

ENPM665 - Final

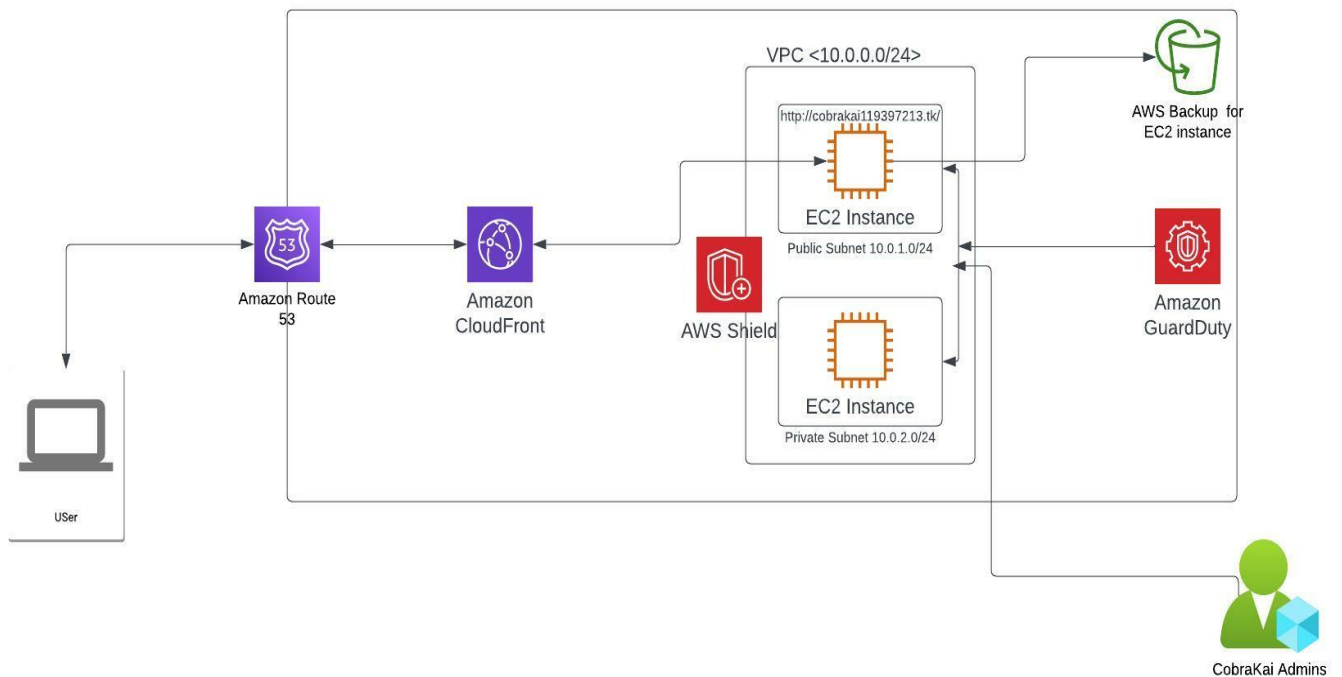
By **Adithya Srinivas Parthasarathy**

UID:119397213

I wanted to provide seven recommendations after moving into AWS from the current on premise server. These recommendations include:

- IAM
- VPCs
- Security groups
- On demand Backup
- Route53
- Guard Duty
- Cloud Trail
- Maice
- CloudFront

The re-architected diagram of the entire scenario is :



Firstly we migrate the on premise server to aws as suggested with help of S3 bucket.

We do this by taking the image given and by adding it to S3 bucket with certain configurations of route-policy.json and trust-policy.json inorder to correctly import the given image into the bucket.

Summary

Destination
s3://cobrakai-119397213

Succeeded
1 file, 1.1 GB (100.00%)

Failed
0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 1.1 GB)

Name	Folder	Type	Size	Status
ENPM809J-Project.ova	-	application/x-virtualbox-ova	1.1 GB	Succeeded

Once that is done, now with the help of Amazon Machine Image (AMI) that we just imported, we can run an EC2 instance with certain security configurations to get the most out of it.

So the idea is to create Virtual Private clouds, security groups, network access control list (ACL) , so that we could add these to our EC2 instance that we will create out of the AMI.

