AWS auto onboarding lambda Function

Code and components:
https://github.com/c0rrosive/PC_CFT_toolkit

Changelog:
11/15/23: Updated policy template to include iam:ListPolicyVersions

Note: If cloud provisioning admin service account is used then the account group id in code must match the one assigned to the access key.

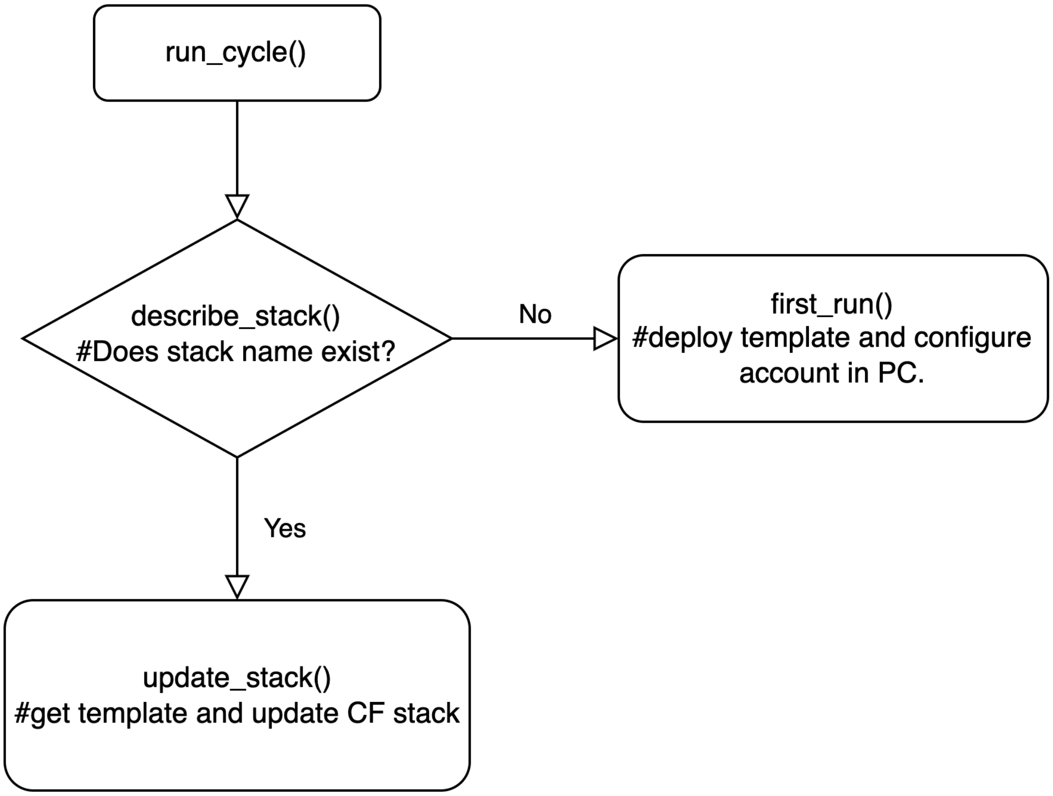
Limitations:
Lambdas have a 15 minute maximum timeout and the stack must be created within this time period for initial onboarding. This does not apply to template updates. Individual account stack creation occurs quickly and should not pose a problem but large organizations where stack creation takes longer than 14 minutes could fail.

Use case:
Third party vendor account with no access
Auto-pilot-permissions

Pre-requisites:

- Prisma cloud access key.
- Cloud account access.
- Lambda layer with PCPI built into zip file.

Workflow:

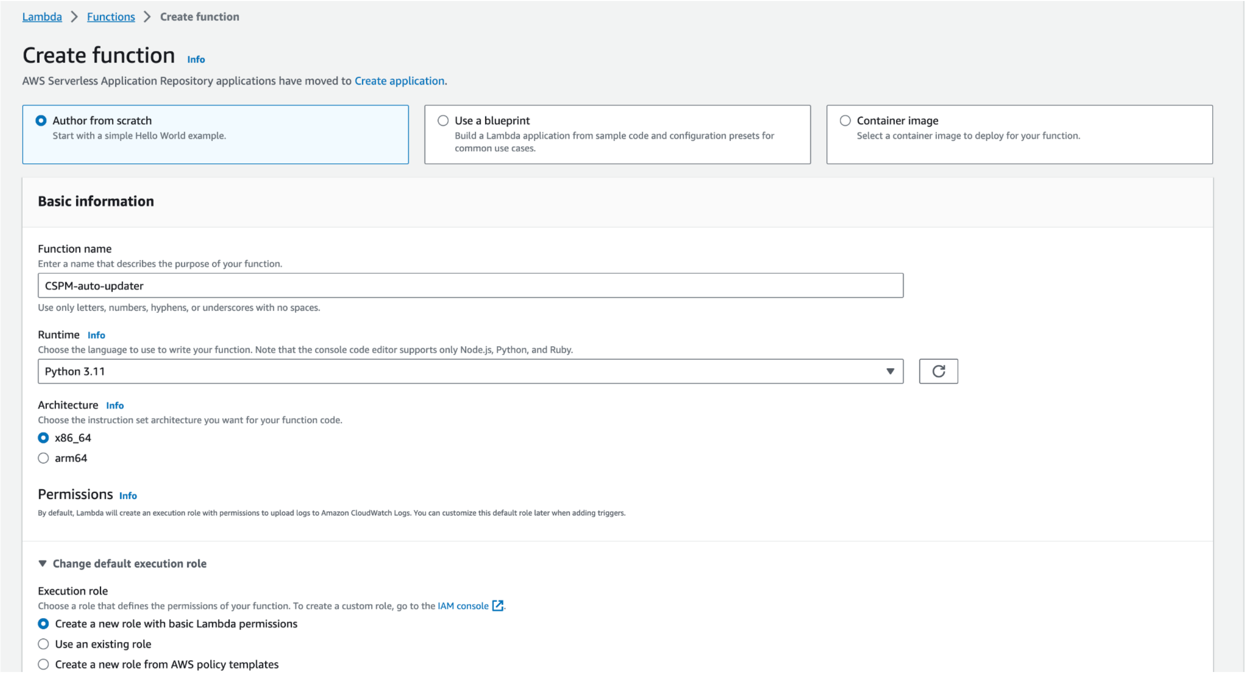


Build lambda layer:

```
#/bin/bash
mkdir lambda-maker
cd lambda-maker/
mkdir python
cd python/
pip3 install pcpi -t .
rm -rf *.dist-info
cd ..
zip -r PCPI-lambda-layer.zip python/
```

Setup instructions:

1. Create python Lambda with a new execution role.



Lambda > Functions > Create function

Create function Info

AWS Serverless Application Repository applications have moved to Create application.

● 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.

Basic information

Function name
Enter a name that describes the purpose of your function.
CSPM-auto-updater
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 3.11

