Container Security

Securing AWS Fargate on Qualys Private Cloud Platform (PCP)

April 17, 2023

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide

Welcome to Qualys Container Security! Container Security enables you to secure AWS Fargate by performing vulnerability and compliance scans on container images whenever an AWS ECS Fargate task is launched.
This document provides guidelines for setting up the connectivity between AWS and your Private Cloud Platform hosting Qualys Container Security servers.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

Getting Started

Qualys Container Security can now be used to secure AWS Fargate for Qualys Private Cloud Platform. In AWS Fargate, we use ‘AWS CloudFormation’ and a ‘Qualys Lambda’ function to trigger scanning automatically when the tasks come into the **Running** state. For AWS to communicate from Lambda and Codebuild functions with your Private Cloud platform, the network connectivity needs to be configured.

The following are the suggested guidelines for establishing connectivity between AWS Lambda and CodeBuild functions, and your Private Cloud Platform that hosts Qualys Container Security servers. While these guidelines are recommended, you can use alternative methods to set up connectivity. Regardless of the method used, it is mandatory to follow steps 2, 3, and 4 to ensure successful connectivity.

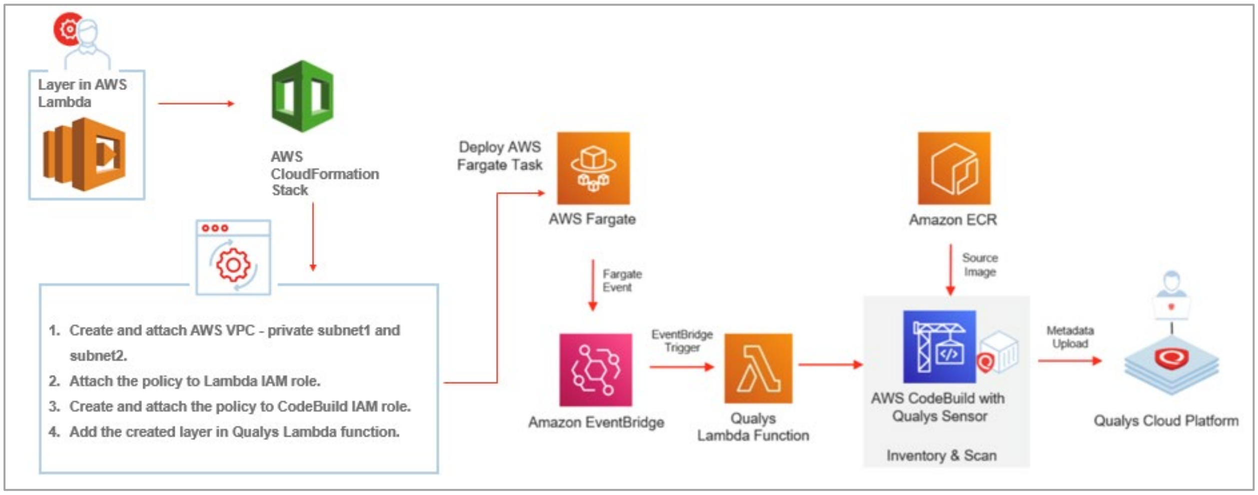
1. Create the lambda and CodeBuild VPC.
2. Create an IAM Policy for CodeBuild.
3. Create a Lambda Layer for custom Root CA Certification.
4. Attach the VPCs and appropriate policies after the stack creation.

Create VPC and Subnets for Lambda and Codebuild

The Amazon Virtual Private Cloud (VPC) allows you to launch AWS resources into a virtual network that you have defined. A subnet is a range of IP addresses in your VPC that enables you to deploy AWS resources in your VPC.

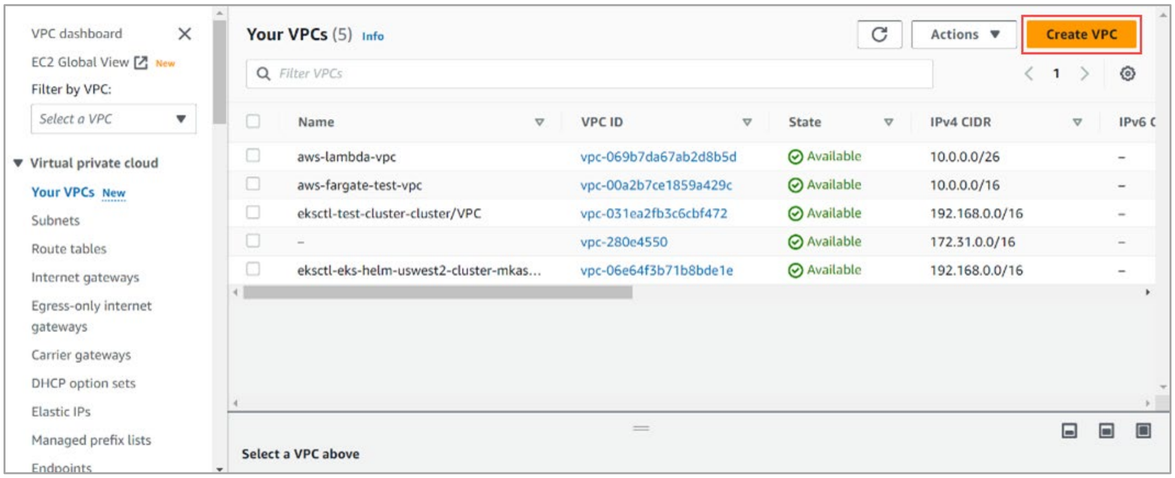
If you are using Qualys Private Cloud Platform, you can create a VPC and private and public subnets in the VPC. This VPC and subnets can be used to communicate with the Lambda and Codebuild functions launched after the stack deployment.

Refer to the VPC application and Other Settings for Lambda and Codebuild after Stack Deployment section for this.



1. Create and attach AWS VPC - private subnet1 and subnet2.
2. Attach the policy to Lambda IAM role.
3. Create and attach the policy to CodeBuild IAM role.
4. Add the created layer in Qualys Lambda function.

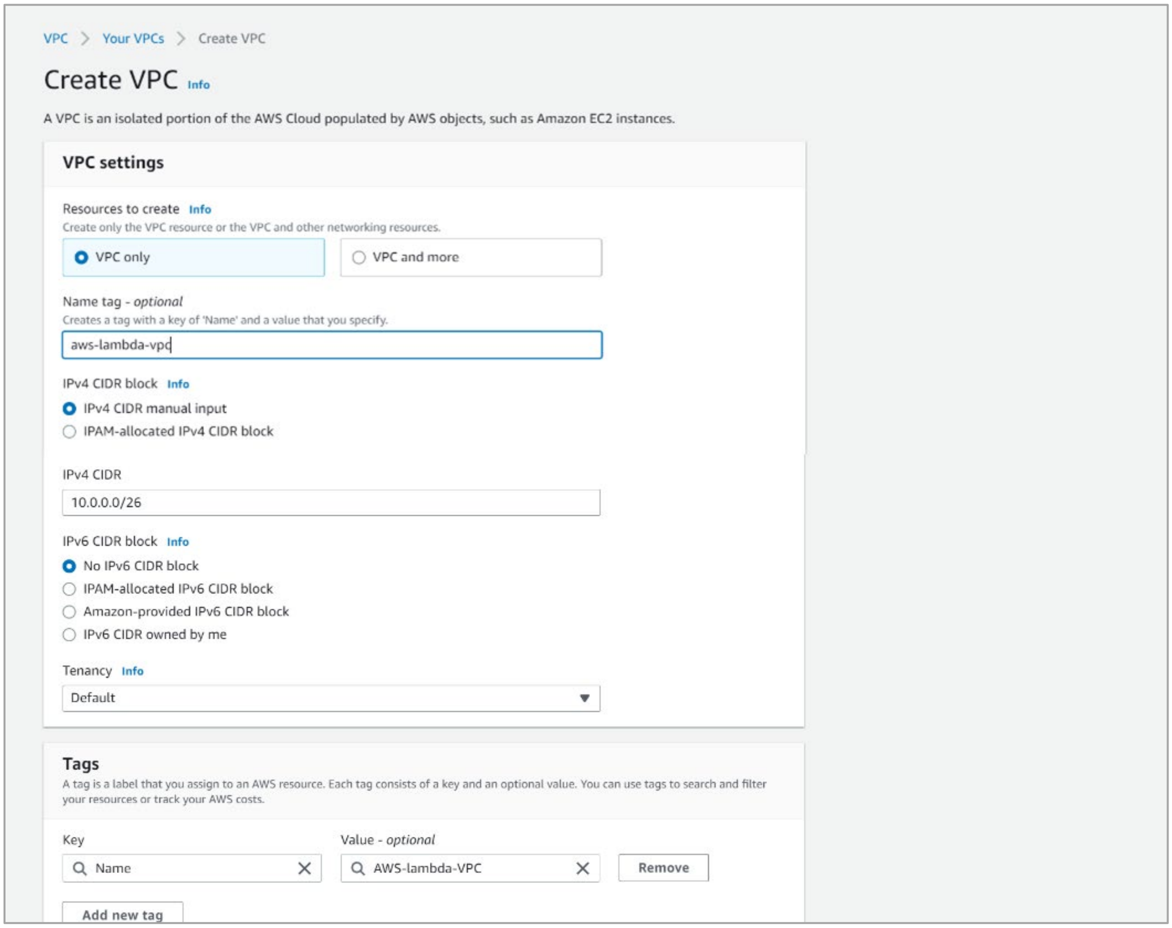
1. Navigate to **AWS VPC service > Your VPCs** and click **Create VPC**.



