

Lab1. Using CloudWatch & CloudTrail

목적

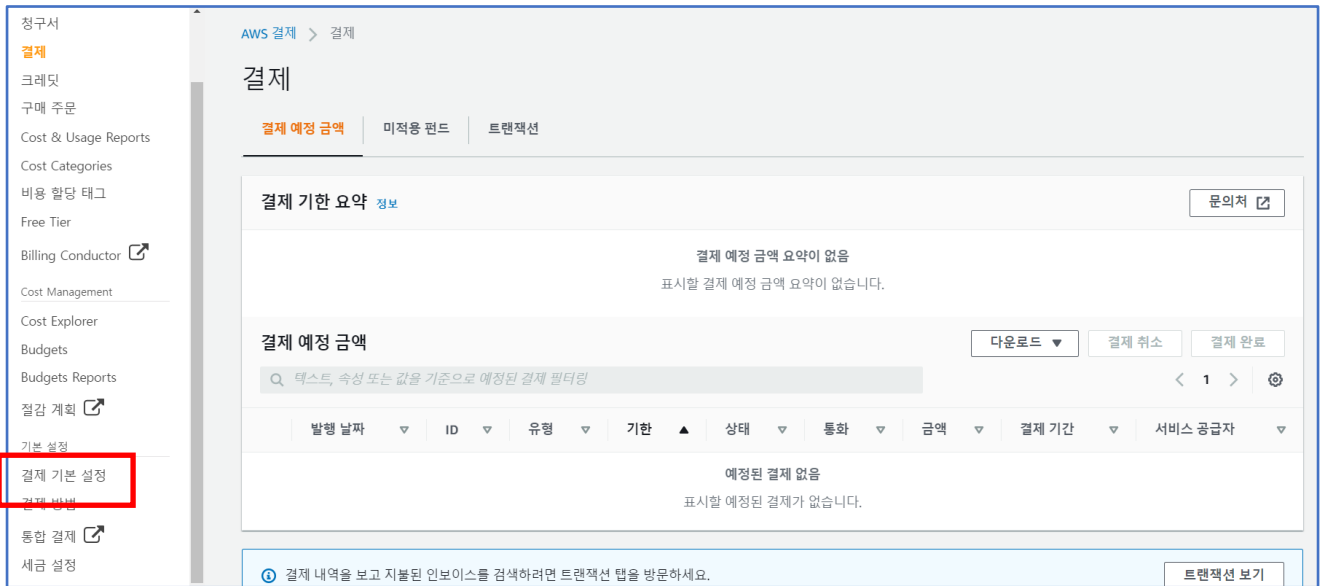
이번 실습에서는 Amazon CloudWatch의 사용을 보여준다. 시나리오에서는 CloudWatch 콘솔을 사용하여 AWS 사용량을 추적하고 특정 지출 임계값을 초과했을 때 이를 알려 주는 결제 경보를 생성할 것이다. 또한 2번째 시나리오에서는 AWS CloudTrail을 사용하는 실습을 한다. CloudTrail 콘솔에서 최근 AWS 계정 활동을 검토하고 이벤트를 조사한다. 그런 다음, 추적을 생성한다. 추적은 Amazon S3 버킷에 저장되는 관리 이벤트 활동의 지속적인 레코드이다. 이벤트 기록과는 달리, 이 지속적인 레코드는 90일로 제한되지 않고, 모든 AWS 리전에서 이벤트를 로그하며, 시간 경과에 따른 보안 및 감사 요구를 충족하는 데 도움이 될 수 있다.

사전 준비물

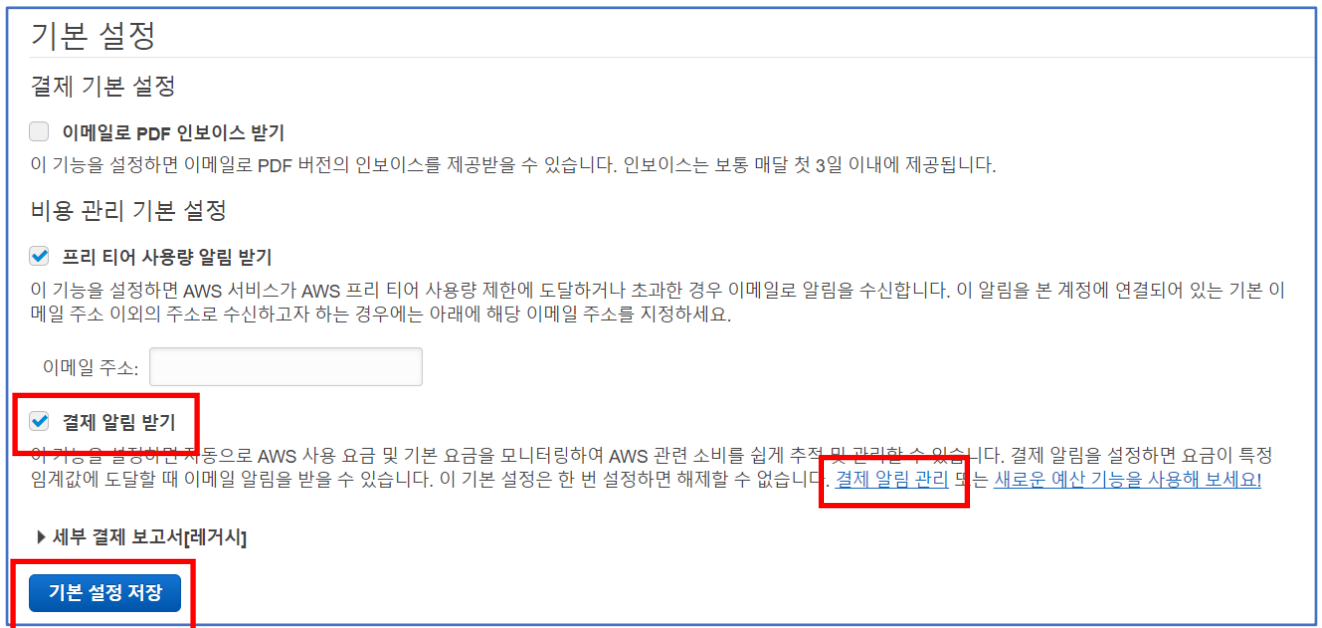
AWS Free-Tier 계정

CloudWatch 경보 생성하기

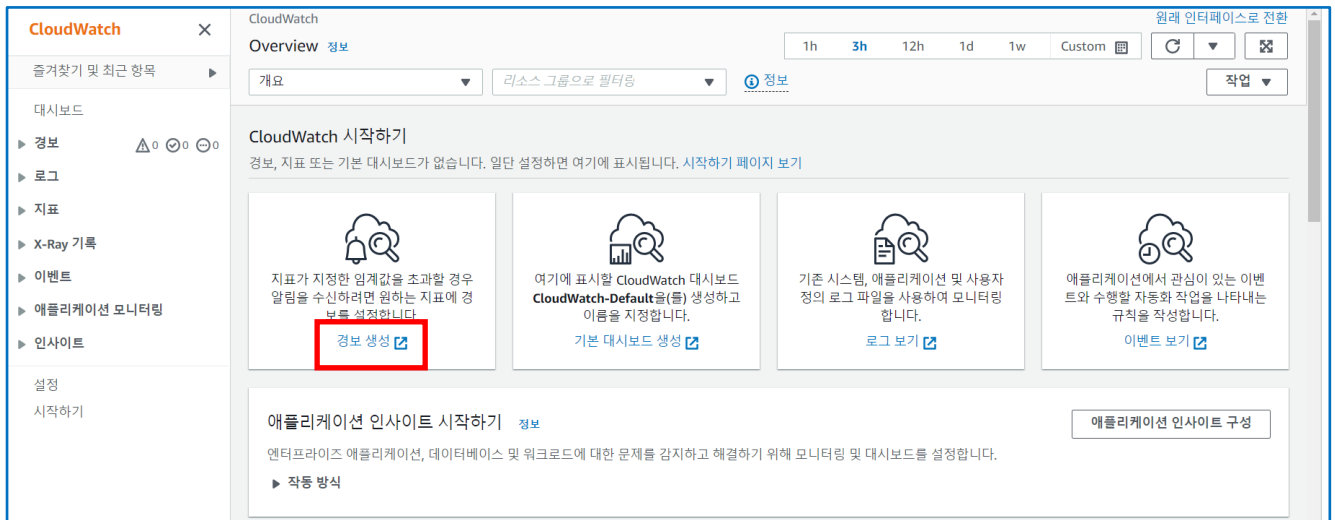
1. 로그인 후 [결제 대시보드] > [기본 설정] > [결제 기본 설정] 메뉴를 선택한다.



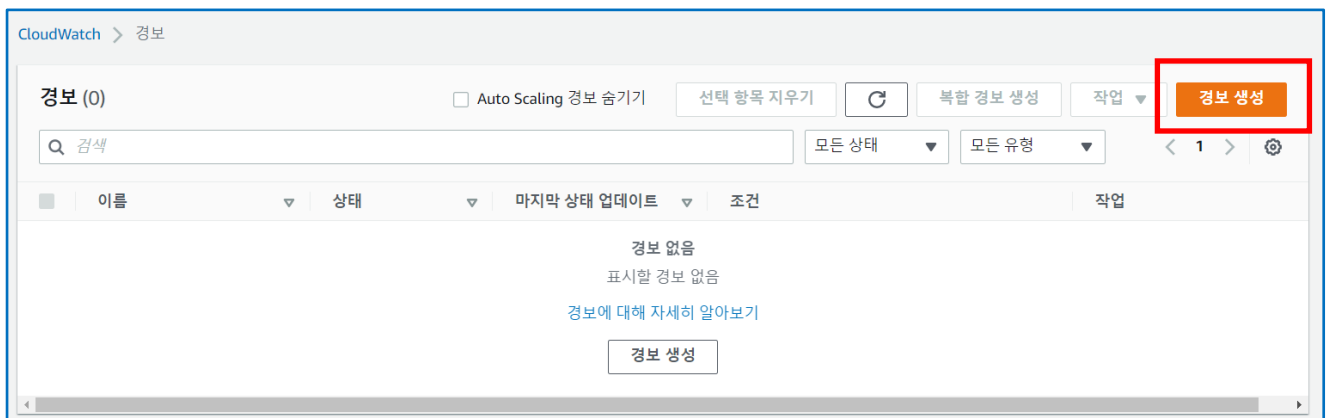
2. [기본 설정] 페이지에서 [결제 알림 받기]를 체크하고, [기본 설정 저장] 버튼을 클릭한다. 그리고 [결제 알림 관리] 링크를 클릭한다.



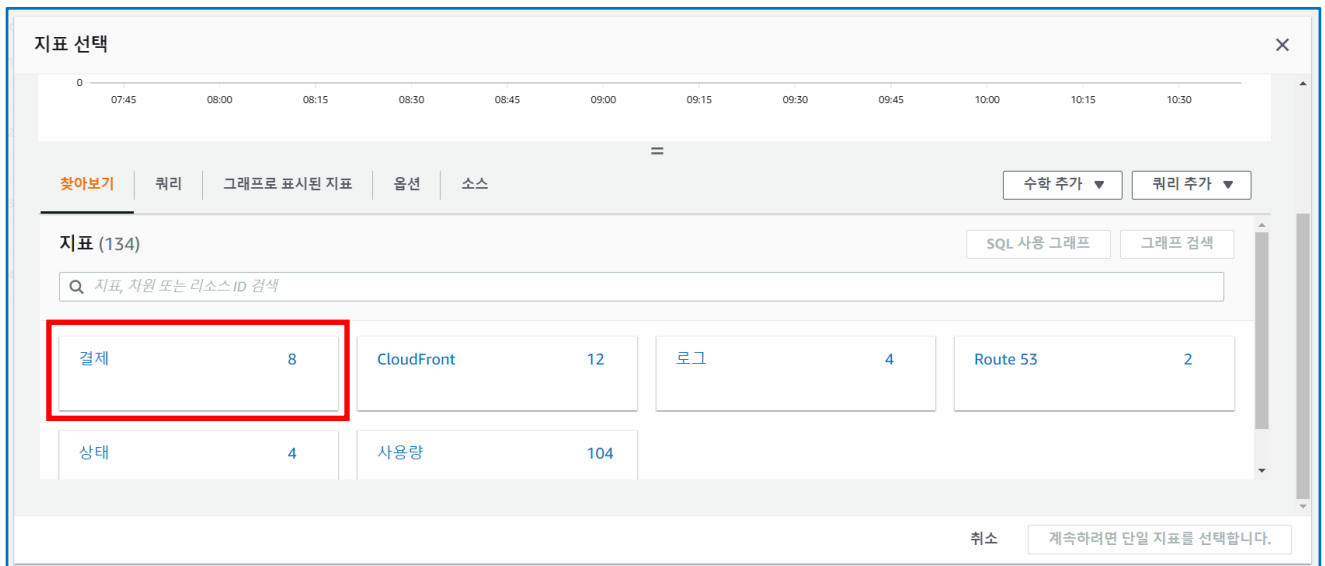
3. **[CloudWatch]** 페이지로 이동했다. **결제 알림**을 활성화했으면 **결제 경보**를 생성할 수 있다. 이 실습에서는 AWS에 대한 예상 요금이 지정된 임계값을 초과할 때 이메일 메시지를 전송하는 경보를 생성한다. **[CloudWatch 시작하기]** 섹션에서 **[경보 생성]**을 클릭한다.



4. **[경보]** 페이지에서, **[경보 생성]** 버튼을 클릭한다.



5. **[지표 선택]** 페이지이다. **[지표]** 섹션에서 **[결제]**를 클릭한다.



6. [예상 요금 합계]를 클릭한다.

지표 (8)

모두 > 결제 Q 지표, 자원 또는 리소스 ID 검색

서비스별	7	예상 요금 합계	1
------	---	----------	---

7. [EstimatedCharges] 항목의 왼쪽의 USD를 체크한 후, [지표 선택] 버튼을 클릭한다.

지표 선택

07:00 07:15 07:30 07:45 08:00 08:15 08:30 08:45 09:00 09:15 09:30 09:45 10:00

EstimatedCharges

찾아보기 쿼리 그래프로 표시된 지표(1) 옵션 소스 수학 추가 쿼리 추가

지표 (1) SQL 사용 그래프 그래프 검색

모두 > 결제 > 예상 요금 합계 Q 지표, 자원 또는 리소스 ID 검색

<input checked="" type="checkbox"/> 통화 (Currency) (1)	지표 이름
<input checked="" type="checkbox"/> USD	EstimatedCharges

취소 지표 선택

8. 먼저 리전을 [아시아 태평양 (서울)]로 변경하고, [지표 이름]이 EstimatedCharges임을 확인하고 페이지를 스크롤다운한다.

지표 및 조건 지정

지표 편집

그래프

이 정보는 6 시간 내 1개의 데이터 포인트에 대해 파란색 줄이 빨간색 줄을 초과할 때 트리거됩니다.

1 0.8 0.6 0.4 0.2 0

05/28 05/30 05/31 06/02

EstimatedCharges

네임스페이스 AWS/Billing

지표 이름 EstimatedCharges

Currency USD

통계 Q 최대 X

기간 6시간

9. 다음과 같이 설정 후, [다음] 버튼을 클릭한다. 즉 해당 월 총 요금이 다음을 초과할 때마다 알림을 설정하는 것이다. 이번 실습에서는 임계값을 200 달러로 설정한다.

조건

임계값 유형

☒ 정적
값을 임계값으로 사용

☐ 이상 탐지
대역을 임계값으로 사용

EstimatedCharges이(가) 다음과 같은 경우에 항상...
경보 조건을 정의합니다.

☒ 보다 큼
> 임계값

☐ 보다 크거나 같음
≥ 임계값

☐ 보다 작거나 같음
≤ 임계값

☐ 보다 작음
< 임계값

...보다
임계값을 정의합니다.

USD

숫자여야 함

▶ 추가 구성

취소 다음

10. [단계 2 작업 구성] 페이지에서, [다음 SNS 주제에 알림을 보냅니다]에서는 [기존 SNS 주제 선택]을 선택하고 [다음으로 알림 전송]은 이메일 주소를 입력한다.

작업 구성

알림

경보 상태 트리거
이 작업을 트리거하는 경보 상태를 정의합니다.

☒ 경보 상태
지표 또는 표현식이 정의된 임계값을 벗어났습니다.

☐ 정상
지표 또는 표현식이 정의된 임계값 범위에 있습니다.

☐ 데이터 부족
경보가 방금 시작되었거나 사용 가능한 데이터가 부족합니다.

다음 SNS 주제에 알림을 보냅니다.
알림을 수신할 SNS(Simple Notification Service) 주제를 정의합니다.

☒ 기존 SNS 주제 선택

☐ 새 주제 생성

☐ 주제 ARN을 사용하여 다른 계정에 알림

다음으로 알림 전송...

X

이 계정의 이메일 목록만 사용할 수 있습니다.

이메일(엔드포인트)
henry@suwon.ac.kr - SNS 콘솔에서 보기

알림 추가

11. 페이지를 스크롤다운하여 [다음] 버튼을 클릭한다.

EC2 작업

이 작업은 EC2 인스턴스별 지표에 대해서만 사용할 수 있습니다.

EC2 작업 추가

Systems Manager 작업 정보

이 작업을 수행하면 경보가 경고 상태 상태일 때 Systems Manager에서 인시던트 또는 Opsitem을 생성합니다.

Systems Manager 작업 추가

취소 이전 **다음**

12. [단계 3 이름 및 설명 추가]에서 [경보 이름]을 lab-myalarm이라고 입력하고 [다음] 버튼을 클릭한다.

CloudWatch > 경고 > 경고 생성

단계 1
지표 및 조건 지정

단계 2
작업 구성

단계 3
이름 및 설명 추가

단계 4
미리 보기 및 생성

이름 및 설명 추가

경보 이름

lab-myalarm

경보 설명 - 선택 사항

경보 설명

최대 1024자(0/1024)

취소 이전 **다음**

13. [경고]가 성공적으로 생성되었다.

CloudWatch > 경고

경고 (1)

☐ Auto Scaling 경고 숨기기

선택 항목 지우기

복합 경고 생성

작업

경고 생성

검색

모든 상태

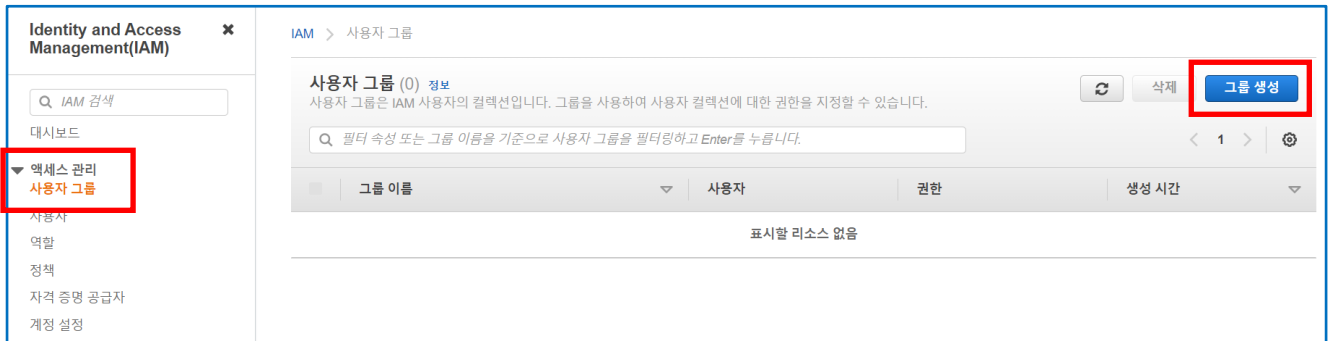
모든 유형

< 1 >

<input type="checkbox"/>	이름	상태	마지막 상태 업데이트	조건	작업
<input type="checkbox"/>	lab-myalarm	데이터 부족	2022-06-04 20:05:55	6 시간 내 1개의 데이터 포인트에 대한 EstimatedCharges > 200	작업이 활성화됨

CloudTrail 사용하기

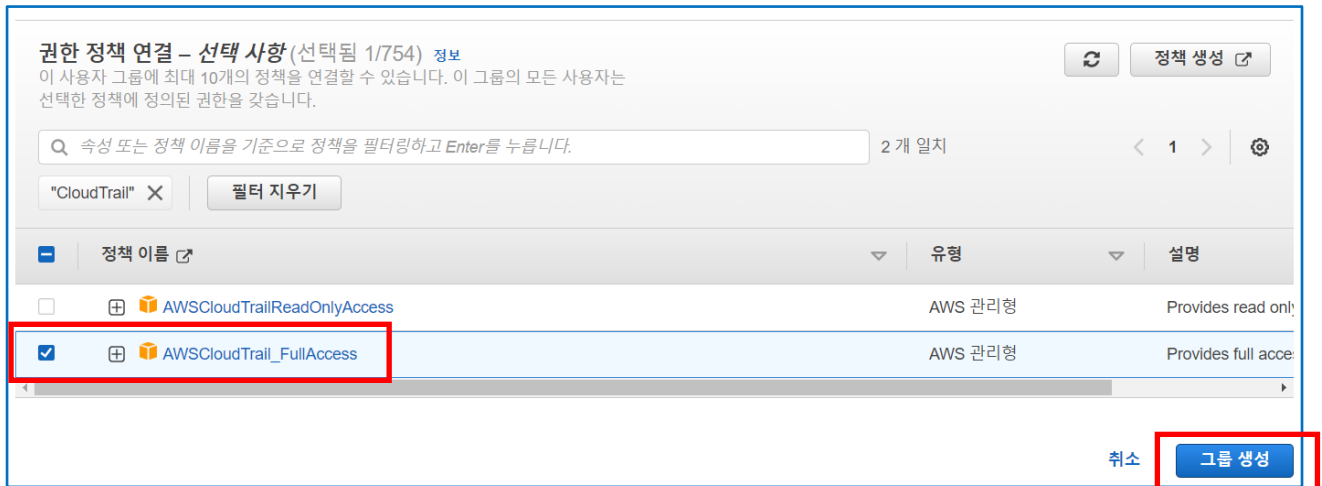
1. 사용자가 **CloudTrail** 추적을 관리할 수 있게 하려면 **IAM** 사용자에게 **CloudTrail** 작업과 연결된 작업을 수행할 수 있는 명시적 권한을 부여해야 한다. 일반적인 접근 방법은 적합한 권한이 있는 **IAM** 그룹을 생성한 다음, 해당 그룹에 개별 IAM 사용자를 추가하는 것이다. 예를 들어 **CloudTrail** 작업에 대한 모든 액세스 권한이 있어야 하는 사용자를 위해 **IAM** 그룹을 생성하고, 추적 정보를 볼 수 있어야 하지만 추적을 생성하거나 변경할 수는 없는 사용자를 위한 그룹을 별도로 생성할 수 있다. [서비스] > [보안, 자격 증명 및 규정 준수] > [IAM]을 클릭하여 **IAM** 페이지로 이동한다. [액세스 관리] > [사용자 그룹]을 클릭하여 [사용자 그룹] 페이지로 이동한다. 페이지 오른쪽의 [그룹 생성] 버튼을 클릭한다.



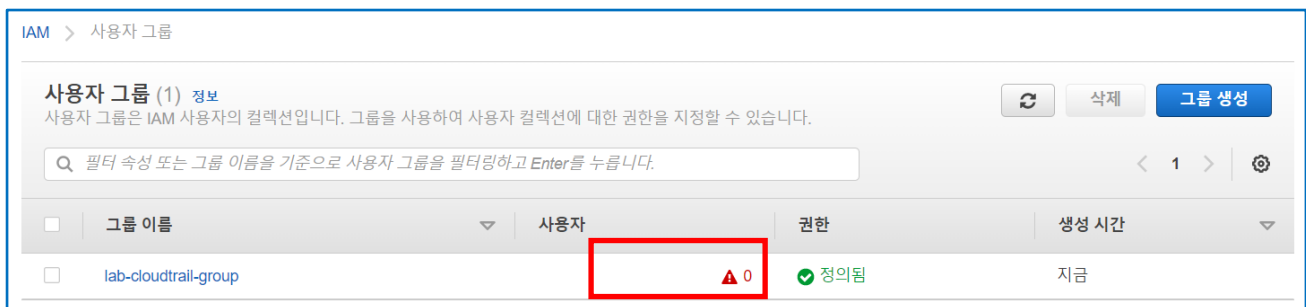
2. [사용자 그룹 생성] 페이지이다. [사용자 그룹 이름]에 lab-cloudtrail-group을 입력하고 페이지를 스크롤다운하여 [권한 정책 연결] 섹션으로 이동한다.



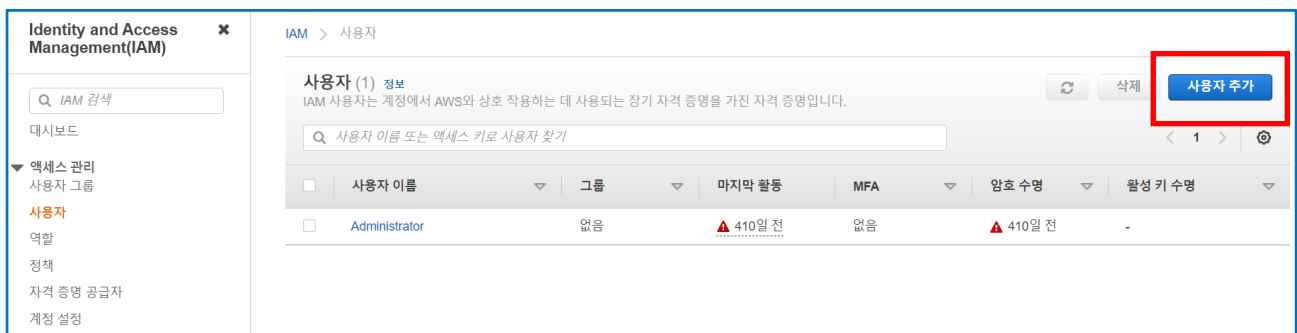
3. [권한 정책 연결] 섹션에서 **CloudTrail**에 필터링하면 2개의 정책이 나온다. **AWSCloudTrail_FullAccess**는 이 그룹의 사용자에게 **CloudTrail** 작업에 대한 모든 액세스 권한을 부여한다. 이러한 사용자는 **Amazon S3 버킷**, **CloudWatch Logs**의 **로그 그룹** 및 추적에 대한 Amazon SNS 주제를 관리할 수 있는(삭제할 수는 없음) 권한이 있다. 그 다음은 **AWSCloudTrailReadOnlyAccess**이다. 이 정책을 통해 그룹의 사용자들은 최근 이벤트 및 이벤트 기록을 포함하여 **CloudTrail** 콘솔을 확인할 수 있다. 또한 이들 사용자는 기존 추적과 버킷을 확인할 수 있다. 사용자는 이벤트 기록 파일을 다운로드할 수 있지만, 추적을 생성하거나 업데이트할 수는 없다. **AWSCloudTrail_FullAccess**를 체크하고 [그룹 생성] 버튼을 클릭한다.



4. IAM 그룹을 생성했다. 아직 해당 그룹에 사용자가 없다. 좌측 메뉴 [액세스 관리] > [사용자]를 클릭한다.



5. [사용자] 페이지에서 [사용자 추가]를 클릭한다.





6. [사용자 이름]에 lab-user라고 입력한다.


7. [AWS 자격 증명 유형 선택]에서 암호 – AWS 관리 콘솔 액세스를 체크하고, [콘솔 비밀번호]는 사용자 지정 비밀번호 Suwon#0307를 입력하고 [비밀번호 재설정 필요]는 체크해제한다. 그리고 [다음: 권한]을 클릭한다.

8. [권한 설정]에서는 그룹에 사용자 추가를, [그룹에 사용자 추가]는 위에서 생성한 **lab-cloudtrail-group**을 체크하고 [다음: 태그]를 클릭한다.

▼ 권한 설정

 그룹에 사용자 추가

 기존 사용자에서 권한 복사

 기존 정책 직접 연결

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 그룹을 사용하여 직무별로 사용자의 권한을 관리하는 것이 좋습니다. [자세히 알아보기](#)

그룹에 사용자 추가

그룹 생성

↺ 새로 고침

Q 검색

1 결과 표시

그룹	연결된 정책
<input checked="" type="checkbox"/> lab-cloudtrail-group	AWSCloudTrail_FullAccess

▶ 권한 경계 설정

취소

이전

다음: 태그

9. [태그 추가]에서 [키]는 **Name**으로, [값]은 **lab-user**로 입력하고 [다음: 검토]를 클릭한다.

태그 추가(선택 사항)

IAM 태그는 사용자 사용자에게 추가할 수 있는 키-값 페어입니다. 태그는 이메일 주소와 같은 사용자 정보를 포함하거나 정책과 같은 내용일 수 있습니다. 태그를 사용하여 이 사용자에게 대한 액세스를 구성, 추적 또는 제어할 수 있습니다. [자세히 알아보기](#)

키	값(선택 사항)	제거
<input type="text" value="Name"/>	<input type="text" value="lab-user"/>	✕

새 키 추가

49 태그를 더 추가할 수 있습니다.

취소

이전

다음: 검토

10. [검토] 페이지에서 각 값을 확인하고 [사용자 만들기]를 클릭한다.

권한 요약

위에 표시된 사용자를 다음 그룹에 추가합니다.

유형	이름
그룹	lab-cloudtrail-group

태그

새로운 사용자 에게 다음 태그가 제공됩니다

키	값
Name	lab-user

취소 이전 **사용자 만들기**

11. [사용자]가 성공적으로 생성되었다. [닫기]를 클릭한다.

✓ **성공**

아래에 표시된 사용자를 생성했습니다. 사용자 보안 자격 증명을 보고 다운로드할 수 있습니다. AWS Management Console 로그인을 위한 사용자 지침을 이메일로 보낼 수도 있습니다. 지금이 이 자격 증명을 다운로드할 수 있는 마지막 기회입니다. 하지만 언제든지 새 자격 증명을 생성할 수 있습니다.

AWS Management Console 액세스 권한이 있는 사용자가 <https://789534828835.signin.aws.amazon.com/console>에 로그인할 수 있습니다.

📄 .csv 다운로드

	사용자	이메일 로그인 지침
▶ ✓	lab-user	이메일 전송 🔗

닫기

12. 방금 생성한 사용자는 lab-cloudtrail-group의 멤버이다.

IAM > 사용자

사용자 (2) 정보 🔄 삭제 사용자 추가

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

🔍 사용자 이름 또는 액세스 키로 사용자 찾기

<input type="checkbox"/>	사용자 이름	그룹	마지막 활동	MFA	암호 수명	활성 키 수명
<input type="checkbox"/>	Administrator	없음	⚠ 410일 전	없음	⚠ 410일 전	-
<input type="checkbox"/>	lab-user	lab-cloudtrail-group	안 함	없음	✓ 1분 전	-

13. 생성한 사용자의 [보안 자격 증명] 탭의 [콘솔 로그인 링크]를 복사한 후, 현재 로그인한 사용자는 로그아웃하고 생성한 사용자로 로그인한다.

사용자 > lab-user

요약

사용자 ARN: `arn:aws:iam::789534828835:user/lab-user`

경로: `/`

생성 시간: 2022-06-04 21:01 UTC+0900

권한 | 그룹 (1) | 태그 (1) | **보안 자격 증명** | 액세스 관리자

로그인 자격 증명

요약	• 콘솔 로그인 링크: https://789534828835.signin.aws.amazon.com/console
콘솔 비밀번호	활성화 (로그인한 적 없음) 관리
할당된 MFA 디바이스	할당되지 않음 관리
서명 인증서	없음

14. 생성한 사용자로 로그인 후, [서비스] > [관리 및 거버넌스] > [CloudTrail]을 클릭한다.

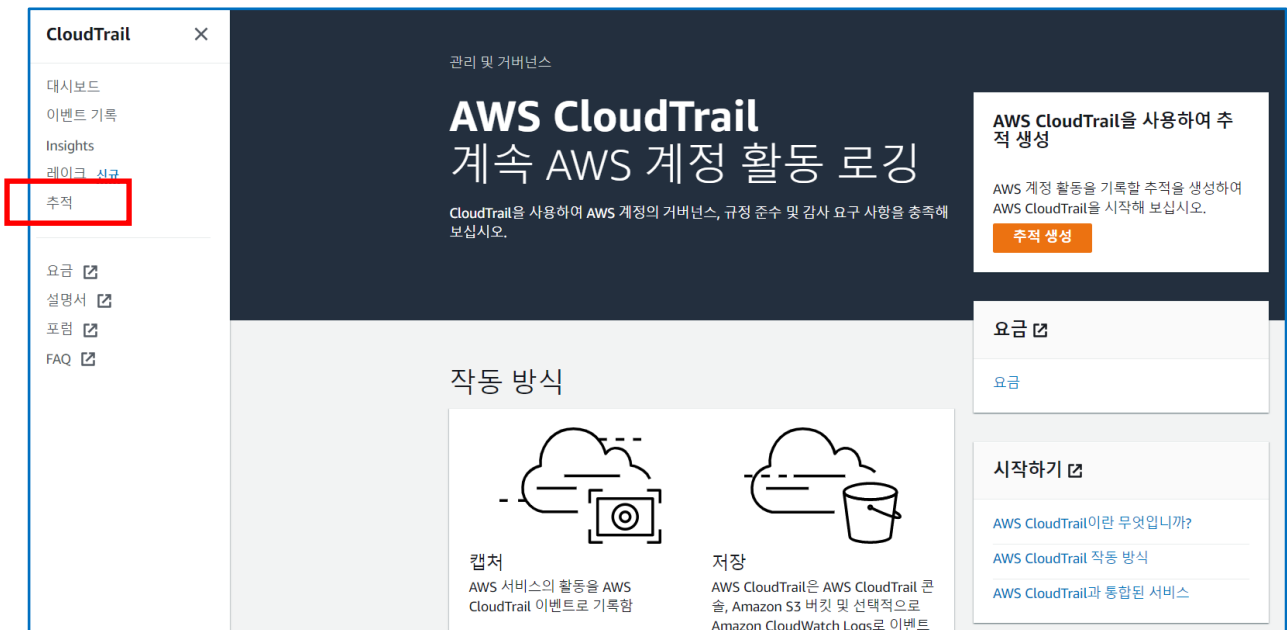
모든 서비스

- AR 및 VR
- AWS 비용 관리
- Customer Enablement
- Machine Learning
- Quantum Technologies
- 개발자 도구
- 게임 개발
- 관리 및 거버넌스**
- 네트워킹 및 콘텐츠 전송
- 데이터베이스
- 로봇 공학
- 마이그레이션 및 전송
- 모바일
- 미디어 서비스

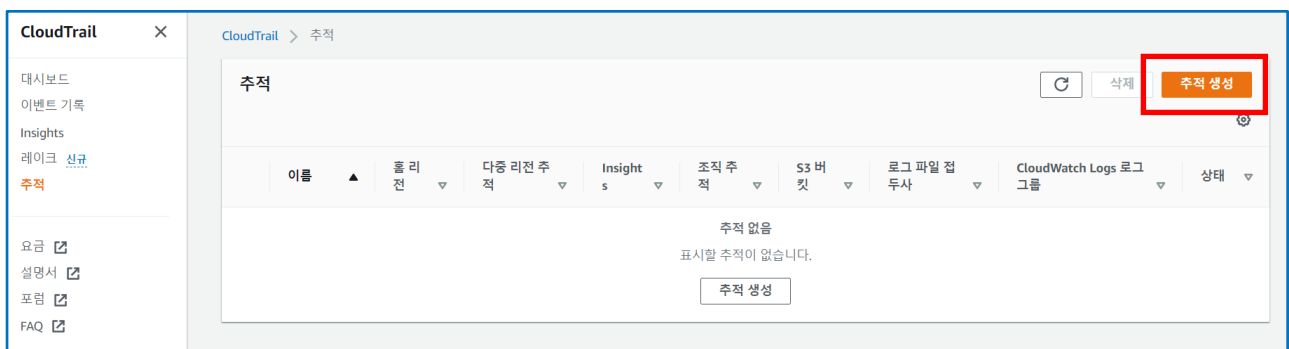
관리 및 거버넌스

- AWS AppConfig**
AWS AppConfig를 사용하여 런타임에 애플리케이션 구성을 업데이트하십시오.
- AWS Auto Scaling**
AWS Auto Scaling을 사용하면 AWS에서 전체 애플리케이션을 신속하게 확장 및 축소할 수 있습니다.
- AWS Chatbot**
AWS용 ChatOps
- CloudFormation**
템플릿을 사용한 리소스 생성 및 관리
- ★ CloudTrail**
사용자 활동 및 API 사용 추적
- ★ CloudWatch**
리소스 및 애플리케이션 모니터링

15. [CloudTrail] 페이지이다. 좌측 메뉴 중 [추적]을 클릭한다.



16. [추적] 페이지이다. [추적 생성] 버튼을 클릭한다.



17. [추적 이름]에서 추적에 이름을 **lab-events-trail**로 지정한다. [스토리지 위치]에서 [새 S3 버킷 생성]을 선택하여 버킷을 생성한다. 버킷을 생성하면 **CloudTrail**은 필요한 버킷 정책을 생성하고 적용한다. 버킷에 이름을 **aws-cloudtrail-logs-xxx-mylog** 지정한다.

단계 1
추적 속성 선택

단계 2
로그 이벤트 선택

단계 3
검토 및 생성

추적 속성 선택

일반 세부 정보
콘솔에서 생성된 추적은 다중 리전 추적입니다. [자세히 알아보기](#)

추적 이름
추적의 표시 이름을 입력합니다.

3~128자입니다. 문자, 숫자, 마침표, 밑줄 및 대시만 허용됩니다.

☒ 조직의 모든 계정에 대해 활성화
조직의 계정을 검토하려면 AWS Organizations를 엽니다. [모든 계정 보기](#)

스토리지 위치 정보

☒ 새 S3 버킷 생성
추적에 대한 로그를 저장할 버킷을 생성합니다.

☐ 기존 S3 버킷 사용
이 추적에 대한 로그를 저장할 기존 버킷을 선택합니다.

추적 로그 버킷 및 폴더
로그를 저장할 새 S3 버킷 이름 및 폴더(점두사)를 입력합니다. 버킷 이름은 전역적으로 고유해야 합니다.

로그는 aws-cloudtrail-logs-789534828835-mylog/AWSLogs/789534828835에 저장됨

18. [로그 파일 SSE-KMS 암호화]를 체크해제하여 비활성화한다. 기본적으로 로그 파일은 SSE-S3 암호화를 통해 암호화된다. [추가 설정]은 기본 값 그대로 둔다. [CloudWatch Logs]도 체크해제하여 비활성화한다. [태그]에서 [키]를 **Name**으로, [값]을 **lab-events-trail**로 입력한다. 그리고 [다음]을 클릭한다.

로그 파일 SSE-KMS 암호화 정보
☐ 활성화됨

▶ 추가 설정

CloudWatch Logs - 선택 사항
추적 로그를 모니터링하고 특정 활동이 발생하면 이를 알리도록 CloudWatch Logs를 구성합니다. 표준 CloudWatch 및 CloudWatch Logs 요금이 적용됩니다. [자세히 알아보기](#)

CloudWatch Logs 정보
☐ 활성화됨

▶ 정책 문서

태그 - 선택 사항 정보
추적을 포함하여 리소스를 관리하고 정리하는 데 도움이 되도록 하나 이상의 태그를 추가할 수 있습니다.

키 **값 - 선택 사항**

× ×

49개의 태그(를) 더 추가할 수 있습니다.

취소

19. [로그 이벤트 선택] 페이지에서 로그할 [이벤트] 유형을 선택한다. 이 추적의 경우 기본값인 [관리 이벤트]를 그대로 사용한다. [관리 이벤트] 섹션에서, [읽기] 및 [쓰기] 이벤트를 모두 체크한다. 나머지 값은 기본값을 사용한다. [다음]을 클릭한다.

단계 1
추적 속성 선택

단계 2
로그 이벤트 선택

단계 3
검토 및 생성

로그 이벤트 선택

이벤트 정보

개별 리소스 또는 AWS 계정의 현재 및 향후 모든 리소스에 대한 API 활동을 기록합니다. [추가 요금이 적용될 수 있음](#)

이벤트 유형
로그할 이벤트 유형을 선택합니다.

☒ 관리 이벤트
AWS 리소스에서 수행된 관리 작업을 캡처합니다.

☐ 데이터 이벤트
리소스에 대해 또는 리소스 내에서 수행된 리소스 작업을 로그합니다.

☐ Insights 이벤트
계정에서 비정상적인 활동, 오류 또는 사용자 행동을 식별합니다.

관리 이벤트 정보

관리 이벤트에서는 AWS 계정의 리소스에서 수행된 관리 작업에 대한 정보를 표시합니다.

i 관리 이벤트의 첫 번째 사본이므로 이 추적의 로그 관리 이벤트에는 추가 요금이 적용되지 않습니다.

API 활동
로그할 활동을 선택합니다.

☒ 읽기 ☒ 쓰기

☐ AWS KMS 이벤트 제외

☐ Amazon RDS Data API API 이벤트 제외

취소

이전

다음

20. [검토 및 생성] 페이지에서 페이지를 스크롤다운하여 [추적 생성]을 클릭한다.

데이터 이벤트

이 추적에 대해 데이터 이벤트 수집이 구성되지 않음

Insights 이벤트

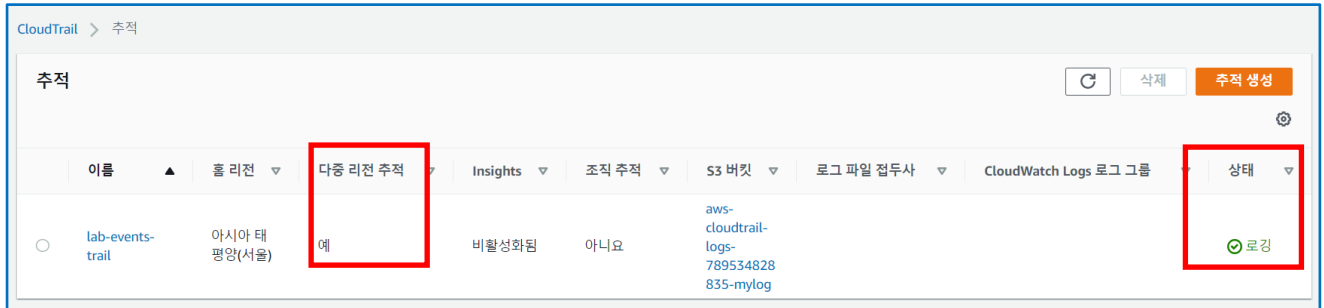
관리 이벤트를 기록하는 추적에서만 CloudTrail 인사이트를 활성화할 수 있습니다. [자세히 알아보기](#)

취소

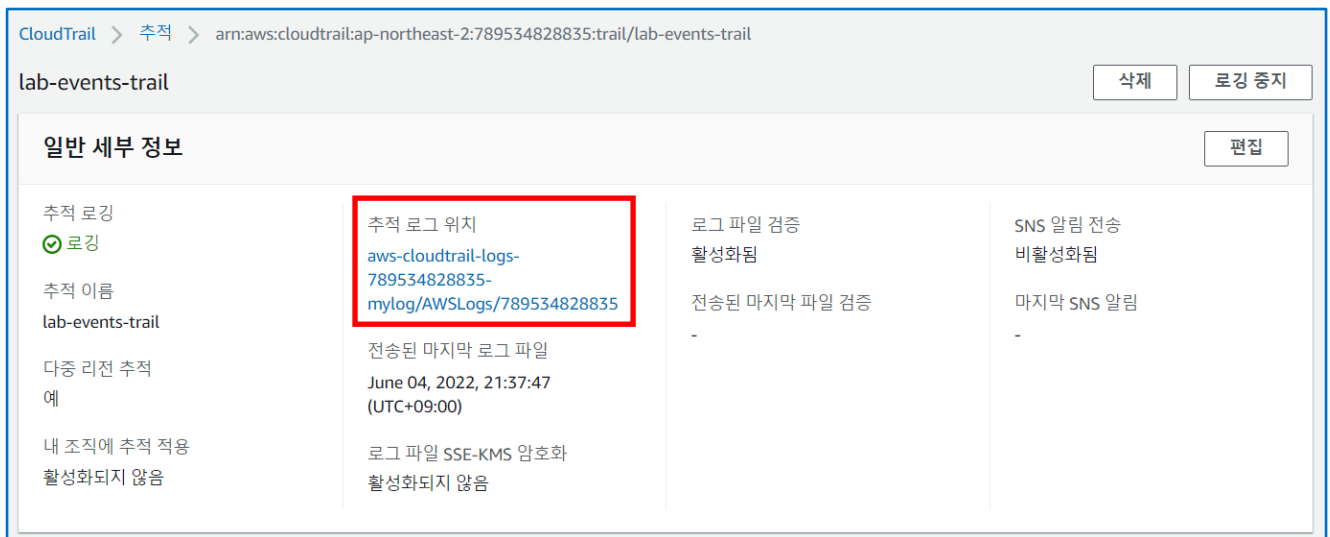
이전

추적 생성

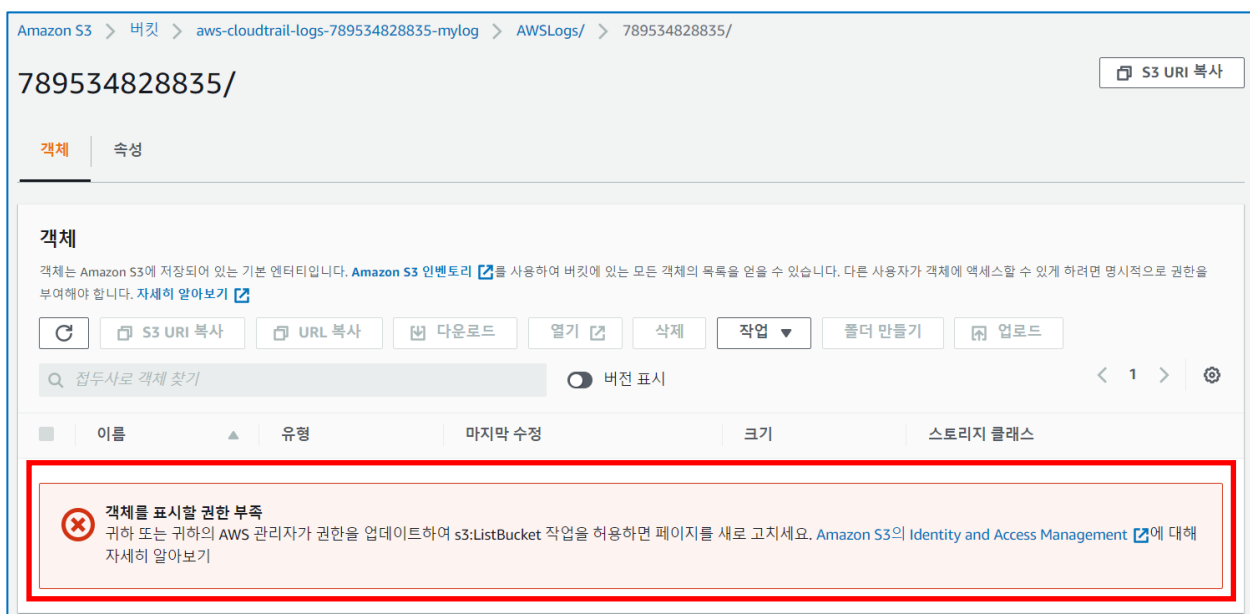
21. [추적]이 성공적으로 생성되었다. 추적은 기본적으로 [다중 리전 추적]으로 설정되며 로깅이 추적에 대해 기본적으로 활성화된다. 방금 생성한 [추적] lab-events-trail을 클릭한다.



22. [추적]의 세부 정보페이지에서 [추적 로그 위치] 링크를 클릭한다.



23. Amazon S3 콘솔이 열리고 로그 파일의 최상위 수준에 해당 버킷이 표시된다. 하지만, 권한이 없다면 다음 그림과 같이 권한 부족 메시지가 나타난다. 다시 관리자로 로그인하여 해당 계정에 s3:ListBucket 권한을 할당하고 페이지를 새로 고친다.



24. 이번 실습에서는 해당 계정에 **AmazonS3FullAccess** 권한을 할당했다.

권한 부여

IAM 정책을 사용하여 권한을 부여합니다. 기존 정책을 할당하거나 새 정책을 생성할 수 있습니다.

그룹에 사용자 추가

기존 사용자에서 권한 복사

기존 정책 직접 연결

정책 생성

정책 필터 9 결과 표시

정책 이름	유형	사용 용도
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS 관리형	없음
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS 관리형	없음
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS 관리형	없음
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS 관리형	없음
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS 관리형	없음
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Backup	AWS 관리형	없음
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Restore	AWS 관리형	없음
<input type="checkbox"/> QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS 관리형	없음

취소

다음: 검토

25. 다시 **lab-user**로 로그인하면 다음 그림과 같이 객체 목록을 확인할 수 있다.

Amazon S3 > 버킷 > aws-cloudtrail-logs-789534828835-mylog > AWSLogs/ > 789534828835/

789534828835/

S3 URI 복사

객체

속성

객체 (2)

객체는 Amazon S3에 저장되어 있는 기본 엔티티입니다. [Amazon S3 인벤토리](#)를 사용하여 버킷에 있는 모든 객체의 목록을 얻을 수 있습니다. 다른 사용자가 객체에 액세스할 수 있게 하려면 명시적으로 권한을 부여해야 합니다. [자세히 알아보기](#)

🔄

S3 URI 복사

URL 복사

다운로드

열기

삭제

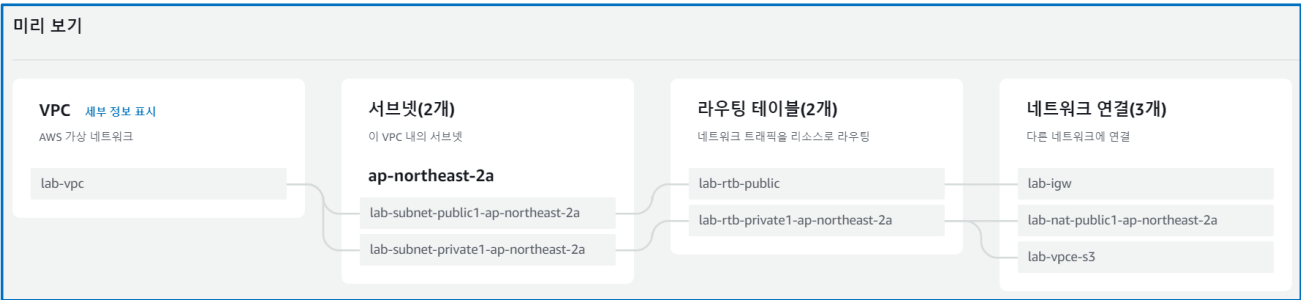
작업 ▼

폴더 만들기

업로드

<input type="checkbox"/>	이름	유형	마지막 수정	크기	스토리지 클래스
<input type="checkbox"/>	CloudTrail-Digest/	폴더	-	-	-
<input type="checkbox"/>	CloudTrail/	폴더	-	-	-

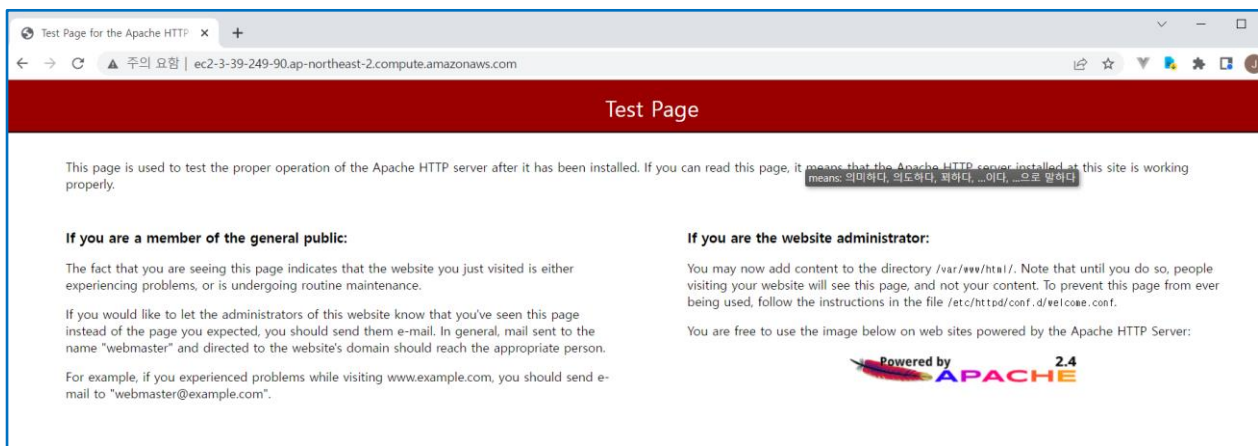
26. 다음과 같이 **VPC**를 생성했다.



27. 또한 다음과 같이 EC2 인스턴스를 생성했다.

EC2 > 인스턴스 > i-0ef7c7e9b90549cb5		
i-0ef7c7e9b90549cb5 (al-ec2)에 대한 인스턴스 요약 정보		
인스턴스 ID i-0ef7c7e9b90549cb5 (al-ec2)	퍼블릭 IPv4 주소 3.39.249.90 개방 주소법	프라이빗 IPv4 주소 10.0.4.186
IPv6 주소 -	인스턴스 상태 실행 중	퍼블릭 IPv4 DNS ec2-3-39-249-90.ap-northeast-2.compute.amazonaws.com 개방 주소법
호스트 이름 유형 IP 이름: ip-10-0-4-186.ap-northeast-2.compute.internal	프라이빗 IP DNS 이름(IPv4만 해당) ip-10-0-4-186.ap-northeast-2.compute.internal	프라이빗 리소스 DNS 이름 응답 IPv4(A)
인스턴스 유형 t2.micro	탄력적 IP 주소 -	자동 할당된 IP 주소 3.39.249.90 [퍼블릭 IP]
VPC ID vpc-08d5da33ab7bde843 (lab-vpc)	AWS Compute Optimizer 찾기 권장 사항을 위해 AWS Compute Optimizer에 옵트인합니다. 자세히 알아보기	IAM 역할 -
서브넷 ID subnet-046b093508608f559 (lab-subnet-public1-ap-northeast-2a)	Auto Scaling 그룹 이름 -	

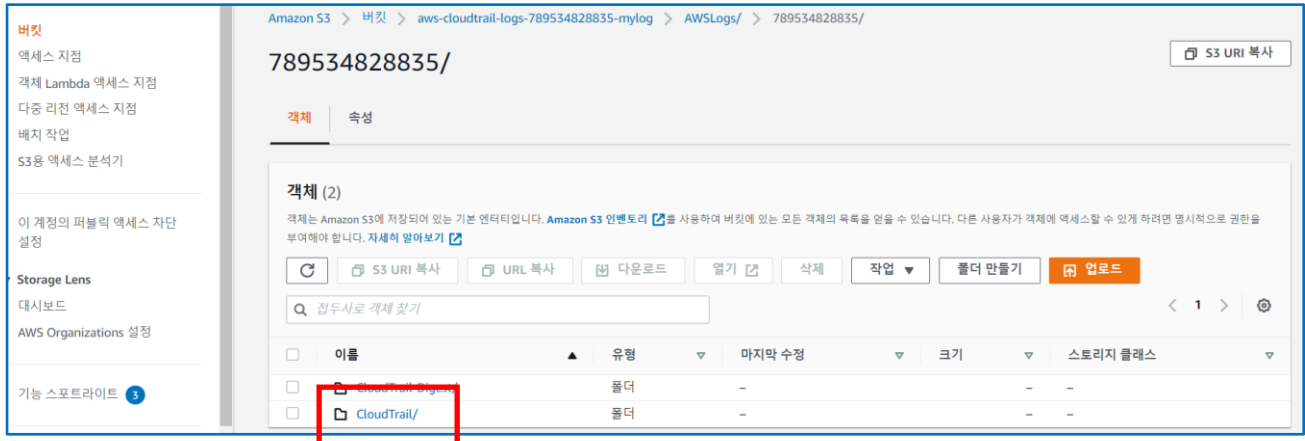
28. 그리고 **Apache Web Server**를 설치하고, **보안 그룹**에 **http 포트 80번** 오픈하고 해당 주소로 접근했다.



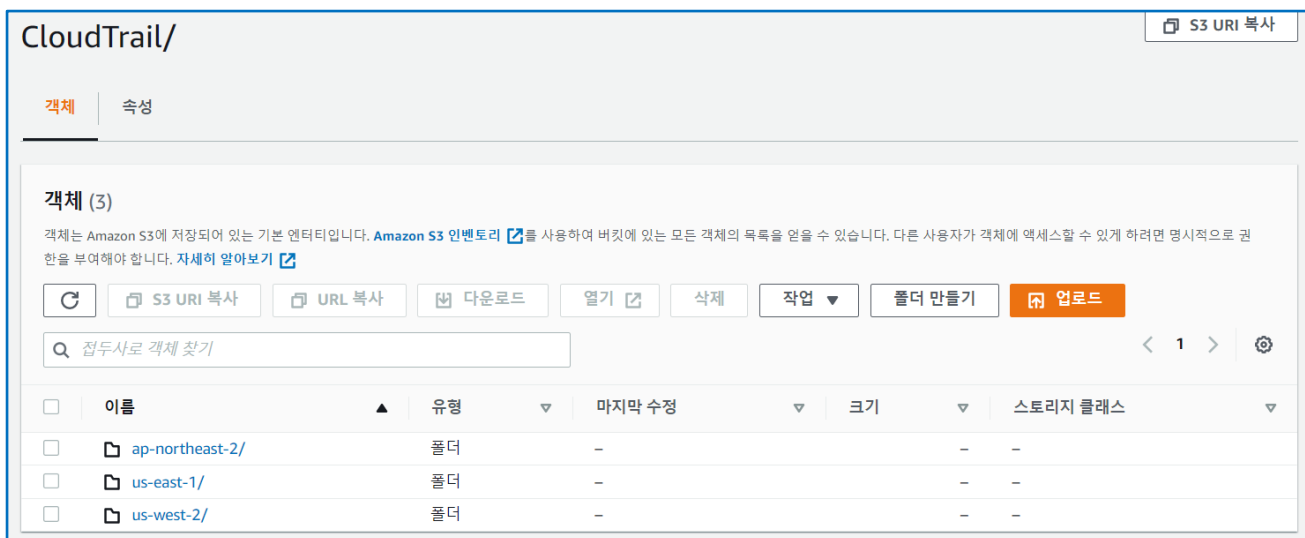
29. **lab-user** 계정으로 로그인하여 **CloudTrail** 페이지로 이동한다. 다음과 같이 **[이벤트 기록]**에 위의 **VPC** 생성과 **EC2 인스턴스**에 대한 작업들이 이벤트로 기록되어 있음을 확인할 수 있다.

CloudTrail	추적 정보		CloudTrail Insights 정보
	이름 lab-events-trail	상태 로깅	
대시보드 이벤트 기록 Insights 레이크 추적	이벤트 기록 정보		CloudTrail Insights가 활성화되지 않음 Insights는 비정상적인 API 활동을 표시하는 이벤트입니다. Insights를 활성화한 후 비정상적인 활동이 기록되면 Insights 이벤트가 이 테이블에 90일 동안 표시됩니다. 이때 추가 요금이 적용됩니다. 자세히 알아보기
	이벤트 이름	이벤트 시간	이벤트 소스
요금 설명서 포럼 FAQ	AuthorizeSecurityGro...	June 04, 2022, 23:13:59 (UTC+0...	ec2.amazonaws.com
	SendSSHPublicKey	June 04, 2022, 23:09:50 (UTC+0...	ec2-instance-connect.amazonaws.com
	SharedSnapshotVolu...	June 04, 2022, 23:07:19 (UTC+0...	ec2.amazonaws.com
	RunInstances	June 04, 2022, 23:07:17 (UTC+0...	ec2.amazonaws.com
	AuthorizeSecurityGro...	June 04, 2022, 23:07:16 (UTC+0...	ec2.amazonaws.com
	전체 이벤트 기록 보기		

30. 이번에는 **CloudTrail**의 [추적]으로 이동하여 위 실습에서 생성한 **lab-events-trail**의 [추적 로그 위치]의 링크를 클릭하여 **S3**로 이동한다. 목록에서 **CloudTrail**의 링크를 클릭한다.



31. **CloudTrail**의 객체인 **ap-northeast-2**의 링크를 클릭한다.



32. 계속 하위 디렉토리로 이동한다. 목록에서 제일 위의 파일을 클릭해본다. 해당 리전에서 활동 로그를 검토하려는 연도, 월 및 일로 버킷 폴더 구조를 탐색한다. 수 많은 파일이 있을 수 있다. 파일 이름은 AWS 계정 ID로 시작하고 .gz 확장명으로 끝난다. 예를 들어 계정 ID가 123456789012인 경우 **123456789012_CloudTrail_ap-northeast-2_20190610T1255abcdeEXAMPLE.json.gz**와 유사한 이름의 파일이 표시된다. 이러한 파일을 보려면 파일을 다운로드하고 압축을 푼 다음 일반 텍스트 편집기 또는 JSON 파일 뷰어에서 파일을 볼 수 있다. 일부 브라우저도 .gz 및 JSON 파일 직접 보기를 지원한다.

Amazon S3 > 버킷 > aws-cloudtrail-logs-789534828835-mylog > AWSLogs/ > 789534828835/ > CloudTrail/ > ap-northeast-2/ > 2022/ > 06/ > 04/

04/ S3 URI 복사

객체 속성

객체 (20)

객체는 Amazon S3에 저장되어 있는 기본 엔터티입니다. [Amazon S3 인벤토리](#)를 사용하여 버킷에 있는 모든 객체의 목록을 얻을 수 있습니다. 다른 사용자가 객체에 액세스할 수 있게 하려면 명시적으로 권한을 부여해야 합니다. [자세히 알아보기](#)

🔄 S3 URI 복사 URL 복사 📄 다운로드 열기 삭제 작업 ▼ 폴더 만들기 업로드

🔍 접두사로 객체 찾기

<input type="checkbox"/>	이름	유형 ▼	마지막 수정 ▼	크기 ▼	스토리지 클래스 ▼
<input type="checkbox"/>	789534828835_CloudTrail_ap-northeast-2_20220604T1245Z_M8EQtH5KvK3jQg22.json.gz	gz	2022. 6. 4. pm 9:42:33 PM KST	3.5KB	Standard
<input type="checkbox"/>	789534828835_CloudTrail_ap-northeast-2_20220604T1250Z_pwm33By7ES7Afd34.json.gz	gz	2022. 6. 4. pm 9:47:44 PM KST	1.5KB	Standard
<input type="checkbox"/>	789534828835_CloudTrail_ap-northeast-2_20220604T1255Z_ZcGZcOkVb9TGcvYp.json.gz	gz	2022. 6. 4. pm 9:52:54 PM KST	2.7KB	Standard

33. 이 로그 파일 항목은 로그인한 IAM 사용자의 자격 증명, 이 사용자가 로그인한 날짜와 시간, 로그인이 성공했다는 것만이 아니라 그보다 많은 정보를 알려준다. 로그인한 IP 주소, 사용한 컴퓨터의 운영 체제와 브라우저 소프트웨어, Multi-Factor Authentication을 사용하지 않았다는 것도 알 수 있다.

```
C: > Temp > 789534828835_CloudTrail_ap-northeast-2_20220604T1245Z_M8EQtH5KvK3jQg22.json > ...
1 [{"Records":[{"eventVersion":"1.08","userIdentity":{"type":"IAMUser",
"principalId":"AIDA3PU7RNER3BH3YTVNG","arn":"arn:aws:iam::789534828835:user/lab-user",
"accountId":"789534828835","accessKeyId":"ASIA3PU7RNER2NQXEFN7","userName":"lab-user",
"sessionContext":{"sessionIssuer":{"webIdFederationData":{"attributes":
{"creationDate":"2022-06-04T12:16:53Z","mfaAuthenticated":"false"}}},
"eventTime":"2022-06-04T12:37:22Z","eventSource":"s3.amazonaws.com","eventName":"CreateBucket",
"awsRegion":"ap-northeast-2","sourceIPAddress":"121.136.18.98","userAgent":["AWSCloudTrail,
aws-internal/3 aws-sdk-java/1.11.1030 Linux/5.4.186-113.361.amzn2int.x86_64
OpenJDK_64-Bit_Server_VM/25.322-b06 java/1.8.0_322 vendor/Oracle_Corporation cfg/retry-mode/
standard]","requestParameters":{"CreateBucketConfiguration":
{"LocationConstraint":"ap-northeast-2","xmlns":"http://s3.amazonaws.com/doc/2006-03-01/"},
"bucketName":"aws-cloudtrail-logs-789534828835-mylog","Host":"s3.ap-northeast-2.amazonaws.com"},
"responseElements":null,"additionalEventData":{"SignatureVersion":"SigV4",
"CipherSuite":"ECDHE-RSA-AES128-GCM-SHA256","bytesTransferredIn":158,
"AuthenticationMethod":"AuthHeader","x-amz-id-2":"KUQ0Rzjq3U
+aV8oxchVK8pxhCAa62Hpg5rBZqr5LQAsCoACJ4X8NMg91C2fG9CUh8NHbtkB7Bjk=","bytesTransferredOut":0},
"requestID":"WTG24FW3AZTGVZAJ","eventID":"661f918a-3c42-48ab-8905-a85aec12eeb6","readOnly":false,
"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"789534828835",
"vpceEndpointId":"vpce-0911e160","eventCategory":"Management","tlsDetails":{"tlsVersion":"TLSv1.
2","cipherSuite":"ECDHE-RSA-AES128-GCM-SHA256","clientProvidedHostHeader":"s3.ap-northeast-2.
amazonaws.com"}},{eventVersion":"1.08","userIdentity":{"type":"AWSService",
"invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2022-06-04T12:37:23Z","eventSource":"s3.
amazonaws.com","eventName":"GetBucketAcl","awsRegion":"ap-northeast-2",
```