



# AWS Secrets Manager & IAM Roles Anywhere UseCase

Dongsoo Shin

Cloud Support Engineer, AWS Premium Support

# Contents

## 1. AWS Secrets Manager를 사용한 보안 암호 관리 방안

- Secrets Manager 소개
- Secrets Manager와 통합되는 서비스
- AWS Secrets Manager를 사용하여 IAM 액세스 키 검색 및 주기적으로 자동 교체하는 방안
- Workflow
- Setup

## 2. IAM Roles Anywhere를 사용하여 AWS 외부에서 실행되는 애플리케이션에서 AWS 리소스 액세스 하는 방안

- Roles Anywhere 소개
- Roles Anywhere 작동 방식
- Roles Anywhere 구성 방식
- Workflow
- Setup



# AWS Secrets Manager를 사용한 보안 암호 관리 방안

# AWS Secrets Manager

보안 암호의 수명 주기를 중앙에서 관리



DB Credential, API Key, Token 등 보안 암호 저장



보안 암호 검색



보안 암호 교체



KMS Key로 생성된 데이터 키로 보안 암호를 암호화하여 저장



캐시 클라이언트를 사용하여 일정 시간 동안 추가 API CALL 없이 캐싱 지원

- Database Password
- Application Credential
- 3rd party API keys
- Authentication token
- **Long-term credentials (access keys)**
- SSH keys
- TLS keys

# Secrets Manager 통합

- Alexa for Business
- AWS App2Container
- Amazon AppFlow
- AWS AppSync
- Amazon Athena
- AWS CodeBuild
- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- AWS Elemental MediaLive
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- Amazon CodeGuru Reviewer
- AWS Elemental MediaPackage

- AWS Elemental MediaTailor
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- AWS Glue DataBrew
- AWS Glue Studio
- AWS IoT SiteWise
- Amazon Kendra
- AWS Launch Wizard
- Amazon Lookout for Metrics
- Amazon Managed Streaming for
- Apache Kafka(Amazon MSK)
- Amazon Managed Workflows for
- Apache Airflow(Amazon MWAA)

- AWS Migration Hub
- AWS OpsWorks for Chef Automate
- Amazon Relational Database Service(Amazon RDS)
- Amazon Redshift
- Amazon Redshift Query Editor V2
- Amazon SageMaker
- AWS Toolkit for JetBrains
- AWS Transfer Family
- Other type of secret

## AWS Secrets Manager를 사용하여 IAM 액세스 키 검색 및 주기적으로 자동 교체하는 방안

```
import boto3
```

```
aws_access_key_id = 'AKIAXXXXXXXXXXXXXXXXXXXXY'  
aws_secret_access_key =  
'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
```

```
session = boto3.Session(
    aws_access_key_id=aws_access_key_id,
    aws_secret_access_key=aws_secret_access_key
)
```

```
if __name__ == '__main__':
```

```
s3 = session.client('s3')
response = s3.list_buckets()
```

출처: <https://www.dailysecu.com/news/articleView.html?idxno=138253>

# AWS Secrets Manager를 사용하여 IAM 액세스 키 검색 및 주기적으로 자동 교체하는 방안

```
import boto3

aws_access_key_id = 'AKIAXXXXXXXXXXXXXX'
aws_secret_access_key = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'

session = boto3.Session(
    aws_access_key_id=aws_access_key_id,
    aws_secret_access_key=aws_secret_access_key
)

if __name__ == '__main__':
    s3 = session.client('s3')
    response = s3.list_buckets()
```



