Automating Single Page App Delivery: The Serverless Way

Serverless Phoenix Meetup - September 2018

@davetownsend

About Me

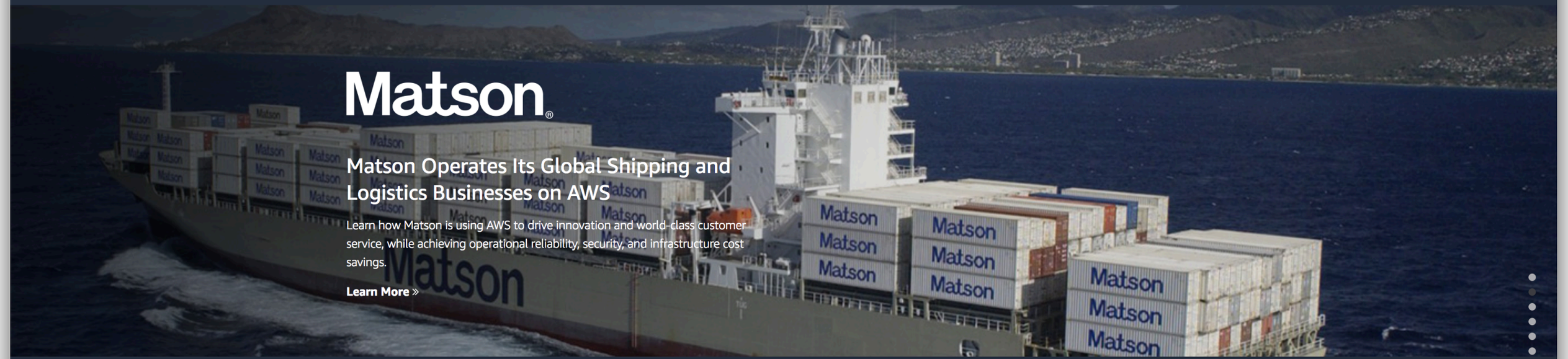
@davetownsend

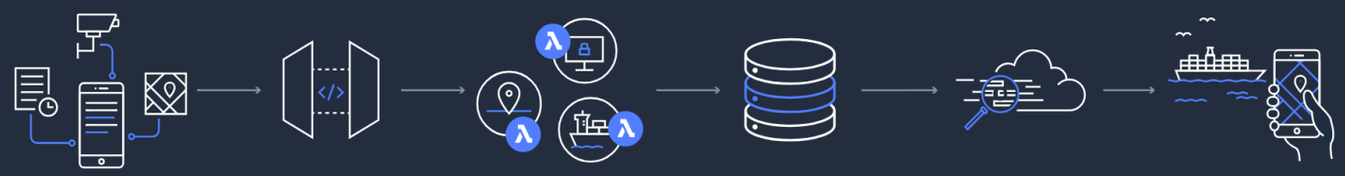
Dave Townsend

Principal Software Engineer

Innovation & Architecture

Matson





Real-Time Container Tracking

Matson built a flagship mobile application for global container tracking that allows customers to perform real-time tracking of their freight shipments. Other valuable features in the application include interactive vessel schedule searching, location-based port map lookups, and live gate-camera feeds.

Mobile Device Access

All mobile devices access AWS via **Amazon API Gateway**. This provides highly available edge located endpoints for access into resources within Matson's existing virtual private clouds.

Serverless Computing

The **AWS Lambda** functions are designed using the microservices pattern and are modeled around specific ocean-based business contexts, such as shipment tracking and vessel schedules.

Database Configuration and Storage

Amazon DynamoDB manages configuration as well as user-feedback configuration and user-feedback notifications sent from mobile devices. DynamoDB Streams provides real-time notifications to Matson's customer service team.

Data Monitoring and Alerts

Matson's customers rely on accurate, up-to-the-minute container tracking and vessel status information. Monitoring and alerting of system events is achieved by using **Amazon CloudWatch**, **Amazon SNS**, **Amazon SES**, **AWS Lambda**, and CloudWatch Logs.

End-to-End Serverless Application

Matson can now offer customers an end-to-end serverless application to help track their shipments, and has no infrastructure to maintain.

aws.amazon.com

Architecting a **production grade** hosting and deployment solution for a **static website**

IN-BOX DIRECT DELIVERS BEST OF WEB

OCTOBER 19-21: Visit Netscape In-Box Direct and take advantage of an amazing array of Web-rich interactive content, delivered right to your mailbox. In-Box Direct maximizes Netscape Navigator 3.0's ability to receive pictures, video, audio, and more.

Netscape unveiled a new line of intranet solutions for an expanding market of rich, open email and groupware. Using Netscape Communicator client software and Netscape SuiteSpot 3.0, corporate customers can build and manage full-service intranets.

Recent independent studies by Zona Research and Forrester Research estimate Netscape's share of the Web server market at 80 percent. Analysts attribute Netscape's lead to its wide range of server solutions and cross-platform architecture.

Netscape intranet customers are already realizing a 1000 percent return on investment in less than three months, according to a recent study by International Data Corporation (IDC). IDC also documented an astoundingly swift time to payback for these companies, with savings and ROI typically beginning as early as six weeks after deployment.

Netscape announced a comprehensive strategy to "embrace and integrate" existing Microsoft platforms and technologies in Netscape client and server software and the Netscape ONE platform. Netscape's action will help customers unify their existing environments with their intranets to deliver a seamless experience.

MORE NEWS: Netscape Calendar provides a group scheduling solution for the enterprise ... US WEST Communications implements Netscape client and server software ... Netscape Catalog Server earns kudos from *PC Week* and *Computerworld* ... Netscape and Progressive Networks support new Real Time Streaming Protocol ... Netscape CEO Jim Barksdale featured in recent *Upside* article.

DOWNLOAD OR PURCHASE THE LATEST NETSCAPE SOFTWARE

Select here and click below

JavaScript Enabled

TRY IT BUY IT INFO

GENERAL STORE SPECIAL

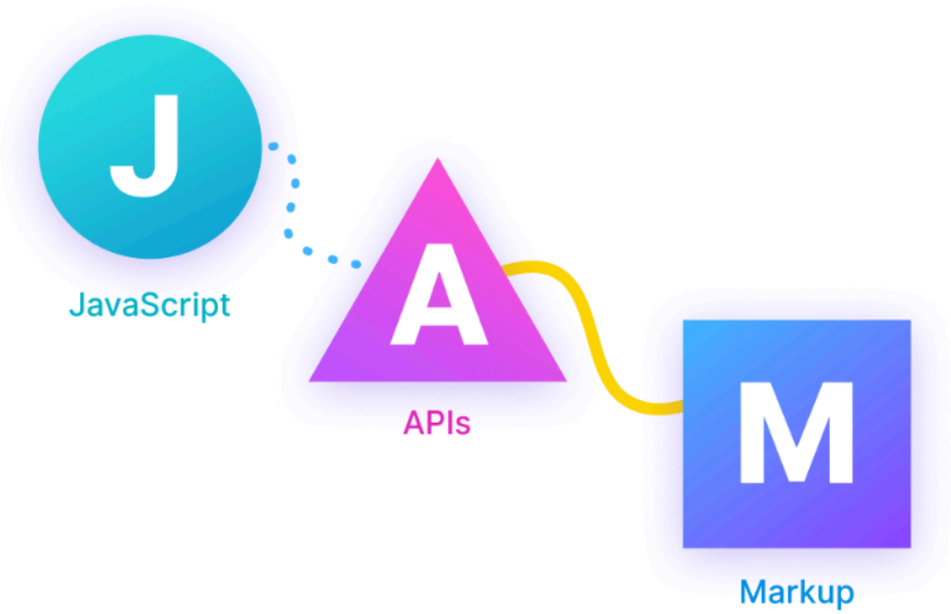
Check out Navigator 3.0 - all platforms. Perfect for fall: Weekender sweatshirts - now only $34 (save $5).

