ATLANTIC TECHNOLOGICAL UNIVERSITY

ASSIGNMENT COVER SHEET

To Be Completed By The Student

Lecturer’s Name: Mrs. Ruth Lennon

Assessment Title: CloudFormation

Submission Date: 20-Nov-2022

Student’s Name: Gourish Biju Id. Number: L00170995\_\_\_\_

Course / Stage Master’s in DevOps

Subject/Module: IaC for DevOps Pipelines (2022/23)

Word Limit: Actual Word Count: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I confirm that the work submitted has been produced solely through my own efforts.

Student’s signature: Gourish Biju Date: 20-Nov-2022

|  |
| --- |
| **Note**: **PENALTIES**   * The total marks available for an assessment will be reduced by 15% for work submitted up to one week late. The total marks available are reduced by 30% for work up to two weeks late. * Assessment work received more than two weeks late, without prior approval by the lecturer will receive a mark of zero. * Marks awarded will be reduced by 10 % if submitted work is greater than 10% above or below the assigned word limit. * A further hard or electronic copy of your submitted work may be requested, and therefore you must keep a copy on disc. * Incidents of alleged plagiarism and cheating are dealt with in accordance with the Institute’s Assessment Regulations   **Plagiarism:** Presenting the ideas, words of someone else without proper acknowledgement. Refer to the Institutes’ procedures and guidelines for the assessment of learners. |

## Conclusion:

The assignment helped us to understand IaC concept with much more clarity. To create a mini corporate network with IaC concept was effective and efficient method the investigate and research and deep dive into the concept. Aws has the right tools and documentation for which help us to implement our idea effectively. The task here was to create a Virtual private cloud in AWS through code. AWS offers all the required resources we need to build develop and deploy the VPC so that its easy for us to configure the resources and get the private cloud up. I have started the work by analysis what all resources and tools are required for creating the corporate like VPC , then I got to research for the best practices for creating a cloud. Most of the data I required was documented in AWS documentation itself and additional resources where taken from other internet sources.

I started by creating VPC named CentralVPC . The internet connectivity to a VPC can only be connected through an Internet Gateway which in this case is called MainGateway(MGW) . Cross stack reference method was used to create the whole network. These resources can be exported to another stack. The cross-stack references methodology helps in code reusability also all stacks can be made independently and we can import the resources with export name given. It also helps us to keep track of the dependencies in the stack as the stack grows. We can use Outputs for importing the resources across stacks. Any change needed to be done in the import value we can simply edit the changes the original stack. Also for code reusability defining parameters was also an effective method. For subnets, instances and even VPCs common rules and properties may be present. Creating a parameter will help us to define the required properties and we can refer the parameters to which all resources we need instead of writing all the properties again. This also helps to keep the code neat and clean so errors can be projected effortlessly.

I have created two public subnets(Publicsubnet0 and Publicsubnet1)on the same availability zone and 2 private subnets (Privatesubnet0 and Privatesubnet1) in two different availability zone on the VPC .One Public subnets hosts a public instance which act as a web server for hosting web hosting purpose which can be accessed publicly through internet and the other public subnet hosts the jumbbox. We have placed the jumbbox so that all the inter subnet connections go through the jumbbox . All the instances in the subnets are associated with a security group for both outgoing and incoming traffic. The public subnet instances are attached to a routetable which connects it to the internet via internet gateway of the VPC. Private subnet0 consists of internal server for hosting the internal data which doesn’t have public access. The other subnet hosts an instance which act as the backup server in case the other fails. The backup server and internal server are placed in different availability zones. All the Ip address allocation to subnets is done through CIDR blocks.

For the Database part of the cloud, we can use AmazonRDS. A database server will be placed in a private subnet with separate security group which only allows TCP connection to the database server and private instances can only access the DB server. Amazon relational database service helps us to manage and scale and operate a relational database like MySQL , PostgreSQL etc.

Scalability was also a keen factor while designing the VPC. Probability of increased traffic in the future cannot be denied for a network. The CIDR allocation was done in such a way that all subnets will be provided with sufficient Ip address range foreseeing this situation. If a load balancer is another AWS service which aid in this kind of situation. A load balancer will automatically distribute the traffic to available targets.

