-scale data centers for many years
    - Important attributes
      - No-descript facilities
      - Robust perimeter controls
      - Strictly controlled physical access
      - Two or more levels of two-factor authentication
    - Controlled, need-based access

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

11

- ■ All access is logged and reviewed
- ■ Separation of Duties
    - ● Employees with physical access don't have logical privileges
- ● **Performance**
    - ○ Business may benefit from the aggregation of the latest generation of computing hardware
    - ○ The number of users utilizing cloud services helps to deliver low costs, in pay as you go computing.

AWS Global Infrastructure overview

At the creation of this document, Amazon has the following global infrastructure:
- ● 21 Geographical Regions
- ● 66 Availability Zone

A Region provides several physical isolated Availability Zones that are connected via high throughput redundant low latency networking. All AWS Regions are totally isolated from other AWS Regions to provide higher availability.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

12

CYBRARY

Availability Zone provides AWS customers with the tools and resources to make all their applications, databases and compute resources faster and more efficient, reliable and scalable.

Startups on AWS: https://aws.amazon.com/solutions/case-studies/

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

13

CYBRARY

Lesson 1.4: Module 1 summary

Skills Learned From This Lesson: AWS, Cloud, Computing, Summary

In this module, you have learnt:

- What is the Cloud?

- How AWS was created

- An Introduction to AWS terminology and reviewed some of the core categories of its service offerings.

- Discussed the value proposition of using AWS

- Took a glance at the Global Infrastructure footprint of AWS

Please proceed to the next module to begin you AWS free tier.

Module 2:
What is the AWS
Free Tier?

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

15

Lesson 2.1: What is the AWS Free Tier?

Skills Learned From This Lesson: AWS, Free Tier, Cloud, Budget, Cost, Billing

What is the AWS free usage Tier?

- AWS offers a free, limited usage tier
- 12 months of free service for some categories
- After the free tier expires, you will go on the pay-as-you-go subscriptions
- It involves 15 GB of outgoing bandwidth aggregated across all services
- For more information please go to https://aws.amazon.com/free

What services are included in the Free Tier?

- Amazon EC2
    - 750 hours free
    - It is like a virtual machine in the cloud
- Amazon Elastic Load Balancing (ELB)
    - 750 hours free
    - It automatically distribution incoming application traffic across multiple targets such EC2 instances, containers or IP addresses
- Amazon RDS
    - 750 hours free
    - Makes it easy to set up and operate a relational database in the cloud
- Amazon ElasticCache
    - 750 hours free
    - It works as an in-memory datastore and cache
- Amazon Elastic Block Store
    - 30 GB of free ELB
    - It provides persistent block store for us with each EC2 instance in the cloud
    - Each EBS environment is automatically replicated within its own Availability Zone to protect you from component failure and offering high availability and durability.
- Amazon S3

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

16

- ○ 5 GB free standard storage
- ○ It is an object storage build to store
- ○ It is designed to deliver 9.99999999999% of durability
- Amazon DynamoDB
  - ○ 25 GB of storage free
  - ○ 25 units of read capacity free
  - ○ 25 units of write capacity free
  - ○ 200 million requests per month free
  - ○ It is a non-relational database that delivers reliable performance at any scale
  - ○ It is full managed, multi-region, multi-master database that provide consistent single digit milliseconds latency
  - ○ It offers built-in security, provides backup, restoration and in-memory caching
  - ○ It is like an Excel spreadsheet in the cloud
- Amazon SimpleDB
  - ○ 25 hours free
  - ○ 1 GB storage free
  - ○ Highly available no-SQL data store that offloads the work of database administration
- Amazon SWF
  - ○ 1,000 WorkFlow executions for free
  - ○ 10,000 activity tasks for free
  - ○ 20,000 workflow days for free
  - ○ It is a full managed state tracker and task coordinator in the cloud
- Amazon Simple Queue Service (SQS)
  - ○ 100,000 request of queue services for free
  - ○ It is a full managed message queuing service
  - ○ You can send, store and receive messages between software components at any volume or requiring other services to be available.
- Amazon SNS
  - ○ 100,000 requests
  - ○ 100,000 http notifications
  - ○ 100,000 email notification services
  - ○ It is a highly reliable, durable, secure, full-managed publisher/subscriber messaging services

- ○ The publisher system can send out messaging systems to a large number of subscribers' endpoints for parallel processes.
- Amazon CloudWatch
  - ○ 10 CloudWatch metrics
  - ○ 10 alarms
  - ○ 1 million API request
  - ○ It is a monitoring and management services
  - ○ It collects monitoring and operation in the form of logs, metrics and events providing a uniform view of AWS resource, application services that run on AWS and your own on-premise servers.
- Amazon CloudFront
  - ○ 50 GB data transfer out
  - ○ 2 million http/https request from Amazon CloudFront
  - ○ It is fast content delivery network services that securely delivers data, videos, applications and APIs to customers global with low latency, high transfer speeds and all within a developer friendly environment.

Who is eligible for the free tier?
- It is available to everyone
- To start using the AWS Free Tier
  - ○ Create an AWS account https://aws.amazon.com/free
  - ○ Subscribe to the service you want to use
  - ○ Enter your credit card information.

Are there any charges in the Free Tier?
- The free tier applies to a selective number of participating AWS services up to a specific maximum amount of usage per month as mentioned earlier.
- When an account goes over the free tier usage limits, the standard AWS services rates will be billed to the credit card.
- An account may be billed for a service that is not covered under the free tier. An example will be if you are running an Amazon EC2 instance type m1.small rather than a t1.micro instance.
- Your usage is calculated each month across all regions and automatically applied to your bill.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

18

What is a Billing Alarm?
- A **Billing alarm** allows you monitor your estimated AWS charges using Amazon CloudWatch.
- When you enable the monitoring of estimates charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data via the Amazon Simple Notification Service (SNS).
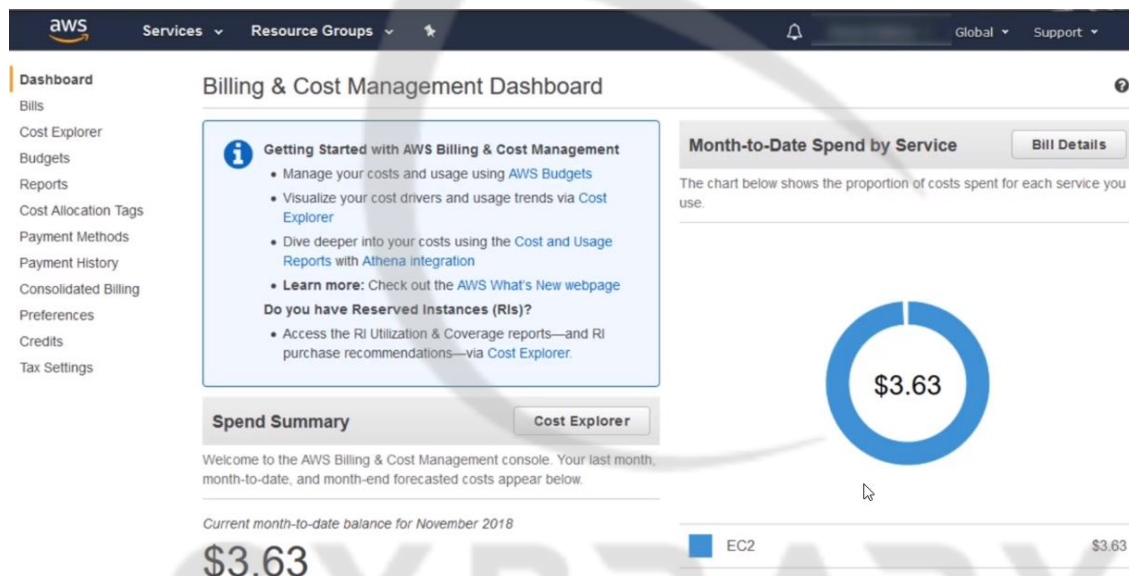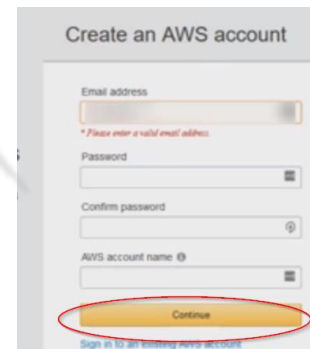- The alarm triggers when your account billing exceeds the threshold that you specified.

Figure 2.1.1 Billing & Costing Management Dashboard

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

19

CYBRARY

Lesson 2.2: Setting up your AWS account

Skills Learned From This Lesson: Account creation, Cloud, AWS, Internet, MFA

Account creation step-by-step

Please note a credit card will be required to setup an AWS account

1. Go to Amazon Web Service portal https://aws.amazon.com
2. Select **Create a Free account**
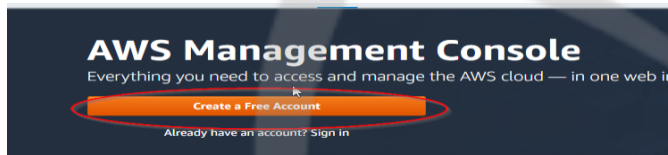
3. Enter the required account information:
   a. **Email address**
   b. **Password**
   c. **AWS account name** (this will be your full name)
4. Select **Continue**
5. On the Contact Information page:
   a. Select Account Type:
      i. Professional - select this type if it is for an organization
      ii. Personal - select this type if it is for your own use
   b. Enter the rest of the details
6. Select **Create Account and continue**
7. Enter your credit card information
8. On the next page, enter your phone to verification and wait for a call and provide Amazon with the code on screen.
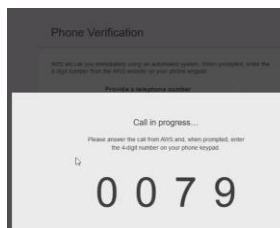
9. Once verified, you can continue
10. Select the **Basic Plan**

---
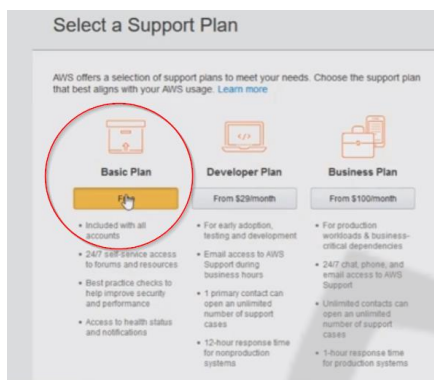
11. You can *Personalize your Experience* but it is not necessary
12. Go straight ahead and log into the **AWS portal**
13. After logging into the portal, I suggest that you set up **Multi-factor Authentication (MFA)** to increase the security of your account.

