데이터 소스에서 스캔을 활성화합니다

Cloud Data Sense

NetApp
May 12, 2022

목차

데이터 소스에서 스캔을 활성화합니다 . . . 1
- Cloud Volumes ONTAP 및 사내 ONTAP에 대한 클라우드 데이터 센스를 시작하십시오 . . . 1
- Azure NetApp Files용 클라우드 데이터 센스를 시작하십시오 . . . 6
- ONTAP용 Amazon FSx에 대한 클라우드 데이터 센스를 시작해 보십시오 . . . 10
- Amazon S3에 대한 Cloud Data Sense 시작하기 . . . 15
- 데이터베이스 스키마를 검색하는 중입니다 . . . 21
- OneDrive 계정 스캔 중 . . . 25
- SharePoint 계정 스캔 중 . . . 28
- Google Drive 계정을 검색하는 중입니다 . . . 32
- 파일 공유를 검색하는 중입니다 . . . 34
- S3 프로토콜을 사용하는 오브젝트 스토리지 스캔 . . . 38

데이터 소스에서 스캔을 활성화합니다

Cloud Volumes ONTAP 및 사내 ONTAP에 대한 클라우드 데이터 센스를 시작하십시오

클라우드 데이터 센스를 사용하여 Cloud Volumes ONTAP 및 온프레미스 ONTAP 볼륨을 스캔하려면 몇 단계를 완료하십시오.

빠른 시작

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

볼륨을 스캔하려면 먼저 Cloud Manager에서 시스템을 작업 환경으로 추가해야 합니다.

- Cloud Volumes ONTAP 시스템의 경우, 이러한 작업 환경을 Cloud Manager에서 이미 사용할 수 있어야 합니다
- 사내 ONTAP 시스템의 경우, "Cloud Manager가 ONTAP 클러스터를 검색해야 합니다"

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

데이터 감지 * 를 클릭하고 * 구성 * 탭을 선택한 다음 특정 작업 환경의 볼륨에 대한 규정 준수 스캔을 활성화합니다.

이제 Cloud Data Sense가 활성화되었으므로 모든 볼륨에 액세스할 수 있는지 확인하십시오.

- 클라우드 데이터 감지 인스턴스에는 각 Cloud Volumes ONTAP 서브넷 또는 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다.
- Cloud Volumes ONTAP의 보안 그룹은 데이터 감지 인스턴스의 인바운드 연결을 허용해야 합니다.
- 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 엑스포트 정책은 데이터 감지 인스턴스에서 액세스할 수 있어야 합니다.
- CIFS 볼륨을 검색하려면 Data Sense에 Active Directory 자격 증명이 필요합니다.

  Compliance * > * Configuration * > * Edit CIFS Credentials * 를 클릭하고 자격 증명을 입력합니다.

스캔할 볼륨을 선택하거나 선택 취소하면 Cloud Data Sense에서 스캔을 시작하거나 중지합니다.

스캔할 데이터 소스 검색

스캔할 데이터 원본이 Cloud Manager 환경에 없으면 현재 캔버스에 추가할 수 있습니다.

Cloud Volumes ONTAP 시스템은 클라우드 관리자의 Canvas에서 이미 사용 가능해야 합니다. 사내 ONTAP 시스템의 경우 가 있어야 합니다 "Cloud Manager가 이러한 클러스터를 검색합니다".

Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 Cloud Volumes ONTAP 및 온-프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행할 수 있습니다 "클라우드 데이터 센스를 클라우드에 배포합니다" 또는 "인터넷 액세스가 가능한 사내 위치".

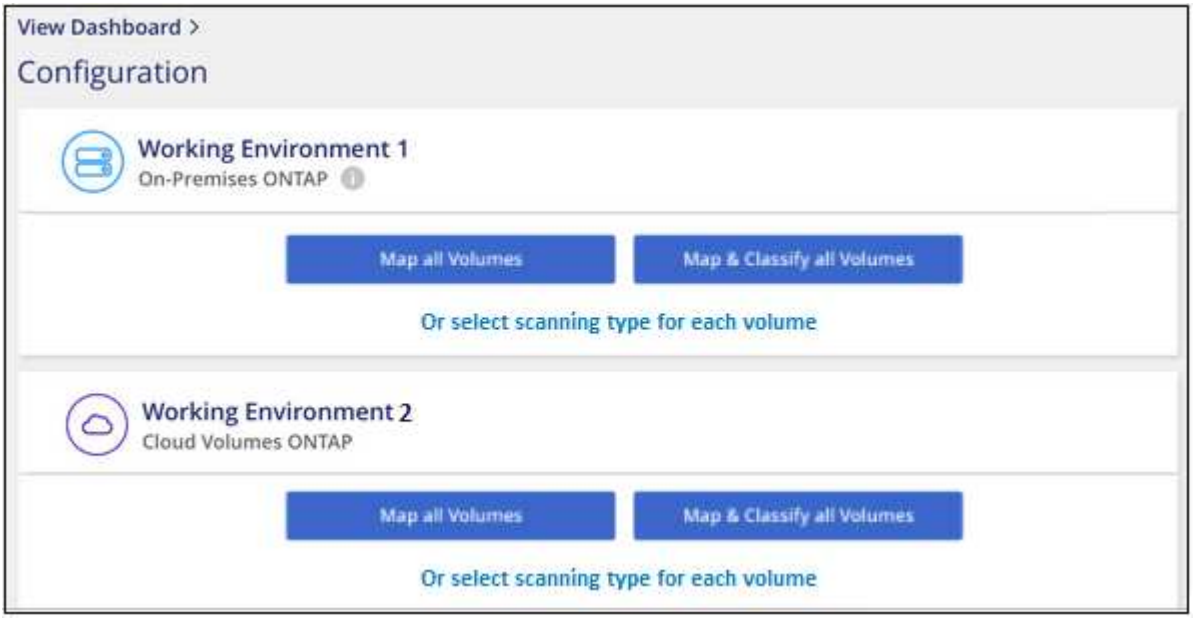
인터넷에 액세스할 수 없는 어두운 사이트에 설치된 온-프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

작업 환경에서 클라우드 데이터 센스를 활성화합니다

Cloud Volumes ONTAP 시스템(AWS, Azure 및 GCP) 및 온프레미스 ONTAP 클러스터에서 클라우드 데이터 센스를 활성화할 수 있습니다.

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.



2. 각 작업 환경의 볼륨을 스캔할 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아봅니다":
   - 모든 볼륨을 매핑하려면 * Map All Volumes * 를 클릭합니다.
   - 모든 볼륨을 매핑하고 분류하려면 * 모든 볼륨 매핑 및 분류 * 를 클릭합니다.
   - 각 볼륨에 대한 스캔을 사용자 정의하려면 * 를 클릭하거나 각 볼륨에 대한 스캐닝 유형을 선택한 다음 매핑 및 /또는 분류할 볼륨을 선택합니다.

     을 참조하십시오 볼륨에서 규정 준수 검사 활성화 및 비활성화 를 참조하십시오.

3. 확인 대화 상자에서 * Approve * (승인 *)를 클릭하여 데이터 센스에서 체적 스캔을 시작하도록 합니다.

Cloud Data Sense는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. Cloud Data Sense에서 초기 스캔을 마치면 Compliance 대시보드에서 결과를 얻을 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이

걸릴 수도 있습니다.

Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인

네트워킹, 보안 그룹 및 엑스포트 정책을 확인하여 Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인하십시오. CIFS 볼륨에 액세스할 수 있도록 CIFS 자격 증명을 사용하여 데이터 센스를 제공해야 합니다.

단계

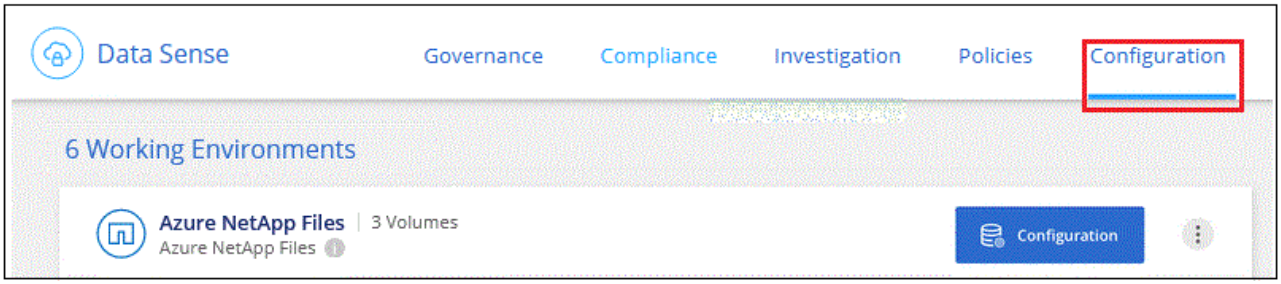
1. 클라우드 데이터 감지 인스턴스와 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터용 볼륨이 포함된 각 네트워크 사이에 네트워크 연결이 있는지 확인하십시오.
2. Cloud Volumes ONTAP용 보안 그룹이 데이터 감지 인스턴스의 인바운드 트래픽을 허용하는지 확인합니다.

   Data Sense 인스턴스의 IP 주소에서 오는 트래픽에 대한 보안 그룹을 열거나 가상 네트워크 내부의 모든 트래픽에 대한 보안 그룹을 열 수 있습니다.

3. 데이터 감지 인스턴스에 대해 다음 포트가 열려 있는지 확인합니다.
   - NFS – 포트 111 및 2049의 경우
   - CIFS – 포트 139 및 445의 경우
4. NFS 볼륨 내보내기 정책에 각 볼륨의 데이터에 액세스할 수 있도록 Data Sense 인스턴스의 IP 주소가 포함되어 있는지 확인합니다.
5. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 센스를 제공합니다.

   a. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.

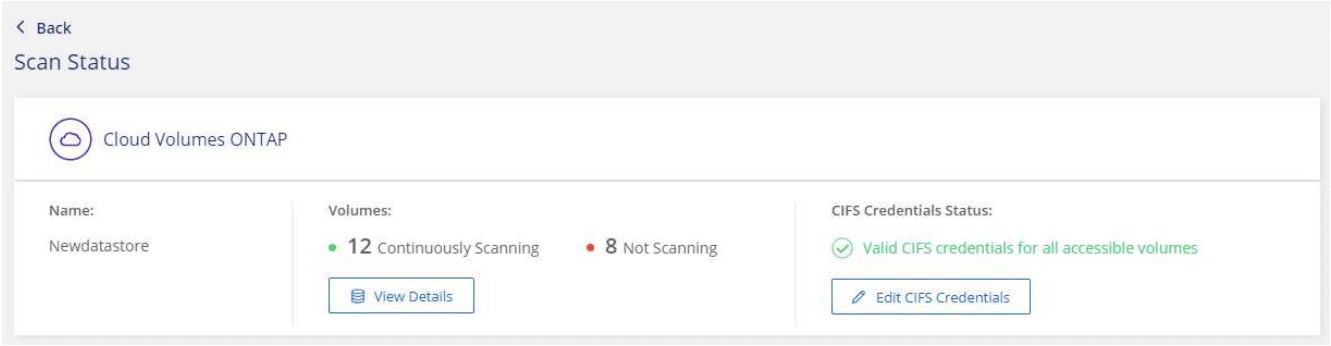
   b. Configuration * 탭을 클릭합니다.



   c. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 Data Sense가 시스템의 CIFS 볼륨을 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

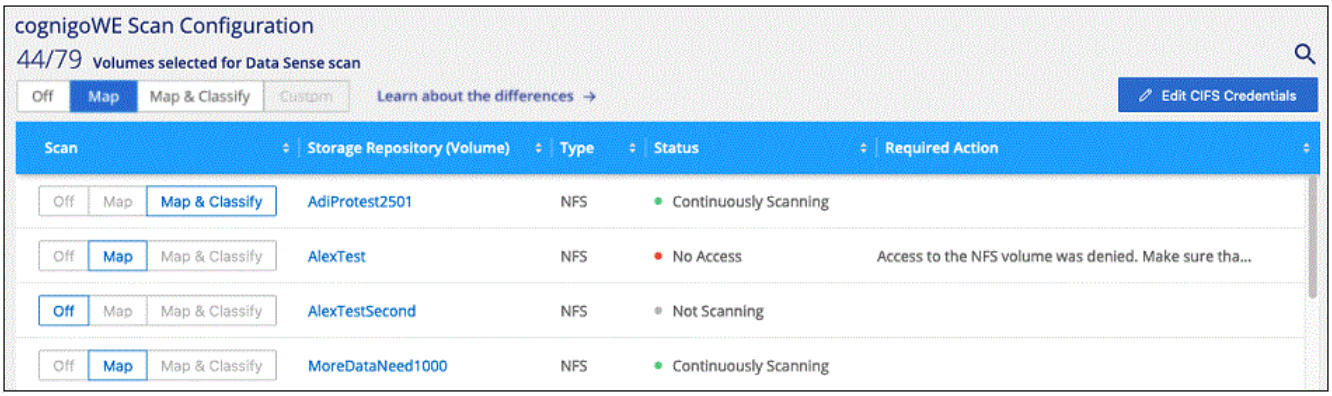
      자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Data Sense에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Data Sense 인스턴스에 저장됩니다.

      자격 증명을 입력한 후 모든 CIFS 볼륨이 성공적으로 인증되었다는 메시지가 표시됩니다.



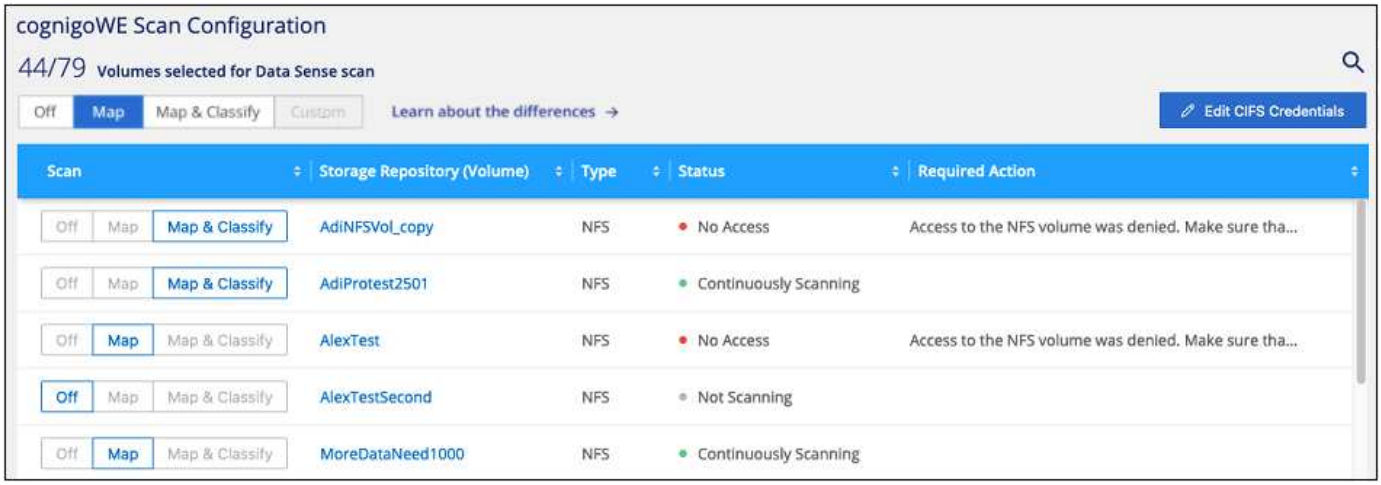
6. Configuration_ 페이지에서 * View Details * 를 클릭하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

   예를 들어, 다음 이미지에는 4개의 볼륨이 나와 있습니다. 이 중 하나는 Data Sense 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 Cloud Data Sense가 스캔할 수 없는 볼륨입니다.