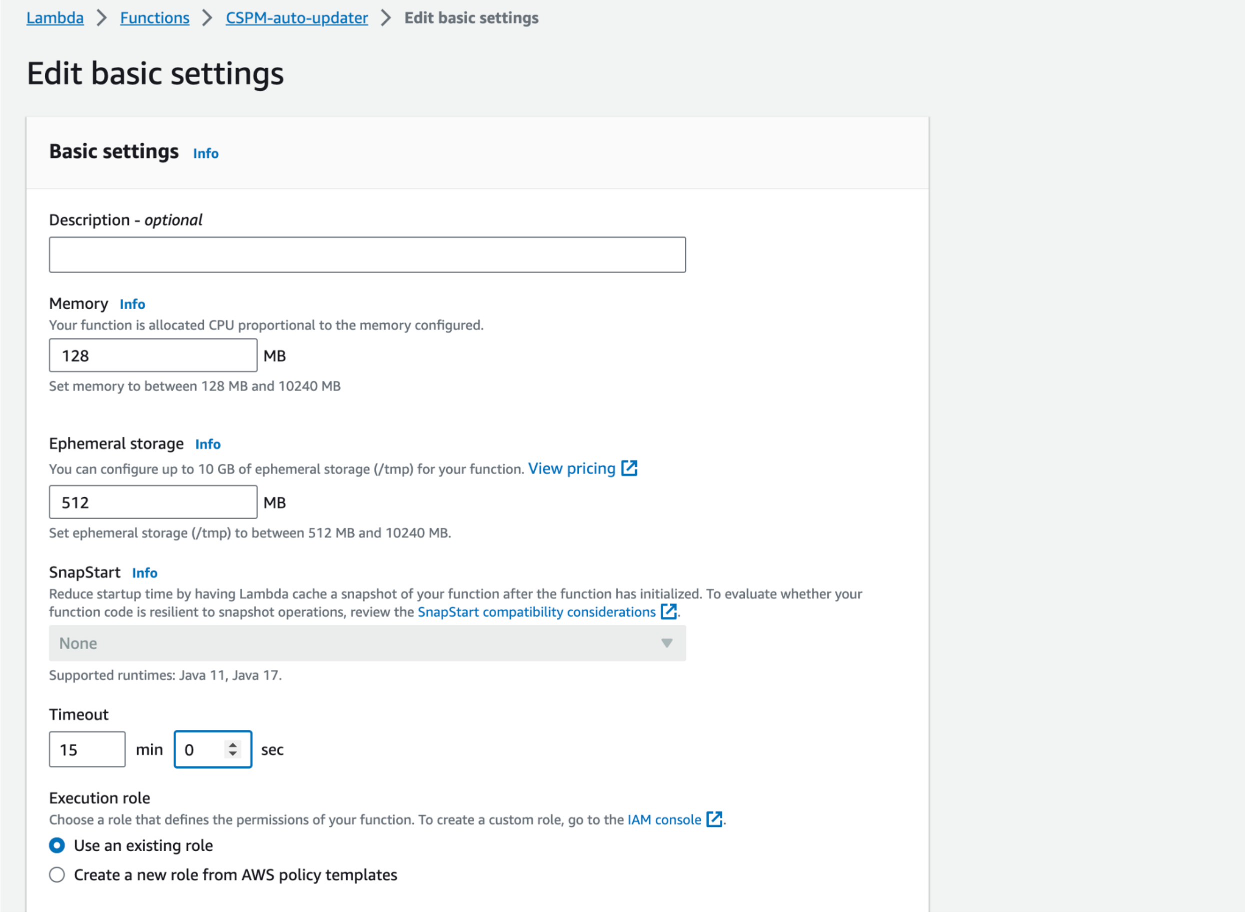
Architecture Info
Choose the instruction set architecture you want for your function code.
● x86_64
○ arm64

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

2. Increase Lambda timeout to the 15 minutes maximum.



Lambda > Functions > CSPM-auto-updater > Edit basic settings

Edit basic settings

Basic settings Info

Description - *optional*

Memory Info

Your function is allocated CPU proportional to the memory configured.

128 MB

Set memory to between 128 MB and 10240 MB

Ephemeral storage Info

You can configure up to 10 GB of ephemeral storage (/tmp) for your function. View pricing

512 MB

Set ephemeral storage (/tmp) to between 512 MB and 10240 MB.

SnapStart Info

Reduce startup time by having Lambda cache a snapshot of your function after the function has initialized. To evaluate whether your function code is resilient to snapshot operations, review the SnapStart compatibility considerations.

None

Supported runtimes: Java 11, Java 17.

