Team Big Data

U-tification

Network Diagram

Date: 11/3/2022

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
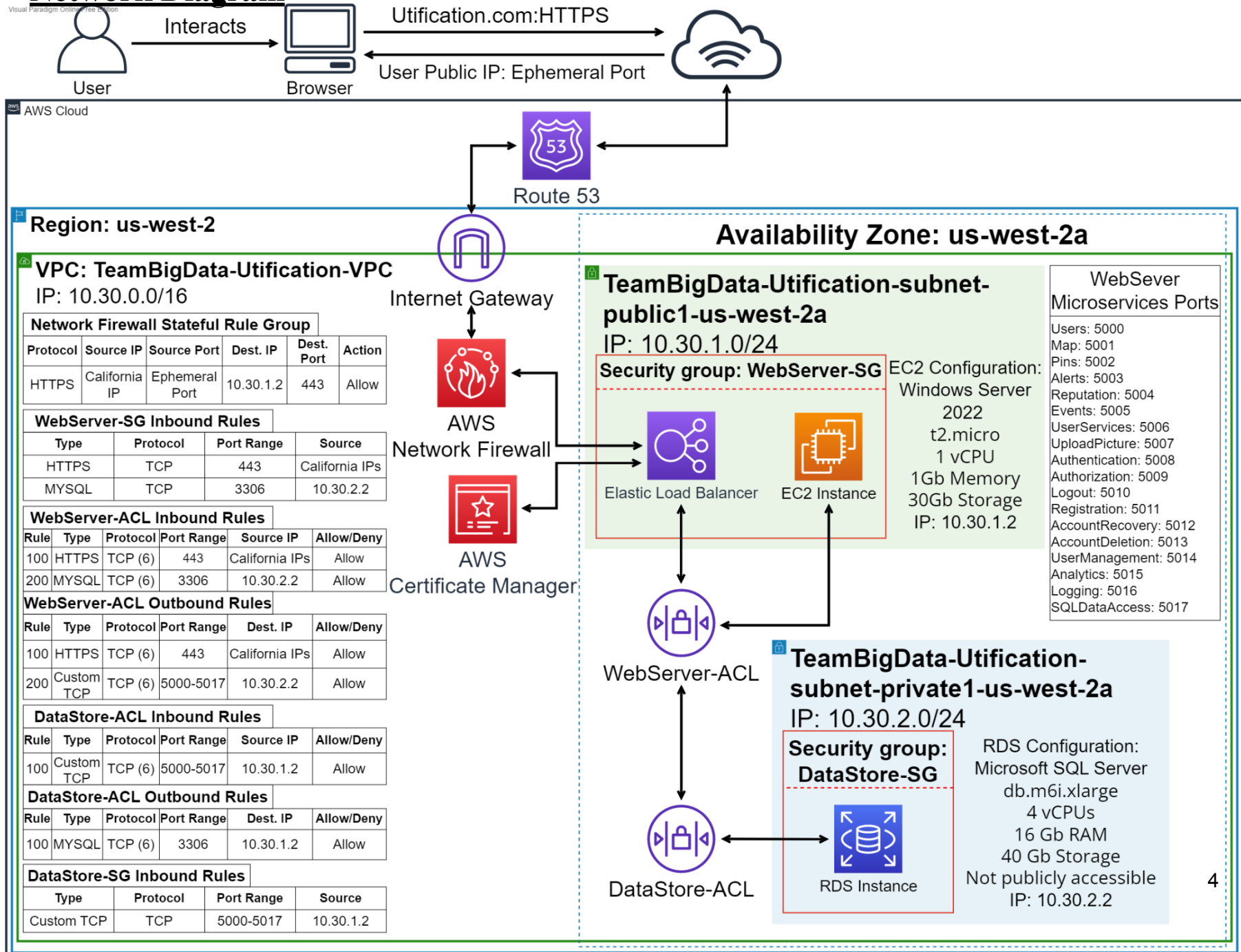
Version History

Current Version: V3

CHANGES

- Modified
    - Network Diagram
- Added
    - Network Diagram Details

Previous Versions: V1, V2

<u>Table of Contents</u>

Network Diagram

User — Interacts → Browser — Utification.com:HTTPS → (Cloud)
(Cloud) — User Public IP: Ephemeral Port → Browser

AWS Cloud

Route 53

Region: us-west-2

Availability Zone: us-west-2a

Internet Gateway

AWS Network Firewall

AWS Certificate Manager

VPC: TeamBigData-Utification-VPC
IP: 10.30.0.0/16

Network Firewall Stateful Rule Group

Protocol	Source IP	Source Port	Dest. IP	Dest. Port	Action
HTTPS	California IP	Ephemeral Port	10.30.1.2	443	Allow

WebServer-SG Inbound Rules

Type	Protocol	Port Range	Source
HTTPS	TCP	443	California IPs
MYSQL	TCP	3306	10.30.2.2

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	10.30.2.2	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)	5000-5017	10.30.2.2	Allow

DataStore-ACL Inbound Rules

Rule	Type	Protocol	Port Range	Source IP	Allow/Deny
100	Custom TCP	TCP (6)	5000-5017	10.30.1.2	Allow

DataStore-ACL Outbound Rules

Rule	Type	Protocol	Port Range	Dest. IP	Allow/Deny
100	MYSQL	TCP (6)	3306	10.30.1.2	Allow

DataStore-SG Inbound Rules

Type	Protocol	Port Range	Source
Custom TCP	TCP	5000-5017	10.30.1.2

WebServer-ACL

DataStore-ACL

TeamBigData-Utification-subnet-public1-us-west-2a
IP: 10.30.1.0/24

Security group: WebServer-SG

Elastic Load Balancer   EC2 Instance

EC2 Configuration:
Windows Server 2022
t2.micro
1 vCPU
1Gb Memory
30Gb Storage
IP: 10.30.1.2

TeamBigData-Utification-subnet-private1-us-west-2a
IP: 10.30.2.0/24

Security group: DataStore-SG

RDS Instance

RDS Configuration:
Microsoft SQL Server
db.m6i.xlarge
4 vCPUs
16 Gb RAM
40 Gb Storage
Not publicly accessible
IP: 10.30.2.2

WebSever Microservices Ports

Users: 5000
Map: 5001
Pins: 5002
Alerts: 5003
Reputation: 5004
Events: 5005
UserServices: 5006
UploadPicture: 5007
Authentication: 5008
Authorization: 5009
Logout: 5010
Registration: 5011
AccountRecovery: 5012
AccountDeletion: 5013
UserManagement: 5014
Analytics: 5015
Logging: 5016
SQLDataAccess: 5017

4

Network Diagram Details

- Route 53, Elastic Load Balancer, and AWS Certificate Manager works together to allow for users to have a secure connection to the web application using the url https://Utification.com.
- 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 Elastic Load Balancer and the EC2 instance. The RDS instance is also allowed to send TCP traffic to the EC2 instance. This limits who can pass traffic through the Elastic Load Balancer and 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 and TCP traffic from the EC2 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 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 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.

<u>References</u>

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.