

Configuration Manual

MSc Research Project Cloud Computing

Chetan Baviskar Student ID: 21166374

School of Computing National College of Ireland

Supervisor:

Dr. Shivani Jaswal

National College of Ireland



MSc Project Submission Sheet

School of Computing

Student Name: Chetan Rajendrakumar Baviskar

Student ID: 21166374

Programme: Cloud Computing

Module: MSc Research Project

Lecturer: 15-12-2022 Submission Due Date:

Project Title: Configuration Manual

Word Count: 1450

Page Count: 13

Year: 2022

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 15-12-2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Chetan Baviskar 21166374

1 Overview

1.1 Purpose of this document

This section of configuration manual describes step-by-step procedure for implementing automation approach for encrypting S3 bucket using AWS Lambda. This manual will contain detailed explanation of each AWS service to achieve this automation. This research project includes AWS services like CloudFormation, Lambda, S3 Bucket, CloudTrail, CloudWatch and so on.

2 Requirement

- AWS Cloud Knowledge.
- Basic Python programming knowledge.
- AWS IAM role access to create user role and update polices if required.

This project is configured on AWS account. Steps for building automation infrastructure are mentioned in further sections below. To create new AWS account, need to visit below mentioned URL.

• AWS Account URL: <u>https://aws.amazon.com</u>

3 Procedure

3.1 Create AWS CloudTrail

First, in order to capture every detail of this process. User needs to enable CloudTrail.

CloudTrail allows user to capture each and every log during the operation in form of API gateway logs.

To enable AWS CloudTrail log, follow below steps:

- Go to CloudTrail from AWS console and click on 'create a trail'.
- Provide a name to trail as shown in <u>figure 1</u>.
- Click apply to all multi region trail, in order to collects all API requests.

				~	
Introducing CloudTrail CloudTrail Lake lets you	ke ery multiple event fields in your logs, across all regions, for auditing ;	and analysis. Learn more [2]			
CloudTrail > Dashboa	> Create trail				
Step 1	Change trail attributes				
Choose trail attributes	Choose trail attributes				
Step 2	General details				
Choose log events	A trail created in the console is a multi-region trail. Learn more	C .			
Step 3	Tail anna				
Review and create	Enter a display name for your trail.		 2		
	s3autoencrypt				
	3-128 characters. Only letters, numbers, periods, underscores, an	1d dashes are allowed.			
	Enable for all accounts in my organization				
	To review accounts in your organization, open AWS Organization	s, See all accounts [
	Storage location Info	_			
	• Create new S3 bucket Create a bucket to store logs for the trail.	 Use existing S3 bucket Choose an existing bucket to store logs for this trail. 			
	Trail log bucket and folder				
	Enter a new S3 bucket name and folder (prefix) to store your log	s. Bucket names must be globally unique.			
	Logs will be stored in aws-cloudtrail-logs-645242957075-ab0c9	239/AW5Logs/645242957075			
	Log file SSE-KMS encryption Info				
	Enabled				

Figure 1: AWS CloudTrail

3.2 AWS CloudFormation

Now, once CloudTrail log option is enabled, Go to CloudFormation on AWS console and create a stack as shown in <u>figure 2</u>.

AWS CloudFormation works based on template file. User can provide all AWS resources configuration along with role to be created, event to be added and their dependencies are added in this template .yaml file so that user can deploy and set up them together in separate stack. Template file help to provision all required resources. This technique also known as 'Infrastructure as Code'.

