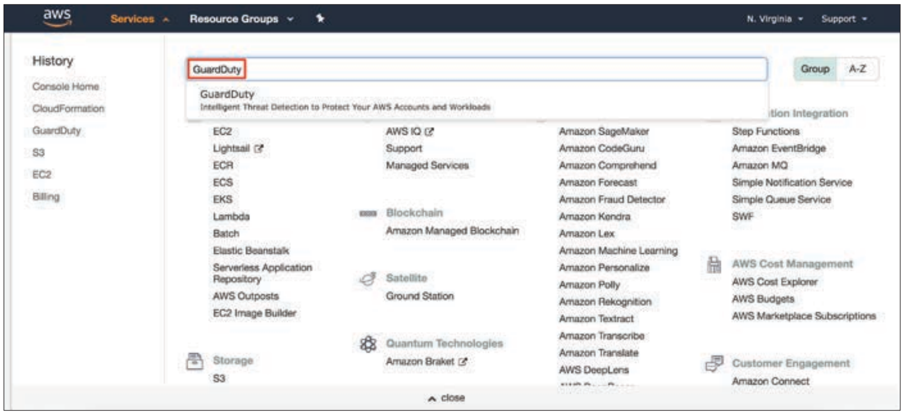
INSTALL GUIDE

Amazon GuardDuty Installation Guide

This guide will describe the steps involved in integrating Recorded Future as a threat intelligence detection source in Amazon GuardDuty. Please note that there are expansive permissions required within S3, CloudWatch, Lambda, IAM, SSM Parameter Store, and GuardDuty to complete this integration. If you do not have sufficient permissions, please contact your AWS Administrator.

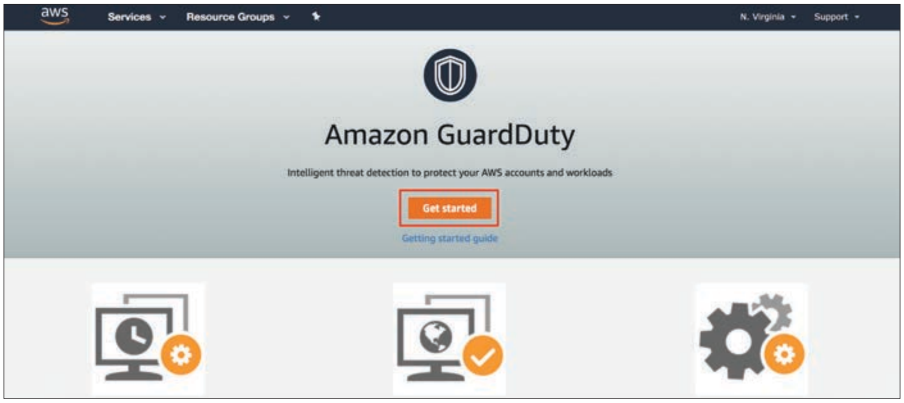
Ensure Amazon GuardDuty Is Enabled

Search for GuardDuty from within your AWS console. Select "GuardDuty".

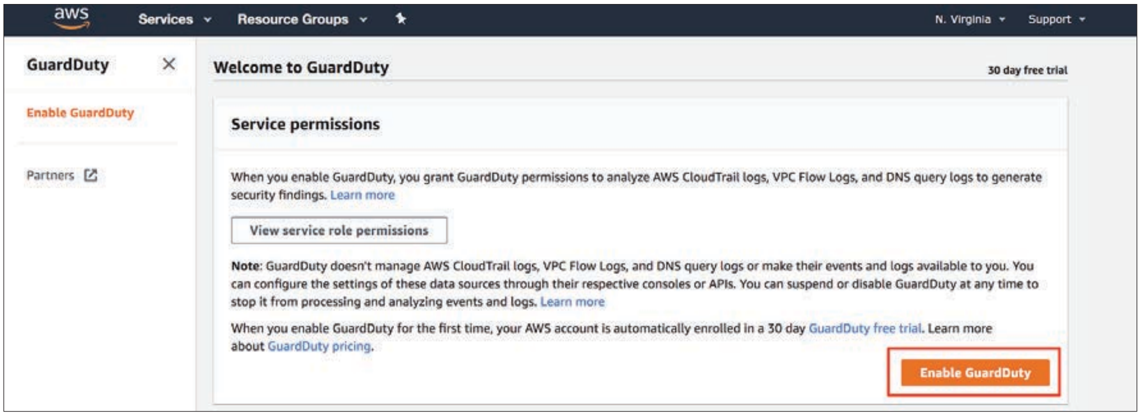


Next, click "Get Started".

