

AWS Project Screenshots

Samuel Diaz

MIS 690: Cloud Computing

San Diego State University

November 01, 2024

Table of Contents

A. AWS IAM (Identity and Access Management)	3
i. Create ‘Admin’ User.....	3
ii. Setup MFA For Root User	6
iii. Setup MFA for Admin Account.....	8
iv. Create ‘Developer’ User	10
v. Create ‘Auditor’ Role	12
vi. Create ‘ReadOnlyBilling’ Role	14
B. Amazon S3 (Simple Storage Service)	16
i. Host the Website for Public Access.....	16
ii. Enable Bucket Versioning.....	20
iii. Enable Lifecycle Policies	21
iv. Create Encrypted Bucket to Store CloudTrail Logs.....	23
C. Route 53.....	25
i. Register Domain Name	25
ii. Redirect custom URL (samueldiaz.tech) to S3 bucket.....	28
D. AWS CloudTrail	30
i. Enable Website Monitoring and Analytics (With Encryption)	30
ii. Move CloudTrail to an Encrypted Bucket.....	32
E. AWS Key Management Service (KMS).....	34
i. Verify the Creation of the CloudTrail Key	34

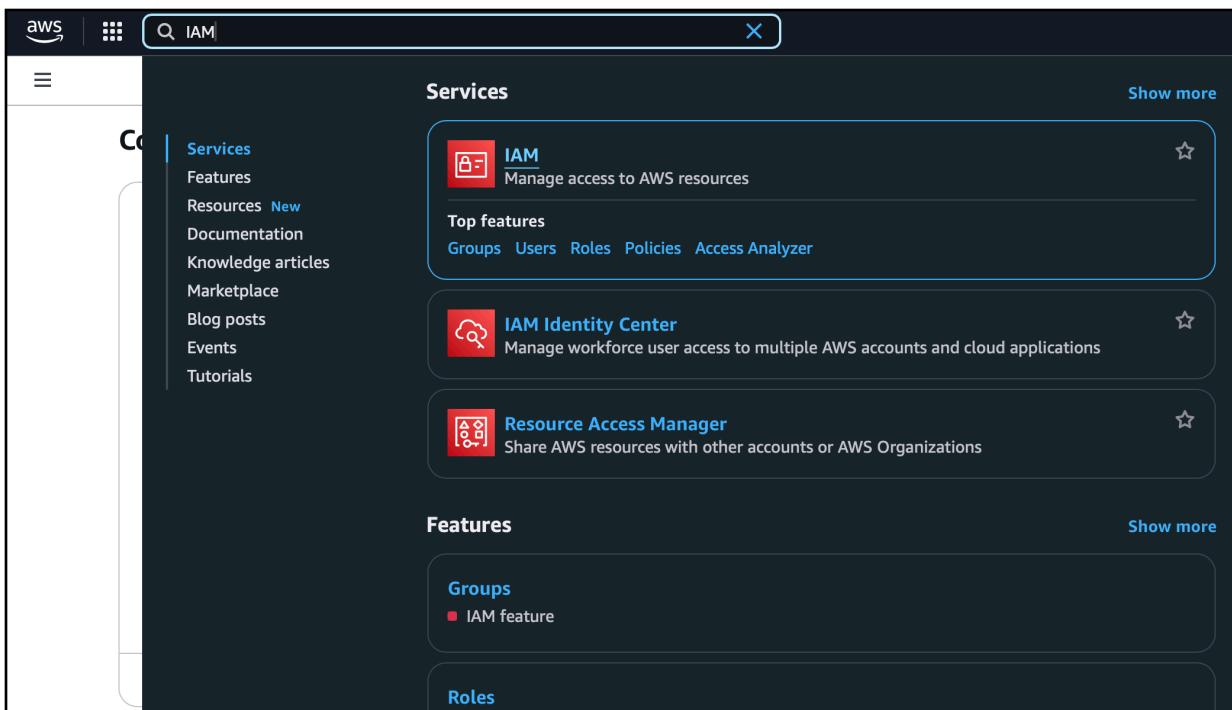
A. AWS IAM (Identity and Access Management)

i. Create ‘Admin’ User

Reasoning: The root user has unrestricted access to all AWS services and resources in the account. If the credentials were compromised, the attacker would have complete control over all resources through my AWS account. These can be a breach of confidentiality and availability, leading to significant financial or data loss. Therefore, it is best to restrict the use of the root account for only initial setup and critical administrative tasks.

Steps:

1. AWS Homepage > Search bar > type and select ‘IAM’



2. Access Management > Users > ‘Create User’

The screenshot shows the AWS IAM 'Users' page. At the top, it says 'Users (0) Info'. Below that, a note states: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' A search bar is present. The main area has a table header with columns: 'User name' (sorted by ascending), 'Path', 'Groups' (sorted by descending), 'Last activity' (sorted by descending), 'MFA' (sorted by descending), 'Password age' (sorted by descending), and 'Console last sign-in'. A message 'No resources to display' is centered below the table. At the top right, there are buttons for 'Delete' (with a trash icon) and 'Create user' (in orange).

3. Specify user details > Username > ‘Admin’ > check ‘Provide user access to the AWS Management Console - optional’ > select ‘I want to create an IAM user’ > Console password > Custom password > type in temporary password > ‘Click next’

The screenshot shows the 'Specify user details' step of a wizard. In the 'User details' section, the 'User name' is set to 'Admin'. A checkbox 'Provide user access to the AWS Management Console - optional' is checked. Below it, a note says: 'If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.' Under 'User type', the 'I want to create an IAM user' option is selected. A note says: 'We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keypairs, or a backup credential for emergency account access.' In the 'Console password' section, the 'Custom password' option is selected. A password field contains '*****'. A checkbox 'Show password' is present. A note at the bottom says: 'We recommend that users must create a new password at next sign-in - Recommended.'

