

cross-account 처리 방법

- S3, ECR, Batch, RDS, Sagemaker

김재일



목차

간단한 소개

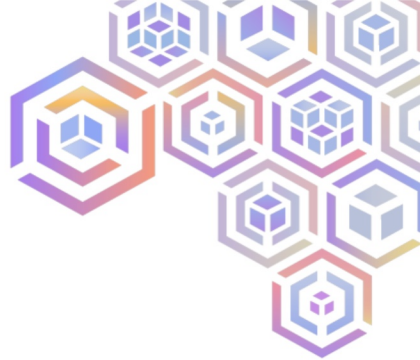
Cross account의 필수 개념 소개

ECR, S3, Batch, EC2, ECS의 Cross Account

RDS의 Snapshot을 통한 Cross Account

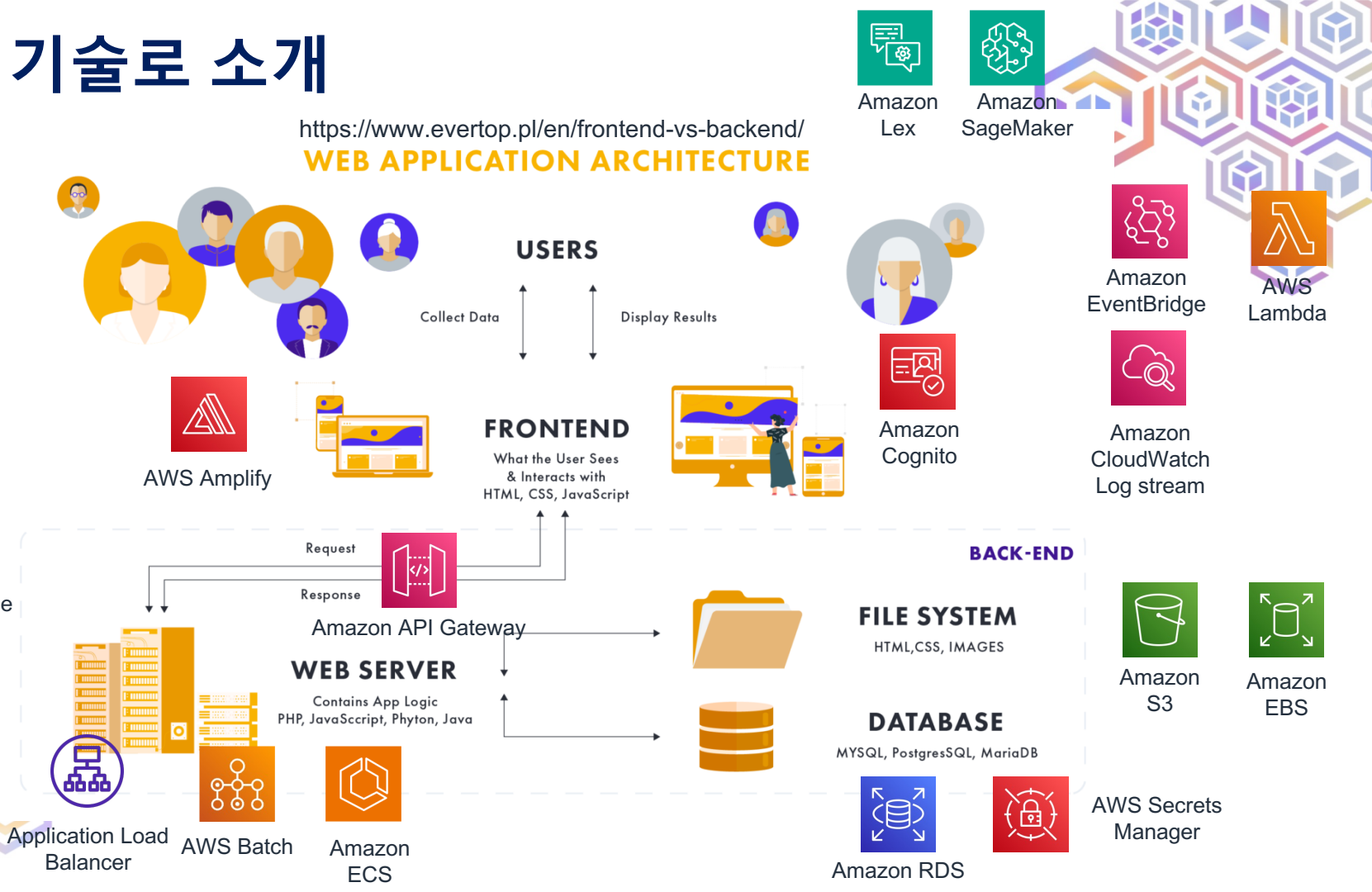
Sagemaker의 Cross Account

(그림은 Google에서 가져옴! 링크를 참고)