• Upload the CloudFormation template file and click 'Next'

aws	Services Q Search	(Option+S)								
=	CloudFormation > Stacks > Create	stack								
	Step 1 Create stack	Create stack								
	Step 2 Specify stack details	Prerequisite - Prepare template								
	Step 3 Configure stack options	Prepare template Every stack is based on a template. A template is a JSON or VIAM. file that contains configuration information about the AWS resources you want to include is the stack. Image: Template is ready Use a sample template								
	Step 4 Review	Specify template A template is a SON or VMM. File that describes your stack's resources and properties.								
		Template source Selecting a template generates an Amazon 53 URL where it will be stored.								
		Amazon S3 URL Upload a template file								
		Upload a template file Choose file JSON or VXML formatted file								
		53 URL: Will be generated when template file is uploaded View in Designer								
		Cancel Next								

Figure 2: AWS CloudFormation template upload

• Provide name to CloudFormation stack as depicted in <u>figure 3</u> and click 'Next'.

aws	Services Q Search	[Option+S]	D	¢	0	Ireland 🔻	chetancloud
=	CloudFormation > Stacks > Crea	ite stack					
	Step 1 Create stack	Specify stack details					
	Step 2 Specify stack details	Stack name					
	Step 3						
	Configure stack options	S3AutoEnrypt					
	Step 4	Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).					
	Review S3AutoEnrypt	Parameters Parameters are defined in your template and allow you to input custom values when you create or update a stack.					
		No parameters There are no parameters defined in your template					
				Cance	a [Previous	Next

Figure 3: AWS CloudFormation stack

• Now, keep all default values as it is and mark it checked the acknowledge as illustrated in <u>figure 4</u>, to allow CloudFormation to create role if required.

aws	Services	Q Search	[Option+S]	D	¢	0	Ireland 🔻	chetancloud 🔻
=			SNS topic ARN					
			No notification options There are no notification options defined					
			Stack creation options					
			Timeout -					
			Termination protection Disabled					
			▶ Quick-create link					
			Capabilities					
			The following resource(s) require capabilities: [AWS:IAM::Role] This template contains identity and Access Management (IAM) resources that might provide entities access Check that you want to create each of these resources and that they have the minimum required permissie [2] I acknowledge that AWS CloudFormation might create IAM resources.	s to mai ons. Le	ke chan am mor	ges to y e 🛃	our AWS acco	int.
			Create change set	G	ancel	Pr	revious	Submit

Figure 4: AWS CloudFormation submission

• Then click on 'Submit' and wait for stack deployment to finish.

aws	Services Q Search		[Opti	ion+S]			٤	¢	0	Ireland 🔻	chetanclo	ud 🔻
=	CloudFormation > Stacks > S3AutoEnrypt			S3AutoEnrypt							0	×
	Stacks (1)	C			Delet	e Update	Sta	ick acti	ons 🔻	Create	stack 🔻	
	Q Filter by stack name			Stack Info Even	nts Resources	Outputs Pa	ramete	rs	Templa	ate Cha	nge sets	
	Active	< 1 >		Resources (4)							C	
				Q Search resources							۲	
	S3AutoEnrypt 2022-12-11 18:22:25 UTC+0000 ⊘ CREATE_COMPLETE			Logical ID 🔺	Physical ID 🛛 🗢	Туре 🗢	St	atus	V	Module	∇	
			П	EventRule	S3AutoEnrypt- EventRule- 1USJU3JRZTUFV	AWS::Events::Rul e	© PI) CREAT .ETE	E_COM			
				LambdaExecutio nRole	S3AutoEnrypt- LambdaExecutio nRole- 1R8CAZLJYSY4C	AWS::IAM::Role	(C) PI) CREAT LETE	E_COM			
				LambdaFunction	S3AutoEnrypt- LambdaFunction -N9wPqBjgWKXI	AWS::Lambda::F unction	P) CREAT LETE	E_COM	-		
				PermissionForEv	S3AutoEnrypt- PermissionForEv entsToInvokeLa	AWS::Lambda::P	e) CREAT	E_COM			

Figure 5: CloudFormation Resource Status.

