Cloud Security: Secure Web Application Design on AWS

NCI Post Graduate Diploma Cyber Security

Author: Jonathon Taaffe

Title: Cloud Security: Secure Web Application Design on AWS
Author: Jonathon Taaffe
Copyright© 2020 Jonathon Taaffe

All rights reserved. This publication is protected by copyright, and permission must be obtained from the author prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this publication, the author assumes no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Warning and Disclaimer
The information is provided on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this publication. The opinions expressed in this publication belong to the author.

Trademark Acknowledgments
All terms mentioned in this publication that are known to be trademarks or service marks have been appropriately capitalised. The author cannot attest to the accuracy of this information. Use of a term in this publication should not be regarded as affecting the validity of any trademark or service mark.

Contents

Executive Summary

CyberSecure.Team (CST) provides Cyber Security services to individuals, organisations and governments. As the Chief Information Security Officer (CISO), I have been tasked with improving the availability and security of our online presence, while ensuring capacity for future services growth.

CST has a globally distributed workforce of 100 employees with further expansion forecasted. Our current online presence is hosted in Ireland with monthly unique hits averaging 40,000.

Our online presence vision is to provide secure tiered interactive subscription-based customer support while also enabling secure private employee interaction.

The C-Board has agreed that our online interactive platform will be a secure blogging-based application enabling global employee interaction.

Requirements Brief

CyberSecure.Team C-Board have defined the following requirements:

- As a Cyber Security services company, our online platform must be resilient to cyber-attacks.
- Globally dispersed workforce securely connects and interact from anywhere, any time.
- Users Create, Read, Update and Delete content.
- Role-Based Access Control (RBAC)[1] for access.
- Burst capacity for organisation and government contracts.
- Scalable online capacity for forecasted employee growth.
- Minimal Capital Expenditure and Asset Purchasing.
- Compliance with relevant Global Legal Requirements.
- Compliance with Industry Security Architecture Standards.
- Confidentiality, Integrity and Availability[2] of data at rest and in transit guaranteed at all times.
- 99.999% availability[3] encompassing scheduled/unscheduled downtime.
- Full system outage recovery time not to exceed 4 hours.

[1] Wikipedia.org [2019] *Role-based Access Control* https://en.wikipedia.org/wiki/Role-based_access_control [Accessed 5th December 2019]
[2] Techopedia.com [2019] *CIA Triad of Information Security* https://www.techopedia.com/definition/25830/cia-triad-of-information-security [Accessed 5th December 2019]
[3] Journal of Cloud Computing [2019] *High availability in clouds: systematic review and research challenges* https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0066-8 [Accessed 5th December 2019]

Analysis

Business Requirements Analysis

Grouping and summarising the C-Board requirements into the following categories clearly identifies the project priorities as follows:

Category	C-Board Requirements Summary
1. Availability and Access	a. Resilience to cyber-attacks b. Securely connect and interact from anywhere, any time c. Burst capacity when required d. Scalable capacity e. Role-Based Access Control (RBAC) f. Confidentiality, Integrity and Availability
2. Expenditure and Compliance	a. Minimal Capital Expenditure and Asset Purchasing b. Global Legal Requirements Compliance c. Industry Security Architecture Standards Compliance
3. DR/BCP Recovery	a. 99.999% availability b. Full system recovery time > 4 hours
4. Web Application Functionality	a. Create, Read, Update and Delete content

Table 1. Grouping and Summarising of C-Board Requirements[4]

Availability and Access: This is the key deliverable for the success of the project. Ensuring the solution is cyber-attack resilient is critical to the reputation and success of the company.

For secure anywhere/anytime access, a secure globally available platform will be required.

Ensuring capacity for burst and forecasted growth while keeping capital expenditure and asset purchasing limited (see requirement 2. a) steers the platform requirements to a secure Cloud-based solution.

To comply with 'Confidentiality, Integrity and Availability of data-at-rest and data-in-transit guaranteed at all times', the solution architecture must incorporate methods to secure data-in-transit and to secure data-at-rest.

Expenditure and Compliance: Complying with minimal capital expenditure and minimal asset purchasing, the Cloud solution will be hosted Off-Premises with no On-Premises server infrastructure.

To ensure compliance with legal and regulatory requirements, a review of the current Cloud Solution Providers (CSP) legal and regulatory compliance alignment is required.

As CST has a number of government contracts, a CSP with experience providing services to government departments is crucial.

DR/BCP: The solution must include all required measures to ensure 5 x 9's availability with rapid recovery in the event of failure.

Web Application Functionality: The web application must provide users with the ability to Create, Read, Update and Delete content.

[4] Taaffe, J [2019] *Table 1. Grouping and Summarising of C-Board Requirements* [Created 5th December 2019]

Solution Functional Requirements

Summarised below are the key functional requirements that must be incorporated into the solution:

Category	Functional Requirements
Cyber-Attack Resilience	Defense in Depth Domain Name Service Security (DNSSEC) Data Breach Prevention Distributed Denial-of-Service (DDoS) Prevention Economic Denial-of-Service (EDoS) Prevention Abusive Bot/Botnet Prevention
Secure Scalable Cost-Effective Platform	Broad Network Access [5] • Global 24x7x365 Availability On-Demand Self-Service [5] Measured Services [5] • Pay-as-you-Go Pricing Model Resource Pooling [5] • Capacity for Anticipated Growth • Burst Capacity
Confidentiality, Integrity and Availability	Data-in-Transit: End-to-End Secure Socket Layer (SSL) Encryption Data-at-Rest: • Virtual Machine Image on Disk Encryption • Data on Disk Encryption Secure Encryption Key Management Rapid Elasticity [5] • Load Balancing • Auto Scaling Redundancy Backup Management
Compliance Requirements	National Institute of Standards and Technology (NIST) 800-171 Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) International Organization for Standardization (ISO) • ISO 27001/2 Information Security Management System (ISMS) • ISO 27017 Information Security Management System (ISMS) Cloud EU General Data Protection Regulation Department of Defense (DoD) Cloud Computing Security Requirements Guide Experience providing services to government departments
Infrastructure	Deployment Model [5] • Off-Premises Service Model [5] • Infrastructure-as-a-Service (IaaS)
Web Application	Role-Based Access Control 2 Factor Authentication Corporate Password Policy Alignment Create, Read, Update and Delete Content

Table 2. Solution Functional Requirements [6]

[5] NIST.gov [2012] *The NIST Definition of Cloud Computing* https://csrc.nist.gov/publications/detail/sp/800-145/final [Accessed 5th December 2019]

[6] Taaffe, Jonathon [2019] *Table 2. Solution Functional Requirements* [Created 5th December 2019]

Cloud Service Provider (CSP) Considerations

CSP Trust and Reputation

As the proposed solution will be a fully On-Cloud Off-Premises solution, trust in the CSP will be paramount. Ensuring the CSP is an industry leader in Cloud Solutions and is an industry trusted CSP is key. Utilising the IaaS Service Model , the CSP will manage all hardware including physical network, server and storage infrastructure. The IaaS service model gives CST full control over the Virtual Network Configuration, Virtual Machine Operating Systems and the proposed Web Application as shown in the following table

Cloud Service Models			
On-Premises IT	**IaaS**	**PaaS**	**SaaS**
Data	**Data**	**Data**	**Data**
Application	**Application**	**Application**	Application
Database	**Database**	Database	Database
Operating System	**Operating System**	Operating System	Operating System
Virtualisation	Virtualisation	Virtualisation	Virtualisation
Physical Servers	Physical Servers	Physical Servers	Physical Servers
Network & Storage	Network & Storage	Network & Storage	Network & Storage
Data Centre	Data Centre	Data Centre	Data Centre

CyberSecure.Team Managed

Cloud Service Provider Managed

Table 3. Cloud Service Models[7]

CSP Transparency

Ensuring the CSP provides extensive, publicly available, up-to-date supporting documentation for their solutions will facilitate a successful deployment. To fulfil with the Compliance Requirements of this deployment the CSP should also publicly provide all relevant certification and accreditation documentation.

CSP Service Level Agreements (SLA's)

Clear and concise CSP SLA's should be publicly available and easily understood and referenced.

The CSP should have publicly available SLA's for the following IaaS service model components:

Area	**Components**
Security	Identity and Access Management (IAM), Certificate and Key Management
Networking	Firewalls, Load Balancers, NAT Gateways, Internet Gateways
Compute	Virtualisation, Virtual Machines, Operating Systems, Auto Scaling
Storage & Databases	Encrypted Storage, Backup and Restore, Redundancy and Replication

Table 4. IaaS Component SLA's [8]

[7] Taaffe, Jonathon [2019] *Table 3. Cloud Service Models* [Created 5th December 2019]

[8] Taaffe, Jonathon [2019] *Table 4. IaaS Component SLA's* [Created 5th December 2019]

Cloud Security Frameworks

In researching Cloud Security standards, Cloud Security Frameworks from the following standards-based organisations were identified as the industry leaders. I have highlighted and summarised the key concepts and components of each framework which is relevant to our deployment scenario.

National Institute of Standards and Technology (NIST)

Guidelines on Security and Privacy in Public Cloud Computing [9]

Below is a summary of NIST's Key Security and Privacy Issues guidelines pertinent to this deployment.

Governance

- Roles and responsibilities between the CSP and CST must be clearly defined.
- System security is a shared responsibility; the CSP manages the infrastructure security and CST will manage virtual network, operating systems and application security.

Compliance

- Legal, regulatory, standards, and specification compliance is also a shared responsibility; the CSP and CST must be aligned with regard to compliance.
- CST has completed a Data Classification program and must ensure Cloud Data Location complies with the assigned classification.
- CSP must provide eDiscovery services

Trust

- Control of certain security and privacy attributes will be transferred from CST to the CSP
- Insider Access: As part of the trust model CST must ensure the CSP has policies and procedures in place to mitigate internal threats.
- Data Ownership: Data ownership rights must be explicitly defined
- Visibility: Monitoring, logging and alerting of all CSP consumed services.
- Data Management/Full Disclosure: CSP must report all data breaches of data in the cloud as well as data breaches of consumers of cloud services data.
- Risk Management: The CSP must manage risk associated with underlying infrastructure.

Architecture

- Attack Surface: A HyperVisor adds an additional attack vector which the CSP must manage.
- Separation of Duties: Virtual IaaS Administrators must be trained to support Virtual Systems and Virtual Networks.
- Virtual Machine Images: CST to manage and control VMI's to ensure latest updates applied
- Client-Side Protection

Identity and Access Management

- Authentication: CST to manage all IAM Groups, Users and Roles.
- Access Control: CST to manage privileges and resource access control.

Software Isolation

- Multi-tenancy: CSP to ensure secure isolation and segregation of resources between co-hosted tenants.
- Attack Vectors: CSP to ensure secure virtual machine isolation to prevent Virtual Machine Escaping.

[9] NIST.gov [2019] *Guidelines on Security and Privacy in Public Cloud Computing* https://csrc.nist.gov/publications/detail/sp/800-144/final [Accessed 5th December 2019]

Data Protection

- Data Access Controls and Data Security: Co-managed between the CSP and CST.
- Data Concentration: Cloud data co-location must be rigorously managed by the CSP.
- Data Isolation: Access controls and data-at-rest/-in-transit encryption must be incorporated.
- Database environments: Integrate DB data encryption with robust data management strategy.
- Encryption Key Management: CSP provides service; CST responsible for key management.
- Data Sanitisation: CSP to maintain industry data sanitisation policies and procedures.

Availability

- Temporary Outages: CST to deploy fault tolerant solution to eliminate outage impact.
- Prolonged Outages: CSP to provide multiple locations which CST will incorporate into solution.
- Denial of Service: CSP manages industry standard DoS/DDoS/EDoS mitigation solutions.

Cloud Computing Security Reference Architecture[10]

NIST's Cloud Computing Security Reference Architecture document outlines the 6 key steps of NIST's Risk Management Framework in a Cloud Ecosystem[11] as follows:

Step 1: Classify information security based on impact analysis.
Step 2: Define information security controls baseline relative to categorisation.
Step 3: Deploy information security controls baseline.
Step 4: Assess information security controls to establish baseline implementation accuracy.
Step 5: Authorise information system controls access based on access requirements.
Step 6: Continually monitor information security controls for configuration drift.

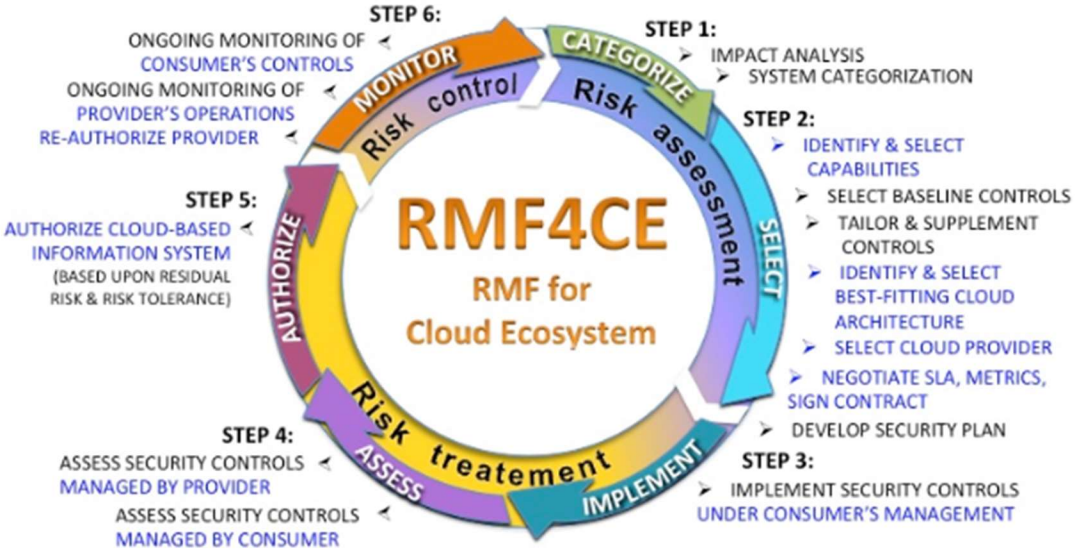


Figure 1. NIST Risk Management Framework in a Cloud Ecosystem [11]

[10] NIST.gov [2019] *NIST Cloud Computing Security Reference Architecture* https://csrc.nist.gov/publications/detail/sp/500-299/draft [Accessed 5th December 2019]
[11] NIST.gov [2019] *Figure 1. NIST Risk Management Framework in a Cloud Ecosystem* https://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity [Accessed 5th December 2019]

Cloud Security Alliance (CSA)

Security and Risk Management[12]

This document focus on *'the core components of an organization's Information Security Program to safeguard assets and detect, assess, and monitor risks inherent in operating activities'* (Warsinkse, 2019).

CST are utilising this management strategy to ensure a secure Cloud Deployment, focussing on the following key areas:

- **Governance Risk & Compliance**
- **Privilege Management Infrastructure**
  - Identity Management
  - Authentication Services
  - Authorization Services
- **Threat & Vulnerability Management**
  - Compliance Testing
  - Vulnerability Management
  - Penetration Testing
  - Threat Management
- **Infrastructure Protection Services**
  - Server Protection
  - End-Point Protection
  - Network Protection
  - Application Protection
- **Data Protection**
  - Data Leakage Prevention
  - Cryptographic Services
- **Policies & Standards**

Security Trust Assurance and Risk (STAR) [13]

CSA's Cloud Customer portal[14] provides:

- STAR Registry[15] detailing CSP security, privacy and compliance posture
- STAR Foundation tools to complete a CSA Governance, Risk Management & Compliance (GRC) self-assessment including:
  - Cloud Controls Matrix (CCM) [16]
  - Consensus Assessment Initiative Questionnaire (CAIQ) [17]
  - Code of Conduct GDPR Compliance [18]

CST will utilise the Consensus Assessment Initiative Questionnaire (CAIQ) to self-evaluate or granular cloud requirements.

CST will utilise the STAR Registry to analyse and evaluate CSP's.

---

[12] CloudSecurityAlliance.org [2019] *CSA Security & Risk Management* https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/ [Accessed 5th December 2019]

[13] CloudSecurityAlliance.org [2019] CSA *Security Trust Assurance and Risk (STAR)* https://cloudsecurityalliance.org/star/ [Accessed 5th December 2019]

[14] CloudSecurityAlliance.org [2019] *CSA Cloud Customers Portal* https://cloudsecurityalliance.org/star/cloud-customer/ [Accessed 5th December 2019]

[15] CloudSecurityAlliance.org [2019] *CSA STAR Registry* https://cloudsecurityalliance.org/star/registry/ [Accessed 5th December 2019]

[16] CloudSecurityAlliance.org [2019] *CSA Cloud Controls Matrix v3.0.1* https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/ [Accessed 5th December 2019]

[17] CloudSecurityAlliance.org [2019] *CSA Consensus Assessment Initiative Questionnaire (CAIQ)* https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/ [Accessed 5th December 2019]

[18] CloudSecurityAlliance.org [2019] *CSA GDPR Center of Excellence Home* https://gdpr.cloudsecurityalliance.org/resource-center/csa-code-of-conduct-for-gdpr-compliance/ [Accessed 5th December 2019]

International Organization for Standardization (ISO)

ISO/IEC 19086-1 Cloud computing — Service level agreement (SLA) framework [19]

The Service Level Agreement (SLA) between CST and the CSP needs to be clearly understood by both parties as the CSP will provide a complete infrastructure services stack. Key SLA components include:

Cloud SLA Best Practices

- **General:** With the varying, complex, interwoven nature of today's CSP's cloud offerings, there may be many separate SLA documents to be reviewed and understood.
- **Design:** CSP's provide Cloud services SLA's online. A review of these documents will be required as part of the CSP evaluation process.
- **Evaluation and Acceptance:** When CST agrees to a Cloud SLA's, acceptance is normally made online by registering for the CSP service and agreeing to the terms of service
- **Implementation and Execution:** CST will have to monitor all cloud services to ensure they are operating as per SLA. This will require initial configuration and fine-tuning.
- **Roles and Responsibilities:** CST and the CSP need to clearly understand their respective Roles and Responsibilities and identify who is accountable for which component

Cloud SLA Content Areas

- **Availability:** This defines the expected uptime/running time of a service. CSP will define the availability and CST will have to monitor the service to ensure the CSP in in compliance with SLA
- **Response Time:** This defines the time taken from when a request is made to a cloud service to when the cloud service provides a response.
- **Cloud Service Capacity:** This includes physical storage, vRAM, and vCPU, and also includes network capacity and data centre locations. CSP capacity will be included in the CSP evaluation
- **Elasticity:** The ability to dynamically allocate capacity based on demand. This includes storage, vRAM, vCPU, network as well as Load Balancer services.
- **Protection of Personally Identifiable Information (PII):** CSP must ensure all PII is securely managed as per GDPR requirements
- **Information Security:** With the transition of trust from CST to the CSP to provide Cloud services, CST must ensure the following Information Security components are managed appropriately
    - Service Monitoring
    - Roles and responsibilities
    - Availability
    - Protection of PII
    - Termination of service
    - Support
    - Service reliability
    - Data backup and restore
    - Data management
    - Attestations, Certifications, Audits
- **Cloud Service Support:** CST will include CSP support offerings in the evaluation process
- **Governance:** Defines the metrics, processes and standards to ensure CST is compliant will all regulations, standards and governance.
- **Service Reliability:** The section includes the CSP's Service Resilience/Fault Tolerance, Backup and Restore, and Disaster Recovery policies, procedures and services all of which will be important to CST for Business Continuity Planning.
- **Data Management:** Defines the processes, metrics, services the CSP employee to ensure compliant Data Management policies.

[19] ISO.org [2016] *Information technology - Cloud computing - Service level agreement (SLA) framework* https://standards.iso.org/ittf/PubliclyAvailableStandards/c067545_ISO_IEC_19086-1_2016.zip [Accessed 5th December 2019]

Cloud Service Provider Evaluation

For over 10 years Cloud Service Providers (CSP) have provided a combination of On-Premises, Off-Premises/On-Cloud and Hybrid Cloud models with IaaS, PaaS and SaaS services to market. According to Crisp Research[20], currently the top 3 CSP's are Amazon Web Services (AWS)[21], Microsoft Azure [22], and Google Cloud Platform [23].

This CSP evaluation will focus on CyberSecure.Team's Solution Functional Requirements developed from the C-Board Requirements to identify a preferred CSP.

Cyber-Attack Resilience	**AWS**	**Azure**	**GCP**
a. Defense in Depth	Y	Y	Y
b. Domain Name Service Security (DNSSEC)	Y	Y	Y
c. Data Breach Prevention	Y	Y	Y
d. Distributed Denial-of-Service (DDoS) Prevention	Y	Y	Y
e. Economic Denial-of-Service (EDoS) Prevention	Y	Y	Y
f. Abusive Bot/Botnet Prevention	Y	Y	Y
Secure Scalable Cost-Effective Platform			
a. Broad Network Access	Y	Y	Y
b. Global 24x7x365 Availability	Y	Y	Y
c. On-Demand Self-Service	Y	Y	Y
d. Measured Services	Y	Y	Y
e. Pay-as-you-Go Pricing Model	Y	Y	Y
f. Resource Pooling	Y	Y	Y
g. Capacity for Anticipated Growth	Y	Y	Y
h. Burst Capacity	Y	Y	Y
Confidentiality, Integrity and Availability			
a. Data-in-Transit: End-to-End Secure Socket Layer (SSL) Encryption	Y	Y	Y
b. Data-at-Rest: Virtual Machine Disk	Y	Y	Y
c. Virtual Machine Image on Disk Encryption	Y	Y	Y
i. Data on Disk Encryption	Y	Y	Y
ii. Secure Encryption Key Management	Y	Y	Y
d. Rapid Elasticity	Y	Y	Y
e. Load Balancing	Y	Y	Y
f. Auto Scaling	Y	Y	Y
g. Redundancy	Y	Y	Y
h. Backup Management	Y	Y	Y

Table 5. Solution Functional Requirements [24]

[20] Crisp Research [2019] *Cloud Computing Vendor & Service Provider Comparison* https://d1.awsstatic.com/analyst-reports/Report_CVU_CC_AWS_ENGL_final.pdf?trk=ar_card [Accessed 5th December 2019]
[21] Amazon Web Services [2019] *Amazon Web Services (AWS)* https://aws.amazon.com/ [Accessed 5th December 2019]
[22] Microsoft Azure [2019] *Microsoft Azure* https://azure.microsoft.com/ [Accessed 5th December 2019]
[23] Google Cloud Platform [2019] *Google Cloud Platform* https://cloud.google.com/ [Accessed 5th December 2019]
[24] Taaffe, Jonathon [2019] *Table 5. Solution Functional Requirements* [Created 5th December 2019]

Compliance Requirements	AWS	Azure	GCP
a. National Institute of Standards and Technology (NIST) 800-171	Y	Y	Y
b. Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)	Y	Y	Y
c. ISO 27017 Information Security Management System (ISMS) Cloud	Y	Y	Y
d. EU General Data Protection Regulation	Y	Y	Y
e. Department of Defense (DoD) Cloud Computing Security Requirements	Y	Y	Y
f. Experience providing services to government departments	Y	N	N
Infrastructure			
a. Model: Off-Premises/On-Cloud	Y	Y	Y
b. Service: IaaS	Y	Y	Y
Web Application			
a. Role-Based Access Control	Y	Y	Y
b. 2 Factor Authentication	Y	Y	Y
c. Corporate Password Policy Alignment	Y	Y	Y
d. Create, Read, Update and Delete Content	Y	Y	Y

Table 5. Solution Functional Requirements [24] (contd.)

From the CSP analysis against CyberSecure.Team's Solution Functional Requirements, each of the Top 3 CSP's provide all required services. The only differentiator is regarding 'Experience providing services to government departments. This is important to CST as it has a number of government contracts and a CSP with experience providing services to government departments is very important.

Chosen Provider: Amazon Web Services (AWS)

For over 10 years Amazon Web Services (AWS) has been the dominating Cloud Service Provider (CSP). With service maturity brings stability, certainty and a reputation that other CSP's are striving for.

AWS are still first to market with many new Cloud-based services. AWS also provides a specific Cloud Platform for Government; GovCloud. To provide this service, AWS complies with the following regulations:

- FedRAMP High baseline
- DOJ's Criminal Justice Information Systems (CJIS) Security Policy
- U.S. International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)
- Department of Defense (DoD) Cloud Computing Security Requirements Guide
- FIPS 140-2, IRS-1075

Secure Architecture

Domain Name Registration – Name.com

Domain Name

CyberSecure.Team Domain Name has been registered with Name.com Domain Name Registrar. This is the root Domain Name for CyberSecure.Team's secure cloud web application.

Domain Registrar	Name.com
Domain Registrar URL	https://www.name.com/
Registered Domain Name	cybersecure.team

Account Security

To secure the Name.com account, take the following steps:

Account Settings

1. Log in to Name.com > navigate to General > Account Settings
2. Under 'EU Citizen Default Whois Privacy' ensure 'Yes, show my personal information in WhoIs Lookups ' is NOT selected
3. Under 'Automatic Advanced Security' click 'Enable Automatic Advanced Security'
4. Under 'Contact Change Transfer Lock' ensure 'Opt-out of the 60-day domain transfer lock' is NOT selected

Email Notifications

1. Log in to Name.com > navigate to General > Email Notifications
2. Under 'Renewal Notification Settings' enable each of the following

   ✓ Email me the day before my services expire
   ✓ Email me on the day that my services expire
   ✓ Email me prior to removal of my expired services

3. Under 'Security Notification Options' enable the following

   ✓ Send Email Notification on Failed Login Attempt

4. Under 'Additional Security Options' enable the following

   ✓ Allow Password Reset Email (Recommended)

Default Account Contacts

1. Log in to Name.com > navigate to General > Default Account Contacts
2. Ensure the following tabs have the correct contact information listed

   - Registrant
   - Administrative
   - Technical
   - Billing

Account Settings Summary

Setting	Status	Description
EU Citizen Default Whois Privacy	Enabled	Contact information unavailable from WhoIs Lookups
Advanced Security	Enabled	• Whois Privacy • Domain Lock Plus
ICANN Contact Change Transfer Lock	Enabled	Changes to registrant contact information triggers 60-day domain transfer lock
Security Notification Options	Enabled	• Send Email Notification on Failed Login Attempt • Allow Password Reset Email
Account Contacts	Registrant Administrative Technical Billing	*Ensure correct contacts are listed*
Default TLD Name Servers	gabe.ns.cloudflare.com june.ns.cloudflare.com	Name Server services provided by CloudFlare
DNS Domain Name Servers	AWS Route53	DNS Domain Name Services provided by Amazon Route53 DNS Services
Account Level IP Address Access Restrictions	Enabled	Local host Public IPv4 IP
Account Password	Complex	Alpha, numeric, special characters
Two Step Verification	Enabled	Password and Authenticator verification code required
Domain Lock Plus	Enabled	• Restrict domain contact information changes • Restrict domain transfer • Additional 2 Factor Authentication required to modify Domain settings
Emergency Recovery Access	Enabled	Use default administrative contact phone number

Table 6. Name.com Account Settings [25]

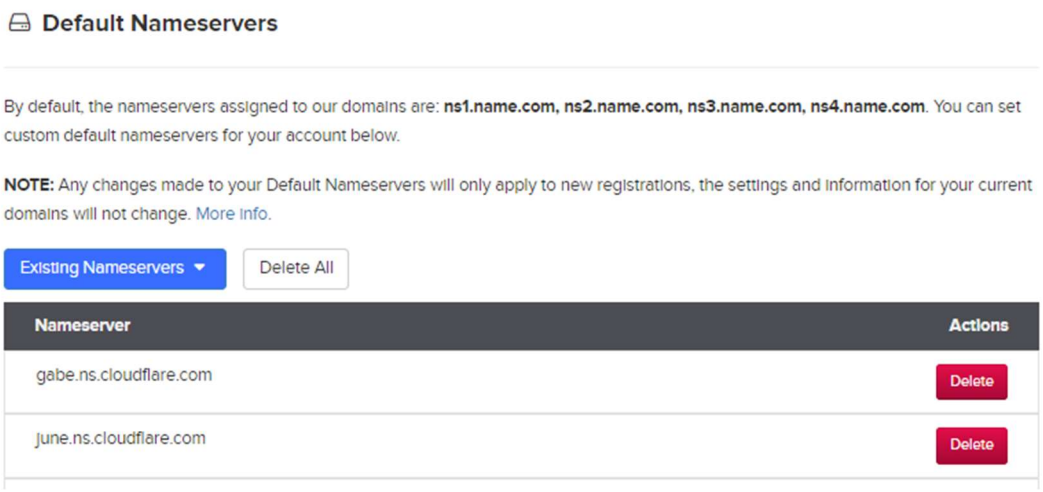
[25] Taaffe, Jonathon [2019] *Table 6. Name.com Account Settings* [Created 5th December 2019]

Nameservers

Cloudflare.com was chosen to provide Web Site and Infrastructure Security (see following section for details), the Default Nameservers on Name.com must be configured as follows:

1. Log in to Name.com > navigate to Account Settings > Default Nameservers
2. Under ‘Nameserver’ enter gabe.ns.cloudflare.com > click Add Nameserver
3. Under ‘Nameserver’ enter june.ns.cloudflare.com > click Add Nameserver

   Confirm the DNS Nameserver configuration on Name.com is as follows:



Security Settings

1. Navigate to Security > Security Settings
2. Under ‘Security Notification Options' ensure the following is selected

   ✓ Send Email Notification on Failed Login Attempt

3. Under 'Account Level IP Address Access Restrictions' > 'Allowed IP Addresses' > 'Add IP Address' > enter the public IP address of the device > Click Add IP

   Note: Current public IP address will be listed in this section

4. Under ‘Name.com API Access’ > select No to disallow use of the API

5. Navigate to Security > Change Password and ensure a complex alpha, numeric, special character password is configured

6. Navigate to Security > Two Step Verification and enable Password and Authenticator verification.
7. Under ‘Domain Lock Plus' select the following

   ✓ Restrict domain contact information changes
   ✓ Restrict domain transfer
   ✓ Additional 2 Factor Authentication required to modify Domain settings

8. Under 'Emergency Recovery Access' select the following

   ✓ Yes, use recovery phone

Web Security – Cloudflare.com

As documented in Table 2. Solution Functional Requirements, systems and services must be deployed to ensure Cyber-Attack Resilience.