4. Set Permissions > 'Attach Policies Directly' > Permission policies > search 'admin' > select 'AdministratorAccess' > Click next

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1289)

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

Filter by Type			
Policy name	Type	Attached entities	
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	0	
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	0	
<input type="checkbox"/> AdministratorAccess-AWSElas...	AWS managed	0	
<input type="checkbox"/> AmazonAPIGatewayAdministr...	AWS managed	0	
<input type="checkbox"/> AmazonNimbleStudio-Studio...	AWS managed	0	
<input type="checkbox"/> AmazonSageMakerAdmin-Ser...	AWS managed	0	

5. Review and verify details > Select 'Create User'

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name Admin	Console password type Custom password	Require password reset Yes
--------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

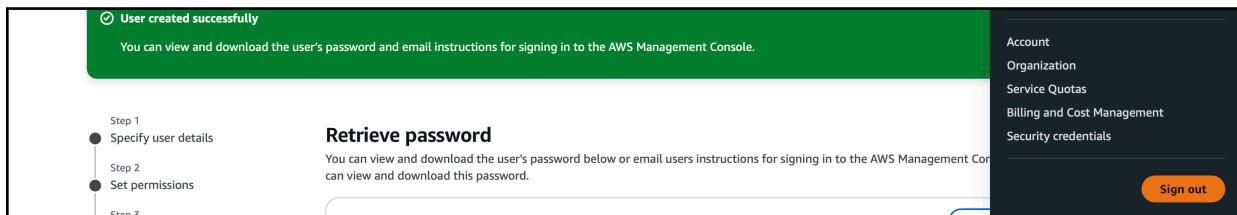
No tags associated with the resource.

[Add new tag](#)

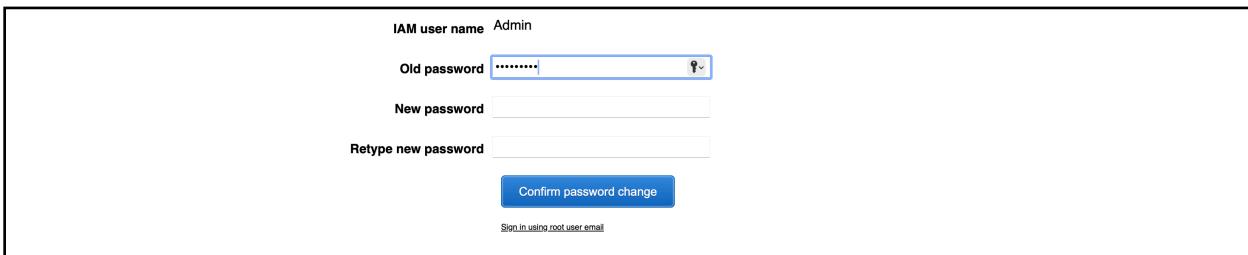
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

6. On drop-in page > Copy the Console sign-in URL > From top right, select account dropdown > click 'Sign out'



7. Paste the provided sign in link into a web browser > sign-in with the Admin credentials you created > You will be prompted to change your password > Confirm password change

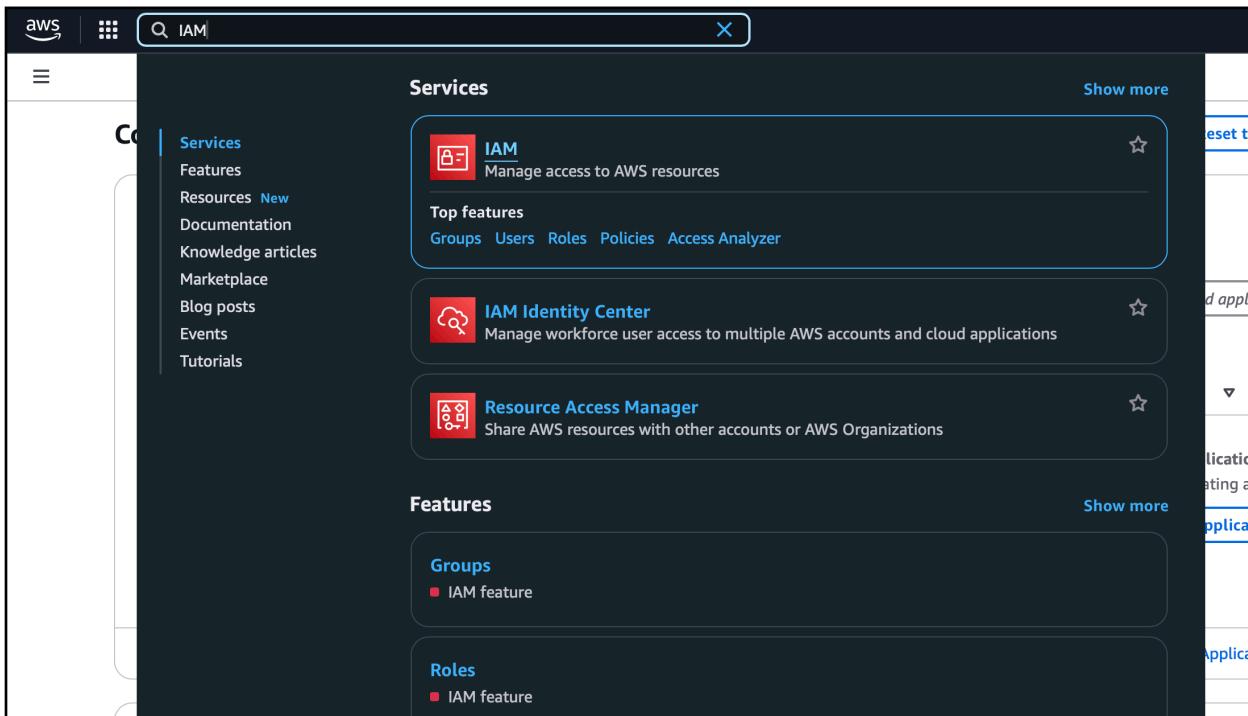


8. Successfully created and logged into Admin account.

ii. Setup MFA For Root User

Reasoning: MFA adds an additional layer of protection to accounts by requiring both 'something you know', your password and 'something you are', the passkey (finger or face to unlock).