Note: This screen will only be available if Amazon GuardDuty has not been previously enabled. If you do not see this screen, Amazon GuardDuty is most likely already enabled, and you may disregard this step.



Click on “Enable GuardDuty”



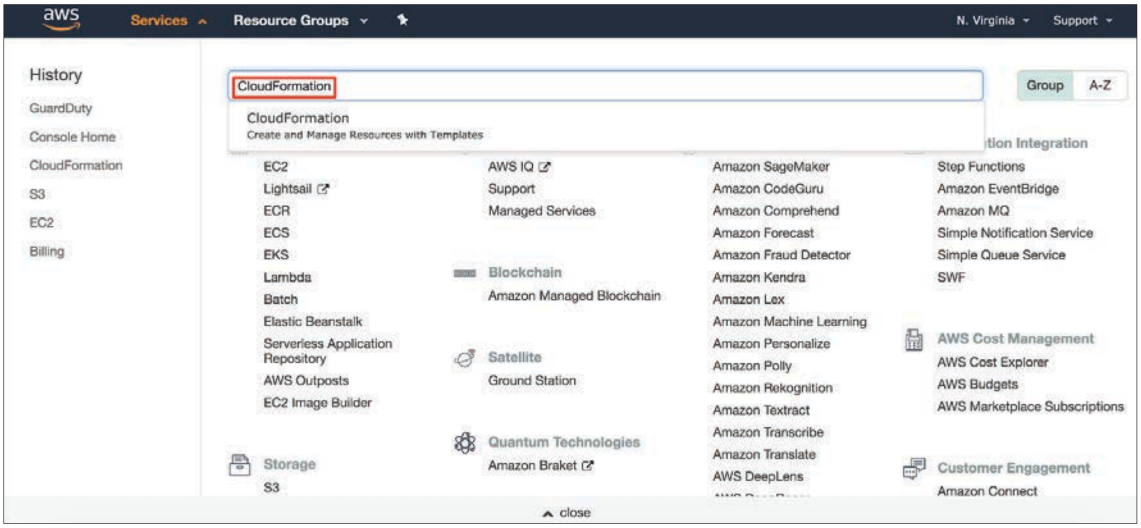
When you enable GuardDuty, you grant GuardDuty permissions to analyze AWS CloudTrail logs, VPC Flow Logs, and DNS query logs to generate security findings. Learn more

Note: GuardDuty doesn't manage AWS CloudTrail logs, VPC Flow Logs, and DNS query logs or make their events and logs available to you. You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable GuardDuty at any time to stop it from processing and analyzing events and logs. Learn more

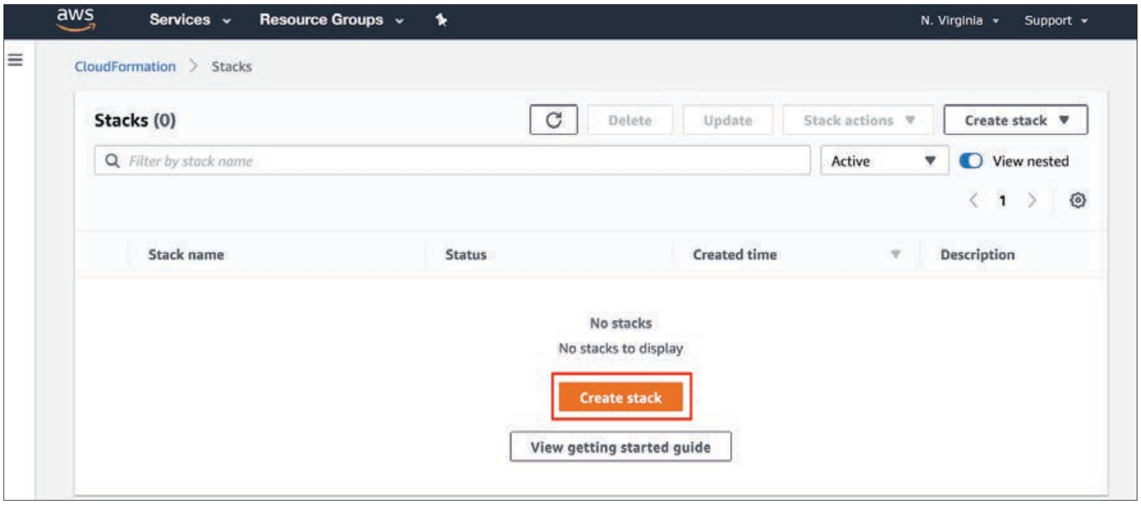
When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day GuardDuty free trial. Learn more about GuardDuty pricing.