Timeout

15 min 0 sec

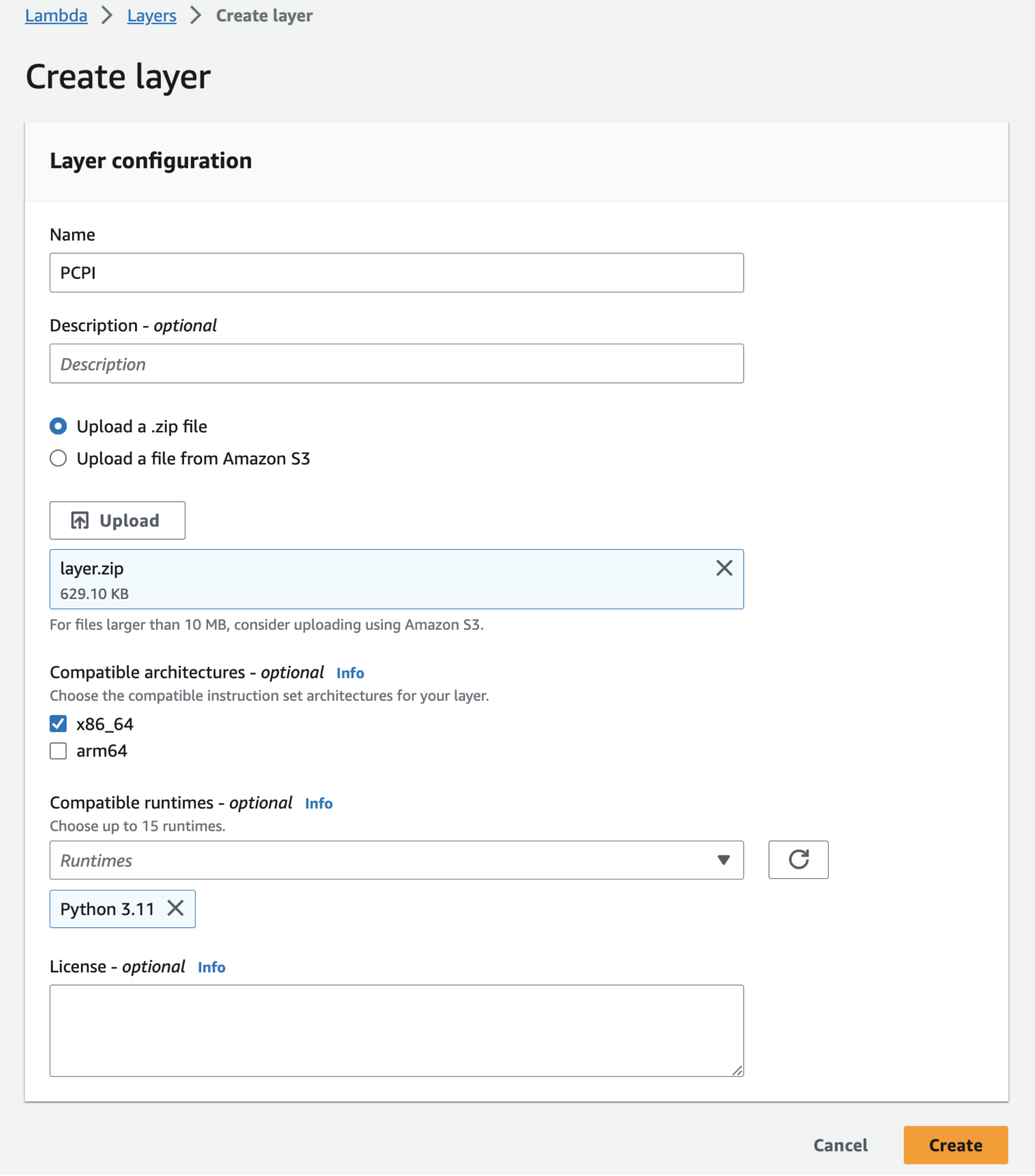
Execution role

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

3. Create a layer with layer.zip containing the PCPI library.



Create layer

Layer configuration

Name: PCPI

Description - *optional*: *Description*

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

layer.zip
629.10 KB

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

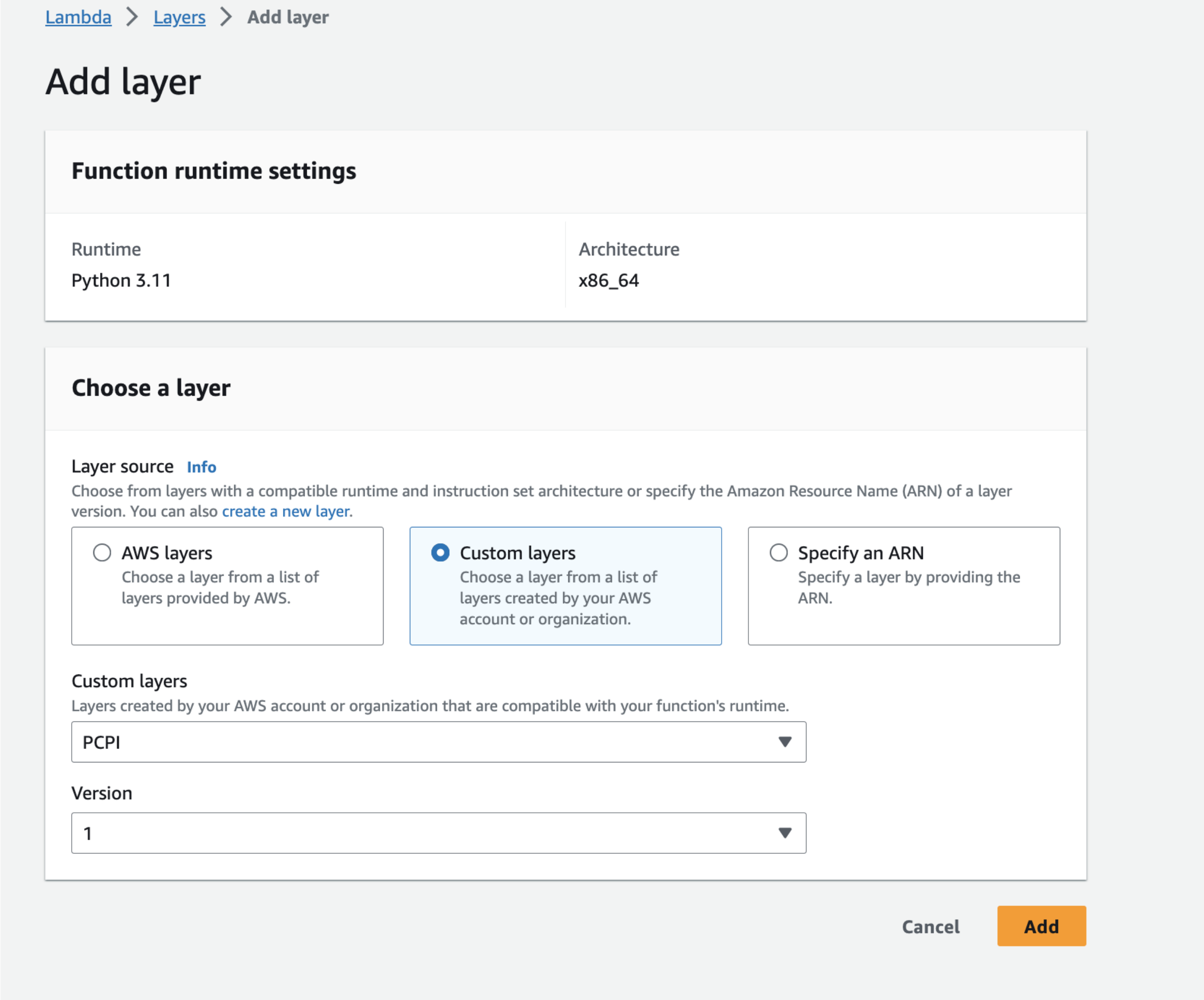
Compatible runtimes - *optional* Info
Choose up to 15 runtimes.

Runtimes

Python 3.11

License - *optional* Info

4. Add layer to function.



Lambda > Layers > Add layer

Add layer

Function runtime settings

Runtime
Python 3.11

Architecture
x86_64

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.

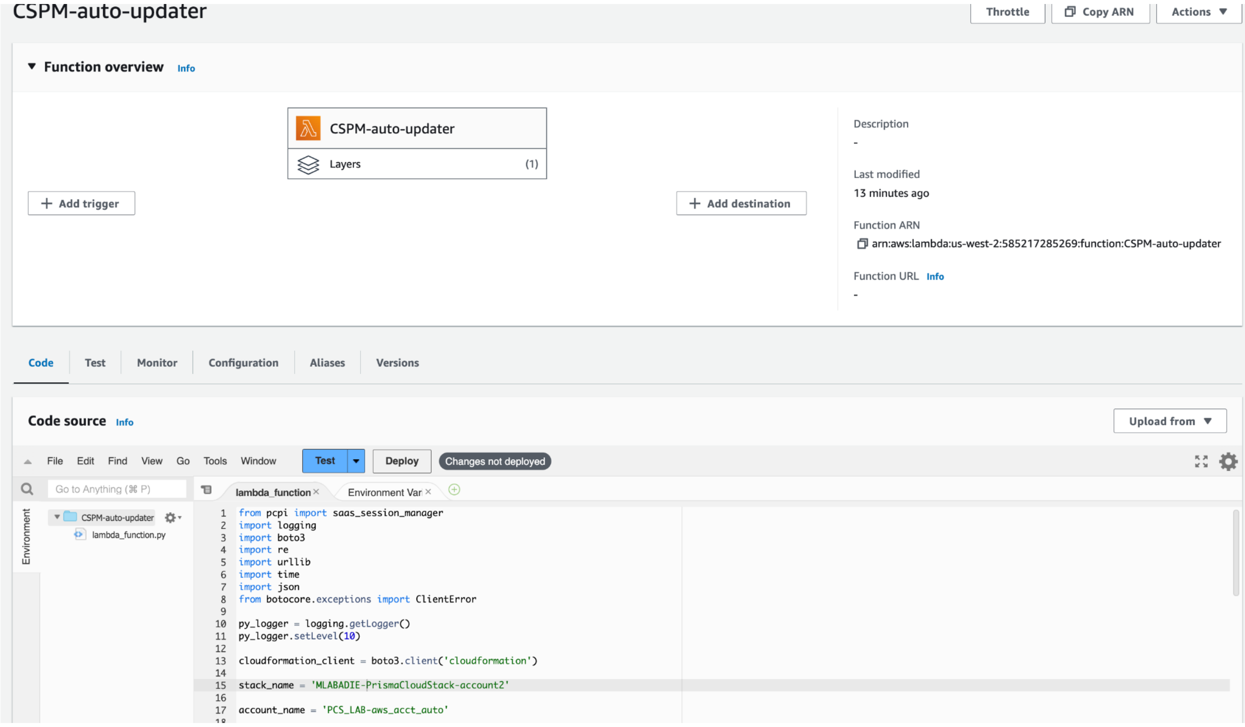
● Custom layers
Choose a layer from a list of layers created by your AWS account or organization.