1. As root user > AWS Homepage > Search bar: type and select 'IAM'



2. IAM Dashboard > Security Recommendations > 'Add MFA'

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with partially visible text: "d Access nt (IAM)", "e gement", "ers", "gs", "anagement New", "ts", "r", "cess", and "ess". The main content area has a header "IAM Dashboard" with an "Info" link. Below it is a section titled "Security recommendations" with a red box containing the number "1". It lists two items: "Add MFA for root user" (with a warning icon) and "Root user has no active access keys" (with a checkmark icon). A blue button labeled "Add MFA" is on the right. Another blue button with a circular arrow icon is at the top right. Below this is a section titled "IAM resources" with a blue circular icon. It shows resource counts: User groups (0), Users (1), Roles (2), Policies (0), and Identity providers (0). At the bottom, there's a "What's new" section with a blue circular icon and a "View all" link.

3. Select MFA device > Device Name: type 'my_passkey' > MFA device: select 'Passkey or security key' > Next

Step 1

Select MFA device

Step 2

Set up device

Select MFA device Info

MFA device name

Device name
This name will be used within the identifying ARN for this device.

Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

Device options
In addition to username and password, you will use this device to authenticate into your account.



Passkey or security key
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.



Authenticator app
Authenticate using a code generated by an app

4. Follow the instructions (place fingerprint or use face unlock) > you have successfully setup MFA for root user.

My security credentials Root user Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types used, see [AWS Security Credentials](#) in AWS General Reference

Account details	
Account name sdiaz	Email address samdiaz1100@gmail.com

[Edit account](#)

iii. Setup MFA for Admin Account

1. Similar to root user: IAM Dashboard > Security Recommendations > ‘Add MFA’

IAM Dashboard Info

Security recommendations 1 C

- ✓ Root user has MFA**
Having multi-factor authentication (MFA) for the root user improves security for this account.
- ⚠ Add MFA for yourself** Add MFA
Add multi-factor authentication (MFA) for yourself to improve security for this account.
- ✓ Your user, Admin, does not have any active access keys that have been unused for more than a year.**
Deactivating or deleting unused access keys improves security.

IAM resources C

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity
-------------	-------	-------	----------	----------

2. Select MFA device > Device Name: type 'my_passkey_admin' > MFA device: select 'Passkey or security key' (Note: ensure passkey is different from root user's) > Next

The screenshot shows the 'Select MFA device' step of a two-step process. Step 1 is 'Select MFA device' (selected), and Step 2 is 'Set up device'. The main area is titled 'MFA device name' with a sub-section 'Device name'. It says 'This name will be used within the identifying ARN for this device.' A text input field contains 'icloud_passkey_admin'. Below it, a note states 'Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.' The next section is 'MFA device' with 'Device options'. It says 'In addition to username and password, you will use this device to authenticate into your account.' A blue box highlights the 'Passkey or security key' option, which is described as 'Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.' Icons for a person, a key, and a biometric sensor are shown.

3. Follow the instructions (place fingerprint or use face unlock) > you have successfully setup MFA for admin user account.

The screenshot shows the 'My security credentials' page in the AWS IAM console. The left sidebar has a 'Search IAM' bar and links for 'Dashboard' and 'Access management'. The main content area is titled 'My security credentials' with a sub-section 'Account details'. It shows the 'User name' as 'Admin'.

iv. Create ‘Developer’ User

1. IAM > Access management > Users > Create user

The screenshot shows the AWS IAM 'Users' list. There is one user entry: 'Admin'. The 'User name' column shows 'Admin'. The 'Path' column shows '/'. The 'Groups' column shows '0'. The 'Last activity' column shows '9 hours ago'. The 'MFA' column shows '0'. The 'Password age' column shows '2 days'. The 'Console last sign-in' column shows 'November 29, 2024, 1...'. At the top right, there are 'Delete' and 'Create user' buttons.

2. Users > Specify user details > User name: type ‘Developer’ > Next

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. On the left, a sidebar shows 'Step 1 Specify user details' (selected), 'Step 2 Set permissions', and 'Step 3 Review and create'. The main area is titled 'Specify user details' and contains a 'User details' section. The 'User name' field is filled with 'Developer'. A note below it says: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)'. There is an optional checkbox 'Provide user access to the AWS Management Console - optional' with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' A callout box at the bottom right says: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user. Learn more'. At the bottom right are 'Cancel' and 'Next' buttons.

3. Set Permissions > Permission options > Attach policies directly > Permission Policies: select 'AmazonS3FullAccess' and 'AmazonEC2FullAccess' > Next

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- Add user to group Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (2/1290)

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

Filter by Type																					
<input type="text" value="AmazonS"/>	<input type="button" value="X"/>	All types	60 matches																		
<input type="checkbox"/> Policy name ▾ <table border="1"> <thead> <tr> <th>Policy name</th> <th>Type</th> <th>Attached entities</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> AmazonS3FullAccess</td> <td>AWS managed</td> <td>0</td> </tr> <tr> <td><input type="checkbox"/> AmazonS3ObjectLambdaExec...</td> <td>AWS managed</td> <td>0</td> </tr> <tr> <td><input type="checkbox"/> AmazonS3OutpostsFullAccess</td> <td>AWS managed</td> <td>0</td> </tr> <tr> <td><input type="checkbox"/> AmazonS3OutpostsReadOnly...</td> <td>AWS managed</td> <td>0</td> </tr> <tr> <td><input type="checkbox"/> AmazonS3ReadOnlyAccess</td> <td>AWS managed</td> <td>0</td> </tr> </tbody> </table>				Policy name	Type	Attached entities	<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	0	<input type="checkbox"/> AmazonS3ObjectLambdaExec...	AWS managed	0	<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	0	<input type="checkbox"/> AmazonS3OutpostsReadOnly...	AWS managed	0	<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	0
Policy name	Type	Attached entities																			
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	0																			
<input type="checkbox"/> AmazonS3ObjectLambdaExec...	AWS managed	0																			
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	0																			
<input type="checkbox"/> AmazonS3OutpostsReadOnly...	AWS managed	0																			
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	0																			