Your VPCs (5) Info

□	Name	VPC ID	State	IPv4 CIDR	IPv6 C
□	aws-lambda-vpc	vpc-069b7da67ab2d8b5d	✓ Available	10.0.0.0/26	–
□	aws-fargate-test-vpc	vpc-00a2b7ce1859a429c	✓ Available	10.0.0.0/16	–
□	eksctl-test-cluster-cluster/VPC	vpc-031ea2fb3c6cbf472	✓ Available	192.168.0.0/16	–
□	–	vpc-280e4550	✓ Available	172.31.0.0/16	–
□	eksctl-eks-helm-uswest2-cluster-mkas...	vpc-06e64f3b71b8bde1e	✓ Available	192.168.0.0/16	–

2. Provide the following details for VPC creation: VPC name, CIDR block and Tenancy.



Create VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
● VPC only ○ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
aws-lambda-vpc

IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/26

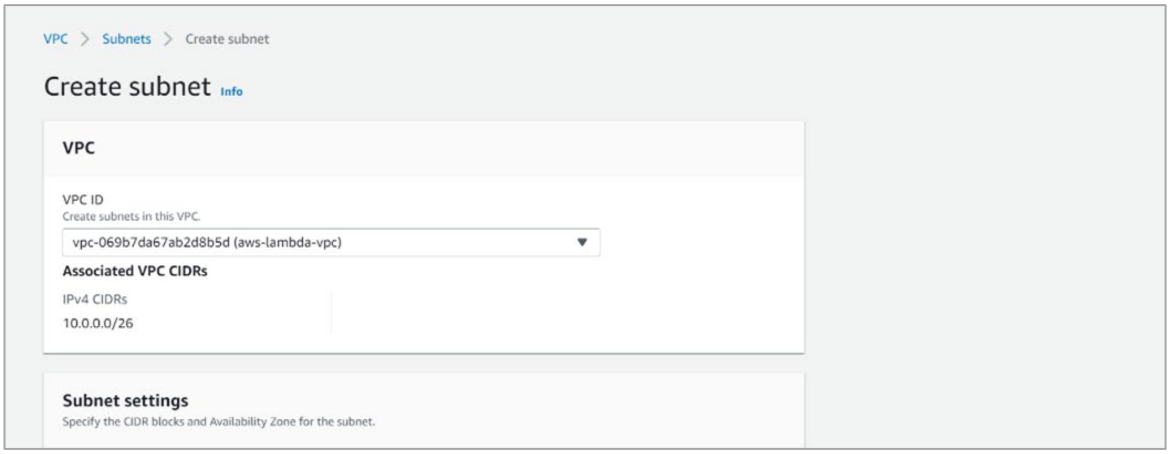
IPv6 CIDR block Info
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy Info
Default

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	AWS-lambda-VPC

3. Navigate to **Subnets** and click **Create Subnet** to create subnets for the above created VPC. Provide the following details: Name tag, VPC, Availability zone, and CIDR block.



Create subnet Info

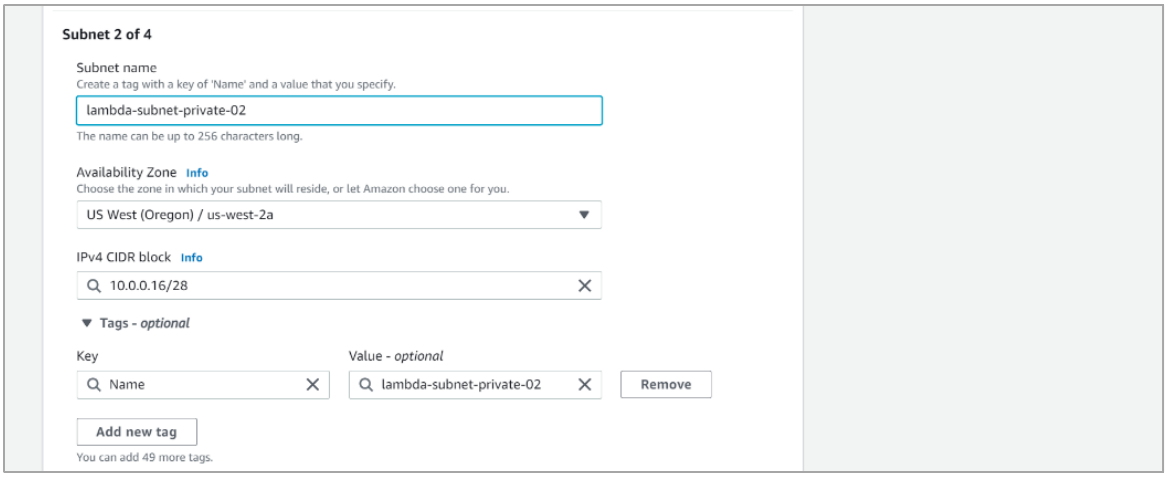
VPC

VPC ID
Create subnets in this VPC.
vpc-069b7da67ab2d8b5d (aws-lambda-vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/26

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.



Subnet 2 of 4

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
lambda-subnet-private-02
The name can be up to 256 characters long.

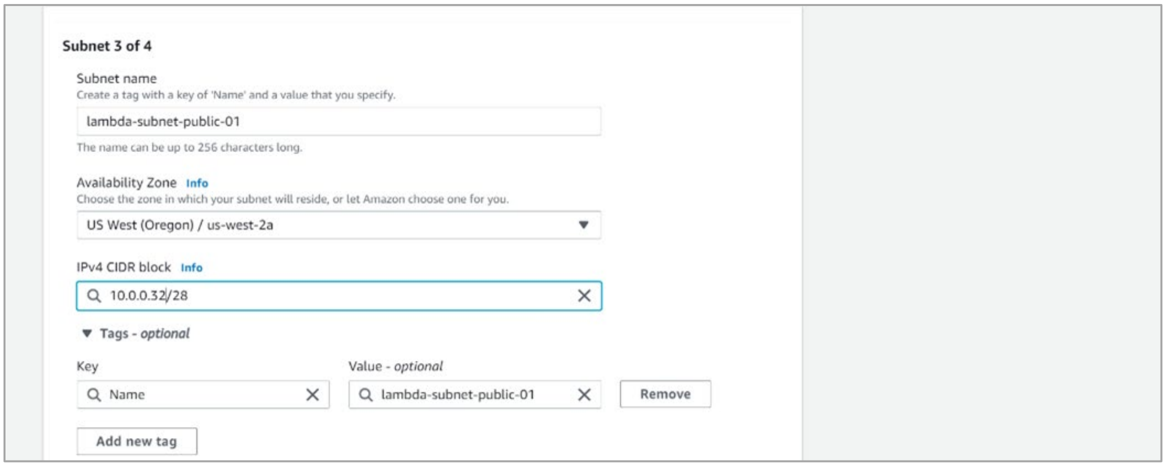
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US West (Oregon) / us-west-2a

IPv4 CIDR block Info
10.0.0.16/28

Tags - *optional*

Key	Value - *optional*
Name	lambda-subnet-private-02

You can add 49 more tags.



Subnet 3 of 4

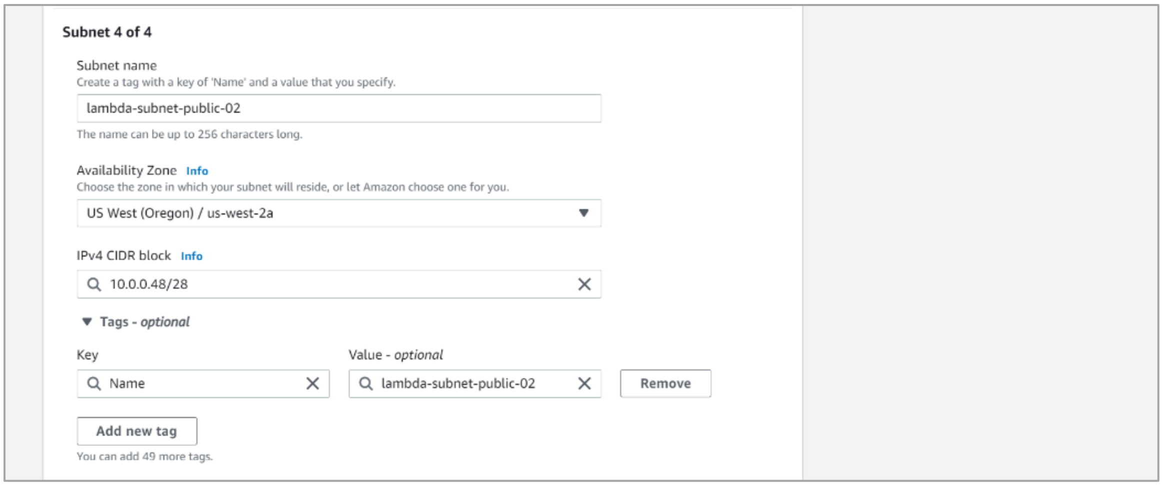
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
lambda-subnet-public-01
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US West (Oregon) / us-west-2a

IPv4 CIDR block Info
10.0.0.32/28

Tags - *optional*

Key	Value - *optional*
Name	lambda-subnet-public-01



Subnet 4 of 4

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
lambda-subnet-public-02
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US West (Oregon) / us-west-2a

IPv4 CIDR block Info
10.0.0.48/28

Tags - *optional*

Key	Value - *optional*
Name	lambda-subnet-public-02

You can add 49 more tags.

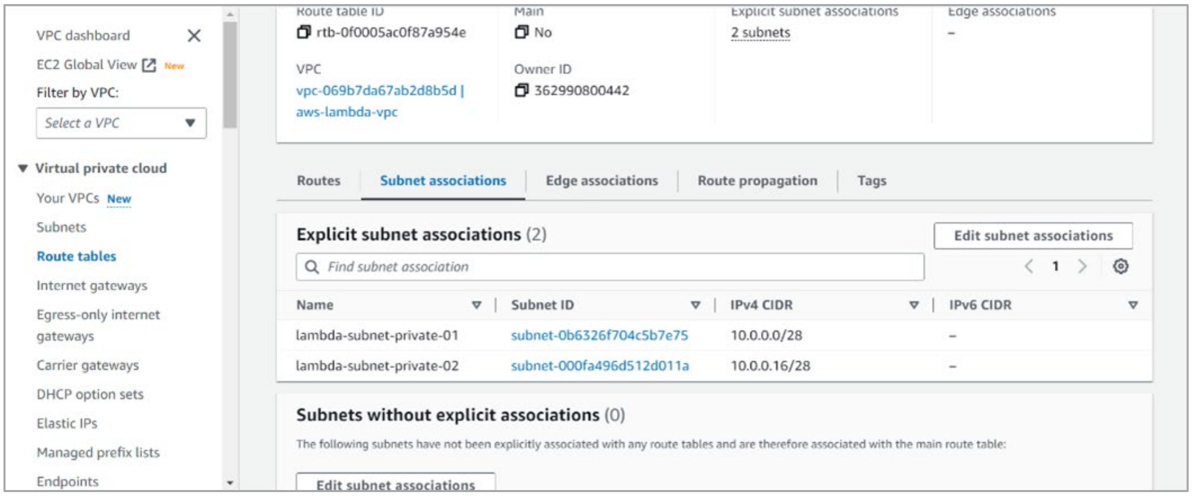
Notes:

- Create four subnets for the VPC: two private and two public subnets.
- The Availability zone for each subnet should be the same.

4. Navigate to **Route tables** and filter tables using the VPC ID. Rename the main route table associated with the VPC to "Public-RT".

