



JJ Tech

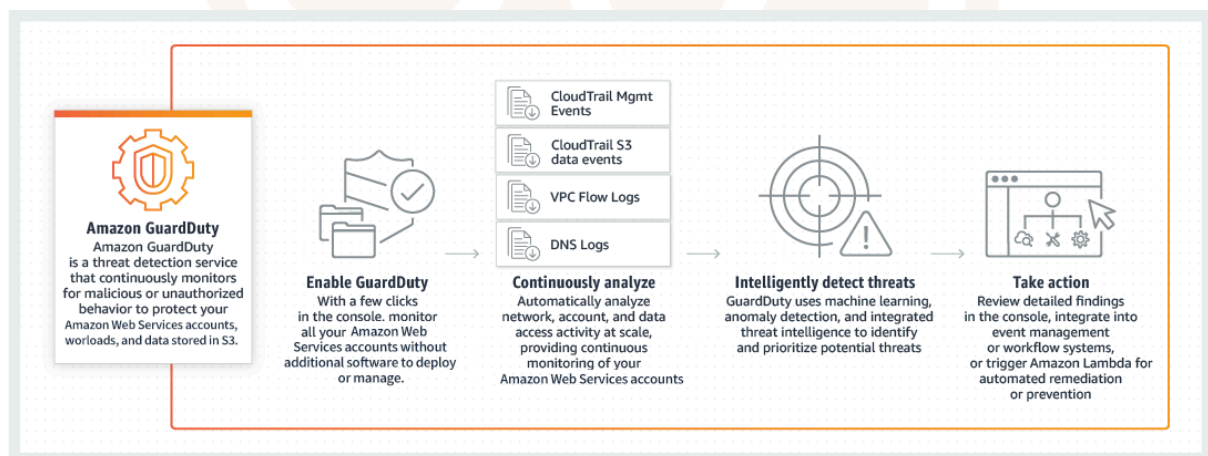
AWS Guard Duty

Protect your AWS accounts with intelligent threat detection

- Achieve organization-wide visibility into possible threats with only a few click
- Expose threats quickly with AWS threat intelligence, behavioural models, and third-party security feeds.
- Mitigate threats early by triggering automated responses.

How it works

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.



+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720





JJ Tech

Terminology

Account

A standard Amazon Web Services (AWS) account that contains your AWS resources. You can sign in to AWS with your account and enable GuardDuty.

You can also invite other accounts to enable GuardDuty and become associated with your AWS account in GuardDuty. If your invitations are accepted, your account is designated as the **administrator** GuardDuty account, and the added accounts become your **member** accounts. You can then view and manage those accounts' GuardDuty findings on their behalf.

Users of the administrator account can configure GuardDuty as well as view and manage GuardDuty findings for their own account and all of their member accounts. You can have up to 5000 member accounts in GuardDuty.

Users of member accounts can configure GuardDuty as well as view and manage GuardDuty findings in their account (either through the GuardDuty management console or GuardDuty API). Users of member accounts can't view or manage findings in other members' accounts.

An AWS account can't be a GuardDuty administrator and member account at the same time. An AWS account can accept only one membership invitation. Accepting a membership invitation is optional.

Detector

All GuardDuty findings are associated with a detector, which is an object that represents the GuardDuty service. The detector is a regional entity, and a unique detector is required in each region GuardDuty operates in. When you enable GuardDuty in a region a new detector with a unique 32 alphanumeric detector ID is generated in that region. The detector ID format looks like this:

12abc34d567e8fa901bc2d34e56789f0

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720





You can find your detector ID for your current region in the console from the **Settings** pane, or programmatically using the ListDetectors API.

JJ Tech

Note

In multiple account environments all findings for member accounts roll up to the administrator account's detector.

Some GuardDuty functionality is configured through the detector, such as configuring CloudWatch Events notification frequency and the enabling or disabling of optional data sources for GuardDuty to process.

Data source

The origin or location of a set of data. To detect unauthorized and unexpected activity in your AWS environment, GuardDuty analyzes and processes data from AWS CloudTrail event logs, VPC Flow Logs, and DNS logs.

Finding

A potential security issue discovered by GuardDuty.

Findings are displayed in the GuardDuty console and contain a detailed description of the security issue. You can also retrieve your generated findings by calling the GetFindings and ListFindings API operations.

You can also see your GuardDuty findings through Amazon CloudWatch events. GuardDuty sends findings to Amazon CloudWatch via HTTPS protocol. For more information.

Suppression rule

Suppression rules allow you to create very specific combinations of attributes to suppress findings. For example, you can define a rule through the GuardDuty filter to auto-archive Recon:EC2/Portscan from only those instances in a specific VPC, running a specific AMI, or with a specific EC2 tag. This rule would result in port scan findings being automatically archived from the instances that meet the criteria. However, it

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



still allows alerting if GuardDuty detects those instances conducting other malicious activity, such as crypto-currency mining.

Suppression rules defined in the GuardDuty administrator account apply to the GuardDuty member accounts. GuardDuty member accounts can't modify suppression rules.

With suppression rules, GuardDuty still generates all findings. Suppression rules provide suppression of findings while maintaining a complete and immutable history of all activity.

Typically suppression rules are used to hide findings that you have determined as false positives for your environment, and reduce the noise from low-value findings so you can focus on larger threats.

Trusted IP list

A list of trusted IP addresses for highly secure communication with your AWS environment. GuardDuty does not generate findings based on trusted IP lists.

Threat list

A list of known malicious IP addresses. GuardDuty generates findings based on threat lists.

GuardDuty Data Sources

- AWS CloudTrail Event Logs
- AWS CloudTrail Management Events
- AWS CloudTrail S3 Data Events
- VPC Flow Logs
- DNS logs

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720





JJ Tech

Severity levels for GuardDuty findings

Each GuardDuty finding has an assigned severity level and value that reflects the potential risk the finding could have to your network as determined by our security engineers. The value of the severity can fall anywhere within the 0.1 to 8.9 range, with higher values indicating greater security risk. To help you determine a response to a potential security issue that is highlighted by a finding, GuardDuty breaks down this range into, High, Medium, and Low severity levels.

Note

Values 0 and 9.0 to 10.0 are currently reserved for future use.

