NetApp Data Classification 문서

NetApp Data Classification

NetApp
November 03, 2025

목차

NetApp Data Classification 문서

릴리스 노트

NetApp Data Classification 의 새로운 기능

NetApp Data Classification 의 새로운 기능을 알아보세요.

2025년 10월 6일

버전 **1.47**

BlueXP classification 는 이제 **NetApp Data Classification** 입니다**.**

BlueXP classification NetApp Data Classification 로 이름이 바뀌었습니다. 이름 변경 외에도 사용자 인터페이스가 향상되었습니다.

BlueXP 는 이제 **NetApp Console** 입니다**.**

BlueXP 데이터 인프라 관리에서의 역할을 더 잘 반영하도록 이름이 바뀌고 재설계되었습니다.

NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경 전반의 스토리지 및 데이터 서비스를 중앙에서 관리하여 실시간 통찰력, 더 빠른 워크플로, 간소화된 관리를 제공합니다.

변경된 사항에 대한 자세한 내용은 다음을 참조하세요. "NetApp Console 릴리스 노트" .

강화된 조사 경험

새로운 검색 필터, 값별 결과 수, 주요 결과를 요약한 실시간 통찰력, 사용자 정의 열과 슬라이드 아웃 세부 정보 창이 포함된 새로 고침된 결과 표를 통해 데이터를 더 빠르게 찾고 이해하세요.

자세한 내용은 다음을 참조하세요. "데이터 조사" .

새로운 거버넌스 및 규정 준수 대시보드

직관적인 위젯, 더욱 명확한 시각 자료, 향상된 로딩 성능을 통해 중요한 통찰력을 더 빠르게 얻으세요. 자세한 내용은 다음을 참조하세요."귀하의 데이터에 대한 거버넌스 정보를 검토하세요" 그리고"귀하의 데이터에 대한 규정 준수 정보 보기" .

저장된 쿼리에 대한 정책(미리 보기)

이제 데이터 분류를 통해 조건부 작업으로 거버넌스를 자동화할 수 있습니다. 자동 삭제, 주기적 이메일 알림 등을 포함한 보존 규칙을 만들 수 있으며, 이 모든 것은 업데이트된 저장된 쿼리 페이지에서 관리할 수 있습니다.

자세한 내용은 다음을 참조하세요. "정책 생성" .

작업(미리 보기)

조사 페이지에서 직접 제어하세요. 파일을 개별적으로 또는 대량으로 삭제, 이동, 복사하거나 태그를 지정하여 효율적인 데이터 관리 및 수정이 가능합니다.

자세한 내용은 다음을 참조하세요. "데이터 조사" .

Google Cloud NetApp Volumes 지원

데이터 분류는 이제 Google Cloud NetApp Volumes 에서 스캐닝을 지원합니다. NetApp Console 에서 Google Cloud NetApp Volumes 쉽게 추가하여 원활한 데이터 스캔 및 분류를 수행할 수 있습니다. 자세한 내용은 다음을

참조하세요. "Google Cloud NetApp Volumes 스캔".

2025년 8월 11일

버전 1.46

이 데이터 분류 릴리스에는 버그 수정과 다음 업데이트가 포함되어 있습니다.

감사 페이지에서 향상된 스캔 이벤트 통찰력

감사 페이지는 이제 BlueXP classification 위한 스캔 이벤트에 대한 향상된 통찰력을 지원합니다. 이제 감사 페이지에 시스템 검사가 시작되는 시점, 시스템 상태, 문제가 표시됩니다. 공유 및 시스템 상태는 매핑 스캔에만 사용할 수 있습니다.

감사 페이지에 대한 자세한 내용은 다음을 참조하세요."NetApp Console 작업 모니터링" .

RHEL 9.6 지원

이 릴리스에서는 다크 사이트 배포를 포함하여 BlueXP classification 의 수동 온프레미스 설치를 위한 Red Hat Enterprise Linux v9.6에 대한 지원이 추가되었습니다.

다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, BlueXP classification 버전 1.30 이상이 필요합니다: Red Hat Enterprise Linux 버전 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 및 9.5.

2025년 7월 14일

버전 1.45

이 BlueXP classification 릴리스에는 리소스 활용도를 최적화하는 코드 변경 사항이 포함되어 있습니다.

스캔을 위해 파일 공유를 추가하는 향상된 워크플로

파일 공유 그룹에 파일 공유를 추가하는 워크플로가 간소화되었습니다. 이 프로세스에서는 이제 인증 유형(Kerberos 또는 NTLM)에 따라 CIFS 프로토콜 지원을 구분합니다.

자세한 내용은 다음을 참조하세요. "파일 공유 스캔" .

향상된 파일 소유자 정보

이제 조사 탭에서 캡처된 파일의 파일 소유자에 대한 자세한 정보를 볼 수 있습니다. 조사 탭에서 파일의 메타데이터를 볼 때 파일 소유자를 찾은 다음 세부 정보 보기를 선택하여 사용자 이름, 이메일, SAM 계정 이름을 확인하세요. 이 사용자가 소유한 다른 항목도 볼 수 있습니다. 이 기능은 Active Directory가 있는 작업 환경에서만 사용할 수 있습니다.

자세한 내용은 다음을 참조하세요. "귀하의 조직에 저장된 데이터를 조사하세요" .

2025년 6월 10일

버전 1.44

이 BlueXP classification 릴리스에는 다음이 포함됩니다.