5. Create another route table and name it for private subnet and attach the created VPC to them.

6. Attach the private subnets to private route table and public subnet to the public (main) route table:
   a. Open the private/public route table, click **Subnet associations**, and then **Edit subnet associations**.
   b. Add the two private/public subnets created and save the association.



Route table ID: rtb-0f0005ac0f87a954e
Main: No
Explicit subnet associations: 2 subnets
Edge associations: –
VPC: vpc-069b7da67ab2d8b5d | aws-lambda-vpc
Owner ID: 362990800442

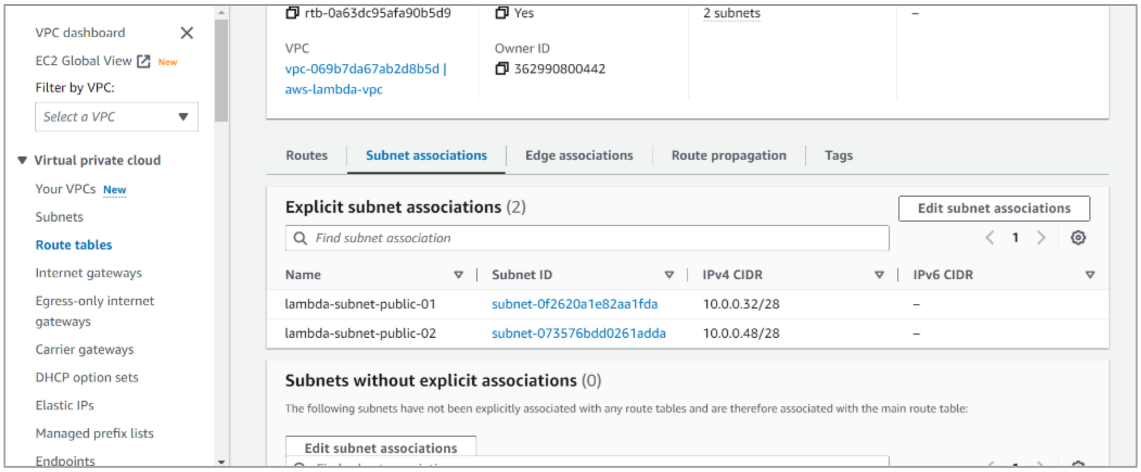
Explicit subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lambda-subnet-private-01	subnet-0b6326f704c5b7e75	10.0.0.0/28	–
lambda-subnet-private-02	subnet-000fa496d512d011a	10.0.0.16/28	–

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Figure 1 Private Route Table



rtb-0a63dc95afa90b5d9	Yes	2 subnets	–
VPC vpc-069b7da67ab2d8b5d | aws-lambda-vpc	Owner ID 362990800442		

Explicit subnet associations (2)

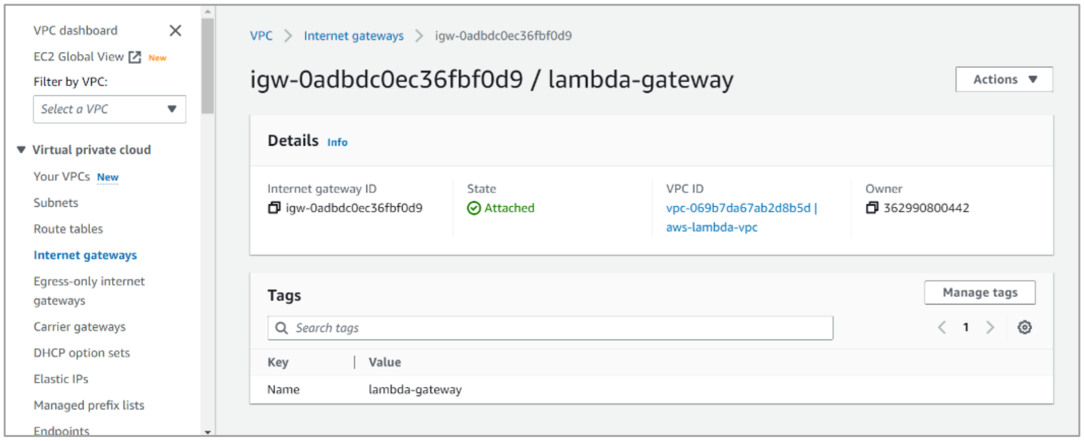
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lambda-subnet-public-01	subnet-0f2620a1e82aa1fda	10.0.0.32/28	–
lambda-subnet-public-02	subnet-073576bdd0261adda	10.0.0.48/28	–

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Figure 2 Public Route Table

7. Create a new Internet gateway and attach it to the VPC.
    a. Click **Internet gateways** in the left pane and create a gateway by giving it an appropriate name.
    b. Click the internet gateway, select **Actions > Attach to VPC** and select the VPC.



igw-0adbdc0ec36fbf0d9 / lambda-gateway

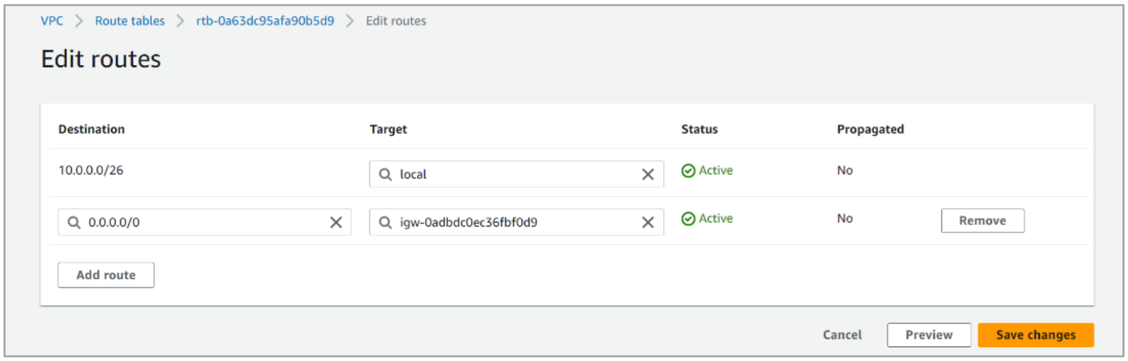
Details

Internet gateway ID	State	VPC ID	Owner
igw-0adbdc0ec36fbf0d9	Attached	vpc-069b7da67ab2d8b5d | aws-lambda-vpc	362990800442

Tags

Key	Value
Name	lambda-gateway

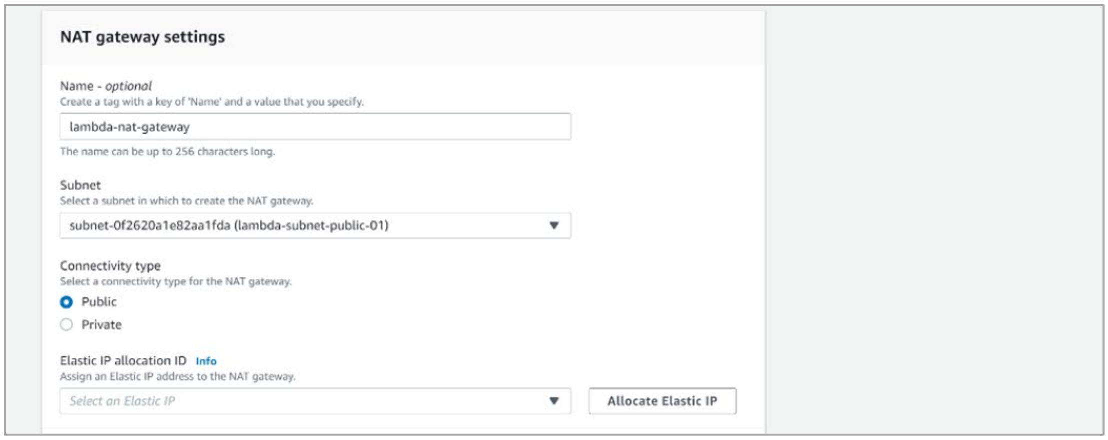
8. Navigate to the public route table, edit and add new routes with the following value:
    - **Destination**: 0.0.0.0/0
    - **Target**: The above created Internet gateway



Edit routes

Destination	Target	Status	Propagated
10.0.0.0/26	local	Active	No
0.0.0.0/0	igw-0adbdc0ec36fbf0d9	Active	No

9. From the left-hand pane, create a new NAT gateway by choosing one of the public subnets. In **NAT gateway settings**, under **Elastic IP allocation ID**, click **Allocate Elastic IP**.
   Note: You must add this elastic IP address in the trusted/permitted list in order to communicate from the AWS cloud to Qualys Container Security service running on your private cloud platform.



NAT gateway settings

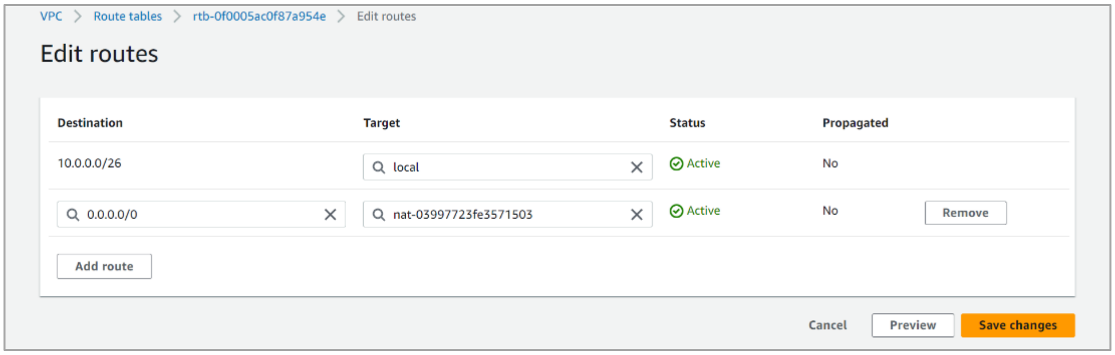
Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
lambda-nat-gateway
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0f2620a1e82aa1fda (lambda-subnet-public-01) ▼

Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
Select an Elastic IP ▼

10. Navigate to **Route Tables.** Click the private route and then **Edit routes** and add the following values:
    - **Destination**: 0.0.0.0/0
    - **Target**: NAT gateway

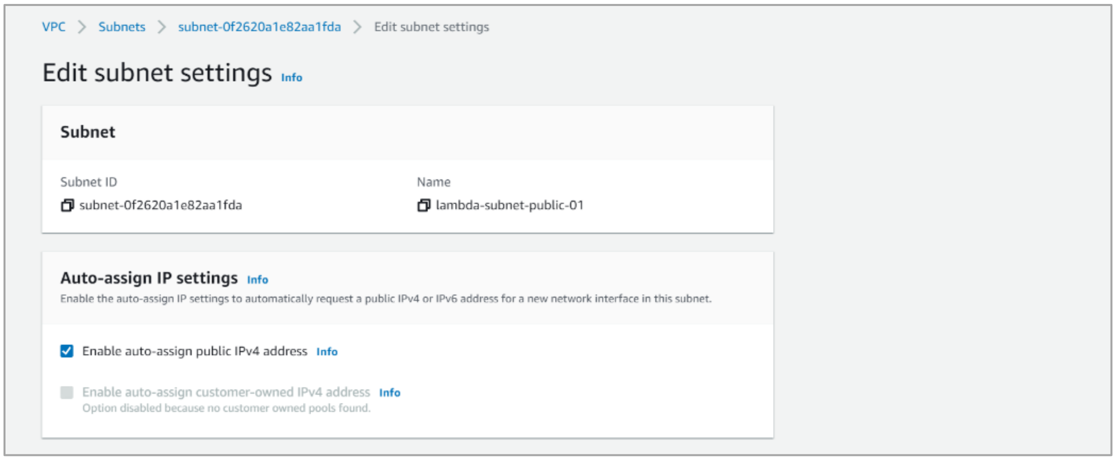


VPC > Route tables > rtb-0f0005ac0f87a954e > Edit routes

Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/26	local	Active	No	
0.0.0.0/0	nat-03997723fe3571503	Active	No	Remove

11. Navigate to **Subnets**. In the created public subnets, click **Edit subnet settings** and select the **Enable auto-assign public IPv4 address** check box.



