

# Troll World Cloud Migration

---

## Design Plan

## Contents

<b>Executive Summary .....</b>	<b>3</b>
1. Application Overview.....	3
2. Current Architecture Overview .....	3
1.1. Risks in Current Architecture.....	3
3. Scope Statement.....	4
4. Cloud Migration Overview.....	4
1.1. Why AWS? .....	4
5. Proposed Implementation.....	4
<b>Detailed Design Plan .....</b>	<b>7</b>
1. Goals of Design .....	7
1.1. Acceptance Criteria.....	7
2. Proposed Architecture.....	7
1.1. Network Zone .....	8
1.2. AWS Server Zone .....	11
1.3. AWS IT Utility Services .....	14
1.4. Credit Card Payment Process .....	16
1.5. Troll World Internal Operations Zone .....	17
1.6. Troll World Internal Server Zone .....	17
3. User Classification and IAM .....	18
<b>Implementation Roadmap .....</b>	<b>22</b>

# Executive Summary

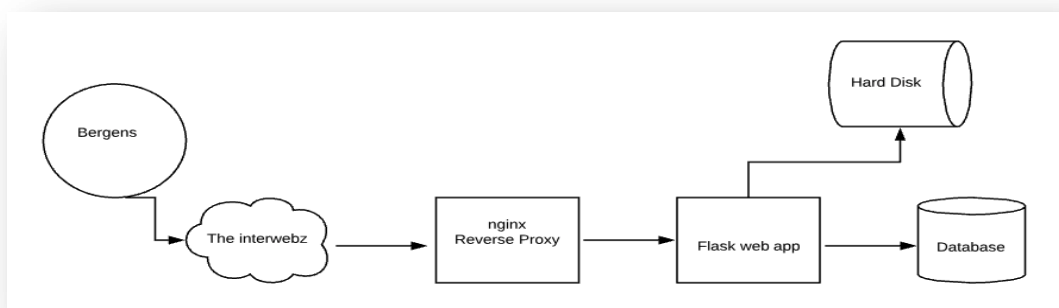
## 1. Application Overview

The Trolls are small creatures who live in an almost perpetual state of happiness, singing, dancing and hugging all day long. After many years of conflict, the Bergens and Trolls are now friends. Bergens now have Trollmania and are interested in everything Troll-related. Bergens are now the largest customers of Troll videos.

ENPM809J Troll World is a website launched by the Trolls, which hosts Troll videos to serve the demands of their customers. This website hosts Troll videos on demand to Bergen customers all around the world.

## 2. Current Architecture Overview

Currently the ENPM809J Troll World website runs in a straightforward architecture, as below.



The features of the current system includes the below,

- Single Linux system
- Code written in Python3 and Flask
- Reverse proxy using Nginx
- Videos stored in hard disks
- MySQL databases used to store queries

### 1.1. Risks in Current Architecture

Many risks exist in the current simplistic architecture, which include the below,

- No patching or backup strategy
- No access management
- Vulnerable to DDoS attacks and compromise attempts by The Chef
- Susceptible to hardware failures and troll errors
- Slow downloads and order processing

### 3. Scope Statement

This document is to provide a technical implementation overview and plan, to migrate the ENPM809J Troll World website from its current architecture to the Cloud. This includes proposing a new architecture to host the ENPM809J Troll World website on AWS cloud and a new architecture to setup the Troll World intranet for internal operations and Troll World development activities.

### 4. Cloud Migration Overview

The ENPM809J Troll World will be hosted from the AWS cloud environment. The IT environment of ENPM809J Troll World will be redesigned to adapt to this migration. The new architecture will split the Troll World IT environment into the cloud-based web hosting environment and a Trolls intranet for development and maintenance activities.

The advantages of migrating to the cloud environment include,

- Maintenance cost will be reduced
- High availability of ENPM809J Troll World website
- Scalability and Elasticity of Cloud resources
- Easy Load Balancing
- Protection from DDoS and common web exploits
- Secure application
- Controlled user access to application components
- Automated deployment and patching
- Enhanced application monitoring and backup mechanism
- Pay as you go features

#### 1.1. Why AWS?

At present, AWS is the leading player in the cloud providers market. Due to their early start, they have gained a higher amount of experience in providing reliable cloud services. Many services provided by AWS integrate seamlessly with on-premise applications. AWS services are API based, and can be configured and scaled easily. AWS also provides robust infrastructure and protection from infrastructure level attacks. AWS also provides security related services such as Web Application Firewall and Shield, which could be configured to protect the Troll World website.

Overall, AWS provides all the services and the required infrastructure to host and maintain the Troll World website. It also provides simple solutions to connect it to the Troll World intranet and to Credit Card payment vendor gateways.

### 5. Proposed Implementation

The ENPM809J Troll World website will be migrated to the AWS cloud and an internal IT environment will be set up to perform the internal operations of the Troll World website. Both the Cloud Environment and the



Internal IT Environment will serve specific purposes and could be accessed by designated users.

The operations that will occur on the Cloud Environment will include,

- EC2 instances will serve as the production environment where ENPM809J Troll World will be hosted
- Autoscaling will be implemented on the EC2 instances to adjust the resources based on request traffic
- DNS service will be provided via Route 53; this will be the entry point when Bergens access the website
- Application will be protected from common web attacks using Web Application Firewall (WAF) and Shield
- Elastic Load Balancing will be implemented to improve application stability
- Elastic Block Storage will be used to store customer and application data
- S3 buckets will be used to store static application content
- EC2 instances and EBS instances will be hosted from 2 different availability zones to avoid sudden application down times
- Credit card processing API will be implemented to connect the Troll World web application to Credit Card vendor gateways
- IAM will be implemented with Multifactor Authentication to provide internal users access to the AWS resources
- Cloud Watch will be implemented to monitor the services that are being used on AWS
- Storage Gateway will be used to periodically backup the application to the Troll World intranet
- Code Deploy will be used to deploy patches from the internal Troll World Internal Server Zone to the AWS based production environment

Operations that will occur in the Troll World intranet would include,

- Internal Server Zone will be implemented to provide development, testing and integration environments
- CA server will be implemented that will store the relevant keys of the users and will act as the internal certifying agent
- LDAP server will be implemented to provide core authentication and authorization services to the Troll World intranet users
- DevOps server will be implemented for automatic patching for the Troll World web application, using the Continuous Integration/Continuous Deployment (CA/CD) methodology
- Internal Data Center will store the application logs and backups that are generated by the AWS Cloud

#### Watch and the AWS Storage Gateway

- Security and Service monitoring will process the log data from all the AWS services used to monitor application health and to detect any unnatural behaviour; Splunk could be used as a monitoring tool

# Detailed Design Plan

## 1. Goals of Design

To redesign the ENPM809J Troll World IT environment which includes the below,

- Troll World website hosted on AWS cloud platform
- Layer separation for various internal and external components
- Access management and control
- Higher application availability and stability
- Patching and backup

### 1.1. Acceptance Criteria

**AC1 :** AWS Troll World should be hosted on AWS, in different availability zones

**AC2 :** Load Balancer should be implemented to improve stability and availability of the application

**AC3 :** IAM should be implemented to manage internal user access to application resources

**AC4 :** Web Application Firewall and request redirecting should be implemented to avoid unauthorised access to application resources

**AC5 :** Credit card processing API should be implemented and integrated with the application

## 2. Proposed Architecture

The ENPM809J Troll World IT environment will be split into the Cloud environment and the Troll World Intranet.