To Set up Multi-factor Authentication (MFA)

1. From the AWS Management Console, search for *MFA*
2. Select **IAM**
3. On the IAM Dashboard, select **Activate MFA on your root account**
4. Select **Manage MFA**
5. Select **Continue to Security Credentials**
6. Extended **Multi-factor Authentication**
7. Select **Activate MFA**
8. Select **Virtual MFA device** (this option we will use *Google Authenticator* on our Android smartphone. You can use any other supported Authenticator on any type device.)
9. Select **Continue**
10. You will choose either to **scan the QR code** using the camera or enter the **code** in the Authenticator
11. You will enter two **MFA code** to verify.
12. That is, it, you are now set up with MFA and your account is secure.

Lesson 2.3: Setting up your AWS Billing Alert

*Skills Learned From This Lesson: **Billing, AWS, Alerting, Cloud, CloudWatch, Charges***

Use Case for Billing Alarm

In this lesson, we are going to learn how to create a billing alarm. Although majority of our time will be spent in the Free tier, it is possible that we may incur some charges that are not a part of the Free tier account or if our uses exceed the Free tier usage limits.
To mitigate against having surprise billing charges, we will create a billing alarm.

Billing Alarm overview

- In AWS, we can create a billing alarm to monitor our estimated usage charges. This is accomplished in AWS using Amazon CloudWatch.
- The estimate charges are calculated and sent to AWS multiple times per day as billing metric data to Amazon CloudWatch.
- This data includes the estimated charges for every service in AWS that we used in addition to the estimated overall total of our AWS charges.
- The alarm triggers when our account billing exceeds the threshold that we specified.
  - It only triggers when actual billing exceeds the billing threshold.
 - It does not use projects of estimated charges that we have used so far for the month.

CYBRARY

How do I set up a Billing Alarm?

1. Log into your AWS Management console https://aws.amazon.com
   a. Enter your credentials
   b. Then enter you MFA code from your device
2. After logging into the console
3. Under the Account, select the **Billing & Costing Management Dashboard**
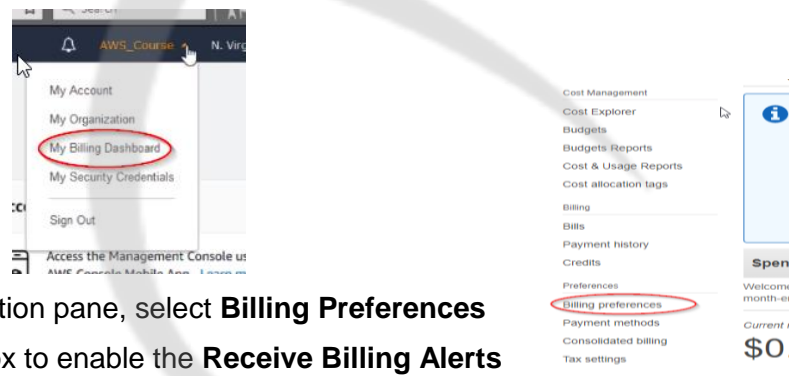
4. In the navigation pane, select **Billing Preferences**
5. Tick checkbox to enable the **Receive Billing Alerts**
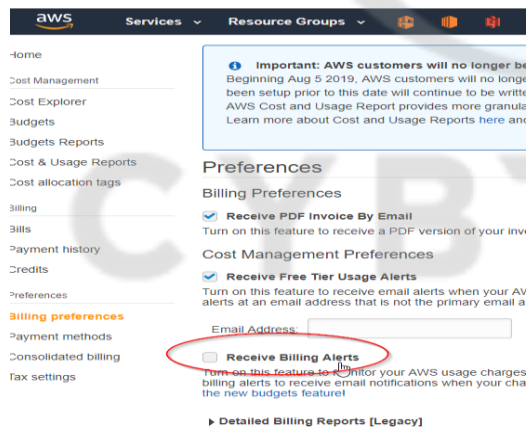
Note: once billing alert is enabled it cannot be turned off.

6. Click **Save Preferences**

7. Click **Manage Billing Alerts**

8. It takes us to the CloudWatch Dashboard, select **Billing**

9. Select **Create Alarm**

10. Scroll down to **Conditions** and select your criteria

11. Enter your US $ value threshold

12. Select **Next**

13. Under **Notification**

    a. Select **In Alarm**

14. For option **Select an SNS topic**:

    a. select **Create new topic**

    b. In **Create a new topic** textbox: [A billing alert name]

    c. For **Email endpoints that will receive the notification**: [enter your email address]

15. Select button: **Create Topic**

16. Click **Next**

17. Enter a **Name** and **Description** for the Billing Alert

18. Click **Next**

19. Review the settings and then select **Create Alarm**

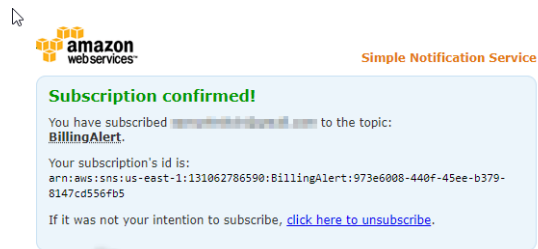20. You will get a verification email for confirmation, go to the email and confirm it.

AWS Notification - Subscription Confirmation ▶ Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com>
to me ▼

You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:131062786590:BillingAlert

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

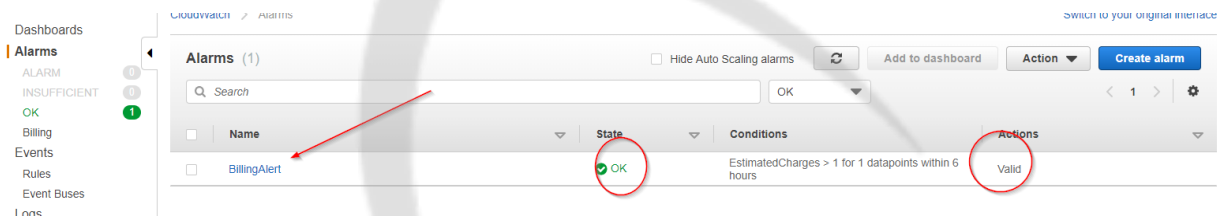21. It will take you to the **SNS confirmation** page

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

24

Subscription confirmed!

You have subscribed █████████████ to the topic: **BillingAlert**.

Your subscription's id is:
arn:aws:sns:us-east-1:131062786590:BillingAlert:973e6008-440f-45ee-b379-8147cd556fb5

If it was not your intention to subscribe, click here to unsubscribe.

22. You can refresh the **CloudWatch Alarm Dashboard**, it should be all OK.

You have successfully created your first billing alarm.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

25

Module 3:
Identity and Access Management (IAM)

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*
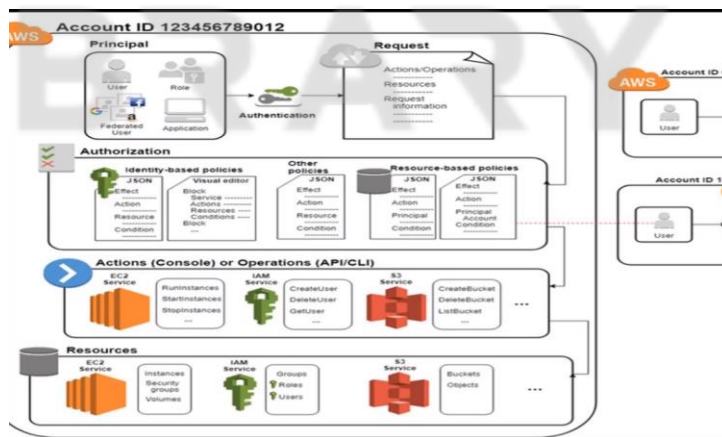
26

CYBRARY

Lesson 3.1: What is IAM (Identity and Access Management)?

Skills Learned From This Lesson: IAM, Authentication, Web services, EC2, Monitoring, MFA

What is IAM?

- AWS Identity and Access Management (IAM) is a web service that enables us to configure access control to AWS resources.
- When we first created our Amazon account, we were able to access all our AWS services by just using our email address, this is known as our root account.
- AWS recommends as a best practice that we not use our root account for daily use but rather that we create an IAM user account instead.
- We should still ensure that we store our root user credentials in a safe place.

IAM Features

- Shared access to your AWS account
  - we can grant permission to other user accounts without sharing our credentials.
- Granular permissions
  - we can grant minimum permissions to user accounts
- Secure access to AWS resources for applications that run on Amazon EC2
- Multi-Factor Authentication (MFA)
- Identity federation
  - Is a feature that can grant temporary access to accounts from other systems
- Identity information for assurance
  - CloudTrail is an auditing service.
  - CloudTrail can be enabled to work with IAM to provide us with logs of who made request for resources within our AWS account.
- It is free to use

Accessing IAM

We can access IAM in four (4) different ways:
- The AWS Management console -this is the method we will use during the course.
- The AWS Command Line Tools
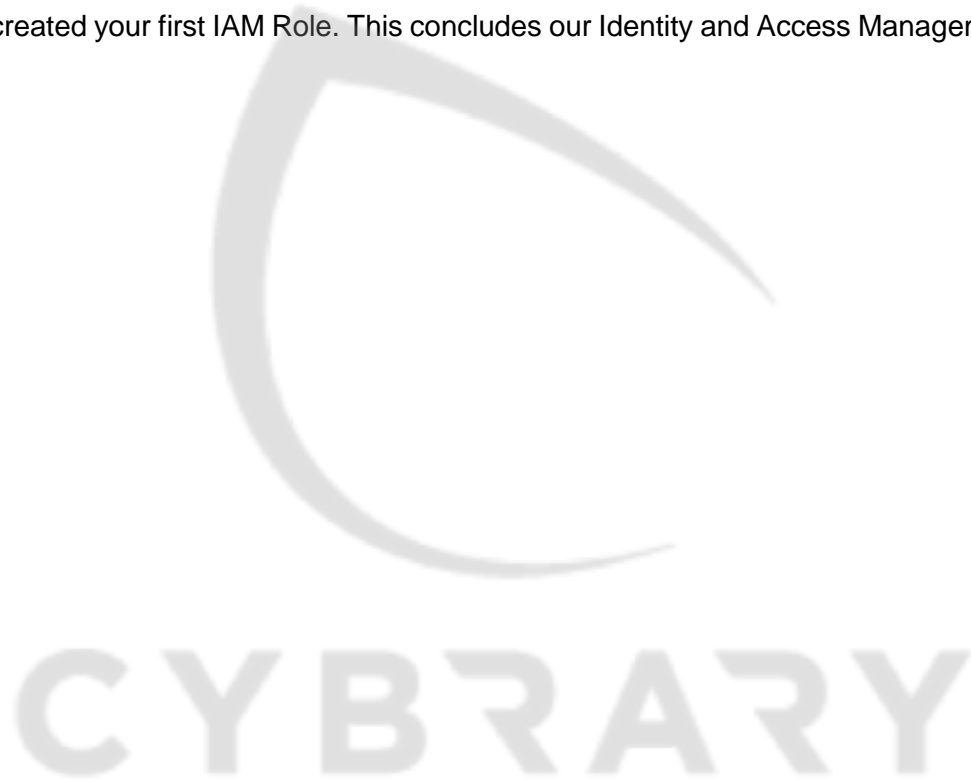
Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

27

- ○ The AWS provide two types of tools:
  - ■ AWS CLI
  - ■ AWS tools for Windows PowerShell
- The AWS SDK (Software Development Kits)
  - ○ AWS provides SDKs and sample codes for popular programming languages platforms such as: Java, python, ruby, .Net, IOS, Android, etc.
- The IAM HTTPs API
  - ○ A developer might access an application using the IAM via the https protocol.