○ 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.
PCPI ▼

Version
1 ▼

5. Add code to lambda.



Description
-

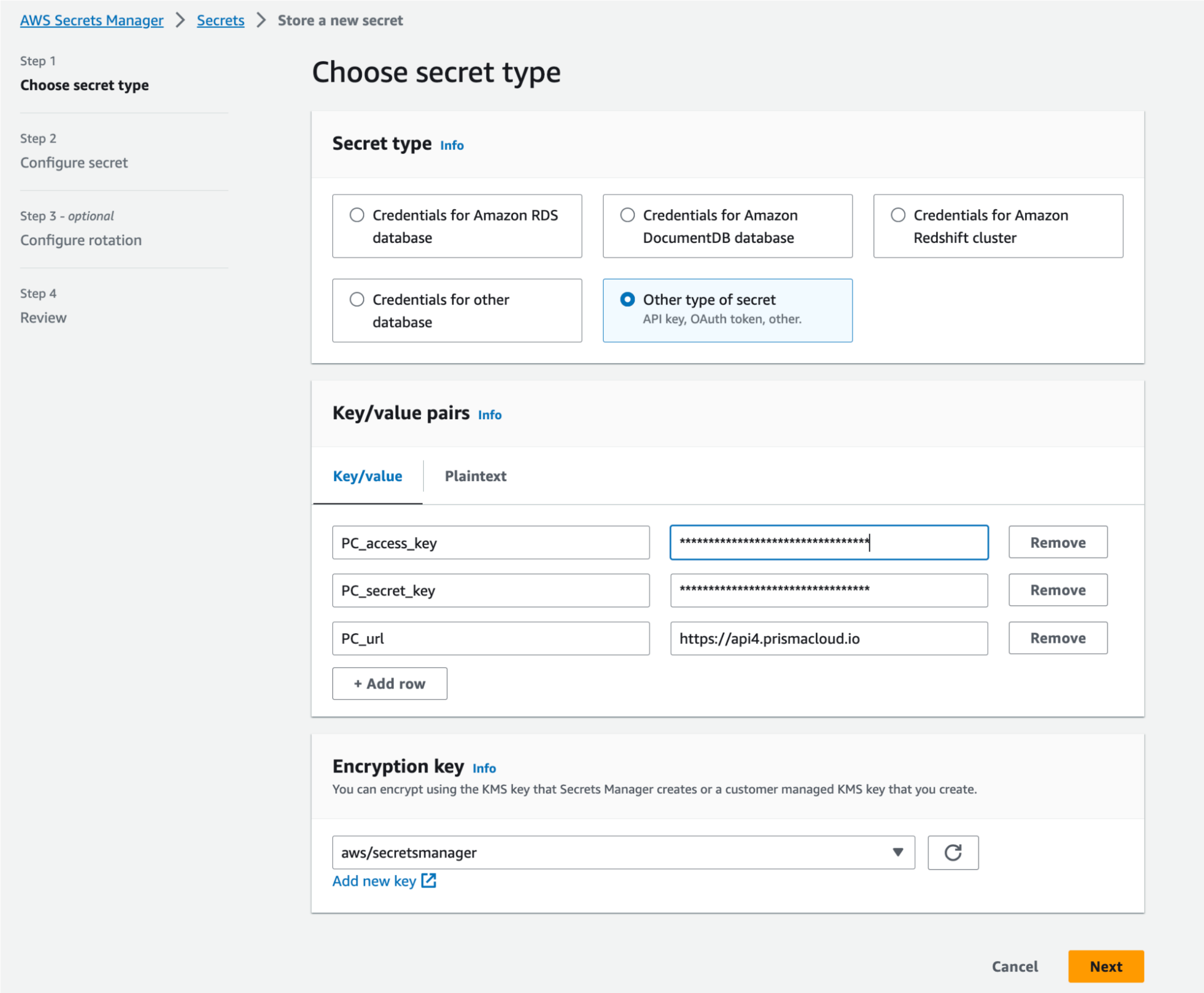
Last modified
13 minutes ago

Function ARN
arn:aws:lambda:us-west-2:585217285269:function:CSPM-auto-updater

Function URL Info
-

```
from pcpi import saas_session_manager
import logging
import boto3
import re
import urllib
import time
import json
from botocore.exceptions import ClientError

py_logger = logging.getLogger()
py_logger.setLevel(10)

cloudformation_client = boto3.client('cloudformation')

stack_name = 'MLABADIE-PrismaCloudStack-account2'

account_name = 'PCS_LAB-aws_acct_auto'
```

6. Create “other type” secret with 3 keys: PC_access_key,PC_secret_key,PC_url.



AWS Secrets Manager > Secrets > Store a new secret

Step 1
Choose secret type

Step 2
Configure secret

Step 3 - *optional*
Configure rotation

Step 4
Review

Choose secret type

Secret type Info

○ Credentials for Amazon RDS database
○ Credentials for Amazon DocumentDB database
○ Credentials for Amazon Redshift cluster
○ Credentials for other database
● Other type of secret
API key, OAuth token, other.

Key/value pairs Info

Key/value | Plaintext

PC_access_key	********************************	Remove
PC_secret_key	********************************	Remove
PC_url	https://api4.prismacloud.io	Remove

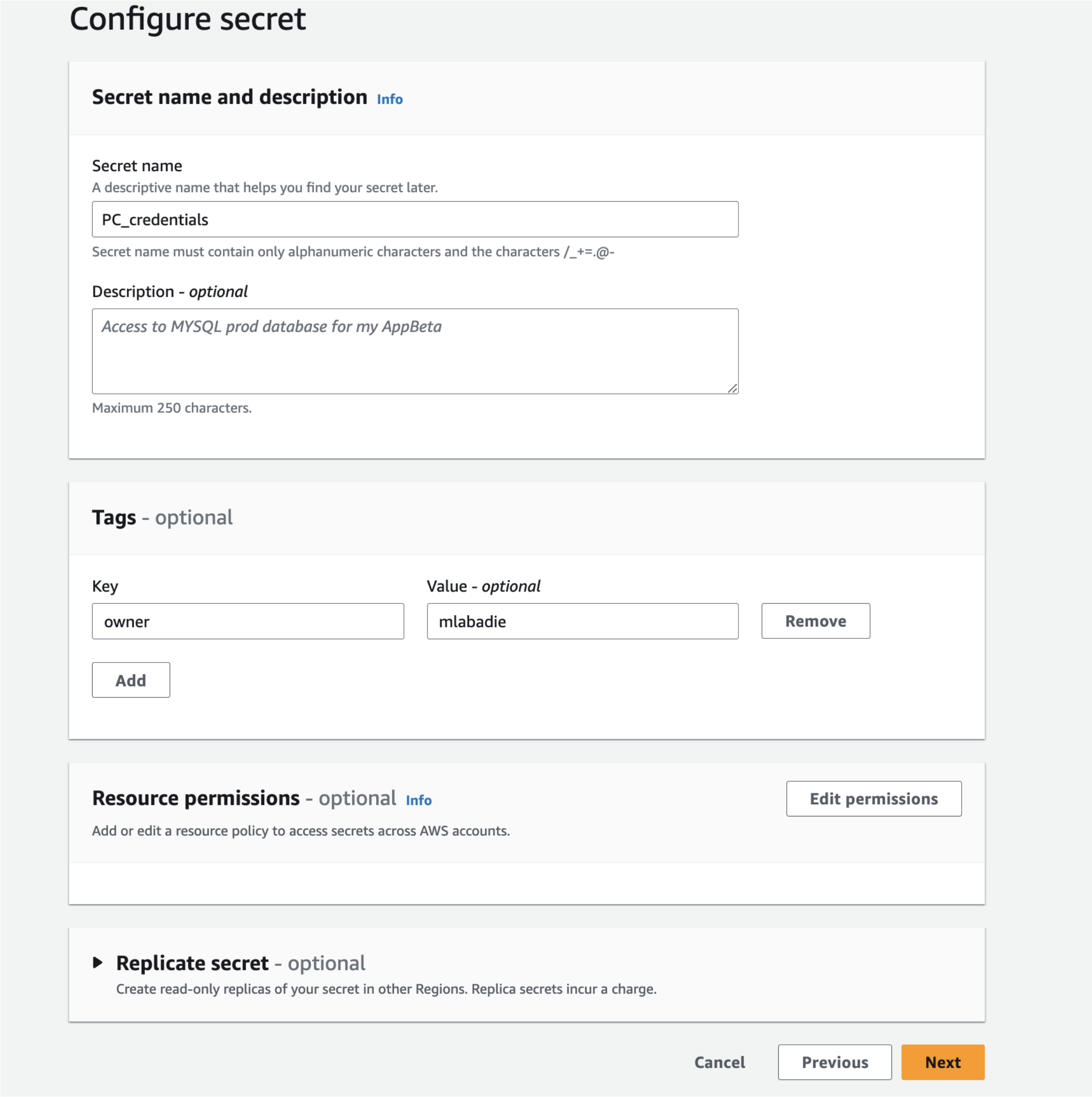
+ Add row

Encryption key Info
You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager ▼

Add new key

Cancel   Next



Configure secret

Secret name and description

Secret name

A descriptive name that helps you find your secret later.

PC_credentials

Secret name must contain only alphanumeric characters and the characters /_+=.@-

Description - *optional*

Access to MYSQL prod database for my AppBeta

Maximum 250 characters.

Tags - optional

Key	Value - *optional*
owner	mlabadie

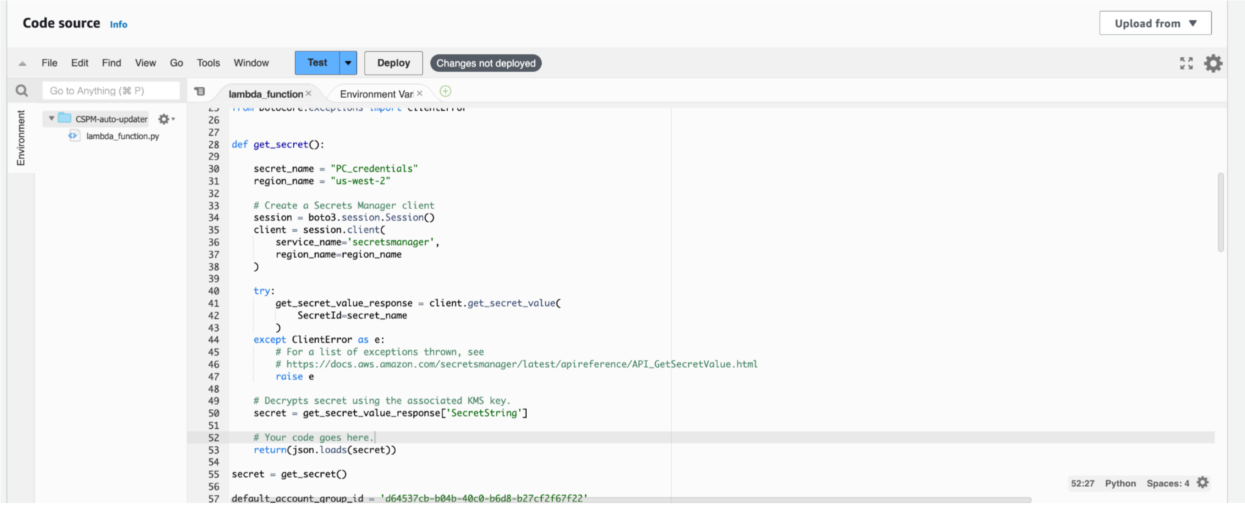
Resource permissions - optional

Add or edit a resource policy to access secrets across AWS accounts.