Secrets Manager

```
import boto3, json

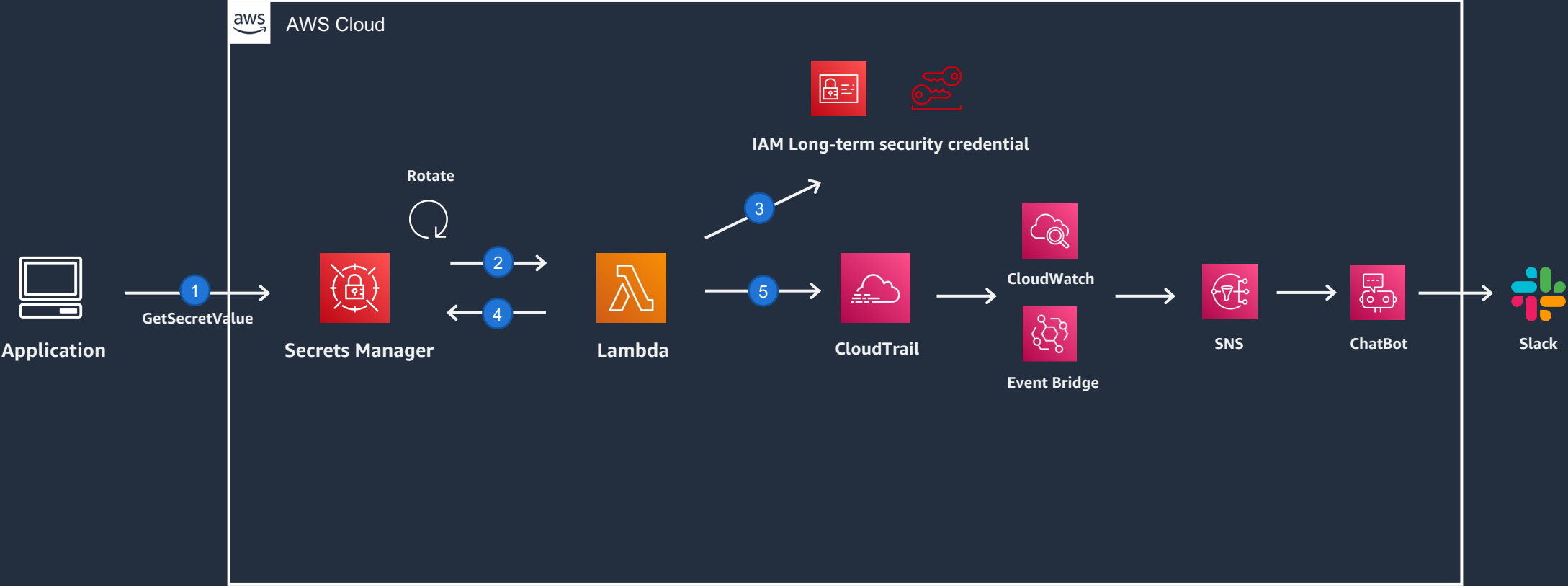
client = boto3.client('secretsmanager', region_name='ap-
northeast-2')
response = client.get_secret_value(
    SecretId = 'Your Secret ID'
)

secretDict = json.loads(response['SecretString'])

session = boto3.Session(
    aws_access_key_id=secretDict['aws_access_key_id'],
    aws_secret_access_key=secretDict['aws_secret_access_key']
)

if __name__ == '__main__':
    s3 = session.client('s3')
    response = s3.list_buckets()
```

# Workflow





# Set up

## Step 1. 액세스 키 확인

```
$ aws iam list-access-keys --user-name "Your User Name"
```

```
{
  "AccessKeyMetadata": [
    {
      "UserName": "Alice",
      "AccessKeyId": "AKIA[REDACTED]UD",
      "Status": "Active",
      "CreateDate": "2023-08-13T07:40:49+00:00"
    },
    {
      "UserName": "Alice",
      "AccessKeyId": "AKIA[REDACTED]5K",
      "Status": "Active",
      "CreateDate": "2023-08-14T09:04:16+00:00"
    }
  ]
}
```

자신의 IAM 사용자에게 대한 액세스 키를 교체하려면 다음 정책에 따른 권한이 있어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "ManageOwnAccessKeys",
    "Effect": "Allow",
    "Action": [
      "iam:CreateAccessKey",
      "iam:DeleteAccessKey",
      "iam:GetAccessKeyLastUsed",
      "iam:GetUser",
      "iam:ListAccessKeys",
      "iam:UpdateAccessKey",
      "iam:TagUser"
    ],
    "Resource": "arn:aws:iam::*:user/${aws:username}"
  }]
}
```



## Step 2. 다른 유형의 보안 암호 생성

다른 유형의 보안 암호 옵션을 사용하면 모든 유형의 서비스에 대한 자격 증명 또는 기타 정보를 저장할 수 있는 보안 암호를 생성 할 수 있습니다.

Secret details

Encryption key  
aws/secretsmanager

Secret name  
test/alice/accesskey

Secret ARN  
arn:aws:secretsmanager:ap-northeast-2:secret

Tags

Secret value

Retrieve and view the secret value.

Key/value

Plaintext

Secret key	Secret value
accesskey	AKIA[REDACTED]5K
secretkey	[REDACTED]
username	Alice
masterarn	arn:aws:secretsmanager:ap-northeast-2:secret:

```
1 import boto3, json
2
3 client = boto3.client('secretsmanager', region_name='ap-northeast-2')
4 response = client.get_secret_value(
5     SecretId = 'test/alice/accesskey'
6 )
7
8 secretDict = json.loads(response['SecretString'])
9 print(secretDict)
10 session = boto3.Session(
11     aws_access_key_id=secretDict['accesskey'],
12     aws_secret_access_key=secretDict['secretkey']
13 )
14
15 if __name__ == '__main__':
16     s3 = session.client('s3')
17     response = s3.list_buckets()
18
19
20 문제 출력 디버그 콘솔 터미널 CODEWHISPERER REFERENCE LOG 주석
```