How Does IAM works?

There are some new terms that we need to get familiar with to better understand the IAM processes.

- **Resources** - contains the user, role, group and policy objects that are stored in IAM. We are able to add, edit and remove resources from IAM.
- **Identities** - These are IAM resource objects that is used for the purpose of identifying and grouping. These objects include user, role and groups.
- **Entities** - these are the IAM resources objects that AWS uses for AWS authentication. These will include users and roles. Roles can be assumed by IAM users in our or in a different account as well as users federated through a web identity service such as SAML (Security Assertion Markup Language)
- **Principal** - person or application that uses an entity to sign in and make requests to AWS resources.

Lesson 3.2: What is an IAM Role?

Skills Learned From This Lesson: IAM Role, Accounts, Security, AWS, Trust Relationship

Definition of IAM Roles

AWS definition of IAM Roles are a secure way to grant permissions to entities that you trust.

- IAM Roles are like a substitute teacher who is given permission to act in the absence of the permanent teacher.
- IAM Roles can be delegated permission to resources
- IAM Roles can grant permission to other AWS users.

Type of trust entities for IAM role

- A**WS service**- relating to services such as EC2, Lambard
- **Another AWS account** for your company or 3rd party
- **Web Identity** - for login services such as Facebook or Google account
- **SAML 2.0 Federation** - this will link with company authentication system such as LDAP

IAM Role Properties

- **Permission** - shows the rights granted to this role
- **Trusted relationship** - displays trusted entities who can assume this role
- **Access Advisors** - this show what or who is accessing this role and when
- **Tag** - use to set identifiable information to use for tracking who and what is assuming it
- **Revoke Sessions** - remove all sessions currently using this role.

Creating an IAM Role

For this demonstration, we are going to create a role for an EC2 instance

1. Go to the *IAM Dashboard*
2. Select **Roles**
3. Select **EC2**
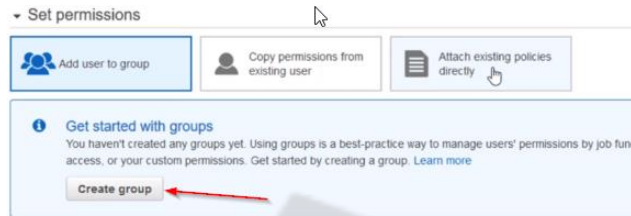
Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

29

4. Search for *EC2F* and select ***AmazonEC2FullAccess***

5. Select **Next**

6. Give the **Role name** and **description**

7. Click **Finish**

You have created your first IAM Role. This concludes our Identity and Access Management.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

30

CYBRARY

Lesson 3.3: Setting up IAM

Skills Learned From This Lesson: IAM, Security, Group, Password Policy

Setting up an IAM user account

1. Log into the AWS Management console
2. From the AWS Console Dashboard, Under the **Find Services**, search for *IAM and press Enter*
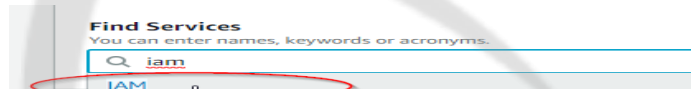
3. Select **Users** from the left option
4. Select **Add Users**
5. Enter your desired username

6. Select the Access type - **AWS Management console access**

7. Enter a custom password or select **auto-generate password**

8. Select **Next Permission**

---

9. Click **Create group**

10. Enter the information
    ○ Group name: *CybraryFullAccess*
    ○ Select Policy name: **AdministratorAccess**
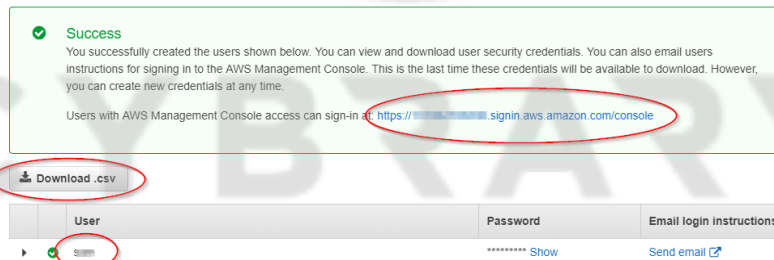11. Click **Create group**
12. Click **Next Tag**
13. Click **Next Review**

14. Click **Create user** after you have reviewed the IAM user account information
15. A URL with the account number is provided to allow the IAM user to sign in to AWS
    ○ https://*xxxxxxxxx*.signin.aws.amazon.com/console
16. Select **Download CSV** to the csv file with the password to send to the user.
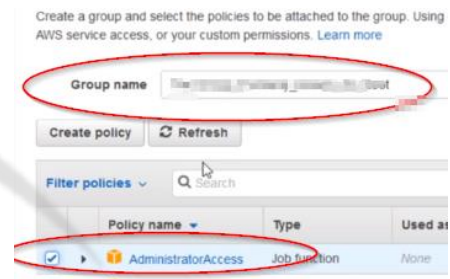
Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

32

Assigning User to Groups

1. Click on the user account
2. Select **Groups** tab
3. Click **Add users to group**
4. Search for the group and select it
5. Click **Add to Groups**

Applying an IAM Password Policy

1. Select **Account Setting**
   a. Here you will be able to apply the password policy
   b. By default, users are allowed to change their own password

- It is best practice to assign users to groups and apply the permissions to the group.
- AWS allows the administrator to send the IAM user credentials straight to the user's email from the console.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

33

Module 4:
Simple Server Storage (S3)

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

34

CYBRARY

Lesson 4.1: What is AWS S3

Skills Learned From This Lesson: S3, Monitoring, Storage, Backup, Cloud

What is Amazon S3?

- S3 stands for Simple Storage Service is an object storage
- Amazon refers to S3 as the storage for the internet
- S3 has 9.99999999999% of data durability

S3 Use Case

- Build applications that relies on internet storage
- Backup and archiving
- Content storage
- Static website hosting
- Disaster recovery

S3 Storage and Object Limitation

- S3 has an unlimited storage size
- The maximum size of individual object is 5TB
- Maximum size for a single upload is 5 GB
- For any file larger than 100 GB, it should be uploaded using the AWS multi-part upload feature

Amazon S3 Performance

- Access Amazon S3 from within the same Region is very fast.
- S3 is optimized to mitigate most server-side latency
- S3 is built to support virtually any number of web applications
- If S3 receives multiple requests from multiple applications simultaneously then the automating scaling and aggregate combined throughput will typically outperform most standalone servers or clusters.

Amazon S3 concepts

- **Buckets**
  - It is a container for objects stored in S3
  - It can be created from the AWS console, Command Line Interface (CLI) or programmatically using the AWS SDK.
  - By default, we can create 100 buckets
  - There is no limit on the number of objects stored in a bucket
  - We can associate each bucket with an Access Control Policy (ACL)
  - This policy will control the creation, deletion and numeration of objects within our bucket
- **Objects**
  - It is a simple key value store
- **Key** is the name we assigned to an object. We use the object key to retrieve the object in our bucket
- **Version ID** is a string that Amazon S3 generates when we add an object to or bucket
- **A Value** - is the content that we are storing. An object value can be any sequence of bytes. Objects can range in size from 0 to 5 TB.
- **Metadata** - is a set of name-value pairs that we can use to store information about our objects.
  - We can assign user-defined metadata to our objects
  - Amazon S3 assigns system-metadata to our objects that it uses for management purposes
- Amazon S3 supports Access Control List (ACL) bucket policies and user-based access control.
- Amazon S3 stores data in at least 3 Availability Zones in which each AZ has up 8 physical data centers.
- Versioning - protects the data from unintended overwrite.

S3 Storage Classes

S3 offers a variety of storage classes that are designed for various use cases:
- **S3 Standard**
  - It is used for general purpose storage of frequently accessed data
- **S3 Intelligent Tiering**
  - It is for data that has unknown or changing access pattern

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

36

- **Standard IA & One-Zone Standard IA**
  - It is used for less frequently access data
- **Amazon Glacier and Amazon Glacier Deep Archive**
  - It is used for long term data archiving

Object Lifecycle Management

We can configure Object Lifecycle Management to assist us with storing our objects cost effectively. A Lifecycle configuration is a set of rules and actions that we can defined that S3 then applies to a group of objects.

There are two types of actions:
- Transition Standard - which defines when objects move to another storage
- Expiration lifecycle Policy - tell when object expires. S3 deletes expired objects for us.

