Cloud Infrastructure Engineer

S3 to upload Platform

Choi Seong Gi I linux1547@hanmail.net

목차

S3 to upload Platform

개요

구축 조건

외부에서 수집된 데이터를 On-premise Server를 통해 S3로 upload 한 후 EC2와 Engineer가 접근할 수 있도록 아키텍처를 설계

요구사항

- AWS계정은 보안을 위해 S3, EC2 별도로 구성
- On-premise Server, Account A의 S3, Account B의 EC2, 사무실 Engineer에게 꼭 필요한 권한만 설정
- 모든 리소스에는 최소한의 권한만 설정할 것
- 권한정보가 유출되었을 시 피해 최소화하도록 설계
- 데이터를 전송하는 네트워크 구간은 보안적으로 안전 확보할 수 있도록 설계

목표

- 제시한 요구사항을 모두 만족
- 관리가 쉽고, 보안적으로 안전하며, 확장성이 좋으며, 고가용성을 보장하며, 장애를 잘 감내하며, 자동 복구를 하는 클라우드 아키텍처 설계

기타사항

- 아키텍처 설계 시 참조한 레퍼런스 명시

전체 구성도

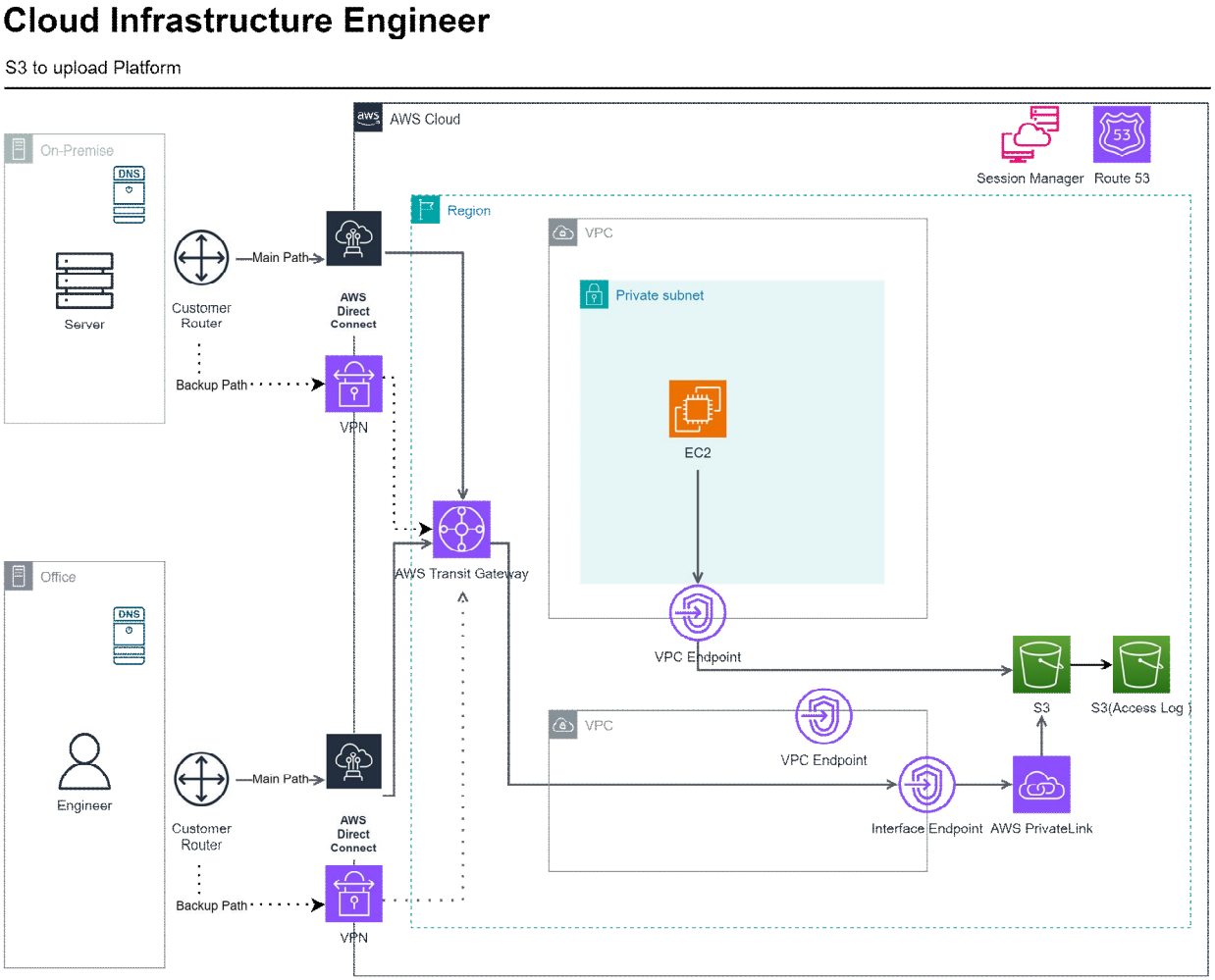
구성 특징