- As per <u>figure 5</u>, In the Resource tab user can monitor status of each resource like EventRule, ExecutionRole, LambdaFuncation and PermissionForEventsToInvokeLambda if status is 'CRETE_COMPLETE' means deployment is successful.
- Once template deployment is successful. As <u>figure 6</u>, user can check template on CloudFormation where Lambda function written using python programming to encrypt S3 bucket automatically as soon as it is created by user.

aws	Services Q 53			×	D 4	0	Ireland 🔻	chetancloud 🔻
=	CloudFormation > Stacks > S3AutoEnrypt		s	3AutoEnrypt				⊚ ×
Ξ	Stacks (1) C () Filter by stack nome Active () View nested () 1 > Stacks Stacks Stacks Stacks () 2022-12-11 18:22:5 UTC-0000 () CREATE_COMPLETE		S	SAutoEnrypt Delete Update Update Stack Info Events Resources Outputs Template AdSTemplate AdSTemplate Communication Properties: Roll:Info@Sillonddis:rfunction Properties: Roll:Info@Sillondis:rfunction Properties: Roll:Info@Sil	Stack	Temp View	Late Ch	⊗ × te stack ▼ ange sets
				<pre>ef Santannerys(coms): s3 = bot3.resourc('s') bucket = 3.Bucket_encryption(Bucket- print('Encryption already set') form a science set's set') form already set') form a set of set's set's set's set's set's set print('Encryption(Diffuentionet) f'sserversidencryption(Diffuentionet) print('Auto Encrypting Bucket.mare) Bucket-bucket.nome, Serversidencryption(Diffuentionet) 'Bucket-bucket.nome, Serversidencryption(Diffuentionet) 'Bucket-bucket.nome, Serversidencryption(Diffuentionet) 'Bucket-bucket.nome, Serversidencryption(Diffuentionet) 'Bucket-bucket.nome,</pre>	ucket.name) error: FoundError' tion(in str(er	ror):	

Figure 6: AWS Lambda function and other resources on CloudFormation template

3.3 Create AWS S3 Bucket.

- Now go to S3 bucket from AWS console to create S3 bucket.
- As presented in <u>figure 7</u>, provide bucket name and keep all other details unchanged.

Services Q Search	[Option+S]	D	¢	0	Global 🔻	ch
nazon S3 > Buckets > Create bucket						
reate bucket Info						
General configuration						
Bucket name						
projectsedici i vo Bucket name must be globally unique and must not contain spaces or up	percase letters. See rules for bucket naming 🔀					
AWS Region						
EU (Ireland) eu-west-1	•					
Copy settings from existing bucket - optional Only the bucket settings in the following configuration are capied. Choose bucket						
Object Ownership Info Control ownership of objects written to this bucket from other AWS acco	nunts and the use of access control lists (ACLs). Object ownership					
determines who can specify access to objects.						
• ACLs disabled (recommended)	ACLs enabled					

Figure 7: S3 Bucket Creation.

aws	Services	Q Search	[Option+S]	E	4	0	Global 🔻	chetancloud 🔻
=	Bucket Ver Disable	ioning						٩
	Tags (0) You can use	• optional ucket tags to track storage costs and organize buckets. Learn more 🕑						
	No tags ass Add tag	oclated with this bucket.						
	Default Automatical	encryption encrypt new objects stored in this bucket. Learn more 🔀						
	Server-side O Disable O Enable	encryption						
	► Advar	ced settings						
	(i) After c	eating the bucket you can upload files and folders to the buc	cket, and configure additional bucket settings.					
			Cancel Create bucket					

Figure 8: Encryption disable while creating bucket

- As illustrated in <u>figure 8</u>, maintain default encryption as disable so that bucket encryption can be happen through AWS Lambda automatically. Now click 'Create bucket'.
- Now, once S3 bucket is created. Head over to CloudFormation console and go to Resource tab click on Lambda function as shown in <u>figure 9</u>.



Figure 9: Lambda Function link on CloudFormation stack

- As presented in <u>figure 10</u>, it is clearly visible that EventBridge (CloudWatch Events) is triggering our Lambda function 'S3AutoEncrypt'.
- It means that, S3 bucket 'projectreseach108' creation event captured by CloudWatch events that leads to Lambda function 'S3AutoEncrypt' to run.