4. Review and Create > Verify permissions > Create User

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name Developer	Console password type None	Require password reset No
------------------------	-------------------------------	------------------------------

Permissions summary

Name ▾	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

5. Successful creation of Developer user.

The screenshot shows the AWS IAM 'Users' page. A success message at the top states 'User created successfully' with a note: 'You can view and download the user's password and email instructions for signing in to the AWS Management Console.' Below this, a table lists two users: 'Admin' and 'Developer'. The 'Developer' row includes a 'Create user' button. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and other IAM features.

v. Create 'Auditor' Role

1. IAM > Access management > Users > Create role

The screenshot shows the AWS IAM 'Roles' page. A success message at the top states 'Role created successfully' with a note: 'You can view and download the role's ARN and assume role instructions for using the role with AWS services.' Below this, a table lists three roles: 'AWSAdministratorAccess', 'AWSLambdaBasicExecutionRole', and 'AmazonS3FullAccess'. The 'AmazonS3FullAccess' row includes a 'Create role' button. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and other IAM features. At the bottom, there are sections for 'Roles Anywhere' and 'Temporary credentials'.

2. Select trusted entity > Trusted entity type: select ‘AWS account’ > An AWS Account > ‘This account’ > Next

Select trusted entity

Trusted entity type

- AWS service
- AWS account
- SAML 2.0 federation
- Web identity

An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- This account (140023363345)
- Another AWS account

Options

- Require external ID (Best practice when a third party will assume this role)
- Require MFA
Requires that the assuming entity use multi-factor authentication.

Cancel **Next**

3. Add Permissions > Permission policies > ‘AWSCloudTrail_ReadOnlyAccess’

Add permissions

Permissions policies (1/999)

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

Policy name	Type	Description
<input type="checkbox"/> AWSCloudTrail_FullAccess	AWS managed	Provides full access to AWS CloudTrail.
<input checked="" type="checkbox"/> AWSCloudTrail_ReadOnlyAccess	AWS managed	Provides read only access to AWS Clou...

Set permissions boundary - optional

Cancel **Previous** **Next**

4. Role name > ‘Auditor’ > Description: type ‘Grants read-only access to CloudTrail logs. Useful for auditors who need to review user activity and API logs for compliance or security analysis.’ > Create role

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=., @-_`^#\$%^&*%;`

Cancel **Previous** **Next**

vi. Create 'ReadOnlyBilling' Role

1. IAM > Access management > Users > Create role
2. Select trusted entity > Trusted entity type > 'AWS account' > An AWS Account > 'This account' > Next

The screenshot shows the 'Select trusted entity' step of the IAM Role creation wizard. On the left, a sidebar lists steps: Step 1 (Select trusted entity, which is selected), Step 2 (Add permissions), and Step 3 (Name, review, and create). The main area is titled 'Select trusted entity' with a 'Info' link. It shows the 'Trusted entity type' section with four options: 'AWS service' (radio button not selected), 'AWS account' (radio button selected), 'SAML 2.0 federation' (radio button not selected), and 'Custom trust policy' (radio button not selected). Below this, the 'An AWS account' section is shown, with the 'This account (140023363345)' option selected. Under 'Options', there are two checkboxes: 'Require external ID' (unchecked) and 'Require MFA' (unchecked). At the bottom right are 'Cancel' and 'Next' buttons.

3. Add Permissions > Permission policies: select 'AWSBillingReadOnlyAccess'

The screenshot shows the 'Add permissions' step of the IAM Role creation wizard. On the left, a sidebar lists steps: Step 1 (Select trusted entity), Step 2 (Add permissions, which is selected), and Step 3 (Name, review, and create). The main area is titled 'Add permissions' with a 'Info' link. It shows the 'Permissions policies (1/999)' section with a search bar containing 'billin'. A table lists four policies: 'AWSBillingConductorFullAccess' (unchecked), 'AWSBillingConductorReadOnlyAccess' (unchecked), 'AWSBillingReadOnlyAccess' (checked and highlighted with a blue border), and 'Billing' (unchecked). The table includes columns for 'Policy name', 'Type', and 'Description'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

4. Role details > Role name: type ‘ReadOnlyBilling’ > Description: type ‘Grants read-only access to CloudTrail logs. Useful for auditors who need to review user activity and API logs for compliance or security analysis.’ > Create role

The screenshot shows the 'Name, review, and create' step of the AWS IAM 'Create role' wizard. The left sidebar shows three steps: 'Select trusted entity' (Step 1), 'Add permissions' (Step 2), and 'Name, review, and create' (Step 3, currently selected). The main area is titled 'Role details'. It contains fields for 'Role name' (ReadOnlyBilling) and 'Description' (Grants read-only access to CloudTrail logs. Useful for auditors who need to review user activity and API logs for compliance or security analysis.). Below these fields is a 'Trust policy' section with a JSON code editor:

```
1 - {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "sts:AssumeRole",  
7     }  
8   ]  
9 }
```

B. Amazon S3 (Simple Storage Service)

i. Host the Website for Public Access

1. AWS Homepage > Search bar: type and select ‘S3’

The screenshot shows the AWS homepage with a search bar at the top containing 'S3'. Below the search bar, there's a sidebar with links like 'Services', 'Features', 'Resources', etc. The main content area is titled 'Services' and lists several services: S3 (Scalable Storage in the Cloud), S3 Glacier (Archive Storage in the Cloud), AWS Snow Family (Large Scale Data Transport), and Storage Gateway (Hybrid Storage Integration). There are also sections for 'Features' (Imports from S3, Feature spotlight) and 'Show more' buttons.

2. Amazon S3 > Buckets > ‘Create Bucket’

The screenshot shows the 'General purpose buckets' tab selected in the AWS S3 console. At the top, there's an 'Account snapshot - updated every 24 hours' section with a 'View Storage Lens dashboard' button. Below it, a search bar says 'Find buckets by name'. The main table header includes columns for 'Name', 'AWS Region', 'IAM Access Analyzer', and 'Creation date'. A message in the center of the page says 'No buckets' and 'You don't have any buckets.' with a 'Create bucket' button.