```
{'accesskey': 'AKIA[REDACTED]5K', 'secretkey': [REDACTED], 'username': 'Alice',
```

### Step 3. 보안 암호 교체를 위한 Lambda 함수 생성

- 1) Secrets Manager는 모든 유형의 암호에 대한 교체 기능을 생성할 수 있는 시작점으로 템플릿을 제공합니다. 액세스 키 교체에 대한 Lambda 예제 코드는 [다음 기사](#)를 참고하실 수 있습니다.
- 2) Lambda 함수가 보안 암호를 교체하기 위해 실행 역할에 아래와 같은 권한 정책이 필요합니다.
- 3) Lambda 리소스 기반 정책을 사용하여 AWS Secrets Manager가 함수를 호출하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource": "Your Secret ARN"
    },
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource": "*"
    }
  ]
}
```

Resource-based policy statements (1) <a href="#">Info</a>					<a href="#">View policy</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Add permissions</a>
<input type="text" value="Find policy statements"/>					< 1 >			
Statement ID	Principal	PrincipalOrgID	Conditions	Action				
<a href="#">accesskey_rotation</a>	secretsmanager.amazonaws.com	-	None	lambda:InvokeFunction				

Step 4. 보안 암호 교체 구성 및 확인

자동 교체를 켜면 cron() 또는 rate() 표현식을 사용하여 보안 암호 교체 일정을 설정할 수 있습니다.

Rotation configuration Info

Rotate secret immediately

Edit rotation

보안암호 즉시 교체

Rotation status  
Enabled

Rotation schedule  
cron(0 0 ? 1/3 2#1 \*) → 3개월마다 첫 번째 일요일 오전 1시

Next rotation date (UTC)  
The next rotation is scheduled to occur on or before this date.  
Mon, October 2, 2023 at 23:59:59 UTC

Lambda rotation function  
The Lambda function that has permissions to rotate this secret.  
alice\_accesskey

Secret details

Encryption key  
aws/secretsmanager

Secret name  
test/alice/accesskey

Secret ARN  
arn:aws:secretsmanager:ap-northeast-2:secret:

Tags

Secret value Info  
Retrieve and view the secret value.

Key/value | Plaintext

Secret key	Secret value
accesskey	AKIA-FO
secretkey	
username	Alice
masterarn	arn:aws:secretsmanager:ap-northeast-2:secret:

```
1 import boto3, json
2
3 client = boto3.client('secretsmanager', region_name='ap-northeast-2')
4 response = client.get_secret_value(
5     SecretId = 'test/alice/accesskey'
6 )
7
8 secretDict = json.loads(response['SecretString'])
9 print(secretDict)
10 session = boto3.Session(
11     aws_access_key_id=secretDict['accesskey'],
12     aws_secret_access_key=secretDict['secretkey']
13 )
14
15 if __name__ == '__main__':
16     s3 = session.client('s3')
17     response = s3.list_buckets()
```


문제 출력 디버그 콘솔 터미널 CODEWHISPERER REFERENCE LOG 주석


```
{'accesskey': 'AKIA-FO', 'secretkey': '...', 'username': 'Alice',
```




## Step 5. 액세스 키 및 알림 확인

```
{
  "AccessKeyMetadata": [
    {
      "UserName": "Alice",
      "AccessKeyId": "AKIA[REDACTED]5K",
      "Status": "Active",
      "CreateDate": "2023-08-14T09:04:16+00:00"
    },
    {
      "UserName": "Alice",
      "AccessKeyId": "AKIA[REDACTED]F0",
      "Status": "Active",
      "CreateDate": "2023-08-14T17:55:05+00:00"
    }
  ]
}
```

aws  오전 2:55

 AWS Service Event via CloudTrail | ap-northeast-2 | Account: [REDACTED]

AWS Service Event via CloudTrail

 AWS API Call via CloudTrail | ap-northeast-2 | Account: [REDACTED]

The API 'aws.secretsmanager:PutSecretValue' was invoked in ap-northeast-2 by user 'arn:aws:sts::[REDACTED]:assumed-role/ali...

<b>User identity</b>	<b>User agent</b>
arn:aws:sts::[REDACTED]:assumed-role/[REDACTED] [REDACTED]alice_accesskey	Boto3/1.26.90 Python/3.8.16 Linux/4.14.255-311- 248.529.amzn2.x86_64 exec- env/AWS_Lambda_python3.8 Botocore/1.29.90
<b>API</b>	<b>Event ID</b>
PutSecretValue	[REDACTED] [REDACTED]
<b>Event time</b>	
Mon, 14 Aug 2023 17:55:05 GMT	