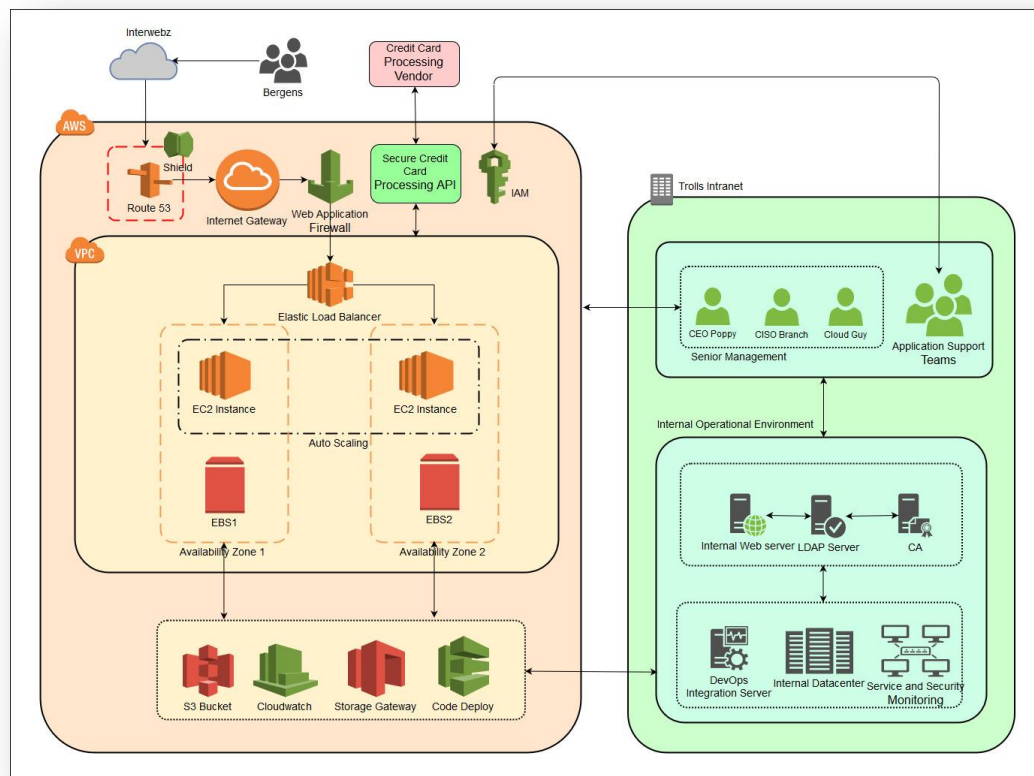
The Cloud Environment will host the Troll World website on the AWS cloud. Customers will access the application through Route53 and Web Application Firewall will be implemented to control customer access.

The AWS infrastructure components will include

- Network Zone
- Server Zone
- AWS IT Utility Services
- Credit Card Payment Process
- Identity and Access Management

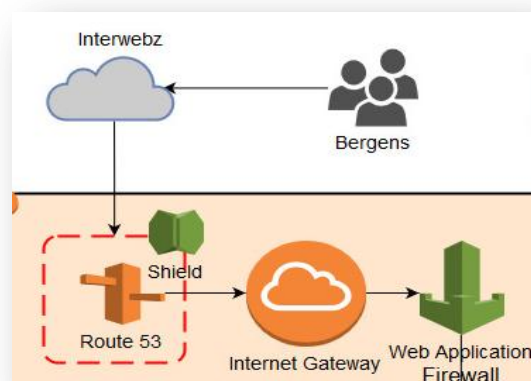
The Troll World intranet would include the Internal Operational zone and the Internal Server zone. These would be used by Troll World employees to develop, monitor, patch and backup ENPM809J Troll World to the Troll World intranet.





### 1.1. Network Zone

The Network Zone will constitute of all the components required to help the Bergens access the ENPM809J Troll World website.



The Bergens will enter the Website via the Interwebz. They will enter the application via Route 53, where Shield will be implemented. Their requests will then be redirected to the Internet Gateway, from where they will reach the Web Application Firewall.

Those requests that pass through the firewall will be able to access the ENPM809J Troll World website.

#### 1.1.1. Route 53

Route 53 is a cloud based Domain Name Service (DNS) that is provided by AWS. It is highly scalable and



available. The existing ENPM809J Troll World domain could be transferred to the AWS Route 53 from the below screens. This will then serve as the entry point for Bergens, who will access the website from the Interwebz.

Route 53 Management Console X

https://console.aws.amazon.com/route53/home#DomainTransfer:

aws Services Resource Groups

1: Select Domain

2: Domain Options

3: Contact Details

4: Review & Purchase

### Transfer Domain to Route 53

You can transfer registration for one or more domains from another registrar to Route 53. Before you continue, do the following:

- Confirm that the domain is transferable. See [Transfer requirements for top-level domains](#).
- For each domain that you want to transfer, perform the first four steps of [Transferring registration for a domain to Route 53](#).

To transfer up to five domains, you can enter each domain name below.  
To transfer more than five domains, you can use the [Transfer multiple domains to Route 53 page](#).

enpm809jtrollworld .com - \$12.00 Check

You can transfer registration for a domain from another registrar to Route 53. [Learn more](#)

Cancel Continue

Shopping cart

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Once registered, the required inbound and outbound endpoints could be specified for requests to this domain from the below screen. This will be used to make sure that the Bergens only access the hosted website and that they do not have access to other AWS resources.

Route 53 Resolver Console X

https://console.aws.amazon.com/route53resolver/home?region=us-east-1#/vpc/vpc-a9da72d3