On-Premise에서 S3에 Upload가 가능하며 요구사항인 네트워크 구간의 보안을 위해 AWS사의 Direct Connect, VPN HA구성하여 설계

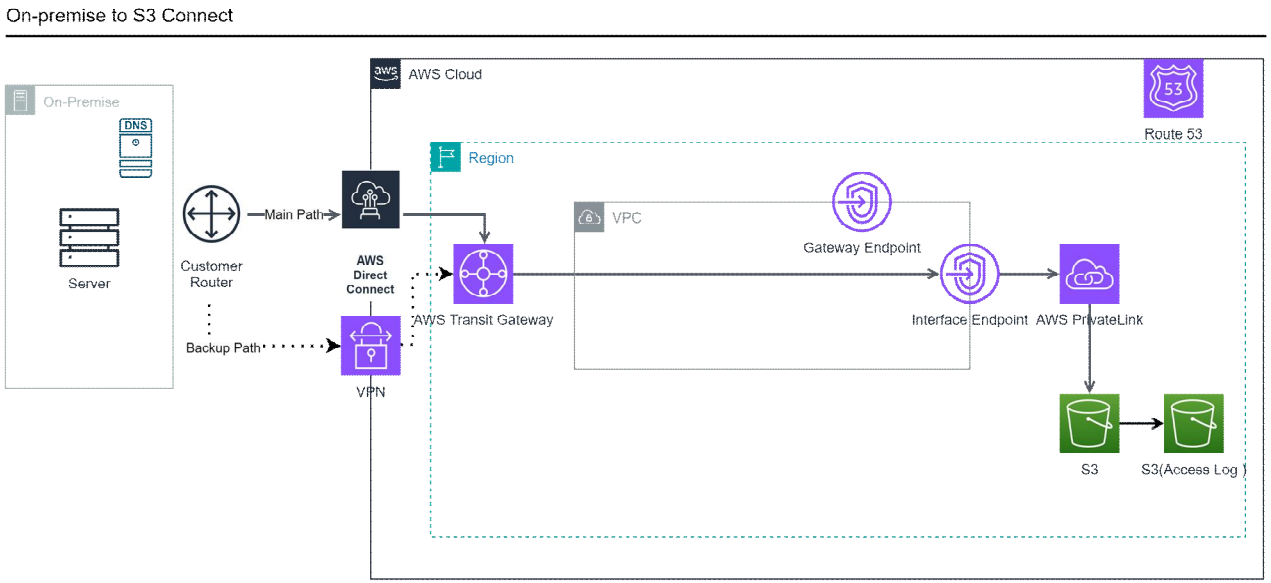
S3는 보안성을 강화하기 위해 Access Log용 S3 Bucket을 별도로 설정

Private Subnet에 Bestion Host없이 접근하기 위해 Session Manager 사용하여 접속

최소 권한의 원칙으로 꼭 필요한 권한만 부여



On-Premise to AWS Cloud



네트워크

- 최대수준의 안전과 보안을 고려하여 Direct Connect와 VPN을 활용한 연결 진행

- Main : Direct Connect L2레벨 암호화
  Backup : Site to Site VPN L3레벨 암호화
- Direct Connect, VPN으로 연결하여, 데이터를 전송하는 네트워크 구간을 보안적으로 안전하게 하는 요구사항 만족

On-Premise to AWS Cloud

- TGW를 통해 VPC내 interface Endpoint를 이용하여 S3에 접근하도록 설정
- S3 Interface Endpoint사용하는 이유는 DNS Name을 지원하여, On-premise에서 간단한 DNS설정으로 Public망이 아닌 DX, VPN망을 통해 접속할 수 있기 때문입니다.