AWS 기술로 소개

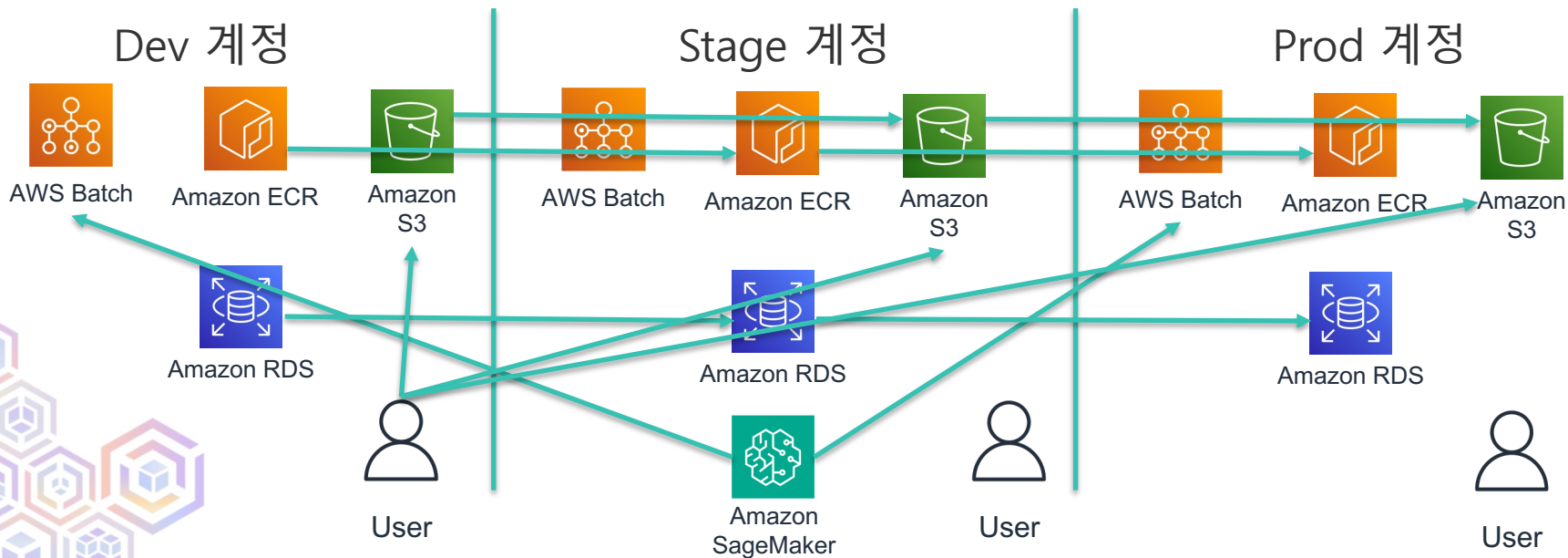
<https://www.evertop.pl/en/frontend-vs-backend/>
WEB APPLICATION ARCHITECTURE



Cross Account ?

Cross Account (교차 계정) 접근 제어?

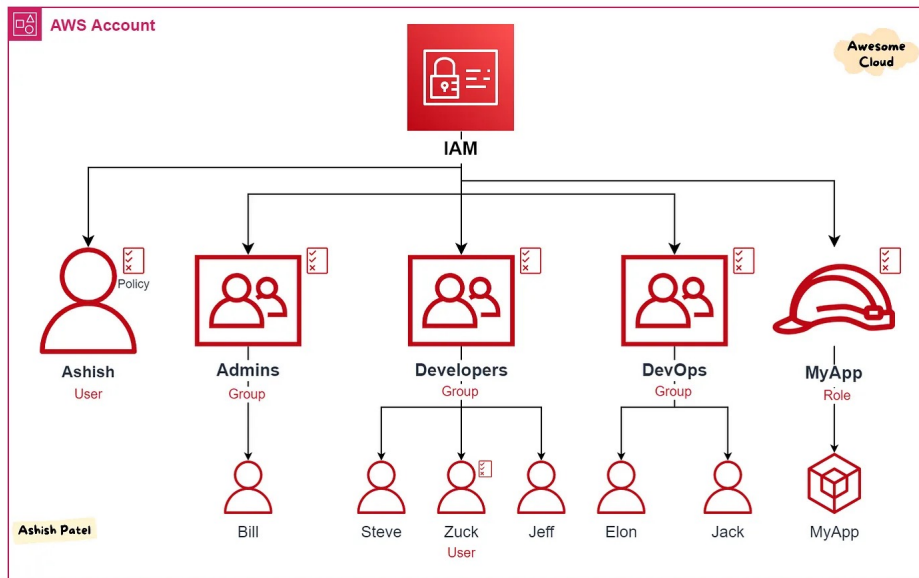
- 계정간에 리소스 접근을 관리하는 기능
- 여러 사용자(IAM User), 여러 AWS 계정



AWS IAM이란?

IAM Identity and Access Management

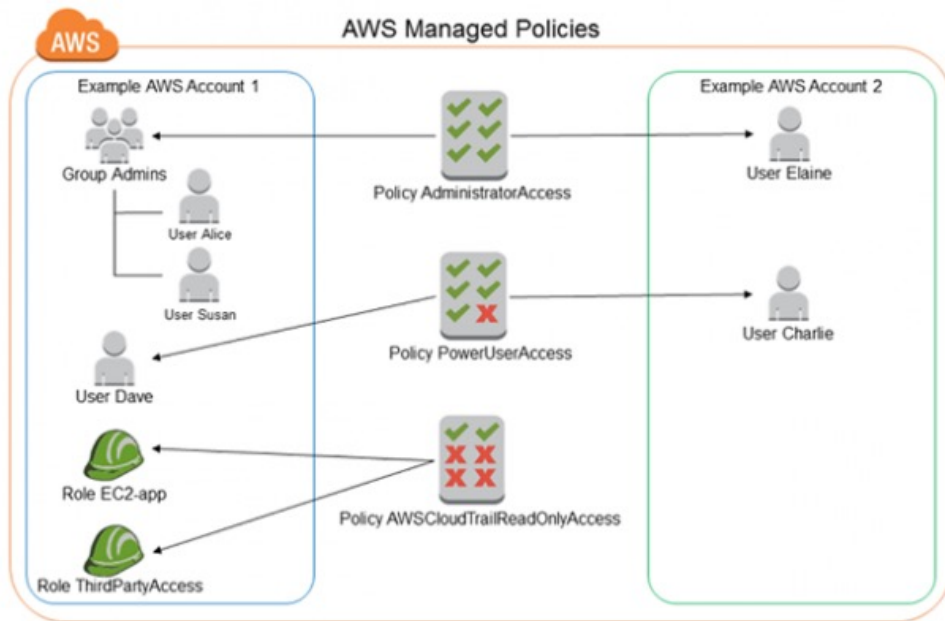
- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- IAM User, Group, Role, Policy



AWS IAM이란?