볼륨에서 규정 준수 검사 활성화 및 비활성화

구성 페이지에서 언제든지 작업 환경에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로, 또는 그 반대로 변경할 수도 있습니다. 모든 볼륨을 검사하는 것이 좋습니다.



대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다

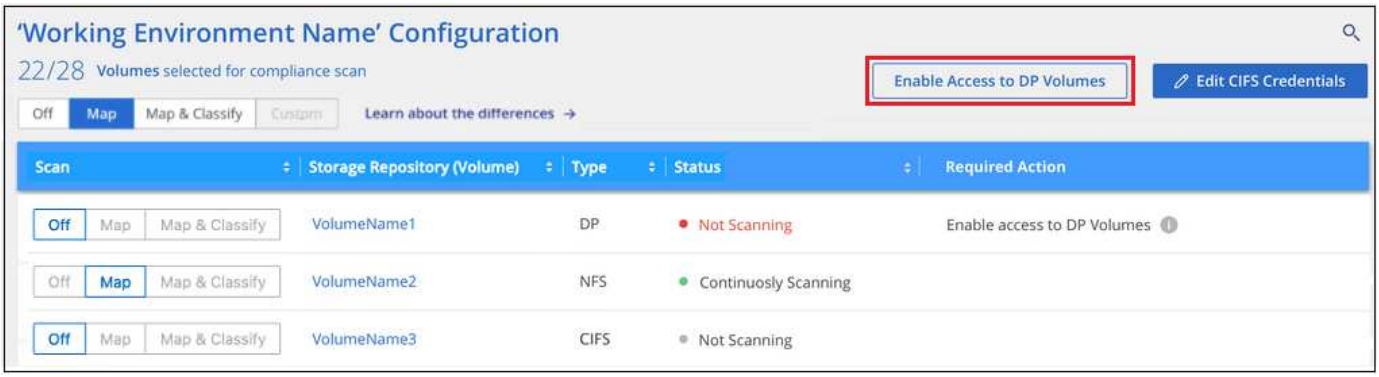
대상:	방법은 다음과 같습니다.
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다
볼륨에서 스캔을 비활성화합니다	볼륨 영역에서 * Off * 를 클릭합니다
모든 볼륨에서 매핑 전용 스캔을 활성화합니다	제목 영역에서 * Map * 을 클릭합니다
모든 볼륨에서 전체 스캔을 활성화합니다	제목 영역에서 * 지도 및 분류 * 를 클릭합니다
모든 볼륨에서 스캔을 비활성화합니다	제목 영역에서 * Off * 를 클릭합니다

작업 환경에 추가된 새 볼륨은 머리글 영역에서 * Map * 또는 * Map & Classify * 설정을 설정한 경우에만 자동으로 스캔됩니다. 제목 영역에서 * 사용자 정의 * 또는 * 끄기 * 로 설정하면 작업 환경에 추가한 새 볼륨마다 매핑 및/또는 전체 스캔을 활성화해야 합니다.

데이터 보호 볼륨을 검색하는 중입니다

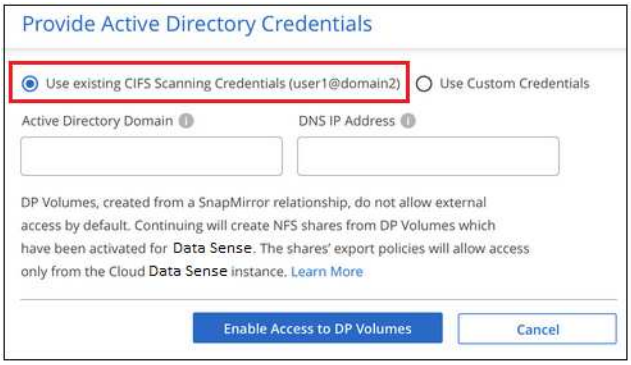
기본적으로 데이터 보호(DP) 볼륨은 외부에서 노출되지 않고 Cloud Data Sense에서 액세스할 수 없기 때문에 스캔되지 않습니다. 이는 사내 ONTAP 시스템 또는 Cloud Volumes ONTAP 시스템에서 SnapMirror 작업을 위한 타겟 볼륨입니다.

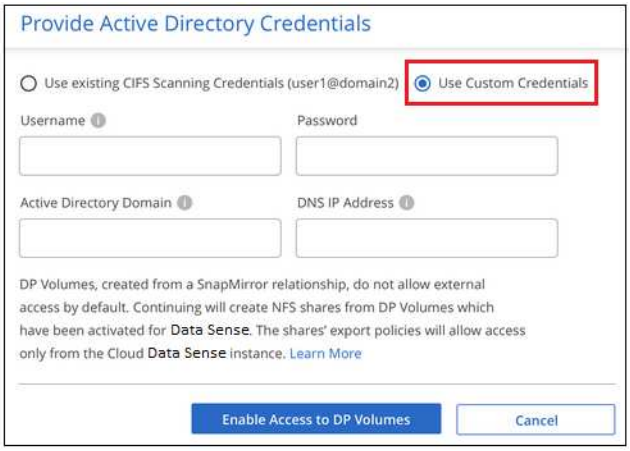
처음에 볼륨 목록은 이러한 볼륨을 *Type* DP*로 식별하며 *Status* Not Scanning* 및 *Required Action* DP 볼륨에 대한 액세스 사용*.



이러한 데이터 보호 볼륨을 스캔하려는 경우:

1. 페이지 맨 위에서 * DP 볼륨에 대한 액세스 활성화 * 를 클릭합니다.
2. 확인 메시지를 검토하고 * DP 볼륨에 대한 액세스 활성화 * 를 다시 클릭합니다.
   - 소스 ONTAP 시스템에서 처음에 NFS 볼륨으로 생성된 볼륨이 설정됩니다.
   - 소스 ONTAP 시스템에서 CIFS 볼륨으로 처음 생성된 볼륨을 사용하려면 CIFS 자격 증명을 입력하여 해당 DP 볼륨을 스캔해야 합니다. Cloud Data Sense가 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 이미 입력한 경우 해당 자격 증명을 사용하거나 다른 관리자 자격 증명 세트를 지정할 수 있습니다.





3. 스캔할 각 DP 볼륨을 활성화합니다 다른 볼륨을 활성화해도 마찬가지입니다.

활성화되면 Cloud Data Sense는 스캔을 위해 활성화된 각 DP 볼륨에서 NFS 공유를 생성합니다. 공유 내보내기 정책은 데이터 감지 인스턴스에서만 액세스를 허용합니다.

- 참고: * 처음에 DP 볼륨에 대한 액세스를 설정한 후 나중에 추가할 때 CIFS 데이터 보호 볼륨이 없는 경우 구성 페이지 맨 위에 * CIFS DP에 대한 액세스 활성화 * 버튼이 나타납니다. 이 버튼을 클릭하고 CIFS 자격 증명을 추가하여 이러한 CIFS DP 볼륨에 대한 액세스를 설정합니다.

Active Directory 자격 증명은 첫 번째 CIFS DP 볼륨의 스토리지 VM에만 등록되므로 해당 SVM의 모든 DP 볼륨이 검사됩니다. 다른 SVM에 상주하는 볼륨에 Active Directory 자격 증명이 등록되지 않으므로 DP 볼륨이 검색되지 않습니다.

Azure NetApp Files용 클라우드 데이터 센스를 시작하십시오

Azure NetApp Files용 클라우드 데이터 센스를 시작하려면 몇 단계를 완료하십시오.

빠른 시작

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

Azure NetApp Files 볼륨을 스캔하기 전에 "구성을 검색하려면 Cloud Manager를 설정해야 합니다".

"Cloud Manager에 클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

Compliance * 를 클릭하고 * Configuration * 탭을 선택한 다음 특정 작업 환경의 볼륨에 대한 규정 준수 검사를 활성화합니다.

이제 Cloud Data Sense가 활성화되었으므로 모든 볼륨에 액세스할 수 있는지 확인하십시오.

- 클라우드 데이터 감지 인스턴스에는 각 Azure NetApp Files 서브넷에 대한 네트워크 연결이 필요합니다.
- 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 엑스포트 정책은 데이터 감지 인스턴스에서 액세스할 수 있어야 합니다.

- CIFS 볼륨을 검색하려면 Data Sense에 Active Directory 자격 증명이 필요합니다.

  Compliance * > * Configuration * > * Edit CIFS Credentials * 를 클릭하고 자격 증명을 입력합니다.

스캔할 볼륨을 선택하거나 선택 취소하면 Cloud Data Sense에서 스캔을 시작하거나 중지합니다.

스캔할 **Azure NetApp Files** 시스템 검색

스캔할 Azure NetApp Files 시스템이 Cloud Manager에 작업 환경으로 설정되어 있지 않으면 현재 캔버스에 추가할 수 있습니다.

"Cloud Manager에서 Azure NetApp Files 시스템을 검색하는 방법을 알아보십시오".

Cloud Data Sense 인스턴스 구축

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

Azure NetApp Files 볼륨을 스캔할 때는 클라우드에 데이터 센스를 구축해야 하며 스캔하려는 볼륨과 동일한 영역에 구축해야 합니다.

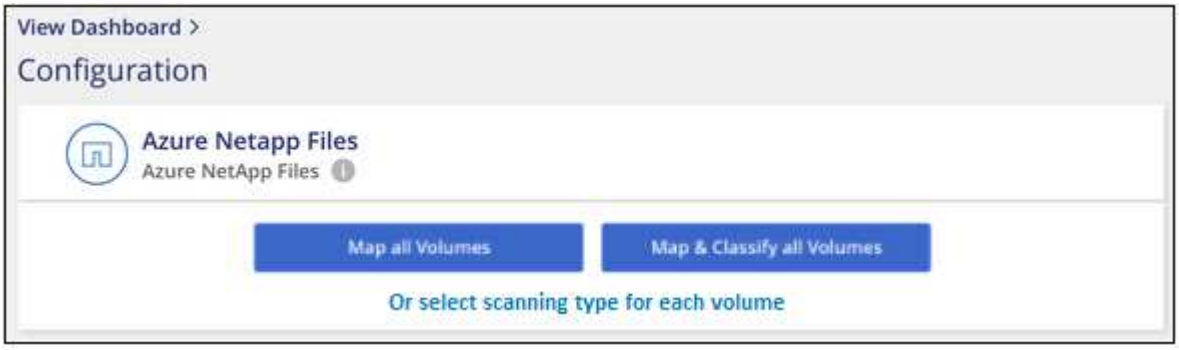
- 참고: * Azure NetApp Files 볼륨을 스캔할 때는 현재 사내 위치에 클라우드 데이터 센스를 배포하는 것이 지원되지 않습니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

작업 환경에서 클라우드 데이터 센스를 활성화합니다

Azure NetApp Files 볼륨에서 클라우드 데이터 센스를 활성화할 수 있습니다.

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.



2. 각 작업 환경의 볼륨을 스캔할 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아봅니다":
   - 모든 볼륨을 매핑하려면 * Map All Volumes * 를 클릭합니다.
   - 모든 볼륨을 매핑하고 분류하려면 * 모든 볼륨 매핑 및 분류 * 를 클릭합니다.
   - 각 볼륨에 대한 스캔을 사용자 정의하려면 * 를 클릭하거나 각 볼륨에 대한 스캐닝 유형을 선택한 다음 매핑 및 /또는 분류할 볼륨을 선택합니다.

     을 참조하십시오 볼륨에서 규정 준수 검사 활성화 및 비활성화 를 참조하십시오.

3. 확인 대화 상자에서 * Approve * (승인 *)를 클릭하여 데이터 센스에서 체적 스캔을 시작하도록 합니다.

Cloud Data Sense는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. Cloud Data Sense에서 초기 스캔을 마치면 Compliance 대시보드에서 결과를 얻을 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인

네트워킹, 보안 그룹 및 엑스포트 정책을 확인하여 Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인하십시오. CIFS 볼륨에 액세스할 수 있도록 CIFS 자격 증명을 사용하여 데이터 센스를 제공해야 합니다.

단계

1. 클라우드 데이터 감지 인스턴스와 Azure NetApp Files용 볼륨이 포함된 각 네트워크 사이에 네트워크 연결이 있는지 확인하십시오.

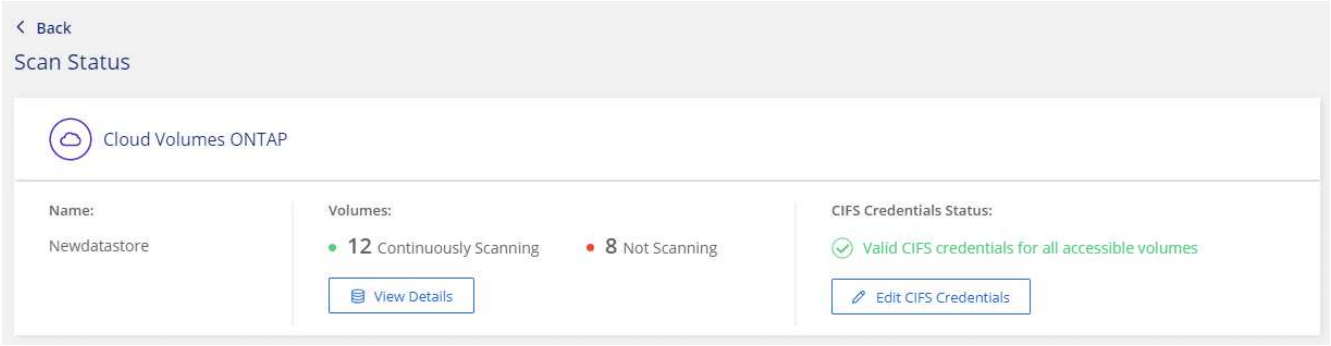
   Azure NetApp Files의 경우 클라우드 데이터 감지는 Cloud Manager와 같은 영역에 있는 볼륨만 스캔할 수 있습니다.

2. 데이터 감지 인스턴스에 대해 다음 포트가 열려 있는지 확인합니다.
   - NFS – 포트 111 및 2049의 경우
   - CIFS – 포트 139 및 445의 경우
3. NFS 볼륨 내보내기 정책에 각 볼륨의 데이터에 액세스할 수 있도록 Data Sense 인스턴스의 IP 주소가 포함되어 있는지 확인합니다.
4. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 센스를 제공합니다.
   a. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.
   b. Configuration * 탭을 클릭합니다.

   c. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 Data Sense가 시스템의 CIFS 볼륨을 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

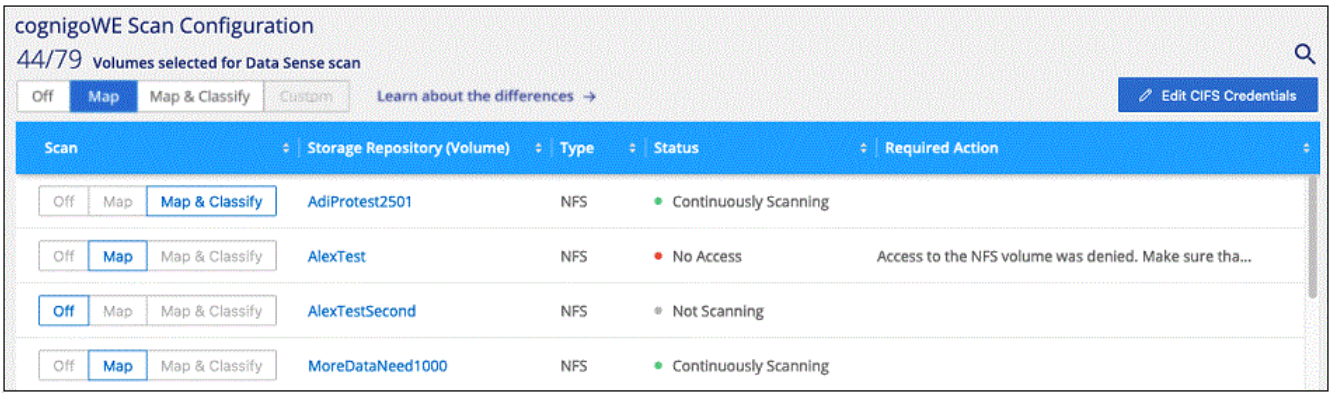
      자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Data Sense에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Data Sense 인스턴스에 저장됩니다.

      자격 증명을 입력한 후 모든 CIFS 볼륨이 성공적으로 인증되었다는 메시지가 표시됩니다.



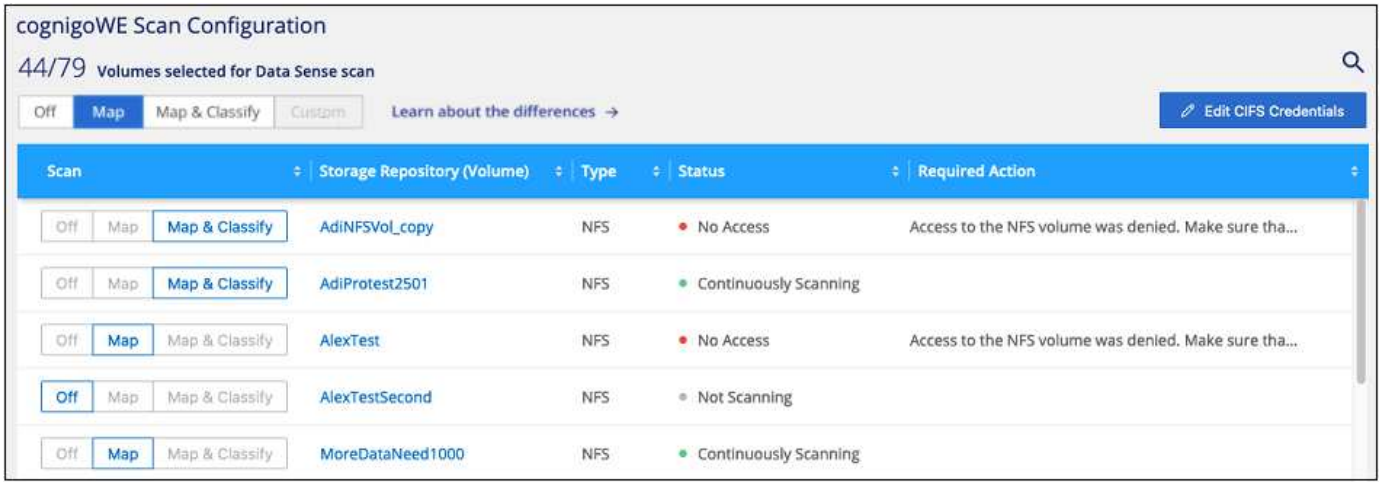
5. Configuration_ 페이지에서 * View Details * 를 클릭하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

   예를 들어, 다음 이미지에는 4개의 볼륨이 나와 있습니다. 이 중 하나는 Data Sense 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 Cloud Data Sense가 스캔할 수 없는 볼륨입니다.



볼륨에서 규정 준수 검사 활성화 및 비활성화

구성 페이지에서 언제든지 작업 환경에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로, 또는 그 반대로 변경할 수도 있습니다. 모든 볼륨을 검사하는 것이 좋습니다.



대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다

대상:	방법은 다음과 같습니다.
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다
볼륨에서 스캔을 비활성화합니다	볼륨 영역에서 * Off * 를 클릭합니다
모든 볼륨에서 매핑 전용 스캔을 활성화합니다	제목 영역에서 * Map * 을 클릭합니다
모든 볼륨에서 전체 스캔을 활성화합니다	제목 영역에서 * 지도 및 분류 * 를 클릭합니다
모든 볼륨에서 스캔을 비활성화합니다	제목 영역에서 * Off * 를 클릭합니다

작업 환경에 추가된 새 볼륨은 머리글 영역에서 * Map * 또는 * Map & Classify * 설정을 설정한 경우에만 자동으로 스캔됩니다. 제목 영역에서 * 사용자 정의 * 또는 * 끄기 * 로 설정하면 작업 환경에 추가한 새 볼륨마다 매핑 및/또는 전체 스캔을 활성화해야 합니다.

ONTAP용 Amazon FSx에 대한 클라우드 데이터 센스를 시작해 보십시오

클라우드 데이터 센스를 사용하여 ONTAP 볼륨에 대한 Amazon FSx 스캔을 시작하려면 몇 단계를 완료하십시오.

시작하기 전에

- 데이터 센스를 구축 및 관리하려면 AWS에 액티브 커넥터가 필요합니다.
- 작업 환경을 생성할 때 선택한 보안 그룹은 Cloud Data Sense 인스턴스의 트래픽을 허용해야 합니다. ONTAP용 FSx 파일 시스템에 연결된 ENI를 사용하여 관련 보안 그룹을 찾은 다음 AWS 관리 콘솔을 사용하여 편집할 수 있습니다.

  "Linux 인스턴스용 AWS 보안 그룹"

  "Windows 인스턴스용 AWS 보안 그룹"

  "AWS의 탄력적인 네트워크 인터페이스(ENI)"

빠른 시작

다음 단계를 따라 빠르게 시작하거나 아래로 스크롤하여 자세한 내용을 확인하십시오.

ONTAP 볼륨에 대해 FSx를 스캔하기 전에 "볼륨이 구성된 FSx 작업 환경이 있어야 합니다".

"Cloud Manager에 클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

데이터 감지 * 를 클릭하고 * 구성 * 탭을 선택한 다음 특정 작업 환경의 볼륨에 대한 규정 준수 스캔을 활성화합니다.

이제 Cloud Data Sense가 활성화되었으므로 모든 볼륨에 액세스할 수 있는지 확인하십시오.

- 클라우드 데이터 감지 인스턴스에는 ONTAP 서브넷을 위해 각 FSx에 대한 네트워크 연결이 필요합니다.
- 데이터 감지 인스턴스에 대해 다음 포트가 열려 있는지 확인합니다.

- NFS – 포트 111 및 2049의 경우
- CIFS – 포트 139 및 445의 경우

- NFS 볼륨 엑스포트 정책은 데이터 감지 인스턴스에서 액세스할 수 있어야 합니다.
- CIFS 볼륨을 검색하려면 Data Sense에 Active Directory 자격 증명이 필요합니다. + * Compliance * > * Configuration * > * Edit CIFS Credentials * 를 클릭하고 자격 증명을 입력합니다.

스캔할 볼륨을 선택하거나 선택 취소하면 Cloud Data Sense에서 스캔을 시작하거나 중지합니다.

검사할 **ONTAP** 파일 시스템용 **FSx** 검색

스캔할 ONTAP 파일 시스템용 FSx가 Cloud Manager에 작업 환경으로 설정되어 있지 않은 경우 이 파일을 캔버스에 추가할 수 있습니다.

"Cloud Manager에서 ONTAP 파일 시스템용 FSx를 검색 또는 생성하는 방법을 확인하십시오".

Cloud Data Sense 인스턴스 구축

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

AWS용 커넥터 및 스캔하려는 FSx 볼륨과 동일한 AWS 네트워크에 데이터 센스를 구축해야 합니다.

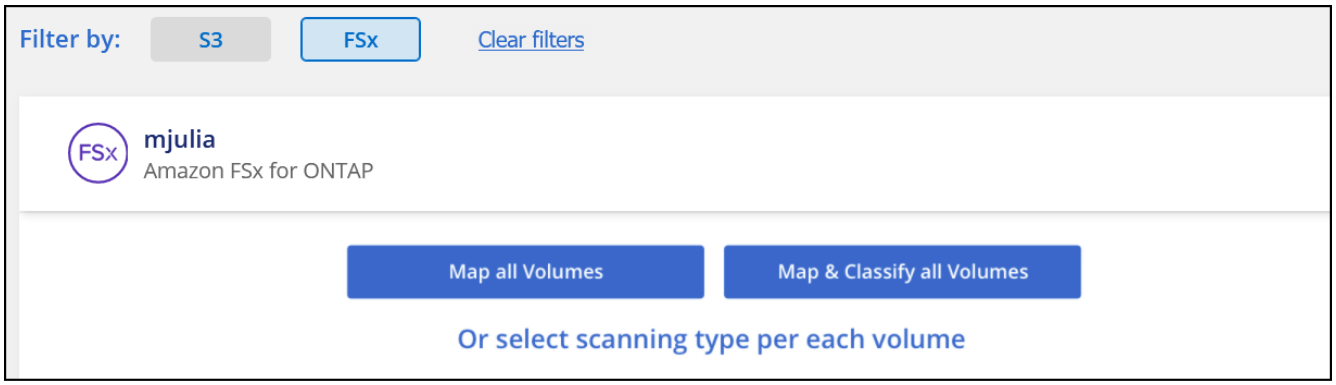
- 참고: * FSx 볼륨을 스캔할 때는 현재 온-프레미스 위치에 클라우드 데이터 감지 배포를 지원하지 않습니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

작업 환경에서 클라우드 데이터 센스를 활성화합니다

ONTAP 볼륨에 대해 FSx에 대한 클라우드 데이터 센스를 활성화할 수 있습니다.

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.



2. 각 작업 환경의 볼륨을 스캔할 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아봅니다":
   - 모든 볼륨을 매핑하려면 * Map All Volumes * 를 클릭합니다.
   - 모든 볼륨을 매핑하고 분류하려면 * 모든 볼륨 매핑 및 분류 * 를 클릭합니다.
   - 각 볼륨에 대한 스캔을 사용자 정의하려면 * 를 클릭하거나 각 볼륨에 대한 스캐닝 유형을 선택한 다음 매핑 및 /또는 분류할 볼륨을 선택합니다.

을 참조하십시오 볼륨에서 규정 준수 검사 활성화 및 비활성화 를 참조하십시오.

3. 확인 대화 상자에서 * Approve * (승인 *)를 클릭하여 데이터 센스에서 체적 스캔을 시작하도록 합니다.

Cloud Data Sense는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. Cloud Data Sense에서 초기 스캔을 마치면 Compliance 대시보드에서 결과를 얻을 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인

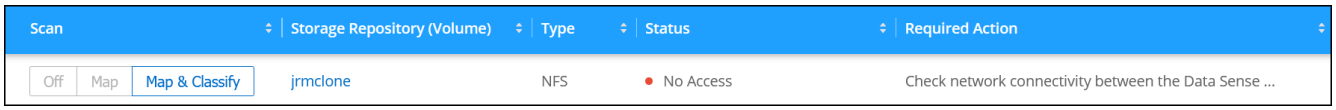
네트워킹, 보안 그룹 및 엑스포트 정책을 확인하여 Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인하십시오.

CIFS 볼륨에 액세스할 수 있도록 CIFS 자격 증명을 사용하여 데이터 센스를 제공해야 합니다.

단계

1. Configuration_페이지에서 * View Details * 를 클릭하여 상태를 검토하고 오류를 수정합니다.

   예를 들어, 다음 이미지는 Data Sense 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 Cloud Data Sense에서 스캔할 수 없는 볼륨을 보여 줍니다.



2. 클라우드 데이터 감지 인스턴스와 ONTAP용 FSx 볼륨을 포함하는 각 네트워크 사이에 네트워크 연결이 있는지 확인합니다.

   ONTAP용 FSx의 경우 Cloud Data Sense는 Cloud Manager와 동일한 영역에서만 볼륨을 스캔할 수 있습니다.

3. 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
   - NFS – 포트 111 및 2049의 경우
   - CIFS – 포트 139 및 445의 경우
4. NFS 볼륨 내보내기 정책에 데이터 감지 인스턴스의 IP 주소가 포함되어 각 볼륨의 데이터에 액세스할 수 있는지 확인합니다.
5. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 센스를 제공합니다.

   a. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.

   b. Configuration * 탭을 클릭합니다.

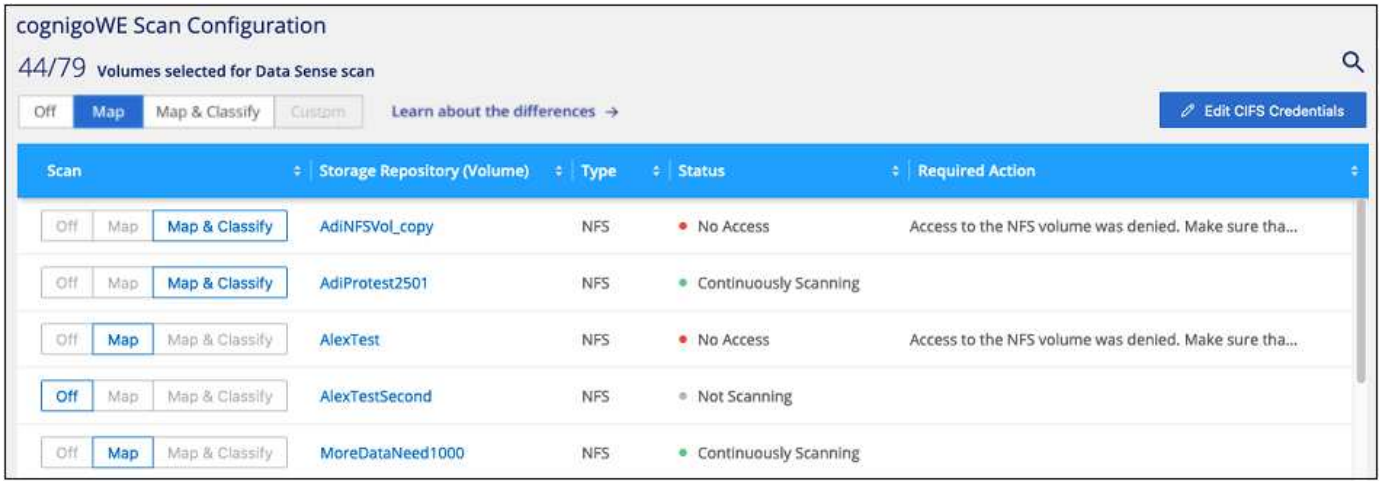
   c. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 Data Sense가 시스템의 CIFS 볼륨을 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

      자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Data Sense에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Data Sense 인스턴스에 저장됩니다.

   자격 증명을 입력한 후 모든 CIFS 볼륨이 성공적으로 인증되었다는 메시지가 표시됩니다.