Figure 10: EventBridge (CloudWatch Events) cause Lambda Function to run.

- To gain more information about Lambda function and to check encryption validation. User need to click on 'view logs in CloudWatch' as depicted in figure 10.
- As illustrated in <u>figure 11</u>, user can scroll down and see logs that bucket name 'projectresearch108' is encrypted automatically.
- As per CloudFormation template, method for lambda function is added to trigger lambda function and provide becket name through API request.

• Also, user can see response logs where status code for http is 200 which describe as a successful response. Hence, objective of this research work to encrypt S3 bucket automatically using AWS Lambda function is achieved.

Services Q Search	[Option+5]	N	⇔ Ø	ireland 🔻	chetanclou
CloudWatch ×	CloudWatch > Log groups > /aws/lambda/S3AutoEnrypt-LambdaFunction-N9wPqBjgWKXI > 2022/12/11/[\$LAT	EST]4bb	7e26b85aa4f0)594d234ef646	196d2
Favorites and recents	Log events	614-0-0-0			
Dashboards	C Actions Create metric filter	ntter pat			
Alarms ▲ o ⊘ o ⊖ o In alarm All alarms	Q. Filter events Clear 1m 30m 1h	12h	Custom 🖽	Display 🔻	0
Logs	► Timestamp Message				
Log groups New	No older events at this moment. Retry				
	2022-12-11T18:32:40.720+00:00 START RequestId: 4b448c2e-2758-43e4-8d4e-408679ee14fb Version	: \$LATEST	r		
Logs insights	▼ 2022-12-11T18:32:42.961+00:00 Auto Encrypting projectresearch108				
Metrics	Auto Encrypting projectresearch108			[Сору
All metrics	▼ 2022-12-11T18:32:43.208+00:00 {'ResponseMetadata': {'RequestId': '2EBTT1MCRY53RXMD', 'HostId	d': 'h]/K	KxMqF10bv08vn	gtlrJ36e81UM8p	ZvHRIIi
Explorer	{'ResponseMetadata': {'RequestId': 'ZEBITIMCRYS3RXMD', 'HostId': 'hJ/KxMqF10bv@8vngtlrJ36eB1UM8pZv	HRIIiimK	G@xUWoVtiC	1	
Streams	<pre>//92uqXbblY=lteMTr9Q29beg4=" MTTP5tatusKode': 2008, "MTTPHeaders': { {x-amz-id=2'; 'hJ/Kokdp1bbv08vng1rJ36e81UM8pZ/MRIIIimK68xJMoVtiC/92uqXbblY+lteMTr9Q29beg4=', 'x-amz-request-id' 'Sun, 11 Dec 2022 18:32:43 GMT', 'server': "AmazorS3', 'content-length: '0'}, 'RetryAttempts': 0)</pre>	: '2EBTT }	IMCRY53RXMD*	, 'date':	Сору
X-Ray traces	2022-12-11T18:32:43.242+00:00 END RequestId: 4b448c2e-2758-43e4-8d4e-408679ee14fb				
Service map	2022-12-11T18:32:43.242+00:00 REPORT RequestId: 4b448c2e-2758-43e4-8d4e-408679ee14fb Duration	on: 2521.	.30 ms Billed	Duration: 252	2 ms Me.,
	No newer events at this moment. Auto retry paused, Resume				

Figure 11: Encryption result of S3 bucket.

• Now, Bucket 'projectreseach108' is encrypted. On top this, user can even receive notification of S3 object insertion or deletion over mail using Simple Notification Service of AWS.

