

Assignment

London Stock Exchange Group

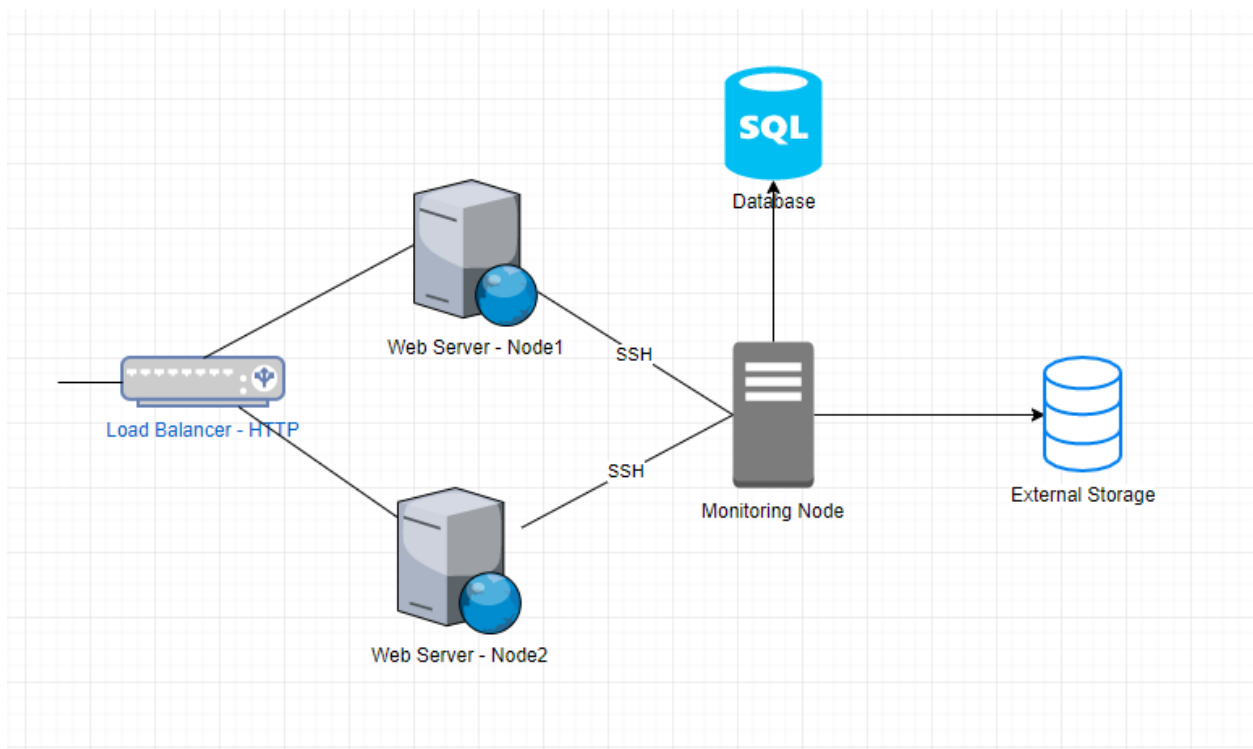


Lahiru Malavige

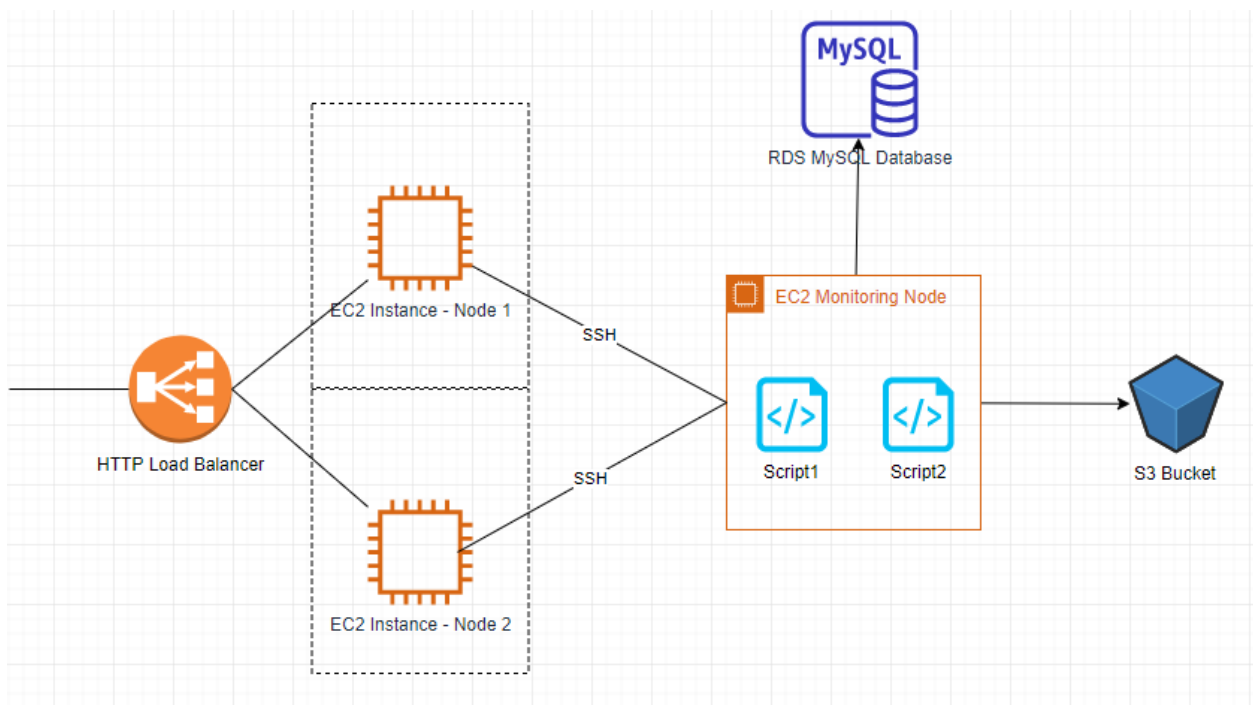
Table of Contents

High Level Architecture Diagram	2
AWS based solution diagram	2
AMI creation	3
Preparing the EC2 instances to create the customized AMI templates	7
Database creation	8