볼륨에서 규정 준수 검사 활성화 및 비활성화

구성 페이지에서 언제든지 작업 환경에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로, 또는 그 반대로 변경할 수도 있습니다. 모든 볼륨을 검사하는 것이 좋습니다.



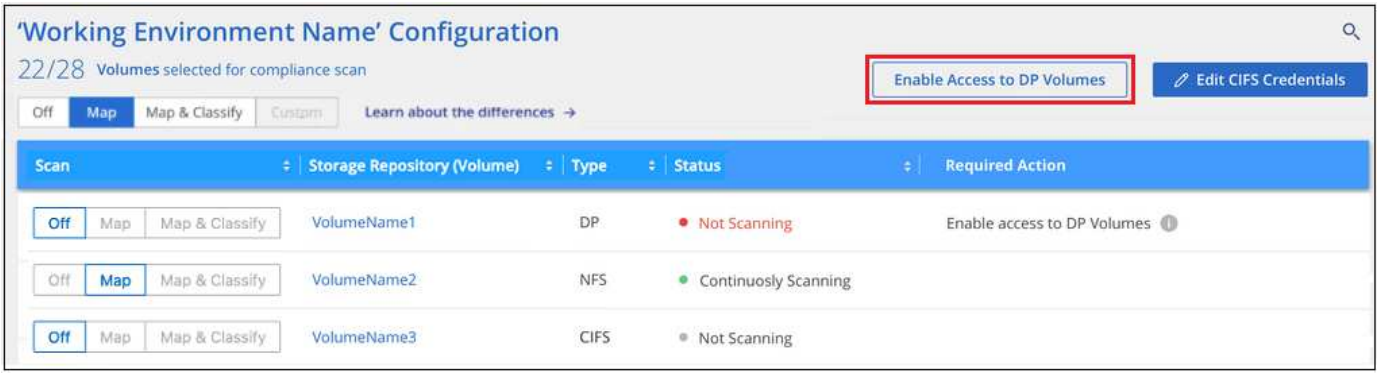
대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다
볼륨에서 스캔을 비활성화합니다	볼륨 영역에서 * Off * 를 클릭합니다
모든 볼륨에서 매핑 전용 스캔을 활성화합니다	제목 영역에서 * Map * 을 클릭합니다
모든 볼륨에서 전체 스캔을 활성화합니다	제목 영역에서 * 지도 및 분류 * 를 클릭합니다
모든 볼륨에서 스캔을 비활성화합니다	제목 영역에서 * Off * 를 클릭합니다

작업 환경에 추가된 새 볼륨은 머리글 영역에서 * Map * 또는 * Map & Classify * 설정을 설정한 경우에만 자동으로 스캔됩니다. 제목 영역에서 * 사용자 정의 * 또는 * 끄기 * 로 설정하면 작업 환경에 추가한 새 볼륨마다 매핑 및/또는 전체 스캔을 활성화해야 합니다.

데이터 보호 볼륨을 검색하는 중입니다

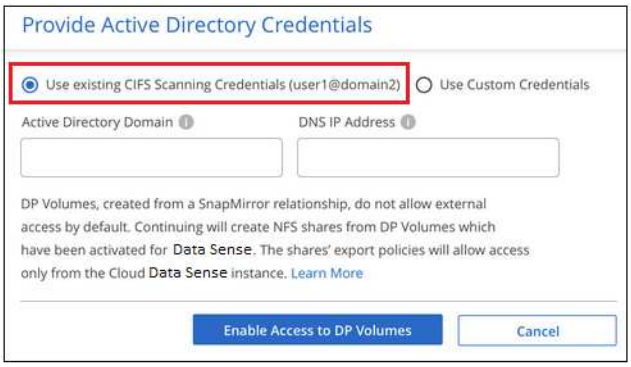
기본적으로 데이터 보호(DP) 볼륨은 외부에서 노출되지 않고 Cloud Data Sense에서 액세스할 수 없기 때문에 스캔되지 않습니다. ONTAP 파일 시스템용 FSx의 SnapMirror 작업을 위한 대상 볼륨입니다.

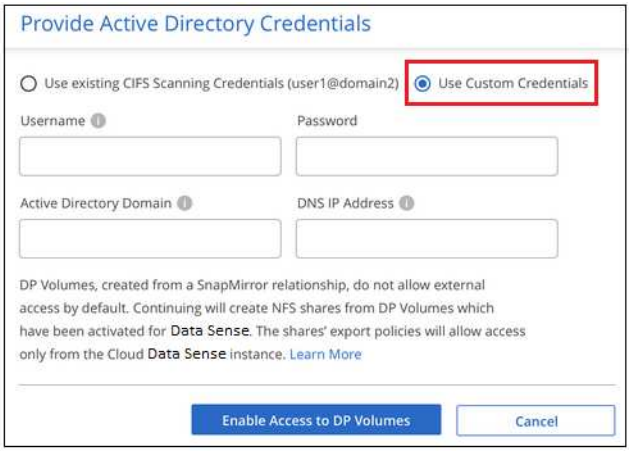
처음에 볼륨 목록은 이러한 볼륨을 *Type** DP*로 식별하며 *Status** Not Scanning* 및 *Required Action** DP 볼륨에 대한 액세스 사용*.



이러한 데이터 보호 볼륨을 스캔하려는 경우:

1. 페이지 맨 위에서 * DP 볼륨에 대한 액세스 활성화 * 를 클릭합니다.
2. 확인 메시지를 검토하고 * DP 볼륨에 대한 액세스 활성화 * 를 다시 클릭합니다.
   - 소스 FSx for ONTAP 파일 시스템에서 처음에 NFS 볼륨으로 생성된 볼륨이 활성화됩니다.
   - 소스 FSx for ONTAP 파일 시스템에서 처음에 CIFS 볼륨으로 생성된 볼륨을 사용하려면 CIFS 자격 증명을 입력하여 해당 DP 볼륨을 스캔해야 합니다. Cloud Data Sense가 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 이미 입력한 경우 해당 자격 증명을 사용하거나 다른 관리자 자격 증명 세트를 지정할 수 있습니다.





3. 스캔할 각 DP 볼륨을 활성화합니다 다른 볼륨을 활성화해도 마찬가지입니다.

활성화되면 Cloud Data Sense는 스캔을 위해 활성화된 각 DP 볼륨에서 NFS 공유를 생성합니다. 공유 내보내기 정책은 데이터 감지 인스턴스에서만 액세스를 허용합니다.

- 참고: * 처음에 DP 볼륨에 대한 액세스를 설정한 후 나중에 추가할 때 CIFS 데이터 보호 볼륨이 없는 경우 구성 페이지 맨 위에 * CIFS DP에 대한 액세스 활성화 * 버튼이 나타납니다. 이 버튼을 클릭하고 CIFS 자격 증명을 추가하여 이러한 CIFS DP 볼륨에 대한 액세스를 설정합니다.

Active Directory 자격 증명은 첫 번째 CIFS DP 볼륨의 스토리지 VM에만 등록되므로 해당 SVM의 모든 DP 볼륨이 검사됩니다. 다른 SVM에 상주하는 볼륨에 Active Directory 자격 증명이 등록되지 않으므로 DP 볼륨이 검색되지 않습니다.

Amazon S3에 대한 Cloud Data Sense 시작하기

Cloud Data Sense는 Amazon S3 버킷을 스캔하여 S3 오브젝트 스토리지에 상주하는 개인적이고 민감한 데이터를 식별할 수 있습니다. Cloud Data Sense는 NetApp 솔루션용으로 만든 버킷에 관계없이 고객의 모든 버킷을 스캔할 수 있습니다.

빠른 시작

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

IAM 역할 준비 및 데이터 센스에서 S3까지 연결 설정을 포함하여 클라우드 환경이 클라우드 데이터 센스에 대한 요구 사항을 충족할 수 있는지 확인합니다. 전체 목록을 참조하십시오.

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

스캔하려는 버킷을 선택하면 Cloud Data Sense에서 스캔을 시작합니다.

S3 사전 요구 사항 검토

다음 요구사항은 S3 버킷 스캔에만 적용됩니다.

Cloud Data Sense 인스턴스에 대해 **IAM** 역할을 설정합니다

Cloud Data Sense는 계정의 S3 버킷에 연결하고 이를 스캔할 수 있는 권한이 필요합니다. 아래에 나열된 권한을 포함하는 IAM 역할을 설정합니다. Amazon S3 작업 환경에서 Data Sense를 활성화하면 Cloud Manager에서 IAM 역할을 선택하라는 메시지가 표시됩니다.

```
{
  "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/*"
          ]
      }
  ]
}
```

Cloud Data Sense에서 **Amazon S3**로 연결할 수 있습니다

클라우드 데이터 센스에 Amazon S3에 대한 연결이 필요합니다. 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 Cloud Data Sense 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 데이터 센스를 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.

Cloud Data Sense 인스턴스 구축

"Cloud Manager에 클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

- 참고: * S3 버킷을 스캔할 때는 현재 사내 위치에 클라우드 데이터 센스를 구축하는 것이 지원되지 않습니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

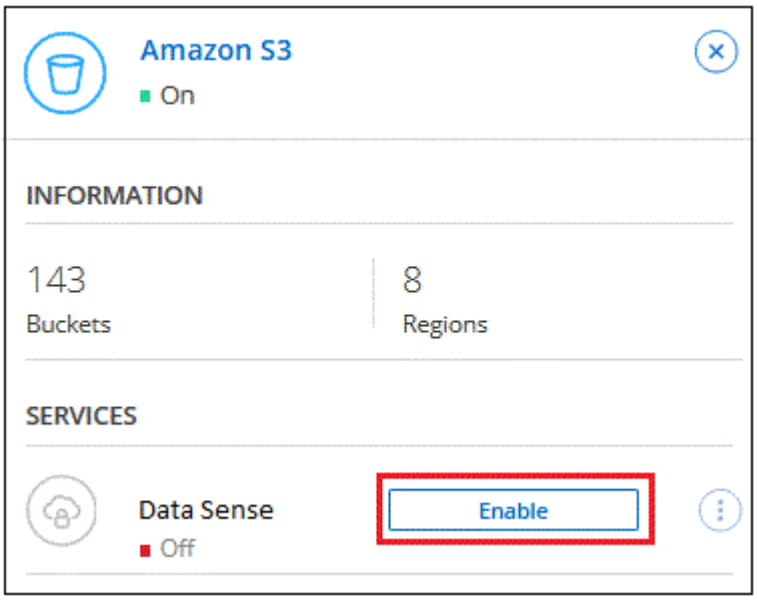
S3 작업 환경에서 데이터 센스를 활성화합니다

사전 요구 사항을 확인한 후 Amazon S3에서 클라우드 데이터 센스를 활성화합니다.

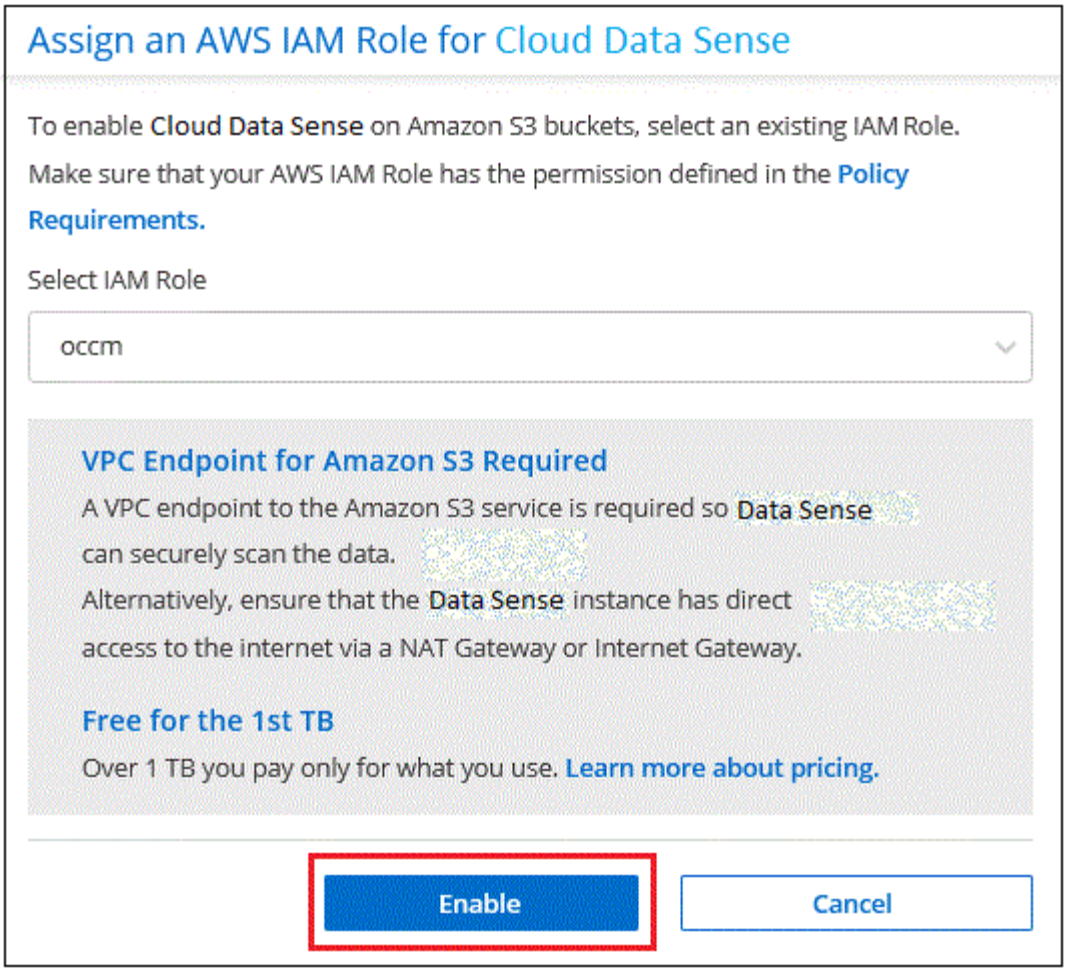
단계

1. Cloud Manager 상단에서 * Canvas * 를 클릭합니다.
2. Amazon S3 작업 환경을 선택합니다.

3. 오른쪽의 데이터 감지 창에서 * 활성화 * 를 클릭합니다.



4. 메시지가 표시되면 가 있는 Cloud Data Sense 인스턴스에 IAM 역할을 할당합니다 필요한 권한.



5. 사용 * 을 클릭합니다.

를 클릭하여 구성 페이지에서 작업 환경에 대한 규정 준수 검사를 활성화할 수도 있습니다 버튼을 클릭하고 * 데이터 감지 활성화 * 를 선택합니다.

Cloud Manager는 IAM 역할을 인스턴스에 할당합니다.

