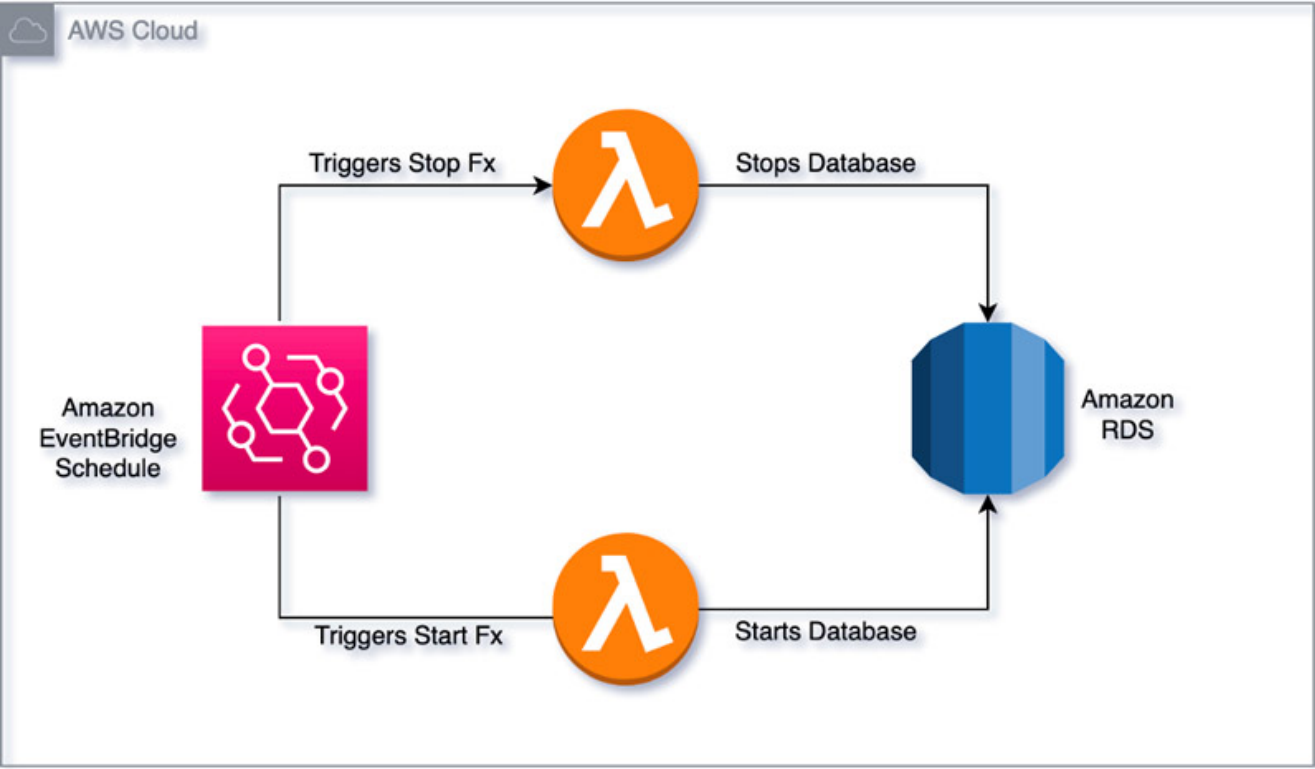


[AWS] Lambda + EventBridge RDS

RDS DB , , I/O ,
IOPS .

Amazon

EventBridge AWS Lambda
RDS /



:

- 1.
2. IAM
3. Lambda
4. EventBridge

5.

1.

AWS

(opt-in)

가

DB

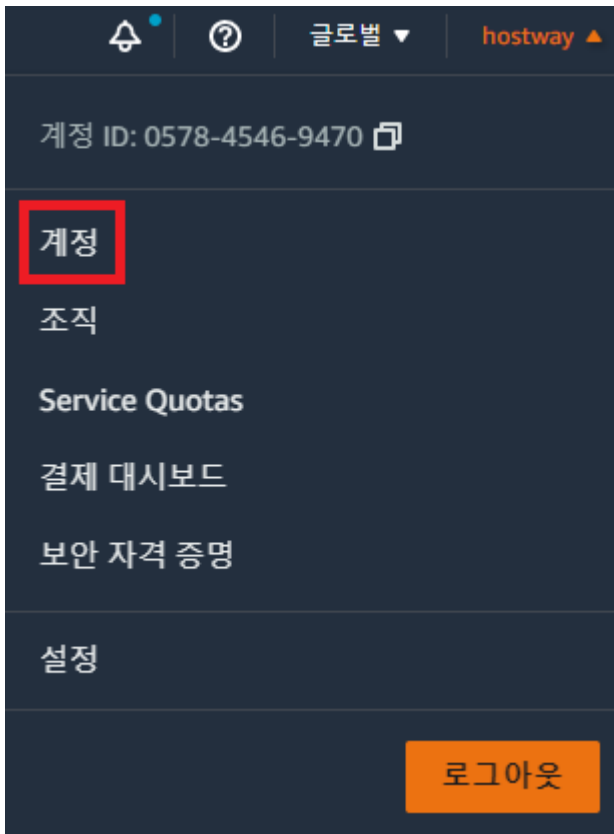
opt-in region

- ()
- ()
- ()
- ()
- ()

1.