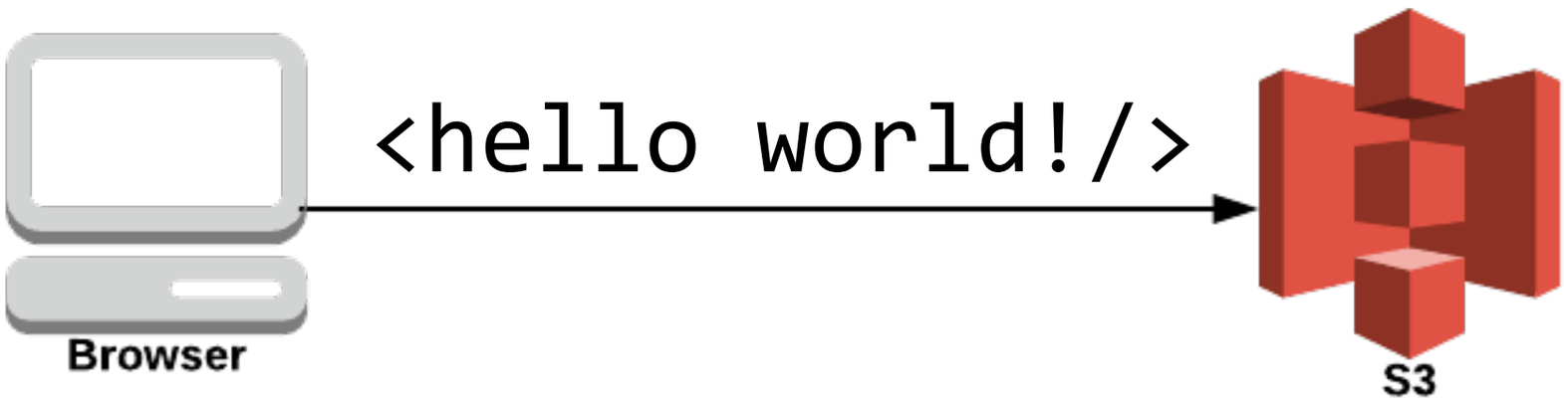
THE MAIN THING: MANY HAPPY RETURNS

Jim Barksdale, President and CEO

In previous columns I've talked about the benefits intranets offer to businesses. Well, now I'm happy to report just how valuable these intranets are. The preliminary report from a study International Data Corporation has undertaken shows that Netscape-based intranets offer companies in many industries a high return on investment (ROI). In fact, the businesses studied are gaining the highest ROIs IDC has ever calculated. ... One of our customers in the study, Cadence Design Systems, had an ROI measured at more than 1700 percent. Cadence uses a Netscape-based intranet as the cornerstone of its sales support system. The system, called OnTrack, solves problems businesses have been experiencing since the days of Willie Loman - getting sales leads, meeting quotas, and generating new business. OnTrack provides supporting materials, custom applications, and reference information to sales reps for each step of the sales process. These are

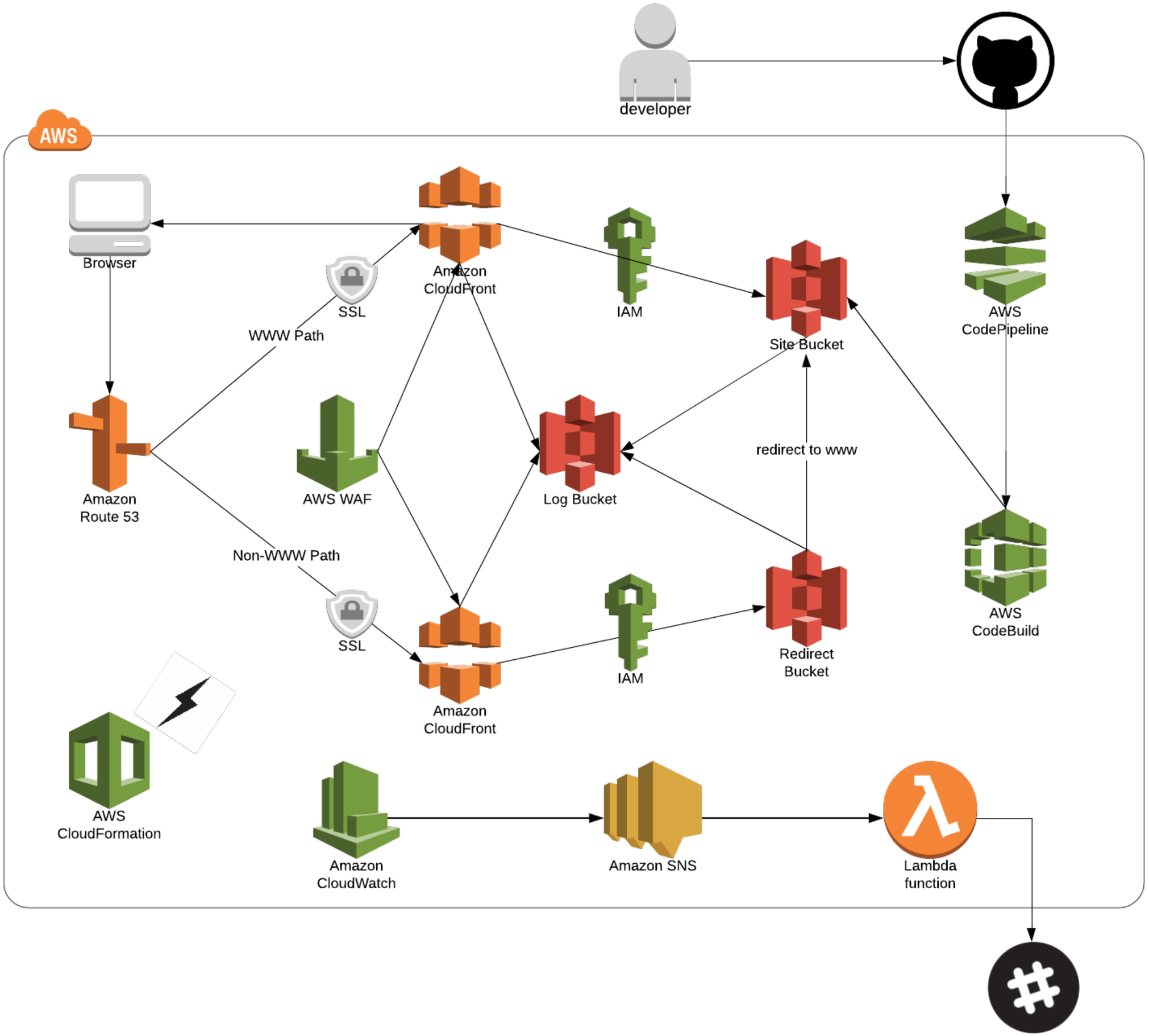
JAM Stack



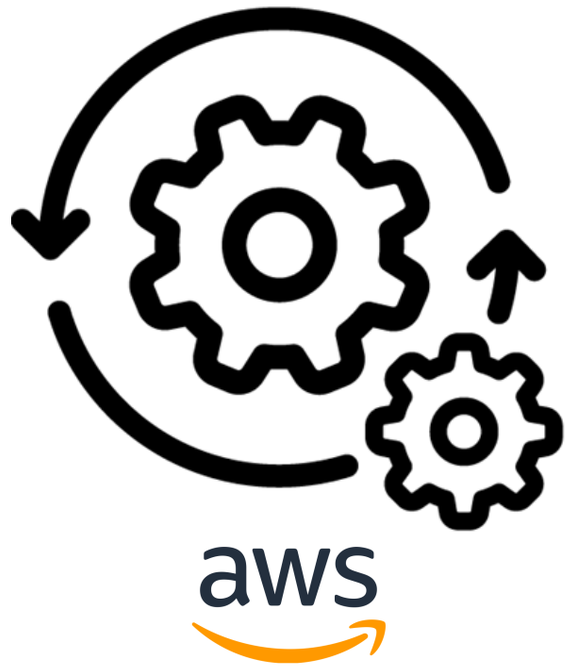

<hello world!/>
Browser
S3

Requirements

- Static Website (React Based - SPA)
- No servers!
- High Performance
- Highly available
- Scalable
- Loggin
- Monitoring
- Globally Distributed Content
- Git-centric, automated deployment pipeline (CI/CD)
- Custom DNS
- SSL
- Whitelist/Blacklist IP’s


developer
AWS
Browser
Amazon
CloudFront
SSL
IAM
Site Bucket
AWS
CodePipeline
WWW Path
Amazon
Route 53
AWS WAF
Log Bucket
redirect to www
Non-WWW Path
SSL
Amazon
CloudFront
IAM
Redirect
Bucket
AWS
CodeBuild
AWS
CloudFormation
Amazon
CloudWatch
Amazon SNS
Lambda
function