Creating a Stack

Navigate to Cloud Formation within your AWS Console.



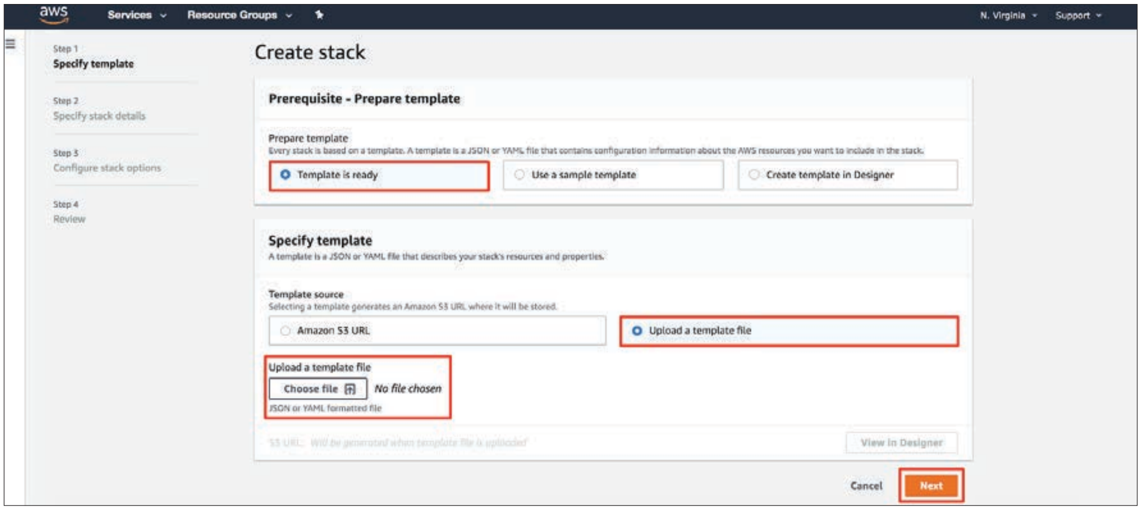
Select “Create Stack”



No stacks

No stacks to display

Select “Template is ready” and “Upload a template file” from the menu screen.
Select “Choose File” and upload the Recorded Future Cloud Formation Template.
Then select “Next”.



Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

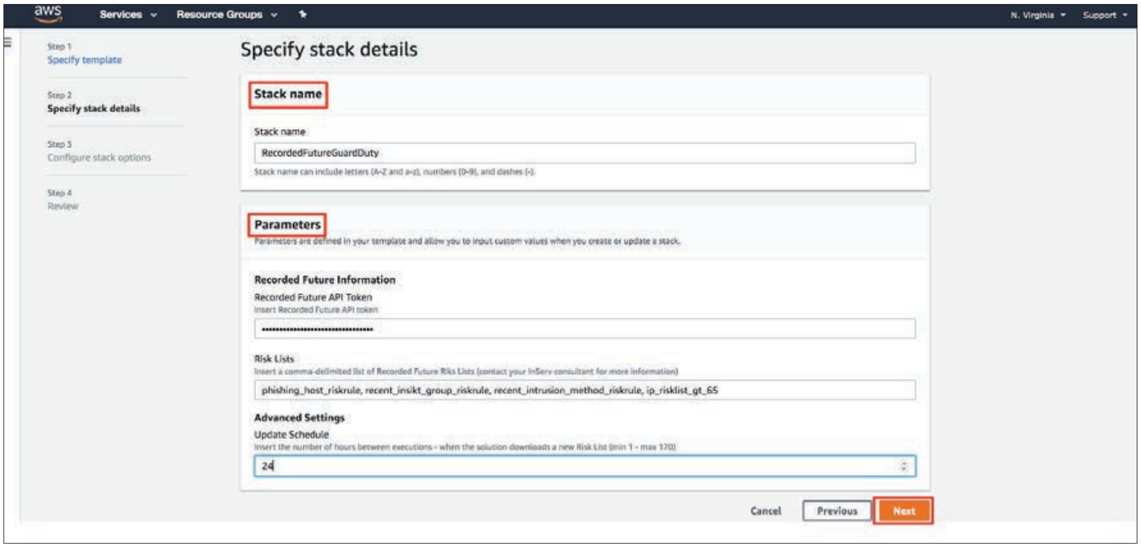
○ Amazon S3 URL ● Upload a template file

Upload a template file
Choose file No file chosen
JSON or YAML formatted file

S3 URL: Will be generated when template file is uploaded

Specify stack parameters and select “Next” to continue.