Versioning support

For more information on AWS Storage Pricing, please check this link: https://aws.amazon.com/s3/pricing

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

37

CYBRARY

Lesson 4.2: Create a S3 Bucket

Skills Learned From This Lesson: S3, Bucket, Storage, Cloud, AWS, HTTP, DNS

Access S3 from Console

Search for **S3** from the AWS console
1. Press **Enter** to go to **S3**
2. Select **Create Bucket**
3. Enter the Bucket name
    - The name must be DNS-complaint
    - The name must be lowercase
    - The name must be unique in AWS
    - The name must between 3 and 63 characters long
4. Select a **Region** where the bucket will be hosted.
5. You can copy the bucket from an existing one
6. Select **Next**
7. Under **Properties** the following options are available:
    - For option **Versioning**
        - Note once enabled, it cannot be versed only disabled.
    - **Server access logging**
    - **Object level logging**
8. Click **Next**
9. For **Set Permissions**
    - **Block All Access** checked (Note: By default, the bucket is private)
10. Select **Next**
11. Click **Create Bucket**

Upload and File to S3 Bucket

1. Click on the **Bucket**
2. Click **Upload**
3. Click **Add files**
4. Browse for the file
5. Click **Upload**

6. Click on the files to see its properties

S3 Bucket Properties

- **Versioning** - keeps multiple versions of an object in the same bucket
- **Server access logging** - set up access log records that provide details about access requests
- **Static website hosting** -host a static website, which does not require server-side technologies
- **Object-level logging** - record object-level API activity using CloudTrail data events feature (additional cost)
- **Default encryption** - Automatically encrypt objects when stored in Amazon S3 Advanced settings
- **Object lock** - prevents objects from being deleted
- **Tags** - use to track your cost against projects or other criteria
- **Transfer acceleration** - enable fast and easy and secure transfers of files to and from your bucket
- **Events** - receive notifications when specific occur in your bucket
- **Requester pays** - the requester will for requests and data transfer

S3 Bucket Permission

- Public Access Settings
- Access Control List
- Bucket Policy
- CORS configuration

S3 Bucket Management

- Lifecycle
- Replication
- Analytics
- Metrics
- Inventory

Lesson 4.3: Create a Static S3 Website

Skills Learned From This Lesson: Website, Internet, S3, Storage, Cloud, Hosting

Hosting Static website in S3

1. For the **AWS Console**
2. Go to **Amazon S3**
3. Click **Create Bucket**
4. Enter the Bucket name: **my-first-static-website**
5. Select **Create Bucket**
6. Click on the Bucket name
7. Select **Properties** tab
8. Click **Static website hosting**
9. Select **Use this bucket to host a website**
10. Enter information:
    - Index document: **index.html**
    - Error document: **error.html**
11. Click **Save**
12. Exit to the S3 Dashboard

Make S3 Bucket Public

1. Highlight the Bucket name
2. Click on Edit **Public access settings**
3. Uncheck **Block All Public Access**
4. Click **Save**
5. Type *confirm*
6. Click **Confirm**

Create a Bucket Policy

1. Click the Bucket name

2. Select Permissions
3. Select Bucket Policy
4. In the Bucket policy editor (json syntax), enter json script below

Json script	explanation

{
  "Version":"2012-10-17",
  "Statement":
   [{
      "Sid":"PublicReadGetObject",
      "Effect":"Allow",
      "Principal":"*",
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::wiztechtalk/*"]
   }]
}
	Version of json we are running
	
	The policy says anyone is allowed to get to the objects in our bucket my-first-static-website.

5. Click **Save**
6. Exit back to S3 dashboard

Upload our content to S3 Bucket

1. Create the following html files
   a. index.html

```
<html>
        <title>
                <head> Welcome Cybrarians!</head>
        </title>
        <body>
                <div align="center">
                        <h1>Welcome Cybrarian to our First Static S3 Site!!</h1>
                        <img src="welcome.jpg">
                </div>
        </body>
</html>
```

   b. error.html

```
<html>
        <title>
                <head> Error Cybrarians!</head>
        </title>
        <body>
```

```
                     <div align="center">
                             <h1>Uh oh... Cybrarian, there appears to be a problem!</h1>
                             <img src="error.jpg">
                     </div>
          </body>
</html>
```

2. Go to S3 Dashboard
3. Select the bucket name
4. Click **Upload**
5. Click **Add files**
6. Browse for the index.html and error.html
7. Select **Upload**
8. Tick box to highlight all files

9. Select **Action → Make public**

10. Click **Make public**

Test Website

1. Select Properties tab (for the bucket)
2. Select Static website hosting
3. Click on Endpoint URL link
   a. http://bucketname.s3-website.us-east-2.amazonaws.com/
4. You should see the Welcome page
5. Use the URL link with any characters at the end e.g.
   a. http://bucketname.s3-website.us-east-2.amazonaws.com/gsgsgg
6. You should get the error page

CYBRARY

## Lesson 4.4: Enabling Versioning on Bucket

Skills Learned From This Lesson: Versioning, S3, Cloud, Storage, Bucket, Website, Hosting

Versioning Overview

- It enables an object to maintain multiple versions of the same object.
- When an object has been uploaded to the S3 bucket before versioning was enabled, the version ID will be null
- When versioning is enabled it cannot be turned off only suspended

Enabling Versioning

1. Go to **S3 Dashboard**
2. Click on the Bucket name
3. Select **Properties** tab
4. Select **Versioning**
5. Select **Enable versioning**
6. Select **Save**
7. Versioning is now enabled on our bucket
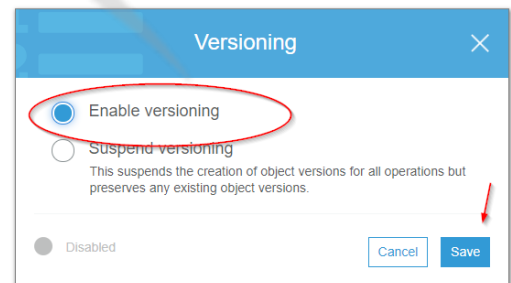
Listing the Versions of the File

1. Click the bucket name
2. Beside **Versions**, Select **Show**
3. You will see the other versions for each file
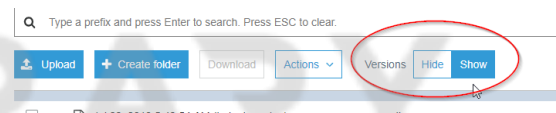
Deleting a Version of a File

1. Ensure the **Versions** option is set to **Show**
2. Select the file version you want to delete
3. Select **Action → Delete**
4. Select **Delete** to confirm

Module 5:
Elastic Cloud Compute (EC2)

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

44

CYBRARY

Lesson 5.1: EC2 Overview

Skills Learned From This Lesson: EC2, Cloud Computing, Storage, EBS, Compute, Pricing

What is Amazon EC2?

- EC2 provides us with scalable computing capacity in the Amazon Web Services (AWS) cloud.
- An EC2 instance will eliminate the requirements for us to spend money on hardware up front
- EC2 provides the opportunity to configure networking, security and manage our storage to support the business needs.
- EC2 enables us to handle changes in requirements
- Aids in forecasting requirements
- Amazon Machine Images (AMI) are preconfigured templates of our instances
- EC2 provides secure login information for our instances using key pairs
  - The public key is stored in AWS
  - The private key is stored by us

There are two types of storage volumes:

- Instance store volumes - non-persistent store that deletes the data when the instance is stopped or terminated
- Amazon Elastic Block Store (EBS) - the data is kept after the instance is stopped or terminated
- Regions and Availability Zones

Instance Types categories:

- General Purpose - Amazon EC2 A1 instances
- Compute Optimized - C5 instances are optimized for compute-intensive workloads: gaming, machine deep learning, AI
- Memory Optimized - used for memory intensive applications such as High-performance databases
- Accelerated Computing - commonly used for machine learning

- ○ Storage Optimized - HDD-based local storage, deliver high disk throughput, and a balance of compute and memory.

Amazon EC2 pricing

- ○ It is free for a year
- ○ Four ways to Pay:
  - ■ On-Demand - pay as we go, per hour or seconds
  - ■ Reserved instances - provide us with a discount of (up to 75%) compared to On-Demand instance pricing
  - ■ Amazon EC2 Spot instances - allow us to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price
  - ■ A Dedicated Host is a physical EC2 server dedicated for our use.
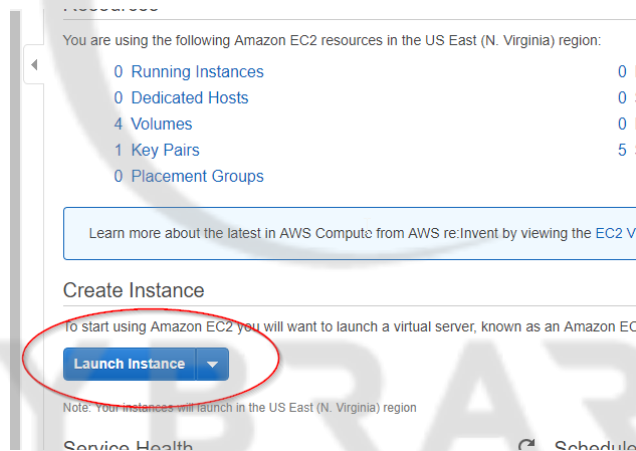
CYBRARY

Lesson 5.2: Create your first EC2 Instance Part 1

Skills Learned From This Lesson: Security, Compute, Storage, Virtualization, Imaging, Firewall, Networking
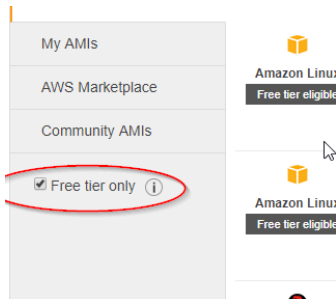
There are two types of Amazon Machine Image (AMI): Hardware Virtual Machine (HVM) and Paravirtual (PV). The differences are how they boot.

Launching an EC2 instances

1. From the AWS Console
2. Search for **EC2** and enter
3. Click on **Launch Instance**

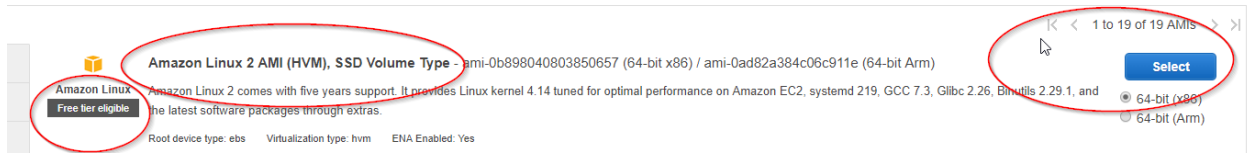4. Tick **Free tier only** checkbox

5. Select **Amazon Linux 2 AMI (HVM)**

6. Choose instance types: **general purpose t2.micro**

7. Click **Next Configure Instance Details**
8. Accept the default and click Next to Add Storage

The root volume is like the C drive and it is deleted when the instance is terminated

9. Click **Next Add Tag** to accept the default

The tag helps you to identify the various EC2 instances which can be group for use with other features in AWS.