3. Region > Select closest region > Bucket name: 'samueldiaz.tech' > scroll down > uncheck 'Block Public Access settings for this bucket' > acknowledge the warning > Click submit

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (Ohio) us-east-2

Bucket type [Info](#)

- General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
- Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)
Format: s3://bucket/prefix

Object Ownership

[Info](#)
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

- ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

4. Amazon S3 > Buckets > 'samueldiaz.tech'

Account snapshot - updated every 24 hours [All AWS Regions](#) [View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets		Directory buckets								
General purpose buckets (1) Info All AWS Regions										
Buckets are containers for data stored in S3.										
<input type="text" value="Find buckets by name"/>										
<table border="1"> <thead> <tr> <th>Name</th> <th>AWS Region</th> <th>IAM Access Analyzer</th> <th>Creation date</th> </tr> </thead> <tbody> <tr> <td>samueldiaz.tech</td> <td>US East (Ohio) us-east-2</td> <td>View analyzer for us-east-2</td> <td>November 27, 2024, 14:55:33 (UTC-08:00)</td> </tr> </tbody> </table>			Name	AWS Region	IAM Access Analyzer	Creation date	samueldiaz.tech	US East (Ohio) us-east-2	View analyzer for us-east-2	November 27, 2024, 14:55:33 (UTC-08:00)
Name	AWS Region	IAM Access Analyzer	Creation date							
samueldiaz.tech	US East (Ohio) us-east-2	View analyzer for us-east-2	November 27, 2024, 14:55:33 (UTC-08:00)							
C Copy ARN Empty Delete Create bucket										
◀ 1 ▶ ⚙										

5. Objects > 'Upload'

Objects (0) [Info](#) [C](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

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](#)

No objects
You don't have any objects in this bucket.

[Upload](#)

6. 'Add folder' > *Locate and select folder with web content* > 'Upload'. The website data has been uploaded.

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

Files and folders (10 total, 5.0 MB)

All files and folders in this table will be uploaded.

Name	Folder	Type	Size
index.html	SamuelDiazPortfolio/	text/html	8.1 KB
styles.css	SamuelDiazPortfolio/css/	text/css	8.6 KB
script.js	SamuelDiazPortfolio/javascript/	application/x-javascript	229.0 B
email.png	SamuelDiazPortfolio/media/	image/png	6.6 KB
linkedin.png.webp	SamuelDiazPortfolio/media/	image/webp	6.3 KB
github.png	SamuelDiazPortfolio/media/	image/png	8.4 KB
SamuelDiazResumeSwe.pdf	SamuelDiazPortfolio/media/	application/pdf	98.2 KB
planning.jpeg	SamuelDiazPortfolio/media/	image/jpeg	1.1 MB
coding.jpeg	SamuelDiazPortfolio/media/	image/jpeg	1.8 MB
computer.jpeg	SamuelDiazPortfolio/media/	image/jpeg	2.0 MB

7. Amazon S3 > Buckets > '[samueldiaz.tech](#)' > 'Properties.' > Static website hosting > 'Edit'

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

[Edit](#)

S3 static website hosting
Disabled

8. Edit static website hosting > Static website hosting: select 'Enable' > Index Document: type 'index.html' > Save Changes

Edit static website hosting [Info](#)

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting
 Disable
 Enable

Hosting type
 Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
 Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

Index document
Specify the home or default page of the website.
index.html

Error document - optional
This is returned when an error occurs.
error.html

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#).

9. Buckets > 'samueldiaz.tech' > Permissions > Edit Bucket Policy > attach Policy (code below) > Save Changes

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN
 arn:aws:s3:::samueldiaz.tech