S3 bucket creation with IAM role access for EC2	13
Setting up the monitoring instance.	17
Setting up the environment - Instructions.....	19
Limitations and Suggestions	20
Output of the solution.	21
Scripts.....	23

High Level Architecture Diagram

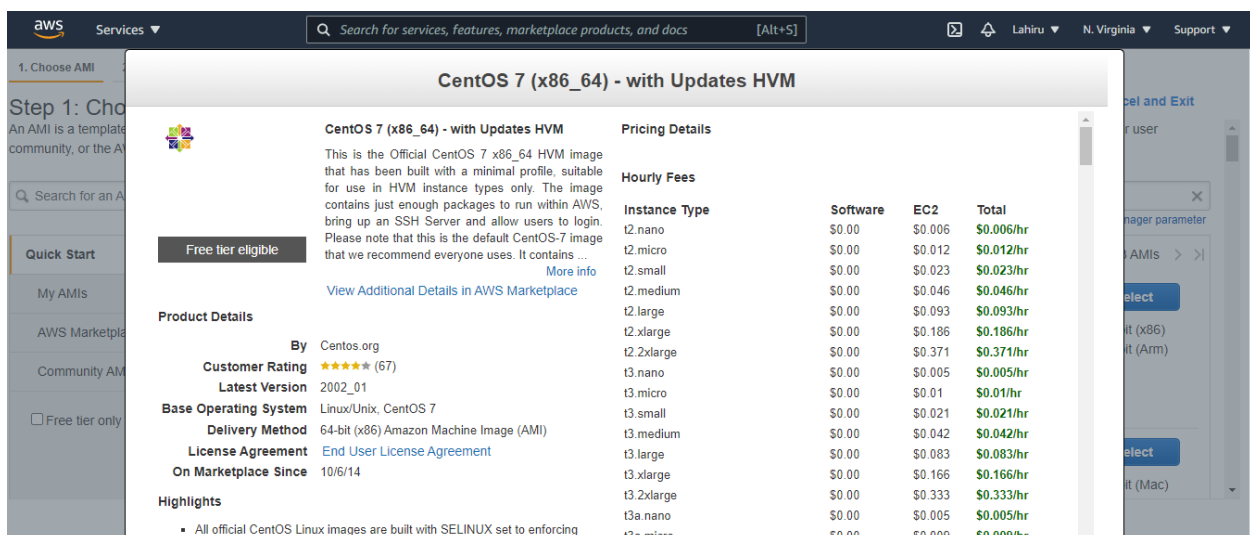
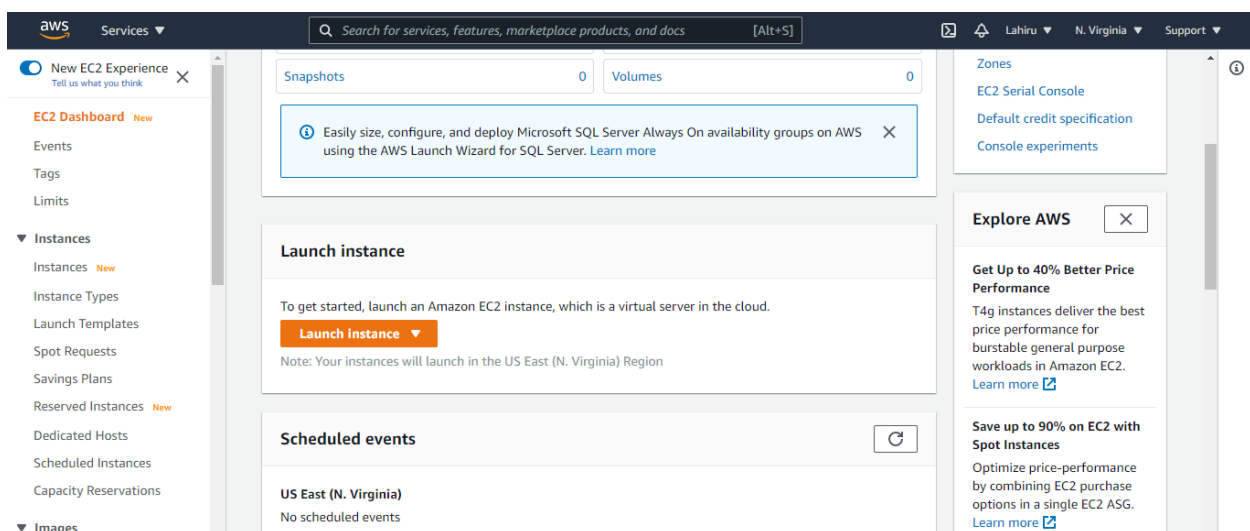