The following is a summary of these specific requirements relevant to Web Infrastructure and Website Security:

Category	Functional Requirements
Cyber-Attack Resilience	Domain Name Service Security (DNSSEC) Distributed Denial-of-Service (DDoS) Prevention Economic Denial-of-Service (EDoS) Prevention Abusive Bot/Botnet Prevention
Secure Scalable Cost-Effective Platform	Broad Network Access Resource Pooling • Capacity for Anticipated Growth • Burst Capacity
Confidentiality, Integrity and Availability	Data-in-Transit: End-to-End Secure Socket Layer (SSL) Encryption Rapid Elasticity • Load Balancing • Auto Scaling

Table 7. Web Infrastructure and Website Security Requirements [26]

[26] Taaffe, Jonathon [2019] *Table 7. Web Infrastructure and Website Security Requirements* [Created 5th December 2019]

Security Services

Researching web infrastructure security and website security service providers, Cloudflare [27] was identified as the industry leader in this domain. Cloudflare also provides the following required services:

- ✓ SSL/TLS Encryption[28]: HTTPS End-to-End browser to web application encryption, mitigating man-in-the-middle attacks, packet sniffing, etc.
- ✓ DDoS Mitigation[29]: Prevent websites and web infrastructure from denial of service attacks.
- ✓ Anycast Network[30]: Absorbs and globally distributes DDoS traffic.
- ✓ DNS Security (DNSSEC) Protection[31]: Guarantees traffic routing to exact servers, mitigating "man-in-the-middle" attacks.
- ✓ Load Balancing[32]: Provides load balancing, geographic routing, and monitoring with failover
- ✓ Content Delivery Network (CDN)[33]: Geographically distributed infrastructure providing highspeed Internet content delivery.

As Cloudflare can provide 100% of the web infrastructure and website security requirements for this deployment and offers these services as part of their Free-Tier offering, CST chose Cloudflare.com as its internet services security provider.

Account Security

As previously mentioned Cloudflare.com's Free Tier will provide all required security services.

Two Factor Authentication has been enabled for the primary account login and enforced for all other members. The following sections outline the Cloudflare.com configuration for the cybersecure.team domain with Security Solution Functional Requirements highlighted in green.

Category	Option	Setting
Overview	Advanced Actions	Cloudflare Services enabled for Site
DNS	Nameservers	NS gabe.ns.cloudflare.com NS june.ns.cloudflare.com
DNS	DNSSEC	Enabled: Protects DNS zone transfers
DNS	CNAME Flattening	Enabled: Required to point to an AWS Elastic Load Balancer
SSL/TLS\Overview	Encryption Mode	Full: End-to-End encryption with a self-signed web server certificate.
SSL/TLS \Edge Certificates	Universal SSL	Hosts: *.cybersecure.team, cybersecure.team Type: Universal Status: Active Certificate: ECDSA with SHA256
SSL/TLS \Edge Certificates	Always use HTTPS	Enabled: Redirect all http:// requests to https://

[27] Cloudflare.com [2019] *The Integrated Global Cloud Platform* https://www.cloudflare.com/ [Accessed 5th December 2019]
[28] Cloudflare.com [2019] *Cloudflare Free SSL/TLS* https://www.cloudflare.com/ssl/ [Accessed 5th December 2019]
[29] Cloudflare.com [2019] *What is a DDoS Attack?* https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ [Accessed 5th December 2019]
[30] Cloudflare.com [2019] *Cloudflare Global Anycast Network* https://www.cloudflare.com/network/ [Accessed 5th December 2019]
[31] Cliudflare.com [2019] *DNSSEC Protection* https://www.cloudflare.com/dns/dnssec/ [Accessed 5th December 2019]
[32] Cloudflare.com [2019] *Cloudflare Load Balancing* https://www.cloudflare.com/load-balancing/ [Accessed 5th December 2019]
[33] Cloudflare.com [2019] *What is a CDN?* https://www.cloudflare.com/learning/cdn/what-is-a-cdn/ [Accessed 5th December 2019]

SSL/TLS \Edge Certificates	HTTP Strict Transport Security (HSTS)	Status: On Max-Age: 0 (Disable) Include subdomains: Off Preload: Off
SSL/TLS \Edge Certificates	Opportunistic Encryption	Improve HTTP/2 performance
SSL/TLS \Edge Certificates	TLS 1.3	Enabled
SSL/TLS \Edge Certificates	Automatic HTTPS Rewrites	All http:// web resource requests automatically changed to https://
SSL/TLS \Edge Certificates	Authenticated Origin Pulls	Web server certificate required for origin pull authentication.
Firewall	Managed Rules	Cloudflare DDoS Protection Enabled for: HTTP Flood UDP Flood SYN Flood ACK Flood QUIC Flood
Caching	Caching Level	Standard
Caching	Browser Cache Expiration	4 Hours
Caching	Always Online	Enabled: Static pages served from Cloudflare cache
Network	HTTP/2	Enabled: Improve web page load time
Network	HTTP/3 (with QUIC)	Enabled: Improve web page load time
Network	0-RTT Connection Resumption	Enabled: Improve client reconnects
Network	IP Geolocation	Enabled: Include country code with each request

Table 80. Cloudflare.com Configuration [34]

[34] Taaffe, Jonathon [2019] *Table 8. Cloudflare.com Configuration* [Created 5th December 2019]

Cloud Services – AWS.amazon.com

Required Services

CyberSecure.Team will configure an AWS non-Default Virtual Private Cloud (VPC) [35] in the EU Ireland Region, spanning multiple Availability Zone's (AZ)[36] with Public Subnet's for Elastic Application Load Balancing (ELB)[37] and Web Services, and Private Subnet's for AWS Relational Database Services [38].

AWS Security Groups (SG)[39] will be configured to only allow specific inbound/outbound network traffic to/from AWS EC2 Virtual Machine Instances[40].

A secure custom AWS Machine Image (AMI)[41] will be created and stored in AWS which will be used by an AWS Auto Scaling Group (ASG)[42] for Elastic Load Balancing (ELB)[43] and for Burst Capacity[44].

For Data-in-Transit, SSL Encryption will be configured for End-to-End Browser to Web Application security.

Utilising AWS Certificate Manager (ACM)[45] SSL Certificates will be configured on the Origin Web Server Instances, the AWS Elastic Application Load Balancer (ELB) and the Front-end Web Infrastructure. AWS Shield[46] will be configured to mitigate Distributed-Denial-of-Service DDoS attacks.

For Data-at-Rest, AWS Key Management Services (KMS) [47] will be used for encrypting AWS Elastic Block Storage (EBS)[48] attached to the AWS Machine Image's. For AWS Relational Database Services, the Database contents will be encrypted[49].

---

[35] Amazon Web Services [2019] *AWS Virtual Private Cloud (VPC)* https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html [Accessed 5th December 2019]
[36] Amazon Web Services [2019] *AWS Regions, Availability Zones, and Local Zones* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html [Accessed 5th December 2019]
[37] Amazon Web Services [2019] *AWS Application Load Balancer* https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html [Accessed 5th December 2019]
[38] Amazon Web Services [2019] *AWS Relational Database Service* https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html [Accessed 5th December 2019]
[39] Amazon Web Services [2019] *AWS Security Groups* https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html [Accessed 5th December 2019]
[40] Amazon Web Services [2019] *AWS Virtual Machine Images* https://aws.amazon.com/ec2/instance-types/ [Accessed 5th December 2019]
[41] Amazon Web Services [2019] *AWS Machine Image* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html [Accessed 5th December 2019]
[42] Amazon Web Services [2019] *AWS Auto Scaling Group* https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html [Accessed 5th December 2019]
[43] Amazon Web Services [2019] *AWS Elastic Load Balancing* https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html [Accessed 5th December 2019]
[44] Amazon Web Services [2019] *AWS Burstable Performance Instances* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html [Accessed 5th December 2019]
[45] Amazon Web Services [2019] AWS Certificate Manager (ACM) https://aws.amazon.com/certificate-manager/ [Accessed 5th December 2019]
[46] Amazon Web Services [2019] *AWS Shield* https://aws.amazon.com/shield/ [Accessed 5th December 2019]
[47] Amazon Web Services [2019] *AWS Key Management Services* https://docs.aws.amazon.com/kms/latest/developerguide/overview.html [Accessed 5th December 2019]
[48] Amazon Web Services [2019] *AWS Elastic Block Storage* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html [Accessed 5th December 2019]
[49] Amazon Web Services [2019] *AWS Key Management Services* https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html [Accessed 5th December 2019]

Functional Requirements

This architecture will satisfy the following Solution Function Requirements

Cyber-Attack Resilience	AWS Service	Satisfied
Defense in Depth	AWS VPC Public Subnets Private Subnets AWS SG's	Yes
Data Breach Prevention	SSL Encryption EBS Encryption RDS Encryption	Yes
Distributed Denial-of-Service (DDoS) Prevention	AWS Shield	Yes
Economic Denial-of-Service (EDoS) Prevention	AWS Shield	Yes
Secure Scalable Cost-Effective Platform		
Broad Network Access	VPC Multi-AZ's	Yes
Global 24x7x365 Availability	VPC Multi-AZ's	Yes
Resource Pooling	AWS ELB AWS ASG	Yes
Capacity for Anticipated Growth	AWS	Yes
Burst Capacity	AWS AMI's	Yes
Confidentiality, Integrity and Availability		
Data-in-Transit: End-to-End Secure Socket Layer (SSL) Encryption	AWS Certificate	Yes
Data-at-Rest: EC2 and AMI	EBS Encryption	Yes
Data-at-Rest: RDS	RDS Encryption	Yes
Secure Encryption Key Management	AWS KMS	Yes
Rapid Elasticity	AWS ELB AWS ASG	Yes
Load Balancing	AWS ELB AWS ASG	Yes
Auto Scaling	AWS ELB AWS ASG	Yes
Redundancy	VPC Multi-AZ's	Yes
Backup Management: EC2	AWS AMI's	Yes
Backup Management: RDS	AWS RDS	Yes

Table 9. Solution Functional Requirements Architectural Components [50]

[50] Taaffe, Jonathon [2019] *Table 6. Solution Functional Requirements Architectural Components* [Created 5th December 2019]

Create an AWS Account

To access Amazon Web Services (AWS) you will require an AWS account and a credit card.

New AWS accounts include 12 months of free tier access. For details of the products and services available go to https://aws.amazon.com/free/

1. Go to https://aws.amazon.com/ > click Create an AWS Account
2. Fill in the following required details:

   - Email address
   - Password

     Password requirements:
     - ✓ be a minimum of 8 or more characters.
     - ✓ include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, non-alphanumeric symbols, for example !@#$%^&*()_+-=[]{}|'
     - ✓ not be identical to your AWS account name or email address

   - Confirm password
   - AWS account name
     - ✓ Choose a name for your account. You can change this name in your account settings after you sign up.

3. Click Continue
4. For the Account details fill in the following required fields:

   - Account type: Professional or Personal
   - Full name:
   - Phone number:
   - Country/Region:
   - Address:
   - City:
   - State / Province or region:
   - Postal code:

   ✓ Check here to indicate that you have read and agree to the terms of the AWS Customer Agreement

5. Click Create Account and Continue
6. On the Payment Information page enter all required details

   Note Regarding AWS Credit Card Access: We use your payment information to verify your identity and only for usage in excess of the AWS Free Tier Limits. We will not charge you for usage below the AWS Free Tier Limits. For more information, see the frequently asked questions.

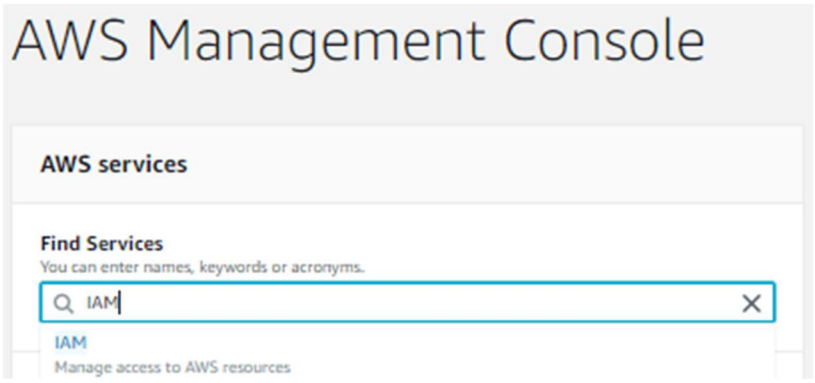
7. Click Verify and Add
8. Once you have verified your AWS account, you will then be able to log in

Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) provides for the configuration of secure access controls to AWS resources. IAM is used to manage Authentication and Authorisation to AWS resources.

As IAM manages all access to AWS resources, configure IAM as per AWS IAM Best Practices[51] as follows:

1. Login to AWS at https://console.aws.amazon.com/
2. On the AWS Management Console under AWS Services enter IAM in Find Services > click IAM



3. In the Identity and Access Management console under IAM users sign-in link click Customize
4. Enter a customised Account Alias for the IAM users sign-in link: > click Yes Create
5. Under Security Status configure the following options

   ✓ Delete your root access keys
   ✓ Activate MFA on your root account
   ✓ Create individual IAM users

   Create an Administrator account with access to the AWS console as follows

   - Username: Administrator
   - AWS access type: AWS Management Console access - with a password
   - Console password type: Complex
   - Require password reset: No

   ✓ Use groups to assign permissions

   Create an Administrators group into which Administrator accounts will be added as follows

   - Group name: Administrators
   - Policy: AdministratorAccess

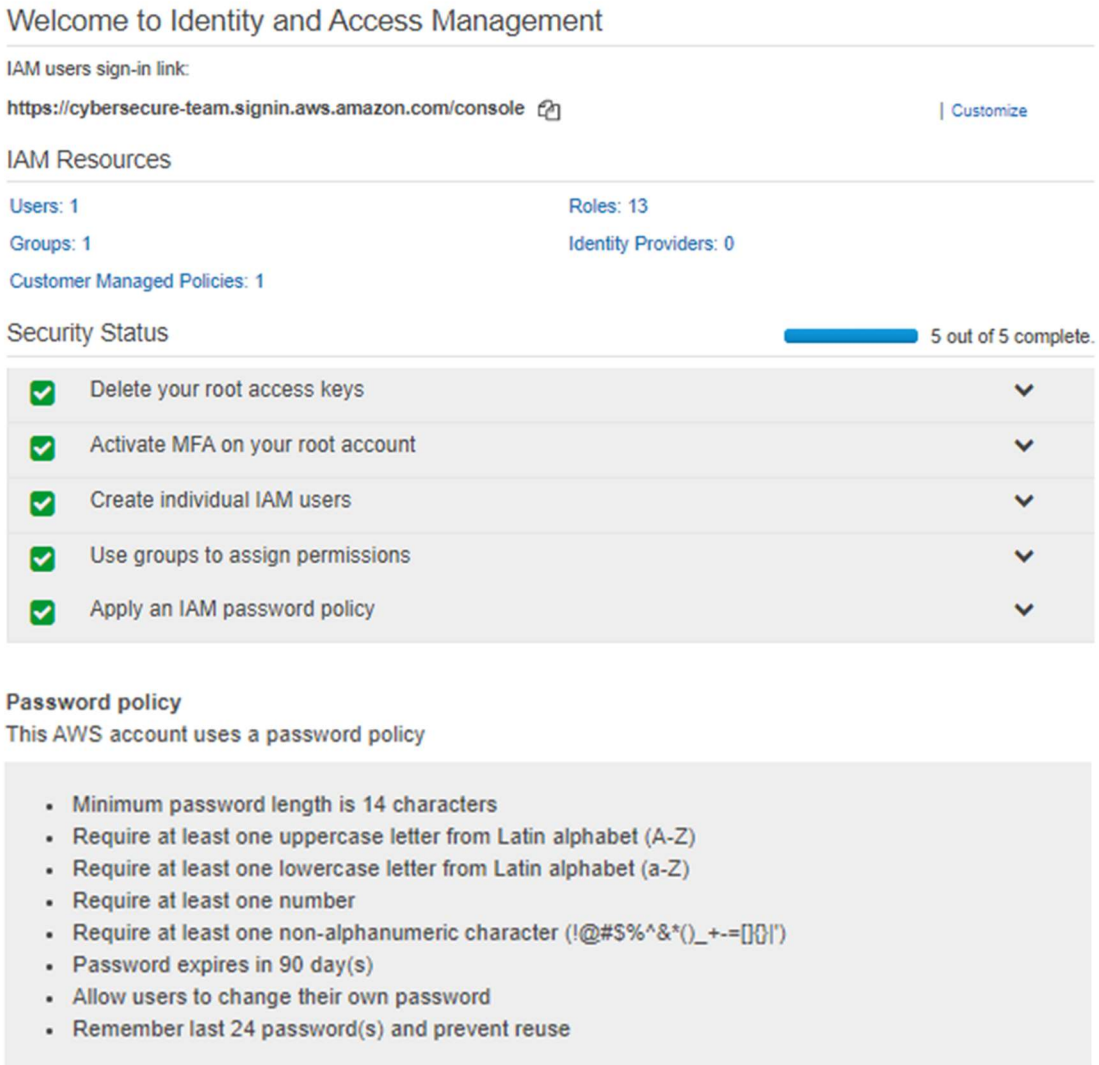
[51] AWS.Amazon.com [2019] IAM Best Practices https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html [Accessed 5th December 2019]

- ✓ Apply an IAM password policy

  Configure an IAM password policy as follows

  - ✓ Enforce minimum password length
    14 characters
  - ✓ Require at least one uppercase letter from Latin alphabet (A-Z)
  - ✓ Require at least one lowercase letter from Latin alphabet (a-z)
  - ✓ Require at least one number
  - ✓ Require at least one non-alphanumeric character (!@#$%^&*()_+-=[]{}|')
  - ✓ Enable password expiration
    Expire passwords in 90 day(s)
  - ✓ Allow users to change their own password
  - ✓ Prevent password reuse
    Remember 24 password(s)

Summary of AWS IAM configuration for cybersecure.team



Virtual Private Cloud (VPC)

AWS Virtual Private Cloud (VPC) is an AWS hosted virtual network in the cloud where AWS resources can be launched with the benefits of AWS scalable services.

Key AWS VPS concepts[52]

- VPC is a dedicated virtual cloud network for individual AWS accounts
- Private and public network subnets are assigned to the VPC
- Network route tables are assigned to the VPC subnets to route traffic
- Internet gateway, which is horizontally scaled, redundant, and highly available, provides a route from within the VPC and the internet

Naming Conventions

The following table explains the naming conventions used to name the VPC resources that will be configured

Service	Item	Acronym	Description
ACM	SSL Certificate	ALB-Cert	Application Load Balancer SSL Certificate
VPC	Elastic IP	EIP	Elastic IP
VPC	NAT Gateway	NAT-GW	NAT Gateway
VPC	Internet Gateway	Internet-GW	Internet Gateway
VPC	Multiple Availability Zones	MZ	Multi Zone
VPC	Environment	P	Production
VPC	Region	EW1	EU (Ireland) eu-west-1
VPC	Availability Zone	A, B or C	eu-west-1a/eu-west-1b/eu-west-1c
VPC	Subnets	PU	Public Subnet
VPC	Subnets	PR	Private Subnet
VPC	Subnet Route Table	PU-RT	Public Subnet Route Table
VPC	Subnet Route Table	PR-RT	Private Subnet Route Table
VPC	Security Groups	SG	Network traffic firewall
EC2	Bastion Host Instance	BH	Bastion Host
EC2	Database Instance	RDS	Relational Database Services
EC2	Web Server Instance	WS	Web Server
EC2	Amazon Machine Image	AMI	Custom Amazon Machine Image
EC2	Application Load Balancer	ALB	Application Load Balancer
EC2	Auto Scaling Launch Config	LC	Launch Configuration
EC2	Auto Scaling Group	ASG	Auto Scaling Group
EC2	Auto Scaling Target Group	TG	Target Group

Table 10. AWS VPC Naming Conventions [53]

Examples

VPC-MZ-CST-EW1	CyberSecure.Team Production Multi Zone VPC in EU (Ireland)
VPC-MZ-CST-EW1-A-BH	Bastion Host in eu-west-1a
VPC-MZ-CST-EW1-B-RDS	RDS Database Server in eu-west-1b
VPC-MZ-CST-EW1-C-WS	Web Server in eu-west-1c

Table 11. Naming Conventions Examples [54]

[52] Amazon.com [2019] *What is Amazon VPC?* https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html [Accessed 5th December 2019]
[53] Taaffe, Jonathon [2019] *Table 10. AWS VPC Naming Conventions* [Created 5th December 2019]
[54] Taaffe, Jonathon [2019] *Table 11. Naming Conventions Examples* [Created 5th December 2019]

Configuration

As per the AWS Required Services section above, the following architectural diagram details the AWS VPC configuration and associated AWS services that will be configured for this deployment.

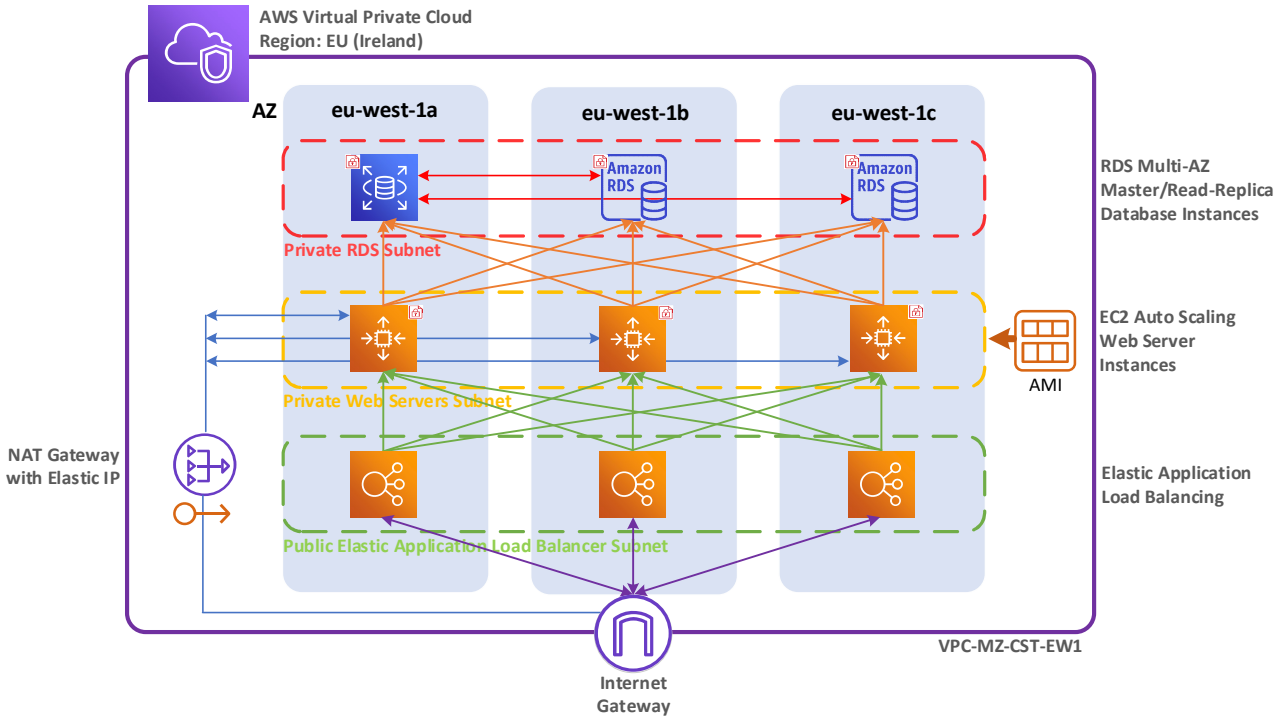


Diagram 1. AWS VPC Architectural Diagram[55]

And the following table details the VPC configuration that will be configured in the proceeding section. This VPC will be configured in the AWS Ireland Region, will be distributed across 3 Availability Zones and will have public and private subnets configured.