**IAM Roles Anywhere를 사용하여 AWS 외부에서 실행되는  
애플리케이션에서 AWS 리소스 액세스 하는 방안**

# IAM Roles Anywhere

AWS 외부 워크로드에서 AWS 리소스에 액세스 할 수 있도록 허용



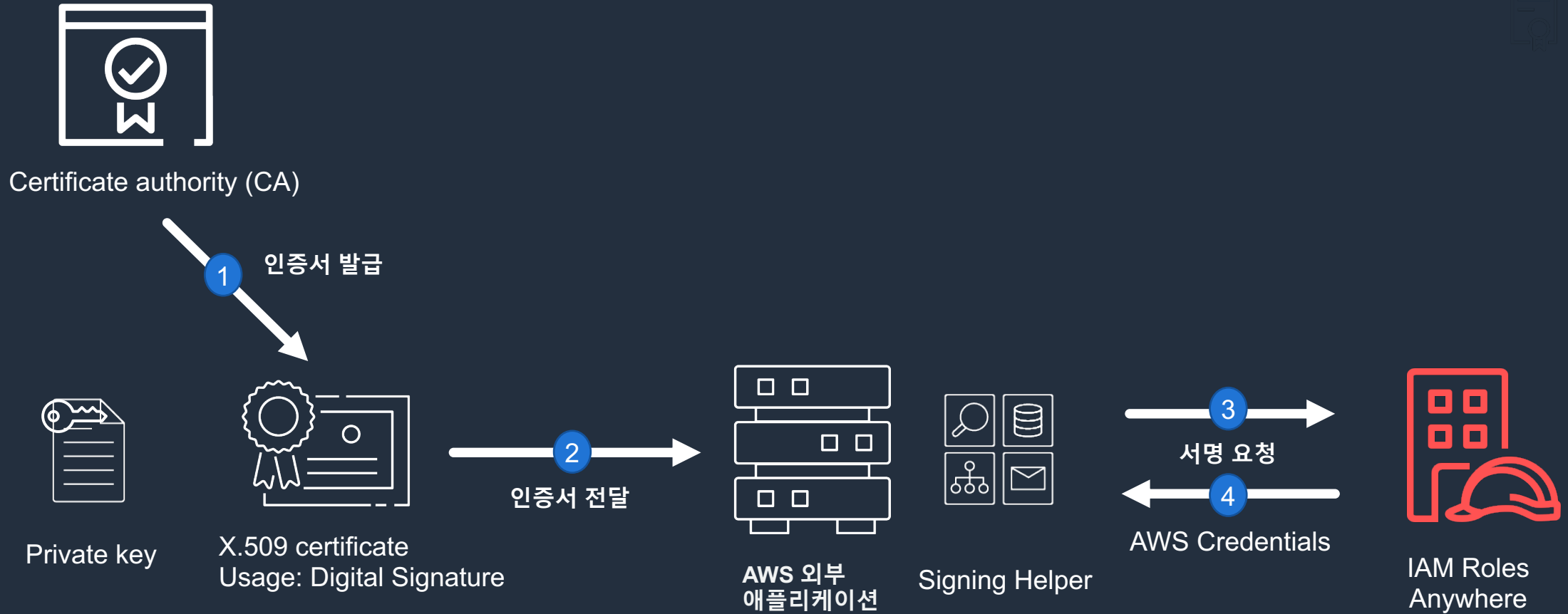
공개 키 인프라(PKI) 기반의 Private CA에서 발급한 X.509 인증서를 사용하여 AWS 외부 애플리케이션에 임시 자격증명 발급



기존과 동일한 IAM Role & Policy를 생성하여 AWS 리소스 액세스 권한제어



# IAM Roles Anywhere 작동 방식





# IAM Roles Anywhere 구성 방식

## Step 1. Trust anchors 생성



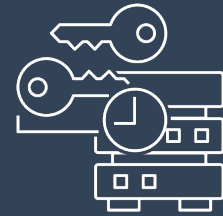
Private CA 업로드  
및 신뢰관계 구축

## Step 2. Profiles 생성



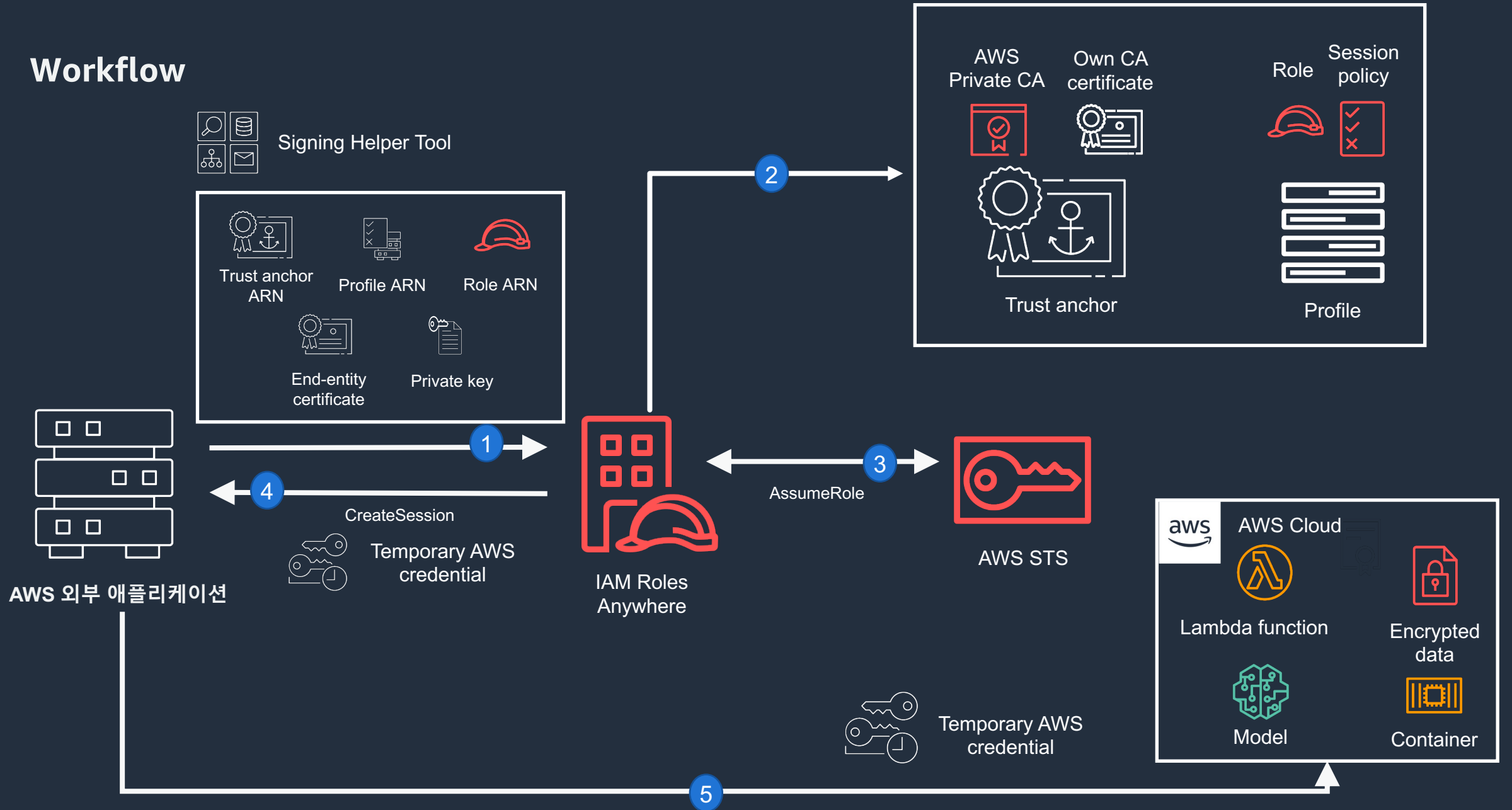
IAM Role & Policy 생성

## Step 3. Signing 요청



임시 자격 증명 요청

# Workflow



# Set up

## Step 1. Private CA 생성

AWS Private CA를 사용하면 조직에서 내부적으로 사용 할 루트 CA 또는 하위 CA를 생성하여 조직의 요구 사항과 일치하는 신뢰 관계의 감사 가능한 계층 구조를 만들 수 있습니다.

AWS Private Certificate Authority

Private certificate authorities

AWS Certificate Manager

AWS Signer

AWS Private Certificate Authority > Private certificate authorities >

Info

Actions

General

Status

Active

CA type

Root

Mode

General-purpose

ARN

arn:aws:acm-pca:ap-northeast-2::certificate-authority/

Created at

2023-03-27T08:34:31Z

Key algorithm

RSA 2048

Expiration date

2033-05-09T05:49:35Z

Signing algorithm

SHA256 RSA

Owner

Key storage security standard

FIPS 140-2 level 3 or higher

Subject

CA certificate

Revocation configuration

Permissions

Tags

Resource shares

Subject

Subject

O=dongsoo Inc, OU=Red Team

Common name (CN)

-

Organization (O)

dongsoo Inc

Country name (C)

-

State or province name

-

Organization unit (OU)

Red Team

Locality name

-

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

19

Step 2. X.509 인증서 요청

AWS PCA에서 생성한 CA에 액세스 할 수 있는 경우 ACM에서 최종 Entity X.509 인증서를 요청할 수 있습니다. 또한 해당 인증서를 추출하여 외부 애플리케이션에 인증서 및 키 파일을 저장할 수 있습니다.