aws Services Resource Groups

Route 53

Dashboard

Hosted zones

Health checks

Traffic flow

Traffic policies

Policy records

Domains

Registered domains

Pending requests

Resolver

VPCs

Inbound endpoints

Outbound endpoints

Rules

### Outbound endpoints (0)

Edit Delete

Search

ID	Name	Status	IP addresses
----	------	--------	--------------

Empty resources

No resources to display

Create outbound endpoint

### Inbound endpoints (0)

Edit Delete

Search

ID	Name	Status	IP addresses
----	------	--------	--------------

Empty resources

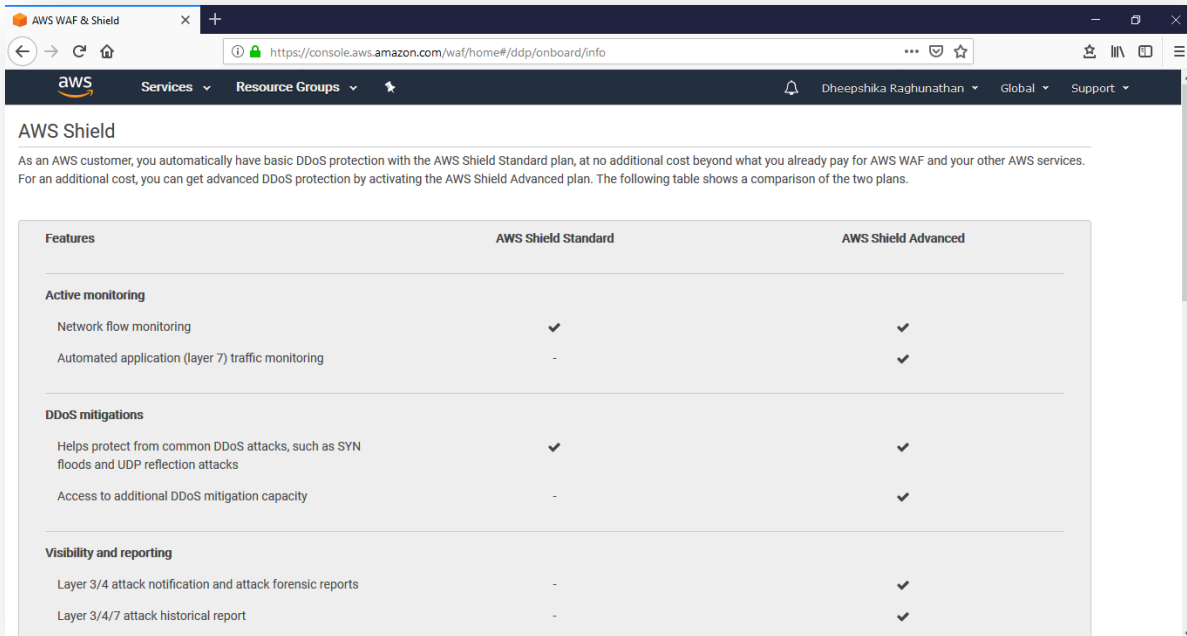
No resources to display

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

### 1.1.2. *AWS Shield*

AWS Shield provides DDoS protection for the applications that use the AWS Web Application Firewall (WAF). The standard level of Shield is automatically activated for all applications that use the WAF. This provides basic DDoS mitigation and monitoring.



The screenshot shows the AWS WAF & Shield console. It includes a header with the AWS logo, navigation tabs for Services and Resource Groups, and a user profile for Dheepshika Raghunathan. The main content area is titled 'AWS Shield' and contains a table comparing the Standard and Advanced plans.

Features	AWS Shield Standard	AWS Shield Advanced
<b>Active monitoring</b>		
Network flow monitoring	✓	✓
Automated application (layer 7) traffic monitoring	-	✓
<b>DDoS mitigations</b>		
Helps protect from common DDoS attacks, such as SYN floods and UDP reflection attacks	✓	✓
Access to additional DDoS mitigation capacity	-	✓
<b>Visibility and reporting</b>		
Layer 3/4 attack notification and attack forensic reports	-	✓
Layer 3/4/7 attack historical report	-	✓

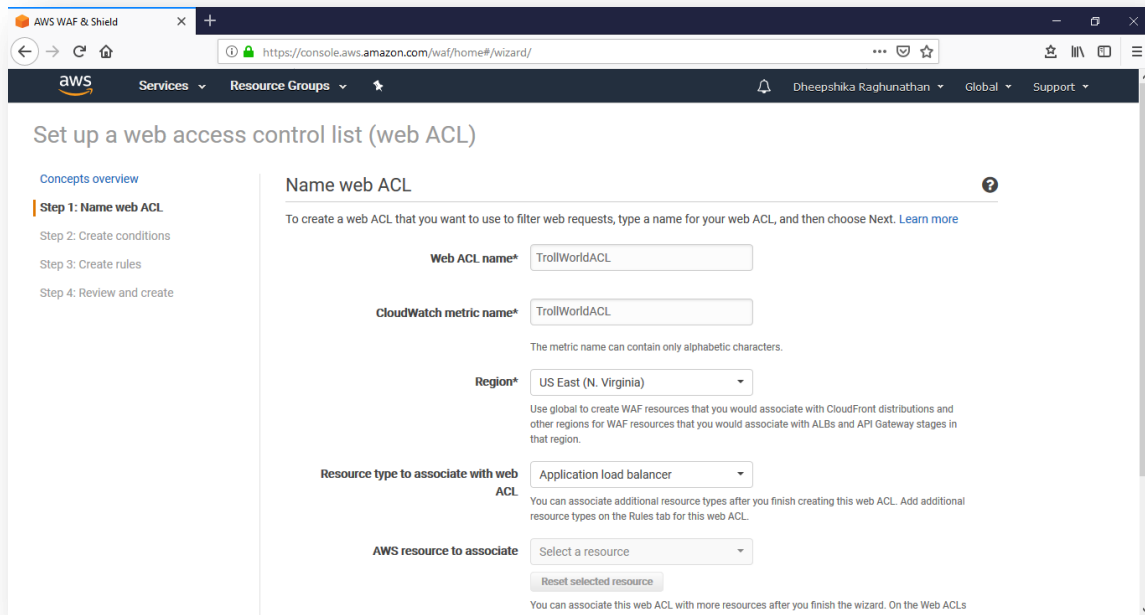
The advanced level of Shield could be activated for a monthly fee.

When used along with Route 53, this would provide protection against all infrastructure attacks.

### 1.1.3. *Web Application Firewall (WAF)*

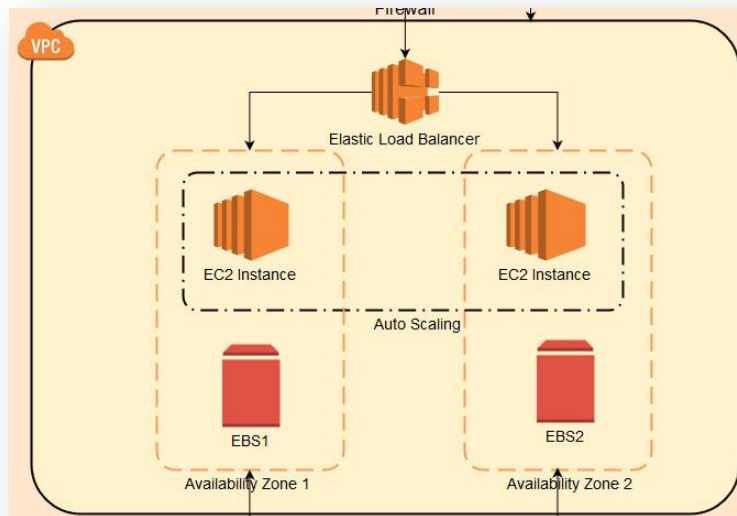
The AWS Web Application Firewall (WAF) lies between the Route 53 and the application VPC. The WAF is a customizable firewall for web applications that are hosted on AWS.

WAF can be used to configure firewall rules to protect the application against common web exploits such as SQL Injection, Cross Site Scripting, etc.



## 1.2. AWS Server Zone

The application servers for ENPM809J Troll World live in this layer.