5

– - AWS



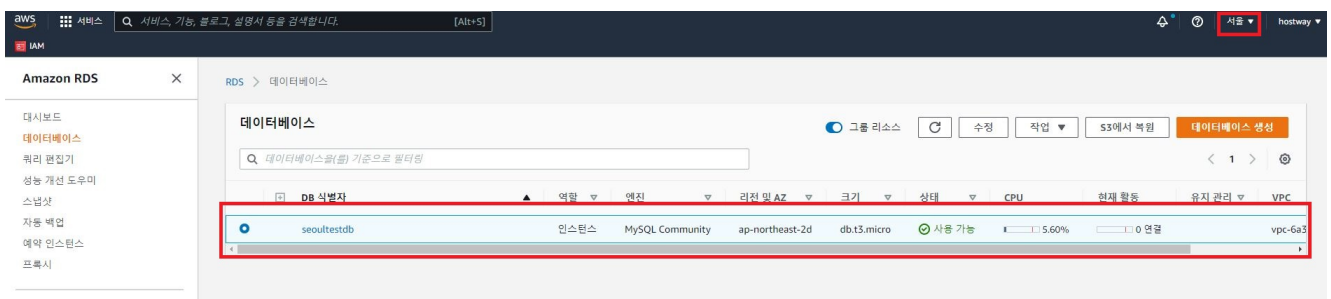
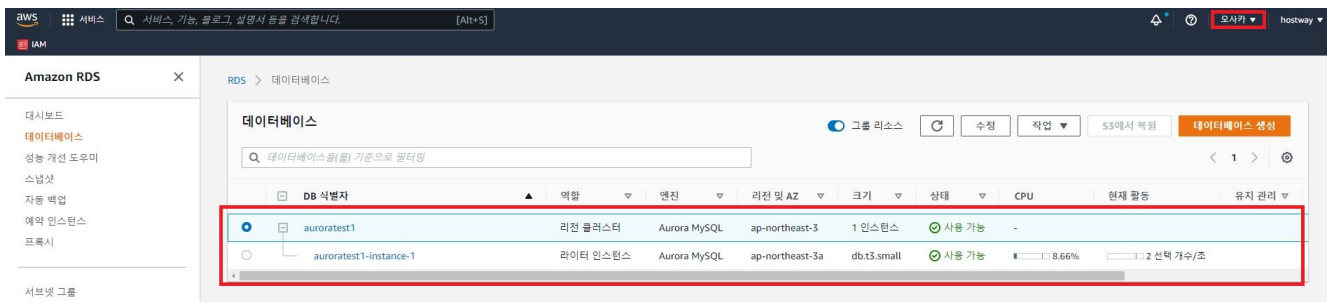
리전	상태	작업
중동 (바레인)	비활성화됨	활성화
아시아 태평양 (자카르타)	비활성화됨	활성화
아프리카 (케이프타운)	비활성화됨	활성화
아시아 태평양 (홍콩)	비활성화됨	활성화
유럽 (밀라노)	비활성화됨	활성화

2. DB 3

: MariaDB

: AWS Aurora

: Mysql



2. IAM

1. RDS Stop/Start

. IAM

—

Identity and Access Management(IAM)

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

정책

자력 증명 공급자

계정 설정

▼ 보고서 액세스

액세스 분석기

아카이브 규칙

분석기

설정

자력 증명 보고서

조직 활동

SCP(서비스 제어 정책)

관련 콘솔

IAM Identity Center

신규

IAM > 정책

정책 (1005) 정보

정책은 권한을 정의하는 AWS의 객체입니다.