Cybersecurity

(1) WhatsApp

(863) Import

Images | EC2

Importing a v...

Instances

3.83.30.66

Configure Air...

Adithya CV...

AWS CloudF...

coherence - C...

The New Mi...

ENPM665 20...

ENPM665-Fil...

Bangladesh >

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances

Search

[Alt+S]

N. Virginia

adithyasrinivas

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Instances (1/1) info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
-	i-0636366346066a4ac	Running	t2.micro	Initializing	No alarms	us-east-1c	ec2-3-83-30-66.comput...	3.83.30.66	-

Instance: i-0636366346066a4ac

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

Instance summary info

Instance ID

i-0636366346066a4ac

IPv6 address

-

Hostname type

IP name: ip-172-31-84-147.ec2.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

Public IPv4 address

3.83.30.66 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-172-31-84-147.ec2.internal

Instance type

t2.micro

VPC ID

Private IPv4 addresses

172.31.84.147

Public IPv4 DNS

ec2-3-83-30-66.compute-1.amazonaws.com | open address

Elastic IP addresses

-

AWS Compute Optimizer finding

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Cobrakai-119397...pem

-2°C Clear

Search

2116

13-12-2022

1) IAM:

Management of identity and access to technological resources is the process of ensuring that the right people have access to the right resources through policies. We could do this by formation of policies and groups which have permission for only certain resources.

We create three **groups** for this purpose:

- Admin
- Developer
- System Administrators

i)Admin

User group name
CobraKai-Admin_access

Creation time
December 13, 2022, 21:28 (UTC-05:00)

ARN
arn:aws:iam::794770513025:group/CobraKai-Admin_access

Users

Permissions

Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.


☐

Policy name [↗](#)

Type

Description

☐

 AdministratorAccess

AWS managed - job function

Provides full access to AWS services and resources.

The administrator group is provided with 'AdministratorAccess' policy which makes sure all the access is granted. We make this for C-Suite executives and founder.

ii)Developer

User group name
CobraKai-Developer_access-119397213

Creation time
December 13, 2022, 21:38 (UTC-05:00)

Users

Permissions

Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.


☐

Policy name [↗](#)

Type

Description

☐

 PowerUserAccess

AWS managed - job function

Provides full access to AWS services and resources, but do

The Developer group is provided with 'PowerUserAccess' policy which provides full access to AWS resources and services, but does not allow management of users and groups. This group is created for Developers.

iii)system administration:

User group name

CobraKai-SystemAdministrator_ access-119397213

Creation time

December 13, 2022, 21:51 (UTC-05:00)

Users


Permissions

Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

<input type="checkbox"/>	Policy name ↗	Type	Description
<input type="checkbox"/>	 SystemAdministrator	AWS managed - job function	Grants full access permissions necessary for resources requi

The System administrator group is provided with 'SystemAdminstrator' policy which grants full access permissions necessary for resources required for development operations.We make this for system admins.

Users:

We add a sample of 5 users as given to us in the document. We add all the C-Suite executives (Johnny Lawrence, Miguel Diaz, Aisha Robinson, Eli "Hawk" Moskowitz) to the CobraKai_admin_access group.

We add Demetri to the Developer-access group followed by Bert to SystemAdministrator groups respectively.

<input type="checkbox"/>	AishaRobinson	CobraKai-Admin_access	Never	None	None
<input type="checkbox"/>	Bert	CobraKai-SystemAdministrator_access-119397213	Never	None	None
<input type="checkbox"/>	Demetri	CobraKai-Developer_access- <u>119397213</u>	Never	None	None
<input type="checkbox"/>	Eli_Hawk_Moskowitz	CobraKai-Admin_access	Never	None	None
<input type="checkbox"/>	JohnnyLawrence	CobraKai-Admin_access	Never	None	None
<input type="checkbox"/>	MiguelDiaz	CobraKai-Admin_access	Never	None	None

2) VPCs:

An Amazon Virtual Private Cloud (Amazon VPC) provides you with a virtual network where you can launch Amazon Web Services resources. The AWS infrastructure enables you to operate this virtual network in a similar way to a traditional data center network with the added bonus of scaling with AWS resources. It provides us with a virtual private network in a given public cloud environment. This can be achieved using Subnets, Network Access control lists and Internet gateways in order to use the VPC to allow only access to certain IP address.