10. Select **Add Tags**
    a. Enter Key: **Cybrary_ec_demo**
11. Click **Next Configure Security Group**

The security group is basically our firewall for EC2

12. Select **Create a new security group**
13. Enter the security group name and description: **Cybrary_DEmo_DMZ**
14. Select **Add Rule**: **HTTP** and **HTTPs**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select f

Assign a security group: ○ Create a **new** security group
○ Select an **existing** security group

Security group name: Cybrary_DEmo_DMZ

Description: launch-wizard-1 created 2019-07-28T07:15:03.162-05:00

Type ⓘ	Protocol ⓘ	Port Range ⓘ
SSH ▼	TCP	22
HTTP ▼	TCP	80
HTTPS ▼	TCP	443

Add Rule

15. Click **Review and Launch**

16. Select **Launch**

When we launch it expects us to choose an existing key pair or create a new one. As a quick analogy, let us think of the key pair as lock box and a key. The lock box represents the public key while the private key can compare to the key that opens the box.

17. Select Creating a new key pair

18. Enter key pair name:

Cybrary_key

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair ▼

Key pair name

Cybrar_key

Download Key Pair

19. Select **Download Key pair**

AWS will generate a private key in a text file.

You have to download the **private key file** (*.pem file) before you can continue. Store

This will be the key that we use to access the EC2 instances

20. Check: I acknowledge having access to the private key.

Choose an existing key pair ▼

Select a key pair

Cybrar_key ▼

☑ I acknowledge that I have access to the selected private key file (Cybrar_key.pem), and that without this file, I won't be able to log into my instance.

Cancel | Launch Instances

AWS wants to ensure we have the private key before launching our EC2 instance.

21. Select **Launch Instance**

22. Scroll down and select **View Instances**

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

50

CYBRARY

Lesson 5.3: Create your first EC2 Instance Part 2

Skills Learned From This Lesson: Linux, SSH, EC2, Private key

Overview

In this lesson we are going to connect to own EC2 public instance using a SSH client on a Linux (ubuntu) box. We are then going to set up a web server using this session.

Interacting with EC2 Instance using a Linux box

1. Create a directory for the ssh key

    mkdir SSH_Keys

2. Show that the directory was created

    ls

3. Move the private key to the directory

    mv private_key.pem SSH_Keys/

4. Change the directory

    cd SSH_Keys/

5. List all files in directory again

    ls

6. Making the key read only elevated privileges

    sudo -s
    chmod 400 private_key.pem

---

7. Log into the EC2 using ssh

    ssh ec2-user@ipaddres_of_EC2 -I private_key.pem

Creating the web server on the public EC2 instance

1. Installing apache on the EC2 instance

    yum install httpd -y

2. Run the system updates

    yum update -y

3. Create a landing page for our directory

    cd /var/www/html
    ls
    nano index.html

4. Enter some html code
5. Close the file: **CRTL+X**
6. Save the file: **SHIFT+Y, Enter**
7. Start the web server service

    services httpd start

8. Open a web browser
9. And type the IP address of the EC2 instance
10. Success!!

CYBRARY

<u>Lesson 5.4</u>: Use Putty for your EC2 Instance

Skills Learned From This Lesson: Windows, SSH, PPK, Compute, Cloud, PuTTY

PuTTY is a free terminal client that runs on Windows and it is very lightweight and easy to install.
PuTTYgen is an add-on tool for putty that allow you to generate the PPK file from the PEM private key file type.

Installing PuTTY

1. Open the browser
2. Search for **putty**
3. Select the link that begins with **"chiark"**
4. Select the package that is based on your Operating System bit version (32-bit or 64-bit)
5. Download the package
6. After package is downloaded, run the installer
7. Accept all the defaults of the installer
8. It is recommended to copy the **putty** and **puttygen** from the installer folder to your **Desktop** to make it easily accessible since it will be used often.

Relaunching the EC2 instance created from the last lesson

1. Log into AWS at https://aws.amazon.com
2. From the **AWS console** search for **EC2**
3. For the **EC2 dashboard**, select the **"Running instances"**
4. Right click the instance and select **Start**
5. Select **Yes Start**

Convert the EC2 instance private key to use with PuTTY

1. Open **puttygen**
2. Select **Load** and navigate to the **.pem** file. (select All Files (*.*) to show the .pem file)
3. Select the .**pem** and open it
4. Select **OK**
5. Select **Save** private key
6. Enter a filename with **.ppk** extension

Using Putty to connect to the EC2 instance

1. Open **PuTTY**
2. Enter Host Name: ec2-user@EC2Instance_IPAddress
3. Select Connection type: **SSH**
4. Copy host name and paste in **Saved Sessions**
5. Under **Category**: expand **SSH** and select **Auth**
6. Under **Authentication** parameters
7. Browse and select private key file .**ppk**
8. Go back to **Session** and select **Save**
9. Select the **ec2** saved session and select **open**
10. Prompted that **private key is not cached**, select **Yes**
11. You are successfully connected

<u>Lesson 5.5</u>: Automating EC2 Bootstrap (downloadable files available as resource)

Skills Learned From This Lesson: Bash, Scripting, EC2, Web Server, Cloud, Automation, Security

Create an HTML file for the landing page

1. HTML file template

```
<!DOCTYPE html>
<html>
        <head>
                <title> Put The Title Here </title>
        </head>
        <body>
                <h1> Put the Header of Body here </h1>
                This is where the body of information goes.
        </body>
</html>
```
2. Save HTML file name with extension *.html

Create new S3 Bucket

1. Log into AWS and go to S3 Dashboard
2. Select Create Bucket
3. Enter bucket name of your choice
4. Select Create bucket

Upload HTML file that was created into the new S3 Bucket

1. Go to S3 and select the Bucket
2. Select Add file and browse for HTML file

Create an IAM Role for EC2 instance

5. Go to **IAM Dashboard**
6. Select **Roles**
7. Select **Create Role**
8. Select **EC2**

9. **Next Permissions**
10. Under **Policy Filter** for **S3** and select **AmazonS3FullAccess**, then **Next**
11. Enter a **Role name** and **description**
12. Select **Create Role**

Write a bash script to automate our EC2 security updates and launch our web server

1. Go to **EC2 dashboard**
2. Select **Launch instance**
3. Select **Amazon Linux 2 AMI**
4. Select instance type **t2.micro**
5. Under configure instance details
   a. Go down to **IAM role** and select role created previously from dropdown
   b. Go to **Advanced Details**
      i.   User data: **as text**
      ii. Enter the following script:

Bash script	Description
#!/bin/bash/	Path to bash interpreter(called sha-bang)
yum install httpd -y	Install web server
yum update -y	Run security update
aws s3 cp s3://[yourbucketname]/your_htmlfilename] /var/www/html/	Copy html file from s3 to web server directory
service httpd start	Start web server
chkconfig httpd on	Check web server

      iii. Add **Storage**
      iv. **Add Volume** and the accept defaults
      v.   Configure security groups and select previously created group from previous lesson
      vi. Select **Review and launch**

---

vii. Use **existing private key pair**

viii. Select **launch**

ix. Once the EC2 instance is running

x. Select the instance, copy the IPv4 public IP address

xi. Browse to the public IP address to test the web server

xii. You will now see the html web page

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

57

Module 6:
Virtual Private Cloud (VPC)

Brought to you by:
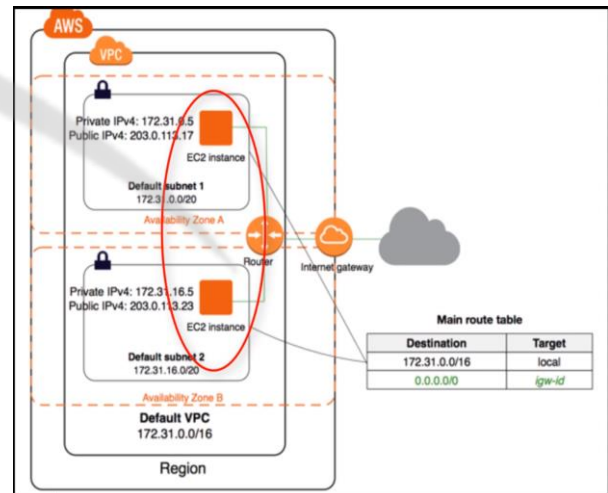
CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

58

CYBRARY

Lesson 6.1: VPC Overview

Skills Learned From This Lesson: VPC, Private Cloud, Networking, Subnetting, Gateway, NAT, VLSM

What is a VPC (Virtual Private Cloud)?

1. **Amazon VPC**
   a. Enables us to launch AWS resources into a virtual network that we define.
   b. It resembles a traditional data center network
   c. is the network portion of the EC2 instance
2. Each AWS Region is supply with a default VPC.
3. The default VPC IPv4 CIDR is **172.31.0.0/16**
4. Each subnet **172.31.0.0/20** resides in its own Availability zone
5. The **Internet Gateway** has two purposes
   a. To provide internet access to the VPC subnets
   b. To provide NATing to the private subnets
6.

IP Address VLSM and CIDR reference link:
- https://cidr.xyz
- http://www.subnet-calculator.com/cidr.php
-

Components of VPC

1. Subnets in each AZ are unique with /20
2. **Internet Gateway**
   a. Connect component to internet
   b. Provides NAT

3. **Security Group** – this is the firewall for the EC2 instances
4. **Network ACL** - is an optional layer that is similar to the security group but controls traffic in and out of the VPC
5. **DHCP Options Sets** - this setting is used to set the DHCP configuration for the VPC

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

60

Lesson 6.2: Create a custom VPC Part 1

Skills Learned From This Lesson: VPC, Architecture, Design, Subnet, Security, EC2, Networking

The remaining lessons in module 6 will take you through the steps of creating a custom VPC as seen in the diagram Figure 6.2.1 below.

Figure 6.2.1 - Virtual Private Cloud (VPC) Design Diagram

The first task is to create our Virtual Private Cloud (VPC):

Creating our Cybrary VPC:

1. Login to aws.amazon.com
2. From the **AWS Management Console**
3. Under **Find Services**, search for *VPC* and click on **VPC**
4. Under the **VPC Dashboard**, click **Your VPCs**
5. Click **Create VPC**
6. Enter the VPC information:
    - Name: *Cybrary_VPC*
    - *IPv4 CIDR block:*   *10.0.0.0/16*
    - *IPv6 CIDR block:*   *No IPv6 CIDR Block*
    - *Tenancy:*   *Default*
7. *Click **Create***
8. Click **Close**

The next step is to create our subnets for both our public and private networks within the VPC.
This task is similar to dividing our company (VPC) into departments (Subnets).