Policy

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "PublicReadGetObject",
6        "Effect": "Allow",
7        "Principal": "*",
8        "Action": [
9          "s3:GetObject"
10         ],
11        "Resource": [
12          "arn:aws:s3:::samueldiaz.tech/*"
13        ]
14      }
15    ]
16  }

```

Edit statement

Select a statement
Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

ii. Enable Bucket Versioning

Reasoning: Versioning has been activated for buckets to ensure that any modifications made are retrievable. Therefore, if modifications or updates cause issues, you are able backtrack to the state your website was previously on.

1. Amazon S3 > Buckets > 'samueldiaz.tech' > Properties > Bucket Versioning > Edit

The screenshot shows the 'Bucket Versioning' configuration page. At the top right is an 'Edit' button. Below it, the section title 'Bucket Versioning' is followed by a detailed description of what versioning does. Underneath, there's a 'Bucket Versioning' setting labeled 'Disabled'. A note about 'Multi-factor authentication (MFA) delete' follows, mentioning it's disabled and providing a link to learn more. The entire page has a light gray background with rounded corners on the main content area.

2. Edit Bucket Versioning > Bucket Versioning > Enable > Save Changes

This screenshot shows the 'Edit Bucket Versioning' dialog. It includes a 'Bucket Versioning' section with a detailed description and an 'Info' link. Below it is a 'Bucket Versioning' setting where 'Enable' is selected (indicated by a blue circle). A note below says 'After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.' At the bottom, there are 'Cancel' and 'Save changes' buttons. The overall design is clean with white backgrounds and blue highlights for interactive elements.

3. Bucket Versioning has now been enabled

The screenshot shows the 'Bucket Versioning' configuration page again, but this time the 'Bucket Versioning' setting is labeled 'Enabled'. The rest of the page content, including the description and the 'Multi-factor authentication (MFA) delete' note, remains the same. The 'Edit' button is visible at the top right.

iii. Enable Lifecycle Policies

1. S3 > Buckets > 'samueldiaz.tech' > Management > Lifecycle rules > Create lifecycle rule

The screenshot shows the AWS S3 console with the 'samueldiaz.tech' bucket selected. The 'Management' tab is active. Under the 'Lifecycle rules' section, there is a message: 'Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time.' Below this is a table header with columns: Lifecycle rule n..., Status, Scope, Current version ..., Noncurrent ver..., Expired object ..., and Incomplete mu...'. A message below the table states 'No lifecycle rules' and 'There are no lifecycle rules for this bucket.' A blue 'Create lifecycle rule' button is located at the bottom of the table area.

2. Create lifecycle rule > Lifecycle rule name: type 'DefaultLifecycle' > Chose a rule scope: select 'Apply to all objects in the bucket' > check 'I acknowledge that this rule...' > Lifecycle rule actions: select 'Permanently delete concurrent versions of objects'

The screenshot shows the 'Create lifecycle rule' wizard. Step 1: Lifecycle rule configuration. It shows the 'Lifecycle rule name' field set to 'DefaultLifecycle'. The 'Choose a rule scope' section has the radio button 'Apply to all objects in the bucket' selected. A note below says: 'If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". [Learn more](#)' and 'I acknowledge that this rule will apply to all objects in the bucket' with a checked checkbox. Step 2: Lifecycle rule actions. It shows a list of actions: 'Transition current versions of objects between storage classes' (unchecked), 'Transition noncurrent versions of objects between storage classes' (unchecked), 'Expire current versions of objects' (unchecked), 'Permanently delete concurrent versions of objects' (checked), and 'Delete expired object delete markers or incomplete multipart uploads' (unchecked). A note below the last action says: 'These actions are not supported when filtering by object tags or object size.'

3. Permanently delete non-current versions of objects > Days after objects become concurrent: type '180' > Number of newer versions to retain - Optional: type '3' > Create rule

Amazon S3 > Buckets > samueldiaz.tech > Lifecycle configuration > Create lifecycle rule

Delete expired object delete markers or incomplete multipart uploads
These actions are not supported when filtering by object tags or object size.

Permanently delete noncurrent versions of objects
Choose when Amazon S3 permanently deletes specified noncurrent versions of objects. [Learn more](#)

Days after objects become noncurrent: 180

Number of newer versions to retain - Optional: 3
Can be 1 to 100 versions. All other noncurrent versions will be moved.

Review transition and expiration actions

Current version actions	Noncurrent versions actions
Day 0 No actions defined.	Day 0 • Objects become noncurrent
	↓
	Day 180 • 3 newest noncurrent versions are retained • All other noncurrent versions are permanently deleted

Create rule

4. Lifecycle rule has been created permanently deleting obsolete versions after 6 months. The top 3 most current versions would be kept, no matter the time elapsed

Lifecycle configuration [Info](#)

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules (1)

Lifecycle rule...	Status	Scope	Current versi...	Noncurrent ...	Expired obje...	Incomplete m...
DefaultLifecycle	Enabled	Entire bucket	-	Permanently delete	-	-

iv. Create Encrypted Bucket to Store CloudTrail Logs

1. Amazon S3 > Buckets > Create bucket > General configuration > Bucket name: type 'samuel diaz.tech-cloudtrail'

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (Ohio) us-east-2

Bucket type [Info](#)

General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)
`samuel diaz.tech-cloudtrail`

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

2. Block Public Access settings for this bucket: check 'Block All Public Access' > Default Encryption > Encryption Type: select 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' > Create bucket

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable

Enable

Advanced settings

[Info](#) After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

3. Verify creation of S3 bucket

The screenshot shows the AWS S3 buckets page. At the top, a green banner displays a success message: "Successfully created bucket 'samueldiaz.tech-cloudtrail'". Below the banner, there's an "Account snapshot" section with an "All AWS Regions" button and a "View Storage Lens dashboard" button. The main area is divided into "General purpose buckets" and "Directory buckets", with "General purpose buckets" being selected. A sub-header "General purpose buckets (2)" includes an "Info" button and an "All AWS Regions" button. A note states: "Buckets are containers for data stored in S3." Below this is a search bar labeled "Find buckets by name". A table lists the buckets:

Name	AWS Region	IAM Access Analyzer	Creation date
samueldiaz.tech	US East (Ohio) us-east-2	View analyzer for us-east-2	November 27, 2024, 14:55:33 (UTC-08:00)
samueldiaz.tech-cloudtrail	US East (Ohio) us-east-2	View analyzer for us-east-2	November 29, 2024, 20:26:39 (UTC-08:00)

Actions for each row include a circular icon, "Copy ARN", "Empty", "Delete", and "Create bucket". Navigation controls like arrows and a refresh icon are also present.