Item	Value		
Availability Zone	eu-west-1a	eu-west-1b	eu-west-1c
VPC Configuration	VPC with Public and Private Subnets		
IPv4 CIDR block	192.168.0.0/22		
IPv6 CIDR block	No IPv6 CIDR Block		
VPC name	VPC-MZ-CST-EW1		
Public subnet's CIDR	192.168.1.0/25	192.168.2.0/25	192.168.3.0/25
Public subnet name	VPC-MZ-CST-EW1-A-PU	VPC-MZ-CST-EW1-B-PU	VPC-MZ-CST-EW1-C-PU
Available IP Addresses	127	127	127
Private subnet's CIDR	192.168.1.128/25	192.168.2.128/25	192.168.3.128/25
Private subnet name	VPC-MZ-CST-EW1-A-PR	VPC-MZ-CST-EW1-B-PR	VPC-MZ-CST-EW1-C-PR
Available IP Addresses	127	127	127
Elastic IP Allocation	Yes		
Enable DNS hostnames	Yes		
Hardware tenancy	Default		

Table 12. VPC Configuration[56]

[55] Taaffe, Jonathon [2019] *Diagram 1. AWS VPC Architectural Diagram* [Created 5th December 2019]
[56] Taaffe, Jonathon [2019] *Table 12. VPC Configuration* [Created 5th December 2019]

Setup

This section includes the steps required to configure the following components for the non-Default VPC for CyberSecure.Team

a. Elastic IP
b. non-Default VPC
c. Classless Internet Domain Routing (CIDR) Block Configuration
d. NAT Gateway
e. Additional Subnets
f. Route Tables
g. Additional Security Groups

1. *Elastic IP Allocation*

An Elastic IP address is a static public IPv4 address reachable from the internet. It can be used to distribute IPv4 traffic to multiple nodes. If a node fails the Elastic IP will ensure no further traffic is routed to the failed node until it is fully operational.

a. Navigate to AWS Console > Services > VPC > Elastic IP's > Allocate New Address
b. For IPv4 address pool select Amazon pool and AWS will auto assign an Elastic IP address
c. In the Elastic IP console, edit the Elastic IP name field and enter VPC-MZ-CST-EW1-EIP

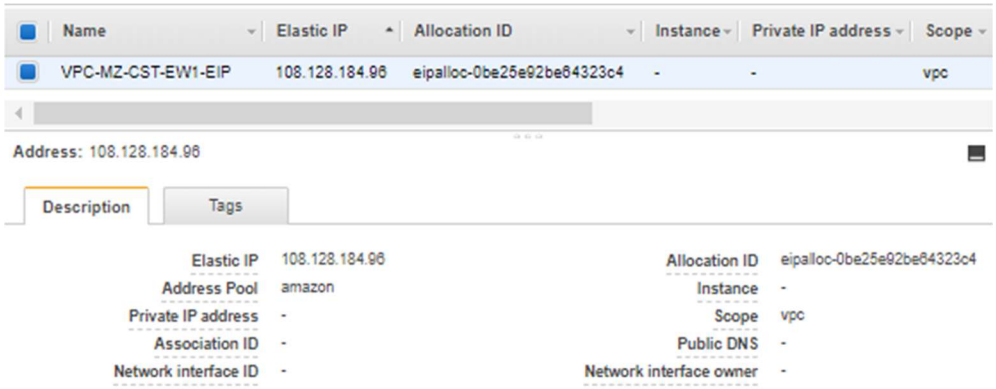


Image 1. Elastic IP Allocation[57]

2. *non-Default VPC*

The following components will be automatically created as part of creating a non-Default VPC

- Non-Default Subnets
- Security Groups
- Network ACLs
- Internet Gateways
- Egress Only Internet Gateways
- Route Tables
- Network Interfaces
- Peering Connections
- Endpoints

[57] Taaffe, Jonathon [2019] *Image 1. Elastic IP Allocation* [Created 5th December 2019]

a. Navigate to AWS Console > Services > VPC > VPC Dashboard > Launch VPC Wizard
b. Select VPC Configuration: VPC with Public and Private Subnets > click Select

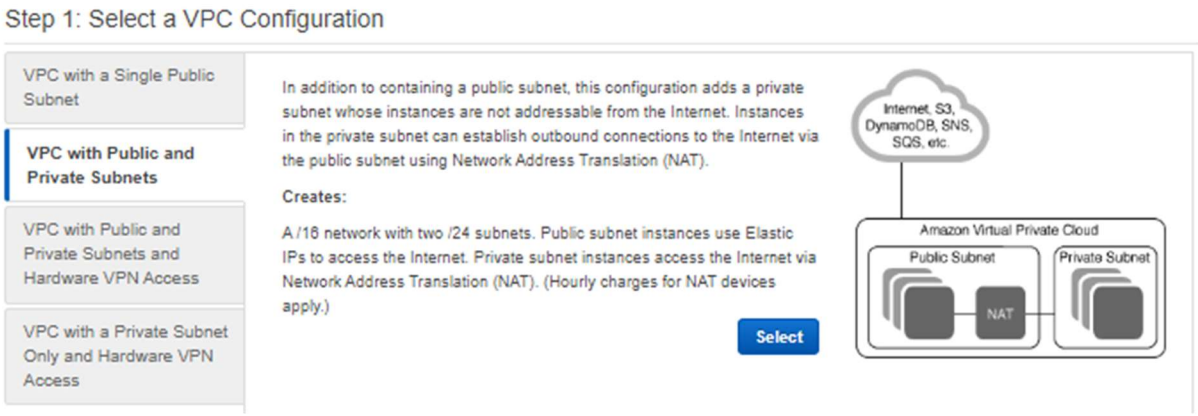


Image 2. Select VPN Configuration[58]

Regarding Class Internet Domain Routing (CIDR) Block Configuration

Using a CIDR Block of 192.168.0.0/22 provides for the following subnet and IP configuration

Availability Zone	eu-west-1a	eu-west-1b	eu-west-1c
Public Subnet IP Range	192.168.1.0/25	192.168.2.0/25	192.168.3.0/25
Number of IP Addresses	127	127	127
Private Subnet IP Range	192.168.1.128/25	192.168.2.128/25	192.168.3.128/25
Number of IP Addresses	127	127	127

Table 13. VPC CIDR Block Configuration [59]

c. The following table details the settings required to configure the VPC with Public and Private Subnets:

Item	**Value**
IPv4 CIDR block	192.168.0.0/22
IPv6 CIDR block	No IPv6 CIDR Block
VPC name	VPC-MZ-CST-EW1
Public subnet's IPv4 CIDR	192.168.1.0/25
Availability Zone	eu-west-1a
Public subnet name	VPC-MZ-CST-EW1-A-PU
Private subnet's IPv4 CIDR	192.168.1.128/25
Availability Zone	eu-west-1a
Private subnet name	VPC-MZ-CST-EW1-A-PR
Elastic IP Allocation	Select previously configured Elastic IP
Service endpoints	None
Enable DNS hostnames	Yes
Hardware tenancy	Default

Table 14. VPC Public and Private Subnets Configuration [60]

[58] Taaffe, Jonathon [2019] *Image 2. Select VPN Configuration* [Created 5th December 2019]
[59] Taaffe, Jonathon [2019] *Table 13. VPC CIDR Block Configuration* [Created 5th December 2019]
[60] Taaffe, Jonathon [2019] *Table 14. VPC Public and Private Subnets Configuration* [Created 5th December 2019]

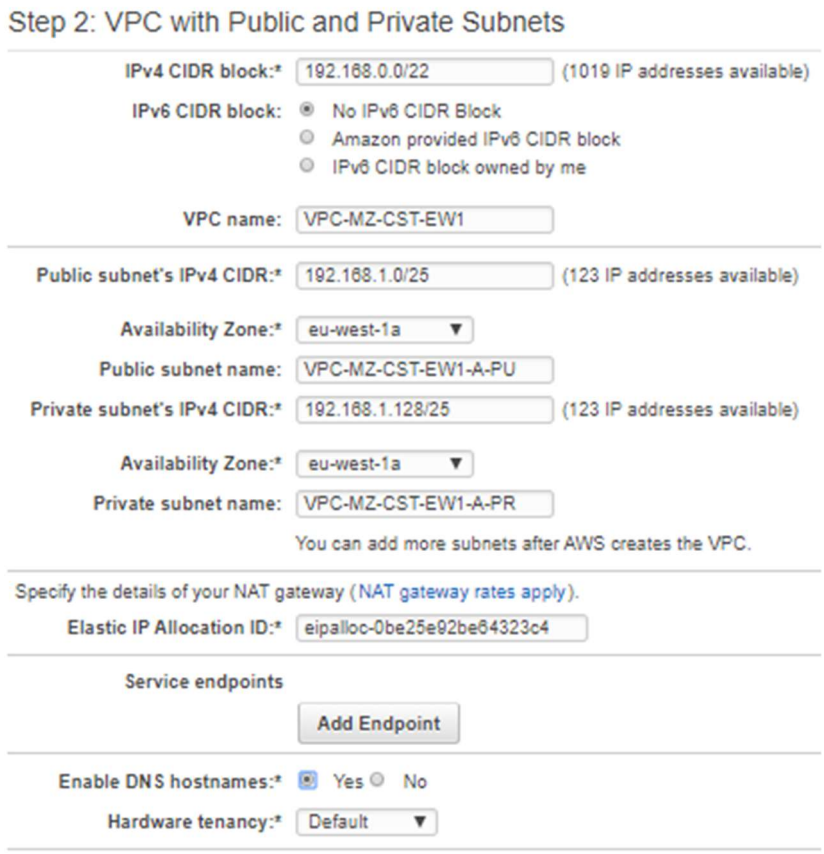


Image 3. Non-Default VPC Configuration[61]

d. Click Create VPC

Note: It will take a maximum of 5 minutes for the VPC to be configured

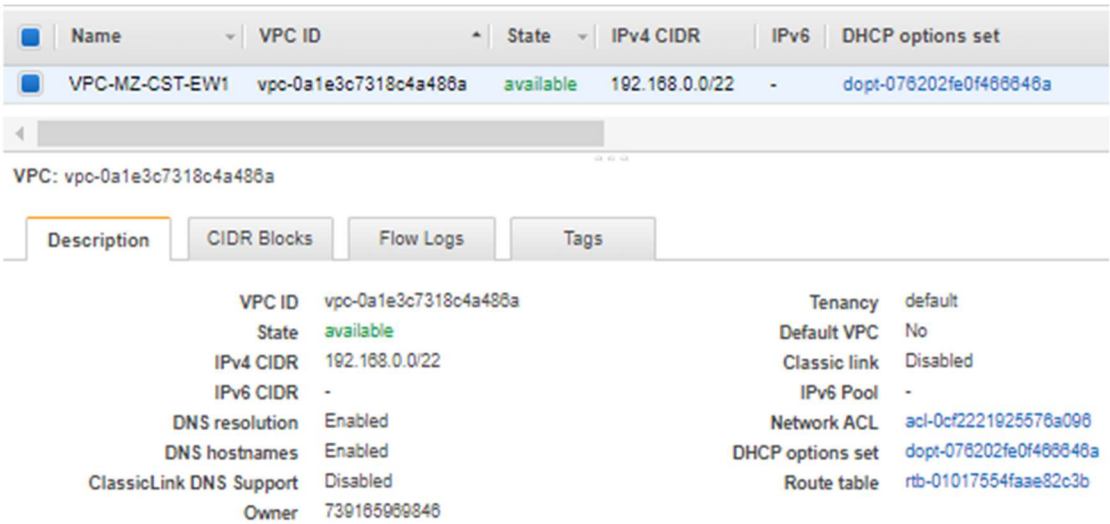


Image 4. Non-Default VPC Configuration[62]

[61] Taaffe, Jonathon [2019] *Image 3. Non-Default VPC Configuration*[Created 5th December 2019]
[62] Taaffe, Jonathon [2019] *Image 4. Non-Default VPC Configuration* [Created 5th December 2019]

Regarding Network Address Translation (NAT) Gateway

A NAT Gateway provides outbound internet connectivity from a Private Subnet in a VPC. A NAT gateway is configured as part of the non-Default VPC setup

Rename NAT Gateway

a. Navigate to AWS Console > Services > VPC > NAT Gateway's
b. Edit the NAT Gateway name field and enter VPC-MZ-CST-EW1-A-PU-NAT-GW

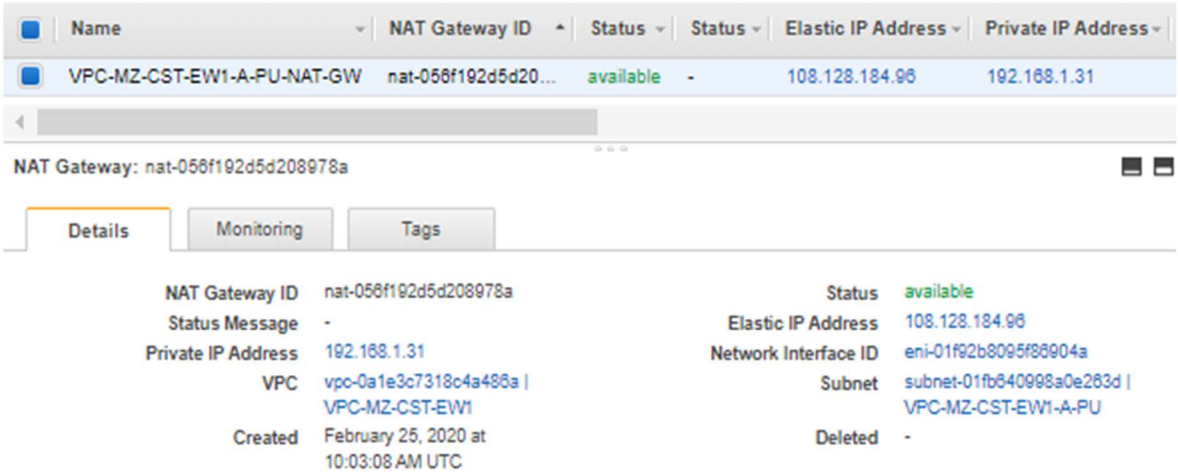


Image 5. NAT Gateway Configuration[63]

3. *Additional Subnets*

As part of the non-Default VPC configuration, one Private and one Public subnet have been created in the eu-west-1a Availability Zone (AZ). To avail of AWS redundancy and failover services additional Private and Public subnets should be created in the remaining Availability Zones in the region; eu-west-1b and eu-west-1c as follows:

eu-west-1b: Navigate to AWS Console > Services > VPC > Subnets > Create Subnet

eu-west-1b Public Subnet	
Name tag	VPC-MZ-CST-EW1-B-PU
VPC	VPC-MZ-CST-EW1
Availability Zone	eu-west-1b
VPC CIDRs	192.168.0.0/22
IPv4 CIDR block	192.168.2.0/25
eu-west-1b Private Subnet	
Name tag	VPC-MZ-CST-EW1-B-PR
VPC	VPC-MZ-CST-EW1
Availability Zone	eu-west-1b
VPC CIDRs	192.168.0.0/22
IPv4 CIDR block	192.168.2.128/25

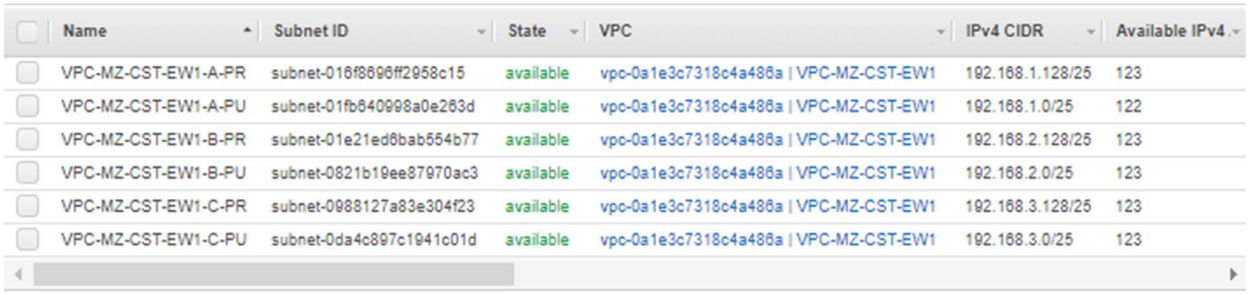
Table 15. Additional eu-west-1b VPC Public and Private Subnets[64]

[63] Taaffe, Jonathon [2019] *Image 5. NAT Gateway Configuration* [Created 5th December 2019]
[64] Taaffe, Jonathon [2019] *Table 15. Additional eu-west-1b VPC Public and Private Subnets* [Created 19th December 2019]

eu-west-1c: Navigate to AWS Console > Services > VPC > Subnets > Create Subnet

eu-west-1c Public Subnet	
Name tag	VPC-MZ-CST-EW1-C-PU
VPC	VPC-MZ-CST-EW1
Availability Zone	eu-west-1c
VPC CIDRs	192.168.0.0/22
IPv4 CIDR block	192.168.3.0/25
eu-west-1c Private Subnet	
Name tag	VPC-MZ-CST-EW1-C-PR
VPC	VPC-MZ-CST-EW1
Availability Zone	eu-west-1c
VPC CIDRs	192.168.0.0/22
IPv4 CIDR block	192.168.3.128/25

Table 16. Additional eu-west-1c VPC Public and Private Subnets [65]



Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4
VPC-MZ-CST-EW1-A-PR	subnet-016f8696ff2958c15	available	vpc-0a1e3c7318c4a486a | VPC-MZ-CST-EW1	192.168.1.128/25	123
VPC-MZ-CST-EW1-A-PU	subnet-01fb640998a0e263d	available	vpc-0a1e3c7318c4a486a | VPC-MZ-CST-EW1	192.168.1.0/25	122
VPC-MZ-CST-EW1-B-PR	subnet-01e21ed6bab554b77	available	vpc-0a1e3c7318c4a486a | VPC-MZ-CST-EW1	192.168.2.128/25	123
VPC-MZ-CST-EW1-B-PU	subnet-0821b19ee87970ac3	available	vpc-0a1e3c7318c4a486a | VPC-MZ-CST-EW1	192.168.2.0/25	123
VPC-MZ-CST-EW1-C-PR	subnet-0988127a83e304f23	available	vpc-0a1e3c7318c4a486a | VPC-MZ-CST-EW1	192.168.3.128/25	123
VPC-MZ-CST-EW1-C-PU	subnet-0da4c897c1941c01d	available	vpc-0a1e3c7318c4a486a | VPC-MZ-CST-EW1	192.168.3.0/25	123

Image 6. Available VPC Public and Private Subnets[66]

4. *Route Tables*

Route Tables are automatically created and applied when creating subnets. An Internet Gateway will be automatically assigned to a Public Subnet, and a NAT Gateway will be automatically assigned to a Private Subnet.

Routes Tables need to be assigned to the additional subnets created in the previous step as follows

Private Subnet Route Table Configuration

a. Navigate to AWS Console > Services > VPC > Route Tables
b. Select the 1st Route Table and click the Routes tab
c. On the Routes tab, under Target confirm NAT-*AWSID* is listed
   If NAT-*AWSID* is not listed select the other Route Table and confirm

   Note: NAT Gateways are only assigned to Private subnets

d. Edit the name field of the Route Table with a Target of NAT-*AWSID* and enter the following

   VPC-MZ-CST-EW1-PR-RT

[65] Taaffe, Jonathon [2019] *Table 16. Additional eu-west-1c VPC Public and Private Subnets* [Created 5th December 2019]
[66] Taaffe, Jonathon [2019] *Image 6. Available VPC Public and Private Subnets* [Created 5th December 2019]

Public Subnet Route Table Configuration

a. Navigate to AWS Console > Services > VPC > Route Tables
b. Select the 2nd Route Table and click the Routes tab
c. On the Routes tab, under Target confirm IGW-*AWSID* is listed
   If IGW-*AWSID* is not listed select the other Route Table and confirm

   Note: IGW is the Internet Gateway and is only assigned to Public Subnets

d. Edit the name field of the Route Table with a Target of IGW-*AWSID* and enter the following

   VPC-MZ-CST-EW1-PU-RT

Route Table Subnet Assignment

With the Private and Public Route Tables renamed, now assign the correct subnets to the correct Route Table

Private Route Table Subnet Association

a. Navigate to AWS Console > Services > VPC > Route Tables
b. Select the Private Route Table VPC-MZ-CST-EW1-PR-RT
c. Click the Subnets Association tab and click Edit Subnets
d. Select the following Private Subnets and click Save

   VPC-MZ-CST-EW1-A-PR
   VPC-MZ-CST-EW1-B-PR
   VPC-MZ-CST-EW1-C-PR

   Private Route Table Subnet Association should be as follows

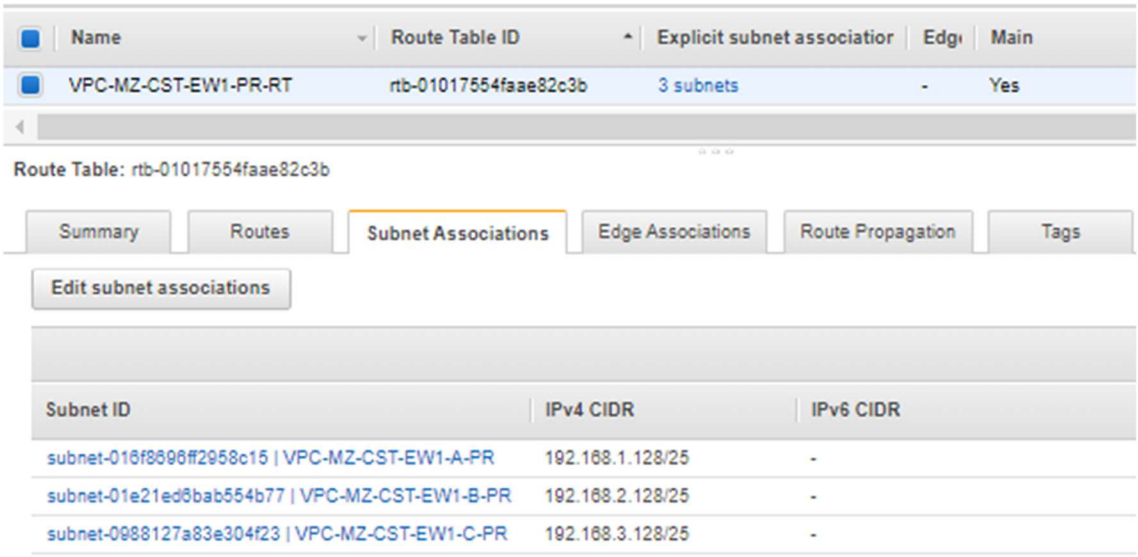


Image 7. Private Route Table Subnet Association[67]

[67] Taaffe, Jonathon [2019] *Image 7. Private Route Table Subnet Association* [Created 5th December 2019]

Public Route Table Subnet Association

a. Navigate to AWS Console > Services > VPC > Route Tables
b. Select the Public Route Table VPC-MZ-CST-EW1-PU-RT
c. Click the Subnets Association tab and click Edit Subnets
d. Select the following Public Subnets

VPC-MZ-CST-EW1-A-PU
VPC-MZ-CST-EW1-B-PU
VPC-MZ-CST-EW1-C-PU

Public Route Table Subnet Association should be as follows

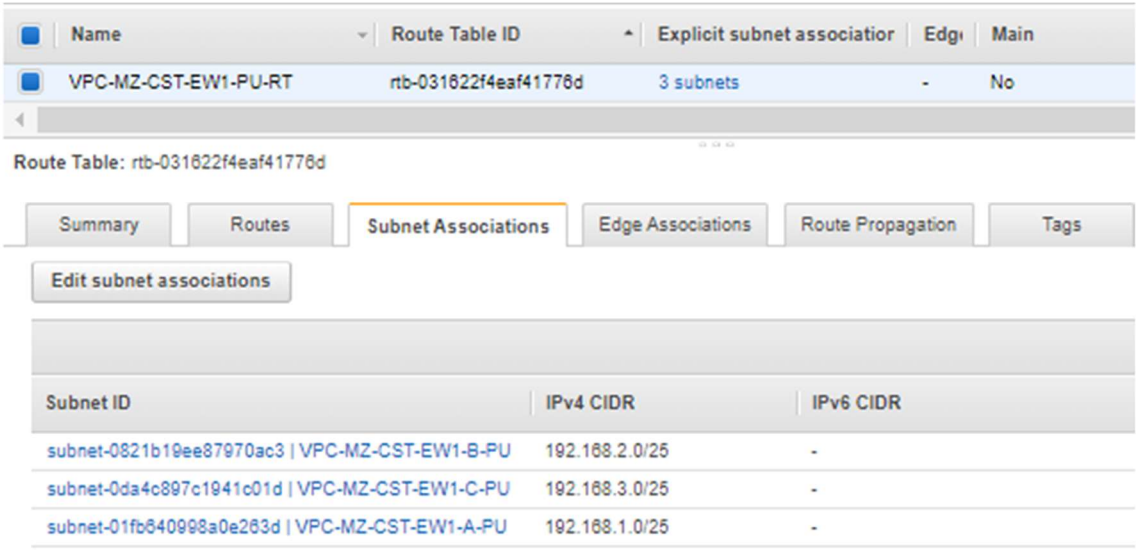


Image 8. Public Route Table Subnet Association[68]

[68] Taaffe, Jonathon [2019] *Image 8. Public Route Table Subnet Association* [Created 5th December 2019]

5. *Security Groups*

AWS Security Groups act as advanced firewalls with traffic restrictions applied at the instance level.

Unlike a firewall where an Allow or Deny rule applies to the whole subnet or VLAN, a Security Group is applied and assigned to EC2 Instances giving more granular control over network traffic filtering.

The following diagram is a high-level graphical representation of the Security Group (SG) mesh configuration:

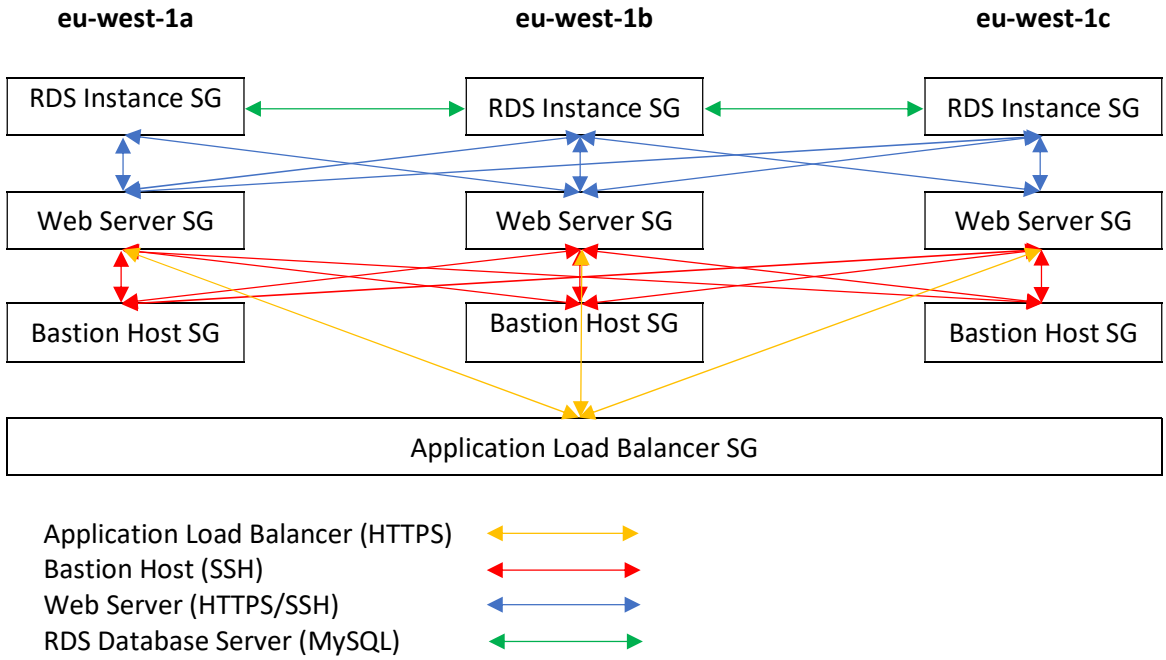


Diagram 2. High-Level Security Group (SG) Mesh Configuration[69]

As Security Groups are assigned at the instance level, the naming convention for Security Groups reflects the primary instance type that will use the Security Group as follows:

Instance Type	Region	Subnet	Security Group Naming Convention
Bastion Host	eu-west-1a	Public	VPC-MZ-CST-EW1-A-BH-SG
Web Server	eu-west-1a	Private	VPC-MZ-CST-EW1-A-WS-SG
RDS DB Server	eu-west-1a	Private	VPC-MZ-CST-EW1-A-RDS-SG
Bastion Host	eu-west-1b	Public	VPC-MZ-CST-EW1-B-BH-SG
Web Server	eu-west-1b	Private	VPC-MZ-CST-EW1-B-WS-SG
RDS DB Server	eu-west-1b	Private	VPC-MZ-CST-EW1-B-RDS-SG
Bastion Host	eu-west-1c	Public	VPC-MZ-CST-EW1-C-BH-SG
Web Server	eu-west-1c	Private	VPC-MZ-CST-EW1-C-WS-SG
RDS DB Server	eu-west-1c	Private	VPC-MZ-CST-EW1-C-RDS-SG
Application Load Balancer	Regional	Public	VPC-MZ-CST-EW1-ALB-SG

Table 17. Security Group Naming Convention [70]

[69] Taaffe, Jonathon [2019] *Diagram 1. High-Level Security Group (SG) Mesh Configuration* [Created 5th December 2019]
[70] Taaffe, Jonathon [2019] *Table 17. Security Group Naming Convention* [Created 5th December 2019]

Create Security Groups

Bastion Host (BH)
A Bastion Host Security Group must be configured for each AZ as follows:

a. Navigate to AWS Console > Services > EC2 > Security Groups > Create Security Group
b. Enter the following details to create the Bastion Host Security Group and click Create

   Security Group Name: VPC-MZ-CST-EW1-A-BH-SG
   Description: VPC-MZ-CST-EW1-A-BH-SG
   VPC: VPC-MZ-CST-EW1

c. Edit the name field of the Bastion Host Security Group and enter VPC-MZ-CST-EW1-A-BH-SG
d. Using the steps above, create 2 additional Bastion Host Security Groups for each AZ
e. Enter the following names for the additional Bastion Host Security Groups

Availability Zone	**eu-west-1b**	**eu-west-1c**
Security Group Name	VPC-MZ-CST-EW1-B-BH-SG	VPC-MZ-CST-EW1-C-BH-SG
Description	VPC-MZ-CST-EW1-B-BH-SG	VPC-MZ-CST-EW1-C-BH-SG
VPC	VPC-MZ-CST-EW1	VPC-MZ-CST-EW1

Table 18. Additional Bastion Host Security Groups[71]

Web Server (WS)
A Web Server Security Group must be configured for each AZ as follows:

a. Navigate to AWS Console > Services > EC2 > Security Groups > Create Security Group
b. Enter the following details to create the Web Server Security Group and click Create

   Security Group Name: VPC-MZ-CST-EW1-A-WS-SG
   Description: VPC-MZ-CST-EW1-A-WS-SG
   VPC: VPC-MZ-CST-EW1

c. Edit the name field of the Bastion Host Security Group and enter VPC-MZ-CST-EW1-A-WS-SG
d. Using the steps above, create additional Web Server Security Groups for each AZ
e. Enter the following names for the additional Bastion Host Security Groups

Availability Zone	**eu-west-1b**	**eu-west-1c**
Security Group Name	VPC-MZ-CST-EW1-B-WS-SG	VPC-MZ-CST-EW1-C-WS-SG
Description	VPC-MZ-CST-EW1-B-WS-SG	VPC-MZ-CST-EW1-C-WS-SG
VPC	VPC-MZ-CST-EW1	VPC-MZ-CST-EW1

Table 19. Additional Web Server Security Groups[72]

[71] Taaffe, Jonathon [2019] *Table 18. Additional Bastion Host Security Groups* [Created 5th December 2019]
[72] Taaffe, Jonathon [2019] *Table 19. Additional Web Server Security Groups* [Created 5th December 2019]

Relational Database Server (RDS)
An RDS Security Group must be configured for each AZ as follows:

a. Navigate to AWS Console > Services > EC2 > Security Groups > Create Security Group
b. Enter the following details to create the RDS Security Group and click Create

Security Group Name: VPC-MZ-CST-EW1-A-RDS-SG
Description: VPC-MZ-CST-EW1-A-RDS-SG
VPC: VPC-MZ-CST-EW1

c. Edit the name field of the Bastion Host Security Group and enter VPC-MZ-CST-EW1-A-RDS-SG
d. Using the steps above, create 2 additional RDS Security Groups for the eu-west-1b and eu-west-1c AZ's
e. Enter the following names for the additional Bastion Host Security Groups

Availability Zone	eu-west-1b	eu-west-1c
Security Group Name	VPC-MZ-CST-EW1-B-RDS-SG	VPC-MZ-CST-EW1-C-RDS-SG
Description	VPC-MZ-CST-EW1-B-RDS-SG	VPC-MZ-CST-EW1-C-RDS-SG
VPC	VPC-MZ-CST-EW1	VPC-MZ-CST-EW1

Table 20. Additional RDS Security Groups[73]

Application Load Balancer (ALB)
Only a single ALB Security Group is required which will span all 3 Availability Zones.

a. Navigate to AWS Console > Services > EC2 > Security Groups > Create Security Group
b. Enter the following details to create the RDS Security Group and click Create

Security Group Name: VPC-MZ-CST-EW1-ALB-SG
Description: VPC-MZ-CST-EW1-ALB-SG
VPC: VPC-MZ-CST-EW1

c. Edit the name field of the Application Load Balancer Security Group and enter VPC-MZ-CST-EW1-ALB-SG

Security Group Summary Configuration

Name	Group ID	Group Name
VPC-MZ-CST-EW1-A-BH-SG	sg-0f819feb867e65531	VPC-MZ-CST-EW1-A-BH-SG
VPC-MZ-CST-EW1-A-RDS-SG	sg-0884728c3bb7af37c	VPC-MZ-CST-EW1-A-RDS-SG
VPC-MZ-CST-EW1-A-WS-SG	sg-0282ba8e7e1fc7931	VPC-MZ-CST-EW1-A-WS-SG
VPC-MZ-CST-EW1-ALB-SG	sg-0f0946550c493b07b	VPC-MZ-CST-EW1-ALB-SG
VPC-MZ-CST-EW1-B-BH-SG	sg-078aef35dfd8c0e9b	VPC-MZ-CST-EW1-B-BH-SG
VPC-MZ-CST-EW1-B-RDS-SG	sg-09ce23880b678e2d0	VPC-MZ-CST-EW1-B-RDS-SG
VPC-MZ-CST-EW1-B-WS-SG	sg-05d0333b8384bba50	VPC-MZ-CST-EW1-B-WS-SG
VPC-MZ-CST-EW1-C-BH-SG	sg-0b3dc2aaa49ede92f	VPC-MZ-CST-EW1-C-BH-SG
VPC-MZ-CST-EW1-C-RDS-SG	sg-0fd333f154c6ee3b6	VPC-MZ-CST-EW1-C-RDS-SG
VPC-MZ-CST-EW1-C-WS-SG	sg-0532fd2662ff0a4dc	VPC-MZ-CST-EW1-C-WS-SG

Image 9. Security Group Summary Configuration[74]

[73] Taaffe, Jonathon [2019] *Table 20. Additional RDS Security Groups* [Created 5th December 2019]
[74] Taaffe, Jonathon [2019] *Image 9. Security Group Summary Configuration* [Created 5th December 2019]

Security Group Rules

With all required Security Groups created, Inbound and Outbound Rules need to be configured within each Security Group for each Instance Type.