Your VPCs (1/2) [Info](#)

Filter VPCs

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	CobraKai-119397213	vpc-09d211877315e6716	Available	10.0.0.0/16	-

We name the VPC as CobraKai-119397213 where '119397213' is the UID.

2.1) Internet Gateways:

To connect the VPCs to another network we usually need a Gateway. The Internet Gateway helps us to connect our VPC (CobraKai-119397213) to the internet.

	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	CobraKai-IG-11939...	igw-03e820008004a7c26	Attached	vpc-09d211877315e6716 CobraKai-...	794770513025
<input type="checkbox"/>	-	igw-06225c82ed3f3732e	Attached	vpc-07704d19789e7fdc2	794770513025

igw-03e820008004a7c26 / CobraKai-IG-119397213

Details Tags

Details

Internet gateway ID	State	VPC ID
igw-03e820008004a7c26	Attached	vpc-09d211877315e6716 CobraKai-119397213

We attach our already existing VPC that we created for this purpose.

2.2) Subnets:

An IP network can be divided logically into subnetworks. Creating a subnet is one way to reduce traffic on a larger network by splitting it into smaller, interconnected networks. As a result, traffic does not have to travel through unnecessary routes, which increases the speed of the network. So we basically split it as a public subnet and private subnet each with its own IP ranges. We need this division since the resources that need to be accessed across the internet need to be in a public subnet, while the ones that don't need to be accessed should be in a private network.

Public subnet:

subnets/subnet-000d7e59e6ab154f1 / **CobraKai_public_119397213**

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID subnet-000d7e59e6ab154f1	Subnet ARN arn:aws:ec2:us-east-1:794770513025:subnet/subnet-000d7e59e6ab154f1	State Available	IPv4 CIDR 10.0.1.0/24
Available IPv4 addresses 251	IPv6 CIDR -	Availability Zone us-east-1d	Availability Zone ID use1-az4

Here we assign the CIDR range of **10.0.1.0/24** for the public subnet.

For the public subnet we created, we add a routing rule as 0.0.0.0/24 in order to allow access from anywhere from the internet.

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny	
100	All traffic	All	All	100.15.123.102/32	Allow	Remove
119397213	All traffic	All	All	0.0.0.0/0	Allow	Remove

Private subnet:

subnets/subnet-0e115feec9c70c0c7 / **CobraKai_private_119397213**

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID subnet-0e115feec9c70c0c7	Subnet ARN arn:aws:ec2:us-east-1:794770513025:subnet/subnet-0e115feec9c70c0c7	State Available	IPv4 CIDR 10.0.2.0/24
Available IPv4 addresses 251	IPv6 CIDR -	Availability Zone us-east-1d	Availability Zone ID use1-az4

Here we assign the CIDR range of 10.0.2.0/24 for the private subnet. And we save subnet associations with each subnet respectively.

2.3) Network Access Control List:

Network ACLs (1/2) [Info](#)

Filter network ACLs

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
-	acl-08b2627ea985515...	6 Subnets	Yes	vpc-07704d19789e7fdc2	2 Inbound rules
<input checked="" type="checkbox"/> CobraKai_NACL-19...	acl-06bc8cb14592db6b4	2 Subnets	Yes	vpc-09d211877315e6716 / CobraKai-...	2 Inbound rules

acl-06bc8cb14592db6b4 **CobraKai_NACL-19397213**

Details **Inbound rules** Outbound rules Subnet associations Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Inbound rules (2)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	100.15.123.102/32	✔ Allow

2.4) Security groups:

We add security group with set of defined inbound and outbound rules:

Security Groups (1/3) [Info](#)

Filter security groups

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
-	sg-0b9c95f4b5b9b3e7a	launch-wizard-1	vpc-07704d19789e7fdc2	launch-wizard-1 create...	794770513025	1 Permission entry
<input checked="" type="checkbox"/> 119397213	sg-0d4f3db664cef15df	default	vpc-09d211877315e6716	default VPC security gr...	794770513025	2 Permission entries
<input type="checkbox"/> CobraKai_SG-1193...	sg-00ca1654507aa081e	default	vpc-07704d19789e7fdc2	default VPC security gr...	794770513025	2 Permission entries

sg-0d4f3db664cef15df - default

Details **Inbound rules** Outbound rules Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Inbound rules (2) [Manage tags](#)

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/> -	sgr-0363b2c13e4350b...	IPv4	All traffic	All	All	100.15.123.102/32
<input type="checkbox"/> -	sgr-0287c2cd6ac3c4191	-	All traffic	All	All	sg-0d4f3db664cef15d...