Q 속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

1 2 3 4 5 6 7 ... 51

정책 이름	유형	다음과 같이 사용	설명
AmazonEC2FullAccess	AWS 관리형	권한 정책 (2)	Provides full access
SecretsManagerReadWrite	AWS 관리형	없음	Provides read/write
AWSIoTThingsRegistration	AWS 관리형	없음	This policy allows us
AmazonDocDBReadOnlyAccess	AWS 관리형	없음	Provides read-only ε
AmazonMQApiFullAccess	AWS 관리형	없음	Provides full access
AWSElementalMediaStoreReadOnly	AWS 관리형	없음	Provides read-only ε
AWSCertificateManagerReadOnly	AWS 관리형	없음	Provides read only ε
AWSQuicksightAthenaAccess	AWS 관리형	없음	Quicksight access k
AWSCloudMapRegisterInstanceAccess	AWS 관리형	없음	Provides registrant I
AWSMarketplaceImageBuildFullAccess	AWS 관리형	없음	Provides full access
AWSCodeCommitPowerUser	AWS 관리형	없음	Provides full access
AWSCodeCommitFullAccess	AWS 관리형	권한 정책 (2)	Provides full access
IAMSelfManageServiceSpecificCredentials	AWS 관리형	없음	Allows an IAM user

2. JSON IAM .

정책 생성

1 2 3

정책은 사용자, 그룹, 또는 역할에 할당할 수 있는 AWS 권한을 정의합니다. 시각적 편집기에서 JSON을 사용하여 정책을 생성하고 편집할 수 있습니다. 자세히 알아보기

시각적 편집기

JSON

관리형 정책 가져오기

1 {

2 "Version": "2012-10-17",

3 "Statement": [

4 {

5 "Sid": "VisualEditor0",

6 "Effect": "Allow",

7 "Action": [

8 "rds:StartDBCluster",

9 "rds:StopDBCluster",

10 "rds:ListTagsForResource",

11 "rds:DescribeDBInstances",

12 "rds:StopDBInstance",

13 "rds:DescribeDBClusters",

14 "rds:StartDBInstance"

15],

16 "Resource": "*"

17 },

18]