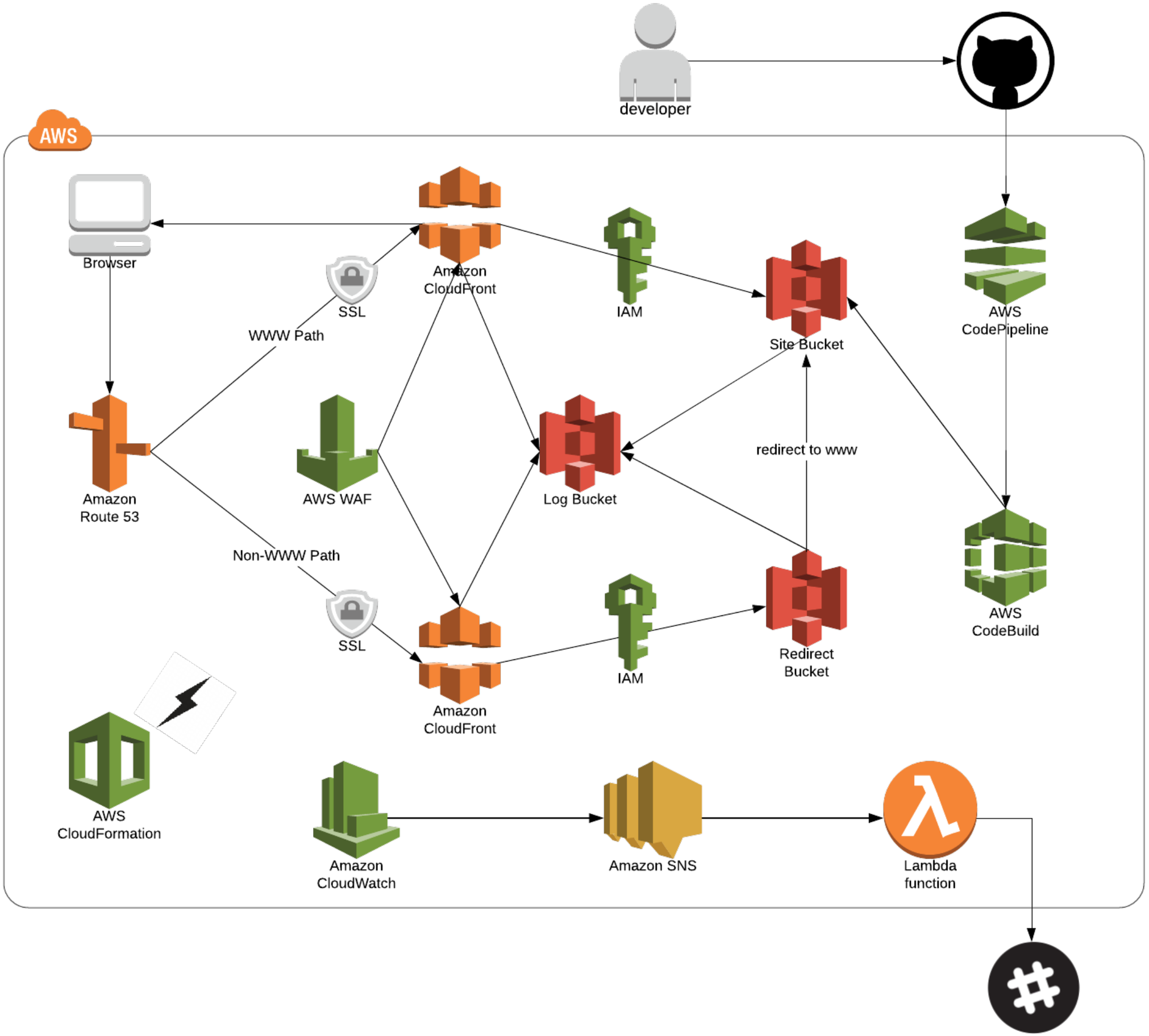
Managed Services



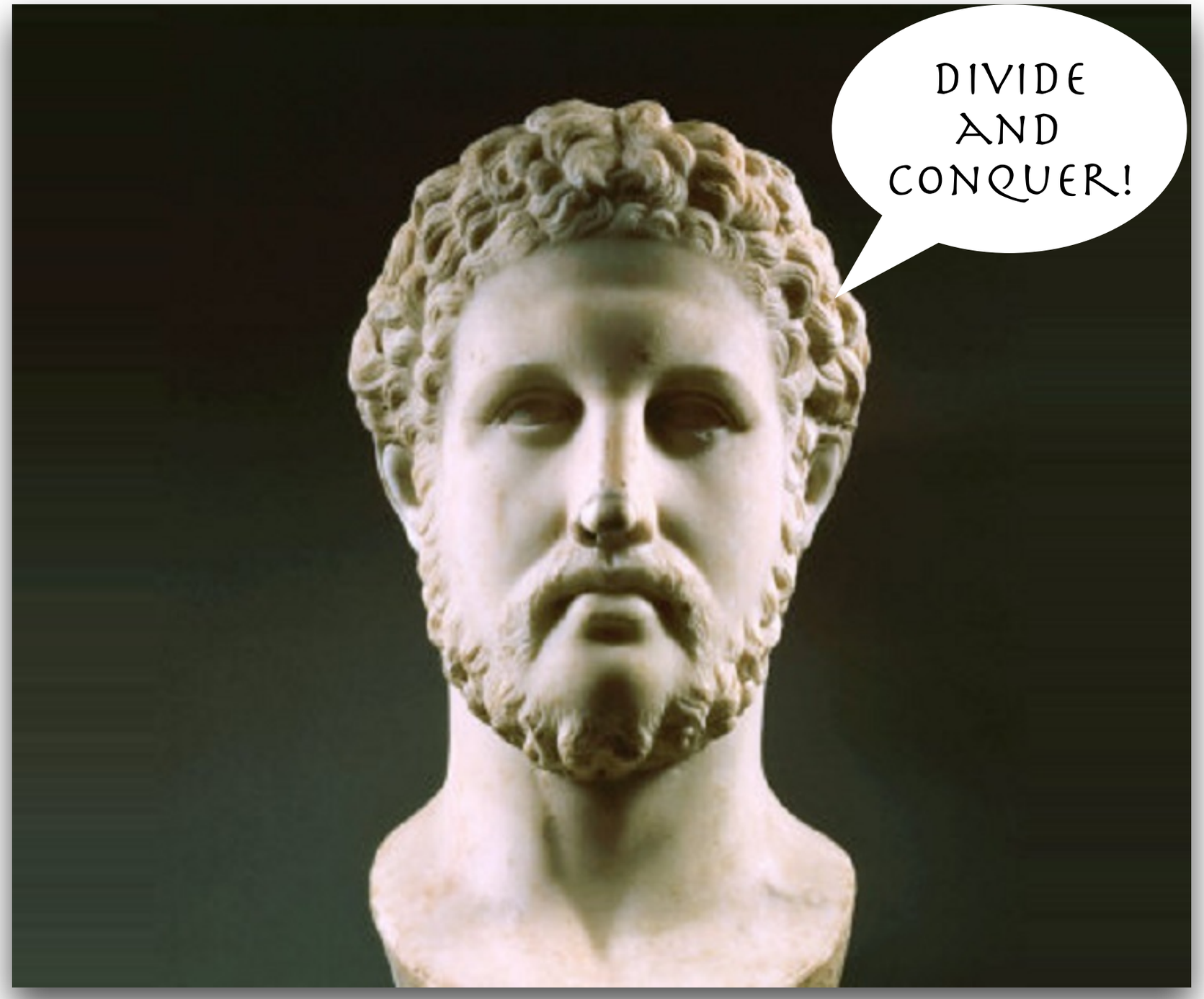
- S3 bucket for site hosting
- S3 bucket for www redirect
- S3 bucket for logs (S3 and CF)
- CloudFront distribution for site bucket
- CloudFront distribution for redirect bucket
- CodePipeline/Code Build (CI/CD)
- CloudWatch filters metrics (monitoring/alerting)
- Lambda + Slack for notifications
- IAM (Cross Account roles)
- WAF
- Route53 (www & non-www)
- CloudFormation for building all of it (optional)

no servers!