Note: An API token from Recorded Future is required for this step. Please reach out to your account manager to obtain an API token for this integration.



Specify stack details

Stack name

Stack name
RecordedFutureGuardDuty
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

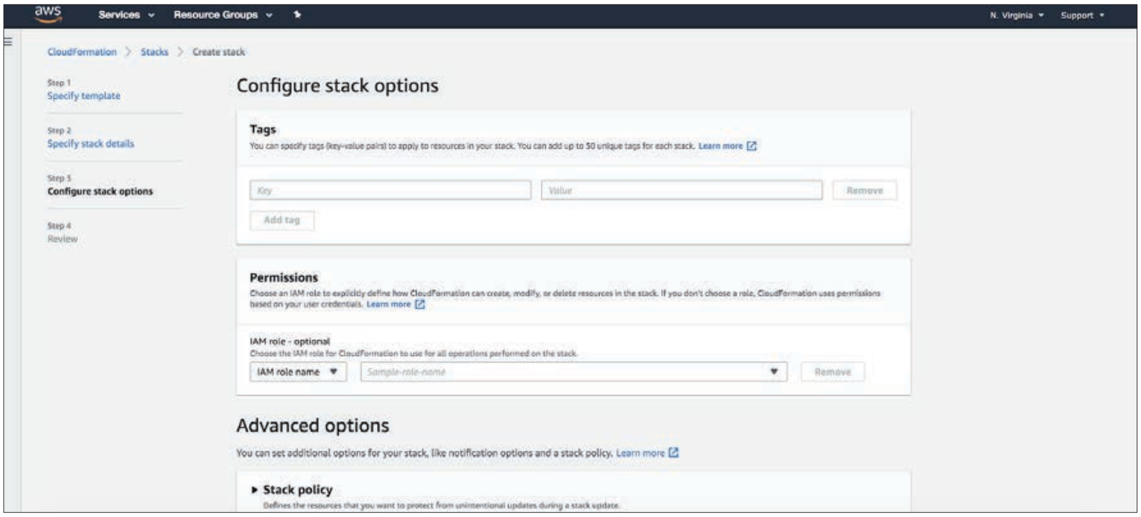
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Recorded Future Information
Recorded Future API Token
Insert Recorded Future API token
••••••••••••••••••••••••••••••••

Risk Lists
Insert a comma-delimited list of Recorded Future Riks Lists (contact your InServ consultant for more information)
phishing_host_riskrule, recent_insikt_group_riskrule, recent_intrusion_method_riskrule, ip_risklist_gt_65

Advanced Settings
Update Schedule
Insert the number of hours between executions - when the solution downloads a new Risk List (min 1 - max 170)
24

Configure any desired stack options. The defaults within this page should be sufficient for the integration.



Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more

Permissions

Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

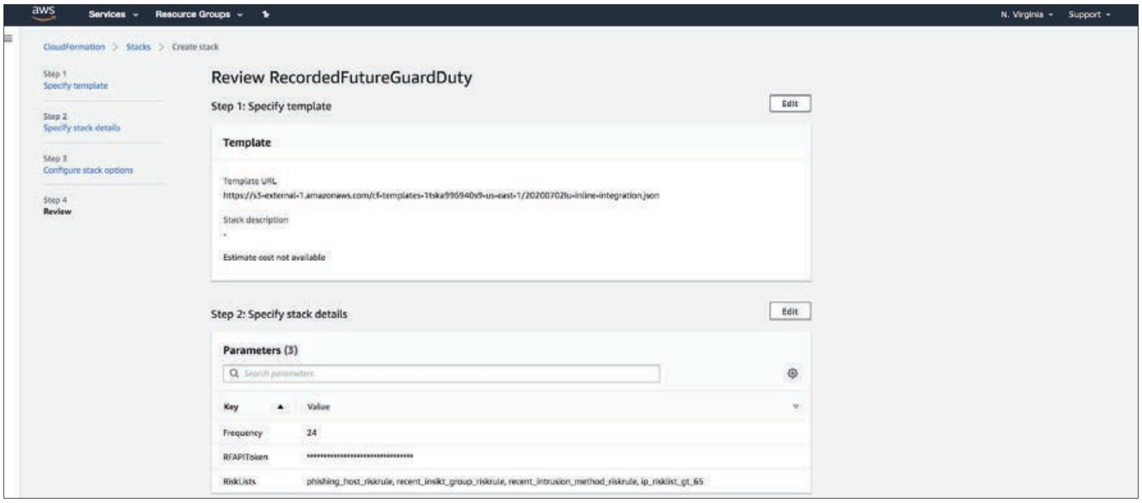
Advanced options

You can set additional options for your stack, like notification options and a stack policy. Learn more

▸ Stack policy

Defines the resources that you want to protect from unintentional updates during a stack update.

Review the stack configurations you previously selected.



Review RecordedFutureGuardDuty

Step 1: Specify template

Template

Template URL
https://s3-external-1.amazonaws.com/cf-templates-1tska996940s9-us-east-1/20200702lu-inline-integration.json

Stack description
-

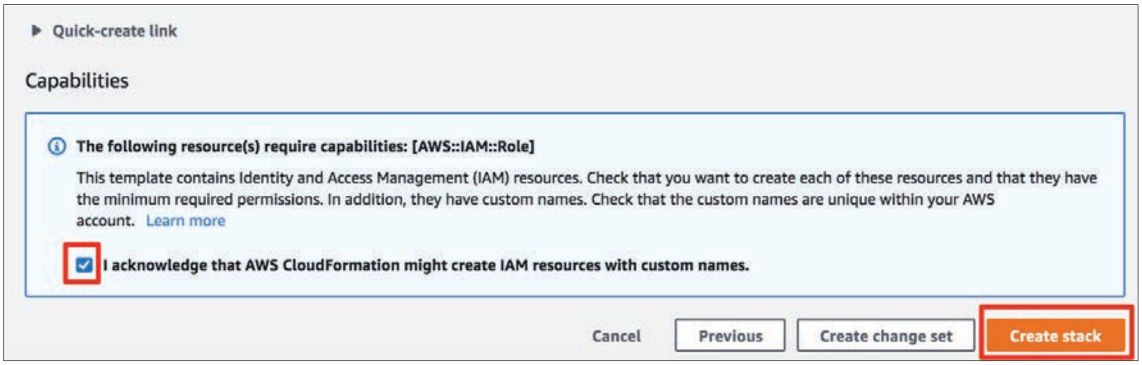
Estimate cost not available

Step 2: Specify stack details

Parameters (3)

Key	Value
Frequency	24
RFAPIToken	********************************
RiskLists	phishing_host_riskrule, recent_insikt_group_riskrule, recent_intrusion_method_riskrule, ip_risklist_gt_65

At the bottom of the stack configuration review page, you will be required to acknowledge that AWS CloudFormation might create IAM resources with custom names. Check the box as shown and select “Create stack”.


▸ Quick-create link

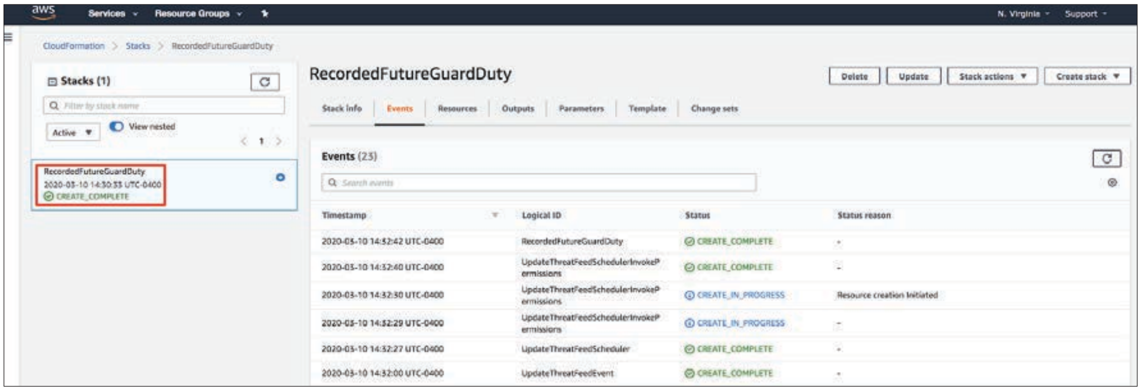
Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more

☑ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

The stack will begin to initialize based on the settings selected. The status of the job will be reported on the page below. Once you see a "CREATE_COMPLETE" note under your stack, your stack will be created. Any errors during this process will be displayed under the "Status Reason" column.