▶ Replicate secret - optional

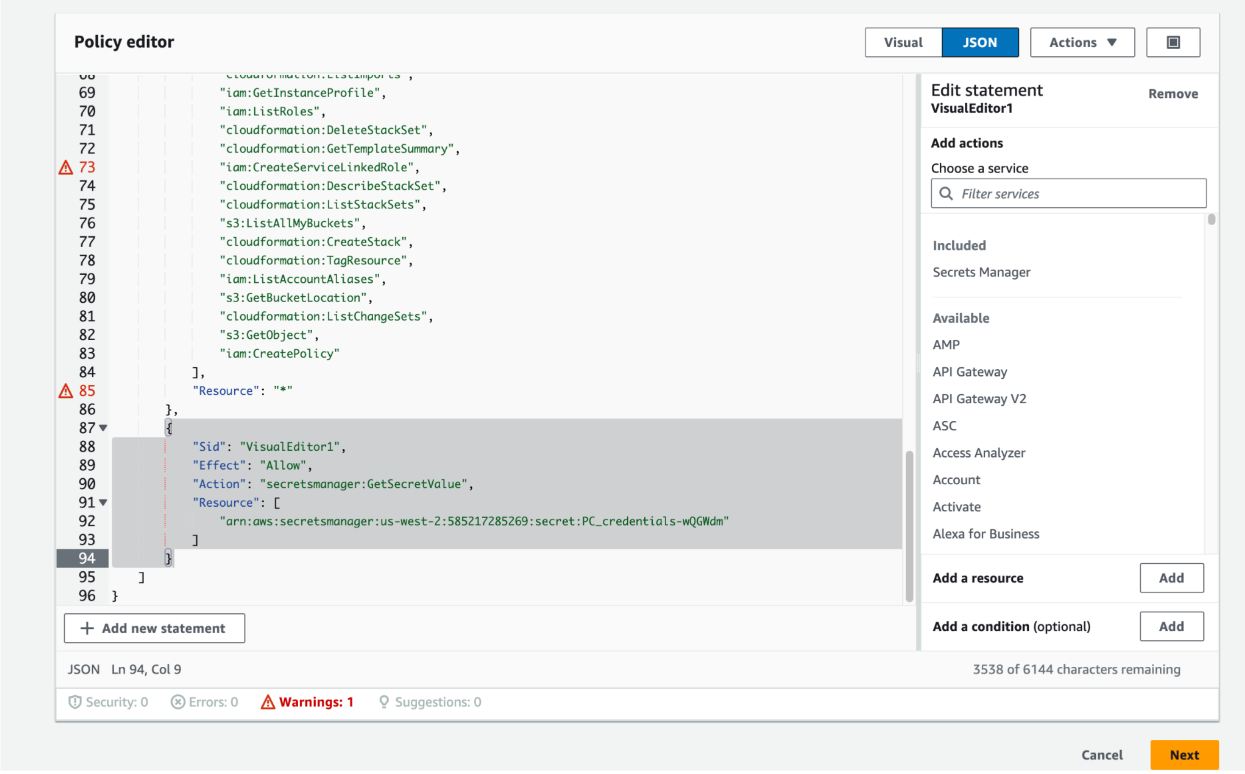
Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

7. Add get secret function to code while keeping return line.



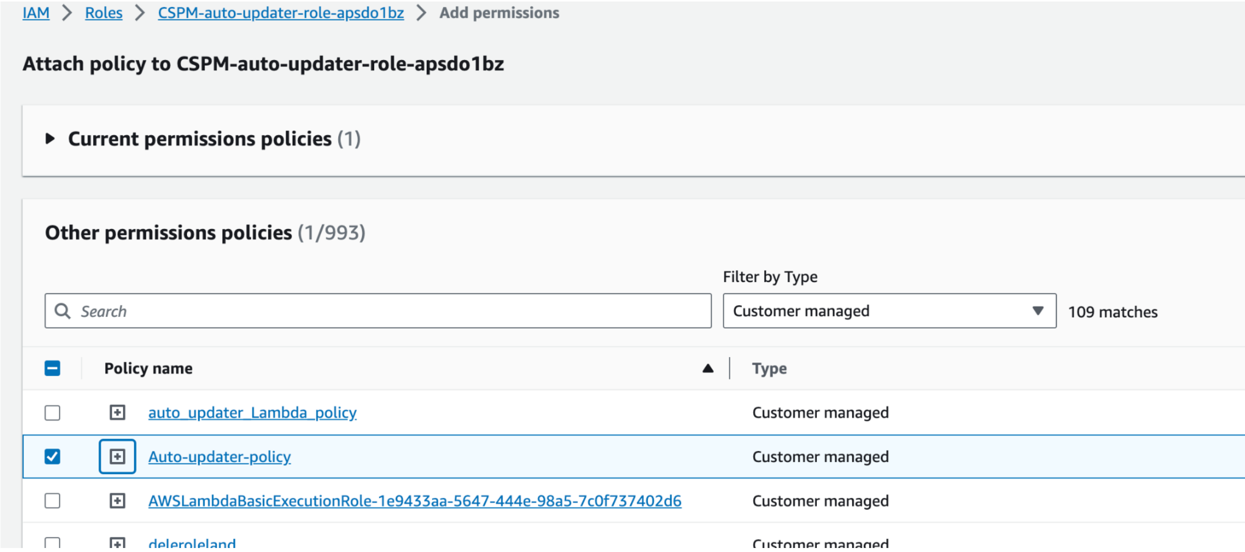
```python
from botocore.exceptions import ClientError


def get_secret():

    secret_name = "PC_credentials"
    region_name = "us-west-2"

    # Create a Secrets Manager client
    session = boto3.session.Session()
    client = session.client(
        service_name='secretsmanager',
        region_name=region_name
    )

    try:
        get_secret_value_response = client.get_secret_value(
            SecretId=secret_name
        )
    except ClientError as e:
        # For a list of exceptions thrown, see
        # https://docs.aws.amazon.com/secretsmanager/latest/apireference/API_GetSecretValue.html
        raise e

    # Decrypts secret using the associated KMS key.
    secret = get_secret_value_response['SecretString']

    # Your code goes here.
    return(json.loads(secret))

secret = get_secret()

default_account_group_id = 'd64537cb-b04b-40c0-b6d8-b27cf2f67f22'
```

8. Create IAM policy with JSON template and add previously created secret ARN.



```json
                "cloudformation:ListImports",
                "iam:GetInstanceProfile",
                "iam:ListRoles",
                "cloudformation:DeleteStackSet",
                "cloudformation:GetTemplateSummary",
                "iam:CreateServiceLinkedRole",
                "cloudformation:DescribeStackSet",
                "cloudformation:ListStackSets",
                "s3:ListAllMyBuckets",
                "cloudformation:CreateStack",
                "cloudformation:TagResource",
                "iam:ListAccountAliases",
                "s3:GetBucketLocation",
                "cloudformation:ListChangeSets",
                "s3:GetObject",
                "iam:CreatePolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": [
                "arn:aws:secretsmanager:us-west-2:585217285269:secret:PC_credentials-wQGWdm"
            ]
        }
    ]
}
```

9. Attach policy to lambda execution role.



IAM > Roles > CSPM-auto-updater-role-apsdo1bz > Add permissions

Attach policy to CSPM-auto-updater-role-apsdo1bz

▸ Current permissions policies (1)