VPC > Subnets > subnet-0f2620a1e82aa1fda > Edit subnet settings

Edit subnet settings Info

Subnet

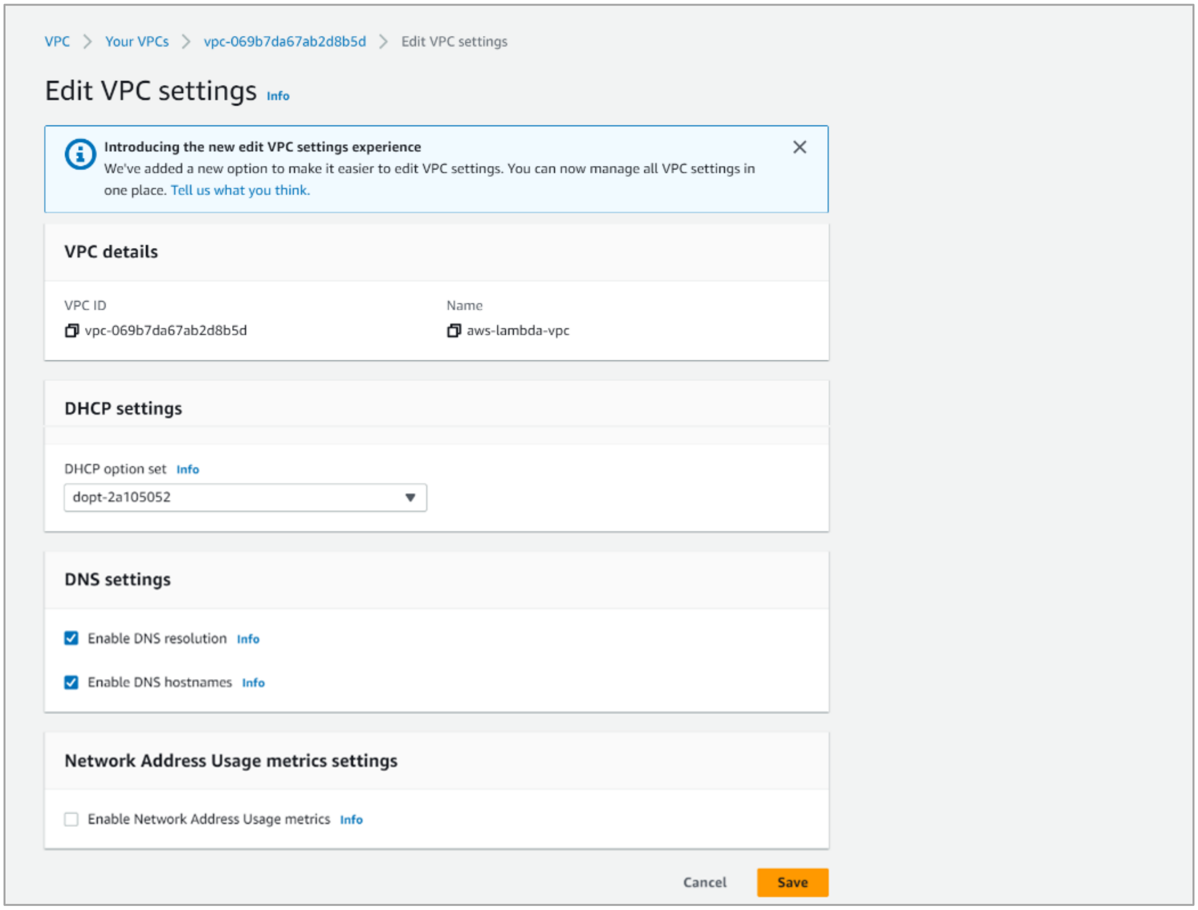
Subnet ID: subnet-0f2620a1e82aa1fda
Name: lambda-subnet-public-01

Auto-assign IP settings Info
Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

☑ Enable auto-assign public IPv4 address Info

□ Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

12. Navigate to the created VPC. Click **Edit VPC settings** and select the **Enable DNS resolution** and **Enable DNS hostnames** check boxes.



VPC > Your VPCs > vpc-069b7da67ab2d8b5d > Edit VPC settings

Edit VPC settings Info

Introducing the new edit VPC settings experience
We've added a new option to make it easier to edit VPC settings. You can now manage all VPC settings in one place. Tell us what you think.

VPC details

VPC ID: vpc-069b7da67ab2d8b5d

Name: aws-lambda-vpc

DHCP settings

DHCP option set Info: dopt-2a105052

DNS settings

☑ Enable DNS resolution Info

☑ Enable DNS hostnames Info

Network Address Usage metrics settings

□ Enable Network Address Usage metrics Info

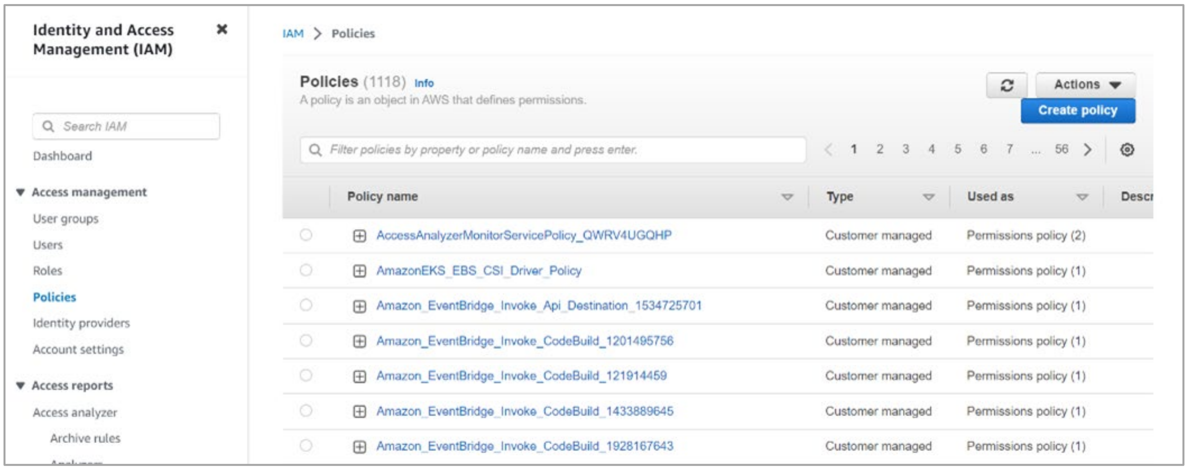
13. Note down the details of the VPC and the created subnets.

Create a Policy for CodeBuild IAM Role

Create a policy to attach to the CodeBuild IAM role created after stack deployment.

Refer to the VPC Application and Other Settings to Lambda and Codebuild after Stack Deployment section for this.

1. Navigate to **Identity and Access Management (IAM)** service **> Policies** and click **Create policy**.



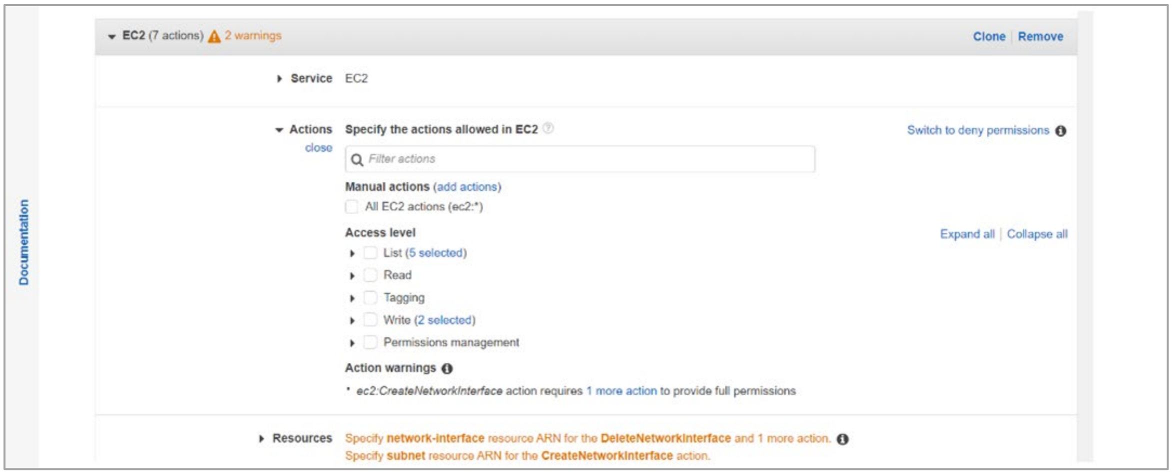
Policies (1118) Info
A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Descr
AccessAnalyzerMonitorServicePolicy_QWRV4UGQHP	Customer managed	Permissions policy (2)	
AmazonEKS_EBS_CSI_Driver_Policy	Customer managed	Permissions policy (1)	
Amazon_EventBridge_Invoke_Api_Destination_1534725701	Customer managed	Permissions policy (1)	
Amazon_EventBridge_Invoke_CodeBuild_1201495756	Customer managed	Permissions policy (1)	
Amazon_EventBridge_Invoke_CodeBuild_121914459	Customer managed	Permissions policy (1)	
Amazon_EventBridge_Invoke_CodeBuild_1433889645	Customer managed	Permissions policy (1)	
Amazon_EventBridge_Invoke_CodeBuild_1928167643	Customer managed	Permissions policy (1)	

2. In **Service**, select **EC2**.

3. In **Actions**, add the following filters:
   - CreateNetworkInterface
   - DescribeNetworkInterfaces
   - DescribeVpcs
   - DeleteNetworkInterface
   - DescribeDhcpOptions
   - DescribeSubnets
   - DescribeSecurityGroups

   Five actions have the **List** access and two actions have the **Write** access.