CloudFormation > Stacks > RecordedFutureGuardDuty

Stacks (1)

RecordedFutureGuardDuty
2020-03-10 14:30:33 UTC-0400
CREATE_COMPLETE

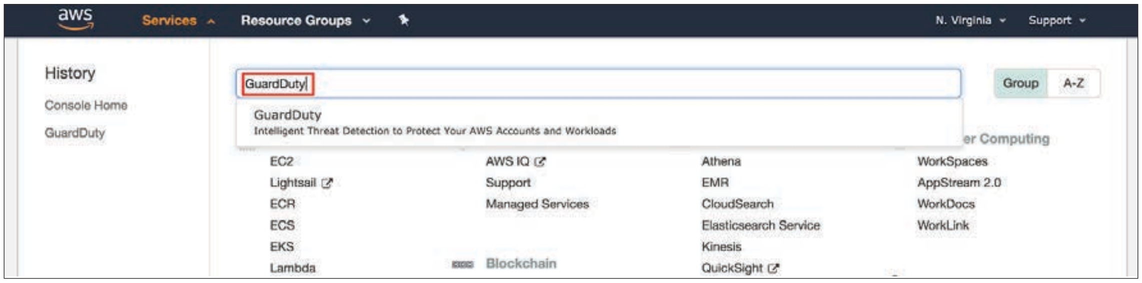
RecordedFutureGuardDuty

Events (23)

Timestamp	Logical ID	Status	Status reason
2020-03-10 14:32:42 UTC-0400	RecordedFutureGuardDuty	CREATE_COMPLETE	-
2020-03-10 14:32:40 UTC-0400	UpdateThreatFeedSchedulerInvokePermissions	CREATE_COMPLETE	-
2020-03-10 14:32:30 UTC-0400	UpdateThreatFeedSchedulerInvokePermissions	CREATE_IN_PROGRESS	Resource creation Initiated
2020-03-10 14:32:29 UTC-0400	UpdateThreatFeedSchedulerInvokePermissions	CREATE_IN_PROGRESS	-
2020-03-10 14:32:27 UTC-0400	UpdateThreatFeedScheduler	CREATE_COMPLETE	-
2020-03-10 14:32:00 UTC-0400	UpdateThreatFeedEvent	CREATE_COMPLETE	-

Verify Successful Stack Creation

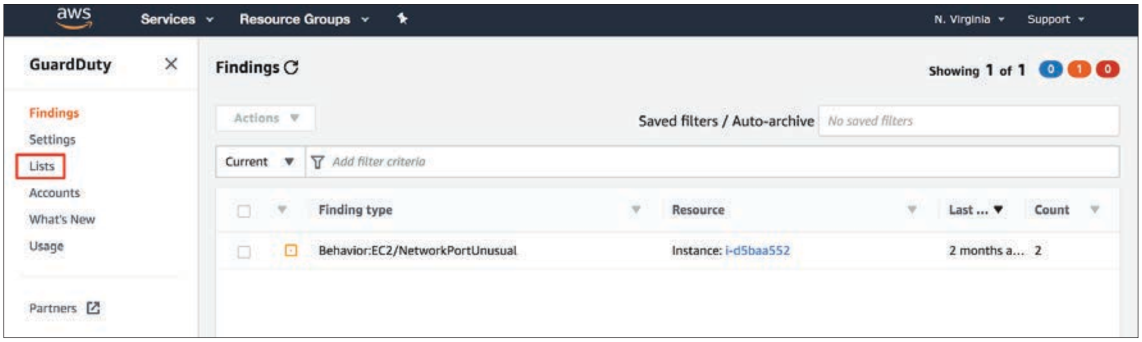
Navigate back to "GuardDuty".



GuardDuty

GuardDuty
Intelligent Threat Detection to Protect Your AWS Accounts and Workloads

On the left side menu, select "Lists" to see list management options.