거버넌스 대시보드의 업데이트 시간이 개선되었습니다.

거버넌스 대시보드의 개별 구성 요소에 대한 업데이트 시간이 개선되었습니다. 다음 표는 각 구성 요소의 업데이트 빈도를 보여줍니다.

요소	업데이트 시간
데이터의 시대	24시간
카테고리	24시간
데이터 개요	5분
중복 파일	2시간
파일 유형	24시간
비업무용 데이터	2시간
공개 권한	24시간
저장된 검색	2시간
민감한 데이터 및 광범위한 권한	24시간
데이터 크기	24시간
오래된 데이터	2시간
민감도 수준별 상위 데이터 저장소	2시간

마지막 업데이트 시간을 보고 중복 파일, 비업무 데이터, 저장된 검색, 오래된 데이터, 민감도 수준별 상위 데이터 저장소 구성 요소를 수동으로 업데이트할 수 있습니다. 거버넌스 대시보드에 대한 자세한 내용은 다음을 참조하세요."조직에 저장된 데이터에 대한 거버넌스 세부 정보 보기" .

성능 및 보안 개선

BlueXP 분류의 성능, 메모리 소비, 보안을 개선하기 위해 개선 사항이 적용되었습니다.

버그 수정

Redis가 업그레이드되어 BlueXP classification 의 안정성이 향상되었습니다. BlueXP classification 이제 Elasticsearch를 사용하여 스캔 중 파일 수 보고의 정확도를 향상시킵니다.

2025년 5월 12일

버전 **1.43**

이 데이터 분류 릴리스에는 다음이 포함됩니다.

분류 스캔 우선 순위 지정

데이터 분류는 매핑 전용 스캔 외에도 맵 및 분류 스캔의 우선순위를 지정하는 기능을 지원하여 어떤 스캔을 먼저 완료할지 선택할 수 있습니다. Map & Classify 스캔의 우선순위 지정은 스캔이 시작되기 전과 시작 중 지원됩니다. 검사가 진행되는 동안 검사의 우선순위를 지정하는 경우 매핑 검사와 분류 검사가 모두 우선순위가 지정됩니다.

자세한 내용은 다음을 참조하세요. "스캔 우선 순위 지정" .

캐나다 개인 식별 정보**(PII)** 데이터 범주 지원

데이터 분류 스캔은 캐나다 PII 데이터 범주를 식별합니다. 이러한 범주에는 모든 캐나다 주와 지역의 은행 정보, 여권 번호, 사회보장번호, 운전면허증 번호, 건강카드 번호가 포함됩니다.

자세한 내용은 다음을 참조하세요. "개인 데이터 범주" .

사용자 정의 분류(미리 보기)

데이터 분류는 Map & Classify 스캔에 대한 사용자 정의 분류를 지원합니다. 사용자 정의 분류를 사용하면 정규 표현식을 사용하여 조직에 맞는 데이터를 캡처하도록 데이터 분류 검사를 맞춤화할 수 있습니다. 이 기능은 현재 미리보기 단계에 있습니다.

자세한 내용은 다음을 참조하세요. "사용자 정의 분류 추가" .

저장된 검색 탭

정책 탭의 이름이 변경되었습니다."저장된 검색" . 기능은 변경되지 않았습니다.

감사 페이지로 스캔 이벤트 보내기

데이터 분류는 분류 이벤트(스캔이 시작될 때와 종료될 때)를 전송하는 것을 지원합니다."NetApp Consle Audit 페이지" .

보안 업데이트

- Keras 패키지가 업데이트되어 취약점(BDSA-2025-0107 및 BDSA-2025-1984)이 완화되었습니다.
- Docker 컨테이너 구성이 업데이트되었습니다. 컨테이너는 더 이상 원시 네트워크 패킷을 제작하기 위해 호스트의 네트워크 인터페이스에 액세스할 수 없습니다. 불필요한 접근을 줄임으로써 업데이트를 통해 잠재적인 보안 위험이 완화됩니다.

성능 향상

RAM 사용량을 줄이고 데이터 분류의 전반적인 성능을 개선하기 위해 코드 개선이 구현되었습니다.

버그 수정

StorageGRID 검사가 실패하고, 조사 페이지 필터 옵션이 로드되지 않으며, 대용량 평가의 경우 데이터 검색 평가가 다운로드되지 않는 버그가 수정되었습니다.

2025년 4월 14일

버전 1.42

이 BlueXP classification 릴리스에는 다음이 포함됩니다.

작업 환경을 위한 대량 스캐닝

BlueXP classification 작업 환경에서 대량 작업을 지원합니다. 작업 환경의 볼륨 전반에 걸쳐 매핑 스캔을 활성화하거나, 맵 및 분류 스캔을 활성화하거나, 스캔을 비활성화하거나, 사용자 정의 구성을 만들 수 있습니다. 개별 볼륨에 대한 선택을 하면 대량 선택이 무시됩니다. 대량 작업을 수행하려면 구성 페이지로 이동하여 선택하세요.

조사 보고서를 로컬로 다운로드하세요

BlueXP classification 데이터 조사 보고서를 로컬로 다운로드하여 브라우저에서 볼 수 있는 기능을 지원합니다. 로컬 옵션을 선택하는 경우 데이터 조사는 CSV 형식으로만 가능하며, 데이터의 처음 10,000개 행만 표시됩니다.