With all this created, we can now spin off an EC2 instance with created Internet gateway, subnets and VPCs.

CobraKai-Serv...
i-004de74a5b059dc45
Running
t2.micro
No alarms
us-east-1d
54.83.69.248

Instance: i-004de74a5b059dc45 (CobraKai-Server-119397213)

Details
Security
Networking
Storage
Status checks
Monitoring
Tags

Instance summary

Instance ID
i-004de74a5b059dc45 (CobraKai-Server-119397213)

IPv6 address
-

Hostname type
IP name: ip-10-0-1-186.ec2.internal

Answer private resource DNS name
IPv4 (A)
54.83.69.248 [Public IP]

Auto-assigned IP address
54.83.69.248 [Public IP]

IAM Role
-

Public IPv4 address
54.83.69.248 | open address

Instance state
Pending

Private IP DNS name (IPv4 only)
ip-10-0-1-186.ec2.internal

Instance type
t2.micro

VPC ID
vpc-09d211877315e6716 (CobraKai-119397213)

Subnet ID
subnet-000d7e59e6ab154f1 (CobraKai_public_119397213)

Private IPv4 addresses
10.0.1.186

Public IPv4 DNS
-

Elastic IP addresses
-

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
-

Instance details

Platform
Linux/UNIX (Inferred)

AMI ID
ami-0014e1c69cd227403

Monitoring
disabled

Associated security groups

Add one or more security groups to the network interface. You can also remove security groups.

launch-wizard-1 (sg-0b9c95f4b5b9b3e7a)
launch-wizard-1

default (sg-00ca1654507aa081e)
default CobraKai_SG-119397213

Security group name

Security group ID

No security groups attached to this network interface

3) Creation of Backups:

There is a need for Backup of the EC2 instance because in case the instance is compromised or attacked under ransomware, the team could always retrieve the latest image of the instance . In addition to automating backup schedules and retention management, the team can create backup policies as well.

Create on-demand backup [Info](#)

Settings

Resource type

EC2 ▼

Instance ID

i-004de74a5b059dc45 ▲



i-004de74a5b059dc45
CobraKai-Server-119397213 ✓

i-0636366346066a4ac

Backup window

☒ Create backup now

Starts within 1 hour.

☐ Customize backup window

Retention period [Info](#)

Days ▼

7

Backup vault [Info](#)

Specify the Backup vault this backup is organized in.

CobraKai_server_backup-119397213 ▼

Create new Backup vault

We choose our EC2 instance and set the retention period as 7 days (basically once every week). We create a separate backup vault for the same.

4) Route 53:

The Amazon Route 53 is a DNS web service that is scalable and highly available. User requests are routed to internet applications running on AWS or on-premises via Route 53. It can load balance and accordingly change origin address dynamically.

For this first we have to create an elastic ip for our ec2 instance. This makes sure that even after restart of ec2 instance the IP address won't be different.

Elastic IP addresses (1/1)

Q 119397213 X

<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS
<input checked="" type="checkbox"/>	CobraKai_EIP	44.212.134.197	Public IP	eipalloc-04bb5dd366c9a2108	-

44.212.134.197

Summary

Tags

Summary

Allocated IPv4 address 44.212.134.197	Type Public IP	Allocation ID eipalloc-04bb5dd366c9a2108
Association ID eipassoc-0ccdd829e30944e5b	Scope VPC	Associated instance ID i-004de74a5b059dc45
Network interface ID eni-0308c0b25862cda43	Network interface owner account ID 794770513025	Public DNS -

For this first we register a domain name called '<http://cobrakai119397213.tk/>'. Now we attach this elastic ip to the hosted zone by creating a record so that we get a set of DNS values. We now add these values to the DNS record of the website.