Bastion Host Inbound Rules

A Bastion Host provides a single point for SSH access into the VPC Public and Private Subnets. The Bastion Host Security Group is configured to only allow Inbound SSH from the Public IPv4 Address of the Administrator's localhost.

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-A-BH-SG, click the Inbound Tab and click Edit
c. Enter the following Inbound Rule for the Bastion Host Security Group and click Save

Type	Protocol	Port	Source	Description
SSH	TCP	22	My IP	Inbound SSH from Administrators IPv4 Address

Table 21. Bastion Host Inbound Security Group Rule[75]

d. Select Security Group VPC-MZ-CST-EW1-B-BH-SG, click the Inbound Tab and click Edit
e. Enter the Inbound Rules for the Bastion Host Security Group listed in the table above and click Save

f. Select Security Group VPC-MZ-CST-EW1-C-BH-SG, click the Inbound Tab and click Edit
g. Enter the Inbound Rules for the Bastion Host Security Group listed in the table above and click Save

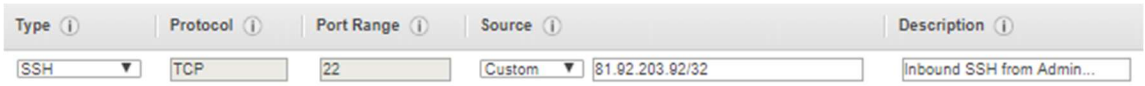


Image 10. Bastion Host Inbound Rule Configuration[76]

[75] Taaffe, Jonathon [2019] *Table 21. Bastion Host Inbound Security Group Rule* [Created 5th December 2019]
[76] Taaffe, Jonathon [2019] *Image 10. Bastion Host Inbound Rule Configuration* [Created 5th December 2019]

Bastion Host Outbound Rules

Outbound rules to allow outbound SSH from Bastion Hosts Security Group to Web Server Security Group.

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-A-BH-SG, click the Outbound Tab and click Edit
c. Enter the following Outbound Rules for the Bastion Host Security Group and click Save

Note1: To add additional Rules click Add Rule
Note2. Outbound HTTP/HTTPS is required for software updates

Type	Protocol	Port	Destination	Description
HTTP	TCP	80	Anywhere	Outbound HTTP to anywhere
HTTPS	TCP	443	Anywhere	Outbound HTTPS to anywhere
SSH	TCP	22	VPC-MZ-CST-EW1-A-WS-SG	Outbound SSH to A Web Server SG
SSH	TCP	22	VPC-MZ-CST-EW1-B-WS-SG	Outbound SSH to B Web Server SG
SSH	TCP	22	VPC-MZ-CST-EW1-C-WS-SG	Outbound SSH to C Web Server SG

Table 22. Bastion Host Outbound Security Group Rules[77]

d. Select Security Group VPC-MZ-CST-EW1-B-BH-SG, click the Outbound Tab and click Edit
e. Enter the Outbound Rules for the Bastion Host Security Group listed in the table above and click Save

f. Select Security Group VPC-MZ-CST-EW1-C-BH-SG, click the Outbound Tab and click Edit
g. Enter the Outbound Rules for the Bastion Host Security Group listed in the table above and click Save

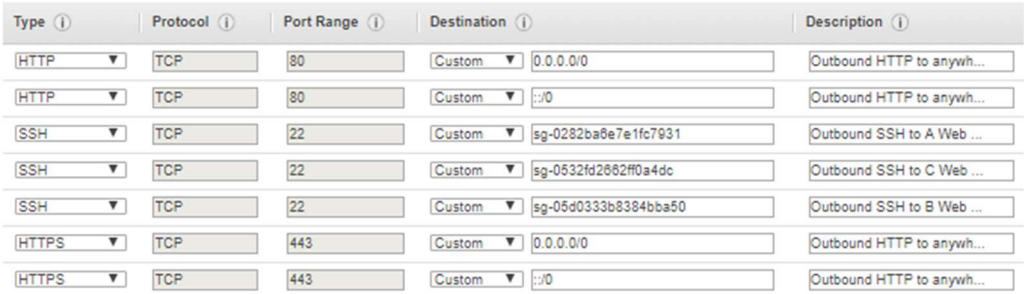


Image 11. Bastion Host Outbound Rules Configuration[78]

[77] Taaffe, Jonathon [2019] *Table 22. Bastion Host Outbound Security Group Rules* [Created 5th December 2019]
[78] Taaffe, Jonathon [2019] *Image 11. Bastion Host Outbound Rules Configuration* [Created 5th December 2019]

Web Server Inbound Rules

With End-to-End SSL Encryption enabled from Browser to Web Server, the Web Server Security Group is configured to allow Inbound HTTPS from any Public IPv4 or IPv6 address. As this solution will use an AWS Application Load Balancer (ALB) inbound HTTPS rules must be added. Inbound SSH rules are also added to allow connectivity from the Bastion Host Security Group.

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-A-WS-SG, click the Inbound Tab and click Edit
c. Enter the following Inbound Rules for the Web Server Security Group and click Save

Type	Protocol	Port	Source	Description
SSH	TCP	22	VPC-MZ-CST-EW1-A-BH-SG	Inbound SSH from A Bastion Host SG
SSH	TCP	22	VPC-MZ-CST-EW1-B-BH-SG	Inbound SSH from B Bastion Host SG
SSH	TCP	22	VPC-MZ-CST-EW1-C-BH-SG	Inbound SSH from C Bastion Host SG
HTTPS	TCP	443	VPC-MZ-CST-EW1-ALB-SG	Inbound HTTPS from ALB SG

Table 23. Web Server Inbound Security Group Rules[79]

d. Select Security Group VPC-MZ-CST-EW1-B-WS-SG, click the Inbound Tab and click Edit
e. Enter the Inbound Rules for the Web Server Security Group listed in the table above and click Save

f. Select Security Group VPC-MZ-CST-EW1-C-WS-SG, click the Inbound Tab and click Edit
g. Enter the Inbound Rules for the Web Server Security Group listed in the table above and click Save

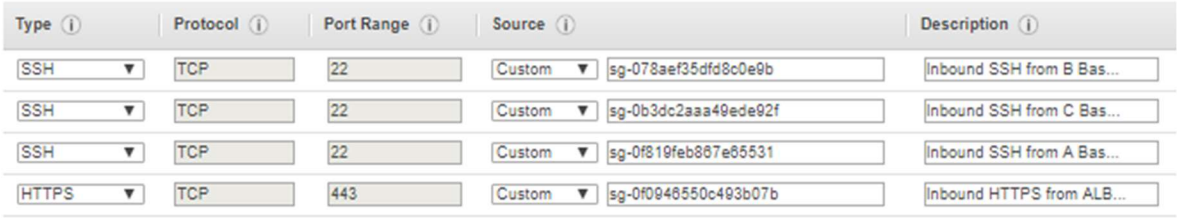


Image 12. Web Server Inbound Rule Configuration[80]

[79] Taaffe, Jonathon [2019] *Table 23. Web Server Inbound Security Group Rules* [Created 5th December 2019]
[80] Taaffe, Jonathon [2019] *Image 12. Web Server Inbound Rule Configuration* [Created 5th December 2019]

Web Server Outbound Rules

Outbound MySQL rules must be configured to allow access to the RDS Database Instances. Outbound HTTPS must also be added to allow HTTPS access to the ALB.

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-A-WS-SG, click the Outbound Tab and click Edit
c. Enter the following Outbound Rules for the Web Server Security Group and click Save

Note1: To add additional Rules click Add Rule
Note2. Outbound HTTP/HTTPS is required for software updates

Type	Protocol	Port	Destination	Description
HTTP	TCP	80	Anywhere	Outbound HTTP to anywhere
HTTPS	TCP	80	Anywhere	Outbound HTTPS to anywhere
MYSQL	TCP	3306	VPC-MZ-CST-EW1-A-RDS-SG	Outbound MySQL to A-RDS-SG
MYSQL	TCP	3306	VPC-MZ-CST-EW1-B-RDS-SG	Outbound MySQL to B-RDS-SG
MYSQL	TCP	3306	VPC-MZ-CST-EW1-C-RDS-SG	Outbound MySQL to C-RDS-SG
HTTPS	TCP	443	VPC-MZ-CST-EW1-ALB-SG	Outbound HTTPS to ALB SG

Table 24. Web Server Outbound Security Group Rules[81]

d. Select Security Group VPC-MZ-CST-EW1-B-WS-SG, click the Outbound Tab and click Edit
e. Enter the Outbound Rules for the Web Server Security Group listed in the table above and click Save

f. Select Security Group VPC-MZ-CST-EW1-B-WS-SG, click the Outbound Tab and click Edit
g. Enter the Outbound Rules for the Web Server Security Group listed in the table above and click Save

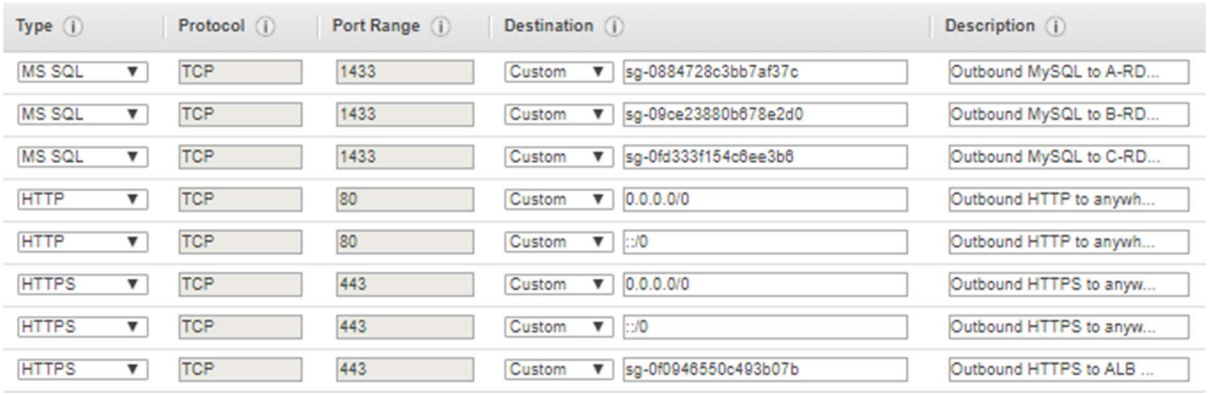


Image 13. Web Server Outbound Rule Configuration[82]

[81] Taaffe, Jonathon [2019] *Table 24. Web Server Outbound Security Group Rules* [Created 5th December 2019]
[82] Taaffe, Jonathon [2019] *Image 13. Web Server Outbound Rule Configuration* [Created 5th December 2019]

RDS Inbound Rules

Inbound MySQL rules must be added to allow DB read/write access from the Web Servers.
Inbound MySQL rules must also be added to allow the RDS DB Instances in eu-west-1b and eu-west-1c access to the RDS DB Instance in eu-west-1a.

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-A-RDS-SG, click the Inbound Tab and click Edit
c. Enter the following Inbound Rules for the RDS Security Group and click Save

Note1: To add additional Rules click Add Rule

Type	Pro	Port	Source	Description
MySQL	TCP	3306	VPC-MZ-CST-EW1-A-RDS-SG	Inbound MySQL from A-RDS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-B-RDS-SG	Inbound MySQL from B-RDS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-C-RDS-SG	Inbound MySQL from C-RDS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-A-WS-SG	Inbound MySQL from A-WS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-B-WS-SG	Inbound MySQL from B-WS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-C-WS-SG	Inbound MySQL from C-WS-SG

Table 25. RDS Inbound Security Group Rules[83]

d. Select Security Group VPC-MZ-CST-EW1-B-RDS-SG, click the Inbound Tab and click Edit
e. Enter the Inbound Rules for the RDS Security Group listed in the table above and click Save

f. Select Security Group VPC-MZ-CST-EW1-C-RDS-SG, click the Inbound Tab and click Edit
g. Enter the Inbound Rules for the RDS Security Group listed in the table above and click Save

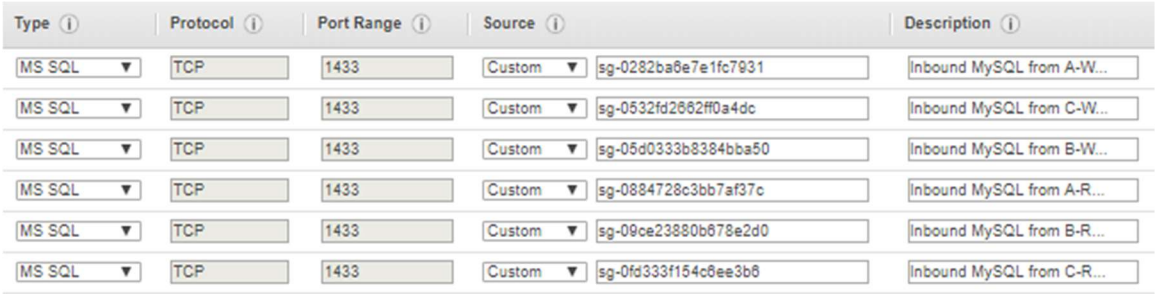


Image 14. RDS Inbound Rules Configuration[84]

[83] Taaffe, Jonathon [2019] *Table 25. RDS Inbound Security Group Rules* [Created 5th December 2019]
[84] Taaffe, Jonathon [2019] *Image 14. RDS Inbound Rules Configuration* [Created 5th December 2019]

RDS Outbound Rules

Outbound MySQL rules must be configured to allow DB post-back to the Web Servers.
Outbound MySQL must also be added to allow the RDS DB instance in eu-west-1a access to eu-west-1b and eu-west-1c

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-ALB-SG, click the Outbound Tab and click Edit
c. Enter the following Outbound Rules for the RDS Security Group and click Save

Note1: To add additional Rules click Add Rule

Type	Pro	Port	Source	Description
MySQL	TCP	3306	VPC-MZ-CST-EW1-A-RDS-SG	Outbound MySQL to A-RDS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-B-RDS-SG	Outbound MySQL to B-RDS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-C-RDS-SG	Outbound MySQL to C-RDS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-A-WS-SG	Outbound MySQL to A-WS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-B-WS-SG	Outbound MySQL to B-WS-SG
MySQL	TCP	3306	VPC-MZ-CST-EW1-C-WS-SG	Outbound MySQL to C-WS-SG

Table 26. RDS Outbound Security Group Rules[85]

d. Select Security Group VPC-MZ-CST-EW1-B-RDS-SG, click the Outbound Tab and click Edit
e. Enter the Outbound Rules for the RDS Security Group listed in the table above and click Save

f. Select Security Group VPC-MZ-CST-EW1-C-RDS-SG, click the Outbound Tab and click Edit
g. Enter the Outbound Rules for the RDS Security Group listed in the table above and click Save

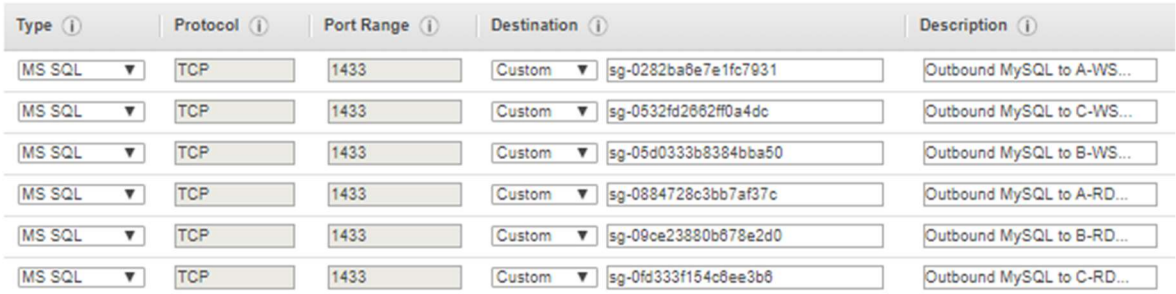


Image 15. RDS Outbound Rules Configuration[86]

[85] Taaffe, Jonathon [2019] *Table 26. RDS Outbound Security Group Rules* [Created 5th December 2019]
[86] Taaffe, Jonathon [2019] *Image 15. RDS Outbound Rules Configuration* [Created 5th December 2019]

ALB Inbound Rules

Inbound HTTPS rules must be added to allow access from the Web Servers in the 3 AZ's
Inbound HTTPS rules must also be added to allow any IPv4 or IPv6 IP access to the Load Balancer.

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-ALB-SG, click the Inbound Tab and click Edit
c. Enter the following Inbound Rules for the ALB Security Group and click Save

Note1: To add additional Rules click Add Rule

Type	Pro	Port	Source	Description
HTTPS	TCP	443	Anywhere	Allow Inbound HTTPS from anywhere
HTTPS	TCP	443	VPC-MZ-CST-EW1-A-WS-SG	Allow Inbound HTTPS from A-WS-SG
HTTPS	TCP	443	VPC-MZ-CST-EW1-B-WS-SG	Allow Inbound HTTPS from B-WS-SG
HTTPS	TCP	443	VPC-MZ-CST-EW1-C-WS-SG	Allow Inbound HTTPS from C-WS-SG

Table 27. ALB Inbound Security Group Rules[87]

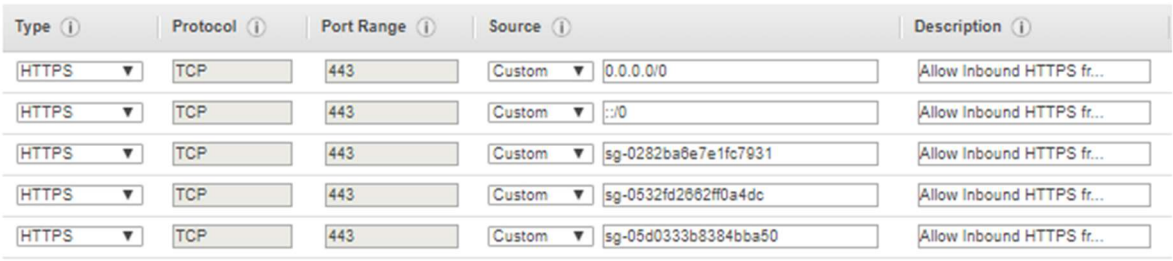


Image 16. ALB Inbound Rules Configuration[88]

[87] Taaffe, Jonathon [2019] *Table 27. ALB Inbound Security Group Rules* [Created 5th December 2019]
[88] Taaffe, Jonathon [2019] *Image 16. ALB Inbound Rules Configuration* [Created 5th December 2019]

ALB Outbound Rules

Outbound HTTPS rules must be configured to allow ALB to communicate with the Web Servers in the 3 AZ's.
Outbound HTTPS rules must be configured to allow ALB to communicate with Browser.

Configuration

a. Navigate to AWS Console > Services > EC2 > Security Groups
b. Select Security Group VPC-MZ-CST-EW1-ALB-SG, click the Outbound Tab and click Edit
c. Enter the following Outbound Rules for the ALB Security Group and click Save

Note1: To add additional Rules click Add Rule

Type	Pro	Port	Destination	Description
HTTPS	TCP	443	Anywhere	Allow Outbound HTTPS to anywhere
HTTPS	TCP	443	VPC-MZ-CST-EW1-A-WS-SG	Allow Outbound HTTPS to A-WS-SG
HTTPS	TCP	443	VPC-MZ-CST-EW1-B-WS-SG	Allow Outbound HTTPS to B-WS-SG
HTTPS	TCP	443	VPC-MZ-CST-EW1-C-WS-SG	Allow Outbound HTTPS to C-WS-SG

Table 28. ALB Outbound Security Group Rules[89]

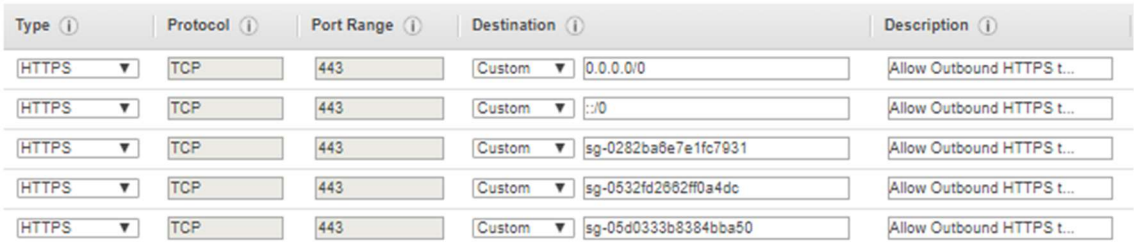


Image 17. ALB Outbound Rules Configuration[90]

[89] Taaffe, Jonathon [2019] *Table 28. ALB Outbound Security Group Rules* [Created 5th December 2019]
[90] Taaffe, Jonathon [2019] *Image 17. ALB Outbound Rules Configuration* [Created 5th December 2019]

Elastic Cloud Compute (EC2) Instances

AWS Elastic Cloud Compute (EC2) is…

> *"a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment."*[91]

Linux Ubuntu EC2 Virtual Machines will be configured to provide compute resources for this deployment.

One Bastion Host instance and one Web Server instance will be deployed in each AZ totalling 6 instances. This configuration will provide capacity and redundancy to this deployment.

Bastion Host

Bastion Hosts will be the primary entry connection point into the VPC from the internet. The Security Group associated with these instances will only permit SSH port 22 access from the public IPV4 address of the Administrators local host.

To access the Web Server Instances within the VPC, first connect to the Bastion Host and then connect over SSH to the Web Server instances.

Bastion Host is the first Instance to be deployed in the VPC and one Bastion Host will be deployed for each Availability Zone (AZ).

Configuration

a. Navigate to AWS Console > Services > EC2 > Instances > Instance > Launch Instance

b. Step 1: Choose an Amazon Machine Image (AMI)

Select the Ubuntu Server 18.04 LTS (HVM), SSD Volume Type AMI, then click Next

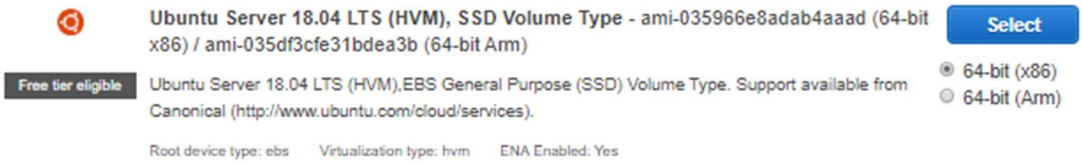


Image 18. Step 1: Choose Amazon Machine Image Choice[92]

c. Step 2: Choose an Instance Type

Select t2.micro Instance Type (General Purpose, EBS Only), then click Next

Image 19. Step 2: Choose Instance Type[93]

[91] AWS.Amazon.com [2019] *Amazon EC2* https://aws.amazon.com/ec2/ [Accessed 5th December 2019]
[92] Taaffe, Jonathon [2019] *Image 18. Step 1: Choose Amazon Machine Image* [Created 5th December 2019]
[93] Taaffe, Jonathon [2019] *Image 19. Step 2: Choose Instance Type* [Created 5th December 2019]

d. Step 3: Configure Instance Details

Configure the instance with the following settings, then click Next
All other settings can be left at default

# of Instances: 1
Network (VPC): VPC-MZ-CST-EW1
Subnet: VPC-MZ-CST-EW1-A-PU
Auto-assign Public IP: Enabled
Shutdown behaviour: Stop
Monitoring: Enabled

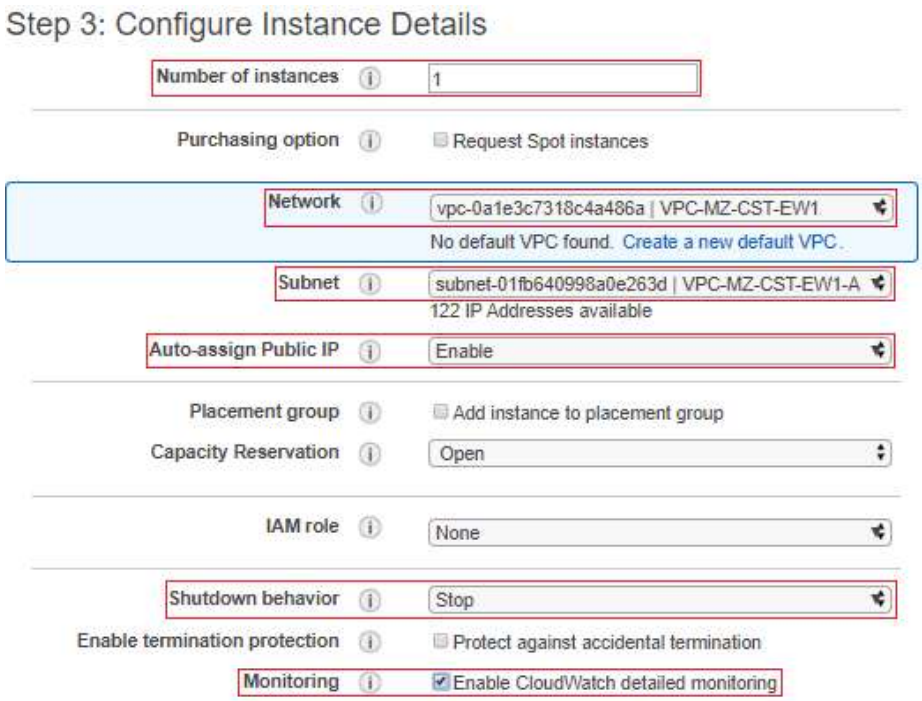


Image 20. Step 3: Configure Instance Details[94]

e. Step 4: Add Storage

Configure the instance with the following settings, then click Next
All other setting can be left at default

Delete on Termination: Deselect
Encryption: (default) aws/ebs

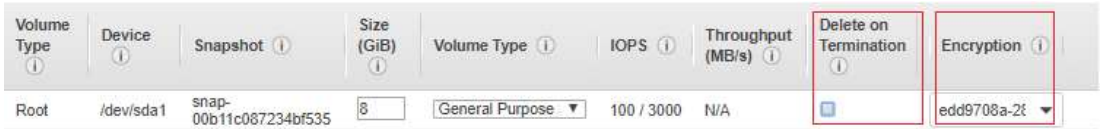


Image 21. Step 4: Add Storage[95]

[94] Taaffe, Jonathon [2019] *Image 20. Step 3: Configure Instance Details* [Created 5th December 2019]
[95] Taaffe, Jonathon [2019] *Image 21. Step 4: Add Storage* [Created 5th December 2019]

f. Step 5: Add Tags

Click Add Tag and add the following details, then click Next

Key: Name

Value: VPC-MZ-CST-EW1-A-BH-01

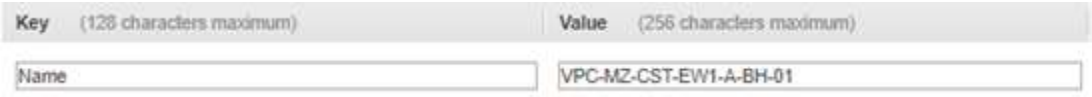


Image 22. Step 5: Add Tags[96]

g. Step 6: Configure Security Group:

Select Assign a security group, select the following existing security groups, then click Review and Launch

Security Group: VPC-MZ-CST-EW1-A-BH-SG

VPC-MZ-CST-EW1-B-BH-SG

VPC-MZ-CST-EW1-C-BH-SG

Image 23. Step 6: Configure Security Group[97]

h. Step 7: Review Instance Launch

Review Instance configuration, confirm configuration, then click Launch

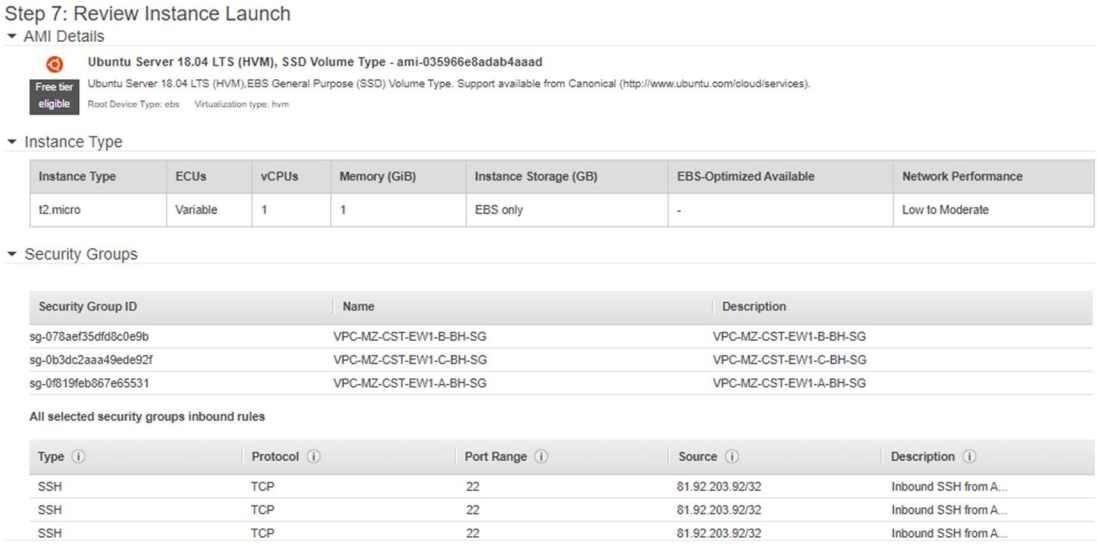


Image 24. Step 7: Review Instance Launch[98]

[96] Taaffe, Jonathon [2019] *Image 22. Step 5: Add Tags* [Created 5th December 2019]

[97] Taaffe, Jonathon [2019] *Image 23. Step 6: Configure Security Group* [Created 5th December 2019]

[98] Taaffe, Jonathon [2019] *Image 24. Step 7: Review Instance Launch* [Created 5th December 2019]

i. **Step 8: Select existing key pair or create new key pair**
    i. From the drop-down menu choose Create a new key pair
    ii. For Key Pair Name enter VPC-MZ-CST-EW1-A-BH-01
    iii. Click Download Key Pair

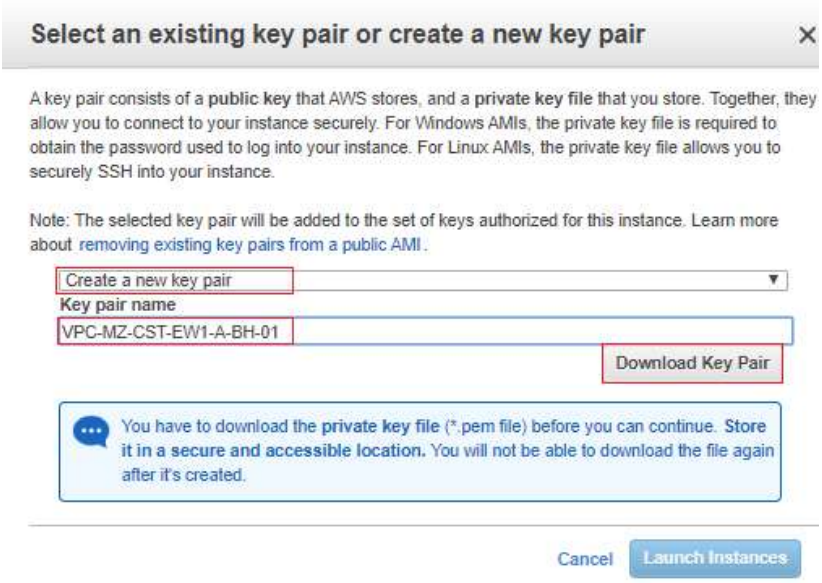


Image 35. Select Existing Key Pair or Created new Key Pair[99]

    iv. Once the Key Pair has been downloaded, click Launch Instance
    v. The Bastion Host instance will now launch

Connection

With both the Bastion Host and Web Server instances running in the eu-west-1a AZ, connect via SSH to the Bastion Host to confirm connectivity

Confirm Security Group Configuration

a. Navigate to AWS Console > Services > VPC > Security Groups
b. Select VPC-MZ-CST-EW1-A-BH-SG > click Inbound Rules tab > click Edit Rules
c. From the drop-down menu under Source select My IP and click Save Rules

Connect with PuTTY

a. Download and Install PuTTY [100]
b. Convert downloaded AWS Private Key using PuTTYgen [101]

> **Important:** Prior to saving the .PPK file, in Key passphrase enter a passphrase and re-enter the same passphrase in Confirm passphrase. This passphrase will be required to open/access the .PPK Private Key for SSH connectivity. Including a Key Passphrase will ensure if the private key is intercepted, it is passphrase protected.

c. Navigate to AWS Console > Services > EC2 > Instances

---

[99] Taaffe, Jonathon [2019] *Image 35. Select Existing Key Pair or Created new Key Pair* {Created 5th December 2019]
[100] PuTTY [2019] *PuTTY: a free SSH and Telnet client* http://www.chiark.greenend.org.uk/~sgtatham/putty/ [Accessed 5th December 2019]
[101] PuTTY [2019] *8.2 Using PuTTYgen, the PuTTY key generator* https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter8.html#pubkey-puttygen [Accessed 5th December 2019]

d. Select VPC-MZ-CST-EW1-A-BH-SG > from the Description tab copy the Public DNS (IPv4) value
e. Open PuTTY and connect to Bastion Host EC2 Instance over SSH [102]

Note: The PuTTY Host Name syntax required to connect to AWS EC2 Ubuntu instances is

ubuntu@*PublicDNS(IPv4)*

Instance Updates
Once successfully connected to the Bastion Host Instance, run the following command to update the instance

```
sudo apt-get update && sudo apt-get upgrade -y
```

Hostname Change
Change the hostname of the Bastion Host instance to the instance name in the AWS console and as per the PuTTY *.pem/*.ppk file, replacing *newhostname* with the required hostname as follows

```
sudo hostnamectl set-hostname newhostname
sudo nano /etc/hosts
    127.0.0.1   newhostname

sudo nano /etc/cloud/cloud.cfg
preserve_hostname: true
```

[102] Amazon Web Services [2019] *AWS Connect to Your Linux Instance* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html [Accessed 5th December 2019]

Web Server

Web Server instances will serve up the web content for the Secure Cloud Application. They will be configured with Apache2 web services, PHP scripting language and WordPress blog application. Security Groups associated with these instances will only permit HTTPS port 443 traffic from the Application Load Balancer. These instances will not have any direct communication from the internet.

To access the Web Server Instances within the VPC, first connect to the Bastion Host and then connect over SSH to the Web Server instances. One Web Server will be deployed into each Availability Zone (AZ).

Configuration

a. Navigate to AWS Console > Services > EC2 > Instances > Instance > Launch Instance

b. Step 1: Choose an Amazon Machine Image (AMI)

Select the Ubuntu Server 18.04 LTS (HVM), SSD Volume Type AMI, then click Next

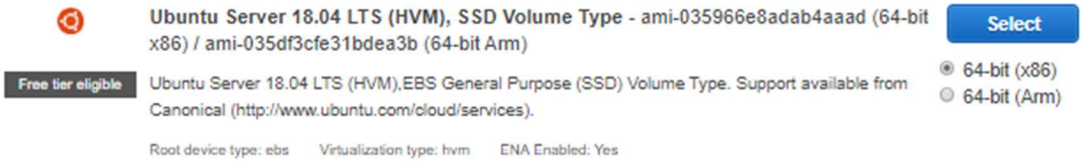


Image 36. Step 1: Choose Amazon Machine Image Choice[103]

c. Step 2: Choose an Instance Type

Select t2.micro Instance Type (General Purpose, EBS Only), then click Next

Image 37. Step 2: Choose Instance Type[104]

d. Step 3: Configure Instance Details

Configure the instance with the following settings, then click Next
All other settings can be left at default

Note: No public IP is required as the ALB will route all traffic to the Web Server instance

# of Instances: 1
Network (VPC): VPC-MZ-CST-EW1
Subnet: VPC-MZ-CST-EW1-A-PR
Auto-assign Public IP: Disable
Shutdown behaviour: Stop
Monitoring: Enabled

[103] Taaffe, Jonathon [2019] *Image 36. Step 1: Choose Amazon Machine Image* [Created 5th December 2019]
[104] Taaffe, Jonathon [2019] *Image 37. Step 2: Choose Instance Type* [Created 5th December 2019]

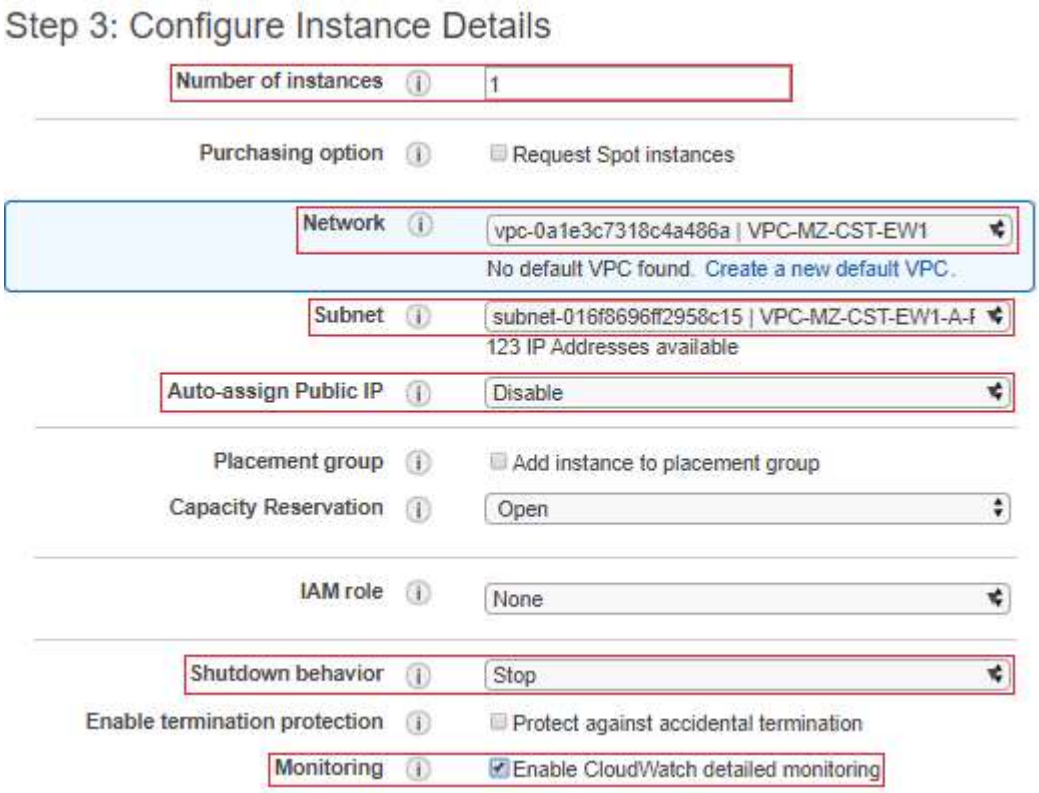


Image 38. Step 3: Configure Instance Details[105]

e. Step 4: Add Storage

Configure the instance with the following settings, then click Next
All other setting can be left at default

Delete on Termination: Deselect
Encryption: (default) aws/ebs

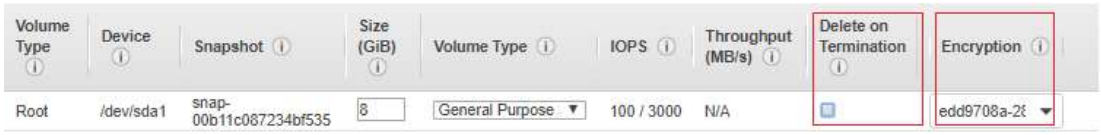


Image 39. Step 4: Add Storage[106]

f. Step 5: Add Tags

Click Add Tag and add the following details, then click Next

Key: Name
Value: VPC-MZ-CST-EW1-A-WS-01

Image 40. Step 5: Add Tags[107]

[105] Taaffe, Jonathon [2019] *Image 38. Step 3: Configure Instance Details* [Created 5th December 2019]
[106] Taaffe, Jonathon [2019] *Image 39. Step 4: Add Storage* [Created 5th December 2019]
[107] Taaffe, Jonathon [2019] *Image 40. Step 5: Add Tags* [Created 5th December 2019]

g. Step 6: Configure Security Group:

Select Assign a security group, select the following existing security groups, then click Review and Launch

Security Group: VPC-MZ-CST-EW1-A-WS-SG
VPC-MZ-CST-EW1-B-WS-SG
VPC-MZ-CST-EW1-C-WS-SG

Image 41. Step 6: Configure Security Group[108]

h. Step 7: Review Instance Launch

Review Instance configuration, confirm configuration, then click Launch

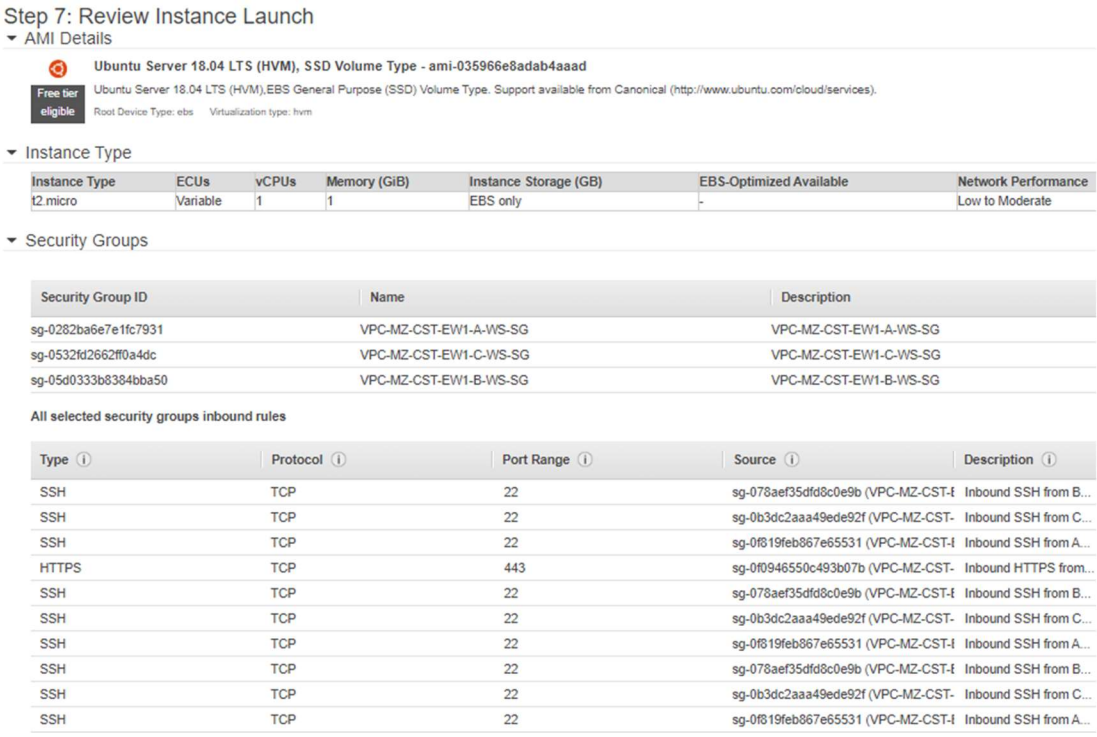


Image 42. Step 7: Review Instance Launch[109]

[108] Taaffe, Jonathon [2019] *Image 41. Step 6: Configure Security Group* [Created 5th December 2019]
[109] Taaffe, Jonathon [2019] *Image 42. Step 7: Review Instance Launch* [Created 5th December 2019]

i. **Step 8: Select existing key pair or create new key pair**

vi. From the drop-down menu choose Create a new key pair

vii. For Key Pair Name enter VPC-MZ-CST-EW1-A-WS-01

viii. Click Download Key Pair

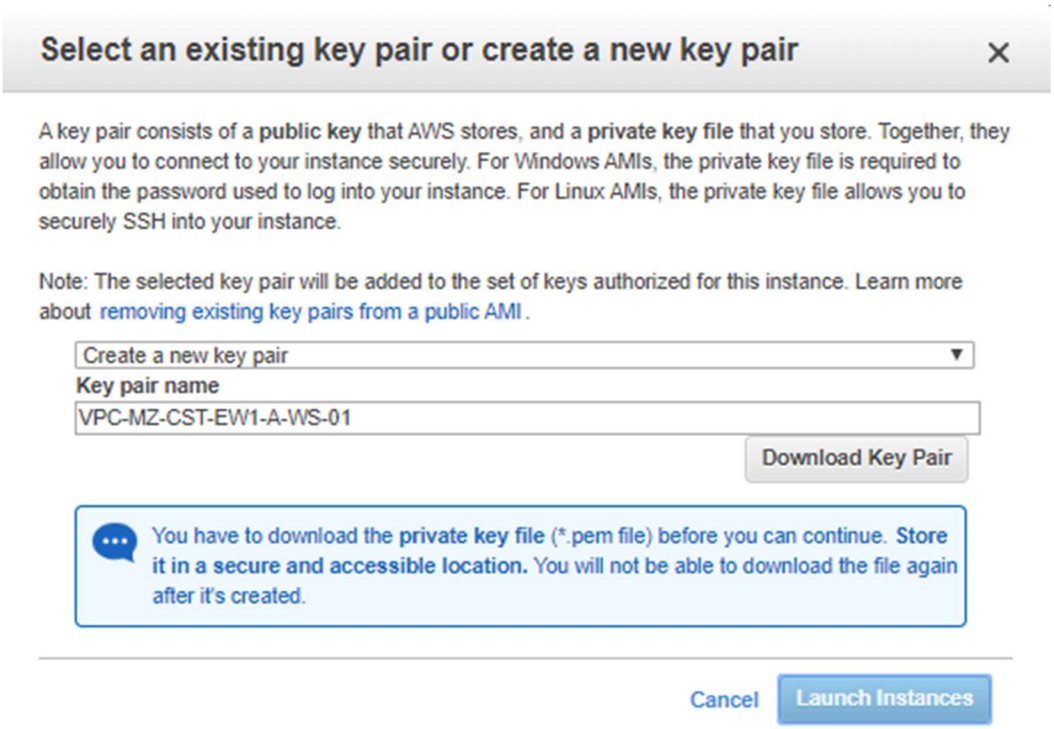


Image 43. Select Existing Key Pair or Created new Key Pair[110]

ix. Once the Key Pair has been downloaded, click Launch Instance

x. The Web Server instance will now launch

Connection

No public IPv4 IP has been assigned to the Web Instance. All Inbound/Outbound traffic will be routed through the Application Load Balancer. To connect over SSH to the Web Instance, first connect to the Bastion Host and then connect to the Web instance.

Connect with PuTTY

Important: PuTTY must be configured for Agent Forwarding to allows Passthrough Key Authentication[111]

a. Download and Install PuTTY [112]

b. Convert downloaded AWS Private Key using PuTTYgen [113]

[110] Taaffe, Jonathon [2019] *Image 43. Select Existing Key Pair or Created new Key Pair* {Created 5th December 2019]

[111] PuTTY [2019] *9.4 Using agent forwarding* https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter9.html#pageant-forward [Accessed 5th December 2019]

[112] PuTTY [2019] *PuTTY: a free SSH and Telnet client* http://www.chiark.greenend.org.uk/~sgtatham/putty/ [Accessed 5th December 2019]

[113] PuTTY [2019] *8.2 Using PuTTYgen, the PuTTY key generator* https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter8.html#pubkey-puttygen [Accessed 5th December 2019]

Important: Prior to saving the .PPK file, in Key passphrase enter a passphrase and re-enter the same passphrase in Confirm passphrase. This passphrase will be required to open/access the .PPK Private Key for SSH connectivity. Including a Key Passphrase will ensure if the private key is intercepted, it is passphrase protected.

c. Configure PuTTY for Agent Forwarding [114]
d. Through PuTTY connect to the Bastion Host Instance over SSH
e. Navigate to AWS Console > Services > EC2 > Instances
f. Select VPC-MZ-CST-EW1-A-WS-SG > from the Description tab copy the Private DNS value
g. From the Bastion Host SSH connection, connect to Web Server EC2 Instance over SSH as follows

```
ssh WebServerPrivateDNS
```

Instance Updates
Once successfully connected to the Web Server Instance, run the following command to update the instance

```
sudo apt-get update && sudo apt-get upgrade -y
```

Hostname Change
Change the hostname of the Web Server instance to the instance name in the AWS console and as per the PuTTY *.pem/*.ppk file, replacing *newhostname* with the required hostname as follows

```
sudo hostnamectl set-hostname newhostname
sudo nano /etc/hosts
    127.0.0.1   newhostname

sudo nano /etc/cloud/cloud.cfg
preserve_hostname: true
```

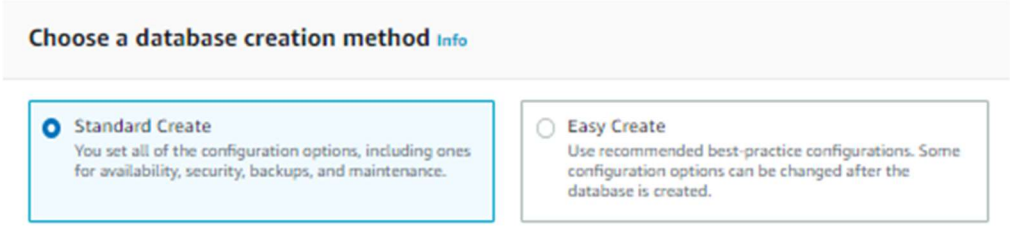
[114] PuTTY [2019] *9.4 Using agent forwarding*
https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter9.html#pageant-forward [Accessed 5th December 2019]

Relational Database Service (RDS)

AWS Relational Database Service (RDS)[115] is a distributed database service that can be configured for Multi Availability Zone access. There is a single Master of the database with Read Replicas available in AZ's of your choice. This configuration ensures Databases services are always available even in the event of 2 of 3 AZ's going offline. This is a Database-as-a-Service (DBaaS) service where AWS manages all layers up to the Database layer. CyberSecure.Team is responsible for securing the RDS configuration and maintaining the data in the database.

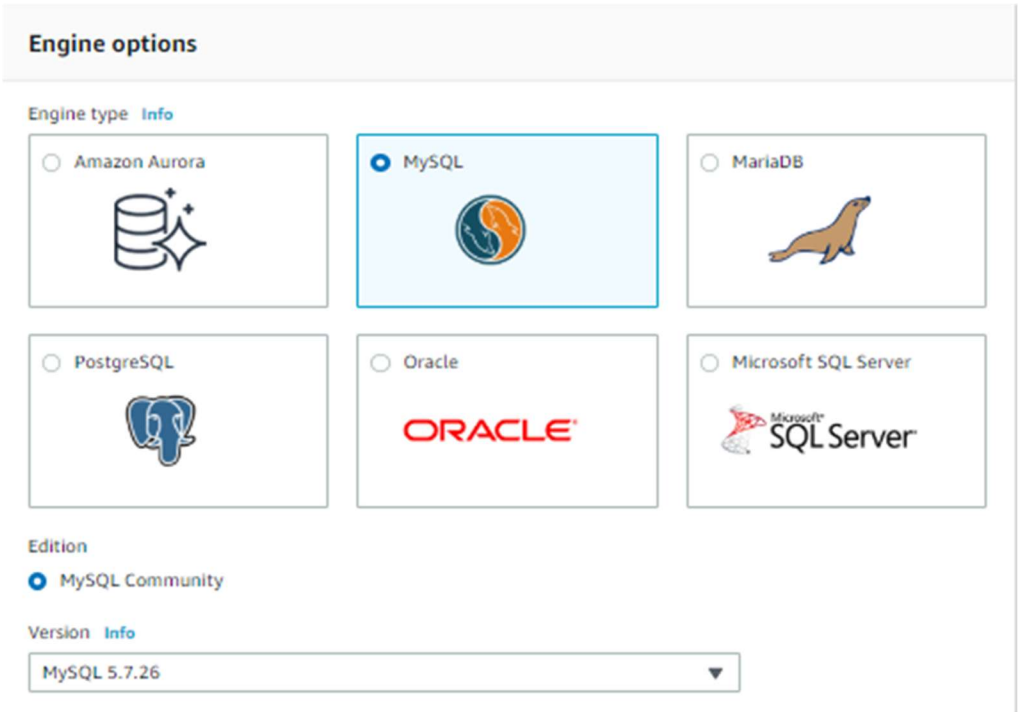
Create

1. Navigate to AWS Console > Services > RDS > Dashboard > Create Database
2. Choose a database creation method: Standard Create



3. Engine Options: Apply settings as follows

Option	Setting	Value
Engine options	Engine Type	MySQL
Engine options	Edition	MySQL Community
Engine options	Version	MySQL 5.7.26



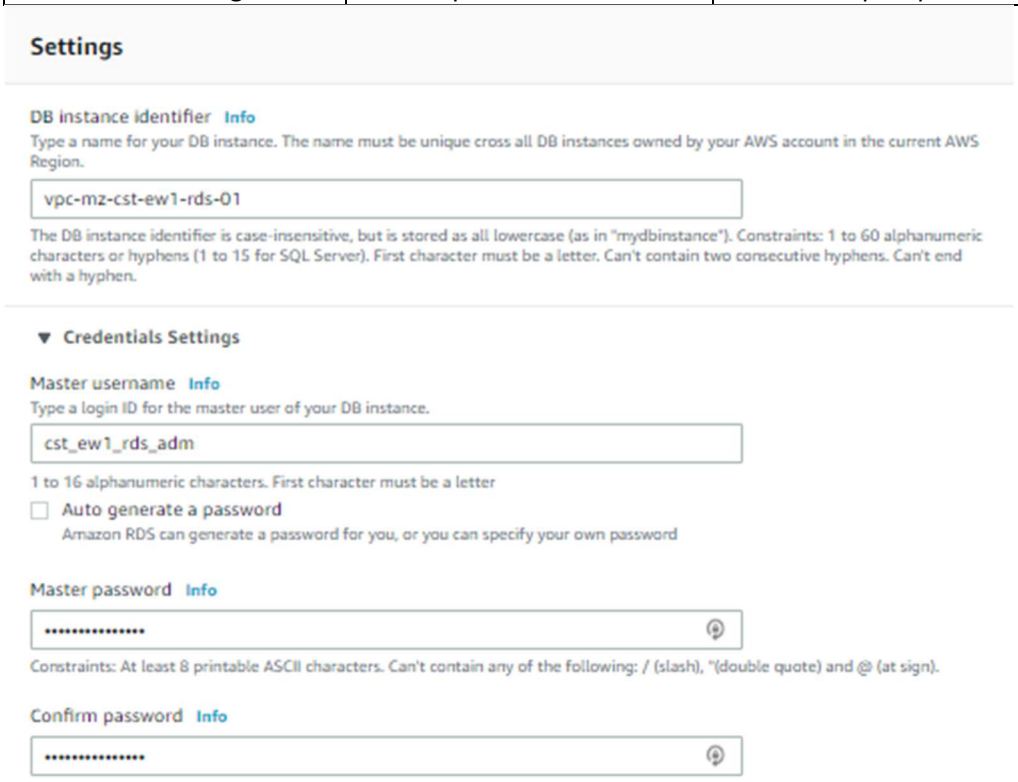
[115] Amazon Web Services [2019] *AWS Relational Database Service* https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html [Accessed 5th December 2019]

4. Templates: Apply settings as follows

Option	Setting	Value
Engine options	Templates	Production

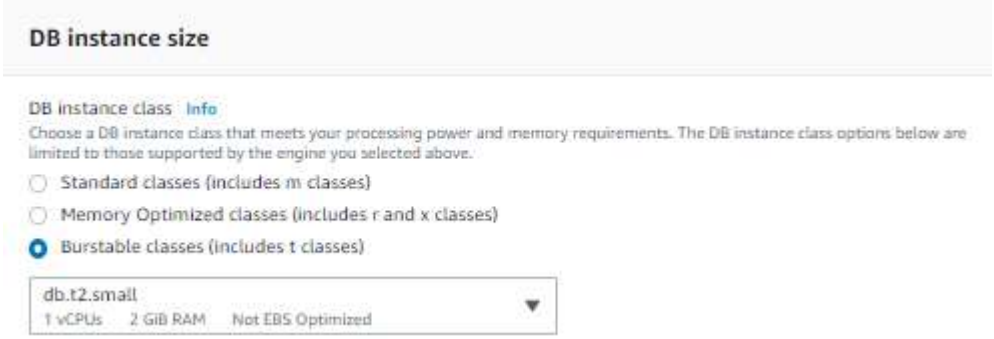
5. Settings: Apply settings as follows
mypasswordrocks

Option	Setting	Value
Settings	DB instance identifier	vpc-mz-cst-ew1-rds-01
Credentials Settings	Master username	cst_ew1_rds_adm
Credentials Settings	Master password	*Ensure complex password configured* [1]



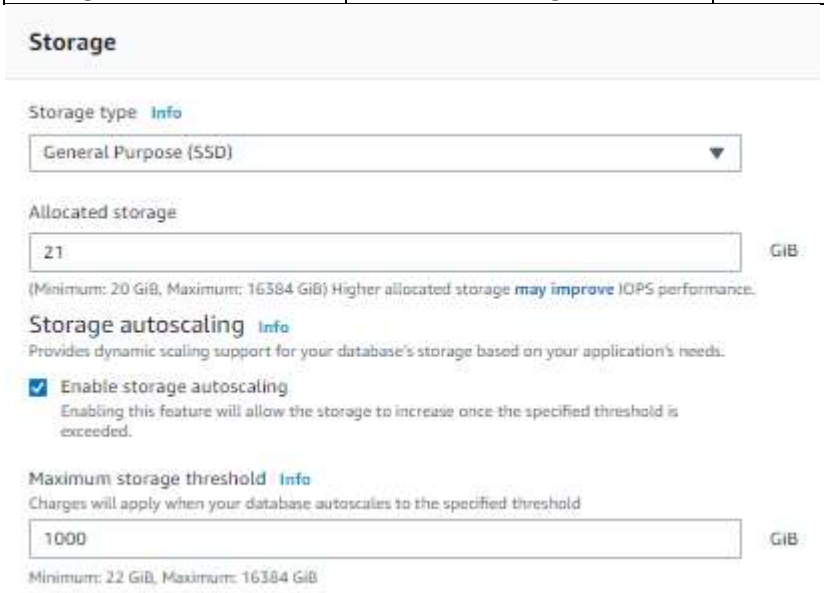
6. DB instance size: Apply settings as follows

Option	Setting	Value
DB instance size	DB instance class: Burstable	db.t2.small [2]



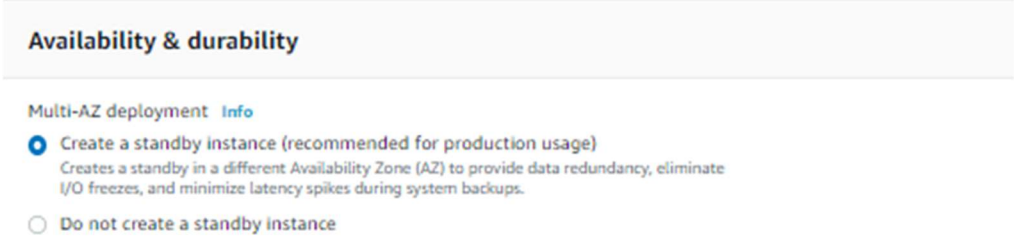
7. Storage: Apply settings as follows

Option	Setting	Value
Storage	Storage type	General Purpose (SSD)
Storage	Allocated storage	21 GiB
Storage	Storage autoscaling	Enable storage autoscaling: Enabled [3]
Storage	Maximum storage threshold	1000 GiB



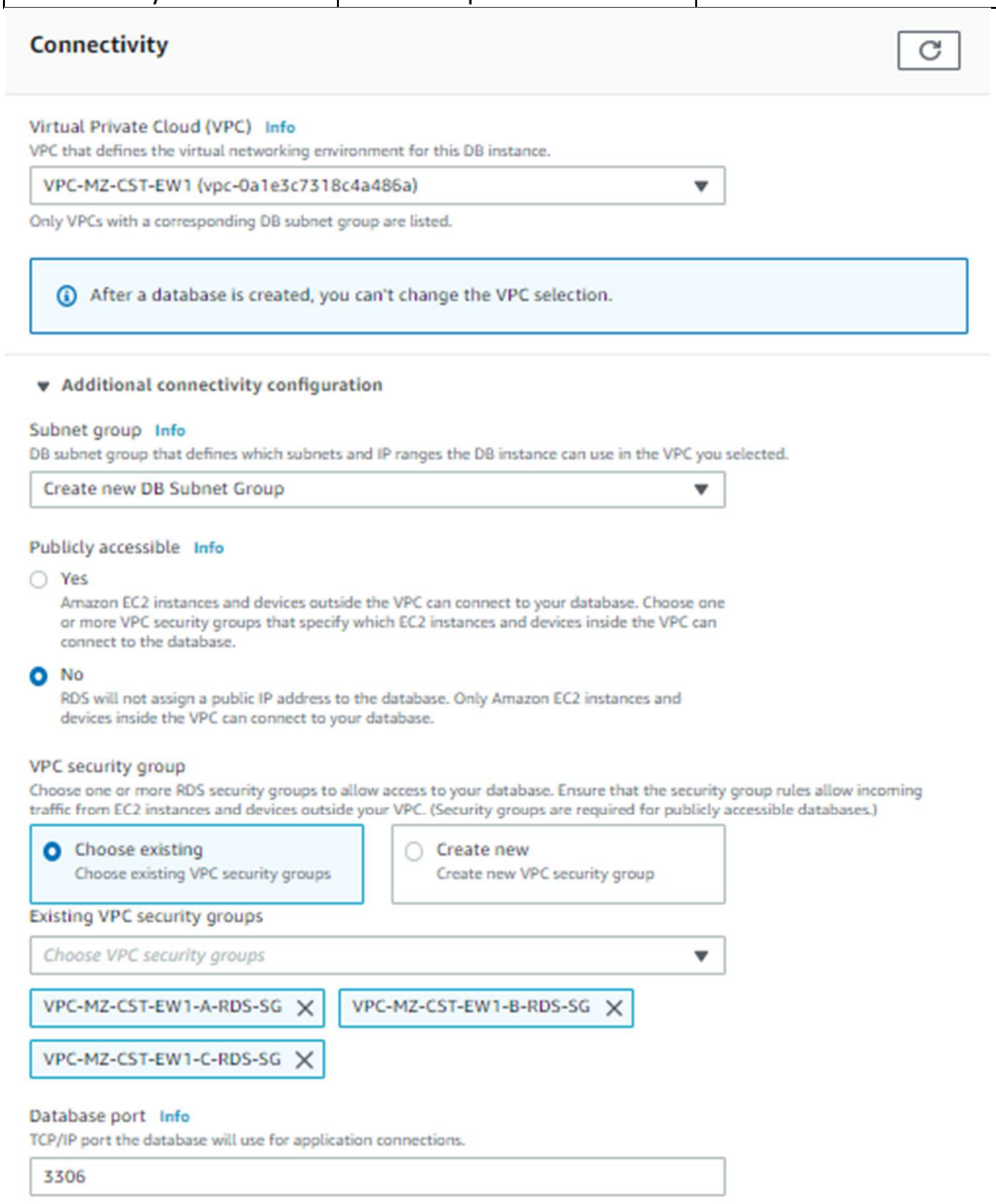
8. Availability & durability: Apply settings as follows

Option	Setting	Value
Availability & durability	Multi-AZ deployment	Create a standby instance [4]



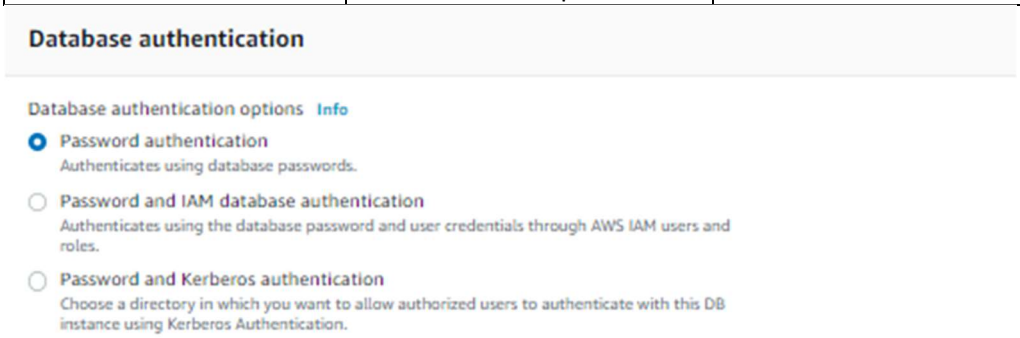
9. Connectivity: Apply settings as follows

Option	Setting	Value
Connectivity	Virtual Private Cloud (VPC)	VPC-MZ-CST-EW1
Connectivity	Connectivity configuration	Subnet group: Create new Subnet Group
Connectivity	Publicly accessible	No [5]
Connectivity	VPC security group	Choose existing
Connectivity	Existing VPC security groups	VPC-MZ-CST-EW1-A-RDS-SG [6]
Connectivity	Existing VPC security groups	VPC-MZ-CST-EW1-B-RDS-SG [6]
Connectivity	Existing VPC security groups	VPC-MZ-CST-EW1-C-RDS-SG [6]
Connectivity	Database port	3306



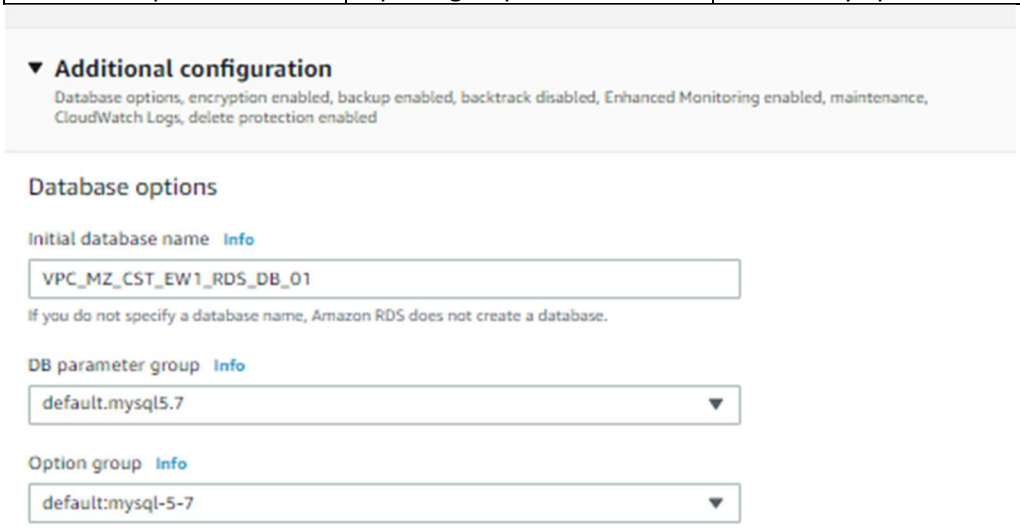
10. Database authentication: Apply settings as follows

Option	Setting	Value
Database authentication	Authentication options	Password authentication [7]



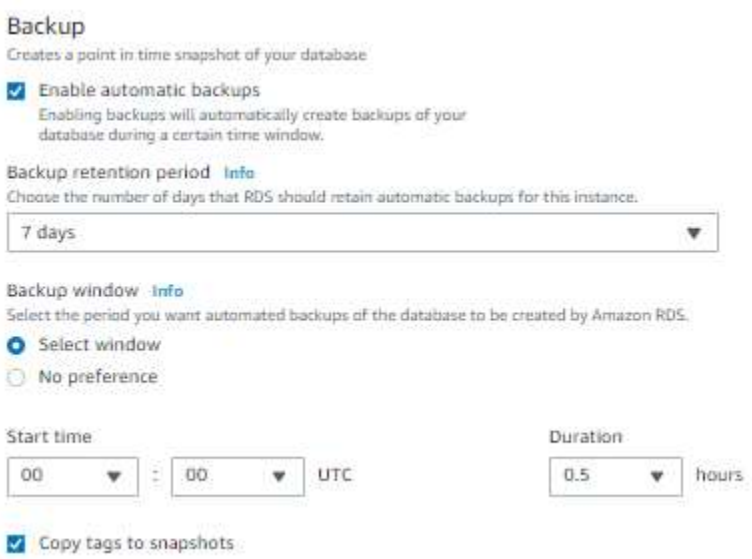
11. Additional Options > Database options: Apply settings as follows

Option	Setting	Value
Database options	Initial database name	VPC_MZ_CST_EW1_RDS_DB_01 [8]
Database options	DB parameter group	default.mysql5.7
Database options	Option group	default:mysql5-7



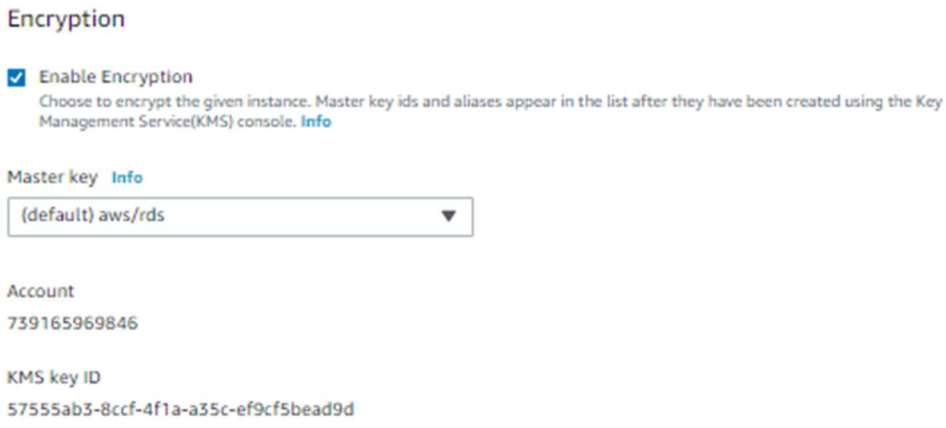
12. Additional Options > Backup: Apply settings as follows

Option	Setting	Value
Backup	Enable automatic backups	Enabled [9]
Backup	Backup retention period	7 days [9]
Backup	Select Window	Start Time: 00:00, Duration: 0.5 Hours [9]
Backup	Copy tags to snapshots	Enabled



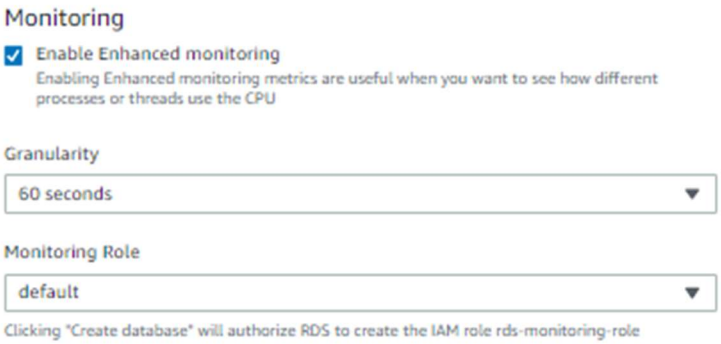
13. Additional Options > Encryption: Apply settings as follows

Option	Setting	Value
Encryption	Enable Encryption	Enabled [10]
Encryption	Master key	(default)aws/rds [10]
Encryption	Account	*AWS Assigned Account Number*
Encryption	KMS key ID	*AWS Assigned KMS Key ID* [10]



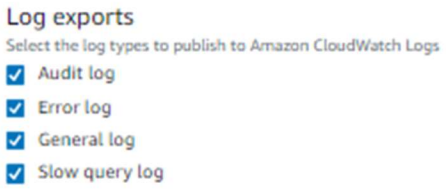
14. Additional Options > Monitoring: Apply settings as follows

Option	Setting	Value
Monitoring	Enhanced monitoring	Enabled [11]
Monitoring	Granularity	60 seconds [11]
Monitoring	Monitoring Role	Default [11]



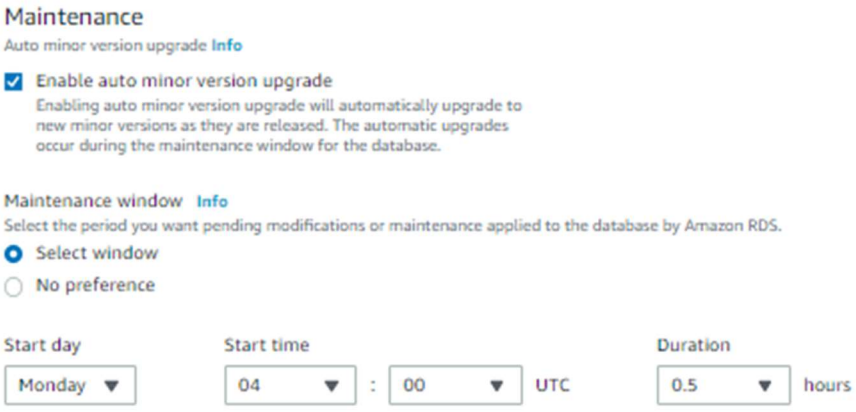
15. Additional Options > Log Exports: Apply settings as follows

Option	Setting	Value
Log Exports	CloudWatch Log Types	Audit log [12]
Log Exports	CloudWatch Log Types	Error log [12]
Log Exports	CloudWatch Log Types	General log [12]
Log Exports	CloudWatch Log Types	Slow query log [12]
Log exports	IAM role	RDS Service Linked Role [12]



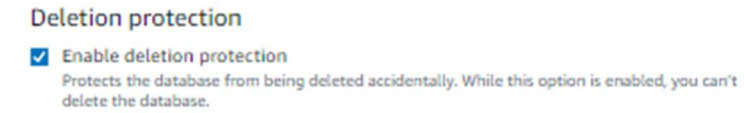
16. Additional Options > Maintenance: Apply settings as follows

Option	Setting	Value
Maintenance	Version upgrade	Auto Minor Enabled [13]
Maintenance	Select Window	Monday: 04:00, Duration: 0.5 Hours [13]



17. Additional Options > Deletion protection: Apply settings as follows

Option	Setting	Value
Deletion protection	Deletion Protection	Enabled [14]



Important Notes regarding RDS Database Configuration

[1]	Master password	Ensure complex password as per company policy
[2]	DB instance class	db.t2.small allows for encryption and burst capacity
[3]	Storage autoscaling: Enabled	Required for burst capacity
[4]	Create a standby instance	1 x Primary read/write master RDS database 2 x Read Replicas in 2 other Availability Zones
[5]	Publicly Accessible: No	RDS Instance will not be publicly available
[6]	VPC-MZ-CST-EW1-A-RDS-SG	RDS Private Security Group only allows MySQL:3306
[6]	VPC-MZ-CST-EW1-B-RDS-SG	RDS Private Security Group only allows MySQL:3306
[6]	VPC-MZ-CST-EW1-C-RDS-SG	RDS Private Security Group only allows MySQL:3306
[7]	Password Authentication	Password authentication for Wordpress connection
[8]	VPC_MZ_CST_EW1_RDS_DB_01	Non-standard Wordpress database name
[9]	Enable automatic backups: Enabled	Automatic backups run daily at 00:00
[10]	Enable Encryption: Enabled	RDS DB encrypted using AWS RDS Private Key
[11]	Enhanced monitoring: Enabled	Enhanced RDS DB monitoring enabled
[12]	CloudWatch Log Types	Logs generated: Audit, Error, General, Slow query
[13]	Version upgrade: Auto Minor	RDS Minor version upgrades automatically applied
[14]	Deletion Protection: Enabled	Prevent RDS DB from being deleted

Note: It will take approximately 15 minutes for the Database to initialise

Validate

As the RDS Database is initialising review the configuration of the RDS database to ensure it is optimally configured as per Solution Requirements.

Quick

a. Navigate to AWS Console > Services > RDS > Databases > select RDS DB > Configuration
b. Confirm the following settings:

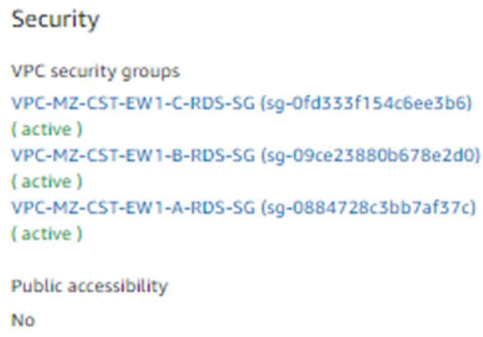
Engine: MySQL Community
Region & AZ: eu-west-1a
Size: db.t2.small

Detailed

Proceed with a detailed verification of the RDS DB once the RDS DB has been successfully created and its status is Available.

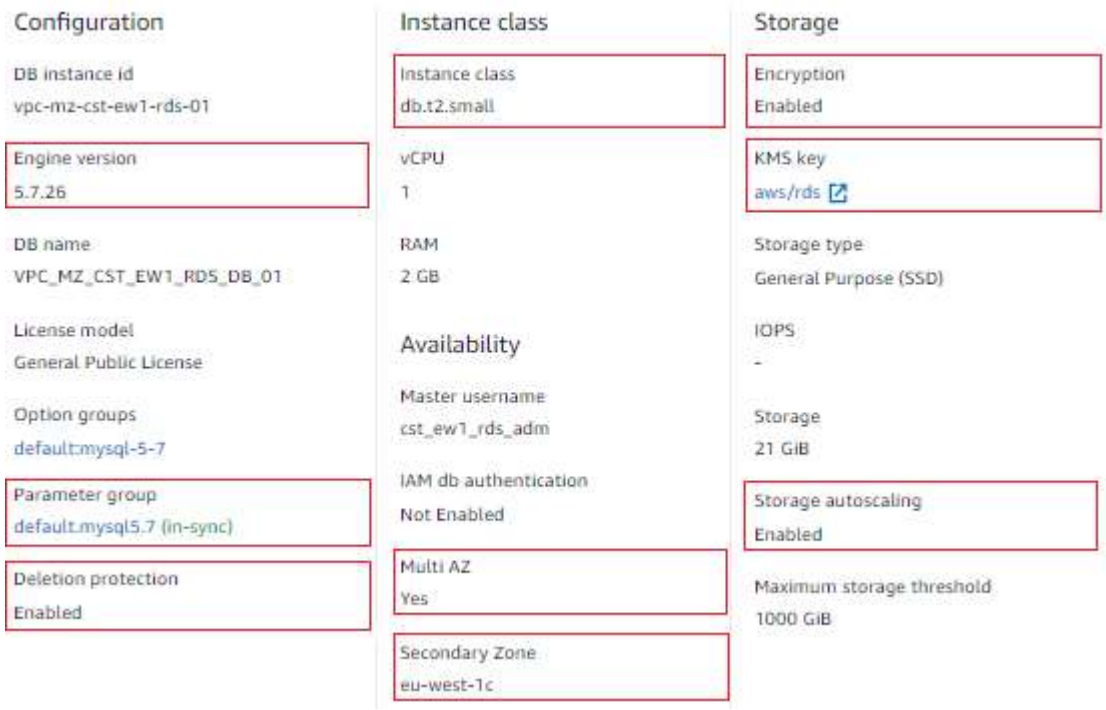
a. Navigate to AWS Console > Services > RDS > Databases > DB Instances > select Database
b. From the details presented, confirm the following
c. Connectivity & security: Confirm the following settings

Tab	Label	Setting	Comment
Connectivity & security	Security	VPC SG's	Ensure 3 Private SG's are listed
Connectivity & security	Security	Public accessibility	No



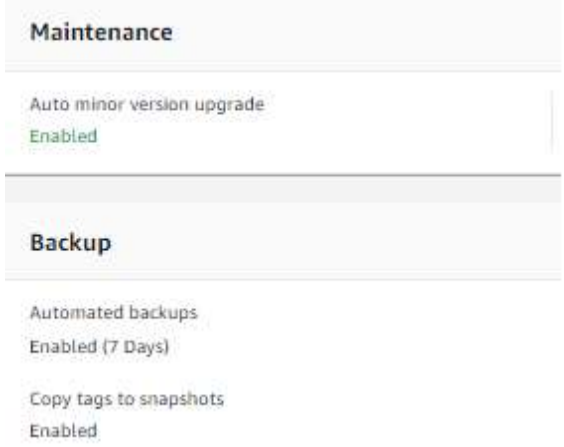
d. Configuration: Confirm the following settings

Tab	Label	Setting	Comment
Configuration	Instance	Engine version	5.7.26
Configuration	Instance	Parameter group	default.mysql5.7
Configuration	Instance	Deletion protection	Enabled
Configuration	Instance	Instance class	db.t2.small
Configuration	Instance	Multi AZ	Yes
Configuration	Instance	Secondary Zone	Confirm different zone than Region & AZ in summary info above
Configuration	Instance	Encryption	Enabled
Configuration	Instance	KMS key	aws/rds
Configuration	Instance	Storage autoscaling	Enabled



e. Maintenance & Backups: Confirm the following settings

Tab	Label	Setting	Comment
Maintenance & Backups	Maintenance	Auto minor version upgrade	Enabled
Maintenance & Backups	Backup	Automated backups	Enabled (7 Days)



Connect

Only the Web Servers are configured to connect to the RDS Database over MySQL:3306. Connect first to the Bastion Host using PuTTY with Key Forwarding, then connect to the Web Server Instance. From the Web Server Instance, connect to the RDS DB using MySQL-Client.

Connect

1. Navigate to AWS Console > Services > RDS > Databases > select RDS Database
2. Under Connectivity & security > Endpoint & port, copy the RDS Endpoint name displayed
3. Navigate to AWS Console > Services > RDS > Databases > select RDS Database
4. Click the Configuration tab and under Availability cop the Master username displayed
5. Connect via PuTTY to the Bastion Host, then SSH to the Web Server Instance
6. Install MySQL-Client on Web Server Instance [116]

   sudo apt install mysql-client -y

7. Connect to RDS Database Instance using mysql-client with following syntax

   mysql -h *RDSDatabaseEndpoint* -u *RDSAdminAccount* -p

   Once you have successfully connected to the RDS database proceed to Configure RDS Database

Configure

1. On the Web Server Instance, at the mysql> prompt, enter the following commands

`SHOW DATABASES;`	*Confirm RDS DB is VPC_MZ_CST_EW1_RDS_DB_01*
`USE VPC_MZ_CST_EW1_RDS_DB_01;`	*Select RDS database*
`SELECT User, Host FROM mysql.user;`	*Confirm DB account cst_ew1_rds_adm*
`GRANT ALL PRIVILEGES ON VPC_MZ_CST_EW1_RDS_DB_01.* TO 'cst_ew1_rds_adm'@'%';`	Grant privileges to the cst_ew1_rds_adm account [1]
`FLUSH PRIVILEGES`	*Apply privileges*

   [1] Wordpress.org recommends granting the wordpress database connection account all privileges to the Wordpress database. In the proceeding steps read/write access to wordpress.conf will be configured only for the www-data group.[117]

2. Once the above commands complete successfully, type Exit.
3. Uninstall MySQL-Client from Web Server
   sudo apt remove mysql-client -y

[116] LinuxConfig.org [2019] *Install MySQL client on Ubuntu* https://linuxconfig.org/install-mysql-on-ubuntu-18-04-bionic-beaver-linux#h6-1-install-mysql-client-on-ubuntu [Accessed 5th December 2019]
[117] Wordpress.org [2019] *Creating Database for WordPress - Using the MySQL Client* https://wordpress.org/support/article/creating-database-for-wordpress/#using-the-mysql-client [Accessed 5th December 2019]

Apache2

Apache2 is an Open Source Web Service which has been available for over 20 years. It's code and configuration is publicly available, easily installed and easily configured on Ubuntu Linux. Due to its longevity and open source code, the current Apache2 release is stable, dependable and highly secure.

Install [118]

On the Web Server Instance, at the :/$ bash prompt, enter the following commands

```
sudo apt update
sudo apt install apache2
sudo systemctl status apache2
sudo systemctl enable apache2
sudo systemctl start apache2
```

Configuration

To configure the Apache2 service to auto-start on Instance reboot, at the :/$ bash prompt, enter the following commands

Command	Details
sudo systemctl status apache2	Confirm Apache2 service status is active
sudo systemctl restart apache2	Restart Apache2 service
sudo systemctl status apache2	Reconfirm Apache2 service status
sudo systemctl enable apache2	Set Apache2 service to auto-start on Instance reboot

Certificates

Use Let's Encrypt Certificate Authority[119] with CertBot[120], configure a Web Server Certificate.

certbot instructions: Apache on Ubuntu 18.04 LTS [121]

On the Web Server Instance, at the :/$ bash prompt, complete the following steps

1. **Add Certbot PPA**

```
sudo apt-get update
sudo apt-get install software-properties-common
sudo add-apt-repository universe
sudo add-apt-repository ppa:certbot/certbot
sudo apt-get update
```

2. **Install Certbot**

```
sudo apt-get install certbot python-certbot-apache
```

3. **Install an SSL certificate and automatically edit Apache configuration**

```
sudo certbot --apache
```

4. **Test Certbot automatic renewal**

```
sudo certbot renew --dry-run
```

---

[118] Ubuntu18.com [2019] *How to Install Apache on Ubuntu 18.04 Server* https://www.ubuntu18.com/install-apache-ubuntu-18/ [Accessed 5th December 2019]
[119] LetsEncrypt.org [2019] *Let's Encrypt* https://letsencrypt.org/ [Accessed 5th December 2019]
[120] CertBot.eff.org [2019] *CertBot* https://certbot.eff.org/ [Accessed 5th December 2019]
[121] CertBot.eff.org [2019] *certbot instructions: Apache on Ubuntu 18.04 LTS* https://certbot.eff.org/lets-encrypt/ubuntubionic-apache [Accessed 5th December 2019]

Wordpress [122]

Configuration

The following wordpress.conf file configuration configures Apache2 to serve Wordpress over HTTPS, port 443.

At the :/$ bash prompt, enter the following command to create a new wordpress.conf file

```
sudo nano /etc/apache2/sites-available/cybersecure.team.ssl.conf
```

Enter the following into the cybersecure.team.ssl.conf file

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerName cybersecure.team
        ServerAlias www.cybersecure.team
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        <Directory /var/www/html/>
                Options +FollowSymlinks
                AllowOverride All
                Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        Include /etc/letsencrypt/options-ssl-apache.conf
        SSLCertificateFile /etc/letsencrypt/live/cybersecure.team/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/cybersecure.team/privkey.pem

        RewriteEngine on
        RewriteCond %{SERVER_NAME} =cybersecure.team [OR]
        RewriteCond %{SERVER_NAME} =www.cybersecure.team
        RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]

</VirtualHost>
</IfModule>
```

Save and close the cybersecure.team.ssl.conf file

[122] Wordpress.org [2019] *How to install WordPress* https://wordpress.org/support/article/how-to-install-wordpress/ [Accessed 5th December 2019]

Download

With our RDS Database correctly configured, Apache2 installed and cybersecure.team.ssl.conf file configured, download latest Wordpress files to the Web Server Instance.

Wordpress was chosen as it is the most commonly used Blog based web application. Due to its wide use and active user and development community Wordpress is a stable Blog platform.

On the Web Server Instance, at the :/$ bash prompt, enter the following commands

Command	**Details**
:/$ cd /tmp	Change to the /tmp directory
:/tmp$ wget https://wordpress.org/latest.tar.gz	Download the latest tar.gz version of Wordpress
:/tmp$ sudo tar -xzvf latest.tar.gz	Unzip Wordpress to the Wordpress directory
:/tmp$ cd wordpress	Change to the /tmp/wordpress directory
:/tmp/wordpress$ sudo mv -v * /var/www/html	Move wordpress files to /var/www/html

Configuration

Configure wp-config.php to allow Wordpress to connect to the RDS Database Instance.

```
sudo cp /var/www/html/wp-config-sample.php /var/www/html/wp-config.php
sudo nano /var/www/html/wp-config.php
```

wp-config.php Database Connection: Under the section **// ** MySQL Settings ** //** enter the following:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'VPC_MZ_CST_P_EW1_PR_WP_DB'  );
/** MySQL database username */
define(  'DB_USER', 'cst_ew1_rds_adm'  );
/** MySQL database password */
define(  'DB_PASSWORD', ' Enter complex password from page 34 '  );
/** MySQL hostname */
define(  'DB_HOST', 'VPC-MZ-CST-ew1-rds-id.cuar6agiw6ov.eu-west-1.rds.amazonaws.com' );
```

Important Note: Hard Coding Username and Password

The username and password are initially configured in plaintext in the wp-config.php file.
This is only temporary measure to allow Wordpress connect to RDS to allow Wordpress to install.
Once Wordpress is successfully installed, the permissions of the Wordpress directories will be modified to only permit access to the www-data group, removing all permissions for others.

Security Keys

Wordpress will now be configured to use Unique Authentication Keys and Salts
Wordpress Random Keys and Salts Generator will provide the following random unique keys and salts:

Key/Salt	Description
'AUTH_KEY',	Authentication key
'SECURE_AUTH_KEY',	Secure authentication key
'LOGGED_IN_KEY',	Logged in key
'NONCE_KEY',	Nonce key
'AUTH_SALT',	Authentication salt
'SECURE_AUTH_SALT'	Secure authentication salt
'LOGGED_IN_SALT'	Logged in salt
'NONCE_SALT'	Nonce salt

1. Access Wordpress Keys and Salts Generator[123] https://api.wordpress.org/secret-key/1.1/salt/
2. In the wp-config.php file, go to the **Authentication Unique Keys and Salts** section
3. Copy and Replace the Wordpress Random Keys and Salts into the following section

```
define( 'AUTH_KEY',          'put your unique phrase here' );
define( 'SECURE_AUTH_KEY',   'put your unique phrase here' );
define( 'LOGGED_IN_KEY',     'put your unique phrase here' );
define( 'NONCE_KEY',         'put your unique phrase here' );
define( 'AUTH_SALT',         'put your unique phrase here' );
define( 'SECURE_AUTH_SALT',  'put your unique phrase here' );
define( 'LOGGED_IN_SALT',    'put your unique phrase here' );
define( 'NONCE_SALT',        'put your unique phrase here' );
```

Securing Wordpress
Directory Permissions

Modify the permissions of the Wordpress directories to only permit access to the www-data local group

Command	Details
sudo chown -R www-data:www-data /var/www/html/	Change directory ownership to www-data
sudo usermod -a -G www-data ubuntu	Add ubuntu user to www-data group
sudo chmod 770 -R /var/www/html/	7: Grants rwx to file owner www-data 7: Grants rwx to group www-data 0: removes all permissions for others

Wordpress File Clean-up: Delete the downloaded Wordpress files

Command	Details
:/$ cd /tmp	Change to /tmp directory
:/tmp$ sudo rm -r wordpress	Remove the wordpress directory
:/tmp$ sudo rm -r latest.tar.gz	Remove the latest.tar.gz Wordpress file
sudo rm /var/www/html/index.html	Remove Apache2 index.html file
sudo rm /var/www/html/phpinfo.php	Remove PHP phpinfo.php file

[123] Wordpress.org [2019] Wordpress Keys and Salts Generator https://api.wordpress.org/secret-key/1.1/salt/ [Accessed 5th December 2019]

Initialisation

At the :/$ bash prompt, enter the following commands

Command	Details
sudo a2ensite cybersecure.team.ssl.conf	Enable cybersecure.team site in Apache2
sudo a2enmod ssl	Enable Apache2 SSL mode
sudo systemctl status apache2	Confirm Apache2 service status
sudo systemctl restart apache2	Restart Apache2 service
sudo systemctl status apache2	Reconfirm Apache2 service status

Application Load Balancing (ALB)

To serve the Web Application over HTTPS:443 an SSL certificate must be installed on the Application load Balancer (ALB).

Create Certificate

Generate an SSL certificate for the cybersecure.team domain on SSL for Free[124]

1. Browse to https://www.sslforfree.com/
2. In the 'Secure | https:// enter your website to secure' field enter cybersecure.team
3. For Domain Verification select Manual Verification, then Manually Verify Domain
4. Download the verification files
5. On the Web Server instance create directory /var/www/html/.well-known
6. On the Web Server instance create directory /var/www/html/.well-known/acme-challenge
7. Upload the verification files to /var/www/html/.well-known/acme-challenge
8. Click Download SSL Certificate

   This will create an SSL certificate with the following encryption:

   Public key: RSA 2048-bit
   Signature algorithm: SHA256WITHRSA

Import Certificate

Import the SSL for Free SSL Certificate into AWS Certificate Manager

1. Navigate to AWS Console > Services > Certificate Manager > Import a Certificate
2. Copy contents of PEM-encoded Certificate body (filename: certificate.crt) from SSL for Free
3. Paste contents into Certificate body field
4. Copy contents of PEM-encoded Certificate private key (filename: private.key) from SSL for Free
5. Paste contents into Certificate private key field
6. Copy contents of PEM-encoded Certificate chain (filename: ca_bundle.crt) from SSL for Free
7. Paste contents into the Certificate chain field
8. Click Next >
9. For Tag Name enter VPC-MZ-CST-EW1-ALB-Cert > click Review and import

[124] SSLforFree.com [2019] *SSL For Free* https://www.sslforfree.com/ [Accessed 5th December 2019]

Amazon Machine Image (AMI)

Using the securely configured Web Server Instance, create and configure a secure custom AWS Machine Image (AMI)[125] which will be stored in AWS and used by our AWS Auto Scaling Group (ASG)[126] for Elastic Load Balancing (ELB)[127] and for Burst Capacity .

Prerequisite: Gracefully shutdown the Web Server Instance; sudo shutdown

Create Custom AMI:

1. Navigate to AWS Console > Services > EC2 > Instances > Select Web Server Instance
2. Right click Web Server Instance > right click > Image > Create Image

    Image name: VPC-MZ-CST-EW1-WS-AMI
    Image description: VPC-MZ-CST-EW1-WS-AMI
    No reboot: Not selected
    Instance Volumes
        Delete on Termination: Ensure this is NOT selected
        Encrypted: Confirm status is Encrypted

3. Click Create Image

    It will take approximately 5 minutes for the AMI image to be created

Identity and Access Management (IAM)

Create an IAM Role specifically for the Web Application Blog for exclusive use by the AWS Auto Scaling and Application Load Balancer services.

1. Navigate to AWS Console > Services > IAM > Roles > Create Role
    Select type of trusted entity: AWS service
    Choose the service that will use this role: EC2
2. Next: Permissions
    Policy Name: AmazonEC2FullAccess
    Set permissions boundary: Create role without a permissions boundary
3. Next: Tags
    Key: IAM EC2 Application Role
    Value: IAM EC2 Application Role for Wordpress
4. Next: Review
    Role Name: IAM_EC2_Application_Role_for_Wordpress
    Role Description: Allows EC2 instances to call AWS services on your behalf.
    Trusted entities: AWS service: ec2.amazonaws.com
    Policies: AWS Managed Policy AmazonEC2FullAccess
5. Permissions boundary: Permissions boundary is not set
6. Create Role

---

[125] Amazon Web Services [2019] *AWS Machine Image* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html [Accessed 5th December 2019]
[126] Amazon Web Services [2019] *AWS Auto Scaling Group* https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html [Accessed 5th December 2019]
[127] Amazon Web Services [2019] *AWS Elastic Load Balancing* https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html [Accessed 5th December 2019]

Create ALB

Prerequisites: Before configuring the Elastic Application Load Balancer ensure all of the following Prerequisites have been successfully completed

Service	Name(s)
Virtual Private Cloud (VPC)	VPC-MZ-CST-EW1
Public Subnets	VPC-MZ-CST-EW1-A-PU VPC-MZ-CST-EW1-B-PU VPC-MZ-CST-EW1-C-PU
Private Subnets	VPC-MZ-CST-EW1-A-PR VPC-MZ-CST-EW1-B-PR VPC-MZ-CST-EW1-C-PR
Elastic IP	VPC-MZ-CST-EW1-EIP
NAT Gateway	VPC-MZ-CST-EW1-NAT-GW
Internet Gateway	VPC-MZ-CST-EW1-Internet-GW
Amazon Machine Image (AMI)	VPC-MZ-CST-EW1-WS-AMI
IAM Role	IAM_EC2_Application_Role_for_Wordpress

Table 26. Elastic Application Load Balancing Prerequisites [128]

Configuration: Navigate to AWS Console > EC2 > Load Balancing > Load Balancer > Create Load Balancer > Application Load Balancer HTTP HTTPS > Create

Step 1: Configure Load Balancer

Item	Value
Name	VPC-MZ-CST-EW1-ALB
Description	VPC-MZ-CST-EU West 1-Application Load Balancer
Scheme	internet-facing
IP address type	IPv4
Listeners: Load Balancer Protocol	HTTPS
Listeners: Load Balancer Port	443
VPC	VPC-MZ-CST-EW1
Availability Zone	eu-west-1a
Public subnet	VPC-MZ-CST-EW1-A-PU
IPv4 Address	Assigned by AWS
Availability Zone	eu-west-1b
Public subnet	VPC-MZ-CST-EW1-B-PU
IPv4 Address	Assigned by AWS
Availability Zone	eu-west-1c
Public subnet	VPC-MZ-CST-EW1-C-PU
IPv4 Address	Assigned by AWS
Tag Key Name	VPC-MZ-CST-EW1-ALB

Table 27. Configure Load Balancer [129]

[128] Taaffe, Jonathon [2019] *Table 26. Elastic Application Load Balancing Prerequisites* [Created 5th December 2019]
[129] Taaffe, Jonathon [2019] *Table 27. Configure Load Balancer* [Created 5th December 2019]

Step 2: Configure Security Settings

Certificate type: Choose a certificate from ACM
Cert Name: cybersecure.team
Security policy: ELBSecurityPolicy-2016-08

Step 3: Configure Security Groups
Assign a security group: Select an existing security group

Name	Details
VPC-MZ-CST-EW1-ALB-SG	Application Load Balancer Security Group
VPC-MZ-CST-EW1-A-WS-SG	eu-west-1a Public Web Server Security Group
VPC-MZ-CST-EW1-B-WS-SG	eu-west-1b Public Web Server Security Group
VPC-MZ-CST-EW1-C-WS-SG	eu-west-1c Public Web Server Security Group

Step 4: Configure Routing

Setting	Choice
Target group	New target group
Name	VPC-MZ-CST-EW1-ALB-TG
Target type	Instance
Protocol	HTTPS
Port	443
Health checks Protocol	HTTPS
Health checks Path	/
Advanced Health Check	Leave default

Step 5: Register Targets

Important: Do not select or register any EC2 Instances as will create Auto Scaling Group

Step 6: Review
Review the Load Balancer Configuration to confirm it is correct.

Step 7: Click Create and once the Load Balancer is successfully created click Close

Important: It will take approximately 5 minutes for the Load Balancer to be provisioned. Do not proceed until the Load Balancer status is Active.

Select the Load Balancer and copy the DNS Name for future reference.

Auto Scaling Launch Configuration

Configure a Launch Configuration which the Application Load Balancer will use to Launch instances of previously created secure custom Web Server AMI Image.

Configuration: Navigate to AWS Console > Services > EC2 > Auto Scaling > Launch Configuration > Create Launch Configuration

Step 1: Choose AMI

From the Left Nav Bar select My AMI's
Select secure custom Web Server Instance AMI: VPC-MZ-CST-EW1-WS-AMI

Step 2: Choose Instance Type

Select: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS)

Step 3: Configure Details

Item	Value
Name	VPC-MZ-CST-EW1-ALB-WS-LC
Purchasing option	None
IAM role	IAM_EC2_Application_Role_for_Wordpress [1]
Monitoring	Enable CloudWatch detailed monitoring: Enabled[2]
IP Address Type	Do not assign a public IP address to any instances [3]
Delete on Termination	Selected [4]
Encrypted	Yes [5]

Configuration Notes

[1]	IAM Role	Web Application Blog IAM Role
[2]	Monitoring	Ensure Monitoring is enabled for all instances launched
[3]	IP Address Type	No public IP address as all traffic routed by ALB
[4]	Delete on Termination	Auto Scaling AMI Instance EBS volume deleted on termination
[5]	Encrypted	EBS volume encrypted ensure data-at-rest encryption

Step 4: Add Storage

Delete on Termination: Ensure this enabled
Encrypted: Confirm EBS volume is encrypted

Step 5: Configure Security Groups

Assign a security group: Select an existing security group

Name	Details
VPC-MZ-CST-EW1-ALB-SG	Application Load Balancer Security Group
VPC-MZ-CST-EW1-A-WS-SG	eu-west-1a Public Web Server Security Group
VPC-MZ-CST-EW1-B-WS-SG	eu-west-1b Public Web Server Security Group
VPC-MZ-CST-EW1-C-WS-SG	eu-west-1c Public Web Server Security Group

Step 6: Review

Review the Launch Configuration to confirm it is correct
Create Launch Configuration

Step 7: Create and Download SSH Private Key
Select Create a New Key Pair
For Key Pair Name enter VPC-MZ-CST-EW1-ALB-WS-LC

Step 8: Click Create Launch Configuration
Step 9: Click Create Auto Scaling Group

Auto Scaling Group

Configure an Auto Scaling Group from which custom secure AMI instances will be launched

Step 1: Configure Auto Scaling group details

Item	Value
Group Name	VPC-MZ-CST-EW1-ALB-WS-ASG
Launch Configuration	VPC-MZ-CST-EW1-ALB-WS-LC
Group size	3 [1]
VPC	VPC-MZ-CST-EW1
Public Subnet	VPC-MZ-CST-EW1-A-PU | eu-west-1a [2]
Public Subnet	VPC-MZ-CST-EW1-B-PU | eu-west-1b [2]
Public Subnet	VPC-MZ-CST-EW1-C-PU | eu-west-1c [2]
Load Balancing	Select: Receive traffic from one or more load balancers [4]
Target Groups	VPC-MZ-CST-EW1-ALB-TG [4]
Health Check Type	EC2
Health Check Grace Period	300 seconds
Monitoring	Enable: CloudWatch detailed monitoring [5]
Instance Protection	None
Service-Linked Role	AWSServiceRoleForAutoScaling [6]

Configuration Notes

[1]	Group Size	Setting size to 3 will ensure an AMI instance is launched in each AZ
[2]	Public Subnet	Public subnets the Application Load Balancer instances will be launched in.
[3]	Load Balancing	Enable ALB Target Group configuration
[4]	Target Groups	Select require Target Group
[5]	Monitoring	Receive alerts from the Auto Scaling Group Instances.
[6]	Service-Linked Role	Permissions to create Auto Scaling Group

Step 2: Configure scaling policies
Select: Keep this group at its initial size

Step 3: Configure Notifications
Add Notification

Send a notification to	VPC-MZ-CST-EW1-ALB-WS-ASG_Notification
With these recipients	admin@cybersecure.team
Whenever instances	launch, terminate, fail to launch, fail to terminate

Step 4: Configure Tags
Key: Name
Value: VPC-MZ-CST-EW1-ALB-WS-ASG

Step 5: Review

Click Review and Review the Auto Scaling Group Configuration
Click Create Auto Scaling Group
Click Close when Auto Scaling Group created

Functional Test

Confirm and Test all components of the Elastic Application Load Balancer

EC2 Instances: Navigate to AWS Console > Services > EC2 > Instances > Instances - Confirm the following:

New Instances have launched	3
New Instance in each Availability Zone: eu-west-1a, eu-west-1b, eu-west-1c	1
Rename new instances name	VPC-MZ-CST-EW1-WS-AMI
Instance Description	
New Instance Status Checks – System	System reachability check passed
New Instance Status Checks – Instance	Instance reachability check passed

Auto Scaling Groups: Navigate to AWS Console > Services > EC2 > Auto Scaling > Auto Scaling Groups > Select Auto Scaling Group > Details - Confirm the following:

Launch Configuration:	VPC-MZ-CST-EW1-ALB-WS-LC
Desired Capacity: 3	3
Min: 3	3
Max: 3	3
Availability Zone(s):	eu-west-1a, eu-west-1b, eu-west-1c
Target Groups:	VPC-MZ-CST-EW1-ALB-TG

Auto Scaling Groups: Navigate to AWS Console > Services > EC2 > Auto Scaling > Auto Scaling Groups > Select Auto Scaling Group > Instances - Confirm the following:

Lifecycle	**Launch Configuration / Template**	**Availability Zone**	**Health Status**
InService	VPC-MZ-CST-EW1-ALB-WS-LC	eu-west-1a	Healthy
InService	VPC-MZ-CST-EW1-ALB-WS-LC	eu-west-1b	Healthy
InService	VPC-MZ-CST-EW1-ALB-WS-LC	eu-west-1c	Healthy

Load Balancer Target Groups: Navigate to AWS Console > Services > EC2 > Load Balancing > Target Groups > Select Target Group > Description - Confirm the following:

Name:	VPC-MZ-CST-EW1-ALB-TG
Protocol:	HTTPS
Port:	443
Target type:	Instance
Load balancer:	VPC-MZ-CST-EW1-ALB

Load Balancer Target Groups: Navigate to AWS Console > Services > EC2 > Load Balancing > Target Groups > Select Target Group > Targets > Registered Targets: Confirm the following:

Port	AZ	Status	Description
443	eu-west-1a	healthy	Target currently passing target group's health checks
443	eu-west-1b	healthy	Target currently passing target group's health checks
443	eu-west-1c	healthy	Target currently passing target group's health checks

Load Balancer Target Groups: Navigate to AWS Console > Services > EC2 > Load Balancing > Target Groups > Select Target Group > Targets > Availability Zones - Confirm the following:

Availability Zone	Target count	Healthy?
eu-west-1a	1	Yes
eu-west-1c	1	Yes
eu-west-1b	1	Yes

Load Balancer Target Groups: Navigate to AWS Console > Services > EC2 > Load Balancing > Target Groups > Select Target Group > Health Checks - Confirm the following:

Protocol: HTTPS
Path: /
Port: traffic port

Load Balancer Connectivity: Navigate to AWS Console > Services > EC2 > Load Balancing > Load Balancer

1. Copy the DNS Name of the Load Balancer

   Example: VPC-MZ-CST-EW1-ALB-*xxxxxxxxxx*.eu-west-1.elb.amazonaws.com

2. Open Browser > https://VPC-MZ-CST-EW1-ALB-*xxxxxxxxxx*.eu-west-1.elb.amazonaws.com

   You should now be connected to the Wordpress Install page

Application Configuration

Install Wordpress

Install Wordpress Blog by browsing to the DNS Name of the Application Load Balancer

Example: https://VPC-MZ-CST-EW1-ALB-*xxxxxxxxxx*.eu-west-1.elb.amazonaws.com

You will be redirected to: http://*ALBDNSName*/wp-admin/install.php

Enter the following details in the Wordpress Blog Install screen:

Label	Value	Details
Language	English (UK)	Wordpress site language
Site Title	CyberSecure.Team	Wordpress site title
Username	VPC_MZ_CST_P_PU_WP_ADM	Wordpress administrator account
Password	Auto generated	Ensure password complies with company password policy
Your Email	webmaster@CyberSecure.Team	Webmaster email address
Search Engine Visibility	Enabled	Discourage search engines from indexing site

Table 28. Wordpress Blog Install Options [130]

Secure Wordpress

By default, Wordpress includes additional configuration items that if left installed and unused increase the Wordpress attack surface. The following security configuration steps should be taken to secure the Wordpress Blog Application:

Action	Steps
Delete Default Post, Page, Comment	Posts > All Posts >Delete default “Hello world” post Pages > All Pages > Delete default “Sample Page” Comments > Delete default comment
Set Your Timezone	Settings > General > Timezone > Dublin
Disable User Registration	Settings > General > Membership >Disable Anyone can register Settings > General > New User Default Role: Subscriber
Discussion/Comments Settings	Settings > Discussion > Disable the following: • Attempt to notify any blogs linked to from the post • Allow link notifications from other blogs • Allow people to submit comments on new posts • Email me whenever • Avatar Display

Table 29. Securing Wordpress Configuration [131]

[130] Taaffe, Jonathon [2019] *Table 28. Wordpress Blog Install Options* [Created 5th December 2019]
[131] Taaffe, Jonathon [2019] *Table 29. Securing Wordpress – Additional Configuration Items* [Created 5th December 2019]

Action	Steps
Comments Settings	Settings > Discussion > Other comment settings > Enable: • Comment author must fill out name and email • Users must be registered and logged in to comment Settings > Discussion > Before a comment appears > Enable: • Comment must be manually approved
WordPress Media Settings	Settings > Media > set all sizes to 0 (zero)
WordPress Permalinks	Settings > Permalinks > Select: Post name

Table 29. Securing Wordpress Configuration Items (contd.)[87]

Plug-ins

The following Wordpress Security Plug-ins are well established and configured on many production Wordpress sites. These plug-ins are available for free, are highly regarded in the Wordpress community and offer enhanced security for Wordpress.

To Install and Activate Wordpress Plugins: Plugins > Add New > search for plugins > Install > Active

Wordpress Security Plugin: All In One WP Security [132]
This plugin offers many security configuration options for Wordpress. Below is a summary table of the security changes implemented with All in One WP Security.

Critical Feature Status	
Admin Username	ON
Login Lockdown	ON
File Permission	ON
Basic Firewall	ON
Login Lockdown	
Enable Login Lockdown Feature	Enabled
Allow Unlock Requests	Disabled
Max Login Attempts	3
Login Retry Time Period (min)	5
Time Length of Lockout (min)	60
Display Generic Error Message	Enabled
Instantly Lockout Invalid Usernames	Enabled

Table 30. All In One WP Security Configuration [133]

[132] Wordpress.org [2019] *All In One WP Security* https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/ [Accessed 5th December 2019]
[133] Taaffe, Jonathon [2019] *Table 30. All In One WP Security Configuration* [Created 5th December 2019]

Wordpress Security Plugin: All In One WP Security (contd.)
Below is the File System Security configuration enabled through All In One Security

		Permissions		
Name	File/Folder	Recommended	Current	Action
Root directory	/var/www/html/	755	770	None
wp-includes/	/var/www/html/wp-includes	755	770	None
.htaccess	/var/www/html/.htaccess	644	644	None
wp-admin/index.php	/var/www/html/wp-admin/index.php	644	770	None
wp-admin/js/	/var/www/html/wp-admin/js/	755	770	None
wp-content/themes/	/var/www/html/wp-content/themes	755	770	None
wp-content/plugins/	/var/www/html/wp-content/plugins	755	770	None
wp-admin/	/var/www/html/wp-admin	755	770	None
wp-content/	/var/www/html/wp-content	755	770	None
wp-config.php	/var/www/html/wp-config.php	640	770	None

Table 31. All In One WP Security File System Security [134]

Wordpress Security Plugin: ShieldSecurity WP Plugin [135]
This is an excellent Wordpress Security Plugin with a multitude of Security Configuration options. Below is a summary table of the Wordpress Security Configuration enabled through ShieldSecurity:

Setting	**Description**
General Settings	Visitor IP: Visitor IP address source is: Automatically Detect Visitor IP
General Settings	Reporting Email: Email address for reports set to: webmaster@cybersecure.team
Security Admin	Security Admin: Security plugin is protected against tampering
Security Admin	Important Options: Important WP options are protected against tampering
Security Admin	WP Admins: Admin users are protected against tampering
Activity Audit Log	Audit Areas: All important events on your site are being logged
Activity Audit Log	Audit Trail: Maximum Audit Trail entries limited to 100
Hack Guard	Scan Frequency: Automatic scanners only run once per day
Hack Guard	WP Core File Scan: Core files scanned regularly for hacks
Hack Guard	Unrecognised Files: Core directories scanned regularly for unrecognised files
Hack Guard	Abandoned Plugins: Abandoned Plugins Scanner is enabled.
Login Guard	Brute Force Login: Login forms are protected against bot attacks
Login Guard	Bot User Register: Registration forms are protected against bot attacks
Login Guard	Brute Force Lost Password: Lost Password forms are protected against bot attacks
Login Guard	Identity Verification: At least 1 2FA option is enabled

Table 32. ShieldSecurity Enabled Security Configuration [136]

[134] Taaffe, Jonathon [2019] *Table 31. All In One WP Security File System Security* [Created 5th December 2019]
[135] Wordpress.org [2019] *Shield Security: Protection with Smarter Automation* https://wordpress.org/plugins/wp-simple-firewall/ [Accessed 5th December 2019]
[136] Taaffe, Jonathon [2019] *Table 32. ShieldSecurity Enabled Security Configuration* [Created 5th December 2019]

Setting	Description
User Management	Idle Users: Idle sessions are terminated after 48 hours
User Management	Lock To IP: Sessions are locked to IP address
User Management	Pwned Passwords: Pwned passwords are blocked on this site
SPAM Blocking	Bot SPAM: Bot SPAM comments are blocked
SPAM Blocking	Human SPAM: Comments posted by humans are checked for SPAM
Automatic Updates	Core Updates: Minor WP Core updates will be installed automatically
Automatic Updates	Self-Auto-Update: Shield is automatically updated
HTTP Security Headers	HTTP Headers: All important security Headers have been set
HTTP Security Headers	Content Security Policies: Content Security Policy is turned on
WordPress Lockdown	File Editing via WP: File editing is disabled
WordPress Lockdown	XML-RPC: XML-RPC is disabled
WordPress Lockdown	REST API: Anonymous REST API is disabled
Firewall	Firewall: Your site is protected against malicious requests
Firewall	Ignore Admins: Firewall rules are also applied to admins

Table 32. ShieldSecurity Enabled Security Configuration (contd.) [92]

Wordpress Security Plugin: Stop User Enumeration [137]
This security plugin attempts to restrict User Enumeration.

Wordpress Security Plugin: Cloudflare WP Plugin [138]
Cloudflare plugin allows you to configure Wordpress settings for optimal connectivity to CloudFlare Internet Web Services.

Wordpress Security Plugin: WP Force SSL [139]
WP Force SSL ensures all web requests to your Wordpress site are converted to HTTPS:443 requests.

[137] Wordpress.org [2019] *Stop User Enumeration* https://wordpress.org/plugins/stop-user-enumeration/ [Accessed 5th December 2019]
[138] Wordpress.org [2019] *Cloudflare Wordpress Plugin* https://wordpress.org/plugins/cloudflare/ [Accessed 5th December 2019]
[139] Wordpress.org [2019] *WP Force SSL* https://wordpress.org/plugins/wp-force-ssl/ [Accessed 5th December 2019]

Security Implementation

AWS Config

AWS Config inventories your AWS resources and allows you to define rules to determine if your AWS resources are optimally configured.

Configure AWS Config: Navigate to AWS Console > Services > Config

Resource types:	All resources (including global resources)
Amazon S3 bucket:	Create new S3 bucket – required to store log files
AWS Config role:	AWSServiceRoleForConfig

Below is a summary of the AWS Config Rule Configuration for VPC-MZ-CST-EW1 Virtual Private Cloud Resources.

Label	Value
ebs-snapshot-public-restorable-check	Checks whether Amazon Elastic Block Store (Amazon EBS) snapshots are not publicly restorable. The rule is NON_COMPLIANT if one or more snapshots with RestorableByUserIds field are set to all, that is, Amazon EBS snapshots are public.
ec2-instance-no-public-ip	Checks whether Amazon Elastic Compute Cloud (Amazon EC2) instances have a public IP association. The rule is NON_COMPLIANT if the publicIp field is present in the Amazon EC2 instance configuration item. This rule applies only to IPv4.
ec2-security-group-attached-to-eni	Checks that security groups are attached to Amazon Elastic Compute Cloud (EC2) instances or an elastic network interfaces (ENIs). The rule returns NON_COMPLIANT if the security group is not associated with an EC2 instance or an ENI.
vpc-sg-open-only-to-authorized-ports	Checks whether any security groups with inbound 0.0.0.0/0 have TCP or UDP ports accessible. The rule is NON_COMPLIANT when a security group with inbound 0.0.0.0/0 has a port accessible which is not specified in the rule parameters.
alb-http-to-https-redirection-check	Checks whether HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers. The rule is NON_COMPLIANT if one or more HTTP listeners of Application Load Balancer do not have HTTP to HTTPS redirection configured.
elb-deletion-protection-enabled	Checks whether an Elastic Load Balancer has deletion protection enabled. The rule is NON_COMPLIANT if deletion_protection.enabled is false.
internet-gateway-authorized-vpc-only	Checks that Internet gateways (IGWs) are only attached to an authorized Amazon Virtual Private Cloud (VPCs). The rule is NON_COMPLIANT if IGWs are not attached to an authorized VPC.

Table 33. AWS Config Rule Configuration – Part 1 [140]

[140] Taaffe, Jonathon [2019] *Table 33. AWS Config Rule Configuration - Part 1* [Created 5th December 2019]

Label	Value
iam-user-mfa-enabled	Checks whether the AWS Identity and Access Management users have multi-factor authentication (MFA) enabled.
mfa-enabled-for-iam-console-access	Checks whether AWS Multi-Factor Authentication (MFA) is enabled for all AWS Identity and Access Management (IAM) users that use a console password. The rule is compliant if MFA is enabled.
iam-policy-no-statements-with-admin-access	Checks whether the default version of AWS Identity and Access Management (IAM) policies do not have administrator access. If any statement has "Effect": "Allow" with "Action": "*" over "Resource": "*", the rule is non-compliant.
vpc-flow-logs-enabled	Checks whether Amazon Virtual Private Cloud flow logs are found and enabled for Amazon VPC.
elb-logging-enabled	Checks whether the Application Load Balancers and the Classic Load Balancers have logging enabled.
ec2-instance-managed-by-systems-manager	Checks whether the Amazon EC2 instances in your account are managed by AWS Systems Manager.
ec2-managedinstance-association-compliance-status-check	Checks whether the compliance status of the AWS Systems Manager association compliance is COMPLIANT or NON_COMPLIANT after the association execution on the instance. The rule is compliant if the field status is COMPLIANT.
ec2-managedinstance-patch-compliance-status-check	Checks whether the compliance status of the AWS Systems Manager patch compliance is COMPLIANT or NON_COMPLIANT after the patch installation on the instance. The rule is compliant if the field status is COMPLIANT.
rds-snapshots-public-prohibited	Checks if Amazon Relational Database Service (Amazon RDS) snapshots are public. The rule is non-compliant if any existing and new Amazon RDS snapshots are public.
iam-root-access-key-check	Checks whether the root user access key is available. The rule is compliant if the user access key does not exist.
vpc-default-security-group-closed	Checks that the default security group of any Amazon Virtual Private Cloud (VPC) does not allow inbound or outbound traffic. The rule is non-compliant if the default security group has one or more inbound or outbound traffic.
rds-instance-public-access-check	Checks whether the Amazon Relational Database Service (RDS) instances are not publicly accessible. The rule is non-compliant if the publiclyAccessible field is true in the instance configuration item.
s3-bucket-replication-enabled	Checks whether the Amazon S3 buckets have cross-region replication enabled.
elb-acm-certificate-required	Checks whether the Elastic Load Balancer(s) uses SSL certificates provided by AWS Certificate Manager. You must use an SSL or HTTPS listener with your Elastic Load Balancer to use this rule.
autoscaling-group-elb-healthcheck-required	Checks whether your Auto Scaling groups that are associated with a load balancer are using Elastic Load Balancing health

Table 34. AWS Config Rule Configuration – Part 2[141]

[141] Taaffe, Jonathon [2019] *Table 34. AWS Config Rule Configuration – Part 2* [Created 5th December 2019]

Label	Value
s3-bucket-public-read-prohibited	Checks that your S3 buckets do not allow public read access. If an S3 bucket policy or bucket ACL allows public read access, the bucket is noncompliant.
s3-bucket-public-write-prohibited	Checks that your S3 buckets do not allow public write access. If an S3 bucket policy or bucket ACL allows public write access, the bucket is noncompliant.
iam-user-group-membership-check	Checks whether IAM users are members of at least one IAM group.
ec2-instance-detailed-monitoring-enabled	Checks whether detailed monitoring is enabled for EC2 instances.
ec2-volume-inuse-check	Checks whether EBS volumes are attached to EC2 instances. Optionally
s3-bucket-logging-enabled	Checks whether logging is enabled for your S3 buckets.
ebs-optimized-instance	Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.
iam-password-policy	Checks whether the account password policy for IAM users meets the specified requirements.
rds-multi-az-support	Checks whether high availability is enabled for your RDS DB instances.
rds-storage-encrypted	Checks whether storage encryption is enabled for your RDS DB instances.
eip-attached	Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.
encrypted-volumes	Checks whether EBS volumes that are in an attached state are encrypted. Optionally, you can specify the ID of a KMS key to use to encrypt the volume.
restricted-ssh	Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.
ec2-instances-in-vpc	Checks whether your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.
root-account-mfa-enabled	Checks whether the root user of your AWS account requires multi-factor authentication for console sign-in.

Table 34. AWS Config Rule Configuration – Part 3 [142]

[142] Taaffe, Jonathon [2019] *Table 34. AWS Config Rule Configuration – Part 3* [Created 5th December 2019]

Acronyms

The following is a list of acronyms used throughout this report collated here for ease of reference.

Category	Acronym	Description
General	CST	CyberSecure.Team
General	CSP	Cloud Service Provider
Business	DR	Disaster Recovery
Business	BCP	Business Continuity Plan
Business	SLA	Service Level Agreement
Business	ISMS	Information Security Management System
Cloud	AWS	Amazon Web Services
Cloud	GCP	Google Cloud Platform
Cloud	IaaS	Infrastructure as a Service
Cloud	PaaS	Platform as a Service
Cloud	SaaS	Software as a Service
Cloud	DBaaS	Database as a Service
Cloud	AMI	Amazon Machine Image
Cloud	VPC	Virtual Private Cloud
Cloud	EIP	Elastic IP
Cloud	AZ	Availability Zone
Cloud	MZ	Multi Availability Zones
Cloud	EW1	eu-west-1 Availability Zone
Cloud	EC2	Elastic Cloud Compute
Cloud	RDS	Relational Database Services
Cloud	ELB	Elastic Load Balancer
Cloud	ALB	Application Load Balancer
Cloud	ASG	Auto Scaling Group
Standards, Regulations	NIST	National Institute of Standards and Technology
Standards, Regulations	RMF4CE	Risk Management Framework in a Cloud Ecosystem
Standards, Regulations	CSA	Cloud Security Alliance
Standards, Regulations	GRC	Governance, Risk Management & Compliance
Standards, Regulations	STAR	Security, Trust and Assurance Registry
Standards, Regulations	CCM	Cloud Controls Matrix
Standards, Regulations	CAIQ	Consensus Assessment Initiative Questionnaire
Standards, Regulations	GDPR	General Data Protection Regulation
Standards, Regulations	DoD	U.S. Department of Defense
Standards, Regulations	FedRAMP	U.S. Federal Risk and Authorization Management Program
Standards, Regulations	DOJ	U.S. Department of Justice
Standards, Regulations	CJIS	U.S. Criminal Justice Information Systems
Standards, Regulations	ITAR	U.S. International Traffic in Arms Regulations
Standards, Regulations	EAR	U.S. Export Administration Regulations
Standards, Regulations	SRG	Security Requirements Guide
Standards, Regulations	FIPS	U.S. Federal Information Processing Standards
Standards, Regulations	ISO	International Organization for Standardization

Technology	IAM	Identity and Access Management
Technology	RBAC	Role-base Access Control
Technology	NAT	Network Address Translation
Technology	DNS	Domain Naming Service
Technology	DNSSEC	Secure DNS Service
Technology	DoS	Denial of Service
Technology	DDoS	Distributed Denial of Service
Technology	EDoS	Economic Denial of Service
Technology	SSH	Secure Shell
Technology	SSL	Secure Sockets Layer

References

The following is the list of references referred to in this report.

1	Wikipedia.org	[2019]	Role-based Access Control	https://en.wikipedia.org/wiki/Role-based_access_control	[Accessed 5th December 2019]
2	Techopedia.com	[2019]	CIA Triad of Information Security	https://www.techopedia.com/definition/25830/cia-triad-of-information-security	[Accessed 5th December 2019]
3	Journal of Cloud Computing	[2019]	High availability in clouds: systematic review and research challenges	https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0066-8	[Accessed 5th December 2019]
4	Taaffe, J	[2019]	Table 1. Grouping and Summarising of C-Board Requirements		[Created 5th December 2019]
5	NIST.gov	[2012]	The NIST Definition of Cloud Computing	https://csrc.nist.gov/publications/detail/sp/800-145/final	[Accessed 5th December 2019]
6	Taaffe, Jonathon	[2019]	Table 2. Solution Functional Requirements		[Created 5th December 2019]
7	Taaffe, Jonathon	[2019]	Table 3. Cloud Service Models		[Created 5th December 2019]
8	Taaffe, Jonathon	[2019]	Table 4. IaaS Component SLA's		[Created 5th December 2019]
9	NIST.gov	[2019]	Guidelines on Security and Privacy in Public Cloud Computing	https://csrc.nist.gov/publications/detail/sp/800-144/final	[Accessed 5th December 2019]
10	NIST.gov	[2019]	NIST Cloud Computing Security Reference Architecture	https://csrc.nist.gov/publications/detail/sp/500-299/draft	[Accessed 5th December 2019]
11	NIST.gov	[2019]	Figure 1. NIST Risk Management Framework in a Cloud Ecosystem	https://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity	[Accessed 5th December 2019]
12	CloudSecurityAlliance.org	[2019]	CSA Security & Risk Management	https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/	[Accessed 5th December 2019]
13	CloudSecurityAlliance.org	[2019]	CSA Security Trust Assurance and Risk (STAR)	https://cloudsecurityalliance.org/star/	[Accessed 5th December 2019]
14	CloudSecurityAlliance.org	[2019]	CSA Cloud Customers Portal	https://cloudsecurityalliance.org/star/cloud-customer/	[Accessed 5th December 2019]
15	CloudSecurityAlliance.org	[2019]	CSA STAR Registry	https://cloudsecurityalliance.org/star/registry/	[Accessed 5th December 2019]
16	CloudSecurityAlliance.org	[2019]	CSA Cloud Controls Matrix v3.0.1	https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/	[Accessed 5th December 2019]
17	CloudSecurityAlliance.org	[2019]	CSA Consensus Assessment Initiative Questionnaire (CAIQ)	https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/	[Accessed 5th December 2019]
18	CloudSecurityAlliance.org	[2019]	CSA GDPR Center of Excellence Home	https://gdpr.cloudsecurityalliance.org/resource-center/csa-code-of-conduct-for-gdpr-compliance/	[Accessed 5th December 2019]
19	ISO.org	[2016]	Information technology - Cloud computing - Service level agreement (SLA) framework	https://standards.iso.org/ittf/PubliclyAvailableStandards/c067545_ISO_IEC_19086-1_2016.zip	[Accessed 5th December 2019]
20	Crisp Research	[2019]	Cloud Computing Vendor & Service Provider Comparison	https://d1.awsstatic.com/analyst-reports/Report_CVU_CC_AWS_ENGL_final.pdf?trk=ar_card	[Accessed 5th December 2019]
21	Amazon Web Services	[2019]	Amazon Web Services (AWS)	https://aws.amazon.com/	[Accessed 5th December 2019]
22	Microsoft Azure	[2019]	Microsoft Azure	https://azure.microsoft.com/	[Accessed 5th December 2019]
23	Google Cloud Platform	[2019]	Google Cloud Platform	https://cloud.google.com/	[Accessed 5th December 2019]
24	Taaffe, Jonathon	[2019]	Table 5. Solution Functional Requirements		[Created 5th December 2019]
25	Taaffe, Jonathon	[2019]	Table 6. Name.com Account Settings		[Created 5th December 2019]
26	Taaffe, Jonathon	[2019]	Table 7. Web Infrastructure and Website Security Requirements		[Created 5th December 2019]
27	Cloudflare.com	[2019]	The Integrated Global Cloud Platform	https://www.cloudflare.com/	[Accessed 5th December 2019]
28	Cloudflare.com	[2019]	Cloudflare Free SSL/TLS	https://www.cloudflare.com/ssl/	[Accessed 5th December 2019]
29	Cloudflare.com	[2019]	What is a DDoS Attack?	https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/	[Accessed 5th December 2019]
30	Cloudflare.com	[2019]	Cloudflare Global Anycast Network	https://www.cloudflare.com/network/	[Accessed 5th December 2019]
31	Cliudflare.com	[2019]	DNSSEC Protection	https://www.cloudflare.com/dns/dnssec/	[Accessed 5th December 2019]
32	Cloudflare.com	[2019]	Cloudflare Load Balancing	https://www.cloudflare.com/load-balancing/	[Accessed 5th December 2019]

33	Cloudflare.com	[2019]	What is a CDN?	https://www.cloudflare.com/learning/cdn/what-is-a-cdn/	[Accessed 5th December 2019]
34	Taaffe, Jonathon	[2019]	Table 8. Cloudflare.com Configuration		[Created 5th December 2019]
35	Amazon Web Services	[2019]	AWS Virtual Private Cloud (VPC)	https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html	[Accessed 5th December 2019]
36	Amazon Web Services	[2019]	AWS Regions, Availability Zones, and Local Zones	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html	[Accessed 5th December 2019]
37	Amazon Web Services	[2019]	AWS Application Load Balancer	https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html	[Accessed 5th December 2019]
38	Amazon Web Services	[2019]	AWS Relational Database Service	https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html	[Accessed 5th December 2019]
39	Amazon Web Services	[2019]	AWS Security Groups	https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html	[Accessed 5th December 2019]
40	Amazon Web Services	[2019]	AWS Virtual Machine Images	https://aws.amazon.com/ec2/instance-types/	[Accessed 5th December 2019]
41	Amazon Web Services	[2019]	AWS Machine Image	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html	[Accessed 5th December 2019]
42	Amazon Web Services	[2019]	AWS Auto Scaling Group	https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html	[Accessed 5th December 2019]
43	Amazon Web Services	[2019]	AWS Elastic Load Balancing	https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html	[Accessed 5th December 2019]
44	Amazon Web Services	[2019]	AWS Burstable Performance Instances	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html	[Accessed 5th December 2019]
45	Amazon Web Services	[2019]	AWS Certificate Manager (ACM)	https://aws.amazon.com/certificate-manager/	[Accessed 5th December 2019]
46	Amazon Web Services	[2019]	AWS Shield	https://aws.amazon.com/shield/	[Accessed 5th December 2019]
47	Amazon Web Services	[2019]	AWS Key Management Services	https://docs.aws.amazon.com/kms/latest/developerguide/overview.html	[Accessed 5th December 2019]
48	Amazon Web Services	[2019]	AWS Elastic Block Storage	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html	[Accessed 5th December 2019]
49	Amazon Web Services	[2019]	AWS Key Management Services	https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html	[Accessed 5th December 2019]
50	Taaffe, Jonathon	[2019]	Table 6. Solution Functional Requirements Architectural Components		[Created 5th December 2019]
51	AWS.Amazon.com	[2019]	IAM Best Practices	https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html	[Accessed 5th December 2019]
52	Amazon.com	[2019]	What is Amazon VPC?	https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html	[Accessed 5th December 2019]
53	Taaffe, Jonathon	[2019]	Table 10. AWS VPC Naming Conventions		[Created 5th December 2019]
54	Taaffe, Jonathon	[2019]	Table 11. Naming Conventions Examples		[Created 5th December 2019]
55	Taaffe, Jonathon	[2019]	Diagram 1. AWS VPC Architectural Diagram		[Created 5th December 2019]
56	Taaffe, Jonathon	[2019]	Table 12. VPC Configuration		[Created 5th December 2019]
57	Taaffe, Jonathon	[2019]	Image 1. Elastic IP Allocation		[Created 5th December 2019]
58	Taaffe, Jonathon	[2019]	Image 2. Select VPN Configuration		[Created 5th December 2019]
59	Taaffe, Jonathon	[2019]	Table 13. VPC CIDR Block Configuration		[Created 5th December 2019]
60	Taaffe, Jonathon	[2019]	Table 14. VPC Public and Private Subnets Configuration		[Created 5th December 2019]
61	Taaffe, Jonathon	[2019]	Image 3. Non-Default VPC Configuration		[Created 5th December 2019]
62	Taaffe, Jonathon	[2019]	Image 4. Non-Default VPC Configuration		[Created 5th December 2019]
63	Taaffe, Jonathon	[2019]	Image 5. NAT Gateway Configuration		[Created 5th December 2019]
64	Taaffe, Jonathon	[2019]	Table 15. Additional eu-west-1b VPC Public and Private Subnets		[Created 19th December 2019]
65	Taaffe, Jonathon	[2019]	Table 16. Additional eu-west-1c VPC Public and Private Subnets		[Created 5th December 2019]
66	Taaffe, Jonathon	[2019]	Image 6. Available VPC Public and Private Subnets		[Created 5th December 2019]
67	Taaffe, Jonathon	[2019]	Image 7. Private Route Table Subnet Association		[Created 5th December 2019]
68	Taaffe, Jonathon	[2019]	Image 8. Public Route Table Subnet Association		[Created 5th December 2019]

69	Taaffe, Jonathon	[2019]	Diagram 1. High-Level Security Group (SG) Mesh Configuration		[Created 5th December 2019]
70	Taaffe, Jonathon	[2019]	Table 17. Security Group Naming Convention		[Created 5th December 2019]
71	Taaffe, Jonathon	[2019]	Table 18. Additional Bastion Host Security Groups		[Created 5th December 2019]
72	Taaffe, Jonathon	[2019]	Table 19. Additional Web Server Security Groups		[Created 5th December 2019]
73	Taaffe, Jonathon	[2019]	Table 20. Additional RDS Security Groups		[Created 5th December 2019]
74	Taaffe, Jonathon	[2019]	Image 9. Security Group Summary Configuration		[Created 5th December 2019]
75	Taaffe, Jonathon	[2019]	Table 21. Bastion Host Inbound Security Group Rule		[Created 5th December 2019]
76	Taaffe, Jonathon	[2019]	Image 10. Bastion Host Inbound Rule Configuration		[Created 5th December 2019]
77	Taaffe, Jonathon	[2019]	Table 22. Bastion Host Outbound Security Group Rules		[Created 5th December 2019]
78	Taaffe, Jonathon	[2019]	Image 11. Bastion Host Outbound Rules Configuration		[Created 5th December 2019]
79	Taaffe, Jonathon	[2019]	Table 23. Web Server Inbound Security Group Rules		[Created 5th December 2019]
80	Taaffe, Jonathon	[2019]	Image 12. Web Server Inbound Rule Configuration		[Created 5th December 2019]
81	Taaffe, Jonathon	[2019]	Table 24. Web Server Outbound Security Group Rules		[Created 5th December 2019]
82	Taaffe, Jonathon	[2019]	Image 13. Web Server Outbound Rule Configuration		[Created 5th December 2019]
83	Taaffe, Jonathon	[2019]	Table 25. RDS Inbound Security Group Rules		[Created 5th December 2019]
84	Taaffe, Jonathon	[2019]	Image 14. RDS Inbound Rules Configuration		[Created 5th December 2019]
85	Taaffe, Jonathon	[2019]	Table 26. RDS Outbound Security Group Rules		[Created 5th December 2019]
86	Taaffe, Jonathon	[2019]	Image 15. RDS Outbound Rules Configuration		[Created 5th December 2019]
87	Taaffe, Jonathon	[2019]	Table 27. ALB Inbound Security Group Rules		[Created 5th December 2019]
88	Taaffe, Jonathon	[2019]	Image 16. ALB Inbound Rules Configuration		[Created 5th December 2019]
89	Taaffe, Jonathon	[2019]	Table 28. ALB Outbound Security Group Rules		[Created 5th December 2019]
90	Taaffe, Jonathon	[2019]	Image 17. ALB Outbound Rules Configuration		[Created 5th December 2019]
91	WS.Amazon.com	[2019]	Amazon EC2	https://aws.amazon.com/ec2/	[Accessed 5th December 2019]
92	Taaffe, Jonathon	[2019]	Image 18. Step 1: Choose Amazon Machine Image		[Created 5th December 2019]
93	Taaffe, Jonathon	[2019]	Image 19. Step 2: Choose Instance Type		[Created 5th December 2019]
94	Taaffe, Jonathon	[2019]	Image 20. Step 3: Configure Instance Details		[Created 5th December 2019]
95	Taaffe, Jonathon	[2019]	Image 21. Step 4: Add Storage		[Created 5th December 2019]
96	Taaffe, Jonathon	[2019]	Image 22. Step 5: Add Tags		[Created 5th December 2019]
97	Taaffe, Jonathon	[2019]	Image 23. Step 6: Configure Security Group		[Created 5th December 2019]
98	Taaffe, Jonathon	[2019]	Image 24. Step 7: Review Instance Launch		[Created 5th December 2019]
99	Taaffe, Jonathon	[2019]	Image 35. Select Existing Key Pair or Created new Key Pair		[Created 5th December 2019]
100	PuTTY	[2019]	PuTTY: a free SSH and Telnet client	http://www.chiark.greenend.org.uk/~sgtatham/putty/	[Accessed 5th December 2019]
101	PuTTY	[2019]	8.2 Using PuTTYgen, the PuTTY key generator	https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter8.html#pubkey-puttygen	[Accessed 5th December 2019]
102	Amazon Web Services	[2019]	AWS Connect to Your Linux Instance	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html	[Accessed 5th December 2019]
103	Taaffe, Jonathon	[2019]	Image 36. Step 1: Choose Amazon Machine Image		[Created 5th December 2019]
104	Taaffe, Jonathon	[2019]	Image 37. Step 2: Choose Instance Type		[Created 5th December 2019]
105	Taaffe, Jonathon	[2019]	Image 38. Step 3: Configure Instance Details		[Created 5th December 2019]
106	Taaffe, Jonathon	[2019]	Image 39. Step 4: Add Storage		[Created 5th December 2019]
107	Taaffe, Jonathon	[2019]	Image 40. Step 5: Add Tags		[Created 5th December 2019]
108	Taaffe, Jonathon	[2019]	Image 41. Step 6: Configure Security Group		[Created 5th December 2019]
109	Taaffe, Jonathon	[2019]	Image 42. Step 7: Review Instance Launch		[Created 5th December 2019]

110	Taaffe, Jonathon	[2019]	Image 43. Select Existing Key Pair or Created new Key Pair		[Created 5th December 2019][
111	PuTTY	[2019]	9.4 Using agent forwarding	https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter9.html#pageant-forward	[Accessed 5th December 2019]
112	PuTTY	[2019]	PuTTY: a free SSH and Telnet client	http://www.chiark.greenend.org.uk/~sgtatham/putty/	[Accessed 5th December 2019]
113	PuTTY	[2019]	8.2 Using PuTTYgen, the PuTTY key generator	https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter8.html#pubkey-puttygen	[Accessed 5th December 2019]
114	PuTTY	[2019]	9.4 Using agent forwarding	https://the.earth.li/~sgtatham/putty/0.73/htmldoc/Chapter9.html#pageant-forward	[Accessed 5th December 2019]
115	Amazon Web Services	[2019]	AWS Relational Database Service	https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html	[Accessed 5th December 2019]
116	LinuxConfig.org	[2019]	Install MySQL client on Ubuntu	https://linuxconfig.org/install-mysql-on-ubuntu-18-04-bionic-beaver-linux#h6-1-install-mysql-client-on-ubuntu	[Accessed 5th December 2019]
117	Wordpress.org	[2019]	Creating Database for WordPress - Using the MySQL Client	https://wordpress.org/support/article/creating-database-for-wordpress/#using-the-mysql-client	[Accessed 5th December 2019]
118	Ubuntu18.com	[2019]	How to Install Apache on Ubuntu 18.04 Server	https://www.ubuntu18.com/install-apache-ubuntu-18/	[Accessed 5th December 2019]
119	LetsEncrypt.org	[2019]	Let's Encrypt	https://letsencrypt.org/	[Accessed 5th December 2019]
120	CertBot.eff.org	[2019]	CertBot	https://certbot.eff.org/	[Accessed 5th December 2019]
121	CertBot.eff.org	[2019]	certbot instructions: Apache on Ubuntu 18.04 LTS	https://certbot.eff.org/lets-encrypt/ubuntubionic-apache	[Accessed 5th December 2019]
122	Wordpress.org	[2019]	How to install WordPress	https://wordpress.org/support/article/how-to-install-wordpress/	[Accessed 5th December 2019]
123	Wordpress.org	[2019]	Wordpress Keys and Salts Generator	https://api.wordpress.org/secret-key/1.1/salt/	[Accessed 5th December 2019]
124	SSLforFree.com	[2019]	SSL For Free	https://www.sslforfree.com/	[Accessed 5th December 2019]
125	Amazon Web Services	[2019]	AWS Machine Image	https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html	[Accessed 5th December 2019]
126	Amazon Web Services	[2019]	AWS Auto Scaling Group	https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html	[Accessed 5th December 2019]
127	Amazon Web Services	[2019]	AWS Elastic Load Balancing	https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html	[Accessed 5th December 2019]
128	Taaffe, Jonathon	[2019]	Table 26. Elastic Application Load Balancing Prerequisites		[Created 5th December 2019]
129	Taaffe, Jonathon	[2019]	Table 27. Configure Load Balancer		[Created 5th December 2019]
130	Taaffe, Jonathon	[2019]	Table 28. Wordpress Blog Install Options		[Created 5th December 2019]
131	Taaffe, Jonathon	[2019]	Table 29. Securing Wordpress – Additional Configuration Items		[Created 5th December 2019]
132	Wordpress.org	[2019]	All In One WP Security	https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/	[Accessed 5th December 2019]
133	Taaffe, Jonathon	[2019]	Table 30. All In One WP Security Configuration		[Created 5th December 2019]
134	Taaffe, Jonathon	[2019]	Table 31. All In One WP Security File System Security		[Created 5th December 2019]
135	Wordpress.org	[2019]	Shield Security: Protection with Smarter Automation	https://wordpress.org/plugins/wp-simple-firewall/	[Accessed 5th December 2019]
136	Taaffe, Jonathon	[2019]	Table 32. ShieldSecurity Enabled Security Configuration		[Created 5th December 2019]
137	Wordpress.org	[2019]	Stop User Enumeration	https://wordpress.org/plugins/stop-user-enumeration/	[Accessed 5th December 2019]
138	Wordpress.org	[2019]	Cloudflare Wordpress Plugin	https://wordpress.org/plugins/cloudflare/	[Accessed 5th December 2019]
139	Wordpress.org	[2019]	WP Force SSL	https://wordpress.org/plugins/wp-force-ssl/	[Accessed 5th December 2019]
140	Taaffe, Jonathon	[2019]	Table 33. AWS Config Rule Configuration - Part 1		[Created 5th December 2019]
141	Taaffe, Jonathon	[2019]	Table 34. AWS Config Rule Configuration – Part 2		[Created 5th December 2019]
142	Taaffe, Jonathon	[2019]	Table 34. AWS Config Rule Configuration – Part 3		[Created 5th December 2019]