자세한 내용은 다음을 참조하세요. "BlueXP classification 사용하여 조직에 저장된 데이터를 조사하세요" .

2025년 3월 10일

버전 1.41

이 BlueXP classification 릴리스에는 일반적인 개선 사항과 버그 수정이 포함되어 있습니다. 여기에는 다음이

포함됩니다.

스캔 상태

BlueXP classification 볼륨의 초기 매핑 및 분류 스캔의 실시간 진행 상황을 추적합니다. 별도의 진행 막대는 매핑 및 분류 스캔을 추적하여 스캔된 전체 파일의 백분율을 나타냅니다. 진행률 표시줄 위에 마우스를 올려 놓으면 검사된 파일 수와 전체 파일을 볼 수 있습니다. 검사 상태를 추적하면 검사 진행 상황에 대한 심층적인 통찰력이 제공되어 검사를 보다 효과적으로 계획하고 리소스 할당을 이해하는 데 도움이 됩니다.

스캔 상태를 보려면 BlueXP classification 에서 구성으로 이동한 다음 작업 환경 구성을 선택하세요. 각 권의 진행 상황은 줄에 따라 표시됩니다.

2025년 2월 19일

버전 **1.40**

이 BlueXP classification 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

RHEL 9.5 지원

이 릴리스에서는 이전에 지원되었던 버전 외에도 Red Hat Enterprise Linux v9.5에 대한 지원이 제공됩니다. 이는 다크 사이트 배포를 포함하여 BlueXP classification 의 모든 수동 온프레미스 설치에 적용됩니다.

다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, BlueXP classification 버전 1.30 이상이 필요합니다: Red Hat Enterprise Linux 버전 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4 및 9.5.

매핑 전용 스캔 우선 순위 지정

매핑 전용 스캔을 수행할 때 가장 중요한 스캔의 우선순위를 지정할 수 있습니다. 이 기능은 작업 환경이 여러 개이고 우선 순위가 높은 스캔을 먼저 완료하려는 경우에 유용합니다.

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.

우선순위는 다음으로 제한됩니다."매핑 전용 스캔" ; 지도 및 분류 스캔에는 사용할 수 없습니다.

자세한 내용은 다음을 참조하세요. "스캔 우선 순위 지정" .

모든 스캔을 다시 시도하세요

BlueXP classification 실패한 모든 스캔을 일괄적으로 다시 시도하는 기능을 지원합니다.

모두 다시 시도 기능을 사용하면 일괄 작업으로 스캔을 다시 시도할 수 있습니다. 네트워크 중단과 같은 일시적인 문제로 인해 분류 스캔이 실패하는 경우, 개별적으로 다시 시도하는 대신 하나의 버튼으로 모든 스캔을 동시에 다시 시도할 수 있습니다. 필요한 만큼 스캔을 다시 시도할 수 있습니다.

모든 스캔을 다시 시도하려면:

1. BlueXP classification 메뉴에서 *구성*을 선택합니다.
2. 실패한 모든 검사를 다시 시도하려면 *모든 검사 다시 시도*를 선택하세요.

향상된 분류 모델 정확도

머신 러닝 모델의 정확도"미리 정의된 카테고리" 11% 개선되었습니다.

2025년 1월 22일

버전 **1.39**

이 BlueXP classification 릴리스에서는 데이터 조사 보고서의 내보내기 프로세스가 업데이트되었습니다. 이 내보내기 업데이트는 데이터에 대한 추가 분석을 수행하거나, 데이터에 대한 추가 시각화를 생성하거나, 데이터 조사 결과를 다른 사람들과 공유하는 데 유용합니다.

이전에는 데이터 조사 보고서 내보내기가 10,000개 행으로 제한되었습니다. 이번 릴리스에서는 이러한 제한이 없어져 모든 데이터를 내보낼 수 있게 되었습니다. 이 변경을 통해 데이터 조사 보고서에서 더 많은 데이터를 내보낼 수 있으므로 데이터 분석에 있어 더 많은 유연성이 제공됩니다.

작업 환경, 볼륨, 대상 폴더, JSON 또는 CSV 형식을 선택할 수 있습니다. 내보낸 파일 이름에는 데이터가 언제 내보내졌는지 식별하는 데 도움이 되는 타임스탬프가 포함됩니다.

지원되는 작업 환경은 다음과 같습니다.

- Cloud Volumes ONTAP
- ONTAP 용 FSx
- ONTAP
- 그룹 공유

데이터 조사 보고서에서 데이터를 내보내는 데는 다음과 같은 제한이 있습니다.

- 다운로드 가능한 최대 레코드 수는 유형(파일, 디렉토리, 테이블)당 5억 개입니다.
- 100만 개의 레코드를 내보내는 데는 약 35분이 걸릴 것으로 예상됩니다.

데이터 조사 및 보고서에 대한 자세한 내용은 다음을 참조하세요. "귀하의 조직에 저장된 데이터를 조사하세요" .

2024년 12월 16일

버전 **1.38**

이 BlueXP classification 릴리스에는 일반적인 개선 사항과 버그 수정이 포함되어 있습니다.

2024년 11월 4일

버전 **1.37**

이 BlueXP classification 릴리스에는 다음과 같은 업데이트가 포함되어 있습니다.