19 }

20 }

21 }

보안: 0 오류: 0 경고: 0 추천: 0

문자 수: 6,144자 중 266자

취소 다음: 태그

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
```

```

    "Effect": "Allow",
    "Action": [
        "rds:StartDBCluster",
        "rds:StopDBCluster",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:StopDBInstance",
        "rds:DescribeDBClusters",
        "rds:StartDBInstance"
    ],
    "Resource": "*"
}
]
}

```

3. RDS-Stop-Start-Policy

정책 생성

1 2 3

정책 검토

이름*

영숫자 및 '+,=,@,~' 문자를 사용합니다. 최대 128자입니다.

설명

최대 1000자입니다. 영숫자 및 '+,=,@,~' 문자를 사용합니다.

요약

Q 필터:

서비스 ▼	액세스 레벨	리소스	요청 조건
허용 (1 / 331 서비스) 나머지 330 표시			
RDS	제한: 목록, 읽기, 쓰기	모든 리소스	없음

태그

키 ▲ 값 ▼

리소스와 연결된 태그가 없습니다.

* 필수

취소

이전

정책 생성

4. RDS Stop/Start

. IAM

—

Identity and Access Management(IAM)

대시보드

▼ 액세스 관리

사용자 그룹

사용자

역할

1

정책

자격 증명 공급자

계정 설정

▼ 보고서 액세스

역세스 분석기

아카이브 규칙

분석기

설정

자격 증명 보고서

조직 활동

SCP(서비스 제어 정책)

권한 콘솔

IAM Identity Center

신규

IAM > 역할

2

역할 (79) 정보

IAM 역할은 단기간 동안 유효한 자격 증명을 가진 특정 권한이 있는 자격 증명입니다. 신뢰할 수 있는 개체가 역할을 맡을 수 있습니다.

검색

1 2 3 4

☐	역할 이름	신뢰할 수 있는 개체	마지막 활동
☐	AWSServiceRoleForApplicationMigrationService	AWS 서비스: mgn (서비스 연결 역할)	23분 전
☐	AWSServiceRoleForAutoScaling	AWS 서비스: autoscaling (서비스 연결 역할)	7일 전
☐	AWSServiceRoleForAWSLicenseManagerRole	AWS 서비스: license-manager (서비스 연결 역할)	142일 전
☐	AWSServiceRoleForBackup	AWS 서비스: backup (서비스 연결 역할)	18시간 전
☐	AWSServiceRoleForClientVPN	AWS 서비스: clientvpn (서비스 연결 역할)	81일 전
☐	AWSServiceRoleForClientVPNConnections	AWS 서비스: clientvpn-connections (서비스 연결 역할)	-
☐	AWSServiceRoleForCloudFrontLogger	AWS 서비스: logger.cloudfront (서비스 연결 역할)	90일 전
☐	AWSServiceRoleForCloudWatchCrossAccount	AWS 서비스: cloudwatch-crossaccount (서비스 연결 역할)	136일 전
☐	AWSServiceRoleForCloudWatchEvents	AWS 서비스: events (서비스 연결 역할)	-
☐	AWSServiceRoleForCodeStarNotifications	AWS 서비스: codestar-notifications (서비스 연결 역할)	209일 전
☐	AWSServiceRoleForConfig	AWS 서비스: config (서비스 연결 역할)	209일 전
☐	AWSServiceRoleForElasticCache	AWS 서비스: elasticsearch (서비스 연결 역할)	91일 전
☐	AWSServiceRoleForElasticLoadBalancing	AWS 서비스: elasticloadbalancing (서비스 연결 역할)	5일 전
☐	AWSServiceRoleForGlobalAccelerator	AWS 서비스: globalaccelerator (서비스 연결 역할)	-

5. AWS Lambda

IAM > 역할 > 역할 생성

1단계

신뢰할 수 있는 엔터티 선택

2단계

권한 추가

3단계

이름 지정, 검토 및 생성

