



# 스캔 데이터 사용 중단

## BlueXP classification

NetApp  
June 14, 2024

# 목차

스캔 데이터 사용 중단 .....	1
Amazon S3 버킷을 스캔합니다 .....	1
OneDrive 계정을 검색합니다 .....	7
SharePoint 계정을 검색합니다 .....	11
Google Drive 계정을 스캔합니다 .....	16
S3 프로토콜을 사용하는 오브젝트 스토리지를 검색합니다 .....	18

# 스캔 데이터 사용 중단

## Amazon S3 버킷을 스캔합니다

BlueXP 분류는 Amazon S3 버킷을 스캔하여 S3 오브젝트 스토리지에 상주하는 개인적이고 민감한 데이터를 식별할 수 있습니다. BlueXP 분류는 NetApp 솔루션용으로 생성되었는지에 관계없이 고객의 모든 버킷을 스캔할 수 있습니다.

• 참고 \* 이 정보는 BlueXP 분류 레거시 버전 1.30 이상에만 해당됩니다.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

1

클라우드 환경에서 **S3** 요구사항을 설정합니다

IAM 역할 준비 및 BlueXP 분류에서 S3로의 연결 설정 등 클라우드 환경이 BlueXP 분류 요구 사항을 충족할 수 있는지 확인합니다. [전체 목록을 참조하십시오.](#)

2

**BlueXP** 분류 인스턴스를 배포합니다

"[BlueXP 분류를 배포합니다](#)" 이미 배포된 인스턴스가 없는 경우

3

**S3** 작업 환경에서 **BlueXP** 분류를 활성화합니다

Amazon S3 작업 환경을 선택하고 \* 활성화 \* 를 클릭한 다음 필요한 권한이 포함된 IAM 역할을 선택합니다.

4

스캔할 버킷을 선택합니다

스캔하려는 버킷을 선택하면 BlueXP 분류가 스캔을 시작합니다.

### S3 사전 요구 사항 검토

다음 요구사항은 S3 버킷 스캔에만 적용됩니다.

**BlueXP** 분류 인스턴스에 대해 **IAM** 역할을 설정합니다

BlueXP 분류에는 계정의 S3 버킷에 연결하고 이를 스캔할 수 있는 권한이 필요합니다. 아래에 나열된 권한을 포함하는 IAM 역할을 설정합니다. BlueXP는 Amazon S3 작업 환경에서 BlueXP 분류를 활성화할 때 IAM 역할을 선택하라는 메시지를 표시합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}

```

### BlueXP 분류에서 Amazon S3로 연결을 제공합니다

BlueXP 분류는 Amazon S3에 연결해야 합니다. 이 연결을 제공하는 가장 좋은 방법은 VPC 엔드포인트를 통해 S3 서비스로 연결하는 것입니다. 자세한 내용은 [을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성"](#).

VPC 엔드포인트를 생성할 때 BlueXP 분류 인스턴스에 해당하는 지역, VPC 및 경로 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 BlueXP 분류가 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 [을 참조하십시오 "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"](#)

또는 NAT 게이트웨이를 사용하여 연결을 제공하는 방법도 있습니다.



프록시를 사용하여 인터넷을 통해 S3로 연결할 수는 없습니다.

### BlueXP 분류 인스턴스 배포

"BlueXP에서 BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

BlueXP가 이 AWS 계정에서 S3 버킷을 자동으로 검색하여 Amazon S3 작업 환경에 표시되도록 AWS에 구축된 Connector를 사용하여 인스턴스를 구축해야 합니다.

- 참고: \* 현재 S3 버킷을 스캔할 때는 구내 위치에 BlueXP 분류 배포를 지원하지 않습니다.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

### S3 작업 환경에서 BlueXP 분류 활성화

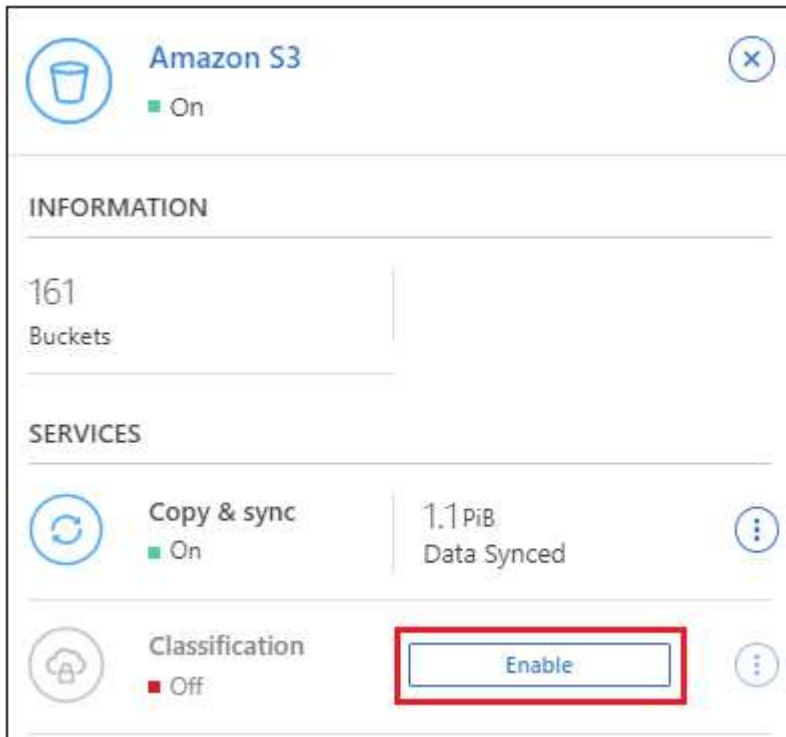
사전 요구 사항을 확인한 후 Amazon S3에서 BlueXP 분류를 활성화합니다.

단계

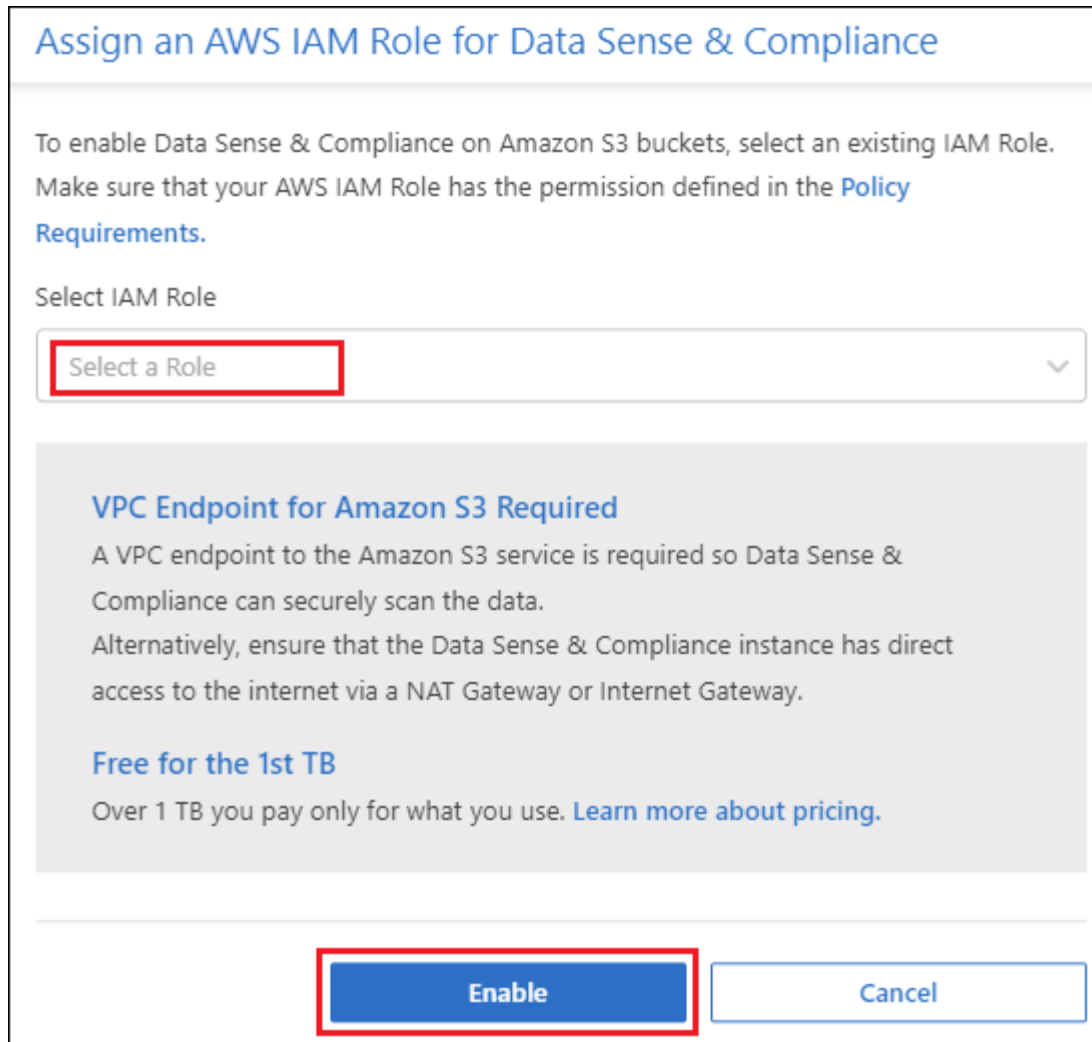
1. BlueXP 왼쪽 탐색 메뉴에서 \* 저장소 > Canvas \* 를 클릭합니다.
2. Amazon S3 작업 환경을 선택합니다.



3. 오른쪽의 서비스 창에서 \* 분류 \* 옆에 있는 \* 활성화 \* 를 클릭합니다.



4. 메시지가 표시되면 의 BlueXP 분류 인스턴스에 IAM 역할을 할당합니다 [필요한 권한](#).



5. 사용 \* 을 클릭합니다.



를 클릭하여 구성 페이지에서 작업 환경에 대한 규정 준수 검사를 활성화할 수도 있습니다 단추를 클릭하고 \* BlueXP 분류 활성화 \* 를 선택합니다.

결과

BlueXP는 인스턴스에 IAM 역할을 할당합니다.

### S3 버킷에서 규정 준수 스캔 활성화 및 비활성화

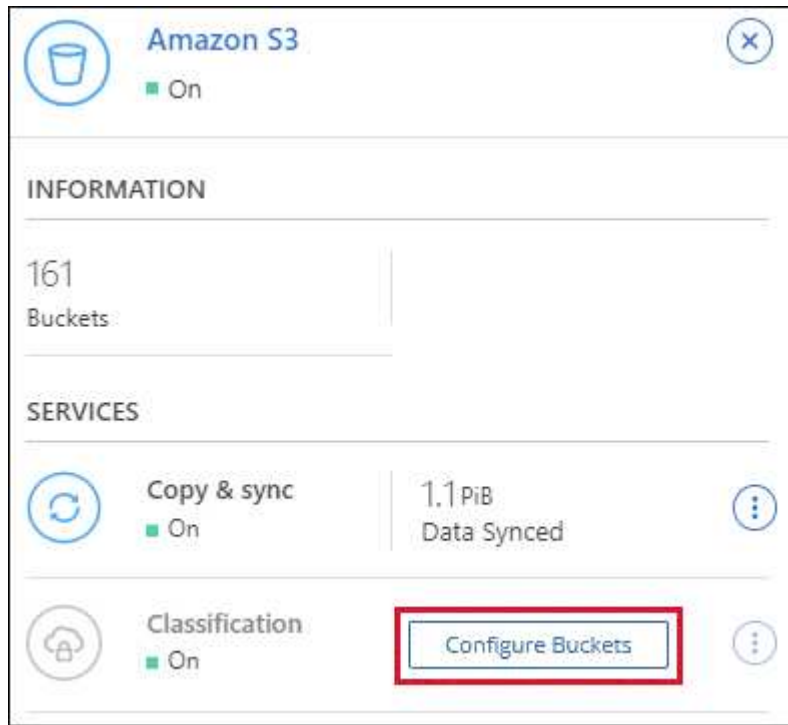
BlueXP에서 Amazon S3에서 BlueXP 분류를 사용하도록 설정한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다.

검사할 S3 버킷이 있는 AWS 계정에서 BlueXP가 실행되고 있으면 해당 버킷을 검색하여 Amazon S3 작업 환경에 표시합니다.

BlueXP 분류도 가능합니다 서로 다른 AWS 계정에 있는 S3 버킷을 스캔합니다.

단계

1. Amazon S3 작업 환경을 선택합니다.
2. 오른쪽의 서비스 창에서 \* 버킷 구성 \* 을 클릭합니다.



3. 버킷에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 활성화합니다.

Amazon S3 Configuration

15/28 Buckets in Scan Scope.

Scan	Bucket Name	Status	Required Action
Off   Map   <b>Map &amp; Classify</b>	BucketName1	● Not Scanning	Add Credentials
Off   <b>Map</b>   Map & Classify	BucketName2	● Continuously Scanning	
<b>Off</b>   Map   Map & Classify	BucketName3	● Not Scanning	

대상:	방법은 다음과 같습니다.
버킷에서 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
버킷에서 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
버킷에서 스캔을 비활성화합니다	Off * 를 클릭합니다

#### 결과

BlueXP 분류는 활성화한 S3 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 옆에 표시됩니다.

#### 추가 **AWS** 계정에서 버킷 스캔

기존 BlueXP 분류 인스턴스에 액세스하기 위해 해당 계정에서 역할을 할당하여 다른 AWS 계정에 있는 S3 버킷을 스캔할 수 있습니다.



## 단계

1. S3 버킷을 스캔하려는 대상 AWS 계정으로 이동하여 \* 다른 AWS 계정 \* 을 선택하여 IAM 역할을 생성합니다.

### Create role




#### Select type of trusted entity

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

#### Specify accounts that can use this role

Account ID\*

- Options
- Require external ID (Best practice when a third party will assume this role)
  - Require MFA 

다음을 수행하십시오.

- BlueXP 분류 인스턴스가 있는 계정의 ID를 입력합니다.
- 최대 CLI/API 세션 지속 시간 \* 을 1시간에서 12시간으로 변경하고 변경 사항을 저장합니다.
- BlueXP 분류 IAM 정책을 부착합니다. 필요한 권한이 있는지 확인합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

2. BlueXP 분류 인스턴스가 있는 소스 AWS 계정으로 이동하여 인스턴스에 연결된 IAM 역할을 선택합니다.
  - a. 최대 CLI/API 세션 지속 시간 \* 을 1시간에서 12시간으로 변경하고 변경 사항을 저장합니다.
  - b. Attach policies \* 를 클릭한 다음 \* Create policy \* 를 클릭합니다.
  - c. "STS:AssumeRole" 작업을 포함하는 정책을 생성하고 타겟 계정에서 생성한 역할의 ARN을 지정합니다.



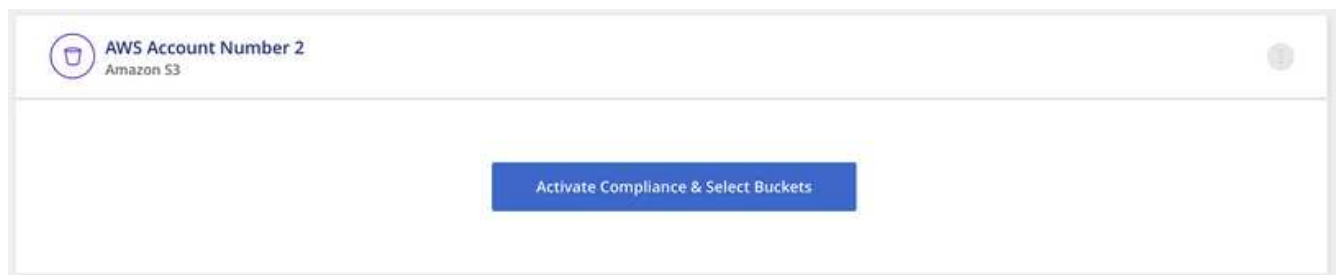
```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}

```

이제 BlueXP 분류 인스턴스 프로파일 계정이 추가 AWS 계정에 액세스할 수 있습니다.

3. Amazon S3 Configuration \* 페이지로 이동하면 새 AWS 계정이 표시됩니다. BlueXP 분류는 새 계정의 작업 환경을 동기화하고 이 정보를 표시하는 데 몇 분 정도 걸릴 수 있습니다.



4. BlueXP 분류 활성화 및 버킷 선택 \* 을 클릭하고 스캔할 버킷을 선택합니다.

결과

BlueXP 분류는 사용자가 활성화한 새 S3 버킷을 스캔하기 시작합니다.

## OneDrive 계정을 검색합니다

BlueXP 분류를 사용하여 사용자의 OneDrive 폴더에 있는 파일을 스캔하려면 몇 단계를

완료하십시오.

• 참고 \* 이 정보는 BlueXP 분류 레거시 버전 1.30 이상에만 해당됩니다.

## 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

1

**OneDrive** 사전 요구 사항을 검토합니다

OneDrive 계정에 로그인할 수 있는 관리자 자격 증명이 있는지 확인합니다.

2

**BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3

**OneDrive** 계정을 추가합니다

관리자 사용자 자격 증명을 사용하여 액세스할 OneDrive 계정에 로그인하여 새 작업 환경으로 추가합니다.

4

사용자를 추가하고 스캔 유형을 선택합니다

스캔할 OneDrive 계정의 사용자 목록을 추가하고 스캔 유형을 선택합니다. 한 번에 최대 100명의 사용자를 추가할 수 있습니다.

## OneDrive 요구 사항 검토

BlueXP 분류를 활성화하기 전에 다음 필수 구성 요소를 검토하여 지원되는 구성이 있는지 확인하십시오.

- 사용자의 파일에 대한 읽기 권한을 제공하는 비즈니스용 OneDrive 계정에 대한 관리자 로그인 자격 증명이 있어야 합니다.
- 스캔할 OneDrive 폴더가 있는 모든 사용자의 전자 메일 주소 목록이 선으로 구분되어 있어야 합니다.

## BlueXP 분류 인스턴스 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

BlueXP 분류는 일 수 있습니다 "클라우드에 구축" 또는 "인터넷 액세스가 가능한 사내 위치".

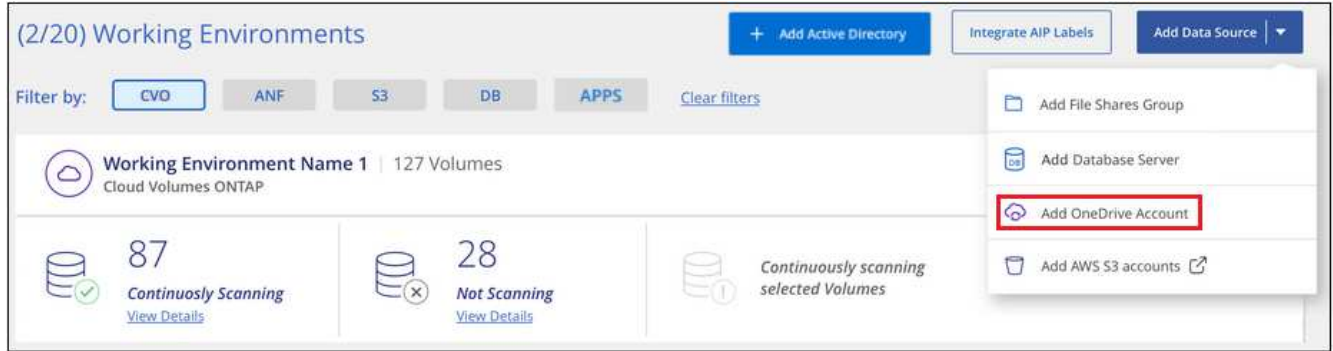
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

## OneDrive 계정 추가

사용자 파일이 있는 OneDrive 계정을 추가합니다.

단계

1. 작업 환경 구성 페이지에서 \* 데이터 소스 추가 \* > \* OneDrive 계정 추가 \* 를 클릭합니다.



2. OneDrive 계정 추가 대화 상자에서 \* OneDrive에 로그인 \* 을 클릭합니다.
3. 나타나는 Microsoft 페이지에서 OneDrive 계정을 선택하고 필요한 관리자 사용자 및 암호를 입력한 다음 \* 수락 \* 을 클릭하여 BlueXP 분류에서 이 계정의 데이터를 읽을 수 있도록 합니다.

OneDrive 계정이 작업 환경 목록에 추가됩니다.

## 규정 준수 검사에 **OneDrive** 사용자 추가

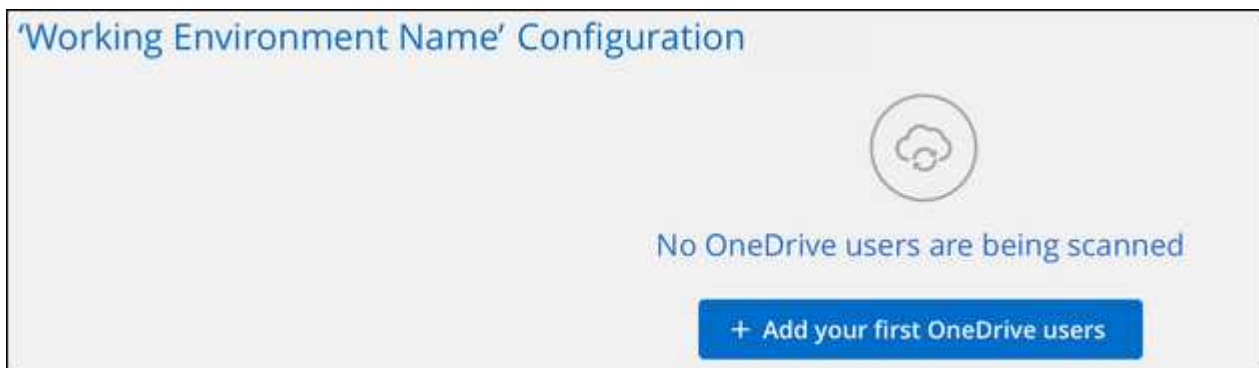
개별 OneDrive 사용자 또는 모든 OneDrive 사용자를 추가하여 파일이 BlueXP 분류에서 검사되도록 할 수 있습니다.

단계

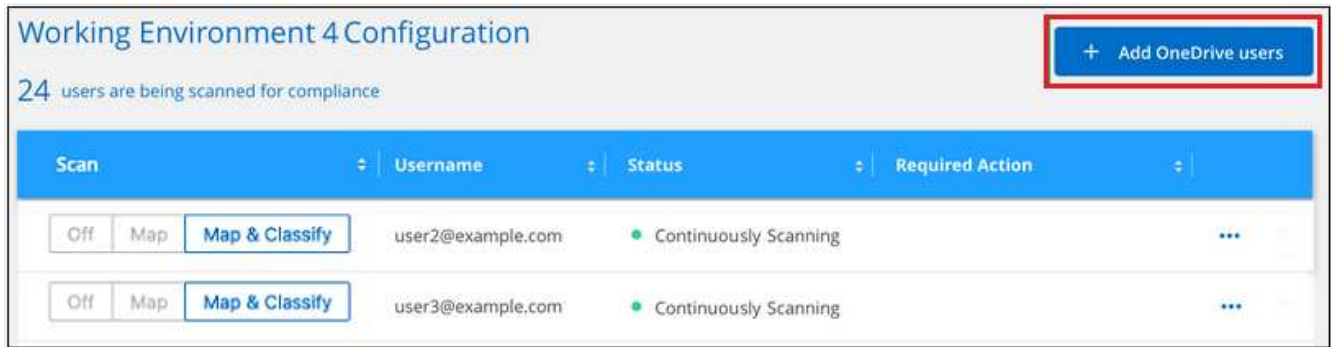
1. Configuration\_ 페이지에서 OneDrive 계정의 \* Configuration \* 버튼을 클릭합니다.



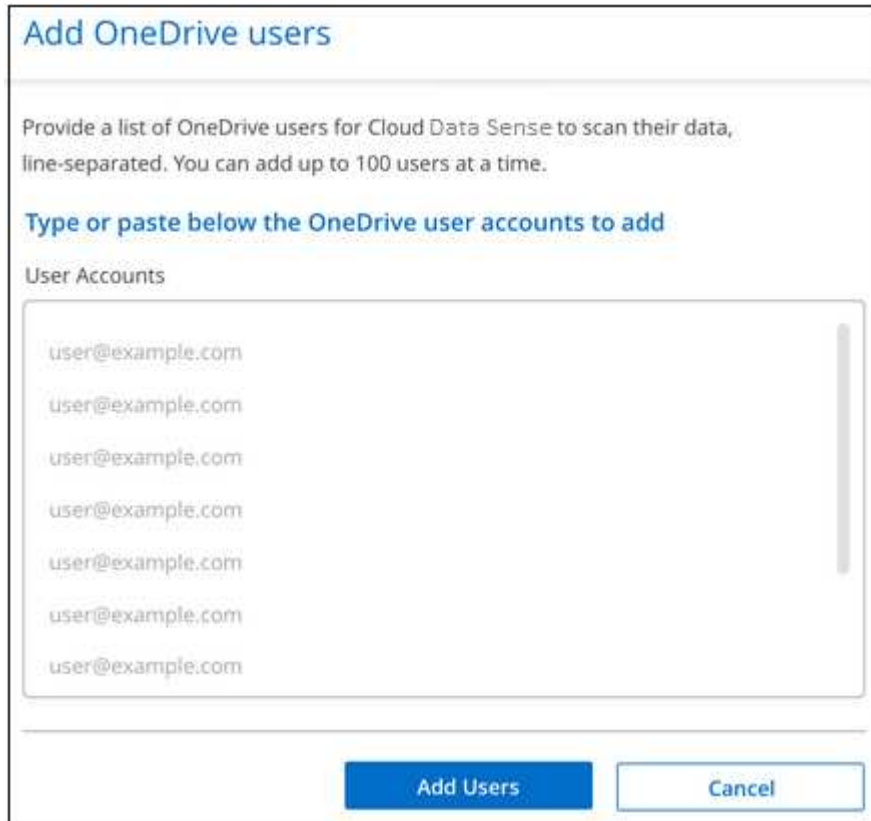
2. 이 OneDrive 계정에 사용자를 처음으로 추가하는 경우 \* 첫 번째 OneDrive 사용자 추가 \* 를 클릭합니다.



OneDrive 계정에서 다른 사용자를 추가하는 경우 \* OneDrive 사용자 추가 \* 를 클릭합니다.



3. 파일을 스캔할 사용자의 이메일 주소를 한 줄에 하나씩 추가하고(세션당 최대 100개) \* 사용자 추가 \* 를 클릭합니다.



확인 대화 상자에 추가된 사용자 수가 표시됩니다.

대화 상자에 추가할 수 없는 사용자가 나열되어 있으면 이 정보를 캡처하여 문제를 해결할 수 있습니다. 경우에 따라 수정된 이메일 주소로 사용자를 다시 추가할 수 있습니다.

4. 사용자 파일에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 활성화합니다.

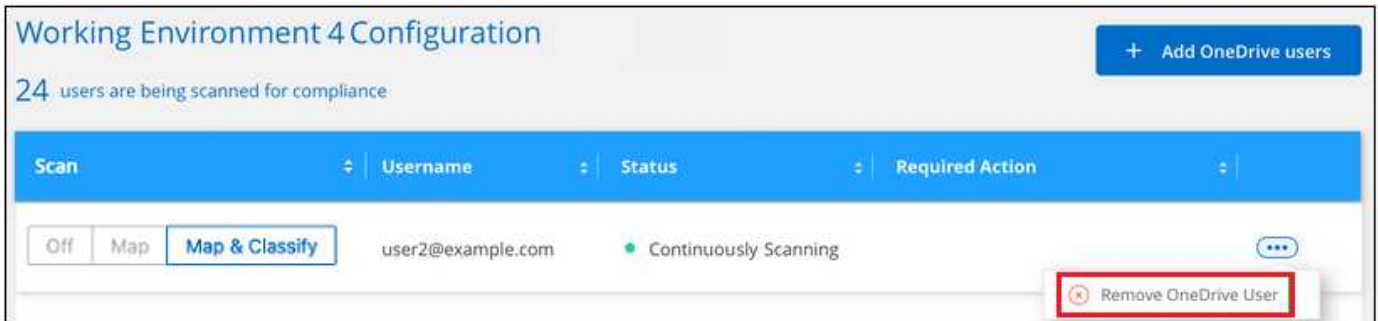
대상:	방법은 다음과 같습니다.
사용자 파일에 대한 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
사용자 파일에 대한 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
사용자 파일 스캔을 비활성화합니다	Off * 를 클릭합니다

결과

BlueXP 분류는 사용자가 추가한 파일의 스캔을 시작하고 그 결과는 대시보드와 다른 위치에 표시됩니다.

## 규정 준수 검사에서 **OneDrive** 사용자 제거

사용자가 회사를 떠나거나 이메일 주소가 변경되면 개별 OneDrive 사용자가 파일을 스캔하지 못하도록 할 수 있습니다. 구성 페이지에서 \* OneDrive 사용자 제거 \* 를 클릭하면 됩니다.



## SharePoint 계정을 검색합니다

BlueXP 분류를 사용하여 SharePoint Online 및 SharePoint On-Premise 계정의 파일 검색을 시작하는 몇 가지 단계를 완료합니다.

- 참고 \* 이 정보는 BlueXP 분류 레거시 버전 1.30 이상에만 해당됩니다.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

1

**SharePoint** 사전 요구 사항을 검토합니다

SharePoint 계정에 로그인할 수 있는 자격 증명이 있고 검색할 SharePoint 사이트의 URL이 있는지 확인합니다.

2

**BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3

**SharePoint** 계정에 로그인합니다

자격 있는 사용자 자격 증명을 사용하여 액세스할 SharePoint 계정에 로그인하여 새 데이터 원본/작업 환경으로 추가합니다.

4

검사할 **SharePoint** 사이트 URL을 추가합니다

SharePoint 계정에서 검색할 SharePoint 사이트 URL 목록을 추가하고 검색 유형을 선택합니다. 한 번에 최대 100개의 URL을 추가할 수 있으며 각 계정에 대해 최대 1,000개의 사이트를 추가할 수 있습니다.

## SharePoint 요구 사항을 검토합니다

다음 필수 구성 요소를 검토하여 SharePoint 계정에서 BlueXP 분류를 활성화할 준비가 되었는지 확인합니다.

- 모든 SharePoint 사이트에 읽기 권한을 제공하는 SharePoint 계정에 대한 관리자 사용자 로그인 자격 증명에 있어야 합니다.
  - SharePoint Online의 경우 관리자가 아닌 계정을 사용할 수 있지만 해당 사용자는 검색할 모든 SharePoint 사이트에 액세스할 수 있는 권한이 있어야 합니다.
- SharePoint 온-프레미스의 경우 SharePoint Server의 URL도 필요합니다.
- 검색할 모든 데이터에 대해 SharePoint 사이트 URL의 줄 구분 목록이 필요합니다.

## BlueXP 분류 인스턴스를 배포합니다

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

- SharePoint Online의 경우 BlueXP 분류는 일 수 있습니다 **"클라우드에 구축"**.
- SharePoint 온-프레미스의 경우 BlueXP 분류를 설치할 수 있습니다 **"인터넷 액세스가 가능한 사내 위치"** 또는 **"인터넷 액세스가 없는 온프레미스 위치"**.

인터넷에 연결되지 않은 사이트에 BlueXP 분류를 설치하는 경우 인터넷에 액세스하지 않고 BlueXP 커넥터도 같은 사이트에 설치해야 합니다. **"자세한 정보"**.

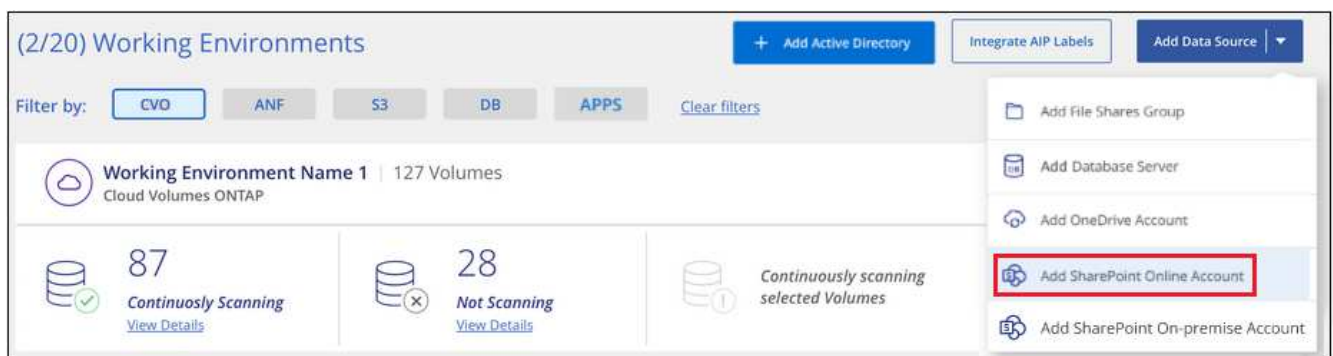
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

## SharePoint Online 계정을 추가합니다

사용자 파일이 있는 SharePoint Online 계정을 추가합니다.

단계

1. 작업 환경 구성 페이지에서 \* 데이터 원본 추가 \* > \* SharePoint Online 계정 추가 \* 를 클릭합니다.



2. SharePoint Online 계정 추가 대화 상자에서 \* SharePoint에 로그인 \* 을 클릭합니다.
3. 나타나는 Microsoft 페이지에서 SharePoint 계정을 선택하고 사용자 및 암호(SharePoint 사이트에 액세스할 수 있는 관리자 사용자 또는 기타 사용자)를 입력한 다음 \* Accept \* 를 클릭하여 BlueXP 분류에서 이 계정의 데이터를 읽을 수 있도록 합니다.

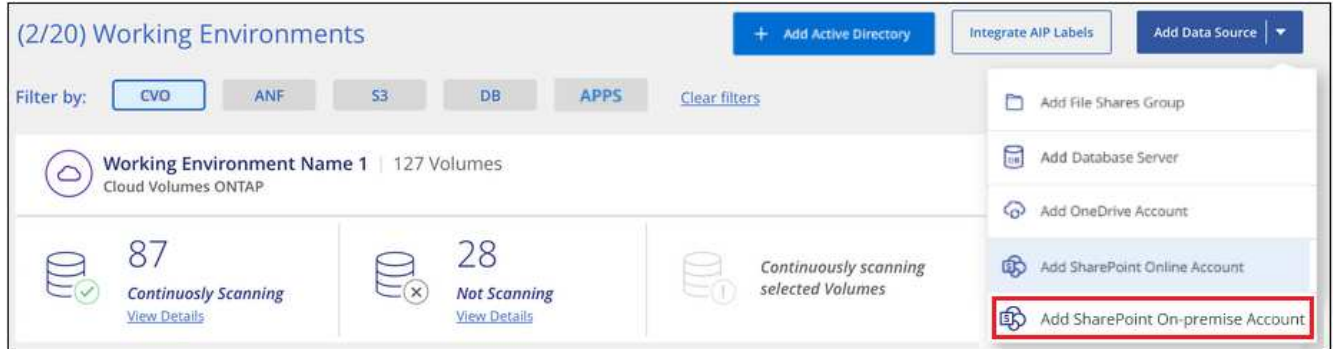
SharePoint Online 계정이 작업 환경 목록에 추가됩니다.

## SharePoint 온-프레미스 계정을 추가합니다

사용자 파일이 있는 SharePoint 온-프레미스 계정을 추가합니다.

단계

1. 작업 환경 구성 페이지에서 \* 데이터 소스 추가 \* > \* SharePoint 온-프레미스 계정 추가 \* 를 클릭합니다.



2. SharePoint 온-프레미스 서버에 로그인 대화 상자에서 다음 정보를 입력합니다.

- "domain/user" 또는 "user@domain" 형식의 admin 사용자 및 admin 암호
- SharePoint Server의 URL입니다

### Log into the SharePoint On-Premises Server

To activate Data Sense on your SharePoint business account, sign in to SharePoint with an Admin user.

Username	Password
<input type="text" value="domain/user or user@domain"/>	<input type="password" value="Password"/>

URL

3. 연결 \* 을 클릭합니다.

SharePoint 온-프레미스 계정이 작업 환경 목록에 추가됩니다.

## 규정 준수 검사에 **SharePoint** 사이트를 추가합니다

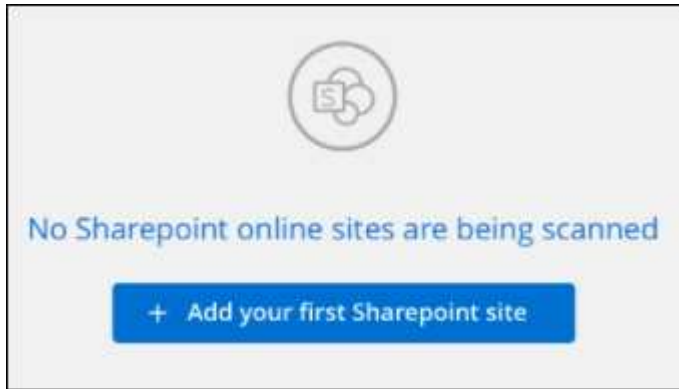
개별 SharePoint 사이트 또는 최대 1,000개의 SharePoint 사이트를 계정에 추가하여 관련 파일을 BlueXP 분류로 검색할 수 있습니다. SharePoint Online 또는 SharePoint 온-프레미스 사이트를 추가하든 단계는 동일합니다.

단계

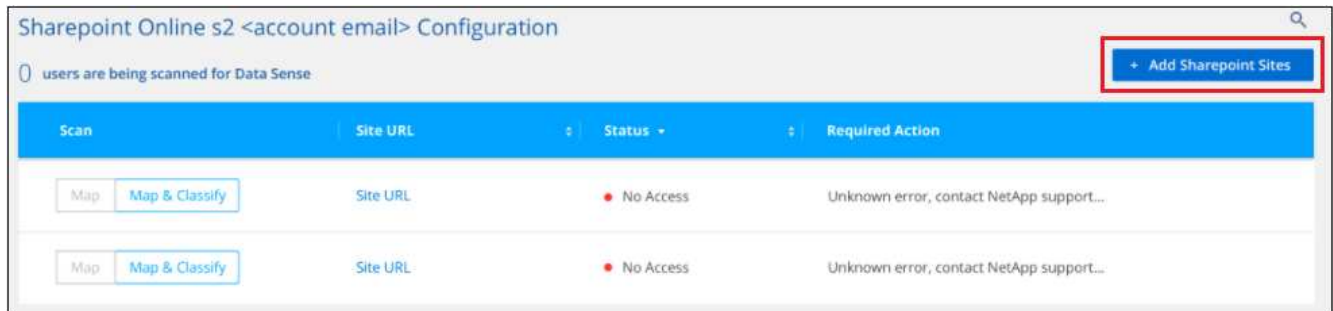
1. Configuration\_ 페이지에서 SharePoint 계정의 \* Configuration \* 버튼을 클릭합니다.



2. 이 SharePoint 계정에 대한 사이트를 처음으로 추가하는 경우 \* 첫 번째 SharePoint 사이트 추가 \* 를 클릭합니다.

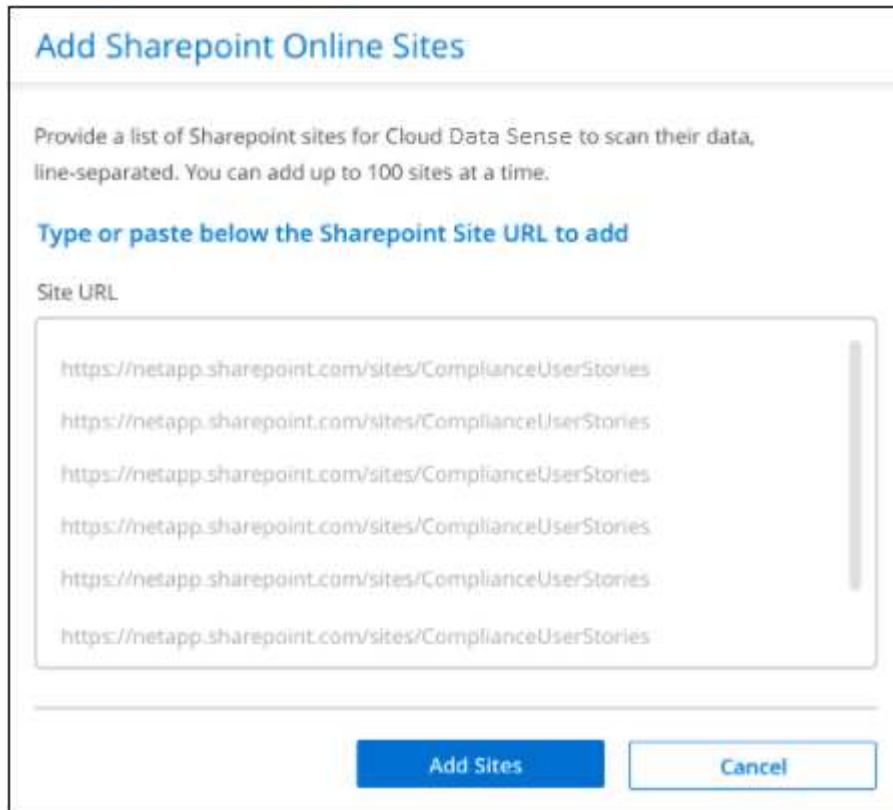


SharePoint 계정에서 사용자를 추가하려면 \* SharePoint 사이트 추가 \* 를 클릭합니다.



3. 파일을 스캔할 사이트의 URL을 한 줄에 하나씩(세션당 최대 100개) 추가하고 \* 사이트 추가 \* 를 클릭합니다.





확인 대화 상자에 추가된 사이트 수가 표시됩니다.

대화 상자에 추가할 수 없는 사이트가 나열되어 있으면 이 정보를 캡처하여 문제를 해결할 수 있습니다. 경우에 따라 수정된 URL을 사용하여 사이트를 다시 추가할 수 있습니다.

4. 이 계정에 대해 100개 이상의 사이트를 추가해야 하는 경우 이 계정에 대한 모든 사이트를 추가할 때까지 \* SharePoint 사이트 추가 \* 를 다시 클릭합니다(계정당 총 사이트 수 최대 1,000개).
5. SharePoint 사이트의 파일에서 매핑 전용 스캔 또는 매핑 및 분류 검사를 사용하도록 설정합니다.

대상:	방법은 다음과 같습니다.
파일에서 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
파일에 대한 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
파일 스캔을 비활성화합니다	Off * 를 클릭합니다

## 결과

BlueXP 분류는 사용자가 추가한 SharePoint 사이트의 파일을 검사하기 시작하고 그 결과는 대시보드와 다른 위치에 표시됩니다.

## 규정 준수 검사에서 **SharePoint** 사이트를 제거합니다

나중에 SharePoint 사이트를 제거하거나 SharePoint 사이트의 파일을 검색하지 않도록 결정한 경우 언제든지 개별 SharePoint 사이트를 제거하여 파일을 검색할 수 있습니다. 구성 페이지에서 \* SharePoint 사이트 제거 \* 를 클릭하기만 하면 됩니다.

Scan	Site URL	Status	Required Action
Off   Map   <b>Map &amp; Classify</b>	Site URL	Continuously Scanning	Remove SharePoint Site
Off   Map   <b>Map &amp; Classify</b>	Site URL	Continuously Scanning	

참고: 이 작업은 수행할 수 있습니다 "BlueXP 분류에서 전체 SharePoint 계정을 삭제합니다" SharePoint 계정에서 사용자 데이터를 더 이상 검색하지 않으려는 경우

## Google Drive 계정을 스캔합니다

BlueXP 분류를 사용하여 Google Drive 계정의 사용자 파일 스캔을 시작하려면 몇 단계를 완료하십시오.

- 참고 \* 이 정보는 BlueXP 분류 레거시 버전 1.30 이상에만 해당됩니다.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

1

**Google Drive** 사전 요구 사항을 검토합니다

Google Drive 계정에 로그인할 수 있는 관리자 자격 증명이 있는지 확인합니다.

2

**BlueXP** 분류를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3

**Google Drive** 계정에 로그인합니다

관리자 사용자 자격 증명을 사용하여 액세스하려는 Google Drive 계정에 로그인하여 새 데이터 소스로 추가합니다.

4

사용자 파일에 대한 스캔 유형을 선택합니다

사용자 파일에 대해 수행할 스캔 유형, 매핑 또는 매핑 및 분류를 선택합니다.

### Google 드라이브 사전 요구 사항을 검토합니다

다음 전제 조건을 검토하여 Google Drive 계정에서 BlueXP 분류를 활성화할 준비가 되었는지 확인합니다.

- 사용자의 파일에 대한 읽기 액세스를 제공하는 Google Drive 계정에 대한 관리자 로그인 자격 증명이 있어야 합니다

## 현재 제한 사항

다음 BlueXP 분류 기능은 현재 Google 드라이브 파일에서 지원되지 않습니다.

- 데이터 조사 페이지에서 파일을 볼 때 단추 모음의 작업은 활성화되지 않습니다. 파일을 복사, 이동, 삭제할 수 없습니다.
- Google Drive의 파일 내에서 사용 권한을 확인할 수 없으므로 조사 페이지에 사용 권한 정보가 표시되지 않습니다.

## BlueXP 분류를 배포합니다

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

BlueXP 분류는 일 수 있습니다 "클라우드에 구축" 또는 "인터넷 액세스가 가능한 사내 위치".

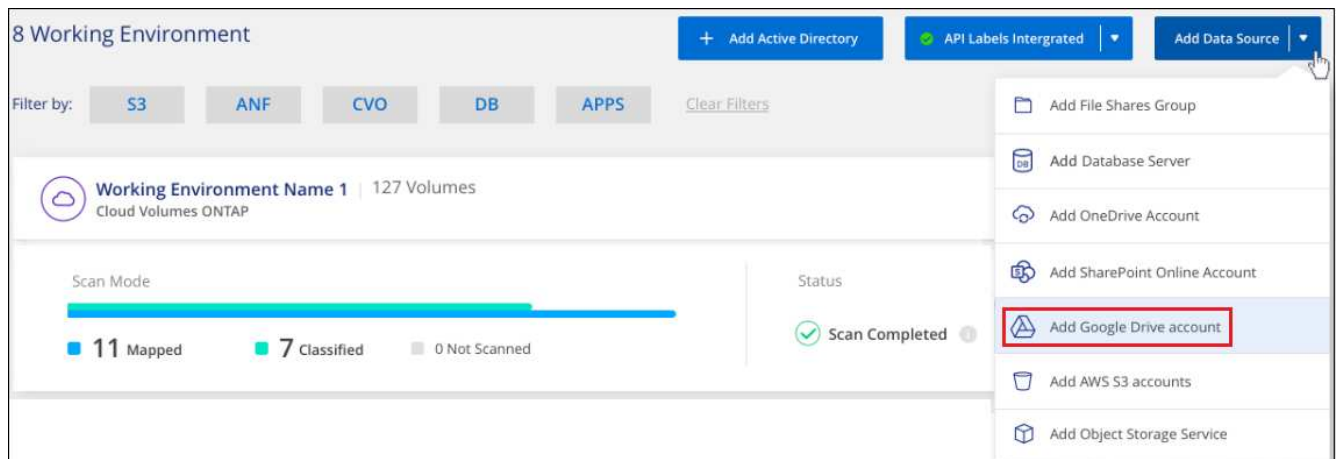
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

## Google Drive 계정을 추가합니다

사용자 파일이 있는 Google Drive 계정을 추가합니다. 여러 사용자의 파일을 스캔하려면 각 사용자에 대해 이 단계를 실행해야 합니다.

### 단계

1. 작업 환경 구성 페이지에서 \* 데이터 소스 추가 \* > \* Google 드라이브 계정 추가 \* 를 클릭합니다.



2. Google 드라이브 계정 추가 대화 상자에서 \* Google 드라이브에 로그인 \* 을 클릭합니다.
3. 나타나는 Google 페이지에서 Google Drive 계정을 선택하고 필요한 관리자 사용자 및 암호를 입력한 다음 \* Accept \* 를 클릭하여 BlueXP 분류에서 이 계정의 데이터를 읽을 수 있도록 합니다.

Google Drive 계정이 작업 환경 목록에 추가됩니다.

## 사용자 데이터에 대한 검색 유형을 선택합니다

BlueXP 분류가 사용자 데이터에 대해 수행할 스캔 유형을 선택합니다.

### 단계

1. Configuration\_ 페이지에서 Google Drive 계정의 \* Configuration \* 버튼을 클릭합니다.



2. Google Drive 계정의 파일에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 활성화합니다.



대상:	방법은 다음과 같습니다.
파일에서 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
파일에 대한 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
파일 스캔을 비활성화합니다	Off * 를 클릭합니다

#### 결과

BlueXP 분류는 사용자가 추가한 Google Drive 계정의 파일 스캔을 시작하고 그 결과는 대시보드와 다른 위치에 표시됩니다.

#### 규정 준수 스캔에서 Google Drive 계정을 제거합니다

단일 사용자의 Google Drive 파일만 단일 Google Drive 계정의 일부이므로, 사용자의 Google Drive 계정에서 파일 검색을 중지하려면 다음을 수행해야 합니다 "[BlueXP 분류에서 Google Drive 계정을 삭제합니다](#)".

### S3 프로토콜을 사용하는 오브젝트 스토리지를 검색합니다

BlueXP 분류를 통해 개체 스토리지 내에서 직접 데이터 스캔을 시작하려면 몇 단계를 완료하십시오. BlueXP 분류는 S3(Simple Storage Service) 프로토콜을 사용하는 오브젝트 스토리지 서비스에서 데이터를 스캔할 수 있습니다. 여기에는 NetApp StorageGRID, IBM Cloud Object Store, Linode, B2 클라우드 스토리지, Amazon S3 등이 포함됩니다.

• 참고 \* 이 정보는 BlueXP 분류 레거시 버전 1.30 이상에만 해당됩니다.

#### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.