AWS based solution diagram



AMI creation

Amazon Machine Image makes it easier to deploy EC2 instances in AWS as it keeps the basic OS configurations of an instance and we can deploy multiple instances using a single AMI in the AWS environment as well. AWS has built in AMIs and also we can make an Amazon Machine Image from a currently running EC2 instance as well. The intention of launching such EC2 instance is to come up with a customized AMI that can be later used in cloudformation in this setup. Two separate AMIs will be created for web nodes and the monitoring node.



- Centos 7 was chosen as the AMI to setup the EC2 instances for this setup.

aws Services [Alt+S] Lahiru N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)
 Note: The vendor recommends using a **t2.micro** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

- The instance type must be chosen to cater the requirement. More computing power and memory, better network performances are more expensive as well.

aws Services [Alt+S] Lahiru N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-7079fb0d (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: ☐ Use subnet setting (Enable)

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)
 Select an IAM role that has read access to Secrets Manager, and that has the following AWS managed policies attached to it: AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess. [Learn more](#)

Shutdown behavior: Stop

Stop - Hibernate behavior: ☐ Enable hibernation as an additional stop behavior

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring
 Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
 Additional charges will apply for dedicated tenancy.

Elastic Inference: ☐ Add an Elastic Inference accelerator

- An EC2 instance is always deployed in a virtual private cloud. There are options to define the subnet. Identity and Access Management plays a major role in security in EC2 instances. If there are already created IAM roles they can be applied. If not, those configurations can be applied later on.

aws Services Search for services, features, marketplace products, and docs [Alt+S] Lahiru N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0cb4f5ff601f70d3c	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

- Size of the storage device in EC2 instance must be declared and the different volume types like SSD, HDD and magnetic disks are given as options. IOPS will also differ according to the volume type and faster storages will require more cost.

aws Services Search for services, features, marketplace products, and docs [Alt+S] Lahiru N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
This resource currently has no tags				

Choose the [Add tag](#) button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

[Add Tag](#) (Up to 50 tags maximum)

- Tags are very useful in configuration management.

aws Services Search for services, features, marketplace products, and docs [Alt+S] Lahiru N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name: CentOS 7 -x86_64- - with Updates HVM-2002_01-AutogenByAWSMP-

Description: This security group was generated by AWS Marketplace and is based on recomm

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere 0.0.0.0/0, :::0	SSH access for the AMI_instance

[Add Rule](#)

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

- Security group will act as the firewall daemon or iptables in a linux server. It gives the option to allow certain ports and IP addresses both inbound and outbound traffic.

aws Services Search for services, features, marketplace products, and docs [Alt+S] Lahiru N. Virginia Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Improve your instances' security. Your security group, CentOS 7 -x86_64- - with Updates HVM-2002_01-AutogenByAWSMP-, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

AMI Details [Edit AMI](#)

CentOS 7 (x86_64) - with Updates HVM

Free tier eligible CentOS Linux 7 x86_64 HVM EBS ENA2002_01 Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on t2.micro instance. Additional taxes or fees may apply. Software charges will begin once you launch this AMI and continue until you terminate the instance.

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's

[Cancel](#) [Previous](#) [Launch](#)

- After reviewing the selected options, the EC2 instance can be launched.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Choose an existing key pair

Select a key pair

No key pairs found

⚠ No key pairs found

You don't have any key pairs. Please create a new key pair by selecting the **Create a new key pair** option above to continue.

[Cancel](#) [Launch Instances](#)

- SSH key pair must be created in order to access the newly created EC2 instance. If there is an already created key pair(.pem) available, that can be used reused for any instance that we deploy through AWS.

Instances (1) Info

🔄

Connect

Instance state ▾

Actions ▾

Launch instances ▾

🔍 Filter instances

< 1 >

⚙️

<input type="checkbox"/>	Name ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	-	i-0983f34880a0991f4	<div><div>✔️</div><div>Running</div><div>🔍</div></div>	t2.micro	<div><div>🕒</div><div>Initializing</div></div>	No alarms +	us-east-1d

- Instance is ready and up and running as shown in the dashboard.