Route 53 > Hosted zones > http://cobrakai119397213.tk/

Public **http://cobrakai119397213.tk/** Info

Delete zone Test record Configure query logging

► Hosted zone details Edit hosted zone

Records (4) DNSSEC signing Hosted zone tags (0)

Records (4) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

Refresh Delete record Import zone file Create record

Filter records by property or value Type Routing policy Alias < 1 > ⚙

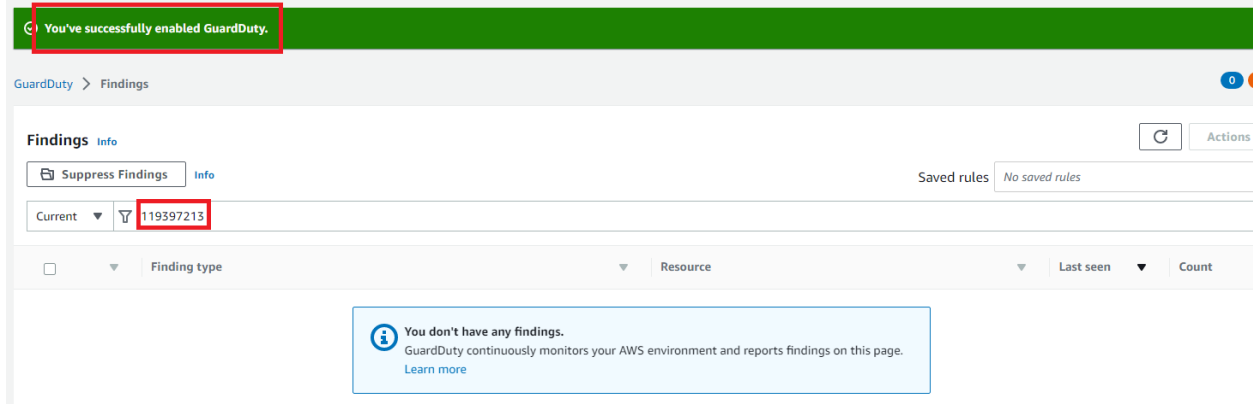
<input type="checkbox"/>	Record name ▼	Type ▼	Routin... ▼	Differ... ▼	Value/Route traffic to ▼
<input type="checkbox"/>	http://cobrakai...	A	Simple	-	44.212.134.197
<input type="checkbox"/>	http://cobrakai...	NS	Simple	-	ns-518.awsdns-00.net. ns-364.awsdns-45.com. ns-1356.awsdns-41.org. ns-1683.awsdns-18.co.uk.

This makes sure that even if one of them fail there are other three that could still provide the service accordingly so that CobraKai team does not lose on customers and the customers don't lose when there is downtime in one line.

5)Guard duty:

Amazon GuardDuty processes data sources (Eg: AWS CloudTrail data events for Amazon S3 logs, CloudTrail management event logs, and various other logs) and monitors them continuously and analyzes them for threats. It does this so by matching with the default premade list of malicious IPs and threat lists and also uses Machine Learning to identify unauthorized, unexpected, and potential malicious activity within a given AWS environment.