C. Route 53

i. Register Domain Name

1. AWS Homepage > Search bar: type and select ‘Route 53’

The screenshot shows the AWS search results page with 'Route 53' selected. The left sidebar includes links for Services, Features, Resources (New), Documentation, Knowledge articles, Marketplace, Blog posts, Tutorials, and Events. The main content area displays three services: 'Route 53' (Scalable DNS and Domain Name Registration), 'Route 53 Resolver' (Resolve DNS queries in your Amazon VPC and on-premises network), and 'Amazon Location Service' (Securely and easily add location data to applications). Below these are sections for 'Features' like 'Route 53 dashboard', 'Route 53 Resolver', and 'Query logging', each with a 'Route 53 feature' badge.

2. Get started > select Register a domain > click Get started

The screenshot shows the 'Get started' page in the AWS Route 53 console. It features a heading 'Get started' with an 'Info' link. Below it is a section titled 'Choose your starting point' with six options: 'Register a domain' (selected, showing a shield icon with a computer monitor and a checkmark), 'Transfer domain' (showing a computer monitor and a shield icon), 'Create hosted zones' (showing three shields connected by dashed lines), 'Configure health checks' (showing a shield icon with a heart rate monitor), 'Configure traffic flow' (showing a shield icon with a complex network diagram), and 'Configure resolvers' (showing a shield icon with a cloud and a database icon). At the bottom right are 'Cancel' and 'Get started' buttons.

3. Register domain > Search for domain: type and select 'samueldiaz.tech' > Proceed to checkout

Route 53 > Registered domains > Register domains

Register domains Info

Pricing for domain names varies by top-level domain (TLD). For more information, view [price with different TLDs](#).

Search for domain

Check availability for a domain

X
Search

Selected domains (0/5)

Search for domains and make a selection

Standard pricing

Pricing for domain names varies by top-level domain (TLD), such as .com or .org.

Search result

ⓘ **samueldiaz.com is not available**
See other available domains below.

Suggested available domains (10)
You can register up to five domains at a time.

Domain	Price/year	Actions
samueldiaz.net	15.00 USD	Select
samueldiaz.io	71.00 USD	Select
samueldiaz.co	31.00 USD	Select
camuel_diaz.com	14.00 USD	Select

4. *Verify pricing* > Next

Route 53 > Registered domains > Register domains > Checkout

Step 1 Pricing
 Step 2 Contact information
 Step 3 Review and submit

Pricing Info

Domain pricing options

Domain name	Duration (price)	Auto-renew
<input type="text" value="samueldiaz.tech"/>	<input type="button" value="1 year (40.00 USD)"/>	<input checked="" type="checkbox"/> On

ⓘ Auto-renew is turned on for 1 domain.
We will send an email to the registrant contact before expiration to remind you that auto-renew is currently turned on. You can turn it off at any time by using the Route 53 console. For more information, see [Renewing Registration for a Domain](#).

Subtotal: **40.00 USD**
Applicable taxes will be calculated at checkout.

[Cancel](#) Next

5. Verify contact information > Click Next

The screenshot shows the 'Contact information' step of a domain registration wizard. On the left, a vertical navigation bar lists steps: Step 1 (Pricing), Step 2 (Contact information, which is selected and highlighted in blue), Step 3 (Review and submit). The main area is titled 'Contact information' with a 'Info' link. It contains fields for 'Registrist contact' (General information, Contact type dropdown, Organization input field), 'First name' and 'Last name' (input fields), 'Email' (input field), and 'Phone number' (input field with a country code prefix '123' and number '3115550188'). A note below the phone number field states: 'Enter country code and phone number. Phone number can only contain digits and no spaces or hyphens.'

6. Terms and conditions > check 'I have read and agree...' > Click Submit

The screenshot shows the 'Terms and conditions' step. It features a heading 'Terms and conditions' and a detailed description of Amazon Route 53's domain registration services. Below the description is a checkbox statement: 'I have read and agree to the Amazon Route 53 Domain Name Registration End User Agreement. I also understand that domain operation charges are non-refundable, and I can't use AWS credits to pay for domain operation fees.' The checkbox is checked. At the bottom are three buttons: 'Cancel', 'Previous' (disabled), and 'Submit'.

7. Your domain name is registered and ready to use.

The screenshot shows a table of domain registration status. The columns are: Domain name, Message, Status, Type, and Submitted. The data row for 'samuelliaz.tech' shows: 'samuelliaz.tech', '-', 'In progress', 'Register domain', and 'November 27, 2024, 14:39 (UTC:-08:00)'. There are filter buttons at the top left ('Filter status' and 'Filter type') and an 'Actions' dropdown at the top right.

Domain name	Message	Status	Type	Submitted
samuelliaz.tech	-	In progress	Register domain	November 27, 2024, 14:39 (UTC:-08:00)

ii. Redirect custom URL (samueldiaz.tech) to S3 bucket

1. Route 53 > DNS Management > Hosted Zone

The screenshot shows the AWS Route 53 service dashboard. On the left, there's a navigation sidebar with various options like Dashboard, Hosted zones (which is selected and highlighted in blue), Health checks, Profiles, IP-based routing, Traffic flow, Domains, Resolver, and DNS Firewall. The main content area is titled "Hosted zones (1)". It displays a table with one row for the hosted zone "samueldiaz.tech". The columns in the table are Hosted zone name, Type, Created by, Record count, Description, and Hosted zone ID. The "samueldiaz.tech" entry has "Public" as its type, "Route 53" as its creator, a record count of 2, and a long Hosted zone ID. At the top right of the table, there are buttons for "View details", "Edit", "Delete", and "Create hosted zone". Below the table, there's a search bar labeled "Filter records by property or value". The bottom of the page includes standard AWS footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

2. Hosted zones > select 'samueldiaz.tech'

The screenshot shows the AWS Route 53 Dashboard. The main header says "Route 53 Dashboard". The dashboard is divided into several sections: "DNS management" (with 1 Hosted zone), "Traffic management" (with a "Create policy" button), "Availability monitoring" (with a "Create health check" button), and "Domain registration" (with 1 Domain). Each section has a brief description and a large blue number indicating the current count (e.g., 1 Hosted zone, 1 Domain).

3. Records > Create record

Public **samueldiaz.tech** Info

[Delete zone](#) [Test record](#) [Configure query logging](#)

▶ **Hosted zone details** [Edit hosted zone](#)

Records (2) Info [DNSSEC signing](#) [Hosted zone tags \(0\)](#)

Records (2) Info [Delete record](#) [Import zone file](#) **Create record**

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

Filter records by property or value [Type](#) [Routing p...](#) [Alias](#)

< 1 > | [⚙️](#)

4. Enable Alias > Route Traffic to: select ‘Alias to S3 website endpoint’ > select region where the website was hosted > select S3 endpoint (the bucket holding the website data) > Create records.