Findings

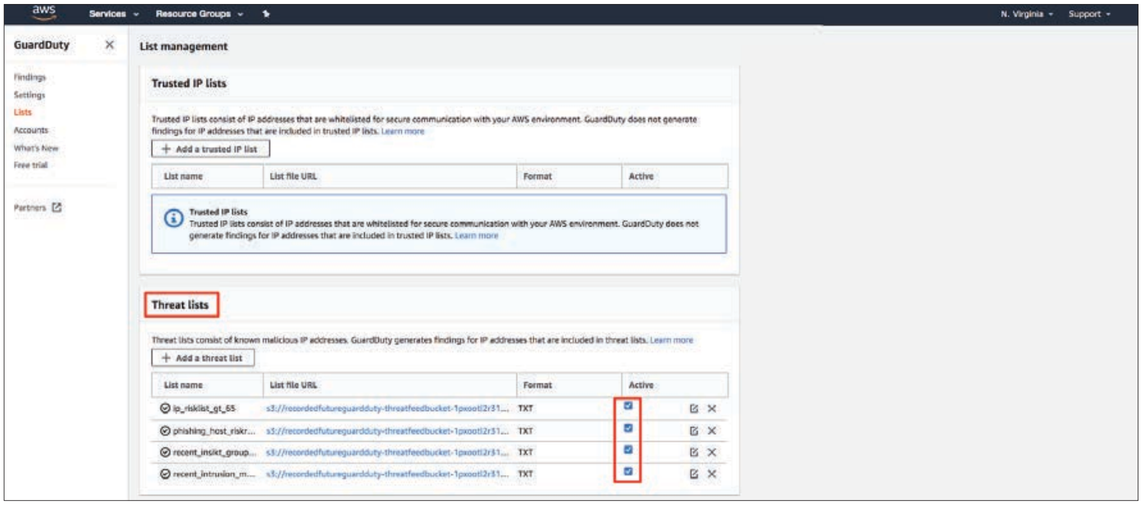
Showing 1 of 1

Saved filters / Auto-archive: No saved filters

Current: Add filter criteria

Finding type	Resource	Last ...	Count
Behavior:EC2/NetworkPortUnusual	Instance: i-d5baa552	2 months a...	2

From here, scroll down to "Threat Lists" and ensure the successful creation of the Recorded Future threat lists inputted into the risklist field of the stack parameters. Ensure each list is active.



List management

Trusted IP lists

Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more

List name	List file URL	Format	Active

Trusted IP lists
Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more

Threat lists

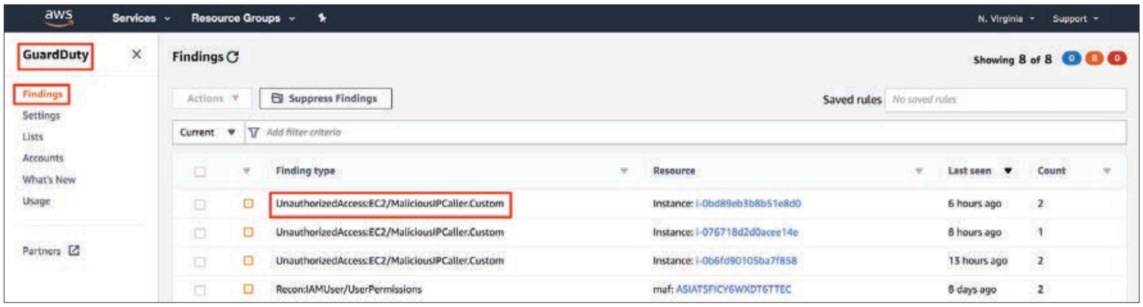
Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more

List name	List file URL	Format	Active
ip_risklist_gt_65	s3://recordedfutureguardduty-threatfeedbucket-1pxootl2r31...	TXT	☑
phishing_host_riskr...	s3://recordedfutureguardduty-threatfeedbucket-1pxootl2r31...	TXT	☑
recent_insikt_group...	s3://recordedfutureguardduty-threatfeedbucket-1pxootl2r31...	TXT	☑
recent_intrusion_m...	s3://recordedfutureguardduty-threatfeedbucket-1pxootl2r31...	TXT	☑

Note: If Recorded Future threat lists have not been created successfully, please check your Lambda function logs for any errors that may appear there under log group ex:
`/aws/lambda/[StackName]-UpdateThreatFeedFunction-[randomstring]`

