CPD Lab 7: Security for Cloud Applications

Introduction

In this lab you will create a Virtual Private Cloud (VPC) and explore related network configurations. You will complete a Qwiklab on AWS Key Management Service (KMS) and review some other security monitoring features.

You had completed a free Qwiklab, 'Introduction to Identity and Access Management' in CPD Lab 1, which you could also repeat if required.

Tasks:

- Task 1: Set up a Virtual Private Cloud (VPC)
- Task 2: Complete the Qwiklab- Introduction to AWS Key Management Service
- Task 3: Review some Security Related Services on AWS
  - AWS Certificate Manager
  - Trusted Advisor
  - Amazon Inspector
  - AWS GuardDuty
- Task 4: Releasing the allocated resources

Task 1: Creating a Virtual Private Cloud (VPC) using VPC Wizard

A VPC allows you to establish an isolated private cloud on AWS public cloud where you can setup networking and define access rules.

In this task you will create a VPC, and configure VPC settings for an elastic IP, private and public subnets, Access Control Lists (ACL), Security Groups, route tables, and Internet Gateway. You will also create an EC2 instance in the VPC.

Step 1: (optional) Review the default VPC for your account

When you created your AWS account, a default VPC was created automatically for you. In the default VPC, there are subnets created for each availability zones by default. Internet Gateway and Route tables are also created and attached automatically.

Once you launched EC2 instances in the default VPC you could also connect to the instances through Internet.

- Navigate to VPC under AWS management console and select the default VPC
- Under 'Description' you can observe the 'Network ACL' and 'Route table'
- From the left navigation pane select 'Subnets' to observe the subnets for the default VPC

- Select one of the subnets and from the tabs below observe entries under the 'Route Table', and 'Network ACL'
- From the left navigation pane select 'Internet Gateways' and select the Internet Gateway corresponding to the default VPC to observe its description

Step 2: Allocating an Elastic IP Address

An elastic IP is a static public IP address that does not change. An EC2 instance allocated elastic IP retains its IP address after a reboot or start/stop. In this step you will allocate an elastic IP address.

- Navigate to VPC under AWS management console
- Select 'Elastic IP' from the left pane
- Click 'Allocate new address'
- On the next screen, let 'IPv4 address pool' value to be 'Amazon pool' and click 'Allocate'
- An IP address gets allocated
- Click 'Close'

Step 3: Creating a Virtual Private Cloud (VPC)

Under VPC you would have a default VPC available but you will create a new VPC using 'VPC Wizard'

- Navigate to VPC under AWS management console
- Click 'VPC Dashboard' from the left navigation pane
- Select 'Launch VPC wizard'
- Select the option, 'VPC with Public and Private Subnet' and click 'Select'
- The subnets and other values will be populated to default values
- For 'VPC Name' enter 'MyVPC'
- For 'Elastic IP Allocation ID' select the Allocation ID of the 'Elastic IP' that you created in Step 2
- Click 'Create VPC'
- It will take few minutes for VPC to be created
- A message appears that 'Your VPC has been successfully created. You can launch instances into the subnets of your VPC. For more information, see Launching an Instance into Your Subnet.'

Step 4: Checking the Internet Gateway

An Internet Gateway is required to allow Internet connection from a VPC

- Select 'Internet Gateway' from the left navigation menu
- Select the gateway corresponding to 'MyVPC' from the displayed 'Internet Gateways'
- Under 'Description' you will observe that it is attached to 'MyVPC'

Step 5: Checking the route table

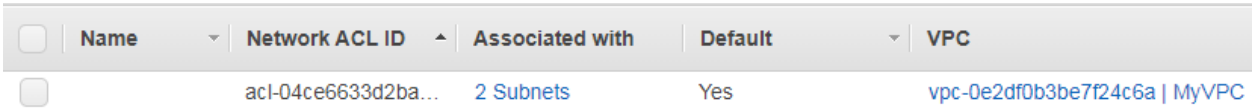
A route table has entries for the local and Internet traffic. You will observe the route table settings for both the public and private subnet.

- Navigate to 'Subnets' from the left navigation pane
- Select 'Public subnet' for 'MyVPC' from the displayed subnets
- Click the tab for 'Route Table'
- Under 'Routes' you will observe an entry for local traffic (local under Target) and another for Internet traffic using Internet Gateway (igw-xxxxxxxxxxx under Target)
- Similarly you can select the 'Private subnet' and repeat the steps above
- Observe that the entry for Internet traffic has an entry like nat-xxxxxxxxxxxxxx signifying that the traffic passes through a NAT gateway

Step 6: Checking the Network ACLs and Security Groups

An Access Control List (ACL) acts as a firewall for the subnet whereas a Security Group (SG) acts as a firewall for an instance.

- Select 'Network ACLs' from the left navigation menu
- Observe that the ACL is associated with both subnets (public and private)



- Select the 'Security Groups' from the left navigation pane
- Select the 'Security Group' for 'MyVPC' from the displayed lists
- Observe the rules under the tabs, 'Inbound Rules' and 'Outbound Rules'

Step 7: Creating an EC2 instance within VPC

You will now create an EC2 instance in the public subnet of MyVPC and will connect to it. The steps below for creating an EC2 instance are mostly similar to those in Lab 2, Task 2, but the ones that are different have been highlighted below (Step 3).