3.4 S3 SNS (Simple Notification Service) Notification

- Go to Simple Notification Service (SNS) from AWS console.
- Click on 'Next Step' this will lead to create topic page as depicted in figure 12.

aws	Services	Q Search	[Option+S]	2 4	© 4	Ireland 🔻	chetancloud 🔻
=	Amazon SNS	> Topics > Create topic					٤
	Create	topic					
	Details						
	Type Info Topic type o	cannot be modified after topic is created					
	FIFC	D (first-in, first-out) tirstiy-preserved message ordering bacty-once message delivery tigh throughput, up to 300 publishes/second iubscription protocols: SQS	• Standard • Best-effort message ordering • At-least once message delivery • Highest throughput in publisher, lacond • Subverging pretocute SQS, landba HTPS SMS, email, mobile application endpoints				
	Name						
	S3-Buck	et-Notify					
	Maximum 2 Display na To use this t						
	Maximum 1	00 characters.]			

Figure 12: AWS SNS Notification

- User can provide topic name and scroll down to click on 'Create topic'
- Once topic is created then user need to create subscription to avail email notification service. Therefore, click on 'Create subscription' as shown in <u>figure 13</u>.

aws iii Services Q Search	[Option+S]	D
Amazon SNS \times	Amazon SNS > Topics > S3-Bucket-Notify	
Dashboard	S3-Bucket-Notify	Edit Delete Publish message
Subscriptions	Details	
Mobile Push notifications Text messaging (SMS) Origination numbers	Name S3-Bucket-Notify ARN am:aws:sns:eu-west-1:645242957075:53-Bucket-Notify Type Standard	Display name S3-Bucket-Notify Topic owner 645242957075
	Subscriptions (1) Edit Delete Reque	st confirmation Confirm subscription Create subscription

Figure 13: Create subscription to topic

- As illustrated in the <u>figure 14</u>, select protocol as 'Email' from drop-down menu.
- User needs to provide email address on which notification can be sent from AWS and then scroll down to click 'Create subscription'.

aws	Services	Q Search	[Option+S]		D .	\$ Ø	Ireland 🔻	chetancloud 🔻
:	Amazon SNS	> Subscriptions > Create subscription						١
	Create	subscription						
	Details							
	Topic ARN							
	Q, arn:a	aws:sns:eu-west-1:645242957075:S3-Bucket-Notify	>	<				
	Protocol The type of	endpoint to subscribe						
	Email		`	*				
	Endpoint An email ac	Idress that can receive notifications from Amazon SNS.						
	chetanb	aviskar1008@gmail.com						
	(i) Afr	ter your subscription is created, you must confirm it. Info						

Figure 14: Provide email address to receive notification.

- Once, subscription is created, AWS will send subscription confirmation email to email address provided.
- As shown in <u>figure 15</u>, user need to provide confirmation by clicking 'confirm subscription'



Figure 15: Subscription Confirmation

- Now, here in this research work another lambda function 'SNS_Lambda' is used to avail SNS service on particular S3 bucket. Need to create role for this lambda function.
- Go to IAM (Identity and Access Management) to create role named as 'SNS_Role' as shown in <u>figure 16</u>.

aws Ervices Q Search	[Option+S]	▷ 🗘 ⑦ Global ▼ chetancloud
Identity and Access Management (IAM)	IAM > Roles > SNS_Role SNS_Role Allows Lambda functions to call AWS services on your behalf. Summary	Delete Edit
Access management User groups Users Roles Policies Identity providers Account settings	Creation date December 11, 2022, 19:23 (UTC) Last activity 9 hours ago Permissions Trust relationships Tags Access Advisor	ARN ⁴ 21 arr:aws:lam::645242957075:role/SNS_Role Maximum session duration 1 hour Revoke sessions
 Access reports Access analyzer Archive rules Analyzers Settings Credential report Organization activity Service control policies (SCPs) 	Permissions policies (2) into You can attach up to 10 managed policies. Q. Filter policies by property or policy name and press enter. Policy name C*	Image: Simulate Remove Add permissions Image: View of the system Image: View of the system

Figure 16: IAM Role creation for SNS Lambda function.