IAM Identity and Access Management

- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- IAM User, Group, Role vs. Policy

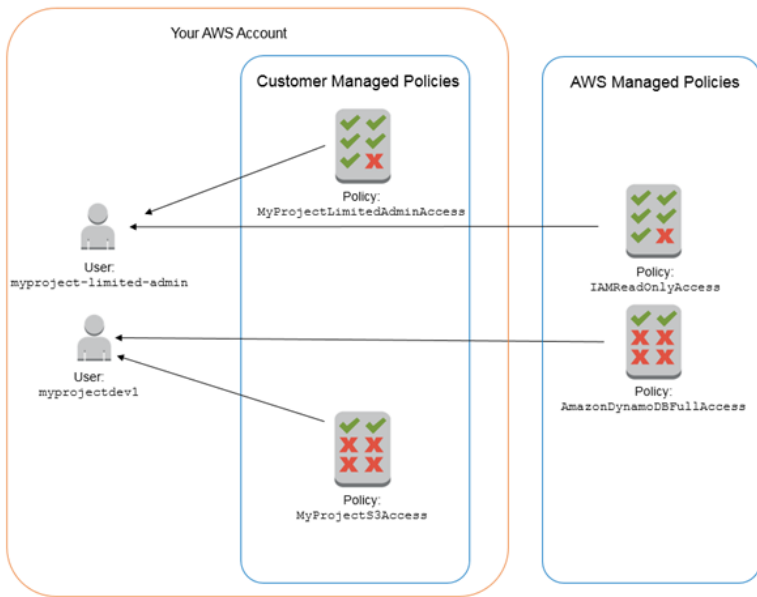


<https://www.testpreptraining.com/tutorial/aws-certified-security-specialty/iam-roles-and-policies-3/>

AWS IAM이란?

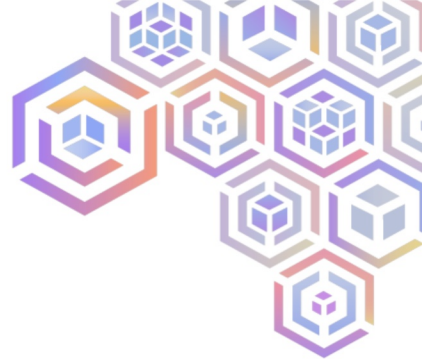
IAM Identity and Access Management

- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- Customer Managed Policies vs. AWS Managed Policies



<https://aws.amazon.com/ko/blogs/security/how-to-create-a-limited-iam-administrator-by-using-managed-policies/>

AWS IAM이란?



IAM Identity and Access Management

- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- Identity-based Policy와 Resource-based Policy

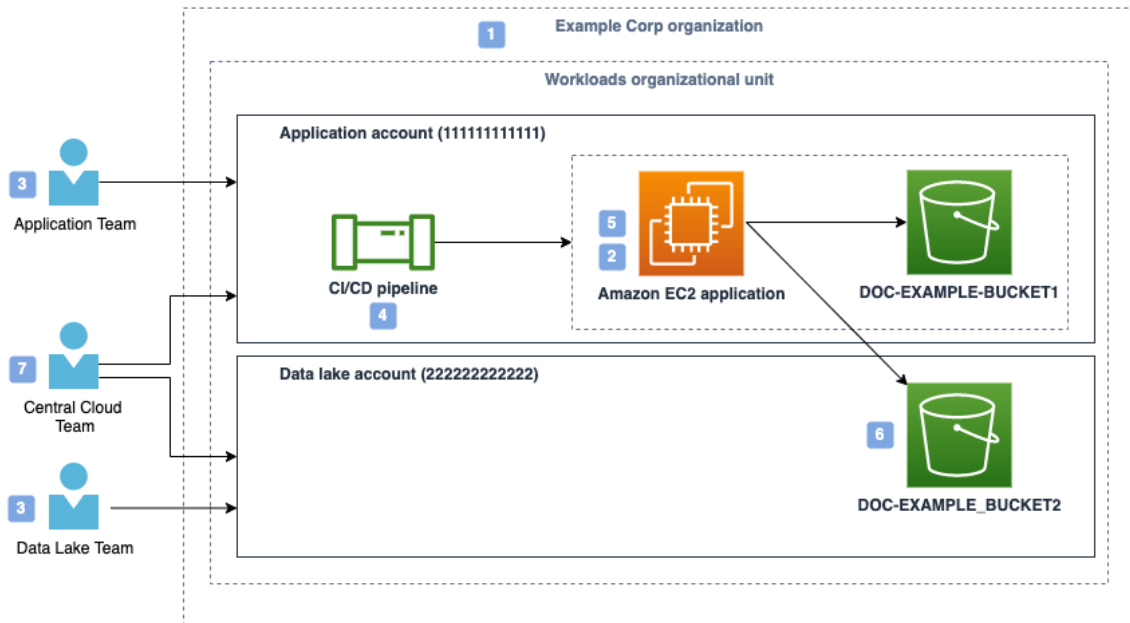
기준	Identity-based Policy	Resource-based Policy
정책이 적용되는 대상	IAM 사용자, 그룹, 또는 역할	AWS 리소스 (예: S3 버킷, Lambda 함수)
주요 목적	사용자의 신원을 기반으로 한 권한 관리	리소스에 대한 접근 권한 관리
권한 할당 방식	사용자, 그룹, 또는 역할에 직접 정책을 할당하여 권한 부여	리소스에 직접 정책을 할당하여, 특정 사용자 또는 역할에 대한 접근을 제어
사용 예시	사용자 A에게 S3 버킷에서 파일을 읽을 수 있는 권한 부여	S3 버킷 정책을 사용하여 특정 IAM 역할에게 버킷에 접근할 수 있도록 허용
권한 관리 범위	사용자 또는 역할이 AWS 서비스에서 수행할 수 있는 작업을 광범위하게 관리	특정 리소스에 대한 세밀한 접근 제어



AWS IAM이란?