Creating our public subnet:

1. Under the **VPC Dashboard**, click **Subnets**
2. Click **Create subnet**
3. Enter the following field:
    - Name: **10.0.10.0_public_us-east-1a**
    - VPC*:   **Cybrary_VPC**
    - Availability Zone: **us-east-1a**
    - IPv4 CIDR block: **10.0.10.0/24**
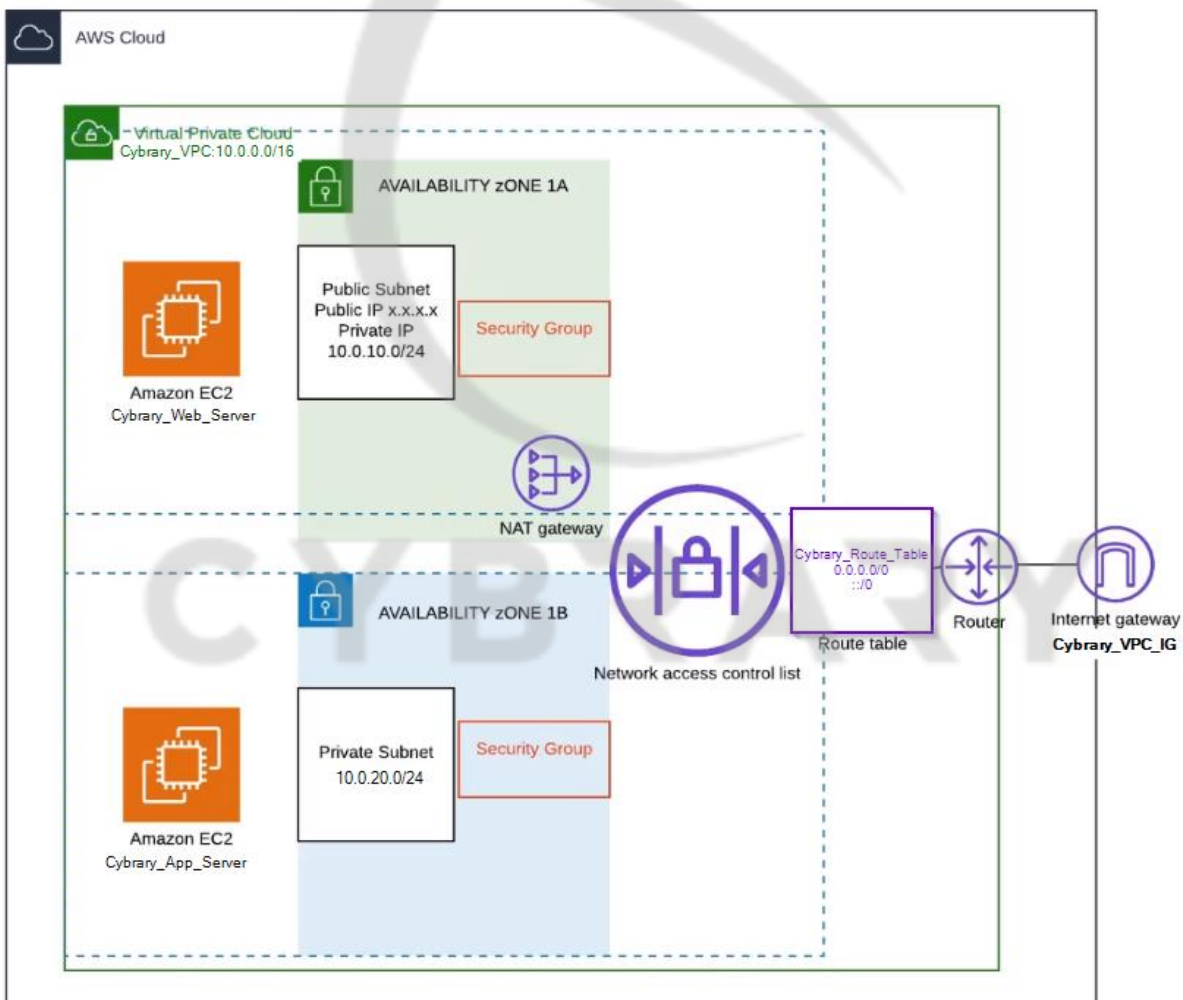
Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

62

4. Click **Create**
5. Click **Close**

Creating our private subnet:

1. Click **Create subnet**
    - Name: **10.0.20.0_private_us-east-1b**
    - VPC*: **Cybrary_VPC**
    - Availability Zone: **us-east-1b**
    - IPv4 CIDR block: **10.0.20.0/24**
    - IPv6 CIDR block: **Don't Assign IPv6**
2. Click **Create**
3. Click **Close**

Now we are going to create our Internet Gateway which is a virtual route that connects a VPC to the internet.

Creating our Internet Gateway:

1. Under **VPC Dashboard**, click **Internet Gateways**
2. Click **Create internet gateway**
3. Enter the gateway information:
    - Name: **Cyrary_VPC_IG**
4. Click **Create**
5. Click **Close**

Now the Internet Gateway has been created, we need to attach it to the VPC that it will provide internet service for.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

63

Attaching Internet gateway to our VPC:

1. Under **Internet Gateways**
2. Highlight the gateway **Cyrary_VPC_IG**
3. Click on menu **Actions**
4. Then select **Attached to VPC**
5. Select VPC **Cybrary_VPC**
6. Click **Attach**

Now the internet gateway **Cybrary_VPC_IG** is assigned to the VPC **Cybrary_VPC**.

Note: AWS by default creates a main route table which is internet facing that is associated with the subnets created in our VPC. This default behavior can present a potential risk for the resources in our VPC. Based on our design objective (Figure 6.2.1), we want to have one private subnet which is not accessible via the internet. To accomplish this objective, we will need to create our own Route Table to get this task done.

Creating our own Route Tables:

1. Under the **VPC Dashboard**, click **Route Tables**
2. Click **Create route table**
3. Enter the following properties:
   ○ Name: **Cybrary_Route_Table**
   ○ VPC: **Cybrary_VPC**
4. Click **Create**

There is an important point to note is that, the route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
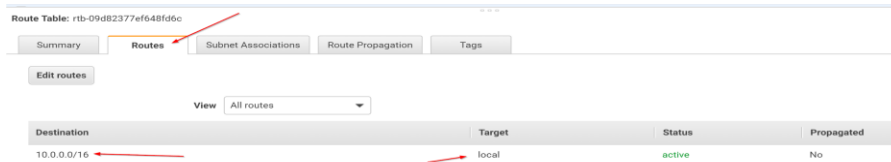
If you check the Routes under the new Route Table as seen below:

CYBRARY

You will notice that only the VPC subnet 10.0.0.0/16 is listed which means that this VPC will not know how to get to the internet. To correct this, you will need to add a default route 0.0.0.0/0 and point it to the Internet Gateway created earlier.

Adding the default route to the Route Table:

1. Highlight the Route Table **Cybrary_Route_Table**

2. Click menu **Actions** → select **Edit routes**

3. Click **Add route**

4. Add the following route:

   ○ Destination: **0.0.0.0/0**

   ○ Target: **internet gateway** → Cybrary_VPC_IG

5. Click **Save routes**

6. Click **Close**

Now, we need to associate the public subnet to the Route Table that has the internet gateway assigned to it since it is now in the main route table.

Associating Public subnet to new Route Table:

1. Under **VPC Dashboard**, click **Subnets**

2. Select the public subnet (*10.0.10.0_public_us-east-1a*)

3. Click menu **Action**

4. Select **Edit route table association**

5. Select route table information:

   ○ Route Table ID: *Cyrary_Route_Table*

---

6. Click **Save**
7. Click **Close**

Now the subnet will have internet access but to make the instances in this subnet accessible from the internet, you will need to set the auto-assign public IP address for this subnet.

To Auto-assign Public IP Address to any of the instance in the public subnet:

- With the same subnet highlighted

- Click **Action** → select **modify auto-assign IP settings**

- Auto-assign IPv4: tick **enable auto assign public IPv4 address**

- Click **Save**

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

66

<u>Lesson 6.3</u>: Create a custom VPC Part 2

Skills Learned From This Lesson: Cloud, EC2, Networking, Storage, Compute, SSH, HTTP, Web server, Internet, Firewall, VPC

Note: Please refer to the <u>Figure 6.2.1 for the VPC design diagram</u> for the overall objective.

In this lesson, we are going to launch our EC2 and build out our security groups.

Building our EC2 instance for public subnet (Internet facing web server):

1. From the AWS Management Console
2. Search for EC2
3. Select EC2
4. From the **EC2 Dashboard**, click **Launch Instance**
5. On the left, tick **Free tier only**
6. Select AMI: **Amazon Linux 2 AMI (HVM), SSD Volume Type**
7. Select Instance Type: **t2.micro (free tier eligible)**
8. Click Next:Configure Instance Details
9. Configure the following instance settings:
    a. Number of Instances: 1
    b. Network: Cybrary_VPC
    c. Subnet: 10.0.10.0_public_us-east-1a
    d. Auto-assign Public IP: Use subnet Settings(enable)
    e. IAM role: EC2_Can_Call_S3 (if not present continue)
    f. Expand Advanced details:
        i. User data: As text

Script	Description
#!/bin/bash	Shag-bang + path of bash script
yum install httpd -y	Installing the apache server
yum install update -y	Install updates
Aws s3 cp s3://your-bucket-name/index.html /var/www/html/ --recursive	Copy index.html to web hosting root

Service httpd start	Start up the apache server
Chkconfig httpd on	Check the status of the web server

10. Next **Add storage**
11. Click Add New Volume
12. Select Volume Type: EBS (use default)
13. Click Next: Add Tags
14. Click Add tags

Key	Value
Name	Cyrary_Web_Server

15. Click Next:Configure Security Group
16. Use the security group parameters:
    ○ Assigned a security group: select create new security group
    ○ Name and description: Cybrary_SG_Web_server

Type	Protocol	Source
SSH	N/A	Anywhere
HTTP	N/A	Anywhere
HTTPS	N/A	Anywhere
Custom ICMP	Echo Reply	Anywhere

17. Click **Review and Launch**
18. Click **Launch**
19. Select Choose an existing key pair
20. Select key pair **Cyrary_DMZ** (if none is present, select create a new pair with this name and ensure to download key pair before proceeding)
21. Tick: I acknowledge
22. Click **Launch instances**
23. Scroll down, click **View Instances**

Follow the same steps above to create the second EC2 instance for the private subnet with the following settings:

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

68

Building our EC2 instance for my private subnet (App server):

1. From the AWS Management Console
2. Search for EC2
3. Select EC2
4. From the **EC2 Dashboard**, click **Launch Instance**
5. On the left, tick **Free tier only**
6. Select AMI: **Amazon Linux 2 AMI (HVM), SSD Volume Type**
7. Select Instance Type: **t2.micro (free tier eligible)**
8. Click Next: Configure Instance Details
9. Configure the following instance settings:
   a. Number of Instances: 1
   b. Network: Cybrary_VPC
   c. Subnet: 10.0.20.0_private_us-east-1a
   d. Auto-assign Public IP: Use subnet Settings(disable)
   e. IAM role: EC2_Can_Call_S3 (if not present continue)
10. Next Add storage
24. Click Add New Volume
25. Select Volume Type: EBS (use default)
26. Click Next: Add Tags
27. Click Add tags

Key	Value
Name	Cyrary_App_Server

28. Click **Next: Configure Security Group**
29. Use the security group parameters:
    ○ Assigned a security group: select create new security group
    ○ Name and description: Cybrary_SG_App_server

Type	Protocol	Source

| SSH | N/A | Anywhere |

30. Click **Review and Launch**
31. Click **Launch**
32. Select Choose the same private key pair
33. Select key pair **Cyrary_DMZ**
34. Tick: I acknowledge
35. Click **Launch instances**

Please ensure to store the private key pair in a save location because you are going to need this key to connect to the EC2 instance.

