

# 185- [JAWS] - 활동 - Amazon S3 작업

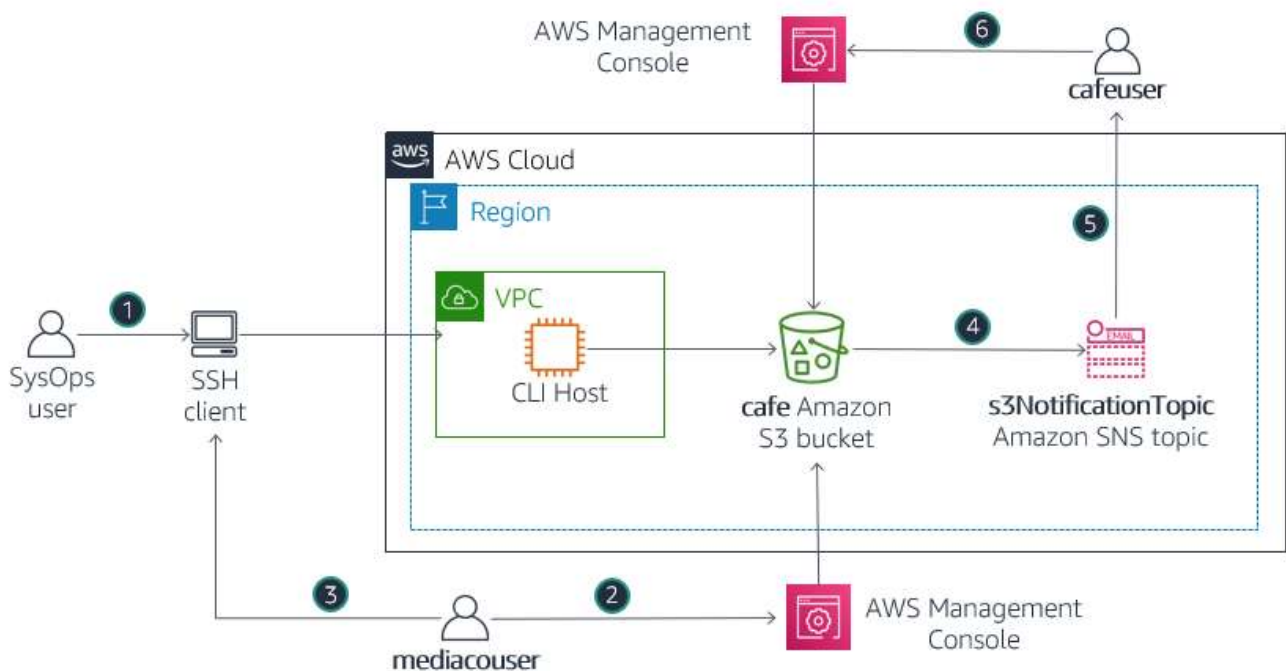
## 활동 - Amazon S3 작업

### 활동 개요

이번 활동에서는 카페 사용자(*cafeuser*)와 카페 판매 제품의 사진을 제공하도록 고용된 외부 미디어 회사 사용자(*mediacouser*) 간에 이미지를 공유할 수 있도록 Amazon S3 버킷을 생성하고 구성합니다. 또한 버킷 콘텐츠가 수정되면 카페 사용자에게 이메일 알림이 전송되도록 S3 버킷을 구성합니다.

이 다이어그램은 Amazon S3 파일 공유 솔루션의 구성 요소 아키텍처 및 다음의 단계로 이루어진 사용 흐름을 설명합니다.

### Amazon S3 공유 버킷 아키텍처 다이어그램:



1. 카페의 시스템 운영자가 *cafe* 라는 이름의 Amazon S3 버킷을 이미지 공유용 컨테이너로 생성 및 구성합니다. 외부 미디어 회사의 사용자가 버킷에서 이미지를 추가, 변경 또는 삭제할 수 있도록 *mediacouser*라는 이름의 AWS Identity and Access Manager(IAM) 사용자가 적절한 S3 권한이 부여된 상태로 미리 생성되었습니다. Martha 또는 Frank 가 알림을 받고 버킷 콘텐츠를 살펴볼 수 있도록 *cafeuser*라는 다른 IAM 사용자 또한 미리 생성되었습니다. 사용자가 역할에 따라 안전하고 적절한 방식으로 버킷에 액세스할 수 있도록 각 사용자에게 필요한 S3 권한을 검토했습니다.
2. 새로운 제품 사진이 있거나 기존 사진을 업데이트해야 할 때는 미디어 회사 담당자가 AWS 관리 콘솔에 *mediacouser*로 로그인하여 버킷 콘텐츠를 업로드, 변경 또는 삭제합니다.
3. *mediacouser*는 또한 AWS Command Line Interface(AWS CLI)를 사용하여 S3 버킷의 콘텐츠를 변경할 수도 있습니다.
4. Amazon S3 가 버킷 콘텐츠 변경을 감지하면 *s3NotificationTopic* Amazon Simple Notification Service(Amazon SNS) 주제에 알림을 게시합니다.
5. **s3NotificationTopic** 을 구독 중인 *cafeuser*는 버킷 콘텐츠 변경 사항이 자세히 나와 있는 이메일 메시지를 받게 됩니다.
6. *cafeuser*는 그런 다음 AWS 관리 콘솔에 로그인하여 새로 업로드된 이미지나 버킷 콘텐츠의 변경 사항을 확인할 수 있습니다.

## 활동 목표

이 활동을 완료하면 다음을 할 수 있게 됩니다.

- *s3api* 및 *s3* AWS CLI 명령을 **사용**하여 Amazon S3 버킷을 생성하고 구성합니다.
- 외부 사용자와 파일 공유가 가능하도록 Amazon S3 버킷을 **구성**합니다.
- Amazon S3 권한을 사용하여 서로 다른 액세스 요구 사항에 따라 Amazon S3 버킷을 **보호**합니다.
- Amazon S3 버킷의 이벤트 알림을 **구성**합니다.

# 비즈니스 사례 관련성

카페의 새로운 비즈니스 요구 사항 - 외부 파트너와 파일 공유



Frank 는 새로운 레시피를 실험하며 카페의 제품 목록을 확장하기 시작했습니다. 새로운 제품을 카페 웹 사이트의 온라인 메뉴에도 올리고 싶어 합니다. 그래서 신제품을 선보이는 사진 포트폴리오를 만들기 위해 외부 미디어 회사를 고용했습니다.

Frank 는 편리하고 안전한 곳 한 자리에서 미디어 회사로부터 사진을 전송받고 싶어 합니다. 또한 사진이 업로드되면 웹 사이트에 배포되기 전에 승인할 수 있도록 이메일 알림을 받기를 원합니다. Frank 는 Sofia 에게 AWS 팀에 솔루션 제안을 요청하라고 부탁드립니다.

AWS 개발자인 Faythe 는 Amazon S3 를 사용하여 외부 파트너와 파일을 공유할 것을 제안합니다.

이번 활동에서는 여러분이 Sofia 의 역할을 맡아 Amazon S3 파일 공유 솔루션을 구현합니다. 또한 Frank 와 미디어 회사 사용자 역할도 맡아 Amazon S3 사용 시나리오를 테스트하고 검증합니다.

## 활동 단계

소요 시간: 이 활동을 완료하는 데는 약 **90 분**이 소요됩니다.

# 활동 환경 시작

7. 지침의 맨 위에서 **Start Lab** 을 클릭하여 실습을 시작합니다.

Start Lab 패널이 열리고 실습 상태가 표시됩니다.

8. 'Lab status: ready' 메시지가 표시되면 **X** 를 클릭하여 Start Lab 패널을 닫습니다.

9. 지침의 맨 위에서 **AWS** 를 클릭합니다.

그러면 새 브라우저 탭에서 AWS 관리 콘솔이 열립니다. 로그인은 자동으로 이루어집니다. **New AWS Console Home** 팝업 창에서 **Maybe later** 를 클릭합니다.

**팁:** 새 브라우저 탭이 열리지 않는 경우 일반적으로 브라우저에서 팝업 창을 열 수 없음을 나타내는 배너 또는 아이콘이 브라우저 상단에 표시됩니다. 배너 또는 아이콘을 클릭하고 'Allow pop ups'를 선택합니다.

10. 이 지침과 함께 표시되도록 AWS 관리 콘솔 탭을 정렬합니다. 두 브라우저 탭이 동시에 표시되어 실습 단계를 보다 쉽게 수행할 수 있게 됩니다.

Credentials

Cloud Access

AWS CLI: 

Show

Cloud Labs

Remaining session time: 02:54:23 (175 minutes)  
Session started at: 2023-08-05T19:02:39-0700  
Session to end at: 2023-08-05T22:02:39-0700  
  
Accumulated lab time: 00:05:00 (5 minutes)  
  
ips -- public:54.212.111.244, private:10.200.0.110

SSH key 

Show

Download PEM

Download PPK

AWS SSO 

Download URL

SecretKey	o1PD7TUE7kLEtIDMS9LvCZN/GcTnOAJp889pCZhQ
LabRegion	us-west-2
AccessKey	AKIAXUYUPVRQ3XVON73J

# 과제 1: SSH 를 사용해 AWS CLI Host 인스턴스에 연결

여러분의 실습 환경에 제공된 **CLI Host** 인스턴스에 대한 보안 셸(SSH) 세션을 열어 시작합니다. Amazon S3 버킷을 만들고 이 활동에서 필요한 대부분의 버킷 구성 작업을 실행하는 데 AWS CLI 를 사용하게 됩니다.

Windows 사용자라면 과제 1.1 에 설명된 단계를 따릅니다. macOS 또는 Linux 사용자라면 과제 1.2 에 설명된 단계를 따릅니다.

## 과제 1.1: Windows SSH

이 지침은 Windows 사용자에게만 적용됩니다.

macOS 또는 Linux 를 사용 중인 경우, [다음 섹션으로 이동](#)합니다.

11. 작업을 완료하기 전에 이 단계에 포함된 3 개의 주요 항목을 읽어보십시오. Details 패널을 연 후에는 이러한 지침을 볼 수 없습니다.
  - 현재 읽고 있는 지침 위에 있는 **Details** 드롭다운 메뉴를 클릭한 다음 **Show** 를 클릭합니다. Credentials 창이 열립니다.
  - **Download PPK** 버튼을 클릭하고 **labsuser.ppk** 파일을 저장합니다. 브라우저에서 이 파일은 일반적으로 Downloads 디렉터리에 저장됩니다.
  - **X** 를 클릭하여 Details 패널을 닫습니다.
12. 필요한 소프트웨어를 다운로드합니다.
  - **PuTTY** 를 사용하여 SSH 를 통해 Amazon EC2 인스턴스에 연결합니다. 컴퓨터에 PuTTY 가 설치되어 있지 않은 경우 [여기에서 다운로드](#)합니다.
13. **putty.exe** 를 엽니다.
14. 시간 초과가 발생하지 않도록 다음과 같이 PuTTY 를 구성합니다.
  - **Connection** 을 클릭합니다.
  - **Seconds between keepalives** 를 **30** 으로 설정합니다.

이렇게 하면 PuTTY 세션을 더 오래 열어 둘 수 있습니다.

15. PuTTY 세션을 다음과 같이 구성합니다.
  - **Session** 을 클릭합니다.

- **Host Name (or IP address):** CLI Host 인스턴스의 **IPv4 퍼블릭 IP** 주소를 복사하여 붙여 넣습니다. 이 주소를 찾으려면 EC2 콘솔로 돌아가서 **Instances** 를 클릭합니다. CLI Host 인스턴스 옆의 확인란을 선택하고 *Description* 탭에서 **IPv4 퍼블릭 IP** 값을 복사합니다.
- PuTTY 로 돌아가 **Connection** 목록에서 **SSH** 를 확장합니다.
- **Auth** 를 클릭합니다(확장하지 말 것).
- **Browse** 를 클릭합니다.
- 다운로드한 lab#.ppk 파일을 찾아 선택합니다.
- **Open** 을 클릭하여 선택합니다.
- **Open** 을 클릭합니다.

16. 호스트를 신뢰하고 호스트에 연결하려면 **Yes** 를 클릭합니다.

17. **login as** 메시지가 나타나면 `ec2-user` 를 입력합니다.

그러면 EC2 인스턴스에 연결됩니다.

18. [Windows 사용자: 다음 과제로 건너뛰려면 여기를 클릭하십시오.](#)

## 과제 1.2: macOS/Linux SSH

이 지침은 Mac/Linux 사용자에게만 적용됩니다. Windows 사용자는 [다음 과제로 건너뛰십시오.](#)

19. 작업을 완료하기 전에 이 단계에 포함된 3 개의 주요 항목을 읽어보십시오. Details 패널을 연 후에는 이러한 지침을 볼 수 없습니다.

- 현재 읽고 있는 지침 위에 있는 **Details** 드롭다운 메뉴를 클릭한 다음 **Show** 를 클릭합니다. Credentials 창이 열립니다.
- **Download PEM** 버튼을 클릭하고 **labsuser.pem** 파일을 저장합니다.
- **X** 를 클릭하여 Details 패널을 닫습니다.

20. 터미널 창을 열고 `cd` 디렉토리를 labsuser.pem 파일이 다운로드된 디렉터리로 변경합니다.

예를 들어 Downloads 디렉터리에 저장된 경우 다음 명령을 실행합니다.

```
cd ~/Downloads
```

21. 다음 명령을 실행하여 키에 대한 권한을 읽기 전용으로 변경합니다.

```
chmod 400 labsuser.pem
```

22. AWS 관리 콘솔로 돌아간 후 EC2 서비스에서 **Instances** 를 클릭합니다. CLI Host 인스턴스 옆의 확인란을 선택합니다.
23. *Description* 탭에서 **IPv4 퍼블릭 IP** 값을 복사합니다.
24. 터미널 창으로 돌아가서 다음 명령을 실행합니다(<public-ip>를 복사한 실제 퍼블릭 IP 주소로 바꿈).

```
ssh -i labsuser.pem ec2-user@<public-ip>
```

25. 이 원격 SSH 서버에 대한 첫 번째 연결을 허용할지 묻는 메시지가 나타나면 **yes** 를 입력합니다.

인증에 키 페어를 사용 중이므로 암호를 묻는 메시지는 나타나지 않습니다.

## 과제 1.2: CLI Host EC2 인스턴스에서 AWS CLI 구성

26. 다음 방법으로 CLI Host 인스턴스가 실행 중인 리전을 찾습니다.

```
curl http://169.254.169.254/latest/dynamic/instance-identity/document | grep region
```

잠시 후 이 리전 정보가 필요합니다.

```
[ec2-user@ip-10-200-0-110 ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/document | grep region
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             Dload  Upload  Total   Spent    Left   Speed
100  476  100  476    0     0  213k      0  --:--:-- --:--:-- --:--:--  232k
"region" : "us-west-2",
```

27. 보안 인증을 사용하여 AWS CLI 소프트웨어를 업데이트합니다.

```
aws configure
```

28. 메시지가 나타나면 다음 정보를 입력합니다.

- **\*\*AWS Access Key ID\*\***: 지침 상단에 있는 <span id="ssb\_voc\_grey">Details</span> 드롭다운 메뉴를 클릭한 다음 <span id="ssb\_voc\_grey">Show</span>를 클릭합니다. **\*\*AccessKey\*\*** 값을 복사하여 터미널 창에 붙여 넣습니다.
- **\*\*AWS Secret Access Key\*\***: 동일한 Credentials 화면에서 **\*\*SecretKey\*\*** 값을 복사하여 붙여 넣습니다.
- **\*\*Default region name\*\***: EC2 인스턴스가 실행 중인 리전 이름을 입력합니다. 이 정보는 방금 전에 찾은 것입니다. 예를 들어 `us-east-1` 또는 `eu-west-2`를 입력합니다.
- **\*\*Default output format\*\***: `json`

```
[ec2-user@ip-10-200-0-110 ~]$ aws configure
AWS Access Key ID [None]: AKIAUYUPVRQ3XVON73J
AWS Secret Access Key [None]: o1PD7TUe7kLEtIDMS9LvCZN/GcTnOAJp889pCZhQ
Default region name [None]: us-west-2
Default output format [None]: json
```

## 과제 2: Amazon S3 공유 버킷 생성 및 초기화

AWS 는 2 가지 AWS CLI 도구(*s3 CLI* 및 *s3api CLI*)를 제공합니다. 이러한 도구는 명령줄 인터페이스를 통해 Amazon S3 서비스와 상호 작용하는 데 사용할 수 있습니다. *s3 CLI* 는 *s3api CLI* 보다 노출되는 명령 수가 적지만, *s3 CLI* 는 가장 널리 실행되는 태스크를 간소화하는 데 도움이 되는 상위 수준의 작업을 지원합니다.

이번 과제에서는 AWS *s3 CLI* 를 사용하여 Amazon S3 공유 버킷을 생성하고 몇 가지 이미지를 사용하여 초기화합니다. 그리고 나서 버킷 콘텐츠를 나열하여 작업이 완료되었는지 확인합니다.

팁:

- [s3 용 AWS CLI 설명서](#)를 참조하여 이 과제에서 사용해야 할 AWS s3 CLI 명령 구문을 정확히 파악합니다.
- 즐겨 쓰는 텍스트 편집기를 사용하여 명령을 실행하기 전에 필요에 따라 명령을 변경합니다. 구체적으로는 명령을 텍스트 편집기에 복사하여 필요한 변경 사항을 적용한 다음 수정된 명령을 SSH 창에 붙여넣는 것이 좋습니다.

29. `<cafe-xxxxnnn>` S3 버킷을 생성합니다. S3 버킷 이름은 Amazon S3 에 있는 기존의 어떤 버킷 이름과도 중복되어서는 안 되기 때문에 이름에 `-xxxxnnn` 형식의 접미사를 추가합니다. 이때 `xxx` 를 본인의 이니셜로 대체합니다. `nnn` 은 임의의 번호로 대체합니다. **CLI Host** 인스턴스의 SSH 창에 다음을 입력합니다.

```
aws s3 mb s3://<cafe-xxxxnnn> --region <region>
```

명령에서 `<cafe-xxxxnnn>`을 고유한 S3 버킷 이름으로 대체합니다. 또한 `<region>`을 CLI Host 인스턴스가 실행 중인 리전으로 대체합니다.

`make_bucket (mb)` 명령 실행이 완료되면 버킷 이름이 반환됩니다.

```
[ec2-user@ip-10-200-0-110 ~]$ aws s3 mb s3://cafe-henry --region us-west-2
make_bucket: cafe-henry
```



30. S3 버킷에서 **/images** 접두부(prefix) 아래에 이미지를 몇 개 로드합니다. CLI 호스트의 **initial-images** 폴더에 샘플 이미지 파일이 있습니다. **CLI Host** 인스턴스의 SSH 창에 다음을 입력합니다.

```
aws s3 sync ~/initial-images/ s3://<cafe-xxxxnn>/images
```

명령에서 **<cafe-xxxxnn>**을 고유한 S3 버킷 이름으로 대체합니다.

*synchronize (sync)* 명령이 실행되면 업로드 중인 이미지 파일의 이름이 표시됩니다.

```
[ec2-user@ip-10-200-0-110 ~]$ aws s3 sync ~/initial-images/ s3://cafe-henry/images
upload: initial-images/Donuts.jpg to s3://cafe-henry/images/Donuts.jpg
upload: initial-images/Cup-of-Hot-Chocolate.jpg to s3://cafe-henry/images/Cup-of-Hot-Chocolate.jpg
upload: initial-images/Strawberry-Tarts.jpg to s3://cafe-henry/images/Strawberry-Tarts.jpg
```

31. **s3 ls** 명령을 사용하여 버킷 콘텐츠를 나열합니다. 사람이 읽을 수 있는 형식으로 목록을 표시하고 객체의 수와 전체 크기를 포함한 요약 총계를 아래에 표시하도록 선택합니다. **CLI Host** 인스턴스의 SSH 창에 다음을 입력합니다.

```
aws s3 ls s3://<cafe-xxxxnn>/images/ --human-readable --summarize
```

명령에서 **<cafe-xxxxnn>**을 고유한 S3 버킷 이름으로 대체합니다.

*list (ls)* 명령 실행이 완료되면 업로드된 이미지 파일의 세부 정보와 함께 파일의 전체 개수와 크기가 표시됩니다.

```
[ec2-user@ip-10-200-0-110 ~]$ aws s3 ls s3://cafe-henry/images/ --human-readable --summarize
2023-08-06 02:14:28 308.7 KiB Cup-of-Hot-Chocolate.jpg
2023-08-06 02:14:28 371.8 KiB Donuts.jpg
2023-08-06 02:14:28 468.0 KiB Strawberry-Tarts.jpg

Total Objects: 3
Total Size: 1.1 MiB
```

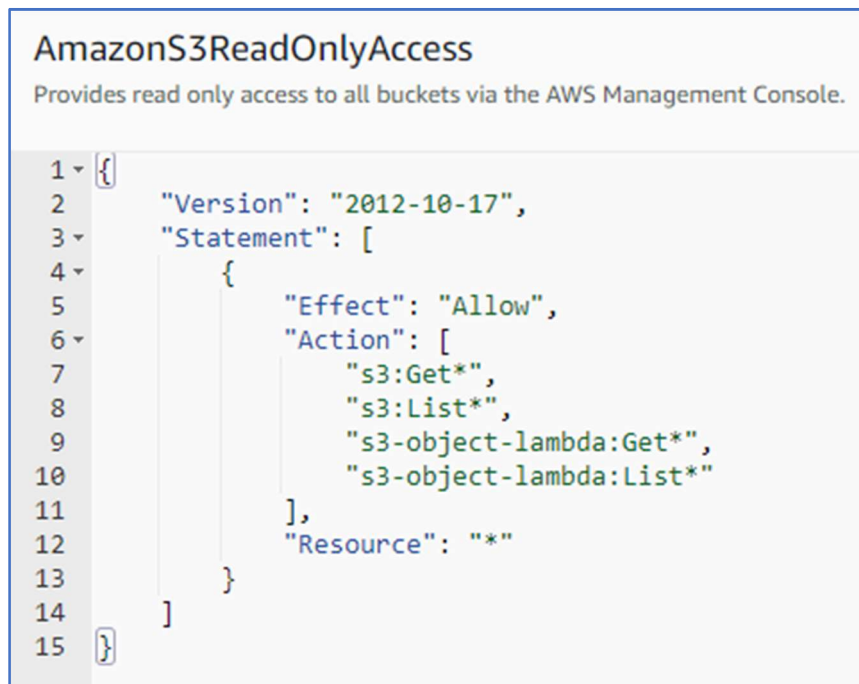
## 과제 3: 미디어 회사 사용자 및 권한 검토

다음으로는 *mediacouser* IAM 사용자에게 할당된 권한을 검토합니다. 이는 여러분을 위해 생성된 사용자입니다. 미디어 회사는 이 사용자를 통해 AWS 관리 콘솔 또는 AWS CLI를 사용하여 S3 공유 버킷에서 이미지를 업로드하고 수정할 수 있습니다. 또한 *cafeuser* 및 *mediacouser* 사용자가 S3 버킷에 액세스할 수 있도록 부여된 권한도 검토합니다.

## 과제 3.1: cafeuser IAM 사용자 검토

이 섹션에서는 *cafeuser* 사용자의 속성을 검토합니다.

32. AWS 관리 콘솔 브라우저 탭에서 **Services > IAM** 을 선택합니다.
33. IAM 콘솔 탐색 창에서 **Users** 를 클릭합니다.
34. 사용자 이름 목록에서 **cafeuser** 를 클릭합니다.
35. **Permissions** 탭에서 *AmazonS3ReadOnlyAccess* 정책 이름 옆의 화살표를 클릭합니다.  
이렇게 하면 정책을 설명하고 정책의 JavaScript Object Notation(JSON) 정의를 보여주는 상자가 열립니다.



36. **{ JSON }** 을 클릭하고 다음과 같은 정책 권한을 살펴봅니다.

- 정책이 어떤 S3 작업을 허용합니까?
- 작업이 어떤 S3 리소스에서 허용됩니까?

강사와 정답을 확인합니다.

## 과제 3.2: mediaco IAM 그룹 검토

이 섹션에서는 *mediaco* 그룹에 할당된 권한을 검토합니다.

37. 왼쪽 탐색 창에서 **User groups** 를 클릭합니다.
38. 그룹 이름 목록에서 **mediaco** 를 클릭합니다.

*mediaco* 그룹에 대한 Summary 페이지가 표시됩니다.

39. **Permissions** 탭에서 *IAMUserChangePassword* 옆의 +를 클릭하여 정책을 확장합니다.



```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "iam:ChangePassword"  
8       ],  
9       "Resource": [  
10        "arn:aws:iam::*:user/${aws:username}"  
11      ]  
12    },  
13    {  
14      "Effect": "Allow",  
15      "Action": [  
16        "iam:GetAccountPasswordPolicy"  
17      ],  
18      "Resource": "*"   
19    }  
20  ]  
21 }
```

40. 사용자가 본인의 암호를 변경하도록 허용하는 AWS 관리 정책을 검토합니다.

41. -를 클릭하여 축소합니다.

42. 마찬가지로 mediaCoPolicy 옆의 +를 클릭합니다.

## mediaCoPolicy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": [  
6         "s3:ListAllMyBuckets",  
7         "s3:GetBucketLocation"  
8       ],  
9       "Resource": [  
10        "arn:aws:s3:::"  
11      ],  
12      "Effect": "Allow",  
13      "Sid": "AllowGroupToSeeBucketListInTheConsole"  
14    },  
15    {  
16      "Action": [  
17        "s3:ListBucket"  
18      ],  
19      "Resource": [  
20        "arn:aws:s3:::cafe-*",  
21        "arn:aws:s3:::cafe-*/*"  
22      ],  
23      "Effect": "Allow",  
24      "Sid": "AllowRootLevelListingOfTheBucket"  
25    },  
  ]  
}
```

```
26 {  
27   "Action": [  
28     "s3:PutObject",  
29     "s3:GetObject",  
30     "s3:GetObjectVersion",  
31     "s3:DeleteObject",  
32     "s3:DeleteObjectVersion"  
33   ],  
34   "Resource": "arn:aws:s3:::cafe-*/images/*",  
35   "Effect": "Allow",  
36   "Sid": "AllowUserSpecificActionsOnlyInTheSpecificPrefix"  
37 }  
38 ]  
39 }
```

**참고:** 정책이 보일 때까지 아래로 스크롤해야 할 수 있습니다.

- **\*\*Sid\*\*** 키 이름 **\*\*AllowGroupToSeeBucketListInTheConsole\*\***로 확인할 수 있는 1 번째 스테이트먼트는 사용자에게 Amazon S3 콘솔을 사용하여 계정의 S3 버킷 목록을 보도록 허용하는 권한을 정의합니다.
- **\*\*Sid\*\*** 키 이름 **\*\*AllowRootLevelListingOfTheBucket\*\***으로 확인할 수 있는 2 번째 스테이트먼트는 사용자가 Amazon S3 콘솔을 사용하여 **\*cafe\*** 버킷에 있는 1 번째 단계 객체와 해당 버킷에 포함된 다른 객체의 목록을 보도록 허용하는 권한을 정의합니다.

- **\*\*Sid\*\*** 키 이름 **\*\*AllowUserSpecificActionsOnlyInTheSpecificPrefix\*\***로 확인할 수 있는 3 번째 스테이트먼트는 사용자가 **\*\*cafe-\*/images\*\*** 폴더의 객체에 실행할 수 있는 액션을 지정하는 권한을 정의합니다. 주요 작업인 **\*GetObject\***, **\*PutObject\***, **\*DeleteObject\***는 각각 **mediacouser**에 부여하려는 **\*읽기\***, **\*쓰기\***, **\*삭제\*** 권한에 상응합니다. 2 가지 추가 작업은 최종 버전 관련 작업에 포함되어 있습니다.

43. -를 클릭하여 축소합니다.

## 과제 3.3: mediacouser IAM 사용자 검토

이 섹션에서는 *mediacouser* 사용자의 속성을 검토합니다.

44. IAM 콘솔 탐색 창에서 **Users**를 클릭합니다.

45. 사용자 이름 목록에서 **mediacouser**를 클릭합니다.

46. Permissions 탭 아래에 2 개의 정책(*IAMUserChangePassword* 및 *mediaCoPolicy*)이 표시됩니다. 이러한 정책은 이전 단계에서 검토한 *mediaco* IAM 그룹에 할당되었습니다.

47. **Groups** 탭을 클릭하여 *mediaco* IAM 그룹을 볼 수 있는지 확인합니다. *mediaco* 사용자는 이 그룹의 구성원이므로 *mediaco* 그룹에 할당된 권한을 상속합니다.

48. **Security credentials(보안 자격 증명)** 탭을 클릭하고 액세스 키 아래의 **Create access key**를 클릭합니다.

- Command Line Interface (CLI)를 선택합니다.
- 하단의 [I understand the above recommendation and want to proceed to create an access key.](위의 권장 사항을 이해했으며 액세스 키 생성을 계속하려고 합니다.) 앞을 체크하고 Next를 클릭합니다.
- Description tag value를 공백으로 두고 [Create access key(액세스 키 만들기)]를 클릭합니다.

49. Retrieve access keys(액세스 키 검색) 페이지에서 액세스 키와 보안 액세스 키 세부 정보를 기록해둡니다.(Download .csv file을 선택하여 다운로드 받아도 됩니다.) 실습의 후반부에서 이 정보가 필요합니다. Done을 클릭합니다.

50. AWS 계정 번호를 복사합니다. 방법은 다음과 같습니다.

- 화면 오른쪽 상단에 있는 **\*\*voclabs/user...\*\*** 드롭다운 메뉴를 클릭합니다.
- 표시되는 계정 번호를 복사합니다. 대시가 포함된 12 자리 번호입니다.
- **\*\*중요\*\***: 콘솔에서 로그아웃하면 **\*\*안 됩니다\*\***. 대신 이 브라우저 탭을 열어둡니다. 나중에 다시 돌아오게 됩니다.

## 과제 3.4: mediacouser 권한 테스트

AWS 관리 콘솔에 *mediacouser*로 로그인하고 S3 공유 버킷의 **images** 폴더 콘텐츠에 보기, 업로드, 삭제 작업을 실행하여 이전에 검토한 권한을 테스트합니다. 이러한 작업은 미디어 회사가 버킷에서 실행할 것으로 예상되는 사용 사례입니다. 또한 외부 사용자가 버킷 권한을 변경하려고 시도하는 무단 사용 사례도 테스트합니다.

51. *mediacouser* 사용자로 AWS 관리 콘솔에 로그인합니다. 방법은 다음과 같습니다.

**중요:** *voclabs...* 사용자로 로그인되어 있는 동안 세션에서 로그아웃하면 안 됩니다.

대신 다음 2 가지 옵션 중 1 개를 선택합니다.

- **옵션 1:** 다른 브라우저 유형을 사용합니다. 예를 들어 Chrome 을 사용하여 이 실습을 시작했으며 Firefox, Safari 또는 Edge 와 같은 다른 브라우저가 있다면 해당 브라우저를 시작합니다.
  - 옵션 1 을 사용하는 경우 아래 옵션 2 섹션은 건너뛵니다.
- **옵션 2:** 같은 브라우저 유형을 사용하되 **시크릿** 또는 **비공개** 브라우저 세션을 엽니다. 옵션 2 의 경우 사용 중인 브라우저 유형에 따라 아래 단계를 따릅니다.
- **Chrome** 을 사용하는 경우: 이 지침을 읽고 있는 브라우저 탭의 오른쪽 상단 모서리에서 세로 점 3 개 아이콘을 클릭한 다음 **New incognito window** 을 선택합니다.
- **Firefox** 또는 **Internet Explorer** 를 사용하는 경우: 이 지침을 읽고 있는 브라우저 탭의 오른쪽 상단 모서리에서 수평선 3 개 아이콘을 클릭한 다음 **새 사생활 보호 창** 을 선택합니다.
- **Safari** 를 사용하는 경우: 바탕 화면 상단의 Safari 메뉴 표시줄에서 파일 > **New Private Window** 를 선택합니다
- **Edge** 를 사용하는 경우: 이 지침을 읽고 있는 브라우저 탭의 오른쪽 상단 모서리에서 가로 점 3 개 아이콘을 클릭한 다음 **New InPrivate window** 을 선택합니다.
- 이제 방금 연 브라우저 탭(**옵션 1 과 2 중 무엇을 따랐는지에 관계없이**) URL 표시줄에 `https://aws.amazon.com/console/` 을 입력하여 이동합니다.
- 표시된 웹 페이지의 IAM 사용자 이름과 암호 필드가 채워져 있지 않다면 페이지 상단에 있는 **My Account** 메뉴에서 **AWS Management Console** 을 선택합니다.
- 이메일 주소와 계정 ID 만 물어보는 화면이 표시된다면 **IAM user** 를 선택하고 방금 복사한 **계정 ID** 를 붙여 넣습니다. 이때 ID 에서 대시를 제거해야 합니다. 그런 다음 **Next** 를 클릭합니다.

- 계정 ID, IAM 사용자 이름, 암호를 물어보는 페이지에서 다음 세부 정보를 입력합니다.

- **Account ID or alias** 에는 복사한 **계정 ID** 를 붙여 넣습니다. 이때 ID 에서 대시를 제거해야 합니다. 이전 화면에서 계정 ID 를 이미 붙여넣었다면 그때 붙여넣은 ID 가 표시되었는지 확인하고 필요한 경우 ID 를 업데이트합니다.
- **IAM user name** 에 `mediacouser` 를 입력합니다.
- **Password** 에 `Training1!` 를 입력합니다.
- **Sign In** 을 클릭합니다.

52. **Services > Storage > S3** 를 선택하거나 **Recently visited** 에서 **S3** 를 선택합니다.

53. 버킷 이름 목록에서 **cafe-xxxnnn** 을 클릭합니다. 여기에서 `xxxnnn` 은 고유한 버킷 이름입니다.

Amazon S3

▶ Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

Buckets (1) Info

Buckets are containers for data stored in S3. [Learn more](#)

↻

Copy content

Empty

Delete

Create bucket

Find buckets by name

< 1 > ⚙

Name	AWS Region	Access	Creation date
cafe-henry	US West (Oregon) us-west-2	Insufficient permissions	August 6, 2023, 11:13:20 (UTC+09:00)

54. **images** 를 클릭합니다. 과제 2 에서 버킷을 초기화했을 때 업로드된 이미지의 목록이 표시됩니다.

Objects (3)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

↻

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

< 1 > ⚙

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	Cup-of-Hot-Chocolate.jpg	jpg	August 6, 2023, 11:14:28 (UTC+09:00)	308.7 KB	Standard
<input type="checkbox"/>	Donuts.jpg	jpg	August 6, 2023, 11:14:28 (UTC+09:00)	371.8 KB	Standard
<input type="checkbox"/>	Strawberry-Tarts.jpg	jpg	August 6, 2023, 11:14:28 (UTC+09:00)	468.0 KB	Standard



55. 보기/ 사용 사례를 테스트합니다. **Donuts.jpg** 를 클릭합니다.

56. **Open** 을 선택합니다.

새 브라우저 탭이 열리고 여러 도넛의 사진이 표시됩니다.

*참고:* 새 브라우저 탭이 열리지 않는 경우 일반적으로 브라우저에서 팝업 창을 열 수 없음을 나타내는 배너 또는 아이콘이 브라우저 상단에 표시됩니다. 배너 또는 아이콘을 클릭하고 'Allow pop ups'를 선택합니다.



57. Donuts.jpg 이미지가 표시된 브라우저 탭을 **닫습니다**.

58. **Console** 탭 상단의 이동 경로에서 **images** 를 클릭하여 **images** 폴더의 내용을 다시 표시합니다.

59. **업로드** 사용 사례를 테스트합니다. **Upload** 를 클릭합니다.

60. **Upload** 대화 상자에서 **Add files** 를 클릭합니다.

61. 로컬 컴퓨터에서 업로드를 테스트할 수 있는 파일 위치로 이동합니다. 그림 파일(jpg 확장자) 또는 단순한 텍스트 파일이 좋습니다.





62. 해당 파일을 선택하고 **Open** 을 클릭합니다.

63. **Upload** 를 클릭합니다. 파일 업로드가 완료되면 **Close** 를 클릭합니다. 해당 파일이 목록에 표시됩니다. 원한다면 파일을 열어 콘텐츠를 확인합니다.



**Objects (4)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	 <a href="#">apples.jpg</a>	jpg	August 6, 2023, 12:19:13 (UTC+09:00)	48.6 KB	Standard
<input type="checkbox"/>	 <a href="#">Cup-of-Hot-Chocolate.jpg</a>	jpg	August 6, 2023, 11:14:28 (UTC+09:00)	308.7 KB	Standard
<input type="checkbox"/>	 <a href="#">Donuts.jpg</a>	jpg	August 6, 2023, 11:14:28 (UTC+09:00)	371.8 KB	Standard
<input type="checkbox"/>	 <a href="#">Strawberry-Tarts.jpg</a>	jpg	August 6, 2023, 11:14:28 (UTC+09:00)	468.0 KB	Standard

64. 삭제 사용 사례를 테스트합니다. **Console** 탭의 이미지 목록에서 **Cup-of-Hot-Chocolate.jpg** 확인란을 선택합니다.

65. **Delete** 를 선택합니다.

66. **Delete objects** 대화 상자의 **Delete objects?** 아래에서 `delete` 를 입력합니다.

67. **Delete objects** 를 선택합니다.

## Delete objects [Info](#)



### You don't have permission to get the Bucket Versioning setting

Without `s3:getBucketVersioning` permission, we cannot determine if this delete action will add a delete marker to your objects or permanently delete them. [Learn more about Identity and access management in Amazon S3](#)



If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.

[Learn more](#)

### Specified objects

< 1 >

Name ▲	Type ▼	Last modified ▼	Size ▼
Cup-of-Hot-Chocolate.jpg	jpg	August 6, 2023, 11:14:28 (UTC+09:00)	308.7 KB

### Delete objects?

To confirm deletion, type *delete* in the text input field.

delete

Cancel

Delete objects

68. 객체가 삭제되어 더 이상 이미지 목록에 표시되지 않습니다.

69. **Close** 를 선택합니다.

70. 마지막으로 mediacouser 가 버킷의 권한을 변경하려고 시도하는 *무단* 사용 사례를 테스트합니다. 상단의 이동 경로에서 **cafe-xxxxnnn** 을 클릭하여 버킷 콘텐츠 목록으로 돌아갑니다.

71. **Permissions** 탭을 클릭합니다. 여기에서 버킷의 권한을 변경할 수 있습니다. *You don't have permission* ~ 과 같은 오류 메시지가 표시됩니다. 이 경우 mediacouser 가 버킷 권한을 변경할 수 없습니다. 또한 버킷의 루트에 직접 파일을 업로드해볼 수도 있습니다. 이 작업 또한 오류로 이어집니다.

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. 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 only to this bucket and its access points. 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 within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit



#### You don't have permission to view the Block public access (bucket settings) configuration

You need `s3:GetAccountPublicAccessBlock` to view the Block public access (bucket settings) configuration. [Learn more about Identity and access management in Amazon S3](#)

▶ API response

72. Amazon S3 콘솔에서 mediacouser 계정을 로그아웃합니다. 하지만 다른 브라우저 탭에서는 voclabs... 사용자로 로그인되어 있어야 합니다.

훌륭합니다! Amazon S3 버킷을 생성하고 다른 사용자와 안전하게 파일을 공유하도록 구성되어 있음을 확인했습니다.

## 과제 4: Amazon S3 공유 버킷에 대한 이벤트 알림 구성

### 과제 개요

이번 과제에서는 버킷의 콘텐츠가 변경될 때마다 이벤트 알림을 생성하여 Amazon SNS 주제에 게시하도록 Amazon S3 공유 버킷을 구성합니다. 그러면 주제가 구독한 사용자에게 이메일로 알림 메시지를 보냅니다. 구체적으로는 다음 단계를 수행합니다.

- `s3NotificationTopic` SNS 주제를 생성합니다.
- 주제에 게시하기 위한 권한을 Amazon S3에 부여합니다.
- `cafeuser`로 주제를 구독합니다.
- S3 버킷에 대한 이벤트 알림 구성을 추가합니다.

## 과제 4.1: s3NotificationTopic 생성 및 구성

73. 표준 **voclabs...** 실습 사용자로 로그인되어 있는 AWS 관리 콘솔 창으로 돌아옵니다.
74. **Services > Application Integration > Simple Notification Service** 를 선택합니다.
75. 필요하다면 왼쪽의 메뉴 아이콘()을 클릭하여 탐색 창을 엽니다.
76. 탐색 창에서 **Topics(주제)**를 선택합니다.
77. **Create topic(주제 생성)**을 클릭합니다.
78. **Standard(표준)**를 선택합니다.
79. **Name** 상자에 `s3NotificationTopic` 을 입력합니다.
80. **Create topic** 을 클릭합니다. s3NotificationTopic 주제가 정상적으로 생성되었다는 메시지가 표시됩니다.
81. 주제 **ARN** 필드의 값을 복사하여 텍스트 편집기에 붙여 넣고 기록해 둡니다. 다음 단계에서 주제의 액세스 정책을 생성할 때와 활동의 후반부에 이 정보가 필요합니다.

`arn:aws:sns:us-west-2:525639593057:s3NotificationTopic`

82. 주제의 액세스 정책을 구성합니다. **s3NotificationTopic** 창에서 **Edit** 을 클릭합니다.
83. **Access policy – optional(액세스 정책 – 선택 사항)** 섹션을 확장합니다.
84. **JSON 편집기**의 내용을 다음 정책으로 바꿉니다.

```
{
  "Version": "2008-10-17",
  "Id": "S3PublishPolicy",
  "Statement": [
    {
      "Sid": "AllowPublishFromS3",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "<ARN of s3NotificationTopic>",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:*:*:<cafe-xxxnnn>"
        }
      }
    }
  ]
}
```

```
]
}
```

JSON 객체에서 **<ARN of s3NotificationTopic>**을 앞서 기록해 둔 주제 ARN의 값으로, **<cafe-xxxxnnn>**을 고유한 S3 버킷 이름으로 대체합니다. 이때 값을 둘러싼 꺾쇠괄호(<>)를 제거해야 합니다.

#### ▼ 액세스 정책 - 선택 사항 정보

이 정책은 주제에 액세스할 수 있는 사용자를 정의합니다. 기본적으로 주제 소유자만 주제에 게시 또는 구독할 수 있습니다.

##### JSON 편집기

```
6      "Sid": "AllowPublishFromS3",
7      "Effect": "Allow",
8      "Principal": {
9        "Service": "s3.amazonaws.com"
10     },
11     "Action": "SNS:Publish",
12     "Resource": "<ARN of s3NotificationTopic>",
13     "Condition": {
14       "ArnLike": {
15         "aws:SourceArn": "arn:aws:s3:*:*:cafe-henry"
16       }
17     }
18   }
19 ]
20 }
```

85. 잠시 시간을 내어 이 정책의 의도를 파악합니다. 정책은 *s3NotificationTopic*에 메시지를 게시할 수 있는 권한을 *cafe* S3 공유 버킷에 부여합니다.

86. **Save changes(변경 사항 저장)**를 클릭합니다.

87. 마지막으로 S3 공유 버킷으로부터 이벤트 알림을 받을 *cafeuser* 사용자(Frank)로 주제를 구독합니다. **s3NotificationTopic** 창에서 **Subscriptions(구독)** 탭을 선택합니다.

88. **Create subscription(구독 생성)**을 클릭합니다.

89. **topic ARN(주제 ARN)** 상자를 클릭하여 옵션으로 표시되는 **s3NotificationTopic**을 선택합니다.

90. **Protocol** 메뉴에서 **Email**을 선택합니다.

91. **Endpoint** 상자에서 액세스 가능한 이메일 주소를 입력합니다.

## 구독 생성

## 세부 정보

주제 ARN

arn:aws:sns:us-west-2:525639593057:s3NotificationTopic

프로토콜


구독할 엔드포인트 유형

이메일

엔드포인트

Amazon SNS의 알림을 수신할 수 있는 이메일 주소입니다.

javaexpert@nate.com


 구독을 생성한 후에는 확인해야 합니다. [정보](#)

**참고:** 이번 활동에서는 여러분이 Frank 라고 가정하고 S3 이벤트 알림을 받습니다.

92. **Create subscription** 을 클릭합니다. 구독이 정상적으로 생성되었다는 메시지가 표시됩니다.

93. 입력한 이메일 주소의 받은 편지함을 확인합니다. 제목이 *AWS Notification - Subscription Confirmation* 인 이메일 메시지가 도착했을 것입니다.

☆ AWS Notification - Subscription Confirmation

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

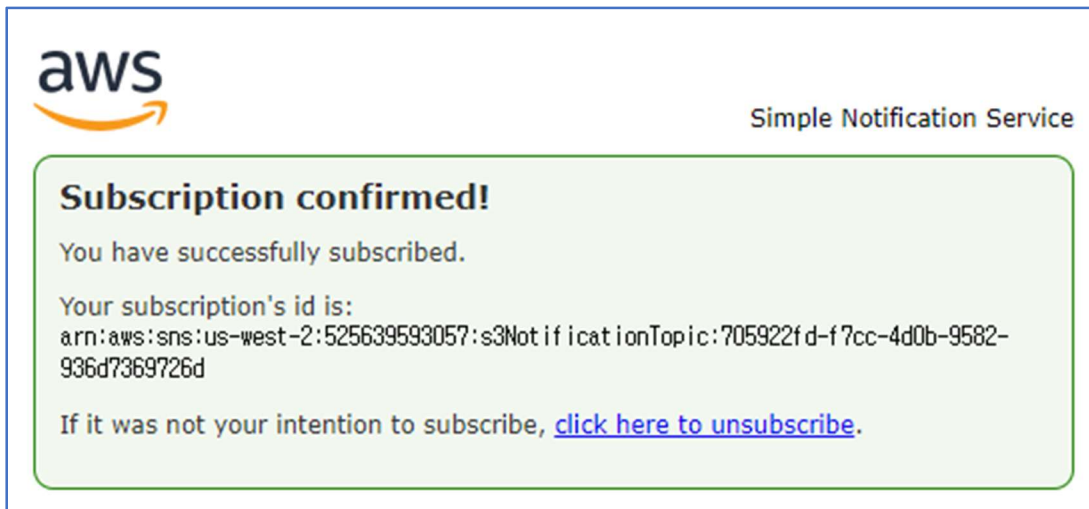
You have chosen to subscribe to the topic:

**arn:aws:sns:us-west-2:525639593057:s3NotificationTopic**

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 confirmation requests please send an email to [sns-opt-out](#)

94. 이메일 메시지를 열고 **Confirm subscription** 을 클릭합니다. 새 브라우저 탭이 열리고 *Subscription confirmed!* 라는 메시지가 포함된 페이지가 표시됩니다.



## 과제 4.2: S3 버킷에 대한 이벤트 알림 구성 추가

이번 과제에서는 Amazon S3 가 게시할 이벤트와 Amazon S3 가 이벤트 알림을 보낼 주제 대상을 지정하는 이벤트 알림 구성 파일을 생성합니다. 그런 다음 *s3api* CLI 를 사용하여 이 구성 파일을 Amazon S3 공유 버킷과 연결합니다.

95. **CLI Host** 인스턴스의 SSH 창에 다음을 입력하여 이름이 **s3EventNotification.json** 인 새 파일을 편집합니다.

```
vi s3EventNotification.json
```

96. 편집기에 `i` 를 입력하여 **삽입** 모드로 변경합니다.
97. 다음 JSON 구성을 사용자 지정한 후 복사하여 편집기 창에 붙여넣습니다.

```
{
  "TopicConfigurations": [
    {
      "TopicArn": "<ARN of s3NotificationTopic>",
      "Events": ["s3:ObjectCreated:*","s3:ObjectRemoved:*"],
      "Filter": {
        "Key": {
          "FilterRules": [
            {
              "Name": "prefix",
              "Value": "images/"
            }
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
}
]
}

```

JSON 객체에서 **<ARN of s3NotificationTopic>**을 앞서 기록한 주제 ARN의 값으로 대체합니다. 그러면 `arn:aws:sns:::s3NotificationTopic`과 같은 형식이 됩니다. 이때 값을 둘러싼 꺾쇠괄호(< >)를 제거해야 합니다.

```

{
  "TopicConfigurations": [
    {
      "TopicArn": "arn:aws:sns:us-west-2:525639593057:s3NotificationTopic",
      "Events": ["s3:ObjectCreated:*", "s3:ObjectRemoved:*"],
      "Filter": {
        "Key": {
          "FilterRules": [
            {
              "Name": "prefix",
              "Value": "images/"
            }
          ]
        }
      }
    }
  ]
}

```

98. 잠시 시간을 내어 이 구성의 의도를 파악합니다. 구성은 접두부(prefix)가 `images/`인 S3 리소스 내 객체에 `ObjectCreated` 또는 `ObjectRemoved` 이벤트가 실행될 때마다 `s3NotificationTopic`에 이벤트 알림을 게시할 것을 Amazon S3에 요청합니다.
99. ESC 키를 눌러 **삽입** 모드를 종료합니다.
100. `:.wq`를 입력하여 파일을 저장하고 텍스트 편집기를 종료합니다.
101. 이벤트 구성 파일을 S3 공유 버킷과 연결합니다. **CLI Host** 인스턴스의 SSH 창에 다음을 입력합니다.

```
aws s3api put-bucket-notification-configuration --bucket <cafe-xxxnnn> --notification-configuration file:///s3EventNotification.json
```

명령에서 **<cafe-xxxnnn>**을 고유한 S3 버킷 이름으로 대체합니다.



102. 잠시 기다린 다음 주제 구독에 사용한 이메일 주소의 받은 편지함을 확인합니다.  
제목이 *Amazon S3 Notification* 인 이메일 메시지가 있을 것입니다.
103. 이메일 메시지를 열어 알림 메시지를 확인합니다. 메시지 내용은 다음과 비슷합니다.

```
{"Service":"Amazon S3","Event":"s3:TestEvent","Time":"2019-04-26T06:04:27.405Z","Bucket":"<cafe-xxxxnnn>","RequestId":"7A87C25E0323B2F4","HostId":"fB3Z...SD////PWubF3E7RYtVupg="}
```

‘Event’ 키의 값이 ‘s3:TestEvent’라는 것에 주목합니다. 이 알림은 여러분이 설정한 이벤트 알림 구성의 테스트로 Amazon S3 가 전송한 것입니다.

## 과제 5: Amazon S3 공유 버킷 이벤트 알림 테스트

이번 과제에서는 *mediacouser*가 버킷에서 실행할 것으로 예상되는 사용 사례를 수행하여 S3 공유 버킷 이벤트 알림 구성을 테스트합니다. 여기에는 버킷에서 객체를 추가 및 삭제하는 작업이 포함되며 이에 따라 Frank에게 이메일 알림이 전송됩니다. 또한 무단 작업을 테스트하여 거부되는지 확인합니다. AWS *s3api* CLI를 사용하여 S3 공유 버킷에서 이러한 작업을 실행합니다.

팁: [s3api 용 AWS CLI 설명서](#)를 사용하여 이 과제에서 사용해야 할 AWS s3api CLI 명령 구문을 정확히 파악합니다.

104. *mediacouser* 보안 인증 정보를 사용하도록 CLI Host의 AWS CLI 클라이언트 소프트웨어를 구성합니다. **CLI Host** 인스턴스의 SSH 창에 다음을 입력합니다.

```
aws configure
```

105. 해당 메시지가 나타나면 다음 정보를 입력합니다.
- **AWS Access Key ID:** *mediacouser*의 액세스 키 ID 값을 복사하여 붙여 넣습니다. 이 정보는 과제 3에서 다운로드한 *accessKeys.csv* 파일에서 찾을 수 있습니다.
  - **AWS Secret Access Key:** 과제 3에서 다운로드한 같은 파일에서 *mediacouser*의 비밀 액세스 키 값을 복사하여 붙여 넣습니다.
  - **Default region name:** 메시지에서 ENTER를 클릭하여 활동 초반부에서 설정한 리전을 그대로 사용합니다.

- **Default output format:** json

106. CLI Host 의 **new-images** 폴더에서 **Caramel-Delight.jpg** 이미지 파일을 업로드하여 추가 사용 사례를 테스트합니다. SSH 창에 다음을 입력합니다.

```
aws s3api put-object --bucket <cafe-xxxxnn> --key images/Caramel-Delight.jpg --body  
~/new-images/Caramel-Delight.jpg
```

명령에서 *<cafe-xxxxnn>*을 고유한 S3 버킷 이름으로 대체해야 합니다. 명령 실행이 완료되면 업로드된 객체의 *ETag*(엔터티 태그)가 반환됩니다.

```
{  
  "ETag": "\"31ac30da619244b0ce786f106e4f3df7\"",  
  "ServerSideEncryption": "AES256"  
}
```

107. s3NotificationTopic 주제를 구독하는 데 사용한 이메일 주소의 받은 편지함을 확인합니다. 제목이 *Amazon S3 Notification* 인 새 이메일 메시지가 있을 것입니다.

108. 이메일 메시지를 열어 알림 메시지를 확인합니다. 다음 사항에 유의합니다.

- 'eventName' 키의 값은 'ObjectCreated:Put'입니다.
- 'key' 객체의 값은 명령에서 지정한 이미지 파일 키인 'images/Caramel-Delight.jpg'입니다.

이 알림은 키가 **images/Caramel-Delight.jpg** 인 새 객체가 S3 공유 버킷에 추가되었음을 나타냅니다.

109. *가져오기* 사용 사례를 테스트합니다. 버킷에서 키가 **images/Donuts.jpg** 인 객체를 가져옵니다. SSH 창에 다음을 입력합니다.

```
aws s3api get-object --bucket <cafe-xxxxnn> --key images/Donuts.jpg Donuts.jpg
```

명령에서 *<cafe-xxxxnn>*을 고유한 S3 버킷 이름으로 대체합니다. 명령 실행이 완료되면 가져온 객체(*ContentLength* 포함)에 대한 일부 메타데이터가 반환됩니다.

```
{  
  "AcceptRanges": "bytes",  
  "ContentType": "image/jpeg",  
  "LastModified": "Sun, 06 Aug 2023 02:14:28 GMT",  
  "ContentLength": 380753,  
  "ETag": "\"405b0bcc53cb5ab713c967dc1422b4f4\"",  
  "ServerSideEncryption": "AES256",  
  "Metadata": {}  
}
```

이 옵션에서는 이메일 알림이 생성되지 않은 것에 주목합니다. 공유 버킷이 객체 생성과 삭제 작업에 대해서만 알림을 전송하도록 구성되었기 때문입니다.

110. 삭제 사용 사례를 테스트합니다. 키가 **images/Strawberry-Tarts.jpg** 인 객체를 버킷에서 삭제합니다. SSH 창에 다음을 입력합니다.

```
aws s3api delete-object --bucket <cafe-xxxxnn> --key images/Strawberry-Tarts.jpg
```

명령에서 **<cafe-xxxxnn>**을 고유한 S3 버킷 이름으로 대체합니다.

111. s3NotificationTopic 주제를 구독하는 데 사용한 이메일 주소의 받은 편지함을 확인합니다. 제목이 *Amazon S3 Notification* 인 새 이메일 메시지가 있을 것입니다.

112. 이메일 메시지를 열어 알림 메시지를 확인합니다. 다음 사항에 유의합니다.

- 'eventName' 키의 값은 'ObjectRemoved:Delete'입니다.
- 'key' 객체의 값은 명령에서 지정한 이미지 파일 키인 'images/Strawberry-Tarts.jpg'입니다.

이 알림은 키가 **images/Strawberry-Tarts.jpg** 인 객체가 S3 공유 버킷에서 삭제되었음을 나타냅니다.

113. 마지막으로 무단 사용 사례를 테스트합니다. **Donuts.jpg** 객체를 누구나 읽을 수 있도록 권한을 변경해봅니다. SSH 창에 다음을 입력합니다.

```
aws s3api put-object-acl --bucket <cafe-xxxxnn> --key images/Donuts.jpg --acl public-read
```

명령에서 **<cafe-xxxxnn>**을 고유한 S3 버킷 이름으로 대체합니다.

명령 실행에 실패하고 다음 오류 메시지가 표시됩니다.

```
An error occurred (AccessDenied) when calling the PutObjectAcl operation: Access Denied
```

S3 공유 버킷의 권한 및 이벤트 알림 구성이 의도한 대로 작동합니다. 수고하셨습니다.



Amazon S3 파일 공유 솔루션으로 카페와 외부 미디어 회사가 이미지를 교환하는 방식이 간소화되었습니다. Frank는 솔루션이 안전하고, 새로운 사진이 업로드되었을 때 자동으로 알림을 받을 수 있어 만족합니다. 또한 같은 접근방식을 사용하여 공급업체와 전자 문서를 주고 받아야겠다고 생각하고 있습니다.

## 활동 완료

---

축하합니다! 실습을 마치셨습니다.

114. 이 페이지의 상단에서 **End Lab**을 클릭하고 **Yes**를 클릭하여 실습 종료를 확인합니다.

'DELETE has been initiated... You may close this message box now'라는 내용의 패널이 표시됩니다.

115. 오른쪽 상단 모서리에 있는 **X**를 클릭하여 패널을 닫습니다.

## 추가 리소스

---

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

여러분의 피드백을 환영합니다. 제안이나 수정 사항을 공유하려면 [AWS Training and Certification Contact Form](#)에서 세부 정보를 제공해 주십시오.

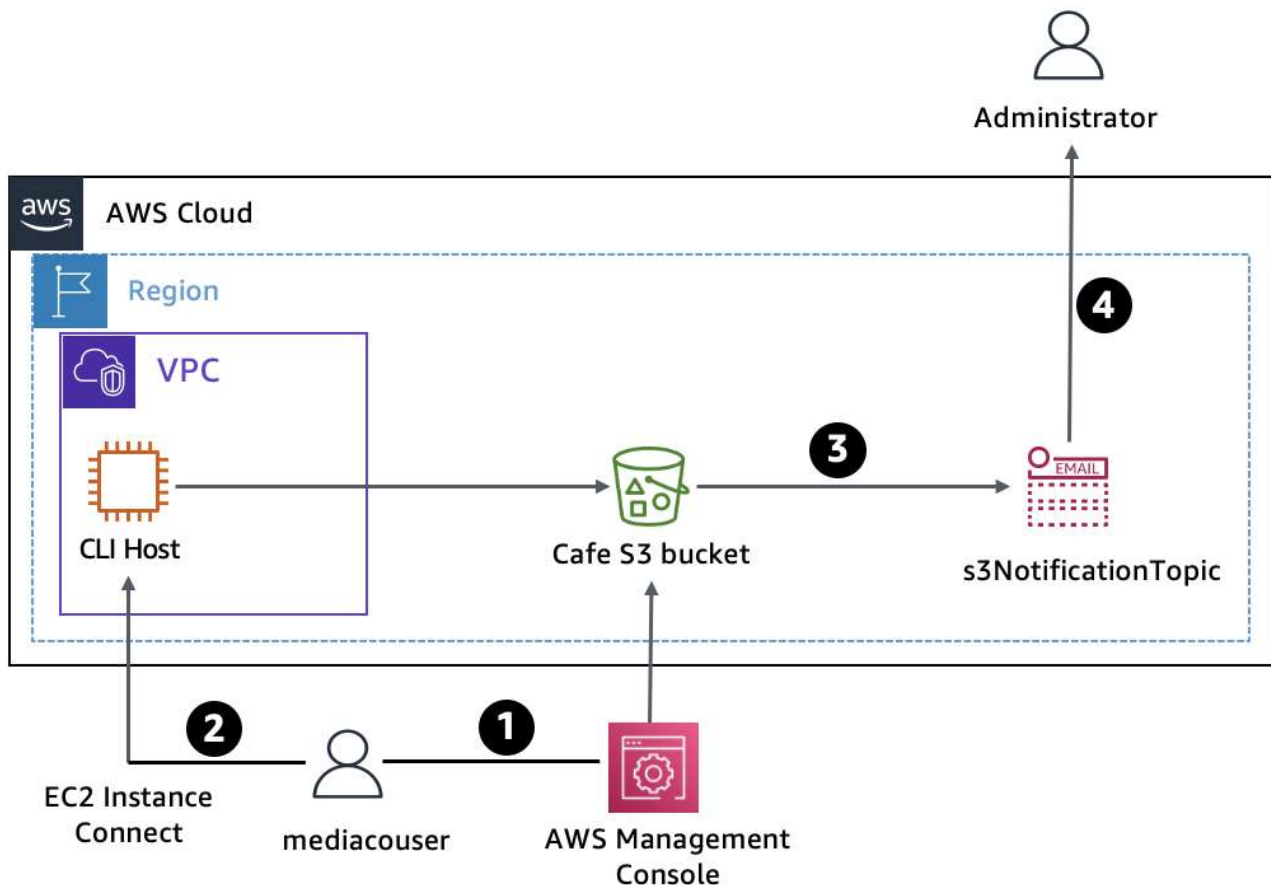
© 2022 Amazon Web Services, Inc. 및 계열사. All rights reserved. 본 내용은 Amazon Web Services, Inc.의 사전 서면 허가 없이 전체 또는 일부를 복제하거나 재배포할 수 없습니다. 상업적인 복제, 대여 또는 판매는 금지됩니다.

# Working with Amazon S3

## Lab overview

In this lab, you create and configure an Amazon Simple Storage Service (Amazon S3) bucket to share images with an external user at a media company (mediacouser) who has been hired to provide pictures of the products that the café sells. You also configure the S3 bucket to automatically send an email notification to the administrator when the bucket contents are modified.

The following diagram shows the component architecture of the Amazon S3 file-sharing solution and illustrates its usage flow.



An AWS Identity and Access Management (IAM) user named **mediacouser**, which represents an external user at a media company, has been pre-created with the appropriate Amazon S3 permissions to allow the user to add, change, or delete images from the bucket. The necessary Amazon S3 permissions are reviewed for each user to make sure that access to the bucket is secure and appropriate for each role.

The following steps describe the usage flow in the diagram:

1. When new product pictures are available or when existing pictures must be updated, a representative from the media company signs in to the AWS Management Console as **mediacouser** to upload, change, or delete the bucket contents.
2. As an alternative, **mediacouser** can use the AWS Command Line Interface (AWS CLI) to change the contents of the S3 bucket.
3. When Amazon S3 detects a change in the contents of the bucket, it publishes an email notification to the **s3NotificationTopic** Amazon Simple Notification Service (Amazon SNS) topic.
4. The administrator who is subscribed to the **s3NotificationTopic** SNS topic receives an email message that contains the details of the changes to the contents of the bucket.

**Note:** In real-world implementations, external users might not receive direct access to CLI Host as depicted in the diagram.

## Objectives

---

By the end of this lab, you will be able to do the following:

- Use the `s3api` and `s3` AWS CLI commands to create and configure an S3 bucket.
- Verify write permissions to a user on an S3 bucket.
- Configure event notification on an S3 bucket.

## Duration

---

This lab requires approximately **90 minutes** to complete.

## Accessing the AWS Management Console

---

1. At the top of these instructions, choose **Start Lab** to launch your lab.

A **Start Lab** panel opens displaying the lab status.

2. Wait until the message "Lab status: ready" appears, and then choose **X** to close the **Start Lab** panel.
3. At the top of these instructions, choose **AWS** to open the AWS Management Console on a new browser tab. The system automatically signs you in.

**Tip** If a new browser tab does not open, a banner or icon at the top of your browser will indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

4. Arrange the AWS Management Console so that it appears alongside these instructions. Ideally, you should be able to see both browser tabs at the same time to follow the lab steps.
5. At the top of these instructions, choose **Details**, and then choose **Show**.
6. From the **Credentials** panel, copy the values for the **AccessKey** and **SecretKey**, and paste them into a text editor. You use these values throughout the lab. After you have copied and pasted the values, choose **X** to close the **Credentials** panel.

## Task 1: Connecting to the CLI Host EC2 instance and configuring the AWS CLI

In this task, you connect to the CLI Host EC2 instance by using EC2 Instance Connect and configure the AWS CLI so that you can run commands.

### Task 1.1: Connecting to the CLI Host EC2 instance

In this task, you use EC2 Instance Connect to connect to the CLI Host EC2 instance.

7. On the **AWS Management Console**, in the **Search** bar, enter and choose **EC2** to open the **EC2 Management Console**.
8. In the navigation pane, choose **Instances**.
9. From the list of instances, select the **CLI Host** instance.
10. Choose **Connect**.
11. On the **EC2 Instance Connect** tab, choose **Connect**.

This option opens a new browser tab with the **EC2 Instance Connect** terminal window.

You use this terminal window to complete the tasks throughout the lab. If the terminal becomes unresponsive, refresh the browser or use the steps in this task to connect again.

### Task 1.2: Configuring the AWS CLI on the CLI Host instance

12. To set up the AWS CLI profile with credentials, run the following command in the EC2 Instance Connect terminal:

```
aws configure
```

13. At the prompts, copy the following values that you pasted into your text editor, and paste them into the terminal window as directed.
  - **AWS Access Key ID:** Enter the value for **AccessKey**.
  - **AWS Secret Access Key:** Enter the value for **SecretKey**.
  - **Default region name:** Enter **us-west-2**.
  - **Default output format:** Enter **json**.

You are ready to run AWS CLI commands to interact with AWS services.

## Task 2: Creating and initializing the S3 share bucket

---

In this task, you use the AWS CLI to create the S3 share bucket and upload a few images.

To do so, you run the following commands in the EC2 Instance Connect terminal window.

14. To create an S3 bucket, run the following command. In the command, replace *<cafe-xxxxnnn>* with your bucket name. Your bucket name must begin with **cafe-** and should include a combination of letters and numbers to make your bucket name unique:

```
aws s3 mb s3://<cafe-xxxxnnn> --region 'us-west-2'
```

You should receive a message similar to the following: `make_bucket: cafe-xxxx99999999`

**Note:** Bucket names cannot contain uppercase letters. If you receive an error when you try to create your S3 bucket, make sure your bucket name doesn't include uppercase letters.

Next, you load some images into the S3 bucket under the `/images` prefix. Sample image files are provided in the `initial-images` folder on the CLI Host.

15. To load images into the bucket, run the following command. In the command, replace *<cafe-xxxxnnn>* with your bucket name:

```
aws s3 sync ~/initial-images/ s3://<cafe-xxxxnnn>/images
```

The command output lists the image files that are being uploaded.

16. To verify that the files were synced to the S3 bucket, run the following command. In the command, replace *<cafe-xxxxnnn>* with your bucket name:

```
aws s3 ls s3://<cafe-xxxxnnn>/images/ --human-readable --summarize
```

You see the details of the image files that were uploaded, including the number of files uploaded and the total size of the files.

## Task 3: Reviewing the IAM group and user permissions

---

Next, you review the permissions assigned to the `mediaco` IAM user group. This group was created to provide a way for the users of the media company to use the AWS Management Console or the AWS CLI to upload and modify images in the S3 share bucket. Creating the group makes it



convenient to manage individual user permissions. You also review the permissions inherited by the `mediacouser` user that is part of the group.

## Task 3.1: Reviewing the `mediaco` IAM group

In this section, you review the permissions assigned to the `mediaco` group.

17. On the **AWS Management Console**, in the **Search** bar, enter and choose `IAM` to open the **IAM Management Console**.
18. In the navigation pane on the left, choose **User groups**.
19. From the **User groups** list, select **mediaco**.

The **Summary** page for the **mediaco** group is displayed.

20. Choose the **Permissions** tab.
21. Next to **IAMUserChangePassword**, choose **+** to expand the policy.

If needed, review the AWS managed policy that permits users to change their own password.

22. To collapse the policy, choose **-**.
23. Next to **mediaCoPolicy**, choose **+** to expand the policy.

**Note:** You might have to scroll down to see the policy.

Notice the following statements in this policy:

- The first statement, identified by the **Sid** key name **AllowGroupToSeeBucketListInTheConsole**, defines permissions that allow the user to use the Amazon S3 console to view the list of S3 buckets in the account.
  - The second statement, identified by the **Sid** key name **AllowRootLevelListingOfTheBucket**, defines permissions that allow the user to use the Amazon S3 console to view the list of first-level objects in the **cafe** bucket and other objects in the bucket.
  - The third statement, identified by the **Sid** key name **AllowUserSpecificActionsOnlyInTheSpecificPrefix**, defines permissions that specify the actions that the user can perform on the objects in the **cafe-\*/images/\*** folder. The main operations are **GetObject**, **PutObject**, and **DeleteObject**, which correspond to the read, write, and delete permissions that you want to grant to the `mediacouser` user. Two additional operations are included for eventual version-related actions.
24. To collapse the policy, choose **-**.

## Task 3.2: Reviewing the `mediacouser` IAM user

In this section, you review the properties of the `mediacouser` user.

25. In the IAM console navigation pane, choose **Users**.
26. From the **Users** list, select **mediacouser**.

On the **Permissions** tab, you should see two policies: **IAMUserChangePassword** and **mediaCoPolicy**. These policies are assigned to the mediaco IAM group that you reviewed in the previous task.

27. To verify that you see the mediaco IAM group, choose the **Groups** tab.

The mediacouser user is a member of this group and therefore inherits the permissions assigned to the mediaco group.

28. Choose the **Security credentials** tab.

29. In the **Access keys** section, choose **Create access key**, and choose the following options:

- Choose **Command Line Interface (CLI)**.
- Select the check box for **I understand the above recommendation and want to proceed to create an access key**.

30. Choose **Next**.

31. Choose **Create access key**.

The following message displays: *Access key created*

32. Choose **Download .csv file**.

33. Choose **Done**.

34. On the **mediacouser** page, from the **Security credentials** tab, copy the **Console sign-in link**.

You use this link in the next task.

## Task 3.3: Testing the mediacouser permissions

In this task, you test the permissions that you have reviewed by signing in to AWS Management Console as mediacouser and performing the view, upload, and delete operations on the contents of the images folder in the S3 share bucket. These actions are the use cases that the external media company user is expected to perform on the bucket. In addition, you test the unauthorized use case, where the external user attempts to change the bucket permissions.

35. To sign in to the AWS Management Console as the mediacouser user, use one of the following options:

**Important:** Do not sign out of the session where you are signed in as the **voclabs/user**. Instead, choose one of two options:

- Option 1: Use a different browser.
- Option 2: Use the same browser type, but open a new incognito or private browser session.

For either option that you choose, enter the **Console sign-in link** that you copied from the previous step into your new browser tab. The AWS Management Console sign-in page opens and already has the **Account ID** populated.

36. On the sign-in page, enter the following credentials:

- Enter the following credentials:
  - **IAM user name:** `mediacouser`.

- **Password:** Training1!.

37. Choose **Sign in**.

38. On the new **AWS Management Console** page, in the **Search** bar, enter and choose **S3** to open the **S3 Management Console**.

39. From the list of buckets, select the bucket that you created earlier.

40. To display the list of images that were uploaded earlier, select **images/**.

41. To test the **view** use case, select **Donuts.jpg**, and choose **Open**.

A new browser tab should open that shows a picture of various donuts.

**Tip:** If a new browser tab does not open, a banner or icon at the top of your browser will indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

42. Close the browser tab that shows the Donuts.jpg image.

43. In the **Console** tab, in the breadcrumb trail at the top, choose **images/** to see the contents of the images folder again.

44. To test the **upload** use case, choose **Upload**.

45. On the **Upload** page, choose **Add files**, and choose any image or picture from your local computer.

46. Choose **Upload**.

47. To close the **Upload: status** page, choose **Close**.

48. Select the file that you uploaded, and choose **Open**.

A new browser tab should open that shows the file that you uploaded.

49. Close the browser tab that shows the file that you uploaded.

50. To test the **delete** use case, in the **Console** tab, in the image list, select the check box for **Cup-of-Hot-Chocolate.jpg**.

51. Choose **Delete**.

52. On the **Delete objects** page, in the **Delete objects?** box, enter **delete**.

53. Choose **Delete objects**.

The object is deleted and no longer appears in the image list.

54. To close the **Delete objects: status** page, choose **Close**.

Next, you test the **unauthorized** use case where mediacouser attempts to change the bucket's permissions.

55. In the breadcrumb trail at the top, choose your bucket to return to the bucket content list.

56. Choose the **Permissions** tab.

This is where you can change a bucket's permissions.

Notice that for **Permissions overview**, the following error message is displayed: "Insufficient permissions." mediacouser is prevented from changing the bucket permissions. You could also try to upload a file directly to the root of the bucket. This action should also fail.

57. Sign out of the Amazon S3 console as **mediacouser**.

You have successfully created an Amazon S3 bucket, and you have confirmed that it is securely configured for file sharing with another user.

## Task 4: Configuring event notifications on the S3 share bucket

In this task, you configure the S3 share bucket to generate an event notification to an SNS topic whenever the contents of the bucket change. The SNS topic then sends an email message to its subscribed users with the notification message. Specifically, you perform the following steps:

- Create the `s3NotificationTopic` SNS topic.
- Grant Amazon S3 permission to publish to the topic.
- Subscribe to the topic.
- Add an event notification configuration to the S3 bucket.

### Task 4.1: Creating and configuring the `s3NotificationTopic` SNS topic

58. Return to the AWS Management Console window where you are signed in as **voclabs/user**.

59. On the **AWS Management Console**, in the **Search** bar, enter `SNS` and choose **Simple Notification Service** to open the **Simple Notification Service** console.

60. If necessary, to open the navigation pane, choose the menu icon () on the left.

61. In the navigation pane, choose **Topics**.

62. Choose **Create topic**.

63. Choose **Standard**.

64. For **Name**, enter `s3NotificationTopic`.

65. Choose **Create topic**.

A message is displayed indicating that the `s3NotificationTopic` SNS topic has been successfully created.

66. From the **s3NotificationTopic** page in the **Details** section, copy and paste the **ARN** value to a text editor. You need this value later in this lab.

67. To configure the topic's access policy, choose **Edit**.

68. Expand the **Access policy - optional** section.

69. Replace the contents of the JSON editor with the following policy. In the JSON object, replace `<ARN of s3NotificationTopic>` with the ARN value that you copied earlier, and replace `<cafe-xxxxnnn>` with your S3 bucket name. Remember to remove the enclosing angle brackets (`<` `>`).

```
{
  "Version": "2008-10-17",
  "Id": "S3PublishPolicy",
  "Statement": [
```

```

{
  "Sid": "AllowPublishFromS3",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "<ARN of s3NotificationTopic>",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:s3:*:*:<cafe-xxxnnn>"
    }
  }
}
]
}

```

Take a moment to review the intent of this policy. It grants the cafe S3 share bucket permission to publish messages to the s3NotificationTopic SNS topic.

70. Choose **Save changes**.

Next, you subscribe to the topic to receive the event notifications from the S3 share bucket.

71. In the **s3NotificationTopic** pane, choose the **Subscriptions** tab.

72. Choose **Create subscription**.

73. Choose the **Topic ARN** box, and choose the **s3NotificationTopic** SNS topic that appears as an option.

74. From the **Protocol** dropdown list, choose **Email**.

75. In the **Endpoint** box, enter an email address that you can access.

76. Choose **Create subscription**.

A message displays that confirms that the subscription was created successfully.

77. Check the inbox for the email address that you provided. You should see an email message with the subject *AWS Notification - Subscription Confirmation*.

78. Open the email message, and choose **Confirm subscription**. A new browser tab opens and displays a page with the message *Subscription confirmed!*

## Task 4.2: Adding an event notification configuration to the S3 bucket

In this task, you create an event notification configuration file that identifies the events that Amazon S3 will publish and the topic destination where Amazon S3 will send the event notifications. You then use the s3api CLI commands to associate this configuration file with the S3 share bucket.

79. In the terminal window for the CLI Host instance, enter the following command to edit a new file named `s3EventNotification.json`:

```
vi s3EventNotification.json
```

80. In the editor, to change to insert mode, press `i`.

81. In the following JSON object, replace `<ARN of s3NotificationTopic>` with the ARN value that you recorded earlier. Remember to remove the enclosing angle brackets (`< >`). Copy and paste your customized JSON configuration into the editor window.

```
{
  "TopicConfigurations": [
    {
      "TopicArn": "<ARN of s3NotificationTopic>",
      "Events": ["s3:ObjectCreated:*","s3:ObjectRemoved:*"],
      "Filter": {
        "Key": {
          "FilterRules": [
            {
              "Name": "prefix",
              "Value": "images/"
            }
          ]
        }
      }
    }
  ]
}
```

Take a moment to review the intent of this configuration. It requests that Amazon S3 publish an event notification to the `s3NotificationTopic` SNS topic whenever an `ObjectCreated` or `ObjectRemoved` event is performed on objects inside an Amazon S3 resource with a prefix of **images/**.

82. Press `ESC` to exit insert mode.

83. To save the file and exit the editor, enter `:wq` and press `Enter`.

84. To associate the event configuration file with the S3 share bucket, run the following command. In the command, replace `<cafe-xxxnnn>` with your S3 bucket name:

```
aws s3api put-bucket-notification-configuration --bucket <cafe-xxxnnn> --notification-configuration file://s3EventNotification.json
```

85. Wait a few moments, and then check the inbox for the email address that you used to subscribe to the topic. You should see an email message with the subject *Amazon S3 Notification*.

86. Open the email message, and examine the notification message. It should be similar to the following:

```
{"Service":"Amazon S3","Event":"s3:TestEvent","Time":"2019-04-26T06:04:27.405Z","Bucket":"","RequestId":"7A87C25E0323B2F4","HostId":"fB3Z...SD////PWubF3E7RYtVupg="}
```

Notice that the value of the **"Event"** key is **"s3:TestEvent"**. Amazon S3 sent this notification as a test of the event notifications configuration that you set up.

## Task 5: Testing the S3 share bucket event notifications

In this task, you test the configuration of the S3 share bucket event notification by performing the use cases that mediacouser expects to perform on the bucket. These actions include putting objects into and deleting objects from the bucket, which send email notifications. You also test an unauthorized operation to verify that it is rejected. You use the AWS s3api CLI command to perform these operations on the S3 share bucket.

87. To configure the CLI Host's AWS CLI client software to use the mediacouser credentials, in the SSH window for the CLI Host instance, enter the following command:

```
aws configure
```

88. At the prompts, enter the following:

- **AWS Access Key ID:** Copy and paste the value of the **Access key ID** of mediacouser, which is in the mediacouser\_accessKeys.csv file that you downloaded in Task 3.
- **AWS Secret Access Key:** Copy and paste the value of the **Secret Access Key** of mediacouser from the same file that you downloaded in Task 3.
- **Default region name:** Press Enter at the prompt to keep the same Region that you selected earlier in this lab.
- **Default output format:** Enter `json`.

Next, you test the **put** use case by uploading the Caramel-Delight.jpg image file from the new-images folder on the CLI Host.

89. To upload this file, run the following command. In the command, replace `<cafe-xxxxnnn>` with your S3 bucket name:

```
aws s3api put-object --bucket <cafe-xxxxnnn> --key images/Caramel-Delight.jpg --body ~/new-images/Caramel-Delight.jpg
```

After the command completes, it returns the **ETag** (Entity tag) of the uploaded object.

90. Check the inbox for the email address that you used to subscribe to the s3NotificationTopic SNS topic. You should see a new email message with the subject *Amazon S3 Notification*.
91. Open the email message, and examine the notification message. Notice the following information:
- The value of the **eventName** key is **ObjectCreated:Put**.
  - The value of the **key** object is **images/Caramel-Delight.jpg**, which is the image file key that you specified in the command.

This notification indicates that a new object with a key of **images/Caramel-Delight.jpg** was added (put) into the S3 share bucket.

Next, you test the **get** use case by getting the object with a key of **images/Donuts.jpg** from the bucket.

92. To get this object, run the following command. In the command, replace *<cafe-xxxxnnn>* with your S3 bucket name:

```
aws s3api get-object --bucket <cafe-xxxxnnn> --key images/Donuts.jpg Donuts.jpg
```

Notice that an email notification was not generated for this operation. This operation does not generate an email notification because the share bucket is configured to send notifications only when objects are created or deleted.

Next, you test the **delete** use case by deleting the object with a key of **images/Strawberry-Tarts.jpg** from the bucket.

93. To delete this object, run the following command. In the command, replace *<cafe-xxxxnnn>* with your S3 bucket name:

```
aws s3api delete-object --bucket <cafe-xxxxnnn> --key images/Strawberry-Tarts.jpg
```

94. Check the inbox for the email address that you used to subscribe to the s3NotificationTopic SNS topic. You should see a new email message with the subject *Amazon S3 Notification*.
95. Open the email message, and examine the notification message. Notice the following information:
- The value of the **eventName** key is **ObjectRemoved:Delete**.
  - The value of the object **key** is **images/Strawberry-Tarts.jpg**, which is the image file key that you specified in the command.

This notification indicates that the object with a key of **images/Strawberry-Tarts.jpg** was deleted from the S3 share bucket.

Finally, you test an unauthorized use case.

96. To try to change the permission of the Donuts.jpg object so that it can be read publicly, run the following command. In the command, replace *<cafe-xxxxnnn>* with your S3 bucket name:

```
aws s3api put-object-acl --bucket <cafe-xxxxnnn> --key images/Donuts.jpg --acl public-read
```

The command fails and displays the following error message as expected: "An error occurred (AccessDenied) when calling the PutObjectAcl operation: Access Denied"

## Conclusion

Congratulations! You now have successfully done the following:

- Used the s3api and s3 AWS CLI commands to create and configure an S3 bucket
- Verified write permissions to a user on an S3 bucket
- Configured event notification on an S3 bucket



# Lab complete

---

Congratulations! You have completed the lab.

97. At the top of this page, choose **End Lab** and then choose **Yes** to confirm that you want to end the lab.

A panel appears indicating that "You may close this message box now. Lab resources are terminating."

98. To close the **End Lab** panel, choose the **X** in the upper-right corner.

## Additional resources

---

- [AWS CLI documentation for s3](#)
- [AWS CLI documentation for s3api](#)

For more information about AWS Training and Certification, see [AWS Training and Certification](#).

*Your feedback is welcome and appreciated.*

If you would like to share any suggestions or corrections, provide the details in the [AWS Training and Certification Contact Form](#).

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.