The following are the currently defined severity levels and values for the GuardDuty findings as well as general recommendations for each:

| Severity level | Value range |
|---|-------------|
| High | 8.9 - 7.0 |
| A High severity level indicates that the resource in question (an EC2 instance or a set of IAM user credentials) is compromised and is actively being used for unauthorized purposes. We recommend that you treat any High severity finding security issue as a priority and take immediate remediation steps to prevent further unauthorized use of your resources. For example, | |

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



| | |
|---|-----------|
| clean up your EC2 instance or terminate it, or rotate the IAM credentials. | |
| Medium | 6.9 - 4.0 |
| <p>A Medium severity level indicates suspicious activity that deviates from normal observed behavior and, depending on your use case, may be indicative of a resource compromise.</p> <p>We recommend that you investigate the implicated resource at your earliest convenience. Remediation steps will vary by resource and Finding family, but in general, you should be looking to confirm that the activity is authorized and consistent with your use case. If you cannot identify the cause, or confirm the activity was authorized, you should consider the resource compromised and follow Remediation Steps to secure the resource.</p> <p>Here are some things to consider when reviewing a Medium level finding:</p> <ul style="list-style-type: none"> • Check if an authorized user has installed new software that changed the behavior of a resource (for example, allowed higher than normal traffic, or enabled communication on a new port). • Check if an authorized user changed the control panel settings, for example, modified a security group setting. • Run an anti-virus scan on the implicated resource to detect unauthorized software. • Verify the permissions that are attached to the implicated IAM role, user, group, or set of credentials. These might have to be changed or rotated. | |
| Low | 3.9 - 1.0 |
| <p>A low severity level indicates attempted suspicious activity that did not compromise your network, for example, a port scan or a failed intrusion attempt.</p> <p>There is no immediate recommended action, but it is worth making note of this information as it may indicate someone is looking for weak points in your network.</p> | |

Findings by resource type

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



The following pages are broken down by each resource type GuardDuty currently generates findings for. The pages contain detailed information on all finding types for that resources type.

- EC2 finding types
- IAM finding types
- S3 finding types

Findings table

The following table lists all finding types by name, resource, data source and severity. A severity listed with an asterisk (*) indicates the finding has variable severities depending the circumstances of the finding, which are described in the details for that finding. Choose the finding name to open more info about that finding.

| FINDING TYPE | RESOURCE | DATA SOURCE | SEVERITY |
|--|----------|---------------|----------|
| Backdoor:EC2/C&CAActivity.B | EC2 | VPC Flow Logs | High |
| Backdoor:EC2/C&CAActivity.B!DNS | EC2 | DNS logs | High |
| Backdoor:EC2/DenialOfService.Dns | EC2 | VPC Flow Logs | High |
| Backdoor:EC2/DenialOfService.Tcp | EC2 | VPC Flow Logs | High |
| Backdoor:EC2/DenialOfService.Udp | EC2 | VPC Flow Logs | High |
| Backdoor:EC2/DenialOfService.UdpOnTcpPorts | EC2 | VPC Flow Logs | High |
| Backdoor:EC2/DenialOfService.UnusualProtocol | EC2 | VPC Flow Logs | High |
| Backdoor:EC2/Spambot | EC2 | VPC Flow Logs | Medium |
| Behavior:EC2/NetworkPortUnusual | EC2 | VPC Flow Logs | Medium |
| Behavior:EC2/TrafficVolumeUnusual | EC2 | VPC Flow Logs | Medium |

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



| | | | |
|--|-----|-----------------------------|---------|
| Credential Access: IAMUser/Anomalous Behavior | IAM | CloudTrail management event | Medium |
| CryptoCurrency: EC2/BitcoinTool.B | EC2 | VPC Flow Logs | High |
| CryptoCurrency: EC2/BitcoinTool.B!DNS | EC2 | DNS logs | High |
| DefenseEvasion: IAMUser/Anomalous Behavior | IAM | CloudTrail management event | Medium |
| Discovery: IAMUser/Anomalous Behavior | IAM | CloudTrail management event | Low |
| Discovery: S3/MaliciousIPCaller | S3 | CloudTrail S3 data event | High |
| Discovery: S3/MaliciousIPCaller.Custom | S3 | CloudTrail S3 data event | High |
| Discovery: S3/TorIPCaller | S3 | CloudTrail S3 data event | Medium |
| Exfiltration: IAMUser/Anomalous Behavior | IAM | CloudTrail management event | High |
| Exfiltration: S3/MaliciousIPCaller | S3 | CloudTrail S3 data event | High |
| Exfiltration: S3/ObjectRead.Unusual | S3 | S3 CloudTrail data event | Medium* |
| Impact: EC2/AbusedDomainRequest.Reputation | EC2 | DNS logs | Medium |
| Impact: EC2/BitcoinDomainRequest.Reputation | EC2 | DNS logs | High |
| Impact: EC2/MaliciousDomainRequest.Reputation | EC2 | DNS logs | High |
| Impact: EC2/PortSweep | EC2 | VPC Flow Logs | High |
| Impact: EC2/SuspiciousDomainRequest.Reputation | EC2 | DNS logs | Low |
| Impact: EC2/WinRMBruteForce | EC2 | VPC Flow Logs | Low* |

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720



| | | | |
|--|-----|--|--------|
| Impact:IAMUser/AnomalousBehavior | IAM | CloudTrail management event | High |
| Impact:S3/MaliciousIPCaller | S3 | CloudTrail S3 data event | High |
| InitialAccess:IAMUser/AnomalousBehavior | IAM | CloudTrail management event | Medium |
| PenTest:IAMUser/KaliLinux | IAM | CloudTrail management event | Medium |
| PenTest:IAMUser/ParrotLinux | IAM | CloudTrail management event | Medium |
| PenTest:IAMUser/PentooLinux | IAM | CloudTrail management event | Medium |
| PenTest:S3/KaliLinux | S3 | CloudTrail S3 data event | Medium |
| PenTest:S3/ParrotLinux | S3 | CloudTrail S3 data event | Medium |
| PenTest:S3/PentooLinux | S3 | CloudTrail S3 data event | Medium |
| Persistence:IAMUser/AnomalousBehavior | IAM | CloudTrail management event | Medium |
| Policy:IAMUser/RootCredentialUsage | IAM | CloudTrail management event or CloudTrail data event | Low |
| Policy:S3/AccountBlockPublicAccessDisabled | S3 | CloudTrail management event | Low |
| Policy:S3/BucketAnonymousAccessGranted | S3 | CloudTrail management event | High |

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



| | | | |
|---|-----|-----------------------------|--------|
| Policy:S3/BucketBlockPublicAccessDisabled | S3 | CloudTrail management event | Low |
| Policy:S3/BucketPublicAccessGranted | S3 | CloudTrail management event | High |
| PrivilegeEscalation:IAMUser/AnomalousBehavior | IAM | CloudTrail management event | Medium |
| Recon:EC2/PortProbeEMRUnprotectedPort | EC2 | VPC Flow Logs | High |
| Recon:EC2/PortProbeUnprotectedPort | EC2 | VPC Flow Logs | Low* |
| Recon:EC2/Portscan | EC2 | VPC Flow Logs | Medium |
| Recon:IAMUser/MaliciousIPCaller | IAM | CloudTrail management event | Medium |
| Recon:IAMUser/MaliciousIPCaller.Custom | IAM | CloudTrail management event | Medium |
| Recon:IAMUser/TorIPCaller | IAM | CloudTrail management event | Medium |
| Stealth:IAMUser/CloudTrailLoggingDisabled | IAM | CloudTrail management event | Low |
| Stealth:IAMUser/PasswordPolicyChange | IAM | CloudTrail management event | Low |
| Stealth:S3/ServerAccessLoggingDisabled | S3 | CloudTrail management event | Low |
| Trojan:EC2/BlackholeTraffic | EC2 | VPC Flow Logs | Medium |
| Trojan:EC2/BlackholeTraffic!DNS | EC2 | DNS logs | Medium |
| Trojan:EC2/DGADomainRequest.B | EC2 | DNS logs | High |
| Trojan:EC2/DGADomainRequest.C!DNS | EC2 | DNS logs | High |
| Trojan:EC2/DNSDataExfiltration | EC2 | DNS logs | High |

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720



| | | | |
|--|-----|-----------------------------|--------|
| Trojan:EC2/DriveBySourceTraffic!DNS | EC2 | DNS logs | High |
| Trojan:EC2/DropPoint | EC2 | VPC Flow Logs | Medium |
| Trojan:EC2/DropPoint!DNS | EC2 | DNS logs | Medium |
| Trojan:EC2/PhishingDomainRequest!DNS | EC2 | DNS logs | High |
| UnauthorizedAccess:EC2/MaliciousIPCaller.Custom | EC2 | VPC Flow Logs | Medium |
| UnauthorizedAccess:EC2/MetadataDNSRebind | EC2 | DNS logs | High |
| UnauthorizedAccess:EC2/RDPBruteForce | EC2 | VPC Flow Logs | Low* |
| UnauthorizedAccess:EC2/SSHBruteForce | EC2 | VPC Flow Logs | Low* |
| UnauthorizedAccess:EC2/TorClient | EC2 | VPC Flow Logs | High |
| UnauthorizedAccess:EC2/TorRelay | EC2 | VPC Flow Logs | High |
| UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B | IAM | CloudTrail management event | Medium |
| UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS | IAM | CloudTrail management event | High |
| UnauthorizedAccess:IAMUser/MaliciousIPCaller | IAM | CloudTrail management event | Medium |
| UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom | IAM | CloudTrail management event | Medium |
| UnauthorizedAccess:IAMUser/TorIPCaller | IAM | CloudTrail management event | Medium |
| UnauthorizedAccess:S3/MaliciousIPCaller.Custom | S3 | CloudTrail S3 data event | High |
| UnauthorizedAccess:S3/TorIPCaller | S3 | CloudTrail S3 data event | |

+1 (410) 8887049
contact@jjtechinc.com

www.jjtechinc.com

14103 Hammermill Field Dr Bowie MD 20720

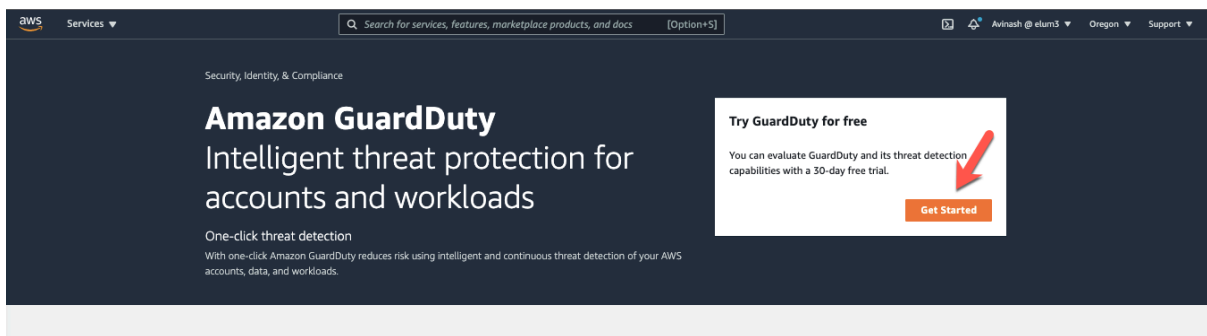




JJ Tech

Enable GuardDuty

- Navigate to Amazon GuardDuty console



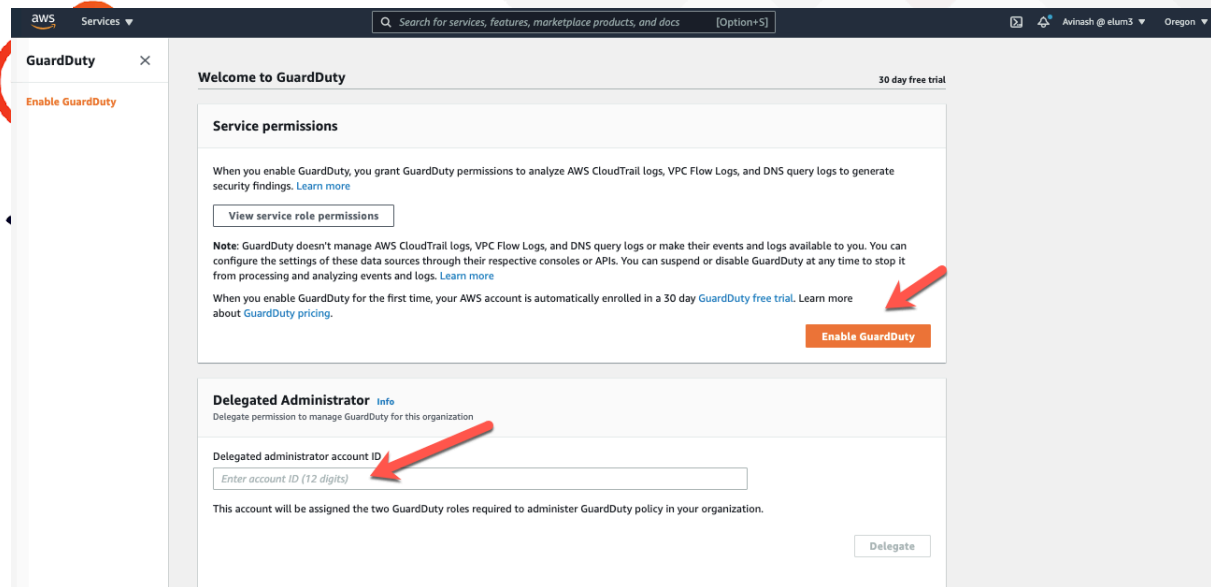
- If you are trying to enable GuardDuty in child accounts you can delegate this to Admin account
- If you are doing this in an individual account , you are not required to delegate access

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





Demo:

Amazon GuardDuty Findings to SNS

Every GuardDuty finding is assigned a finding ID. For every finding with a unique finding ID, GuardDuty aggregates all subsequent occurrences of a particular finding that take place in six-hour intervals into a single event. GuardDuty then sends a notification about these subsequent occurrences based on this event. We can use this to push the notifications into SNS topic, and getting the security teams to investigate the findings.

This AWS Lambda function will help you to automatically push GuardDuty findings to an SNS topic which can be used by ITSM tools for their workflows.