- On-Premise의 DNS 설정은 s3.ap-northeast-2.amazonaws.com에 대해 Conditional Forwarders를 설정하여 AWS Route53 Resolver에 대한 Inbound Endpoint IP로 구성됩니다.

- S3에 대한 Interface Endpoint를 설정하면, On-Premise에서 해당 S3 버킷에 대한 쿼리를 하게 되면 DX 또는 VPN으로 연결된 AWS Route53 DNS로 Forward됩니다. 이를 통해 Interface Endpoint를 통해 쿼리에 대한 답변을 받을 수 있습니다.

- 이러한 구성을 통해 외부 Public망이 아닌 DX, VPN망으로 S3 Bucket을 접속할 수 있습니다.

On-Premise to AWS Cloud

IAM권한 – On-Premise Server

요구사항

- On-premise Server에서 AWS Cloud 내 S3에 Write 권한을 가지고 Upload

적용사항

- 사용자를 생성한 후 읽기와 쓰기 권한을 적용한 정책을 할당했습니다. 그 다음 해당 사용자에 대한 액세스 키를 발급받아, 이 키를 On-Premise 서버에 적용합니다.

권한 정책의 JSON 구성

```
{
    "Id": "Policy1702539685882",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1702539680084",
            "Action": [
                "s3:GetObject",  //  S3 객체 읽기
                "s3:ListBucket", // S3 버킷 리스트 확인
                "s3:PutObject" // S3 버킷내 Upload(write)권한
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::test-s3-upload-seonggi13/*" // 위 해당 규칙이 적용될 Resource (여기서는 S3버킷)
        }
    ]
}
```

Office to AWS Cloud

네트워크

- On-Premise to AWS Cloud연결과 동일하게 Direct Connect와 VPN을 활용한 연결 진행

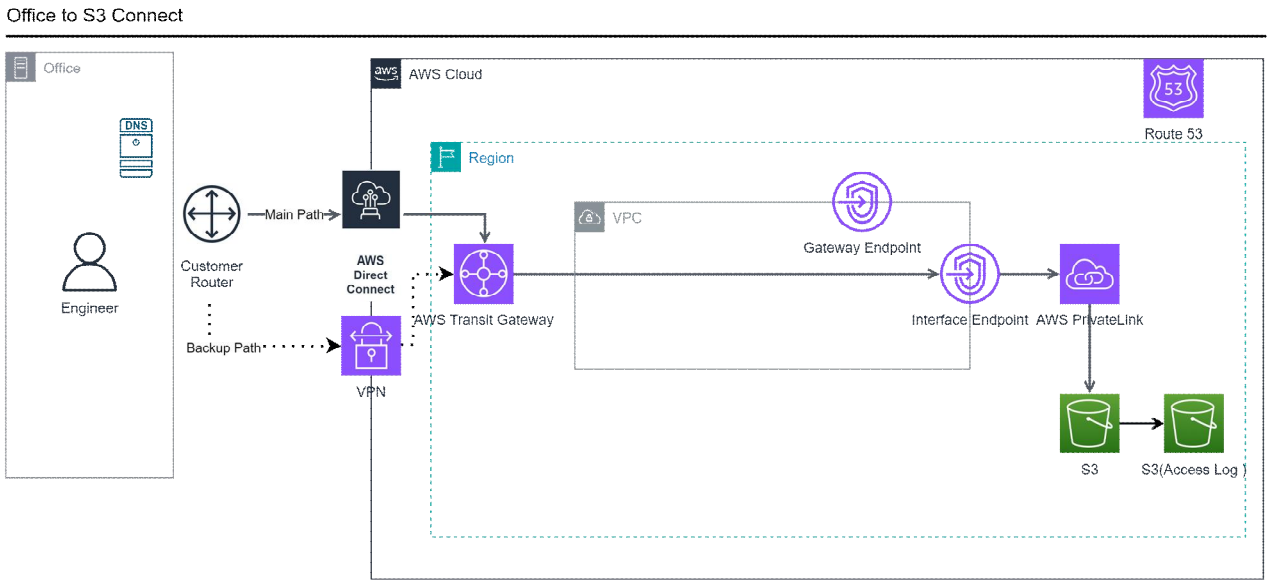
IAM권한 – Office(User)

요구사항

- Engineer들은 AWS Cloud 내 S3 Bucket 객체들에 대해서 Read만 가능

적용사항

- 사용자를 생성한 후 읽기만 가능한 권한 정책을 부여하고, 그 사용자에게 액세스 키를 발급받아 Engineer이 사용하는 PC에 적용합니다.



Office to AWS Cloud

권한 정책의 JSON 구성

- test-s3-upload-seonggi13 S3 Bucket에 대한 버킷 리스트와 Bucket내 객체 읽기만 가능하도록 권한부여
  Resource에 모든 리소스가 아닌 꼭 적용될 Bucket만 지정하여 권한이 탈취되어도 다른 Resource접근 불가하도록 설정

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",     // S3 버킷 리스트 확인
                "s3:GetObject"  //  S3 객체 읽기
            ],
            "Resource": [
                "arn:aws:s3:::test-s3-upload-seonggi13/*"  // 위 해당 규칙이 적용될 Resource (여기서는 S3버킷)
            ]
        }
    ]
}
```

AWS EC2

네트워크

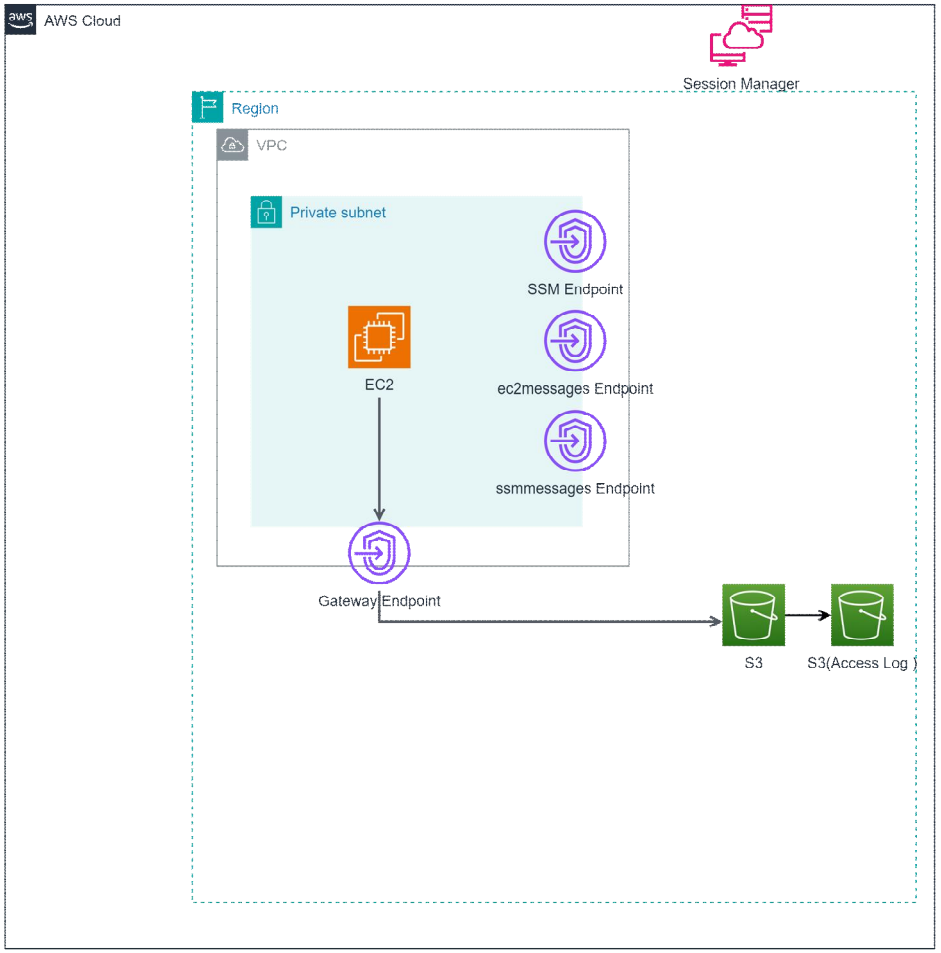
- Private Subnet에 Bestion Host없이 접근하기 위해 Session Manager를 사용하여 접속합니다.

적용사항

- EC2에 ssm agent설치
- Session Manager Private Subnet접속을 위해 Endpoint 3개 설정
- EC2에서 gateway endpoint를 통해 public망이 아닌 바로 S3로 접속합니다.

특이사항

- EC2, S3는 관리의 편의성과 보안성을 유지하기 위해 다른 AWS 계정을 사용합니다.



AWS EC2

IAM권한 – EC2

요구사항

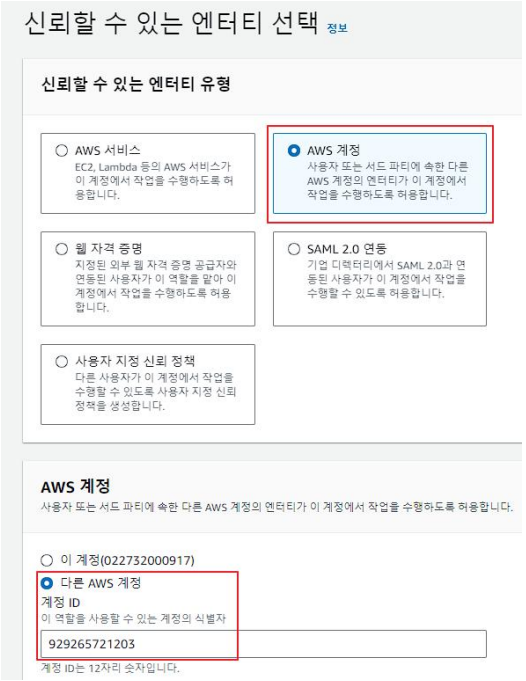
- EC2 내에서 S3 Bucket 객체들에 대해서 Read만 가능
  Account 계정B를 사용 중인 EC2에서 Account 계정A인 S3로 접속 가능하도록 권한설계

적용사항

- 계정 A = EC2
  계정 B = S3
- 계정 B에서 역할을 생성합니다. 이때 신뢰할 수 있는 엔티티 유형에 AWS계정을 선택 하고
  계정ID에 계정A의 ID번호를 입력합니다.
  정책을 읽기만 가능하도록 생성하고, 역할에 연결합니다.
  읽기만 가능하도록 권한 정책 설정 후 IAM에서 역할과 연결 후 EC2에 연결하여, 해당 EC2에서는
  지정된 S3에 읽기만 가능하도록 설정합니다.

계정 B 권한 정책 JSON

```
{
    "Id": "Policy1703432685882",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt17023432380084",
            "Action": [
                "s3:GetObject",  //  S3 객체 읽기
                "s3:ListBucket", // S3 버킷 리스트 확인
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::test-s3-upload-seonggi13/*" // 위 해당 규칙이 적용될 Resource (여기서는 S3버킷)
        }
    ]
}
```



AWS EC2

적용사항

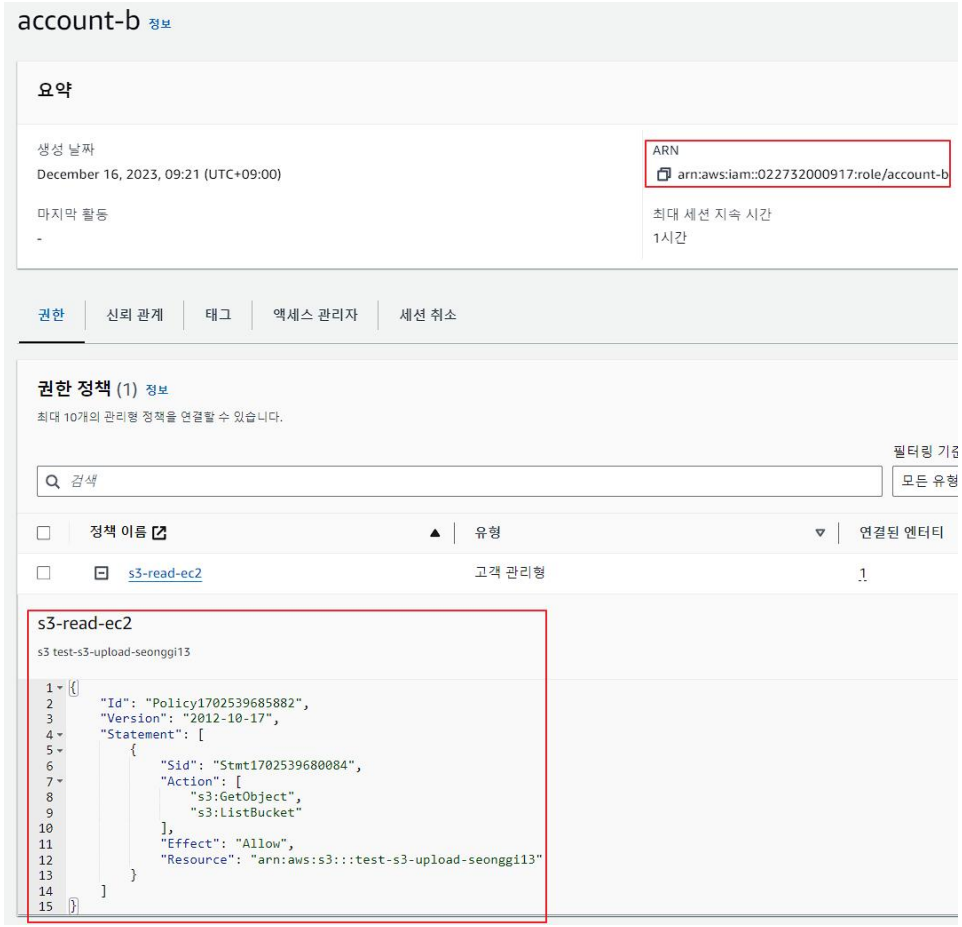
- 계정 A = EC2
  계정 B = S3
- 계정 A에서도 역할을 생성합니다. EC2이므로 신뢰할 수 있는 엔티티 유형에 AWS서비스-EC2를 선택합니다.
  정책을 아래와 같이 입력합니다. Principal 부분에 계정B에서 생성한 역할 ARN을 입력합니다.
- 생성한 계정 A역활을 EC2에 연결합니다.

계정 A의 권한 정책 JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::022732000917:role/account-b" // 계정B의 ARN
        }
    ]
}
```

AWS EC2

계정 B의 권한 정책 JSON과 ARN



AWS EC2

EC2 적용

- EC2 접속하여 config 파일에 역할에 대한 프로필을 생성합니다.
- aws sts 명령어로 A계정에서 동작하는 EC2에서 계정 B에 적용된 profile을 확인하고, s3 ls 명령어를 통해 계정B에 생성된 S3 Bucket에 접속을 확인합니다.

```
[ec2-user@ip-172-31-1-181 .aws]$ aws sts get-caller-identity --profile account-a
{
    "UserId": "AROAQKSXOZ2KQOOZQEFJ6:botocore-session-1702687610",
    "Account": "022732000917",
    "Arn": "arn:aws:sts::022732000917:assumed-role/account-b/botocore-session-1702687610"
}
[ec2-user@ip-172-31-1-181 .aws]$ aws s3 ls test-s3-upload-seonggi13/proxy.txt --profile account-a
2023-12-15 13:16:52        151 proxy.txt
[ec2-user@ip-172-31-1-181 .aws]$
```

레퍼런스

Amazon S3에 대한 VPC 엔드포인트 전략 선택
https://aws.amazon.com/ko/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

S3 Interface Endpoint에 대한 DNS Name 지원
https://devocean.sk.com/blog/techBoardDetail.do?ID=164685&boardType=techBlog

S3용 PrivateLink
https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/userguide/privatelink-interface-endpoints.html

Amazon S3에 대한 게이트웨이 엔드포인트
https://docs.aws.amazon.com/ko_kr/vpc/latest/privatelink/vpc-endpoints-s3.html

EC2에서 다른 계정의 S3버킷 접속방안
https://repost.aws/ko/knowledge-center/s3-instance-access-bucket

Thank you