신뢰할 수 있는 엔터티 선택

신뢰할 수 있는 엔터티 유형

☒ AWS 서비스

EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

☐ AWS 계정

사용자 또는 서드 파티에 속한 다른 AWS 계정의 엔터티가 이 계정에서 작업을 수행하도록 허용합니다.

☐ 웹 자격 증명

지정된 외부 웹 자격 증명 공급자와 연동된 사용자가 이 역할을 맡아 이 계정에서 작업을 수행하도록 허용합니다.

☐ SAML 2.0 연동

기밀 디렉터리에서 SAML 2.0과 연동된 사용자가 이 계정에서 작업을 수행할 수 있도록 허용합니다.

☐ 사용자 지정 신뢰 정책

다른 사용자가 이 계정에서 작업을 수행할 수 있도록 사용자 지정 신뢰 정책을 생성합니다.

사용 사례

EC2, Lambda 등의 AWS 서비스가 이 계정에서 작업을 수행하도록 허용합니다.

일반 사용 사례

☐ EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

다른 AWS 서비스의 사용 사례:

사용 사례를 조회할 서비스 선택

취소

다음

6. RDS-Stop-Start-Policy

IAM > 역할 > 역할 생성

1단계

신뢰할 수 있는 엔터티 선택

2단계

권한 추가

3단계

이름 지정, 검토 및 생성

권한 추가

권한 정책 (선택된 1/804)

새 역할에 연결할 정책을 하나 이상 선택합니다.

검색

1 개 일치

"RDS-STOP-START"

필터 지우기

☒	정책 이름	유형	설명
☒	RDS-Stop-Start-Policy	고객 관...	

▶ 권한 환경 설정 - 선택 사항

권한 환경을 설정하여 이 역할이 가질 수 있는 최대 권한을 제어합니다. 이는 일반적인 설정은 아니지만 권한 관리를 다른 사용자에게 위임하는 데 사용할 수 있습니다.

취소

이전

다음

7. RDS-Stop-Start-Role

IAM > 역할 > 역할 생성

1단계
신뢰할 수 있는 엔티티 선택

2단계
권한 추가

3단계
이름 지정, 검토 및 생성

이름 지정, 검토 및 생성

역할 세부 정보

역할 이름

이 역할을 신뢰하는 엔티티 이름은 입력합니다.

RDS-Stop-Start-Role

최대 64자입니다. 영숫자 및 '*=@_-' 문자를 사용하세요.

설명

이 역할에 대하여 간단한 설명을 추가합니다.

Allows Lambda functions to call AWS services on your behalf.

최대 1,000자입니다. 영숫자 및 '*=@_-' 문자를 사용하세요.

3. Lambda

AWS Lambda

RDS DB

Stop

Region

Region

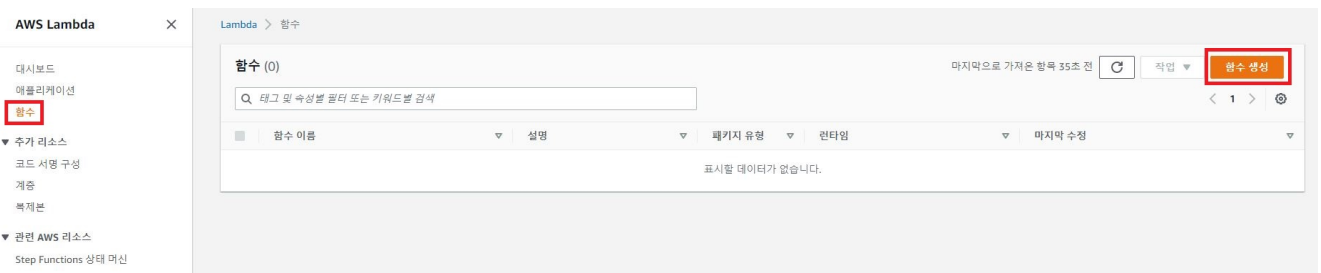
1. RDS

Stop

Lambda

. Lambda

—



2.

: StopRDS

: Python 3.9

:

—

—

RDS-Stop-Start-Role

함수 이름
 함수의 용도를 설명하는 이름을 입력합니다.

공백 없이 문자, 숫자, 하이픈 또는 밑줄만 사용합니다.

런타임 정보
 함수를 작성하는 데 사용할 언어를 선택합니다. 콘솔 코드 편집기는 Node.js, Python 및 Ruby만 지원합니다.

아키텍처 정보
 함수 코드에 대해 원하는 명령 세트 아키텍처를 선택합니다.
☒ x86_64
☐ arm64

권한 정보
 기본적으로 Lambda는 Amazon CloudWatch Logs에 로그를 업로드하는 권한을 가진 실행 역할을 생성합니다. 이 기본 역할은 나중에 트리거를 추가할 때 사용자 지정할 수 있습니다.

▼ 기본 실행 역할 변경

실행 역할
 함수에 대한 권한을 정의하는 역할을 선택합니다. 사용자 지정 역할을 생성하려면 IAM 콘솔로 이동합니다.

☐ 기본 Lambda 권한을 가진 새 역할 생성
☒ 기존 역할 사용
☐ AWS 정책 템플릿에서 새 역할 생성

기존 역할
 생성한 기존 역할 중에 이 Lambda 함수와 함께 사용할 역할을 선택합니다. 이 역할에는 Amazon CloudWatch Logs에 로그를 업로드할 수 있는 권한이 있어야 합니다.

IAM 콘솔에서 RDS-Stop-Start-Role 역할을 확인합니다.

▶ 고급 설정

취소

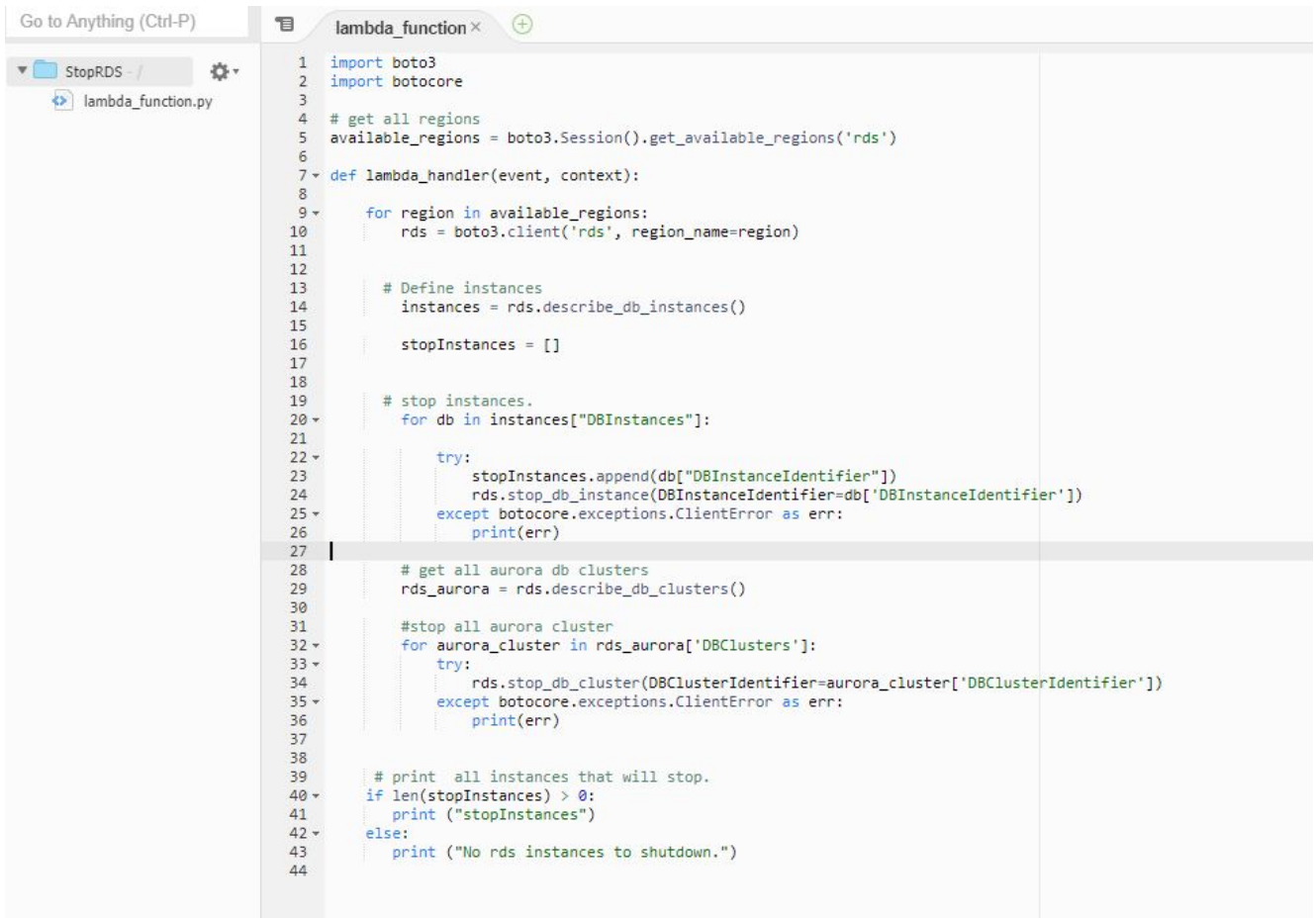
3. Boto3, Botocore

Python

Boto : AWS Python
(SDK) 가

Boto3

□ Botocore : AWS low-level
API 가 .