IAM Identity and Access Management

- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- Identity-based Policy와 Resource-based Policy



	Policy type
1	Service control policy (SCP)
2	Permissions boundary
3	Identity-based policy
4	Identity-based policy
5	Identity-based policy
6	Resource-based policy
7	Identity-based policy

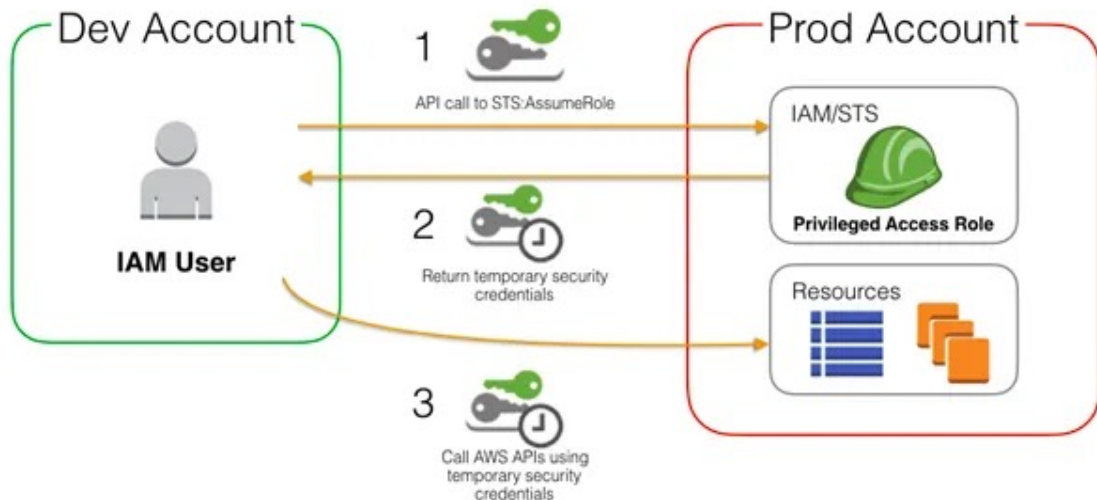
<https://aws.amazon.com/ko/blogs/security/iam-policy-types-how-and-when-to-use-them/>

AWS IAM이란?

IAM Identity and Access Management

- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- Assume role: Returns a set of temporary security credentials that you can use to access AWS resources

AWS STS(Security Token Service)



AWS IAM이란?

IAM Identity and Access Management

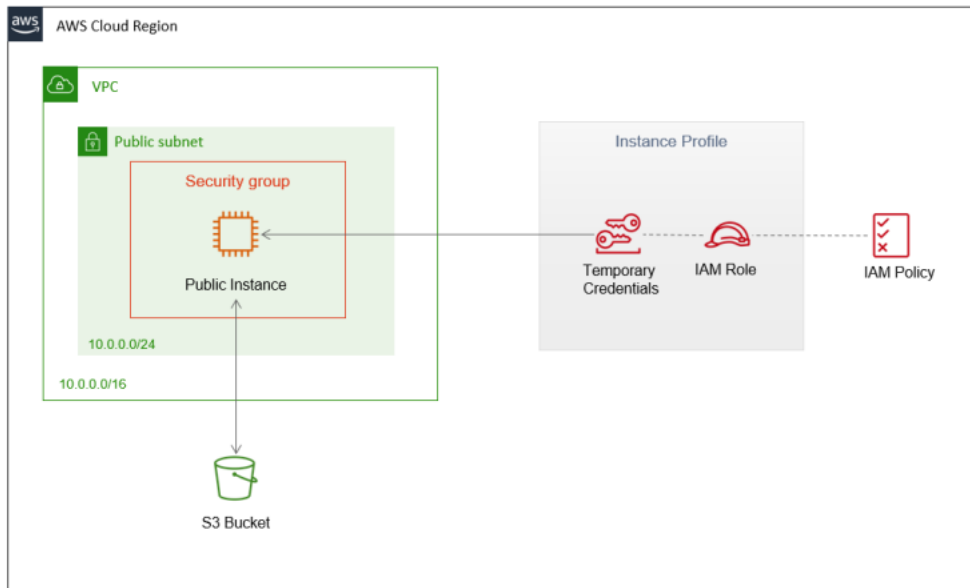
- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- EC2: Instance Role vs. Instance Profile

Permissions | **Trust relationships** | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

