데이터 분류 사용

NetApp Data Classification

NetApp
February 11, 2026

목차

데이터 분류 사용

NetApp Data Classification 사용하여 조직에 저장된 데이터에 대한 거버넌스 세부 정보를 확인하세요.

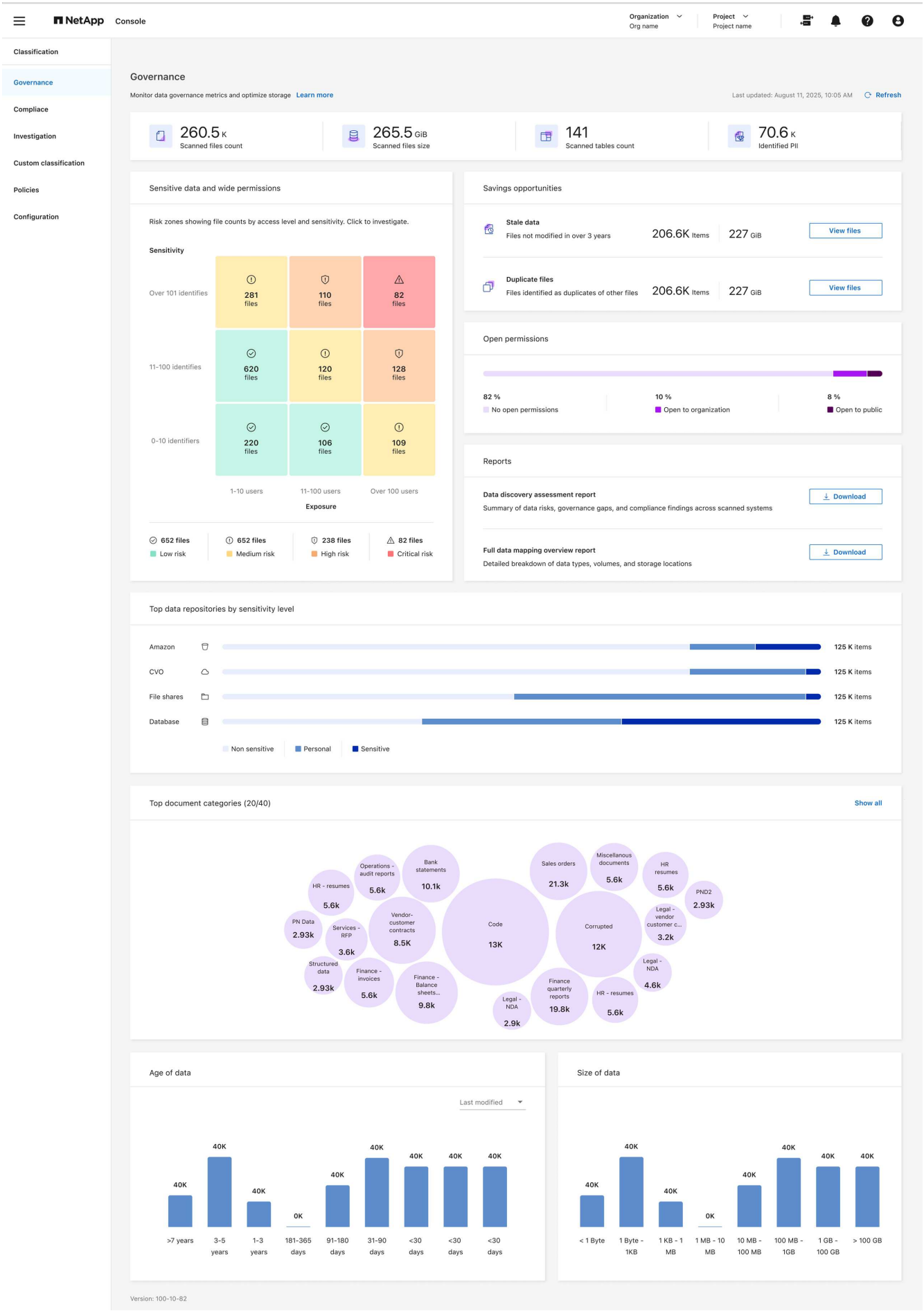
조직의 스토리지 리소스에 있는 데이터와 관련된 비용을 제어하세요. NetApp Data Classification 시스템에서 오래된 데이터, 중복 파일, 매우 큰 파일의 양을 파악하여 일부 파일을 제거할지 아니면 비용이 덜 드는 개체 스토리지로 계층화할지 결정할 수 있도록 도와줍니다.

여기부터 연구를 시작해야 합니다. 거버넌스 대시보드에서 추가 조사할 영역을 선택할 수 있습니다.

또한 온프레미스 위치에서 클라우드로 데이터를 마이그레이션할 계획이라면 데이터를 이동하기 전에 데이터 크기를 확인하고 데이터에 중요한 정보가 포함되어 있는지 확인할 수 있습니다.

거버넌스 대시보드를 검토하세요

거버넌스 대시보드는 스토리지 리소스에 저장된 데이터와 관련된 비용을 제어하고 효율성을 높이는 데 도움이 되는 정보를 제공합니다.


NetApp Console
Organization
Org name
Project
Project name
Classification
Governance
Compliace
Investigation
Custom classification
Policies
Configuration
Governance
Monitor data governance metrics and optimize storage Learn more
Last updated: August 11, 2025, 10:05 AM
Refresh
260.5 K
Scanned files count
265.5 GiB
Scanned files size
141
Scanned tables count
70.6 K
Identified PII
Sensitive data and wide permissions
Risk zones showing file counts by access level and sensitivity. Click to investigate.
Sensitivity
Over 101 identifies
11-100 identifies
0-10 identifiers
281 files
110 files
82 files
620 files
120 files
128 files
220 files
106 files
109 files
1-10 users
11-100 users
Over 100 users
Exposure
652 files
Low risk
652 files
Medium risk
238 files
High risk
82 files
Critical risk
Savings opportunities
Stale data
Files not modified in over 3 years
206.6K Items
227 GiB
View files
Duplicate files
Files identified as duplicates of other files
206.6K Items
227 GiB
View files
Open permissions
82 %
No open permissions
10 %
Open to organization
8 %
Open to public
Reports
Data discovery assessment report
Summary of data risks, governance gaps, and compliance findings across scanned systems
Download
Full data mapping overview report
Detailed breakdown of data types, volumes, and storage locations
Download
Top data repositories by sensitivity level
Amazon
CVO
File shares
Database
125 K items
Non sensitive
Personal
Sensitive
Top document categories (20/40)
Show all
Operations - audit reports 5.6k
Bank statements 10.1k
Sales orders 21.3k
Miscellanous documents 5.6k
HR resumes 5.6k
PND2 2.93k
HR - resumes 5.6k
PN Data 2.93k
Services - RFP 3.6k
Vendor-customer contracts 8.5K
Code 13K
Corrupted 12K
Legal - vendor customer c... 3.2k
Structured data 2.93k
Finance - invoices 5.6k
Finance - Balance sheets... 9.8k
Legal - NDA 2.9k
Finance quarterly reports 19.8k
HR - resumes 5.6k
Legal - NDA 4.6k
Age of data
Last modified
40K
>7 years
40K
3-5 years
40K
1-3 years
0K
181-365 days
40K
91-180 days
40K
31-90 days
40K
<30 days
40K
<30 days
40K
<30 days
Size of data
40K
< 1 Byte
40K
1 Byte - 1KB
40K
1 KB - 1 MB
0K
1 MB - 10 MB
40K
10 MB - 100 MB
40K
100 MB - 1GB
40K
1 GB - 100 GB
40K
> 100 GB
Version: 100-10-82

단계

1. NetApp Console 메뉴에서 *거버넌스 > 분류*를 선택합니다.
2. *거버넌스*를 선택하세요.

   거버넌스 대시보드가 나타납니다.

저축 기회 검토

Saving Opportunities 구성 요소는 삭제하거나 비용이 덜 드는 개체 저장소로 계층화할 수 있는 데이터를 보여줍니다. _Saving Opportunities_의 데이터는 2시간마다 업데이트됩니다. 수동으로 데이터를 업데이트할 수도 있습니다.

단계

1. 데이터 분류 메뉴에서 *거버넌스*를 선택합니다.
2. 거버넌스 대시보드의 각 저축 기회 타일에서 *저장소 최적화*를 선택하면 조사 페이지에서 필터링된 결과를 볼 수 있습니다. 삭제하거나 비용이 덜 드는 저장소로 옮겨야 할 데이터를 찾으려면 _비용 절감 기회_를 조사하세요.
   - 오래된 데이터 - 기본적으로 마지막 수정일로부터 3년 이상 지난 데이터는 오래된 데이터로 간주됩니다. [오래된 데이터의 정의를 사용자 지정할 수 있습니다](task-stale-data.html).
   - 중복 파일 - 스캔하는 데이터 소스의 다른 위치에 중복된 파일입니다. "어떤 유형의 중복 파일이 표시되는지 확인하세요" .

데이터 소스 중 하나라도 데이터 계층화를 구현하는 경우 이미 개체 스토리지에 있는 오래된 데이터는 오래된 데이터 범주에서 식별할 수 있습니다.

데이터 발견 평가 보고서 작성

데이터 발견 평가 보고서는 스캔된 환경에 대한 높은 수준의 분석을 제공하여 문제가 있는 영역과 잠재적인 수정 단계를 보여줍니다. 결과는 데이터 매핑과 분류를 기반으로 합니다. 이 보고서의 목적은 데이터 세트의 세 가지 중요한 측면에 대한 인식을 높이는 것입니다.

특징	설명
데이터 거버넌스 문제	귀하가 소유한 모든 데이터에 대한 자세한 그림과 비용을 절감하기 위해 데이터 양을 줄일 수 있는 영역에 대한 그림입니다.
데이터 보안 노출	광범위한 액세스 권한으로 인해 내부 또는 외부 공격을 통해 데이터에 액세스할 수 있는 영역입니다.
데이터 규정 준수 격차	보안과 DSAR(데이터 주체 접근 요청)을 위해 귀하의 개인 정보 또는 민감한 개인 정보가 어디에 있는지 알려드립니다.

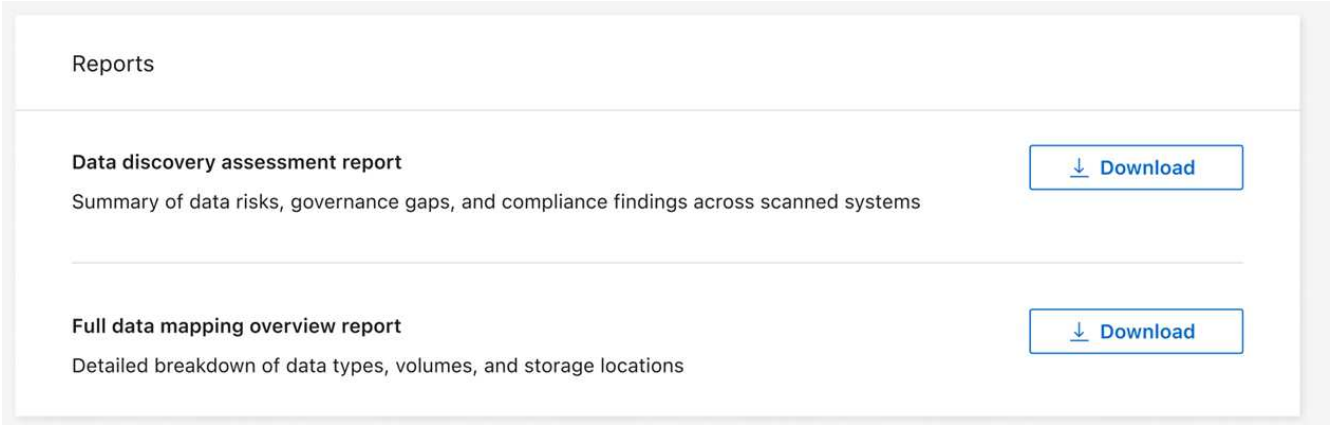
보고서를 사용하면 다음과 같은 작업을 수행할 수 있습니다.

- 보존 정책을 변경하거나 특정 데이터(오래된 데이터 또는 중복 데이터)를 이동 또는 삭제하여 보관 비용을 줄이세요.
- 글로벌 그룹 관리 정책을 개정하여 광범위한 권한이 있는 데이터를 보호하세요.
- PII를 보다 안전한 데이터 저장소로 옮겨 개인 정보나 민감한 개인 정보가 포함된 데이터를 보호하세요.

단계

1. 데이터 분류에서 *거버넌스*를 선택합니다.

2. 보고서 타일에서 *데이터 검색 평가 보고서*를 선택합니다.



결과

데이터 분류는 검토하고 공유할 수 있는 PDF 보고서를 생성합니다.

데이터 매핑 개요 보고서 만들기

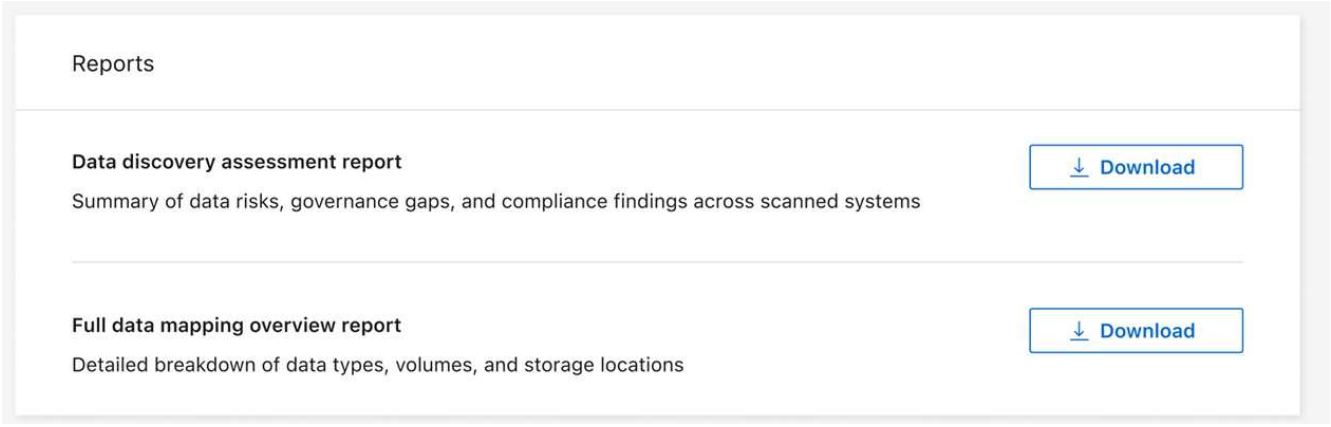
데이터 매핑 개요 보고서는 마이그레이션, 백업, 보안 및 규정 준수 프로세스에 대한 결정을 내리는 데 도움이 되도록 회사 데이터 소스에 저장된 데이터에 대한 개요를 제공합니다. 이 보고서는 모든 시스템과 데이터 소스를 요약합니다. 또한 각 시스템에 대한 분석도 제공합니다.

보고서에는 다음과 같은 정보가 포함되어 있습니다.

범주	설명
사용 용량	모든 시스템에 대해: 각 시스템의 파일 수와 사용된 용량을 나열합니다. 단일 시스템의 경우: 가장 많은 용량을 사용하는 파일을 나열합니다.
데이터의 시대	파일이 생성된 날짜, 마지막으로 수정된 날짜 또는 마지막으로 액세스된 날짜에 대한 세 가지 차트와 그래프를 제공합니다. 특정 날짜 범위를 기준으로 파일 수와 사용된 용량을 나열합니다.
데이터 크기	시스템의 특정 크기 범위 내에 존재하는 파일의 수를 나열합니다.

단계

1. 데이터 분류에서 *거버넌스*를 선택합니다.
2. 보고서 타일에서 *전체 데이터 매핑 개요 보고서*를 선택합니다.



결과

데이터 분류는 필요에 따라 검토하고 다른 그룹으로 보낼 수 있는 PDF 보고서를 생성합니다.

보고서가 1MB보다 크면 PDF 파일이 데이터 분류 인스턴스에 보관되고 정확한 위치에 대한 팝업 메시지가 표시됩니다. 사내 Linux 머신이나 클라우드에 배포한 Linux 머신에 Data Classification을 설치한 경우 PDF 파일로 바로 이동할 수 있습니다. 데이터 분류가 클라우드에 배포되면 PDF 파일을 다운로드하려면 SSH를 통해 데이터 분류 인스턴스에 대한 권한을 부여해야 합니다.

데이터 민감도별로 나열된 상위 데이터 저장소를 검토하세요.

데이터 매핑 개요 보고서의 민감도 수준별 상위 데이터 저장소 영역에는 가장 민감한 항목이 포함된 상위 4개 데이터 저장소(시스템 및 데이터 소스)가 나열됩니다. 각 시스템의 막대형 차트는 다음과 같이 구분됩니다.

- 민감하지 않은 데이터
- 개인정보
- 민감한 개인 데이터

이 데이터는 2시간마다 새로 고쳐지며, 수동으로 새로 고칠 수 있습니다.

단계

1. 각 카테고리에 속한 총 항목 수를 보려면 막대의 각 섹션 위에 커서를 올려놓으세요.
2. 조사 페이지에 나타날 결과를 필터링하려면 막대에서 각 영역을 선택하고 자세히 조사하세요.

민감한 데이터와 광범위한 권한 검토

거버넌스 대시보드의 민감한 데이터 및 광범위한 권한 영역에서는 민감한 데이터가 포함되어 있고 광범위한 권한이 있는 파일의 수가 표시됩니다. 표에는 다음과 같은 유형의 권한이 나와 있습니다.

- 수평축에는 가장 제한적인 허가부터 가장 관대한 제한까지 있습니다.
- 수직축에는 가장 민감하지 않은 데이터부터 가장 민감한 데이터까지 나열되어 있습니다.

단계

1. 각 카테고리에 있는 총 파일 수를 보려면 각 상자 위에 커서를 올려놓으세요.
2. 조사 페이지에 나타날 결과를 필터링하려면 상자를 선택하고 자세히 조사하세요.

공개 허가 유형별로 나열된 데이터 검토

데이터 매핑 개요 보고서의 열린 권한 영역에는 스캔 중인 모든 파일에 대해 각 유형의 권한에 대한 백분율이 표시됩니다. 차트에서는 다음과 같은 유형의 권한을 보여줍니다.

- 공개 허가 없음
- 조직에 개방적
- 대중에게 공개
- 알 수 없는 액세스

단계

1. 각 카테고리에 있는 총 파일 수를 보려면 각 상자 위에 커서를 올려놓으세요.
2. 조사 페이지에 나타날 결과를 필터링하려면 상자를 선택하고 자세히 조사하세요.

데이터의 연령과 크기를 검토하세요

데이터 매핑 개요 보고서의 연령 및 크기 그래프에 있는 항목을 조사하여 삭제하거나 비용이 덜 드는 개체 저장소로 계층화해야 할 데이터가 있는지 확인할 수 있습니다.

단계

1. 데이터 연령 차트에서 데이터 연령에 대한 자세한 내용을 보려면 차트의 한 지점 위에 커서를 놓습니다.
2. 연령이나 사이즈 범위로 필터링하려면 해당 연령이나 사이즈를 선택하세요.
    - 데이터 연령 그래프 - 데이터가 생성된 시간, 마지막으로 액세스된 시간 또는 마지막으로 수정된 시간을 기준으로 데이터를 분류합니다.
    - 데이터 그래프의 크기 - 크기에 따라 데이터를 분류합니다.

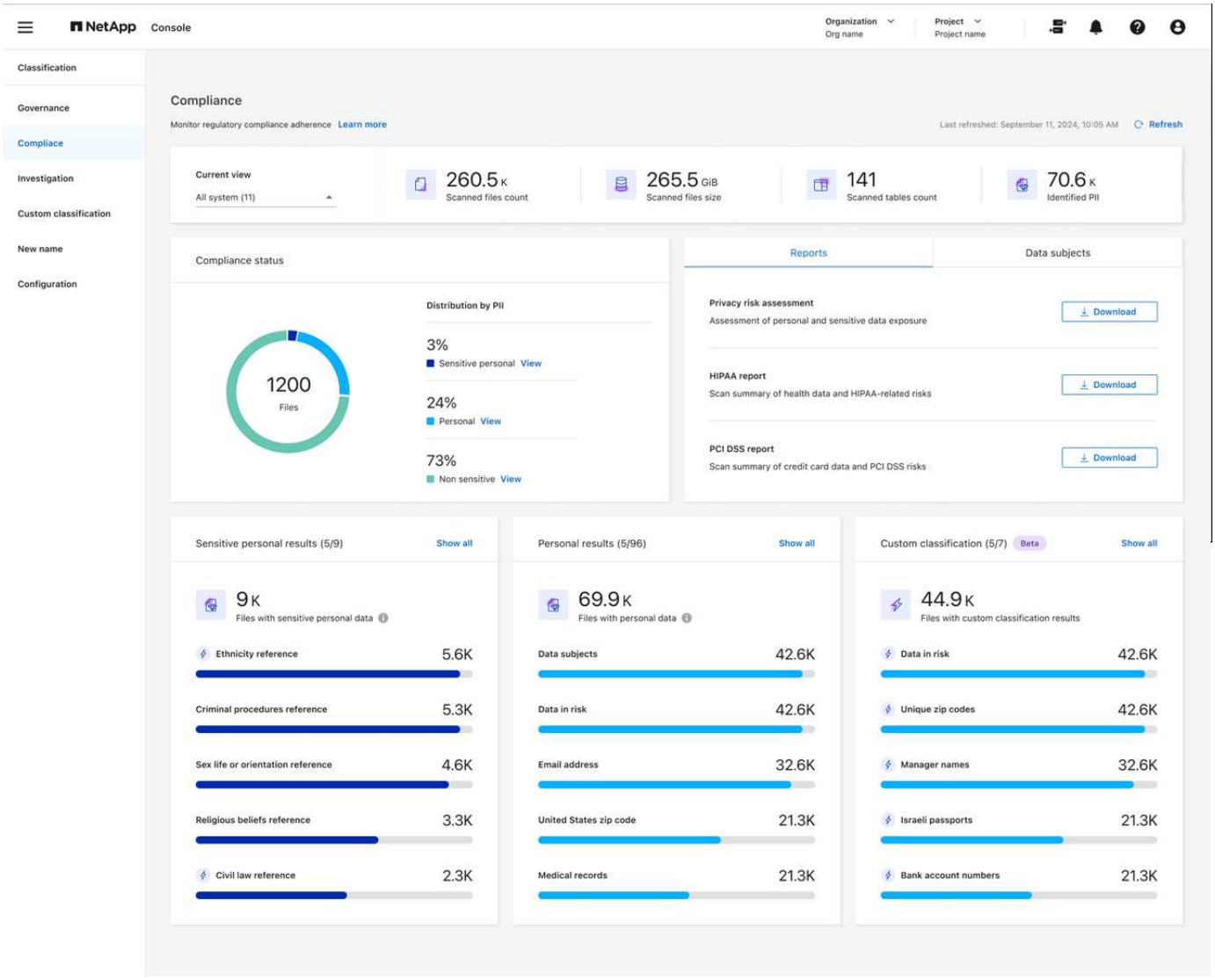
데이터 소스 중 하나라도 데이터 계층화를 구현하는 경우 개체 스토리지에 이미 있는 오래된 데이터는 데이터 연령 그래프에서 식별될 수 있습니다.

NetApp Data Classification 사용하여 조직에 저장된 개인 데이터에 대한 규정 준수 세부 정보를 확인하세요.

귀하의 조직 내 개인 데이터(PII) 및 민감한 개인 데이터(SPII)에 대한 세부 정보를 확인하여 개인 데이터를 제어하세요. NetApp Data Classification 데이터에서 찾은 범주와 파일 유형을 검토하여 가시성을 얻을 수도 있습니다.

파일 수준 규정 준수 세부 정보는 전체 분류 스캔을 수행한 경우에만 사용할 수 있습니다. 매핑 전용 스캔에서는 파일 수준 세부 정보가 생성되지 않습니다.

기본적으로 데이터 분류 대시보드에는 모든 시스템과 데이터베이스에 대한 규정 준수 데이터가 표시됩니다. 일부 시스템에 대한 데이터만 보려면 해당 시스템을 선택하세요.



데이터 조사 페이지에서 결과를 필터링하고 결과 보고서를 CSV 파일로 다운로드할 수 있습니다. 보다"데이터 조사 페이지에서 데이터 필터링" 자세한 내용은.

개인 정보가 포함된 파일 보기

데이터 분류는 데이터 내의 특정 단어, 문자열, 패턴(정규식)을 자동으로 식별합니다. "예를 들어, 신용카드 번호, 주민등록번호, 은행 계좌번호, 비밀번호 등이 있습니다."데이터 분류는 개별 파일, 디렉토리(공유 및 폴더) 내의 파일, 데이터베이스 테이블에서 이러한 유형의 정보를 식별합니다.

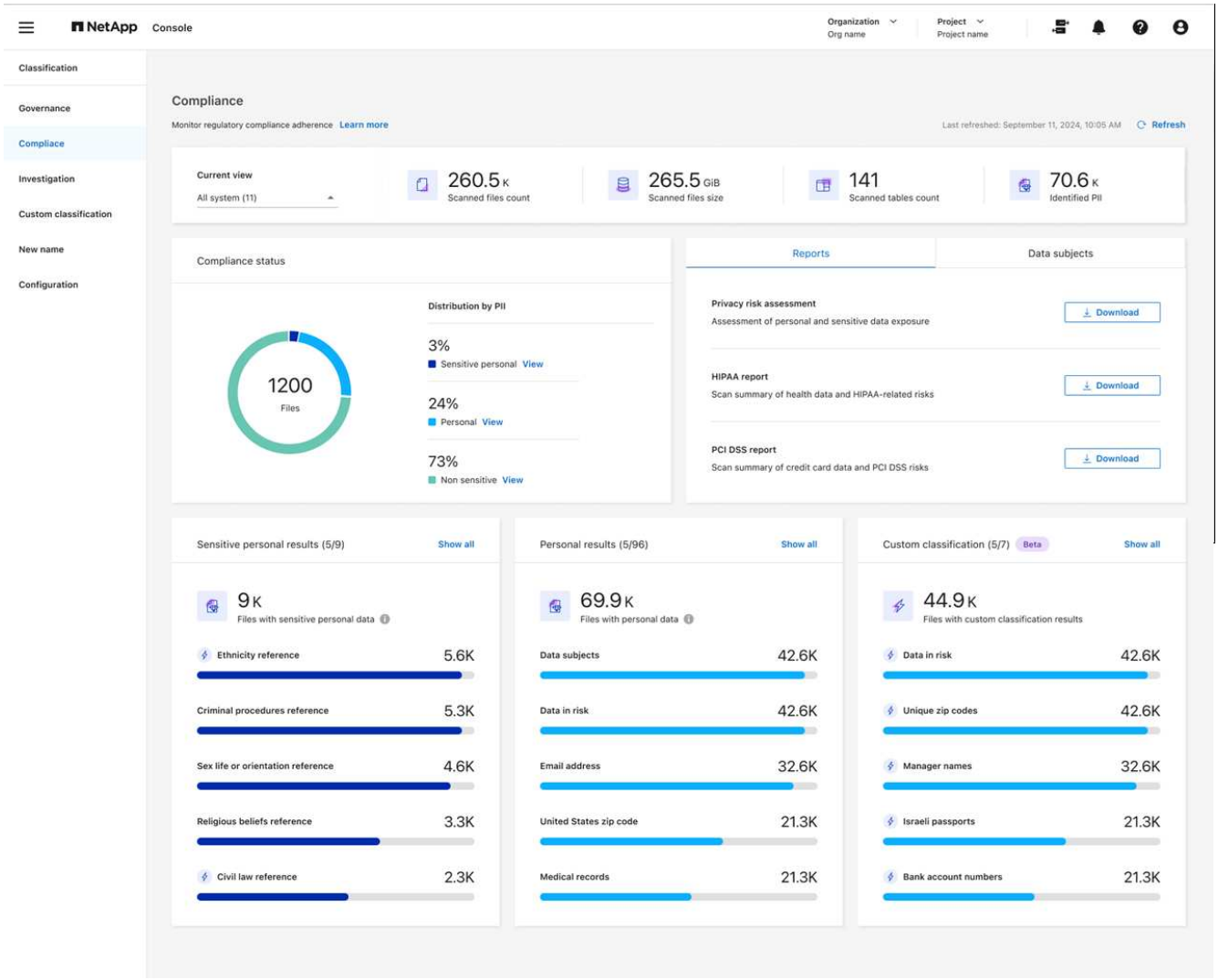
귀하의 조직과 관련된 개인 데이터를 식별하기 위해 사용자 정의 검색어를 만들 수도 있습니다. 자세한 내용은 다음을 참조하세요. "사용자 정의 분류 만들기" .

일부 유형의 개인 데이터의 경우, 데이터 분류는 근접성 검증_을 사용하여 결과를 검증합니다. 검증은 발견된 개인 데이터와 가까운 하나 이상의 미리 정의된 키워드를 찾는 방식으로 수행됩니다. 예를 들어, 데이터 분류는 미국 사회 보장 번호*(SSN)* 옆에 근접 단어*(예: _SSN* 또는 사회 보장)가 있는 경우 해당 번호를 SSN으로 식별합니다. "개인정보 표" 데이터 분류가 근접성 검증을 사용하는 경우를 보여줍니다.

단계

1. 데이터 분류 메뉴에서 규정 준수 탭을 선택합니다.

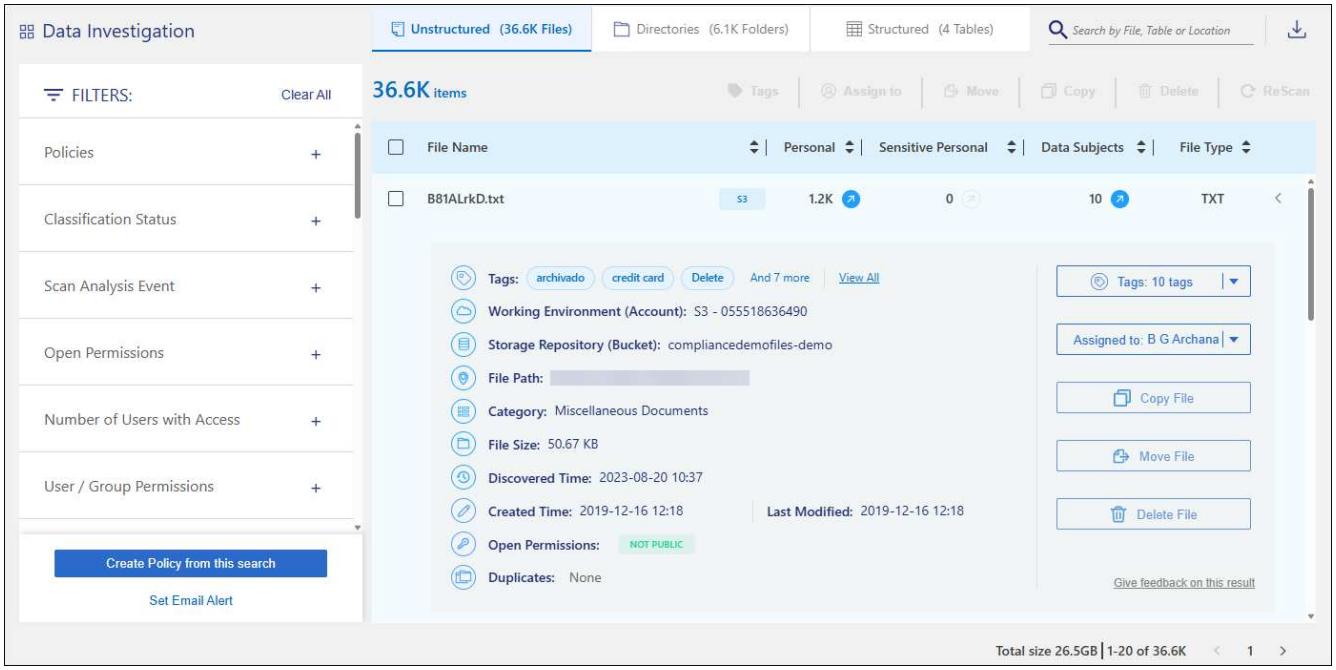
2. 모든 개인 데이터의 세부 정보를 조사하려면 개인 데이터 비율 옆에 있는 아이콘을 선택하세요.

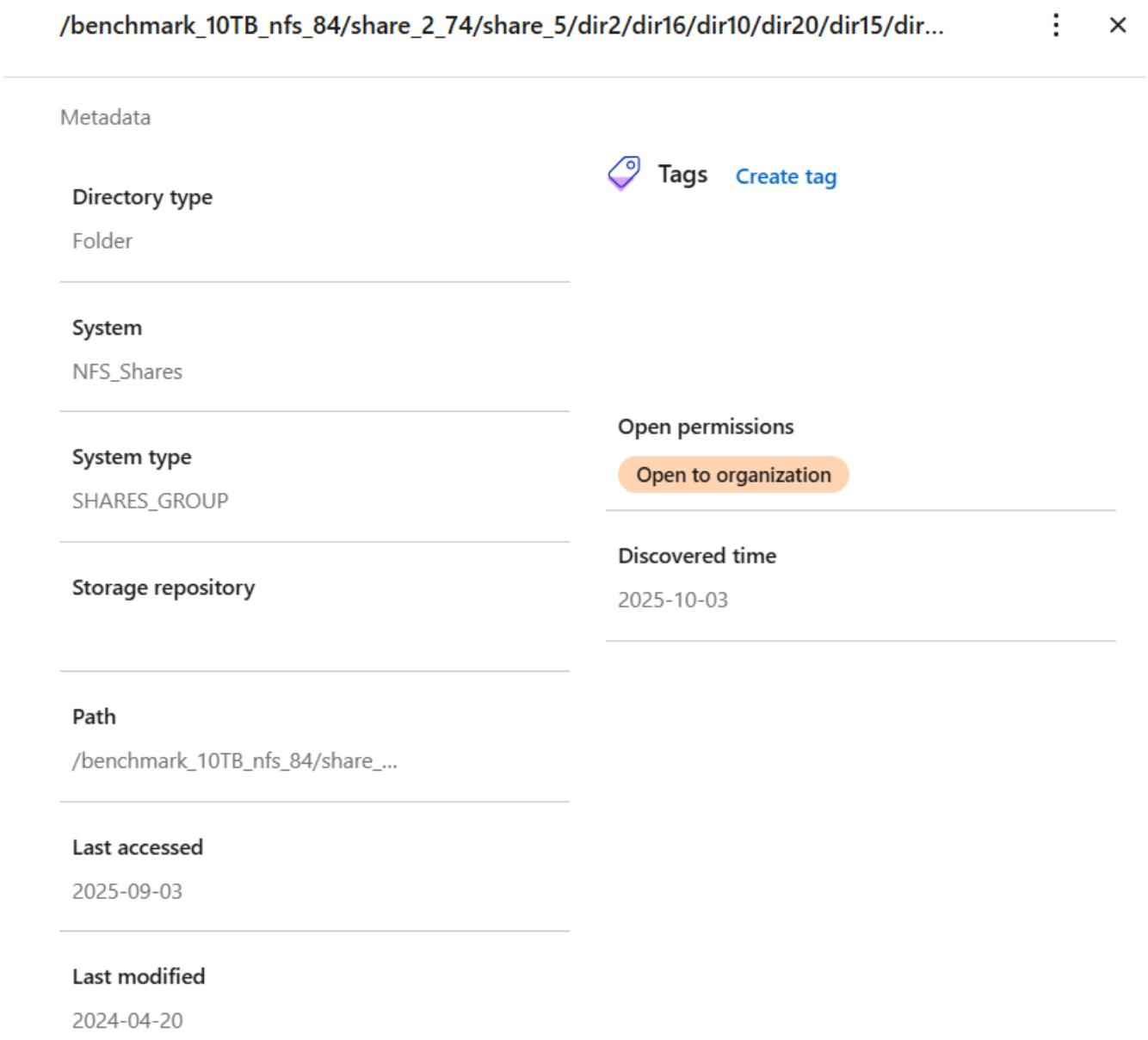


3. 특정 유형의 개인 데이터에 대한 세부 정보를 조사하려면 모두 보기*를 선택한 다음 특정 유형의 개인 데이터(예: 이메일 주소)에 대한 *조사 결과 화살표 아이콘을 선택합니다.

4. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하여 데이터를 조사하고, 조사 결과 화살표를 선택하여 가려진 정보를 확인하거나 파일 목록을 다운로드합니다.

   다음 이미지는 디렉토리(공유 및 폴더)에서 발견된 개인 데이터를 보여줍니다. 구조적 탭에서는 데이터베이스에서 찾은 개인 데이터를 볼 수 있습니다. 비정형 탭에서는 파일 수준 데이터를 볼 수 있습니다.





민감한 개인 데이터가 포함된 파일 보기

데이터 분류는 개인 정보 보호 규정에 정의된 대로 특수 유형의 민감한 개인 정보를 자동으로 식별합니다. "GDPR 제9조 및 제10조" . 예를 들어, 개인의 건강, 민족적 기원, 성적 지향에 대한 정보입니다. "전체 목록을 확인하세요" . 데이터 분류는 개별 파일, 디렉토리(공유 및 폴더) 내의 파일, 데이터베이스 테이블에서 이러한 유형의 정보를 식별합니다.

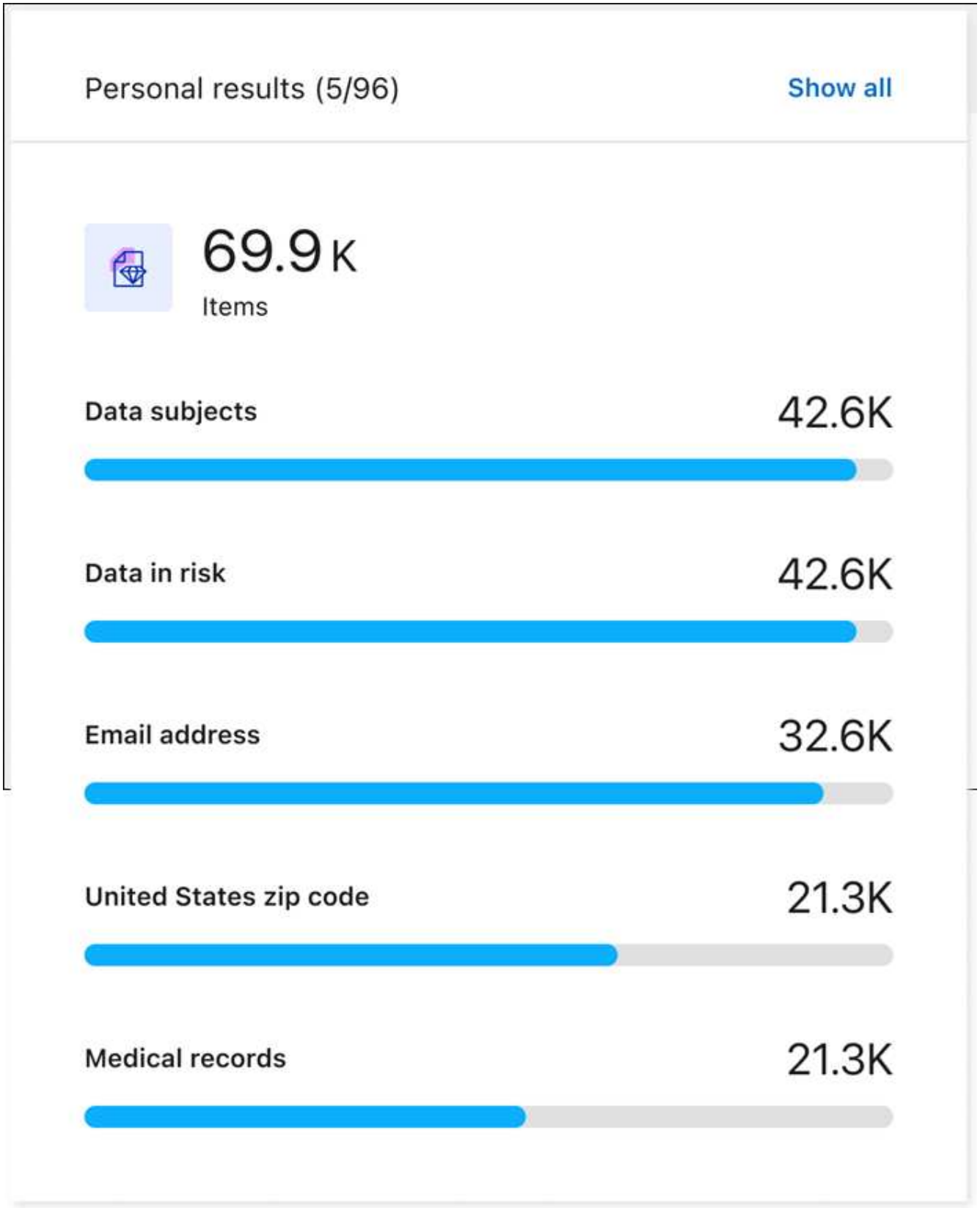
데이터 분류는 AI, 자연어 처리(NLP), 머신 러닝(ML), 인지 컴퓨팅(CC)을 사용하여 스캔하는 콘텐츠의 의미를 이해하고 엔터티를 추출하여 그에 따라 분류합니다.

예를 들어, 민감한 GDPR 데이터 범주 중 하나는 민족적 기원입니다. 데이터 분류는 자연어 처리(NLP) 기능을 갖추고 있어 "조지는 멕시코인이다"라는 문장(GDPR 제9조에 명시된 민감한 데이터를 나타냄)과 "조지는 멕시코 음식을 먹고 있다"라는 문장의 차이를 구분할 수 있습니다.

민감한 개인 데이터를 스캔할 때는 영어만 지원됩니다. 나중에 더 많은 언어에 대한 지원이 추가될 예정입니다.

단계

1. 데이터 분류 메뉴에서 *규정 준수*를 선택합니다.
2. 모든 민감한 개인 데이터의 세부 정보를 조사하려면 민감한 개인 결과 카드를 찾은 다음 모두 표시를 선택하세요.



.

3. 특정 유형의 민감한 개인 데이터에 대한 세부 정보를 조사하려면 모두 보기*를 선택한 다음 특정 유형의 민감한 개인 데이터에 대한 *조사 결과 화살표 아이콘을 선택하세요.
4. 검색, 정렬, 특정 파일에 대한 세부 정보 확장, *결과 조사*를 클릭하여 가려진 정보를 확인하거나 파일 목록을 다운로드하여 데이터를 조사합니다.

NetApp Data Classification 의 개인 데이터 범주

NetApp Data Classification 볼륨과 데이터베이스에서 식별할 수 있는 개인 데이터 유형은 다양합니다.

데이터 분류는 두 가지 유형의 개인 데이터를 식별합니다.

- 개인 식별 정보**(PII)**
- 민감한 개인 정보**(SPII)**

추가적인 국민 신분증 번호나 의료 식별자 등 다른 개인 데이터 유형을 식별하기 위한 데이터 분류가 필요한 경우 계정 관리자에게 문의하세요.

개인정보의 종류

파일에서 발견되는 개인 데이터, 즉 개인 식별 정보(PII)는 일반적인 개인 데이터이거나 국가 식별자일 수 있습니다. 아래 표의 세 번째 열은 데이터 분류가 다음을 사용하는지 여부를 식별합니다."근접성 검증" 식별자에 대한 결과를 검증합니다.

이러한 항목을 인식할 수 있는 언어는 표에 표시되어 있습니다.

유형	식별자	근접성 검증?	영어	독일 사람	스페인 사람	프랑스 국민	일본어
일반적인	신용카드 번호	예	✓	✓	✓		✓
	데이터 주체	아니요	✓	✓	✓		
	이메일 주소	아니요	✓	✓	✓		✓
	IBAN 번호(국제 은행 계좌 번호)	아니요	✓	✓	✓		✓
	IP 주소	아니요	✓	✓	✓		✓
	비밀번호	예	✓	✓	✓		✓

유형	식별자	근접성 검증?	영어	독일 사람	스페인 사람	프랑스 국민	일본어
국가 식별자							

유형	식별자	근접성 검증?	영어	독일 사람	스페인 사람	프랑스 국민	일본어

유형	식별자	근접성 검증?	영어	독일 사람	스페인 사람	프랑스 국민	일본어
	번호(Sozialversicherungsnummer)						
	독일 세금 식별 번호(Steuerliche Identifikationsnummer)	예	✓	✓	✓		
	그리스 신분증	예	✓	✓	✓		
	헝가리 세금 식별 번호	예	✓	✓	✓		
	아일랜드 신분증(PPS)	예	✓	✓	✓		
	이스라엘 신분증	예	✓	✓	✓		
	이탈리아 세금 식별 번호	예	✓	✓	✓		
	일본 개인식별번호(개인 및 법인 모두)	예	✓	✓	✓		✓
	라트비아 신분증	예	✓	✓	✓		
	리투아니아 신분증	예	✓	✓	✓		
	룩셈부르크 ID	예	✓	✓	✓		
	몰타 신분증	예	✓	✓	✓		
	국민건강보험공단(NHS) 번호	예	✓	✓	✓		
	뉴질랜드 은행 계좌	예	✓	✓	✓		
	뉴질랜드 운전면허증	예	✓	✓	✓		
	뉴질랜드 IRD 번호(세금 ID)	예	✓	✓	✓		
	뉴질랜드 NHI(국민건강지수) 수치	예	✓	✓	✓		
	뉴질랜드 여권 번호	예	✓	✓	✓		
	폴란드 신분증(PESEL)	예	✓	✓	✓		
	포르투갈 세금 식별 번호(NIF)	예	✓	✓	✓		
	루마니아 신분증(CNP)	예	✓	✓	✓		
	싱가포르 국민등록 신분증(NRIC)	예	✓	✓	✓		
	슬로베니아 신분증(EMSO)	예	✓	✓	✓		
	남아프리카 공화국 신분증	예	✓	✓	✓		
	스페인 세금 식별 번호	예	✓	✓	✓		
	스웨덴 신분증	예	✓	✓	✓		
	영국 신분증(NINO)	예	✓	✓	✓		
	미국 캘리포니아 운전면허증	예	✓	✓	✓		
	미국 인디애나 운전면허증	예	✓	✓	✓		
	미국 뉴욕 운전면허증	예	✓	✓	✓		
	미국 텍사스 운전면허증	예	✓	✓	✓		
	미국 사회보장번호(SSN)	예	✓	✓	✓		

민감한 개인 데이터의 유형

데이터 분류를 통해 파일에서 다음과 같은 민감한 개인 정보(SPII)를 찾을 수 있습니다.

다음 SPII는 현재 영어로만 인식 가능합니다.

- 형사소송참조: 자연인의 형사 유죄 판결 및 범죄에 관한 데이터.
- 민족 참조: 자연인의 인종 또는 민족적 기원에 관한 데이터.
- 건강정보: 개인의 건강에 관한 데이터입니다.
- **ICD-9-CM** 의료 코드: 의료 및 건강 산업에서 사용되는 코드입니다.
- **ICD-10-CM** 의료 코드: 의료 및 건강 산업에서 사용되는 코드입니다.
- 철학적 신념 참고: 자연인의 철학적 신념에 관한 데이터입니다.
- 정치적 의견 참고: 자연인의 정치적 의견에 관한 데이터입니다.
- 종교적 신념 참조: 자연인의 종교적 신념에 관한 데이터입니다.
- 성생활 또는 성적 지향에 대한 참고 자료: 자연인의 성생활 또는 성적 지향에 대한 데이터입니다.

카테고리 유형

데이터 분류는 다음과 같이 데이터를 분류합니다.

이러한 범주의 대부분은 영어, 독일어, 스페인어로 인식할 수 있습니다.

범주	유형	영어	독일 사람	스페인 사람
재원	대차대조표	✓	✓	✓
	구매 주문서	✓	✓	✓
	송장	✓	✓	✓
	분기별 보고서	✓	✓	✓
인사부	배경 조사	✓		✓
	보상 계획	✓	✓	✓
	직원 계약	✓		✓
	직원 리뷰	✓		✓
	건강	✓		✓
	이력서	✓	✓	✓
합법적인	비밀 유지 계약(NDA)	✓	✓	✓
	공급업체-고객 계약	✓	✓	✓
마케팅	캠페인	✓	✓	✓
	컨퍼런스	✓	✓	✓
운영	감사 보고서	✓	✓	✓
매상	판매 주문	✓	✓	

범주	유형	영어	독일 사람	스페인 사람
서비스	RFI	✓		✓
	RFP	✓		✓
	암퇘지	✓	✓	✓
	훈련	✓	✓	✓
지원하다	불만 및 티켓	✓	✓	✓

다음 메타데이터도 동일한 지원 언어로 분류되고 식별됩니다.

- 응용 프로그램 데이터
- 보관 파일
- 오디오
- 데이터 분류 비즈니스 애플리케이션 데이터의 빵가루
- CAD 파일
- 암호
- 부패한
- 데이터베이스 및 인덱스 파일
- 디자인 파일
- 이메일 신청 데이터
- 암호화됨(엔트로피 점수가 높은 파일)
- 실행 파일
- 재무 응용 데이터
- 건강 애플리케이션 데이터
- 이미지
- 로그
- 기타 문서
- 다양한 프레젠테이션
- 기타 스프레드시트
- 기타 "알 수 없음"
- 암호로 보호된 파일
- 구조화된 데이터
- 비디오
- 0바이트 파일

파일 유형

데이터 분류는 모든 파일을 스캔하여 범주 및 메타데이터에 대한 통찰력을 제공하고 대시보드의 파일 유형 섹션에 모든

파일 유형을 표시합니다. 데이터 분류가 개인 식별 정보(PII)를 감지하거나 DSAR 검색을 수행하는 경우 다음 파일 형식만 지원됩니다.

`.CSV, .DCM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides`

발견된 정보의 정확성

NetApp 데이터 분류를 통해 식별된 개인 데이터 및 민감한 개인 데이터의 정확성을 100% 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 검증해야 합니다.

아래 표는 테스트 결과에 따르면 데이터 분류를 통해 찾은 정보의 정확도를 보여줍니다. 이를 _정밀도_와 _재현율_로 구분해 보겠습니다.

정도

데이터 분류에서 찾은 내용이 올바르게 식별되었을 확률입니다. 예를 들어, 개인 데이터의 정확도가 90%라는 것은 개인 정보가 포함된 것으로 확인된 파일 10개 중 9개가 실제로 개인 정보를 포함하고 있다는 것을 의미합니다. 10개 파일 중 1개는 거짓 양성입니다.

상기하다

데이터 분류가 무엇을 찾아야 할지 알 수 있는 확률입니다. 예를 들어, 개인 데이터의 회수율이 70%라는 것은 데이터 분류를 통해 조직 내에서 실제로 개인 정보가 포함된 파일 10개 중 7개를 식별할 수 있다는 것을 의미합니다. 데이터 분류를 수행하면 데이터의 30%가 누락되어 대시보드에 나타나지 않습니다.

우리는 결과의 정확도를 지속적으로 개선하고 있습니다. 이러한 개선 사항은 향후 데이터 분류 릴리스에서 자동으로 제공됩니다.

유형	정도	상기하다
개인 정보 - 일반	90%-95%	60%-80%
개인 정보 - 국가 식별자	30%-60%	40%-60%
민감한 개인 데이터	80%-95%	20%-30%
카테고리	90%-97%	60%-80%

NetApp Data Classification 에서 사용자 정의 분류 만들기

NetApp Data Classification 하면 조직의 규제 및 준수 요구 사항에 맞는 데이터를 식별하기 위해 사용자 지정 범주 또는 개별 식별자를 생성할 수 있습니다.

데이터 분류는 범주형과 개인 식별자형, 두 가지 유형의 사용자 지정 분류기를 지원합니다. 사용자 지정 카테고리는 사용자가 업로드한 파일 세트를 기반으로 생성되며, 데이터 분류 기능은 이를 통해 조직 내 유사한 데이터를 식별하는 AI 모델을 구축합니다(예: 의료 연구 기관은 임상 분석 카테고리를 생성할 수 있습니다). 사용자 지정 개인 식별자는 키워드 목록 또는 정규 표현식(regex)을 사용하여 생성되며, 규정 준수 위험을 초래할 수 있는 조직별 특정 정보를 식별하는 데 사용됩니다.

모든 사용자 지정 분류는 사용자 지정 분류 대시보드에서 확인할 수 있습니다.

사용자 지정 개인 식별자를 생성하세요

데이터 분류 기능을 사용하면 문맥 키워드 또는 정규 표현식을 사용하여 조직 고유의 데이터를 식별하는 맞춤형 개인 식별자를 생성할 수 있습니다.

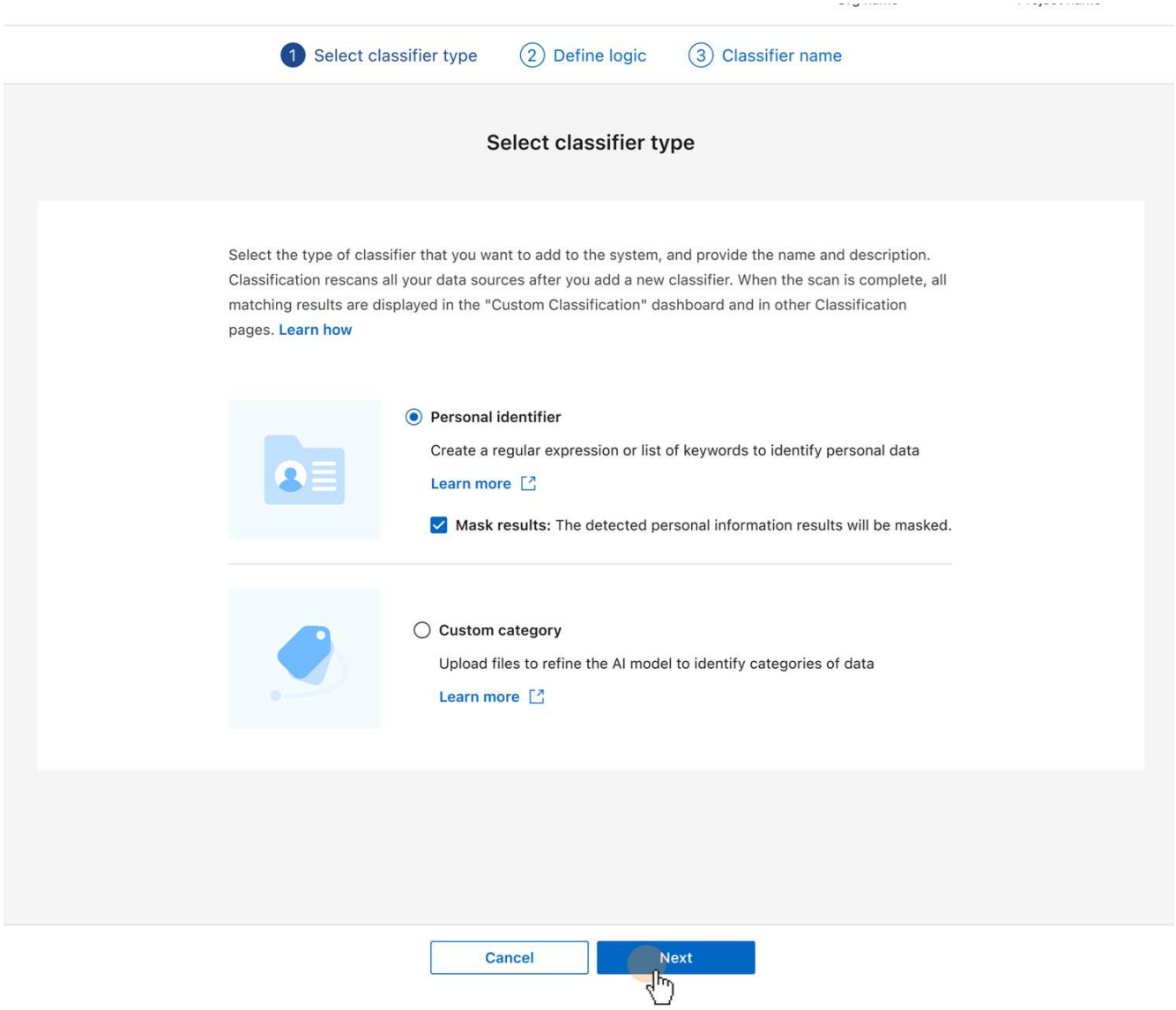
키워드 요구 사항

키워드 목록을 사용하여 개인 식별자를 생성하는 경우, 해당 목록은 다음 요구 사항을 충족해야 합니다.

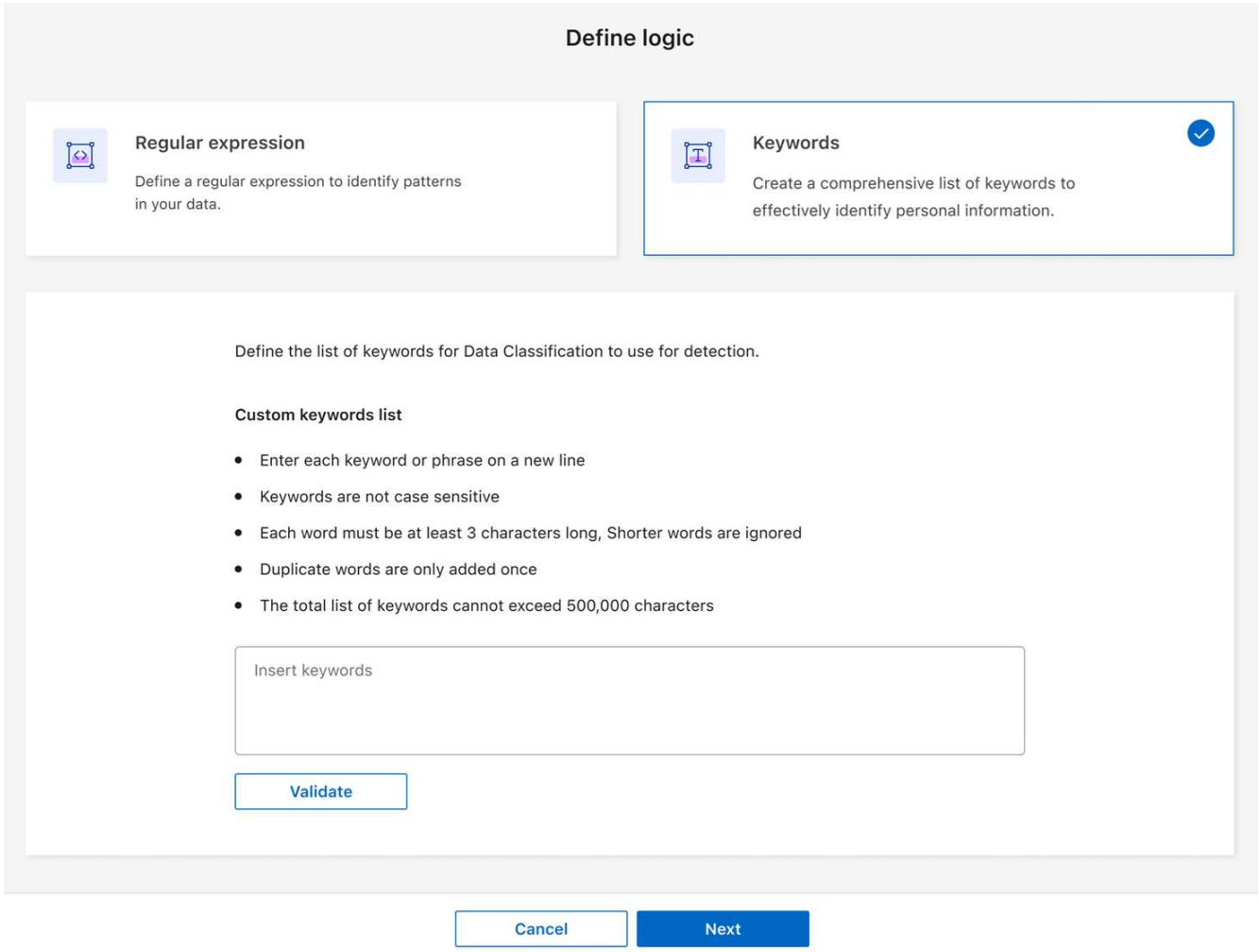
- 키워드 입력은 대소문자를 구분하지 않습니다.
- 키워드는 최소 세 글자 이상이어야 합니다. 세 글자 미만의 단어는 모두 무시됩니다.
- 중복되는 단어는 한 번만 추가됩니다.
- 키워드 목록의 총 길이는 50만 자를 초과할 수 없습니다. 목록에는 최소 하나 이상의 키워드가 포함되어야 합니다.

단계

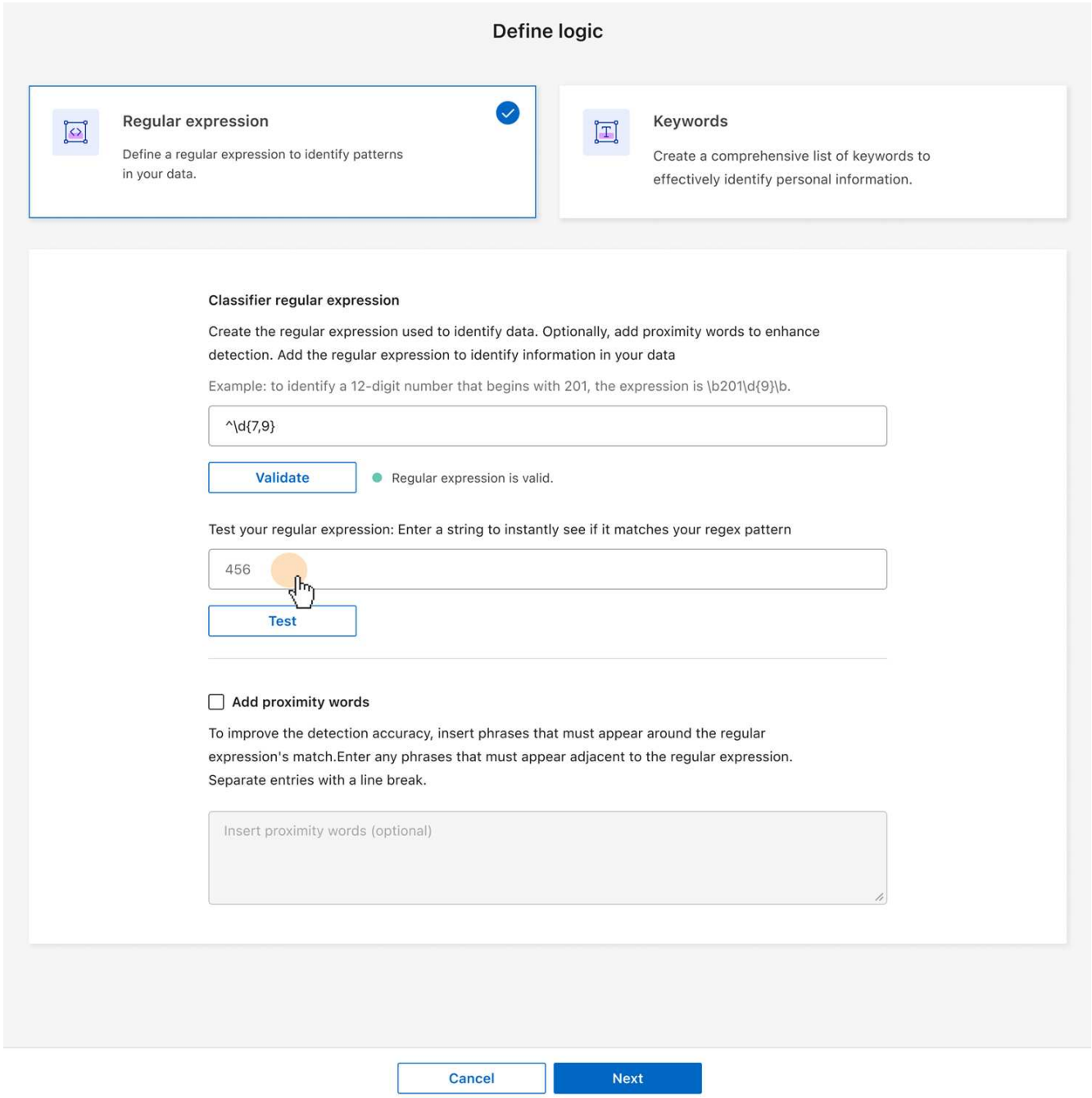
1. 사용자 정의 분류 탭을 선택합니다.
2. 사용자 지정 분류기를 만들려면 **+** 새 분류기를 선택하세요.
3. *개인 식별자*를 선택하세요. 선택적으로 결과 마스킹을 선택하여 감지된 개인 정보를 가릴 수 있습니다.
4. 다음을 선택하세요.



5. 키워드를 사용하여 분류기를 추가하려면 키워드를 선택하십시오. 각 항목을 한 줄씩 입력하여 키워드 목록을 작성하세요. 키워드가 요구 사항을 충족하는지 확인하십시오.



분류기를 정규 표현식으로 추가하려면 정규 표현식을 선택한 다음 데이터의 특정 정보를 감지하는 패턴을 추가하세요. 입력 내용의 구문을 확인하려면 유효성 검사를 선택하세요.



a. 선택적으로, 정규 표현식 패턴과 일치해야 하는 샘플 문자열을 입력한 다음 테스트를 선택하여 확인하십시오.

b. 선택적으로 근접어를 추가할 수 있습니다. 근접어를 추가하면 데이터 분류는 근접어가 일치하는 문자열에 인접해 있는 경우에만 정규 표현식 패턴에 플래그를 지정합니다.

6. 다음을 선택하세요.
7. 대시보드에서 사용자 지정 카테고리를 식별하려면 분류기 이름과 설명을 입력하세요.
8. 사용자 지정 개인 식별자를 생성하려면 저장을 선택하십시오.

사용자 지정 개인 식별자를 생성하면 해당 결과가 다음 예약된 검사에 반영됩니다. 결과를 더 빨리 얻으려면 필요할 때 스캔을 실행하세요. 결과를 보려면 다음을 참조하세요. 규정 준수 보고서 생성.

사용자 지정 카테고리를 만드세요

사용자 지정 카테고리를 사용하면 조직에 특화된 데이터 분류가 가능합니다. 사용자 지정 카테고리는 사용자가 업로드한 텍스트 파일을 기반으로 생성되며, 데이터 분류 기능은 이를 바탕으로 AI 모델을 만들어 다른 파일에서 유사한 정보를 식별합니다.

훈련 데이터 요구 사항

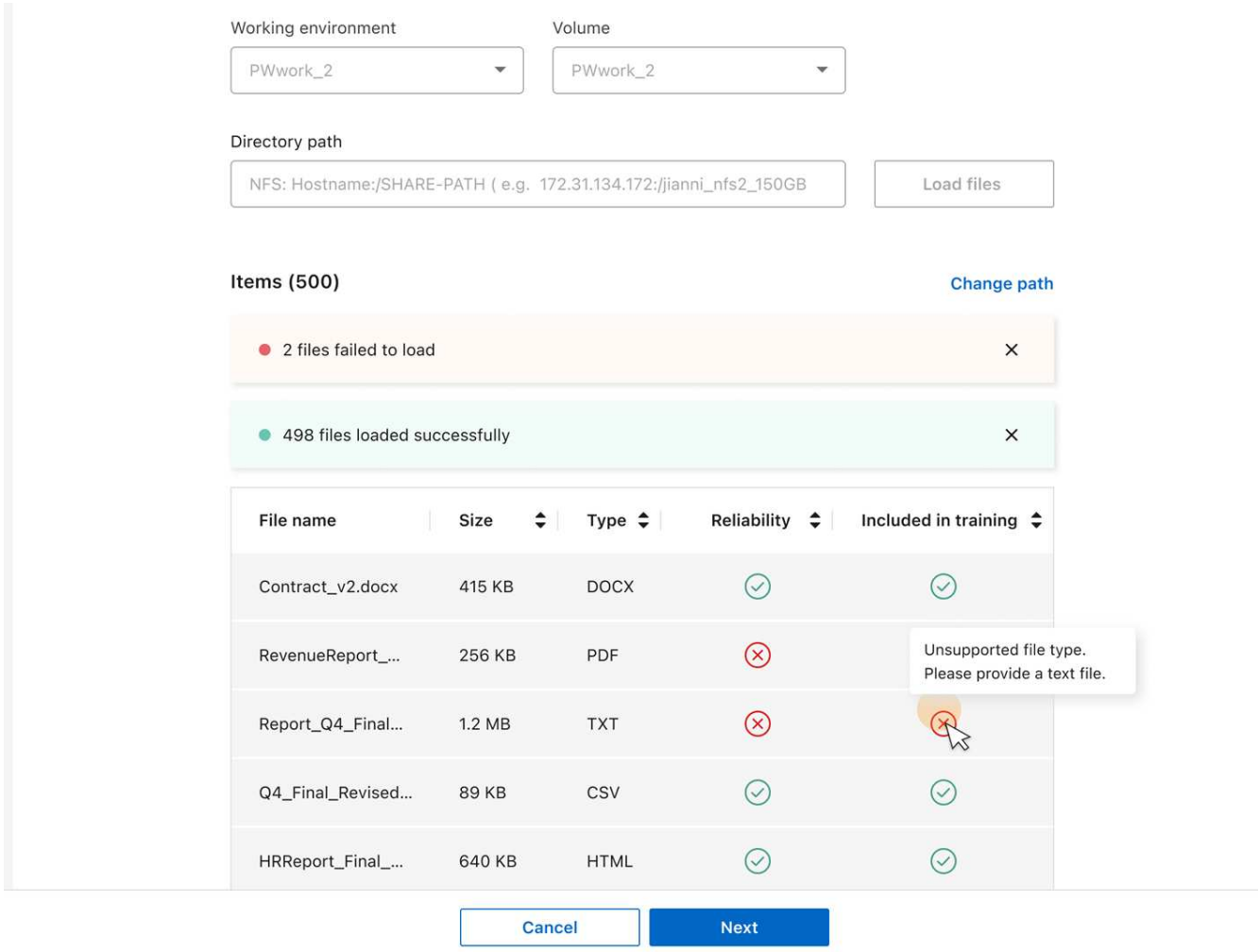
- 학습 데이터 세트는 최소 25개의 파일을 포함해야 합니다. 최대 파일 개수는 1,000개입니다.
- 모든 파일은 제공하신 파일 경로에 직접 위치해야 합니다.
- 모든 파일의 크기는 100바이트보다 커야 합니다.
- 데이터 분류 학습 데이터는 CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS 또는 XLSX 파일 형식 중 하나여야 합니다. 지원되는 모든 파일 형식을 조합하여 업로드할 수 있습니다.

단계

1. NetApp Data Classification 에서 *사용자 지정 분류*를 선택합니다.
2. *+ 새 분류기*를 선택하세요.
3. 분류 유형으로 *사용자 지정 카테고리*를 선택한 다음 다음을 클릭하세요.
4. 텍스트 기반 파일 모음을 사용하여 사용자 지정 카테고리에 대한 로직을 정의하세요. *작업 주소*의 IP 주소를 입력한 다음 드롭다운 메뉴에서 *볼륨*을 선택하십시오.

   학습 데이터가 포함된 디렉터리의 디렉터리 경로를 입력하십시오.

5. 파일 검사를 수행하려면 데이터 분류에서 파일 불러오기를 선택하십시오. 파일이 교육용으로 적합하다고 판단되면 파일 이름, 크기, 유형 및 참고 사항이 나열된 파일 요약을 검토할 수 있습니다.



Data Classification은 데이터 학습에 필요한 예상 완료 시간을 표시합니다. .. 파일 경로를 변경하거나 파일을 다시 업로드하려면 **Change path**를 선택한 다음 데이터를 입력하고 파일을 다시 로드하십시오.

6. 업로드된 파일에 만족하시면 다음을 선택하세요.
7. 대시보드에서 사용자 지정 카테고리를 식별하려면 분류기 이름과 설명을 입력하세요.
8. 저장을 선택하여 사용자 지정 카테고리를 만드세요.

결과

사용자 지정 카테고리를 생성하면 해당 결과가 다음 예약된 스캔에 반영됩니다. 결과를 더 빨리 얻으려면 수동으로 스캔을 시작하세요.

사용자 지정 분류기를 편집합니다

개인 식별자를 생성한 후에도 해당 식별자의 로직을 수정할 수 있습니다. 개인 식별자의 유형이나 논리 유형은 변경할 수 없습니다. 예를 들어 사용자 지정 범주를 사용자 지정 개인 식별자로 변경할 수 없습니다. 키워드 기반 사용자 지정 식별자를 정규 표현식 기반 사용자 지정 식별자로 변경할 수도 없습니다.

단계

1. NetApp Data Classification 에서 *사용자 지정 분류*를 선택합니다.
2. 삭제하려는 분류기를 선택한 다음 작업 메뉴를 선택하세요. ... 줄의 맨 끝에.

3. 논리 편집을 선택하세요.
4. 키워드를 수정하려면 해당 키워드를 추가, 삭제 또는 편집하세요. 정규 표현식을 수정하는 경우 새 정규 표현식을 입력하고 유효성을 검사하십시오. 선택적으로 근접 키워드를 추가할 수 있습니다.
5. 변경 사항을 적용하려면 저장을 선택하세요.

사용자 지정 분류기를 삭제합니다

1. NetApp Data Classification 에서 *사용자 지정 분류*를 선택합니다.
2. 삭제하려는 분류기를 선택한 다음 작업 메뉴를 선택하세요. … 줄의 맨 끝에.
3. 분류자 삭제를 선택하세요.

다음 단계

- 규정 준수 보고서 생성

NetApp Data Classification 사용하여 조직에 저장된 데이터를 조사하세요

데이터 조사 대시보드는 파일 및 디렉터리 수준의 데이터 통찰력을 표시하여 결과를 정렬하고 필터링할 수 있습니다. 데이터 조사 페이지에서는 파일 및 디렉토리 메타데이터와 권한에 대한 통찰력을 제공하고 중복 파일을 식별합니다. 파일, 디렉토리, 데이터베이스 수준의 통찰력을 바탕으로 조직의 규정 준수를 개선하고 저장 공간을 절약하기 위한 조치를 취할 수 있습니다. 데이터 조사 페이지에서는 파일 이동, 복사, 삭제도 지원합니다.

조사 페이지에서 통찰력을 얻으려면 데이터 소스에 대한 전체 분류 스캔을 수행해야 합니다. 매핑 전용 스캔을 거친 데이터 소스에는 파일 수준 세부 정보가 표시되지 않습니다.

데이터 조사 구조

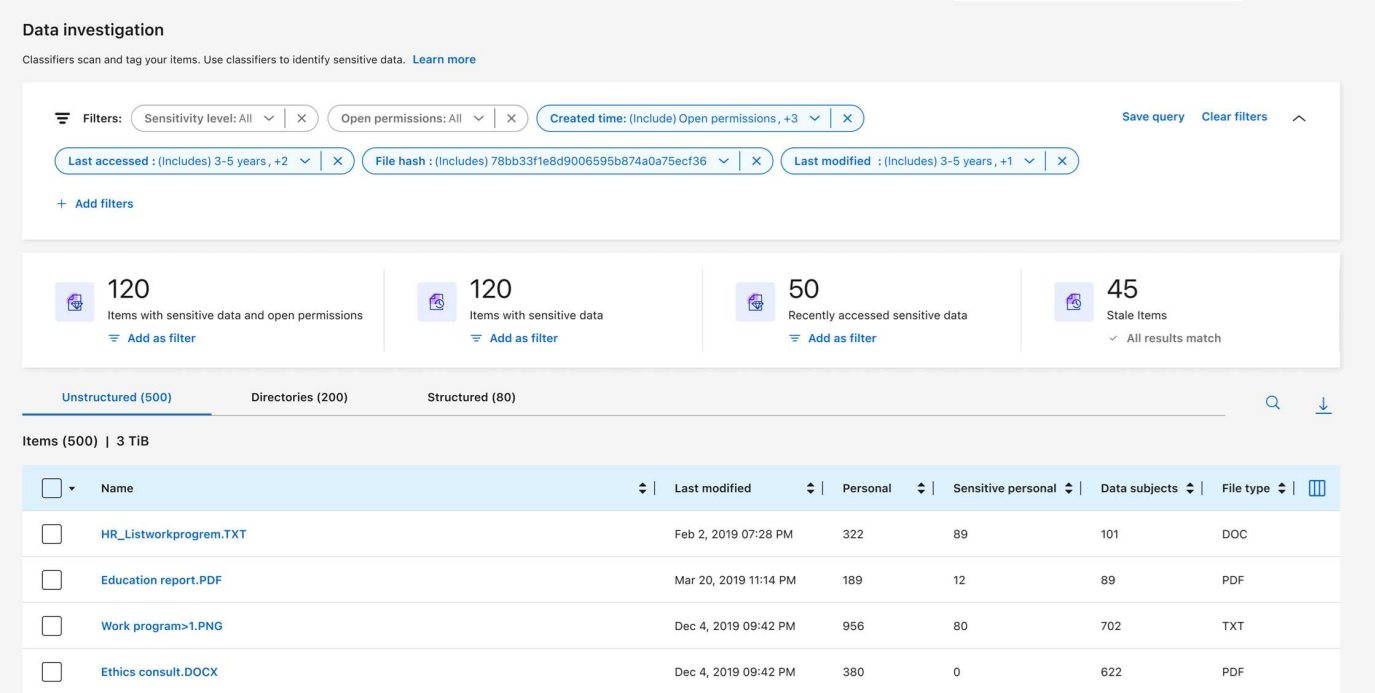
데이터 조사 페이지는 데이터를 세 개의 탭으로 분류합니다.

- 비정형 데이터: 파일 데이터
- 디렉토리: 폴더 및 파일 공유
- 구조화된: 데이터베이스

데이터 필터

데이터 조사 페이지는 다양한 필터를 제공하여 데이터를 정렬하여 필요한 정보를 찾을 수 있도록 해줍니다. 여러 필터를 함께 사용할 수 있습니다.

필터를 추가하려면 필터 추가 버튼을 선택하세요.



필터 감도 및 콘텐츠

다음 필터를 사용하여 데이터에 얼마나 많은 민감한 정보가 포함되어 있는지 확인하세요.

필터	세부
범주	선택하세요"카테고리 유형" .
민감도 수준	민감도 수준을 선택하세요: 개인, 민감한 개인, 민감하지 않음.
식별자의 수	파일별로 감지된 민감한 식별자의 범위를 선택합니다. 개인정보와 민감한 개인정보가 포함됩니다. 디렉토리에서 필터링할 때, 데이터 분류는 각 폴더(및 하위 폴더)에 있는 모든 파일의 일치 항목을 합산합니다. 참고: 2023년 12월(버전 1.26.6) 릴리스에서는 디렉토리별 개인 식별 정보(PII) 데이터 수를 계산하는 옵션이 제거되었습니다.
개인 정보	선택하세요"개인 정보 유형" .
민감한 개인 데이터	선택하세요"민감한 개인 데이터의 유형" .
데이터 주체	데이터 주체의 성명 또는 알려진 식별자를 입력하세요. "여기에서 데이터 주체에 대해 자세히 알아보세요." .

사용자 소유자 및 사용자 권한 필터링

다음 필터를 사용하여 파일 소유자와 데이터 액세스 권한을 확인하세요.

필터	세부
공개 권한	데이터와 폴더/공유 내에서 권한 유형을 선택하세요.
사용자/그룹 권한	하나 이상의 사용자 이름 및/또는 그룹 이름을 선택하거나 이름의 일부를 입력하세요.
파일 소유자	파일 소유자 이름을 입력하세요.

필터	세부
접근 권한이 있는 사용자 수	하나 이상의 카테고리 범위를 선택하여 특정 수의 사용자에게 공개되는 파일과 폴더를 표시합니다.

시간순으로 필터링

다음 필터를 사용하여 시간 기준에 따라 데이터를 확인하세요.

필터	세부
생성 시간	파일이 생성된 시간 범위를 선택하세요. 검색 결과를 더욱 구체화하기 위해 사용자 정의 시간 범위를 지정할 수도 있습니다.
발견된 시간	데이터 분류가 파일을 발견한 시간 범위를 선택하세요. 검색 결과를 더욱 구체화하기 위해 사용자 정의 시간 범위를 지정할 수도 있습니다.
마지막 수정일	파일이 마지막으로 수정된 시간 범위를 선택하세요. 검색 결과를 더욱 구체화하기 위해 사용자 정의 시간 범위를 지정할 수도 있습니다.
마지막 접속	파일이나 디렉토리*에 마지막으로 액세스한 시간 범위를 선택하세요. 검색 결과를 더욱 구체화하기 위해 사용자 정의 시간 범위를 지정할 수도 있습니다. 데이터 분류가 스캔하는 파일 유형의 경우, 이는 데이터 분류가 해당 파일을 스캔한 마지막 시간입니다.

{별표} 디렉토리의 마지막 액세스 시간은 NFS 또는 CIFS 공유에만 사용할 수 있습니다.

필터 메타데이터

다음 필터를 사용하여 위치, 크기, 디렉토리 또는 파일 유형을 기준으로 데이터를 확인하세요.

필터	세부
파일 경로	쿼리에 포함하거나 제외할 부분 또는 전체 경로를 최대 20개 입력하세요. 포함 경로와 제외 경로를 모두 입력하면 데이터 분류는 먼저 포함 경로에 있는 모든 파일을 찾은 다음 제외 경로에서 파일을 제거한 다음 결과를 표시합니다. 이 필터에서 "*"를 사용해도 아무런 효과가 없으며, 특정 폴더를 검사에서 제외할 수 없습니다. 구성된 공유 아래의 모든 디렉터리와 파일이 검사됩니다.
디렉토리 유형	디렉토리 유형을 "공유" 또는 "폴더" 중에서 선택하세요.
파일 형식	선택하세요"파일 유형" .
파일 크기	파일 크기 범위를 선택하세요.
파일 해시	이름이 다르더라도 특정 파일을 찾으려면 파일 해시를 입력하세요.

필터 보관 유형

다음 필터를 사용하여 저장 유형별로 데이터를 확인하세요.

필터	세부
시스템 유형	시스템 유형을 선택하세요.
시스템 환경 이름	특정 시스템을 선택하세요.

필터	세부
저장소 저장소	볼륨이나 스키마 등 저장소 저장소를 선택합니다.

필터 쿼리

다음 필터를 사용하여 저장된 쿼리별로 데이터를 확인하세요.

필터	세부
저장된 쿼리	저장된 쿼리를 하나 또는 여러 개 선택하세요. 로 가다"저장된 쿼리 탭" 기존에 저장된 쿼리 목록을 보고 새 쿼리를 만듭니다.
태그	선택하다"태그 또는 태그들" 귀하의 파일에 할당된 것입니다.

필터 분석 상태

다음 필터를 사용하여 데이터 분류 스캔 상태별로 데이터를 확인하세요.

필터	세부
분석 상태	보류 중인 첫 번째 검사, 검사 완료, 보류 중인 재검사 또는 검사에 실패한 파일 목록을 표시하는 옵션을 선택하세요.
스캔 분석 이벤트	데이터 분류에서 마지막 액세스 시간을 되돌릴 수 없어 분류되지 않은 파일을 볼지, 아니면 데이터 분류에서 마지막 액세스 시간을 되돌릴 수 없어도 분류된 파일을 볼지 선택합니다.

""마지막 액세스 시간" 타임스탬프에 대한 세부 정보 보기"스캔 분석 이벤트를 사용하여 필터링할 때 조사 페이지에 나타나는 항목에 대한 자세한 내용은 다음을 참조하세요.

중복된 데이터 필터링

다음 필터를 사용하여 저장소에 중복된 파일을 확인하세요.

필터	세부
중복	파일이 저장소에 복제되는지 여부를 선택합니다.

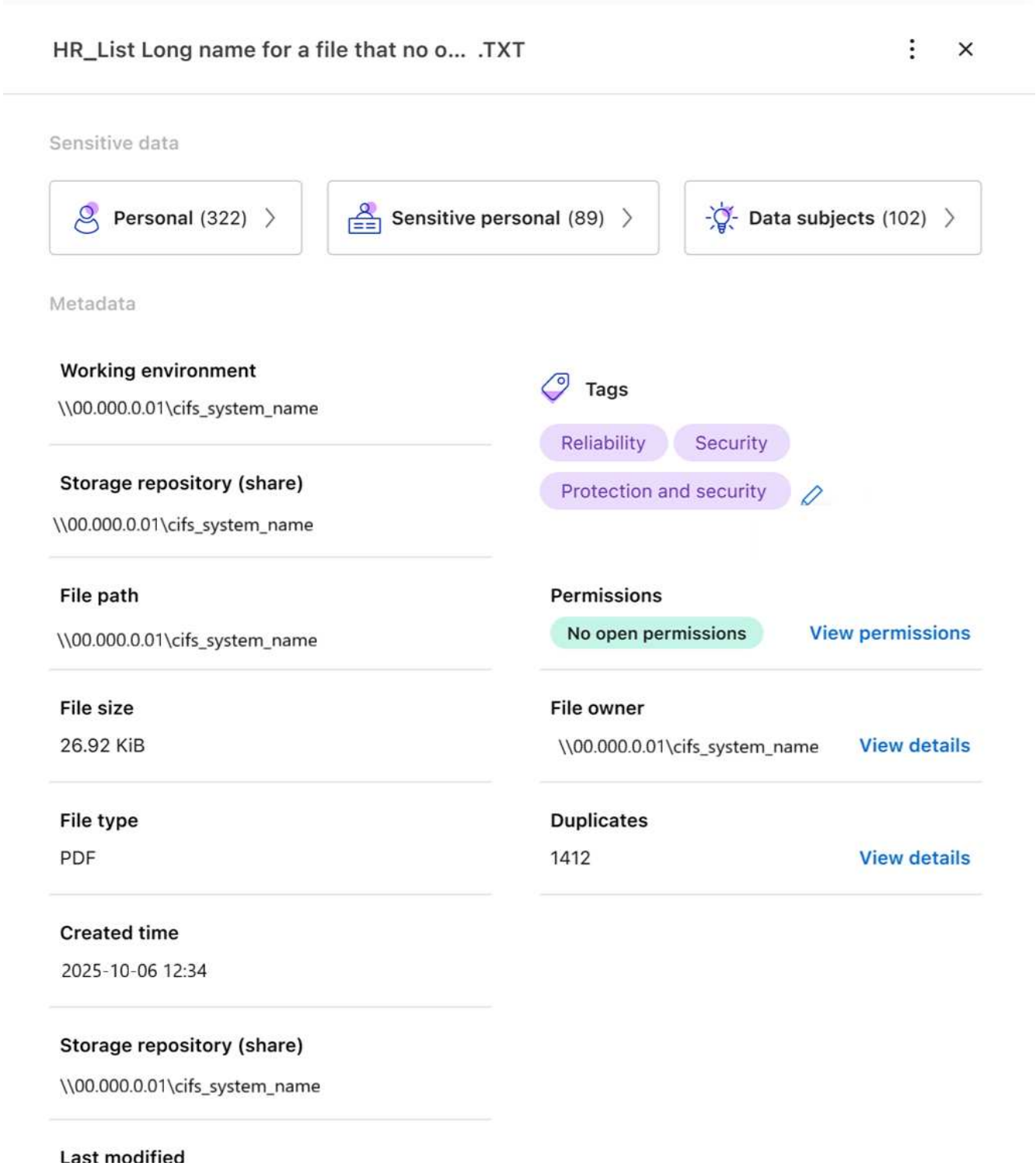
파일 메타데이터 보기

메타데이터는 파일이 있는 시스템과 볼륨을 보여줄 뿐만 아니라 파일 권한, 파일 소유자, 해당 파일의 중복 여부 등 훨씬 더 많은 정보를 보여줍니다. 이 정보는 당신이 계획하고 있다면 유용합니다"저장된 쿼리 생성" 데이터를 필터링하는 데 사용할 수 있는 모든 정보를 볼 수 있기 때문입니다.

정보의 가용성은 데이터 소스에 따라 달라집니다. 예를 들어, 데이터베이스 파일의 볼륨 이름과 권한은 공유되지 않습니다.

단계

1. 데이터 분류 메뉴에서 *조사*를 선택합니다.
2. 오른쪽의 데이터 조사 목록에서 아래쪽 캐럿을 선택하세요. 각 파일의 오른쪽에 있는 버튼을 클릭하면 파일 메타데이터를 볼 수 있습니다.



3. 선택적으로 태그 생성 버튼을 사용하여 파일에 태그를 생성하거나 추가할 수 있습니다. 드롭다운 메뉴에서 기존 태그를 선택하거나 **+** 추가 버튼을 사용하여 새 태그를 추가합니다. 태그를 사용하여 데이터를 필터링할 수 있습니다.

파일 및 디렉토리에 대한 사용자 권한 보기

파일이나 디렉토리에 액세스할 수 있는 모든 사용자 또는 그룹과 해당 사용자가 가진 권한 유형을 나열한 목록을 보려면 *모든 권한 보기*를 선택합니다. 이 옵션은 CIFS 공유의 데이터에만 사용할 수 있습니다.

사용자 및 그룹 이름 대신 보안 식별자(SID)를 사용하는 경우 Active Directory를 데이터 분류에 통합해야 합니다.

자세한 내용은 다음을 참조하세요. "데이터 분류에 Active Directory 추가" .

단계

1. 데이터 분류 메뉴에서 *조사*를 선택합니다.
2. 오른쪽의 데이터 조사 목록에서 아래쪽 캐럿을 선택하세요. 각 파일의 오른쪽에 있는 버튼을 클릭하면 파일 메타데이터를 볼 수 있습니다.
3. 파일이나 디렉토리에 액세스할 수 있는 모든 사용자 또는 그룹과 이들이 가진 권한 유형을 나열하려면, 열린 권한 필드에서 *모든 권한 보기*를 선택합니다.

   데이터 분류에서는 목록에 최대 100명의 사용자가 표시됩니다.

4. 아래쪽 캐럿을 선택하세요 그룹에 속한 사용자 목록을 보려면 해당 그룹의 버튼을 클릭하세요.

   그룹의 한 수준을 확장하면 그룹에 속한 사용자를 볼 수 있습니다.

5. 사용자 또는 그룹 이름을 선택하면 조사 페이지가 새로 고쳐져 해당 사용자 또는 그룹이 액세스할 수 있는 모든 파일과 디렉터리를 볼 수 있습니다.

저장 시스템에서 중복 파일을 확인하세요

저장 시스템에 중복된 파일이 저장되어 있는지 확인할 수 있습니다. 이 기능은 저장 공간을 절약할 수 있는 영역을 파악하는 데 유용합니다. 특정 권한이나 민감한 정보가 있는 특정 파일이 저장 시스템에 불필요하게 복제되지 않도록 하는 것도 좋습니다.

데이터 분류는 다음과 같은 경우 모든 파일(데이터베이스 제외)의 중복을 비교합니다.

- 1MB 이상
- 또는 개인 정보나 민감한 개인 정보가 포함되어 있습니다.

데이터 분류는 해싱 기술을 사용하여 중복 파일을 확인합니다. 어떤 파일의 해시 코드가 다른 파일과 동일하다면, 파일 이름이 다르더라도 두 파일은 정확히 중복됩니다.

단계

1. 데이터 분류 메뉴에서 *조사*를 선택합니다.
2. 필터 창에서 "파일 크기"와 "중복"("중복 있음")을 선택하여 특정 크기 범위의 파일 중 사용자 환경에서 중복된 파일을 확인합니다.
3. 선택적으로 중복 파일 목록을 다운로드하여 스토리지 관리자에게 보내면 어떤 파일을 삭제할지 결정할 수 있습니다.
4. 선택적으로 중복된 파일을 삭제, 태그 지정 또는 이동할 수 있습니다. 작업을 수행할 파일을 선택한 다음, 적절한 작업을 선택합니다.

특정 파일이 중복되었는지 확인

단일 파일에 중복이 있는지 확인할 수 있습니다.

단계

1. 데이터 분류 메뉴에서 *조사*를 선택합니다.
2. 데이터 조사 목록에서 다음을 선택하세요. 각 파일의 오른쪽에 있는 버튼을 클릭하면 파일 메타데이터를 볼 수

있습니다.

파일에 중복이 있는 경우 이 정보는 중복 필드 옆에 나타납니다.

3. 중복 파일 목록과 해당 위치를 보려면 *세부 정보 보기*를 선택하세요.
4. 다음 페이지에서 *중복 보기*를 선택하여 조사 페이지에서 파일을 확인하세요.
5. 선택적으로 중복된 파일을 삭제, 태그 지정 또는 이동할 수 있습니다. 작업을 수행할 파일을 선택한 다음, 적절한 작업을 선택합니다.

이 페이지에 제공된 "파일 해시" 값을 사용하여 조사 페이지에 직접 입력하면 언제든지 특정 중복 파일을 검색할 수 있습니다. 또는 저장된 쿼리에서 사용할 수도 있습니다.

보고서를 다운로드하세요

필터링된 결과를 CSV 또는 JSON 형식으로 다운로드할 수 있습니다.

데이터 분류가 파일(비정형 데이터), 디렉토리(폴더 및 파일 공유), 데이터베이스(정형 데이터)를 스캔하는 경우 최대 3개의 보고서 파일을 다운로드할 수 있습니다.

파일은 고정된 수의 행 또는 레코드가 있는 파일로 분할됩니다.

- JSON: 보고서당 100,000개의 레코드가 생성되는데 걸리는 시간은 약 5분입니다.
- CSV: 보고서당 200,000개의 레코드가 생성되는데 걸리는 시간은 약 4분입니다.

이 브라우저에서 볼 수 있도록 CSV 파일 버전을 다운로드할 수 있습니다. 이 버전은 10,000개의 레코드로 제한됩니다.

다운로드 가능한 보고서에 포함된 내용

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

- 파일 이름
- 위치 유형
- 시스템 이름
- 저장소 저장소(예: 볼륨, 버킷, 공유)
- 저장소 유형
- 파일 경로
- 파일 유형
- 파일 크기(MB)
- 생성 시간
- 마지막 수정
- 마지막 접속
- 파일 소유자

    - 파일 소유자 데이터에는 Active Directory가 구성된 경우 계정 이름, SAM 계정 이름 및 이메일 주소가 포함됩니다.
- 범주
- 개인정보
- 민감한 개인 정보
- 공개 권한
- 스캔 분석 오류
- 삭제 감지 날짜

  삭제 감지 날짜는 파일이 삭제되거나 이동된 날짜를 식별합니다. 이를 통해 중요한 파일이 이동된 시점을 식별할 수 있습니다. 삭제된 파일은 대시보드나 조사 페이지에 표시되는 파일 번호 수에 포함되지 않습니다. 해당 파일은 CSV 보고서에만 나타납니다.

*비정형 디렉터리 데이터 보고서*에는 폴더와 파일 공유에 대한 다음 정보가 포함됩니다.

- 시스템 유형
- 시스템 이름
- 디렉토리 이름
- 저장 저장소(예: 폴더 또는 파일 공유)
- 디렉토리 소유자
- 생성 시간
- 발견된 시간
- 마지막 수정
- 마지막 접속
- 공개 권한
- 디렉토리 유형

*구조화된 데이터 보고서*에는 데이터베이스 테이블에 대한 다음 정보가 포함됩니다.

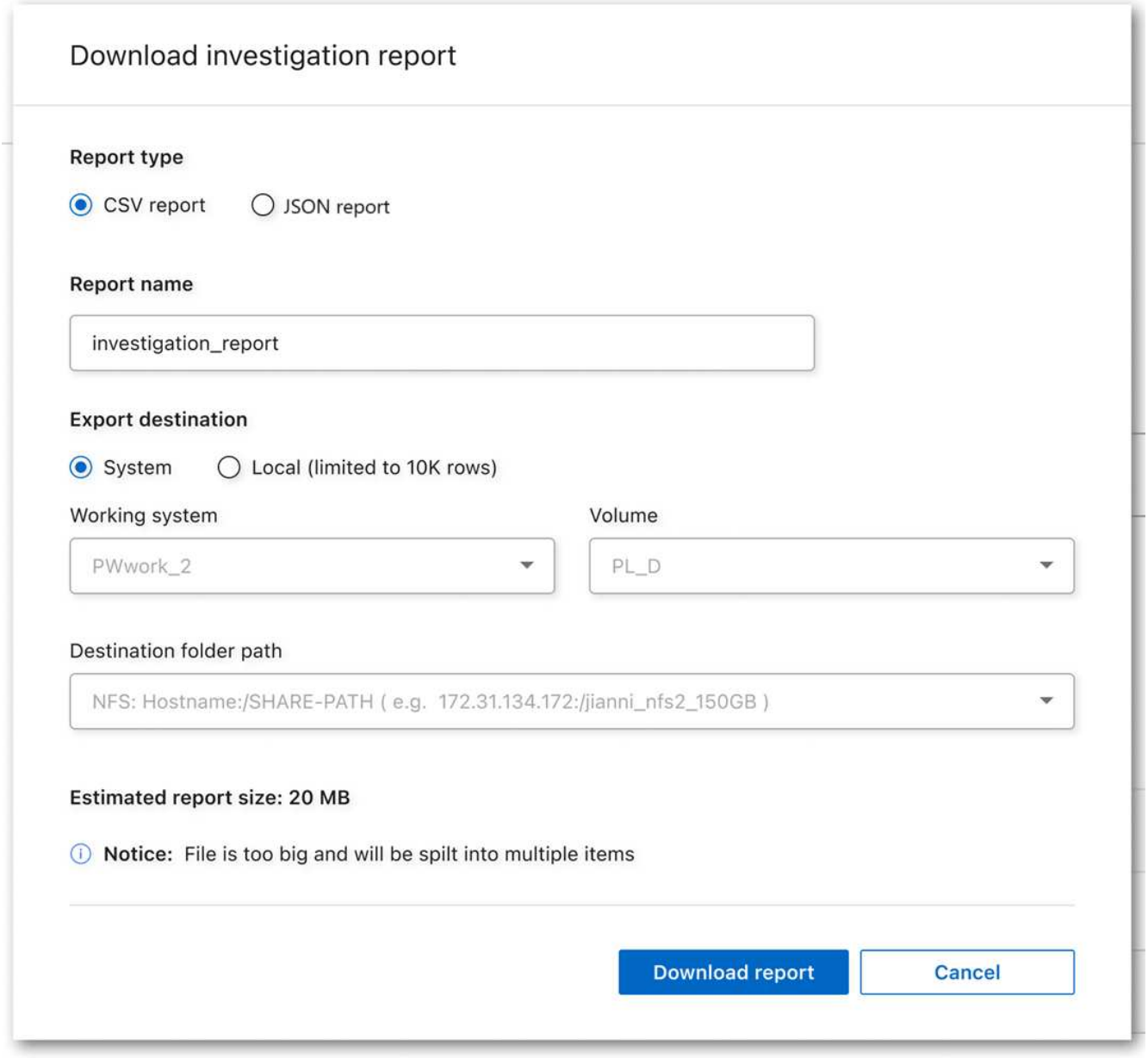
- DB 테이블 이름
- 위치 유형
- 시스템 이름
- 저장 저장소(예: 스키마)
- 열 개수
- 행 개수
- 개인정보
- 민감한 개인 정보

보고서 생성 단계

1. 데이터 조사 페이지에서 다음을 선택하세요. 페이지 오른쪽 상단에 있는 버튼입니다.
2. 보고서 유형을 선택하세요: CSV 또는 JSON.
3. 보고서 이름을 입력하세요.
4. 전체 보고서를 다운로드하려면 시스템을 선택한 다음 해당 드롭다운 메뉴에서 시스템과 볼륨을 선택하세요. 대상 폴더 경로를 제공합니다.

   브라우저에서 보고서를 다운로드하려면 로컬을 선택하세요. 이 옵션은 보고서를 처음 10,000개 행으로 제한하고 **CSV** 형식으로 제한됩니다. 로컬을 선택하면 다른 필드를 작성할 필요가 없습니다.

5. 보고서 다운로드를 선택하세요.



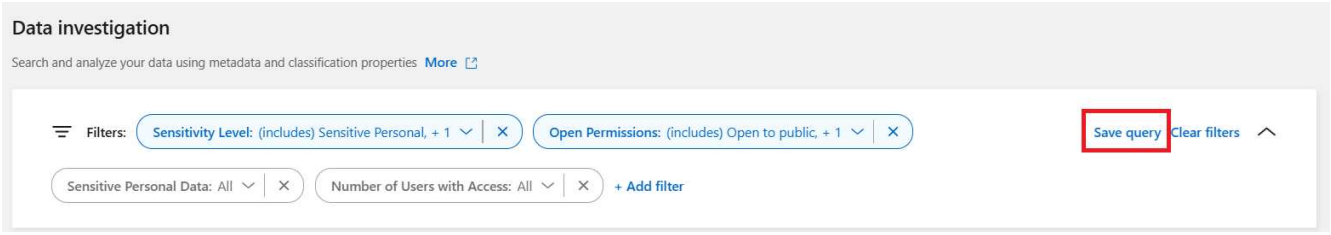
결과

보고서를 다운로드 중이라는 메시지가 대화 상자에 표시됩니다.

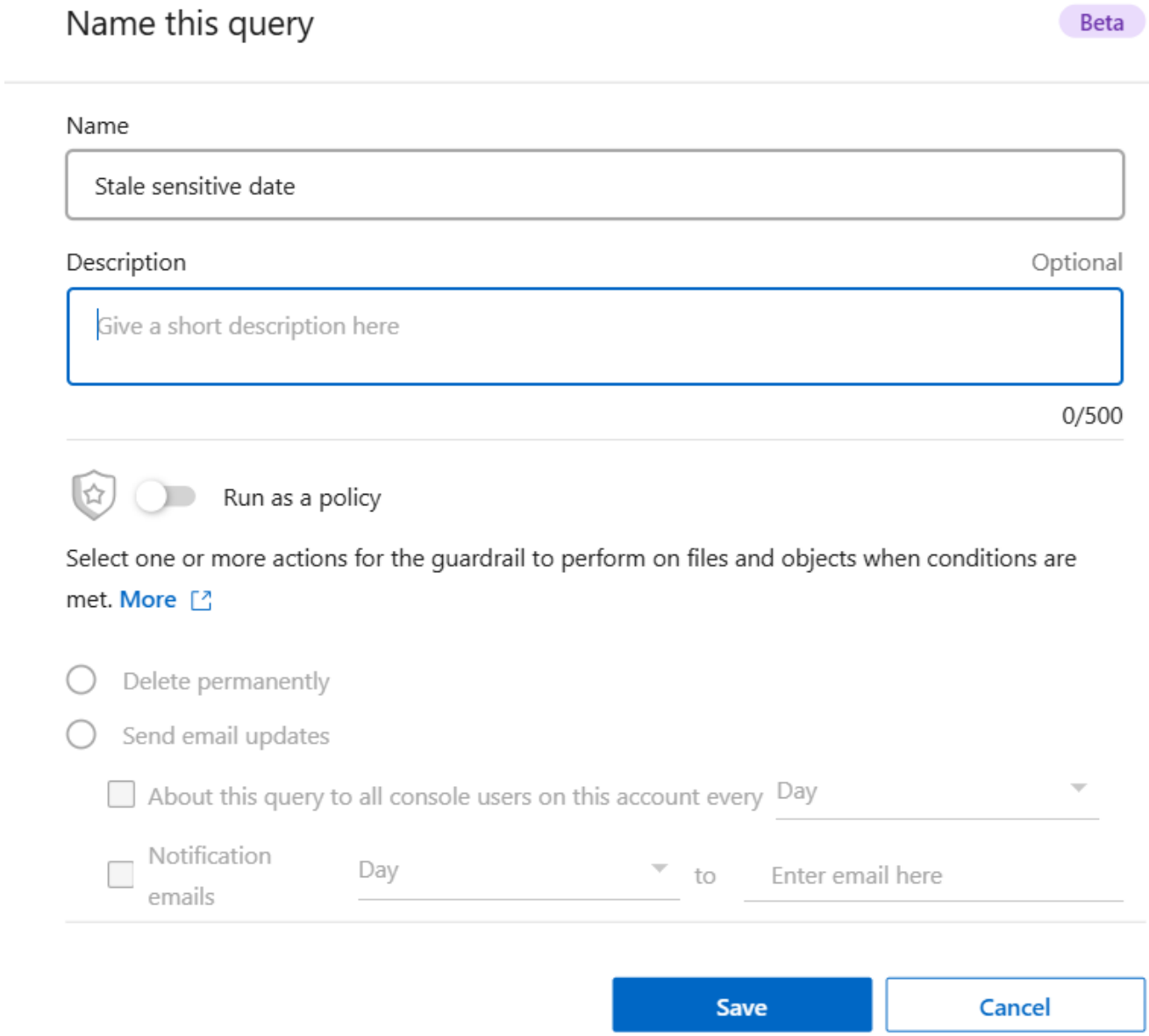
선택한 필터를 기반으로 저장된 쿼리를 만듭니다.

단계

1. 조사 탭에서 사용할 필터를 선택하여 검색을 정의합니다. 보다"조사 페이지에서 데이터 필터링" 자세한 내용은.
2. 모든 필터 특성을 원하는 대로 설정한 후 *쿼리 저장*을 선택하세요.



3. 저장된 쿼리의 이름을 지정하고 설명을 추가합니다. 이름은 고유해야 합니다.
4. 선택적으로 쿼리를 정책으로 저장할 수 있습니다.
   a. 쿼리를 정책으로 저장하려면 정책으로 실행 토글을 전환합니다.
   b. 영구적으로 삭제 또는 *이메일 업데이트 보내기*를 선택하세요. 이메일 업데이트를 선택하면 쿼리 결과를 매일, 매주 또는 매월 모든 콘솔 사용자에게 이메일로 보낼 수 있습니다. 또는 동일한 빈도로 특정 이메일 주소로 알림을 보낼 수도 있습니다.
5. *저장*을 선택하세요.



검색이나 정책을 만든 후에는 저장된 쿼리 탭에서 볼 수 있습니다.

결과가 저장된 쿼리 페이지에 나타나기까지 최대 15분이 걸릴 수 있습니다.

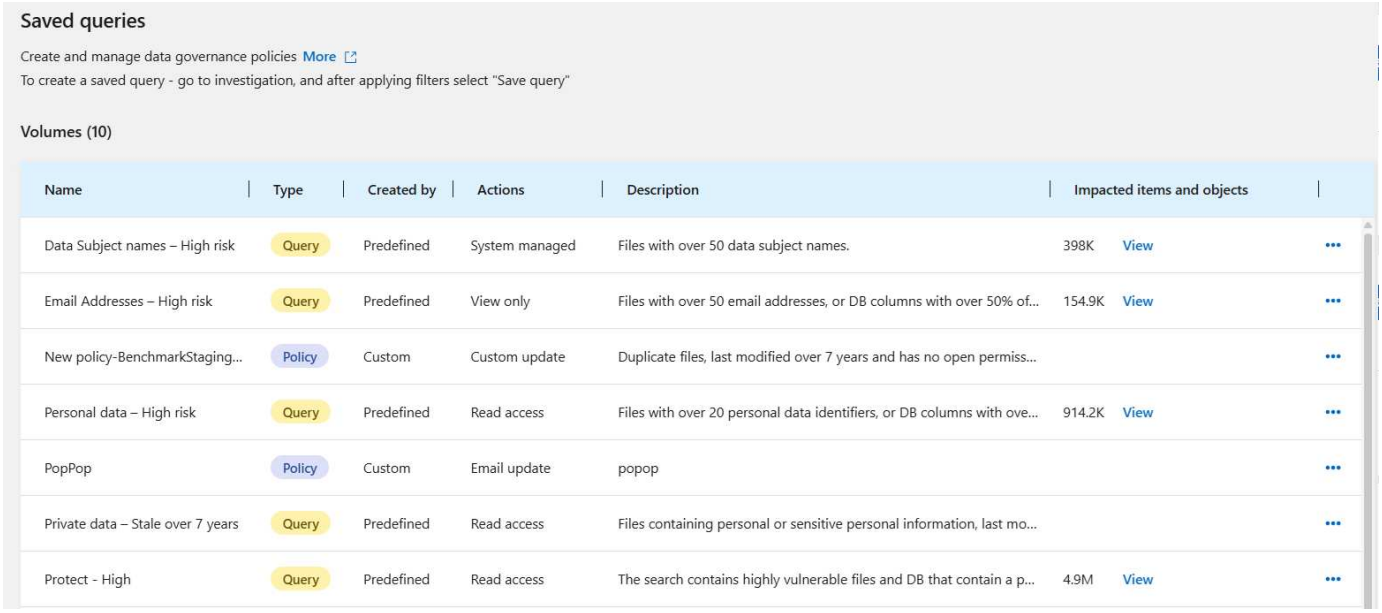
NetApp Data Classification 사용하여 저장된 쿼리 관리

NetaApp 데이터 분류는 검색어 저장을 지원합니다. 저장된 쿼리를 사용하면 사용자 정의 필터를 만들어 데이터 조사 페이지에서 자주 사용되는 쿼리를 정렬할 수 있습니다. 데이터 분류에는 일반적인 요청을 기반으로 한 미리 정의된 저장된 쿼리도 포함됩니다.

규정 준수 대시보드의 저장된 쿼리 탭에는 이 데이터 분류 인스턴스에서 사용할 수 있는 모든 사전 정의 및 사용자 지정 저장된 쿼리가 나열됩니다.

저장된 쿼리는 정책으로도 저장할 수 있습니다. 쿼리가 데이터를 필터링하는 반면, 정책을 사용하면 데이터에 대한 작업을 수행할 수 있습니다. 정책을 사용하면 발견된 데이터를 삭제하거나 발견된 데이터에 대한 이메일 업데이트를 보낼 수 있습니다.

저장된 쿼리는 조사 페이지의 필터 목록에도 표시됩니다.



조사 페이지에서 저장된 쿼리 결과 보기

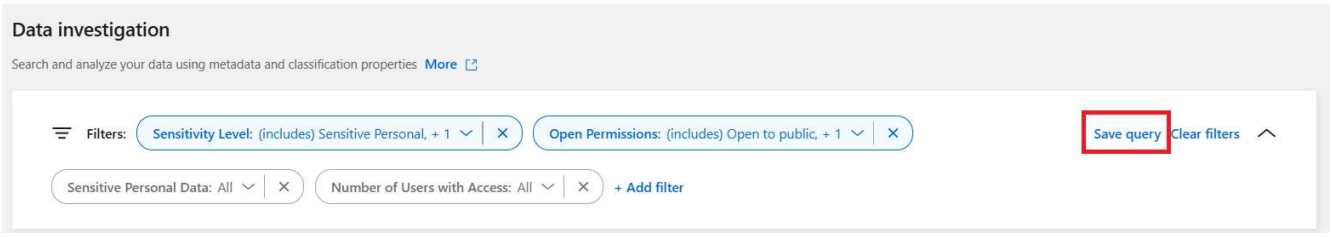
조사 페이지에서 저장된 쿼리에 대한 결과를 표시하려면 다음을 선택하십시오. 특정 검색에 대한 버튼을 클릭한 다음 *결과 조사*를 선택하세요.

저장된 쿼리 및 정책 생성

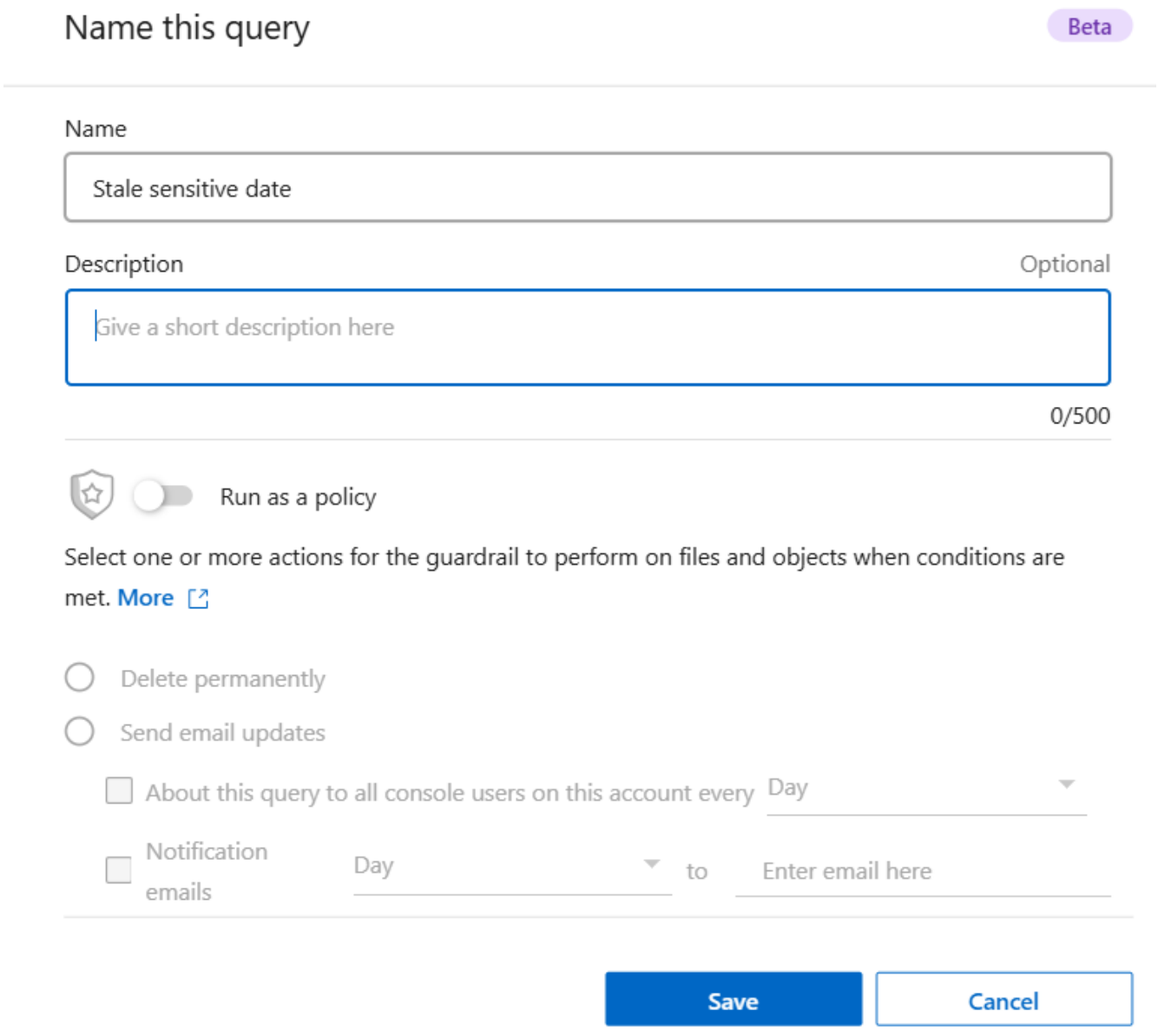
귀하의 조직에 맞는 특정 쿼리에 대한 결과를 제공하는 사용자 정의 저장된 쿼리를 만들 수 있습니다. 검색 기준과 일치하는 모든 파일과 디렉토리(공유 및 폴더)에 대한 결과가 반환됩니다.

단계

1. 조사 탭에서 사용할 필터를 선택하여 검색을 정의합니다. 보다"조사 페이지에서 데이터 필터링" 자세한 내용은.
2. 모든 필터 특성을 원하는 대로 설정한 후 *쿼리 저장*을 선택하세요.



3. 저장된 쿼리의 이름을 지정하고 설명을 추가합니다. 이름은 고유해야 합니다.
4. 선택적으로 쿼리를 정책으로 저장할 수 있습니다.
   a. 쿼리를 정책으로 저장하려면 정책으로 실행 토글을 전환합니다.
   b. 영구적으로 삭제 또는 *이메일 업데이트 보내기*를 선택하세요. 이메일 업데이트를 선택하면 쿼리 결과를 매일, 매주 또는 매월 모든 콘솔 사용자에게 이메일로 보낼 수 있습니다. 또는 동일한 빈도로 특정 이메일 주소로 알림을 보낼 수도 있습니다.
5. *저장*을 선택하세요.



검색이나 정책을 만든 후에는 저장된 쿼리 탭에서 볼 수 있습니다.

저장된 쿼리 또는 정책 편집

저장된 쿼리의 이름과 설명을 수정할 수 있습니다. 쿼리를 정책으로 변환할 수도 있고, 그 반대로도 가능합니다.

기본으로 저장된 쿼리는 수정할 수 없습니다. 저장된 쿼리의 필터는 수정할 수 없습니다. 저장된 쿼리의 조사 결과를 다시 보고, 필터를 변경하거나 수정한 다음 새 쿼리나 정책으로 저장할 수 있습니다.

단계

1. 저장된 쿼리 페이지에서 변경하려는 검색에 대해 *검색 편집*을 선택합니다.

2. 이름과 설명 필드를 변경합니다. 이름과 설명 필드만 변경합니다.

   선택적으로 쿼리를 정책으로 변환하거나 정책을 저장된 쿼리로 변환할 수 있습니다. 필요에 따라 정책으로 실행 토글을 전환합니다. .. 쿼리를 정책으로 변환하는 경우 영구적으로 삭제 또는 *이메일 업데이트 보내기*를 선택하세요. 이메일 업데이트를 선택하면 쿼리 결과를 매일, 매주 또는 매월 모든 콘솔 사용자에게 이메일로 보낼 수 있습니다. 또는 동일한 빈도로 특정 이메일 주소로 알림을 보낼 수도 있습니다.

3. 변경 사항을 완료하려면 *저장*을 선택하세요.

저장된 쿼리 삭제

더 이상 필요하지 않은 사용자 정의 저장된 쿼리나 정책을 삭제할 수 있습니다. 기본적으로 저장된 쿼리는 삭제할 수 없습니다.

저장된 쿼리를 삭제하려면 다음을 선택하세요. 특정 검색에 대한 버튼을 클릭하고 *쿼리 삭제*를 선택한 다음 확인 대화 상자에서 *쿼리 삭제*를 다시 선택하세요.

기본 쿼리

데이터 분류는 다음과 같은 시스템 정의 검색 쿼리를 제공합니다.

- 데이터 주체 이름 **-** 고위험

  50개 이상의 데이터 주체 이름이 있는 파일

- 이메일 주소 **-** 고위험

  이메일 주소가 50개 이상인 파일 또는 행의 50% 이상이 이메일 주소를 포함하는 데이터베이스 열

- 개인 정보 **-** 고위험

  개인 데이터 식별자가 20개 이상인 파일 또는 개인 데이터 식별자가 포함된 행이 50% 이상인 데이터베이스 열

- 개인 데이터 **- 7**년 이상 보관됨

  개인 정보 또는 민감한 개인 정보가 포함된 파일(최종 수정일로부터 7년 이상)

- 보호 - 높음

  비밀번호, 신용 카드 정보, IBAN 번호 또는 사회 보장 번호가 포함된 파일 또는 데이터베이스 열

- 보호 - 낮음

  3년 이상 접근되지 않은 파일

- 보호 - 중간

  신분증 번호, 세금 식별 번호, 운전면허증 번호, 의료 ID 또는 여권 번호를 포함한 개인 데이터 식별자가 포함된 파일 또는 데이터베이스 열이 포함된 파일

- 민감한 개인 정보 - 고위험

  민감한 개인 데이터 식별자가 20개 이상인 파일 또는 민감한 개인 데이터가 포함된 행이 50% 이상인 데이터베이스 열

저장소에 대한 NetApp Data Classification 검사 설정 변경

각 시스템과 데이터 소스에서 데이터가 스캔되는 방식을 관리할 수 있습니다. "저장소" 기준으로 변경할 수 있습니다. 즉, 스캔하는 데이터 소스의 유형에 따라 각 볼륨, 스키마, 사용자 등에 대해 변경할 수 있습니다.

변경할 수 있는 사항 중 일부는 저장소를 스캔할지 여부와 NetApp Data Classification 수행되는지 여부입니다."매핑 스캔 또는 매핑 및 분류 스캔" . 예를 들어, 일정 시간 동안 볼륨 스캔을 중지해야 하는 경우 스캔을 일시 중지하고 다시 시작할 수도 있습니다.

저장소의 스캔 상태 보기

NetApp Data Classification 각 시스템과 데이터 소스에 대해 스캔하는 개별 저장소(볼륨, 버킷 등)를 볼 수 있습니다. 또한 "매핑"된 항목 수와 "분류"된 항목 수를 확인할 수 있습니다. 전체 AI 식별이 모든 데이터에 대해 수행되므로 분류에 더 오랜 시간이 걸립니다.

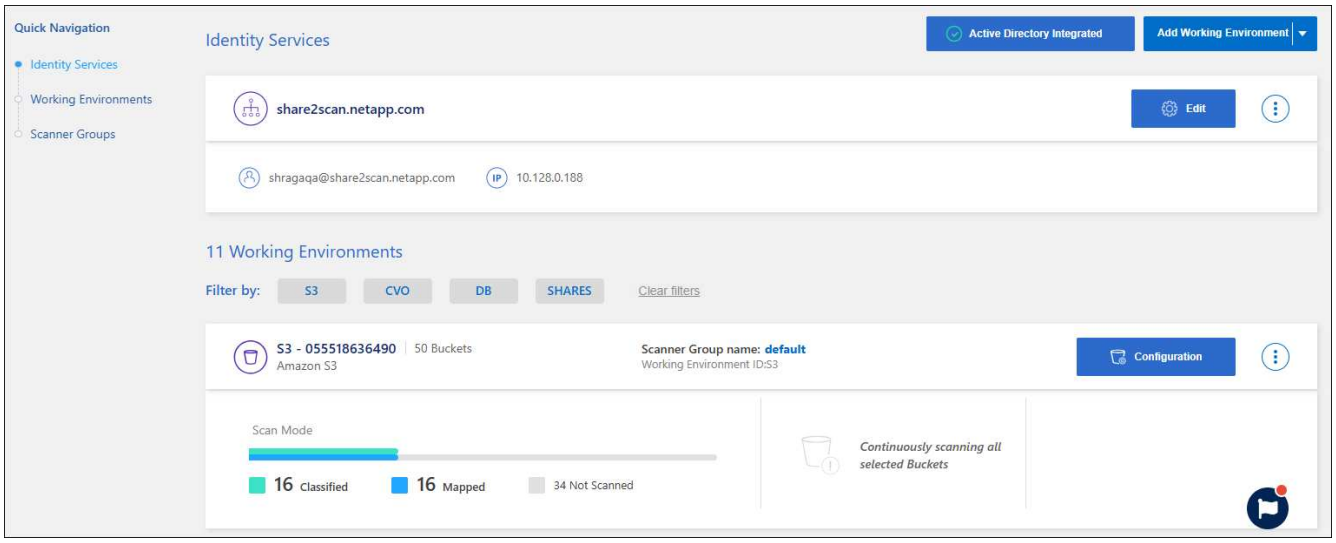
각 작업 환경의 스캐닝 상태는 구성 페이지에서 볼 수 있습니다.

- 초기화 (밝은 파란색 점): 지도 또는 분류 구성이 활성화되었습니다. 이는 "대기 대기열" 상태로 전환되기 직전에 나타납니다.
- 보류 대기열 (주황색 점): 스캔 작업이 스캔 대기열에 나열되기를 기다리고 있습니다.
- 대기 중 (주황색 점): 작업이 스캐닝 대기열에 성공적으로 추가되었습니다. 시스템은 대기 순서가 되면 볼륨을 매핑하거나 분류하기 시작합니다.
- 실행 중 (녹색 점): 대기 중이던 스캔 작업이 선택한 저장소에서 활발하게 진행 중입니다.
- 완료 (녹색 점): 저장소 스캔이 완료되었습니다.
- 일시 중지 (회색 점): 스캐닝을 일시 중지했습니다. 볼륨의 변화는 시스템에 표시되지 않지만, 스캔된 통찰력은 계속 사용할 수 있습니다.
- 오류 (빨간색 점): 문제가 발생하여 검사를 완료할 수 없습니다. 작업을 완료해야 하는 경우, "필수 작업" 열 아래의 도구 설명에 오류가 표시됩니다. 그렇지 않으면 시스템은 "오류" 상태를 표시하고 복구를 시도합니다. 완료되면 상태가 변경됩니다.

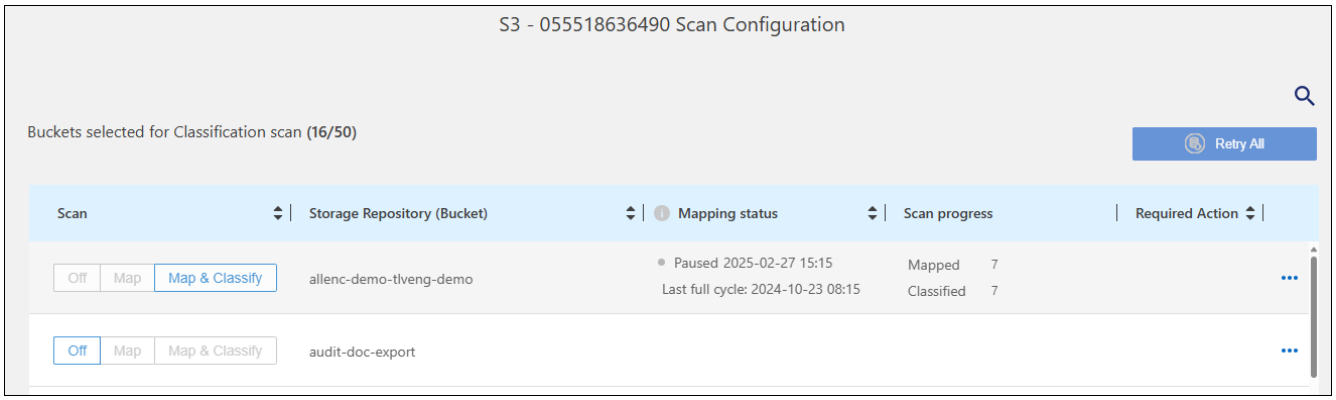
- 스캔 안 함: 볼륨 구성이 "끄기"로 선택되어 시스템이 볼륨을 스캔하지 않습니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.



2. 구성 탭에서 시스템의 구성 버튼을 선택합니다.
3. 스캔 구성 페이지에서 모든 저장소의 스캔 설정을 확인합니다.



4. 검사하는 동안 매핑 상태 열의 진행률 표시줄 위에 커서를 올려 놓으면 해당 저장소에 대해 매핑되거나 분류될 대기열의 파일 수를 볼 수 있습니다.

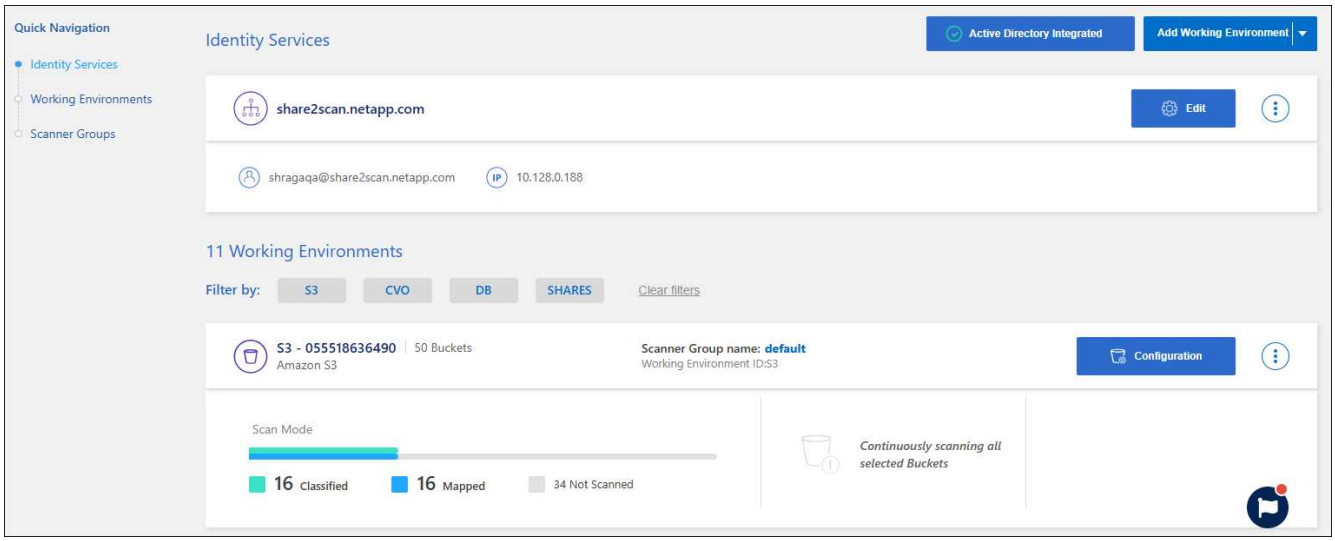
저장소 스캐닝 유형 변경

구성 페이지에서 언제든지 시스템의 매핑 전용 스캔이나 매핑 및 분류 스캔을 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 변경할 수도 있고, 그 반대로도 가능합니다.

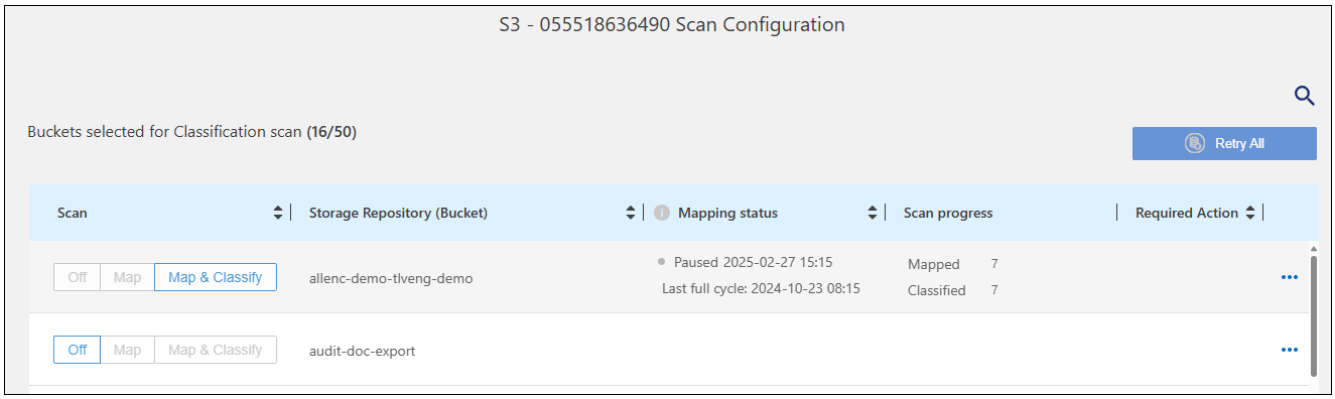
데이터베이스는 매핑 전용 스캔으로 설정할 수 없습니다. 데이터베이스 스캐닝은 켜거나 끌 수 있습니다. 켜짐은 맵 및 분류와 동일합니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 탭에서 시스템의 구성 버튼을 선택합니다.

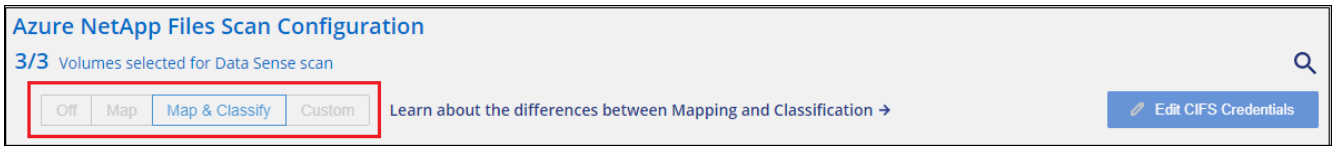


3. 스캔 구성 페이지에서 저장소(이 예에서는 버킷)를 변경하여 매핑 또는 매핑 및 분류 스캔을 수행합니다.



특정 유형의 시스템에서는 페이지 상단의 버튼 막대를 사용하여 모든 저장소에 대한 스캐닝 유형을 전역적으로 변경할 수 있습니다. 이는 Cloud Volumes ONTAP, 온프레미스 ONTAP, Azure NetApp Files 및 Amazon FSx for ONTAP 시스템에 유효합니다.

아래 예에서는 Azure NetApp Files 시스템의 버튼 모음을 보여줍니다.



스캔 우선 순위 지정

가장 중요한 매핑 전용 스캔을 우선 순위로 지정하거나 스캔을 매핑 및 분류하여 우선 순위가 높은 스캔이 먼저 완료되도록 할 수 있습니다.

기본적으로 스캔은 시작된 순서에 따라 대기열에 추가됩니다. 검사의 우선순위를 지정하는 기능을 사용하면 검사를 대기열의 앞으로 옮길 수 있습니다. 여러 스캔에 우선순위를 지정할 수 있습니다. 우선순위는 선입선출 순서로 지정됩니다. 즉, 우선순위를 지정한 첫 번째 스캔이 대기열의 앞으로 이동하고, 두 번째로 우선순위를 지정한 스캔이 대기열의 두 번째가 되는 식입니다.

우선권은 한 번만 부여됩니다. 매핑 데이터의 자동 재스캔은 기본 순서대로 수행됩니다.

단계

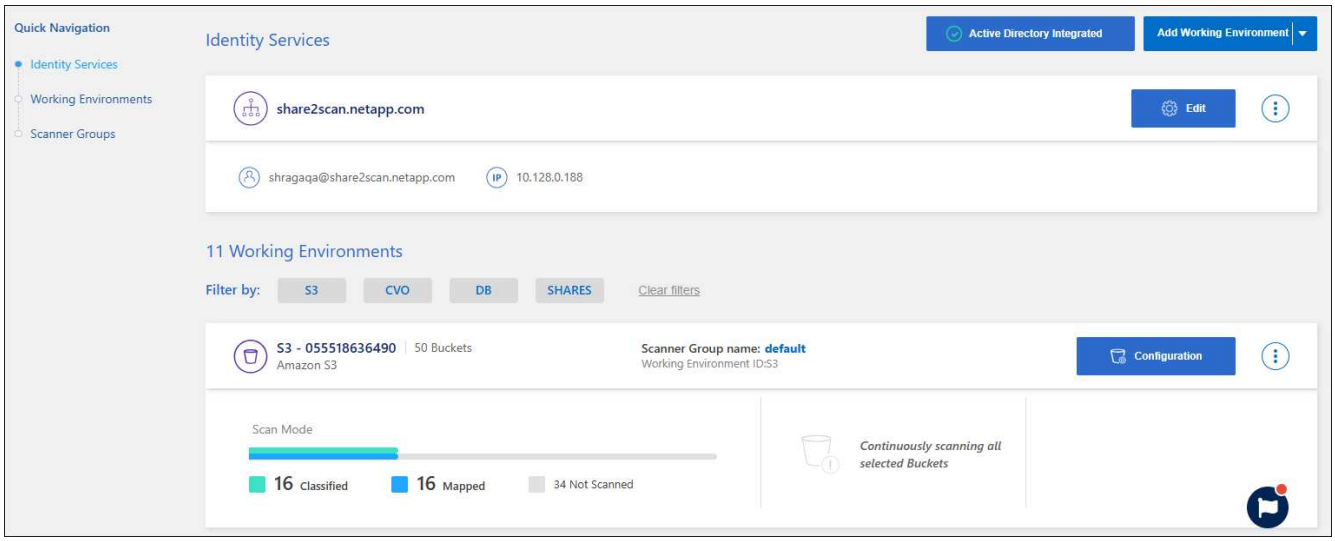
1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 우선순위를 지정할 리소스를 선택하세요.
3. 행동으로부터 ... 옵션에서 *스캔 우선 순위*를 선택하세요.

저장소 스캔 중지

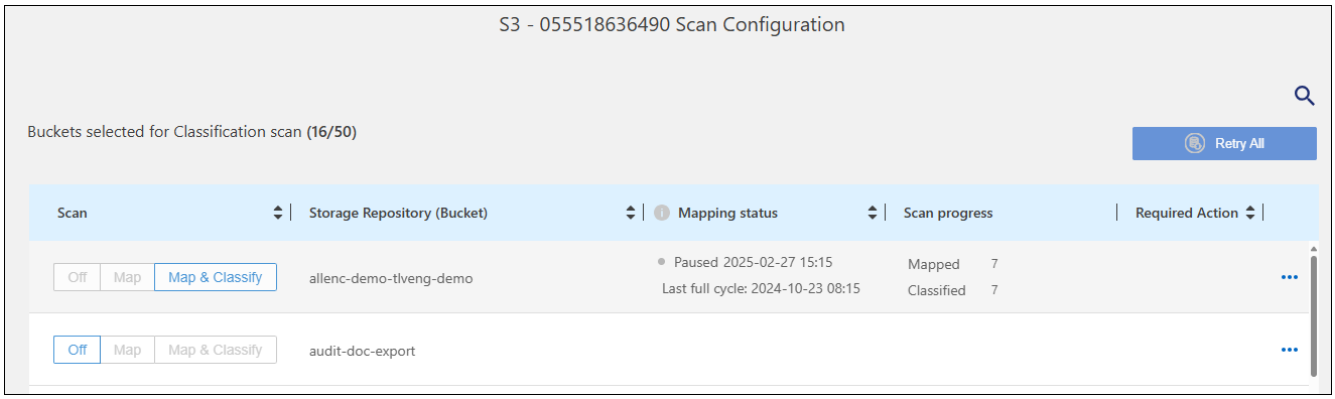
더 이상 규정 준수 여부를 모니터링할 필요가 없으면 저장소(예: 볼륨) 스캔을 중지할 수 있습니다. 스캐닝을 "끄면" 됩니다. 스캐닝을 끄면 해당 볼륨에 대한 모든 인덱싱 및 정보가 시스템에서 제거되고, 데이터 스캐닝에 대한 요금 청구도 중단됩니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 탭에서 시스템의 구성 버튼을 선택합니다.



3. 스캔 구성 페이지에서 *끄기*를 선택하여 특정 버킷에 대한 스캔을 중지합니다.



저장소 스캐닝 일시 중지 및 재개

특정 콘텐츠 스캔을 일시적으로 중지하려면 저장소에서 스캔을 "일시 중지"할 수 있습니다. 스캐닝을 일시 중지하면 데이터 분류가 향후 저장소의 변경 사항이나 추가 사항에 대한 스캐닝을 수행하지 않습니다. 모든 현재 스캔 결과는

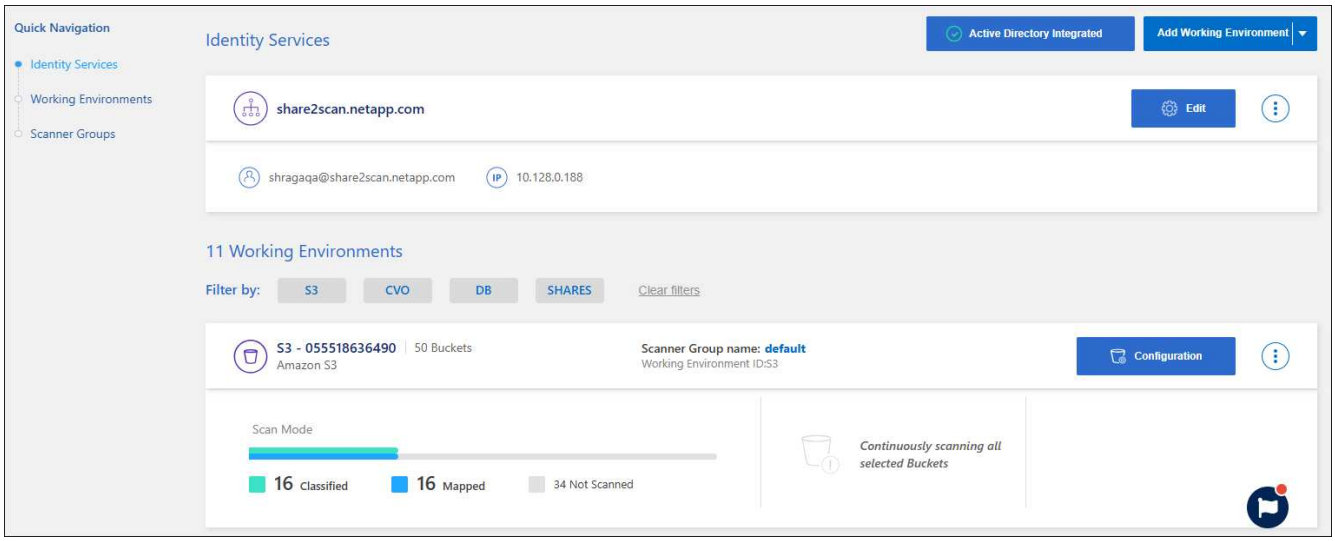
데이터 분류에서 계속 접근할 수 있습니다.

스캔을 일시 중지하더라도 데이터가 시스템에 계속 남아 있기 때문에 요금이 청구되지 않습니다.

언제든지 스캐닝을 다시 시작할 수 있습니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 탭에서 시스템의 구성 버튼을 선택합니다.



3. 스캔 구성 페이지에서 작업을 선택하세요. ••• 상.
4. 볼륨에 대한 스캐닝을 일시 중지하려면 *일시 중지*를 선택하고, 이전에 일시 중지했던 볼륨에 대한 스캐닝을 재개하려면 *다시 시작*을 선택합니다.

NetApp Data Classification 준수 보고서 보기

NetApp Data Classification 조직의 데이터 개인정보 보호 프로그램 상태를 더 잘 이해하는 데 사용할 수 있는 보고서를 제공합니다.

기본적으로 데이터 분류 대시보드에는 모든 시스템, 데이터베이스 및 데이터 소스에 대한 규정 준수 및 거버넌스 데이터가 표시됩니다. 일부 시스템에 대한 데이터만 포함된 보고서를 보려면 필터링을 통해 해당 시스템만 볼 수 있습니다.

- 규정 준수 보고서는 데이터 소스에 대한 전체 분류 스캔을 수행하는 경우에만 사용할 수 있습니다. 매핑 전용 스캔을 거친 데이터 소스는 데이터 매핑 보고서만 생성할 수 있습니다.
- NetApp 데이터 분류를 통해 식별된 개인 데이터 및 민감한 개인 데이터의 정확성을 100% 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 검증해야 합니다.

데이터 분류에 사용할 수 있는 보고서는 다음과 같습니다.

- 데이터 발견 평가 보고서: 스캔된 환경에 대한 높은 수준의 분석을 제공하여 시스템 결과를 강조하고 우려되는 영역과 잠재적인 수정 단계를 보여줍니다. 이 보고서는 거버넌스 대시보드에서 사용할 수 있습니다.

- 전체 데이터 매핑 개요 보고서: 시스템에 있는 파일의 크기와 개수에 대한 정보를 제공합니다. 여기에는 사용 용량, 데이터 기간, 데이터 크기, 파일 유형이 포함됩니다. 이 보고서는 거버넌스 대시보드에서 사용할 수 있습니다.
- 데이터 주체 접근 요청 보고서: 데이터 주체의 구체적인 이름이나 개인 식별자에 대한 정보가 포함된 모든 파일에 대한 보고서를 추출할 수 있습니다. 이 보고서는 규정 준수 대시보드에서 사용할 수 있습니다.
- **HIPAA** 보고서: 파일 전체에서 건강 정보의 분포를 파악하는 데 도움이 됩니다. 이 보고서는 규정 준수 대시보드에서 사용할 수 있습니다.
- **PCI DSS** 보고서: 파일 전체에서 신용카드 정보의 분포를 파악하는 데 도움이 됩니다. 이 보고서는 규정 준수 대시보드에서 사용할 수 있습니다.
- 개인정보 위험 평가 보고서: 귀하의 데이터로부터 개인정보 보호에 대한 통찰력과 개인정보 보호 위험 점수를 제공합니다. 이 보고서는 규정 준수 대시보드에서 사용할 수 있습니다.
- 특정 정보 유형에 대한 보고서: 개인 데이터와 민감한 개인 데이터가 포함된 식별된 파일에 대한 세부 정보가 포함된 보고서를 이용할 수 있습니다. 또한 파일을 범주 및 파일 유형별로 분류하여 볼 수도 있습니다.

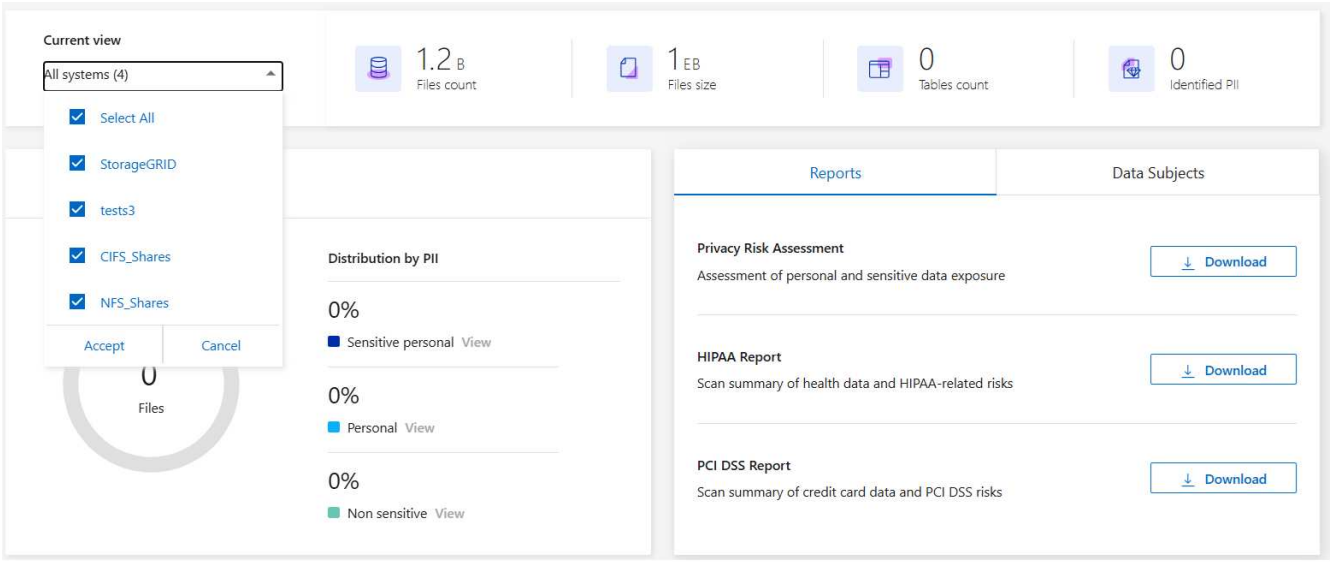
보고서를 위한 시스템을 선택하세요

데이터 분류 규정 준수 대시보드의 내용을 필터링하여 모든 시스템과 데이터베이스에 대한 규정 준수 데이터를 보거나 특정 시스템에 대한 규정 준수 데이터만 볼 수 있습니다.

대시보드를 필터링하면 데이터 분류가 규정 준수 데이터의 범위를 지정하고 선택한 시스템에만 보고합니다.

단계

1. 데이터 분류 메뉴에서 *규정 준수*를 선택합니다.
2. 시스템 필터 드롭다운을 선택한 다음 시스템을 선택하세요.
3. 동의를 선택하여 선택 사항을 확인하세요.



데이터 주체 접근 요청 보고서

유럽 GDPR과 같은 개인정보 보호 규정은 데이터 주체(고객이나 직원 등)에게 개인 데이터에 접근할 권리를 부여합니다. 데이터 주체가 이러한 정보를 요청하는 경우, 이를 DSAR(데이터 주체 접근 요청)이라고 합니다. 각 기관은 이러한 요청에 "불필요한 지연 없이", 늦어도 접수 후 한 달 이내에 응답해야 합니다.

DSAR에 응답하려면 주체의 전체 이름이나 알려진 식별자(예: 이메일 주소)를 검색한 다음 보고서를 다운로드할 수 있습니다. 이 보고서는 귀하의 조직이 GDPR 또는 유사한 데이터 개인정보 보호법을 준수하는 데 도움이 되도록 설계되었습니다.

데이터 분류는 **DSAR**에 대응하는 데 어떻게 도움이 될 수 있나요**?**

데이터 주체 검색을 수행하면 데이터 분류는 해당 개인의 이름이나 식별자가 포함된 모든 파일을 찾습니다. 데이터 분류는 이름이나 식별자에 대해 최신 사전 색인화된 데이터를 확인합니다. 새로운 스캔이 시작되지 않습니다.

검색이 완료되면 데이터 주체 접근 요청 보고서에 대한 파일 목록을 다운로드할 수 있습니다. 보고서는 데이터에서 얻은 통찰력을 모아 법적 용어로 표현하여 해당 개인에게 다시 보낼 수 있습니다.

현재 데이터베이스에서는 데이터 주체 검색이 지원되지 않습니다.

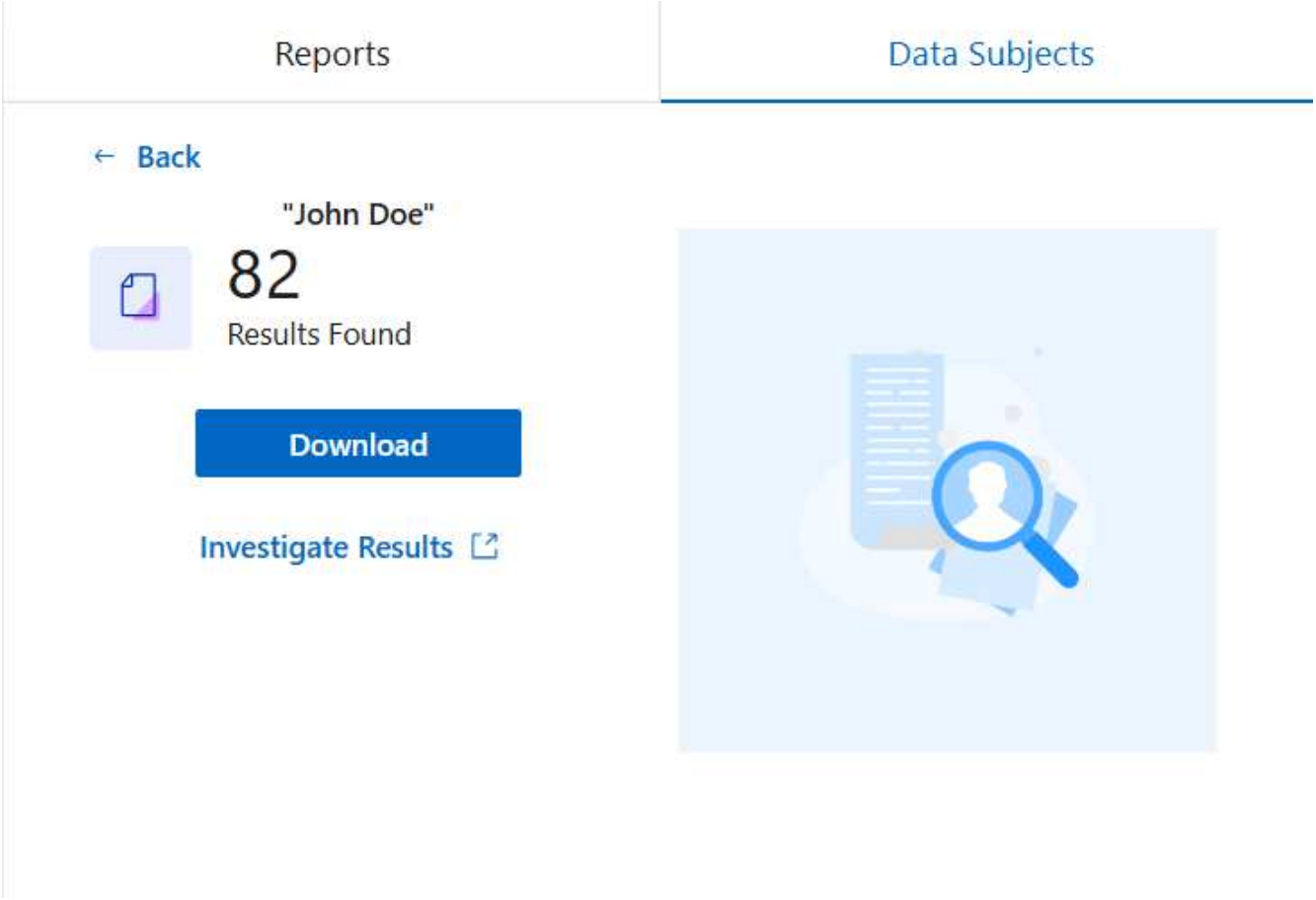
데이터 주체 검색 및 보고서 다운로드

데이터 주체의 성명 또는 알려진 식별자를 검색한 다음 파일 목록 보고서 또는 DSAR 보고서를 다운로드합니다. 검색은 다음과 같이 가능합니다."모든 개인 정보 유형" .

데이터 주체의 이름을 검색할 때 영어, 독일어, 일본어, 스페인어가 지원됩니다. 나중에 더 많은 언어에 대한 지원이 추가될 예정입니다.

단계

1. 데이터 분류 메뉴에서 *규정 준수*를 선택합니다.
2. 규정 준수 페이지에서 데이터 주체 탭을 찾으세요.
3. 데이터 주체 섹션에서 이름이나 알려진 식별자를 입력한 다음 검색을 선택합니다.
4. 검색이 완료되면 다운로드를 선택하여 데이터 주체 액세스 요청 응답에 액세스하세요. 결과 조사를 선택하면 데이터 조사 페이지에서 자세한 정보를 볼 수 있습니다
   .



5. 데이터 분류에서 결과를 검토하거나 다운로드 아이콘을 선택하여 보고서로 다운로드하세요.

   a. 다운로드 아이콘을 선택하면 다운로드 설정을 구성합니다.

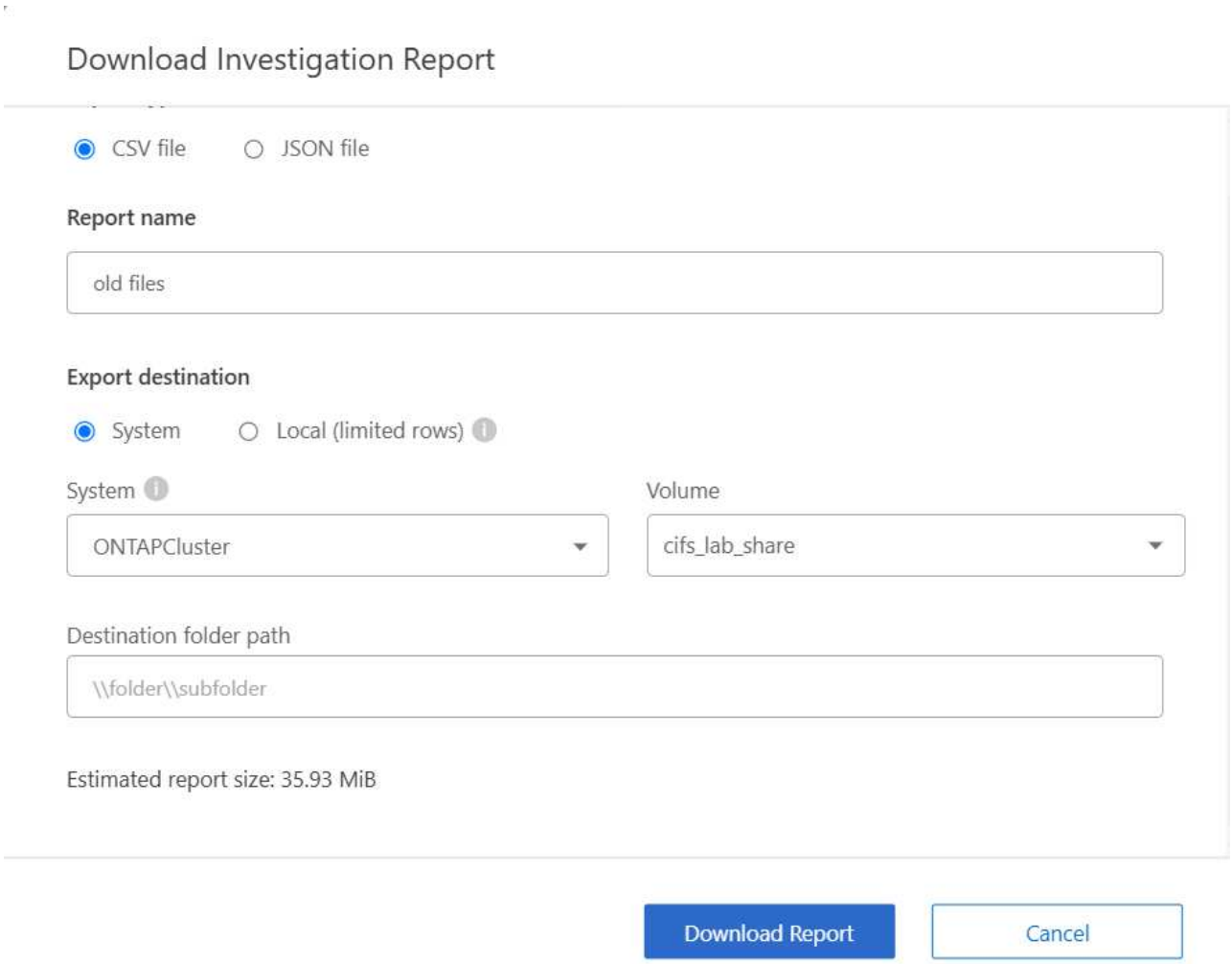
      - 영화 형식을 선택하세요: CSV 또는 JSON
      - *보고서 이름*을 입력하세요
      - 내보내기 대상을 선택하세요: 시스템 또는 로컬 컴퓨터.

        시스템을 선택하면 모든 데이터가 다운로드됩니다. 또한 시스템, 볼륨, *대상 폴더 경로*도 선택해야 합니다.

*로컬*을 선택하면 보고서가 구조화되지 않은 데이터의 처음 10,000행, 구조화되지 않은 데이터의 5,000행, 구조화된 데이터의 1,000행으로 제한됩니다.

   a. 보고서 다운로드를 선택하여 다운로드를 시작하세요

      .



건강보험 이동성 및 책임법(HIPAA) 보고서

건강보험 양도성 및 책임법(HIPAA) 보고서는 건강 정보가 포함된 파일을 식별하는 데 도움이 될 수 있습니다. 이는 귀하의 조직이 HIPAA 데이터 개인정보 보호법을 준수하도록 돕기 위해 고안되었습니다. 데이터 분류에서 찾는 정보는 다음과 같습니다.

- 건강 참조 패턴
- ICD-10-CM 의료 코드
- ICD-9-CM 의료 코드
- HR - 건강 카테고리
- 건강 애플리케이션 데이터 범주

보고서에는 다음과 같은 정보가 포함되어 있습니다.

- 개요: 건강 정보가 포함된 파일의 수와 해당 시스템.
- 암호화: 암호화되었거나 암호화되지 않은 시스템에 있는 건강 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP 에만 해당됩니다.
- 랜섬웨어 보호: 랜섬웨어 보호가 활성화되어 있거나 활성화되어 있지 않은 시스템에 있는 상태 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP 에만 해당됩니다.

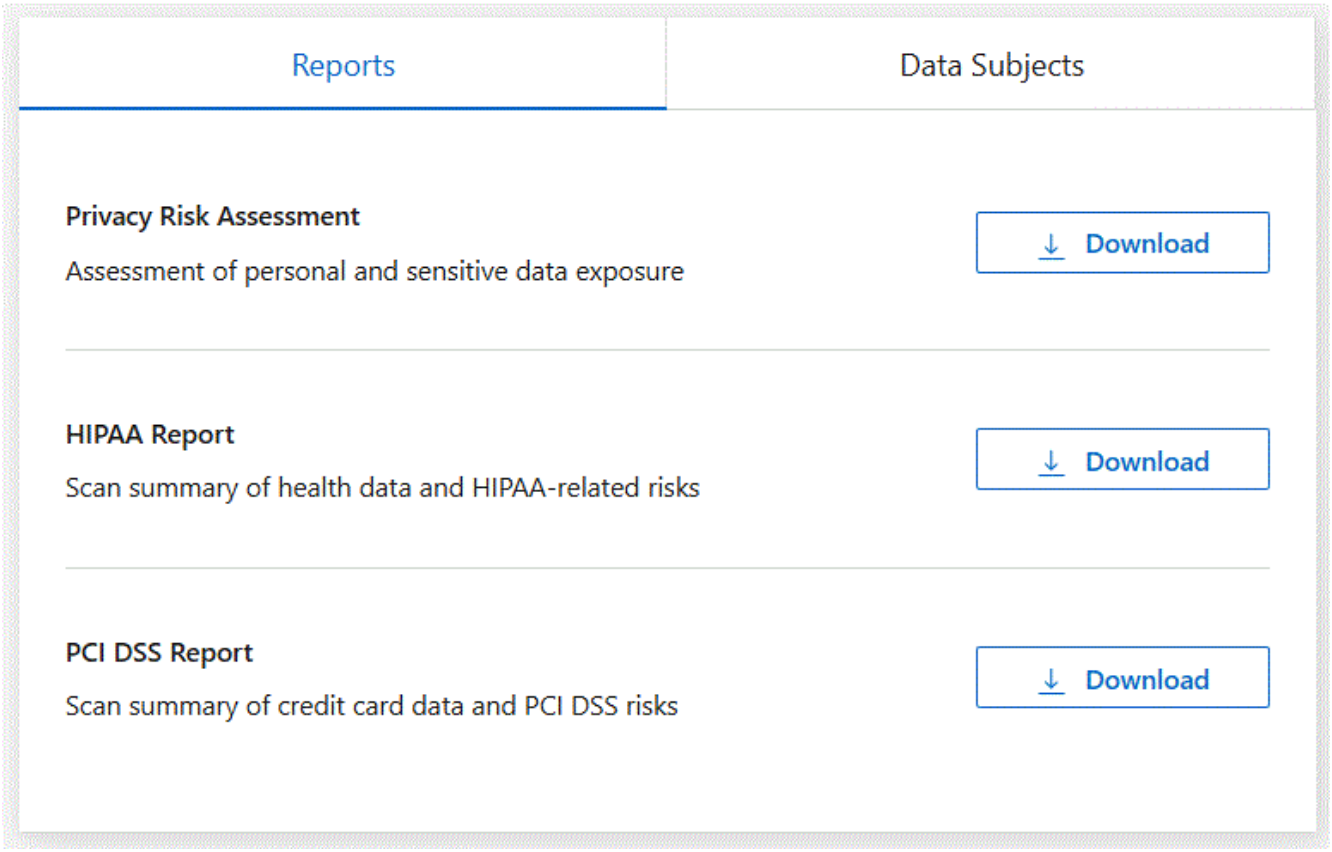
- 보존 기간: 파일이 마지막으로 수정된 기간입니다. 이는 건강 정보를 처리하는 데 필요한 기간 이상으로 보관하면 안 되기 때문에 유용합니다.
- 건강 정보 배포: 건강 정보가 발견된 시스템과 암호화 및 랜섬웨어 보호가 활성화되어 있는지 여부.

HIPAA 보고서 생성

보고서를 생성하려면 규정 준수 탭으로 이동하세요.

단계

1. 데이터 분류 메뉴에서 *규정 준수*를 선택합니다.
2. 보고서 창을 찾으세요. **HIPAA** 보고서 옆에 있는 다운로드 아이콘을 선택하세요.



결과

데이터 분류는 PDF 보고서를 생성합니다.

결제 카드 산업 데이터 보안 표준(PCI DSS) 보고서

결제 카드 업계 데이터 보안 표준(PCI DSS) 보고서는 파일 전체에서 신용카드 정보의 분포를 파악하는 데 도움이 될 수 있습니다.

보고서에는 다음과 같은 정보가 포함되어 있습니다.

- 개요: 신용카드 정보가 들어 있는 파일의 개수와 해당 시스템은 무엇인가?
- 암호화: 암호화되었거나 암호화되지 않은 시스템에 있는 신용카드 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP 에만 해당됩니다.

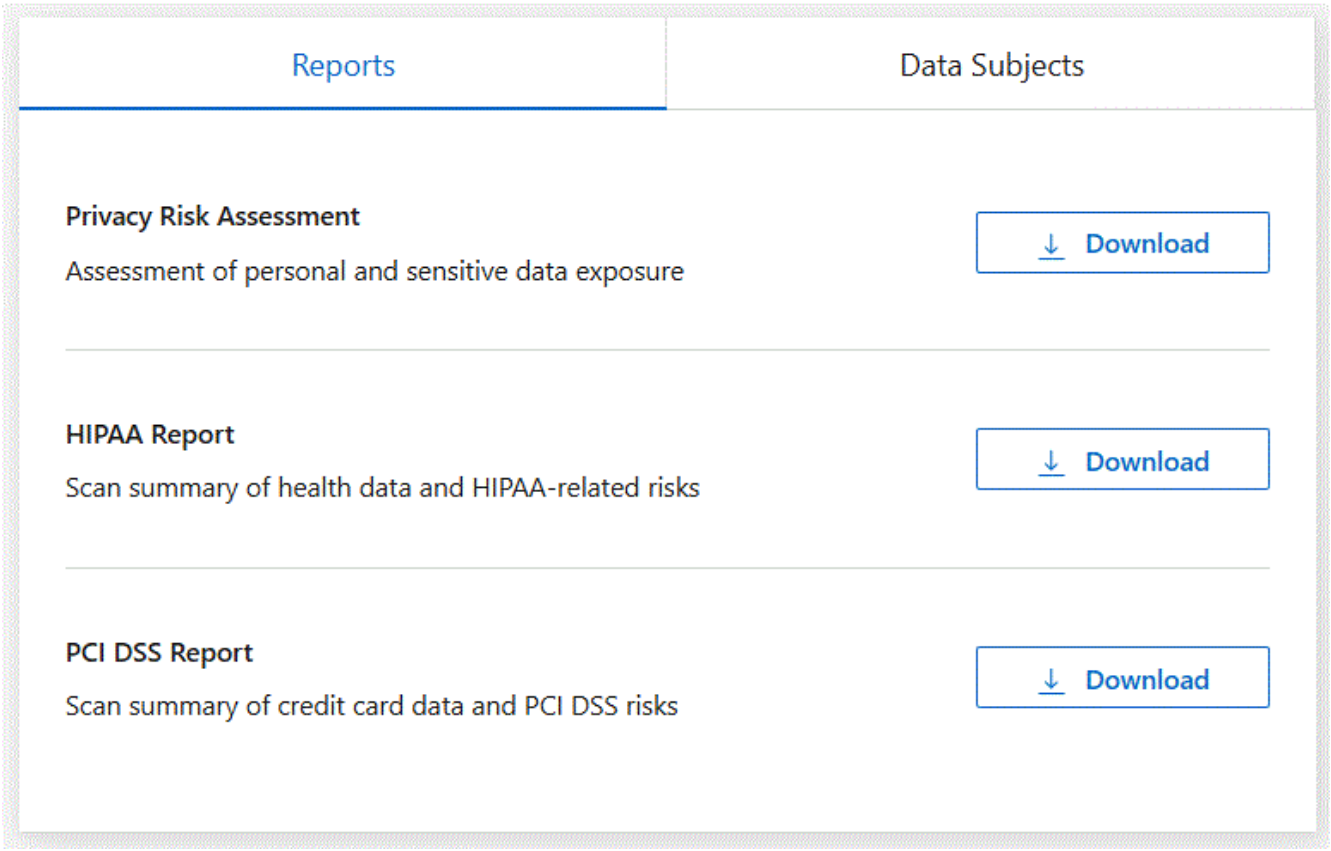
- 랜섬웨어 보호: 랜섬웨어 보호가 활성화되어 있거나 활성화되어 있지 않은 시스템에 있는 신용카드 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP 에만 해당됩니다.
- 보존 기간: 파일이 마지막으로 수정된 기간입니다. 이는 신용카드 정보를 처리하는 데 필요한 기간 이상으로 보관하면 안 되기 때문에 유용합니다.
- 신용카드 정보 배포: 신용카드 정보가 발견된 시스템과 암호화 및 랜섬웨어 보호가 활성화되어 있는지 여부.

PCI DSS 보고서 생성

보고서를 생성하려면 규정 준수 탭으로 이동하세요.

단계

1. 데이터 분류 메뉴에서 *규정 준수*를 선택합니다.
2. 보고서 창을 찾으세요. **PCI DSS** 보고서 옆에 있는 다운로드 아이콘을 선택하세요.



결과

데이터 분류는 필요에 따라 검토하고 다른 그룹으로 보낼 수 있는 PDF 보고서를 생성합니다.

개인정보 위험 평가 보고서

개인정보 위험 평가 보고서는 GDPR 및 CCPA와 같은 개인정보 보호 규정에서 요구하는 대로 조직의 개인정보 위험 상태에 대한 개요를 제공합니다.

보고서에는 다음과 같은 정보가 포함되어 있습니다.

- 준수 상태: 심각도 점수와 데이터의 분포(민감하지 않은 정보, 개인 정보 또는 민감한 개인 정보)

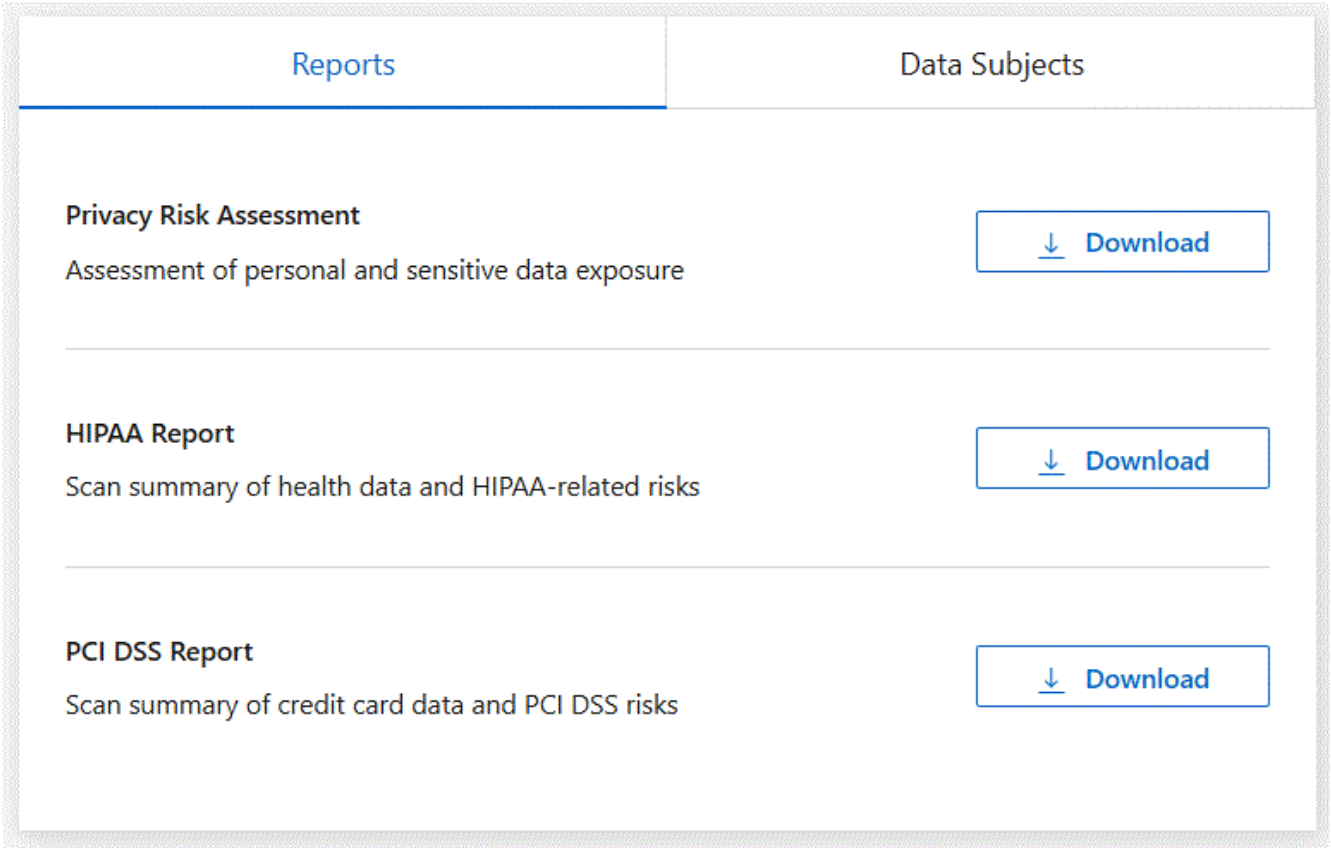
- 평가 개요: 발견된 개인 데이터 유형과 데이터 범주에 대한 분석입니다.
- 이 평가에서 데이터 주체는 다음과 같습니다. 국가 식별자가 발견된 위치별 사람의 수입니다.

개인정보 위험 평가 보고서 생성

보고서를 생성하려면 규정 준수 탭으로 이동하세요.

단계

1. 데이터 분류 메뉴에서 *규정 준수*를 선택합니다.
2. 보고서 창을 찾으세요. 개인정보 위험 평가 보고서 옆에 있는 다운로드 아이콘을 선택하세요.



결과

데이터 분류는 필요에 따라 검토하고 다른 그룹으로 보낼 수 있는 PDF 보고서를 생성합니다.

심각도 점수

데이터 분류는 세 가지 변수를 기반으로 개인정보 보호 위험 평가 보고서의 심각도 점수를 계산합니다.

- 모든 데이터 중 개인 데이터가 차지하는 비율.
- 모든 데이터 중 민감한 개인 데이터가 차지하는 비율입니다.
- 국민 ID, 사회 보장 번호, 세금 ID 번호와 같은 국가 식별자를 통해 결정되는 데이터 주체를 포함하는 파일의 비율입니다.

점수를 결정하는 데 사용된 논리는 다음과 같습니다.

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

NetApp Data Classification 상태 모니터링

NetApp Data Classification 상태 모니터 대시보드는 성능에 대한 실시간 모니터링과 통찰력을 제공합니다. Health Monitor는 데이터 분류 인프라, 시스템 상태, 사용 지표 및 활용 데이터에 대한 정보를 수집하여 문제를 식별하고 해결할 수 있도록 지원합니다.

건강 모니터 통찰력

Health Monitor 대시보드는 4가지 범주로 정보를 표시합니다.

- 인프라 상태

  버전 상태, 시스템 안정성, 배포 유형, 머신 규모 등의 정보를 확인하세요.

- 문제가 있는 컨테이너

  자주 중지되거나 다시 시작되는 컨테이너에 대한 통찰력을 얻으려면 문제가 있는 컨테이너 필드를 검토하세요. 이 정보를 사용하여 특정 컨테이너를 조사하세요.

- 시스템 정보

  시스템 정보 패널은 공개 및 비공개 IP 주소, 호스트 이름, 운영 체제, 콘솔 버전, 콘솔 ID와 같은 NetApp Console 및 데이터 분류에 대한 중요한 정보를 캡처합니다.

- 사용 및 활용

  CPU 사용량, 디스크 활용도, 디스크 사용량, 메모리 사용량을 검토합니다. 이러한 값은 저장 단위(GB) 또는 전체 사용량의 백분율로 표시됩니다. 필드에 경고가 표시되면 해당 경고를 선택하여 정보와 수정 권장 사항을 확인하세요.

Health Monitor 대시보드에 액세스하세요

1. 데이터 분류에서 구성을 선택합니다.
2. 구성 제목 아래에서 데이터 분류 상태 모니터를 선택합니다.
3. Health Monitor 대시보드에서는 다음을 수행할 수 있습니다.
   - 사용량과 활용도를 검토하세요. 사용 또는 활용도 측정 항목에 경고가 표시되는 경우, 해당 경고를 선택하여 문제를 해결하기 위한 권장 사항을 확인하세요.
   - 그래프를 전환하여 CPU 사용량, 디스크 활용도, 디스크 사용량, 메모리 사용량을 표시합니다. x축을 변경하여 시간(6, 12 또는 24) 또는 일(2, 7 또는 14)에 따른 콘텐츠를 표시할 수 있습니다.
   - 최신 데이터 지표를 보려면 대시보드를 새로 고칩니다.