That is, it for this lesson and we continue in the next lesson.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

70

Lesson 6.4: Create a custom VPC Part 3

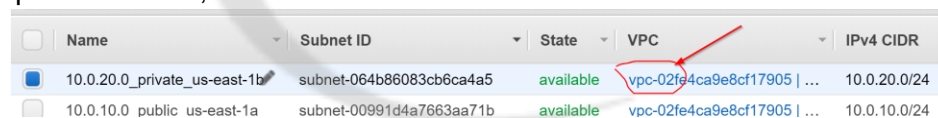*Skills Learned From This Lesson: VPC, Networking, EC2, Computing, Security Groups, Private key, SSH*

Note: Please refer to the Figure 6.2.1 for the VPC design diagram.

In this lesson we are going to connect to the public EC2 instance through which we will connect to our private EC2 instance.
In the last lesson, the private subnet was left in the default VPC (main), we need to edit the default VPC to facilitate communication with the public subnet.
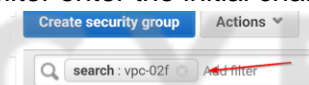
We will need to edit the Security group of the default VPC to configure this option:

1. First, we need to get the VPC identification
2. Under the VPC **Dashboard**, select **Subnets**
3. For the private subnet, make note of VPC name initial characters

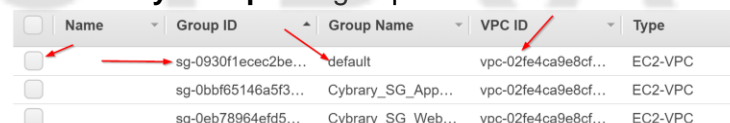|	Name	Subnet ID	State	VPC	IPv4 CIDR
☑	10.0.20.0_private_us-east-1b	subnet-064b86083cb6ca4a5	available	vpc-02fe4ca9e8cf17905 | ...	10.0.20.0/24
☐	10.0.10.0_public_us-east-1a	subnet-00991d4a7663aa71b	available	vpc-02fe4ca9e8cf17905 | ...	10.0.10.0/24

4. Click **Security Group**
5. In the filter enter the initial characters *vpc-02f* and press **Enter**
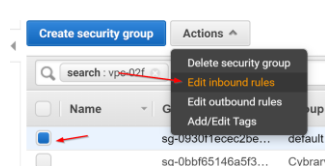
Create security group | Actions ▾

🔍 search : vpc-02f ⊗ Add filter

6. Select the **Security Group** with group name default

	Name	Group ID	Group Name	VPC ID	Type
☐		sg-0930f1ecec2be...	default	vpc-02fe4ca9e8cf...	EC2-VPC
☐		sg-0bbf65146a5f3...	Cybrary_SG_App...	vpc-02fe4ca9e8cf...	EC2-VPC
☐		sg-0eb78964efd5...	Cybrary_SG_Web...	vpc-02fe4ca9e8cf...	EC2-VPC

7. Select **Action → edit inbound rules**

Create security group | Actions ▲

🔍 search : vpc-02f ⊗

Delete security group
Edit inbound rules
Edit outbound rules
Add/Edit Tags

	Name	G	up
☑		sg-0930f1ecec2be...	default
☐		sg-0bbf65146a5f3...	Cybrary

8. Click **Add rule**:
    a. Type: **All TCP**
    b. Source: sg-xxxxxx (default)
9. Click **Save rules**
10. Click **Close**

Accessing the EC2 public instance:

1. Go to the **EC2 Dashboard** and get the public IP address of the EC2 public instance.

2. Under **Resources**, select *Running instances*

3. Select the EC2 instance *Cybrary_Web_Server*

4. Under description, search for IPv4 Public IP

5. Copy the **IP address** to Clipboard

6. Login to linux that will be used to connect to EC2 instance

7. open ssh ec2-user@ip_address [private-key-file.pem]

8. Click **Yes** to accept.

Note that it is not practical to constantly applying the private key to ssh session whenever you want to connect to your EC2 instance. An option of storing the private key on the server is not safe as it creates a security risk. In-addition, applying the private key to the public EC2 instance will not allow you to connect to the private EC2 instance without transferring the key. With these limitations in mind, there is a solution to use SSH forwarding agent. This method allows you to store the key in memory and then it forwards it to the second instance from memory (this method is demonstrated from linux).

Using Linux client:
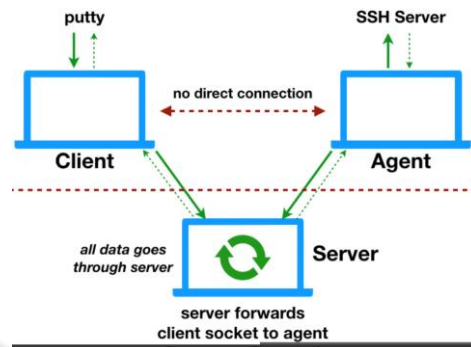
1. ssh -add **Cybrary_DMZ.pem** (add key to memory)
2. ssh-add -l (list the key in memory)
3. ssh -A ec2-user@ipaddress (archive key in memory)
4. You have logged into the EC2 public instance

We are now going to connect to the private EC2 instance through public EC2 instance (Bastion host)

What is a Bastion host, it is a computer that is accessible public which is used to access other computers within a private subnet. See diagram outlining this connection method. This is a security best practices since we only access the computer through the jump host.
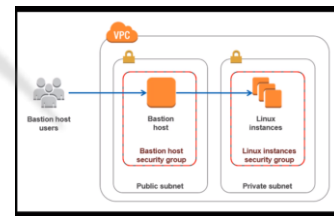
Connecting to our private EC2 instance:

1. Go to the **EC2 Dashboard**
2. Get the private ip address of the EC2 instance
3. Then go on the bastion host
4. Enter cmd: ssh -A ec2-user@private_ip-address
5. You are connected.

CYBRARY

Lesson 6.5: Create a custom VPC Part 4

Skills Learned From This Lesson: NAT, Gateway, Networking, VPC, EC2, IP address, Protocol, Security

Note: Please refer to the Figure 6.2.1 for the VPC design diagram.

What is the NAT Gateway?

The Network Address Translation Gateway is a highly available AWS managed service that makes it easy for us to connect to the internet from our EC2 instances that are located within our private subnet.

NAT Gateway features:

- Built-in Redundancy for High Availability
- NATing
- It used Elastic IP Address
- Capable of 10 Gbps of bursty TCP, UDP and ICMP traffic

In this lesson we are going to connect the private EC2 instance to the Internet using the NAT Gateway.

Please note that the NAT Gateway will incur charges due to the Elastic IP. Also the NAT Gateway is not included in the Free Tier subscription. You can continue this lab session with this in mind or just follow through.

1. Go to **EC2 Dashboard**
2. There should be two instances
1. Go to **VPC**
2. Select **NAT Gateway**
3. Create NAT Gateway
4. Assigned it to the public subnet (*10.0.10.0_public_us-east-1a*)
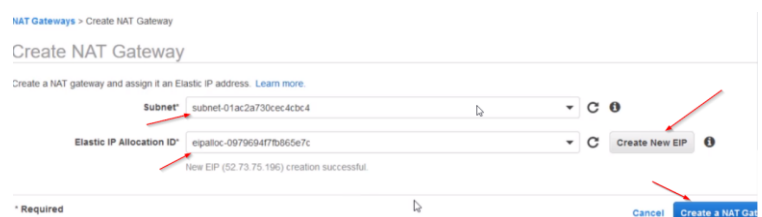
5. Select **Create a New EIP**
6. Select **Create a NAT Gateway**

Wait for the NAT Gateway to be created and to start-up which will take a while.

Next step is to edit the Route table for the private subnet:

(This task is to allow tell our private subnet to send all unknown traffic to NAT Gateway)

1. Go to **VPC Dashboard**,
2. Go to **Route Tables**
3. Select the route table that is associated with the private subnet
4. Select menu **Actions**
5. Click **edit routes**
6. Select **Add route**
7. Enter route information

   a. Destination: **0.0.0.0/0**
   b. Target: **NAT Gateway** - select our gateway from list
8. Select **Save routes**

Next step, is to check if the EC2 instance can reach the internet through our NAT Gateway:

1. Go to EC2 Dashboard
2. Select Running Instances
7. Start up both EC2 instances
8. Record the public and the private IP address of the two EC2 instances
9. Go to linux client and try to access the EC2 instance using SSH client and the private key as done previously here.
10. Once you have logged into the private EC2 instance through the Public EC2 instance, run the following commands:

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

75

- ○ sudo -s   (elevate to admin role)
- ○ yum update -y   (run update on linux)

11. Once successful, it is an indication that the NAT gateway is working.

Please make sure to delete the NAT Gateway after completing this lesson.

For more information about Amazon NAT Gateway, please refer to the AWS documentation [here](#).