I found that different methodologies can be used to develop the VPC like nested stack or a single yaml file. I have gone with cross-stack reference method as I believe it offers more to the code reusability aspect as between cross stack and nested stack its difficult to decide which is the best practice. In nested stack the main use is that the whole infrastructure can be controlled from a single point because root stack and other related stacks can be found in the S3 bucket. Developing the whole infrastructure in a single stack is a worst practise as the complexity increases and more effort would be needed to find the errors.

There are other many services which AWS offers for CloudFormation, most of them are paid services. ElasticIP address is one such feature I came across while researching for this assignment. ElasticIp is assigned to our AWS account and can be used to get connectivity for a private subnet to internet through a NAT gateway. Elastic Load balancer which help in scaling for the instances is also one of the other feature.

I have found AWS CloudFormation a powerful tool for creating private cloud how it boost the IaC concept . I have also learned the different aspect which can be helpful in future and way of approach towards a similar situation in a more practical scenario.

## References and Bibliography:

AWS CloudFormation User Guide. (n.d.). [online] Available at: <https://s3.cn-north-1.amazonaws.com.cn/aws-dam-prod/china/pdf/cfn-ug.pdf>.

docs.aws.amazon.com. (n.d.). Infrastructure as Code - Introduction to DevOps on AWS. [online] Available at: <https://docs.aws.amazon.com/whitepapers/latest/introduction-devops-aws/infrastructure-as-code.html>.

Qadir,Allah-Nawaz (2021).How to Maximize Your Ability to Reuse Code Across Projects.[online] Available at: <https://www.crowdbotics.com/blog/how-to-maximize-code-reuse-across-projects>

# Appendices

# GitHub repository Link:

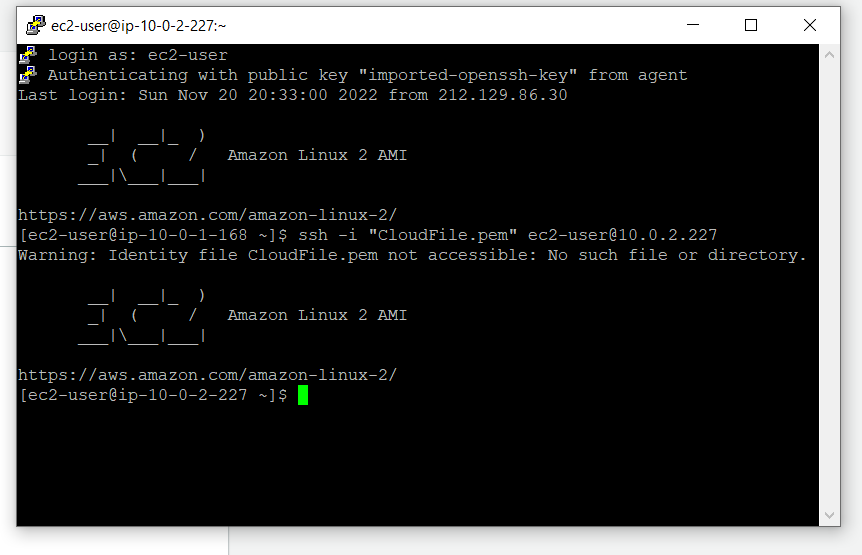
# Table 1:Network traffic

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port** | **Source** | **Destination** | **Allow/Deny** |
| SSH | TCP | 22 | 10.0.1.0/24 | 10.0.2.0/24 | Allow |
| SSH | TCP | 22 | 10.0.1.0/24 | 10.0.3.0/24 | Allow |
| SSH | TCP | 22 | 10.0.1.0/24 | 10.0.4.0/24 | Allow |
| RDS | TCP | 3306 | 10.0.2.0/24 | 10.0.5.0/24 | Allow |
| RDS | TCP | 3306 | 10.0.2.0/24 | 10.0.6.0/24 | Allow |

## Table 2:CIDR address range

|  |  |
| --- | --- |
| **Resource** | **CIDR Block** |
| VPC | 10.0.0.0/16 |
| Jump Box | 10.0.1.0/24 |
| Private Instance | 10.0.2.0/24 |
| Private Instance2 | 10.0.3.0/24 |
| Public Instance2 | 10.0.4.0/24 |
| RDS | 10.0.5.0/24 & 10.0.6.0/24 |

# Figure 1: establishing connection from jumbbox to private instance



# Figure 2: Change set for updating security group:

