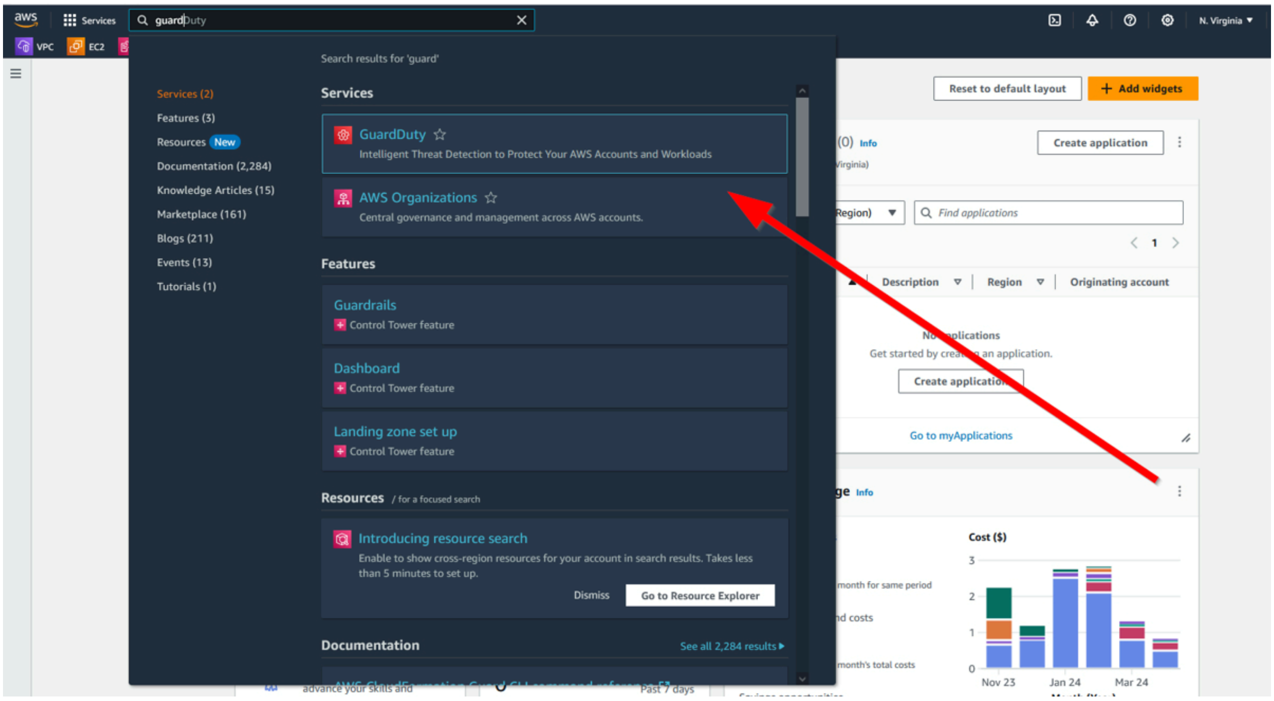
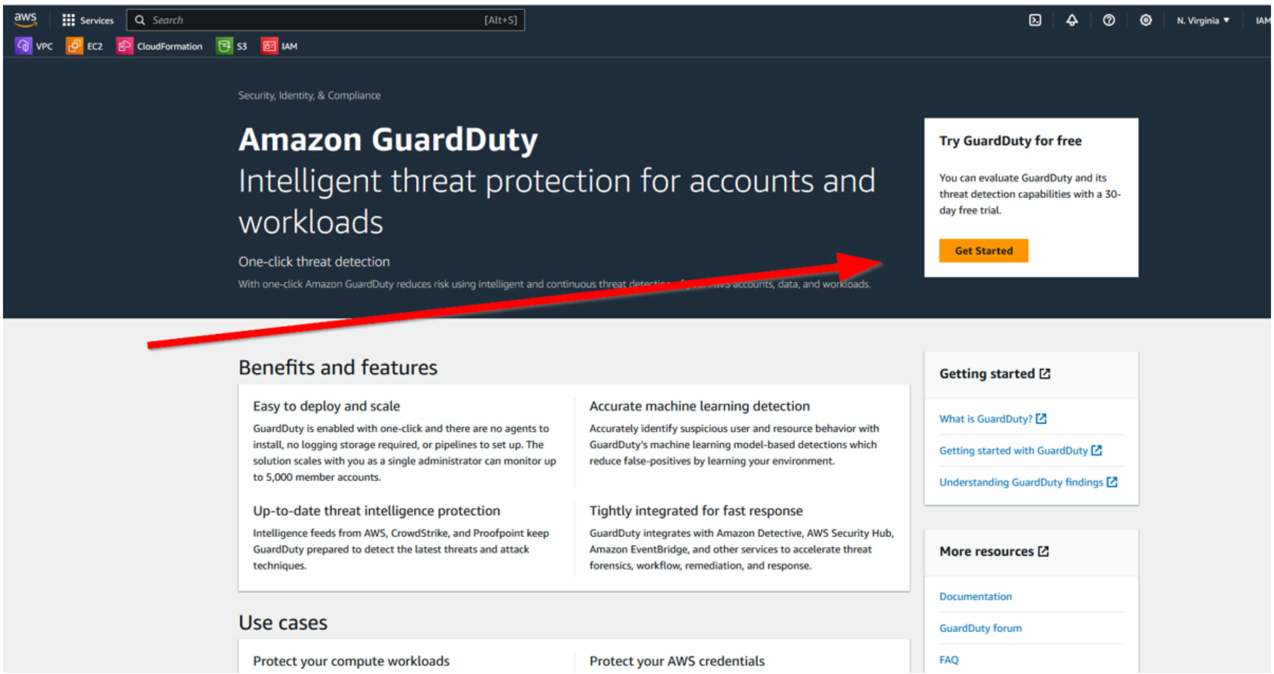
# Cloud Walkthrough: Setting up Emails for AWS GuardDuty Findings

The following is a quick write up I did of how to setup Emails from AWS SNS for alerting on AWS GuardDuty findings within an affected AWS Account using AWS EventBridge.

The following shows how to select the AWS GuardDuty service while also showing the AWS GuardDuty prices that apply to according Log and Cloudtrail analysis that starts after a 30 day trail that everyone should be aware of.





Security, Identity, & Compliance

Amazon GuardDuty

Intelligent threat protection for accounts and workloads

One-click threat detection

With one-click Amazon GuardDuty reduces risk using intelligent and continuous threat detection of your AWS accounts, data, and workloads.

Try GuardDuty for free

You can evaluate GuardDuty and its threat detection capabilities with a 30-day free trial.

Get Started

Benefits and features

Easy to deploy and scale

GuardDuty is enabled with one-click and there are no agents to install, no logging storage required, or pipelines to set up. The solution scales with you as a single administrator can monitor up to 5,000 member accounts.

Accurate machine learning detection

Accurately identify suspicious user and resource behavior with GuardDuty's machine learning model-based detections which reduce false-positives by learning your environment.

Up-to-date threat intelligence protection

Intelligence feeds from AWS, CrowdStrike, and Proofpoint keep GuardDuty prepared to detect the latest threats and attack techniques.

Tightly integrated for fast response

GuardDuty integrates with Amazon Detective, AWS Security Hub, Amazon EventBridge, and other services to accelerate threat forensics, workflow, remediation, and response.

Use cases

Protect your compute workloads

Protect your AWS credentials

Getting started

What is GuardDuty?

Getting started with GuardDuty

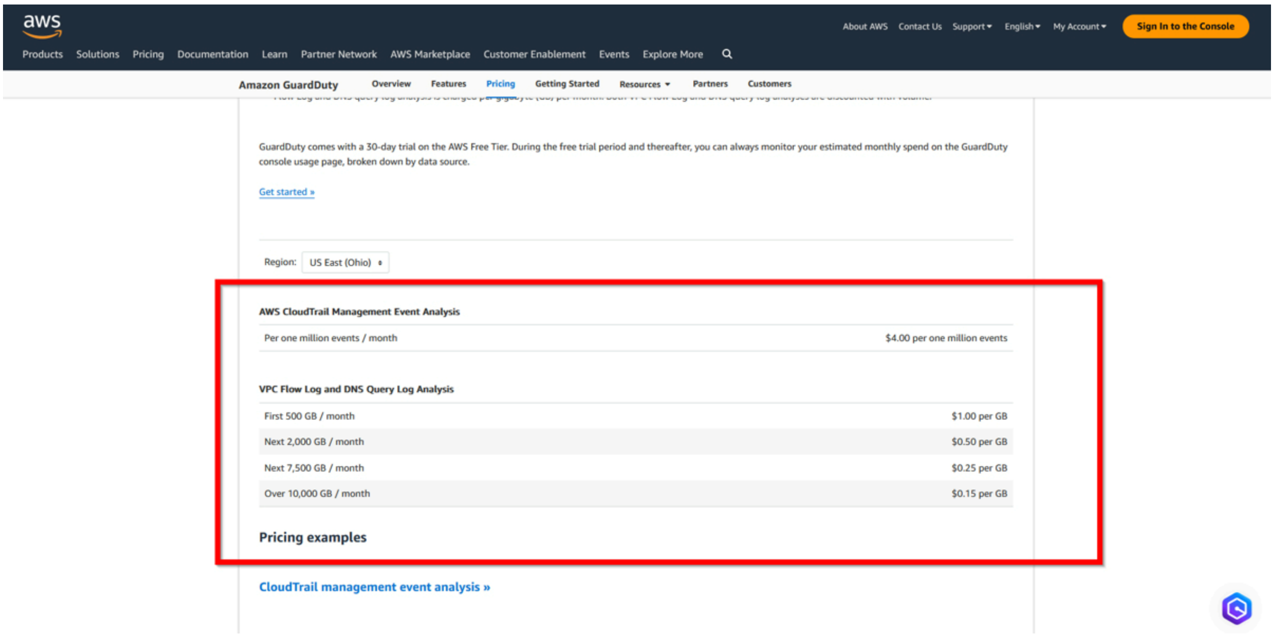
Understanding GuardDuty findings

More resources

Documentation

GuardDuty forum

FAQ



Flow Log and DNS query log analysis is charged per gigabyte (GB) per month. Both VPC Flow Log and DNS query log analyses are discounted with volume.

GuardDuty comes with a 30-day trial on the AWS Free Tier. During the free trial period and thereafter, you can always monitor your estimated monthly spend on the GuardDuty console usage page, broken down by data source.

Get started »

Region: US East (Ohio)

AWS CloudTrail Management Event Analysis

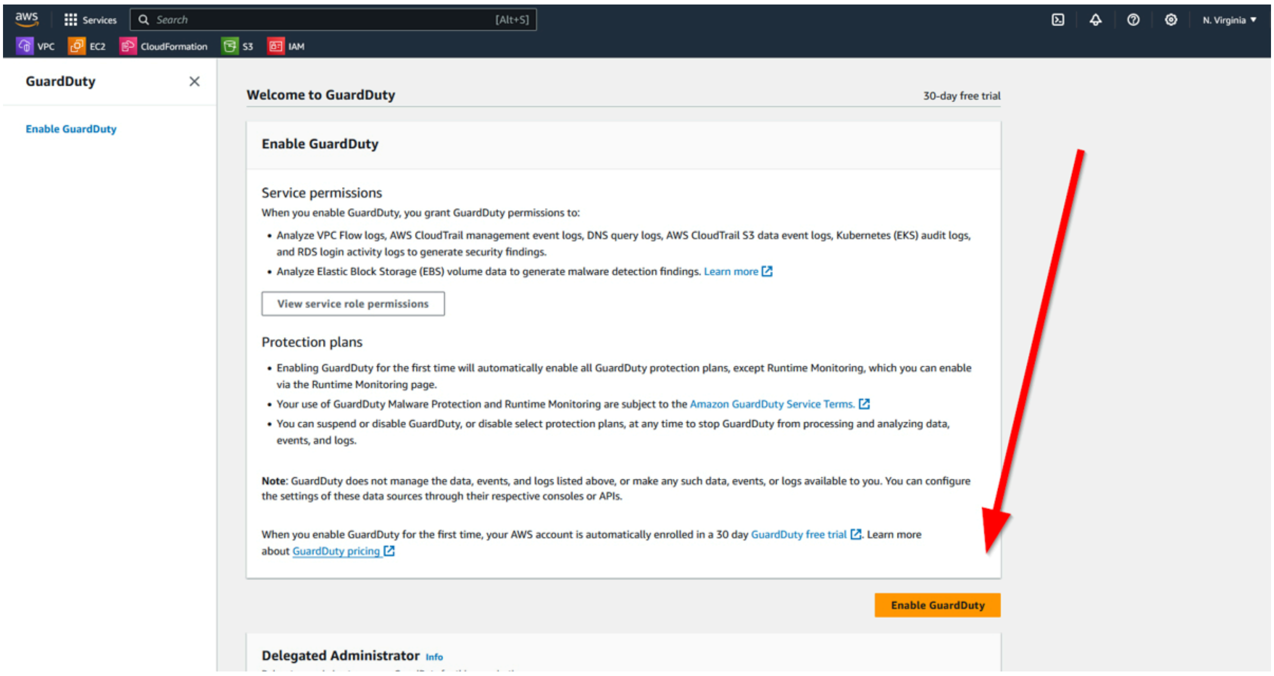
| | |
|---|---|
| Per one million events / month | $4.00 per one million events |

VPC Flow Log and DNS Query Log Analysis

| | |
|---|---|
| First 500 GB / month | $1.00 per GB |
| Next 2,000 GB / month | $0.50 per GB |
| Next 7,500 GB / month | $0.25 per GB |
| Over 10,000 GB / month | $0.15 per GB |

Pricing examples

CloudTrail management event analysis »



Welcome to GuardDuty

30-day free trial

Enable GuardDuty

Service permissions

When you enable GuardDuty, you grant GuardDuty permissions to:

- Analyze VPC Flow logs, AWS CloudTrail management event logs, DNS query logs, AWS CloudTrail S3 data event logs, Kubernetes (EKS) audit logs, and RDS login activity logs to generate security findings.
- Analyze Elastic Block Storage (EBS) volume data to generate malware detection findings. Learn more

View service role permissions

Protection plans

- Enabling GuardDuty for the first time will automatically enable all GuardDuty protection plans, except Runtime Monitoring, which you can enable via the Runtime Monitoring page.
- Your use of GuardDuty Malware Protection and Runtime Monitoring are subject to the Amazon GuardDuty Service Terms.
- You can suspend or disable GuardDuty, or disable select protection plans, at any time to stop GuardDuty from processing and analyzing data, events, and logs.

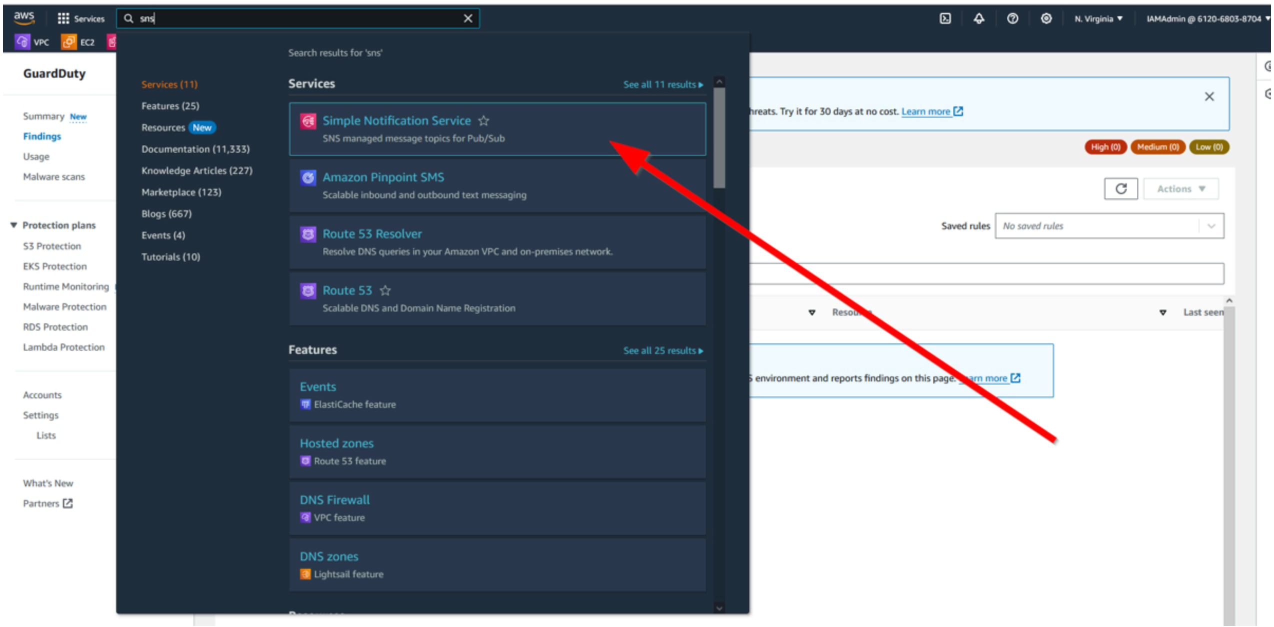
Note: GuardDuty does not manage the data, events, and logs listed above, or make any such data, events, or logs available to you. You can configure the settings of these data sources through their respective consoles or APIs.

When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day GuardDuty free trial. Learn more about GuardDuty pricing

Enable GuardDuty

Delegated Administrator Info

The following shows how to create an AWS SNS Topic for the AWS SNS service that allows for easy alerting in this case alerts to a specified email which will be connected later to AWS GuardDuty findings.



Search results for 'sns'

Services — See all 11 results

Simple Notification Service
SNS managed message topics for Pub/Sub

Amazon Pinpoint SMS
Scalable inbound and outbound text messaging

Route 53 Resolver
Resolve DNS queries in your Amazon VPC and on-premises network.

Route 53
Scalable DNS and Domain Name Registration

Features — See all 25 results

Events
ElastiCache feature

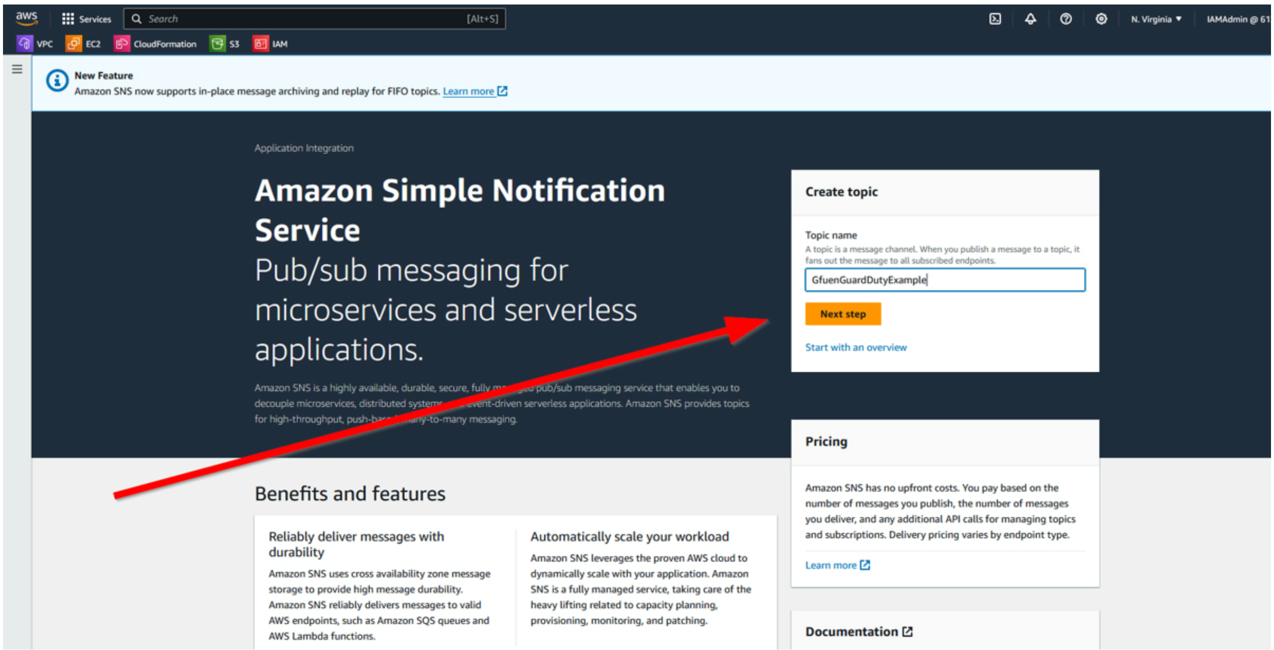
Hosted zones
Route 53 feature

DNS Firewall
VPC feature

DNS zones
Lightsail feature

hreats. Try it for 30 days at no cost. Learn more

environment and reports findings on this page. Learn more



**New Feature**
Amazon SNS now supports in-place message archiving and replay for FIFO topics. Learn more

Application Integration

**Amazon Simple Notification Service**
Pub/sub messaging for microservices and serverless applications.

Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and event-driven serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging.

**Create topic**

Topic name
A topic is a message channel. When you publish a message to a topic, it fans out the message to all subscribed endpoints.
GfuenGuardDutyExample

Next step

Start with an overview

**Pricing**

Amazon SNS has no upfront costs. You pay based on the number of messages you publish, the number of messages you deliver, and any additional API calls for managing topics and subscriptions. Delivery pricing varies by endpoint type.

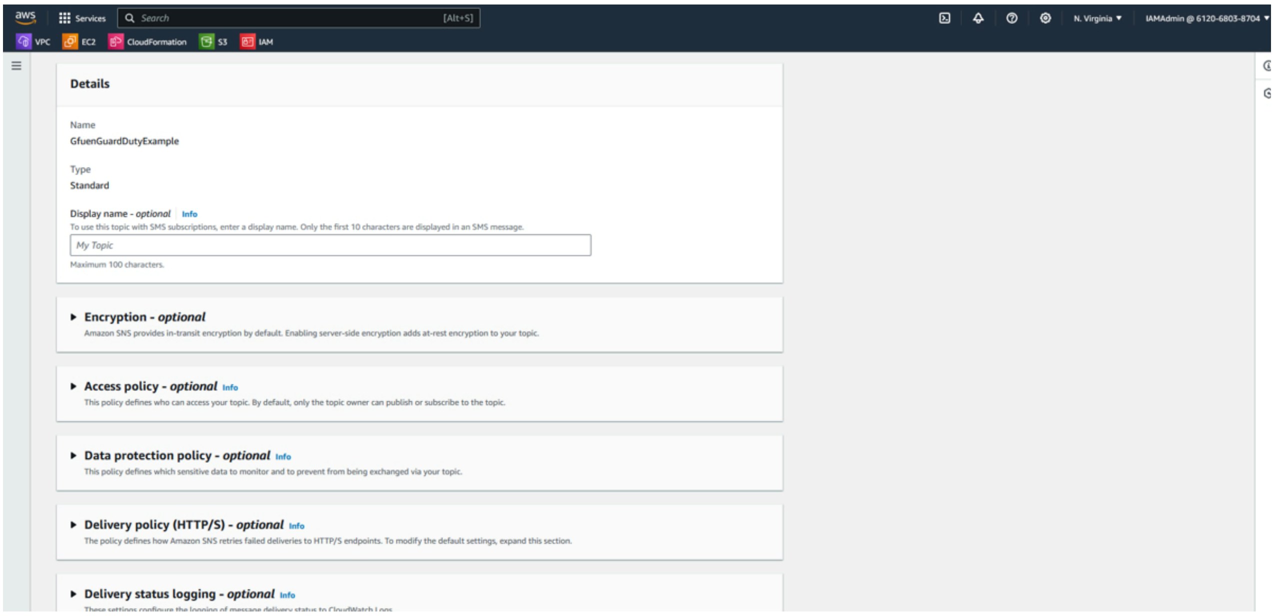
Learn more

**Documentation**

Benefits and features

Reliably deliver messages with durability
Amazon SNS uses cross availability zone message storage to provide high message durability. Amazon SNS reliably delivers messages to valid AWS endpoints, such as Amazon SQS queues and AWS Lambda functions.

Automatically scale your workload
Amazon SNS leverages the proven AWS cloud to dynamically scale with your application. Amazon SNS is a fully managed service, taking care of the heavy lifting related to capacity planning, provisioning, monitoring, and patching.



**Details**

Name
GfuenGuardDutyExample

Type
Standard

Display name - *optional* Info
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.
My Topic
Maximum 100 characters.

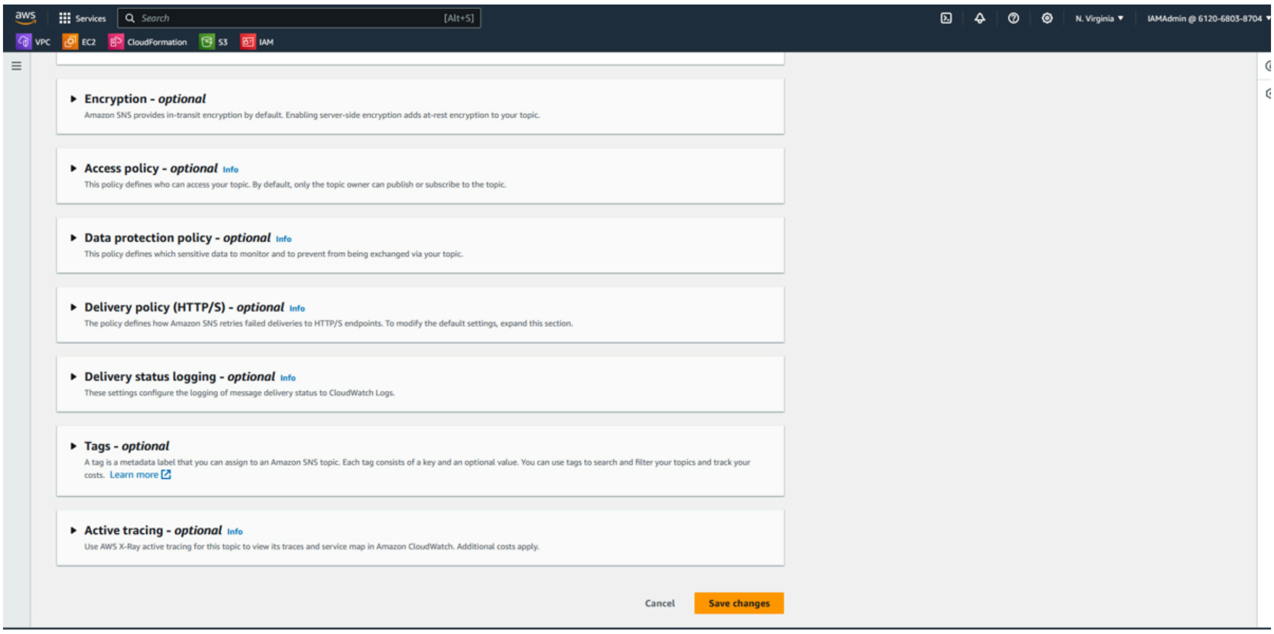
▸ **Encryption - *optional***
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

▸ **Access policy - *optional*** Info
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

▸ **Data protection policy - *optional*** Info
This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

▸ **Delivery policy (HTTP/S) - *optional*** Info
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.

▸ **Delivery status logging - *optional*** Info
These settings configure the logging of message delivery status to CloudWatch Logs



**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.

**Data protection policy - *optional***
This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

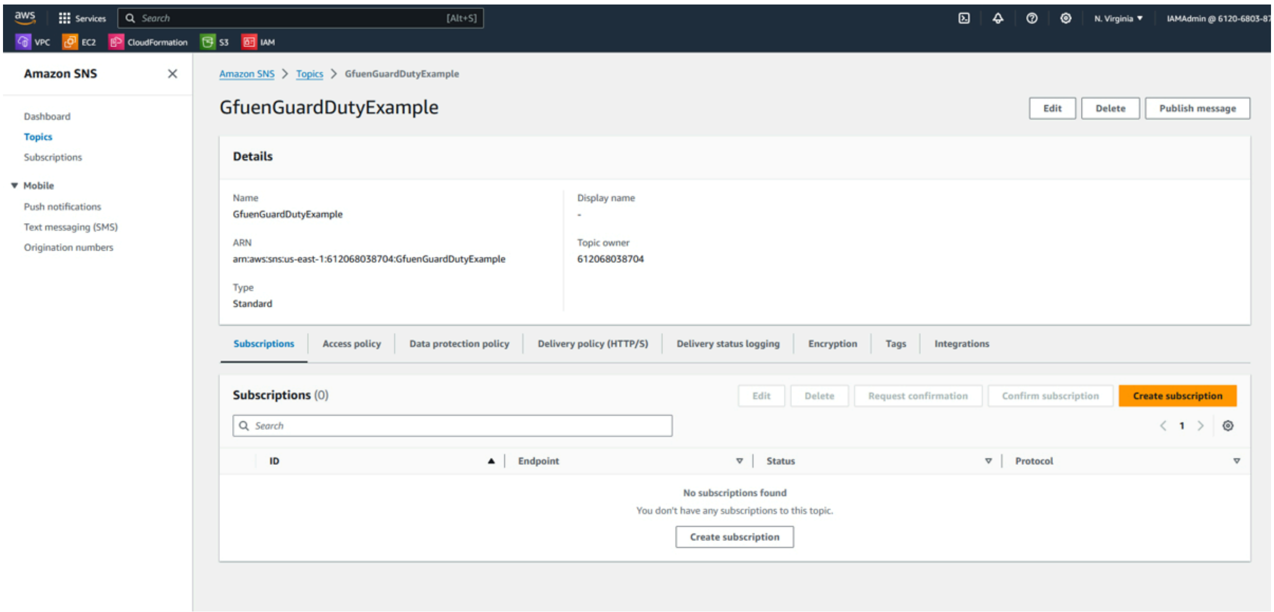
**Delivery policy (HTTP/S) - *optional***
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.

**Delivery status logging - *optional***
These settings configure the logging of message delivery status to CloudWatch Logs.

**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.

**Active tracing - *optional***
Use AWS X-Ray active tracing for this topic to view its traces and service map in Amazon CloudWatch. Additional costs apply.

The following shows to enable the AWS SNS Topic to be subscribed to an email for easy alerting according to the AWS administrator.



GfuenGuardDutyExample

**Details**

Name
GfuenGuardDutyExample

ARN
arn:aws:sns:us-east-1:612068038704:GfuenGuardDutyExample

Type
Standard

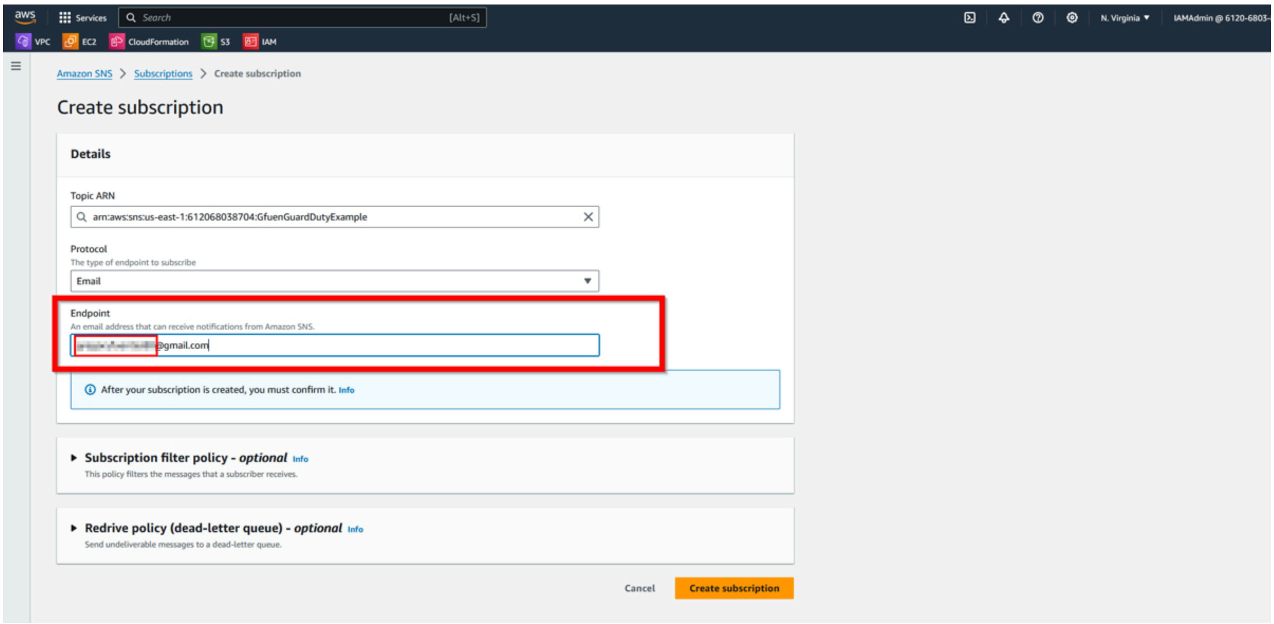
Display name
-

Topic owner
612068038704

**Subscriptions** (0)

| ID | Endpoint | Status | Protocol |
|---|---|---|---|

No subscriptions found
You don't have any subscriptions to this topic.



Create subscription

Details

Topic ARN: arn:aws:sns:us-east-1:612068038704:GfuenGuardDutyExample

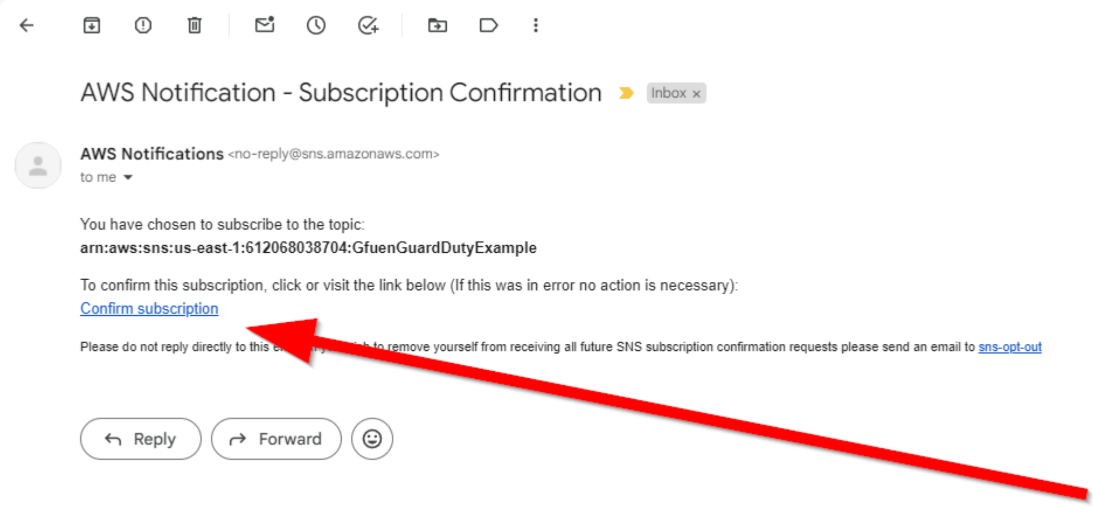
Protocol
The type of endpoint to subscribe
Email

Endpoint
An email address that can receive notifications from Amazon SNS.
[redacted]@gmail.com

After your subscription is created, you must confirm it. Info

▸ Subscription filter policy - *optional* Info
This policy filters the messages that a subscriber receives.

▸ Redrive policy (dead-letter queue) - *optional* Info
Send undeliverable messages to a dead-letter queue.



AWS Notification - Subscription Confirmation

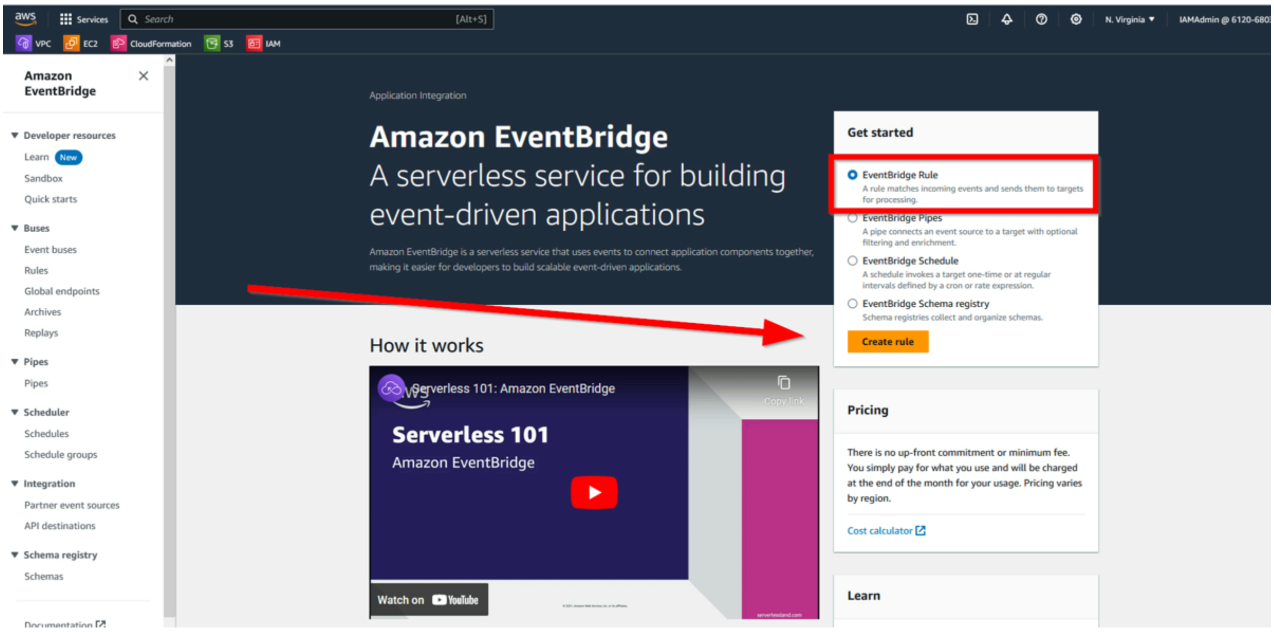
**AWS Notifications** <no-reply@sns.amazonaws.com>
to me ▾

You have chosen to subscribe to the topic:
**arn:aws:sns:us-east-1:612068038704:GfuenGuardDutyExample**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription

Please do not reply directly to this e[illegible] to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

Finally, the following shows how to access and create an AWS EventBridge rule where configuration allows AWS GuardDuty All Events to trigger the AWS SNS Topic which then will allow an alert to go to the specified subscribed email setup earlier.



Application Integration

## Amazon EventBridge

A serverless service for building event-driven applications

Amazon EventBridge is a serverless service that uses events to connect application components together, making it easier for developers to build scalable event-driven applications.

How it works

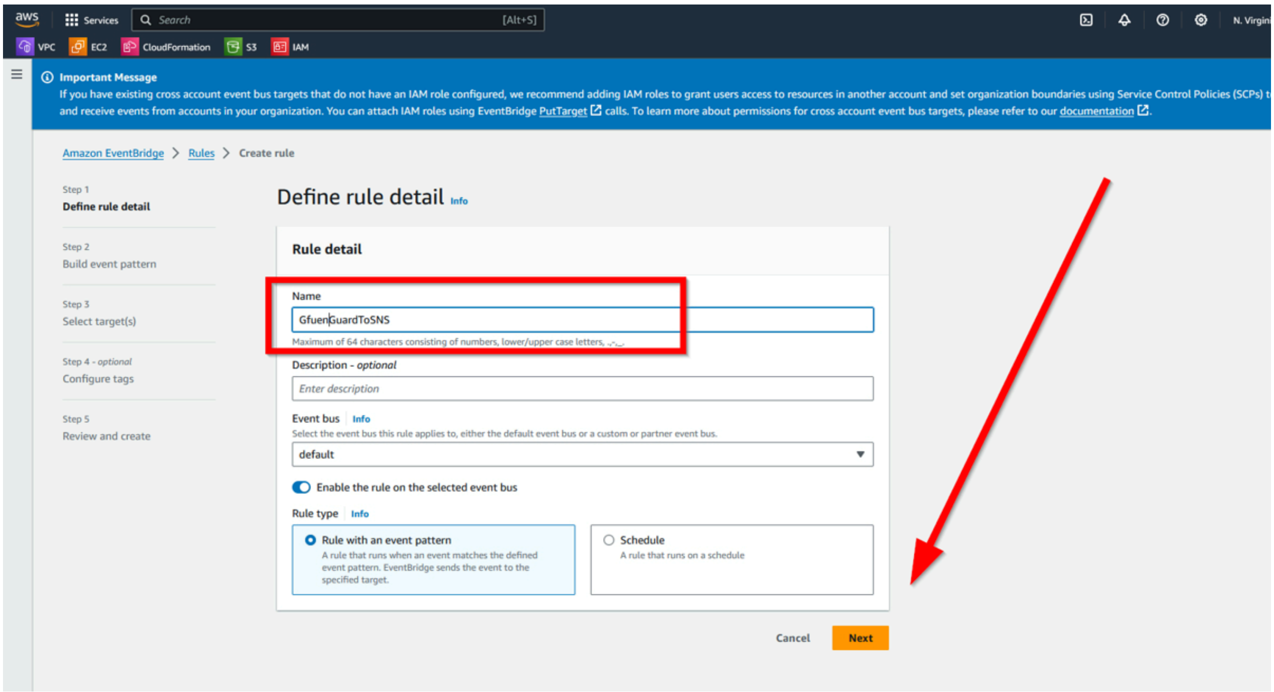
Get started

- ● EventBridge Rule
  A rule matches incoming events and sends them to targets for processing.
- ○ EventBridge Pipes
  A pipe connects an event source to a target with optional filtering and enrichment.
- ○ EventBridge Schedule
  A schedule invokes a target one-time or at regular intervals defined by a cron or rate expression.
- ○ EventBridge Schema registry
  Schema registries collect and organize schemas.

Create rule

Pricing

There is no up-front commitment or minimum fee. You simply pay for what you use and will be charged at the end of the month for your usage. Pricing varies by region.



Important Message
If you have existing cross account event bus targets that do not have an IAM role configured, we recommend adding IAM roles to grant users access to resources in another account and set organization boundaries using Service Control Policies (SCPs) t and receive events from accounts in your organization. You can attach IAM roles using EventBridge PutTarget calls. To learn more about permissions for cross account event bus targets, please refer to our documentation.

Amazon EventBridge > Rules > Create rule

Step 1
Define rule detail

Step 2
Build event pattern

Step 3
Select target(s)

Step 4 - *optional*
Configure tags

Step 5
Review and create

Define rule detail Info

Rule detail

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

Description - *optional*
Enter description

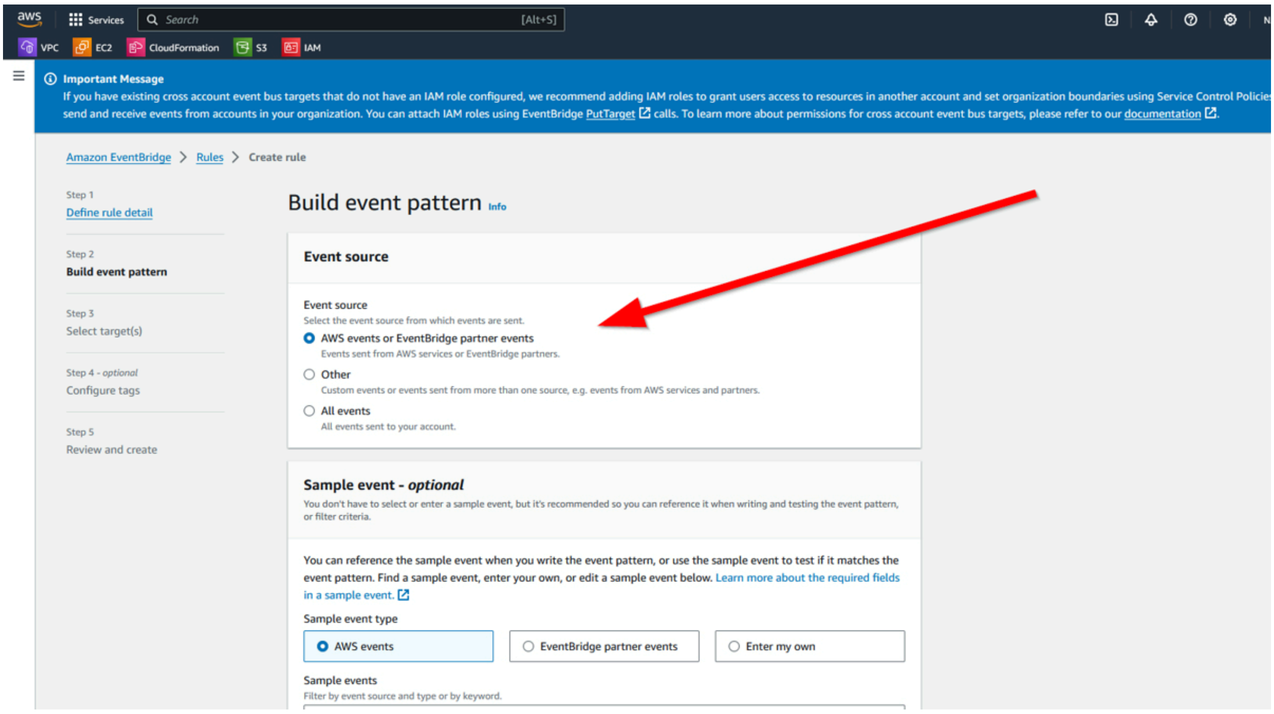
Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default

Enable the rule on the selected event bus

Rule type Info

- ● Rule with an event pattern
  A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
- ○ Schedule
  A rule that runs on a schedule

Cancel Next



**Important Message**
If you have existing cross account event bus targets that do not have an IAM role configured, we recommend adding IAM roles to grant users access to resources in another account and set organization boundaries using Service Control Policie send and receive events from accounts in your organization. You can attach IAM roles using EventBridge PutTarget calls. To learn more about permissions for cross account event bus targets, please refer to our documentation.

Amazon EventBridge > Rules > Create rule

Step 1
Define rule detail

Step 2
Build event pattern

Step 3
Select target(s)

Step 4 - *optional*
Configure tags

Step 5
Review and create

## Build event pattern Info

**Event source**

Event source
Select the event source from which events are sent.

● AWS events or EventBridge partner events
Events sent from AWS services or EventBridge partners.

○ Other
Custom events or events sent from more than one source, e.g. events from AWS services and partners.

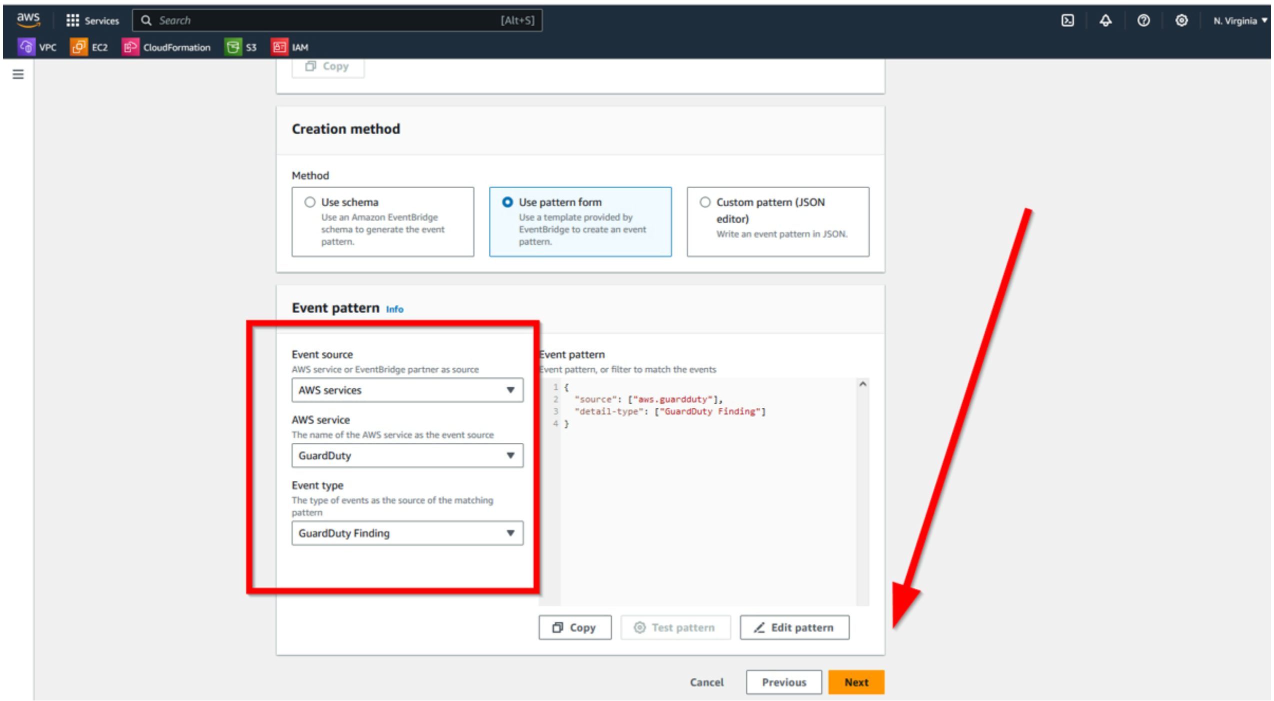
○ All events
All events sent to your account.

**Sample event - *optional***
You don't have to select or enter a sample event, but it's recommended so you can reference it when writing and testing the event pattern, or filter criteria.

You can reference the sample event when you write the event pattern, or use the sample event to test if it matches the event pattern. Find a sample event, enter your own, or edit a sample event below. Learn more about the required fields in a sample event.

Sample event type
● AWS events ○ EventBridge partner events ○ Enter my own

Sample events
Filter by event source and type or by keyword.



**Creation method**

Method

○ Use schema
Use an Amazon EventBridge schema to generate the event pattern.

● Use pattern form
Use a template provided by EventBridge to create an event pattern.

○ Custom pattern (JSON editor)
Write an event pattern in JSON.

**Event pattern** Info

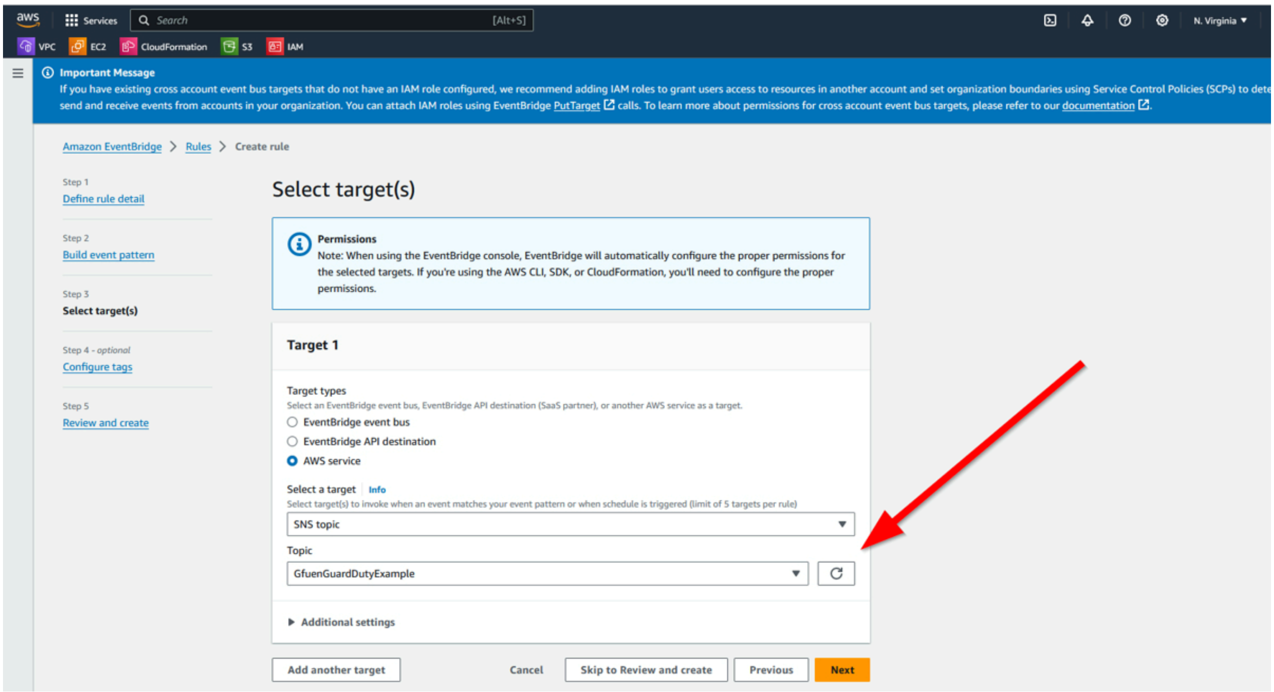
Event source
AWS service or EventBridge partner as source
AWS services

AWS service
The name of the AWS service as the event source
GuardDuty

Event type
The type of events as the source of the matching pattern
GuardDuty Finding

Event pattern
Event pattern, or filter to match the events

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



**Important Message**
If you have existing cross account event bus targets that do not have an IAM role configured, we recommend adding IAM roles to grant users access to resources in another account and set organization boundaries using Service Control Policies (SCPs) to dete
send and receive events from accounts in your organization. You can attach IAM roles using EventBridge PutTarget calls. To learn more about permissions for cross account event bus targets, please refer to our documentation.

Amazon EventBridge > Rules > Create rule

Select target(s)

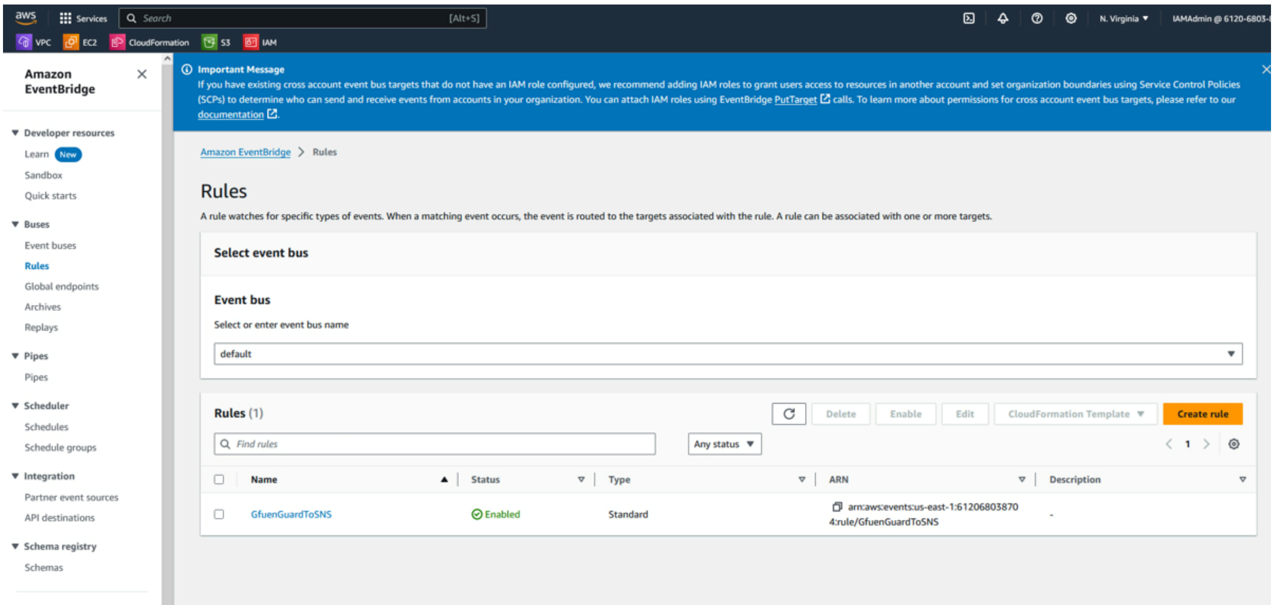
**Permissions**
Note: When using the EventBridge console, EventBridge will automatically configure the proper permissions for the selected targets. If you're using the AWS CLI, SDK, or CloudFormation, you'll need to configure the proper permissions.

**Target 1**

Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.
○ EventBridge event bus
○ EventBridge API destination
● AWS service

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

Topic
GfuenGuardDutyExample



**Important Message**
If you have existing cross account event bus targets that do not have an IAM role configured, we recommend adding IAM roles to grant users access to resources in another account and set organization boundaries using Service Control Policies (SCPs) to determine who can send and receive events from accounts in your organization. You can attach IAM roles using EventBridge PutTarget calls. To learn more about permissions for cross account event bus targets, please refer to our documentation.

Amazon EventBridge > Rules

Rules

A rule watches for specific types of events. When a matching event occurs, the event is routed to the targets associated with the rule. A rule can be associated with one or more targets.

**Select event bus**

**Event bus**
Select or enter event bus name
default

**Rules** (1)

| □ | Name | Status | Type | ARN | Description |
|---|---|---|---|---|---|
| □ | GfuenGuardToSNS | ✓ Enabled | Standard | arn:aws:events:us-east-1:612068038704:rule/GfuenGuardToSNS | - |