Preparing the EC2 instances to create the customized AMI templates

```

1 AWS AMI
[centos@ip-172-31-30-246 ~]$ sudo yum install httpd
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: d36uatko69830t.cloudfront.net
 * extras: d36uatko69830t.cloudfront.net
 * updates: d36uatko69830t.cloudfront.net
Resolving Dependencies
--> Running transaction check
--> Package httpd.x86_64 0:2.4.6-97.el7.centos will be installed
--> Processing Dependency: httpd-tools = 2.4.6-97.el7.centos for package: httpd-2.4.6-97.el7.centos.x86_64
--> Processing Dependency: system-logos >= 7.92.1-1 for package: httpd-2.4.6-97.el7.centos.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.6-97.el7.centos.x86_64
--> Processing Dependency: libaprutil-1.so.0()(64bit) for package: httpd-2.4.6-97.el7.centos.x86_64
--> Processing Dependency: libapr-1.so.0()(64bit) for package: httpd-2.4.6-97.el7.centos.x86_64
--> Running transaction check
--> Package apr.x86_64 0:1.4.8-7.el7 will be installed
--> Package apr-util.x86_64 0:1.5.2-6.el7 will be installed
--> Package centos-logos.noarch 0:70.0.6-3.el7.centos will be installed
--> Package httpd-tools.x86_64 0:2.4.6-97.el7.centos will be installed
--> Package mailcap.noarch 0:2.1.41-2.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

Package Arch Version Repository Size
Installing:
httpd x86_64 2.4.6-97.el7.centos updates 2.7 M
Installing for dependencies:
apr x86_64 1.4.8-7.el7 base 104 k
apr-util x86_64 1.5.2-6.el7 base 92 k
centos-logos noarch 70.0.6-3.el7.centos base 21 M
httpd-tools x86_64 2.4.6-97.el7.centos updates 93 k
mailcap noarch 2.1.41-2.el7 base 31 k

```

- Installing httpd (apache) web service in order to setup the web service.

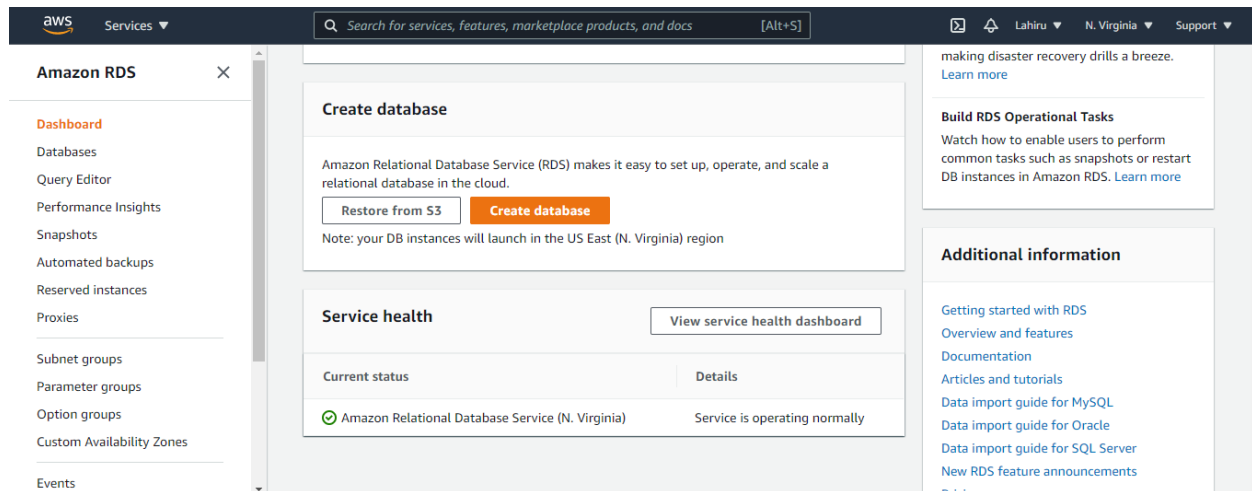
```

VirtualHost *:80>
    ServerName www.assignment.com
    ServerAlias assignment.com
    DocumentRoot /var/www/aws_assignment/public_html
    ErrorLog /var/www/aws_assignment/error.log
    CustomLog /var/www/aws_assignment/requests.log combined
</VirtualHost>
~
~
~

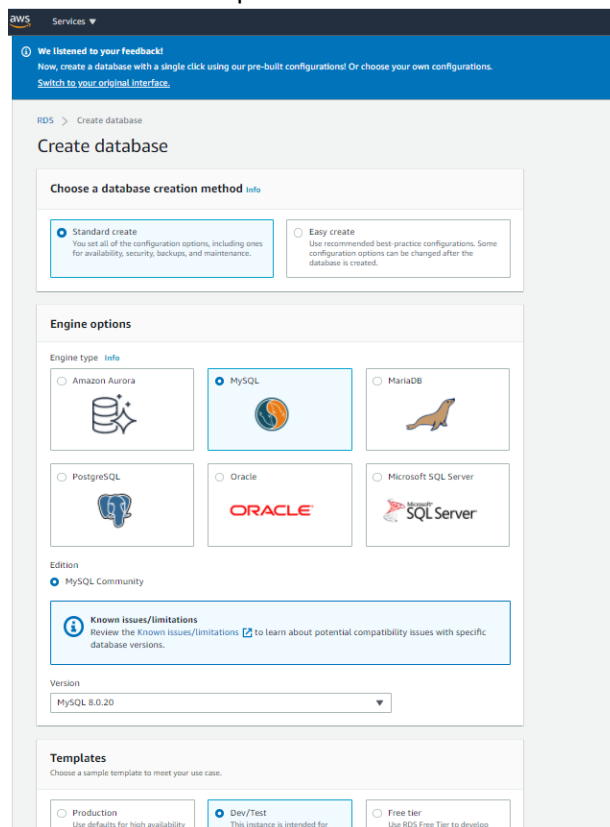
```

- Virtual host is created (/etc/httpd/conf.d/assignment.com.conf) in order to serve the web page which is placed in the document root. Virtual hosting allows multiple web applications to be served in one server. It is recommended rather than using the default web root with default config file.