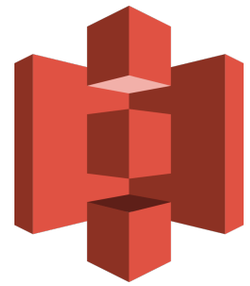
serviceful


developer
AWS
Browser
Amazon
CloudFront
SSL
IAM
Site Bucket
AWS
CodePipeline
WWW Path
Amazon
Route 53
AWS WAF
Log Bucket
redirect to www
Non-WWW Path
SSL
Amazon
CloudFront
IAM
Redirect
Bucket
AWS
CodeBuild
AWS
CloudFormation
Amazon
CloudWatch
Amazon SNS
Lambda
function

CloudFormation

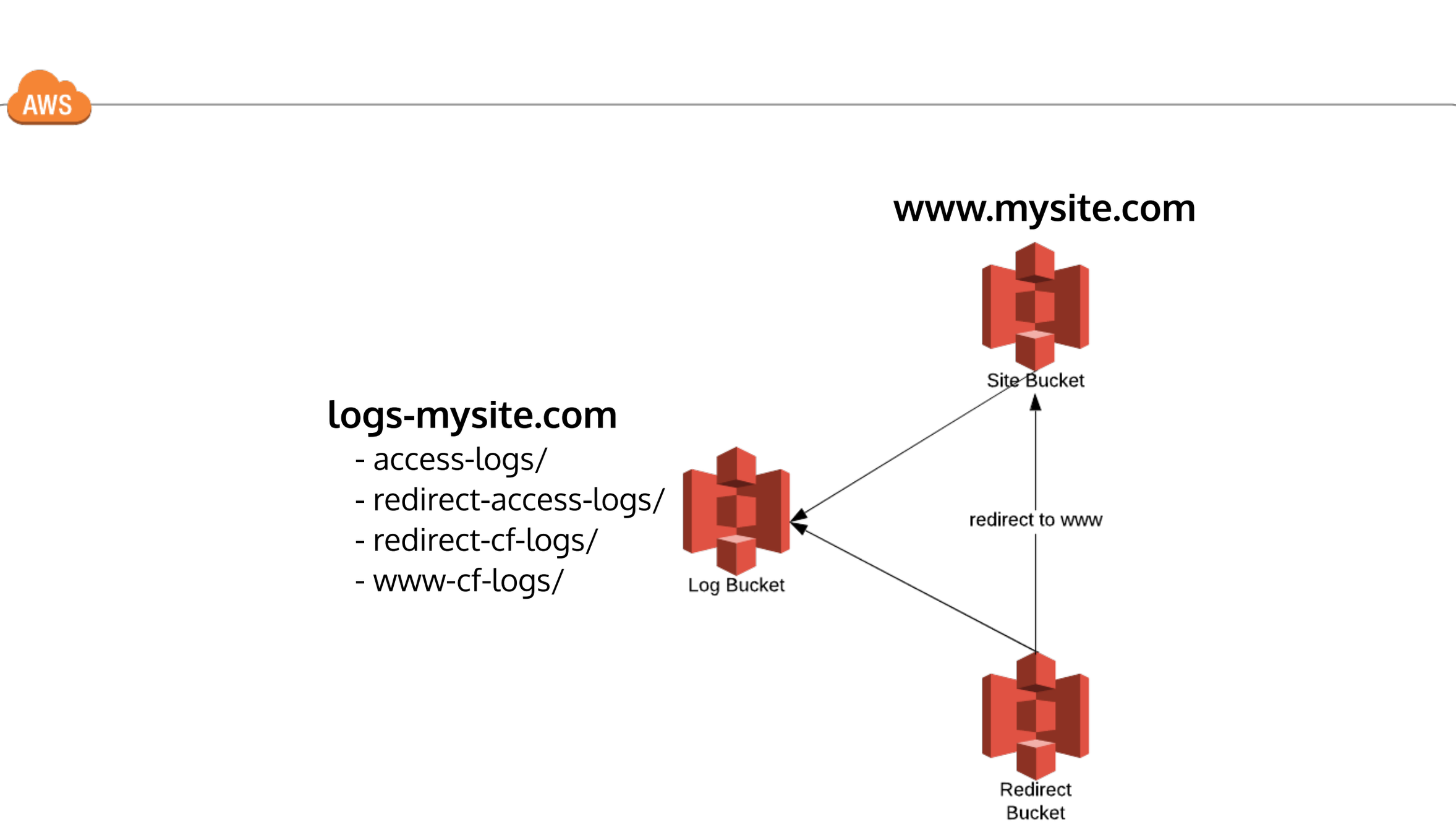

DIVIDE
AND
CONQUER!

S3



S3 Site Bucket

```
MySiteBucket": {
   "Type": "AWS::S3::Bucket",
   "DeletionPolicy": "Retain",
   "Properties": {
     "BucketName": { "Fn::Sub": "www.${DomainName}" },
     "AccessControl": "Private",
     "WebsiteConfiguration": {
       "IndexDocument": "index.html"
      }
   }
}
```

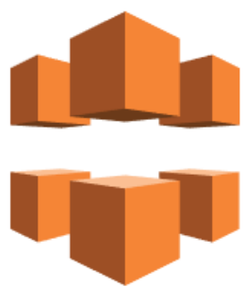



```
"RedirectAllRequestsTo": {
   "HostName": { "Fn::Sub": "www.${DomainName}" },
   "Protocol": "https"
}
```

S3 LifeCycle Rules for Log purging

```
"LifecycleConfiguration": {
   "Rules": [
     {
       "Id": "purge-access-logs",
       “Prefix": access-logs/",
       "Status": "Enabled",
       "ExpirationInDays": 30
     }
   ]
}
```

CloudFront

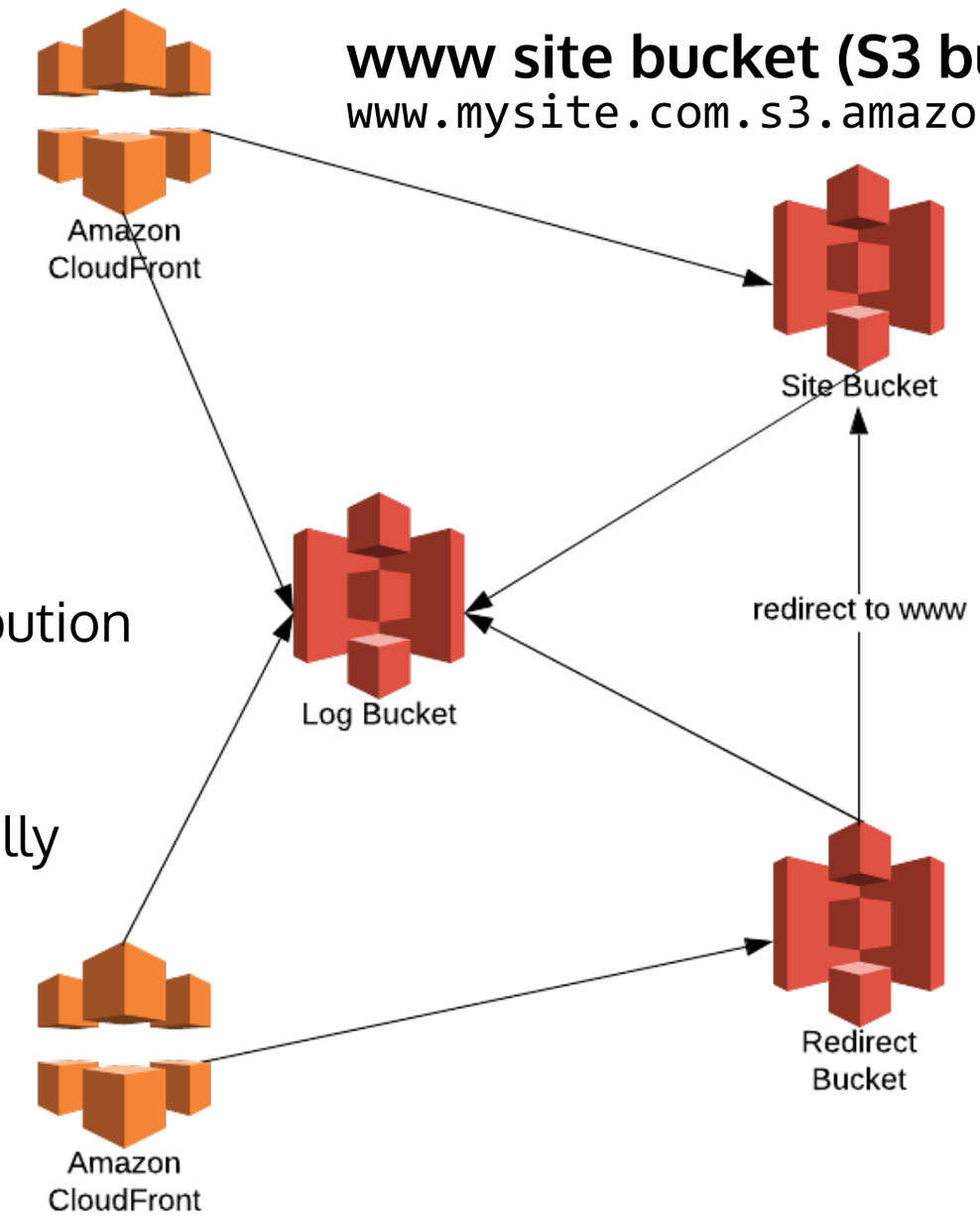


- Use origin cache headers
  (set these in S3)

