



클라우드 데이터 센스를 사용하십시오 Cloud Data Sense

NetApp
May 12, 2022

목차

클라우드 데이터 센스를 사용하십시오	1
조직에 저장된 데이터에 대한 거버넌스 세부 정보 보기	1
조직에 저장된 데이터에 대한 규정 준수 세부 정보 보기	5
개인 데이터 구성	15
개인 데이터 관리	31
Data Fusion를 사용하여 개인 데이터 식별자를 추가합니다	42
준수 보고서 보기	45
데이터 주체 액세스 요청에 응답	52
개인 데이터의 범주입니다	54
클라우드 데이터 센스에서 데이터 소스를 제거합니다	60

클라우드 데이터 센스를 사용하십시오

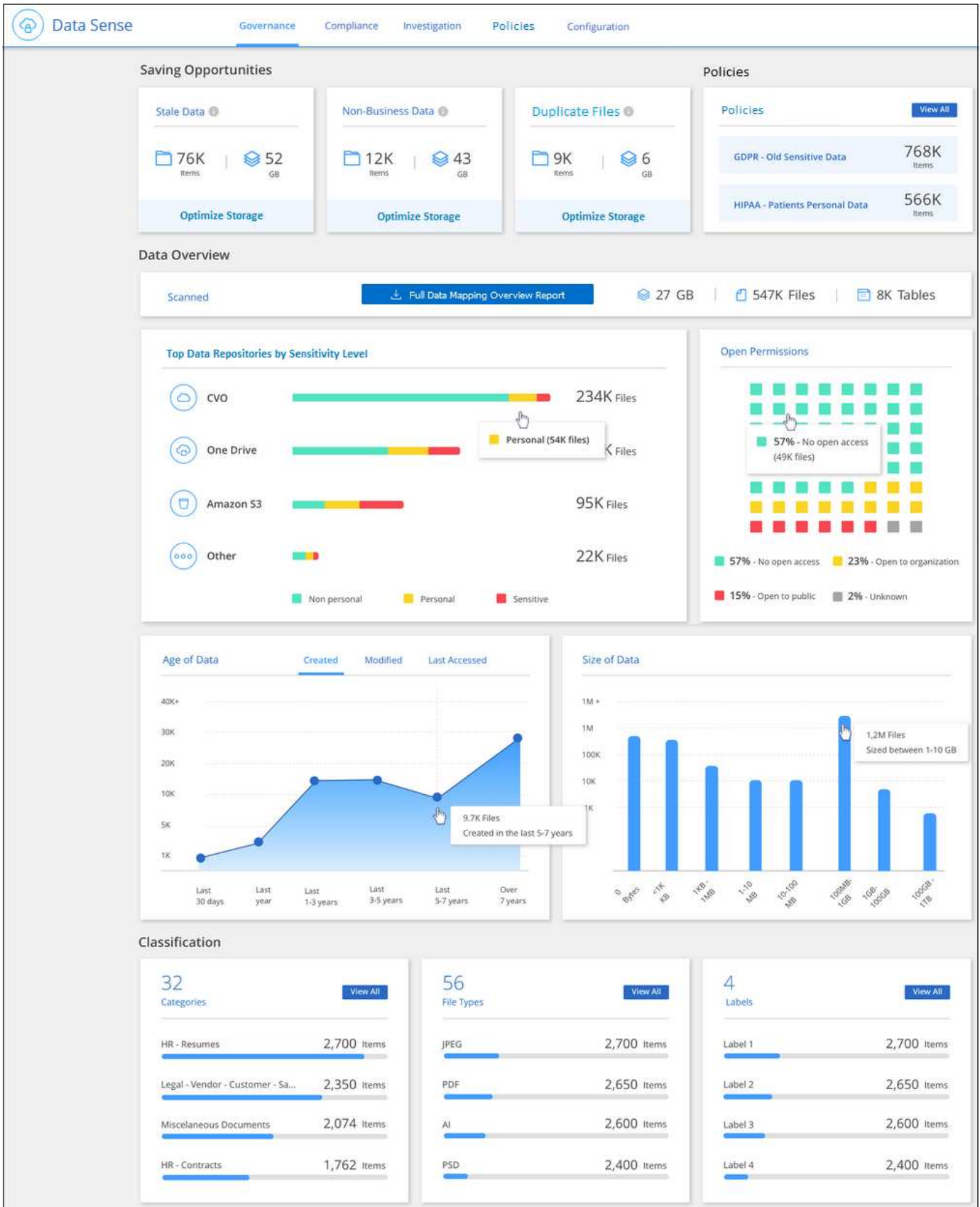
조직에 저장된 데이터에 대한 거버넌스 세부 정보 보기

조직의 스토리지 리소스에 있는 데이터와 관련된 비용을 제어할 수 있습니다. Cloud Data Sense는 오래된 데이터, 비업무용 데이터, 중복 파일 및 시스템의 대용량 파일을 식별하므로 일부 파일을 제거하거나 더 저렴한 오브젝트 스토리지에 계층화할 것인지 결정할 수 있습니다.

또한, 데이터를 사내 위치에서 클라우드로 마이그레이션하려는 경우 데이터의 크기와 데이터를 이동하기 전에 중요한 정보가 포함되어 있는지 여부를 확인할 수 있습니다.

Governance 대시보드

Governance 대시보드는 스토리지 리소스에 저장된 데이터와 관련된 효율성을 높이고 비용을 제어할 수 있는 정보를 제공합니다.



기획 저장

삭제할 데이터가 있는지 또는 더 저렴한 오브젝트 스토리지에 계층화해야 하는지 여부를 확인하려면 *Saving*

Opportunities 영역의 항목을 조사하십시오. 조사 페이지에서 필터링된 결과를 보려면 각 항목을 클릭합니다.

- * 오래된 데이터 * - 3년 전에 마지막으로 수정된 데이터
- * 비 비즈니스 데이터 * - 범주 또는 파일 형식에 따라 업무와 관련이 없는 것으로 간주되는 데이터 여기에는 다음이 포함됩니다.
 - 애플리케이션 데이터
 - 오디오
 - 실행 파일
 - 이미지
 - 로그
 - 비디오
 - 기타(일반 "기타" 범주)
- * 중복 파일 * - 스캔할 데이터 원본의 다른 위치에 중복되는 파일입니다. ["어떤 유형의 중복 파일이 표시되는지 확인합니다"](#).

결과 수가 가장 많은 정책입니다

조사 페이지에 결과를 표시하려면 *_Policy_* 영역에서 정책 이름을 클릭합니다. 사용 가능한 모든 정책 목록을 보려면 * 모두 보기 * 를 클릭합니다.

을 클릭합니다 ["여기"](#) 정책에 대해 자세히 알아보십시오.

데이터 개요

스캔 중인 모든 데이터의 간단한 개요 버튼을 클릭하여 모든 작업 환경 및 데이터 소스에 대한 사용 용량, 데이터 수명, 데이터 크기 및 파일 유형이 포함된 전체 데이터 매핑 보고서를 다운로드합니다. 을 참조하십시오 ["데이터 매핑 보고서"](#) 을 참조하십시오.

데이터 민감도에 따라 나열된 상위 데이터 리포지토리

민감도 수준별 상위 데이터 리포지토리_영역에는 가장 중요한 항목이 포함된 상위 4개의 데이터 리포지토리(작업 환경 및 데이터 소스)가 나열됩니다. 각 작업 환경의 막대 차트는 다음과 같이 구분됩니다.

- 비개인 데이터
- 개인 데이터
- 민감한 개인 데이터

각 섹션 위로 마우스를 가져가면 각 범주의 총 항목 수를 볼 수 있습니다.

조사 페이지에서 필터링된 결과를 보려면 각 영역을 클릭하여 더 자세히 조사할 수 있습니다.

열기 권한 유형별로 나열된 데이터

Open Permissions_ 영역에는 스캔되는 모든 파일에 대해 존재하는 각 권한 유형의 백분율이 표시됩니다. 차트에는 다음과 같은 유형의 사용 권한이 표시됩니다.

- 개방 액세스 없음
- 조직에 열기
- 공개
- 알 수 없는 액세스

각 섹션 위로 마우스를 가져가면 각 범주의 총 파일 수를 볼 수 있습니다. 조사 페이지에서 필터링된 결과를 보려면 각 영역을 클릭하여 더 자세히 조사할 수 있습니다.

데이터 기간 및 데이터 크기 그래프

Age_and_Size_graphs의 항목을 조사하여 삭제해야 할 데이터가 있는지 또는 더 저렴한 오브젝트 스토리지에 계층화해야 하는지 여부를 확인해야 할 수 있습니다.

차트의 한 지점 위로 마우스를 가져가면 해당 범주의 데이터 사용 기간 또는 크기에 대한 세부 정보를 볼 수 있습니다. 해당 기간 또는 크기 범위로 필터링된 모든 파일을 보려면 클릭합니다.

- * 데이터 그래프의 기간 * - 데이터가 생성된 시간, 마지막으로 액세스한 시간 또는 마지막으로 수정된 시간을 기준으로 데이터를 분류합니다.
- * 데이터 그래프 크기 * - 크기에 따라 데이터를 분류합니다.

가장 많이 식별된 데이터 분류

Classification_area는 가장 많이 식별된 목록을 제공합니다 "범주", "파일 형식", 및 "AIP 레이블" 스캔 데이터.

범주

범주는 보유한 정보의 유형을 표시하여 데이터의 상태를 이해하는 데 도움이 됩니다. 예를 들어 "이력서" 또는 "직원 계약"과 같은 범주에는 중요한 데이터가 포함될 수 있습니다. 결과를 조사할 때 직원 계약이 안전하지 않은 위치에 저장되어 있는 것을 발견할 수 있습니다. 그런 다음 해당 문제를 해결할 수 있습니다.

을 참조하십시오 ["범주별로 파일 보기"](#) 를 참조하십시오.

파일 형식

파일 형식을 검토하면 특정 파일 형식이 올바르게 저장되지 않은 것을 발견할 수 있으므로 중요한 데이터를 제어하는 데 도움이 됩니다.

을 참조하십시오 ["파일 형식 보기"](#) 를 참조하십시오.

AIP 레이블

AIP(Azure Information Protection)에 가입한 경우 콘텐츠에 레이블을 적용하여 문서와 파일을 분류하고 보호할 수 있습니다. 파일에 할당된 가장 많이 사용되는 AIP 레이블을 검토하면 파일에서 가장 많이 사용되는 레이블을 확인할 수 있습니다.

을 참조하십시오 ["AIP 레이블"](#) 를 참조하십시오.

조직에 저장된 데이터에 대한 규정 준수 세부 정보 보기

조직의 개인 데이터 및 민감한 개인 데이터에 대한 세부 정보를 확인하여 개인 데이터를 제어할 수 있습니다. Cloud Data Sense가 데이터에서 발견한 범주와 파일 형식을 검토하여 가시성을 확보할 수도 있습니다.



이 섹션에 설명된 기능은 데이터 소스에서 전체 분류 검사를 수행하도록 선택한 경우에만 사용할 수 있습니다. 매핑 전용 스캔이 있는 데이터 원본은 파일 수준 세부 정보를 표시하지 않습니다.

기본적으로 Cloud Data Sense 대시보드에는 모든 작업 환경 및 데이터베이스의 규정 준수 데이터가 표시됩니다.



일부 작업 환경에 대한 데이터만 보려면 [작업 환경을 선택합니다](#).

또한 데이터 조사 페이지에서 결과를 필터링하고 결과 보고서를 CSV 파일로 다운로드할 수도 있습니다. 을 참조하십시오 [데이터 조사 페이지의 데이터 필터링](#) 를 참조하십시오.

개인 데이터가 포함된 파일 보기

Cloud Data Sense는 데이터 내에서 특정 단어, 문자열 및 패턴(Regex)을 자동으로 식별합니다. 예를 들어 개인 식별 정보(PII), 신용 카드 번호, 주민 등록 번호, 은행 계좌 번호, 암호, 있습니다. "[전체 목록을 참조하십시오](#)".

또한 스캔할 데이터베이스 서버를 추가한 경우 [Data Fusion](#) 기능을 사용하여 파일을 스캔하여 데이터베이스의 고유 식별자가 해당 파일 또는 기타 데이터베이스에서 검색되는지 여부를 확인할 수 있습니다. 을 참조하십시오 "[Data Fusion를 사용하여 개인 데이터 식별자를 추가합니다](#)" 를 참조하십시오.

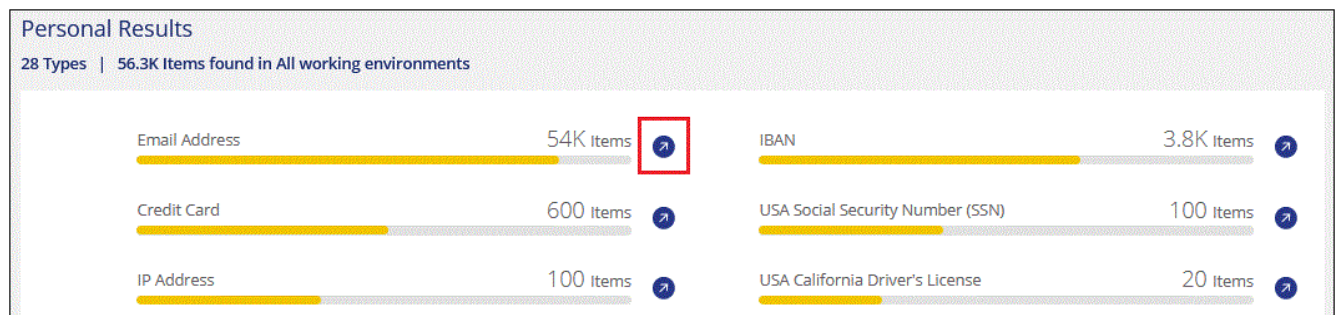
일부 개인 데이터 유형의 경우 데이터 센스에서 근접성 검증_을 사용하여 결과를 검증합니다. 유효성 검사는 발견된 개인 데이터 근처에서 하나 이상의 미리 정의된 키워드를 찾는 방식으로 수행됩니다. 예를 들어, 데이터 센스에서 미국을 식별합니다 주민등록번호(SSN) 옆에 근접 단어가 있는 경우 주민등록번호로 사용 — 예: `_SSN_OR_Social security`. "[개인 데이터 표](#)" 데이터 센스에서 근접 유효성 검사를 사용하는 경우를 표시합니다.

단계

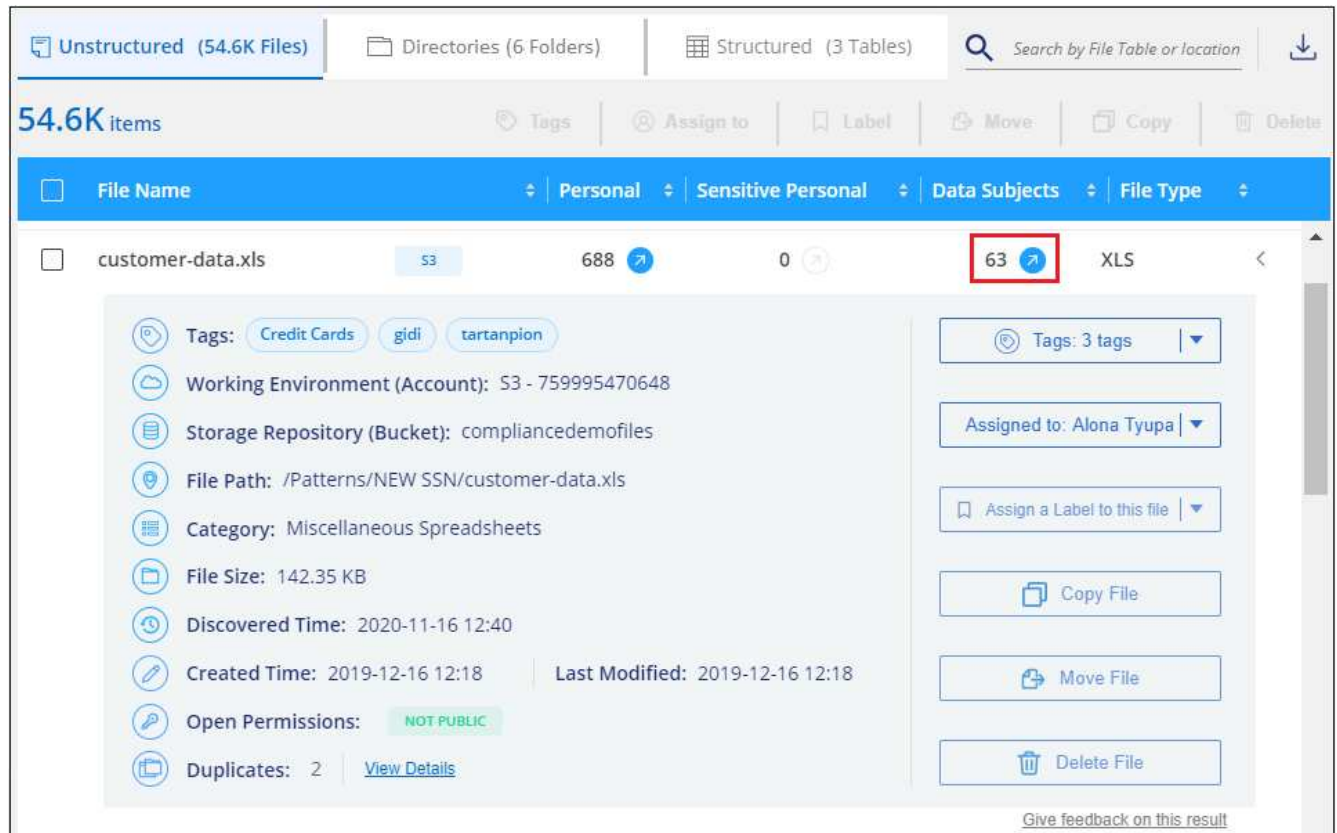
1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭하고 * 규정 준수 * 탭을 클릭합니다.
2. 모든 개인 데이터에 대한 세부 정보를 조사하려면 개인 데이터 백분율 옆에 있는 아이콘을 클릭합니다.



3. 특정 유형의 개인 데이터에 대한 세부 정보를 조사하려면 * 모두 보기 * 를 클릭한 다음 특정 유형의 개인 데이터(예: 전자 메일 주소)에 대한 * 조사 결과 * 아이콘을 클릭합니다.



4. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을 다운로드하여 데이터를 조사합니다.



중요한 개인 데이터가 들어 있는 파일 보기

Cloud Data Sense는 와 같은 개인 정보 보호 규정에 정의된 대로 민감한 개인 정보의 특수한 유형을 자동으로 식별합니다 "GDPR 9조 및 10조". 예를 들어, 개인의 건강, 인종 또는 성적 취향과 관련된 정보를 제공합니다. "전체 목록을 참조하십시오".

Cloud Data Sense는 인공지능(AI), 자연어 처리(NLP), 머신 러닝(ML) 및 코그니티브 컴퓨팅(CC)을 사용하여 엔터티를 추출하고 그에 따라 범주화하기 위해 검색하는 내용의 의미를 파악합니다.

예를 들어, 중요한 GDPR 데이터 범주 중 하나는 인종입니다. 데이터 센스는 NLP 기능으로 인해 "George is Mexican"(GDPR 제9조에 명시된 민감한 데이터 표시)과 "George is eating Mexican food"라는 문장의 차이를 구별할 수 있습니다.



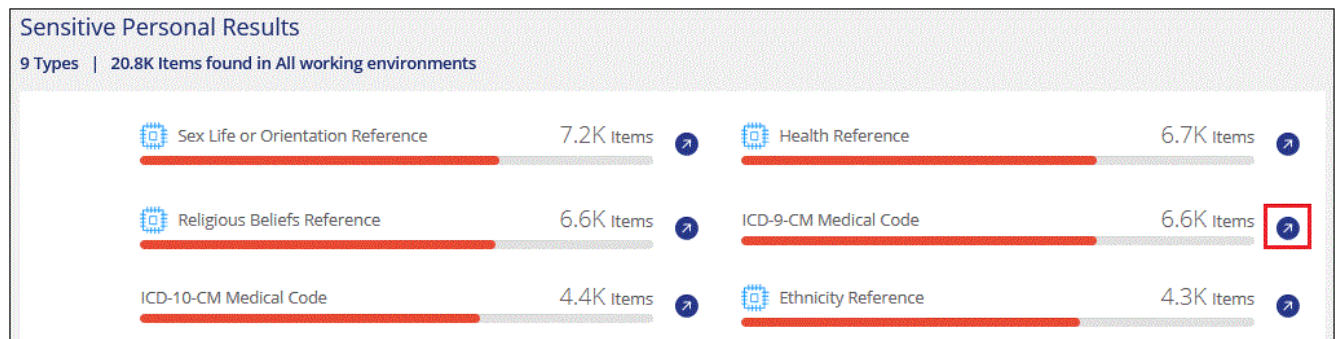
민감한 개인 데이터를 검색할 때는 영어로만 지원됩니다. 더 많은 언어에 대한 지원은 나중에 추가됩니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭하고 * 규정 준수 * 탭을 클릭합니다.
2. 중요한 모든 개인 데이터에 대한 세부 정보를 조사하려면 중요한 개인 데이터 백분을 옆에 있는 아이콘을 클릭합니다.



3. 특정 유형의 중요한 개인 데이터에 대한 세부 정보를 조사하려면 * 모두 보기 * 를 클릭한 다음 특정 유형의 중요한 개인 데이터에 대해 * 결과 조사 * 아이콘을 클릭합니다.



4. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을 다운로드하여 데이터를 조사합니다.

범주별로 파일 보기

Cloud Data Sense는 스캔한 데이터를 다양한 유형의 범주로 나눕니다. 범주는 각 파일의 콘텐츠 및 메타데이터에 대한 AI 분석을 기반으로 하는 주제입니다. ["범주 목록을 참조하십시오"](#).

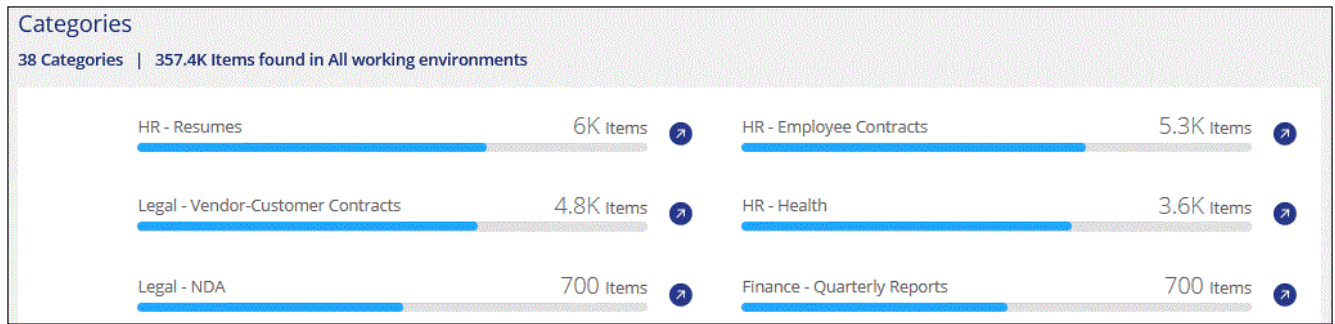
범주는 보유한 정보의 유형을 표시하여 데이터의 상태를 이해하는 데 도움이 됩니다. 예를 들어 이력서 또는 직원 계약과 같은 범주에는 중요한 데이터가 포함될 수 있습니다. 결과를 조사할 때 직원 계약이 안전하지 않은 위치에 저장되어 있는 것을 발견할 수 있습니다. 그런 다음 해당 문제를 해결할 수 있습니다.



영어, 독일어 및 스페인어가 범주에 지원됩니다. 더 많은 언어에 대한 지원은 나중에 추가됩니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭하고 * 규정 준수 * 탭을 클릭합니다.
2. 기본 화면에서 직접 상위 4개 범주 중 하나에 대한 * 조사 결과 * 아이콘을 클릭하거나 * 모두 보기 * 를 클릭한 다음 범주 중 하나에 대한 아이콘을 클릭합니다.



3. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을 다운로드하여 데이터를 조사합니다.

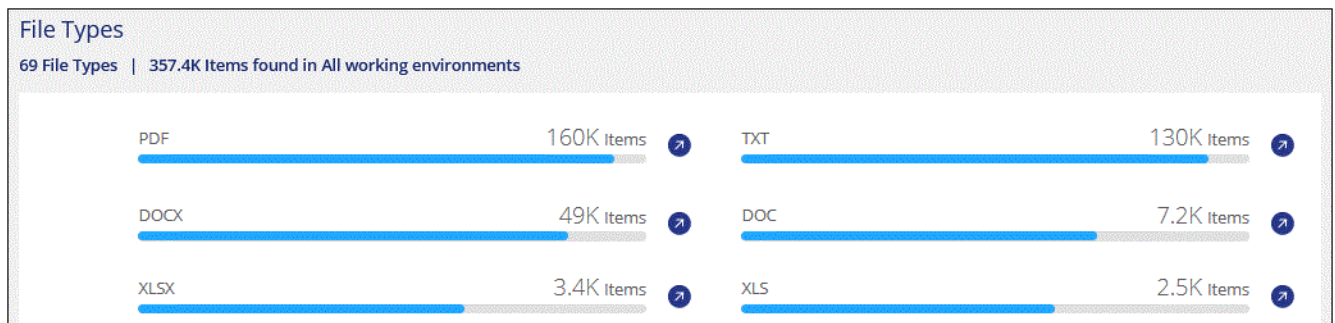
파일 형식별로 파일 보기

Cloud Data Sense는 스캔한 데이터를 파일 형식별로 분해합니다. 파일 형식을 검토하면 특정 파일 형식이 올바르게 저장되지 않은 것을 발견할 수 있으므로 중요한 데이터를 제어하는 데 도움이 됩니다. ["파일 형식 목록을 참조하십시오"](#).

예를 들어 조직에 대한 매우 중요한 정보가 포함된 CAD 파일을 저장할 수 있습니다. 보안이 설정되지 않은 경우 사용 권한을 제한하거나 파일을 다른 위치로 이동하여 중요한 데이터를 제어할 수 있습니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭하고 * 규정 준수 * 탭을 클릭합니다.
2. 기본 화면에서 직접 상위 4개 파일 유형 중 하나에 대한 * 조사 결과 * 아이콘을 클릭하거나 * 모두 보기 * 를 클릭한 다음 파일 유형에 대한 아이콘을 클릭합니다.



3. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을 다운로드하여 데이터를 조사합니다.

파일 메타데이터 보기

데이터 조사 결과 창에서 을(를) 클릭할 수 있습니다. 모든 단일 파일에서 파일 메타데이터를 볼 수 있습니다.

파일이 있는 작업 환경과 볼륨을 보여 주는 것 외에도 메타데이터는 파일 권한, 파일 소유자, 이 파일의 중복 여부 및 할당된 AIP 레이블(있는 경우)을 비롯하여 훨씬 더 많은 정보를 표시합니다 "클라우드 데이터 센스에 AIP가 통합되어 있습니다"를 클릭합니다. 이 정보는 를 계획 중인 경우에 유용합니다 "정책을 생성합니다" 데이터를 필터링하는 데 사용할 수 있는 모든 정보를 볼 수 있기 때문입니다.

모든 데이터 원본에 대해 모든 정보를 사용할 수 있는 것은 아니며 해당 데이터 원본에 적합한 정보일 뿐입니다. 예를 들어 볼륨 이름, 권한 및 AIP 레이블은 데이터베이스 파일과 관련이 없습니다.

단일 파일의 세부 정보를 볼 때 파일에 대해 수행할 수 있는 몇 가지 작업이 있습니다.

- 파일을 NFS 공유로 이동하거나 복사할 수 있습니다. 을 참조하십시오 "소스 파일을 NFS 공유로 이동하는 중입니다" 및 "소스 파일을 NFS 공유에 복사하는 중입니다" 를 참조하십시오.
- 파일을 삭제할 수 있습니다. 을 참조하십시오 "원본 파일을 삭제하는 중입니다" 를 참조하십시오.
- 파일에 특정 상태를 할당할 수 있습니다. 을 참조하십시오 "태그 적용 중" 를 참조하십시오.
- 파일을 Cloud Manager 사용자에게 할당하여 파일에 대해 수행해야 하는 후속 작업을 책임질 수 있습니다. 을 참조하십시오 "파일에 사용자 할당" 를 참조하십시오.
- AIP 레이블을 Cloud Data Sense와 통합한 경우 이 파일에 레이블을 지정하거나 이미 있는 경우 다른 레이블로 변경할 수 있습니다. 을 참조하십시오 "AIP 레이블을 수동으로 할당합니다" 를 참조하십시오.

파일에 대한 권한 보기

파일에 대한 액세스 권한이 있는 모든 사용자 또는 그룹의 목록과 사용 권한 유형을 보려면 * 모든 권한 보기 * 를 클릭합니다. 이 버튼은 CIFS 공유, SharePoint, OneDrive에 있는 파일에만 사용할 수 있습니다.

사용자 및 그룹 이름 대신 SID(보안 식별자)가 표시되는 경우 Active Directory를 데이터 센스에 통합해야 합니다. "이

작업을 수행하는 방법을 확인하십시오".

The screenshot shows a file management interface. On the left, a sidebar lists file details for "Expense Report TPO-1060.pdf": Working Environment: WorkingEnvironment1, Repository: Volume Name, File Path: /Prod/labs-base/Expense Report TPO-1060.pdf, Category: Legal, File Size: 22 MB, Last Modified: 2019-08-06 07:51, Open Permissions: NO OPEN PERMISSIONS, and File Owner: Avy. A red box highlights the "View all Permissions" link. On the right, a pop-up window titled "Permissions list for 'Expense Report TPO-1060.pdf'" displays a table of permissions.

User / Group	Name	Read	Write
User Name		✓	✓
Group Name		✓	✓
Group Name		✓	✓
John L		✓	✓
George H		✓	✓
Paul M		✓	✓
Ringo S		✓	✓

사용자 또는 그룹의 이름을 클릭하면 "사용자/그룹 권한" 필터에 해당 사용자 또는 그룹의 이름과 함께 조사 페이지가 표시되어 사용자 또는 그룹이 액세스할 수 있는 모든 파일을 볼 수 있습니다.

또한 를 클릭할 수도 있습니다 ✓ 모든 그룹에 대해 그룹에 속한 사용자 목록을 표시합니다.

스토리지 시스템에서 중복 파일을 확인하는 중입니다

중복 파일이 스토리지 시스템에 저장되어 있는지 확인할 수 있습니다. 이 기능은 저장 공간을 절약할 수 있는 영역을 확인하고자 할 때 유용합니다. 또한 특정 사용 권한이나 중요한 정보가 있는 특정 파일이 스토리지 시스템에서 불필요하게 복제되지 않도록 하는 것이 도움이 될 수 있습니다.

데이터 센스(Data Sense)는 해시 기술을 사용하여 중복 파일을 결정합니다. 파일에 다른 파일과 동일한 해시 코드가 있으면 파일 이름이 다르더라도 파일이 정확하게 중복되었는지 100% 확인할 수 있습니다.

중복 파일 목록을 다운로드하여 스토리지 관리자에게 전송하여 삭제할 수 있는 파일이 있는지 확인할 수 있습니다. 아니면 가능합니다 "파일을 삭제합니다" 특정 버전의 파일이 필요하지 않을 경우

복제된 모든 파일을 봅니다

작업 환경 및 스캔할 데이터 원본에 중복되는 모든 파일의 목록을 보려면 데이터 조사 페이지에서 * 중복 > 중복 항목 있음 * 이라는 필터를 사용하면 됩니다.

최소 크기가 50MB이고 개인 정보 또는 민감한 개인 정보가 포함된 모든 파일 형식(데이터베이스 제외)의 중복 파일이 결과 페이지에 표시됩니다.

특정 파일이 중복되어 있는지 확인합니다

단일 파일에 중복이 있는지 확인하려면 데이터 조사 결과 창에서 을(를) 클릭합니다 ✓ 모든 단일 파일에서 파일

메타데이터를 볼 수 있습니다. 특정 파일의 복제본이 있는 경우 이 정보는 *Duplicates* 필드 옆에 표시됩니다.

중복 파일 목록과 파일이 있는 위치를 보려면 * 세부 정보 보기 * 를 클릭합니다. 다음 페이지에서 * 중복 보기 * 를 클릭하여 조사 페이지에서 파일을 봅니다.

🕒

Last Modified: 2019-08-06 07:51

🔗

Open Permissions: NO OPEN PERMISSIONS [View all Permissions](#)

👤

File Owner: Asaf Ley

📁

Duplicates: 3 [View Details](#)

Duplicates of File 'Name 1'

📁

Duplicates: 3

📊

Total Size of all Duplicates: 1GB

🔍

File Hash: xxxxxx

[View Duplicates](#)

[Close](#)

3 Items

<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type	
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼



이 페이지에 제공된 "파일 해시" 값을 사용하여 조사 페이지에 직접 입력하여 특정 중복 파일을 언제든지 검색할 수도 있고, 정책에 사용할 수도 있습니다.

특정 작업 환경에 대한 대시보드 데이터 보기

Cloud Data Sense 대시보드의 콘텐츠를 필터링하여 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터를 확인하거나 특정 작업 환경에 대한 규정 준수 데이터를 확인할 수 있습니다.

대시보드를 필터링할 때 데이터 센스에서 규정 준수 데이터와 보고서의 범위를 선택한 작업 환경만으로 설정합니다.

단계

1. 필터 드롭다운을 클릭하고 데이터를 보려는 작업 환경을 선택한 다음 * 보기 * 를 클릭합니다.



데이터 조사 페이지의 데이터 필터링

조사 페이지의 내용을 필터링하여 원하는 결과만 표시할 수 있습니다. 이 기능은 데이터를 구체화한 후 페이지 상단의 단추 모음을 사용하여 파일 복사, 파일 이동, 파일에 태그 또는 AIP 레이블 추가 등의 다양한 작업을 수행할 수 있으므로 매우 강력한 기능입니다.

페이지 내용을 구체화한 후 보고서로 다운로드하려면 을 클릭합니다. 버튼을 클릭하여 .csv 파일을 저장합니다.

Data Investigation

Unstructured (364K Files)

Directories (64 Folders)

Structured (45 Tables)

Search by file or DB table

FILTERS:

Clear All

Policies

+

Open Permissions

+

File Owner

+

Label

+

Working Environment Type

2

+

Working Environment

+

Storage Repository

2

+

364K items

Tags

Assign to

Label

Move

Copy

Delete

<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type	
<input type="checkbox"/>	cgdpr_yes_adam.txt	ANF	0	797	111	TXT	▼
<input type="checkbox"/>	cgdpr_yes_adam.txt	ANF	0	797	111	TXT	▼
<input type="checkbox"/>	true positive.txt	ANF	0	611	111	TXT	▼
<input type="checkbox"/>	cgdpr_yes_adam.txt	ANF	0	611	111	TXT	▼
<input type="checkbox"/>	true positive.txt	ANF	0	611	111	TXT	▼
<input type="checkbox"/>	true positive.txt	ANF	0	611	111	TXT	▼
<input type="checkbox"/>	cgdpr_yes_adam.txt	ANF	0	611	111	TXT	▼
<input type="checkbox"/>	cgdpr_yes_adam.txt	ANF	0	611	111	TXT	▼

- 최상위 탭을 사용하면 파일(구조화되지 않은 데이터), 디렉토리(폴더 및 파일 공유) 또는 데이터베이스(구조화된 데이터)에서 데이터를 볼 수 있습니다.
- 각 열의 맨 위에 있는 컨트롤을 사용하여 결과를 숫자 또는 사전순으로 정렬할 수 있습니다.
- 왼쪽 창 필터를 사용하면 다음 속성 중에서 선택하여 결과를 구체화할 수 있습니다.

필터	세부 정보
정책	정책 또는 정책을 선택합니다. 이동 "여기" 기존 정책 목록을 보고 고유한 사용자 지정 정책을 만들려면
사용 권한을 엽니다	데이터 및 폴더/공유 내에서 사용 권한 유형을 선택합니다
사용자/그룹 권한	하나 이상의 사용자 이름 및/또는 그룹 이름을 선택하거나 부분 이름을 입력합니다
파일 소유자	파일 소유자 이름을 입력합니다
라벨	를 선택합니다 "AIP 레이블" 파일에 할당됩니다
작업 환경 유형	작업 환경의 유형을 선택합니다. OneDrive, SharePoint 및 Google Drive는 "클라우드 앱"으로 분류됩니다.
작업 환경 이름	특정 작업 환경을 선택합니다
저장소 저장소	볼륨 또는 스키마와 같은 스토리지 리포지토리를 선택합니다
파일 경로	부분 경로 또는 전체 경로를 입력합니다
범주	를 선택합니다 "범주 유형"
감도 수준	감도 수준을 선택합니다
개인 데이터	를 선택합니다 "개인 데이터의 유형입니다"
민감한 개인 데이터	를 선택합니다 "중요한 개인 데이터의 유형"
데이터 제목	데이터 주체의 전체 이름 또는 알려진 식별자를 입력합니다
디렉터리 유형	"공유" 또는 "폴더"와 같은 디렉터리 유형을 선택합니다.

필터	세부 정보
파일 형식	를 선택합니다 "파일 유형"
파일 크기	파일 크기 범위를 선택합니다
만든 시간	파일이 생성된 범위를 선택합니다
검색된 시간	Data Sense가 파일을 검색할 때 범위를 선택합니다
마지막 수정	파일이 마지막으로 수정된 범위를 선택합니다
마지막 액세스	파일을 마지막으로 액세스한 범위를 선택합니다. 데이터 센스에서 스캔하는 파일 유형의 경우, 데이터 센스에서 파일을 스캔한 마지막 시간입니다.
중복	파일이 리포지토리에서 복제되는지 여부를 선택합니다
파일 해시	파일 해시를 입력하여 이름이 다르더라도 특정 파일을 찾습니다
태그	를 선택합니다 "태그 또는 태그" 파일에 할당됩니다
할당 대상	파일이 할당된 사람의 이름을 선택합니다

버튼 모음과 정책에서 사용할 수 있는 작업은 현재 "디렉토리" 수준에서 지원되지 않습니다.

개인 데이터 구성

Cloud Data Sense는 개인 데이터를 관리하고 구성할 수 있는 다양한 방법을 제공합니다. 따라서 가장 중요한 데이터를 더 쉽게 볼 수 있습니다.

- 에 가입되어 있는 경우 "AIP(Azure Information Protection)" 파일을 분류 및 보호하기 위해 Cloud Data Sense를 사용하여 AIP 레이블을 관리할 수 있습니다.
- 조직 또는 일부 유형의 추가 작업에 대해 표시할 파일에 태그를 추가할 수 있습니다.
- Cloud Manager 사용자를 특정 파일 또는 여러 파일에 할당하여 파일 관리를 책임질 수 있습니다.
- "정책" 기능을 사용하면 버튼 하나를 클릭하여 결과를 쉽게 볼 수 있도록 사용자 지정 검색 쿼리를 직접 만들 수 있습니다.
- 특정 중요 정책에서 결과를 반환하는 경우 Cloud Manager 사용자에게 이메일 경고를 보낼 수 있습니다.



이 섹션에 설명된 기능은 데이터 소스에서 전체 분류 검사를 수행하도록 선택한 경우에만 사용할 수 있습니다. 매핑 전용 스캔이 있는 데이터 원본은 파일 수준 세부 정보를 표시하지 않습니다.

태그나 라벨을 사용해야 합니까?

다음은 Data Sense 태깅 및 Azure Information Protection 레이블과 비교한 것입니다.

태그	라벨
파일 태그는 데이터 센스의 통합된 부분입니다.	Azure 정보 보호(AIP)에 가입해야 합니다.
태그는 데이터 감지 데이터베이스에만 보관되며 파일에 기록되지 않습니다. 파일 또는 액세스되거나 수정된 파일은 변경되지 않습니다.	레이블은 파일의 일부이며 레이블이 변경되면 파일이 변경됩니다. 또한 이 변경 사항은 액세스 및 수정된 파일 시간도 변경합니다.

태그	라벨
한 파일에 여러 개의 태그를 지정할 수 있습니다.	단일 파일에 하나의 레이블이 있을 수 있습니다.
태그는 복사, 이동, 삭제, 정책 실행 등의 내부 데이터 감지 작업에 사용할 수 있습니다. 등	파일을 읽을 수 있는 다른 시스템은 추가 자동화에 사용할 수 있는 레이블을 볼 수 있습니다.
단일 API 호출만 사용하여 파일에 태그가 있는지 확인합니다.	

AIP 레이블을 사용하여 데이터를 분류합니다

구독한 경우 Cloud Data Sense에서 검색 중인 파일에서 AIP 레이블을 관리할 수 있습니다 ["AIP\(Azure Information Protection\)"](#). AIP를 사용하면 콘텐츠에 레이블을 적용하여 문서와 파일을 분류하고 보호할 수 있습니다. 데이터 센스를 사용하면 파일에 이미 할당된 라벨을 보고, 파일에 라벨을 추가하고, 라벨이 이미 있을 때 라벨을 변경할 수 있습니다.

Cloud Data Sense는 .DOC, .DOCX, .PDF, .PPTX, .XLS 파일 형식 내에서 AIP 레이블을 지원합니다. XLSX



- 현재 30MB를 초과하는 파일의 레이블은 변경할 수 없습니다. OneDrive, SharePoint 및 Google Drive 계정의 경우 최대 파일 크기는 4MB입니다.
- 파일에 AIP에 더 이상 존재하지 않는 레이블이 있는 경우 Cloud Data Sense는 이 레이블을 레이블이 없는 파일로 간주합니다.
- 인터넷에 액세스할 수 없는 온프레미스 위치(어두운 사이트라고도 함)에 Data Sense 인스턴스를 배포한 경우에는 AIP 레이블 기능을 사용할 수 없습니다.

작업 공간에 AIP 레이블 통합

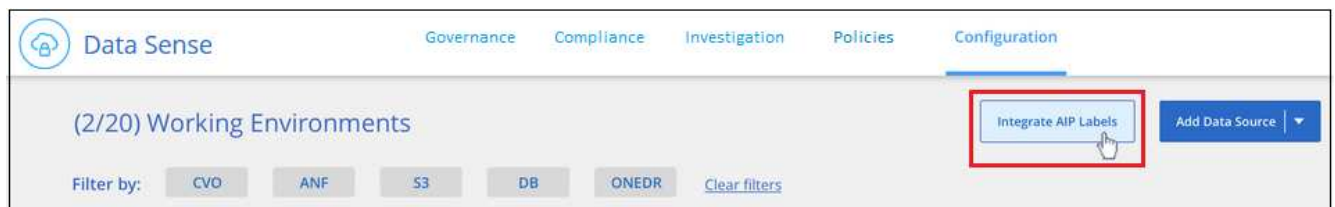
AIP 레이블을 관리하려면 AIP 레이블 기능을 기존 Azure 계정에 로그인하여 Cloud Data Sense에 통합해야 합니다. 활성화되면 모든 파일의 AIP 레이블을 관리할 수 있습니다 ["운영 환경 및 데이터 소스"](#) 를 살펴보세요.

요구 사항

- 계정 및 Azure 정보 보호 라이선스가 있어야 합니다.
- Azure 계정에 대한 로그인 자격 증명이 있어야 합니다.
- Amazon S3 버킷에 있는 파일의 레이블을 변경하려면 IAM 역할에 권한 '3:PutObject'가 포함되어 있는지 확인하십시오. 을 참조하십시오 ["IAM 역할 설정"](#).

단계

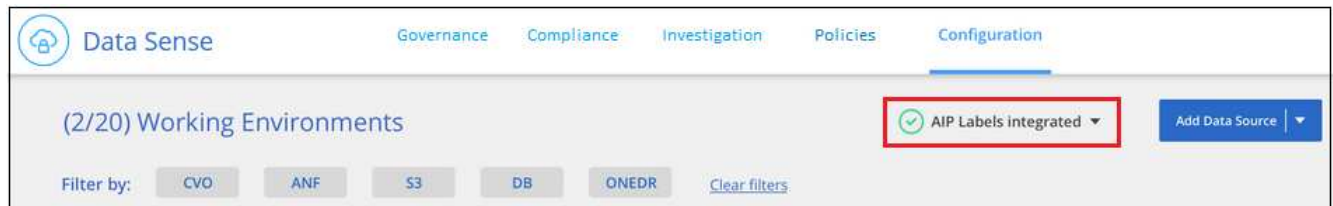
1. 클라우드 데이터 감지 구성 페이지에서 * AIP 레이블 통합 * 을 클릭합니다.



2. AIP 레이블 통합 대화 상자에서 * Azure에 로그인 * 을 클릭합니다.
3. Microsoft 페이지가 나타나면 계정을 선택하고 필요한 자격 증명을 입력합니다.
4. Cloud Data Sense 탭으로 돌아가면 "AIP 라벨이 <ACCOUNT_NAME> 계정과 성공적으로 통합되었습니다."라는

메시지가 표시됩니다.

5. 닫기 * 를 클릭하면 페이지 상단에 _AIP 라벨 통합 _이라는 텍스트가 표시됩니다.



조사 페이지의 결과 창에서 AIP 레이블을 보고 할당할 수 있습니다. 정책을 사용하여 파일에 AIP 레이블을 할당할 수도 있습니다.

파일의 **AIP** 레이블 보기

파일에 할당된 현재 AIP 레이블을 볼 수 있습니다.

데이터 조사 결과 창에서 을 클릭합니다 ▼ 파일 메타데이터 세부 정보를 확장합니다.



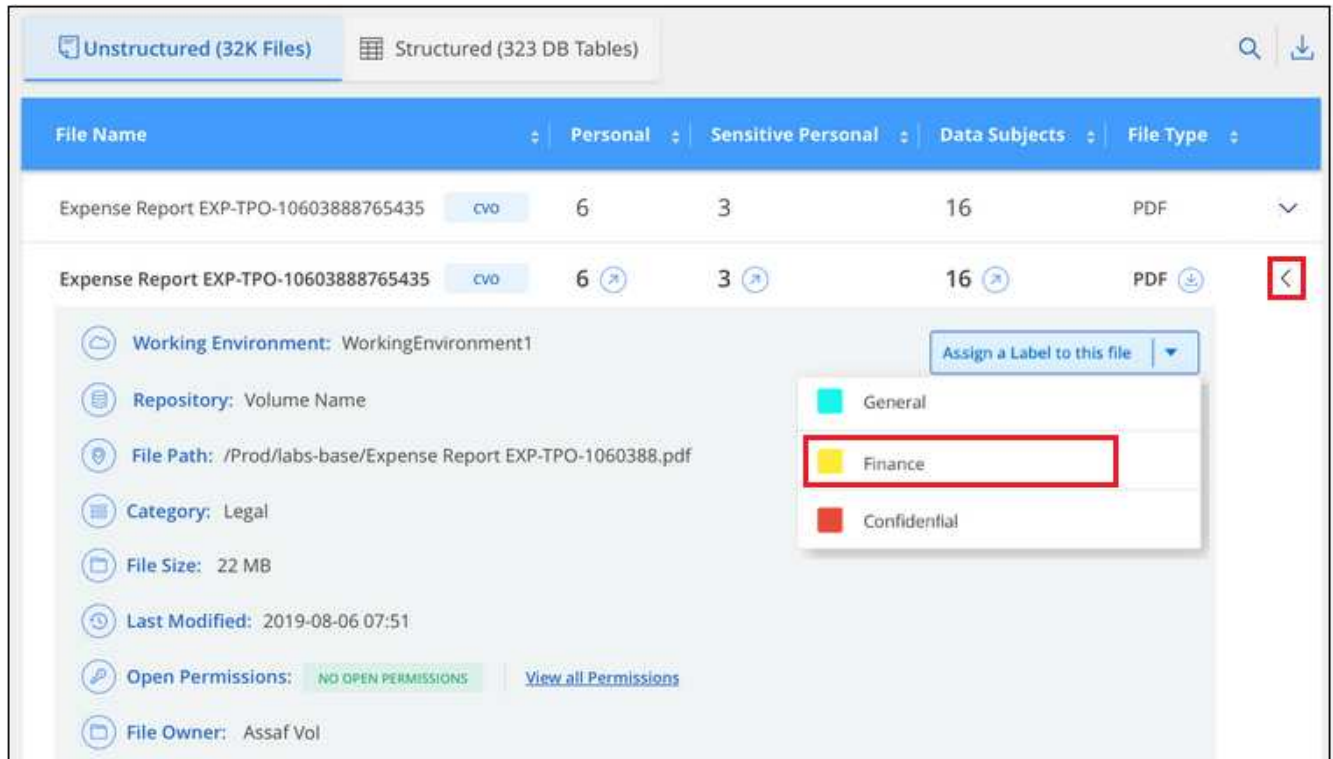
AIP 레이블을 수동으로 할당합니다

Cloud Data Sense를 사용하여 파일에서 AIP 레이블을 추가, 변경 및 제거할 수 있습니다.

다음 단계에 따라 AIP 레이블을 단일 파일에 할당합니다.

단계

1. 데이터 조사 결과 창에서 을 클릭합니다 ▼ 파일 메타데이터 세부 정보를 확장합니다.



2. 이 파일에 레이블 지정 * 을 클릭한 다음 레이블을 선택합니다.

파일 메타데이터에 레이블이 나타납니다.

AIP 레이블을 여러 파일에 할당하려면 다음과 같이 하십시오.

단계

1. 데이터 조사 결과 창에서 레이블을 지정할 파일을 선택합니다.



◦ 개별 파일을 선택하려면 각 파일(☒ Volume_1)를 클릭합니다.

◦ 현재 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭합니다.

2. 버튼 모음에서 * Label * 을 클릭하고 AIP 레이블을 선택합니다.



선택한 모든 파일의 메타데이터에 AIP 레이블이 추가됩니다.

AIP 레이블을 정책에 자동으로 할당합니다

정책 기준을 충족하는 모든 파일에 AIP 레이블을 할당할 수 있습니다. 정책을 생성할 때 AIP 레이블을 지정하거나 정책을 편집할 때 레이블을 추가할 수 있습니다.

Cloud Data Sense가 파일을 스캔하면 파일에 레이블이 계속 추가되거나 업데이트됩니다.

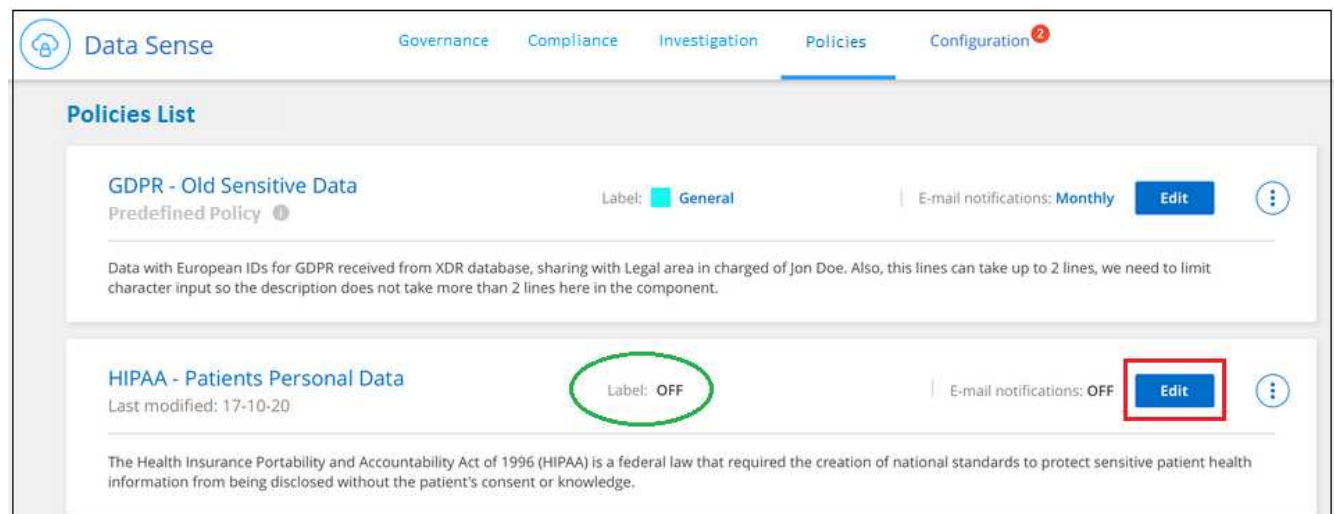
레이블이 파일에 이미 적용되었는지 여부와 레이블의 분류 수준에 따라 레이블을 변경할 때 다음 작업이 수행됩니다.

파일이...	그러면...
레이블이 없습니다	라벨이 추가됩니다
낮은 수준의 분류에 대한 기존 레이블이 있습니다	더 높은 수준의 라벨이 추가됩니다
더 높은 수준의 분류에 대한 기존 레이블이 있습니다	더 높은 수준의 레이블이 유지됩니다
는 수동으로 또는 정책에 의해 레이블이 할당됩니다	더 높은 수준의 라벨이 추가됩니다
는 두 정책에 의해 두 개의 서로 다른 레이블을 할당합니다	더 높은 수준의 라벨이 추가됩니다

기존 정책에 AIP 레이블을 추가하려면 다음 단계를 따르십시오.

단계

1. 정책 목록 페이지에서 AIP 레이블을 추가하거나 변경할 정책에 대해 * 편집 * 을 클릭합니다.



2. 정책 편집 페이지에서 확인란을 선택하여 정책 매개 변수와 일치하는 파일에 대해 자동 레이블을 활성화하고 레이블을 선택합니다(예: * General *).

3. Save Policy * 를 클릭하면 Policy 설명에 레이블이 표시됩니다.



정책이 레이블로 구성되었지만 이후에 AIP에서 레이블이 제거된 경우 레이블 이름은 OFF로 설정되고 레이블은 더 이상 할당되지 않습니다.

AIP 통합 제거

파일에서 AIP 레이블을 더 이상 관리할 수 없는 경우 Cloud Data Sense 인터페이스에서 AIP 계정을 제거할 수 있습니다.

데이터 센스를 사용하여 추가한 레이블은 변경되지 않습니다. 파일에 있는 레이블은 현재 있는 그대로 유지됩니다.

단계

1. Configuration_페이지에서 * AIP Labels integrated > Remove Integration * 을 클릭합니다.

2. 확인 대화 상자에서 * 통합 제거 * 를 클릭합니다.

태그를 적용하여 스캔한 파일을 관리합니다

특정 유형의 추가 작업에 대해 표시할 파일에 태그를 추가할 수 있습니다. 예를 들어 일부 중복 파일을 발견하여 이 중 하나를 삭제하려 할 수 있지만 삭제해야 할 파일을 확인해야 합니다. 파일에 "삭제 확인"이라는 태그를 추가할 수 있으므로 이 파일에 몇 가지 조사 및 향후 작업이 필요하다는 것을 알 수 있습니다.

Data Sense를 사용하면 파일에 할당된 태그를 보거나, 파일에서 태그를 추가 또는 제거하거나, 이름을 변경하거나, 기존 태그를 삭제할 수 있습니다.

AIP 레이블과 같은 방식으로 태그가 파일에 추가되지 않습니다. 이 태그는 Cloud Data Sense를 사용하는 Cloud Manager 사용자가 볼 수 있으므로 파일을 삭제하거나 일부 후속 작업 유형을 확인해야 하는지 확인할 수 있습니다.

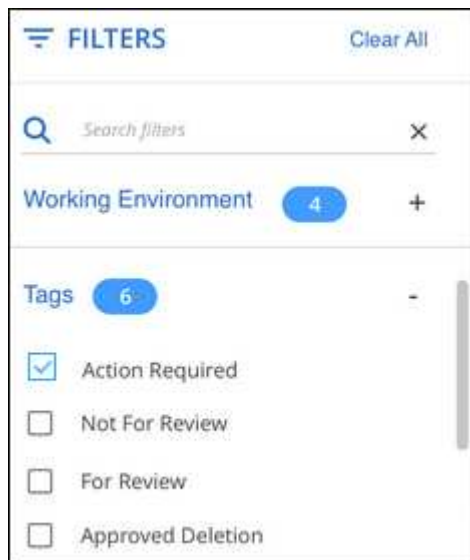


Cloud Data Sense에서 파일에 할당된 태그는 볼륨 또는 가상 머신 인스턴스와 같은 리소스에 추가할 수 있는 태그와 관련이 없습니다. 데이터 감지 태그는 파일 레벨에 적용됩니다.

특정 태그가 적용된 파일 보기

특정 태그가 지정된 모든 파일을 볼 수 있습니다.

1. 클라우드 데이터 센스에서 * 조사 * 탭을 클릭합니다.
2. 데이터 조사 페이지의 필터 창에서 * 태그 * 를 클릭한 다음 필요한 태그를 선택합니다.



조사 결과 창에는 해당 태그가 지정된 모든 파일이 표시됩니다.

파일에 태그 지정

단일 파일 또는 파일 그룹에 태그를 추가할 수 있습니다.

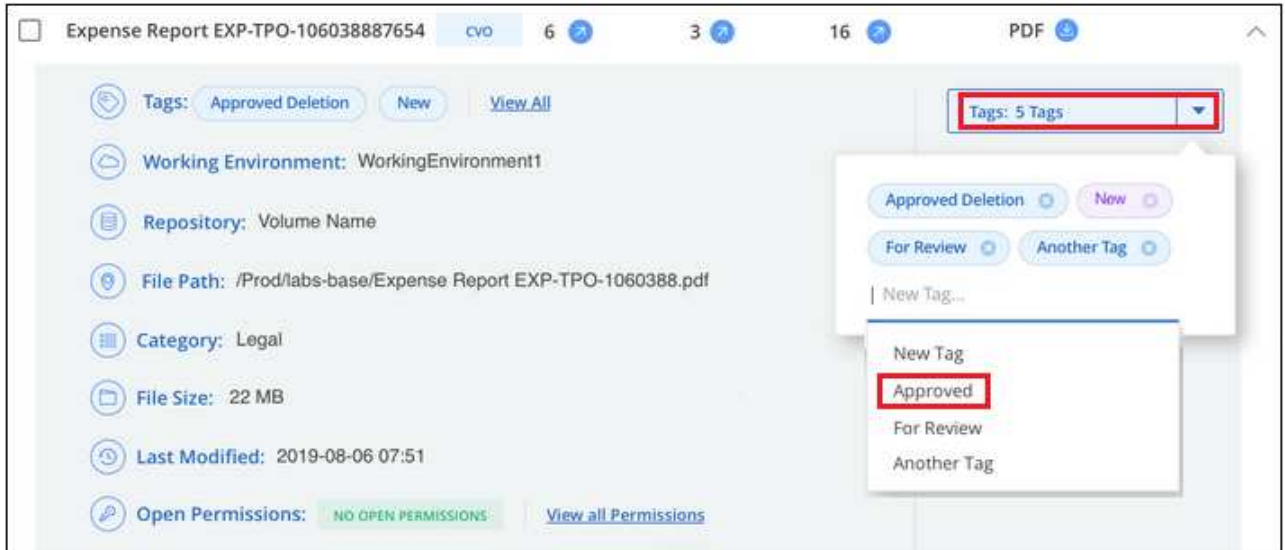
단일 파일에 태그 추가하기:

단계

1. 데이터 조사 결과 창에서 을 클릭합니다. 파일 메타데이터 세부 정보를 확장합니다.
2. 태그 * 필드를 클릭하면 현재 할당된 태그가 표시됩니다.

3. 태그 또는 태그 추가:

- 기존 태그를 지정하려면 * 새 태그... * 필드를 클릭하고 태그 이름을 입력합니다. 찾고 있는 태그가 나타나면 해당 태그를 선택하고 * Enter * 를 누릅니다.
- 새 태그를 만들어 파일에 할당하려면 * 새 태그... * 필드를 클릭하고 새 태그의 이름을 입력한 다음 * Enter * 를 누릅니다.



태그가 파일 메타데이터에 나타납니다.

여러 파일에 태그 추가하기:

단계

1. 데이터 조사 결과 창에서 태그를 지정할 파일을 선택합니다.

2345 items							Tags	Assign to	Label	Copy	Move	Delete
<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type						
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF						
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF						

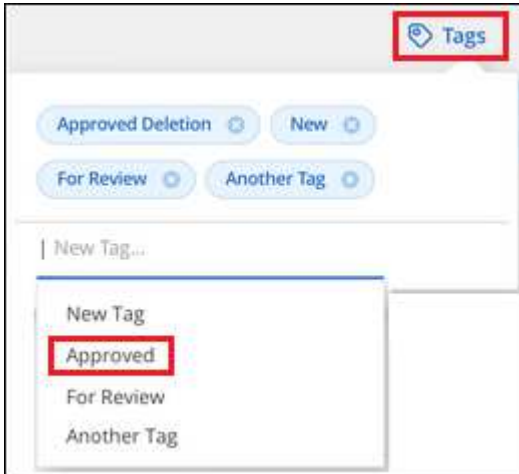
- 개별 파일을 선택하려면 각 파일(☒ Volume_1)를 클릭합니다.
- 현재 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭합니다.

2. 버튼 모음에서 * 태그 * 를 클릭하면 현재 할당된 태그가 표시됩니다.

3. 태그 또는 태그 추가:

- 기존 태그를 지정하려면 * 새 태그... * 필드를 클릭하고 태그 이름을 입력합니다. 찾고 있는 태그가 나타나면 해당 태그를 선택하고 * Enter * 를 누릅니다.

- 새 태그를 만들어 파일에 할당하려면 * 새 태그... * 필드를 클릭하고 새 태그의 이름을 입력한 다음 * Enter * 를 누릅니다.



- 승인 확인 대화 상자에서 태그 추가를 승인하고 선택한 모든 파일의 메타데이터에 태그가 추가됩니다.

파일에서 태그를 삭제하는 중입니다

더 이상 사용하지 않아도 되는 태그는 삭제할 수 있습니다.

기존 태그에 대해 * x * 를 클릭하기만 하면 됩니다.



여러 파일을 선택한 경우 태그가 모든 파일에서 제거됩니다.

특정 파일을 관리할 사용자 할당

Cloud Manager 사용자를 특정 파일 또는 여러 파일에 할당하여 해당 파일에 대해 수행해야 하는 후속 작업을 책임질 수 있습니다. 이 기능은 종종 기능과 함께 사용되어 파일에 사용자 정의 상태 태그를 추가합니다.

예를 들어 너무 많은 사용자가 읽기 및 쓰기 액세스(열린 권한)를 수행할 수 있도록 특정 개인 데이터가 포함된 파일이 있을 수 있습니다. 따라서 상태 태그 "권한 변경"을 할당하고 이 파일을 사용자 "Joan Smith"에게 할당하여 문제 해결 방법을 결정할 수 있습니다. 문제를 해결하면 상태 태그를 "완료됨"으로 변경할 수 있습니다.

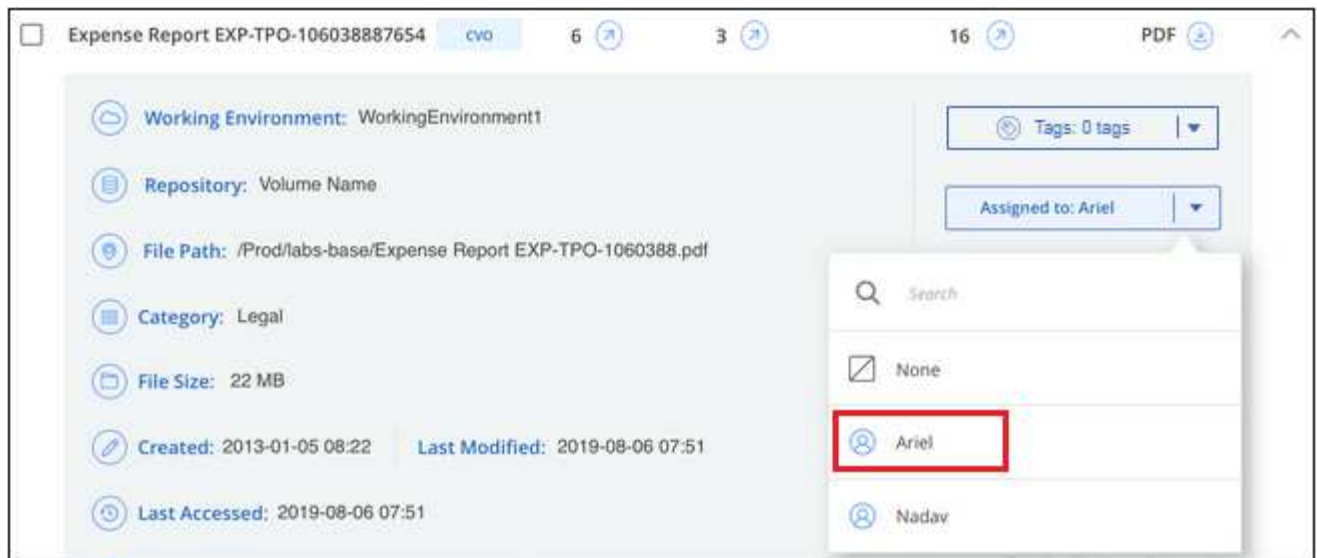
사용자 이름은 파일 메타데이터의 일부로 파일에 추가되지 않습니다. Cloud Data Sense를 사용할 때 Cloud Manager 사용자만 이 이름을 볼 수 있습니다.

조사 페이지의 새 필터를 사용하면 "담당자" 필드에 동일한 사람이 있는 모든 파일을 쉽게 볼 수 있습니다.

사용자를 단일 파일에 할당하려면 다음을 수행합니다.

단계

1. 데이터 조사 결과 창에서 을 클릭합니다 ▼ 파일 메타데이터 세부 정보를 확장합니다.
2. Assigned to * 필드를 클릭하고 사용자 이름을 선택합니다.



사용자 이름이 파일 메타데이터에 나타납니다.

사용자를 여러 파일에 할당하려면:

단계

1. 데이터 조사 결과 창에서 사용자에게 할당할 파일을 선택합니다.

2345 items							Tags	Assign to	Label	Copy	Move	Delete
<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type						
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-10603887654	cvo	6	3	16	PDF						
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-10603887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-10603887654	cvo	6	3	6	PDF						
<input type="checkbox"/>	Expense Report EXP-TPO-10603887654	cvo	6	3	6	PDF						

◦ 개별 파일을 선택하려면 각 파일(☒ Volume_1)를 클릭합니다.

◦ 현재 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭합니다.

2. 버튼 모음에서 * Assign to * (할당 대상 *)를 클릭하고 사용자 이름을 선택합니다.



선택한 모든 파일의 메타데이터에 사용자가 추가됩니다.

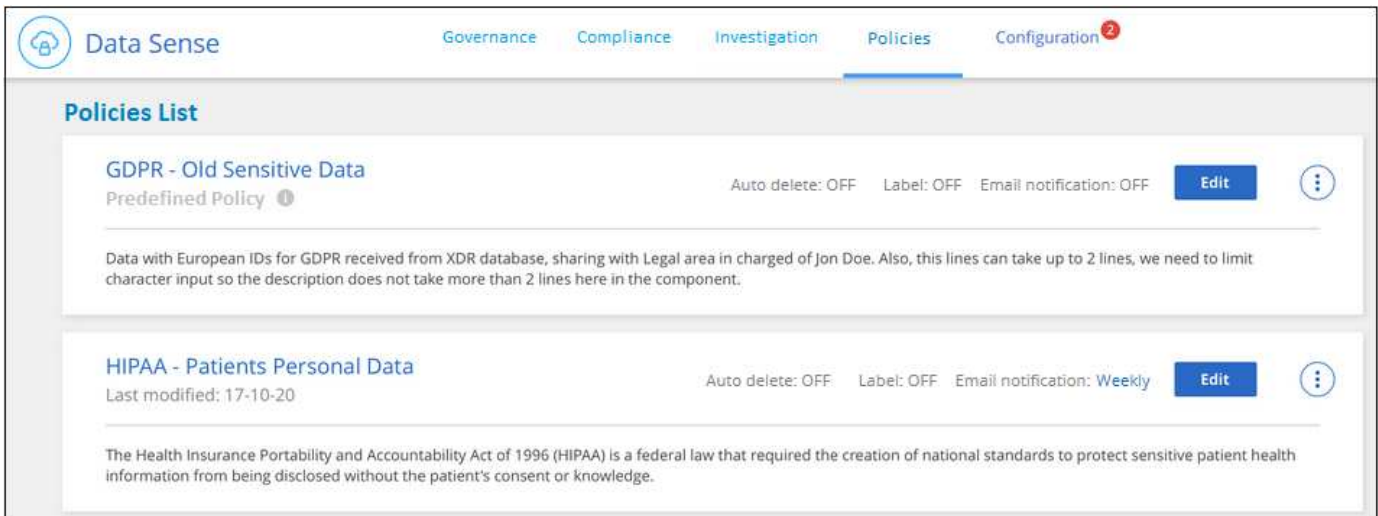
정책을 사용하여 데이터 제어

정책은 자주 요청하는 규정 준수 쿼리에 대한 조사 페이지에 검색 결과를 제공하는 사용자 지정 필터의 즐겨찾기 목록과 같습니다. Cloud Data Sense는 일반적인 고객 요청에 따라 미리 정의된 정책 세트를 제공합니다. 조직에 특정한 검색 결과를 제공하는 사용자 지정 정책을 만들 수 있습니다.

정책은 다음과 같은 기능을 제공합니다.

- [사전 정의된 정책](#) 구성하는 방법에 대해 설명합니다
- 고유한 사용자 지정 정책을 만들 수 있습니다
- 클릭 한 번으로 정책의 결과가 포함된 조사 페이지를 시작합니다
- 특정 중요 정책에서 결과를 반환할 때 Cloud Manager 사용자에게 이메일 경고를 보내 데이터를 보호하기 위한 알림을 받을 수 있습니다
- AIP(Azure Information Protection) 레이블을 정책에 정의된 조건과 일치하는 모든 파일에 자동으로 할당합니다
- 특정 정책이 결과를 반환하면 데이터를 자동으로 보호할 수 있도록 파일을 자동으로 삭제합니다(하루에 한 번)

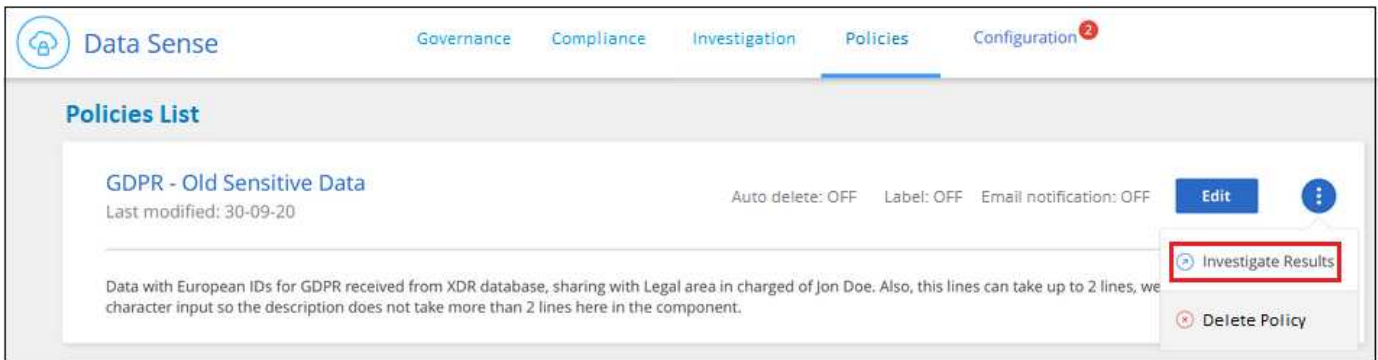
규정 준수 대시보드의 * Policies * 탭에는 이 Cloud Data Sense 인스턴스에서 사용할 수 있는 사전 정의된 정책과 맞춤형 정책이 모두 나열됩니다.



또한 조사 페이지의 필터 목록에 정책이 표시됩니다.

조사 페이지에서 정책 결과를 봅니다

조사 페이지에 정책의 결과를 표시하려면 을 클릭합니다 . 단추를 클릭하여 특정 정책을 선택한 다음 * 결과 조사 * 를 선택합니다.



사용자 지정 정책을 만드는 중입니다

조직에 맞는 검색 결과를 제공하는 사용자 지정 정책을 만들 수 있습니다.

단계

1. 데이터 조사 페이지에서 사용할 필터를 모두 선택하여 검색을 정의합니다. 을 참조하십시오 "데이터 조사 페이지의 데이터 필터링" 를 참조하십시오.
2. 원하는 방식으로 모든 필터 특성을 찾은 후 * 이 검색에서 정책 생성 * 을 클릭합니다.



3. 정책의 이름을 지정하고 정책에서 수행할 수 있는 다른 작업을 선택합니다.

- a. 고유한 이름과 설명을 입력합니다.
- b. 필요한 경우 정책 매개 변수와 일치하는 파일을 자동으로 삭제하려면 확인란을 선택합니다. 에 대해 자세히 알아보십시오 ["정책을 사용하여 소스 파일을 삭제하는 중입니다"](#).
- c. 필요한 경우 알림 이메일을 Cloud Manager 사용자에게 보내려면 확인란을 선택하고 이메일을 보낼 간격을 선택합니다. 에 대해 자세히 알아보십시오 ["정책 결과에 따라 이메일 알림을 보냅니다"](#).
- d. 필요한 경우 정책 매개 변수와 일치하는 파일에 AIP 레이블을 자동으로 할당하려면 확인란을 선택하고 레이블을 선택합니다. (이미 AIP 레이블을 통합한 경우에만 해당됩니다. 에 대해 자세히 알아보십시오 ["AIP 레이블"](#)참조)
- e. Create Policy * 를 클릭합니다.

Create Policy

This will create a new Policy according to the current selected filters and search term. You can view or delete this later from the "Policies" tab.

Note it may take up to 15 minutes for results to be displayed for a new Policy.

Name this Policy

New Policy to view all files that were created over 60 days ago

Give it a detailed description that explains what it searches for

See if any files greater than 60 days old should be deleted from the system

☐ Automatically delete files that match this policy (Every Day)

☒ Send email updates about this Policy to Cloud Manager users on this account every Day

☐ Automatically label this Policy's matches with: Select a label

Create Policy Cancel

새 정책이 정책 탭에 나타납니다.

규정을 준수하지 않는 데이터가 발견되면 이메일 경고를 보냅니다

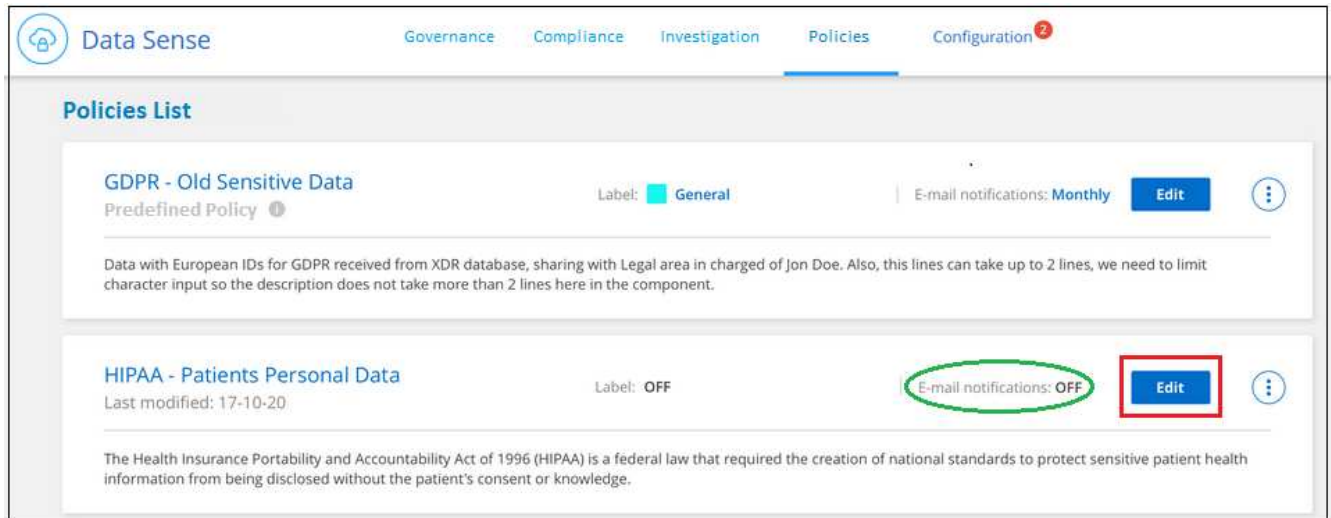
Cloud Data Sense는 특정 중요 정책이 결과를 반환할 때 클라우드 관리자 사용자에게 이메일 경고를 보내 데이터를 보호하기 위한 알림을 받을 수 있도록 합니다. 매일, 매주 또는 매월 이메일 알림을 보내도록 선택할 수 있습니다.

정책을 만들거나 정책을 편집할 때 이 설정을 구성할 수 있습니다.

기존 정책에 전자 메일 업데이트를 추가하려면 다음 단계를 따릅니다.

단계

1. 정책 목록 페이지에서 이메일 설정을 추가(또는 변경)할 정책에 대해 * 편집 * 을 클릭합니다.



2. 정책 편집 페이지에서 Cloud Manager 사용자에게 알림 이메일을 보내려면 확인란을 선택하고 이메일을 보낼 간격을 선택합니다(예: 매 * 주 *).

3. 정책 저장 * 을 클릭하면 이메일이 전송되는 간격이 정책 설명에 표시됩니다.

정책의 결과가 있는 경우 첫 번째 이메일이 전송되지만 정책 기준을 충족하는 파일이 있는 경우에만 전송됩니다. 알림 이메일에는 개인 정보가 전송되지 않습니다. 이메일에는 정책 기준과 일치하는 파일이 있으며 정책 결과에 대한 링크가 표시됩니다.

정책 편집

정책 유형에 따라 정책의 특정 부분을 수정할 수 있습니다.

- 사용자 지정 정책 - *Name*, *Description*, 이메일 알림 전송 여부 및 AIP 레이블 추가 여부를 수정할 수 있습니다.
- 사전 정의된 정책 - 이메일 알림 전송 여부와 AIP 레이블 추가 여부만 수정할 수 있습니다.




사용자 지정 정책의 필터 매개 변수를 변경해야 하는 경우 원하는 매개 변수를 사용하여 새 정책을 만든 다음 이전 정책을 삭제해야 합니다.

정책을 수정하려면 * 편집 * 버튼을 클릭하고 _정책 편집_ 페이지에 변경 사항을 입력한 다음 * 정책 저장 * 을 클릭합니다.

정책을 삭제하는 중입니다

사용자 지정 정책이 더 이상 필요하지 않은 경우 만든 모든 사용자 지정 정책을 삭제할 수 있습니다. 미리 정의된 정책은 삭제할 수 없습니다.

정책을 삭제하려면 를 클릭합니다  특정 정책의 버튼 * 정책 삭제 * 를 클릭한 다음 확인 대화 상자에서 * 정책 삭제 * 를 다시 클릭합니다.

사전 정의된 정책 목록입니다

Cloud Data Sense는 다음과 같은 시스템 정의 정책을 제공합니다.

이름	설명	논리
S3 공개된 프라이빗 데이터	S3 개인 정보 또는 민감한 개인 정보가 포함된 개체(공개 공개 공개 공개 공개 읽기 액세스 포함).	S3 공용 및 개인 정보 또는 민감한 개인 정보 포함
PCI DSS – 30일 이상 오래된 데이터	신용 카드 정보가 포함된 파일로, 30일 전에 마지막으로 수정되었습니다.	신용 카드가 포함되어 있으며 30일 동안 마지막으로 수정한 것입니다
HIPAA – 30일 이상 오래된 데이터	30일 전에 마지막으로 수정된 상태 정보가 포함된 파일	건강 데이터(HIPAA 보고서와 같은 방식으로 정의) 및 30일 동안 마지막으로 수정된 상태 데이터가 포함됩니다
프라이빗 데이터가 7년 이상 오래되었습니다	7년 전에 마지막으로 수정한 개인 정보 또는 민감한 개인 정보가 포함된 파일	7년 전에 마지막으로 수정한 개인 정보 또는 민감한 개인 정보가 포함된 파일
GDPR – 유럽 시민	EU 국가의 시민권자 또는 EU 국가의 시민을 식별할 수 있는 DB 테이블의 5개 이상의 식별자를 포함하는 파일.	한 국가의 EU 식별자가 포함된 열의 15% 이상이 포함된 행을 포함하는 (1) EU 시민 또는 DB 테이블의 5개 이상의 식별자를 포함하는 파일. (유럽 국가의 국가 식별자 중 하나. 브라질, 캘리포니아, 미국 SSN, 이스라엘, 남아프리카 제외)
CCPA – 캘리포니아 주민	이 식별자가 포함된 10개 이상의 California Driver의 라이선스 식별자 또는 DB 테이블을 포함하는 파일입니다.	10개 이상의 캘리포니아 드라이버 라이선스 식별자 또는 캘리포니아 드라이버 라이선스가 포함된 DB 테이블이 포함된 파일
데이터 주체 이름 – 높은 위험	데이터 주체 이름이 50개 이상인 파일	데이터 주체 이름이 50개 이상인 파일
이메일 주소 – 높은 위험	이메일 주소가 50개 이상인 파일 또는 이메일 주소가 포함된 행의 50% 이상이 있는 DB 열	이메일 주소가 50개 이상인 파일 또는 이메일 주소가 포함된 행의 50% 이상이 있는 DB 열
개인 데이터 – 높은 위험	개인 데이터 식별자가 20개가 넘는 파일 또는 개인 데이터 식별자가 포함된 행의 50% 이상이 포함된 DB 열	20개가 넘는 개인 파일 또는 개인 행이 50% 이상 포함된 DB 열

이름	설명	논리
민감한 개인 데이터 – 높은 위험	중요한 개인 데이터 식별자가 20개가 넘는 파일 또는 중요한 개인 데이터가 포함된 행의 50% 이상이 포함된 DB 열	20개 이상의 민감한 개인 파일이 있는 파일 또는 중요한 개인 정보가 포함된 행의 50% 이상이 있는 DB 열

개인 데이터 관리

Cloud Data Sense는 여러 가지 방법으로 개인 데이터를 관리할 수 있습니다. 일부 기능을 사용하면 데이터 마이그레이션을 쉽게 준비할 수 있을 뿐만 아니라 다른 기능도 데이터를 변경할 수 있습니다.

- 특정 데이터의 복사본을 만들어 다른 NFS 위치로 이동하려는 경우 대상 NFS 공유에 파일을 복사할 수 있습니다.
- 클론 복제된 새 볼륨의 소스 볼륨에서 선택한 파일만 포함하여 ONTAP 볼륨을 새 볼륨으로 복제할 수 있습니다. 이 기능은 데이터를 마이그레이션하고 원본 볼륨에서 특정 파일을 제외하려는 경우에 유용합니다.
- 소스 리포지토리에서 특정 대상 위치의 디렉토리로 파일을 복사 및 동기화할 수 있습니다. 이 기능은 소스 파일에 대한 최종 작업이 아직 남아 있는 동안 소스 시스템 간에 데이터를 마이그레이션하는 경우에 유용합니다.
- 데이터 센스에서 스캔 중인 소스 파일을 모든 NFS 공유로 이동할 수 있습니다.
- 안전하지 않거나 위험한 것으로 보이는 파일을 스토리지 시스템에 남겨 두거나 중복으로 식별한 경우 삭제할 수 있습니다.



- 이 섹션에 설명된 기능은 데이터 소스에서 전체 분류 검사를 수행하도록 선택한 경우에만 사용할 수 있습니다. 매핑 전용 스캔이 있는 데이터 원본은 파일 수준 세부 정보를 표시하지 않습니다.
- Google Drive 계정의 데이터는 현재 이러한 기능을 사용할 수 없습니다.

원본 파일을 복사하는 중입니다

데이터 센스에서 스캔 중인 모든 소스 파일을 복사할 수 있습니다. 달성하려는 목표에 따라 세 가지 유형의 복사 작업이 있습니다.

- * 동일 또는 다른 볼륨 또는 데이터 소스에서 대상 NFS 공유로 파일 * 복사

특정 데이터의 복사본을 만들어 다른 NFS 위치로 이동하려는 경우 유용합니다.

- * 동일한 애그리게이트의 새 볼륨에 ONTAP 볼륨 * 을 클론 복제하지만 새로운 클론 복제된 볼륨의 소스 볼륨에서 선택한 파일만 포함됩니다.

이 기능은 데이터를 마이그레이션하고 원본 볼륨에서 특정 파일을 제외하려는 경우에 유용합니다. 이 작업은 를 사용합니다 "플렉스클론" 볼륨을 빠르게 복제한 다음 * 선택하지 않은 * 파일을 제거하는 기능입니다.

- * 단일 소스 저장소(ONTAP 볼륨, S3 버킷, NFS 공유 등)의 파일 * 을 특정 대상(타겟) 위치의 디렉토리로 복사 및 동기화합니다.

이 기능은 소스 시스템 간에 데이터를 마이그레이션하는 경우에 유용합니다. 초기 복사 후 서비스는 사용자가 설정한 일정에 따라 변경된 데이터를 동기화합니다. 이 작업은 를 사용합니다 "NetApp Cloud Sync를 참조하십시오" 소스에서 타겟으로 데이터를 복제 및 동기화하는 기능

소스 파일을 **NFS** 공유에 복사하는 중입니다

Data Sense에서 스캔 중인 소스 파일을 모든 NFS 공유로 복사할 수 있습니다. NFS 공유는 데이터 센스에 통합할 필요가 없으며 선택한 모든 파일이 "<host_name>:/<share_path>" 형식으로 복사될 NFS 공유의 이름을 알아야 합니다.



데이터베이스에 있는 파일은 복사할 수 없습니다.

요구 사항

- 파일을 복사하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 파일을 복사하려면 대상 NFS 공유에서 Data Sense 인스턴스에서 액세스할 수 있어야 합니다.
- 한 번에 최대 100,000개의 파일을 복사할 수 있습니다.

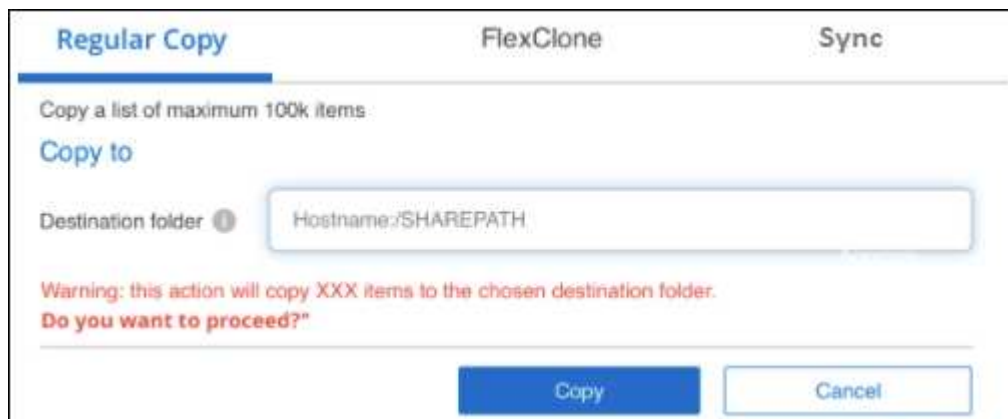
단계

1. 데이터 조사 결과 창에서 복사할 파일을 선택하고 * 복사 * 를 클릭합니다.



- 개별 파일을 선택하려면 각 파일(☒ Volume_1)를 클릭합니다.
- 현재 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭합니다.
- 모든 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭한 다음 팝업 메시지에서 [All 20 Items on this page selected](#) [Select all Items in list \(63K Items\)](#) 목록에서 * 모든 항목 선택(xxx개 항목) * 을 클릭합니다.

2. 파일 복사 대화 상자에서 * 일반 복사 * 탭을 선택합니다.



3. 선택한 모든 파일이 복사될 NFS 공유의 이름을 "<host_name>:/<share_path>" 형식으로 입력하고 * Copy * 를 클릭합니다.

복사 작업 상태와 함께 대화 상자가 나타납니다.

에서 복사 작업의 진행률을 볼 수 있습니다 [작업 상태 창](#).

파일의 메타데이터 세부 정보를 볼 때 개별 파일을 복사할 수도 있습니다. 파일 복사 * 를 클릭하기만 하면 됩니다.



볼륨 데이터를 새 볼륨에 클로닝

NetApp_FlexClone_기능을 사용하여 데이터 센스에서 스캔 중인 기존 ONTAP 볼륨을 클론 복제할 수 있습니다. 이렇게 하면 선택한 파일만 포함하면서 볼륨을 빠르게 복제할 수 있습니다. 이 기능은 데이터를 마이그레이션하는 동안 원본 볼륨에서 특정 파일을 제외하려는 경우 또는 테스트할 볼륨의 복사본을 만들려는 경우에 유용합니다.

새 볼륨은 소스 볼륨과 동일한 애그리게이트에 생성됩니다. 이 작업을 시작하기 전에 aggregate에서 이 새 볼륨을 위한 공간이 충분한지 확인하십시오. 필요한 경우 스토리지 관리자에게 문의하십시오.

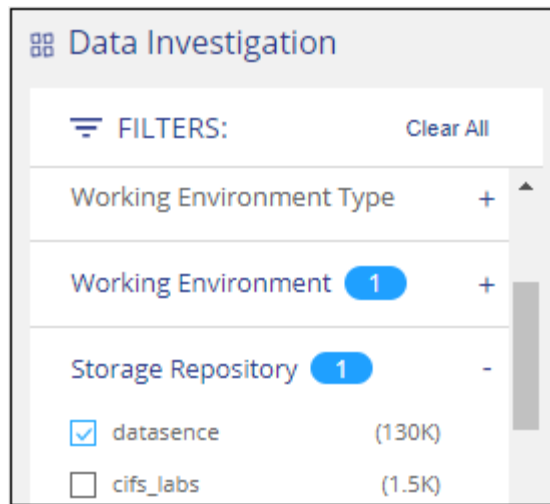
- 참고: * FlexGroup 볼륨은 FlexClone에서 지원하지 않으므로 복제할 수 없습니다.

요구 사항

- 파일을 복사하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 선택한 모든 파일은 동일한 볼륨에서 가져온 것이어야 하며 볼륨이 온라인 상태여야 합니다.
- 볼륨은 Cloud Volumes ONTAP 또는 사내 ONTAP 시스템이어야 합니다. 현재 다른 데이터 원본은 지원되지 않습니다.
- FlexClone 라이선스가 클러스터에 설치되어 있어야 합니다. 이 라이선스는 Cloud Volumes ONTAP 시스템에 기본적으로 설치됩니다.

단계

1. 데이터 조사 창에서 단일 * 작업 환경 * 과 단일 * 저장소 * 를 선택하여 모든 파일이 동일한 ONTAP 볼륨에서 생성되도록 필터를 만듭니다.



새 볼륨에 복제할 파일만 표시되도록 다른 필터를 적용합니다.

2. 조사 결과 창에서 복제할 파일을 선택하고 * 복사 * 를 클릭합니다.



- 개별 파일을 선택하려면 각 파일(☒ Volume_1)를 클릭합니다.
- 현재 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭합니다.
- 모든 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭한 다음 팝업 메시지에서 [All 20 Items on this page selected](#) [Select all Items in list \(63K Items\)](#) 목록에서 * 모든 항목 선택(xxx개 항목) * 을 클릭합니다.

3. 파일 복사 대화 상자에서 * FlexClone * 탭을 선택합니다. 이 페이지에는 볼륨에서 복제할 총 파일 수(선택한 파일)와 클론 복제된 볼륨에서 포함/삭제되지 않은 파일 수(선택하지 않은 파일)가 표시됩니다.

4. 새 볼륨의 이름을 입력하고 * FlexClone * 을 클릭합니다.

클론 작업의 상태가 표시된 대화 상자가 나타납니다.

클론 복제된 새 볼륨은 소스 볼륨과 동일한 애그리게이트에 생성됩니다.

에서 클론 작업의 진행률을 볼 수 있습니다 [작업 상태 창](#).

소스 볼륨이 있는 작업 환경에 대해 데이터 센스를 활성화하면 처음에 * 모든 볼륨 매핑 * 또는 * 모든 볼륨 매핑 및 분류 * 를 선택한 경우 데이터 센스에서 복제된 새 볼륨을 자동으로 스캔합니다. 처음에 이러한 선택 항목을 사용하지 않은 경우 이 새 볼륨을 스캔하려면 가 필요합니다 ["수동으로 볼륨에서 스캔을 활성화합니다"](#).

소스 파일을 대상 시스템에 복사 및 동기화 중입니다

Data Sense가 스캔 중인 소스 파일을 지원되는 비정형 데이터 소스에서 특정 대상 위치의 디렉토리로 복사할 수 있습니다 (["Cloud Sync에서 지원하는 타겟 위치입니다"](#))를 클릭합니다. 초기 복제 후에는 구성된 일정에 따라 파일에서 변경된 모든 데이터가 동기화됩니다.

이 기능은 소스 시스템 간에 데이터를 마이그레이션하는 경우에 유용합니다. 이 작업은 를 사용합니다 ["NetApp Cloud Sync를 참조하십시오"](#) 소스에서 타겟으로 데이터를 복제 및 동기화하는 기능



데이터베이스, OneDrive 계정 또는 SharePoint 계정에 있는 파일은 복사 및 동기화할 수 없습니다.

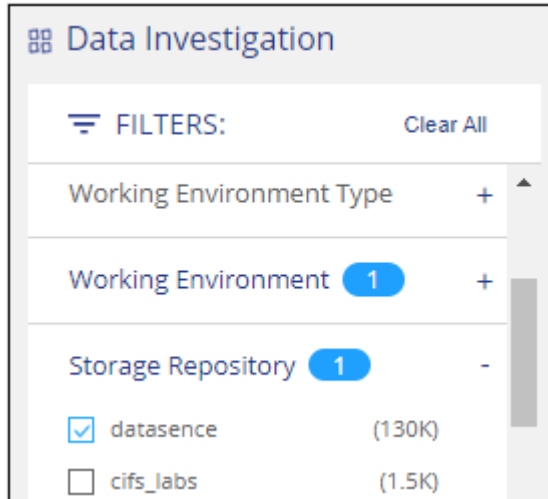
요구 사항

- 파일을 복사 및 동기화하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 선택한 모든 파일은 동일한 소스 저장소(ONTAP 볼륨, S3 버킷, NFS 또는 CIFS 공유 등)에서 가져온 것이어야 합니다.
- Cloud Sync 서비스를 활성화하고 소스 시스템과 타겟 시스템 간에 파일을 전송하는 데 사용할 수 있는 데이터 브로커를 하나 이상 구성해야 합니다. 부터 시작되는 Cloud Sync 요구 사항을 검토합니다 ["빠른 시작 설명"](#).

Cloud Sync 서비스에는 동기화 관계에 대한 별도의 서비스 요금이 부과되며, 클라우드에 데이터 브로커를 구축할 경우 리소스 요금이 발생합니다.

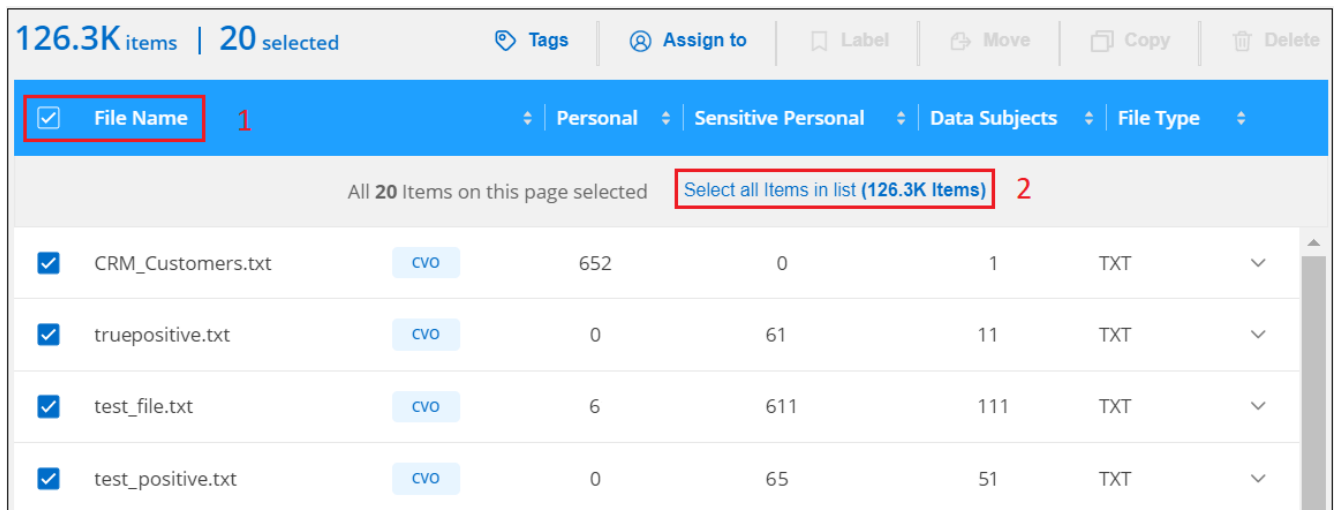
단계

1. 데이터 조사 창에서 하나의 * 작업 환경 * 과 하나의 * 저장소 저장소 * 를 선택하여 모든 파일이 동일한 리포지토리의 파일인지 확인하는 필터를 만듭니다.

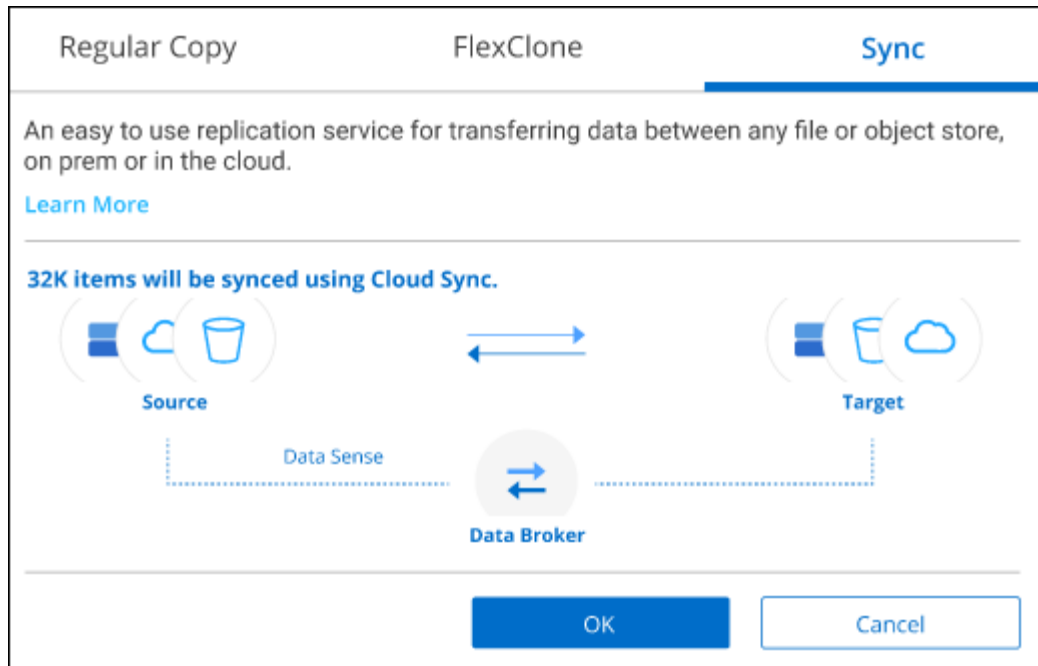


대상 시스템에 복사 및 동기화할 파일만 표시되도록 다른 필터를 적용합니다.

2. 조사 결과 창에서 제목 행(☒ File Name)를 선택한 다음 팝업 메시지를 표시합니다
All 20 Items on this page selected Select all Items in list (63K Items) 목록에서 모든 항목 선택(xxx개 항목) * 을 클릭한 다음 * 복사 * 를 클릭합니다.



3. 파일 복사 대화 상자에서 * 동기화 * 탭을 선택합니다.



4. 선택한 파일을 대상 위치에 동기화하려면 * 확인 * 을 클릭합니다.

Cloud Sync UI는 Cloud Manager에서 열립니다.

동기화 관계를 정의하라는 메시지가 표시됩니다. 소스 시스템은 데이터 센스에서 이미 선택한 리포지토리와 파일을 기반으로 미리 채워집니다.

5. 대상 시스템을 선택한 다음 사용하려는 데이터 브로커를 선택(또는 생성)해야 합니다. 부터 시작되는 Cloud Sync 요구 사항을 검토합니다 **"빠른 시작 설명"**.

파일이 대상 시스템에 복사되고 사용자가 정의한 일정에 따라 동기화됩니다. 1회 동기화를 선택하면 파일이 한 번만 복사되고 동기화됩니다. 주기적 동기화를 선택하면 일정에 따라 파일이 동기화됩니다. 필터를 사용하여 만든 쿼리와 일치하는 새 파일이 소스 시스템에 추가되는 경우 해당 _new_files는 대상에 복사되고 나중에 동기화됩니다.

데이터 센스에서 일반적인 Cloud Sync 작업을 호출하면 일부 작업이 비활성화됩니다.

- 소스 * 에서 파일 삭제 또는 * 대상 * 에서 파일 삭제 버튼을 사용할 수 없습니다.
- 보고서 실행이 비활성화됩니다.

소스 파일을 **NFS** 공유로 이동하는 중입니다

데이터 센스에서 스캔 중인 소스 파일을 모든 NFS 공유로 이동할 수 있습니다. NFS 공유는 데이터 센스에 통합할 필요가 없습니다(참조 **"파일 공유를 검색하는 중입니다"**)를 클릭합니다.



데이터베이스에 있는 파일은 이동할 수 없습니다.

파일을 이동하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.

파일을 이동하려면 NFS 공유를 통해 Data Sense 인스턴스에서 액세스할 수 있어야 합니다.

단계

1. 데이터 조사 결과 창에서 이동할 파일을 선택합니다.

2345 items

Tags

Assign to

Label

Copy

Move

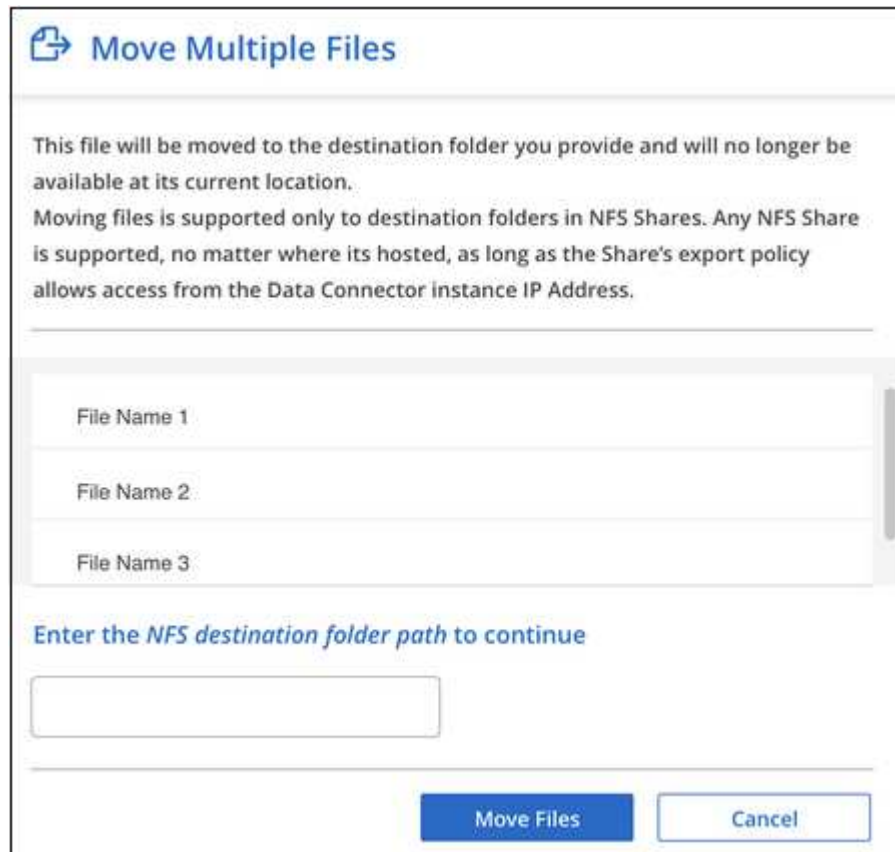
Delete

<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type	
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼

◦ 개별 파일을 선택하려면 각 파일(☒ Volume_1)를 클릭합니다.

◦ 현재 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭합니다.

2. 단추 모음에서 * 이동 * 을 클릭합니다.



Move Multiple Files

This file will be moved to the destination folder you provide and will no longer be available at its current location.
Moving files is supported only to destination folders in NFS Shares. Any NFS Share is supported, no matter where its hosted, as long as the Share's export policy allows access from the Data Connector instance IP Address.

File Name 1
File Name 2
File Name 3

Enter the *NFS destination folder path* to continue

Move Files **Cancel**

3. Move Files 대화 상자에서 선택한 모든 파일이 "<host_name>:/<share_path>" 형식으로 이동될 NFS 공유의 이름을 입력하고 * Move Files * 를 클릭합니다.

파일의 메타데이터 세부 정보를 볼 때 개별 파일을 이동할 수도 있습니다. 파일 이동 * 을 클릭하기만 하면 됩니다.



원본 파일을 삭제하는 중입니다

안전하지 않거나 너무 위험한 소스 파일을 스토리지 시스템에 남겨 두거나 중복으로 식별한 경우 영구적으로 제거할 수 있습니다. 이 작업은 영구적이며 실행 취소 또는 복원이 없습니다.

조사 창에서 파일을 수동으로 삭제하거나 정책을 자동으로 사용할 수 있습니다.



데이터베이스에 있는 파일은 삭제할 수 없습니다.

파일을 삭제하려면 다음 권한이 필요합니다.

- NFS 데이터의 경우 - 내보내기 정책을 쓰기 권한으로 정의해야 합니다.
- CIFS 데이터의 경우 - CIFS 자격 증명에 쓰기 권한이 있어야 합니다.
- S3 데이터의 경우 - IAM 역할에는 's3:DeleteObject' 권한이 포함되어야 합니다.

소스 파일을 수동으로 삭제하는 중입니다

요구 사항

- 파일을 삭제하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 한 번에 최대 100,000개의 파일을 삭제할 수 있습니다.

단계

1. 데이터 조사 결과 창에서 삭제할 파일을 선택합니다.



- 개별 파일을 선택하려면 각 파일(☒ Volume_1)를 클릭합니다.
- 현재 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭합니다.
- 모든 페이지의 모든 파일을 선택하려면 제목 행(☒ File Name)를 클릭한 다음 팝업 메시지에서 [All 20 Items on this page selected](#) [Select all Items in list \(63K Items\)](#) 목록에서 * 모든 항목 선택(xxx개 항목) * 을 클릭합니다.

2. 버튼 모음에서 * 삭제 * 를 클릭합니다.

3. 삭제 작업은 영구적이므로 후속 _Delete File_ 대화 상자에 " * 영구 삭제 * "를 입력하고 * 파일 삭제 * 를 클릭해야 합니다.

에서 삭제 작업의 진행률을 볼 수 있습니다 [작업 상태 창](#).

파일의 메타데이터 세부 정보를 볼 때 개별 파일을 삭제할 수도 있습니다. 파일 삭제 * 를 클릭하기만 하면 됩니다.



정책을 사용하여 소스 파일을 자동으로 삭제합니다

사용자 지정 정책을 만들어 정책과 일치하는 파일을 삭제할 수 있습니다. 예를 들어, 지난 30일 동안 데이터 센스에서 검색한 중요한 정보가 포함된 파일을 삭제할 수 있습니다.

계정 관리자만 파일을 자동으로 삭제하는 정책을 만들 수 있습니다.



정책과 일치하는 모든 파일이 하루에 한 번 영구적으로 삭제됩니다.

단계

1. 데이터 조사 페이지에서 사용할 필터를 모두 선택하여 검색을 정의합니다. 을 참조하십시오 ["데이터 조사 페이지의 데이터 필터링"](#) 를 참조하십시오.
2. 원하는 방식으로 모든 필터 특성을 찾은 후 * 이 검색에서 정책 생성 * 을 클릭합니다.
3. 정책의 이름을 지정하고 정책에서 수행할 수 있는 다른 작업을 선택합니다.
 - a. 고유한 이름과 설명을 입력합니다.
 - b. "이 정책과 일치하는 파일을 자동으로 삭제" 확인란을 선택하고 * 영구적으로 삭제 * 를 입력하여 이 정책에 따라 파일을 영구적으로 삭제할 것인지 확인합니다.
 - c. Create Policy * 를 클릭합니다.

Create Policy

This will create a new Policy according to the current selected filters and search term.
You can view or delete this later from the "Policies" tab.

Note it may take up to 15 minutes for results to be displayed for a new Policy.

Name this Policy

Delete files with sensitive data

Give it a detailed description that explains what it searches for

Delete files that contain sensitive information and that were discovered in the past 30 days

☒ Automatically delete files that match this policy (Every Day)
Type "permanently delete" to continue with the deletion.

permanently delete

☐ Send email updates about this Policy to Cloud Manager users on this account every Day

☐ Automatically label this Policy's matches with: Select a label

Create Policy Cancel

새 정책이 정책 탭에 나타납니다. 정책과 일치하는 파일은 정책이 실행될 때 하루에 한 번 삭제됩니다.

에서 삭제된 파일 목록을 볼 수 있습니다 [작업 상태 창](#).

준수 작업의 상태 보기

100개의 파일을 삭제하는 등 여러 파일에 대해 조사 결과 창에서 작업을 실행할 경우 프로세스에 약간의 시간이 걸릴 수 있습니다. 모든 파일에 언제 적용되었는지 알 수 있도록 **_Action Status_** 창에서 이러한 비동기 작업의 상태를 모니터링할 수 있습니다. 이를 통해 성공적으로 완료된 작업, 현재 진행 중인 작업 및 실패한 작업을 볼 수 있으므로 문제를 진단하고 해결할 수 있습니다.

상태는 다음과 같습니다.

- 완료되었습니다
- 진행 중
- 대기열에 있습니다
- 취소됨
- 실패했습니다

참고: "대기 중" 또는 "진행 중" 상태의 작업은 취소할 수 있습니다.

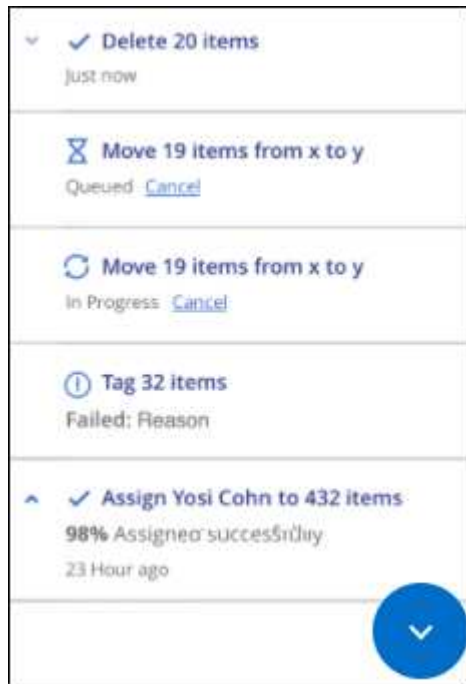
단계

1.

데이터 감지 UI의 오른쪽 하단에 * 작업 상태 * 버튼이 있습니다



2. 이 버튼을 클릭하면 최근 20개 작업이 나열됩니다.



작업 이름을 클릭하여 해당 작업에 해당하는 세부 정보를 볼 수 있습니다.

Data Fusion를 사용하여 개인 데이터 식별자를 추가합니다

Data Fusion _ 라는 기능을 사용하면 조직의 데이터를 스캔하여 데이터베이스의 고유 식별자가 파일 또는 기타 데이터베이스에서 검색되는지 여부를 확인할 수 있습니다. 기본적으로 클라우드 데이터 감지 스캔에서 식별된 "개인 데이터" 목록을 만듭니다. 이렇게 하면 잠재적으로 중요한 데이터가 _all_your 파일에 있는 위치를 전체적으로 파악할 수 있습니다.

자체 데이터베이스를 스캔하기 때문에 데이터가 저장된 언어가 향후 Cloud Data Sense 스캔에서 데이터를 식별하는 데 사용됩니다.



이 섹션에 설명된 기능은 데이터 소스에서 전체 분류 검사를 수행하도록 선택한 경우에만 사용할 수 있습니다. 매핑 전용 스캔이 있는 데이터 원본은 파일 수준 세부 정보를 표시하지 않습니다.

데이터베이스에서 사용자 지정 개인 데이터 식별자를 만듭니다

데이터베이스 테이블에서 특정 열 또는 열을 선택하여 클라우드 데이터 센스가 해당 스캔에서 찾을 추가 식별자를 선택할 수 있습니다. 예를 들어, 아래 다이어그램은 Data Fusion를 사용하여 볼륨, 버킷 및 데이터베이스를 검사하여 Oracle 데이터베이스에서 모든 고객 ID를 확인하는 방법을 보여 줍니다.

Databases -- Structured Data

Database: Oracle
Schema: Accounts
Table: Customers
Column: Customer ID

Account	Name	Customer ID	Address
1234	ABC Co	135876	125 Main St
1235	XYZ Co	213536	35A Brick R
1236	Cat Co	359264	55 Wind Av
1237	Dog Co	472637	11025 Cor
1238	Zebra Co	582455	36 Sahara
...

Scan your volumes and buckets for occurrences of the Customer IDs in your Oracle database

Files -- Unstructured Data

File in Volume 1

```
XXXXXXXXXXXXX
xx213536xxx
XXXXXXXXXXXXX
xx472637xxx
XXXXXXXXXXXXX
XXXXXXXXXXXXX
```

File in Volume 2

```
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
xxx472637xx
```

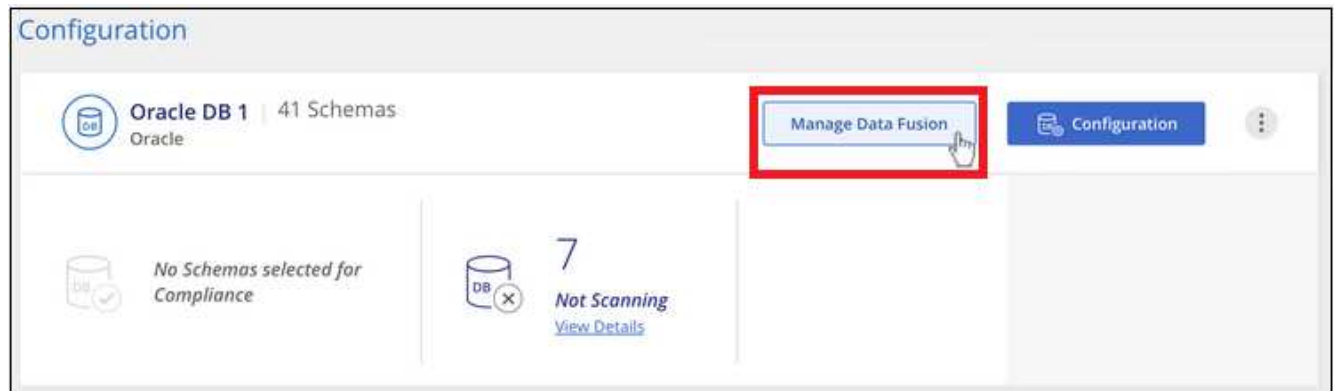
File in Bucket 1

```
XXXXXXXXXXXXX
XXXXXXXXXXXXX
xx213536xxx
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
```

보시다시피, 2개의 볼륨과 1개의 S3 버킷에서 2개의 고유 고객 ID가 발견되었습니다. 데이터베이스 테이블의 모든 일치 항목도 식별됩니다.

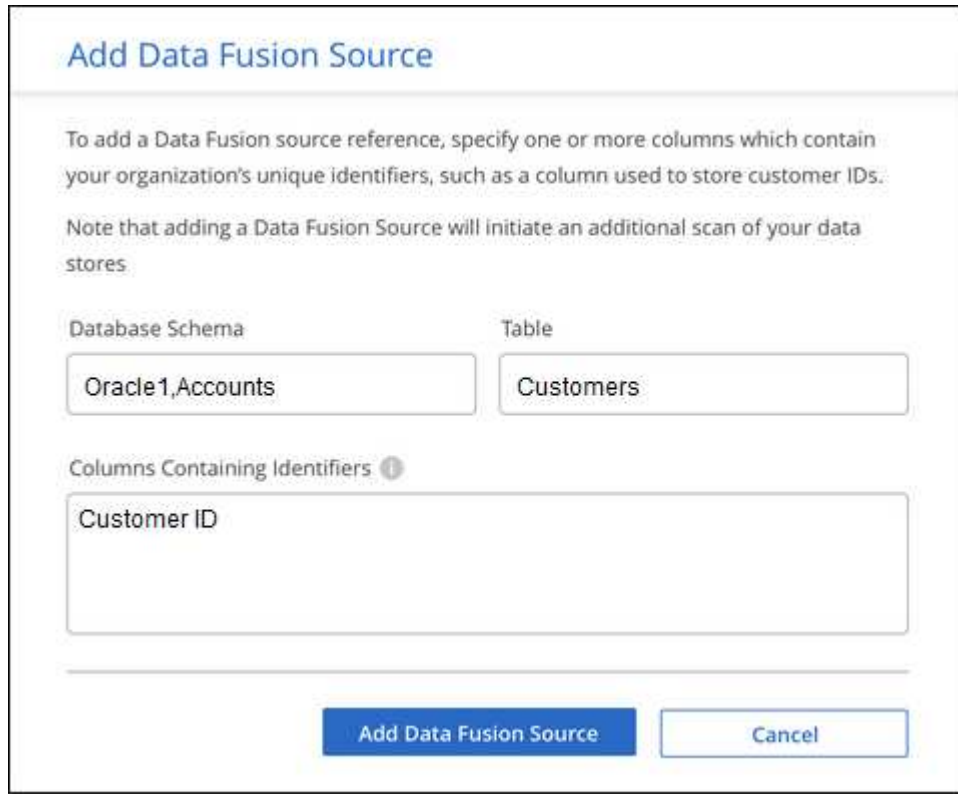
이(가) 있어야 합니다 "하나 이상의 데이터베이스 서버가 추가되었습니다" 클라우드 데이터 센스에 데이터를 추가하려면 먼저 Fusion 소스를 추가해야 합니다.

1. 구성 페이지에서 소스 데이터가 있는 데이터베이스에서 * 데이터 관리 Fusion * 를 클릭합니다.



2. 다음 페이지에서 * 데이터 Fusion 소스 추가 * 를 클릭합니다.
3. Add Data Fusion Source _ 페이지에서 다음을 수행합니다.
 - a. 드롭다운 메뉴에서 데이터베이스 스키마를 선택합니다.
 - b. 해당 스키마에 테이블 이름을 입력합니다.
 - c. 사용할 고유 식별자가 포함된 열 또는 열을 입력합니다.

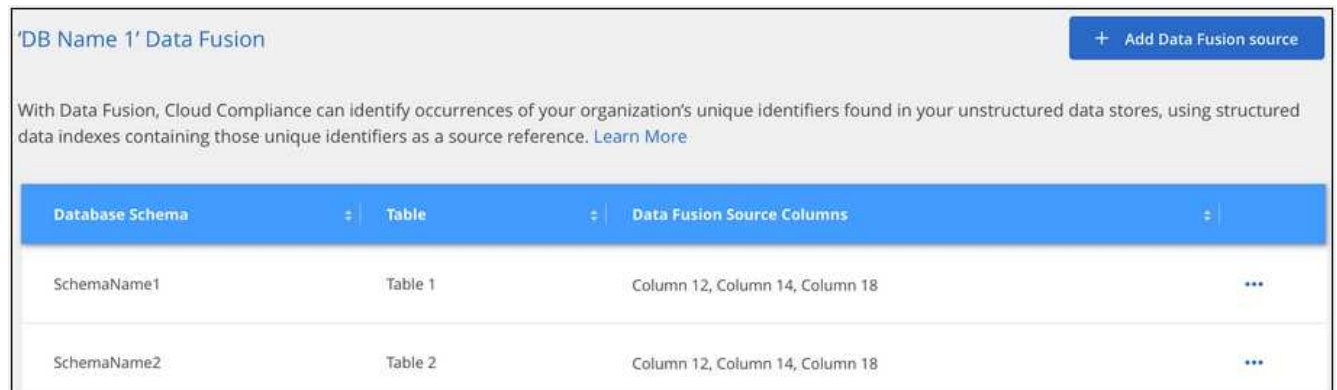
여러 열을 추가할 때는 각 열 이름 또는 표 보기 이름을 별도의 줄에 입력합니다.



The dialog box is titled "Add Data Fusion Source". It contains the following text: "To add a Data Fusion source reference, specify one or more columns which contain your organization's unique identifiers, such as a column used to store customer IDs." and "Note that adding a Data Fusion Source will initiate an additional scan of your data stores". There are two input fields: "Database Schema" with the value "Oracle1,Accounts" and "Table" with the value "Customers". Below these is a section titled "Columns Containing Identifiers" with a list box containing "Customer ID". At the bottom are two buttons: "Add Data Fusion Source" and "Cancel".

4. 데이터 Fusion 소스 추가 * 를 클릭합니다.

Data Fusion 인벤토리 페이지에는 클라우드 데이터 센스를 위해 구성된 데이터베이스 소스 열이 표시됩니다.



The page is titled "'DB Name 1' Data Fusion" and has a button "+ Add Data Fusion source" in the top right. Below the title is a paragraph: "With Data Fusion, Cloud Compliance can identify occurrences of your organization's unique identifiers found in your unstructured data stores, using structured data indexes containing those unique identifiers as a source reference. [Learn More](#)". Below this is a table with the following data:

Database Schema	Table	Data Fusion Source Columns	
SchemaName1	Table 1	Column 12, Column 14, Column 18	...
SchemaName2	Table 2	Column 12, Column 14, Column 18	...

다음 검사 후 결과에는 "개인" 결과 섹션의 대시보드 및 "개인 데이터" 필터의 조사 페이지에 이 새로운 정보가 포함됩니다. 추가한 각 원본 열이 필터 목록에 "Table.Column"(예: "Customers.Customer ID")로 나타납니다.

Data Fusion 소스를 삭제합니다

특정 Data Fusion 소스를 사용하여 파일을 검색하지 않기로 결정한 경우 Data Fusion 인벤토리 페이지에서 소스 행을 선택하고 * Delete Data Fusion Source * 를 클릭할 수 있습니다.



준수 보고서 보기

Cloud Data Sense는 조직의 데이터 개인 정보 보호 프로그램 상태를 더 잘 이해하는 데 사용할 수 있는 보고서를 제공합니다.

기본적으로 Cloud Data Sense 대시보드에는 모든 작업 환경, 데이터베이스 및 데이터 소스에 대한 규정 준수 및 거버넌스 데이터가 표시됩니다. 일부 작업 환경에 대한 데이터만 포함된 보고서를 보려면 [작업 환경을 선택합니다](#).



- 이 섹션에 설명된 보고서는 데이터 소스에서 전체 분류 검사를 수행하도록 선택한 경우에만 사용할 수 있습니다. 매핑 전용 스캔이 있는 데이터 원본은 데이터 매핑 보고서만 생성할 수 있습니다.
- NetApp은 Cloud Data Sense에서 식별할 수 있는 개인 데이터와 민감한 개인 데이터의 100% 정확성을 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 확인해야 합니다.

개인 정보 보호 위험 평가 보고서

개인 정보 보호 위험 평가 보고서는 GDPR 및 CCPA와 같은 개인 정보 보호 규정에 따라 조직의 개인 정보 보호 위험 상태에 대한 개요를 제공합니다. 보고서에는 다음 정보가 포함됩니다.

준수 상태

A [심각도 점수](#) 또한 데이터가 중요하지 않거나 개인적이거나 민감한 개인이든 상관없이 배포할 수 있습니다.

평가 개요

발견된 개인 데이터 유형 및 데이터 범주에 대한 분석.

이 평가의 데이터 주체

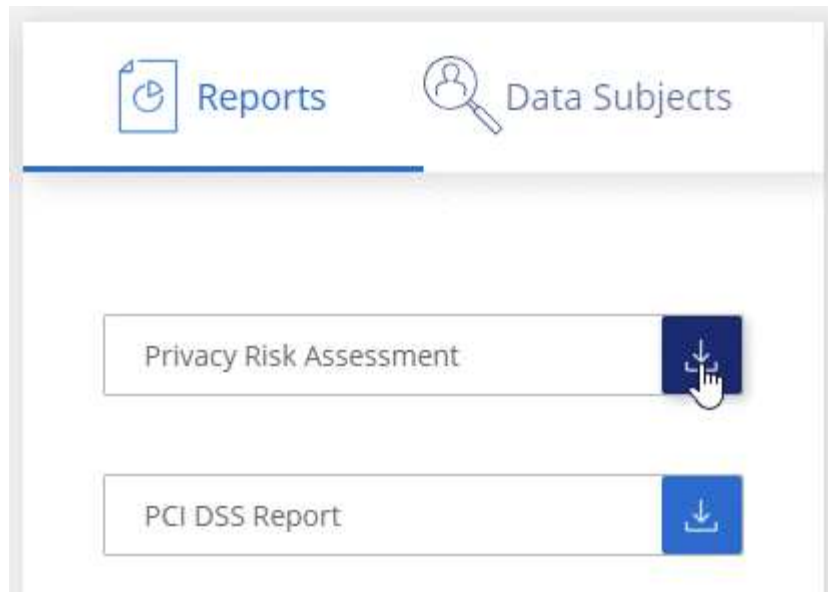
국가 식별자가 발견된 위치별 사람 수.

개인 정보 보호 위험 평가 보고서 생성

데이터 감지 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.
2. Compliance * 를 클릭한 다음 * Reports * 에서 * Privacy Risk Assessment * 옆에 있는 다운로드 아이콘을 클릭합니다.



Cloud Data Sense는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

심각도 점수

Cloud Data Sense는 세 가지 변수를 기준으로 개인 정보 보호 위험 평가 보고서의 심각도 점수를 계산합니다.

- 모든 데이터 중 개인 데이터의 비율입니다.
- 모든 데이터 중 중요한 개인 데이터의 비율입니다.
- 국가 ID, 사회 보장 번호 및 세금 ID 번호와 같은 국가 식별자에 의해 결정되는 데이터 주제가 포함된 파일의 비율입니다.

점수를 결정하는 데 사용되는 논리는 다음과 같습니다.

심각도 점수	논리
0	세 가지 변수는 모두 정확히 0%입니다
1	변수 중 하나가 0%보다 큼니다
2	변수 중 하나가 3%보다 큼니다
3	변수 중 두 개가 3%보다 큼니다
4	변수 중 3개가 3%보다 큼니다
5	변수 중 하나가 6%보다 큼니다
6	변수 중 두 개가 6%보다 큼니다
7	변수 중 3개가 6%보다 큼니다
8	변수 중 하나가 15%보다 큼니다
9	변수 중 두 개가 15%보다 큼니다
10	세 개의 변수가 15%보다 큼니다

PCI DSS 보고서

PCI DSS(Payment Card Industry Data Security Standard) 보고서를 통해 파일 전체에서 신용 카드 정보의 분포를 확인할 수 있습니다. 보고서에는 다음 정보가 포함됩니다.

개요

신용 카드 정보와 작업 환경이 포함된 파일 수

암호화

암호화 또는 암호화되지 않은 작업 환경에 있는 신용 카드 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

랜섬웨어 보호

랜섬웨어 보호가 활성화된 작업 환경에 있는 신용 카드 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

보존

파일이 마지막으로 수정된 기간. 이 기능은 신용 카드 정보를 처리하는 데 필요한 것보다 더 오래 보관해서는 안 되기 때문에 유용합니다.

신용 카드 정보 배포

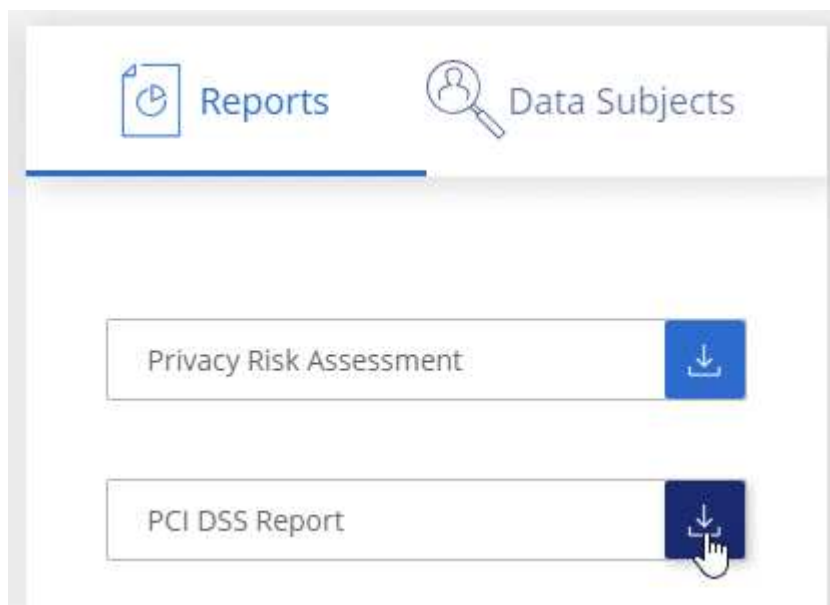
신용 카드 정보가 발견된 작업 환경 및 암호화 및 랜섬웨어 방지 기능이 활성화되어 있는지 여부

PCI DSS 보고서 생성

데이터 감지 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.
2. 규정 준수 * 를 클릭한 다음 * 보고서 * 에서 * PCI DSS 보고서 * 옆에 있는 다운로드 아이콘을 클릭합니다.



Cloud Data Sense는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

HIPAA 보고서

HIPAA(Health Insurance Portability and Accountability Act) 보고서를 통해 건강 정보가 포함된 파일을 확인할 수 있습니다. 이 솔루션은 HIPAA 데이터 개인 정보 보호법을 준수하기 위한 조직의 요구 사항을 지원하도록 설계되었습니다. Cloud Data Sense에서 찾는 정보는 다음과 같습니다.

- 상태 참조 패턴
- ICD-10-cm 의료 코드
- ICD-9-cm 의료 코드
- HR – 건강 범주
- 상태 응용 프로그램 데이터 범주입니다

보고서에는 다음 정보가 포함됩니다.

개요

상태 정보가 포함된 파일 수와 작업 환경이 포함된 파일 수

암호화

암호화 또는 암호화되지 않은 작업 환경에 있는 상태 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

랜섬웨어 보호

랜섬웨어 보호가 활성화된 작업 환경에 대한 상태 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

보존

파일이 마지막으로 수정된 기간. 이 기능은 건강 정보를 처리하는 데 필요한 것보다 오래 보관할 필요가 없기 때문에 유용합니다.

건강 정보 배포

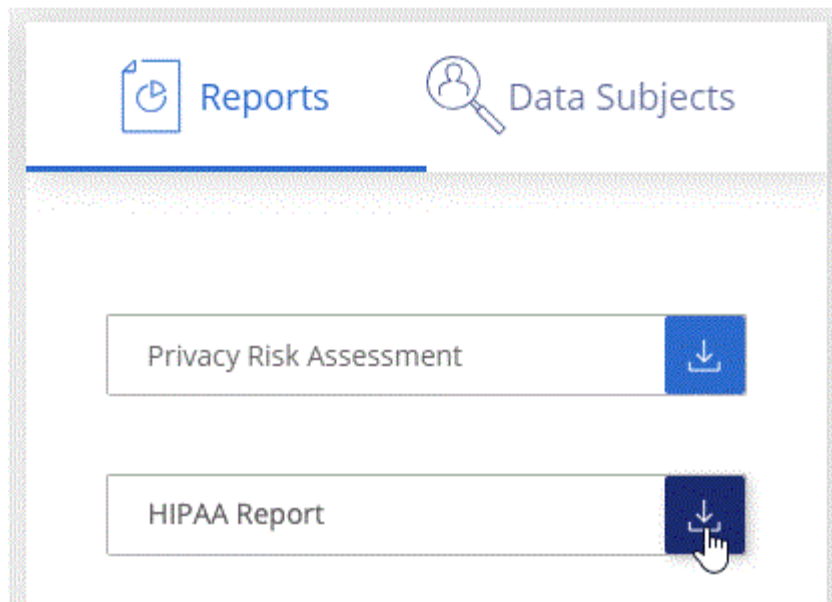
상태 정보가 발견된 작업 환경 및 암호화 및 랜섬웨어 방지 기능이 활성화되어 있는지 여부

HIPAA 보고서 생성

데이터 감지 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.
2. 규정 준수 * 를 클릭한 다음 * 보고서 * 에서 * HIPAA 보고서 * 옆에 있는 다운로드 아이콘을 클릭합니다.



Cloud Data Sense는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

데이터 매핑 보고서

데이터 매핑 보고서는 마이그레이션, 백업, 보안 및 규정 준수 프로세스를 결정하는 데 도움이 되도록 기업 데이터 소스에 저장되는 데이터에 대한 개요를 제공합니다. 이 보고서에는 먼저 작업 환경 및 데이터 소스를 모두 요약하는 개요 보고서가 나열되어 있으며 각 작업 환경에 대한 분석을 제공합니다.

보고서에는 다음 정보가 포함됩니다.

사용 용량

모든 작업 환경: 각 작업 환경의 파일 수와 사용된 용량을 나열합니다. 단일 작업 환경의 경우: 최대 용량을 사용하는 파일을 나열합니다.

데이터 사용 기간

파일이 생성되거나, 마지막으로 수정되거나, 마지막으로 액세스된 시간에 대한 3개의 차트와 그래프를 제공합니다. 특정 날짜 범위를 기준으로 파일 수와 사용된 용량을 나열합니다.

데이터 크기

작업 환경의 특정 크기 범위 내에 있는 파일 수를 나열합니다.

파일 형식

에는 작업 환경에 저장되는 각 파일 유형의 총 파일 수와 사용된 용량이 나와 있습니다.

데이터 매핑 보고서 생성

데이터 감지 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.
2. Governance * 를 클릭한 다음 Governance Dashboard에서 * Full Data Mapping Overview Report * 버튼을 클릭합니다.



Cloud Data Sense는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.


데이터 조사 보고서

데이터 조사 보고서는 데이터 조사 페이지의 내용을 다운로드하는 것입니다. "[데이터 조사 페이지에 대해 자세히 알아보십시오](#)".

보고서를 로컬 컴퓨터에 .csv 파일로 저장할 수 있으며, 여기에는 최대 5,000개의 데이터 행이 포함될 수 있습니다. 데이터 센스가 데이터베이스 테이블(구조화된 데이터) 및 파일(구조화되지 않은 데이터)을 검색하는 경우 .csv 보고서를 최대 2개까지 다운로드할 수 있습니다.

데이터 조사 보고서 생성

단계

1. 데이터 조사 페이지에서 을 클릭합니다  버튼을 클릭합니다.

보고서를 다운로드하는 중이라는 메시지가 대화 상자에 표시됩니다.

각 데이터 조사 보고서에 포함된 내용

비정형 파일 데이터 보고서 * 에는 파일에 대한 다음 정보가 포함됩니다.

- 파일 이름입니다
- 위치 유형
- 작업 환경 이름입니다
- 스토리지 저장소(예: 볼륨, 버킷, 공유)
- 작업 환경 유형입니다
- 파일 경로
- 파일 형식
- 파일 크기
- 만든 시간
- 마지막 수정
- 마지막 액세스
- 파일 소유자
- 범주
- 개인 정보
- 민감한 개인 정보
- 삭제 감지 날짜입니다

삭제 감지 날짜는 파일이 삭제되거나 이동된 날짜를 나타냅니다. 이렇게 하면 중요한 파일이 이동된 시기를 식별할 수 있습니다. 삭제된 파일은 대시보드나 조사 페이지에 나타나는 파일 번호 개수에 포함되지 않습니다. 파일은 CSV 보고서에만 나타납니다.

Structured Data Report *에는 데이터베이스 테이블에 대한 다음 정보가 포함되어 있습니다.

- DB 테이블 이름입니다
- 위치 유형
- 작업 환경 이름입니다
- 스토리지 저장소(예: 스키마)
- 열 개수
- 행 수
- 개인 정보
- 민감한 개인 정보
- 참고: * 폴더에 대한 정보는 현재 보고서에서 사용할 수 없습니다.

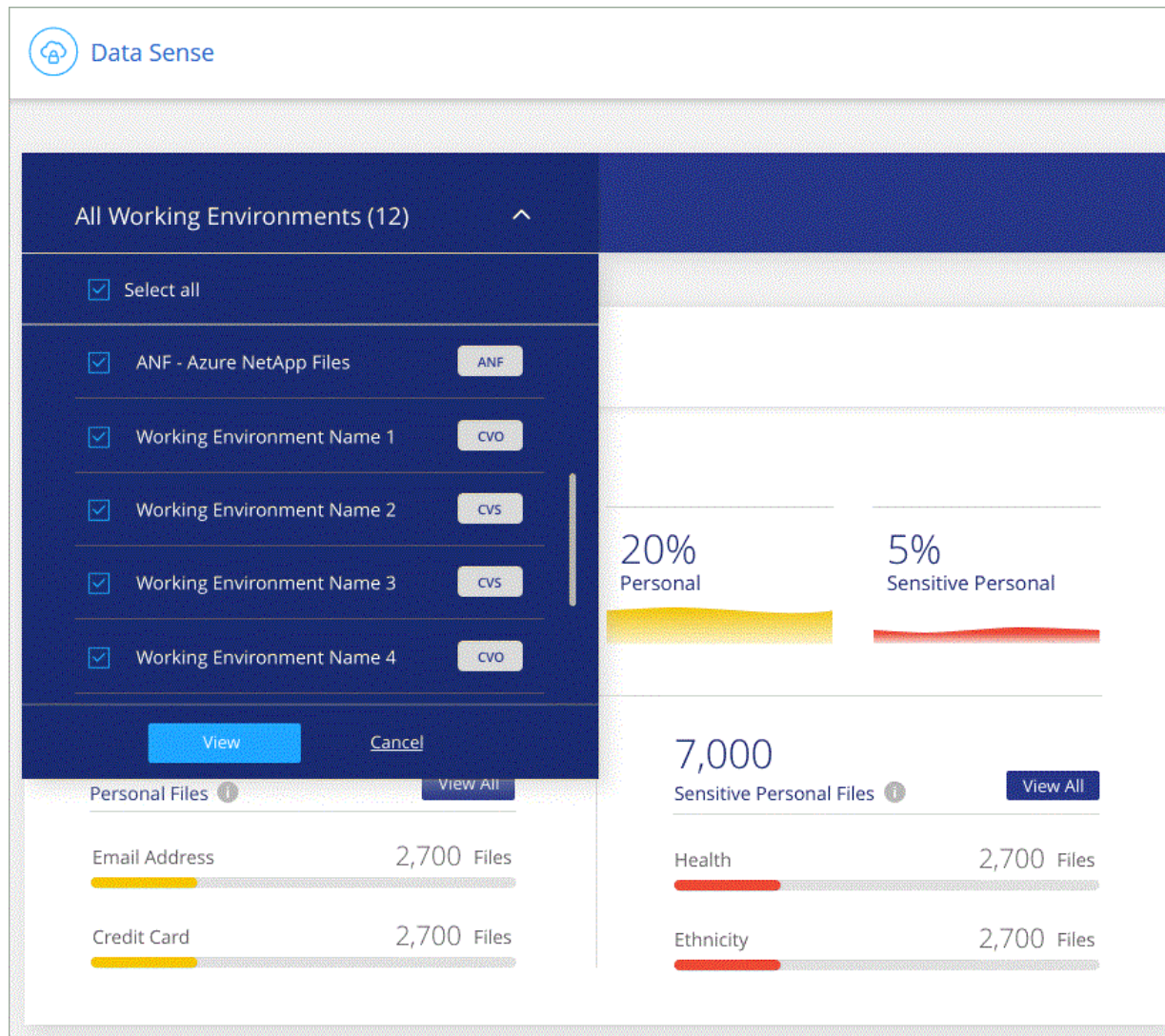
보고서에 사용할 작업 환경 선택

Cloud Data Sense Compliance 대시보드의 콘텐츠를 필터링하여 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터를 확인하거나 특정 작업 환경에 대한 규정 준수 데이터를 확인할 수 있습니다.

대시보드를 필터링할 때 데이터 센스에서 규정 준수 데이터와 보고서의 범위를 선택한 작업 환경만으로 설정합니다.

단계

1. 필터 드롭다운을 클릭하고 데이터를 보려는 작업 환경을 선택한 다음 * 보기 * 를 클릭합니다.



데이터 주체 액세스 요청에 응답

피해자의 전체 이름 또는 알려진 식별자(예: 이메일 주소)를 검색한 다음 보고서를 다운로드하여 Data Subject Access Request(SAR)에 응답합니다. 이 보고서는 GDPR 또는 이와 유사한 데이터 개인 정보 보호 법률을 준수하기 위한 조직의 요구 사항을 지원하도록 설계되었습니다.



SAR 기능은 데이터 소스에서 전체 분류 스캔을 수행하도록 선택한 경우에만 사용할 수 있습니다. 매핑 전용 스캔이 있는 데이터 원본은 파일 수준 세부 정보를 제공하지 않습니다.



NetApp은 Cloud Data Sense에서 식별할 수 있는 개인 데이터와 민감한 개인 데이터의 100% 정확성을 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 확인해야 합니다.

데이터 주체 액세스 요청이란 무엇입니까?

유럽 GDPR과 같은 개인 정보 보호 규정은 데이터 주체(고객 또는 직원 등)에게 개인 데이터에 액세스할 수 있는 권한을 부여합니다. 데이터 피해자가 이 정보를 요청하는 경우 이를 SAR(데이터 주체 액세스 요청)이라고 합니다. 조직은 이러한 요청에 대해 "부당한 지연 없이", 그리고 수령 후 1개월 이내에 응답해야 합니다.

SAR에 대응하는 데 Cloud Data Sense가 어떤 도움을 줄 수 있습니까?

데이터 주체 검색을 수행할 때 Cloud Data Sense는 해당 사용자의 이름이나 식별자가 포함된 모든 파일, 버킷, OneDrive 및 SharePoint 계정을 찾습니다. Data Sense는 이름 또는 식별자에 대해 미리 인덱싱된 최신 데이터를 확인합니다. 새 스캔은 시작되지 않습니다.

검색이 완료되면 데이터 주체 액세스 요청 보고서에 대한 파일 목록을 다운로드할 수 있습니다. 이 보고서는 데이터에서 얻은 통찰력을 집계하여 해당 사람에게 다시 보낼 수 있는 법적 용어로 저장합니다.



현재 데이터베이스 내에서 데이터 주제 검색이 지원되지 않습니다.

데이터 주체 검색 및 보고서 다운로드

데이터 주체의 전체 이름 또는 알려진 식별자를 검색한 다음 파일 목록 보고서 또는 DSAR 보고서를 다운로드합니다. 검색할 수 있는 기준 **"모든 개인 정보 유형입니다"**.

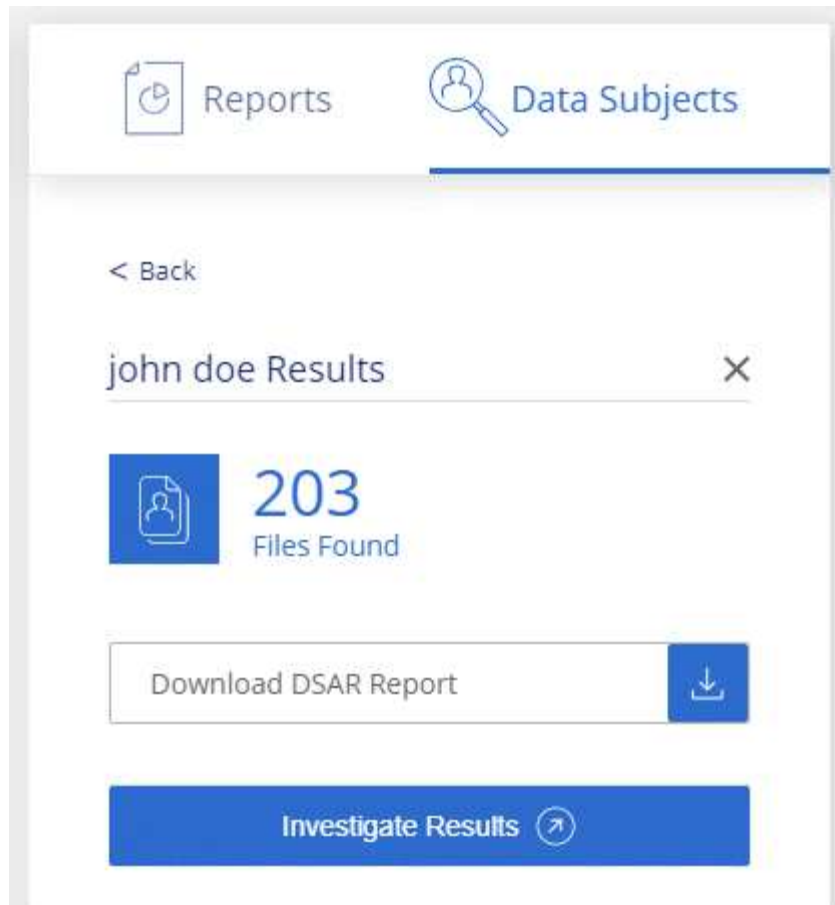


데이터 주체 이름을 검색할 때 영어, 독일어 및 스페인어가 지원됩니다. 더 많은 언어에 대한 지원은 나중에 추가됩니다.

단계

1. Cloud Manager 상단에서 * 데이터 감지 * 를 클릭합니다.
2. 데이터 제목 * 을 클릭합니다.
3. 데이터 제목의 전체 이름 또는 알려진 식별자를 검색합니다.

다음은 name_john doe_에 대한 검색을 보여 주는 예입니다.



4. 사용 가능한 옵션 중 하나를 선택합니다.

- * DSAR 보고서 다운로드 *: 데이터 주체에 전송할 수 있는 액세스 요청에 대한 공식 응답입니다. 이 보고서에는 데이터 주체에 대해 Cloud Data Sense에서 찾을 수 있고 템플릿으로 사용하도록 설계된 데이터를 기반으로 자동으로 생성된 정보가 포함됩니다. 양식을 작성하여 내부적으로 검토한 후 데이터 제목으로 보내야 합니다.
- * 결과 조사 *: 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 파일 목록을 다운로드하여 데이터를 조사할 수 있는 페이지입니다.



10,000개가 넘는 결과가 있을 경우 파일 목록에 최상위 10,000개만 표시됩니다.

개인 데이터의 범주입니다

Cloud Data Sense는 다양한 유형의 프라이빗 데이터를 볼륨, Amazon S3 버킷, 데이터베이스, OneDrive 폴더, SharePoint 계정에서 식별할 수 있습니다. Google Drive 계정을 만듭니다. 아래 범주를 참조하십시오.



Cloud Data Sense를 사용하여 추가 국가 ID 번호 또는 의료 식별자 등과 같은 다른 프라이빗 데이터 유형을 식별하려면 ng-contact-data-sense@netapp.com 으로 이메일을 보내 요청하십시오.

개인 데이터의 유형입니다

파일에서 발견된 개인 데이터는 일반 개인 데이터 또는 국가 식별자일 수 있습니다. 세 번째 열에는 Cloud Data Sense가 사용되는지 여부를 확인할 수 있습니다. "근접 확인" 식별자에 대한 결과를 검증합니다.

이 범주의 항목은 모든 언어로 인식할 수 있습니다.

데이터베이스 서버를 검색하는 경우 파일에 있는 개인 데이터 목록에 추가할 수 있습니다. Data Fusion_Feature를 사용하면 데이터베이스 테이블에서 열을 선택하여 클라우드 데이터 센스가 '스캔'에서 찾을 추가 식별자를 선택할 수 있습니다. 을 참조하십시오 ["Data Fusion를 사용하여 개인 데이터 식별자를 추가합니다"](#) 를 참조하십시오.

유형	ID입니다	근접성 검증?
일반	이메일 주소입니다	아니요
	신용 카드 번호입니다	아니요
	IBAN 번호(국제 은행 계좌 번호)	아니요
	IP 주소입니다	아니요
	암호	예

유형	ID입니다	근접성 검증?
국가 식별자		
56		

	룩셈부르크 ID입니다	예
	몰타 ID	예
유형	NHS(National Health Service) 번호	예접성 검증?
	폴란드어 ID(PESEL)	예
	포르투갈어 세금 식별 번호(NIF)	예
	루마니아어 ID(CNP)	예
	슬로베니아어 ID(EMSO)	예
	남아프리카 ID	예
	스페인어 세금 식별 번호	예
	스웨덴 iD	예
	영국 ID(Nino)	예
	미국 주민등록번호	예

중요한 개인 데이터의 유형

Cloud Data Sense가 파일에서 찾을 수 있는 중요한 개인 데이터에는 다음 목록이 포함됩니다. 이 범주의 항목은 현재 영어로만 인식할 수 있습니다.

형사 절차 참조

자연인의 범죄 소신 및 범죄에 관한 데이터.

인종 참조

자연인의 인종 또는 민족에 관한 데이터.

상태 참조

자연인의 건강에 관한 데이터.

ICD-9-cm 의료 코드

의료 및 의료 산업에서 사용되는 코드.

ICD-10-CM 의료 코드

의료 및 의료 산업에서 사용되는 코드.

철학적 신념 기준

자연인의 철학적 신념에 관한 데이터.

정치적 견해 참조

자연인의 정치적 의견에 관한 자료.

종교적 신념 참조

자연인의 종교적 신념에 관한 데이터.

성생활 또는 오리엔테이션 참조

자연인의 성생활 또는 성적 취향과 관련된 데이터.

범주 유형

Cloud Data Sense는 다음과 같이 데이터를 분류합니다. 이러한 범주의 대부분은 영어, 독일어 및 스페인어로 인정될 수 있습니다.

범주	유형	영어	독일어	스페인어
재무	밸런스 시트	✓	✓	✓
	구매 주문	✓	✓	✓
	인보이스	✓	✓	✓
	분기별 보고서	✓	✓	✓
시간	배경 확인	✓		✓
	보상 계획	✓	✓	✓
	직원 계약	✓		✓
	직원 검토	✓		✓
	상태	✓		✓
	다시 시작합니다	✓	✓	✓
법적 고지	NDAS	✓	✓	✓
	공급업체 - 고객 계약	✓	✓	✓
마케팅	캠페인	✓	✓	✓
	회의	✓	✓	✓
운영	감사 보고서	✓	✓	✓
판매	판매 주문	✓	✓	
서비스	RFI	✓		✓
	RFP	✓		✓
	SOW	✓	✓	✓
	교육	✓	✓	✓
지원	불만 및 티켓	✓	✓	✓

다음 메타데이터도 분류되어 동일한 지원 언어로 식별됩니다.

- 애플리케이션 데이터
- 파일 보관
- 오디오
- 비즈니스 애플리케이션 데이터
- CAD 파일
- 코드
- 손상되었습니다

- 데이터베이스 및 인덱스 파일
- 설계 파일
- 이메일 애플리케이션 데이터
- 암호화
- 실행 파일
- 재무 애플리케이션 데이터
- 상태 응용 프로그램 데이터
- 이미지
- 로그
- 기타 문서
- 기타 프레젠테이션
- 기타 스프레드시트
- 기타 "알 수 없음"
- 정형 데이터
- 비디오
- 0바이트 파일

파일 유형

Cloud Data Sense는 모든 파일에서 범주 및 메타데이터 정보를 검색하고 대시보드의 파일 형식 섹션에 모든 파일 형식을 표시합니다.

그러나 데이터 센스에서 PII(개인 식별 정보)를 감지하거나 DSAR 검색을 수행할 경우 다음 파일 형식만 지원됩니다.

' .csv, .dcm, .dicom, .DOC, .DOCX, .JSON, .pdf, .PPTX, .rtf, .TXT, XLS, .XLSX, Docs, Sheets, Slides '

정보가 정확합니다

NetApp은 Cloud Data Sense에서 식별할 수 있는 개인 데이터와 민감한 개인 데이터의 100% 정확성을 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 확인해야 합니다.

테스트를 기준으로 아래 표는 Data Sense에서 찾은 정보의 정확성을 보여줍니다. 정밀 _ 및 _ 리콜 _ 을(를) 통해 분해합니다.

정밀도

데이터 센스에서 발견한 것이 정확하게 식별되었을 확률입니다. 예를 들어, 개인 데이터의 정밀도가 90%이면 개인 정보가 포함된 것으로 확인된 10개 파일 중 9개가 개인 정보를 포함하고 있음을 의미합니다. 10개 파일 중 1개는 위양성입니다.

리콜

데이터 센스에서 필요한 것을 찾을 수 있는 확률입니다. 예를 들어 개인 데이터의 리콜 비율이 70%이면 데이터 센스에서 조직에 개인 정보가 실제로 포함된 10개 파일 중 7개를 식별할 수 있습니다. 데이터 센스에서 데이터의 30%를 누락하면 대시보드에 표시되지 않습니다.

우리는 결과의 정확성을 지속적으로 개선하고 있습니다. 이러한 향상된 기능은 향후 Data Sense 릴리즈에서 자동으로 제공될 예정입니다.


유형	정밀도	리콜
개인 데이터 - 일반	90% - 95%	60%~80%
개인 데이터 - 국가 식별자	30% ~ 60%	40% ~ 60%
민감한 개인 데이터	80% - 95%	20% - 30%
범주	90% - 97%	60%~80%

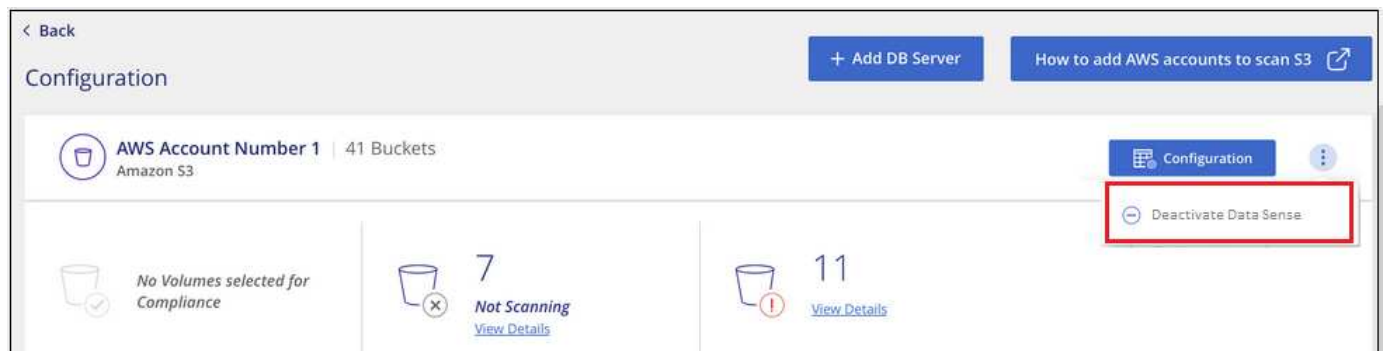
클라우드 데이터 센스에서 데이터 소스를 제거합니다

필요한 경우, 하나 이상의 작업 환경, 데이터베이스, 파일 공유 그룹, OneDrive 계정, Google Drive 계정, SharePoint 계정을 사용할 수 있습니다. 작업 환경에서 데이터 센스를 더 이상 사용하지 않으려면 Cloud Data Sense 인스턴스도 삭제할 수 있습니다.

작업 환경에 대한 규정 준수 검사 비활성화

스캔을 비활성화하면 Cloud Data Sense는 더 이상 작업 환경의 데이터를 스캔하지 않고 Data Sense 인스턴스에서 인덱싱된 규정 준수 정보를 제거합니다(작업 환경 자체의 데이터는 삭제되지 않음).

1. Configuration_ 페이지에서 을 클릭합니다  작업 환경 행에 있는 단추를 클릭한 다음 * 데이터 감지 비활성화 * 를 클릭합니다.



작업 환경을 선택할 때 서비스 패널에서 작업 환경에 대한 준수 검사를 비활성화할 수도 있습니다.

클라우드 데이터 센스에서 데이터베이스를 제거하는 중입니다

특정 데이터베이스를 더 이상 스캔하지 않으려면 Cloud Data Sense 인터페이스에서 해당 데이터베이스를 삭제하고 모든 스캔을 중지할 수 있습니다.


1. Configuration_ 페이지에서 을 클릭합니다  단추를 클릭한 다음 * DB 서버 제거 * 를 클릭합니다.



클라우드 데이터 센스에서 **OneDrive, SharePoint** 또는 **Google Drive** 계정을 제거합니다

특정 OneDrive 계정, 특정 SharePoint 계정 또는 Google Drive 계정에서 사용자 파일을 더 이상 스캔하지 않으려면 Cloud Data Sense 인터페이스에서 계정을 삭제하고 모든 스캔을 중지할 수 있습니다.

단계

1. Configuration_ 페이지에서 을 클릭합니다  단추를 클릭하고 * OneDrive 계정 제거 *, * SharePoint 계정 제거 * 또는 * Google 드라이브 계정 제거 * 를 클릭합니다.



2. 확인 대화 상자에서 * 계정 삭제 * 를 클릭합니다.

Cloud Data Sense에서 파일 공유 그룹을 제거하는 중입니다

파일 공유 그룹에서 사용자 파일을 더 이상 스캔하지 않으려면 Cloud Data Sense 인터페이스에서 파일 공유 그룹을 삭제하고 모든 스캔을 중지할 수 있습니다.

단계

1. Configuration_ 페이지에서 을 클릭합니다  File Shares Group 행의 버튼을 클릭한 다음 * Remove File Shares Group * 을 클릭합니다.



2. 확인 대화 상자에서 * 공유 그룹 삭제 * 를 클릭합니다.

데이터 감지 스캔 속도를 줄입니다

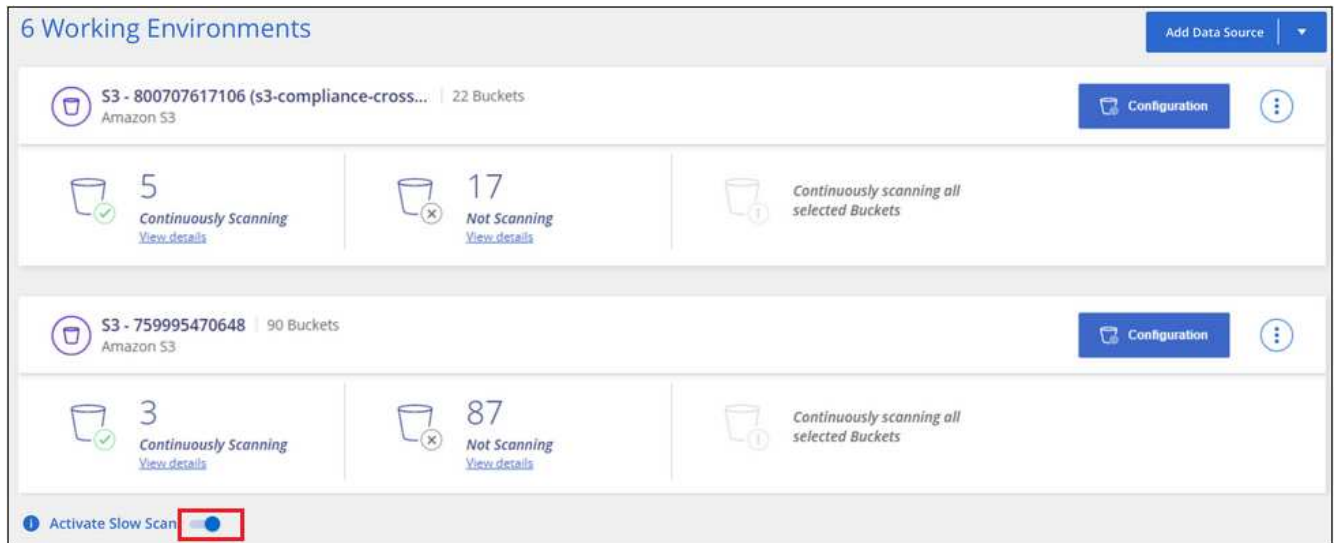
데이터 스캔은 스토리지 시스템과 데이터에 경미한 영향을 줍니다. 그러나 아주 작은 충격에도 신경 쓰면 데이터 센스를 구성하여 "느린" 스캔을 수행할 수 있습니다. 이 옵션을 설정하면 모든 데이터 소스에서 느린 스캔이 사용됩니다. 단일 작업 환경 또는 데이터 원본에 대해 느린 스캔을 구성할 수 없습니다.



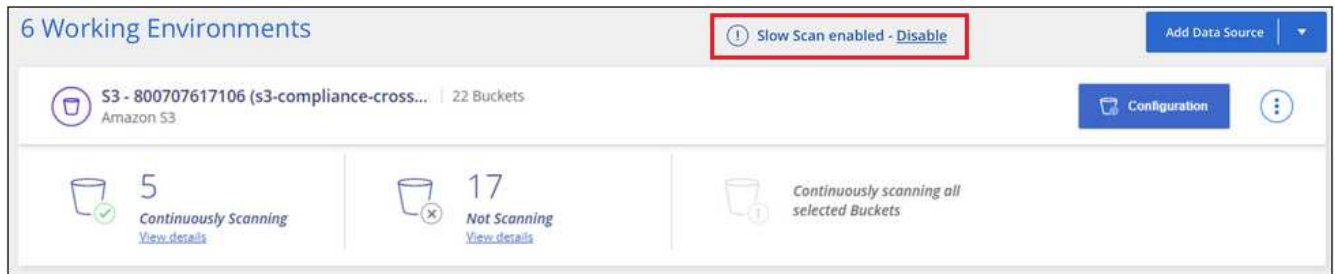
데이터베이스를 스캔할 때는 스캔 속도를 줄일 수 없습니다.

단계

1. Configuration_page 하단에서 슬라이더를 오른쪽으로 이동하여 저속 스캔을 활성화합니다.



구성 페이지 맨 위에는 저속 스캔이 활성화되어 있습니다.



2. 이 메시지에서 * Disable * 을 클릭하여 저속 스캔을 비활성화할 수 있습니다.

클라우드 데이터 감지 인스턴스를 삭제하는 중입니다

더 이상 데이터 센스를 사용하지 않으려면 Cloud Data Sense 인스턴스를 삭제할 수 있습니다. 인스턴스를 삭제하면 인덱싱된 데이터가 있는 연결된 디스크도 삭제됩니다.

1. 클라우드 공급자의 콘솔로 이동하여 Cloud Data Sense 인스턴스를 삭제합니다.

인스턴스의 이름은 *CloudCompliance_*이며 생성된 해시(*UUID*)와 연결됩니다. 예: *_CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.