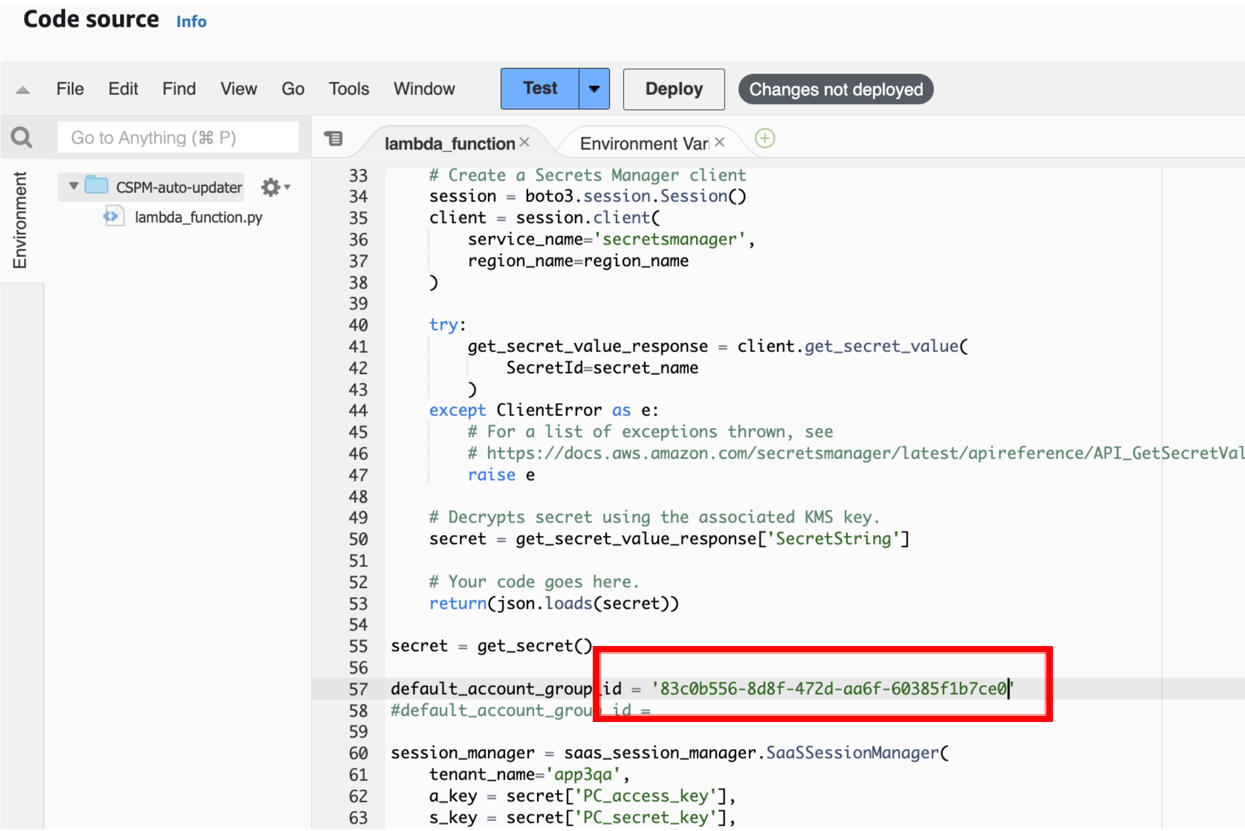
Other permissions policies (1/993)

Filter by Type

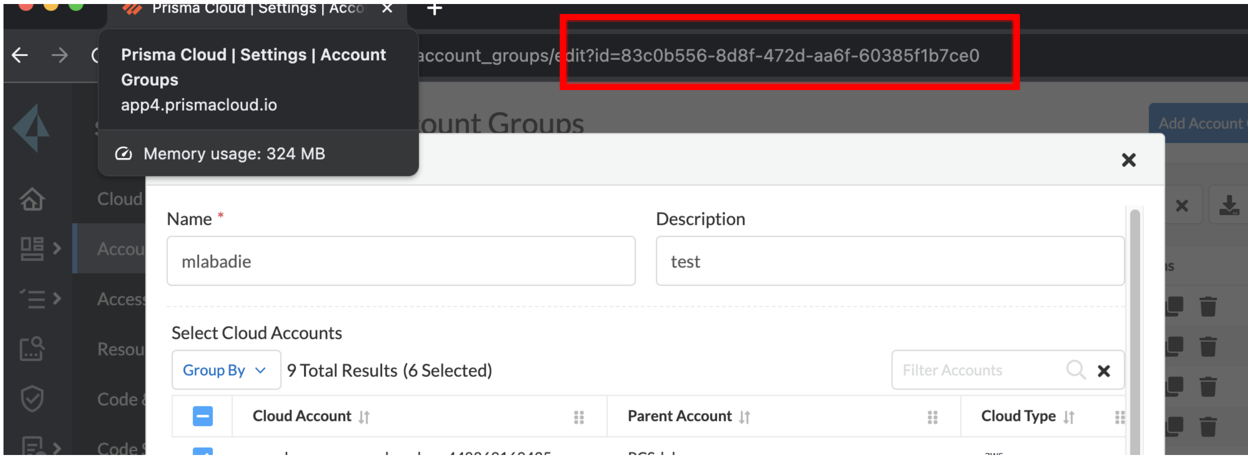
Search | Customer managed ▼ | 109 matches

▬	Policy name ▲	Type
□	⊞ auto_updater_Lambda_policy	Customer managed
☑	⊞ Auto-updater-policy	Customer managed
□	⊞ AWSLambdaBasicExecutionRole-1e9433aa-5647-444e-98a5-7c0f737402d6	Customer managed
□	⊞ deleroleland	Customer managed

10. Edit default account group ID in code.



```
    # Create a Secrets Manager client
    session = boto3.session.Session()
    client = session.client(
        service_name='secretsmanager',
        region_name=region_name
    )

    try:
        get_secret_value_response = client.get_secret_value(
            SecretId=secret_name
        )
    except ClientError as e:
        # For a list of exceptions thrown, see
        # https://docs.aws.amazon.com/secretsmanager/latest/apireference/API_GetSecretVal
        raise e

    # Decrypts secret using the associated KMS key.
    secret = get_secret_value_response['SecretString']

    # Your code goes here.
    return(json.loads(secret))

secret = get_secret()

default_account_group_id = '83c0b556-8d8f-472d-aa6f-60385f1b7ce0'
#default_account_group_id =

session_manager = saas_session_manager.SaaSSessionManager(
    tenant_name='app3qa',
    a_key = secret['PC_access_key'],
    s_key = secret['PC_secret_key'],
```