S3 버킷에서 규정 준수 스캔 활성화 및 비활성화

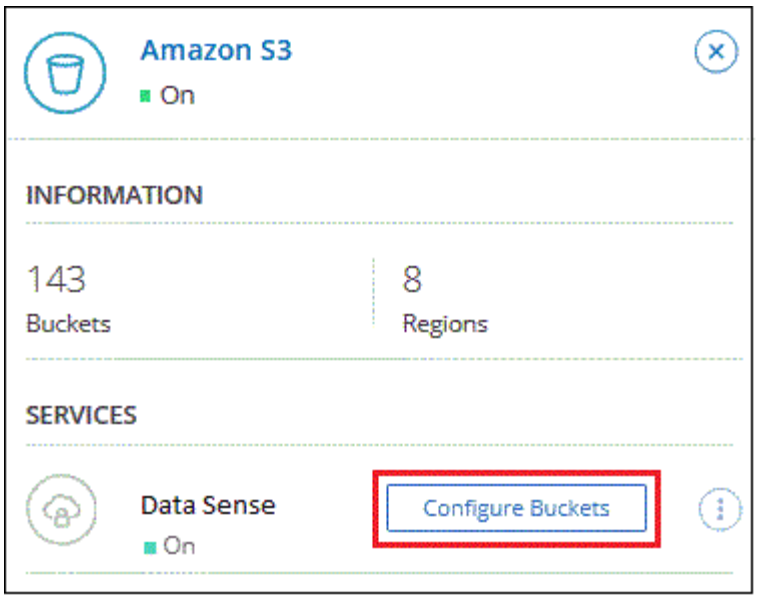
Cloud Manager를 사용하여 Amazon S3에서 Cloud Data Sense를 사용하도록 설정한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다.

Cloud Manager가 검사할 S3 버킷이 있는 AWS 계정에서 실행 중인 경우 해당 버킷을 검색하고 Amazon S3 작업 환경에 표시합니다.

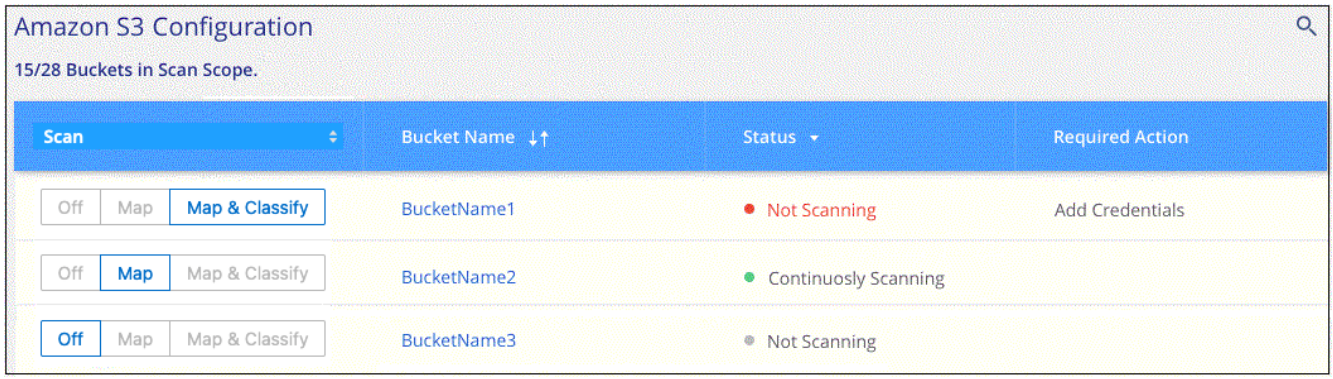
클라우드 데이터 센스도 가능합니다 서로 다른 AWS 계정에 있는 S3 버킷을 스캔합니다.

단계

1. Amazon S3 작업 환경을 선택합니다.
2. 오른쪽 창에서 * 버킷 구성 * 을 클릭합니다.



3. 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

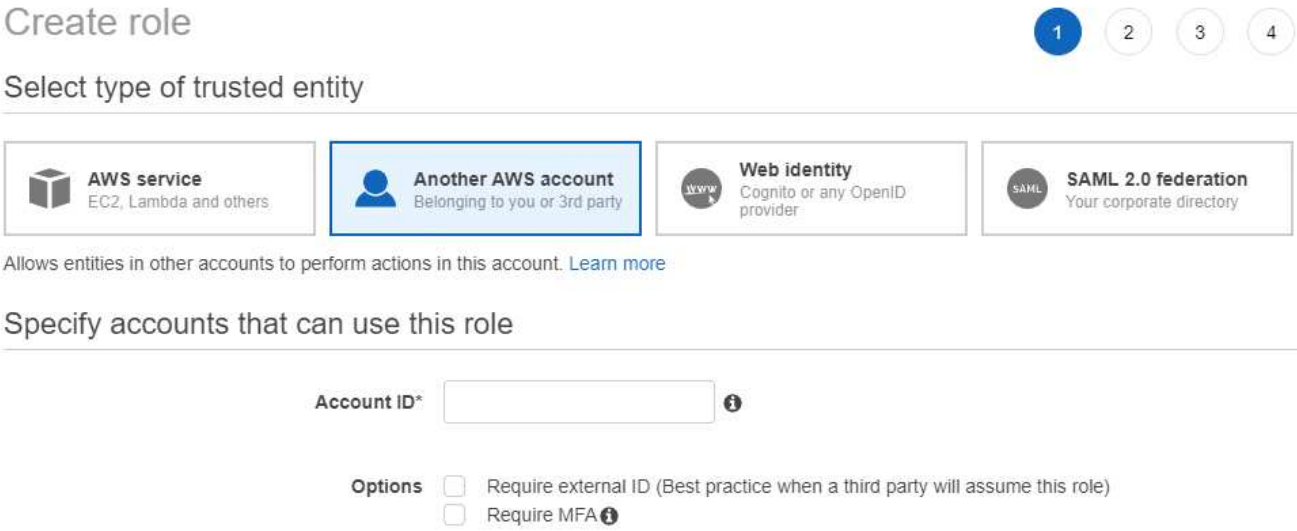
Cloud Data Sense는 활성화한 S3 버킷을 검색하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

추가 AWS 계정에서 버킷 스캔

기존 Cloud Data Sense 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.



다음을 수행하십시오.

- Cloud Data Sense 인스턴스가 있는 계정의 ID를 입력합니다.
- 최대 CLI/API 세션 지속 시간 * 을 1시간에서 12시간으로 변경하고 변경 사항을 저장합니다.
- Cloud Data Sense IAM 정책을 연결합니다. 필요한 권한이 있는지 확인합니다.

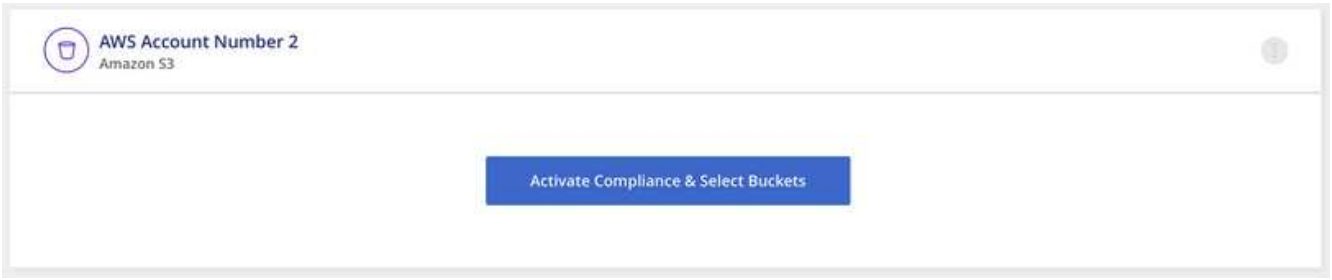
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Data Sense 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 Cloud Data Sense 인스턴스 프로필 계정이 추가 AWS 계정에 액세스할 수 있습니다.

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



4. Activate Data Sense & Select Bucket * 을 클릭하고 스캔할 버킷을 선택합니다.

Cloud Data Sense는 사용자가 활성화한 새로운 S3 버킷을 스캔하기 시작합니다.

데이터베이스 스키마를 검색하는 중입니다

클라우드 데이터 센스를 사용하여 데이터베이스 스키마 스캔을 시작하려면 몇 단계를 완료하십시오.

빠른 시작

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

데이터베이스가 지원되고 데이터베이스에 연결하는 데 필요한 정보가 있는지 확인합니다.

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

액세스할 데이터베이스 서버를 추가합니다.

스캔할 스키마를 선택합니다.

사전 요구 사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

지원되는 데이터베이스

Cloud Data Sense는 다음 데이터베이스에서 스키마를 검색할 수 있습니다.

- Amazon Relational Database Service(Amazon RDS)
- MongoDB
- MySQL
- 오라클
- PostgreSQL
- SAP HANA를 참조하십시오
- SQL Server(MSSQL)

데이터베이스에서 통계 수집 기능 * 을 활성화해야 합니다.

데이터베이스 요구 사항

Cloud Data Sense 인스턴스에 연결된 모든 데이터베이스는 호스팅 위치에 관계없이 검색할 수 있습니다. 데이터베이스에 연결하려면 다음 정보만 필요합니다.

- IP 주소 또는 호스트 이름입니다
- 포트
- 서비스 이름(Oracle 데이터베이스 액세스에만 해당)
- 스키마에 대한 읽기 액세스를 허용하는 자격 증명

  사용자 이름과 암호를 선택할 때는 검사할 모든 스키마와 테이블에 대한 읽기 권한이 있는 스키마를 선택해야 합니다. 필요한 모든 권한을 사용하여 Cloud Data Sense 시스템의 전용 사용자를 생성하는 것이 좋습니다.

- 참고: * MongoDB의 경우 읽기 전용 관리자 역할이 필요합니다.

Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 데이터베이스 스키마를 스캔하는 경우 를 사용할 수 있습니다 "클라우드 데이터 센스를 클라우드에 배포합니다" 또는 "인터넷에 액세스할 수 있는 온프레미스 위치에 데이터 센스를 배포하십시오".

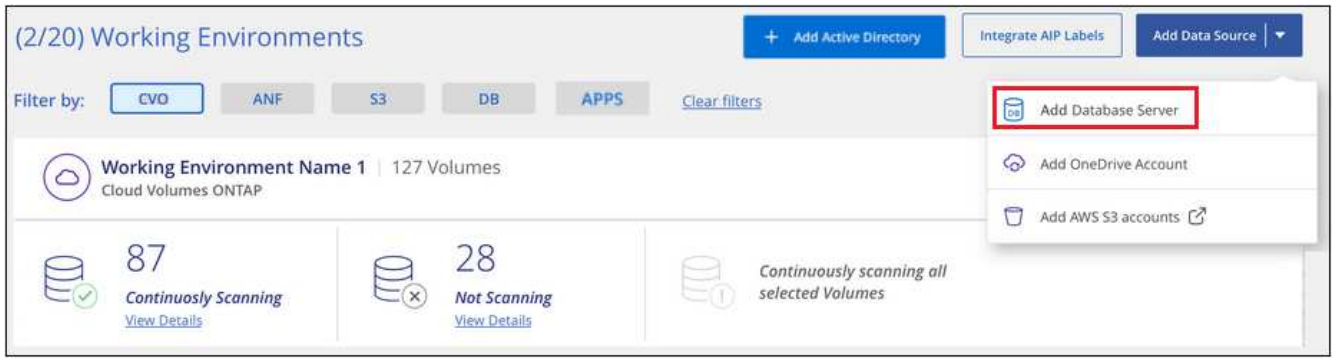
인터넷에 액세스할 수 없는 어두운 사이트에 설치된 데이터베이스 스키마를 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

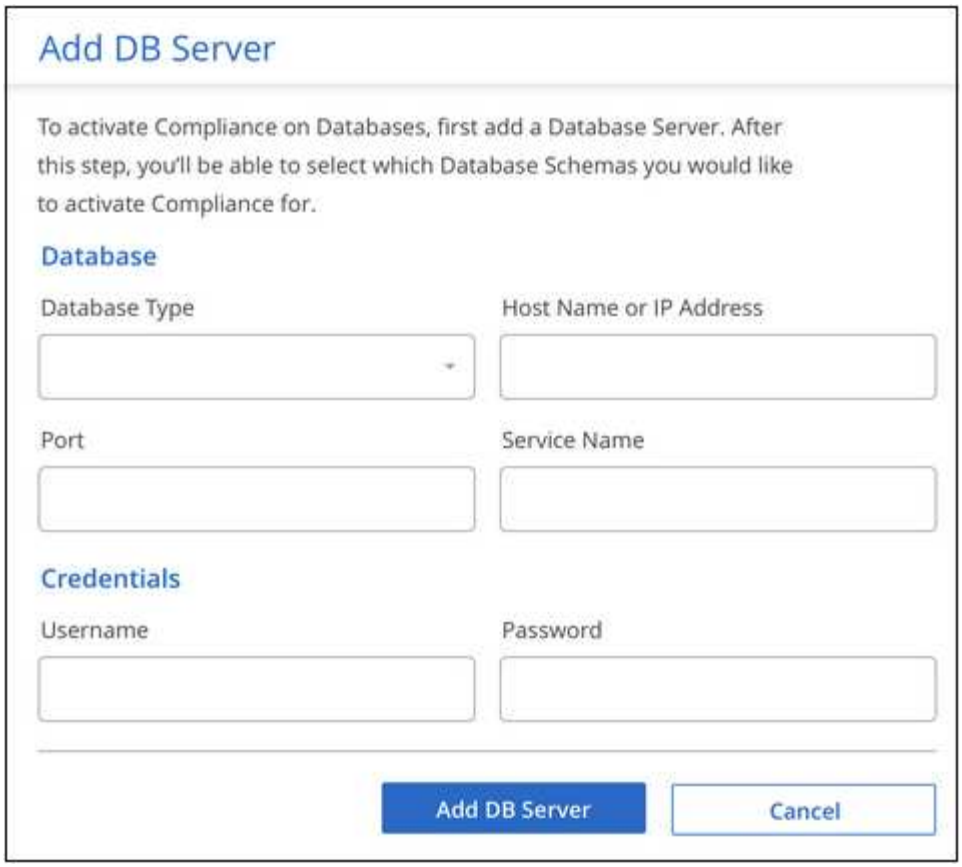
데이터베이스 서버 추가

스키마가 있는 데이터베이스 서버를 추가합니다.

1. 작업 환경 구성 페이지에서 * 데이터 소스 추가 * > * 데이터베이스 서버 추가 * 를 클릭합니다.



2. 필요한 정보를 입력하여 데이터베이스 서버를 식별합니다.
   a. 데이터베이스 유형을 선택합니다.
   b. 데이터베이스에 연결할 포트와 호스트 이름 또는 IP 주소를 입력합니다.
   c. Oracle 데이터베이스의 경우 서비스 이름을 입력합니다.
   d. 클라우드 데이터 센스에서 서버에 액세스할 수 있도록 자격 증명을 입력합니다.
   e. DB 서버 추가 * 를 클릭합니다.



데이터베이스가 작업 환경 목록에 추가됩니다.