Create record Info

Quick create record [Switch to wizard](#)

Record 1 [Delete](#)

Record name Info subdomain samueldiaz.tech

Keep blank to create a record for the root domain.

Alias

Record type Info A – Routes traffic to an IPv4 address and some AWS resources

Route traffic to Info

Alias to S3 website endpoint s3-website.us-east-2.amazonaws.com

US East (Ohio)

s3-website.us-east-2.amazonaws.com

Routing policy Info Simple routing

Evaluate target health Yes

[Add another record](#)

[Cancel](#) **Create records**

D. AWS CloudTrail

i. Enable Website Monitoring and Analytics (With Encryption)

1. CloudTrail > Create a Trail > Trail name: type 'WebsiteTrail' > Storage location: select 'Use existing bucket' > Trail log bucket name: browse and select '[samueldiaz.tech](#)' > Log file SSE-KMS encryption: check 'enabled' >...

The screenshot shows the 'Choose trail attributes' step of the 'Create trail' wizard. On the left, there's a navigation sidebar with three steps: Step 1 (Choose trail attributes), Step 2 (Choose log events), and Step 3 (Review and create). The main area is titled 'Choose trail attributes' and contains several configuration sections:

- General details:** A note states that a trail created in the console is a multi-region trail. It includes a 'Trail name' field with 'WebsiteTrail' typed in, a note about character limits (3-128 characters), and a checkbox for enabling it for all accounts in the organization.
- Storage location:** Offers two options: 'Create new S3 bucket' (radio button) and 'Use existing S3 bucket' (radio button, selected), with a note about choosing an existing bucket for logs.
- Trail log bucket name:** A text input field with 'samueldiaz.tech' typed in, a clear button, and a 'Browse' button.
- Prefix - optional:** A text input field with 'prefix' typed in.
- Log file SSE-KMS encryption:** A section with a note about encryption being enabled by default, a checkbox for 'Enabled' (which is checked), and a note about creating or choosing an existing KMS key.

2.> AWS KMS alias: type 'WebsiteKMS' > Log file validation: check 'Enabled' > select 'Next'

The screenshot shows the 'AWS KMS alias' configuration step of the 'Create trail' wizard. It includes the following fields:

- Log file SSE-KMS encryption:** A section with a note about being enabled by default, a checked checkbox for 'Enabled', and a note about creating or choosing an existing KMS key.
- Customer managed AWS KMS key:** Radio buttons for 'New' (selected) and 'Existing'.
- AWS KMS alias:** A text input field with 'WebsiteKMS' typed in, with a note about the region requirement.
- Additional settings:** A section with a note about log file validation, a checked checkbox for 'Enabled', and a note about SNS notification delivery.
- CloudWatch Logs - optional:** A section with a note about CloudWatch Logs monitoring, a checkbox for 'Enabled' (unchecked), and a note about policy documents.
- Encrypt log files with SSE-KMS:** A note explaining that SSE-KMS encryption is set to Enabled by default and provides links to SSE-KMS and SSE-S3 encryption documentation.
- Log file SSE-KMS encryption:** A note explaining the encryption policy choice between New, Existing, and Enabled.
- CloudWatch Logs:** A note about CloudWatch Logs monitoring and policy documents.
- Policy document:** A note about manually editing the key policy.

3. Choose log events > Events: select ‘Management events’ and ‘Data events’

Choose log events

Events Info
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

Event type
Choose the type of events that you want to log.

Management events
Capture management operations performed on your AWS resources.

Data events
Log the resource operations performed on or within a resource.

Insights events
Identify unusual activity, errors, or user behavior in your account.

Network activity events
Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

4. Management events: check ‘Read’ and ‘Write’ > Next > Data events > Resource Type: select ‘S3’ > Log selector template > select ‘Log all events’ > Next

Management events Info
Management events show information about management operations performed on resources in your AWS account.

API activity
Choose the activities you want to log.

Read **Write**

Exclude AWS KMS events

Exclude Amazon RDS Data API events

5. Review and Create > review options and click ‘Create Trail’

ii. Move CloudTrail to an Encrypted Bucket

1. CloudTrail > Trails > WebsiteTrail > General Details > Edit

The screenshot shows the 'General details' section of the CloudTrail configuration. At the top right are 'Delete' and 'Stop logging' buttons. Below them is an 'Edit' button. The main area contains tabs for 'Trail logging', 'Trail log location', 'Log file validation', and 'SNS notification delivery'. The 'Trail log location' tab is currently selected.

2. General details > Storage location > Use existing S3 bucket > Browse > 'samueldiaz.tech-cloudtrail' > Choose > Save changes

This screenshot shows the 'Storage location' configuration for the CloudTrail. It includes fields for 'Trail name' (set to 'WebsiteTrail'), 'Enable for all accounts in my organization' (unchecked), and 'Storage location' options. Under 'Storage location', the 'Use existing S3 bucket' option is selected, pointing to the 'samueldiaz.tech-cloudtrail' bucket. Other options like 'Create new S3 bucket' are also shown. Below this, there are fields for 'Trail log bucket name' (set to 'samueldiaz.tech-cloudtrail') and 'Prefix - optional'.

3. Successfully moved CloudTrail logs to a private bucket ‘samueldiaz.tech-cloudtrail’ .

The screenshot shows the AWS S3 console interface for the bucket 'samueldiaz.tech-cloudtrail'. The 'Objects' tab is active, displaying one object named 'AWSLogs/'. The object is listed as a folder. The interface includes standard S3 actions like Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload. A search bar at the top allows finding objects by prefix. The table header for the object list includes columns for Name, Type, Last modified, Size, and Storage class.

Name	Type	Last modified	Size	Storage class
AWSLogs/	Folder	-	-	-

E. AWS Key Management Service (KMS)

i. Verify the Creation of the CloudTrail Key

Note: This step branches from the step ‘Enable Website Monitoring and Analytics (with Encryption)’ where you enabled CloudTrail with KMS.

1. AWS Homepage > Search bar: type and select ‘Key Management Service’

The screenshot shows the AWS search results page with the search term 'KMS' entered. The 'Key Management Service (KMS)' is highlighted with a blue border. Other services listed include Managed Services, MediaStore, and AWS Firewall Manager. A sidebar on the left provides navigation links for KMS, Customer managed keys, and Custom key stores.

2. Verify whether the key created in the previous step has been successfully generated.

The screenshot shows the 'Customer managed keys' list in the AWS KMS console. There is one key named 'WebsiteKMS' listed. The table columns include Aliases, Key ID, Status, Key type, Key spec, and Key usage. The key 'WebsiteKMS' has an alias 'WebsiteKMS', a key ID starting with '885332c9-7d13-4b...', an enabled status, a symmetric key type, a symmetric key spec, and is used for 'Encrypt and decrypt' operations.

Aliases	Key ID	Status	Key type	Key spec	Key usage
WebsiteKMS	885332c9-7d13-4b...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt