

Team Big Data

U-tification

Network Diagram

Date: 11/8/2022

Team Leader: Joseph Armas

Team Members: Joshua Gherman

Rhoy Oviedo

Frank Curry

Ghabrille Ampo

David DeGirolamo

Git Repository: <https://github.com/JosephArmas/cecs-491A-Team-Big-Data>

Version History

Current Version: V4

CHANGES

- Modified
 - Network Diagram
 - Network Diagram Details → Design Decisions
- Added
 - Network Diagram Details

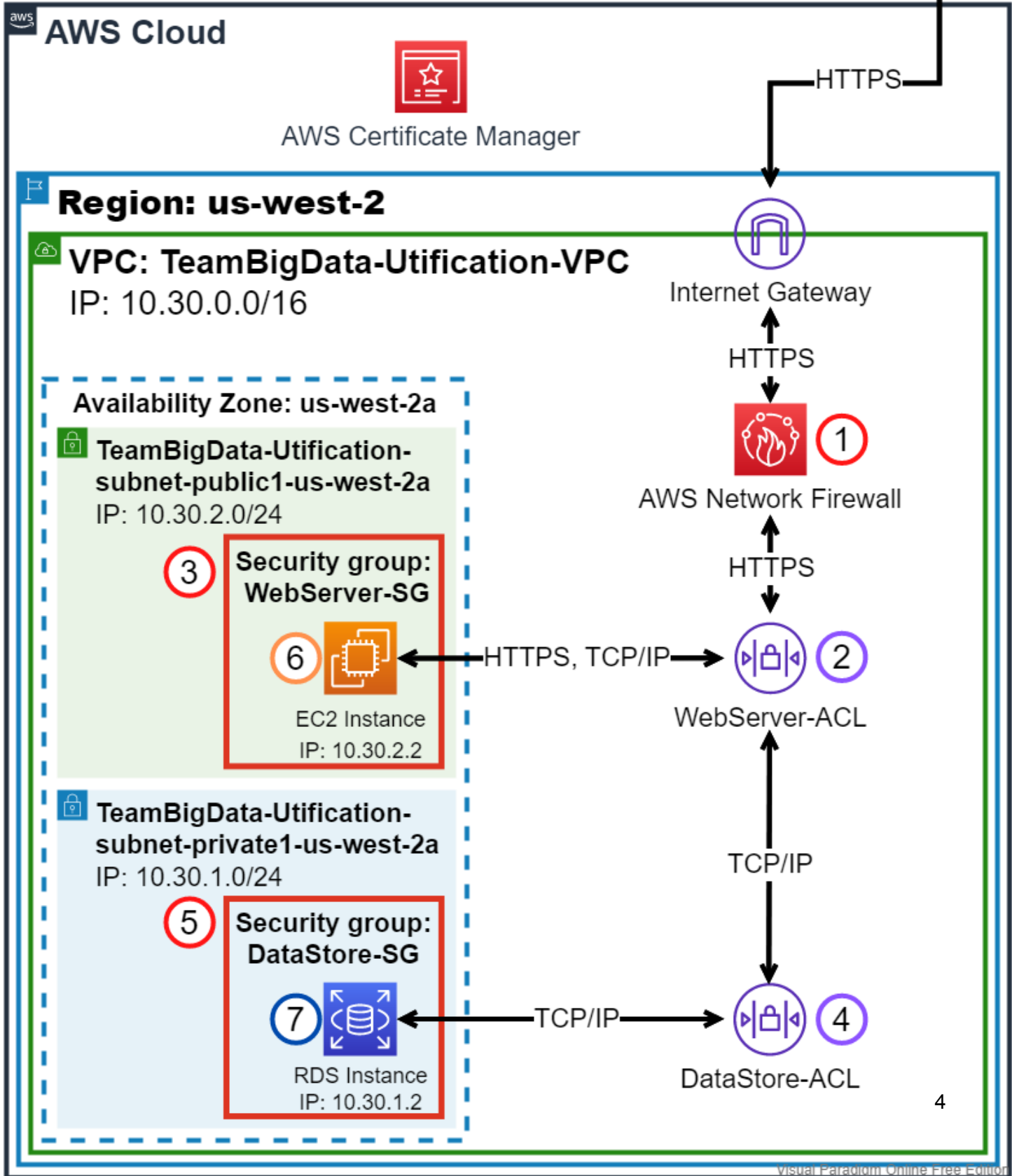
Previous Versions: V1, V2, V3

Table of Contents

High Level Design:	Page
Cover	1
Version History	2
Table of Contents	3
Network Diagram	4
Network Diagram Details	5/6
Design Decisions	7
References	8

Network Diagram

Visual Paradigm Online Free Edition



Network Diagram Details

1

Network Firewall Stateful Rule Group

Protocol	Source IP	Source Port	Dest. IP	Dest. Port	Action
HTTPS	California IP	Ephemeral Port	10.30.2.2	443	Allow

2

WebServer-ACL Inbound Rules

Rule	Type	Protocol	Port Range	Source IP	Allow/Deny
100	HTTPS	TCP (6)	443	California IPs	Allow
200	MYSQL	TCP (6)	3306	10.30.1.2	Allow

WebServer-ACL Outbound Rules

Rule	Type	Protocol	Port Range	Dest. IP	Allow/Deny
100	HTTPS	TCP (6)	443	California IPs	Allow
200	Custom TCP	TCP (6)	5000-5014	10.30.1.2	Allow

3

WebServer-SG Inbound Rules

Type	Protocol	Port Range	Source
HTTPS	TCP	443	California IPs
MYSQL	TCP	3306	10.30.1.2

4

DataStore-ACL Inbound Rules

Rule	Type	Protocol	Port Range	Source IP	Allow/Deny
100	Custom TCP	TCP (6)	5000-5014	10.30.2.2	Allow

DataStore-ACL Outbound Rules

Rule	Type	Protocol	Port Range	Dest. IP	Allow/Deny
100	MYSQL	TCP (6)	3306	10.30.2.2	Allow

5

DataStore-SG Inbound Rules

Type	Protocol	Port Range	Source
Custom TCP	TCP	5000-5014	10.30.2.2

Visual Paradigm Online Free Edition

6

EC2 Configuration:

Windows Server 2022

t2.micro

1 vCPU

1Gb Memory

30Gb Storage

IP: 10.30.2.2

WebSever Microservices Ports

Users: 5000

Map: 5001

Pins: 5002

Alerts: 5003

Reputation: 5004

Events: 5005

User Services: 5006

Upload Picture: 5007

Logging: 5008

Sign in/out: 5009

Registration: 5010

User Management: 5011

Analytics: 5012

UI: 5013

SQL Data Access: 5014

7

RDS Configuration:

Microsoft SQL Server

db.m6i.xlarge

4 vCPUs

16 Gb RAM

200 Gb Storage

Not publicly accessible

IP: 10.30.1.2

Visual Paradigm Online Free Edition

Design Decisions

- AWS Certificate Manager provides the certificate for users to have a secure connection to the web server using HTTPS with the AWS given URL.
- AWS Network Firewall allows for only California IPs using https to connect to the web application.
- WebServer Security Group inbound rules allow HTTPS traffic from California IPs to the EC2 instance and TCP traffic from the RDS instance to the EC2 instance. This limits who can connect to the EC2 instance.
- WebServer Access Control List inbound rules allow HTTPS traffic from California IPs and TCP traffic from the Data Store to the EC2 instance. The outbound rules allow HTTPS traffic from the EC2 instance to the user and TCP/IP traffic from the EC2 instance to the RDS instance. This limits who can communicate to the EC2 instance.
- DataStore Access Control List inbound rules allow TCP traffic from the EC2 instance to the RDS instance. The outbound rules allow for TCP traffic from the RDS instance to the EC2 instance. This limits the RDS to only be able to only communicate with the EC2 instance.
- DataStore Security Group inbound rules allow TCP traffic from the EC2 instance to the RDS instance. This limits the RDS to only be able to only communicate with the EC2 instance.
- The reason for choosing the EC2 instance is that it is the best free tier configuration.
- The reason for choosing the RDS instance is that it is the best free tier configuration. Having the RDS be not publicly accessible ensures that it cannot establish a connection through the internet to it and alter its contents.

References

Ltd, Allies Computing. “How to Handle Ephemeral Ports in Security Groups and Network

ACLS - Allies Computing.” Alliescomputing.com,

<https://alliescomputing.com/knowledge-base/>

how-to-handle-ephemeral-ports-in-security-groups-and-network-acls.

“Visual Paradigm Online - Suite of Powerful Tools.” Visual Paradigm Online - Suite of Powerful

Tools, <https://online.visual-paradigm.com/>.

Web Application Hosting in the AWS Cloud - AWS Whitepaper.

<https://docs.aws.amazon.com/whitepapers/latest/web-application-hosting-best-practices/>

web-application-hosting-best-practices.pdf.

YouTube, YouTube, 3 Jan. 2022, <https://www.youtube.com/watch?v=WNFknf9zyZg>. Accessed 3

Nov. 2022.