account_groups/edit?id=83c0b556-8d8f-472d-aa6f-60385f1b7ce0

Name * mlabadie

Description test

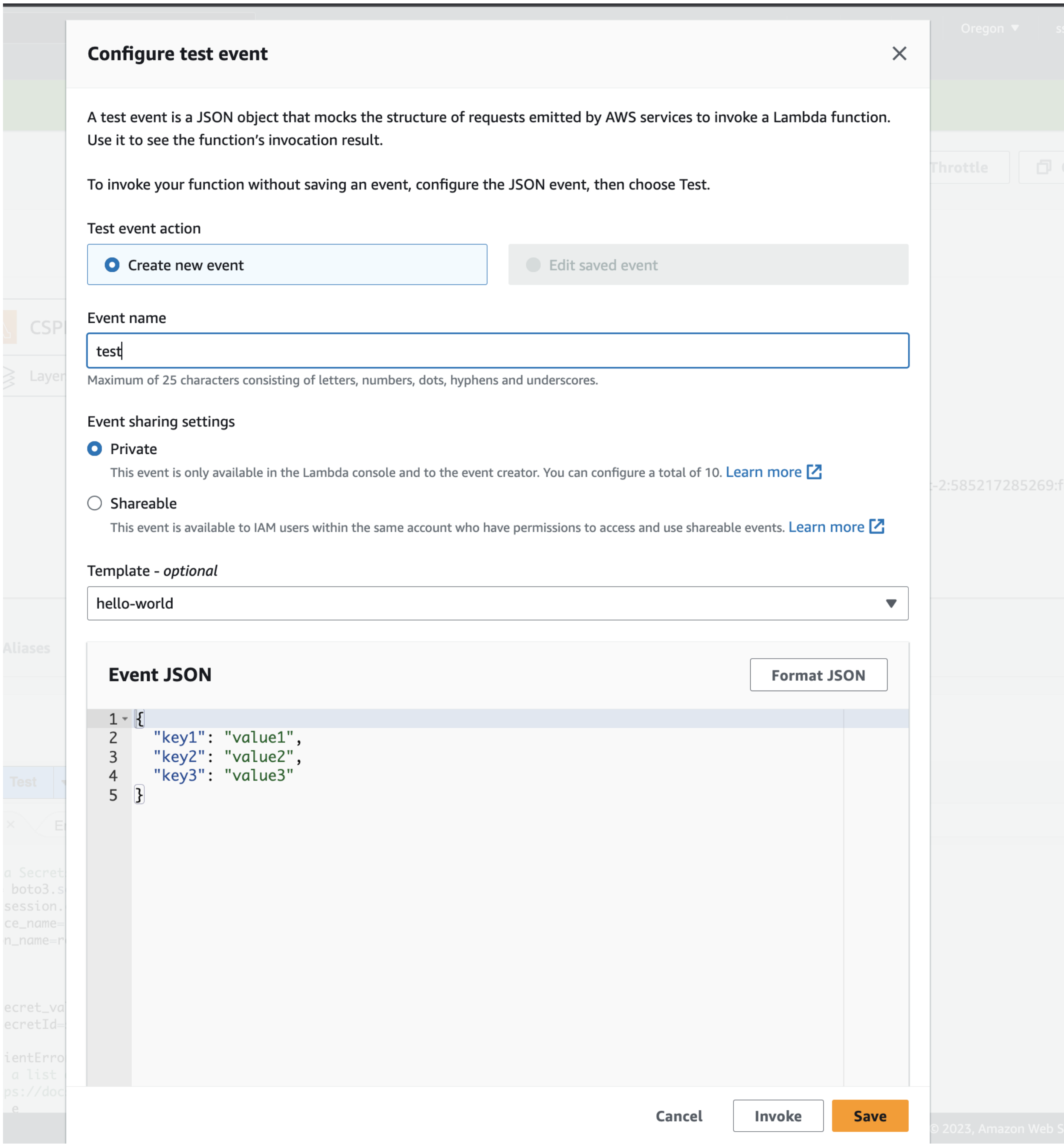
Select Cloud Accounts

Group By 9 Total Results (6 Selected)

Filter Accounts

Cloud Account	Parent Account	Cloud Type

11. Deploy & Test with blank event, doesn't use event or context.



Configure test event

A test event is a JSON object that mocks the structure of requests emitted by AWS services to invoke a Lambda function. Use it to see the function's invocation result.

To invoke your function without saving an event, configure the JSON event, then choose Test.

Test event action

● Create new event ○ Edit saved event

Event name

test

Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings

● Private

This event is only available in the Lambda console and to the event creator. You can configure a total of 10. Learn more

○ Shareable

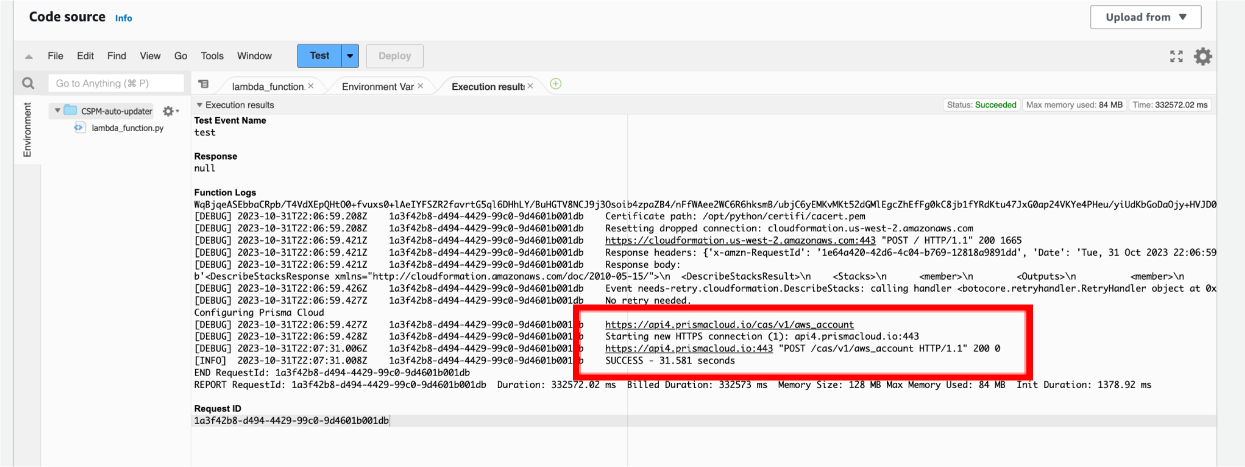
This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more

Template - *optional*

hello-world

Event JSON

```
{
  "key1": "value1",
  "key2": "value2",
  "key3": "value3"
}
```