RHEL 8.10 지원

이 릴리스에서는 이전에 지원되었던 버전 외에도 Red Hat Enterprise Linux v8.10에 대한 지원이 제공됩니다. 이는 다크 사이트 배포를 포함하여 BlueXP classification 의 모든 수동 온프레미스 설치에 적용됩니다.

다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, BlueXP classification 버전 1.30 이상이 필요합니다:

Red Hat Enterprise Linux 버전 8.8, 8.10, 9.0, 9.1, 9.2, 9.3 및 9.4.

자세히 알아보세요 "BlueXP classification" .

NFS v4.1 지원

이 릴리스에서는 이전에 지원되었던 버전 외에도 NFS v4.1에 대한 지원이 제공됩니다.

자세히 알아보세요 "BlueXP classification" .

2024년 10월 10일

버전 **1.36**

RHEL 9.4 지원

이 릴리스에서는 이전에 지원되었던 버전 외에도 Red Hat Enterprise Linux v9.4에 대한 지원이 제공됩니다. 이는 다크 사이트 배포를 포함하여 BlueXP classification 의 모든 수동 온프레미스 설치에 적용됩니다.

다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, BlueXP classification 버전 1.30 이상이 필요합니다: Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2, 9.3 및 9.4.

자세히 알아보세요 "BlueXP classification 배포 개요" .

향상된 스캔 성능

이 릴리스에서는 향상된 스캔 성능이 제공됩니다.

2024년 9월 2일

버전 **1.35**

StorageGRID 데이터 스캔

BlueXP classification StorageGRID 에서 데이터 스캐닝을 지원합니다.

자세한 내용은 다음을 참조하세요."StorageGRID 데이터 스캔" .

2024년 8월 5일

버전 **1.34**

이 BlueXP classification 릴리스에는 다음 업데이트가 포함되어 있습니다.

CentOS에서 **Ubuntu**로 변경

BlueXP classification Microsoft Azure 및 Google Cloud Platform(GCP)용 Linux 운영 체제를 CentOS 7.9에서 Ubuntu 22.04로 업데이트했습니다.

배포 세부 사항은 다음을 참조하세요. "인터넷 접속이 가능한 Linux 호스트에 설치하고 Linux 호스트 시스템을 준비합니다." .

2024년 7월 1일

버전 1.33

Ubuntu 지원

이 릴리스는 Ubuntu 24.04 Linux 플랫폼을 지원합니다.

매핑 스캔은 메타데이터를 수집합니다.

다음 메타데이터는 매핑 스캔 중에 파일에서 추출되어 거버넌스, 규정 준수 및 조사 대시보드에 표시됩니다.

- 작업 환경
- 작업 환경 유형
- 저장 저장소
- 파일 유형
- 사용된 용량
- 파일 수
- 파일 크기
- 파일 생성
- 파일 마지막 접근
- 파일이 마지막으로 수정되었습니다
- 파일 발견 시간
- 권한 추출

대시보드의 추가 데이터

이 릴리스에서는 매핑 스캔 중에 거버넌스, 규정 준수 및 조사 대시보드에 표시되는 데이터가 업데이트되었습니다.

자세한 내용은 다음을 참조하십시오. "매핑 스캔과 분류 스캔의 차이점은 무엇입니까?" .

2024년 6월 5일

버전 1.32

구성 페이지의 새 매핑 상태 열

이 릴리스에서는 이제 구성 페이지에 새로운 매핑 상태 열이 표시됩니다. 새로운 열은 매핑이 실행 중인지, 대기 중인지, 일시 중지된 상태인지 등을 식별하는 데 도움이 됩니다.

상태에 대한 설명은 다음을 참조하세요. "스캔 설정 변경" .

2024년 5월 15일

버전 1.31

분류는 BlueXP 의 핵심 서비스로 제공됩니다.

BlueXP classification 이제 커넥터당 최대 500TiB의 스캔 데이터에 대해 추가 비용 없이 BlueXP 의 핵심 기능으로

제공됩니다. 분류 라이센스나 유료 구독이 필요하지 않습니다. 이 새로운 버전에서는 BlueXP classification 기능을 NetApp 스토리지 시스템 스캐닝에 집중하므로 일부 기존 기능은 이전에 라이선스 비용을 지불한 고객만 사용할 수 있습니다. 유료 계약이 종료되면 해당 레거시 기능의 사용은 만료됩니다.

데이터 분류는 스캔할 수 있는 데이터 양에 제한을 두지 않습니다. 각 콘솔 에이전트는 500TiB의 데이터를 스캔하고 표시하는 것을 지원합니다. 500TiB 이상의 데이터를 스캔하려면"다른 콘솔 에이전트를 설치하세요" 그 다음에"다른 데이터 분류 인스턴스 배포" . + 콘솔 UI는 단일 커넥터의 데이터를 표시합니다. 여러 콘솔 에이전트의 데이터를 보는 방법에 대한 팁은 다음을 참조하세요."여러 콘솔 에이전트와 함께 작업" .

2024년 4월 1일

버전 1.30

RHEL v8.8 및 **v9.3 BlueXP classification** 에 대한 지원이 추가되었습니다**.**

이 릴리스에서는 Docker 엔진이 아닌 Podman이 필요한 기존 지원 버전 9.x 외에도 Red Hat Enterprise Linux v8.8 및 v9.3에 대한 지원이 제공됩니다. 이는 BlueXP classification 의 모든 수동 온프레미스 설치에 적용됩니다.

다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, BlueXP classification 버전 1.30 이상이 필요합니다: Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3.