EC2 (7 actions) ⚠ 2 warnings

Service EC2

Actions close
Specify the actions allowed in EC2

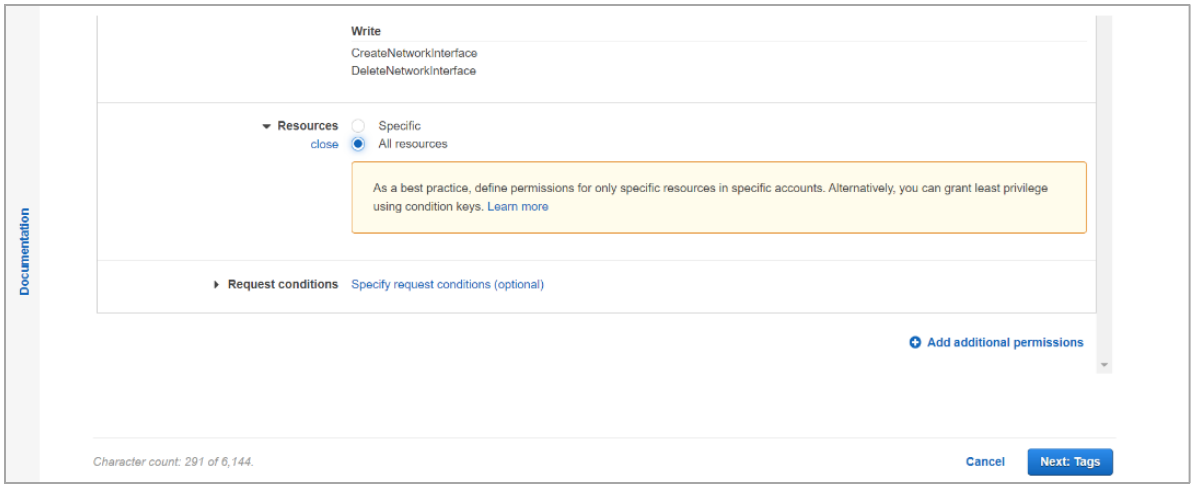
Manual actions (add actions)
□ All EC2 actions (ec2:*)

Access level
□ List (5 selected)
□ Read
□ Tagging
□ Write (2 selected)
□ Permissions management

Action warnings
- ec2:CreateNetworkInterface action requires 1 more action to provide full permissions

Resources
Specify network-interface resource ARN for the DeleteNetworkInterface and 1 more action.
Specify subnet resource ARN for the CreateNetworkInterface action.

4. Under **Resources**, select the **All resources** option.



Write
CreateNetworkInterface
DeleteNetworkInterface

Resources ○ Specific
close ● All resources

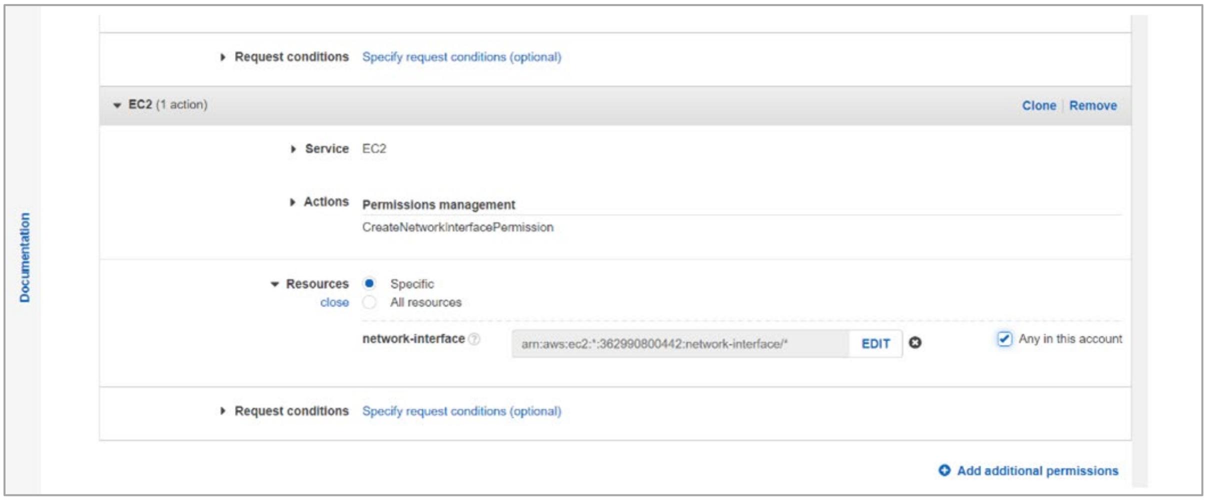
As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more

Request conditions Specify request conditions (optional)

5. Click **Add additional permissions** and select the service as EC2.

6. Add the following filter in **Actions**: CreateNetworkInterfacePermission

7. Under **Resources**, select **Specific** and for **network-interface**, select the **Any in this account** check box.
   It adds the following resource: "Resource": "arn:aws:ec2:*:<AWS-account-id>:network-interface/*".



Request conditions Specify request conditions (optional)

EC2 (1 action) Clone | Remove

Service EC2

Actions **Permissions management**
CreateNetworkInterfacePermission

Resources ● Specific
close ○ All resources

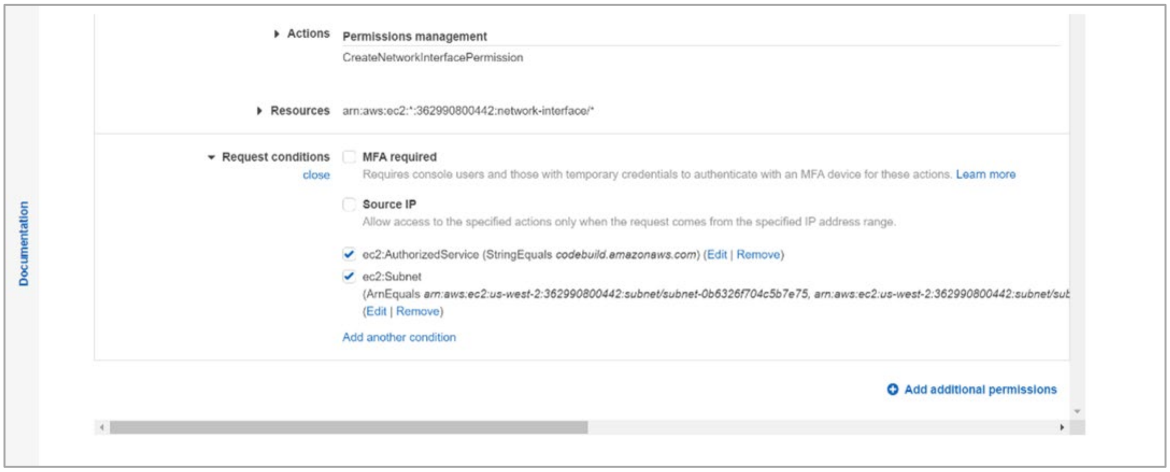
network-interface arn:aws:ec2:*:362990800442:network-interface/* EDIT ☑ Any in this account

Request conditions Specify request conditions (optional)

8. Under **Request conditions**, click **Add Condition** and specify the following details:
   - **Condition key**: ec2:AuthorizedService
   - **Qualifier**: Default
   - **Operator**: StringEquals
   - **Value**: codebuild.amazonaws.com

9. Click **Add another condition** and add the following details in the condition:
   - **Condition key**: ec2:Subnet
   - **Qualifier**: Default

- **Operator**: ArnEquals
- **Value**: *<Values of ARN of all four subnets created for Codebuild and lambda>*



Actions: **Permissions management**
CreateNetworkInterfacePermission

Resources: arn:aws:ec2:*:362990800442:network-interface/*

Request conditions
close

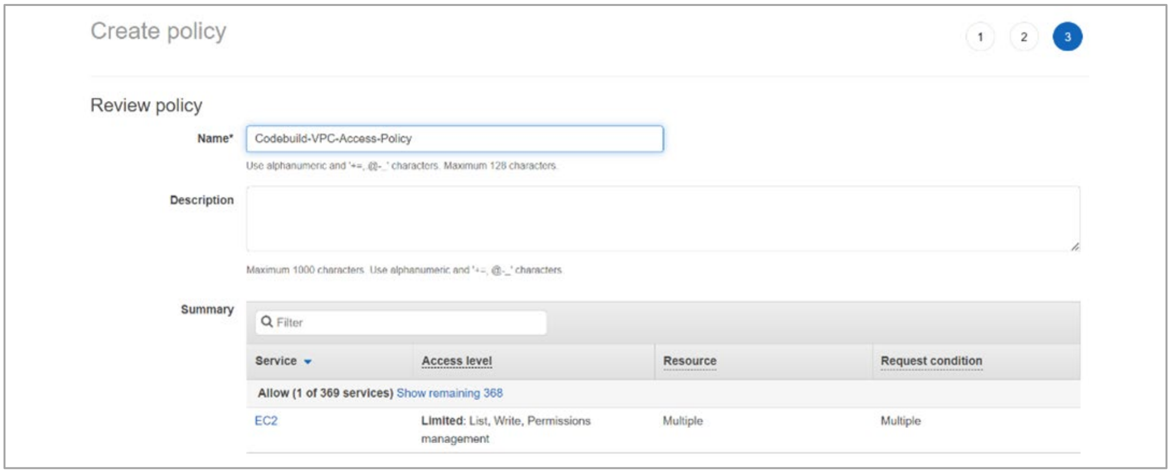
□ **MFA required**
Requires console users and those with temporary credentials to authenticate with an MFA device for these actions. Learn more

□ **Source IP**
Allow access to the specified actions only when the request comes from the specified IP address range.

☑ ec2:AuthorizedService (StringEquals *codebuild.amazonaws.com*) (Edit | Remove)

☑ ec2:Subnet
(ArnEquals *arn:aws:ec2:us-west-2:362990800442:subnet/subnet-0b6326f704c5b7e75, arn:aws:ec2:us-west-2:362990800442:subnet/sub*
(Edit | Remove)

10. Keep on clicking **Next** until the **Review policy** page, specify appropriate name to the policy, and click **Create policy**.