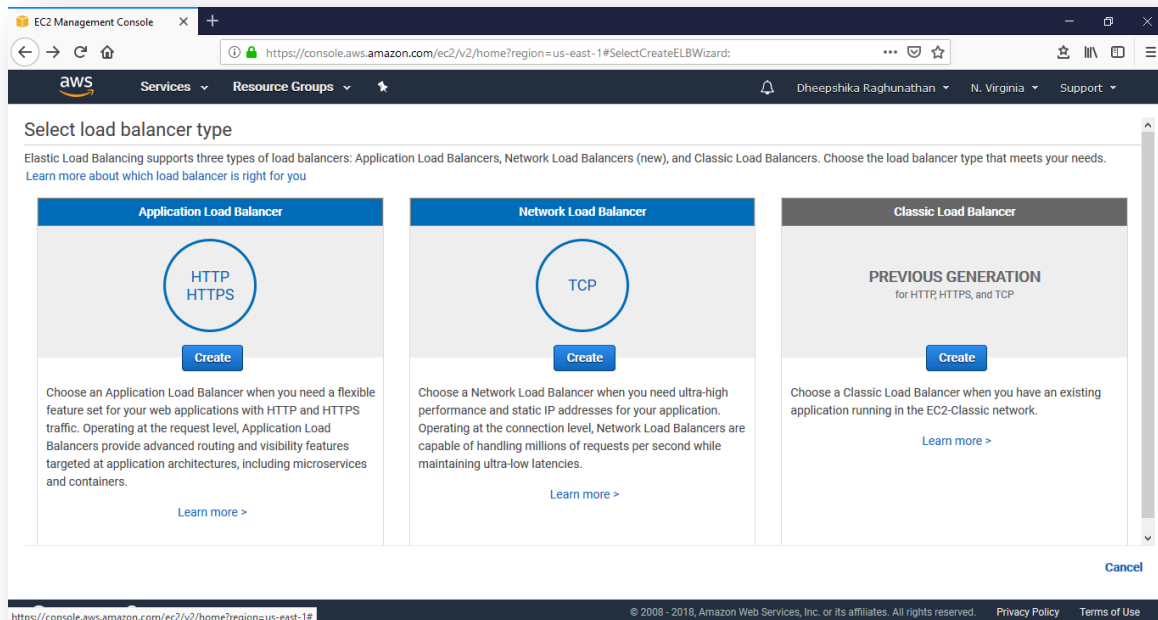
The requests to the Troll World website reach this zone from the Web Application Firewall. These requests are sent to the Elastic Load Balancer. From here the requests are sent to the appropriate EC2 instance.

The ENPM809J Troll World will be hosted on 2 geographically distinct availability zones. Each availability zone will include an EC2 instance to host the website and an Elastic Block Storage instance to store the Bergen's customer details.

Auto-scaling will be implemented on these EC2 instances to improve application performance.

### 1.1.1. Elastic Load Balancer (EBS)

The EBS will be used to automatically distribute the incoming traffic across the EC2 instances in both the availability zones.

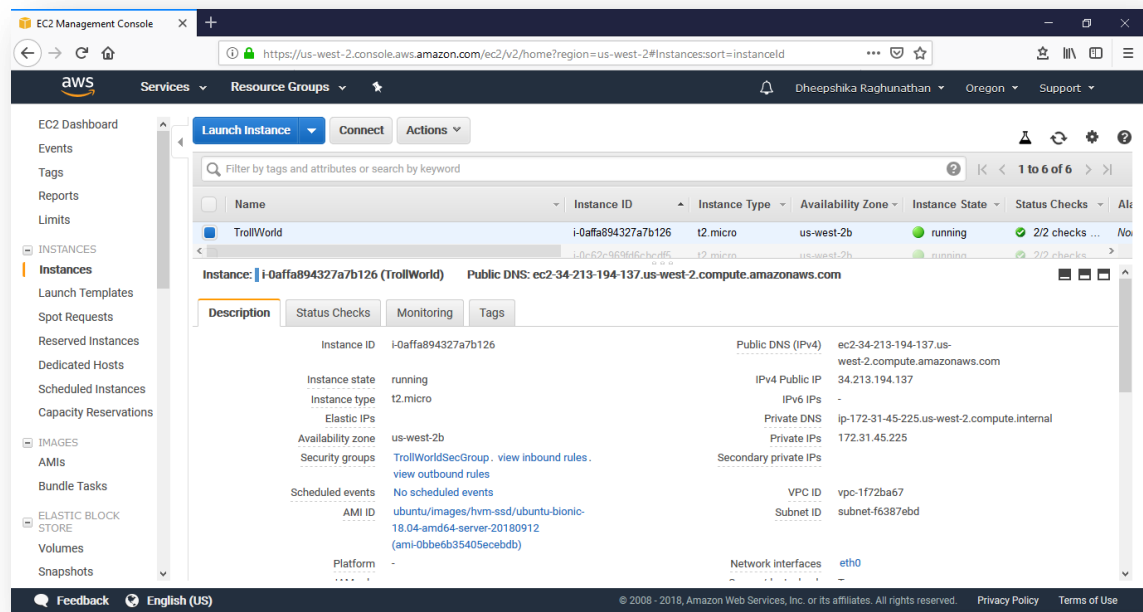


EBS Application load balancer will be used, which will work on the application layer to distribute the incoming HTTP/HTTPS requests, including microservices.

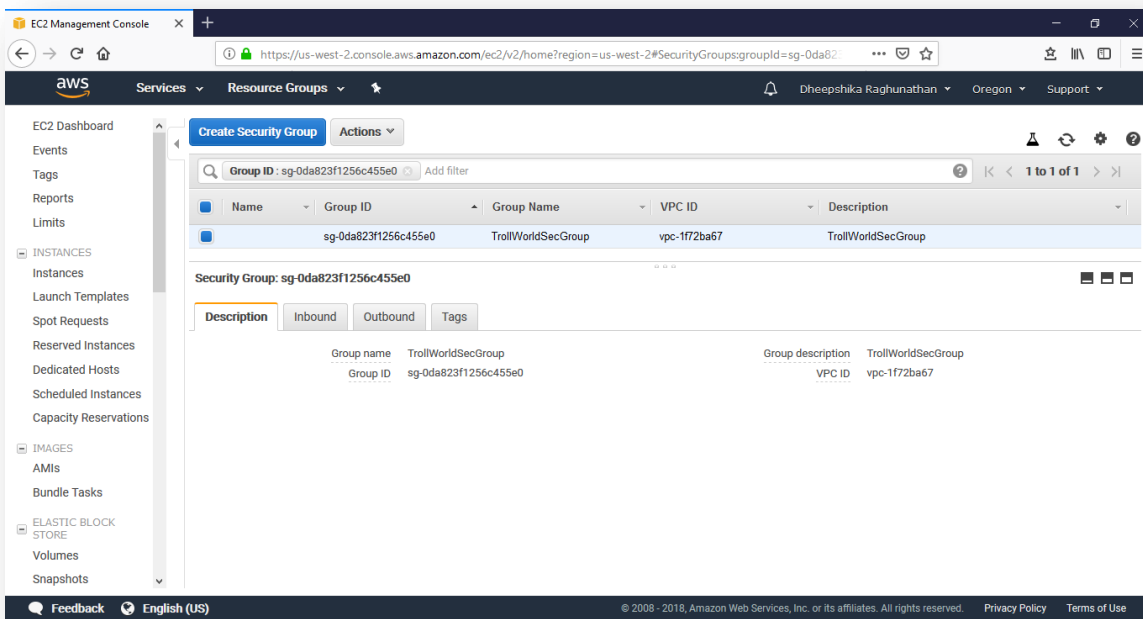
### 1.1.2. EC2

Elastic Compute Cloud (EC2) provides resizable computing capacity on the cloud. EC2 could be used to run server instances for ENPM809J Troll World website.

EC2 instances will be used to host the application on Ubuntu 18 server. Two EC2 instances will be launched in two geographically distinct availability zones. The static content to be used by the EC2 instances could be stored in S3 buckets.



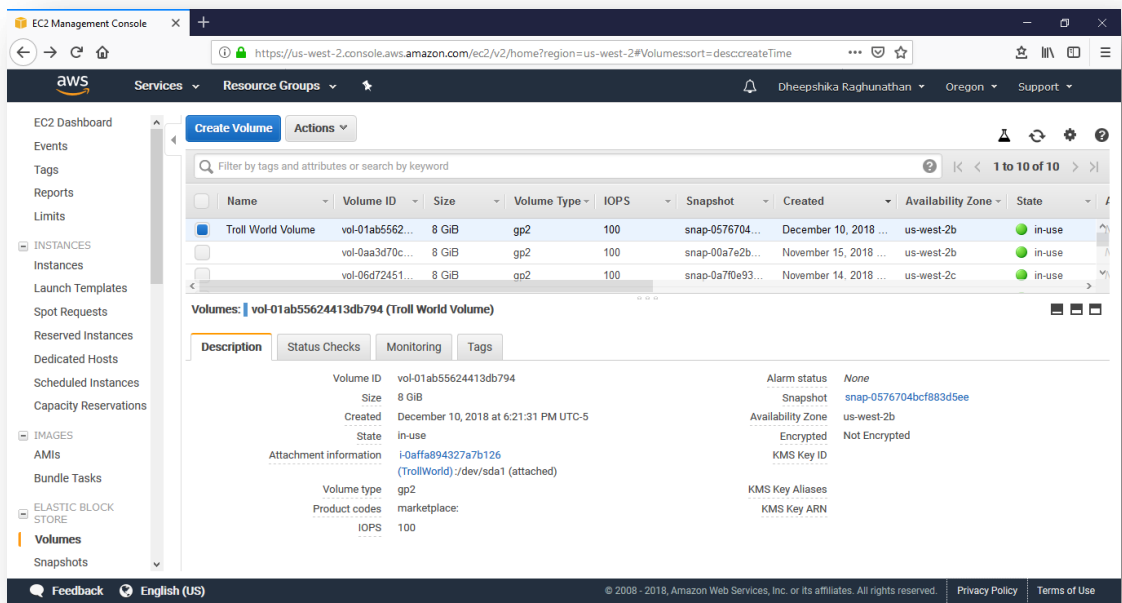
Security Groups could be configured for each EC2 instance to configure the inbound and outbound rules for the server.



**1.1.3. Elastic Block Storage (EBS)**

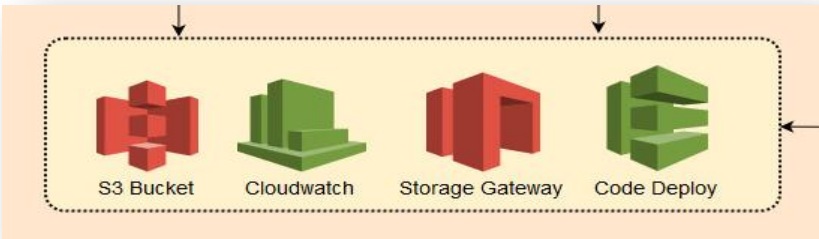
The customer data for ENPM809J Troll World could be stored in the Elastic Block Storage instances. With the growing numbers of the Bergen customers, it is essential for the website to store all customer related information, such as credit card information, address information etc, in an expandable and reliable storage.





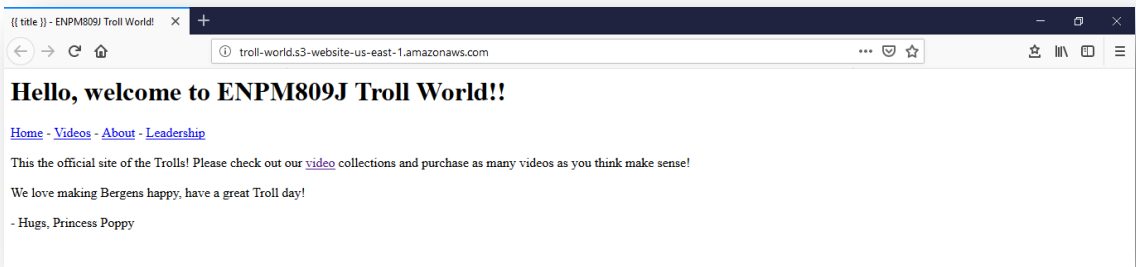
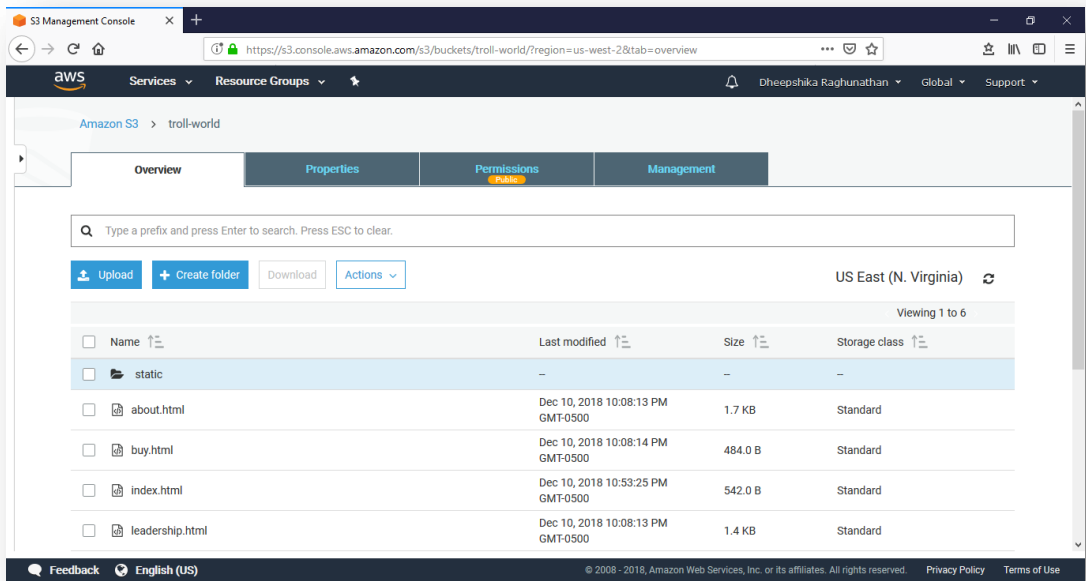
The EBS provides a flexible and persistent block storage service for EC2 instances. The EBS instances are replicated in each availability zone to ensure high data availability.

**1.3. AWS IT Utility Services**  
The AWS IT Utility Services includes all the backend utilities that will be used for the ENPM809J Troll World website. These would include storage, deployment, backup and monitoring services offered by AWS.



**1.1.1. S3 Buckets**  
S3 buckets are highly scalable storage solutions provided by AWS. The S3 bucket will be used to store the static content for the Troll World website. This may include the static HTML pages and videos that are to be shared with the Bergens on demand.



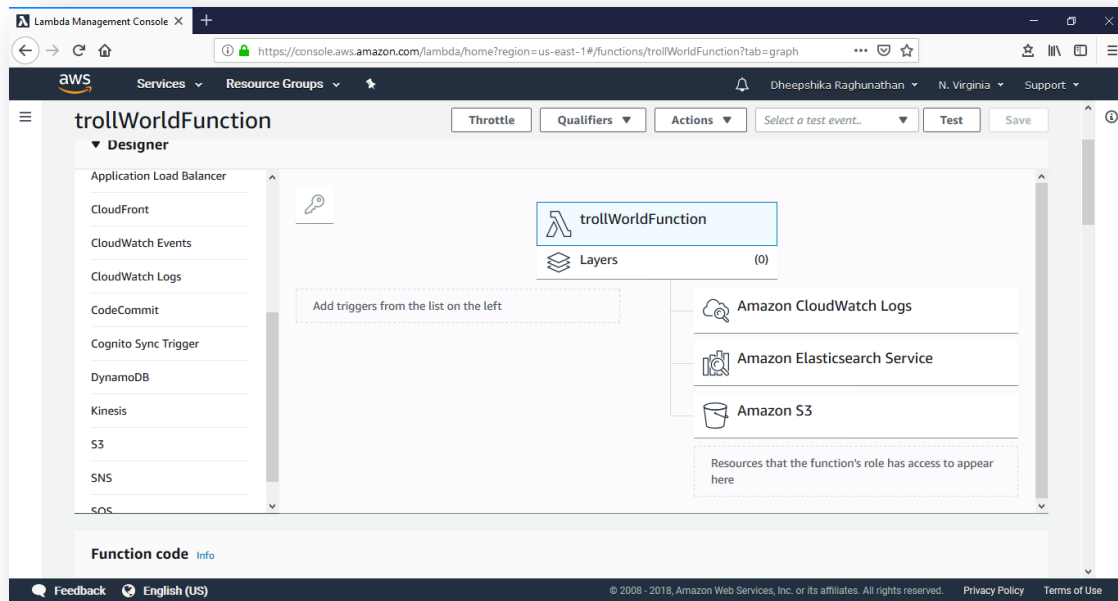


This static content could be used by the ENPM809J Troll World website as needed.

### 1.1.2. CloudWatch

The AWS CloudWatch provides an on demand monitoring service for applications hosted on AWS. This will be used by the Troll World website to collect monitoring and operational data from various AWS services that are being used. This data will be accessed by the Troll World Service and Monitoring from the Troll World intranet. Further processing of the collected data will occur here.





Lambda functions could be used to obtain the CloudWatch logs, which will then be sent to the internal Service Application Server for further processing.

#### 1.1.3. Storage Gateway & Code Deploy

The AWS Storage Gateway provides a storage service that could be used easily by the on-premise applications. This will be used by the Troll World internal application server to backup the Troll World website to the internal application server regularly. The application will be backed up every week periodically and before each deployment. The backups will be retained for a 1 year period, after which they will be purged.

The AWS Code Deploy is a service that enables the on-premise applications to deploy code onto the AWS services that are being used. This will be used to deploy the Troll World application code, configuration changes, and patches from the development environment in the internal application server to the instances running on AWS cloud.

#### 1.4. Credit Card Payment Process

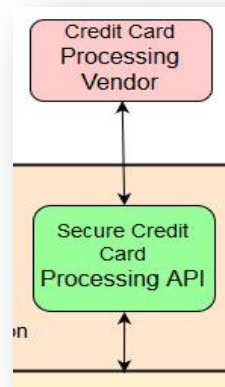
AWS provides various Credit Card payment APIs, which could be explored to be used by the Troll World website. These are secure 3<sup>rd</sup> party APIs that will connect the application to the Credit Card vendor gateways.

While many 3<sup>rd</sup> party APIs are available, a suitable Credit Card payment API would be DevPay, as it satisfies all the requirements of the ENPM809J Troll World application.

##### 1.1.1. DevPay

- Billing and accounting management service
- Runs on top of Amazon web Services
- Provides on demand payment pipelines and automatically meters usage
- Uses, Amazon Payments, AWS's trusted billing infrastructure to process payments

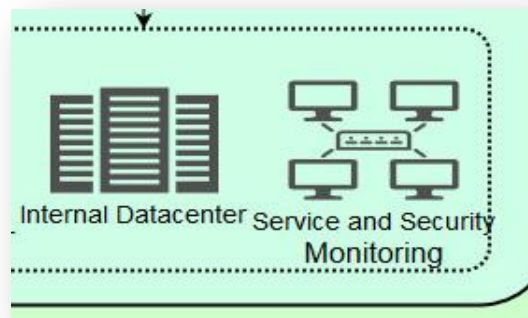




### 1.5. Troll World Internal Operations Zone

The Troll World Internal Data Center will store the backup of the Troll World website, which it will receive periodically from AWS Storage Gateway. The backup data will include the application state, customer information and a copy of all the static content.

The static content will be stored in the database internally. This data center will receive backups of the application state and the Bergen customers periodically every week and before each deployment via the AWS Storage Gateway.



The Service and Security Monitoring unit will be the core management and log server in the Troll World intranet. It will receive application logs from the AWS Cloud Watch. The data sent to this unit will be one way, that is, no AWS service will receive any data from this unit directly.

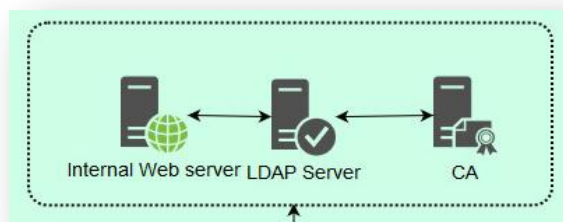
This will be used to monitor the application running on AWS cloud and to detect any unusual behaviour. The data received from AWS Cloud Watch will be in the form of log dump. Splunk instances will be run on this unit to process the log information.

The Service and Monitoring unit will also implement the data retention policies, which will dictate the amount of time that the backup data will be retained in the Internal Data Centers. This unit will also be responsible for running the data purge jobs periodically.

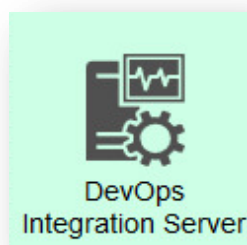
### 1.6. Troll World Internal Server Zone

This zone forms the development and testing environment for the ENPM809J Troll World website. The internal

web server host the application in the development environment.



The LDAP and CA servers will be used to authorise the internal users to the Troll World intranet who will have access to the Troll World intranet resources, such as, the development environment, data centers and the Service and Monitoring unit. The internal users may include Branch, Smidge, Guy Diamond, Biggie, Cooper, etc.

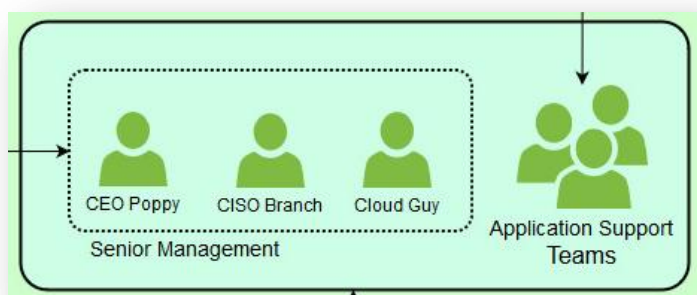


The DevOps server will be implemented internally to drive automatic integration and automation testing of the integrated website. When it is ready, this server will connect with the AWS Code Deploy to deploy the code in the AWS Cloud production environment. This will drive the Continuous Integration/Continuous Deployment concept in the Troll World IT Environment.

### 3. User Classification and IAM

The internal users in the Troll World IT environment will be classified as

- Senior Management
- Application Support Teams



The senior management will consist of

- Princess Poppy, CEO
- Branch, CISO
- Cloud Guy, AWS Admin

These users will have access across the Troll World IT Environment, to both the intranet resources and to the AWS resources.

The Application Support team will include,

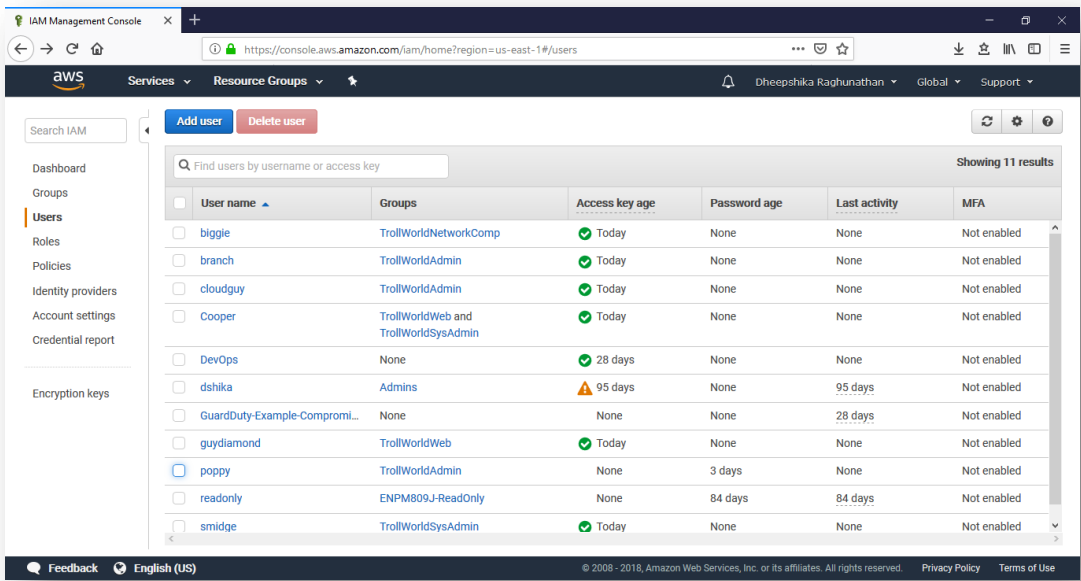
- Smidge, System Administrator
- Guy Diamond, Web Developer
- Biggie, Network Engineer
- Cooper, Web Developer/System Administrator

The Application Support team users will have access to select internal and AWS resources required to perform their duties successfully.

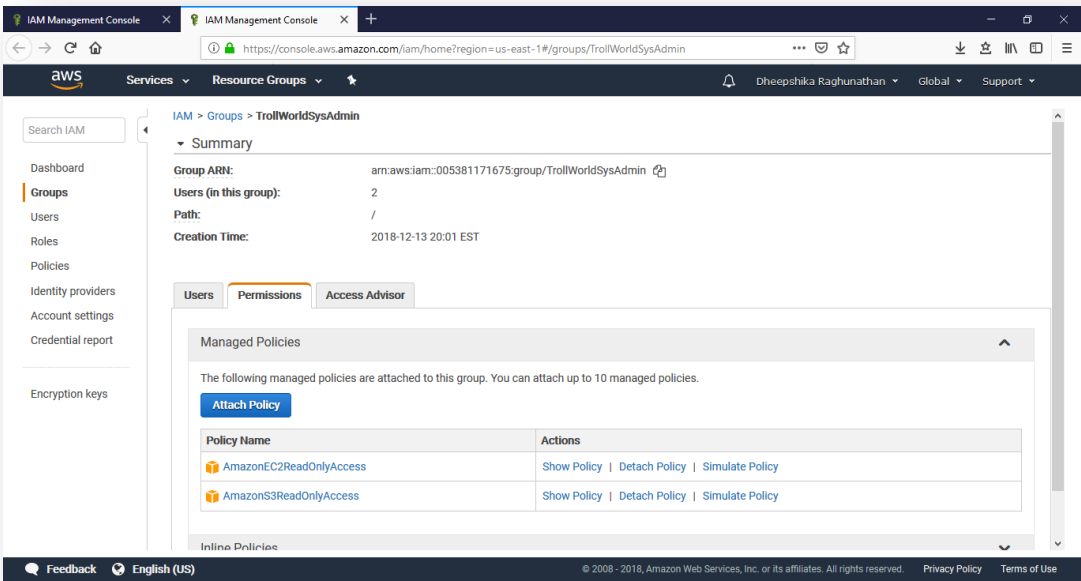
Multifactor Authentication will be implemented for all internal users. AWS Identity and Access Management (IAM) will be used to provide internal users access to various AWS resources.

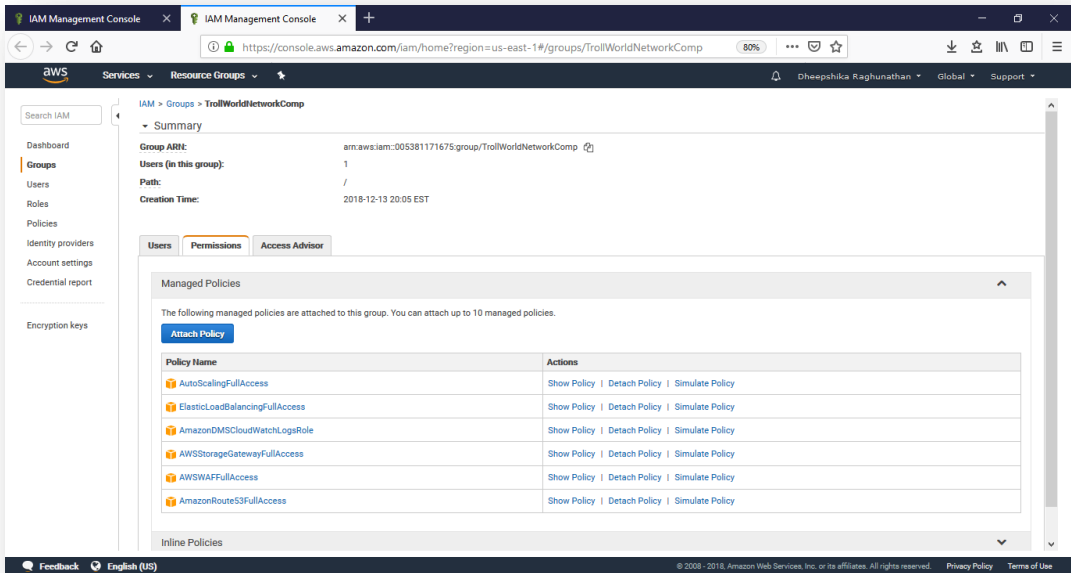
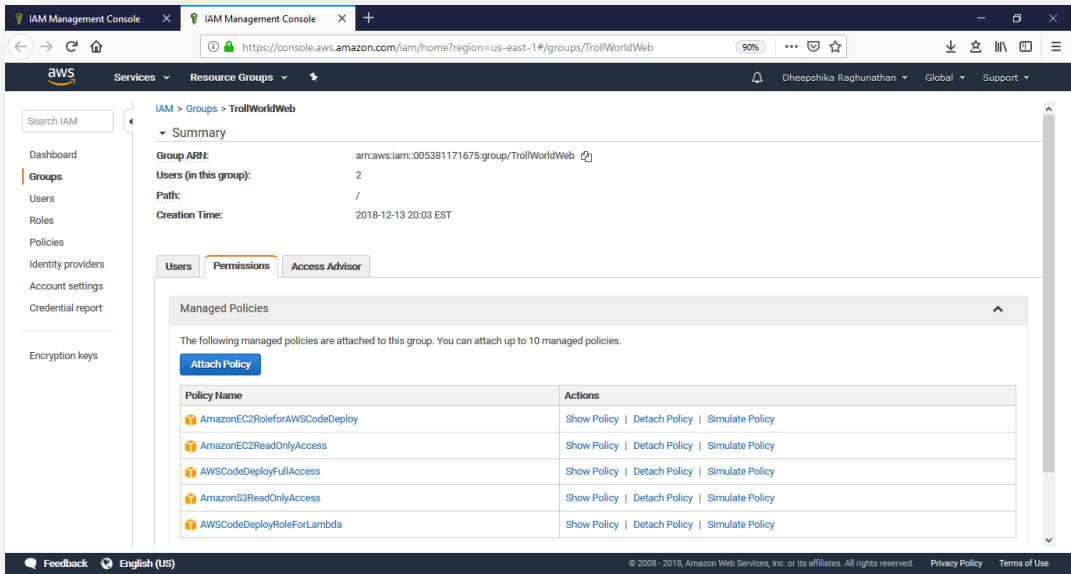
User/Access	System Administration	Web Component	Network Component
<b>Smidge</b>	✓		
<b>Guy Diamond</b>		✓	
<b>Biggie</b>			✓
<b>Cooper</b>	✓	✓	

Various IAM Groups could be created to limit the internal users access to various AWS resources, as required. Each group will be associated with policies that will provide specific access to each AWS resource used.

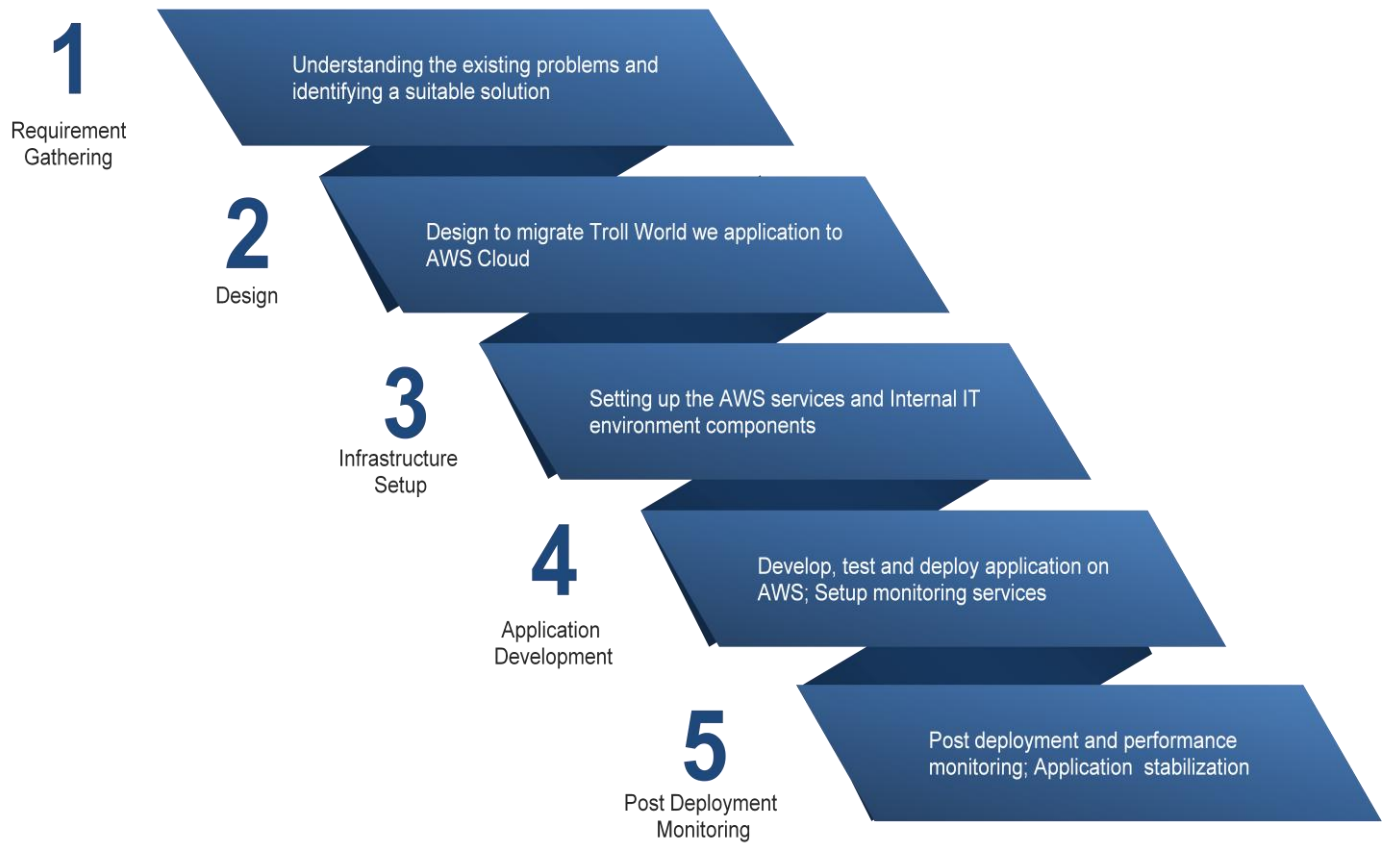


Will those in the Admin group will receive full admin access to all the resources, the other groups' accessed will be limited to their purpose.





# Implementation Roadmap



With the given resources, it might take nearly 6 months to migrate the ENPM809J Troll World website to AWS cloud and to implement the Troll World intranet. After the go-live, post deployment and performance monitoring will be carried out, and fixes will be provided until the application stabilizes.