AWS Certificate Manager (ACM)

List certificates

Request certificate

Import certificate

AWS Private CA

AWS Certificate Manager > Certificates >

ExportDelete

Certificate status

Identifier

Status

ARN

Type

arn:aws:acm:ap-northeast-2::certificate,

Issued

Private

Domains (1)

Domain

Status

dongsooanywhere.com

Success

Details

In use

No

Serial number

1

Requested at

May 09, 2023, 14:51:21 (UTC+09:00)

Renewal eligibility

Eligible

Domain name

dongsooanywhere.com

Public key info

RSA 2048

Issued at

May 09, 2023, 14:51:34 (UTC+09:00)

{{ctrl.translations\_CA}}

arn:aws:acm-pca:ap-northeast-2::certificate-authority,

Number of additional names

0

Signature algorithm

SHA-256 with RSA

Not before

May 09, 2023, 13:51:24 (UTC+09:00)

Can be used with

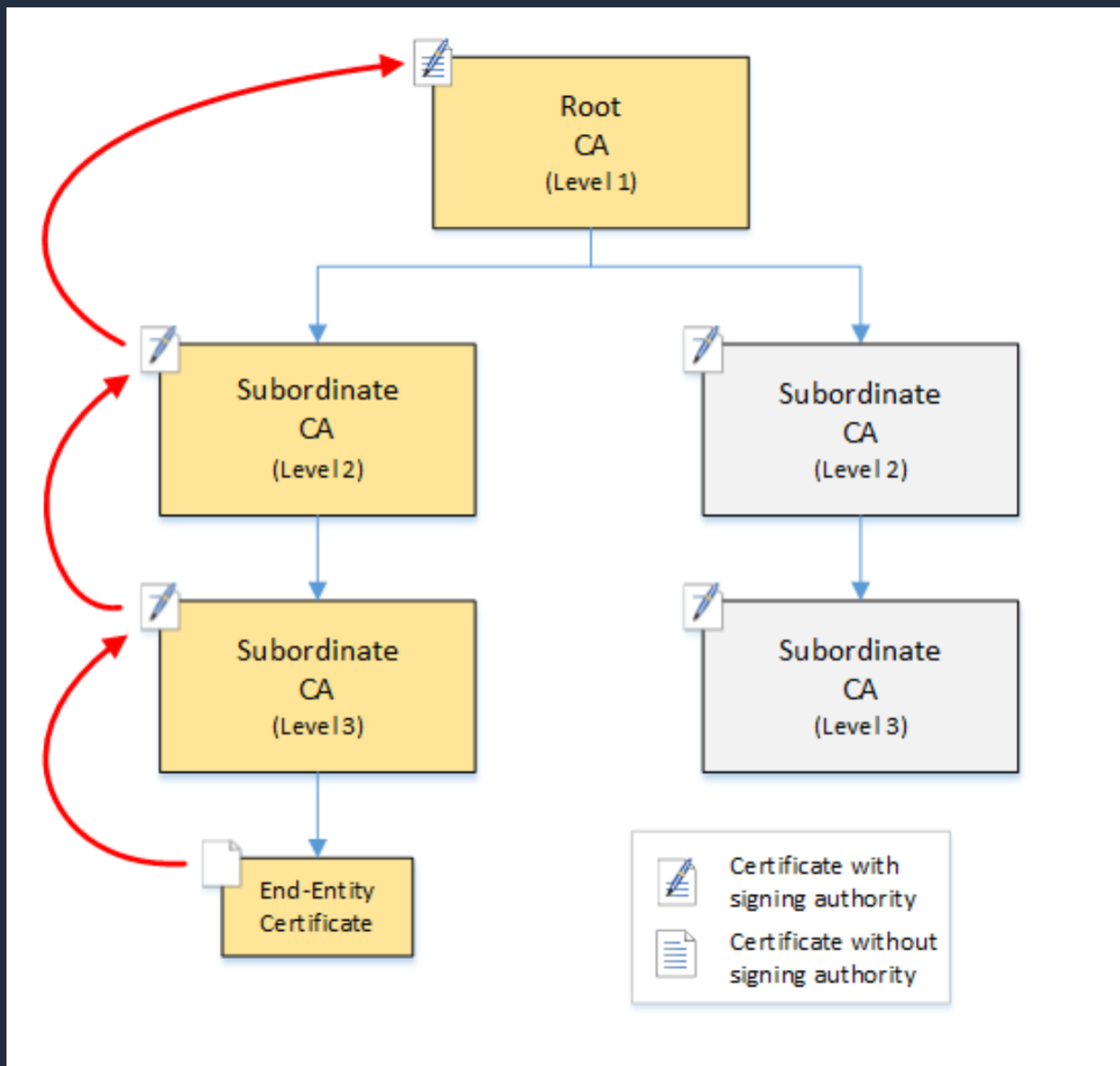
CloudFront, Elastic Load Balancing, API Gateway and other integrated services.

Not after

June 09, 2024, 14:51:24 (UTC+09:00)



최종 Entity X.509 인증서가 클라이언트에 제공되면 루트 CA로 돌아가는 인증 경로에서 신뢰 체인을 구성하려고 시도합니다. 그렇기 위해서는 루트 CA가 신뢰 저장소에 등록이 되어야 하며 IAM Roles Anywhere Trust Anchor에 Root CA를 등록합니다.