```
1 import boto3
2 import botocore
3
4 # get all regions
5 available_regions = boto3.Session().get_available_regions('rds')
6
7 def lambda_handler(event, context):
8
9     for region in available_regions:
10         rds = boto3.client('rds', region_name=region)
11
12         # Define instances
13         instances = rds.describe_db_instances()
14
15         stopInstances = []
16
17         # stop instances.
18         for db in instances["DBInstances"]:
19             try:
20                 stopInstances.append(db["DBInstanceIdentifier"])
21                 rds.stop_db_instance(DBInstanceIdentifier=db["DBInstanceIdentifier"])
22             except botocore.exceptions.ClientError as err:
23                 print(err)
24
25     # get all aurora db clusters
26     rds_aurora = rds.describe_db_clusters()
27
28     #stop all aurora cluster
29     for aurora_cluster in rds_aurora["DBClusters"]:
30         try:
31             rds.stop_db_cluster(DBClusterIdentifier=aurora_cluster["DBClusterIdentifier"])
32         except botocore.exceptions.ClientError as err:
33             print(err)
34
35     # print all instances that will stop.
36     if len(stopInstances) > 0:
37         print ("stopInstances")
38     else:
39         print ("No rds instances to shutdown.")
40
41
42
43
44
```

```
# StopRDS
[
import boto3
import botocore
[
# get all regions
available_regions                                     =
boto3.Session().get_available_regions('rds')
[
def lambda_handler(event, context):
[
    for region in available_regions:
        rds = boto3.client('rds', region_name=region)
[
[
        # Define instances
        instances = rds.describe_db_instances()
[
        stopInstances = []
[
[
[
```

```

        # stop instances.
        for db in instances["DBInstances"]:
            try:

                stopInstances.append(db["DBInstanceIdentifier"])

                rds.stop_db_instance(DBInstanceIdentifier=db['DBInstanceIdentifier'])
            except botocore.exceptions.ClientError as err:
                print(err)

            # get all aurora db clusters
            rds_aurora = rds.describe_db_clusters()

            # stop all aurora cluster
            for aurora_cluster in rds_aurora['DBClusters']:
                try:

                    rds.stop_db_cluster(DBClusterIdentifier=aurora_cluster['DBClusterIdentifier'])
                except botocore.exceptions.ClientError as err:
                    print(err)

            # print all instances that will stop.
            if len(stopInstances) > 0:
                print ("stopInstances")
            else:
                print ("No rds instances to shutdown.")

```

stop_db_instance API Aurora

Aurora DB

stop_db_cluster API

.

StartRDS

.

StartRDS

```

import boto3
import botocore

```

```

# get all regions
available_regions
boto3.Session().get_available_regions('rds')
=
[]
def lambda_handler(event, context):
[]
    for region in available_regions:
        rds = boto3.client('rds', region_name=region)
[]
[]
        # Define instances
        instances = rds.describe_db_instances()
[]
        startInstances = []
[]
[]
        # start instances.
        for db in instances["DBInstances"]:
[]
            try:

startInstances.append(db["DBInstanceIdentifier"])

        rds.start_db_instance(DBInstanceIdentifier=db['DBInstanceIdentifier'])
            except botocore.exceptions.ClientError as err:
                print(err)
[]
        # get all aurora db clusters
        rds_aurora = rds.describe_db_clusters()
[]
        # stop all aurora cluster
        for aurora_cluster in rds_aurora['DBClusters']:
            try:

rds.start_db_cluster(DBClusterIdentifier=aurora_cluster['DBClusterIdentifier'])
            except botocore.exceptions.ClientError as err:
                print(err)
[]
[]

```