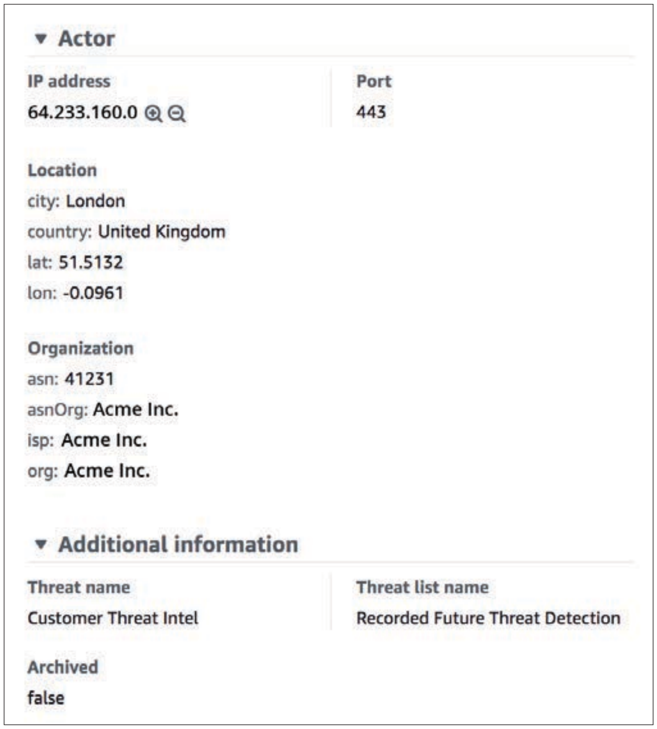
Check for Any Findings from the Threat List

Navigate to the GuardDuty home page. Select "Findings" and select a finding.



	Finding type	Resource	Last seen	Count
□	UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Instance: i-0bd89eb3b8b51e8d0	6 hours ago	2
□	UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Instance: i-076718d2d0acee14e	8 hours ago	1
□	UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Instance: i-0b6fd90105ba7f858	13 hours ago	2
□	Recon:IAMUser/UserPermissions	maf: ASIAT5FICY6WXDT6TTEC	8 days ago	2

A panel on the right side will display a summary of the hit as well as the threat list this IP was found on.



▾ Actor

IP address
64.233.160.0

Port
443

Location
city: London
country: United Kingdom
lat: 51.5132
lon: -0.0961

Organization
asn: 41231
asnOrg: Acme Inc.
isp: Acme Inc.
org: Acme Inc.

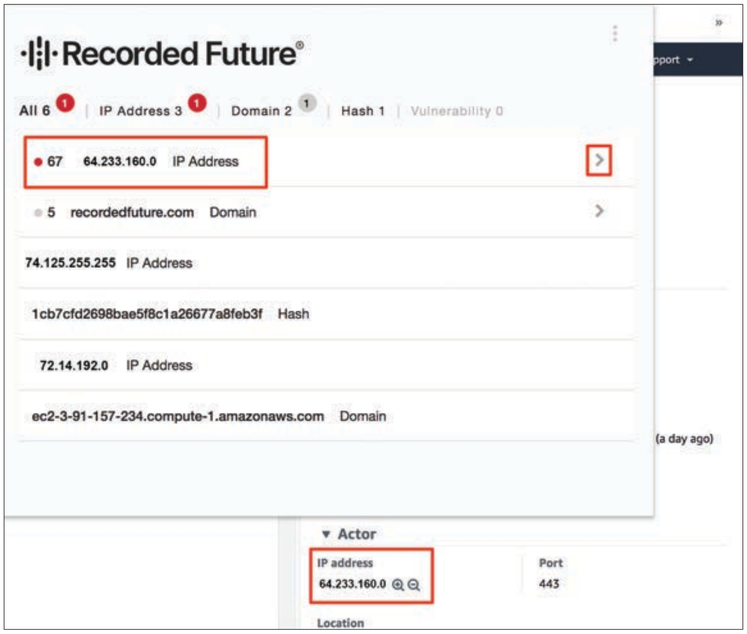
▾ Additional information

Threat name
Customer Threat Intel

Threat list name
Recorded Future Threat Detection

Archived
false

Use the Recorded Future Browser Extension to provide context as to "why" the indicator is risky.


Recorded Future®
All 6 1 | IP Address 3 1 | Domain 2 1 | Hash 1 | Vulnerability 0
»
pport ▾

● 67 64.233.160.0 IP Address

● 5 recordedfuture.com Domain

74.125.255.255 IP Address

1cb7cfd2698bae5f8c1a26677a8feb3f Hash

72.14.192.0 IP Address

ec2-3-91-157-234.compute-1.amazonaws.com Domain

(a day ago)

▾ Actor

IP address
64.233.160.0

Port
443

Location

ABOUT RECORDED FUTURE