Database creation



- AWS provide various database solutions like Relational Database Solution (RDS), Aurora, DynamoDB. A simple RDS solution like mysql can be used for this solution since we need to just store the timestamp and the status in the database only.



Settings

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ **Credentials Settings**

Master username [Info](#)
Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter

☐ **Auto generate a password**
Amazon RDS can generate a password for you, or you can specify your own password

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

Confirm password [Info](#)

- DB identifier, master username and password must be provided.

DB instance class

DB instance class [Info](#)
Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

☒ Standard classes (includes m classes)
☐ Memory optimized classes (includes r and x classes)
☐ Burstable classes (includes t classes)

db.m6g.large
2 vCPUs 8 GiB RAM Network: 4,750 Mbps ▼

☐ Include previous generation classes

Storage

Storage type [Info](#)

General Purpose (SSD) ▼

Allocated storage

20 GiB

(Minimum: 20 GiB, Maximum: 65,536 GiB) Higher allocated storage **may improve** IOPS performance.

[Provisioning less than 100 GiB of General Purpose \(SSD\) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose \(SSD\) IO credit balance. \[Learn more\]\(#\)](#)

- Database can be chosen from the given options to cater the requirement of the solution. The high performance database solutions will cost more.

Connectivity



Virtual private cloud (VPC) [Info](#)

VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-7079fb0d) ▼

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default ▼

Public access [Info](#)

☐ Yes

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

☒ No

RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group

Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

☐

Choose existing

Choose existing VPC security groups

☒

Create new

Create new VPC security group

New VPC security group name

AWS_Assignment_RDS

Availability Zone [Info](#)

No preference ▼

▼ Additional configuration

Database port [Info](#)

TCP/IP port that the database will use for application connections.

3306

- Database is also created under the same virtual private cloud and the default port is chosen as 3306.

Database authentication

Database authentication options [Info](#)

- ☒ Password authentication
Authenticates using database passwords.
- ☐ Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.
- ☐ Password and Kerberos authentication (not available for this version)
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

► Additional configuration


Database options, encryption enabled, backup enabled, backtrack disabled, Performance Insights enabled, Enhanced Monitoring enabled, maintenance, CloudWatch Logs, delete protection disabled

Estimated monthly costs

DB instance	110.96 USD
Storage	2.30 USD
Total	113.26 USD

This billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).

 You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Cancel

Create database

- Different authentication modes can be chosen for the database. IAM based authentication requires IAM roles to be created and applied. The password authentication is the classic way of accessing the DBMS. This username and password will be used by the monitoring instance to connect to the DBMS.

```

[root@ip-172-31-30-246 ~]# mysql -h database-1.crdxxeqjw7mf.us-east-1.rds.amazonaws.com -u admin -P 3306 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 87
Server version: 8.0.20 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> create database web_page_status;
Query OK, 1 row affected (0.00 sec)

MySQL [(none)]> use web_page_status;
Database changed
MySQL [web_page_status]> create table status(status VARCHAR(50) NOT NULL, timestamp DATE NOT NULL);
Query OK, 0 rows affected (0.02 sec)

MySQL [web_page_status]> show tables;
+-----+
| Tables_in_web_page_status |
+-----+
| status                     |
+-----+
1 row in set (0.00 sec)

MySQL [web_page_status]> exit
Bye

```

- Logged in to the RDS through mysql client and created the database and table. Values will be inserted in to the table during the execution of the script1. Password is stored in the .my.cnf file and read/write permission changed only to the owner.

S3 bucket creation with IAM role access for EC2

Amazon S3 Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name
awsassignmentlahiru
Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region
US East (N. Virginia) us-east-1

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)

Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**

- AWS provides a wide range of storage solutions like Amazon S3, Cloudfront, EFS, EBS, glacier and storage gateway. All these solutions serve different purposes and has different costing architectures. Therefore, simple object-based storage solution which is known as S3 bucket is ideal for this solutions to store the logs. It operates independent and can be easily accessed through IAM roles.

Identity and Access Management (IAM)

Roles

What are IAM roles?
IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

[Create role](#) [Delete role](#)

Q Search

Role name	Trusted entities	Last activity
<input type="checkbox"/> AWSServiceRoleForRDS	AWS service: rds (Service-Linked role)	2 days
<input type="checkbox"/> AWSServiceRoleForSupport	AWS service: support (Service-Linked role)	None
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	AWS service: trustedadvisor (Service-Linked ...)	None
<input type="checkbox"/> rds-monitoring-role	AWS service: monitoring rds	Yesterday

- Access can be granted to the S3 bucket by assigning the IAM role to the instance or users.

aws Services

Search for services, features, marketplace products, and docs [Alt+S]

Create role

1 2 3 4

Select type of trusted entity

AWS service
 EC2, Lambda and others

Another AWS account
 Belonging to you or 3rd party

Web identity
 Cognito or any OpenID provider

SAML 2.0 federation
 Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway	CodeBuild	EMR	IoT SiteWise	RDS
AWS Backup	CodeDeploy	EMR Containers	IoT Things Graph	Redshift
AWS Chatbot	CodeGuru	ElastiCache	KMS	Rekognition
AWS Marketplace	CodeStar Notifications	Elastic Beanstalk	Kinesis	RoboMaker
AWS Support	Comprehend	Elastic Container Registry	Lake Formation	S3
Amplify	Config	Elastic Container Service	Lambda	SMS

- Two use cases provided as the options to select to create the IAM role. Monitoring node needs access to the S3 bucket to push the log files. That requires the EC2 instance to access the S3 bucket using IAM role.