### Step 3. Trust Anchor 생성

트러스트 앵커(Trust anchors)를 구성하여 IAM Roles Anywhere와 인증 기관(CA) 간에 신뢰를 설정합니다.

Identity and Access Management (IAM)

Dashboard

Access management

User Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCP)

Create a trust anchor

Establish trust between AWS and your Certificate Authority (CA) to authenticate requests from your on-premises workloads.

Trust anchor

Region

Use the Region selector on the console navigation bar to switch AWS Region.

ap-northeast-2

Trust anchor name

dongsooanywhere

Use only letters, numbers, hyphens, or underscores.

Certificate authority (CA) source

AWS Certificate Manager Private CA

External certificate bundle

AWS Certificate Manager Private CA (2)

Certificate authorities (CA) from AWS Certificate Manager in your account for this region.

Filter private certificate authorities

< 1 >

ID	CA common name	Type	Status
		ROOT	Active

Notification settings

Customize notification settings to based on public key infrastructure. Roles Anywhere will use these settings to send certificate expiration events through Amazon Event Bridge, AWS Health and Amazon CloudWatch metric.

Event	Channel	Status	Threshold
CA certificate expiry event	All	Enabled	45 Days
End entity certificate expiry event	All	Enabled	45 Days

Tags - optional

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.

No tags associated with this resource.

Add new tag

You can add up to 50 more tags

Cancel

Create a trust anchor



## Step 4. Profile 생성

IAM Roles Anywhere 서비스 주체를 신뢰하는 IAM 역할을 생성합니다

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "rolesanywhere.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession",
        "sts:SetSourceIdentity"
      ],
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:rolesanywhere:region:account:trust-
anchor/TA_ID"
          ]
        }
      }
    }
  ]
}
```

IAM Roles Anywhere 프로파일(Profiles)을 사용하면 역할 자격 증명의 범위를 대상 권한 수준으로 낮출 수 있는 세션 정책을 사전 구성할 수 있습니다.

IAM > Roles > Roles Anywhere > Profile: profileanywhereS3Readaccess > Edit

### Edit profile [Info](#)

#### Profile

Profile name

Use only letters, numbers, hyphens, or underscores.

#### Roles

Roles with the Roles Anywhere trust policy that will be assumed by your non AWS workload.

Role

 **IAM Roles Anywhere 서비스 주체를 신뢰하는 IAM 역할**

Add another role

Don't see the roles you need? Add Roles Anywhere as a trusted entity to your desired roles. [See steps for how to add the trust policy.](#)

#### Session policies - optional

Session policies limit the permissions granted by the role's permissions policy and are assigned to the role session when the role is assumed.

Managed policies

Select up to 10 managed policies to attach.

☐ Inline policy

Cancel Save changes

## Step 5. 서명 요청 및 테스트

임시 보안 자격 증명을 얻지 않으면 외부 애플리케이션에서 AWS 리소스에 액세스 할 수 없습니다.

```
ubuntu@ip-10-1-1-104:~/rolesanywhere$ aws s3 ls s3://rolesanywheretestbucket
```

```
Unable to locate credentials. You can configure credentials by running "aws configure".
```

임시 보안 자격 증명을 얻기 위해 aws\_signing\_helper를 사용하여 인증서로 서명을 요청할 수 있습니다.

```
ubuntu@ip-172-31-4-146:~/rolesanywhere$ ls -al
total 12356
drwxrwxr-x  2 ubuntu ubuntu    4096 Jul 28 07:09 .
drwxr-xr-x 10 ubuntu ubuntu    4096 Jul 27 09:21 ..
-rwxrwxr-x  1 ubuntu ubuntu 12627368 Jul 26 00:42 aws_signing_helper
-rw-rw-r--  1 ubuntu ubuntu   1253 Jul 27 07:11 certificate.pem
-rw-rw-r--  1 ubuntu ubuntu   1143 Jul 27 07:11 certificate_chain.pem
-rw-----  1 ubuntu ubuntu   1675 Jul 27 07:27 decrypted_private_key.pem
-rw-rw-r--  1 ubuntu ubuntu   1875 Jul 27 07:12 private_key.pem
```





```

ubuntu@ip-172-31-4-146:~/rolesanywhere$ ./aws_signing_helper credential-process --trust-anchor-arn arn:aws:rolesanywhere:ap-northeast-2:██████████:trust-anchor/██████████ --profile-arn arn:aws:rolesanywhere:ap-northeast-2:██████████:profile/██████████ --role-arn arn:aws:iam::██████████:role/rolesAnywhereS3 --certificate certificate.pem --private-key decrypted_private_key.pem
{"Version":1,"AccessKeyId":"ASIAW██████████K","SecretAccessKey":"G██████████T","SessionToken":"IQo
6
d
a
a
c
B
5
"
Expiration":"2023-07-28T09:01:16Z"}ubuntu@ip-172-31-4-146:~/rolesanywhere$

```

\$ ./aws\_signing\_helper credential-process --trust-anchor-arn <Your Trust Anchor ARN> --profile-arn <Your Profile ARN> --role-arn <Your Role ARN> --certificate <Your Certificate> --private-key <Your Decrypt Private Key>