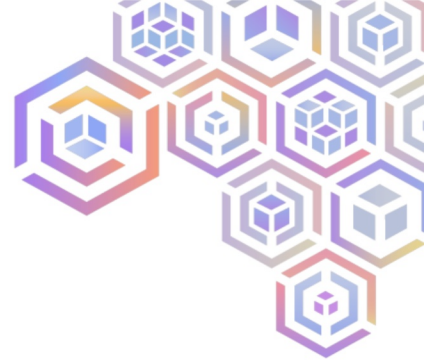
```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": "ec2.amazonaws.com"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```



AWS IAM이란?

IAM Identity and Access Management

- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스
- ECS & Fargate: Execution role vs Task(Job) role

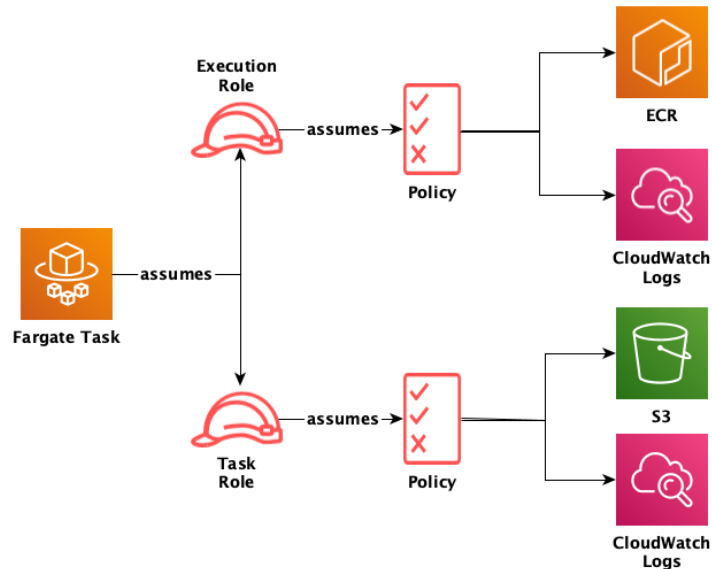


Permissions | **Trust relationships** | Tags | Access Advisor | Revoke sessions

Trusted entities

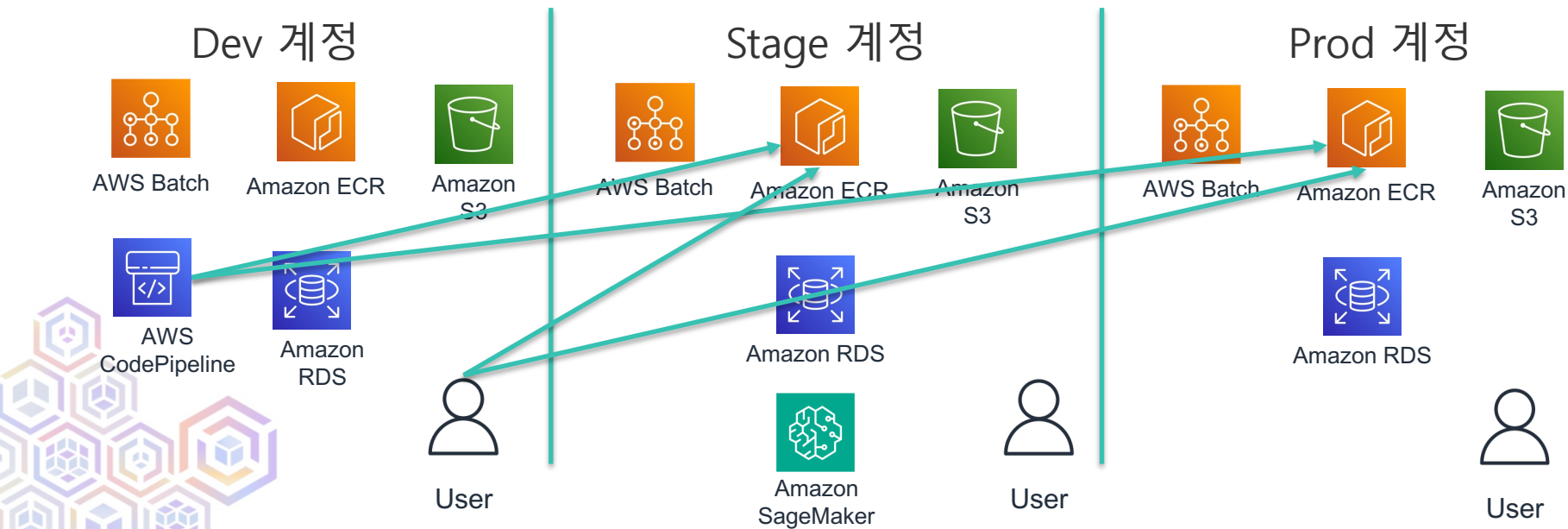
Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": "ecs-tasks.amazonaws.com"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

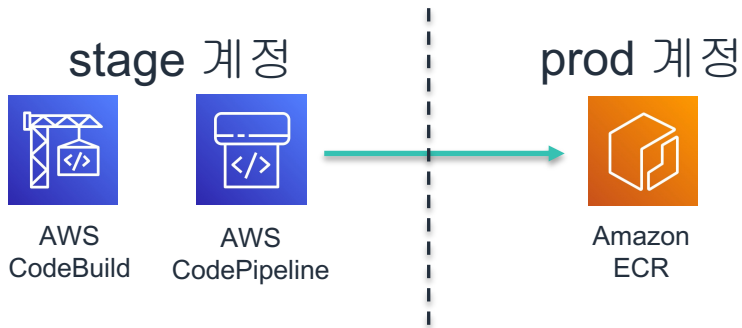


ECR의 Cross account 예제

ECR 시나리오



ECR의 Cross account 예제

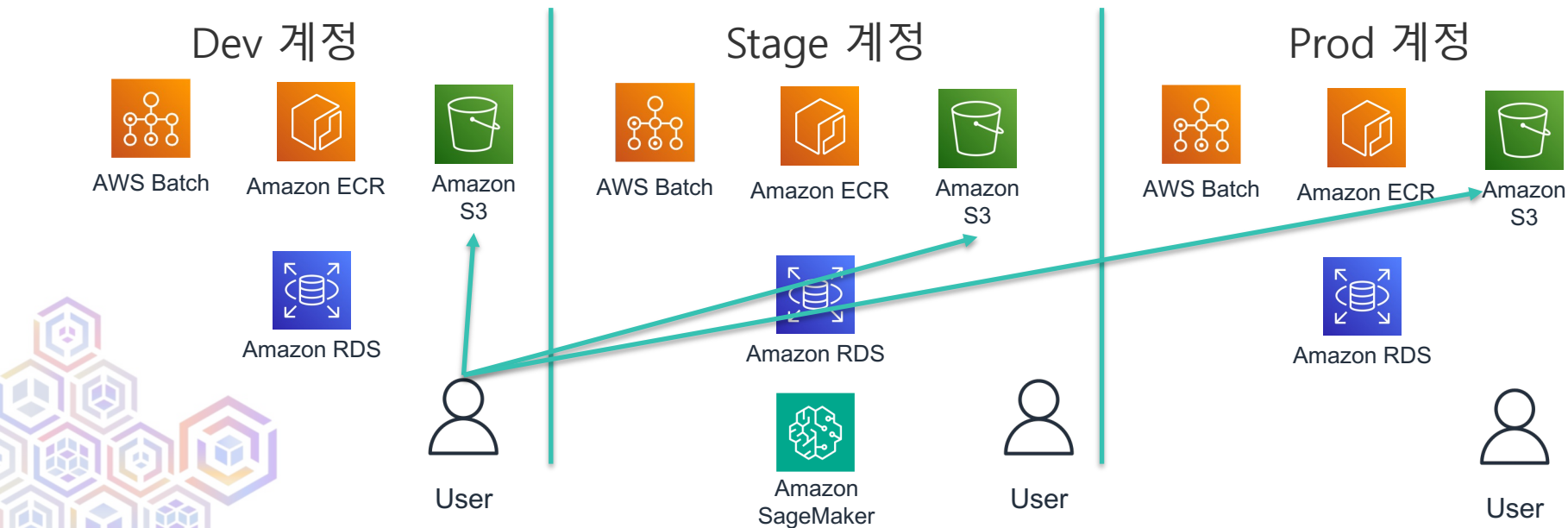


- Codebuild에서 본 계정 외에 다른 계정도 Image push가 가능
- Root는 특정 계정(User, Codepipeline) 에서 접근 가능
- User는 일부 사용자가 이미지를 가져오도록 허용

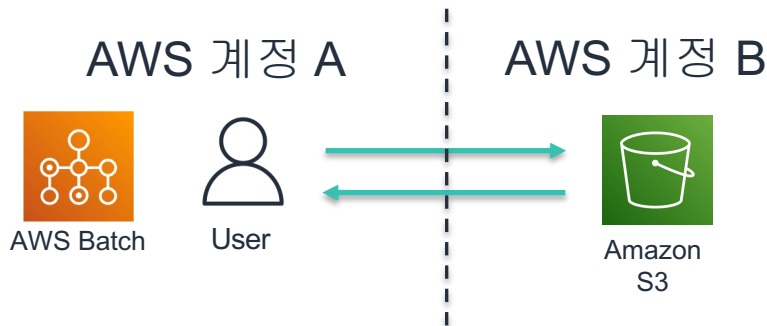
```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "PushImages",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::6726xxxxxxx:root",
          "arn:aws:iam::6745xxxxxxx:user:user1"
        ]
      },
      "Action": [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ]
    }
  ]
}
```

S3의 Cross account 예제

S3 시나리오



S3의 Cross account 예제



- S3의 권한을 이용하여, 입력, 출력은 B 계정에, 실행은 A 계정에서 처리하도록 설정
- Ex) `aws s3 sync/cp`
- 다른 계정 데이터 활용 가능 (www.ai-mstudio.com)
- 만약 Custom KMS를 사용하는 경우 권한 설정 필요

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::61616xxxx:role/InstanceRole",
        "arn:aws:iam::61616xxxx:role/JobRole",
        "arn:aws:iam::61616xxxx:role/TaskRole",
        "arn:aws:iam::61616xxxx :user/user1"
      ]
    },
    "Action": ["s3:*"],
    "Resource": [
      "arn:aws:s3:::bucket/*",
      "arn:aws:s3:::bucket"
    ]
  }
]}
```