Search for services, features, marketplace products, and docs [Alt+S]

Create role

1 2 3 4

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies Showing 8 results

	Policy name	Used as
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	None
<input checked="" type="checkbox"/>	AmazonS3FullAccess	None
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	None
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	None
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	None
<input type="checkbox"/>	IVSRecordToS3	None
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	None
<input type="checkbox"/>	S3StorageLensServiceRolePolicy	None

Set permissions boundary

* Required

Cancel Previous **Next: Tags**

- Full access to S3 bucket is granted to the IAM role that is being created.

1 2 3 4

Create role

- Instances (1/1) [Info](#)

Instance state: running

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm
<input checked="" type="checkbox"/>	-	i-0983f34880a0991f4	Running	t2.micro	2/2 checks passed	No alarm

Actions

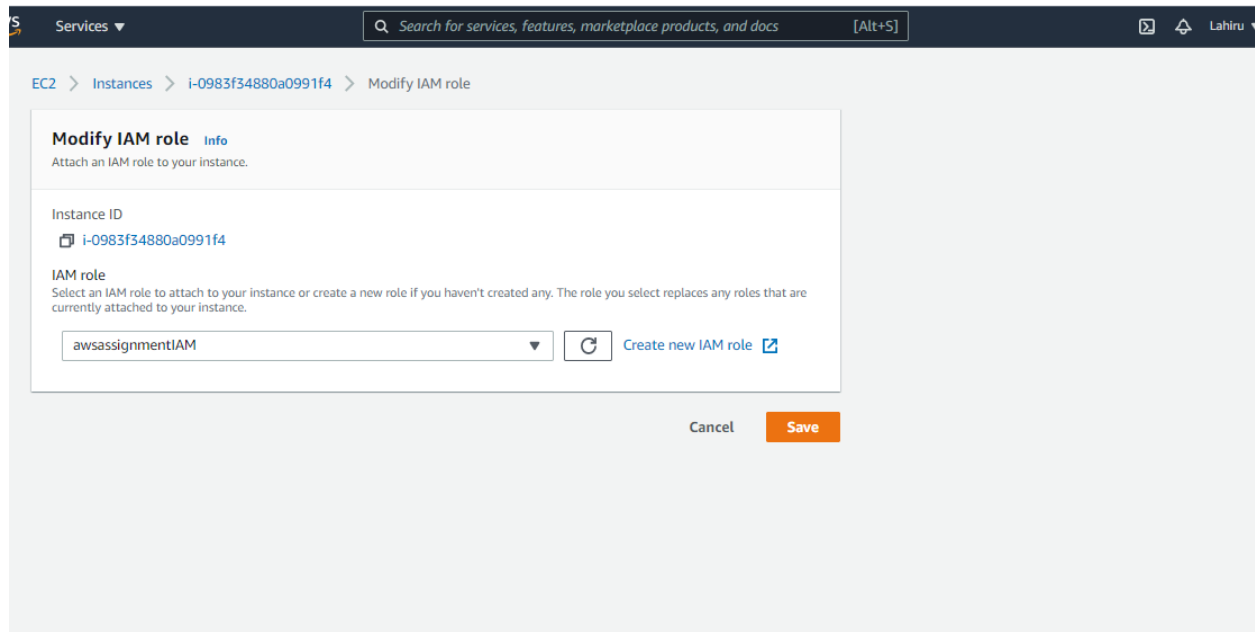
 - Connect
 - View details
 - Manage instance state
 - Instance settings
 - Networking
 - Security
 - Image and templates
 - Monitor and troubleshoot

Change security groups

Get Windows password

Modify IAM role

Instance: i-0983f34880a0991f4



- Final step is to apply the IAM role to the monitoring instance

Setting up the monitoring instance.

```
[centos@ip-172-31-37-229 ~]$ sudo yum install postfix
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: d36uatko69830t.cloudfront.net
 * extras: d36uatko69830t.cloudfront.net
 * updates: d36uatko69830t.cloudfront.net
Resolving Dependencies
--> Running transaction check
--> Package postfix.x86_64 2:2.10.1-9.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved
```

Package	Arch	Version	Repository	Size
Installing: postfix	x86_64	2:2.10.1-9.el7	base	2.4 M

Transaction Summary

Install 1 Package

Total download size: 2.4 M

Installed size: 12 M

Is this ok [y/d/N]:

```
[centos@ip-172-31-37-229 ~]$ sudo yum install mailx
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: d36uatko69830t.cloudfront.net
 * extras: d36uatko69830t.cloudfront.net
 * updates: d36uatko69830t.cloudfront.net
Resolving Dependencies
--> Running transaction check
--> Package mailx.x86_64 0:12.5-19.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved
```