```
# print all instances that will stop.
if len(startInstances) > 0:
    print ("startInstances")
else:
    print ("No rds instances to start.")
```

4. EventBridge

1. Amazon EventBridge



2. RDS_Instances_Stop

Amazon EventBridge > 규칙 > 규칙 생성

1단계
규칙 세부 정보 정의

2단계
일정 정의

3단계
대상 선택

4단계 - 선택 사항
태그 구성

5단계
검토 및 생성

규칙 세부 정보 정의 정보

규칙 세부 정보

이름

숫자, 대/소문자, 마침표(.), 대시(-), 밑줄(_)를 사용하여 최대 64자로 지정합니다.

설명 - 선택 사항

이벤트 버스 정보
 이 규칙이 적용되는 이벤트 버스(기본 이벤트 버스 또는 사용자 지정 또는 파트너 이벤트 버스)를 선택합니다.

☒ 선택한 이벤트 버스에 대해 규칙 활성화

규칙 유형 정보

☐ 이벤트 패턴이 있는 규칙
 이벤트가 정의된 이벤트 패턴과 일치할 때 실행되는 규칙입니다. EventBridge는 지정된 대상으로 이벤트를 전송합니다.

☒ 일정
 일정에 따라 실행되는 규칙입니다.

취소

3. Cron . 0 9 * * ? *

6 Lambda .

cron .

https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/services-cloudwatchevents-expressions.html

1단계

규칙 세부 정보 정의

2단계

일정 정의

3단계

대상 선택

4단계 - 선택 사항

태그 구성

5단계

검토 및 생성

일정 정의 정보

일정 패턴

일정 패턴

요구 사항에 가장 잘 맞는 일정 유형을 선택합니다.

● 매월 첫 번째 월요일 오전 8시(PST)와 같이 특정 시간에 실행되는 세분화된 일정입니다.

○ 10분마다와 같이 일정한 빈도로 실행되는 일정입니다.

Cron 식 정보

일정에 대한 cron 표현식 정의

 cron ()

대 시간 분 일 월요일 연도

140

시간

10

not

요일

연도

다음 10개 트리거 날짜

현지 시간대

2022년 8월 8일 오후 06:00 GMT+9

2022년 8월 9일 오후 06:00 GMT+9

2022년 8월 10일 오후 06:00 GMT+9

2022년 8월 11일 오후 06:00 GMT+9

2022년 8월 12일 오후 06:00 GMT+9

2022년 8월 13일 오후 06:00 GMT+9

2022년 8월 14일 오후 06:00 GMT+9

2022년 8월 15일 오후 06:00 GMT+9

2022년 8월 16일 오후 06:00 GMT+9

2022년 8월 17일 오후 06:00 GMT+9

취소

이전

다음

4. AWS

StopRDS

■

5.

Lambda , EventBridge 3 Region DB

1. Amazon Lambda StopRDS , StopTest
hello-world

코드테스트모니터링구성별칭버전

테스트 이벤트

저장테스트

이벤트를 저장하지 않고 함수를 호출하려면 JSON 이벤트를 구성한 다음 테스트를 선택합니다.

이벤트 작업 테스트

새 이벤트 생성

저장된 이벤트 편집

이벤트 이름

StopTest

문자, 숫자, 언더바 및 하이픈을 사용하여 최대 25자로 구성합니다.

이벤트 공유 설정

프라이빗

공유 가능

이 이벤트는 Lambda 콘솔 및 이벤트 생성자만 사용할 수 있습니다. 총 10개를 구성할 수 있습니다. 자세히 알아보기

이 이벤트는 공유 가능한 이벤트에 액세스하고 이를 사용할 수 있는 권한이 있는 동일한 계정 내 IAM 사용자가 사용할 수 있습니다. 자세히 알아보기

템플릿 - 선택 사항

hello-world

이벤트 JSON

JSON 형식 지정

1

{

2

"key1": "value1",

3

"key2": "value2",

4

"key3": "value3"

5

}

2.

코드

테스트

모니터링

구성

별칭

버전

테스트 이벤트

삭제

저장

테스트

이벤트를 저장하지 않고 함수를 호출하려면 이벤트를 수정한 다음 테스트를 선택합니다. Lambda는 수정된 이벤트를 사용하여 함수를 호출하지만 변경 사항 저장을 선택할 때까지 원래 이벤트를 덮어쓰지 않습니다.

이벤트 작업 테스트

○ 새 이벤트 생성

● 저장된 이벤트 편집

이벤트 이름

StopTest

↻

이벤트 JSON

JSON 형식 지정