Review policy

Name*: Codebuild-VPC-Access-Policy
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

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

Summary

Service	Access level	Resource	Request condition
Allow (1 of 369 services) Show remaining 368			
EC2	**Limited**: List, Write, Permissions management	Multiple	Multiple

Create AWS Lambda Layer to Make Custom Root CA Certificate for Lambda Function

Do you need an AWS lambda layer for Fargate scanning? If your answer to any of the following questions is NO, you can skip this Lambda layer creation step.

- Are you using Qualys Private Cloud platform (https://www.qualys.com/private-cloud/)?
- Is your Qualys PCP server certificate signed using custom Root CA?
  How to check if server certificates are signed using custom Root CA?
  Check with your operations team or validate yourself using the following steps:
  a. Navigate to the Qualys private cloud platform URL.
  b. Click the padlock icon in the browser address bar to view the website's SSL/TLS certificate.
  c. Look for the **Issuer** field in the certificate details.
     If the issuer is a well-known CA, such as DigiCert, Let's Encrypt, or GoDaddy, then the certificate is signed by a well-known root CA.
     If the issuer is not a well-known CA, you can check if the certificate is signed by a custom root CA by looking at the **Certificate Authority** or **Chain of Trust** section in the certificate details. If there is a custom root CA in the chain of trust, then the certificate is signed by a custom root CA.

What is AWS lambda layer?

AWS Lambda layers are a distribution mechanism for libraries, custom runtimes, and other function dependencies. You can use layers to package and share libraries or other code that can be used across multiple functions.

A Lambda layer is a ZIP archive that contains libraries, a custom runtime, or other dependencies. When you create a Lambda function, you can reference one or more layers that are then included in the function's deployment package. This allows you to keep your function code separate from its dependencies, making it easier to manage and update your code and dependencies independently.

One important note from the AWS documentation is “Lambda extracts the layer contents into the /opt directory when setting up the execution environment for the function”. This means the content of zip file added in the layer is extracted and made available in the /opt directory for AWS lambda functions at the time of execution.

For more information, see:
Using layers with your Lambda function
Creating and sharing Lambda layers

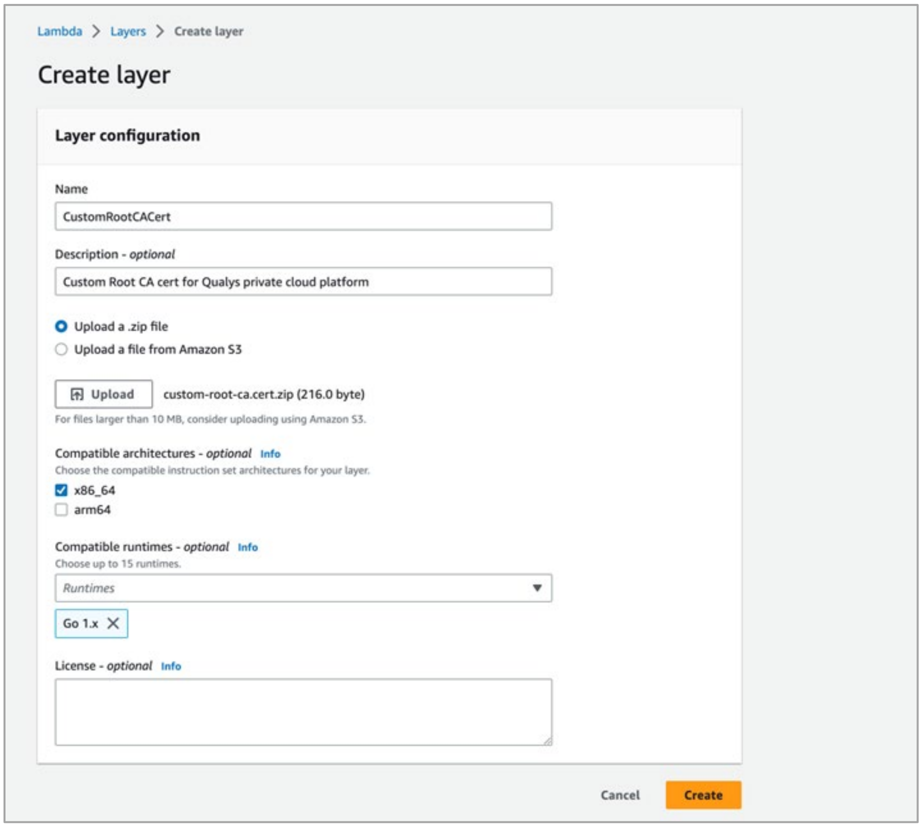
Create AWS Lambda Layer using AWS Console

1. Get the custom root CA certificate for your Qualys private cloud platform. For example, custom-root-ca.cert.

2. Compress the above file to a zip file. For example, custom-root-ca.cert.zip.

3. Create a new lambda layer on AWS console.
   a. Navigate to **Lambda Service > Layers** (on the left-hand side) and click **Create layer**.
   b. Specify name and description for the AWS lambda layer.
   c. Upload the created zip file.
   d. (Optional) Select the architecture as **x86_64**.
   e. From **Compatible runtimes**, select **Go 1.x**.

   Note: You do not need to provide license information.



Lambda > Layers > Create layer

Create layer

Layer configuration

Name

CustomRootCACert

Description - *optional*

Custom Root CA cert for Qualys private cloud platform

● Upload a .zip file
○ Upload a file from Amazon S3

Upload custom-root-ca.cert.zip (216.0 byte)

For files larger than 10 MB, consider uploading using Amazon S3.

Compatible architectures - *optional* Info

Choose the compatible instruction set architectures for your layer.

☑ x86_64
☐ arm64

Compatible runtimes - *optional* Info

Choose up to 15 runtimes.

Runtimes

Go 1.x ✕

License - *optional* Info

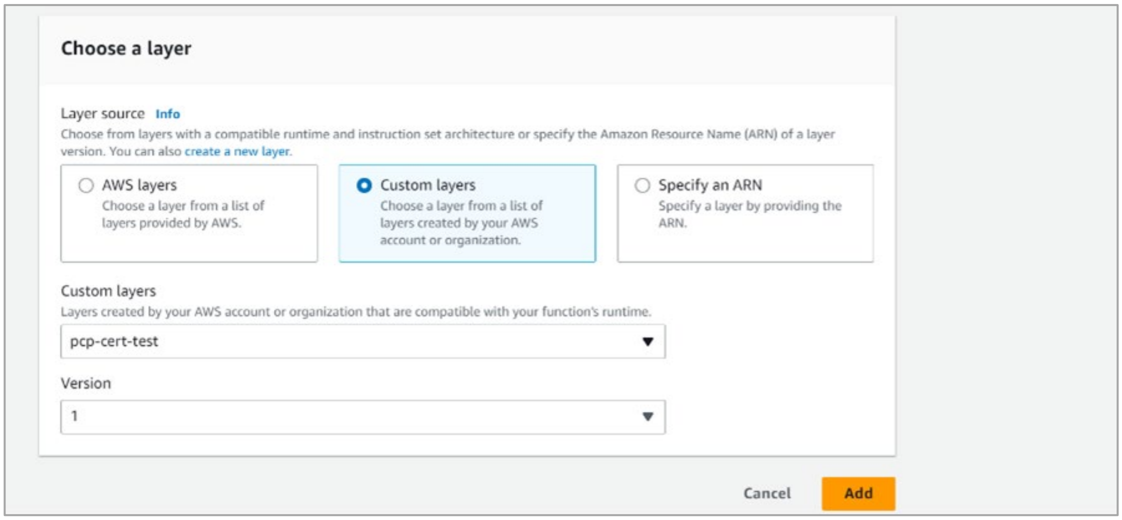
4. Note down the ARN or the name of the AWS lambda layer created to use later during the AWS Fargate scanning stack deployment.

5. Deploy AWS Fargate scanning stack using AWS console.

   While deploying the stack, specify the **QualysPodCustomRootCertPath** parameter value as **/opt/<custom certificate path in the zip file uploaded in layer>**.

For example, for the layer created in the above section, the **QualysPodCustomRootCertPath** parameter value is: **QualysPodCustomRootCertPath = /opt/custom-root-ca.cert**.

6. After the stack is deployed, add the created layer to the Lambda function.
   a. Navigate to Lambda Function: "QualysECSFargateImageScanningLambda" function.
   b. Under **Function overview**, select **layers** and click **Add a layer**.
   c. In **Layer source**, select **Custom layers**.
   d. Select the custom layer and version.



Choose a layer

Layer source Info

Choose from layers with a compatible runtime and instruction set architecture or specify the Amazon Resource Name (ARN) of a layer version. You can also create a new layer.

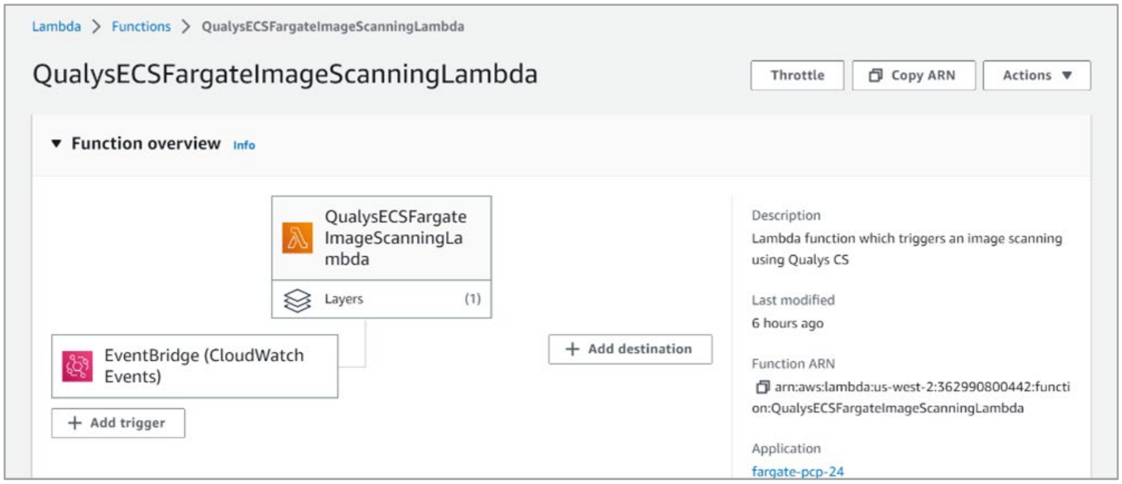
○ AWS layers
Choose a layer from a list of layers provided by AWS.

● Custom layers
Choose a layer from a list of layers created by your AWS account or organization.

○ Specify an ARN
Specify a layer by providing the ARN.

Custom layers
Layers created by your AWS account or organization that are compatible with your function's runtime.
pcp-cert-test ▼

Version
1 ▼



QualysECSFargateImageScanningLambda

▼ Function overview Info

QualysECSFargateImageScanningLambda
Layers (1)

EventBridge (CloudWatch Events)

Description
Lambda function which triggers an image scanning using Qualys CS

Last modified
6 hours ago

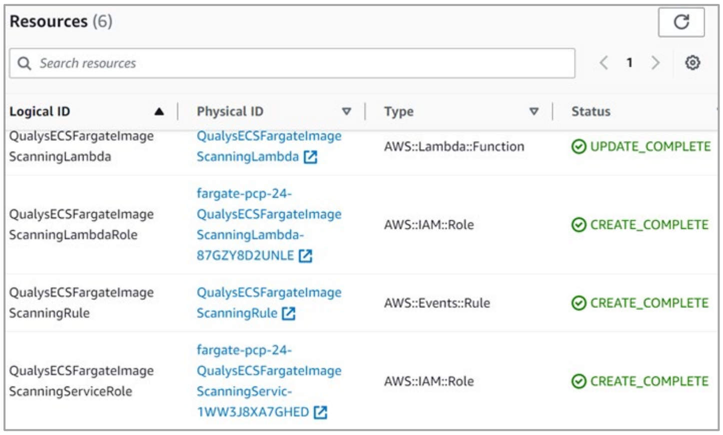
Function ARN
arn:aws:lambda:us-west-2:362990800442:function:QualysECSFargateImageScanningLambda

Application
fargate-pcp-24

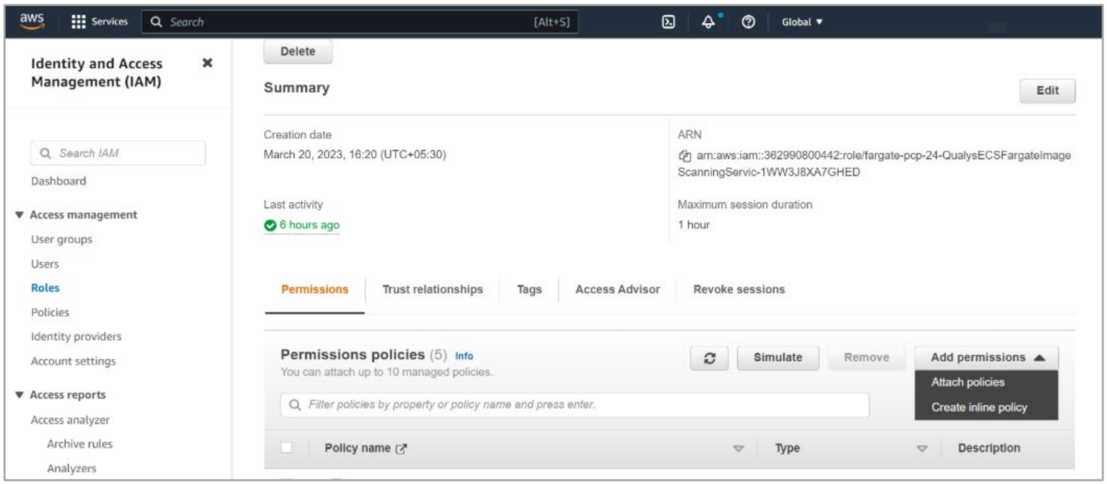
VPC Application and Other Settings for Lambda and Codebuild after Stack Deployment

Deploy the stack using the provided CloudFormation template. Once the stack is deployed or updated, navigate to the **Resources** tab in the stack.

1. Click the "QualysECSFargateImageScanningServiceRole" IAM service role. Select **Add permissions > Attach policies** and select **Codebuild-Qualys-VPC-Access**.



Logical ID	Physical ID	Type	Status
QualysECSFargateImage ScanningLambda	QualysECSFargateImage ScanningLambda	AWS::Lambda::Function	UPDATE_COMPLETE
QualysECSFargateImage ScanningLambdaRole	fargate-pcp-24-QualysECSFargateImage ScanningLambda-87GZY8D2UNLE	AWS::IAM::Role	CREATE_COMPLETE
QualysECSFargateImage ScanningRule	QualysECSFargateImage ScanningRule	AWS::Events::Rule	CREATE_COMPLETE
QualysECSFargateImage ScanningServiceRole	fargate-pcp-24-QualysECSFargateImage ScanningServic-1WW3J8XA7GHED	AWS::IAM::Role	CREATE_COMPLETE



Summary

Creation date: March 20, 2023, 16:20 (UTC+05:30)

ARN: arn:aws:iam::362990800442:role/fargate-pcp-24-QualysECSFargateImage ScanningServic-1WW3J8XA7GHED

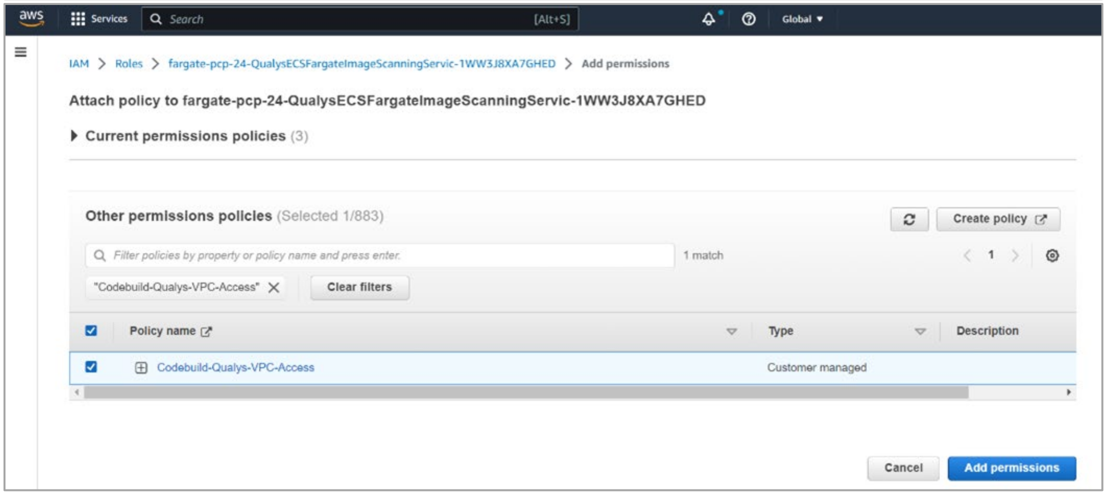
Last activity: 6 hours ago

Maximum session duration: 1 hour

Permissions policies (5) Info

You can attach up to 10 managed policies.

Policy name	Type	Description



IAM > Roles > fargate-pcp-24-QualysECSFargateImageScanningServic-1WW3J8XA7GHED > Add permissions

Attach policy to fargate-pcp-24-QualysECSFargateImageScanningServic-1WW3J8XA7GHED

▸ Current permissions policies (3)

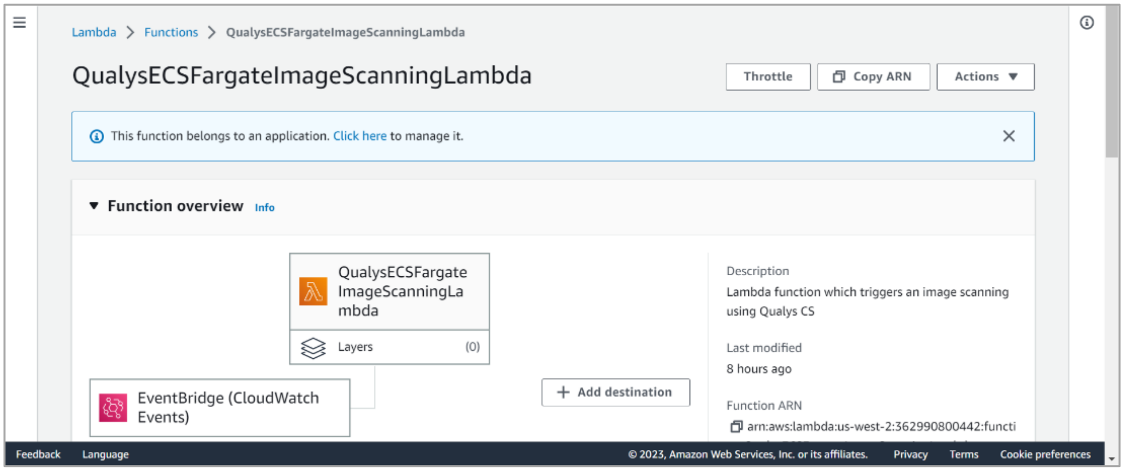
Other permissions policies (Selected 1/883)

"Codebuild-Qualys-VPC-Access" ✕

☑	Policy name	Type	Description
☑	Codebuild-Qualys-VPC-Access	Customer managed	

2. Click “QualysECSFargateImageScanningLambdaRole” IAM service role. Select **Add permissions > Attach policies** and select AWSLambdaVPCAccessExecutionRole.

3. Navigate to the “QualysECSFargateImageScanningLambda” Lambda function. In the **Configuration** tab, under **VPC**, click **Edit** and add the created VPC, the first private subnet, and the default security group.



Lambda > Functions > QualysECSFargateImageScanningLambda

QualysECSFargateImageScanningLambda

Throttle
Copy ARN
Actions ▼

This function belongs to an application. Click here to manage it.