S3의 Cross account 예제



도움말 | S3 파일 업로드

파일 업로드를 위한 S3 연결 방법 안내입니다.

- SSE-S3를 사용한 서버측 암호화 및 ACL 비활성화만 지원
- mp4, mt2s만 지원
- ap-northeast-2 리전만 지원

0. 연결을 원하는 버킷명

skt-test-input-bucket

1. '권한' 탭을 선택합니다.

2. '편집' 버튼을 선택합니다.

버킷 정책

JSON으로 작성된 버킷 정책은 버킷에 저장된 객체에 대한 액세스 권한을 제공합니다. 버킷 정책은 다른 계정이 소유한 객체에는 적용되지 않습니다. [자세히 알아보기](#)

이 버킷에 대해 피블릭 액세스 차단 설정이 활성화되어 있기 때문에 피블릭 액세스가 차단됩니다. 활성화된 설정을 확인하려면 이 버킷의 피블릭 액세스 차단 설정을 확인하세요. [Amazon S3 피블릭 액세스 차단 사용](#)에 대해 자세히 알아보기

표시할 정책이 없습니다.

버킷 정책

JSON으로 작성된 버킷 정책은 버킷에 저장된 객체에 대한 액세스 권한을 제공합니다. 버킷 정책은 다른 계정이 소유한 객체에는 적용되지 않습니다. [자세히 알아보기](#)

정책 예제 | 정책 생성기

닫기

도움말 | S3 파일 업로드

파일 업로드를 위한 S3 연결 방법 안내입니다.

버킷 정책

JSON으로 작성된 버킷 정책은 버킷에 저장된 객체에 대한 액세스 권한을 제공합니다. 버킷 정책은 다른 계정이 소유한 객체에는 적용되지 않습니다. [자세히 알아보기](#)