자세히 알아보세요 "BlueXP classification 배포 개요" .

온프레미스에 있는 RHEL 8 또는 9 호스트에 커넥터를 설치하는 경우 BlueXP classification 지원됩니다. RHEL 8 또는 9 호스트가 AWS, Azure 또는 Google Cloud에 있는 경우 지원되지 않습니다.

감사 로그 수집 활성화 옵션이 제거되었습니다**.**

감사 로그 수집을 활성화하는 옵션이 비활성화되었습니다.

스캔 속도가 향상되었습니다

보조 스캐너 노드의 스캔 성능이 개선되었습니다. 스캔에 대한 처리 능력이 더 필요하면 스캐너 노드를 추가할 수 있습니다. 자세한 내용은 다음을 참조하세요. "인터넷 접속이 가능한 호스트에 BlueXP classification 설치합니다." .

자동 업그레이드

인터넷 접속이 가능한 시스템에 BlueXP classification 배포한 경우 시스템이 자동으로 업그레이드됩니다. 이전에는 마지막 사용자 활동 이후 특정 시간이 경과한 후에 업그레이드가 이루어졌습니다. 이 릴리스에서는 현지 시간이 오전 1시에서 오전 5시 사이인 경우 BlueXP classification 자동으로 업그레이드됩니다. 현지 시간이 이 시간대를 벗어나면 마지막 사용자 활동 이후 특정 시간이 경과한 후에 업그레이드가 수행됩니다. 자세한 내용은 다음을 참조하세요. "인터넷 접속이 가능한 Linux 호스트에 설치" .

인터넷 접속 없이 BlueXP classification 배포한 경우 수동으로 업그레이드해야 합니다. 자세한 내용은 다음을 참조하세요. "인터넷 접속이 없는 Linux 호스트에 BlueXP classification 설치" .

2024년 3월 4일

버전 1.29

이제 특정 데이터 소스 디렉토리에 있는 스캐닝 데이터를 제외할 수 있습니다**.**

BlueXP classification 특정 데이터 소스 디렉토리에 있는 스캐닝 데이터를 제외하려면 BlueXP classification 에서 처리하는 구성 파일에 이러한 디렉토리 이름을 추가할 수 있습니다. 이 기능을 사용하면 불필요한 디렉토리를 스캔하지

않아도 되고, 잘못된 개인 데이터 결과가 반환되는 것을 방지할 수 있습니다.

"자세히 알아보기" .

초대형 인스턴스 지원이 이제 인증되었습니다.

2억 5천만 개가 넘는 파일을 검사하기 위해 BlueXP classification 필요한 경우 클라우드 배포 또는 온프레미스 설치에서 Extra Large 인스턴스를 사용할 수 있습니다. 이러한 유형의 시스템은 최대 5억 개의 파일을 검사할 수 있습니다.

"자세히 알아보기" .

2024년 1월 10일

버전 **1.27**

조사 페이지 결과에는 총 항목 수 외에도 총 크기가 표시됩니다.

조사 페이지에서 필터링된 결과에는 총 파일 수 외에도 항목의 총 크기가 표시됩니다. 이 기능은 파일을 이동하거나, 파일을 삭제하는 등의 작업에 도움이 될 수 있습니다.

추가 그룹 **ID**를 **"**조직에 공개**"**로 구성합니다.

그룹에 원래 해당 권한이 설정되지 않은 경우, 이제 BlueXP classification 에서 직접 NFS의 그룹 ID를 "조직에 개방됨"으로 간주하도록 구성할 수 있습니다. 이러한 그룹 ID가 첨부된 모든 파일과 폴더는 조사 세부 정보 페이지에서 "조직에 공개됨"으로 표시됩니다. 방법을 확인하세요"추가 그룹 ID를 "조직에 공개"로 추가합니다." .

2023년 12월 14일

버전 **1.26.6**

이번 릴리스에는 몇 가지 사소한 개선 사항이 포함되었습니다.

이 릴리스에서는 다음 옵션도 제거되었습니다.

- 감사 로그 수집을 활성화하는 옵션이 비활성화되었습니다.
- 디렉토리 조사 중에 디렉토리별 개인 식별 정보(PII) 데이터 수를 계산하는 옵션을 사용할 수 없습니다. "귀하의 조직에 저장된 데이터를 조사하세요" .
- Azure Information Protection(AIP) 레이블을 사용하여 데이터를 통합하는 옵션이 비활성화되었습니다.

2023년 11월 6일

버전 **1.26.3**

이 릴리스에서는 다음 문제가 해결되었습니다.

- 대시보드에서 시스템이 스캔한 파일 수를 표시할 때 발생하는 불일치를 해결했습니다.
- 이름과 메타데이터에 특수 문자가 포함된 파일과 디렉토리를 처리하고 보고하여 스캐닝 동작을 개선했습니다.

2023년 10월 4일

버전 **1.26**

RHEL 버전 **9**에서 **BlueXP classification** 의 온프레미스 설치 지원

Red Hat Enterprise Linux 버전 8과 9는 BlueXP classification 설치에 필요한 Docker 엔진을 지원하지 않습니다. 이제 Podman 버전 4 이상을 컨테이너 인프라로 사용하여 RHEL 9.0, 9.1 및 9.2에서 BlueXP classification 설치를 지원합니다. 사용자 환경에서 최신 버전의 RHEL을 사용해야 하는 경우 이제 Podman을 사용할 때 BlueXP classification (버전 1.26 이상)를 설치할 수 있습니다.

현재 RHEL 9.x를 사용할 경우 다크 사이트 설치나 분산 스캐닝 환경(마스터 및 원격 스캐너 노드 사용)은 지원되지 않습니다.

2023년 9월 5일

버전 **1.25**

소규모 및 중규모 배포는 일시적으로 사용할 수 없습니다**.**

AWS에서 BlueXP classification 인스턴스를 배포할 때 *배포 > 구성*을 선택하고 소규모 또는 중규모 인스턴스를 선택하는 옵션은 현재 사용할 수 없습니다. *배포 > 배포*를 선택하면 대용량 인스턴스 크기를 사용하여 인스턴스를 배포할 수 있습니다.

조사 결과 페이지에서 최대 **100,000**개 항목에 태그를 적용합니다**.**

과거에는 조사 결과 페이지에서 한 번에 하나의 페이지(20개 항목)에만 태그를 적용할 수 있었습니다. 이제 조사 결과 페이지에서 모든 항목을 선택하고 모든 항목에 태그를 적용할 수 있습니다. 한 번에 최대 100,000개 항목까지 적용할 수 있습니다.

최소 **1MB**의 파일 크기를 갖는 중복 파일을 식별합니다**.**

BlueXP classification 파일 크기가 50MB 이상인 경우에만 중복 파일을 식별하는 데 사용됩니다. 이제 1MB로 시작하는 중복 파일을 식별할 수 있습니다. 조사 페이지 필터인 "파일 크기"와 "중복"을 사용하여 사용자 환경에서 특정 크기의 어떤 파일이 중복되었는지 확인할 수 있습니다.

2023년 7월 17일

버전 **1.24**

BlueXP classification 를 통해 두 가지 새로운 유형의 독일 개인 데이터가 식별되었습니다**.**

BlueXP classification 다음 유형의 데이터를 포함하는 파일을 식별하고 분류할 수 있습니다.

- 독일 ID(Personalausweisnummer)
- 독일 사회 보장 번호(Sozialversicherungsnummer)

"BlueXP classification 귀하의 데이터에서 식별할 수 있는 모든 유형의 개인 데이터를 확인하세요." .

BlueXP classification 제한 모드와 비공개 모드에서 완벽하게 지원됩니다**.**

이제 BlueXP classification 인터넷 접속이 불가능한 사이트(개인 모드)와 아웃바운드 인터넷 접속이 제한된 사이트(제한 모드)에서도 완벽하게 지원됩니다. "커넥터용 BlueXP 배포 모드에 대해 자세히 알아보세요." .

BlueXP classification 의 개인 모드 설치를 업그레이드할 때 버전을 건너뛸 수 있는 기능

이제 순차적이지 않더라도 최신 버전의 BlueXP classification 로 업그레이드할 수 있습니다. 즉, BlueXP classification 한 번에 한 버전씩 업그레이드해야 하는 현재 제한은 더 이상 필요하지 않습니다. 이 기능은 1.24 버전부터 적용됩니다.

BlueXP classification API를 이제 사용할 수 있습니다**.**

BlueXP classification API를 사용하면 스캔 중인 데이터에 대한 작업을 수행하고, 쿼리를 만들고, 정보를 내보낼 수 있습니다. 대화형 문서는 Swagger를 사용하여 사용할 수 있습니다. 문서는 조사, 규정 준수, 거버넌스, 구성을 포함한 여러 범주로 구분됩니다. 각 카테고리는 BlueXP classification UI의 탭을 참조합니다.

"BlueXP classification API에 대해 자세히 알아보세요" .

2023년 6월 6일

버전 **1.23**

이제 데이터 주체 이름을 검색할 때 일본어가 지원됩니다**.**

이제 데이터 주체 접근 요청(DSAR)에 대한 응답으로 주체의 이름을 검색할 때 일본어 이름을 입력할 수 있습니다. 생성할 수 있습니다"데이터 주체 접근 요청 보고서" 그 결과 정보를 사용하여. 일본어 이름도 입력할 수 있습니다."데이터 조사 페이지의 "데이터 주체" 필터" 주제의 이름이 포함된 파일을 식별합니다.

Ubuntu는 이제 **BlueXP classification** 설치할 수 있는 지원되는 **Linux** 배포판입니다**.**

Ubuntu 22.04는 BlueXP classification 에 지원되는 운영 체제로 인증되었습니다. 설치 프로그램의 버전 1.23을 사용하면 네트워크의 Ubuntu Linux 호스트나 클라우드의 Linux 호스트에 BlueXP classification 설치할 수 있습니다. "Ubuntu가 설치된 호스트에 BlueXP classification 설치하는 방법을 알아보세요." .

Red Hat Enterprise Linux 8.6 및 **8.7**은 더 이상 새로운 **BlueXP classification** 설치에서 지원되지 않습니다**.**

Docker는 Red Hat이 더 이상 필수 조건이므로 이러한 버전은 새로운 배포에서는 지원되지 않습니다. RHEL 8.6 또는 8.7에서 실행되는 기존 BlueXP classification 머신이 있는 경우 NetApp 해당 구성을 계속 지원합니다.