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*
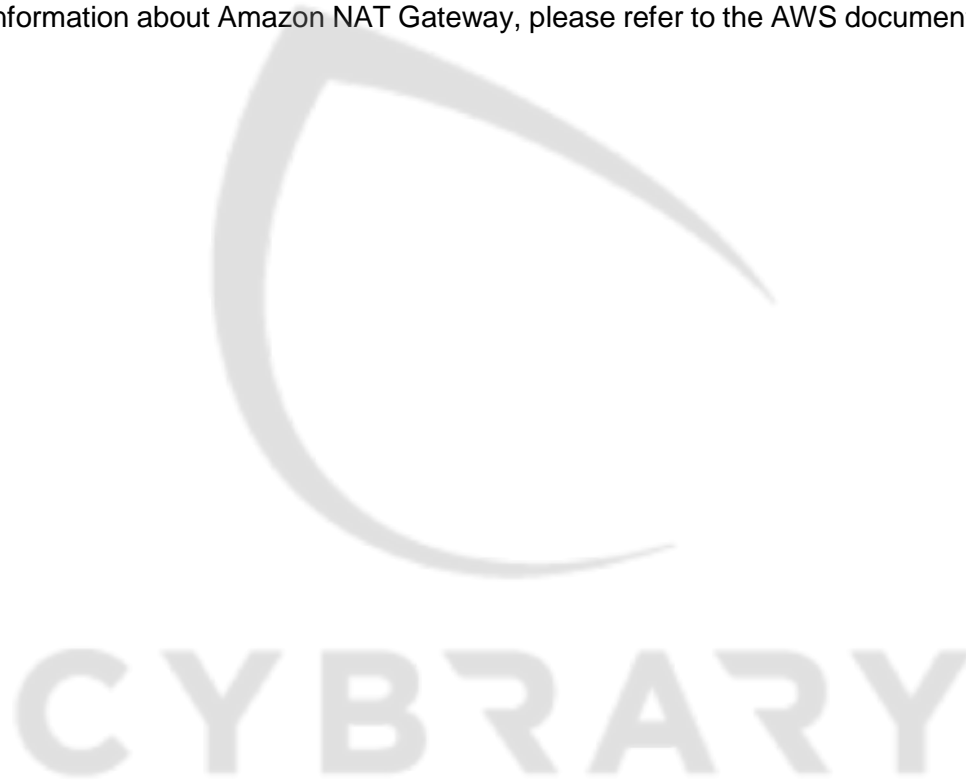
76

CYBRARY

Lesson 6.6: Create a custom VPC Part 5

Skills Learned From This Lesson: MySQL, RDS, VPC, Networking, Security Group, EC2,

Note: Please refer to the [Figure 6.2.1 for the VPC design diagram](#).

In this lesson we are going to create a Relational Database (RDS) instance using MySQL and launch it from within our private subnet. We will also create a script to build and launch our public facing php server.

Since this is an introductory AWS course, this will not include a topic on database provided within the AWS platform. Amazon has a great selection of SQL and non-SQL database offerings that you can and will use as you go further in your cloud career.
Database theory is beyond the scope of this course but we will share the 20,000 foot view of the MySQL relational database that we will create in this lesson. Amazon RDS makes it easier for us to build, operate and scale a relational database in the AWS cloud. Amazon RDS manages the backups, handles software patching, automatic failover detection and recovery. Essential AWS handles all the database maintenance for us permitting us to focus on the administration. For more information, check the FAQ [here](#)

Creating a RDS MySQL instance:

1. Go to the AWS Console
2. Search for RDS
3. Click RDS to go to the RDS Dashboard
4. Click create database
5. Under Engine option, select MySQL
6. Under Templates, select Free tier
7. Scroll down to settings
8. Enter credential settings:
    - DB Cluster identifier: **cybrarymysqlcluster**
    - Master username: **cybrarymysqldb**

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

77

- ○ Master password: **cybrarymysqldb**
- ○ Confirm password: **cybrarymysqldb**

9. Under Connectivity

- ○ VPC: **Cybrary_VPC**
- ○ Public Accessible: **No**
- ○ VPC Security group: Create New: **Cybrary_SG_DB**
- ○ Availability Zone: **us-east-1b**

10. Under advanced configuration

- ○ Db instance name: **cybrarymysqldb**

11. Select create database

Now we need to perform this step for the DB Security Group to allow our public web server to access the SQL server:

1. Go to **RDS Dashboard**
2. Select **Databases**
3. Select **new database**
4. Under **Connection and Security** tab
   a. Click **VPC Security group**
5. It will navigate you to the **Security Group** section
6. Select **Inbound**
7. Select **Edit**
8. Click **Add Rule**
9. Enter rule:
   a. Type: **Custom TCP Rule**
   b. Protocol: **3306**
   c. Source: enter sg and select **Cybrary_SG_Web server**
10. Click **Save**

Building another EC2 instance for public subnet (Internet facing web server) with php script:

1. From the AWS Management Console
2. Search for EC2
3. Select **EC2**
4. From the **EC2 Dashboard**, click **Launch Instance**
5. On the left, tick **Free tier only**
6. Select AMI: **Amazon Linux 2 AMI (HVM), SSD Volume Type**
7. Select Instance Type: **t2.micro (free tier eligible)**
8. Click Next:Configure Instance Details
9. Configure the following instance settings:

   a. Number of Instances: 1

   b. Network: Cybrary_VPC

   c. Subnet: 10.0.10.0_public_us-east-1a

   d. Auto-assign Public IP: Use subnet Settings(enable)

   e. IAM role: EC2_Can_Call_S3 (if not present continue)

   f. Expand Advanced details:

      i. User data: As text

Script	Description
#!/bin/bash	Shag-bang + path of bash script
yum install httpd php php-mysql -y	Installing the apache server, php & mysql
yum update -y	Install updates
chkconfig httpd on	Check the status of the web server
service httpd start	Start up the apache server
echo "<?php phpinfo();?> > /var/www/html/index.php	Create a php info file
cd /var/www/html	Change to web hosting directory

wget https://s3.amazonaws.com/cybrar-rocks/dbconnect.php	Get the DB connection php file and store in the web hosting path

The dbconnect.php files has the following script:

```
// Generic PHP script to connect to Demo Cybrary MySQL Server
//
<html>
    <head>
        <title>Cybrary AWS Connect to MySQL Server</title>
    </head>
    <body>
    // connection to the database
        <?php
            $dbhost = 'aws-rds-endpoint';
            $dbuser = 'cybrarymysqldb';
            $dbpass = 'cybrarymysqldb';
            $conn = mysql_connect($dbhost, $dbuser, $dbpass);

            if(! $conn ) {
                die('Could not connect: ' . mysql_error());
            }
            echo 'Connected successfully to Cybrary MySQL database.';
            mysql_close($conn);
        ?>
    </body>
</html>
```

10. Next Add storage

11. Click Next: Add Tags

12. Click Add tags

Key	Value
Name	Cyrary_Web_Server

13. Click Next: Configure Security Group

14. Use the security group parameters:

   ○ Assigned a security group: select existing security group

   ○ Name and description: Cybrary_SG_Web_server

15. Click Review and Launch

16. Click Launch

17. Select Choose an existing key pair

18. Select key pair Cyrary_DMZ

19. Tick: I acknowledge

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

80

20. Click Launch instances

21. Scroll down, click View Instances

22. Go to the EC2 instance

23. Copy the Public IP address

24. And paste it in a browser, you should get the phpinfo() page

25. SSH to the EC2 instance

26. Run the following command:

    ○ sudo -s   (elevate to admin mode)
    ○ cd /var/www/html/   (change directory)
    ○ ls   (list files in path)

27. You should see two files:
    ○ index.html
    ○ dbconnect.php

We need to edit the dbconnect.php to include the RDS instance name:

1. Enter command: nano dbconnect.php

2. Go to RDS Dashboard

3. Go to Databases

4. Select our db instance

5. Under connection and security → Endpoint & port

6. Copy our endpoint (e.g. cybrarymysqldb.cxkuzf6hgjd8.us-east-1.rds.amazonaws.com)

7. Paste the endpoint into our dbconnect.php file for the connection parameter dbhost

8. Press CTRL+X   - to exit editing

9. SHIFT + Y   - to save

10. Now go back to the browser and enter url: http://public_ip_Address/dbconnect.php

11. If it is successful, You will get the message:

// Generic PHP script to connect to Demo Cybrary MySQL Server // // connection to the database Connected successfully to Cybrary MySQL database.

Congratulations, you have completed your first VPC design and configuration by deploying a PHP web server from a MySQL relational database. This sets you on the path of becoming an AWS Certified Solutions Architect.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

82

Module 7:
Course Closing Remarks

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

83

Lesson 7.1: AWS Course Closing Remarks

Skills Learned From This Lesson: AWS, Cloud Computing, MFA, IAM, S3, Website, EC2, Automate, BASH, script, VPC, Networking, NAT Gateway, MySQL, Certification, Learning Path

Welcome to the final module of this course. I want to thank you for making it this far and allowing me to privilege of sharing AWS knowledge with you.

This study guide had covered the following topics and tasks:

1. An Introduction of Cloud
2. A Brief History of AWS and the value proposition of cloud computing
3. Setup an Account with Multi-Factor Authentication (MFA)
4. Discuss some functionality of Identity & Access Management (IAM) from a high level
5. Amazon S3 storage
6. Create a Static website
7. Creating EC2 Instances and automate tasks via bash script
8. Creating our own Custom VPC complete with:
   - Public & Private subnets (VLSM)
   - Security Groups (firewall)
   - NAT Gateways (Internet)
   - MySQL (RDS)

I hope you find this study guide useful and it was developed as the first step for anyone who is interested in learning AWS and its offerings. This study guide has merely scratched the surface of what is available. However, after competing this study guide, you have started the foundational topics that are necessary to prepare for an actual AWS Certifications.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

84

CYBRARY

The AWS Certification Journey

The instructor Shaun Balkum earlier in his career, he was introduced to AWS through a colleague while working on a network project. During this time, his colleague had just attempted the exam and failed but he was still excited and determined to acquire the desired AWS certification. On another occasion, his colleague encouraged him to consider pursuing it. At the same time, the projects that they were working on, many of the customers were actively exploring AWS cloud services. Shaun took the step to purchase the book AWS Certified Solution Architect Official Study Guide published by AWS and he proceeded to devour the book from cover to cover in 3 months. He also opened a Free Tier account, read numerous whitepapers and documentations. He watched numerous AWS re:Invent videos on Youtube and practice via the Free tier each night. Three months later, Shaun sat for and passed the AWS Solutions Architect Associate exam. After that, Shaun intent was to stop there, but at the time, there was only 5 AWS certification. Shaun decided to set a new goal to acquire all 3 Associate certifications (including Developer and SysOps Administrator). After that Shaun felt obligated to acquire the AWS Professional certifications as well. The entire AWS certification (Associate & Professional) took Shaun a year to complete them all. Subsequent years, AWS developed the five (5) specialty certifications which leads to a total of 11 AWS Certifications that can be acquired.

Recommendation

Shaun recommends that after completing this course, you should pursue the AWS Certified Solutions Architect Associate credential. This track will provide the necessary foundation for the AWS technologies. Some of which you will be familiar after taking this course, but others will be brand new to you. After reaching that milestone, it will be your decision for the next step based on your goals set for your professional career. One important note is that you cannot go wrong when choosing a cloud certification. Thank you again for your time and I hope it was useful to you.