Step-1

+1 (410) 8887049

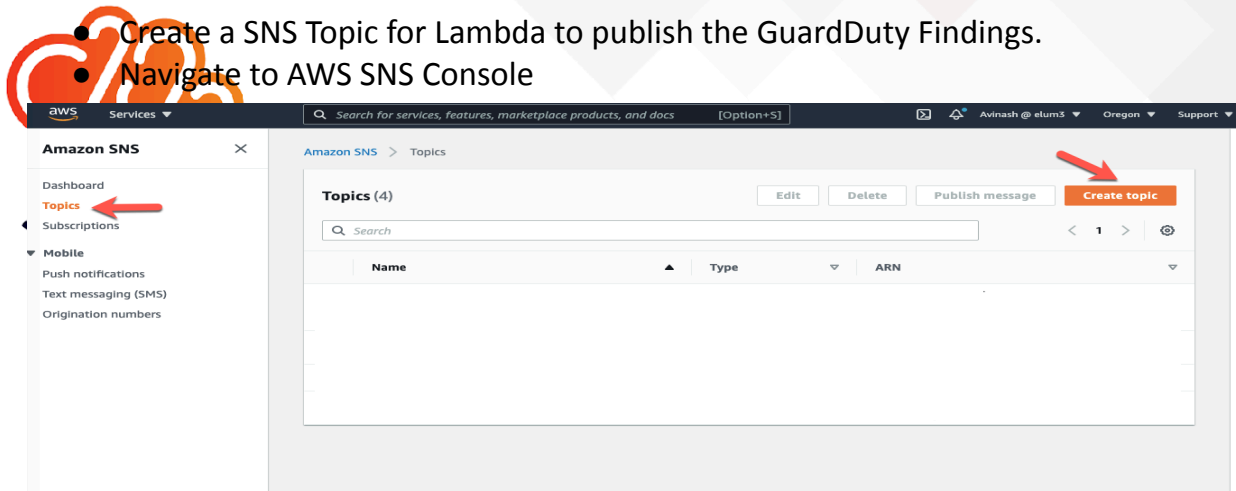
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



- Create a SNS Topic for Lambda to publish the GuardDuty Findings.
- Navigate to AWS SNS Console



JJ Tech

+1 (410) 8887049
contact@jjtechinc.co



www.jjtechinc.co



14103 Hammermill Field Dr Bowie MD 20720



Create topic

Details

Type [Info](#)

Topic type cannot be modified after topic is created

☐ FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

☒ Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name

JJTech-GuarDuty-SNS

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - optional

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message. [Info](#)

JJTech-GuarDuty-SNS

Maximum 100 characters, including hyphens (-) and underscores (_).

► Encryption - optional

Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

► Access policy - optional

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. [Info](#)

► Delivery retry policy (HTTP/S) - optional

The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section. [Info](#)

► Delivery status logging - optional

These settings configure the logging of message delivery status to CloudWatch Logs. [Info](#)

► Tags - optional

A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. [Learn more](#)

Cancel

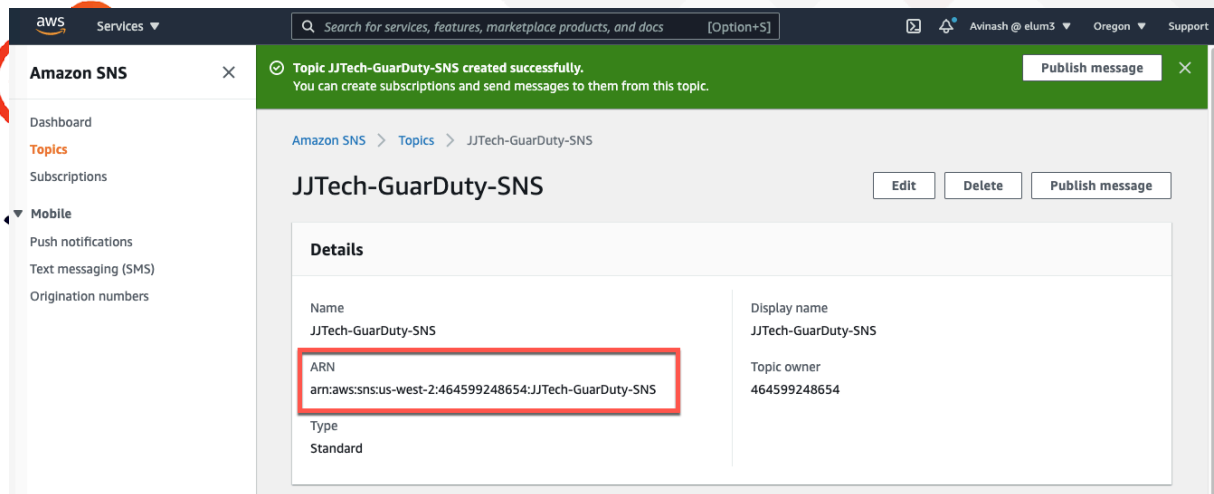
Create topic

+1 (410) 8887049
contact@jjtechinc.co

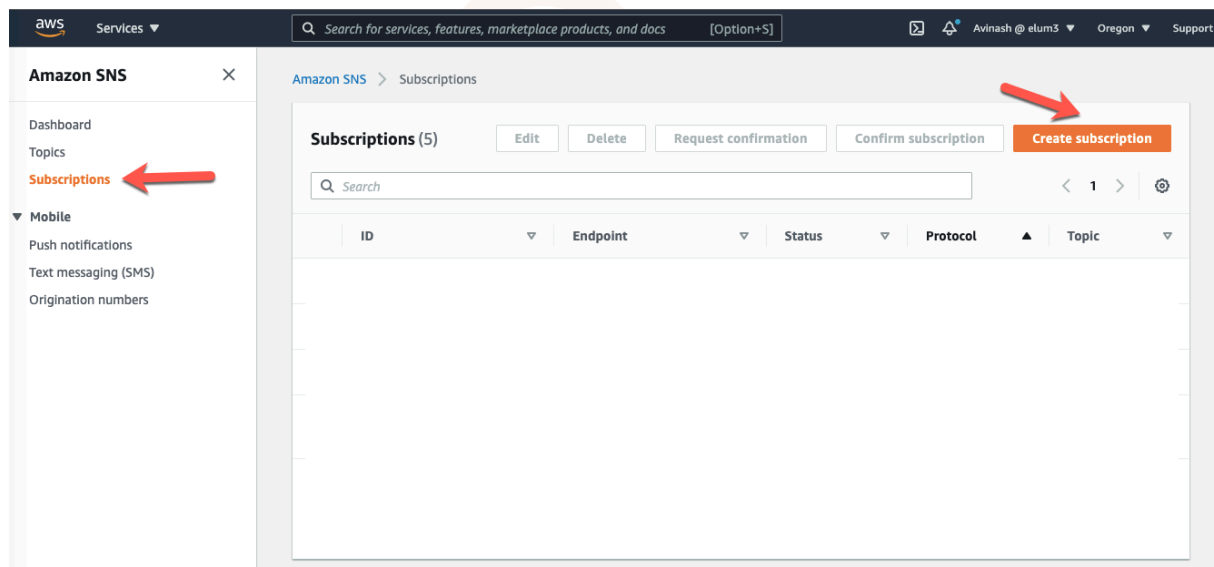
www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





- Now you can subscribe the SNS topic with your mail id.



JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Create subscription

Details

Topic ARN

arn:aws:sns:us-west-2:464599248654:JJTech-GuarDuty-SNS

Protocol

The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

avinash_mamidi@jjtechinc.co

After your subscription is created, you must confirm it. [Info](#)

Subscription filter policy - optional

This policy filters the messages that a subscriber receives. [Info](#)

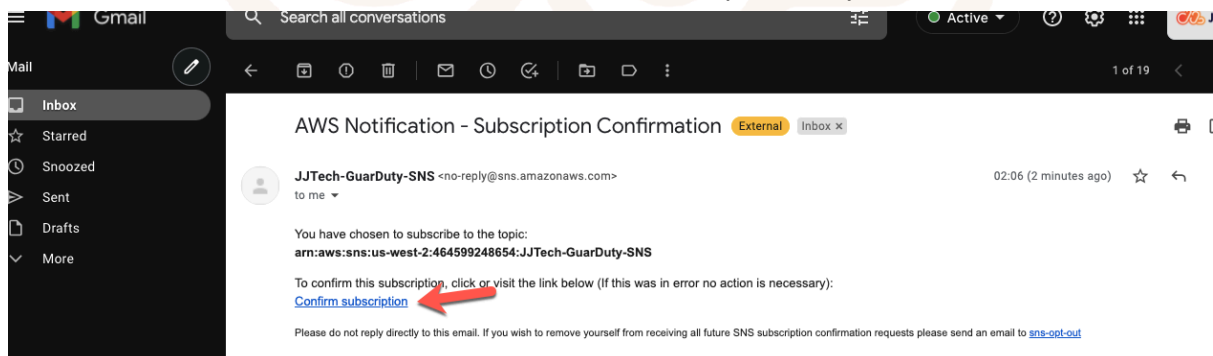
Redrive policy (dead-letter queue) - optional

Send undeliverable messages to a dead-letter queue. [Info](#)

Cancel

Create subscription

- You will receive a mail to confirm the subscription to your mail



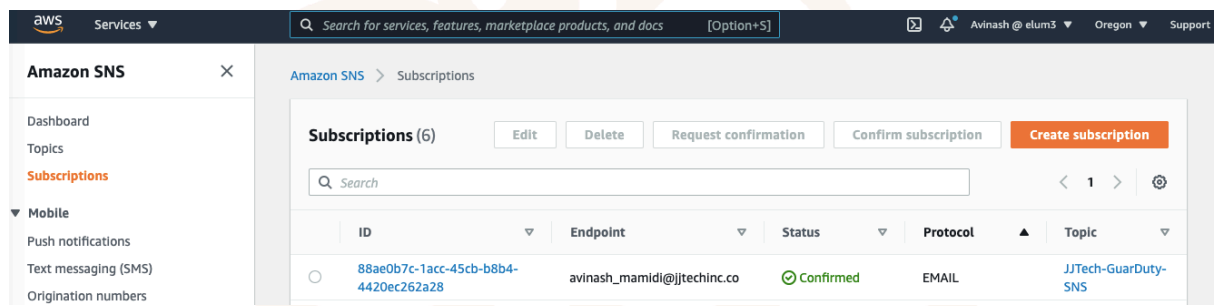
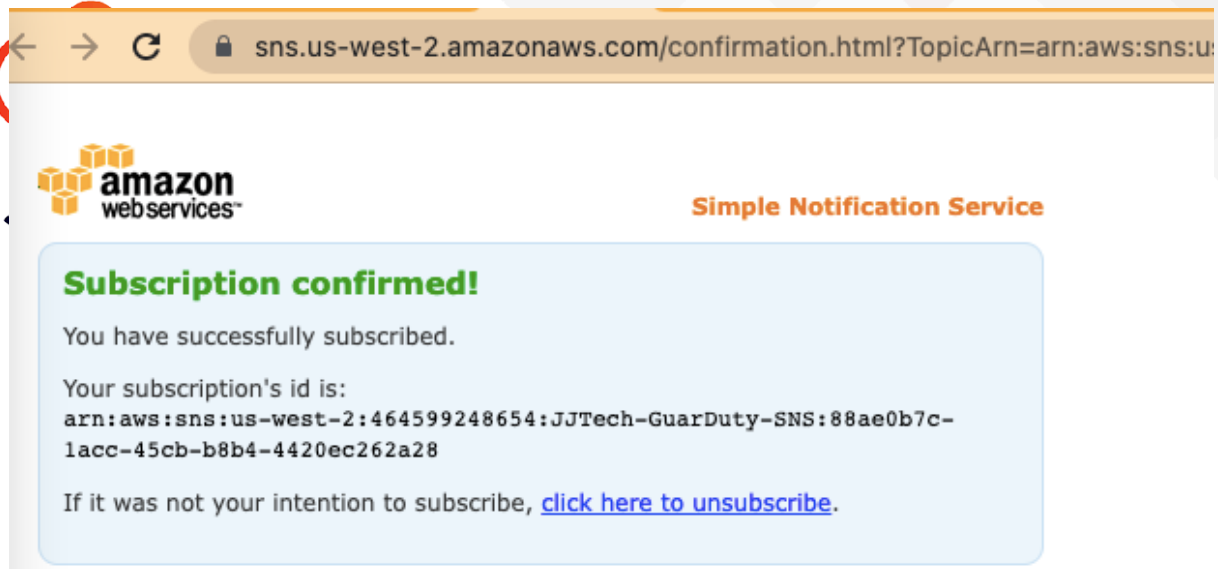
+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

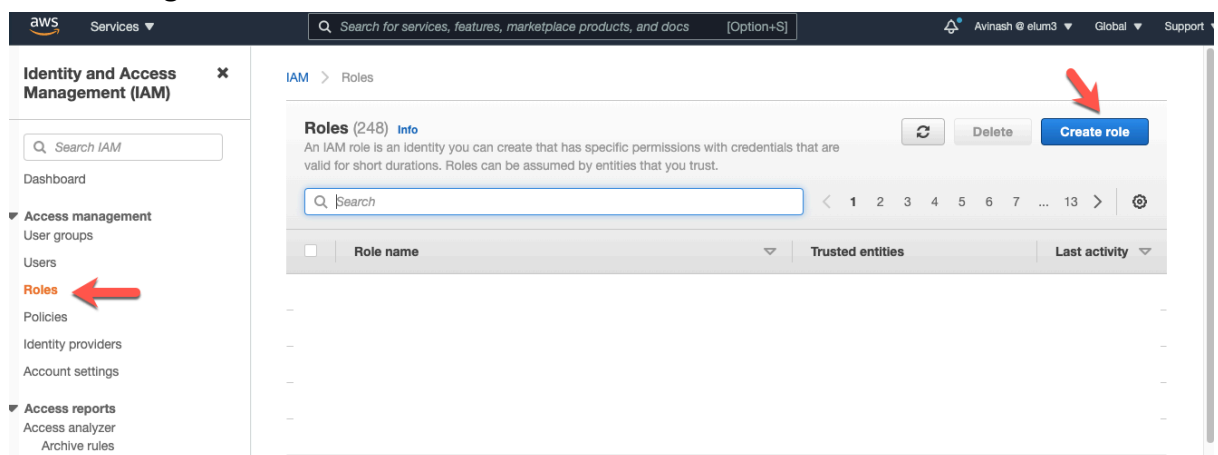
14103 Hammermil Field Dr Bowie MD 20720





Step-2 : Create a IAM role for the Lambda function

- Navigate to IAM Console



+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Create role


1


2


3


4

Select type of trusted entity

**AWS service**
EC2, Lambda and others

**Another AWS account**
Belonging to you or 3rd party

**Web identity**
Cognito or any OpenID provider

**SAML 2.0 federation**
Your corporate directory

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

Choose a use case

Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

| | | | | |
|---------------------------------|--|--|----------------------------------|-----------------------------|
| API Gateway | CloudWatch Events | EMR | IoT SiteWise | RAM |
| AWS Backup | CodeBuild | EMR Containers | IoT Things Graph | RDS |
| AWS Chatbot | CodeDeploy | ElastiCache | KMS | Redshift |
| AWS Marketplace | CodeGuru | Elastic Beanstalk | Kinesis | Rekognition |
| AWS Support | CodeStar Notifications | Elastic Container Registry | Lake Formation | RoboMaker |

* Required

Cancel

Next: Permissions

JJ Tech

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Create role

1

2

3

4

▼ Attach permissions policies

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

Create policy



Filter policies ▼

Q AWSLambdaBasicExecutionRole

Showing 23 results

| | Policy name ▼ | Used as |
|-------------------------------------|---|-------------------------|
| <input checked="" type="checkbox"/> | AWSLambdaBasicExecutionRole | Permissions policy (12) |
| <input type="checkbox"/> | AWSLambdaBasicExecutionRole-0457599d-4b38-4305-b151-902785f8129f | Permissions policy (1) |
| <input type="checkbox"/> | AWSLambdaBasicExecutionRole-07111a140-9353-49c2-b7c3-92f815022c2b | Permissions policy (1) |
| <input type="checkbox"/> | AWSLambdaBasicExecutionRole-0c444622-3756-4643-9407-882745b780f6 | Permissions policy (1) |
| <input type="checkbox"/> | AWSLambdaBasicExecutionRole-22739936-14ff-4c3e-9d0b-86203c68ca4a | Permissions policy (1) |
| <input type="checkbox"/> | AWSLambdaBasicExecutionRole-2a548e4d-30d7-411c-9dde-59eae2caf03a | Permissions policy (1) |
| <input type="checkbox"/> | AWSLambdaBasicExecutionRole-33d56a2e-e2f6-449f-85a3-ea9995745d60 | Permissions policy (1) |
| <input type="checkbox"/> | AWSLambdaBasicExecutionRole-376732c7-5125-4ef2-a13a-acb539df12d8 | Permissions policy (1) |

► Set permissions boundary

* Required

Cancel

Previous

Next: Tags

bas

JJ Tech

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Create role

1234

Review

Provide the required information below and review this role before you create it.

Role name*

JJTech-GuardDuty-Lambda-Role

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

Role description


Allows Lambda functions to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities

AWS service: lambda.amazonaws.com

Policies

 AWSLambdaBasicExecutionRole [↗](#)

Permissions boundary

Permissions boundary is not set

No tags were added.

* Required

Cancel

Previous

Create role

- Navigate to the role you created

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles**
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)

Summary Delete role

Role ARN arn:aws:iam::464599248654:role/JJTech-GuardDuty-Lambda-Role

Role description Allows Lambda functions to call AWS services on your behalf. [Edit](#)

Instance Profile ARNs [Copy](#)

Path /

Creation time 2021-11-04 02:30 UTC+0530

Last activity Not accessed in the tracking period

Maximum session duration 1 hour [Edit](#)

Permissions Trust relationships Tags Access Advisor Revoke sessions

Permissions policies (1 policy applied)

[Attach policies](#) [Add inline policy](#)

| Policy name | Policy type |
|---|--------------------|
| AWSLambdaBasicExecutionRole | AWS managed policy |

- Update the SNS Topic ARN which was created in Step -

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": "<ARN-OF-YOUR-SNS-TOPIC>"
    }
  ]
}
```

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Create policy

1 2

Review policy

Before you create this policy, provide the required information and review this policy.

Name* SNS-topic-access

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Summary

Filter

| Service | Access level | Resource | Request condition |
|--|----------------|---|-------------------|
| Allow (1 of 299 services) Show remaining 298 | | | |
| SNS | Limited: Write | TopicName string like JJTech-GuarDuty-SNS | None |

* Required

Cancel

Previous

Create policy

Step 3: Create Lambda Function

- Navigate to Lambda console

The screenshot shows the AWS Lambda console. The left sidebar has a 'Functions' link highlighted with a red arrow. The main content area shows the 'Functions (29)' page with a 'Create function' button highlighted with a red arrow. The page includes a search bar, a refresh button, and a table with columns for Function name, Description, Package type, Runtime, Code size, and Last modified.

JJ Tech

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Lambda > Functions > Create function

Create function Info

Choose one of the following options to create your function.

Author from scratch ☒

Start with a simple Hello World example.

Use a blueprint ☐

Build a Lambda application from sample code and configuration presets for common use cases.

Container image ☐

Select a container image to deploy for your function.

Browse serverless app repository ☐

Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name
Enter a name that describes the purpose of your function.

JJTech-GuardDuty-lambda

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Python 3.6

Architecture Info
Choose the instruction set architecture you want for your function code.

☒ x86_64
☐ arm64

Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

☐ Create a new role with basic Lambda permissions
☒ Use an existing role
☐ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

JJTech-GuardDuty-Lambda-Role

[View the JJTech-GuardDuty-Lambda-Role role](#) on the IAM console.

► Advanced settings

Cancel Create function

- Get the code from below link

<https://raw.githubusercontent.com/JJTechInc/Serverless-GuardDuty-Findings-to-SNS/main/Serverless-GuardDuty-Findings-To-SNS.py>

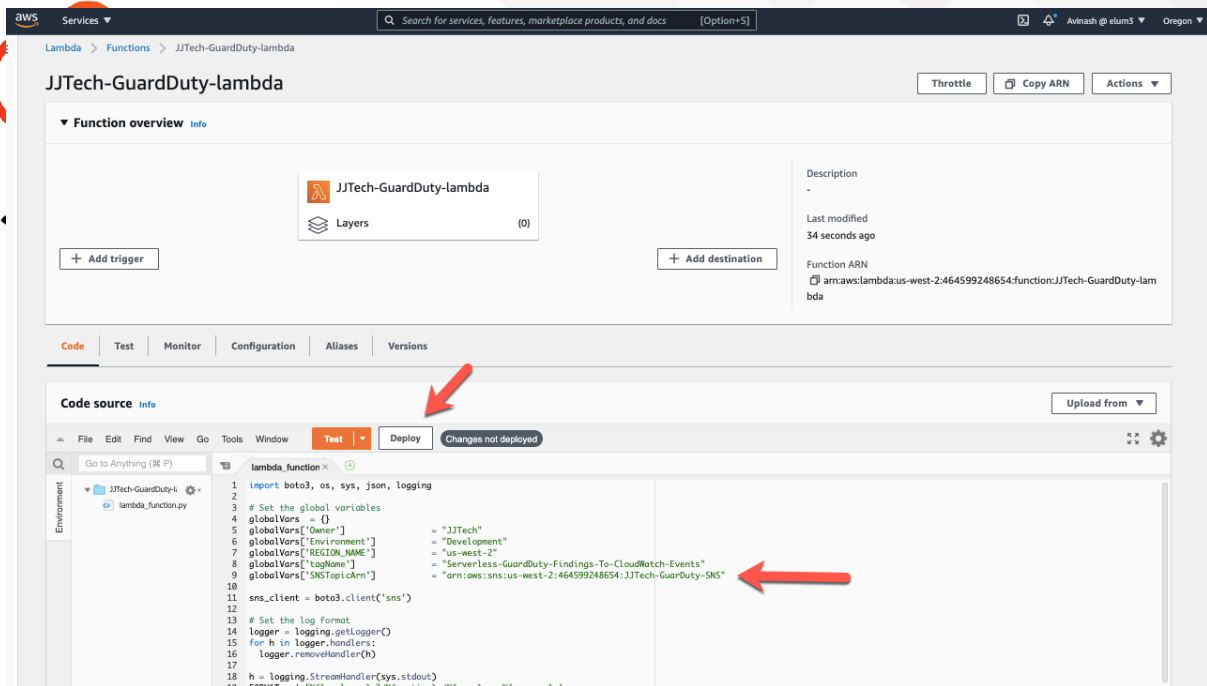
- Change line 9 with your SNS topic ARN you created at Step 1
- Then Deploy the new code to the lambda function

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720





- Now we have to increase the lambda timeout

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Edit basic settings

Basic settings [Info](#)

Description - *optional*

Memory (MB) [Info](#)
Your function is allocated CPU proportional to the memory configured.
 MB
Set memory to between 128 MB and 10240 MB

Timeout
 min sec

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).
☒ Use an existing role
☐ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

[View the JJTech-GuardDuty-Lambda-Role role](#) on the IAM console.

STEP 4: Create Cloudwatch rule to trigger the lambda

- Create Cloudwatch rule to trigger lambda whenever New GuardDuty finding is available. So that we will get notified with the details to our mail
- Navigate to EventBridge console

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Application Integration

Amazon EventBridge

Build event-driven applications at scale

Amazon EventBridge is a serverless event bus that makes it easier to build event-driven applications at scale using events generated from your applications, integrated Software-as-a-Service (SaaS) applications, and AWS services.

Create a new rule

Create a rule. Choose an AWS service, SaaS app or custom app as event source, define event pattern, and attach an AWS service or SaaS apps via API Destination as target(s).

Create rule

View rules

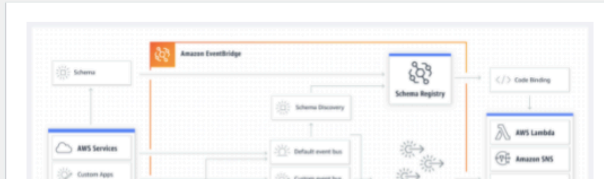
Schema registry

Find existing AWS service event schemas, generate one from an event bus, or create your own custom schemas.

Automatically generate code bindings and IDE integrations for events in EventBridge.

Go to schema registry

How it works



JJ Tech

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



EventBridge - Learning content

Tell us what topics you would like to see more learning material for (tutorials, videos, blog posts, etc.).

[Provide Feedback](#)

Create rule

A rule watches for certain events and then routes them to AWS targets that you choose. You can create a rule that performs an AWS action automatically when another AWS action happens, or a rule that performs an AWS action regularly on a set schedule.

Name and description

Name

JJTech-GuardDuty-Trigger

Maximum of 64 characters consisting of lower/upper case letters, -, _, .

Description - optional

JJTech-GuardDuty-Trigger

Define pattern

Build or customize an Event Pattern or set a Schedule to invoke Targets.

☒ Event pattern [Info](#)

Build a pattern to match events

☐ Schedule [Info](#)

Invoke your targets on a schedule

Event matching pattern

You can use pre-defined pattern provided by a service or create a custom pattern

☒ Pre-defined pattern by service☐ Custom pattern

Service provider

AWS services or custom/partner services

AWS

Service name

The name of partner service selected as the event source

GuardDuty

Event type

The type of events as the source of the matching pattern

GuardDuty Finding

Event pattern

[Copy](#)[Edit](#)

```
1 {
2   "source": ["aws.guardduty"],
3   "detail-type": ["GuardDuty Finding"]
4 }
```

[▶ Sample event\(s\)](#)[▶ Test event pattern](#)

Select event bus

Select an event bus for this rule.

☒ AWS default event bus☐ Custom or partner event bus☒ Enable the rule on the selected event bus

+1 (410) 8887049

@jjtechinc.co

@jjtechinc.co

Baltimore MD 20720



Select targets

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

Target Remove

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

Lambda function

Function

JJTech-GuardDuty-lambda

- ▶ Configure version/alias
- ▶ Configure input
- ▶ Retry policy and dead-letter queue

Add target

Tags - optional

| Key | Value | |
|--|--|-------------------------|
| <input type="text" value="Enter key"/> | <input type="text" value="Enter value"/> | Remove tag |

Add tag

Cancel Create

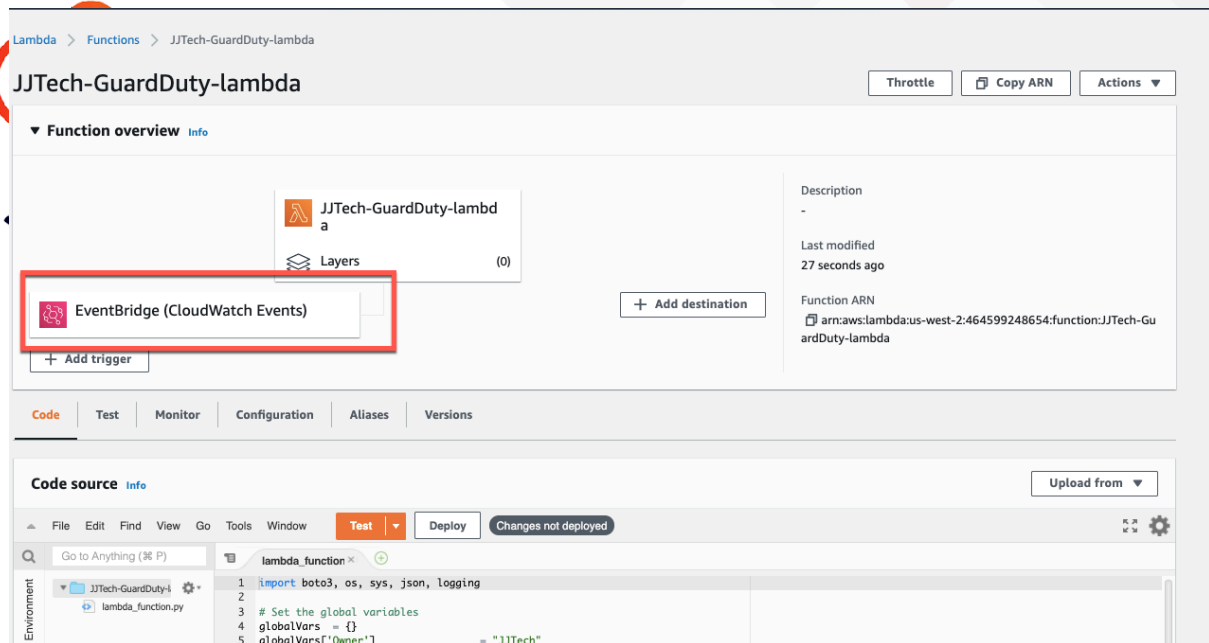
- Now if you navigate to Lambda console you should see below trigger to be configured

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





Step 5: Test the solution

- Navigate to Amazon GuardDuty console
- Let's create some sample findings in Guardduty

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



GuardDuty

Findings
Usage
Settings
Lists
S3 Protection
Accounts

What's New
Partners

Enter account ID (12 digits)

This account will be assigned the two GuardDuty roles required to administer GuardDuty policy in your organization.

Delegate

Findings export options Info

Findings are automatically sent to CloudWatch Events. You can also export findings to an S3 bucket. New findings are exported within 5 minutes. You can modify the frequency for updated findings below.

Frequency for updated findings
Update CWE and S3 every 6 hours (default) Save

S3 bucket

You have not configured findings export to S3 Configure now

Sample findings Info

Sample findings help you visualize and analyze the finding types that GuardDuty generates. When you generate sample findings, GuardDuty populates your current findings list with one sample finding for each finding type.

Generate sample findings

GuardDuty

Findings
Usage

Settings
Lists
S3 Protection
Accounts

What's New
Partners

New feature: GuardDuty is now available in the AWS Asia Pacific (Osaka) Region
You can now extend your continuous security monitoring and threat detection to the AWS Asia Pacific (Osaka) Region. [Learn more](#)

GuardDuty > Findings Showing 74 of 74 12 30 32

Findings Info

Suppress Findings Info

Saved rules No saved rules

Current Add filter criteria

| | Finding type | Resource | Last seen | Count |
|--------------------------|---|--|-----------------|-------|
| <input type="checkbox"/> | [SAMPLE] Behavior:EC2/TrafficVolumeUnusual | Instance: i-999999999 | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] Exfiltration:IAMUser/AnomalousBehavior | GeneratedFindingUserName: GeneratedFindingAccessKe | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] UnauthorizedAccess:IAMUser/TorIPCaller | GeneratedFindingUserName: GeneratedFindingAccessKe | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B | GeneratedFindingUserName: GeneratedFindingAccessKe | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] Cryptocurrency:EC2/BitcoinTool.BIDNS | Instance: i-999999999 | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] UnauthorizedAccess:IAMUser/MaliciousIPCaller | GeneratedFindingUserName: GeneratedFindingAccessKe | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] Exfiltration:S3/ObjectRead.Unusual | GeneratedFindingUserName: GeneratedFindingAccessKe | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] Stealth:S3/ServerAccessLoggingDisabled | GeneratedFindingUserName: GeneratedFindingAccessKe | a few second... | 1 |
| <input type="checkbox"/> | [SAMPLE] UnauthorizedAccess:EC2/MaliciousIPCaller.Custom | Instance: i-999999999 | a few second... | 1 |

- You will receive mails whenever new finding is available in GuardDuty
- Based on the issue you have to fix them

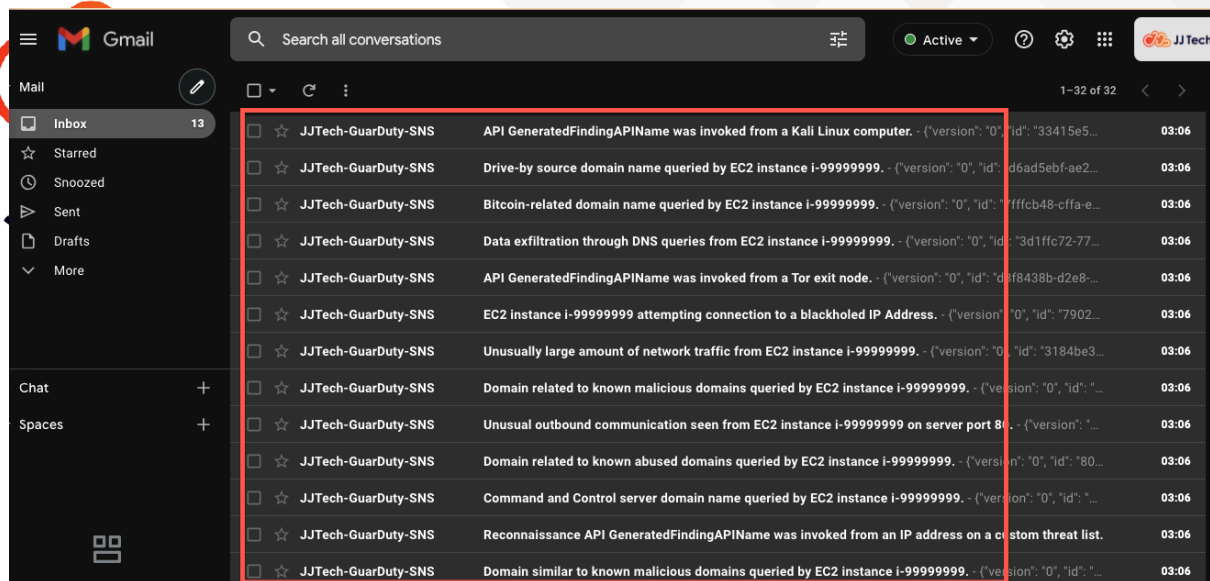
+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





- For example If an EC2 instance got compromised try to terminate
- If an EC2 instance is getting malicious traffic try to block them in NACL or restrict access to respective networks in Security group and so on

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720