정책 예제

정책 생성기

버킷 ARN

arn:aws:s3::skt-test-input-bucket

정책

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::[redacted]:role/BatchJobRole",
9           "arn:aws:iam::[redacted]:role/H265MediaConvertRole",
10          "arn:aws:iam::[redacted]:role/BatchInstanceRole"
11        ]
12      },
13      "Action": [
14        "s3:GetObject",
15        "s3:ListBucket",
16        "s3:PutObject"
17      ],
18      "Resource": [
19        "arn:aws:s3::skt-test-input-bucket/*"
20      ]
21    }
22  ]
23 }
```

문 편집

문 선택

정책에서 기존 문을 선택하거나 새 문을 추가합니다.

+ 새 문 추가

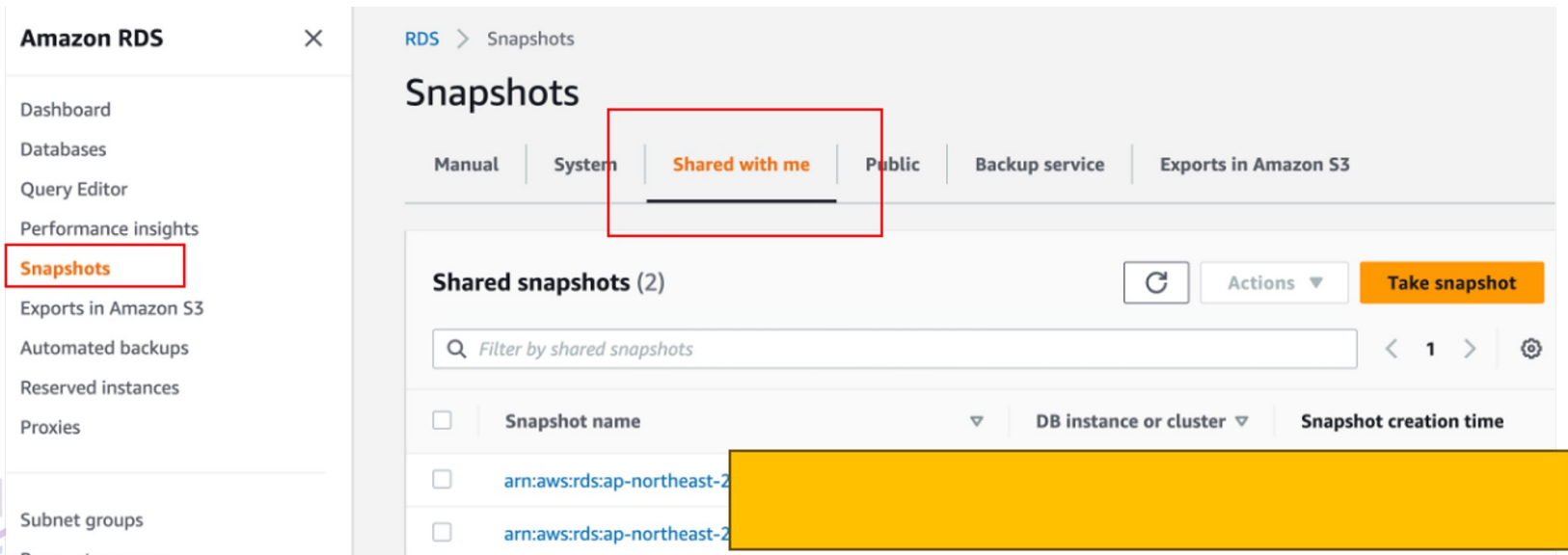
3. '정책' 영역에 스크립트를 붙여넣습니다.
클립보드에 스크립트 복사하기

닫기

RDS의 Cross account 예제

RDS Snapshot

- Shared with me 를 통해 공유 가능



The screenshot displays the Amazon RDS Snapshots console. On the left, the navigation menu includes 'Snapshots', which is highlighted with a red box. The main panel shows the 'Snapshots' page with tabs for 'Manual', 'System', 'Shared with me', 'Public', 'Backup service', and 'Exports in Amazon S3'. The 'Shared with me' tab is selected and highlighted with a red box. Below the tabs, the section 'Shared snapshots (2)' is visible, featuring a search bar and a 'Take snapshot' button. A table lists shared snapshots with columns for 'Snapshot name', 'DB instance or cluster', and 'Snapshot creation time'. The first two rows of the table are partially obscured by a yellow redaction box.

<input type="checkbox"/>	Snapshot name	DB instance or cluster	Snapshot creation time
<input type="checkbox"/>	arn:aws:rds:ap-northeast-2		
<input type="checkbox"/>	arn:aws:rds:ap-northeast-2		

RDS의 Cross account 예제

RDS Snapshot 활용

- KMS 문제 확인

<https://devocean.sk.com/blog/techBoardDetail.do?ID=164941&boardType=techBlog>

- RAM Resource Access Manager
이용 가능
- Switch Role을 통한
설정 가능

<https://medium.com/@labcloud/%EA%B5%90%EC%B0%A8-%EA%B3%84%EC%A0%95-%EC%A0%91%EA%B7%BC-cross-account-access-%EC%82%AC%EC%9A%A9%ED%95%B4%EB%B3%B4%EA%B8%B0-afe6a3fa2066>

- 그 외에도 다양한 방법

Amazon RDS

Dashboard

Databases

Query Editor

Performance insights

Snapshots

Exports in Amazon S3

Automated backups

Reserved instances

Proxies