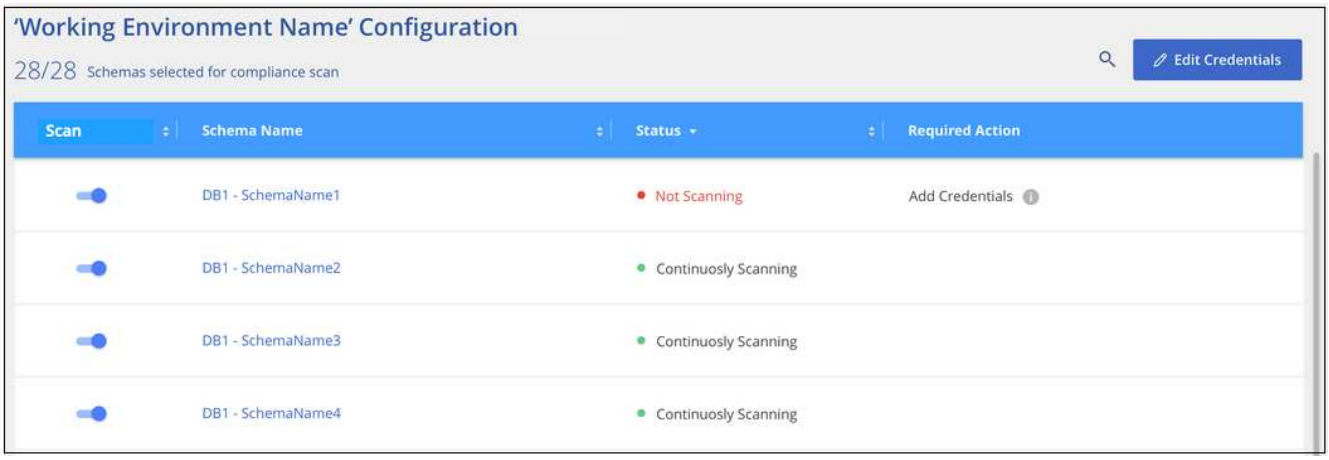
데이터베이스 스키마에서 규정 준수 검사를 활성화 및 비활성화합니다

언제든지 스키마를 중지하거나 전체 스캔을 시작할 수 있습니다.

데이터베이스 스키마에 대한 매핑 전용 검사를 선택하는 옵션은 없습니다.

1. Configuration_ 페이지에서 구성할 데이터베이스의 * Configuration * 버튼을 클릭합니다.

2. 슬라이더를 오른쪽으로 이동하여 스캔할 스키마를 선택합니다.



클라우드 데이터 센스가 활성화한 데이터베이스 스키마를 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

OneDrive 계정 스캔 중

Cloud Data Sense를 사용하여 사용자의 OneDrive 폴더에 있는 파일을 스캔하려면 몇 단계를 완료하십시오.

빠른 시작

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

OneDrive 계정에 로그인할 수 있는 관리자 자격 증명이 있는지 확인합니다.

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

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

OneDrive 요구 사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 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.

Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

데이터 센스 가능 "클라우드에 구축" 또는 "인터넷 액세스가 가능한 사내 위치".

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

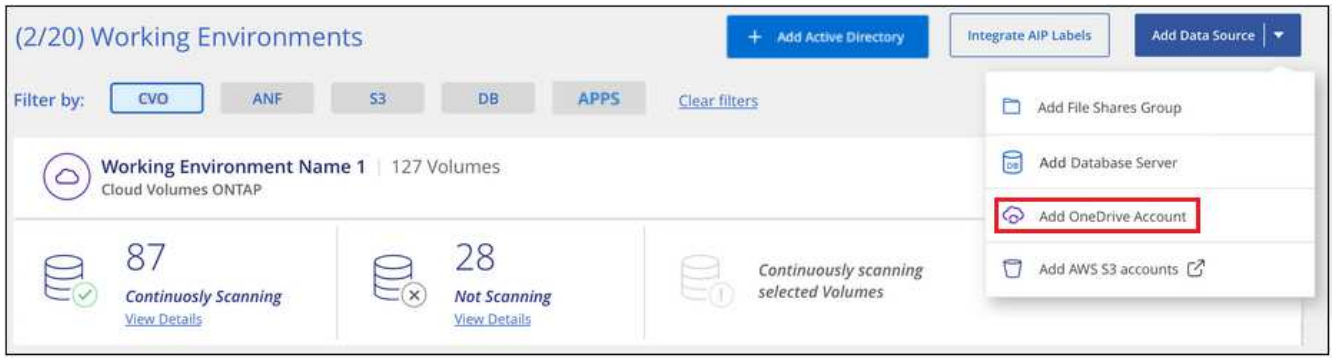
데이터 센스도 가능합니다 "인터넷에 액세스할 수 없는 온프레미스 위치에 배포되었습니다". 하지만 로컬 OneDrive 파일을 검색하려면 몇 개의 선택 끝점에 인터넷 액세스를 제공해야 합니다. "필요한 엔드포인트 목록은 여기 를 참조하십시오".

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. Microsoft 페이지가 나타나면 OneDrive 계정을 선택하고 필요한 관리자 사용자 및 암호를 입력한 다음 * 수락 * 을 클릭하여 Cloud Data Sense가 이 계정에서 데이터를 읽을 수 있도록 합니다.

OneDrive 계정이 작업 환경 목록에 추가됩니다.

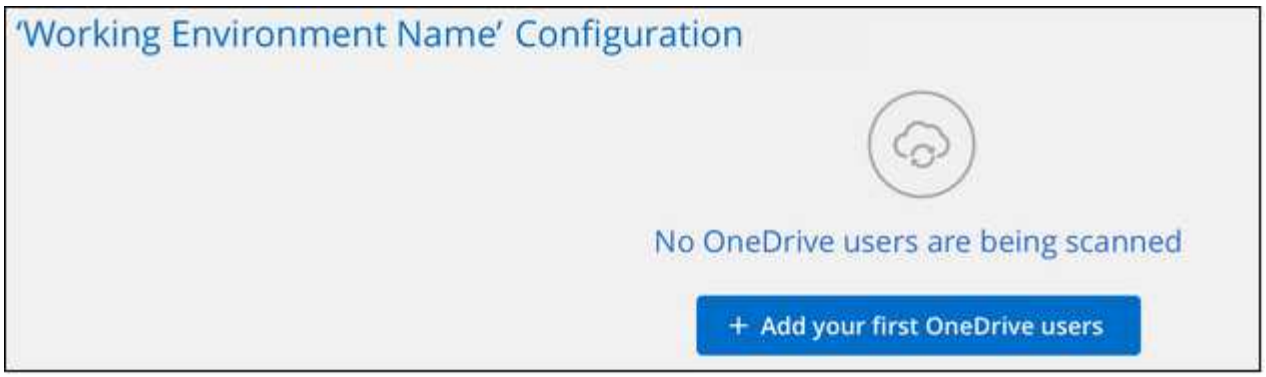
규정 준수 검사에 OneDrive 사용자 추가

개별 OneDrive 사용자 또는 모든 OneDrive 사용자를 추가하여 Cloud Data Sense에서 파일을 검색할 수 있습니다.

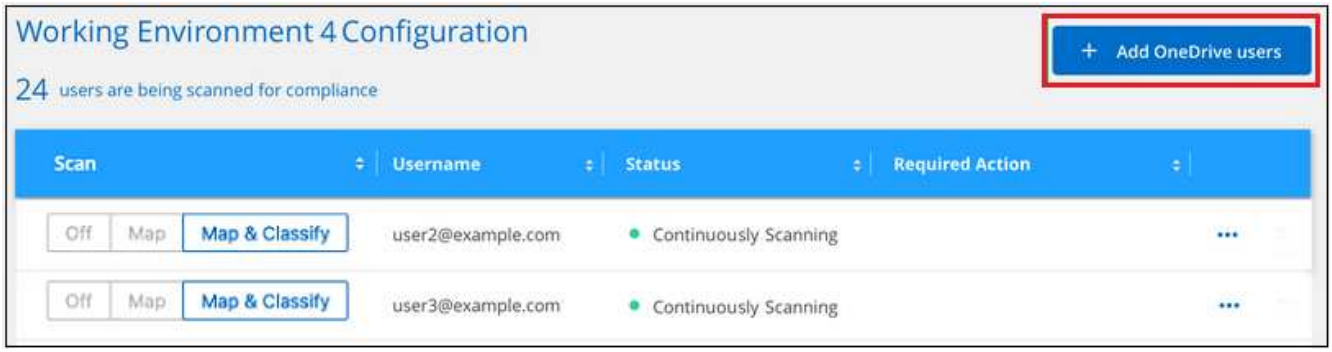
단계

1. Configuration_ 페이지에서 OneDrive 계정의 * Configuration * 버튼을 클릭합니다.

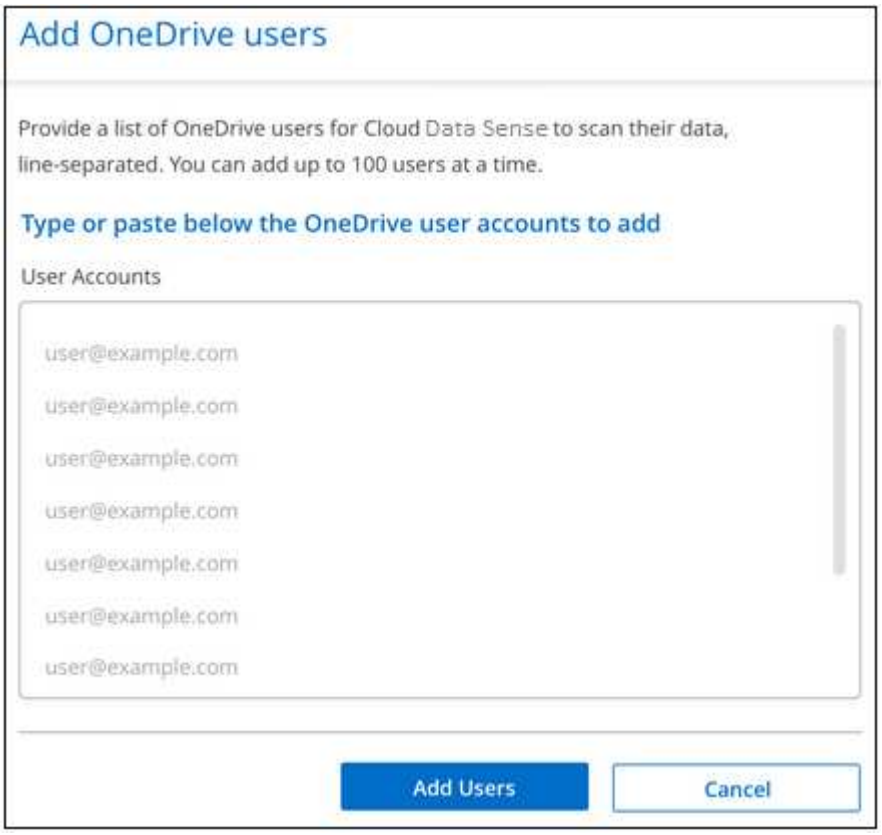
2. 이 OneDrive 계정에 사용자를 처음으로 추가하는 경우 * 첫 번째 OneDrive 사용자 추가 * 를 클릭합니다.



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.

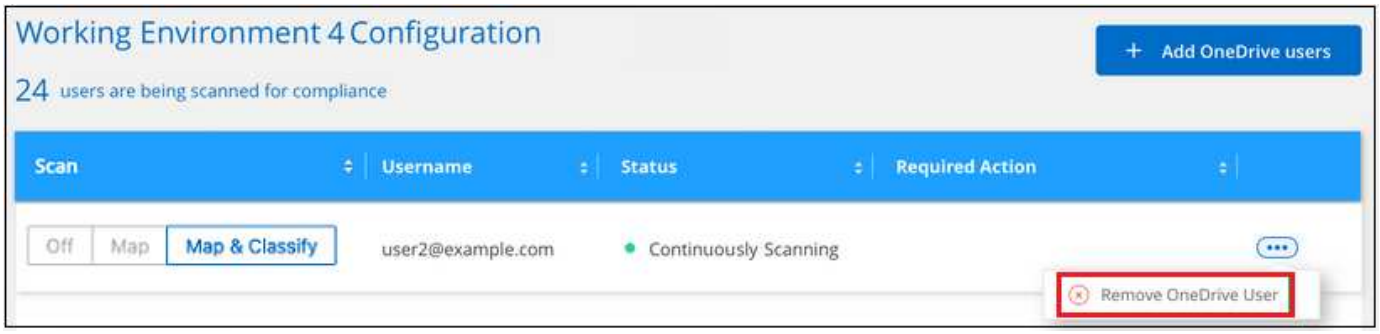
4. 사용자 파일에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 활성화합니다.

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

Cloud Data Sense는 추가한 사용자의 파일 스캔을 시작하고, 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.



참고: 이 작업은 수행할 수 있습니다 "데이터 센스에서 전체 OneDrive 계정을 삭제합니다" 더 이상 OneDrive 계정에서 사용자 데이터를 스캔하지 않으려는 경우

SharePoint 계정 스캔 중

Cloud Data Sense를 사용하여 SharePoint 계정의 파일 스캔을 시작하려면 몇 단계를 완료하십시오.

빠른 시작

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

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

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

SharePoint 계정에서 검색할 SharePoint 사이트 URL 목록을 추가하고 검색 유형을 선택합니다. 한 번에 최대 100개의 URL을 추가할 수 있습니다.

SharePoint 요구 사항 검토

다음 필수 구성 요소를 검토하여 SharePoint 계정에서 Cloud Data Sense를 활성화할 준비가 되었는지 확인합니다.

- 모든 SharePoint 사이트에 읽기 권한을 제공하는 SharePoint 계정에 대한 관리자 로그인 자격 증명이 있어야 합니다.
- 검색할 모든 데이터에 대해 SharePoint 사이트 URL의 줄 구분 목록이 필요합니다.

Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

데이터 센스 가능 "클라우드에 구축" 또는 "인터넷 액세스가 가능한 사내 위치".

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

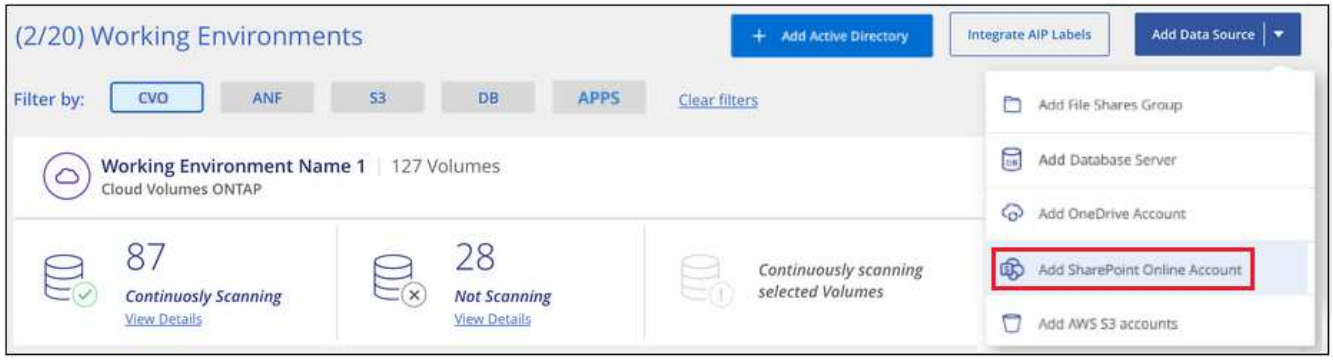
데이터 센스도 가능합니다 "인터넷에 액세스할 수 없는 온프레미스 위치에 배포되었습니다". 그러나 로컬 SharePoint 파일을 검색하려면 몇 개의 선택 끝점에 인터넷 액세스를 제공해야 합니다. "필요한 엔드포인트 목록은 여기 를 참조하십시오".

SharePoint 계정을 추가하는 중입니다

사용자 파일이 있는 SharePoint 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 필요한 관리자 사용자 및 암호를 입력한 다음 * 수락 * 을 클릭하여 Cloud Data Sense가 이 계정에서 데이터를 읽을 수 있도록 합니다.

SharePoint 계정이 작업 환경 목록에 추가됩니다.