Status: Succeeded Max memory used: 84 MB Time: 332572.02 ms

Test Event Name

```
test
```

Response

```
null
```

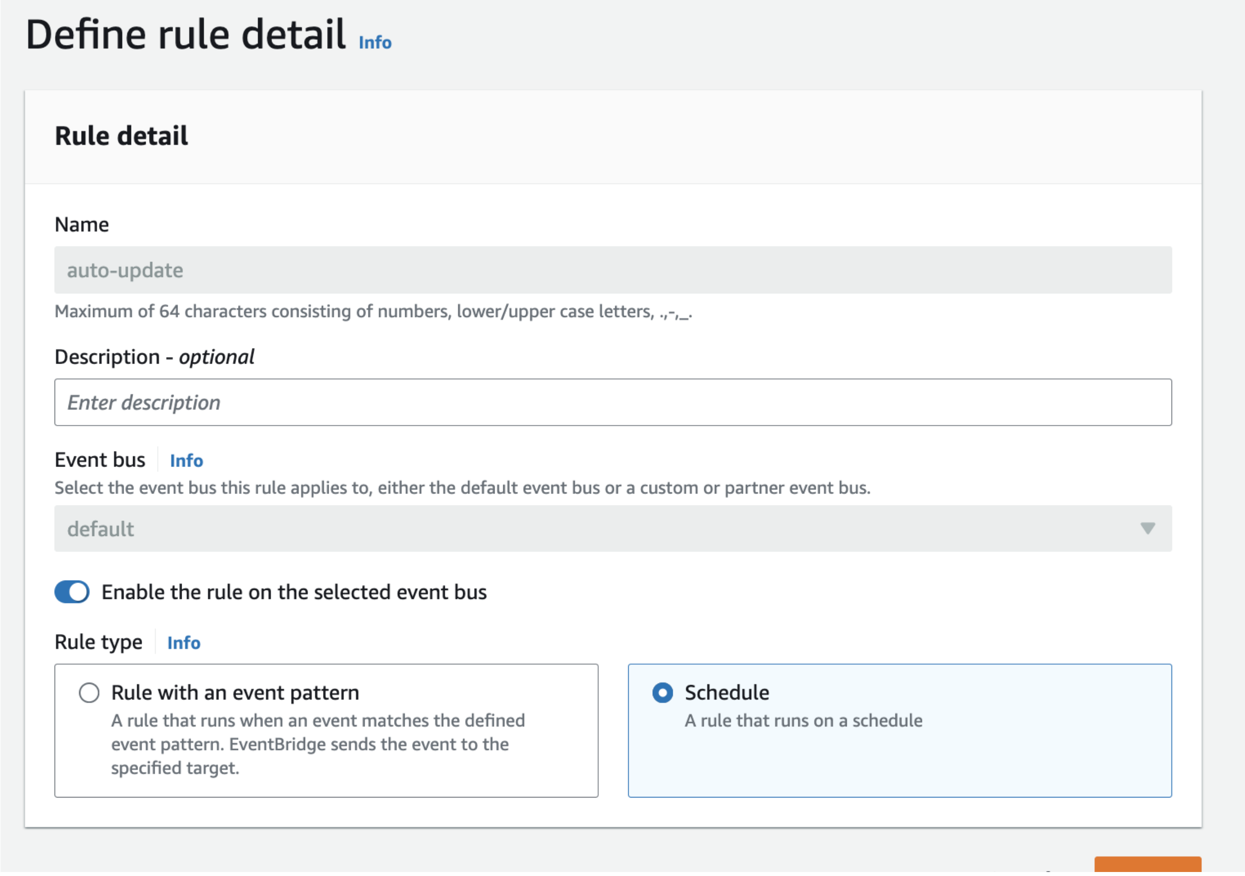
Function Logs

```
WqBjqeASEbbaCRpb/T4VdXEpQHtO0+fvuxs0+lAeIYFSZR2favrtG5ql6DHhLY/BuHGTV8NCJ9j3Osoib4zpaZB4/nFfWAee2WC6R6hksmB/ubjC6yEMKvMKt52dGMlEgcZhEfFg0kC8jb1fYRdKtu47JxG0ap24VKYe4PHeu/yiUdKbGoDaOjy+HVJD0
[DEBUG] 2023-10-31T22:06:59.208Z    1a3f42b8-d494-4429-99c0-9d4601b001db    Certificate path: /opt/python/certifi/cacert.pem
[DEBUG] 2023-10-31T22:06:59.208Z    1a3f42b8-d494-4429-99c0-9d4601b001db    Resetting dropped connection: cloudformation.us-west-2.amazonaws.com
[DEBUG] 2023-10-31T22:06:59.421Z    1a3f42b8-d494-4429-99c0-9d4601b001db    https://cloudformation.us-west-2.amazonaws.com:443 "POST / HTTP/1.1" 200 1665
[DEBUG] 2023-10-31T22:06:59.421Z    1a3f42b8-d494-4429-99c0-9d4601b001db    Response headers: {'x-amzn-RequestId': '1e64a420-42d6-4c04-b769-12818a9891dd', 'Date': 'Tue, 31 Oct 2023 22:06:59
[DEBUG] 2023-10-31T22:06:59.421Z    1a3f42b8-d494-4429-99c0-9d4601b001db    Response body:
b'<DescribeStacksResponse xmlns="http://cloudformation.amazonaws.com/doc/2010-05-15/">\n  <DescribeStacksResult>\n    <Stacks>\n      <member>\n        <Outputs>\n          <member>\n
[DEBUG] 2023-10-31T22:06:59.426Z    1a3f42b8-d494-4429-99c0-9d4601b001db    Event needs-retry.cloudformation.DescribeStacks: calling handler <botocore.retryhandler.RetryHandler object at 0x
[DEBUG] 2023-10-31T22:06:59.427Z    1a3f42b8-d494-4429-99c0-9d4601b001db    No retry needed.
Configuring Prisma Cloud
[DEBUG] 2023-10-31T22:06:59.427Z    1a3f42b8-d494-4429-99c0-9d4601b001db    https://api4.prismacloud.io/cas/v1/aws_account
[DEBUG] 2023-10-31T22:06:59.428Z    1a3f42b8-d494-4429-99c0-9d4601b001db    Starting new HTTPS connection (1): api4.prismacloud.io:443
[DEBUG] 2023-10-31T22:07:31.006Z    1a3f42b8-d494-4429-99c0-9d4601b001db    https://api4.prismacloud.io:443 "POST /cas/v1/aws_account HTTP/1.1" 200 0
[INFO]  2023-10-31T22:07:31.008Z    1a3f42b8-d494-4429-99c0-9d4601b001db    SUCCESS - 31.581 seconds
END RequestId: 1a3f42b8-d494-4429-99c0-9d4601b001db
REPORT RequestId: 1a3f42b8-d494-4429-99c0-9d4601b001db  Duration: 332572.02 ms  Billed Duration: 332573 ms  Memory Size: 128 MB Max Memory Used: 84 MB  Init Duration: 1378.92 ms
```

Request ID

```
1a3f42b8-d494-4429-99c0-9d4601b001db
```

12. Schedule using trigger with eventbridge and new rule: cron(15 10 ? * 6L *)



Define rule detail Info

Rule detail

Name

auto-update

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.

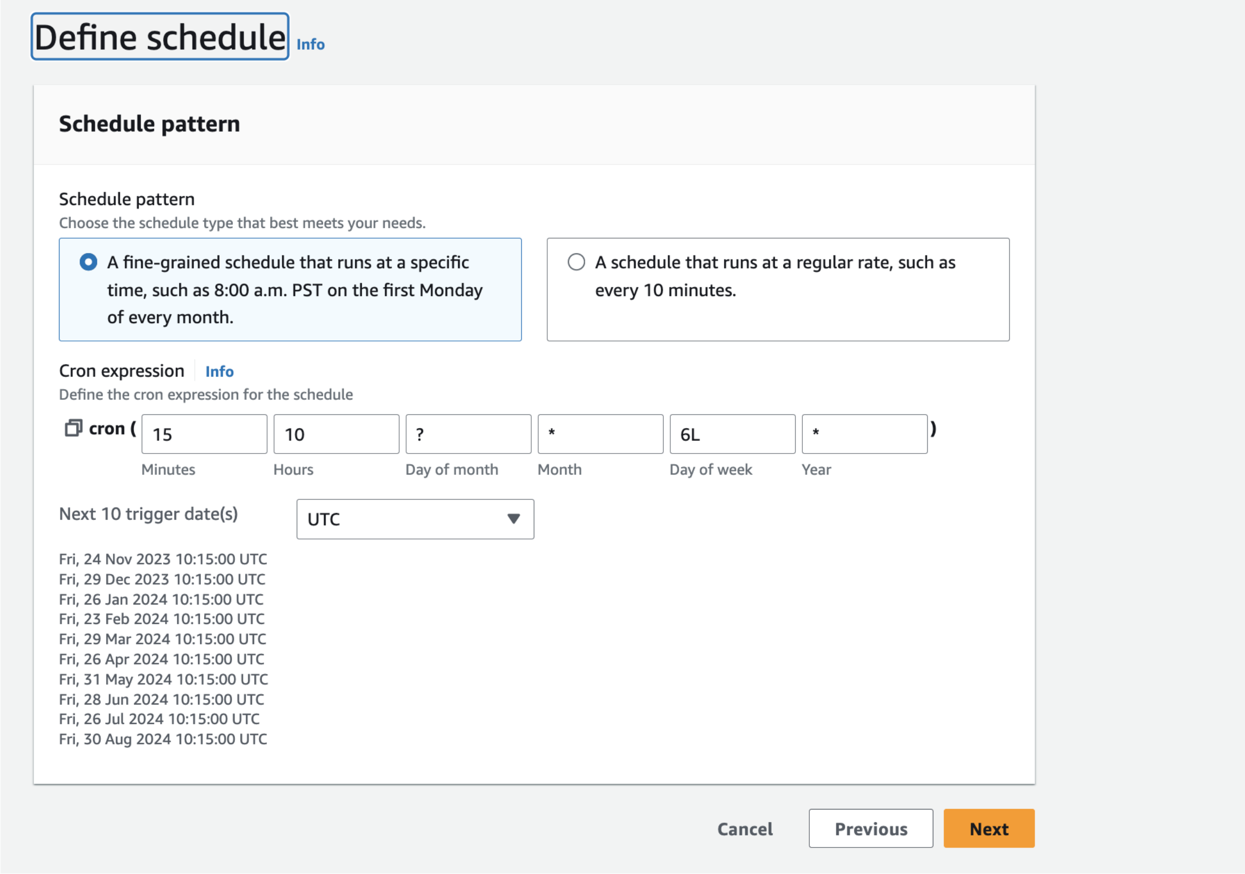
default

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



Define schedule

Schedule pattern

Schedule pattern

Choose the schedule type that best meets your needs.

● A fine-grained schedule that runs at a specific time, such as 8:00 a.m. PST on the first Monday of every month.

○ A schedule that runs at a regular rate, such as every 10 minutes.

Cron expression

Define the cron expression for the schedule

	Minutes	Hours	Day of month	Month	Day of week	Year	
cron (	15	10	?	*	6L	*	)

Next 10 trigger date(s) UTC

```
Fri, 24 Nov 2023 10:15:00 UTC
Fri, 29 Dec 2023 10:15:00 UTC
Fri, 26 Jan 2024 10:15:00 UTC
Fri, 23 Feb 2024 10:15:00 UTC
Fri, 29 Mar 2024 10:15:00 UTC
Fri, 26 Apr 2024 10:15:00 UTC
Fri, 31 May 2024 10:15:00 UTC
Fri, 28 Jun 2024 10:15:00 UTC
Fri, 26 Jul 2024 10:15:00 UTC
Fri, 30 Aug 2024 10:15:00 UTC
```