Subnet groups

Parameter groups

Option groups

Custom engine versions

Events

Event subscriptions

Recommendations 0

Certificate update

Snapshot permissions

Preferences

You are sharing an encrypted DB snapshot. When you share an encrypted DB snapshot, you give the other account permission to make a copy of the DB Snapshot.

DB snapshot

test-snapshot


DB snapshot visibility



☐ Private

☐ Public

AWS account ID

Add

AWS account ID	Delete
105 	<input type="checkbox"/>
672 	<input type="checkbox"/>

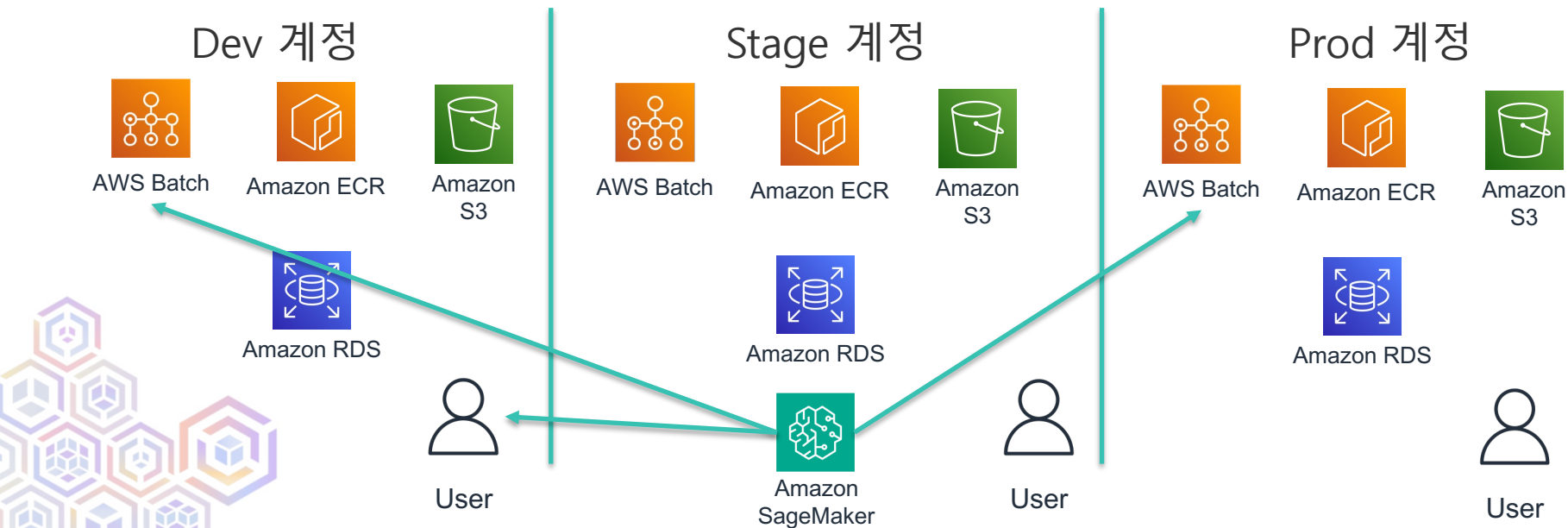
 To share your encrypted snapshot with another account, you will also need to share the custom master key with the other account through KMS. [Learn more](#) 

Cancel

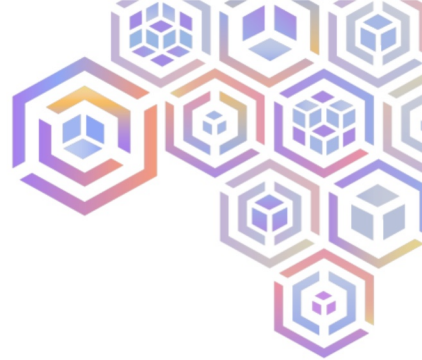
Save

Sagemaker의 Cross account 예제

Sagemaker 시나리오



Sagemaker의 Cross account 예제



Sagemaker 의 cross account 접근

- Policy를 통해 role 정의

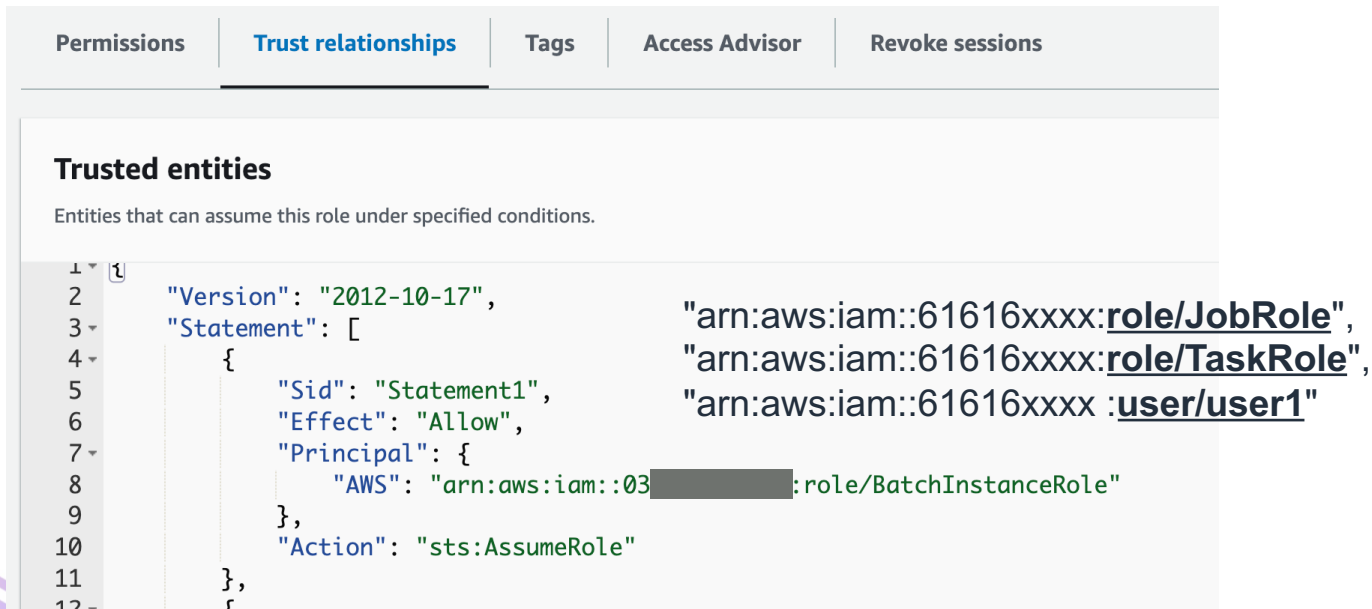
```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": "sagemaker:InvokeEndpoint",  
    "Resource": [  
      "arn:aws:sagemaker:ap-northeast-2:669xxxxxxx:endpoint/*" ]  
    }  
  ]  
}
```



Sagemaker의 Cross account 예제

Sagemaker 의 cross account 접근

- Trust relationship을 통해 다른 계정 접근하게 설정



The screenshot displays the AWS IAM console interface, specifically the 'Trust relationships' tab for a role. The 'Trusted entities' section shows a list of entities that can assume the role. The JSON policy document is visible, showing the 'AssumeRole' action for the 'BatchInstanceRole' in the source account.

Permissions: Trust relationships Tags Access Advisor Revoke sessions

Trusted entities
Entities that can assume this role under specified conditions.

```
1  {  
2    "Version": "2012-10-17",  
3    "Statement": [  
4      {  
5        "Sid": "Statement1",  
6        "Effect": "Allow",  
7        "Principal": {  
8          "AWS": "arn:aws:iam::03[redacted]:role/BatchInstanceRole"  
9        },  
10       "Action": "sts:AssumeRole"  
11     },  
12   ]  
13 }
```

"arn:aws:iam::61616xxxx:role/JobRole",
"arn:aws:iam::61616xxxx:role/TaskRole",
"arn:aws:iam::61616xxxx:user/user1"

Q&A