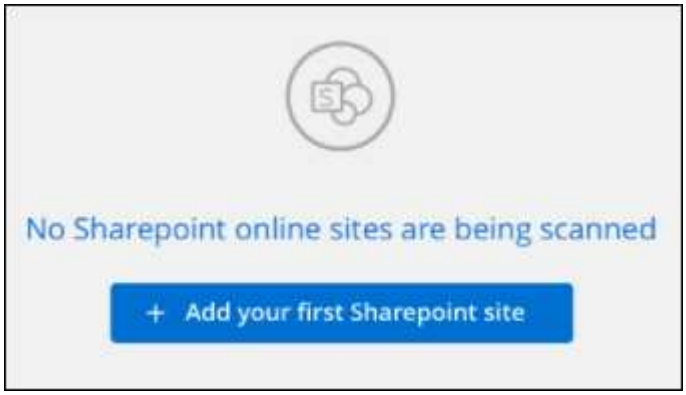
규정 준수 검사에 SharePoint 사이트 추가

Cloud Data Sense에서 연결된 파일을 검사하도록 개별 SharePoint 사이트 또는 계정의 모든 SharePoint 사이트를 추가할 수 있습니다.

단계

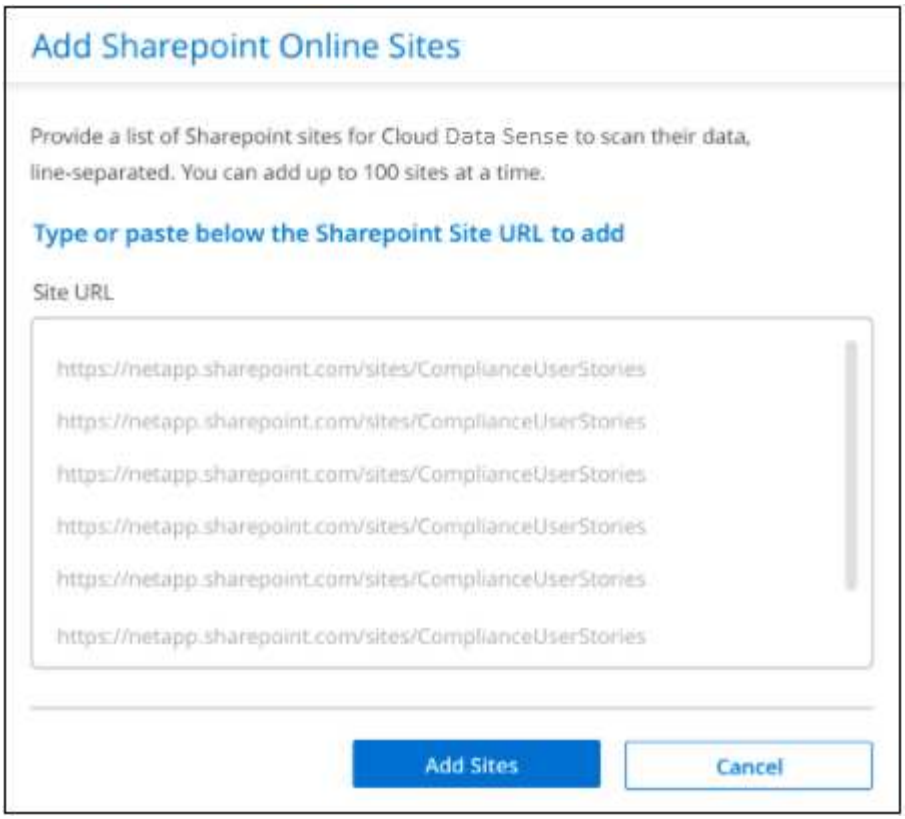
1. Configuration_ 페이지에서 SharePoint 계정의 * Configuration * 버튼을 클릭합니다.

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.

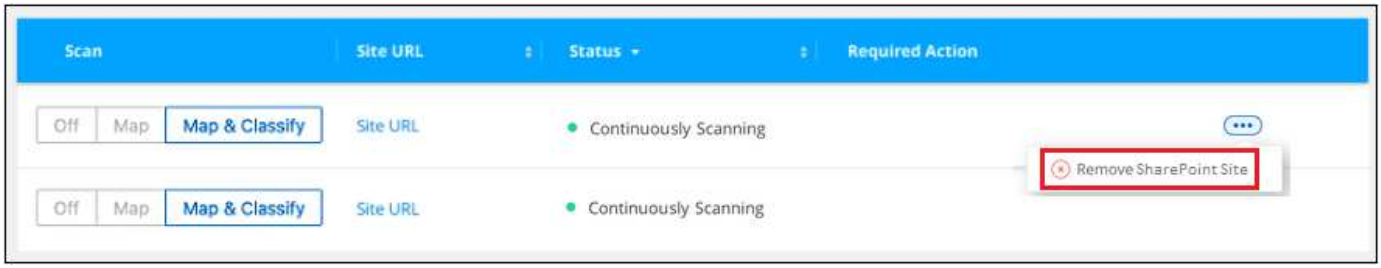
4. SharePoint 사이트의 파일에서 매핑 전용 스캔 또는 매핑 및 분류 검사를 사용하도록 설정합니다.

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

Cloud Data Sense는 추가한 SharePoint 사이트의 파일을 스캔하기 시작하며, 그 결과는 대시보드와 다른 위치에 표시됩니다.

규정 준수 검사에서 **SharePoint** 사이트 제거

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.



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

Google Drive 계정을 검색하는 중입니다

Cloud Data Sense를 사용하여 Google Drive 계정의 사용자 파일 스캔을 시작하려면 몇 단계를 완료하십시오.

빠른 시작

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

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

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

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

Google Drive 요구 사항 검토

다음 전제 조건을 검토하여 Google Drive 계정에서 Cloud Data Sense를 활성화할 준비가 되었는지 확인합니다.

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

현재 제한 사항

다음 데이터 감지 기능은 현재 Google Drive 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.

클라우드 데이터 센스를 구축하는 중입니다

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

데이터 센스 가능 "클라우드에 구축" 또는 "인터넷 액세스가 가능한 사내 위치".

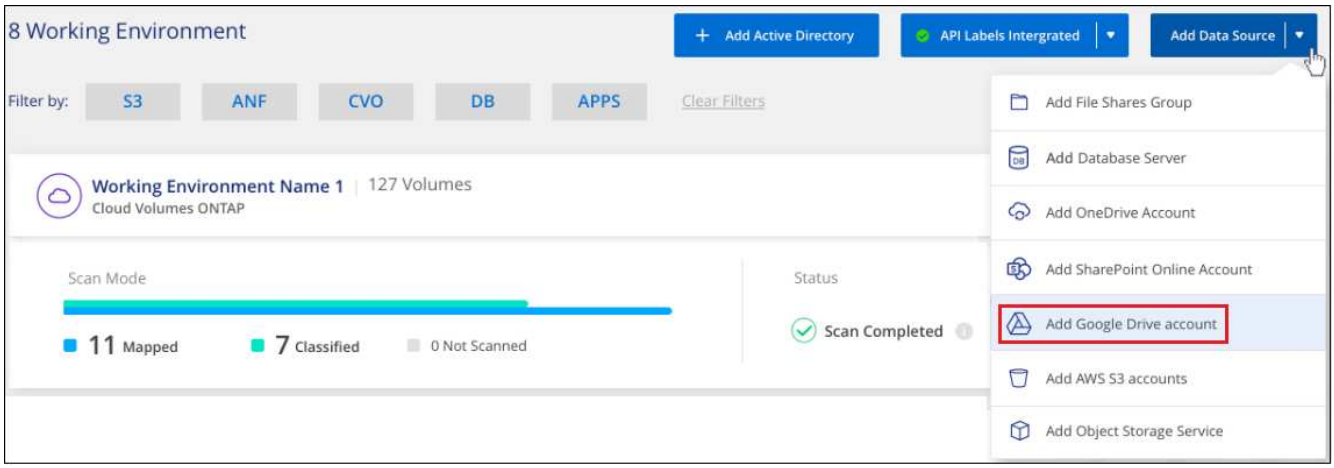
데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

Google Drive 계정을 추가하는 중입니다

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 * 수락 * 을 클릭하여 Cloud Data Sense가 이 계정에서 데이터를 읽을 수 있도록 합니다.

Google Drive 계정이 작업 환경 목록에 추가됩니다.

사용자 데이터에 대한 스캔 유형을 선택합니다

사용자 데이터에 대해 Cloud Data Sense가 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

Cloud Data Sense는 추가한 Google Drive 계정의 파일 스캔을 시작하고, 결과는 대시보드와 다른 위치에 표시됩니다.

규정 준수 검사에서 **Google Drive** 계정을 제거하는 중입니다

단일 사용자의 Google Drive 파일만 단일 Google Drive 계정의 일부이므로, 사용자의 Google Drive 계정에서 파일 검색을 중지하려면 다음을 수행해야 합니다 "데이터 센스에서 Google Drive 계정을 삭제합니다".

파일 공유를 검색하는 중입니다

Cloud Data Sense를 사용하여 NetApp이 아닌 NFS 또는 CIFS 파일 공유 스캔을 시작하려면 몇 가지 단계를 완료하십시오. 이러한 파일 공유는 사내 또는 클라우드에 상주할 수 있습니다.

빠른 시작

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

CIFS(SMB) 공유의 경우 공유를 액세스할 수 있는 자격 증명이 있는지 확인합니다.

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

그룹은 검사할 파일 공유의 컨테이너이며 해당 파일 공유의 작업 환경 이름으로 사용됩니다.

스캔할 파일 공유 목록을 추가하고 스캔 유형을 선택합니다. 한 번에 최대 100개의 파일 공유를 추가할 수 있습니다.

파일 공유 요구 사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

- 공유는 클라우드 또는 온프레미스 등 어디서나 호스팅할 수 있습니다. 이는 타사 스토리지 시스템에 상주하는 파일 공유입니다.
- Data Sense 인스턴스와 공유 사이에 네트워크 연결이 있어야 합니다.
- 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- '<host_name>:/<share_path>' 형식으로 추가하려는 공유 목록이 필요합니다. 공유를 개별적으로 입력하거나 스캔하려는 파일 공유의 라인 분리 목록을 제공할 수 있습니다.
- CIFS(SMB) 공유의 경우 공유에 대한 읽기 액세스를 제공하는 Active Directory 자격 증명이 있는지 확인합니다. Cloud Data Sense에서 상승된 권한이 필요한 데이터를 검색해야 하는 경우 관리자 자격 증명이 선호됩니다.

Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 비NetApp NFS 또는 CIFS 파일 공유를 스캔하는 경우 다음을 수행할 수 있습니다 "클라우드 데이터 센스를 클라우드에 배포합니다" 또는 "인터넷에 액세스할 수 있는 온프레미스 위치에 데이터 센스를 배포하십시오".

인터넷에 액세스할 수 없는 어두운 사이트에 설치된 비 NetApp NFS 또는 CIFS 파일 공유를 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

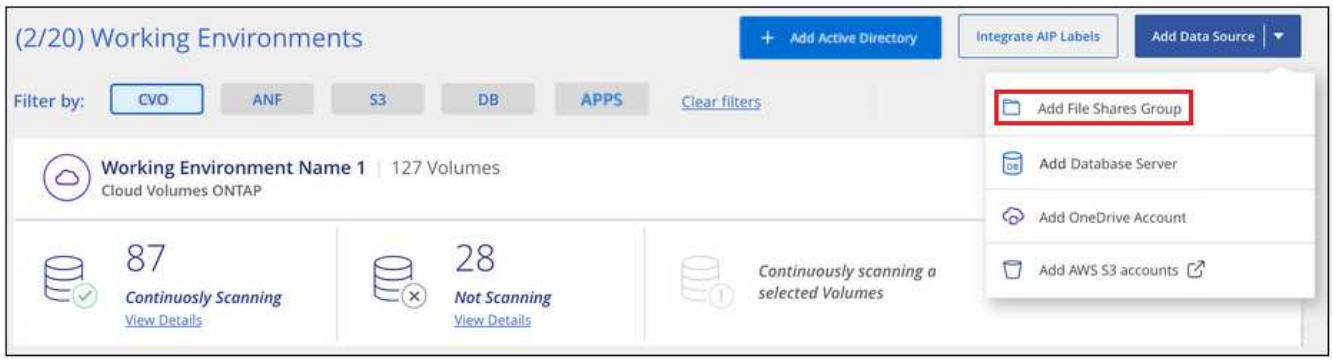
파일 공유에 대한 그룹을 생성하는 중입니다

파일 공유를 추가하려면 먼저 파일 공유 "그룹"을 추가해야 합니다. 그룹은 검색할 파일 공유의 컨테이너이며 그룹 이름은 해당 파일 공유의 작업 환경 이름으로 사용됩니다.

동일한 그룹에서 NFS 및 CIFS 공유를 혼합할 수 있지만, 그룹의 모든 CIFS 파일 공유는 동일한 Active Directory 자격 증명을 사용해야 합니다. 다른 자격 증명을 사용하는 CIFS 공유를 추가하려는 경우 고유한 각 자격 증명 세트에 대해 별도의 그룹을 만들어야 합니다.

단계

1. 작업 환경 구성 페이지에서 * 데이터 소스 추가 * > * 파일 공유 그룹 추가 * 를 클릭합니다.



2. 파일 공유 그룹 추가 대화 상자에서 공유 그룹의 이름을 입력하고 * 계속 * 을 클릭합니다.

새 파일 공유 그룹이 작업 환경 목록에 추가됩니다.

그룹에 파일 공유를 추가하는 중입니다

파일 공유를 파일 공유 그룹에 추가하면 해당 공유의 파일이 Cloud Data Sense에 의해 스캔됩니다. '<host_name>:/<share_path>' 형식으로 공유를 추가합니다.

개별 파일 공유를 추가하거나 스캔할 파일 공유의 줄별 목록을 제공할 수 있습니다. 한 번에 최대 100개의 공유를 추가할 수 있습니다.

단일 그룹에 NFS 및 CIFS 공유를 모두 추가하는 경우 NFS 공유를 한 번 추가한 다음 CIFS 공유를 다시 추가하는 프로세스를 실행해야 합니다.

