

# 186- [JAWS] - 실습 - 인프라 모니터링

## 인프라 모니터링

### 실습 개요

애플리케이션 및 인프라 모니터링은 안정적이고 일관된 IT 서비스 제공에 매우 중요합니다.

모니터링 요구 사항은 장기 분석을 위한 통계 수집부터 변경 및 중단에 대한 신속한 대응까지 다양합니다. 모니터링은 인프라가 조직 표준을 충족하는지 지속적으로 확인함으로써 규정 준수 보고도 지원할 수 있습니다.

이 실습에서는 Amazon CloudWatch Metrics, Amazon CloudWatch Logs, Amazon CloudWatch Events, AWS Config 를 사용하여 애플리케이션과 인프라를 모니터링하는 방법을 설명합니다.

이 실습을 완료하면 다음을 할 수 있게 됩니다.

- AWS Systems Manager Run Command 를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 CloudWatch 에이전트 설치
- CloudWatch 에이전트 및 CloudWatch Logs 를 사용하여 애플리케이션 로그 모니터링
- CloudWatch 에이전트 및 CloudWatch Metrics 를 사용하여 시스템 지표 모니터링
- CloudWatch Events 를 사용하여 실시간 알림 생성
- AWS Config 를 사용하여 인프라 규정 준수 추적

#### 소요 시간

본 실습을 완료하는 데는 약 **60 분**이 소요됩니다.

## AWS Management Console 액세스

1. 지침의 맨 위에서 **실습 시작(Start Lab)**을 선택하여 실습을 시작합니다.

실습시작(Start Lab) 패널이 열리고 실습 상태가 표시됩니다.

2. "**실습 상태: 준비(Lab status: ready)**" 메시지가 표시되면 **X**를 선택하여 Start Lab 패널을 닫습니다.

3. 지침의 맨 위에서 **AWS**를 선택합니다.

새 브라우저 탭에서 AWS Management Console 이 열립니다. 시스템에 자동으로 로그인됩니다.

**팁:** 새 브라우저 탭이 열리지 않는 경우 일반적으로 브라우저에서 팝업 창을 열 수 없음을 나타내는 배너 또는 아이콘이 브라우저 상단에 표시됩니다. 배너 또는 아이콘을 선택하고 **팝업 허용**을 선택합니다.

4. 이 지침과 함께 표시되도록 AWS Management Console 탭을 정렬합니다. 두 브라우저 탭이 동시에 표시되어 실습 단계를 보다 쉽게 수행할 수 있게 됩니다.

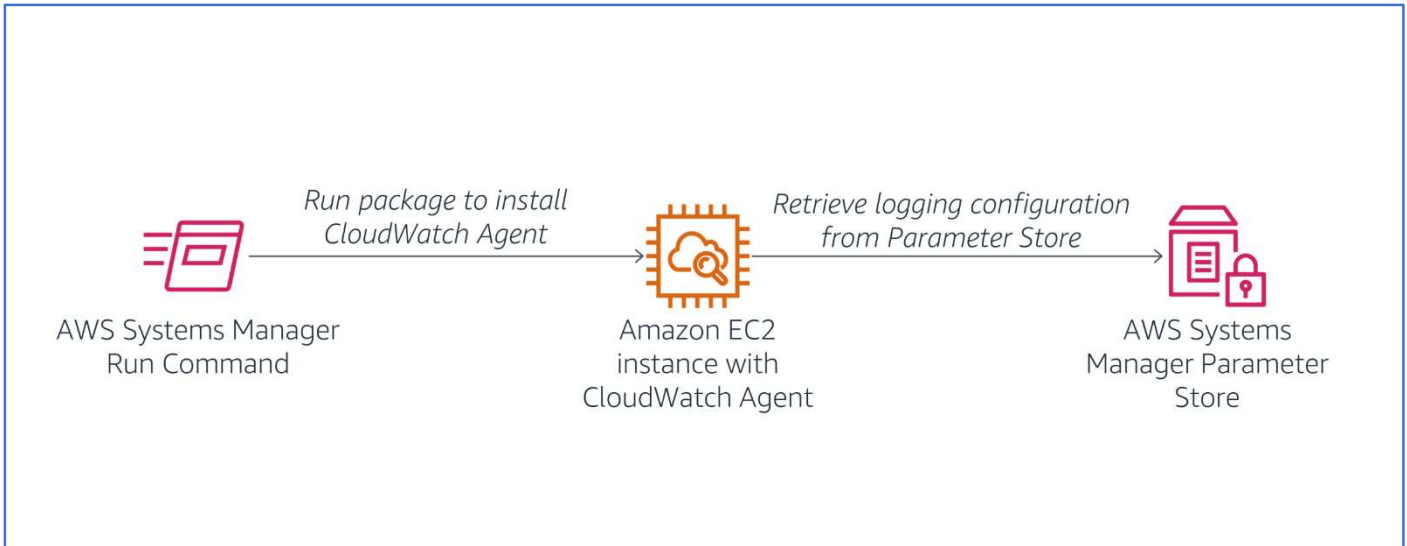
이 실습 도중 리전을 변경하지 마십시오.

## 과제 1: CloudWatch 에이전트 설치

CloudWatch 에이전트를 사용하여 EC2 인스턴스와 온프레미스 서버에서 다음을 포함한 지표를 수집할 수 있습니다.

- **EC2 인스턴스의 시스템 수준 지표:** CPU 할당, 사용 가능한 디스크 공간, 메모리 사용률 등이 포함됩니다. 이러한 지표는 머신 자체에서 수집되며 CloudWatch 가 수집하는 표준 CloudWatch 지표를 보완합니다.
- **온프레미스 서버의 시스템 수준 지표:** 이를 통해 AWS 가 관리하지 않는 하이브리드 환경과 서버를 모니터링할 수 있습니다.
- **시스템 및 애플리케이션 로그:** Linux 서버와 Windows 서버의 로그가 모두 해당됩니다.
- **사용자 지정 지표:** [StatsD](#) 및 [collectd](#) 프로토콜을 사용하는 애플리케이션과 서비스의 지표입니다.

이 과제에서는 Systems Manager 를 사용하여 EC2 인스턴스에 CloudWatch 에이전트를 설치합니다. 애플리케이션 지표와 시스템 지표를 모두 수집하도록 에이전트를 구성합니다.



5. **AWS 관리 콘솔**의 **서비스(Services)** 메뉴에서 **Systems Manager** 를 선택합니다.

6. 왼쪽 탐색 창에서 **Run Command**(노드 관리 > 명령 실행)를 선택합니다.

표시되는 탐색 창이 없는 경우 왼쪽 상단 모서리의 아이콘을 선택하여 표시합니다.

Run Command 는 CloudWatch 에이전트를 설치하는 미리 작성된 명령을 배포하는 데 사용합니다.

7. **명령 실행(Run a Command)**를 선택합니다.

8. **AWS-ConfigureAWSPackage** 옆의 버튼을 선택합니다. (일반적으로 목록 위쪽에 표시됨)

9. **파라미터 명령(Command parameters)** 섹션으로 스크롤하고 다음 정보를 구성합니다.

- **작업(Action):** **설치(Install)**를 선택합니다.
- **이름(Name):** **AmazonCloudWatchAgent** 를 입력합니다.
- **버전(Versions):** **latest** 를 입력합니다.

10. **대상(Targets)** 섹션에서 **수동으로 인스턴스 선택(Choose instances manually)**를 선택한 다음 **인스턴스(Instances)** 아래에서 **Web Server** 옆의 확인란을 선택합니다.

이 구성은 웹 서버에 CloudWatch 에이전트를 설치합니다.

11. 페이지 하단에서 **실행(Run)**을 선택합니다.

12. **전체 상태(Overall status)**가 **성공(Success)**으로 바뀔 때까지 기다립니다. 이따금 페이지 상단의 새로고침을 선택하여 상태를 업데이트할 수 있습니다.

작업의 출력 결과에서 성공적으로 실행되었음을 알 수 있습니다.

AWS Systems Manager > 명령 실행 > 명령 ID: f4f84ad4-ac00-48b1-8cc0-83f67302cb0a

명령 ID: f4f84ad4-ac00-48b1-8cc0-83f67302cb0a

명령 상태

전체 상태 ✔ 성공	상세 상태 ✔ 성공	대상 개수 1	완료 개수 1	오류 횟수 0	전송 제한 시간 초과 횟수 0
---------------	---------------	------------	------------	------------	---------------------

대상 및 출력

출력 보기

인스턴스 ID	인스턴스 이름	상태	상세 상태	시작 시간	완료 시간
i-0a44dbc469dab1851	ip-10-0-0-12.us-west-2.compute.internal	✔ 성공	✔ 성공	Sun, 06 Aug 2023 05:03:09 GMT	Sun, 06 Aug 2023 05:03:24 GMT

13. 대상 및 출력(Targets and outputs)에서 인스턴스 ID(Instance ID) 아래 표시되는 인스턴스 이름을 선택합니다.

14. 1 단계 - 출력(Step 1 - Output)을 확장합니다.

다음 메시지가 표시되어야 합니다.

**arn:aws:ssm:::package/AmazonCloudWatchAgent** 를 성공적으로  
설치했습니다.(Successfully installed  
**arn:aws:ssm:::package/AmazonCloudWatchAgent.**)

단계 1 - 명령 설명 및 상태

상태 ✔ 성공	상세 상태 ✔ 성공	응답 코드 0
단계 이름 createDownloadFolder	시작 시간 Sun, 06 Aug 2023 05:03:09 GMT	완료 시간 Sun, 06 Aug 2023 05:03:09 GMT

▼ Output

The command output displays a maximum of 48,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a logs group when you run the command.

Step execution skipped due to unsatisfied preconditions: '"StringEquals": [platformType, Windows]'. Step name: createDownloadFolder

Copy Download

사전 조건이 충족되지 않아 실행 단계를 건너웁니다.'"StringEquals": [platformType, Windows]'. 단계 이름: createDownloadFolder(Step name: createDownloadFolder)라는 메시지가 표시되면 2 단계 - 출력(Step 2 - Output)을 대신 확장합니다. 사용 중인 인스턴스가 Linux AMI 에서 생성되었기 때문에 이 옵션을 선택할 수 있는 것입니다. 이 메시지는 무시해도 됩니다.

이제 원하는 로그 정보를 수집하도록 CloudWatch 에이전트를 구성합니다. 인스턴스에 웹 서버가 설치되어 있으므로 웹 서버 로그와 일반적인 시스템 지표를 수집하도록 CloudWatch 에이전트를 구성합니다.

구성 파일을 AWS Systems Manager Parameter Store 에 저장하면 CloudWatch 에이전트가 구성 파일을 가져올 수 있습니다.

15. 왼쪽 탐색 창에서 **파라미터 스토어(Parameter Store)**를 선택합니다.

16. **파라미터 생성(Create parameter)**을 선택하고 다음 정보를 구성합니다.

- **이름(Name):** Monitor-Web-Server 를 입력합니다.
- **설명(Description):** Collect web logs and system metrics 를 입력합니다.
- **값(Value):** 다음 구성을 복사하여 붙여넣습니다.

```
{
  "logs": {
    "logs_collected": {
      "files": {
        "collect_list": [
          {
            "log_group_name": "HttpAccessLog",
            "file_path": "/var/log/httpd/access_log",
            "log_stream_name": "{instance_id}",
            "timestamp_format": "%b %d %H:%M:%S"
          },
          {
            "log_group_name": "HttpErrorLog",
            "file_path": "/var/log/httpd/error_log",
            "log_stream_name": "{instance_id}",
            "timestamp_format": "%b %d %H:%M:%S"
          }
        ]
      }
    }
  },
  "metrics": {
    "metrics_collected": {
      "cpu": {
        "measurement": [
```

```
    "cpu_usage_idle",
    "cpu_usage_iowait",
    "cpu_usage_user",
    "cpu_usage_system"
  ],
  "metrics_collection_interval": 10,
  "totalcpu": false
},
"disk": {
  "measurement": [
    "used_percent",
    "inodes_free"
  ],
  "metrics_collection_interval": 10,
  "resources": [
    "*"
  ]
},
"diskio": {
  "measurement": [
    "io_time"
  ],
  "metrics_collection_interval": 10,
  "resources": [
    "*"
  ]
},
"mem": {
  "measurement": [
    "mem_used_percent"
  ],
  "metrics_collection_interval": 10
},
"swap": {
  "measurement": [
    "swap_used_percent"
  ],
```

```

    "metrics_collection_interval": 10
  }
}
}
}

```

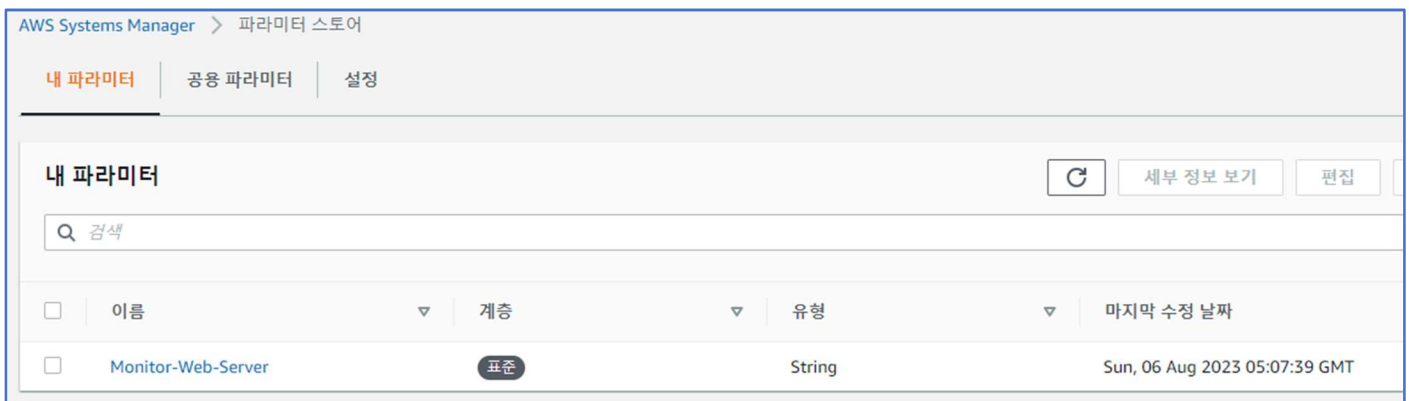
위의 구성을 검사합니다. 이 구성은 모니터링할 다음 항목을 정의합니다.

- **로그(Logs):** 수집하여 CloudWatch Logs 로 전송할 2 개의 웹 서버 로그 파일
- **지표(Metrics):** Amazon CloudWatch Metrics 로 전송할 CPU, 디스크, 메모리 지표

17. **파라미터 생성(Create parameter)**을 선택합니다.

이 파라미터는 CloudWatch 에이전트를 시작할 때 참조됩니다.

이제 다른 Run Command 를 사용하여 웹 서버에서 CloudWatch 에이전트를 시작합니다.



18. 왼쪽 탐색 창에서 **Run Command** 를 선택합니다.

19. **Run command** 를 선택합니다.

20. 상자를 선택하고 다음을 선택합니다.

- **문서 이름 접두사(Document name prefix)**를 선택합니다.
- **Equals** 를 선택합니다.
- **AmazonCloudWatch-ManageAgent** 를 입력합니다.
- 필터가 **Document name prefix : Equals : AmazonCloudWatch-ManageAgent** 인지 확인합니다.
- Enter 키를 누릅니다.

명령을 실행하기 전에 명령의 정의를 볼 수 있습니다.

명령 문서

실행할 명령 유형을 선택합니다.

Q 키워드로 검색하거나 태그 또는 속성으로 필터링

문서 이름 접두사: **Equals: AmazonCloudWatch-ManagedAgent** X

Clear filters

	이름	소유자	플랫폼 유형
<input type="radio"/>	AmazonCloudWatch-ManagedAgent	Amazon	Windows, Linux, MacOS

21. **AmazonCloudWatch-ManagedAgent** 를 선택합니다(이름 자체를 선택).

명령의 정의를 보여주는 새 웹 브라우저 탭이 열립니다.

각 탭의 콘텐츠를 탐색하여 명령 문서가 어떻게 정의되는지 확인합니다.

22. **콘텐츠(Content)** 탭을 선택하고 맨 아래로 스크롤하여 대상 인스턴스에서 실행될 실제 스크립트를 확인합니다.

이 스크립트는 앞서 정의한 CloudWatch 에이전트 구성을 가져오므로 AWS Systems Manager Parameter Store 를 참조합니다.

23. 현재 웹 브라우저 탭을 닫습니다. 그러면 앞서 사용하던 **명령 실행(Run a command)** 탭으로 돌아갑니다.

**AmazonCloudWatch-ManagedAgent** 옆의 버튼을 선택했는지 확인합니다.

24. **파라미터 명령(Command parameters)** 섹션에서 다음 정보를 구성합니다.

- **작업(Action):** 구성(configure)를 선택합니다.
- **모드(Mode):** ec2 를 선택합니다.
- **선택적 구성 소스(Optional Configuration Source):** ssm 을 선택합니다.
- **선택적 구성 위치(Optional Configuration Location):** Monitor-Web-Server 를 입력합니다.
- **선택적 재시작(Optional Restart):** 예(yes)를 선택합니다.

이렇게 하면 이전에 Parameter Store 에 저장한 구성을 사용하도록 에이전트가 구성됩니다.



## 명령 파라미터

### Action

The action CloudWatch Agent should take.

configure

### Mode

Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.

ec2

### Optional Configuration Source

Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use for amazon-cloudwatch-agent.

ssm

### Optional Configuration Location

Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name.

Monitor-Web-Server

### Optional Restart

Only for 'configure' related actions. If 'yes', restarts the agent to use the new configuration. Otherwise the new config will only apply on the next agent res

yes

25. **대상(Targets)** 섹션에서 **수동으로 인스턴스 선택(Choose instances manually)**를 선택합니다.

26. **인스턴스(Instances)** 섹션에서 **Web Server** 옆의 확인란을 선택합니다.

27. **실행(Run)**을 선택합니다.

28. **전체 상태(Overall status)**가 **성공(Success)**으로 바뀔 때까지 기다립니다. 이따금 페이지 상단의 새로고침을 선택하여 상태를 업데이트할 수 있습니다.

이제 CloudWatch 에이전트가 인스턴스에서 실행되어 로그 및 지표 데이터를 CloudWatch 로 전송합니다.

AWS Systems Manager > 명령 실행 > 명령 ID: dd6a4ba6-9dea-4922-a6cb-e0241682b647

명령 ID: dd6a4ba6-9dea-4922-a6cb-e0241682b647



명령 취소

명령 재실행

Copy to new

### 명령 상태

전체 상태

🟢 성공

상세 상태

🟢 성공

대상 개수

1

완료 개수

1

오류 횟수

0

전송 제한 시간 초과 횟수

0

### 대상 및 출력

출력 보기

Q

< 1 >

인스턴스 ID

인스턴스 이름

상태

상세 상태

시작 시간

완료 시간

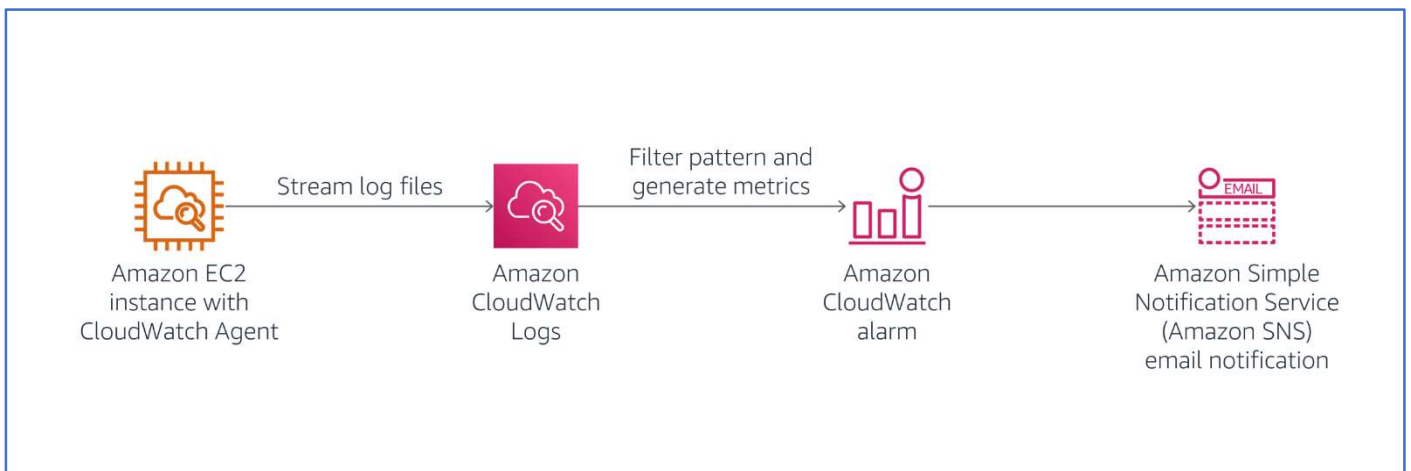
○ i-0a44dbc469dab1851 ip-10-0-0-12.us-west-2.compute.internal 🟢 성공 🟢 성공 Sun, 06 Aug 2023 05:11:10 GMT Sun, 06 Aug 2023 05:11:11 GMT

## 과제 2: CloudWatch Logs 를 사용하여 애플리케이션 로그 모니터링

CloudWatch Logs 로 로그 데이터를 사용하여 애플리케이션 및 시스템을 모니터링할 수 있습니다. 예를 들어 CloudWatch Logs 는 애플리케이션 로그에서 오류 발생 개수를 추적하고 오류 비율이 지정된 임계값을 초과할 때마다 알림을 전송할 수 있습니다.

CloudWatch Logs 는 기존 로그 데이터를 모니터링에 사용하므로 코드를 변경할 필요가 없습니다. 예를 들어 특정 리터럴 문자(예: 'NullPointerException')에 대한 애플리케이션 로그를 모니터링하거나 로그 데이터의 특정 위치(예: 웹 서버 액세스 로그의 404 상태 코드)에서 리터럴 문자의 출현 횟수를 계산할 수 있습니다. 원하는 용어가 검색되면 CloudWatch Logs 는 지정된 CloudWatch 지표에 데이터를 보고합니다. 로그 데이터는 전송 시는 물론 저장 시에도 암호화됩니다.

이 과제에서는 웹 서버에서 로그 데이터를 생성한 다음 CloudWatch Logs 를 사용하여 로그를 모니터링합니다.



웹 서버가 생성하는 로그 데이터 유형은 다음 두 가지입니다.

- 액세스 로그
- 오류 로그

먼저 웹 서버에 액세스합니다.

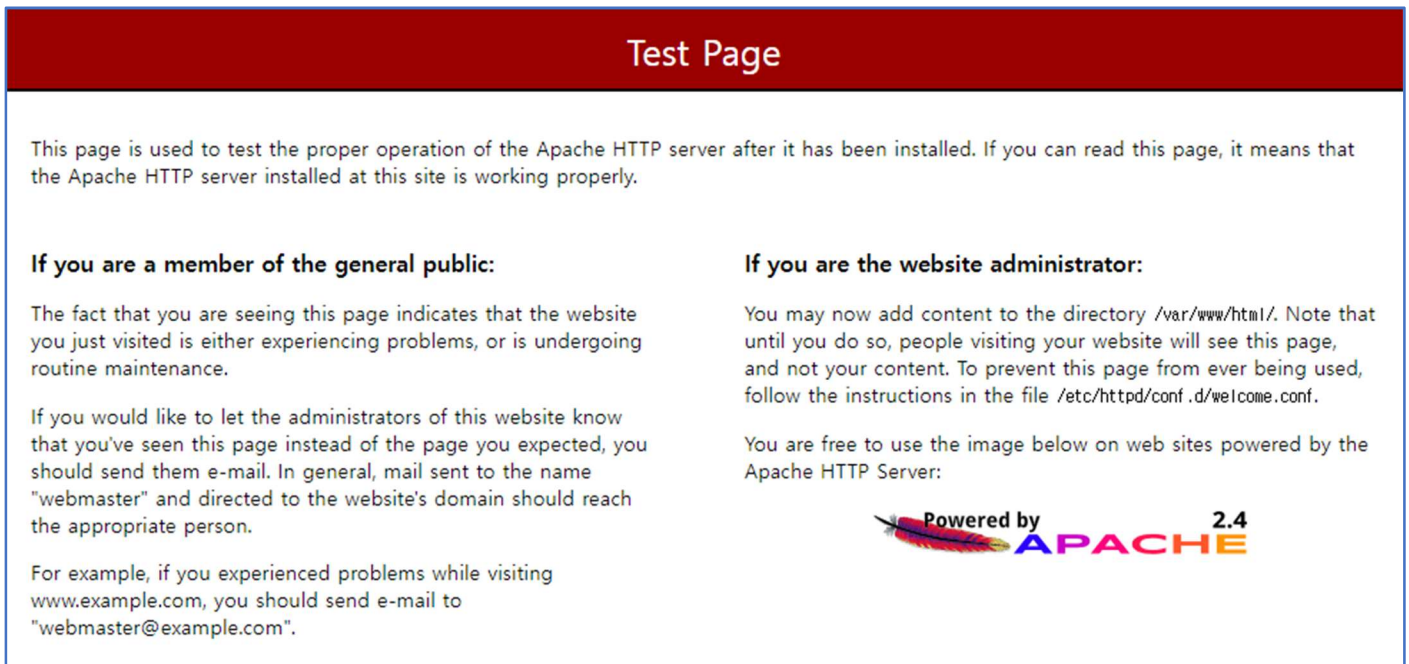
29. 지침 위에 있는 **세부 정보(Details)** 드롭다운 메뉴를 선택한 후 **보기(Show)**를 선택합니다.

**WebServerIP** 값을 복사합니다.

30. 새 웹 브라우저 탭을 열고 복사한 **WebServerIP** 를 붙여넣은 다음 Enter 키를 누릅니다.

웹 서버 **테스트 페이지(Test Page)**가 표시됩니다.

이제 존재하지 않는 페이지에 액세스를 시도하여 로그 데이터를 생성합니다.



31. 브라우저 URL 에 `/start` 를 추가하고 Enter 키를 누릅니다.

페이지를 찾을 수 없으므로 오류 메시지가 표시됩니다. 그래도 괜찮습니다. CloudWatch Logs 로 전송되는 액세스 로그에 데이터가 생성됩니다.



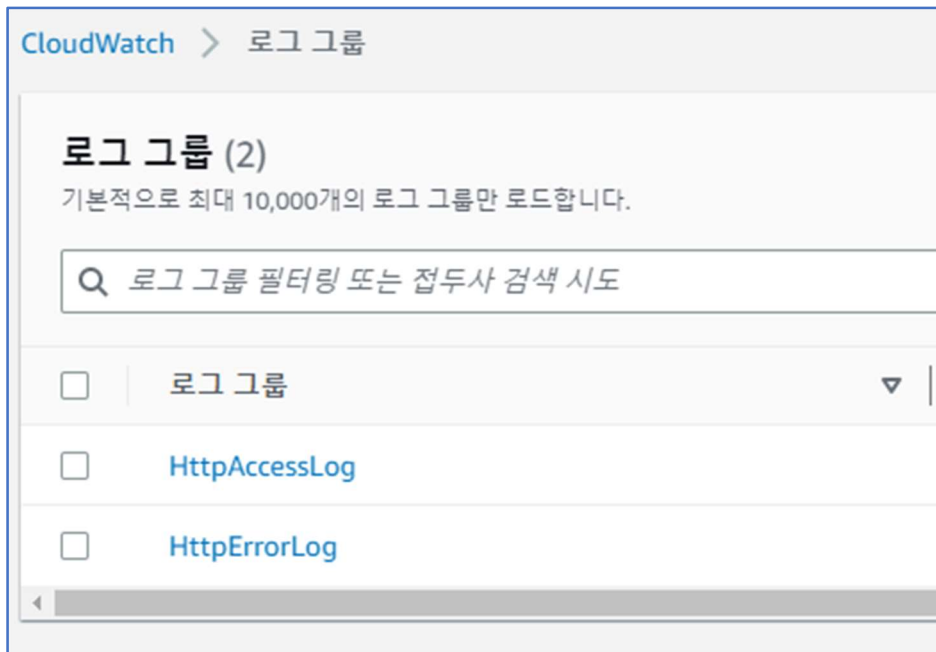
32. 웹 브라우저에서 이 탭을 계속 열어 두고 AWS Management Console 이 표시된 브라우저 탭으로 돌아갑니다.

33. **서비스(Services)** 메뉴에서 **CloudWatch** 를 선택합니다.

34. 왼쪽 탐색 창에서 **로그 그룹(Log groups)**를 선택합니다.

**HttpAccessLog** 와 **HttpErrorLog** 라는 2 개의 로그가 나열되어야 합니다.

이러한 로그가 나열되지 않으면 잠시 기다린 다음 **새로 고침(Refresh)**을 클릭합니다.



35. **HttpAccessLog** 를 선택합니다(이름 자체를 선택).

36. **로그 스트림(Logs streams)** 섹션의 표에서 **로그 스트림(Log stream)**을 선택합니다(이름 자체를 선택). 로그가 연결된 EC2 인스턴스와 ID 가 같습니다.

웹 서버로 전송된 **GET** 요청으로 구성된 로그 데이터가 표시되어야 합니다. 아이콘을 클릭하여 행을 확장하면 추가 정보를 볼 수 있습니다. 로그 데이터에는 요청을 한 컴퓨터와 브라우저에 대한 정보가 포함되어 있습니다.

**/start** 요청과 404 코드가 있는 행이 표시됩니다. 이 코드는 페이지를 찾을 수 없었다는 뜻입니다.

이를 통해 EC2 인스턴스 또는 온프레미스 서버에서 CloudWatch Logs 로 로그 파일이 자동으로 전송되는 방법을 알 수 있습니다. 개별 서버에 로그인하지 않고 로그 데이터에 액세스할 수 있습니다. 웹 서버의 Auto Scaling 플릿과 같은 여러 서버에서 로그 데이터를 수집할 수도 있습니다.

로그 이벤트	
아래의 필터 막대를 사용하여 로그 이벤트의 용어, 구문 또는 값을 검색하고 매칭할 수 있습니다. <a href="#">필터 패턴에 대해 자세히 알아보기</a>	
Q 이벤트 필터링	지우기 1m 30m 1h 12h 사용자 지정 디스플레이 ▼
타임스탬프	메시지
현재 이전 이벤트가 없습니다. <a href="#">재시도</a>	
▶ 2023-08-06T14:21:50.002+09:00	121.136.18.98 - - [06/Aug/2023:05:21:49 +0000] "GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
▶ 2023-08-06T14:21:50.333+09:00	121.136.18.98 - - [06/Aug/2023:05:21:49 +0000] "GET /icons/apache_pb2.gif HTTP/1.1" 200 4234 "http://52.24.50.172/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
▶ 2023-08-06T14:21:54.665+09:00	121.136.18.98 - - [06/Aug/2023:05:21:50 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://52.24.50.172/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
▶ 2023-08-06T14:22:46.665+09:00	121.136.18.98 - - [06/Aug/2023:05:22:41 +0000] "GET /start HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
현재 최신 이벤트가 없습니다. <a href="#">자동 재시도를 일시 중지했습니다.</a> <a href="#">재개</a>	

# CloudWatch Logs 에서 지표 필터 생성

이제 로그 파일에서 **404 오류**를 식별하도록 필터를 구성합니다. 이 오류는 일반적으로 웹 서버에서 잘못된 링크가 생성되어 사용자가 클릭하고 있다는 의미입니다.

37. 왼쪽 탐색 창에서 **로그 그룹(Log groups)**를 선택합니다.

38. **HttpAccessLog** 옆의 확인란을 선택합니다.

39. **작업(Actions)** 드롭다운 메뉴에서 **지표 필터 생성(Create metric filter)**을 선택합니다.

필터 패턴은 로그 파일의 필드를 정의하고 특정 값으로 데이터를 필터링합니다.

40. **필터 패턴(Filter pattern)** 상자에 다음 행을 붙여넣습니다.

```
[ip, id, user, timestamp, request, status_code=404, size]
```

이 행은 CloudWatch Logs 에 로그 데이터의 필드를 어떻게 해석해야 하는지 알려주고, 페이지를 찾을 수 없었음을 나타내는 **status\_code=404** 가 있는 행만 찾도록 필터를 정의합니다.

41. **패턴 테스트(Test pattern)** 섹션에서 **Select log data to test** 드롭다운 메뉴를 사용하여 EC2 인스턴스 ID 를 선택합니다. ID 는 **i-0f07ab62aae4xxxx9** 와 비슷한 형식입니다.

42. **패턴 테스트(Test pattern)** 을 선택합니다.

43. **결과(Results)** 섹션에서 **테스트 결과 보기(Show test results)**를 선택합니다.

**404 \$status\_code** 가 포함된 결과가 하나 이상 표시되어야 합니다. 이는 요청된 페이지를 찾을 수 없었다는 의미입니다.

## 패턴 정의

### 필터 패턴 생성

지표 필터를 사용하여 CloudWatch Logs로 전송되는 로그 그룹에서 이벤트를 모니터링할 수 있습니다. 특정 항목을 모니터링 및 집계하거나 로그 이벤트에서 값을 추출하고 결과를 특정 지표에 연결할 수 있습니다. [패턴 구문에 대해 자세히 알아보십시오.](#)

#### 패턴 필터링

로그 이벤트에서 일치될 항목 또는 패턴을 지정하여 지표를 생성합니다.

[ip, id, user, timestamp, request, status\_code=404, size]



### 패턴 테스트

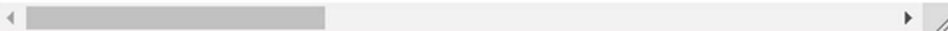
#### 테스트할 로그 데이터 선택

i-0a44dbc469dab1851

#### 로그 이벤트 메시지

필터 패턴을 사용하여 테스트할 로그 데이터를 입력합니다. 줄 바꿈을 사용하여 로그 이벤트를 구분하십시오.

```
121.136.18.98 - - [06/Aug/2023:05:21:49 +0000] "GET / HTTP/1.1" 403 3630 "-" "N
121.136.18.98 - - [06/Aug/2023:05:21:49 +0000] "GET /icons/apache_pb2.gif HTTP
121.136.18.98 - - [06/Aug/2023:05:21:50 +0000] "GET /favicon.ico HTTP/1.1" 404
121.136.18.98 - - [06/Aug/2023:05:22:41 +0000] "GET /start HTTP/1.1" 404 196 "-
```



패턴 테스트

#### 결과

위의 로그 이벤트 메시지를 선택하고 '패턴 테스트'를 클릭하여 결과를 확인하십시오.

Cancel

Next

44. 다음(Next)을 선택합니다.

45. 필터 이름 생성(Create filter name) 섹션의 필터 이름(Filter name) 상자에 404Errors를 입력합니다.

46. 지표 세부 정보(Metric details) 섹션에서 다음 정보를 구성합니다.

- 지표 네임스페이스(Metric namespace): LogMetrics를 입력합니다.
- 지표 이름(Metric name): 404Errors를 입력합니다.
- 지표 값(Metric value): 1을 입력합니다.

47. 다음(Next)을 선택합니다.

48. 검토 및 생성(Review and create) 페이지에서 지표 필터 생성(Create metric filter)를 선택합니다.

이제 이 지표 필터를 경보에서 사용할 수 있습니다.

## Review and create

Step 1: Pattern

Edit

### 필터 패턴 생성

패턴 필터링  
[ip, id, user, timestamp, request, status\_code=404, size]

Step 2: Metric

Edit

### 지표 할당

이름 필터링	지표 이름
404Errors	404Errors
지표 네임스페이스	지표 값
LogMetrics	1
기본값	Unit
-	-

Cancel

Previous

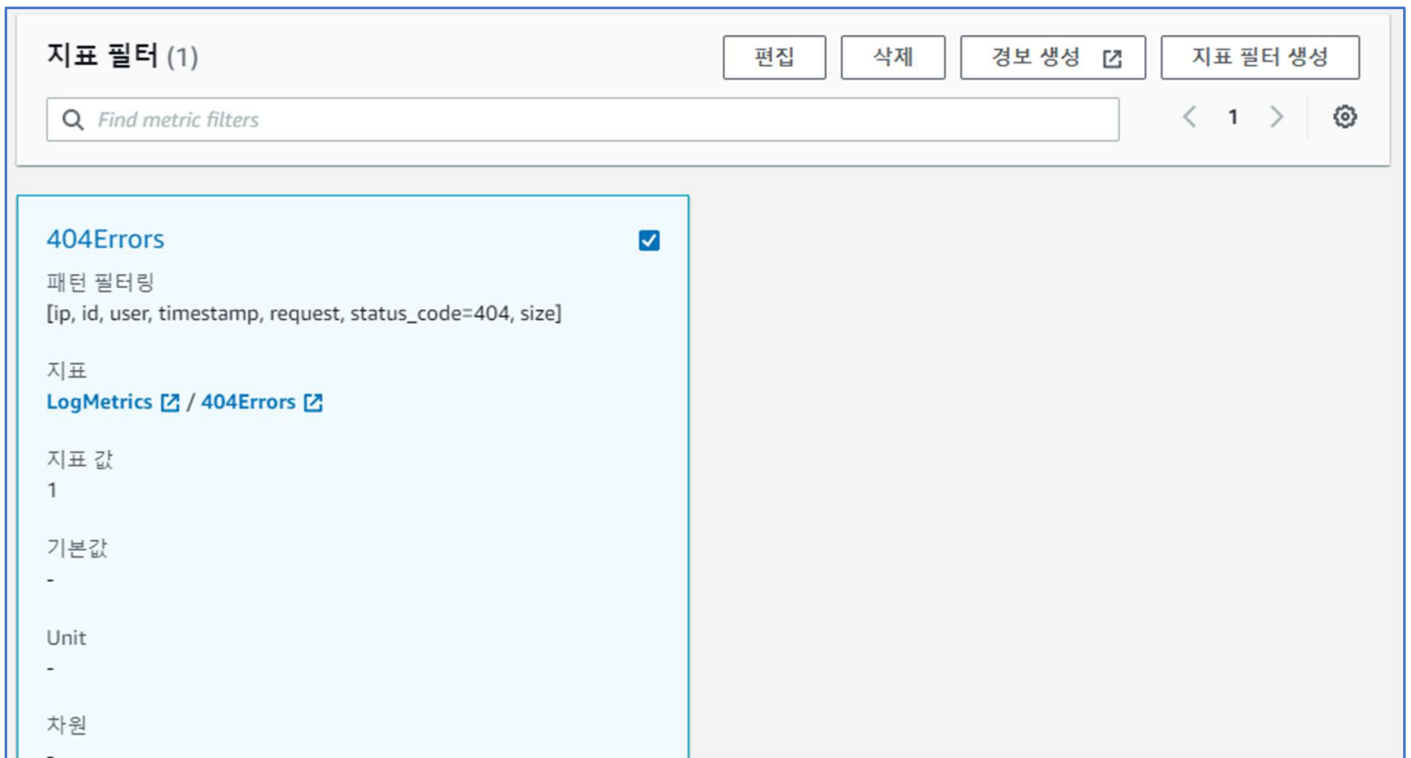
지표 필터 생성

## 필터를 사용하여 경보 생성

이제 **404 Not Found** 오류가 너무 많이 수신될 때 알림을 전송하도록 경보를 구성합니다.

49. **404Errors** 패널에서 오른쪽 상단 모서리에 있는 확인란을 선택합니다.

50. **지표 필터(Metric filters)** 섹션에서 **경보 생성(Create alarm)**을 선택합니다.



51. 다음 설정을 구성합니다.

- **지표(Metrics)** 섹션에서 **기간(Period)**으로 **1 분(minute)**를 선택합니다.
- **조건(Conditions)** 섹션에서 다음을 선택합니다.
  - 다음 경우 항상: **404Errors(Whenever 404Errors is): Greater/Equal** 을 선택합니다.
  - **than: 5** 를 입력합니다.



0

03:00

04:00

05:00

404Errors

기간

1분

조건

임계값 유형

☒ 정적  
값을 임계값으로 사용

☐ 이상 탐지  
대역을 임계값으로 사용

404Errors이(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.

5

↕

숫자여야 함

▶ 추가 구성

- 다음(Next)을 선택합니다.

52. 알림(Notification) 섹션에서 다음을 구성합니다.

- SNS 주제 선택(Select an SNS Topic): 새 주제 생성(Create new topic)을 선택합니다.
- 알림을 받을 이메일 엔드포인트(Email endpoints that will receive the notification): 강의실에서 액세스할 수 있는 이메일 주소를 입력합니다.
- 주제 생성(Create topic)을 선택합니다.

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.

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...

이 계정의 이메일 목록만 사용할 수 있습니다.

이메일(엔드포인트)

javaexpert@nate.com - SNS 콘솔에서 보기

알림 추가

- 다음(Next)을 선택합니다.

53. 이름 및 설명(Name and description)의 경우 다음 설정을 구성합니다.

- 경보 이름(Alarm name): 404 Errors 를 입력합니다.
- 경보 설명(Alarm description): Alert when too many 404s detected on an instance 를 입력합니다.
- 다음(Next)을 선택합니다.

## 이름 및 설명 추가

### 이름 및 설명

경보 이름

404 Errors


경보 설명 - 선택 사항 서식 가이드라인 보기

편집

미리 보기

Alert when too many 404s detected on an instance

최대 1024자(48/1024)

 마크다운 서식은 콘솔에서 경보를 볼 때만 적용됩니다. 설명은 경보 알림에서 일반 텍스트 서식으로 유지됩니다.

취소


이전

다음

54. **경보 생성(Create alarm)**을 선택합니다.

55. 이메일로 가서 확인 메시지를 찾고 **구독 확인(Confirm subscription)** 링크를 선택합니다.

☆ AWS Notification - Subscription Confirmation

 보낸사람 : "AWS Notifications" <no-reply@sns.amazonaws.com> | 주소록추가 | 수신차단

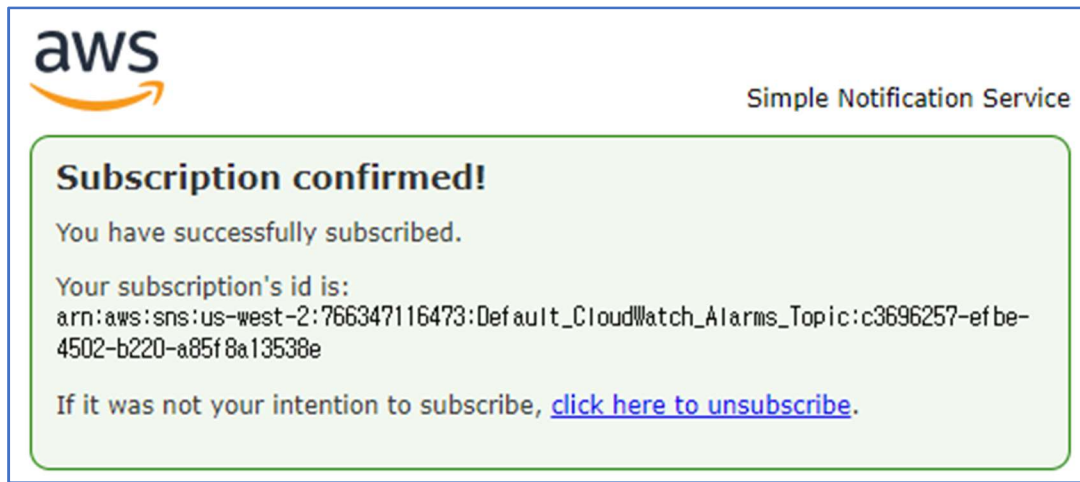
You have chosen to subscribe to the topic:

**arn:aws:sns:us-west-2:766347116473:Default\_CloudWatch\_Alarms\_Topic**

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):

[Confirm subscription](#)

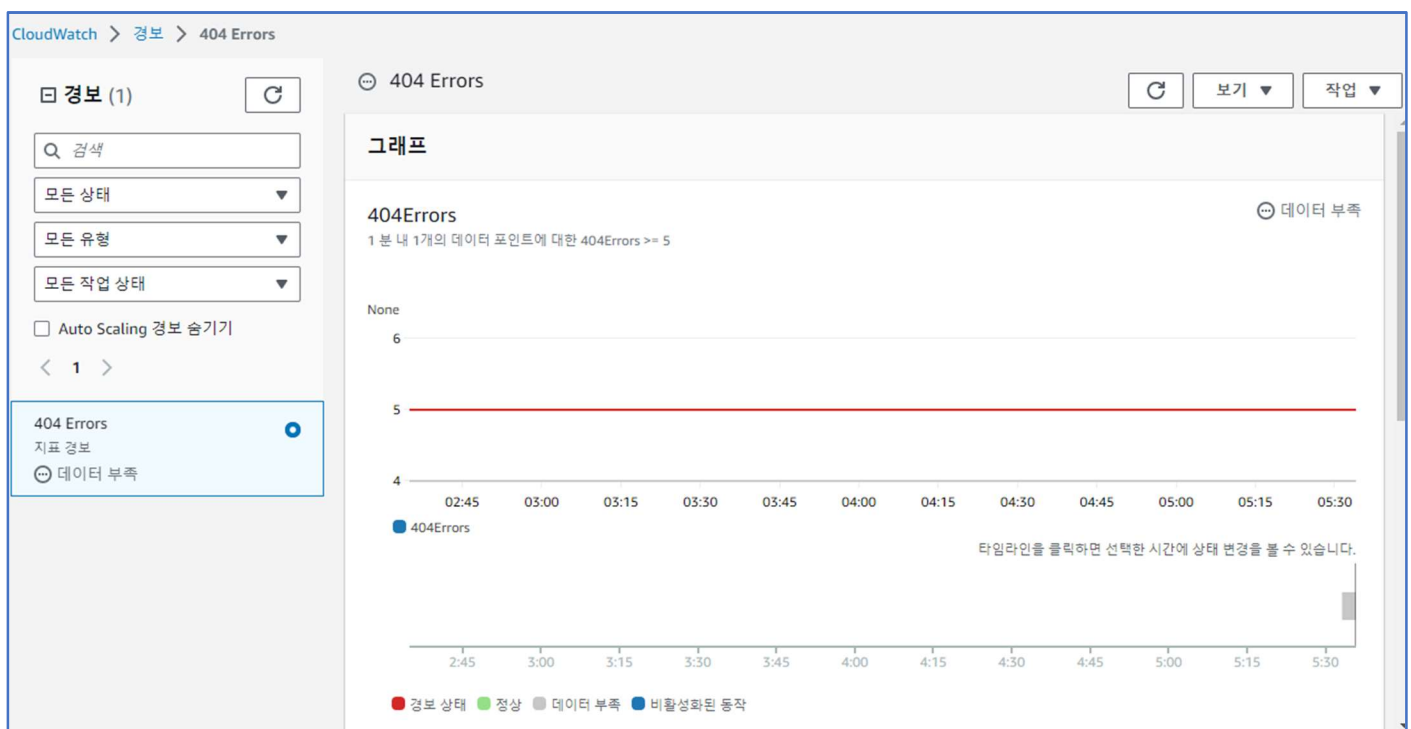
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirma



56. AWS Management Console 로 돌아갑니다.

57. 왼쪽 탐색 창에서 **CloudWatch** 를 선택합니다(맨 위).

경보가 **주황색**이어야 합니다. 이는 경보를 트리거할 데이터가 충분하지 않다는 의미입니다. 이 경보는 지난 1 분 동안 데이터가 수신되지 않았기 때문에 표시됩니다.



이제 웹 서버에서 액세스하여 로그 데이터를 생성합니다.

58. 웹 서버가 열린 웹 브라우저 탭으로 돌아갑니다.

웹 브라우저 탭이 더 이상 열려 있지 않다면 지침 위에 있는 **세부 정보(Details)** 드롭다운 메뉴를 선택하고 **보기(Show)**를 선택합니다.

**WebServerIP** 값을 복사하여 새 웹 브라우저 탭에 붙여넣습니다.

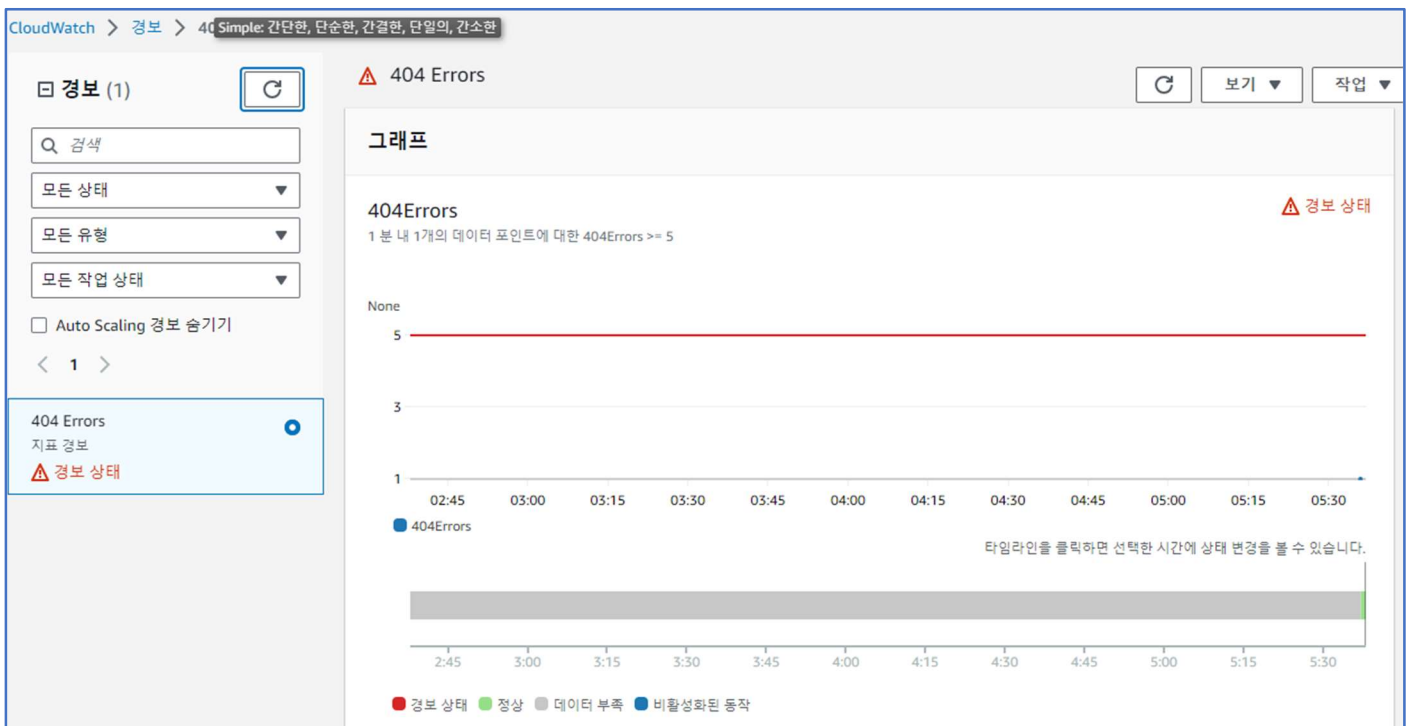
59. IP 주소 뒤에 페이지 이름을 추가하여 존재하지 않는 페이지로 이동을 시도합니다. 이 단계를 5 번 이상 반복합니다.

예를 들면 `http://192.0.2.0/start2` 를 입력합니다.

요청마다 별도의 로그 항목이 생성됩니다.

60. 경보가 트리거될 때까지 1~2 분 기다립니다. AWS Management Console 에서 이따금 **새로 고침(Refresh)**을 선택하여 상태를 업데이트할 수 있습니다.

CloudWatch 페이지에 표시된 그래프가 **빨간색**으로 바뀌어 **경보** 상태임을 나타내야 합니다.



61. 이메일을 확인합니다. 제목이 **ALARM: "404 Errors"**인 이메일이 있을 것입니다.

이 과제는 애플리케이션 로그 데이터로부터 경보를 생성하고 로그 파일에서 비정상적 동작이 감지될 때 경보를 수신하는 방법을 보여줍니다. CloudWatch Logs 안에서 로그 파일에 액세스하여 추가 분석을 통해 경보를 트리거한 활동을 진단할 수 있습니다.

☆ **ALARM: "404 Errors" in US West (Oregon)**

보낸사람 : "AWS Notifications" <no-reply@sns.amazonaws.com> 주소록추가 수신차단

23-08-06 14:38

You are receiving this email because your Amazon CloudWatch Alarm "404 Errors" in the US West (Oregon) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [8.0 (06/08/23 05:37:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Sunday 06 August, 2023 05:38:17 UTC".

View this alarm in the AWS Management Console:  
<https://us-west-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-west-2#alarmsV2:alarm/404%20Errors>

Alarm Details:

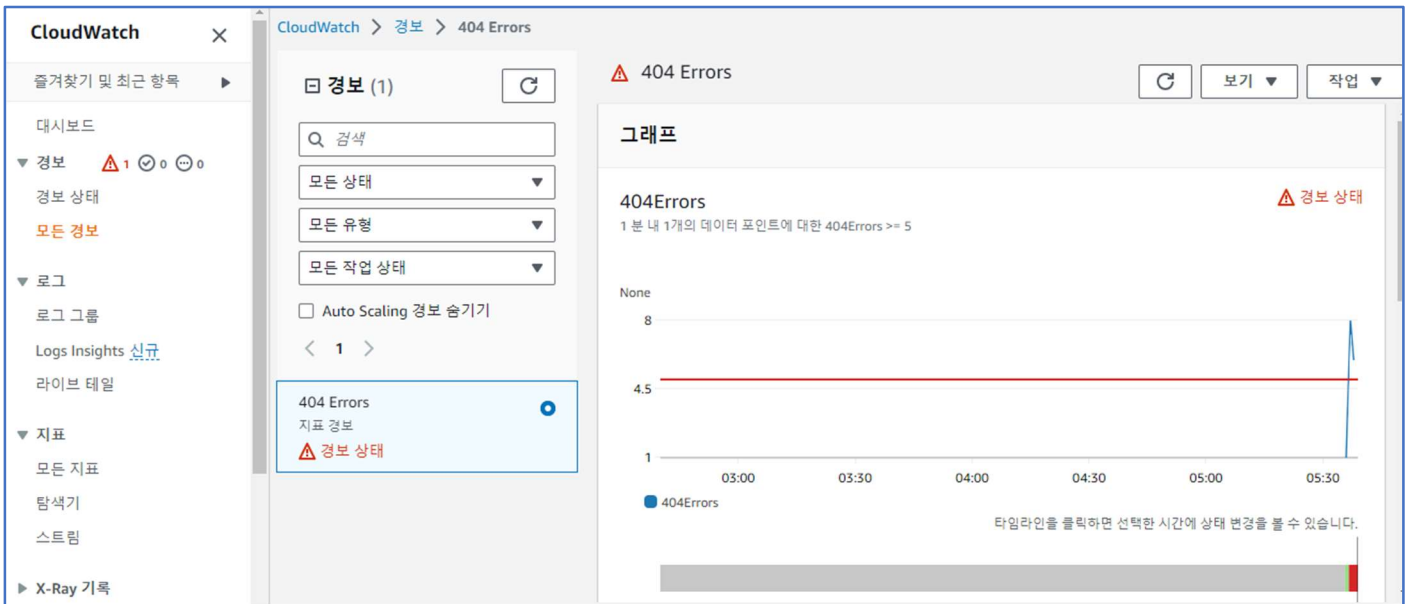
- Name: 404 Errors
- Description: Alert when too many 404s detected on an instance
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [8.0 (06/08/23 05:37:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Sunday 06 August, 2023 05:38:17 UTC
- AWS Account: 766347116473
- Alarm Arn: arn:aws:cloudwatch:us-west-2:766347116473:alarm:404 Errors

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 5.0 for at least 1 of the last 1 period(s) of 60 seconds.

Monitored Metric:

- MetricNamespace: LogMetrics
- MetricName: 404Errors
- Dimensions:
- Period: 60 seconds



# 과제 3: CloudWatch 를 사용하여 인스턴스 지표 모니터링

지표는 시스템 성능에 대한 데이터입니다. CloudWatch 는 AWS 서비스에 대한 지표를 저장합니다. CloudWatch 에이전트를 통해 또는 애플리케이션에서 직접 사용자의 애플리케이션 지표를 게시할 수도 있습니다. CloudWatch 는 검색, 그래프, 대시보드, 경보 지표를 제공할 수 있습니다.

이번 과제에서는 CloudWatch 가 제공하는 지표를 사용합니다.



62. **서비스(Services)** 메뉴에서 **EC2** 를 선택합니다.
63. 왼쪽 탐색 창에서 **인스턴스(Instances)**를 선택합니다.
64. **Web Server** 옆에 있는 확인란을 선택합니다.
65. 페이지 하단에서 **모니터링(Monitoring)** 탭을 선택합니다.

제공된 지표를 살펴봅니다. 차트를 선택하여 더 많은 정보를 표시할 수도 있습니다.

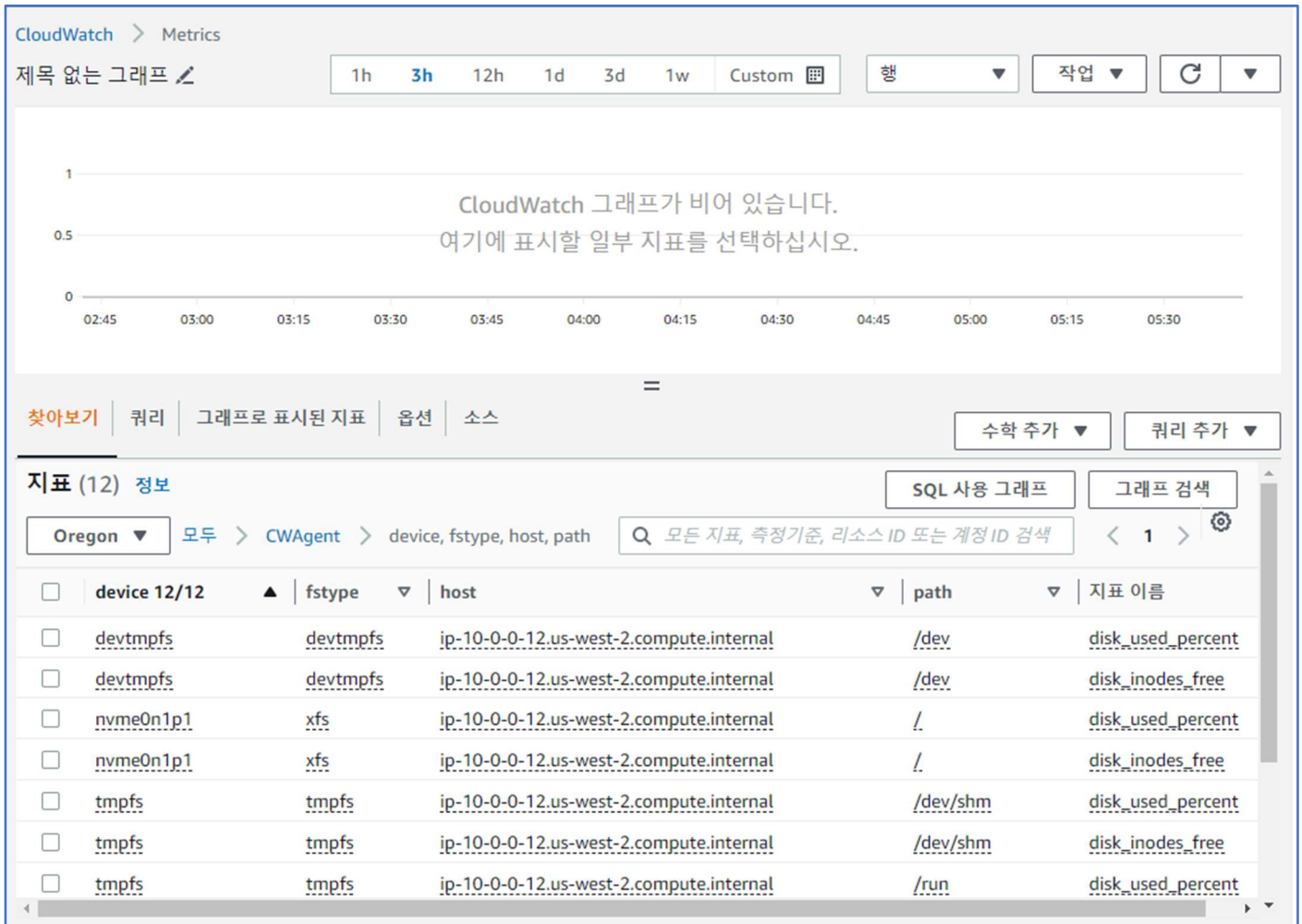
CloudWatch 는 인스턴스의 CPU, 디스크, 네트워크 사용량에 대한 지표를 캡처합니다. 이 지표는 외부에서 인스턴스를 가상 머신으로서 측정하지만, 여유 메모리 또는 여유 디스크 공간과 같은 인스턴스 내부 상황에 대한 정보는 제공하지 않습니다. 다행히 CloudWatch 에이전트가 캡처하는 정보를 사용하면 인스턴스 내부 상황에 대한 정보를 얻을 수 있습니다. CloudWatch 에이전트는 지표를 수집하기 위해 인스턴스 내부에서 실행되기 때문입니다.

66. **서비스(Services)** 메뉴에서 **CloudWatch** 를 선택합니다.
67. 왼쪽 탐색 창에서 **지표(Metrics)**아래의 **All metrics** 를 선택합니다.

페이지 하단에 CloudWatch 가 수집한 여러 지표가 표시됩니다. 이러한 지표 중 일부는 AWS 가 자동으로 생성하며, 일부는 CloudWatch 가 수집합니다.

68. **CWAgent** 를 선택하고 **device, fstype, host, path** 를 선택합니다.

CloudWatch 에이전트가 캡처하고 있는 디스크 공간 지표가 표시됩니다.



69. 표 위에 있는 **모든 지표(All metrics)** 탭[**모두 > CWAgent > device, fstype, host, path**(**All > CWAgent > device, fstype, host, path**)라고 나와 있는 행]에서 **CWAgent** 를 선택합니다.

70. **host** 를 선택합니다.

시스템 메모리와 관련된 지표를 볼 수 있습니다.



찾아보기	쿼리	그래프로 표시된 지표	옵션	소스	수학 추가 ▼	쿼리 추가 ▼
지표 (2) 정보					SQL 사용 그래프	그래프 검색
Oregon ▼	모두 >	CWAgent >	host	Q 모든 지표, 측정기준, 리소스 ID 또는 계정 ID 검색	< 1 >	⚙
<input type="checkbox"/>	host 2/2		▲	지표 이름	▼	
<input type="checkbox"/>	ip-10-0-0-12.us-west-2.compute.internal			mem_used_percent		
<input type="checkbox"/>	ip-10-0-0-12.us-west-2.compute.internal			swap_used_percent		

71. 표 위에 있는 모든 지표(All metrics) 탭[모두 > CWAgent > device, fstype, host, path(All > CWAgent > device, fstype, host, path)라고 나와 있는 행]에서 모두(All)를 선택합니다.

CloudWatch 가 캡처 중인 다른 지표도 살펴봅니다. 이러한 지표는 AWS 계정에서 사용되는 AWS 서비스로부터 전송된 자동 생성 지표입니다.

그래프에 표시할 지표를 선택할 수 있습니다.

## 과제 4: 실시간 알림 생성

CloudWatch Events 는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. 간단한 규칙을 사용하여 일치하는 이벤트를 찾고 이러한 이벤트를 하나 이상의 대상 함수 또는 스트림으로 라우팅할 수 있습니다. CloudWatch Events 는 작동상 변경 사항이 발생하면 항상 이를 감지합니다.

CloudWatch Events 는 환경에 응답하기 위한 메시지를 전송하고, 함수를 활성화하고, 변경 사항을 적용하고, 상태 정보를 캡처하는 등 이러한 작동상 변경에 응답하고 필요에 따라 교정 조치를 취합니다. 또한 CloudWatch Events 를 사용하여 cron 또는 rate 표현식을 통해 특정 시간에 스스로 트리거되는 자동 작업을 예약할 수 있습니다.

이 과제에서는 인스턴스가 중지 또는 종료될 때 사용자에게 알리는 실시간 알림을 생성합니다.



72. 왼쪽 탐색 창에서 **Events** 아래의 **규칙(Rules)**을 선택합니다.

73. **규칙 생성(Create rule)**을 선택합니다.

74. **Define rule detail** 페이지에서 Name 에 Instance\_Stopped\_Terminated 을 입력 후 Next 를 클릭합니다.

**Build event pattern** 페이지에서 Event pattern 섹션을 찾습니다. AWS service 드롭다운 메뉴에서 EC2 를 선택하고 Event type 드롭다운 메뉴에서 EC2 Instance State-change Notification 을 선택합니다. Specific state(s)에서 중지됨(stopped) 및 종료됨(terminated)를 선택하고 **Next** 를 클릭합니다.

## 이벤트 패턴 정보

### 이벤트 소스

AWS 서비스 또는 EventBridge 파트너를 소스로 제공

AWS 서비스

### AWS 서비스

이벤트 소스로 사용되는 AWS 서비스 이름

EC2

### 이벤트 유형

패턴을 매칭하는 데 소스로 사용할 이벤트 유형

EC2 Instance State-change Notification

☐ 모든 상태

☒ 특정 상태

stopped X

terminated X

☒ 모든 인스턴스

☐ 특정 인스턴스 ID

### 이벤트 패턴

이벤트 패턴 또는 이벤트와 일치하는 필터

```
1 {
2   "source": ["aws.ec2"],
3   "detail-type": ["EC2 Instance State-change Notification"],
4   "detail": {
5     "state": ["stopped", "terminated"]
6   }
7 }
```

복사

테스트 패턴

패턴 편집

취소

이전

다음

75. **Select target(s)**의 Target 1 에서 다음과 같이 설정하고 Next 를 선택합니다.

- **Select a target : SNS topic**
- **Topic : Default\_CloudWatch\_Alarms\_Topic** 에서 **Default\_CloudWatch\_Alarms\_Topic** 옵션을 선택합니다.

## 대상 선택



### 권한

참고: EventBridge 콘솔을 사용할 때, EventBridge는 선택된 대상에 대한 적절한 권한을 자동으로 구성합니다. AWS CLI, SDK 또는 CloudFormation을 사용하는 경우 적절한 권한을 구성해야 합니다.

### 대상 1개

#### 대상 유형

EventBridge 이벤트 버스, EventBridge API 대상(SaaS 파트너) 또는 다른 AWS 서비스를 대상으로 선택합니다.

- ☐ EventBridge 이벤트 버스
- ☐ EventBridge API 대상
- ☒ AWS 서비스

#### 대상 선택 | 정보

이벤트가 이벤트 패턴과 일치하거나 일정이 트리거될 때 호출할 대상을 선택합니다(규칙당 5개의 대상으로 제한).

SNS 주제

#### 주제

Default\_CloudWatch\_Alarms\_Topic



76. **Configure tags(태그 구성) - optional** 에서 **Next** 선택 후 **Create rule** 을 선택합니다.

## 실시간 알림 구성

Amazon Simple Notification Service(Amazon SNS)가 휴대전화(SMS) 또는 이메일 주소로 실시간 알림을 전송하도록 구성할 수 있습니다. SMS 메시징을 구성하려면 AWS Support 를 통해 티켓을 열어야 하고 계정 변경 사항을 구성할 시간도 있어야 하므로 앞서 이 연습을 완료하기 위해 사용했던 이메일 주소를 똑같이 사용하겠습니다.

[Amazon Simple Notification Service 개발자 가이드](#)에서 SNS 로 SMS 메시징을 구성하는 방법을 자세히 알아보십시오.

77. **서비스(Services) 메뉴에서 간단 알림 서비스(Simple Notification Service)**를 선택합니다.
78. 왼쪽 탐색 창에서 **주제(Topics)**를 선택합니다.
79. **이름(Name)** 열에서 링크를 선택합니다.

이메일 주소에 연결된 단일 구독 1 개가 표시됩니다. 이는 과제 2 에서 구성한 주제입니다.

Amazon SNS > 주제 > Default\_CloudWatch\_Alarms\_Topic

Default\_CloudWatch\_Alarms\_Topic

세부 정보

이름 Default_CloudWatch_Alarms_Topic	표시 이름 -
ARN arn:aws:sns:us-west-2:766347116473:Default_CloudWatch_Alarms_Topic	주제 소유자 766347116473
유형 표준	

구독 | 액세스 정책 | 데이터 보호 정책 | 전송 정책(HTTP/S) | 전송 상태 로깅 | 암호화 | 태그 | 통합

구독 (1)

검색

ID	엔드포인트	상태
c3696257-efbe-4502-b220-a85f8a13538e	javaexpert@nate.com	확인됨

80. 서비스(Services) 메뉴에서 EC2 를 선택합니다.
81. 왼쪽 탐색 창에서 인스턴스(Instances)를 선택합니다.
82. Web Server 옆에 있는 확인란을 선택합니다.
83. 인스턴스 상태(Instance state) 를 선택하고 인스턴스 중지(Stop instance) 및 중지(Stop)을 차례로 선택합니다.

웹 서버 인스턴스가 중지 중(Stopping) 상태가 됩니다. 1 분 후 중지 됨(Stopped) 상태가 됩니다.

중단된 인스턴스에 대해 자세히 설명하는 이메일을 받게 됩니다.

☆ AWS Notification Message

보낸사람: "AWS Notifications" <no-reply@sns.amazonaws.com> | 주소록추가 | 수신차단

23-

```
{
  "version": "0",
  "id": "9c7779b1-16f8-d323-1b4a-8959c75bc2e8",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "766347116473",
  "time": "2023-08-06T05:52:37Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2:766347116473:instance/i-0a44dbc469dab1851"
  ],
  "detail": {
    "instance-id": "i-0a44dbc469dab1851",
    "state": "stopped"
  }
}
```

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:  
[https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:766347116473:Default\\_CloudWatch\\_Alarms\\_Topic:c3696257-efbe-4502-b220-a85f8a13538e&Endpoint=javaexpert@nate.com](https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:766347116473:Default_CloudWatch_Alarms_Topic:c3696257-efbe-4502-b220-a85f8a13538e&Endpoint=javaexpert@nate.com)

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

☆ AWS Notification Message

보낸사람: "AWS Notifications" <no-reply@sns.amazonaws.com> | 주소록추가 | 수신차단

23-08-06 15:14

```
{
  "version": "0",
  "id": "9accb61e-c5be-8907-da1f-17c3966f4edd",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "766347116473",
  "time": "2023-08-06T06:14:09Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2:766347116473:instance/i-0a44dbc469dab1851"
  ],
  "detail": {
    "instance-id": "i-0a44dbc469dab1851",
    "state": "terminated"
  }
}
```

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:  
[https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:766347116473:Default\\_CloudWatch\\_Alarms\\_Topic:c3696257-efbe-4502-b220-a85f8a13538e&Endpoint=javaexpert@nate.com](https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:766347116473:Default_CloudWatch_Alarms_Topic:c3696257-efbe-4502-b220-a85f8a13538e&Endpoint=javaexpert@nate.com)

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

이 메시지는 JSON 형식입니다. 보다 쉽게 읽을 수 있는 메시지를 수신하기 위해 CloudWatch Events 에 의해 트리거되는 AWS Lambda 함수를 생성할 수 있습니다. 그러면 Lambda 함수가 보다 읽기 쉬운 메시지 형식을 지정해 Amazon SNS 를 통해 전송할 수 있습니다.

이 과제는 인프라 변경 시 실시간 알림을 수신하는 방법을 보여줍니다.

## 과제 5: 인프라 규정 준수 모니터링

AWS Config 는 AWS 리소스의 구성을 측정, 감사 및 평가할 수 있는 서비스입니다. AWS Config 는 AWS 리소스 구성을 지속적으로 모니터링하고 기록하며, 원하는 구성을 기준으로 기록된 구성을 자동으로 평가합니다.

AWS Config 를 사용하면 AWS 리소스 간 구성 및 관계의 변화를 검토하고, 자세한 리소스 구성 기록을 분석하며, 내부 지침에 지정되어 있는 구성을 기준으로 전반적인 규정 준수 여부를 확인할 수 있습니다. AWS Config 를 통해 규정 준수 감사, 보안 분석, 변경 관리 및 운영 문제 해결 작업을 간소화할 수 있습니다.

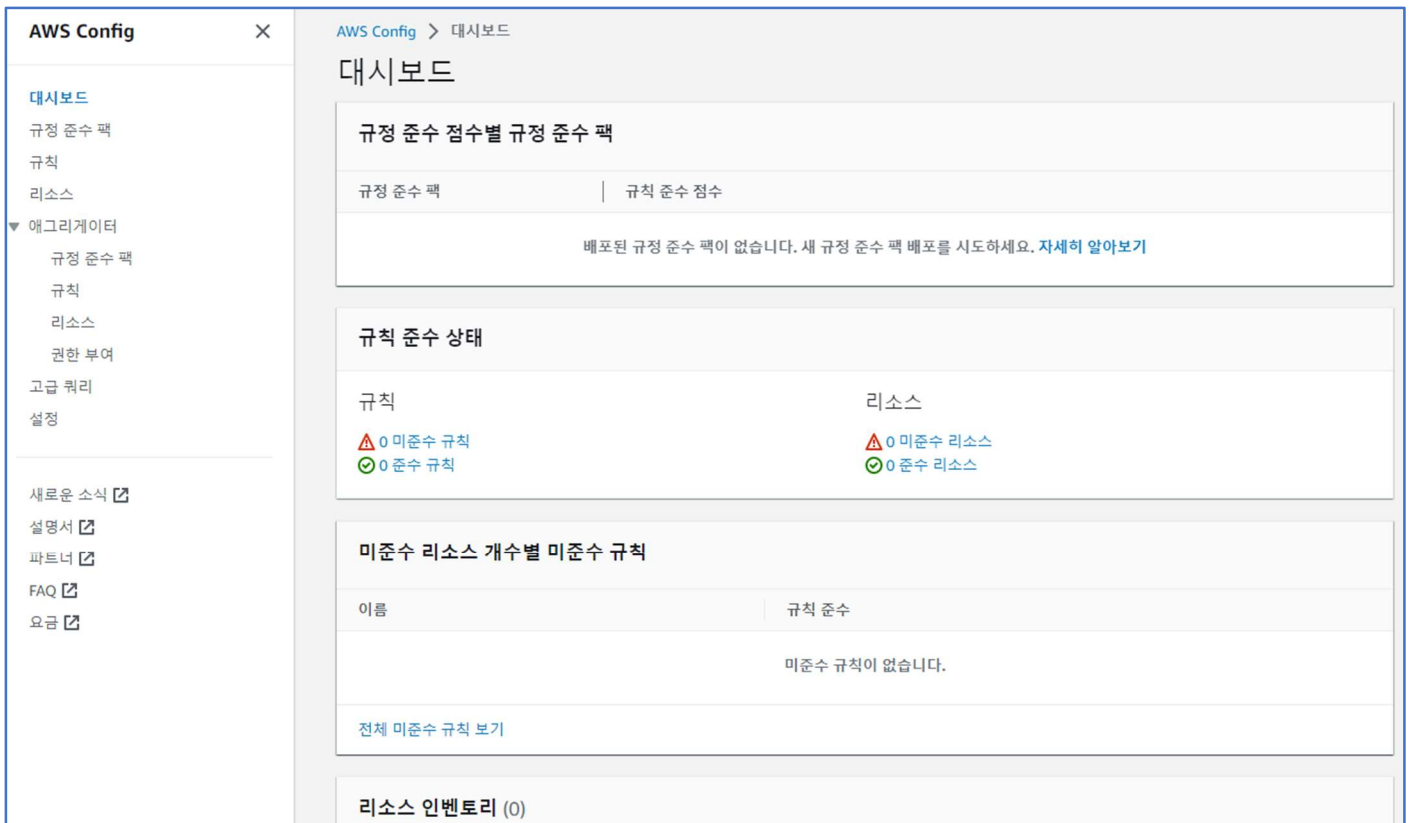
이번 과제에서는 AWS Config 규칙을 활성화하여 태깅 및 Amazon Elastic Block Store(Amazon EBS) 볼륨의 규정 준수를 확인합니다.

84. **서비스(Services)** 메뉴에서 **Config** 를 선택합니다.

85. **시작하기(Get started)** 버튼이 표시되면 다음을 수행합니다.

- **시작하기(Get Started)**를 선택합니다.
- **다음(Next)**을 선택합니다.
- **다음(Next)**을 선택합니다.
- **확인(Confirm)**을 선택합니다.

이렇게 하면 초기 사용을 위해 AWS Config 가 구성됩니다. **AWS Config 오신 것을 환영합니다.(Welcome to AWS Config)** 창이 나타납니다. 이 창은 닫아도 됩니다.



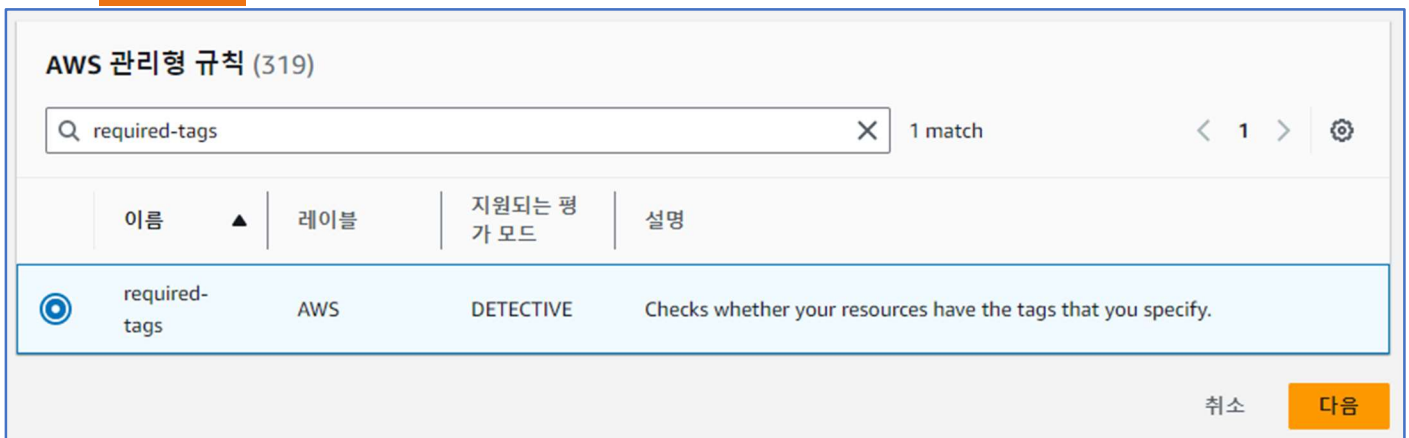
86. 왼쪽 탐색 창에서 위쪽에 있는 **규칙(Rules)**을 선택합니다.

87. **규칙 추가(Add Rule)**을 선택합니다.

88. 검색 필드의 **AWS Managed Rules** 섹션에서 **required-tags**를 입력합니다.

89. **required-tags** 옆에 있는 버튼을 선택합니다.

90. **다음(Next)**을 선택합니다.



리소스마다 project 코드를 요구하는 규칙을 구성합니다.

91. **규칙 구성(Configure rule)** 페이지에서 **파라미터(Parameters)**로 스크롤하고 다음 설정을 구성합니다.

- **tag1Key** 오른쪽에 **project**를 입력합니다(기존 값이 있으면 교체).

## 파라미터

규칙 파라미터는 리소스가 평가되는 속성(예: 필수 태그 또는 S3 버킷)을 정의합니다. 유효하지 않은(키 또는 값이 누락된) 선택적 파

키

tag1Key

값

project

- 페이지 하단의 **다음(Next)**을 선택합니다.
- **규칙 추가(Add rule)**을 선택합니다.

이 규칙은 이제 **project** 태그가 없는 리소스를 찾습니다. 작업 완료에는 몇 분 정도 소요되므로 다음 단계로 진행합니다. 기다릴 필요는 없습니다.

이제 EC2 인스턴스에 연결되지 않은 Amazon EBS 볼륨을 찾는 규칙을 추가합니다.

92. **규칙 추가(Add rule)**을 선택합니다.
93. 검색 필드의 **AWS Managed Rules** 섹션에서 **ec2-volume-inuse-check**를 입력합니다.
94. **ec2-volume-inuse-check** 옆에 있는 버튼을 선택합니다.

### AWS 관리형 규칙 (319)

ec2-volume-inuse-check



1 match

< 1 >



이름



레이블

지원되는 평가 모드

설명



ec2-volume-inuse-check

EC2

DETECTIVE

Checks whether EBS volumes are attached to EC2 instances.

취소

다음

95. **다음(Next)**을 선택합니다.
96. 다시 **다음(Next)**을 선택합니다.
97. **규칙 추가(Add rule)**을 선택합니다.
98. 적어도 하나의 규칙이 평가를 완료할 때까지 기다립니다. 필요한 경우 브라우저 페이지를 새로 고칩니다.

**범위 내 리소스 없음(No resources in scope)** 메시지가 표시되면 몇 분 더 기다리십시오. 이 메시지는 사용 가능한 리소스를 AWS Config가 여전히 탐색 중임을 뜻합니다. 메시지는 시간이 지나면 사라집니다.

99. 각 규칙을 선택하여 감사 결과를 봅니다.

결과에는 다음이 표시되어야 합니다.



- **required-tags:** 규정을 준수하는 EC2 인스턴스 1 개(웹 서버에 **project** 태그가 있으므로)와 **project** 태그가 없는 규정 미준수 리소스 여러 개

범위 내 리소스					
전체 ▼		세부 정보 보기		문제 해결	🔄
		< 1 2 ... >		⚙️	
	ID	유형	상태	주석	규칙 준수
<input type="radio"/>	i-0a44dbc469dab1851	EC2 Instance	-	-	✅ 준수
<input type="radio"/>	igw-04dd88cde60136efe	EC2 InternetGateway	-	-	⚠️ 미준수
<input type="radio"/>	igw-0b39e1ed6b68fb9...	EC2 InternetGateway	-	-	⚠️ 미준수

- **ec2-volume-inuse-check:** 규정 준수 볼륨 1 개(인스턴스에 연결됨)와 규정 미준수 볼륨 1 개(인스턴스에 연결되지 않음)

범위 내 리소스					
전체 ▼		세부 정보 보기		문제 해결	🔄
		< 1 >		⚙️	
	ID	유형	상태	주석	규칙 준수
<input type="radio"/>	vol-04da8922132146...	EC2 Volume	-	-	✅ 준수
<input type="radio"/>	vol-08484ef925df2037a	EC2 Volume	-	-	⚠️ 미준수

AWS Config 에는 사전 정의된 대규모 규정 준수 검사 라이브러리가 있으며, AWS Lambda 를 사용하여 자체 AWS Config 규칙을 작성하는 방법으로 추가 검사를 생성할 수 있습니다.

## 실습 완료

축하합니다. 실습을 마쳤습니다.

100. 이 페이지의 상단에서 **실습 종료**를 선택하고 **예**를 선택하여 실습 종료를 확인합니다.

**\*\*삭제가 시작되었습니다.(DELETE has been initiated...)** 이제 이 메시지 상자를 닫아도 됩니다.**\*\* (You may close this message box now.\*\*)**라는 내용의 패널이 표시됩니다.

101. 오른쪽 상단 모서리에 있는 **X** 를 선택하여 패널을 닫습니다.

## 추가 리소스

AWS Training and Certification 에 대한 자세한 내용은 <https://aws.amazon.com/training/>을 참조하십시오.

여러분의 피드백을 환영합니다.

제안이나 수정 사항을 공유하려면 [AWS Training and Certification 연락처 양식](#)에서 세부 정보를 제공해 주십시오.

© 2021 Amazon Web Services, Inc. and its affiliates. All rights reserved. 본 내용은 Amazon Web Services, Inc.의 사전 서면 허가 없이 전체 또는 일부를 복제하거나 재배포할 수 없습니다. 상업적인 복제, 대여 또는 판매는 금지됩니다.