BlueXP classification ONTAP 시스템에서 **FPolicy** 이벤트를 수신하기 위한 **FPolicy** 수집기로 구성될 수 있습니다**.**

작업 환경의 볼륨에서 감지된 파일 액세스 이벤트에 대해 BlueXP classification 시스템에서 파일 액세스 감사 로그를 수집하도록 설정할 수 있습니다. BlueXP classification 다음과 같은 유형의 FPolicy 이벤트와 파일에 대한 작업을 수행한 사용자를 캡처할 수 있습니다: 만들기, 읽기, 쓰기, 삭제, 이름 바꾸기, 소유자/권한 변경, SACL/DACL 변경.

이제 다크 사이트에서 **Data Sense BYOL** 라이선스가 지원됩니다**.**

이제 다크 사이트에서 Data Sense BYOL 라이선스를 BlueXP digital wallet 에 업로드하여 라이선스가 부족해질 때 알림을 받을 수 있습니다.

2023년 4월 3일

버전 **1.22**

새로운 데이터 발견 평가 보고서

데이터 검색 평가 보고서는 스캔한 환경에 대한 높은 수준의 분석을 제공하여 시스템 결과를 강조하고 문제가 있는 영역과 잠재적인 수정 단계를 보여줍니다. 이 보고서의 목적은 데이터 세트의 데이터 거버넌스 문제, 데이터 보안 노출, 데이터 규정 준수 격차에 대한 인식을 높이는 것입니다. "데이터 발견 평가 보고서를 생성하고 사용하는 방법을 알아보세요." .

클라우드의 소규모 인스턴스에 **BlueXP classification** 배포하는 기능

AWS 환경에서 BlueXP Connector를 통해 BlueXP classification 배포할 때 이제 기본 인스턴스에서 사용할 수 있는 것보다 더 작은 두 개의 인스턴스 유형 중에서 선택할 수 있습니다. 소규모 환경을 스캔하는 경우 클라우드 비용을

절감하는 데 도움이 될 수 있습니다. 하지만 작은 인스턴스를 사용할 때는 몇 가지 제한이 있습니다. "사용 가능한 인스턴스 유형 및 제한 사항을 확인하세요." .

이제 **BlueXP classification** 설치 전에 **Linux** 시스템을 검증하기 위한 독립 실행형 스크립트를 사용할 수 있습니다**.**

BlueXP classification 설치를 실행하지 않고도 Linux 시스템이 모든 필수 구성 요소를 충족하는지 확인하려면 필수 구성 요소만 테스트하는 별도의 스크립트를 다운로드할 수 있습니다. "Linux 호스트가 BlueXP classification 설치할 준비가 되었는지 확인하는 방법을 알아보세요." .

2023년 3월 7일

버전 **1.21**

BlueXP classification UI에서 사용자 정의 범주를 추가하는 새로운 기능

이제 BlueXP classification 통해 사용자 정의 범주를 추가할 수 있으므로 BlueXP classification 통해 해당 범주에 맞는 파일을 식별할 수 있습니다. BlueXP classification 에는 많은 것이 있습니다 "미리 정의된 카테고리" 따라서 이 기능을 사용하면 사용자 정의 범주를 추가하여 조직에 고유한 정보가 데이터에서 어디에 있는지 식별할 수 있습니다.

이제 **BlueXP classification UI**에서 사용자 정의 키워드를 추가할 수 있습니다**.**

BlueXP classification 향후 스캔에서 BlueXP classification 식별할 수 있는 사용자 정의 키워드를 추가하는 기능을 갖추고 있습니다. 하지만 키워드를 추가하려면 BlueXP classification Linux 호스트에 로그인하고 명령줄 인터페이스를 사용해야 합니다. 이번 릴리스에서는 BlueXP classification UI에 사용자 정의 키워드를 추가하는 기능이 추가되어 키워드를 매우 쉽게 추가하고 편집할 수 있습니다.

"마지막 액세스 시간**"**이 변경될 때 **BlueXP classification** 가 파일을 스캔하지 않도록 하는 기능

기본적으로 BlueXP classification 적절한 "쓰기" 권한이 없으면 시스템은 볼륨의 파일을 검사하지 않습니다. BlueXP classification "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 하지만 파일의 마지막 액세스 시간이 원래 시간으로 재설정되는 것이 문제가 되지 않는다면 구성 페이지에서 이 동작을 재정의하여 BlueXP classification 권한에 관계없이 볼륨을 검사하도록 할 수 있습니다.

이 기능과 함께 "스캔 분석 이벤트"라는 새 필터가 추가되어 BlueXP classification 에서 마지막 액세스 시간을 되돌릴 수 없어 분류되지 않은 파일이나 BlueXP classification 마지막 액세스 시간을 되돌릴 수 없어도 분류된 파일을 볼 수 있습니다.

""마지막 액세스 시간 타임스탬프" 및 BlueXP classification 에 필요한 권한에 대해 자세히 알아보세요." .

BlueXP classification 통해 **3**가지 새로운 유형의 개인 데이터가 식별되었습니다**.**

BlueXP classification 다음 유형의 데이터를 포함하는 파일을 식별하고 분류할 수 있습니다.

- 보츠와나 신분증(오망) 번호
- 보츠와나 여권 번호
- 싱가포르 국민등록 신분증(NRIC)

"BlueXP classification 귀하의 데이터에서 식별할 수 있는 모든 유형의 개인 데이터를 확인하세요." .