단계

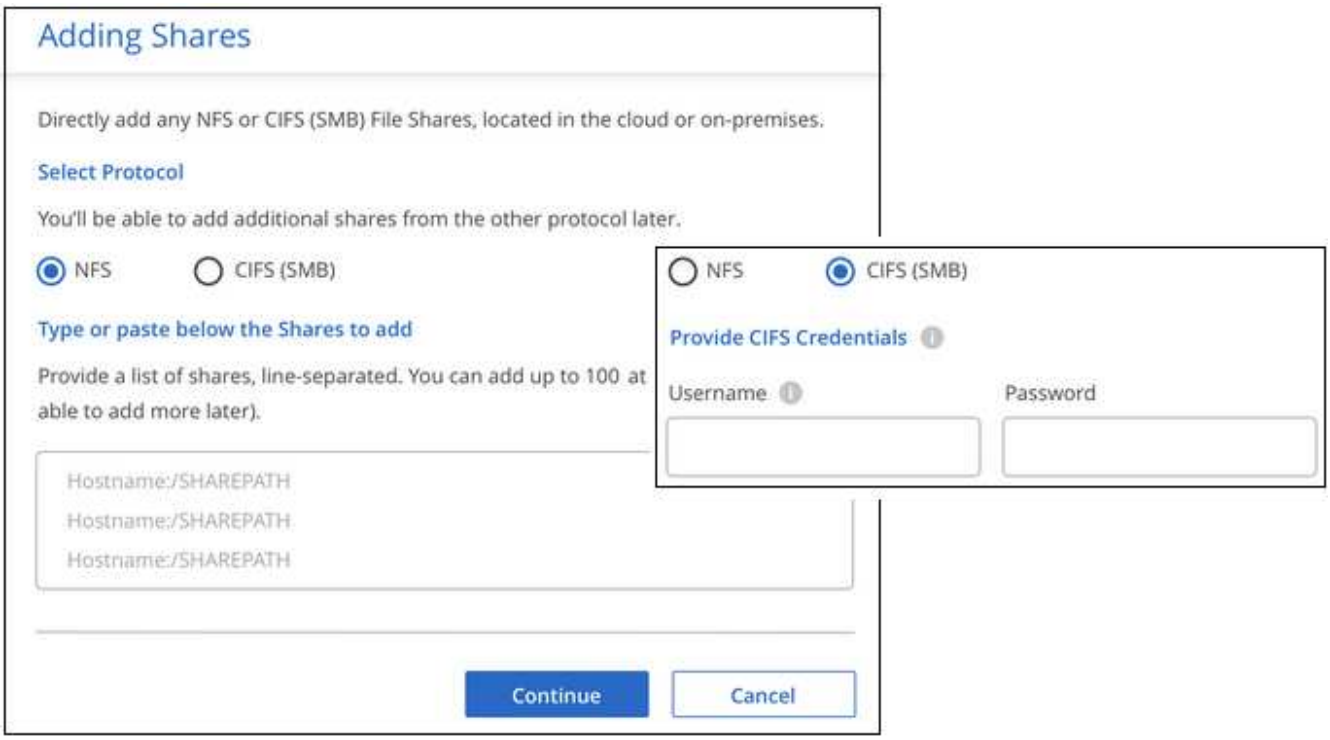
1. 작업 환경 페이지에서 파일 공유 그룹에 대한 * 구성 * 버튼을 클릭합니다.

2. 이 파일 공유 그룹에 대한 파일 공유를 처음으로 추가하는 경우 * 첫 번째 공유 추가 * 를 클릭합니다.

기존 그룹에 파일 공유를 추가하는 경우 * 공유 추가 * 를 클릭합니다.

3. 추가할 파일 공유의 프로토콜을 선택하고, 스캔하려는 파일 공유를 한 줄에 하나씩 추가하고, * 계속 * 을 클릭합니다.

CIFS(SMB) 공유를 추가할 때는 공유에 대한 읽기 액세스를 제공하는 Active Directory 자격 증명을 입력해야 합니다. 관리자 자격 증명을 사용하는 것이 좋습니다.



확인 대화 상자에 추가된 공유 수가 표시됩니다.

대화 상자에 추가할 수 없는 공유가 나열된 경우 이 정보를 캡처하여 문제를 해결할 수 있습니다. 경우에 따라 수정된 호스트 이름 또는 공유 이름으로 공유를 다시 추가할 수 있습니다.

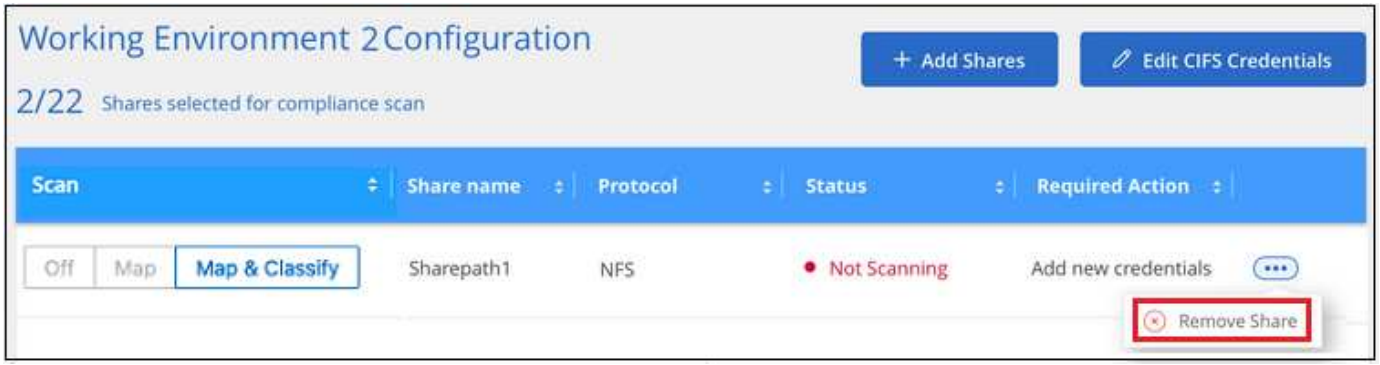
4. 각 파일 공유에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 활성화합니다.

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

Cloud Data Sense는 추가한 파일 공유의 파일 스캔을 시작하고 그 결과는 대시보드와 다른 위치에 표시됩니다.

규정 준수 검사에서 파일 공유를 제거합니다

특정 파일 공유를 더 이상 스캔할 필요가 없는 경우 언제든지 개별 파일 공유를 제거하여 파일을 검색할 수 있습니다. 구성 페이지에서 * 공유 제거 * 를 클릭하기만 하면 됩니다.



S3 프로토콜을 사용하는 오브젝트 스토리지 스캔

Cloud Data Sense를 사용하여 오브젝트 스토리지 내에서 직접 데이터 스캔을 시작하려면 몇 가지 단계를 완료하십시오. Data Sense는 S3(Simple Storage Service) 프로토콜을 사용하는 오브젝트 스토리지 서비스에서 데이터를 스캔할 수 있습니다. 여기에는 NetApp StorageGRID, IBM Cloud Object Store, Azure Blob(MinIO 사용), Linode, B2 클라우드 스토리지, Amazon S3 등이 포함됩니다.

빠른 시작

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

객체 스토리지 서비스에 연결하려면 엔드포인트 URL이 있어야 합니다.

Cloud Data Sense가 버킷에 액세스할 수 있도록 오브젝트 스토리지 공급자로부터 액세스 키 및 비밀 키가 있어야 합니다.

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

클라우드 데이터 센스에 오브젝트 스토리지 서비스를 추가합니다.

스캔하려는 버킷을 선택하면 Cloud Data Sense에서 스캔을 시작합니다.

오브젝트 스토리지의 요구사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

- 객체 스토리지 서비스에 연결하려면 엔드포인트 URL이 있어야 합니다.
- 데이터 센스에서 버킷에 액세스할 수 있도록 오브젝트 스토리지 공급자로부터 액세스 키 및 비밀 키가 있어야 합니다.
- Azure Blob을 지원하려면 을 사용해야 합니다 "MinIO 서비스".

Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 S3 오브젝트 스토리지에서 데이터를 스캔하는 경우 "클라우드 데이터 센스를 클라우드에 배포합니다" 또는 "인터넷에 액세스할 수 있는 온프레미스 위치에 데이터 센스를 배포하십시오".

인터넷에 액세스할 수 없는 어두운 사이트에 설치된 S3 오브젝트 스토리지에서 데이터를 스캔하는 경우, 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

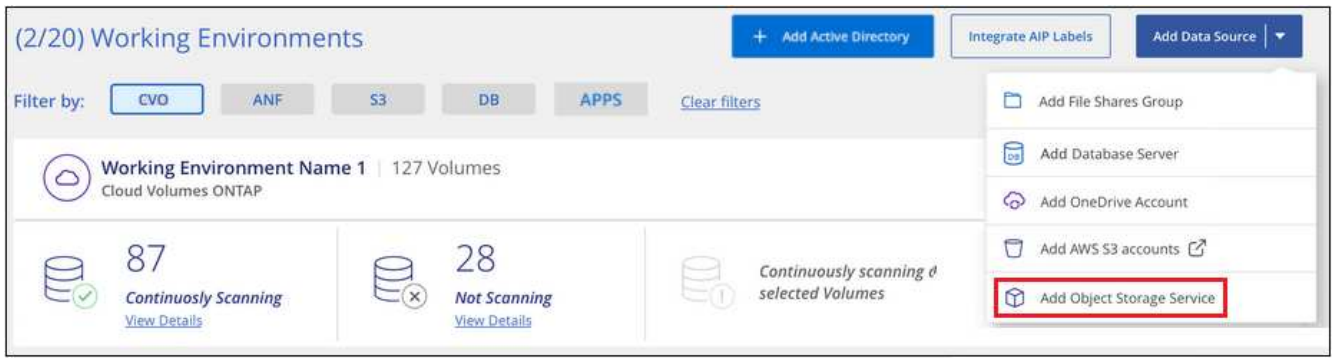
데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

클라우드 데이터 센스에 오브젝트 스토리지 서비스 추가

오브젝트 스토리지 서비스를 추가합니다.

단계

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

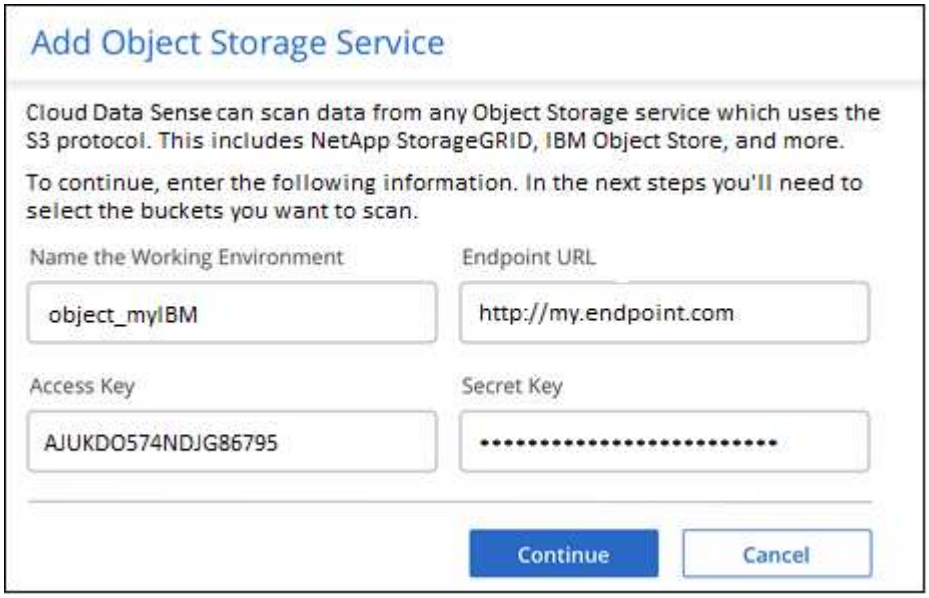


2. 개체 스토리지 서비스 추가 대화 상자에서 개체 스토리지 서비스에 대한 세부 정보를 입력하고 * 계속 * 을 클릭합니다.

   a. 작업 환경에 사용할 이름을 입력합니다. 이 이름은 연결하려는 오브젝트 스토리지 서비스의 이름을 반영해야 합니다.

   b. 객체 스토리지 서비스에 액세스하려면 엔드포인트 URL을 입력하십시오.

   c. 클라우드 데이터 센스에서 오브젝트 스토리지에 있는 버킷에 액세스할 수 있도록 액세스 키와 비밀 키를 입력합니다.



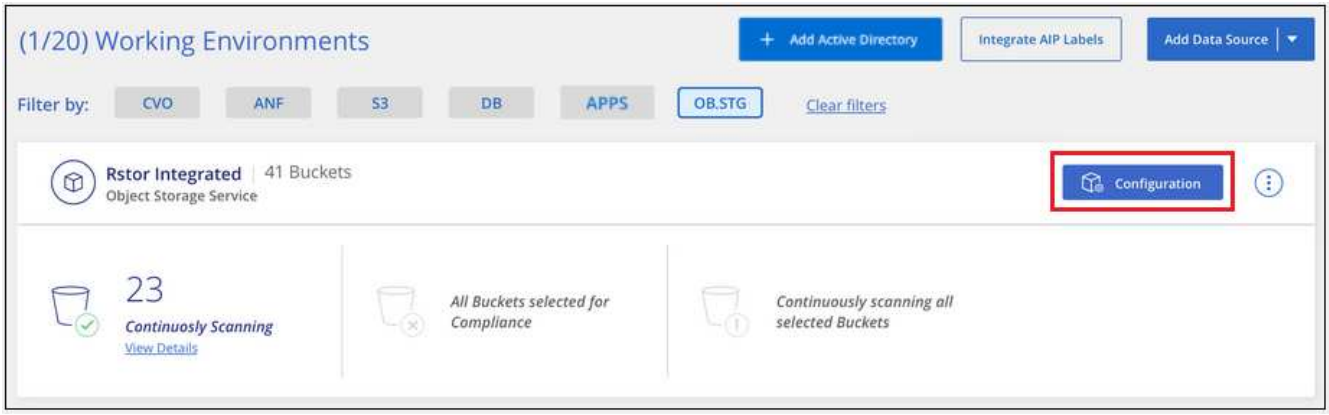
새로운 오브젝트 스토리지 서비스가 작업 환경 목록에 추가됩니다.

오브젝트 스토리지 버킷에 대한 규정 준수 검사 설정 및 해제

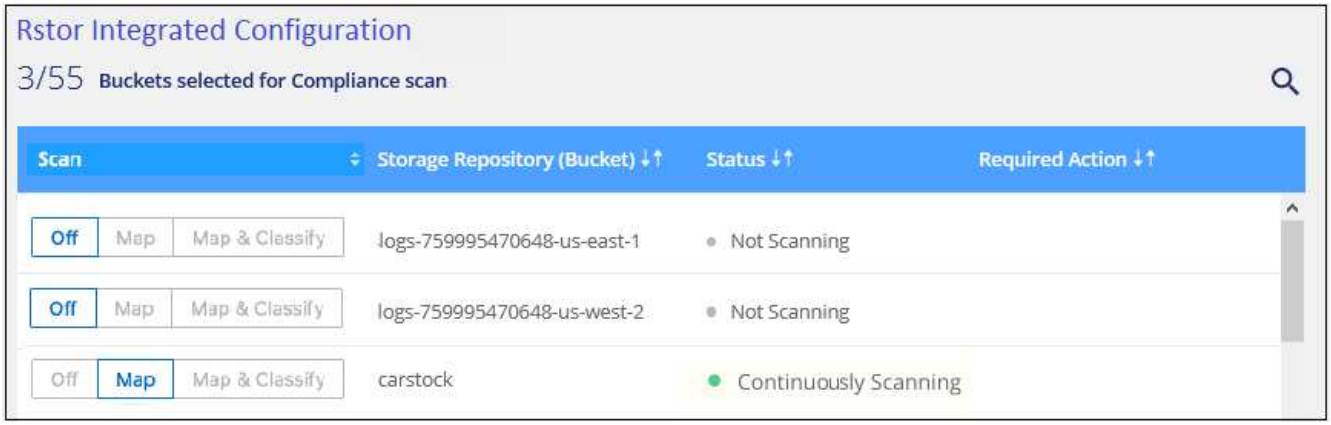
오브젝트 스토리지 서비스에서 클라우드 데이터 센스를 활성화한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다. Data Sense는 이러한 버킷을 검색하여 사용자가 만든 작업 환경에 표시합니다.

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

Cloud Data Sense는 사용자가 활성화한 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.