오브젝트 스토리지의 사전 요구 사항을 검토합니다

객체 스토리지 서비스에 연결하려면 엔드포인트 URL이 있어야 합니다.

BlueXP 분류가 버킷에 액세스할 수 있도록 객체 스토리지 공급업체의 액세스 키 및 비밀 키가 있어야 합니다.

2

BlueXP 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3

오브젝트 스토리지 서비스를 추가합니다

BlueXP 분류에 오브젝트 스토리지 서비스를 추가합니다.

4

스캔할 버킷을 선택합니다

스캔하려는 버킷을 선택하면 BlueXP 분류가 스캔을 시작합니다.

## 오브젝트 스토리지의 요구사항 검토

BlueXP 분류를 활성화하기 전에 다음 필수 구성 요소를 검토하여 지원되는 구성이 있는지 확인하십시오.

- 객체 스토리지 서비스에 연결하려면 엔드포인트 URL이 있어야 합니다.
- BlueXP 분류가 버킷에 액세스할 수 있도록 객체 스토리지 공급업체의 액세스 키 및 비밀 키가 있어야 합니다.

## BlueXP 분류 인스턴스 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

인터넷을 통해 액세스할 수 있는 S3 오브젝트 스토리지에서 데이터를 스캔하는 경우 "[클라우드에 BlueXP 분류를 배포합니다](#)" 또는 "[인터넷 액세스가 가능한 사내 위치에 BlueXP 분류를 배포합니다](#)".

인터넷에 액세스할 수 없는 어두운 사이트에 설치된 S3 오브젝트 스토리지에서 데이터를 스캔하는 경우, 다음을 수행해야 합니다 "[인터넷에 액세스할 수 없는 동일한 사내 위치에 BlueXP 분류를 배포합니다](#)". 또한 BlueXP Connector를 동일한 사내 위치에 배포해야 합니다.

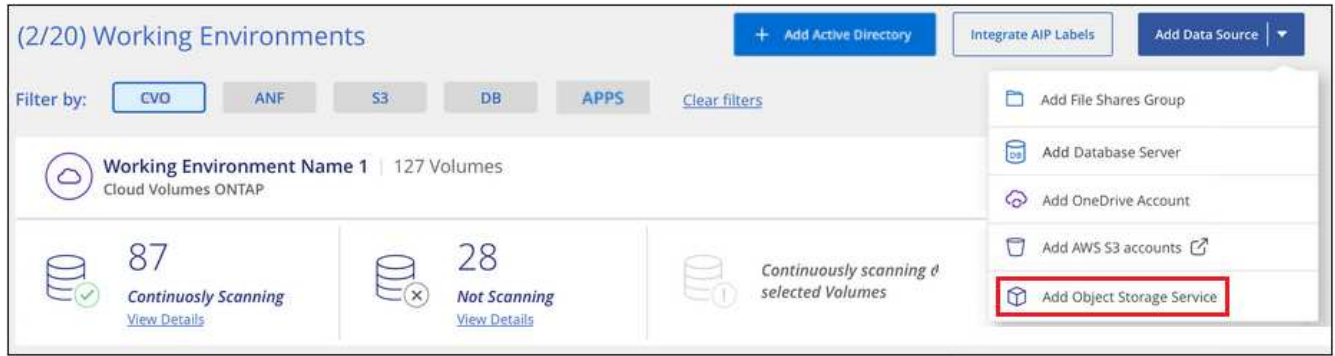
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

## BlueXP 분류에 오브젝트 스토리지 서비스 추가

오브젝트 스토리지 서비스를 추가합니다.

단계

1. 작업 환경 구성 페이지에서 \* 데이터 소스 추가 \* > \* 객체 스토리지 서비스 추가 \* 를 클릭합니다.



2. 개체 스토리지 서비스 추가 대화 상자에서 개체 스토리지 서비스에 대한 세부 정보를 입력하고 \* 계속 \* 을 클릭합니다.
  - a. 작업 환경에 사용할 이름을 입력합니다. 이 이름은 연결하려는 오브젝트 스토리지 서비스의 이름을 반영해야 합니다.
  - b. 객체 스토리지 서비스에 액세스하려면 엔드포인트 URL을 입력하십시오.
  - c. 액세스 키 및 비밀 키를 입력하여 BlueXP 분류가 오브젝트 저장소의 버킷에 액세스할 수 있도록 합니다.

### Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKDO574NDJG86795"/>	<input type="password" value="....."/>

결과

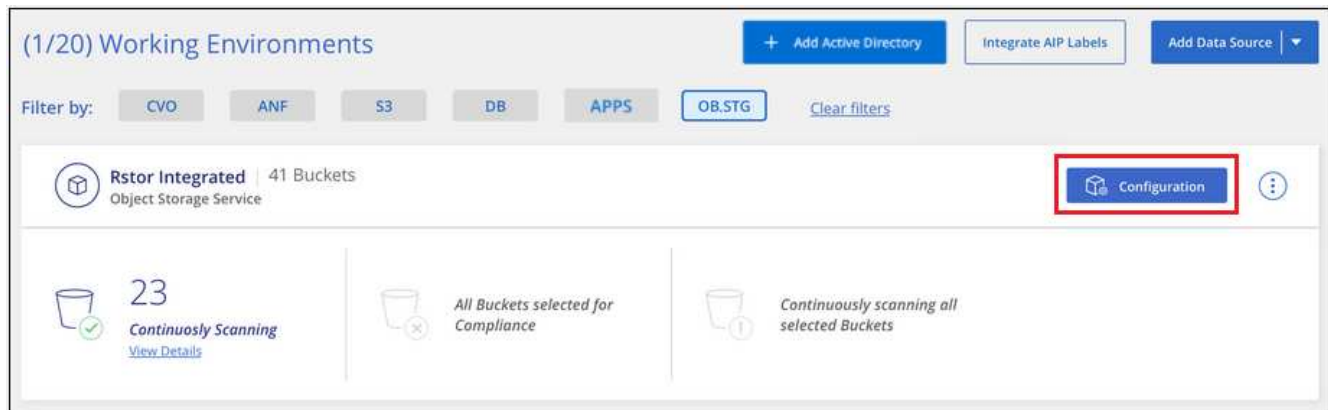
새로운 오브젝트 스토리지 서비스가 작업 환경 목록에 추가됩니다.

## 오브젝트 스토리지 버킷에 대한 규정 준수 검사 설정 및 해제

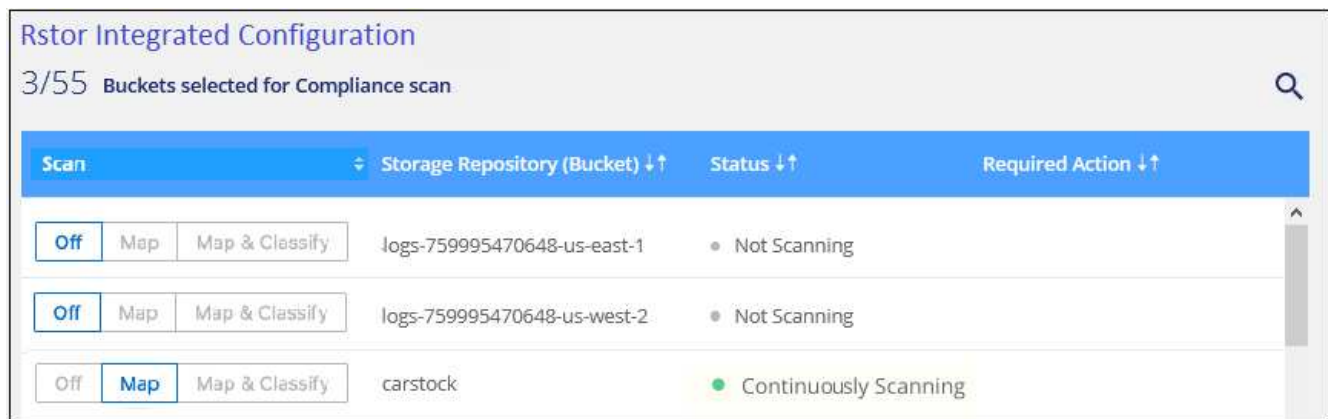
오브젝트 스토리지 서비스에서 BlueXP 분류를 활성화한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다. BlueXP 분류는 이러한 버킷을 검색하여 사용자가 만든 작업 환경에 표시합니다.

단계

1. 구성 페이지의 오브젝트 스토리지 서비스 작업 환경에서 \* 구성 \* 을 클릭합니다.



2. 버킷에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 활성화합니다.



대상:	방법은 다음과 같습니다.
버킷에서 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
버킷에서 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
버킷에서 스캔을 비활성화합니다	Off * 를 클릭합니다

결과

BlueXP 분류는 활성화한 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.



## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.