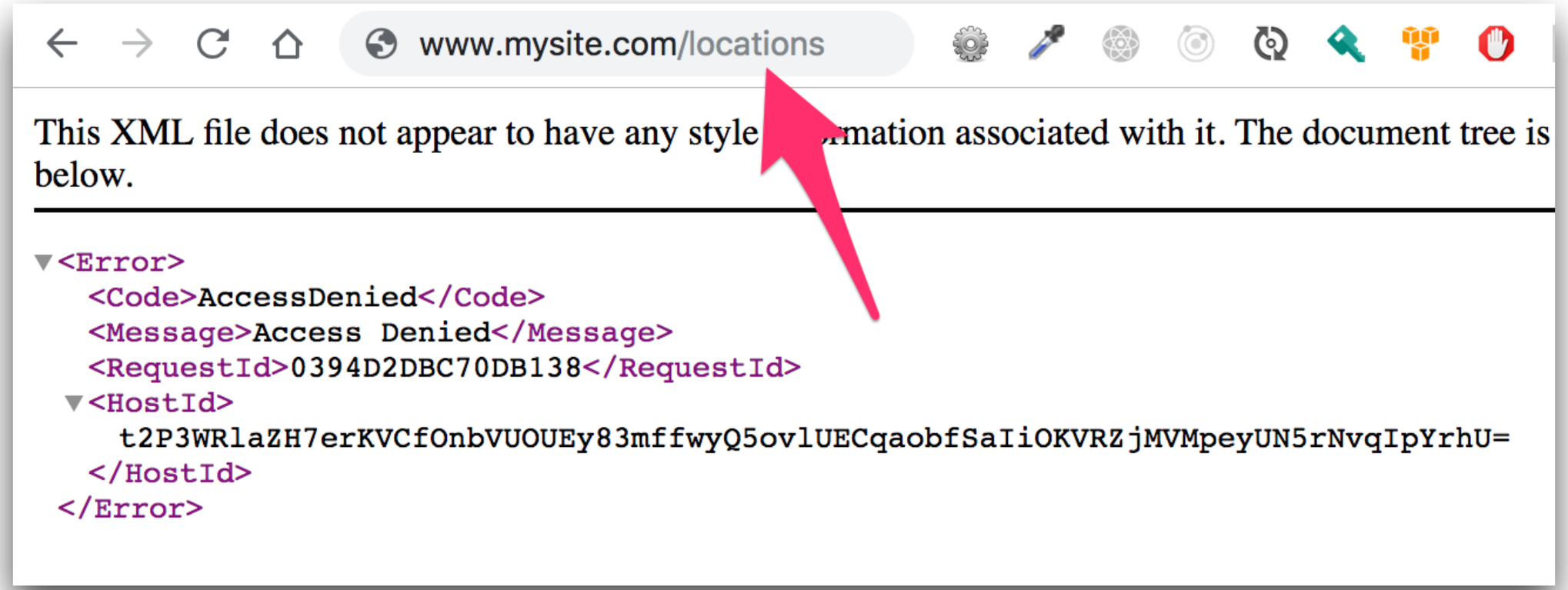
- Create Origin Access Identity
  and assign to the www distribution
  (optional... but not really)

- Compress objects automatically
  (gzip'd at the edge!)

- Set error page for 403's



Client Side Routing Error



CloudFront Error Page Config

Console view

	HTTP Error Code	Error Caching Minimum TTL ▼	Response Page Path	HTTP Response Code
☐	403	0	/index.html	200

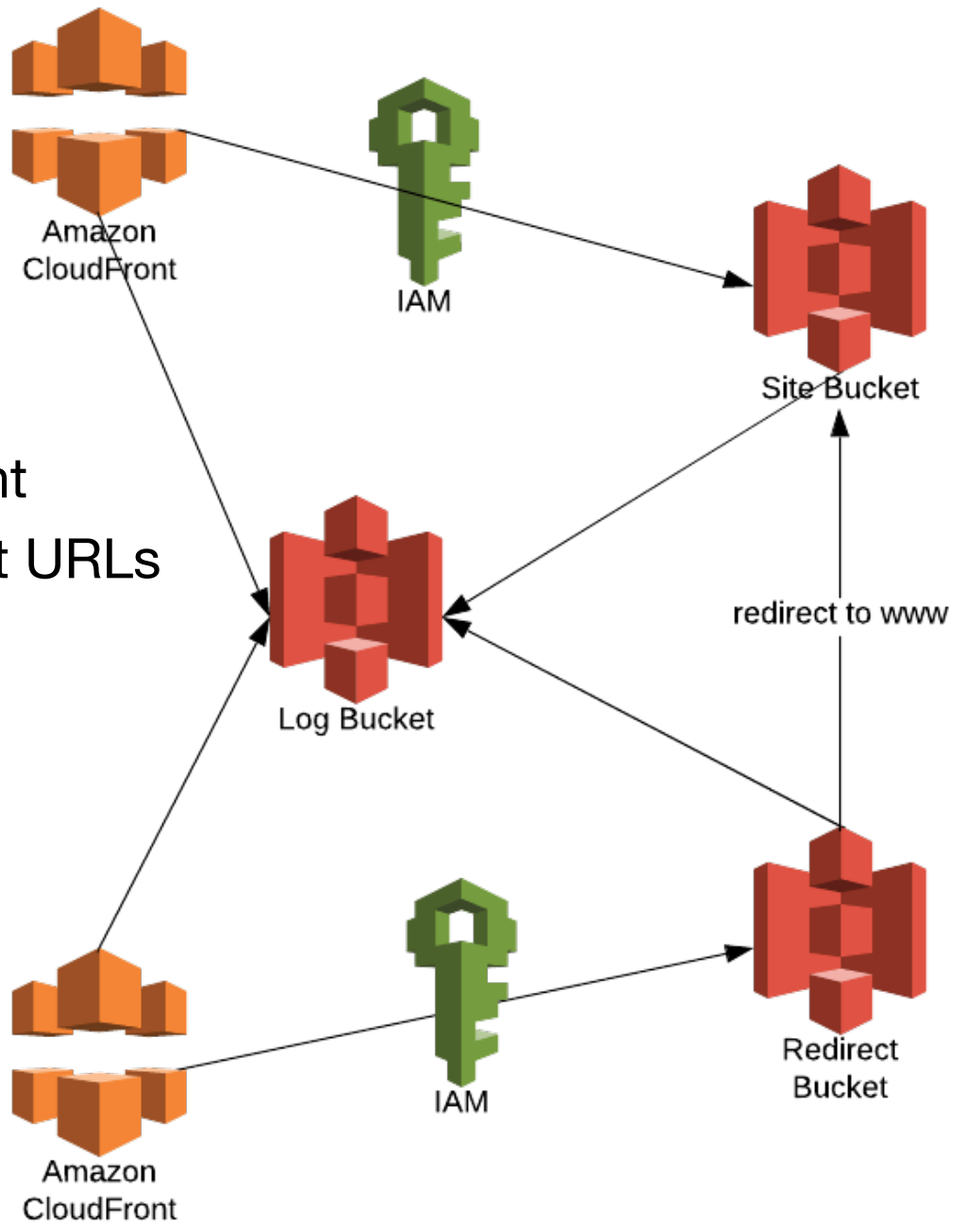
```
"CustomErrorResponses": [
  {
    "ErrorCachingMinTTL": 0,
    "ErrorCode": 403,
    "ResponseCode": 200,
    "ResponsePagePath": "/index.html"
  }
]
```

CloudFormation

IAM Policy- Origin Access Identity

AWS

- Restricts Access to S3 Content
- Ensures access by CloudFront URLs
- Assigned to CF Dist
- Added in bucket policy



Origin Access Identity

```
"OAI": {
   "Type": "AWS::CloudFront::CloudFrontOriginAccessIdentity",
   "Properties": {
     "CloudFrontOriginAccessIdentityConfig": {
       "Comment": { "Fn::Sub": "${DomainName}-oai" }
     }
   }
}
```

CloudFormation

Assign Origin Access Identity Assignment

```
"S3OriginConfig": {
  "OriginAccessIdentity": {
     "Fn::Sub": "origin-access-identity/cloudfront/${OAI}"
  }
}
```

www distribution origin config

```
{
  "Action": ["s3:GetObject"],
  "Effect": "Allow",
  "Resource": { "Fn::Sub": "arn:aws:s3:::${SiteBucket}/*" },
  "Principal": {
    "AWS": {
      “Fn::Sub":
         "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity ${OAI}"
     }
  }
}
```

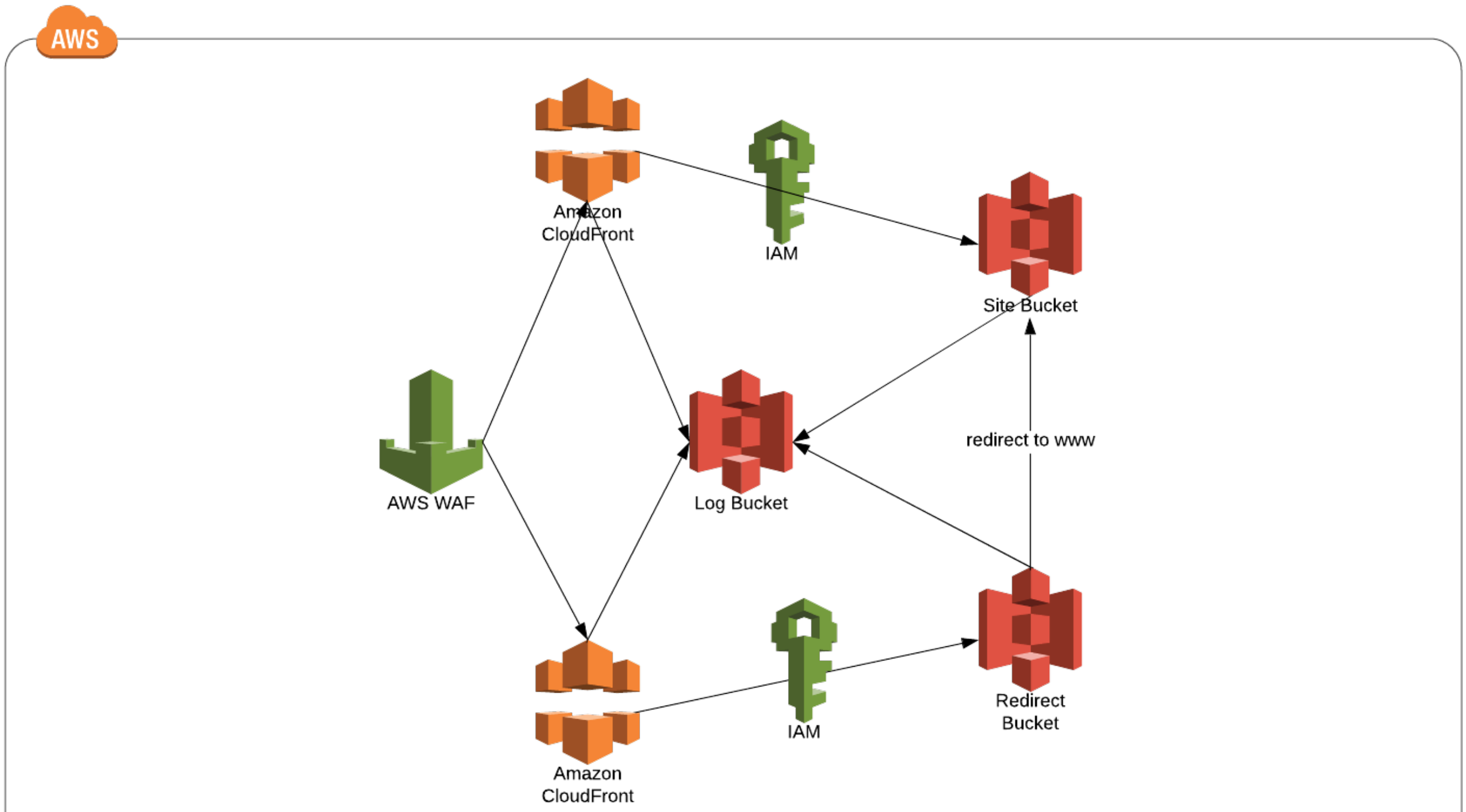
CF bucket policy

Origin Access Identity - Cont'd

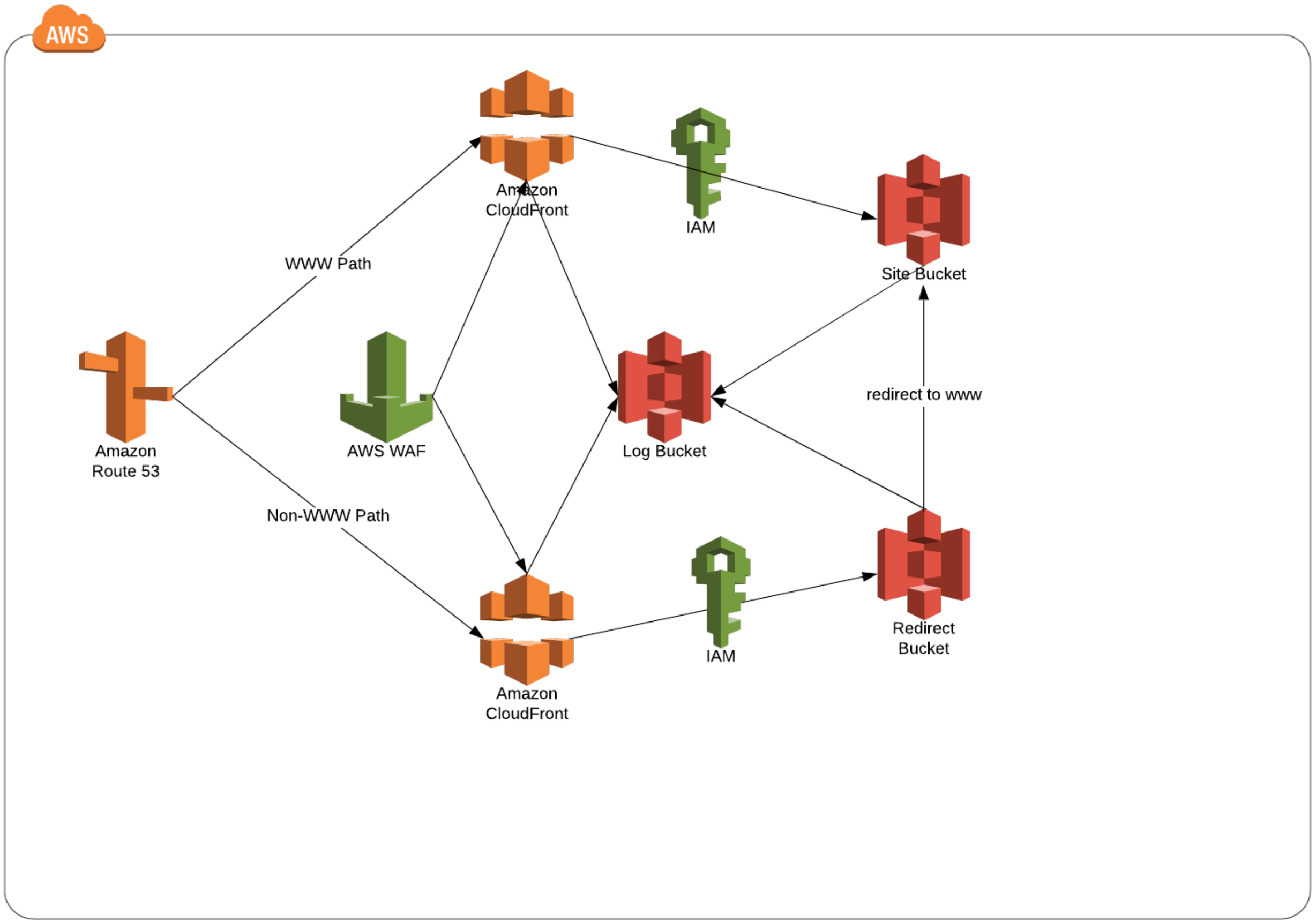
```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity ABC123"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::www.mysite.com/*"
    }
  ]
}
```