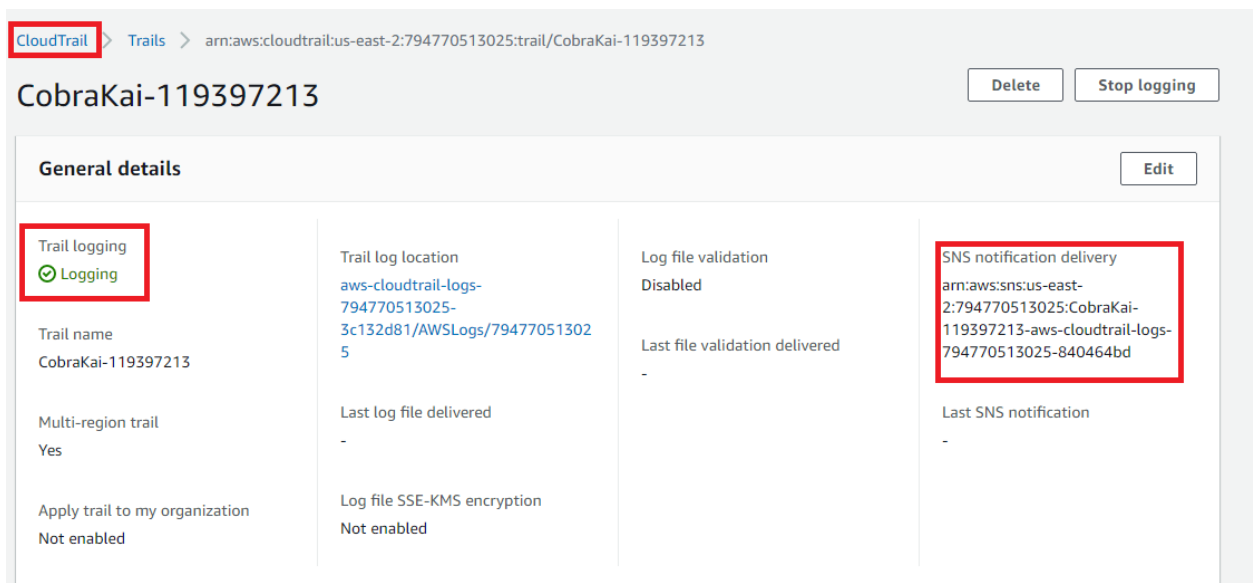
Enabling AWS Guard duty for the account.



6) Cloud Trail:

With the help of AWS CloudTrail, the CobraKai team can govern, enable operational and risk audit, and comply with your AWS account. All the usage of AWS services is recorded for this purpose. This can be viewed under the events history tab.

So we created a new trail for this purpose. We add an additional SNS notification system for this so that the team can keep track of various events happening.



We could see events history:

119397213

2

✕

✓ Enabled
Automated sensitive data discovery was enabled for your account. It can take up to 48 hours for the results to appear in your account.

Amazon Macie > Settings > Automated discovery

Automated sensitive data discovery [Info](#)

As a Macie administrator, you can use Macie to continually discover sensitive data in S3 buckets that you or your organization own. Macie selects samples of S3 objects and inspects them for the presence of sensitive data. You can review the results in discovery statistics and other data that Macie builds automatically for your organization's S3 buckets.

ⓘ Automated sensitive data discovery is enabled for your account. Review and verify the settings below.

Ok

Status
Continually select and inspect samples of S3 objects.

Disable

✓ Automated sensitive data discovery is currently enabled for your account.
Free trial 29 days remaining.

S3 buckets
By default, Macie selects sample objects from all of your organization's S3 buckets. You can exclude specific buckets from the analysis.

Edit

1

All - All buckets are currently included.

8) Cloud front:

This is a content delivery network which helps the end users to have a very good user experience by caching the content and minimizing the latency. If the requested content is present in the edge location, then cloudfront instantly provides it, otherwise it fetches the content from the web server behind the edgelocation and provides it.

CloudFront > Distributions > E2024YNOPQ7KX6

E2024YNOPQ7KX6

General

Origins

Behaviors

Error pages

Geographic restrictions

Invalidations

Tags

Origins

	Origin name	Origin domain	Origin path	Origin type
<input type="radio"/>	cobrakai119397213.tk	cobrakai119397213.tk		Custom Origin



We enable cloud front for this account by adding the registered domain name .

[CloudFront](#) > [Distributions](#) > E2024YNOPQ7KX6

E2024YNOPQ7KX6

[General](#) | [Origins](#) | [Behaviors](#) | [Error pages](#) | [Geographic restrictions](#) | [Invalidations](#) | [Tags](#)

Details

Distribution domain name  d3itxe854fzv6.cloudfront.net	ARN  arn:aws:cloudfront::794770513025:distribution/E2024YNOPQ7KX6
--	---

9) AWS Shield:

AWS Shield standard protects the AWS infrastructure from different types of Distributed Denial of Service attacks. So the CobraiKai team could use this to protect their resources from Daniel LaRusso's attempts to stage a DDoS attack against the platform. It is automatically enabled, if the cobraKai team feels they want further security there is always AWS shield Advanced which is resilient against 99% of DDOS attacks.