```

ubuntu@ip-172-31-4-146:~/rolesanywhere$ export AWS_ACCESS_KEY_ID=ASIAW██████████K
ubuntu@ip-172-31-4-146:~/rolesanywhere$ export AWS_SECRET_ACCESS_KEY=G██████████LT
ubuntu@ip-172-31-4-146:~/rolesanywhere$ export AWS_SESSION_TOKEN=IQo
6
d
a
a
c
B
5
"
Expiration":"2023-07-28T09:01:16Z"}

ubuntu@ip-172-31-4-146:~/rolesanywhere$ aws sts get-caller-identity
{
  "UserId": "AROAN██████████",
  "Account": "██████████",
  "Arn": "arn:aws:sts::██████████:assumed-role/rolesAnywhereS3/██████████"
}
ubuntu@ip-172-31-4-146:~/rolesanywhere$ aws s3 ls s3://rolesanywheretestbucket
2023-07-28 07:51:29      0 congratulation.txt

```



# 관련 자료

- [AWS Secrets Manager를 사용하여 IAM 액세스 키를 주기적으로 자동 교체하는 방안](#)

[https://repost.aws/ko/articles/ARlcbggX4aSf2j83UR1bvrrw/aws-secrets-manager%EB%A5%BC-%EC%82%AC%EC%9A%A9%ED%95%98%EC%97%AC-iam-%EC%95%A1%EC%84%B8%EC%8A%A4-%ED%82%A4%EB%A5%BC-%EC%A3%BC%EA%B8%B0%EC%A0%81%EC%9C%BC%EB%A1%9C-%EC%9E%90%EB%8F%99-%EA%B5%90%EC%B2%B4%ED%95%98%EB%8A%94-%EB%B0%A9%EC%95%88?sc\\_ichannel=ha&sc\\_ilang=ko&sc\\_isite=repost&sc\\_iplace=hp&sc\\_icontent=ARlcbggX4aSf2j83UR1bvrrw&sc\\_ipos=1](https://repost.aws/ko/articles/ARlcbggX4aSf2j83UR1bvrrw/aws-secrets-manager%EB%A5%BC-%EC%82%AC%EC%9A%A9%ED%95%98%EC%97%AC-iam-%EC%95%A1%EC%84%B8%EC%8A%A4-%ED%82%A4%EB%A5%BC-%EC%A3%BC%EA%B8%B0%EC%A0%81%EC%9C%BC%EB%A1%9C-%EC%9E%90%EB%8F%99-%EA%B5%90%EC%B2%B4%ED%95%98%EB%8A%94-%EB%B0%A9%EC%95%88?sc_ichannel=ha&sc_ilang=ko&sc_isite=repost&sc_iplace=hp&sc_icontent=ARlcbggX4aSf2j83UR1bvrrw&sc_ipos=1)

- [IAM Roles Anywhere를 사용하여 AWS 외부에서 실행되는 애플리케이션에서 AWS 리소스 액세스 하는 방안](#)

[https://repost.aws/ko/articles/ARuzTUwUK\\_QpW2U0m0PvNAAw/iam-roles-anywhere%EB%A5%BC-%EC%82%AC%EC%9A%A9%ED%95%98%EC%97%AC-aws-%EC%99%B8%EB%B6%80%EC%97%90%EC%84%9C-%EC%8B%A4%ED%96%89%EB%90%98%EB%8A%94-%EC%95%A0%ED%94%8C%EB%A6%AC%EC%BC%80%EC%9D%B4%EC%85%98%EC%97%90%EC%84%9C-aws-%EB%A6%AC%EC%86%8C%EC%8A%A4-%EC%95%A1%EC%84%B8%EC%8A%A4-%ED%95%98%EB%8A%94-%EB%B0%A9%EC%95%88](https://repost.aws/ko/articles/ARuzTUwUK_QpW2U0m0PvNAAw/iam-roles-anywhere%EB%A5%BC-%EC%82%AC%EC%9A%A9%ED%95%98%EC%97%AC-aws-%EC%99%B8%EB%B6%80%EC%97%90%EC%84%9C-%EC%8B%A4%ED%96%89%EB%90%98%EB%8A%94-%EC%95%A0%ED%94%8C%EB%A6%AC%EC%BC%80%EC%9D%B4%EC%85%98%EC%97%90%EC%84%9C-aws-%EB%A6%AC%EC%86%8C%EC%8A%A4-%EC%95%A1%EC%84%B8%EC%8A%A4-%ED%95%98%EB%8A%94-%EB%B0%A9%EC%95%88)





# Thank you!