- Go to AWS Lambda from AWS console and create 'SNS_Lambda' with selecting SNS_Role. Lambda function code is attached into code artifact submission.
- Once Lambda is created. User can go to lambda and click on 'Add trigger' to use AWS resource as shown in <u>figure 17</u>. In this research work S3 bucket used hence select S3 bucket from drop-down menu.

aws	Services Q IAM	×	D
=	Lambda > Functions > SNS_Lambd	fa	Throttle T Copy ARN Actions
	▼ Function overview Info		
	S3 + Add trigger	SNS_Lambda Layers (0) (4) Amazon SNS + Add destination	Description - Last modified 9 hours ago Function ARN D arraws:lambda:eu-west-1:645242957075:function:SNS_Lambda Function URL Info -
	Code Test Monitor		
	Code source Info		Upload from 🔻
	A File Edit Find View Go Q Go to Anything (% P) T E	Tools Window Test Test Import ison	50 ()

Figure 17: Lambda function for SNS service.

- Once S3 bucket is selected, user can choose particular bucket and event type as per shown in <u>figure 18</u>. Now, scroll down and click 'Add'.
- Here, in this research project Create and Delete event are used so that any object from S3 bucket created or deleted user will receive notification of the same.

aws	III Services Q IAM X	
≡	Lambda 汝 Add trigger	٥
	Add trigger	
	Trigger configuration Info	
	S3 aws storage ▼	
	Bucket Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.	
	Q s3/projectresearch108 X C Bucket region: eu-west-1	
	Event type Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.	
	All object create events	
	Prefix - optional Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.	
	e.g. images/	
	Suffix - optional Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.	
	e.gjpg	

Figure 18: Adding object create event trigger for SNS service.

- Now, user can upload any object on mentioned bucket 'projectresearch108' to check SNS service working or not.
- As shown in <u>figure 19</u>, email notification of topic 'S3-Bucket-Notify' that object creation on S3 bucket 'projectreseach108' that means SNS service working successfully.

=	🌱 Gmail	٩ :	Search mail	幸	Q	¢		0
0	Compose	÷			6 of 21,138	<	>	
	Inbox 14,280		AWS Notification Message Index ×		×	8	Ø	
\$ 0	Starred Snoozed		S3-Bucket-Notify <no-reply@sns.amazonaws.com> to me *</no-reply@sns.amazonaws.com>		Dec 11, 2022, 7:30 PM (10 hours ago) 🛛 🛧	4	1	ø
	Shoozed Sent Une * (Version*1.0**/imestamp*2022.12-11119.30.35.2872**/request/Context*C*/request/60.3168.4946-862a-33611/61aef9**/functionAm*:am:awsiambda:eu-west- 15.45224957075:function/SNS_LambdaSLATEST* condition*Success* approximate/moleCount*1]*request/Payload**(Records*{(revent/version*2.1*, "eventSource**aws: 3************************************							0

Figure 19: SNS topic S3-Bucket-Notify email notification to user

Therefore, even if user forgot to encrypt S3 bucket, using this approach bucket can secured as lambda will trigger immediately if S3 bucket is created and provide encryption to secure the bucket.

In this way, AWS Cloud based automated encryption approach and alert notification of S3 bucket using lambda is configured and implemented to protect not only security of S3 bucket but also privacy of S3 objects in the bucket.

References

CloudFormation, A. (2022) AWS CloudFormation Features, Amazon Web Services, Inc. Available at: <u>https://aws.amazon.com/cloudformation/features/</u>.

CloudTrail, A. (2022) AWS CloudTrail Features - Amazon Web Services, Amazon Web Services, Inc. Available at: <u>https://aws.amazon.com/cloudtrail/features/.</u>

SNS, A. (2022) Amazon Simple Notification Service (SNS) Features | Messaging Service | AWS, Amazon Web Services, Inc. Available at: https://aws.amazon.com/sns/features/.