▼ Function overview Info

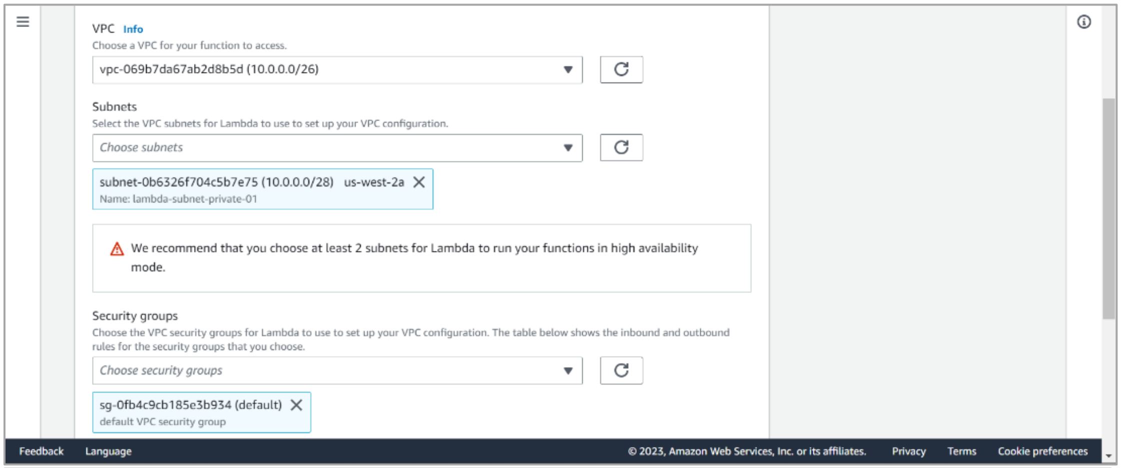
QualysECSFargateImageScanningLambda
Layers (0)
EventBridge (CloudWatch Events)
+ Add destination

Description
Lambda function which triggers an image scanning using Qualys CS

Last modified
8 hours ago

Function ARN
arn:aws:lambda:us-west-2:362990800442:functi

Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



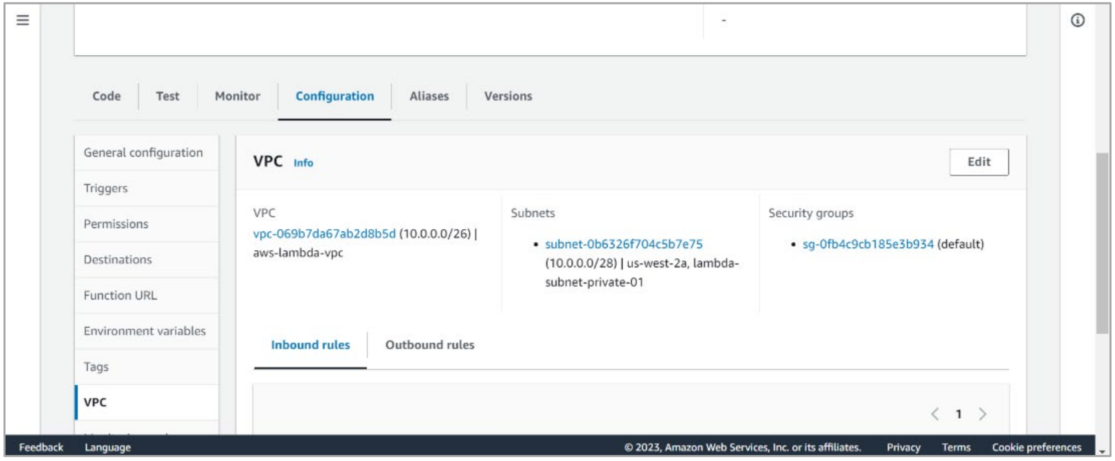
VPC Info
Choose a VPC for your function to access.
vpc-069b7da67ab2d8b5d (10.0.0.0/26)

Subnets
Select the VPC subnets for Lambda to use to set up your VPC configuration.
Choose subnets
subnet-0b6326f704c5b7e75 (10.0.0.0/28) us-west-2a
Name: lambda-subnet-private-01

We recommend that you choose at least 2 subnets for Lambda to run your functions in high availability mode.

Security groups
Choose the VPC security groups for Lambda to use to set up your VPC configuration. The table below shows the inbound and outbound rules for the security groups that you choose.
Choose security groups
sg-0fb4c9cb185e3b934 (default)
default VPC security group

Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Code
Test
Monitor
Configuration
Aliases
Versions
General configuration
Triggers
Permissions
Destinations
Function URL
Environment variables
Tags
VPC
Edit

VPC Info

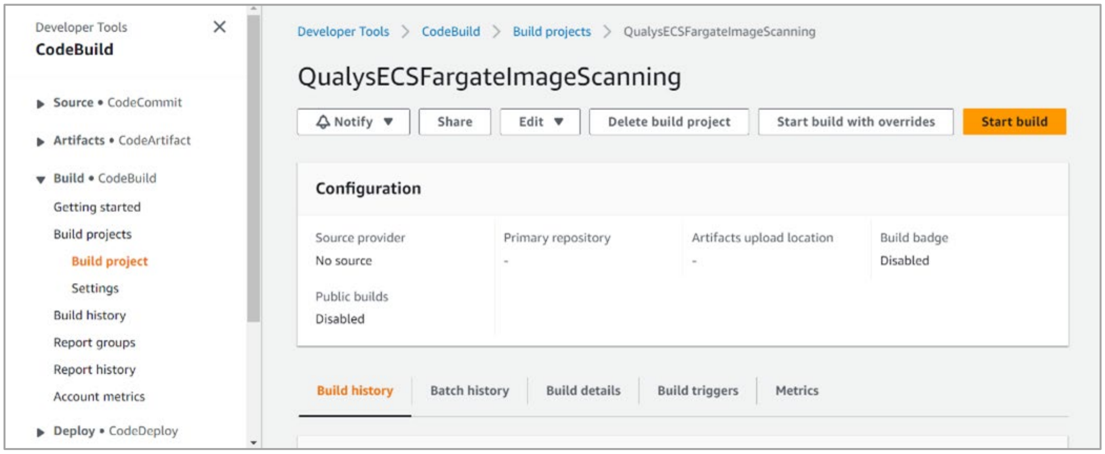
VPC
vpc-069b7da67ab2d8b5d (10.0.0.0/26) | aws-lambda-vpc

Subnets
- subnet-0b6326f704c5b7e75 (10.0.0.0/28) | us-west-2a, lambda-subnet-private-01

Security groups
- sg-0fb4c9cb185e3b934 (default)

Inbound rules
Outbound rules
< 1 >
Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

4. Navigate to **CodeBuild** service **> Build projects > “QualysECSFargateImageScanning” project**.

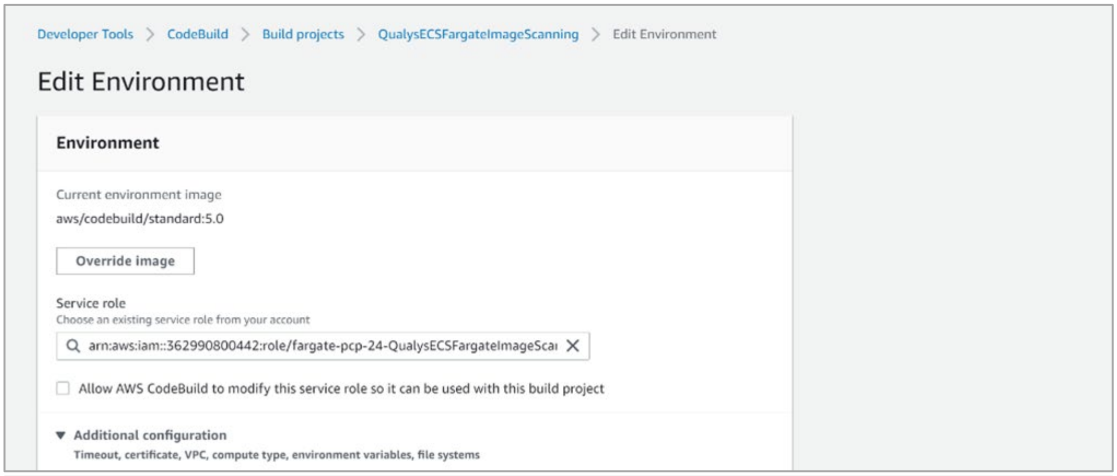


QualysECSFargateImageScanning

Configuration

Source provider	Primary repository	Artifacts upload location	Build badge
No source	-	-	Disabled
Public builds Disabled			

Select **Edit > Environment**. Under Additional configuration, add the created VPC, the second private Subnet, the default security group. Clear the **Allow AWS CodeBuild to modify this service role so it can be used with this build project** check box.


Developer Tools > CodeBuild > Build projects > QualysECSFargateImageScanning > Edit Environment
Override image

Edit Environment

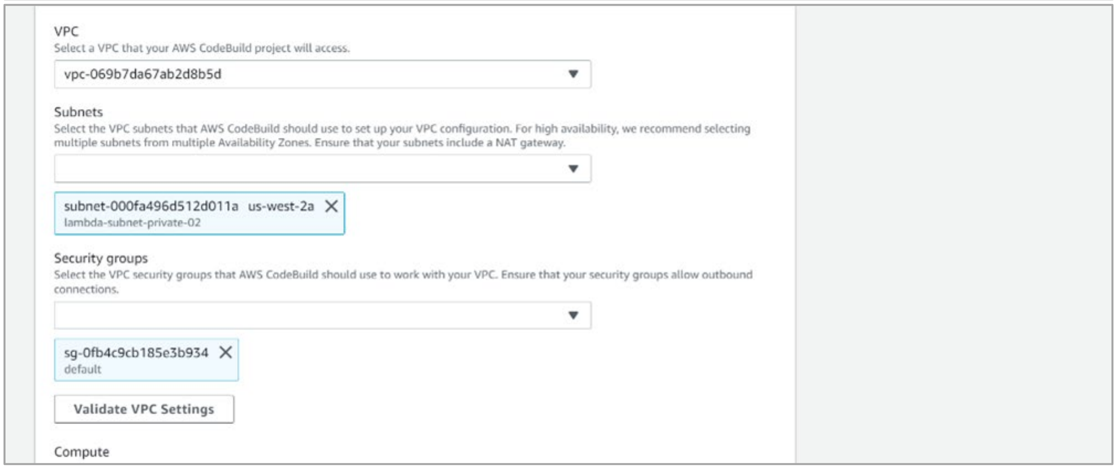
Environment

Current environment image
aws/codebuild/standard:5.0

Service role
Choose an existing service role from your account
arn:aws:iam::362990800442:role/fargate-pcp-24-QualysECSFargateImageScai

☐ Allow AWS CodeBuild to modify this service role so it can be used with this build project

▼ Additional configuration
Timeout, certificate, VPC, compute type, environment variables, file systems



VPC
Select a VPC that your AWS CodeBuild project will access.
vpc-069b7da67ab2d8b5d

Subnets
Select the VPC subnets that AWS CodeBuild should use to set up your VPC configuration. For high availability, we recommend selecting multiple subnets from multiple Availability Zones. Ensure that your subnets include a NAT gateway.
subnet-000fa496d512d011a us-west-2a
lambda-subnet-private-02

Security groups
Select the VPC security groups that AWS CodeBuild should use to work with your VPC. Ensure that your security groups allow outbound connections.
sg-0fb4c9cb185e3b934
default

Compute

Your stack is now ready to use. You can now launch an AWS task for scanning.