```

1 {
2   "key1": "value1",
3   "key2": "value2",
4   "key3": "value3"
5 }

```

3. 가

코드

테스트

모니터링

구성

별칭

버전

실행 결과: 성공 (로그)

▶ 세부 정보

테스트 이벤트

삭제

저장

테스트

4. 3 RDS

데이터베이스

그룹 리소스

수정

작업

S3에서 복원

데이터베이스 생성

Q 데이터베이스(들) 기준으로 필터링

< 1 >

DB 식별자	역할	엔진	클래스	상태	CPU	현재 활동	유지 관리	VPC	다중 AZ
maria db hongkong	인스턴스	MariaDB	db.t3.micro	중지 중	-	0 연결		vpc-0ea2134f0c1c6990a	예

데이터베이스

그룹 리소스

↻

수정

작업

S3에서 복원

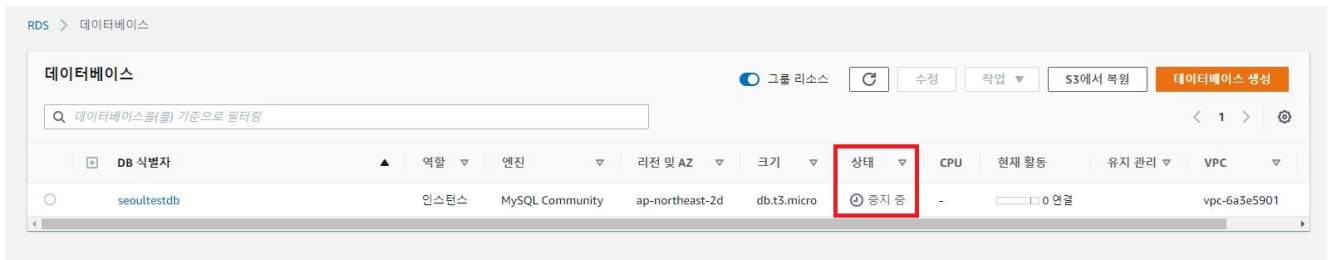
데이터베이스 생성

Q 데이터베이스(들) 기준으로 필터링

< 1 >

⚙

DB 식별자	역할	엔진	리전 및 AZ	크기	상태	CPU	현재 활동	유지 관리	VPC
auroratest1	리전 클러스터	Aurora MySQL	ap-northeast-3	1 인스턴스	중지 중	-	-	-	-
auroratest1-instance-1	라이터 인스턴스	Aurora MySQL	ap-northeast-3a	db.t3.small	중지 중	-	2 선택 개수/초	vpc-0d1fa	-



Mysql , opt-in
Aurora DB Cluster

Mssql
Stop

Stop

AMI
?

AWS

CMK

AMI AWS

가

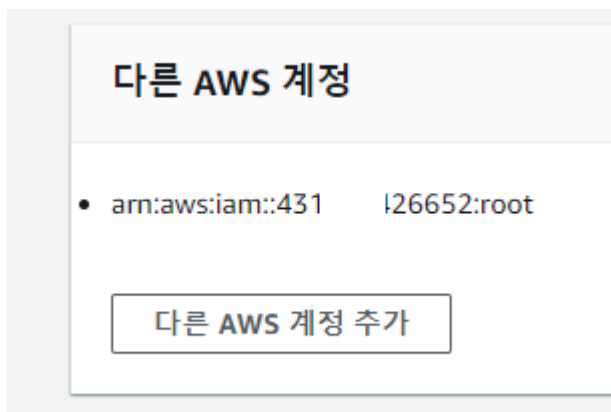
(Terminated)

```
#
# AMI IAM IAM
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyImageAttribute"
      ],
      "Resource": [
        "arn:aws:ec2:us-west-2::image/<0e9fcdb7ae40e8f4c>"
      ]
    }
  ]
}
```

```

##                                     id ( ami-xxxxxxxxxxxxxxxxxxxxx      xxx
    )
    ]
  }
]
}

# KMS                               Key      가
#      AMI      KMS      가      AWS Account
.
```



```

#                               CMK
#                               IAM
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-west-2:891977874274:key/bc52517a-676b-4f1a-9d1a-d50241563abc"
      ]
    }
  ]
}

##      AMI      KMS Key
    ]
  }
]
}
```

EC2 가

.

AWS

Docs

:

<https://aws.amazon.com/ko/blogs/security/how-to-share-encrypted-amis-across-accounts-to-launch-encrypted-ec2-instances/>