S3 Bucket Policy

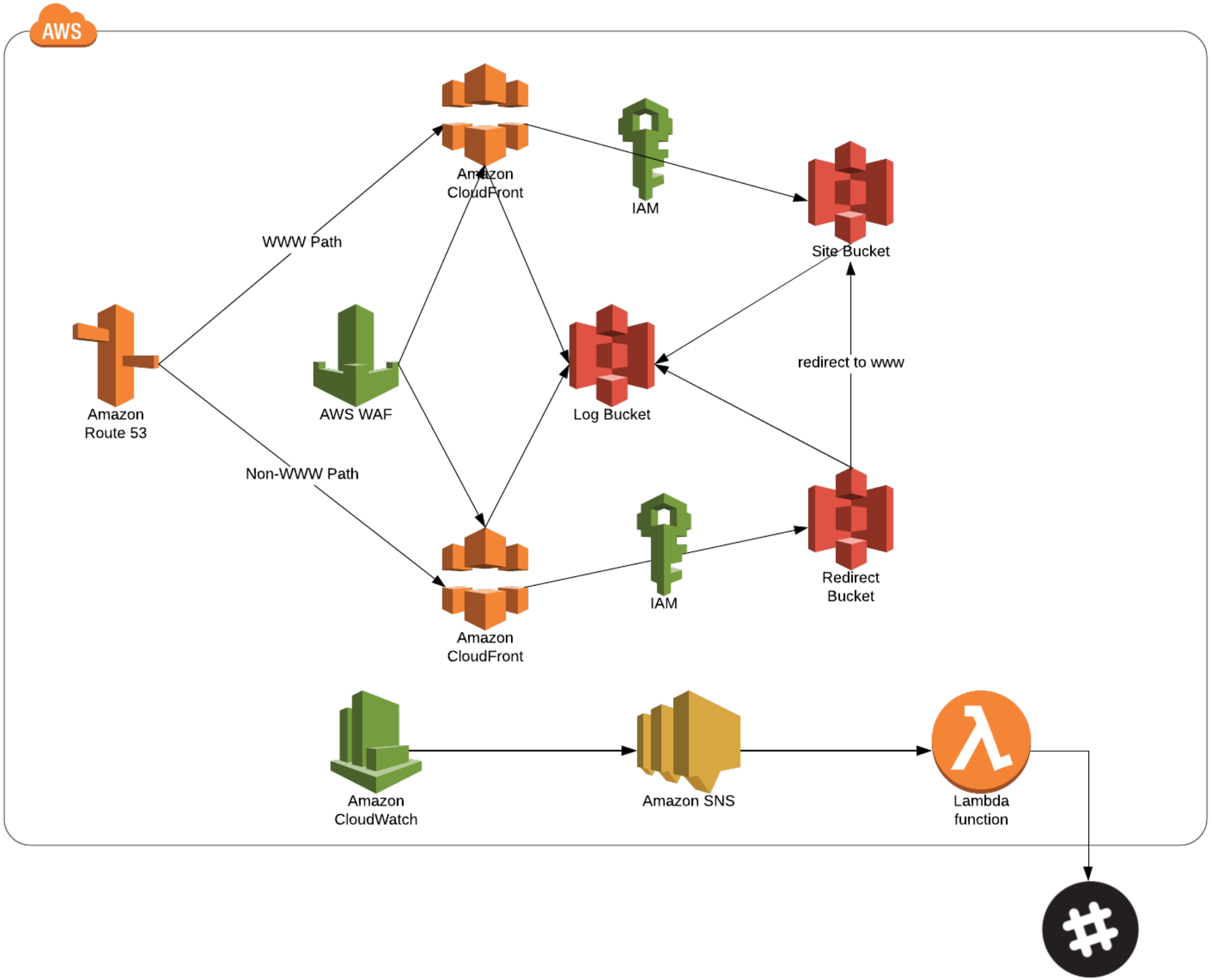
Web Application Firewall (WAF)


AWS
Amazon CloudFront
IAM
Site Bucket
AWS WAF
Log Bucket
redirect to www
Amazon CloudFront
IAM
Redirect Bucket

Route 53


AWS
Amazon CloudFront
IAM
Site Bucket
WWW Path
Amazon Route 53
AWS WAF
Log Bucket
redirect to www
Non-WWW Path
Amazon CloudFront
IAM
Redirect Bucket

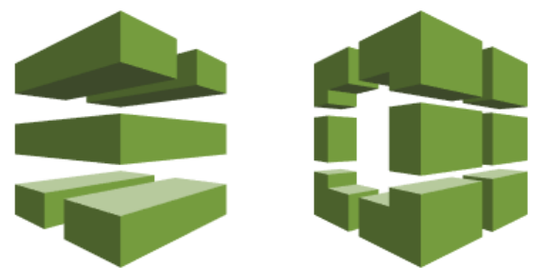
Monitoring with CloudWatch (and friends)

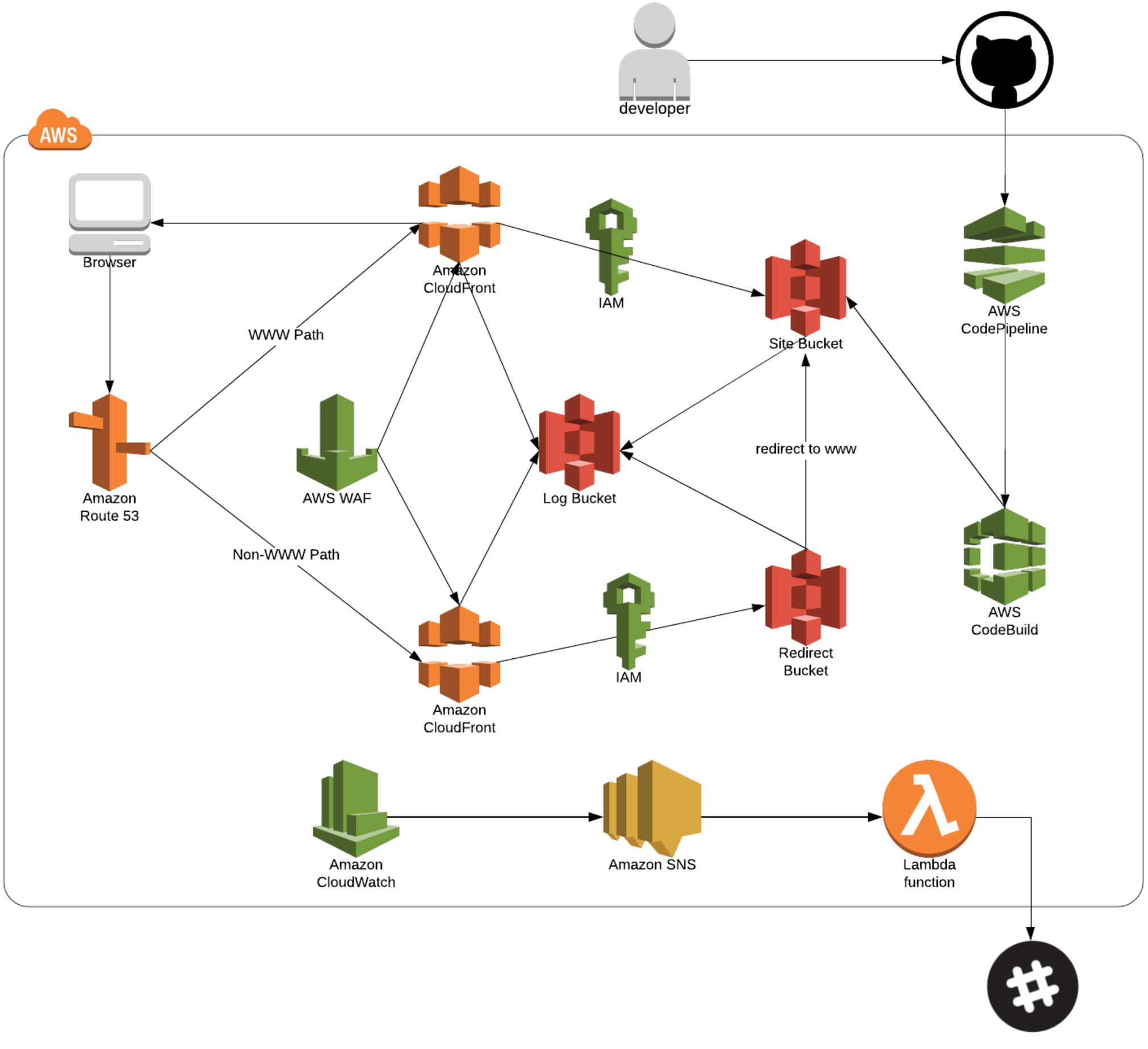

AWS
Amazon
CloudFront
IAM
Site Bucket
WWW Path
Amazon
Route 53
AWS WAF
Log Bucket
redirect to www
Non-WWW Path
Amazon
CloudFront
IAM
Redirect
Bucket
Amazon
CloudWatch
Amazon SNS
Lambda
function