- Select EC2 from Services in the AWS console
- Click 'Launch Instance'
- Step 1: 'Choose an Instance Type',
  - You are presented with a choice of Amazon Machine Images (AMI)
  - Type 'WordPress' to search
  - Go to 'AWS Marketplace' and select

'WordPress Certified by Bitnami and Automatic' Linux/Unix, Ubuntu 16.04 | 64-bit (x86) Amazon Machine Image (AMI)

- Click continue on the dialog box

- Step 2: Choose an Instance Type
  - Select t2.micro 'Free tier eligible', click Next
- Step 3: Configure Instance Details
  - **For 'Network' select 'MyVPC'**
  - **For 'Subnet' select 'Public Subnet'**
  - **For 'Auto-assign Public IP' select 'Enable'**
- Step 4: Add Storage – click Next
- Step 5: Add Tag – click Next
- Step 6: Configure Security Group
  - For 'Assign a security group' select 'Select an existing security group' and select the security group for MyVPC
- Step 7: Review Instance Launch – review and launch the instance by clicking 'Launch'
- In the dialog box that pops up: 'Select an existing key pair or create a new key pair'
  - Choose 'Create a new key pair'
  - Key pair name: MyKeyPair
  - Click 'Download Key pair' which downloads the MyKeyPair.pem file. This file will be used for the SSH connection in 'Task 2'
  - Click Launch Instances
- Check the newly created instance under EC2 running instances

Step 8: Access the EC2 instance

You should now try to connect to the EC2 instance running within a public subnet in your VPC on AWS

- Navigate to EC2 Dashboard and select the EC2 instance
- From the 'Description' tab copy the public DNS and access it through a browser
- The connection attempt to the EC2 instance will fail

Hands-on

Add an inbound rule to the Security Group of 'MyVPC' so that the connection to EC2 instance (from Task 1, Step 8 above) is established

Task 2: Complete the Qwiklab - Introduction to AWS Key Management Service

This is a free lab of 50 minutes duration. Open Qwiklabs.com and search for 'Introduction to AWS Key Management Service'. In this task you will complete the following:

- Create an Encryption Key
- Create an S3 bucket with CloudTrail logging functions
- Encrypt data stored in a S3 bucket using an encryption key
- Monitor encryption key usage using CloudTrail
- Manage encryption keys for users and roles

In addition, you can also view a video, 'Getting Started with AWS Key Management Service' at https://youtu.be/-5MPXHvKDnc

Task 3: Review Security Related Services on AWS

In this task you will review some of the services that are useful from a security perspective.

1. AWS Certificate Manager

The manager allows free creation of SSL/TLS certificates for AWS based websites and applications.

https://docs.aws.amazon.com/acm/latest/userguide/setup.html
https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

2. Trusted Advisor

AWS Trusted Advisor acts like your customized cloud expert, and it helps you provision your resources by following best practices. Trusted Advisor inspects your AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps. Since 2013, customers have viewed over 2.6 million best-practice recommendations and realized over $350 million in estimated cost reductions.

https://aws.amazon.com/blogs/aws/trusted-advisor-console-basic/
https://www.amazonaws.cn/en/support/trustedadvisor/

3. Amazon Inspector

Amazon Inspector tests the network accessibility of your Amazon EC2 instances and the security state of your applications that run on those instances. Amazon Inspector assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings that is organized by level of severity.

https://docs.aws.amazon.com/inspector/latest/userguide/inspector_introduction.html

4. Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

https://aws.amazon.com/guardduty/

Task 4: Releasing the allocated resources

You may not be able to delete 'MyVPC' first due to the other components that relate to it. So deleting the VPC requires deleting its other connected resources (such as subnets) prior to it. Also take care that you do not delete resources relating to the default VPC of your account (which should be identifiable by its separate ID)

Make sure that you have released all the resources created in tasks above including:

- Terminate EC2 instance and Key-Pair
- Delete the private subnet
- Delete the NAT Gateway
- Delete the public subnet
- Delete the VPC
- Deleting the VPC also deletes (Subnets, Security Groups, Network ACLs, Internet Gateways, Route Tables, Network Interfaces)
- Release the Elastic IP address
- Check that all resources have been deleted

Links

The links below are for your reference only in case further information is required to help complete tasks above:

Task 1

1. Establishing a Virtual Private Cloud (VPC)
   https://aws.amazon.com/vpc/getting-started/

   Tutorial: Creating a VPC with Public and Private Subnets for Your Compute Environments
   https://docs.aws.amazon.com/batch/latest/userguide/create-public-private-vpc.html#vpc-next-steps

Why can't I connect to an Amazon EC2 instance within my Amazon VPC from the internet?

https://aws.amazon.com/premiumsupport/knowledge-center/vpc-connect-instance/