Package	Arch	Version	Repository	Size
Installing: mailx	x86_64	12.5-19.el7	base	245 k

Transaction Summary

Install 1 Package

Total download size: 245 k

- The monitoring instance need to send emails to an external party (application support team). Therefore, the mailx and postfix packages installed in order to do the email configurations.

```
relayhost = [smtp.gmail.com]:587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_tls_security_level = encrypt
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
inet_protocols = ipv4
~
~
~
~
~
~
~
```

- Main configurations for the postfix. SMTP relay is useful in forwarding the email rather than maintaining a mail server. Therefore, relayhost is given as smtp.gmail.com which is provided by the gmail. Credentials are saved in the /etc/postfix/sasl_passwd file.

```
[smtp.gmail.com]:587 alerts.aws.assignment@gmail.com: [REDACTED]  
~  
~
```

- Sender email address and the password is stored in the file

```
[centos@ip-172-31-30-246 ~]$ sudo postmap /etc/postfix/sasl_passwd  
[centos@ip-172-31-30-246 ~]$ ll /etc/postfix/sasl_passwd.db  
-rw-----. 1 root root 12288 Apr 29 18:07 /etc/postfix/sasl_passwd.db  
[centos@ip-172-31-30-246 ~]$
```

- Run `postmap /etc/postfix/sasl_passwd` command and restart the postfix service

Setting up the environment - Instructions.

1. Run the cloudformation script in https://gitlab.com/lahirumal/aws_assignment
2. Since cloudformation script uses private AMIs and the AMI ID values in the environment.json file must be changed in order to execute under a different AWS account.
3. Install httpd in the web instances using 'yum install httpd'
4. Install postfix and mailx using 'yum install postfix' and 'yum install mailx' in monitoring instance.
5. Copy the configuration files as provided in the folder to the required locations as mentioned below.
 - a. .my.cnf -> /home/centos/.my.cnf in Monitoring server (AMI)
 - b. assignment.com.conf -> /etc/httpd/conf.d/assignment.com.conf in web instances (AMI)
 - c. httpd.conf -> /etc/httpd/conf/httpd.conf in web instances (AMI)
 - d. main.cf -> /etc/postfix/main.cf in Monitoring server (AMI)
 - e. sasl_password -> /etc/postfix/sasl_passwd (Run postmap /etc/postfix/sasl_passwd) in Monitoring server (AMI)
 - f. script1.sh -> /home/centos/script1.sh
 - g. script2.sh -> /home/centos/script2.sh
6. Both the scripts are recommended to be copied to a home folder of the user (centos) that the scripts are being executed and the below contrab entries must be placed under the particular user in each server
 - a. Web application nodes.
 - i. 59 23 * * * sh /home/centos/log_rotate.sh > /dev/null 2>&1
 - ii. 00 08 * * 1-5 sudo /bin/systemctl start httpd.service > /dev/null 2>&1
 - iii. 00 16 * * 1-5 sudo /bin/systemctl stop httpd.service > /dev/null 2>&1
 - b. Monitoring node (Based on the time interval to execute the periodic check and log extraction – every 30 minutes).
 - i. */30 * * * * sh /home/centos/script1.sh > /dev/null 2>&1
 - ii. 00 00 * * * * sh /home/centos/script2.sh > /dev/null 2>&1
7. It is recommended to create two AMIs using the above steps and then pass the AMI IDs to the cloudformation script which will automate the process. Before executing the cloudformation script, an IAM role with the name 'awsassignmentIAM' needed to be created with the below policies.
 - a. AutoScalingReadOnlyAccess
 - b. AmazonS3FullAccess
 - c. EC2InstanceConnect
8. SSH key pair needed to be created in the name "AWS_Assignment_AMI" in order to access the servers via ssh. Key will be applied to each instances via the cloudformation script.
9. Once everything is ready execute the below command to create the cloudformation stack using the cloudformation.yaml and environment.json file in the local PC.
 - a. aws cloudformation create-stack --stack-name startmyinstance --template-body file://cloudformation.yaml --parameters <file:///environment.json>

Limitations and Suggestions

- Public DNS is suggested to be used for the web application. Currently the end point of the load balancer is hard coded .
 - Eg - `http://startmyin-loadbala-641fppoj4jun-781586019.us-east-1.elb.amazonaws.com`
- SSL certificate can be installed at the load balancer level will provide more security to the web application.
- Private DNS can be used for the MySQL RDS to connect from the monitoring instance. Currently the end point is hard coded into the script.
 - Eg - `lseg-rds.crdxxeqjw7mf.us-east-1.rds.amazonaws.com`
- Resources with least costs were used in the solution and therefore the better performance, security and logging features provided by AWS are not used.

Output of the solution.