CloudWatch Alarm

```
CloudFront5xxAlarm:
    Type: AWS::CloudWatch::Alarm
    Properties:
      AlarmName: mysite-CloudFront-5xxErrorRate
      Dimensions:
        - Name: DistributionId
          Value: !Ref DistributionId
      AlarmActions:
        - !Ref TopicARN
      MetricName: 5xxErrorRate
      Namespace: AWS/CloudFront
      Statistic: Average
      Period: 60
      EvaluationPeriods: 1
      TreatMissingData: notBreaching
      ComparisonOperator: GreaterThanThreshold
      Threshold: 1
```

CI/CD /w CodePipeline & CodeBuild




developer
AWS
Browser
Amazon
CloudFront
IAM
Site Bucket
AWS
CodePipeline
WWW Path
Amazon
Route 53
AWS WAF
Log Bucket
redirect to www
Non-WWW Path
AWS
CodeBuild
Redirect
Bucket
IAM
Amazon
CloudFront
Amazon
CloudWatch
Amazon SNS
Lambda
function

IAM Cross Account Role Access

IAM Cross Account Role - Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:RestoreObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::www.mysite.com/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      “Resource": "arn:aws:s3:::www.mysite.com"
    }
  ]
}
```

least privilege policy

IAM Cross Account Role - Trust Relationship

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789010:role/service-role/CodeBuildRole",
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

CodeBuild Role - Policy

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
          "arn:aws:iam::123456789010:role/mysite-deployer-role"
      ]
  }
}
```

CodeBuild - Cross Account Deployment

```
…
  post_build:
    commands:
      - role=$(aws sts assume-role --role-arn $ROLE_ARN –role-session-name \
            mysite-session --duration-seconds $DURATION)

      - SECRET=$(echo $role | awk '{print $12}' | tr -d '"' | tr -d ',')
      - TOKEN=$(echo $role | awk '{print $14}' | tr -d '"' | tr -d ',')
      - KEY=$(echo $role | awk '{print $18}' | tr -d '"' | tr -d ',')
      - export AWS_ACCESS_KEY_ID=$KEY
      - export AWS_SESSION_TOKEN=$TOKEN
      - export AWS_SECRET_ACCESS_KEY=$SECRET
      - export AWS_DEFAULT_REGION=us-west-2
…
```

buildspec.yml

Deploy with S3 Sync

```
- aws s3 sync --cache-control "max-age=${TTL_SECONDS}" \
        –delete build/ "s3://${BUCKET}" --exclude='index.html'

- aws s3 cp --cache-control "max-age=0" \
        build/index.html "s3://${BUCKET}/index.html"
```

buildspec.yml

main.05006982.js Latest version

Overview | Properties | Permissions | Select from

Storage class

Use the most appropriate storage class based on frequency of access.

Learn more

Standard

Encryption

Use encryption to protect your data while in-transit and at rest.

Learn more

None

Metadata

+ Add Metadata | Delete | Edit

Key	Value
Cache-Control	max-age=31536000
Content-Type	application/javascript

Cancel | Save

index.html Latest version

Overview | Properties | Permissions | Select from

Storage class

Use the most appropriate storage class based on frequency of access.

Learn more

Standard

Encryption

Use encryption to protect your data while in-transit and at rest.

Learn more

None

Metadata

+ Add Metadata | Delete | Edit

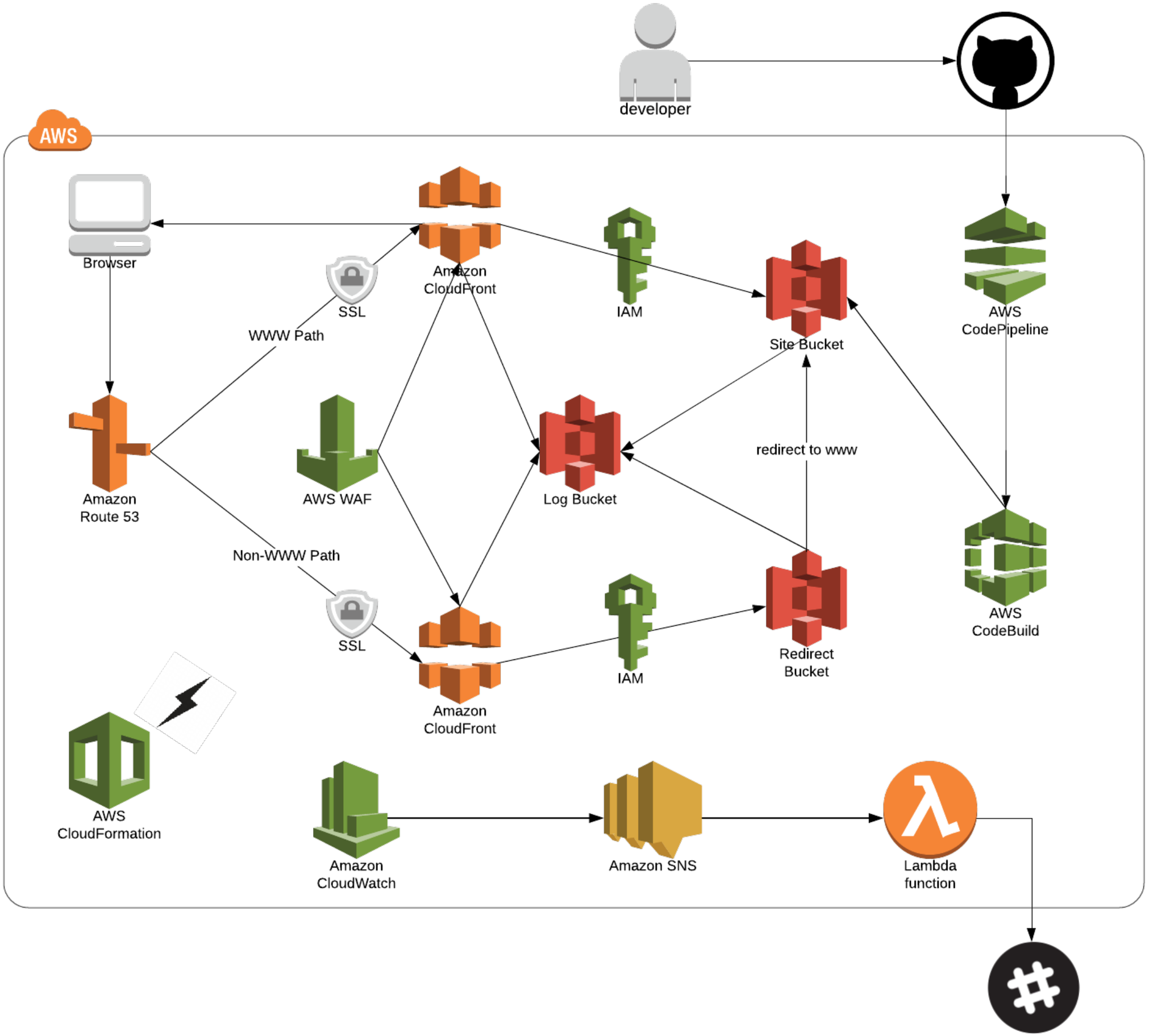
Key	Value
Cache-Control	max-age=0
Content-Type	text/html

Cancel | Save

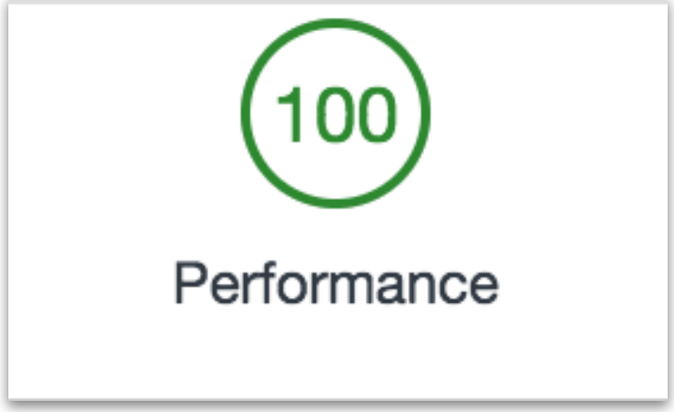
CloudFormation FTW!

CloudFormation Templates

- Cross account role
- Deployment pipeline
- Website infra
- Monitoring


developer
AWS
Browser
Amazon
CloudFront
SSL
IAM
Site Bucket
AWS
CodePipeline
WWW Path
Amazon
Route 53
AWS WAF
Log Bucket
redirect to www
Non-WWW Path
SSL
Amazon
CloudFront
IAM
Redirect
Bucket
AWS
CodeBuild
AWS
CloudFormation
Amazon
CloudWatch
Amazon SNS
Lambda
function

Lighthouse Audit 😎👊



@davetownsend