



SUMMIT
ONLINE

S3, 넌 이것까지 할 수 있네

(Amazon S3 신규 기능 소개)

김세준
솔루션즈 아키텍트
AWS Korea

Agenda

비용 절감

보안 및 접근

데이터 관리

Amazon S3 스토리지 클래스



S3 Standard



S3 Intelligent-Tiering



S3 Standard-IA



S3 One Zone-IA



S3 Glacier



S3 Glacier Deep Archive

Frequent

Access frequency

Archive

최신 스토리지 클래스



S3 Intelligent-Tiering

클라우드 스토리지 **관리** 혁신



S3 Glacier Deep Archive

클라우드 스토리지 **비용** 혁신

S3 Glacier Deep Archive

2019년 3월 출시



GB당
\$0.002/월



Tape
관리 불필요



99.9999999999%
내구성



12 시간 내에
데이터 복구

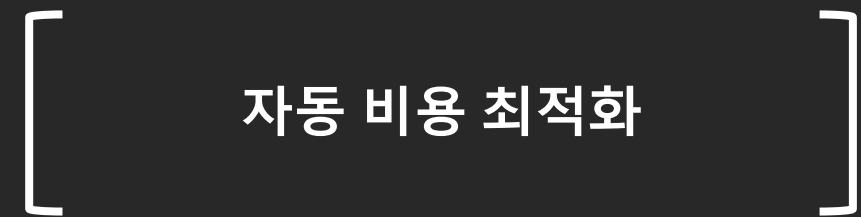
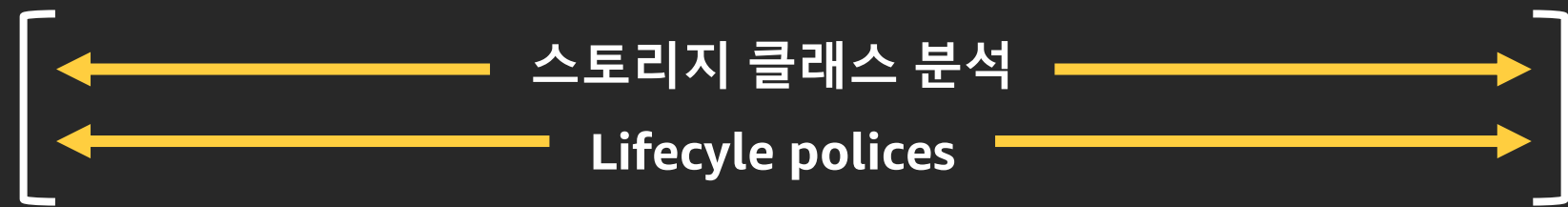
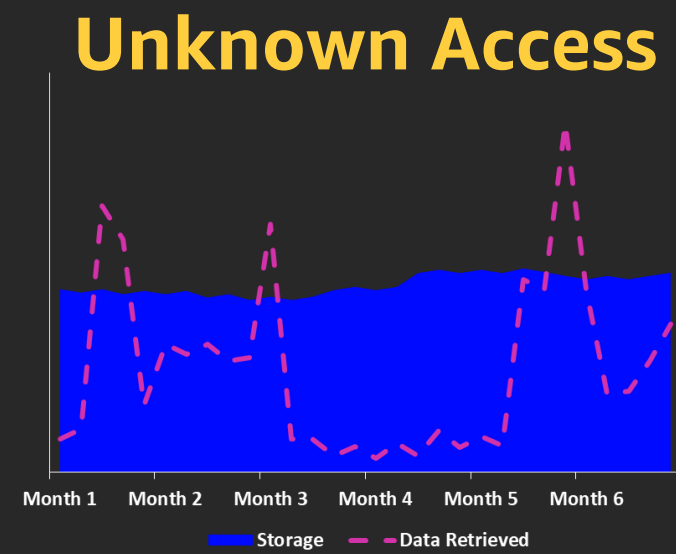
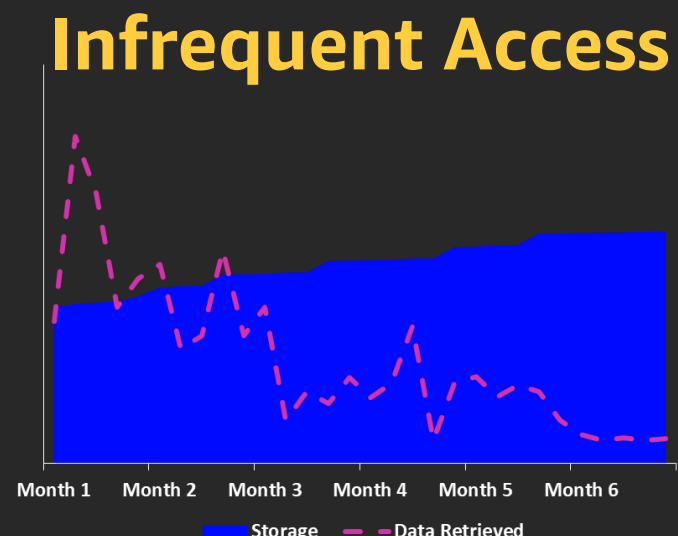
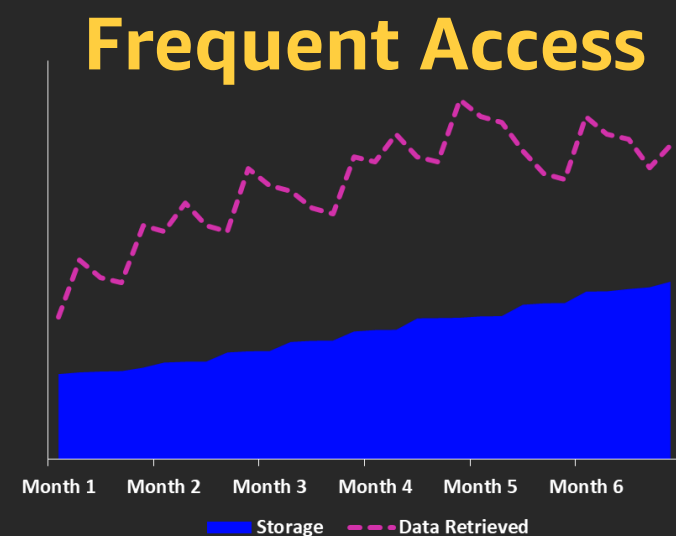
S3 Glacier Deep Archive

2019년 3월 출시

	S3 Glacier	S3 Glacier Deep Archive
비 용	GB 당 * \$0.005 / 월	GB 당 * \$0.002 / 월
검색 시간	긴급: 1-5 분 표준: 3-5 시간 대량: 5-12 시간	표준: 12 시간 대량: 48 시간
최소 저장 기간	90 일	180 일

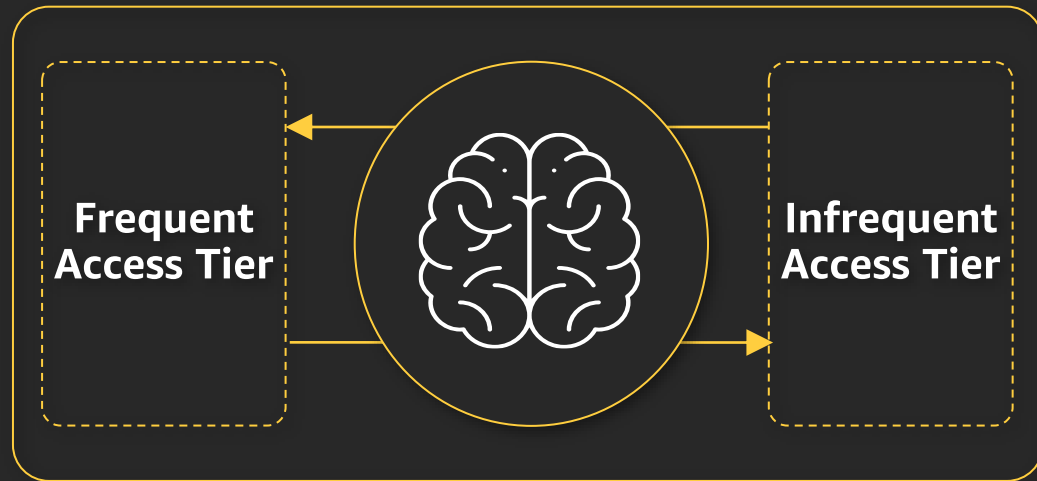
S3 Intelligent-Tiering

re:Invent 2018 출시



S3 Intelligent-Tiering

작동 원리



1. PUT의 선택적 플래그를 사용하거나 수명주기 정책을 사용하여 **S3 Intelligent-Tiering**에 객체 배치
2. 객체는 처음 30 일 동안 **Frequent Access** 계층으로 분류됩니다.
3. **30 일** 동안 개체에 액세스하지 않으면 자동으로 **Infrequent Access** 계층으로 분류 됩니다.
4. **Infrequent Access** 계층의 객체에 액세스하면 다시 30 일 동안 자동으로 **Frequent Access**로 다시 분류됩니다.

성능 영향 없음, 운영 오버 헤드 없음, 검색 비용 없음

S3 Inventory - Intelligent Tiering 접근 분석

2019년 10월 출시

NEW!

- 객체 별 계층 가시성 제공
- 액세스 패턴에 대한 통찰력 제공
- 스토리지 비용 이해

The screenshot shows the 'Advanced settings' for an S3 Inventory. The 'Output format' is set to 'CSV'. Under 'Object versions', 'Include all versions' is selected. In the 'Optional fields' section, 'Intelligent-Tiering: Access tier' is checked and highlighted with a yellow box. Other optional fields like 'Size', 'Last modified date', 'Storage class', 'Etag', 'Multipart upload', 'Replication status', 'Encryption status', 'Retention mode', 'Retain until date', and 'Legal hold status' are also checked. The 'Encryption' section is set to 'None'. Buttons for 'Cancel' and 'Save' are at the bottom.

The screenshot shows a query result for 'access tiers'. The query is: `1 SELECT object, accesstier, storageclass FROM oregon`. The results table has three columns: 'object', 'accesstier', and 'storageclass'. The 'accesstier' column is highlighted with a yellow box. The results show 10 objects, all with 'INTELLIGENT_TIERING' storage class. The 'accesstier' values are 'FREQUENT' for objects 1, 3, 4, and 5, and 'INFREQUENT' for objects 2, 6, 7, 8, 9, and 10.

	object	accesstier	storageclass
1	KIDS-A.JPG	FREQUENT	INTELLIGENT_TIERING
2	KIDS-AA.JPG	INFREQUENT	INTELLIGENT_TIERING
3	KIDS-B.JPG	FREQUENT	INTELLIGENT_TIERING
4	KIDS-BB.JPG	FREQUENT	INTELLIGENT_TIERING
5	KIDS-BBB.JPG	INFREQUENT	INTELLIGENT_TIERING
6	KIDS-BBBB.JPG	INFREQUENT	INTELLIGENT_TIERING
7	KIDS-C.JPG	INFREQUENT	INTELLIGENT_TIERING
8	KIDS-CC.JPG	INFREQUENT	INTELLIGENT_TIERING
9	KIDS-D.JPG	INFREQUENT	INTELLIGENT_TIERING
10	KIDS-DDD.JPG	INFREQUENT	INTELLIGENT_TIERING

Amazon S3 신규 기능

비용 절감

S3 Glacier Deep Archive

S3 Intelligent-Tiering

Access tiers in inventory reports

보안 및 접근

데이터 관리

Block public access

re:Invent 2018 출시



우발적인 공개 액세스를 사전 차단

계정 또는 버킷 레벨 차단

ACL 액세스, 버킷 정책 액세스 또는 둘 다에 적용 가능

aws Services Resource Groups

Amazon S3

Buckets

Batch operations

Block public access (account settings)

Feature spotlight

Block public access (account settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply account-wide for all current and future buckets. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- ☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through *new* public bucket policies**
S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through *any* public bucket policies**
S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

Cancel Save

Access Analyzer for S3

re:Invent 2019 출시

NEW!

Amazon S3 > Access analyzer for S3

Access analyzer for S3

Asia Pacific (Singapore) (ap-southeast-1) ▼

The buckets listed below are configured to allow access by anyone using the internet or authenticated AWS users, including AWS users outside of your organization. AWS recommends that you restrict access immediately. Review each bucket to verify the access. View detailed findings on the [IAM console](#) or [Learn more](#).

3 buckets are configured to allow access to anyone on the internet or any other AWS users. Review this risky configuration immediately
Explore other Regions to identify other buckets in your account that may also be at risk.

[Download report](#)

Buckets with public access (3)

These buckets can be accessed by anyone on the internet. Unless you require a public configuration for a specific and verified use case, AWS recommends that you block all public access to your buckets. [Learn more](#)

Status: All ▼

	Bucket name ▼	Discovered by Access Analyzer ▼	Shared through ▼	Status ▼	Access level ▼
<input checked="" type="radio"/>	bdemobucket	2 hours ago	Access control list	Active	List, Read
<input type="radio"/>	areinventdemobucket	2 hours ago	Access control list	Active	Write
<input type="radio"/>	ademobucket	2 hours ago	Access control list, Bucket policy	Active	Write, Read, List

[Block all public access](#) [View findings](#) [Mark as active](#) [Archive](#)

Buckets with access from other AWS accounts - including third party AWS accounts (3)

These buckets are conditionally shared with other AWS accounts. To ensure that you only grant access to the intended accounts, AWS recommends that you review access to these buckets.

Status: All ▼

	Bucket name ▼	Discovered by Access Analyzer ▼	Shared through ▼	Status ▼	Access level ▼
<input type="radio"/>	example-destinationbucket	2 hours ago	Access control list	Active	List, Read
<input type="radio"/>	demobucket2019	2 hours ago	Access control list	Active	List, Read
<input type="radio"/>	amsterdambucket	2 hours ago	Access control list	Active	Write, Read, List

[View findings](#) [Mark as active](#) [Archive](#)

- 공유 액세스를 위한 버킷 모니터링
- 추가 비용없이 S3 콘솔에서 사용가능
- 퍼블릭 및 다른 계정 접근 내역 제공

Access Analyzer for S3

re:Invent 2019 출시

NEW!

Amazon S3 > Access analyzer for S3

Access analyzer for S3 Asia Pacific (Singapore) (ap-southeast-1) ▼

The buckets listed below are configured to allow access by anyone using the internet or authenticated AWS users, including AWS users outside of your organization. AWS recommends that you restrict access immediately. Review each bucket to verify the access. View detailed findings on the [IAM console](#) or [Learn more](#)

3 buckets are configured to allow access to anyone on the internet or any other AWS users. Review this risky configuration immediately
Explore other Regions to identify other buckets in your account that may also be at risk.

[Download report](#)

Buckets with public access (3)
These buckets can be accessed by anyone on the internet. Unless you require a public configuration for a specific and verified use case, AWS recommends that you block all public access to your buckets. [Learn more](#)

Status: All < 1 > ⚙

	Bucket name ▼	Discovered by Access Analyzer ▼	Shared through ▼	Status ▼	Access level ▼
<input checked="" type="radio"/>	bdemobucket	2 hours ago	Access control list	Active	List, Read
<input type="radio"/>	areinventdemobucket	2 hours ago	Access control list	Active	Write
<input type="radio"/>	ademobucket	2 hours ago	Access control list, Bucket policy	Active	Write, Read, List

[Block all public access](#) [View findings](#) [Mark as active](#) [Archive](#)

Buckets with access from other AWS accounts - including third party AWS accounts (3)
These buckets are conditionally shared with other AWS accounts. To ensure that you only grant access to the intended accounts, AWS recommends that you review access to these buckets.

Status: All < 1 > ⚙

	Bucket name ▼	Discovered by Access Analyzer ▼	Shared through ▼	Status ▼	Access level ▼
<input type="radio"/>	example-destinationbucket	2 hours ago	Access control list	Active	List, Read
<input type="radio"/>	demobucket2019	2 hours ago	Access control list	Active	List, Read
<input type="radio"/>	amsterdambucket	2 hours ago	Access control list	Active	Write, Read, List

[View findings](#) [Mark as active](#) [Archive](#)

공개 액세스 식별
분석 결과 보관
원 클릭 차단
교차 계정 액세스 감사

Amazon S3 Access Points

re:Invent 2019 출시

NEW!

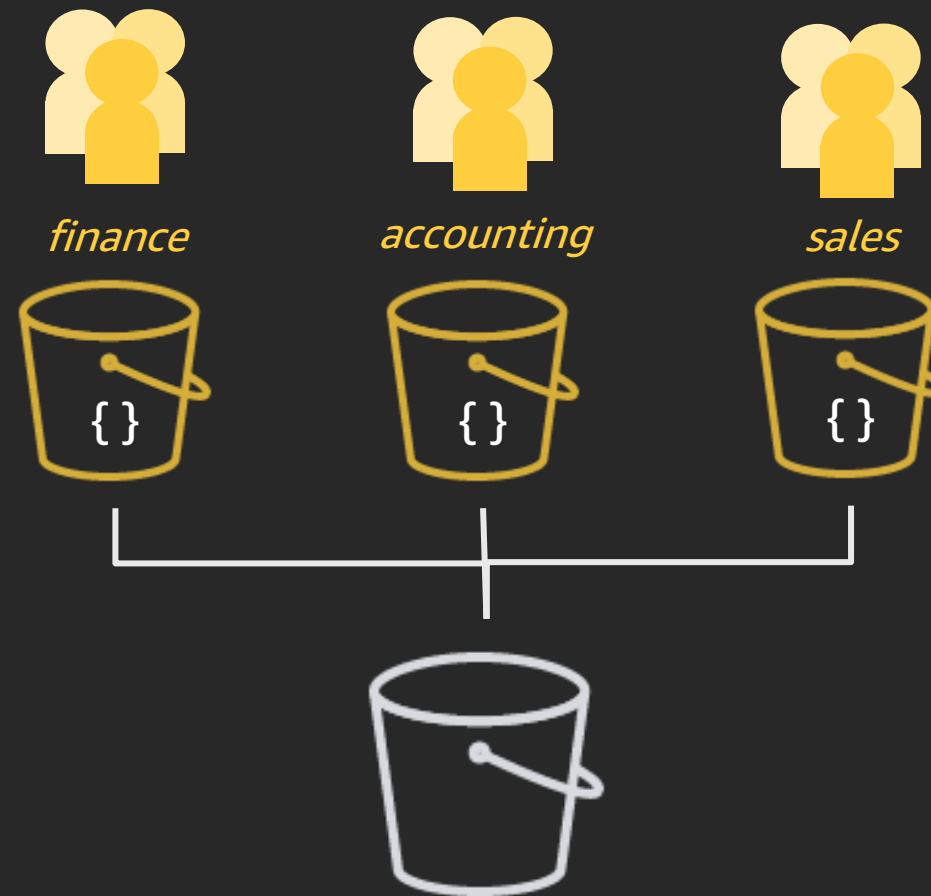


reinvent-bucket.s3.amazonaws.com

Amazon S3 Access Points

re:Invent 2019 출시

NEW!



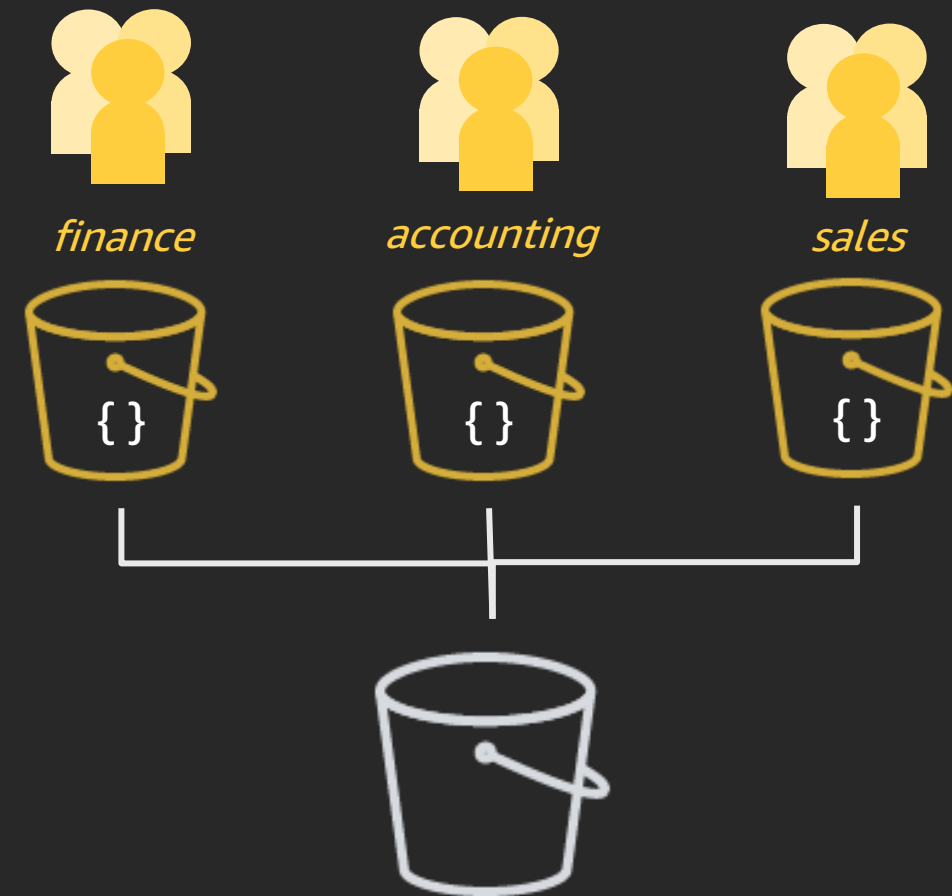
reinvent-bucket.s3.amazonaws.com

Amazon S3 Access Points

re:Invent 2019 출시

NEW!

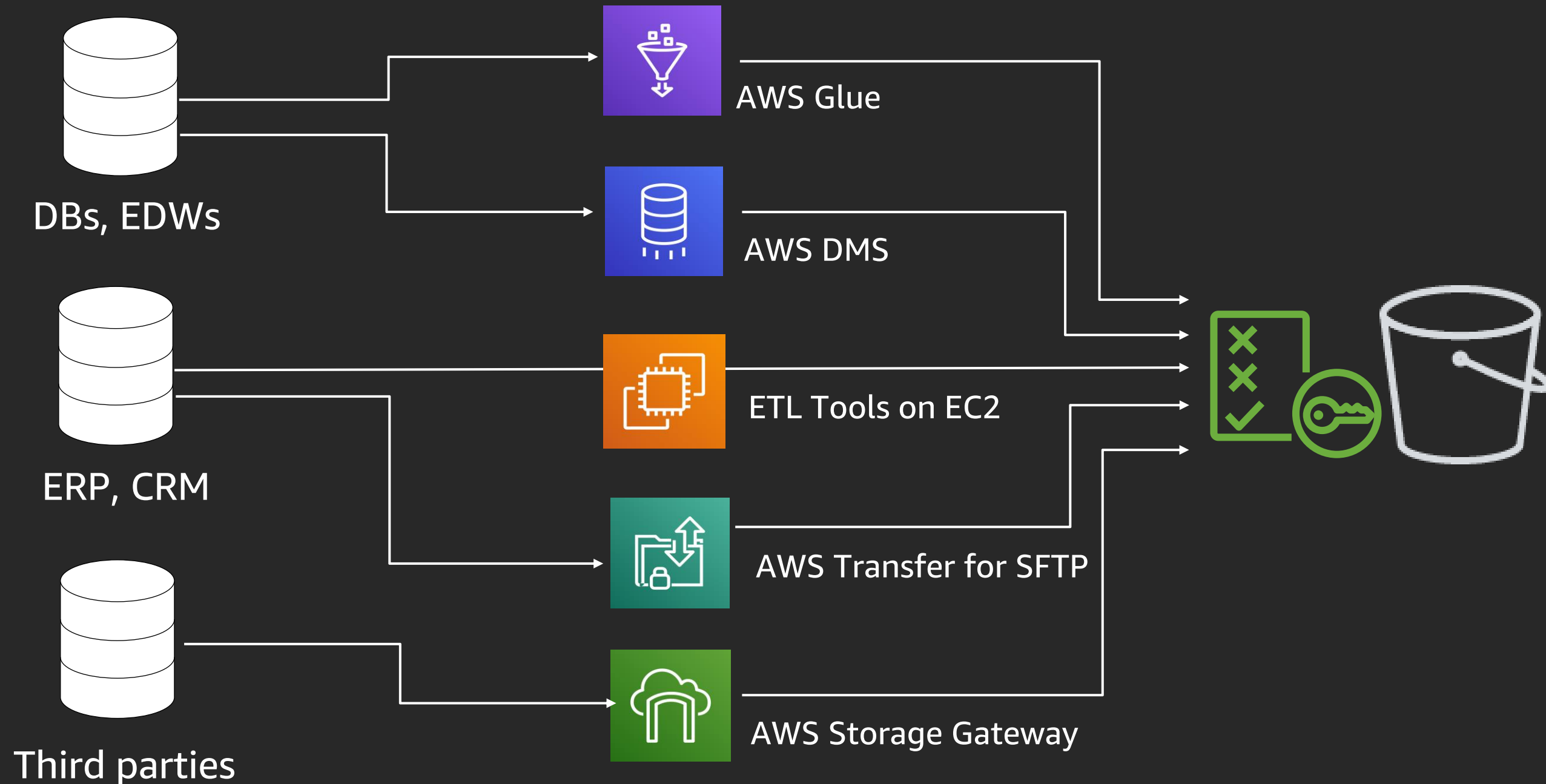
1. 공유 버킷을 통한 액세스 관리 간소화
2. 새로운 네임 스페이스 설정
3. 네트워크 트래픽을 특정 VPC로 제한



reinvent-bucket.s3.amazonaws.com

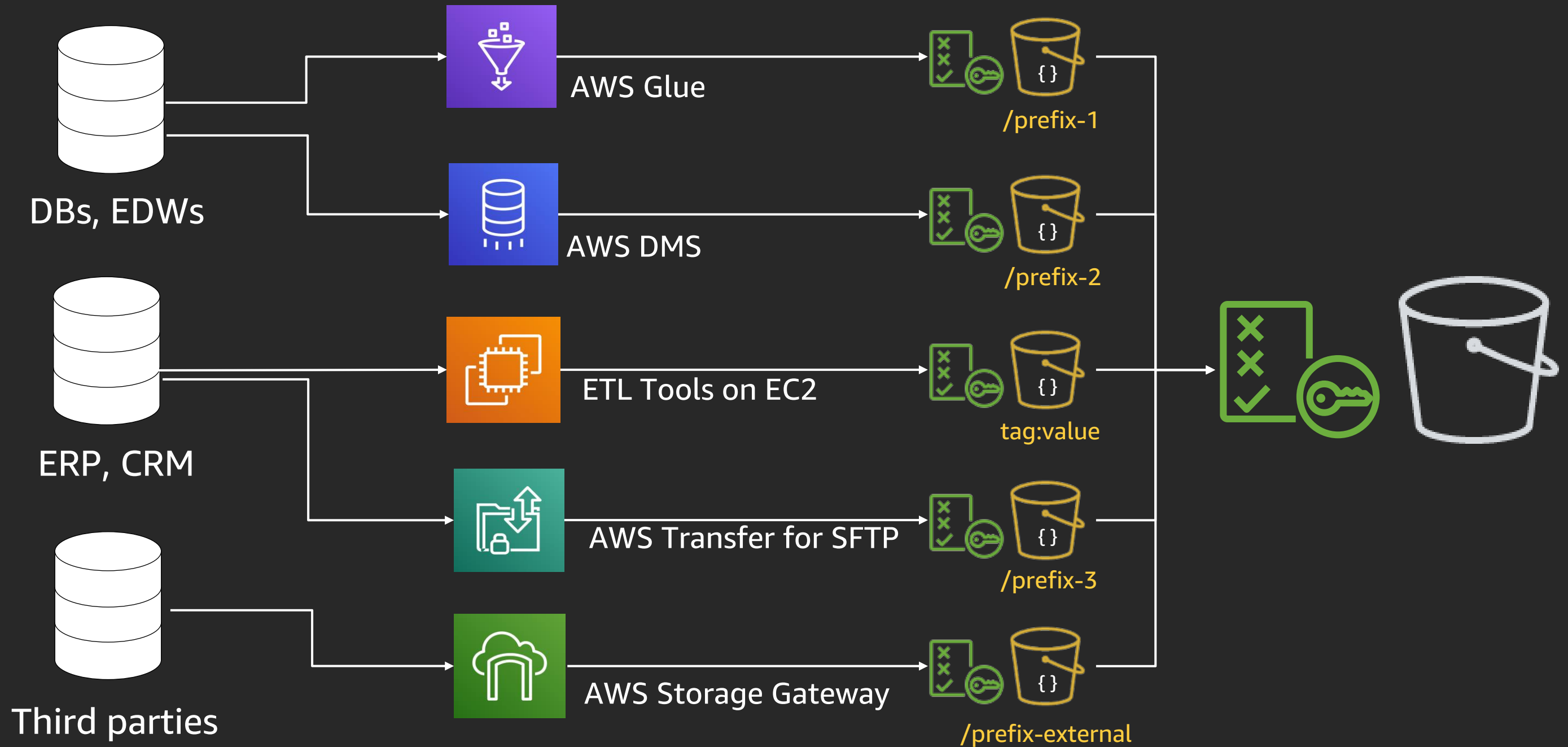
Amazon S3 Access Points

현재 - 공유 버킷에 대한 액세스 관리 : 데이터 레이크



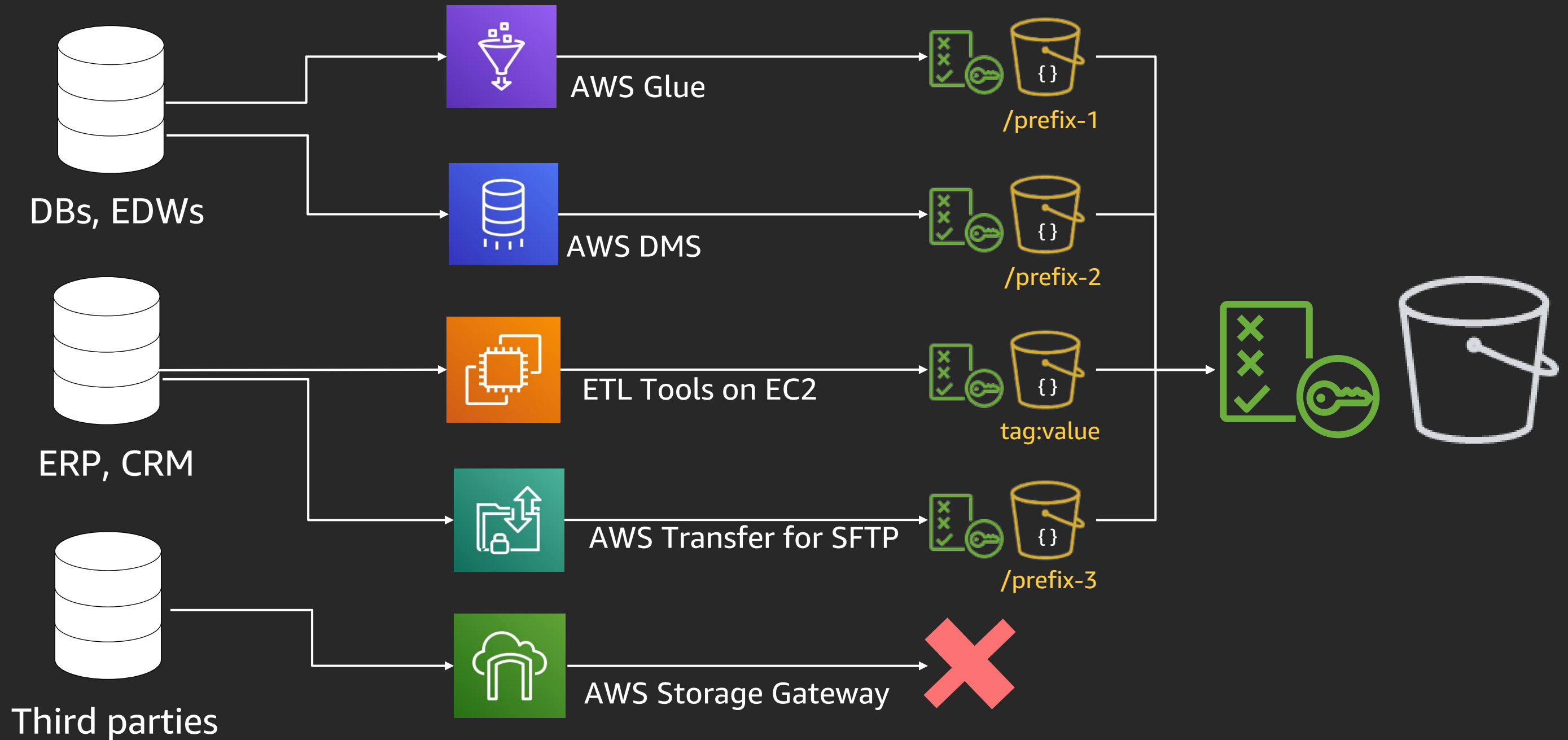
Amazon S3 Access Points

Access Points - 공유 버킷에 대한 액세스 관리 : 데이터 레이크



Amazon S3 Access Points

Access Points - 공유 버킷에 대한 액세스 관리 : 데이터 레이크



Amazon S3 Access Points

계정 및 지역 네임스페이스

ACCESS POINTS를 위한 새로운 이름 규칙

my-ap-123456789.s3-accesspoint.us-west-2.amazonaws.com



Name

AWS account

New subdomain

Region

Amazon S3 Access Points

계정 및 지역 네임스페이스

`my-ap-123456789.s3-accesspoint.us-west-2.amazonaws.com`

Name

AWS account

New subdomain

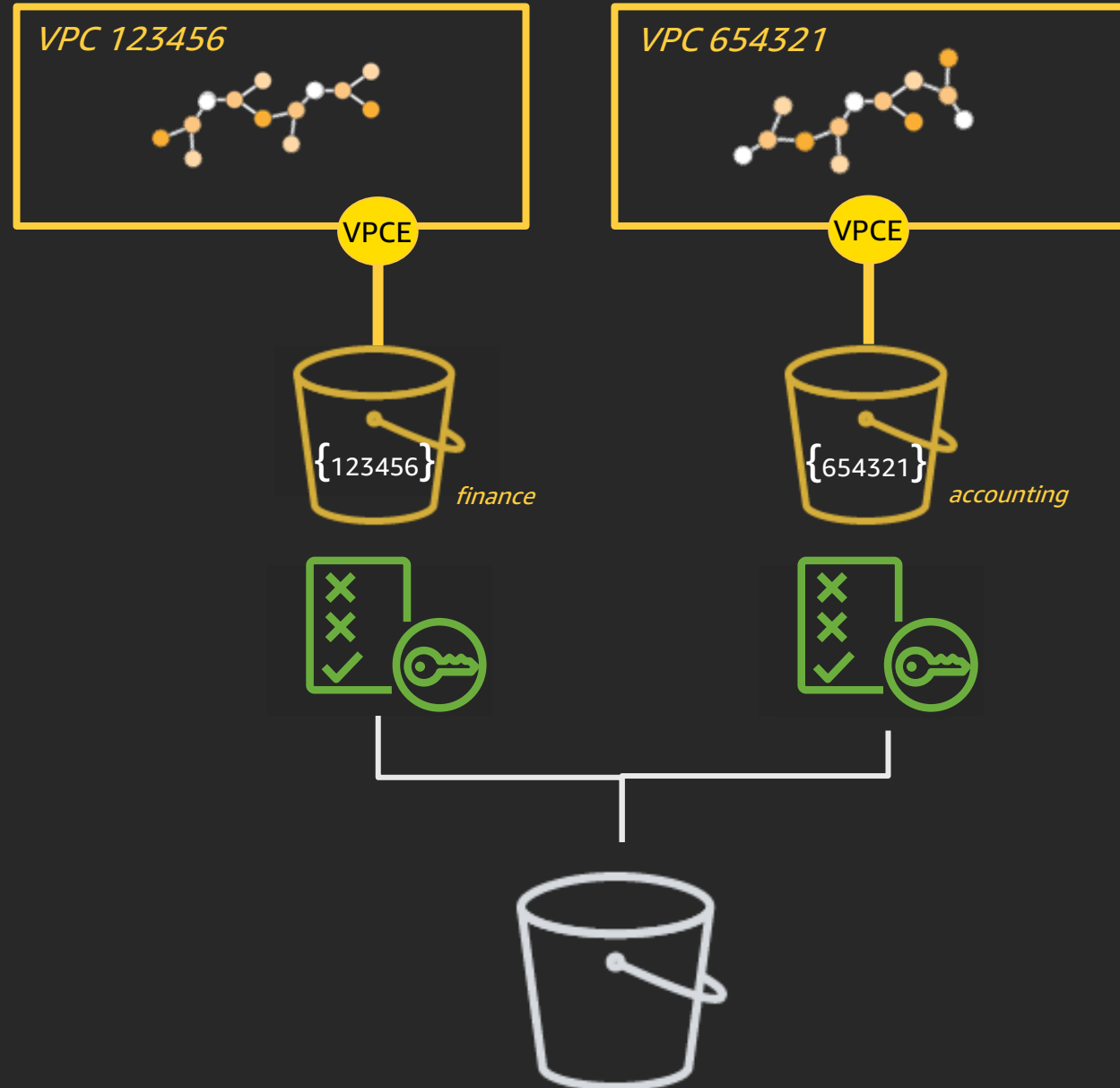
Region



- 다른 리전에서 동일 이름 재 사용 가능
- 원하는 이름 생성 가능 보장
- 계정 당 최대 1,000 개의 액세스 포인트 생성

Amazon S3 Access Points

Access Points - VPC 바인딩



reinvent-bucket.s3.amazonaws.com

type:vpc

Amazon S3 > ademobucket > Create access point

Create access point

Region
Asia Pacific (Singapore)
Region is determined by bucket location

Access point name

Access point names must be unique within the account for this Region, and comply with the [rules for](#)

Network access type

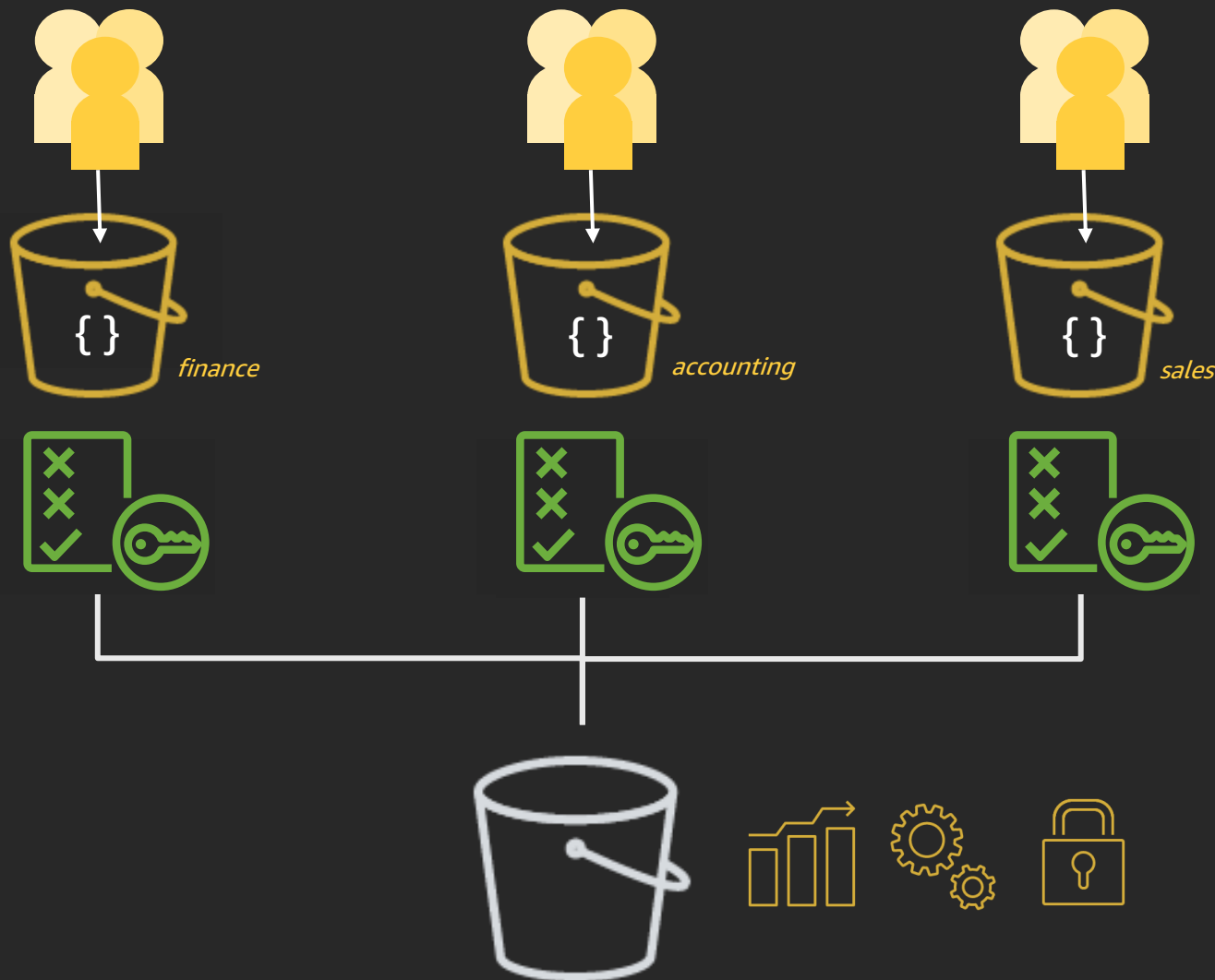
☐ Virtual private cloud (VPC)
No internet access. Requests are made over a specified VPC only.

☒ Internet

- 버킷 접근을 VPC만 가능하도록 설정
- 버킷에 대한 직접 데이터 액세스 비활성화
- VPC endpoint 정책과 동시 적용

Amazon S3 Access Points

요약



접근 대상을 여러 그룹으로 세분화

데이터 레이크 & 멀티 테넌트 환경 유용

각 그룹은 자신의 액세스 포인트 소유

계정 및 리전 액세스 포인트를 VPC 로 바인딩 가능

Access point 별 정책 적용 가능

Access Point를 사용하는 그룹에 권한 및 액세스 설정 가능

중앙 집중식 제어 유지

다양한 Access Points 가지지만, 스토리지 관리를 위한 정책 유지

Amazon S3 Access Points

동작원리

Amazon S3 > ademobucket

ademobucket

Overview

Properties

Permissions

Management

Access points

Access points can be used to provide access to your bucket. The S3 console doesn't support using virtual private cloud (VPC) access points to access bucket resources. To access bucket resources from a VPC access point, you'll need to use the AWS CLI, AWS SDK, or Amazon S3 REST API. [Learn more](#)

Search by name

+ Create access point

Use this access point

Edit access point policy

Delete

Viewing 1 to 9

Name	Network access type	Access
<input type="radio"/> accounting	Internet	Bucket and objects not public
<input checked="" type="radio"/> development	Internet	Bucket and objects not public
<input type="radio"/> finance	Internet	Bucket and objects not public
<input type="radio"/> marketing	Internet	Bucket and objects not public
<input type="radio"/> product	Internet	Bucket and objects not public
<input type="radio"/> program	Internet	Bucket and objects not public
<input type="radio"/> sales	Internet	Bucket and objects not public
<input type="radio"/> support	Internet	Bucket and objects not public
<input type="radio"/> test	Internet	Bucket and objects not public

Amazon S3 Access Points

작동방식

Amazon S3 > ademobucket

Access point: development

ademobucket

Overview

✔ You are now using access point: development

Your access to this bucket's resources is determined by the access point configuration.

To view bucket properties, permissions and management, choose **Exit access point**.

Exit access point

🔍 Type a prefix and press Enter to search. Press ESC to clear. You can also search for tags by typing in a tag key name.

📁 Upload

➕ Create folder

⬇️ Download

⌵ Actions

Asia Pacific (Singapore) 🔄

Viewing 1 to 10

<input type="checkbox"/> Name ▾	Last modified ▾	Size ▾	Storage class ▾
<input type="checkbox"/> 📁 aa	--	--	--
<input type="checkbox"/> 📄 IMG_6188.CR2	Jun 17, 2019 12:34:19 PM GMT-0700	22.1 MB	One Zone-IA
<input type="checkbox"/> 📄 IMG_6189.CR2	May 6, 2019 3:39:04 PM GMT-0700	32.6 MB	One Zone-IA
<input type="checkbox"/> 📄 IMG_6190.CR2	May 6, 2019 3:39:04 PM GMT-0700	33.4 MB	One Zone-IA

Amazon S3 신규 기능

비용 절감

S3 Glacier Deep Archive
S3 Intelligent-Tiering
Access tiers in inventory reports

보안 및 접근

S3 Block Public Access
S3 Access Analyzer
S3 Access Points

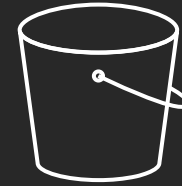
데이터 관리

S3 Batch Operations

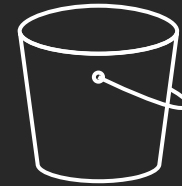
2019년 4월 출시



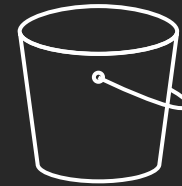
태그 교체



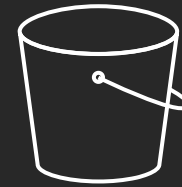
액세스 제어 변경



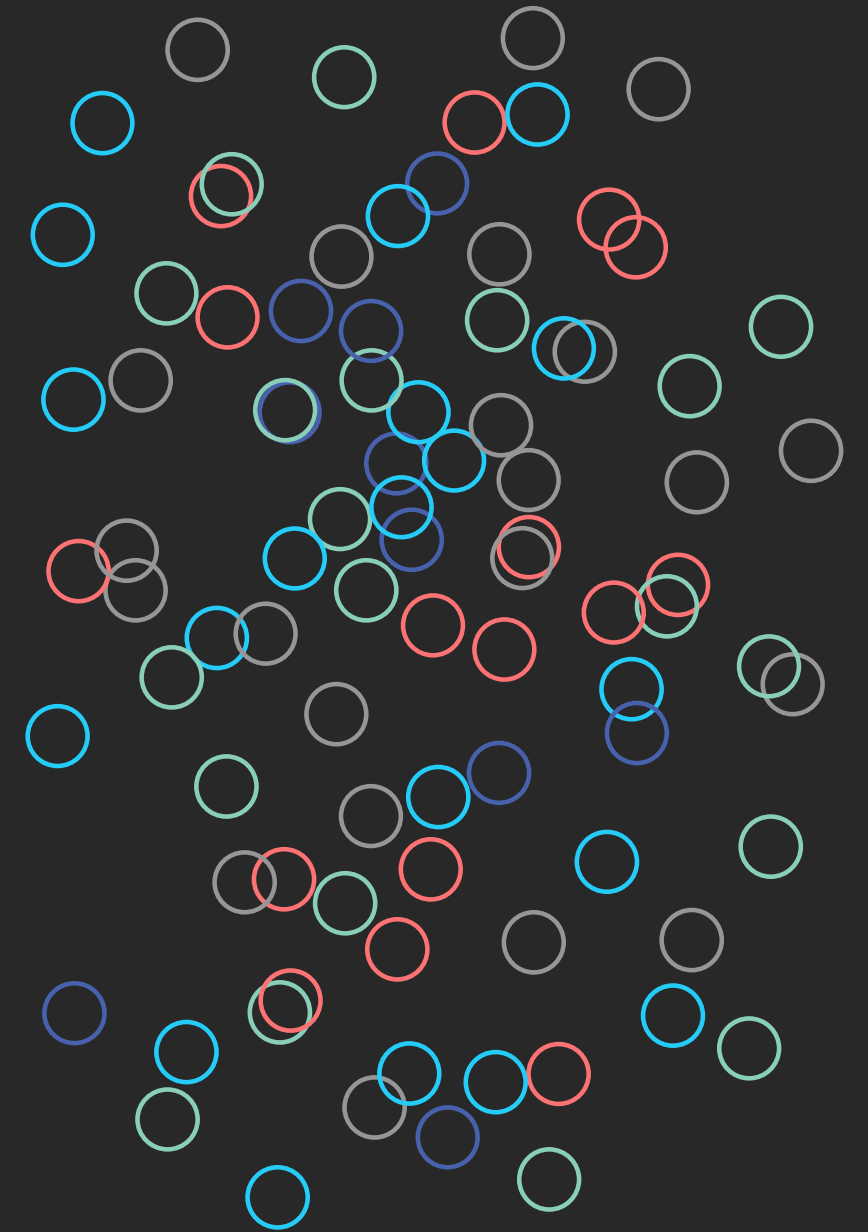
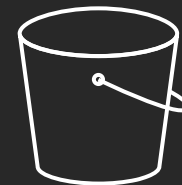
Amazon S3 Glacier
에서 객체 복구



객체 복사



Lambda 실행



S3 Batch Operations

2019년 4월 출시



태그 교체



액세스 제어 변경



Amazon S3 Glacier
에서 객체 복구



객체 복사



Lambda 실행



S3 Batch Operations

대규모 관리

Amazon S3

Buckets

Batch operations

Block public access (account settings)

Feature spotlight

S3 batch operations

A job is used to execute batch operations on a list of S3 objects. The list of S3 objects is contained in a manifest object, which can be an S3 inventory report or a list of objects that you generate. After the total number of objects listed in the manifest has been confirmed, the job status will update to *Awaiting your confirmation*, and you must **Confirm and run** the job within 14 days. Job events are published to [CloudWatch Events](#). Jobs are deleted 90 days after they finish. [Learn more](#)

Search by job ID or description

Status: All

Region: US West (Oregon)

+ Create job

Clone job

Update priority

Confirm and run

Cancel job

Viewing 1 to 18 of 18 jobs

Job ID	Description	Operation	Date created	Status	Total objects	% Complete	Total failed (rate)	Priority
a4b72a5b-60b2-491d-b388-783ba9168aab	2019-11-13 Copy	PUT copy	Nov 13, 2019 3:00:53 PM GMT-0800	Completing	338	100%	3 (< 1%)	19
6b8e8ded-7ae3-4b01-af7e-6d279b02eea7	2019-11-13 Copy	PUT copy	Nov 13, 2019 2:58:50 PM GMT-0800	Complete	338	100%	0 (0%)	1
7152f667-0a25-4f38-af4a-103beeba7b63	2019-11-13 Copy	PUT copy	Nov 13, 2019 2:49:38 PM GMT-0800	Complete	362	100%	0 (0%)	22
0b428f7f-0327-4dbd-83f7-aeb70ed680ef	2019-11-11 Set-Tags	PUT copy	Nov 11, 2019 10:41:29 AM GMT-0800	Complete	15	100%	15 (100%)	10
7349f868-3f83-4cab-a24d-f7b8f17e9154	2019-11-11 Set-Tags	PUT copy	Nov 11, 2019 10:38:00 AM GMT-0800	Complete	15	100%	15 (100%)	10
172f4ee9-2e6a-4738-884a-3cf6beb26241	2019-11-11 Set-Tags	Replace all tags	Nov 11, 2019 10:35:55 AM GMT-0800	Complete	15	100%	0 (0%)	10
09c36b73-67f0-4c52-93ab-6ebe4a52aed6	2019-11-11 Set-Tags	Replace all tags	Nov 11, 2019 8:32:56 AM GMT-0800	Complete	15	100%	0 (0%)	10
bfb144c7-d1af-4b7b-bae3-02c711632f3f	2019-11-11 Set-Tags	Replace all tags	Nov 11, 2019 8:28:43 AM GMT-0800	Failed	0	0%	0 (0%)	10

내 데이터로 무엇을
했습니까?

작업 상태는
어떻습니까?

내 작업은 얼마나
성공 했습니까?

S3 Batch Operations

대규모 관리

Total objects ⓘ ▼	% Complete ▼	Total failed (rate) ⓘ ▼
338	100%	3 (< 1%)
338	100%	0 (0%)
362	100%	0 (0%)
15	100%	15 (100%)
15	100%	15 (100%)
15	100%	0 (0%)
15	100%	0 (0%)
0	0%	0 (0%)

Completion report

Generate completion report

Yes

Completion report scope

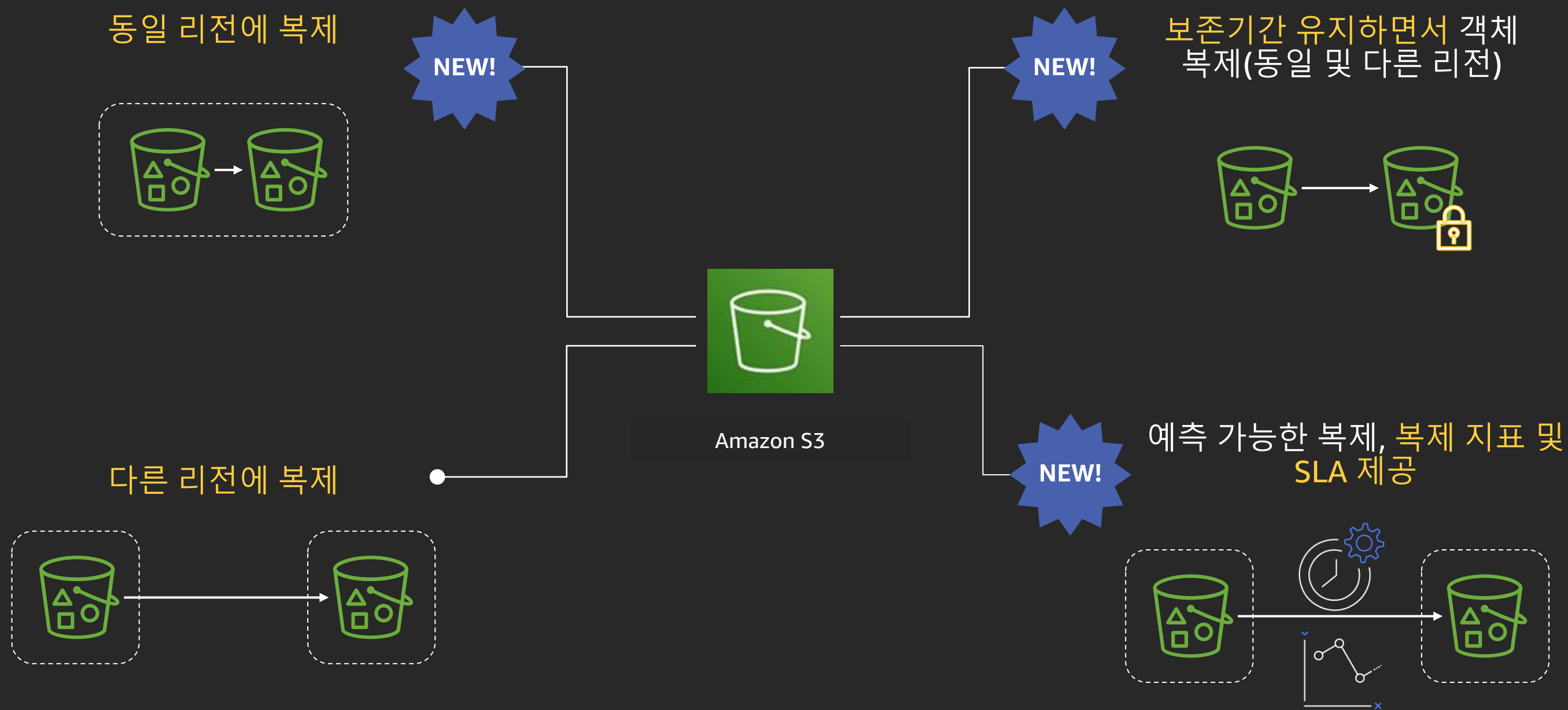
All tasks

Completion report destination

s3://oregon-inventory-reports/batch-operations/bops-report

pmeighan-6	small-objects/small-object-15452653113-2.txt	failed	403 AccessDenied	Acc
pmeighan-6	small-objects/small-object-1545265383-2.txt	failed	403 AccessDenied	Acc
pmeighan-6	small-objects/small-object-154565387-4.txt	failed	403 AccessDenied	Acc

S3 replication



S3 Same-Region replication

리전 내 자동 비동기 복제

NEW!

Amazon S3 > paul-demo-oregon

Overview Properties Permissions Management

Lifecycle Replication Analytics Metrics Inventory

✓ Replication configuration updated successfully.

Source	Destination
Bucket paul-demo-oregon	Bucket paul-demo-replica-oregon
Region US West (Oregon)	Region US West (Oregon)

+ Add rule Edit priorities Edit Delete Actions

Rule name	Scope	Storage class	Replicated
Replicate to Deep Archive	Entire bucket	Glacier Deep Archive	Same as source

데이터 선택

전체 버킷 복제
...또는 prefix 기반
...또는 태그 기반

동일 복사본

두번째 복사본 생성
데이터 변경에 따른 연속 복제
자동으로 모든 객체의 모든 버전을 유지

소유권 변경

복제본 객체에서 ACL을 자동으로 변경
객체 수준 권한 재 설정
실수로 데이터를 삭제 하지 못하도록 보호

크로스 어카운트

다른 계정으로 복제
“아카이브” account 로 복제
AWS 루트 계정 손상으로부터 보호

스토리지 클래스
설정

엔터프라이즈급 스토리지 복제 기능 제공
...또는 동일 클래스 / S3 Standard IA 복제
...또는 S3 Glacier로 바로 복제

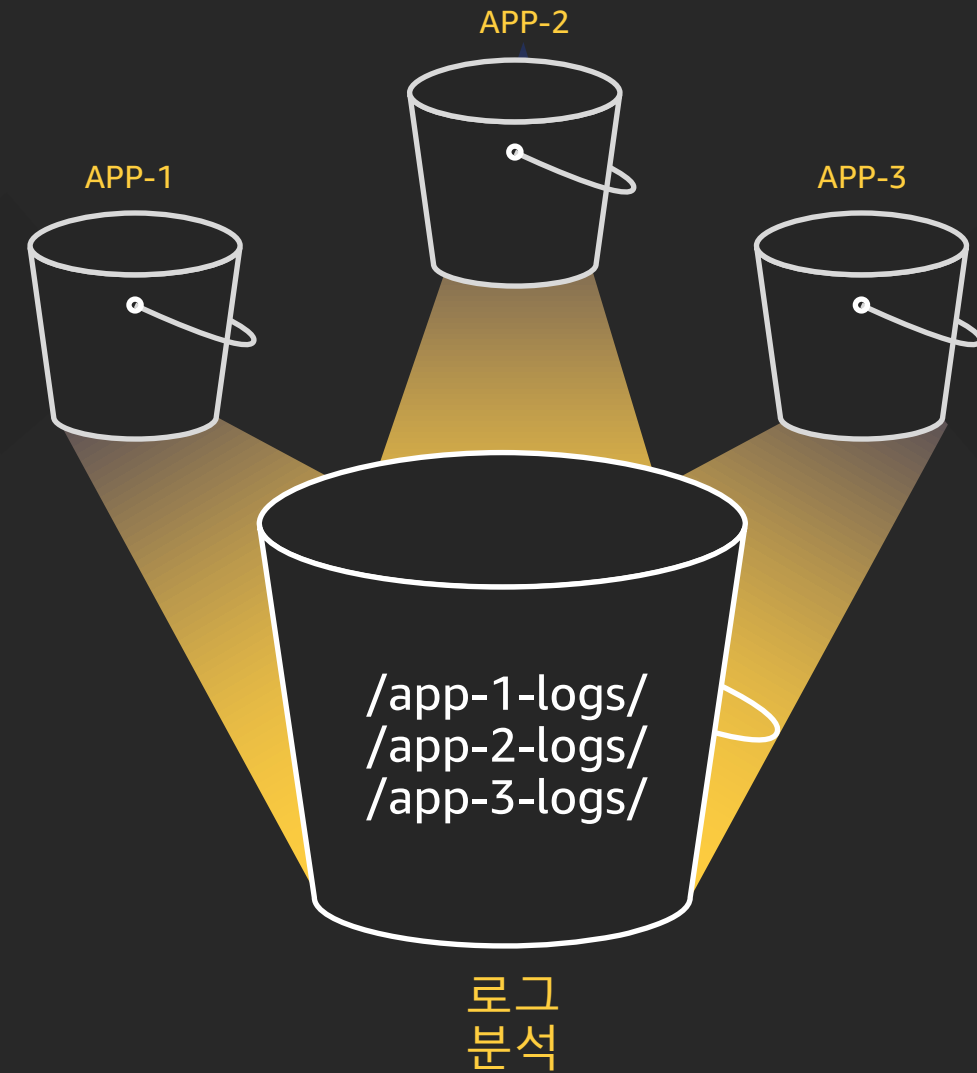
S3 Same-Region replication

리전 내 자동 비동기 복제

NEW!



백업 및 휴먼 에러 보호

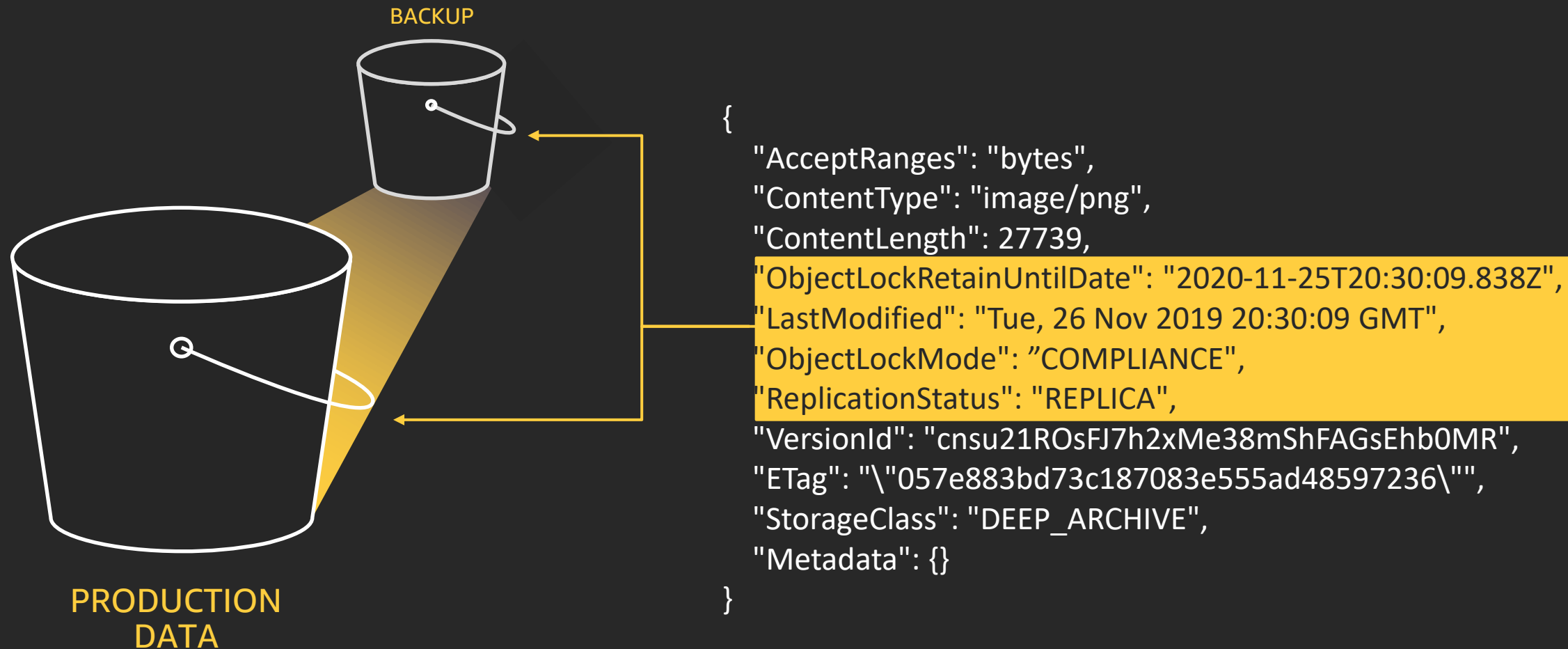


LOG 집계

S3 retention control replication

NEW!

여러 사본에 보존 기간 동기화



Amazon S3 replication time control

15분 내 예측 가능한 데이터 복제

NEW!



예측 가능한
복제 시간



Amazon S3 Service
Level Agreement (SLA)
지원



Amazon CloudWatch
메트릭 및 이벤트
통보를 이용한
복제 모니터링 제공

Amazon S3 replication time control

15분 내 예측 가능한 데이터 복제

NEW!

Replication rule

1 Set source

2 Set destination

3 Configure rule options

4 Review

You can replicate objects across buckets in different AWS Regions (cross-Region replication) or you can replicate objects across buckets in the same AWS Region (same-Region replication). [Learn more](#) or see [Amazon S3 pricing](#)

pmeighan-2

Destination options

Storage class

☐ Change the storage class for the replicated objects

Choose a storage class based on your use case and access requirements. There are **per-request fees** when replicating data to any S3 or S3 Glacier storage class. [Learn more](#) or see [Amazon S3 pricing](#)

Object ownership

☐ Change object ownership to destination bucket owner

Replication time control settings

☒ S3 Replication Time Control

Replication Time Control replicates 99.99% of your new objects within 15 minutes. Additional per-GB Data Transfer fees and CloudWatch metrics fees apply. [Learn more](#)

Previous

Next

Overview

Properties

Permissions

Management

Lifecycle

Replication

Analytics

Metrics

Inventory

Source	Destination	Permissions	Edit global settings
Bucket pmeighan-1	Bucket pmeighan-2	IAM role s3crr_role_for_pmeighan-1_to_pmeighan-2	
Region US East (Ohio)	Region US West (Oregon)	Bucket policy Copy	

+ Add rule

Edit priorities

Edit

Delete

Actions

Viewing 1 to 1 of 1							
Rule name	Scope	Storage class	Replicated object owner	KMS-encrypted objects	Status	Replication time control	Priority
<input type="radio"/> whole-bucket-pmeighan-2	Entire bucket	Same as source	Same as source bucket	Do not replicate	Enabled	Enabled	1

Amazon S3 replication time control

높은 수준의 예측 가능한 복제 시간

NEW!

복제 완료

15

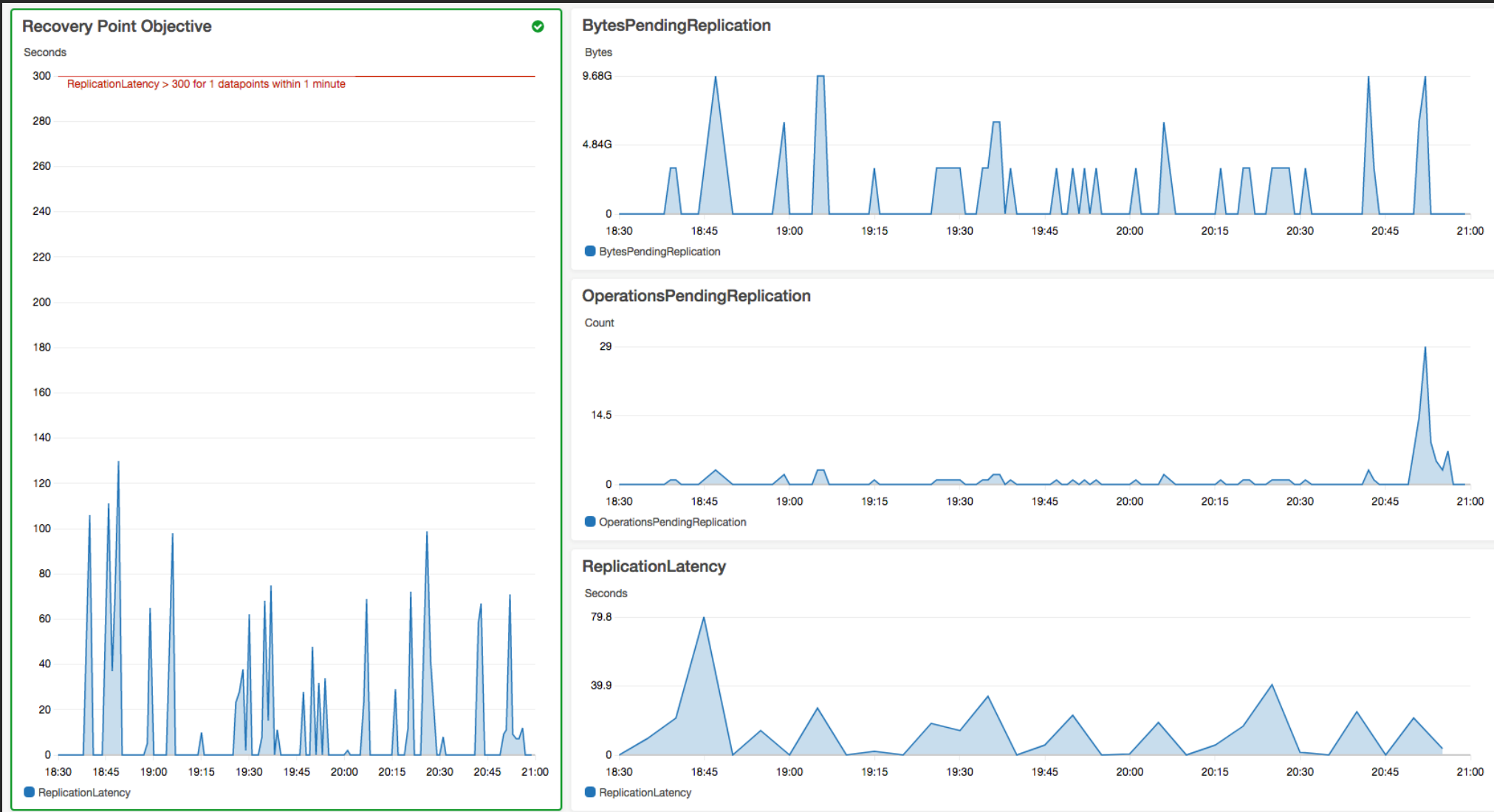
분
혹은 내

99.9% 모든 객체의
AWS SLA 지원

Amazon S3 replication time control

복제 프로세스에 대한 가시성

NEW!



보류중인 복제 양(Bytes)

설정된 복제 규칙에 대해 복제 보류중인 객체의 총 바이트 수

보류중인 복제 작업

설정된 복제 규칙에 대해 복제 보류중인 작업 수

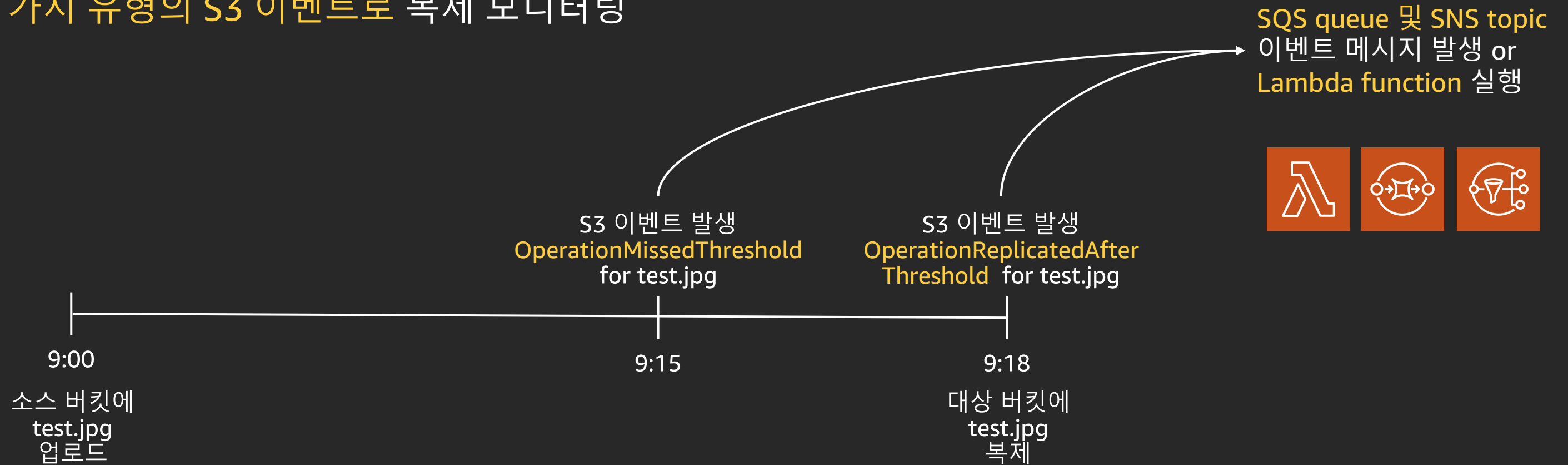
복제 대기 시간

설정된 복제 규칙에 대해 대상 리전이 소스 리전 보다 지연된 최대 시간

Amazon S3 replication time control

NEW!

3 가지 유형의 S3 이벤트로 복제 모니터링



Amazon S3 신규 기능

비용 절감

- S3 Glacier Deep Archive
- S3 Intelligent-Tiering
- Access tiers in inventory reports

보안 및 접근

- S3 Block Public Access
- S3 Access Analyzer
- S3 Access Points

데이터 관리

- S3 Batch Operations
- S3 Same-Region replication
- S3 replication time control

여러분의 소중한 피드백을 기다립니다!
강연 평가 및 설문 조사에 참여해 주세요.

감사합니다