- Web page is loading from the web application.

```
[centos@ip-10-192-21-42 aws_assignment]$ ls
error.log  error.log_ip-10-192-21-42.ec2.internal_043021  public_html  requests.log  requests.log_ip-10-192-21-42.ec2.internal_043021
[centos@ip-10-192-21-42 aws_assignment]$
```

```
[centos@ip-10-192-20-85 aws_assignment]$ ls
error.log  error.log_ip-10-192-20-85.ec2.internal_043021  public_html  requests.log  requests.log_ip-10-192-20-85.ec2.internal_043021
[centos@ip-10-192-20-85 aws_assignment]$
```

- Logs are rotated in the web server instances.

```
[centos@ip-10-192-10-155 ~]$ ls
script1.log  script1.sh  script2.log  script2.sh
[centos@ip-10-192-10-155 ~]$ cat script1.log

04/30/21 03:00:11 Web service is up
04/30/21 03:00:11 Script_1 successfully executed
04/30/21 03:00:12 Web service is up
04/30/21 03:00:12 Script_1 successfully executed
[centos@ip-10-192-10-155 ~]$
```

- Script 1 is getting successfully executed at both web instances.

```

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 217
Server version: 8.0.20 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> use web_page_status;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [web_page_status]> select * from status_log
-> ;
+-----+-----+
| status | timestamp |
+-----+-----+
| success | 04/30/21 03:00:11 |
| success | 04/30/21 03:00:12 |
+-----+-----+
2 rows in set (0.01 sec)

MySQL [web_page_status]> █

```

- Database is getting updated successfully.

```

[centos@ip-10-192-10-155 ~]$ ls
10.192.20.85_index.html 10.192.21.42_index.html script12.log script1.log script1.sh script2.log script2.sh
[centos@ip-10-192-10-155 ~]$ ./script2.sh
EC2 Instance IPs
10.192.21.42 10.192.20.85
index.html
error_log_ip-10-192-21-42.ec2.internal_043021 100% 124 91.3KB/s 00:00
requests_log_ip-10-192-21-42.ec2.internal_043021 100% 1638 738.1KB/s 00:00
upload_0430210312.tar.gz to s3://awsassignmentseg/upload_0430210312.tar.gz 100% 1638 669.5KB/s 00:00
index.html
error_log_ip-10-192-20-85.ec2.internal_043021 100% 124 166.5KB/s 00:00
requests_log_ip-10-192-20-85.ec2.internal_043021 100% 223KB 29.6MB/s 00:00
upload_0430210312.tar.gz to s3://awsassignmentseg/upload_0430210312.tar.gz 100% 223KB 30.2MB/s 00:00
[centos@ip-10-192-10-155 ~]$ cat script2.log
04/30/21 03:12:12 Script_2 successfully executed
04/30/21 03:12:12 Script_2 successfully executed
[centos@ip-10-192-10-155 ~]$ █

```

- Script2 getting successfully executed.


Amazon S3 > awsassignmentseg

awsassignmentseg

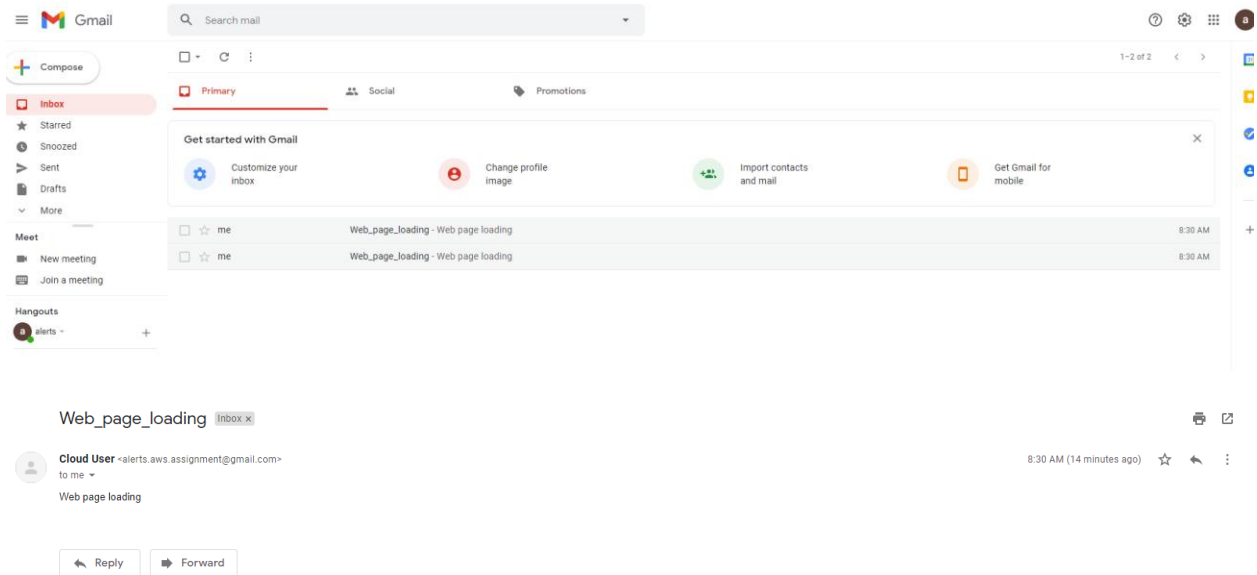
Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	 upload_0430210312.tar.gz	gz	April 30, 2021, 08:42:16 (UTC+05:30)	19.7 KB	Standard

- Compressed file is successfully uploaded in to the S3 bucket.



- Email notifications are sent to the alerts inbox for both web instances.

Scripts

Scripts are available at https://gitlab.com/lahirumal/aws_assignment as well.

1. Cloudformation.yaml
2. Environment.json
3. Script1.sh
4. Script2.sh