디렉토리에 대한 업데이트된 기능

- 데이터 조사 보고서의 "간단한 CSV 보고서" 옵션에 이제 디렉토리의 정보가 포함됩니다.
- "마지막 액세스" 시간 필터는 이제 파일과 디렉토리 모두에 대한 마지막 액세스 시간을 표시합니다.

설치 개선 사항

- 인터넷 접속이 불가능한 사이트(다크 사이트)를 위한 BlueXP classification 설치 프로그램은 이제 성공적인 설치를 위해 시스템 및 네트워킹 요구 사항이 제대로 갖춰져 있는지 사전 검사를 수행합니다.
- 설치 감사 로그 파일이 이제 저장되었습니다. `/ops/netapp/install_logs` .

2023년 2월 5일

버전 **1.20**

모든 이메일 주소로 정책 기반 알림 이메일을 보낼 수 있는 기능

이전 버전의 BlueXP classification 에서는 특정 중요 정책에 대한 결과가 반환되면 계정의 BlueXP 사용자에게 이메일 알림을 보낼 수 있었습니다. 이 기능을 사용하면 온라인 상태가 아닐 때 데이터를 보호하기 위한 알림을 받을 수 있습니다. 이제 BlueXP 계정에 없는 다른 사용자(최대 20개 이메일 주소)에게도 정책에서 이메일 알림을 보낼 수 있습니다.

"정책 결과에 따라 이메일 알림을 보내는 방법에 대해 자세히 알아보세요." .

이제 **BlueXP classification UI**에서 개인 패턴을 추가할 수 있습니다**.**

BlueXP classification BlueXP classification 스캔에서 식별할 수 있는 맞춤형 "개인 데이터"를 추가하는 기능을 갖추고 있습니다. 하지만 사용자 정의 패턴을 추가하려면 BlueXP classification Linux 호스트에 로그인하고 명령줄을 사용해야 했습니다. 이번 릴리스에서는 정규식을 사용하여 개인 패턴을 추가하는 기능이 BlueXP classification UI에 추가되어 이러한 사용자 정의 패턴을 매우 쉽게 추가하고 편집할 수 있습니다.

BlueXP classification 사용하여 **1,500**만 개의 파일을 이동할 수 있는 기능

과거에는 BlueXP classification 최대 100,000개의 소스 파일을 모든 NFS 공유로 옮길 수 있었습니다. 이제 최대 1,500만 개의 파일을 한 번에 이동할 수 있습니다.

SharePoint Online 파일에 액세스할 수 있는 사용자 수를 볼 수 있는 기능

"액세스 권한이 있는 사용자 수" 필터는 이제 SharePoint Online 저장소에 저장된 파일을 지원합니다. 과거에는 CIFS 공유에 있는 파일만 지원되었습니다. 현재 Active Directory 기반이 아닌 SharePoint 그룹은 이 필터에 포함되지 않습니다.

새로운 **"**부분적 성공**"** 상태가 작업 상태 패널에 추가되었습니다**.**

새로운 "부분적 성공" 상태는 BlueXP classification 작업이 완료되었고 일부 항목은 실패하고 일부 항목은 성공했음을 나타냅니다. 예를 들어, 100개의 파일을 이동하거나 삭제할 때입니다. 또한, "완료" 상태의 이름이 "성공"으로 변경되었습니다. 과거에는 "완료" 상태에 성공한 작업과 실패한 작업이 나열되었습니다. 이제 "성공" 상태는 모든 항목에 대한 모든 작업이 성공했음을 의미합니다. "작업 상태 패널을 보는 방법 보기" .

2023년 1월 9일

버전 **1.19**

민감한 데이터가 포함되어 있고 지나치게 허용적인 파일 차트를 볼 수 있는 기능

거버넌스 대시보드에 새로운 민감한 데이터 및 광범위한 권한 영역이 추가되었는데, 이 영역은 민감한 데이터(민감한 데이터와 민감한 개인 데이터 모두 포함)를 포함하고 지나치게 권한이 부여된 파일의 히트맵을 제공합니다. 이를 통해 민감한 데이터와 관련하여 어떤 위험이 있는지 파악하는 데 도움이 될 수 있습니다. "자세히 알아보기" .

데이터 조사 페이지에서 세 가지 새로운 필터를 사용할 수 있습니다**.**

데이터 조사 페이지에 표시되는 결과를 구체화하기 위해 새로운 필터를 사용할 수 있습니다.

- "액세스 권한이 있는 사용자 수" 필터는 특정 수의 사용자에게 열려 있는 파일과 폴더를 보여줍니다. 결과를 구체화하기 위해 숫자 범위를 선택할 수 있습니다. 예를 들어, 51~100명의 사용자가 접근할 수 있는 파일을 확인할 수 있습니다.
- 이제 "생성 시간", "검색 시간", "마지막 수정" 및 "마지막 액세스" 필터를 사용하여 미리 정의된 날짜 범위를 선택하는 대신 사용자 지정 날짜 범위를 만들 수 있습니다. 예를 들어, "생성 시간"이 "6개월 이상"인 파일이나 "마지막 수정 날짜"가 "지난 10일 이내"인 파일을 찾을 수 있습니다.
- 이제 "파일 경로" 필터를 사용하여 필터링된 쿼리 결과에서 제외할 경로를 지정할 수 있습니다. 특정 데이터를 포함하고 제외하는 경로를 입력하면 BlueXP classification 먼저 포함된 경로에 있는 모든 파일을 찾은 다음, 제외된 경로에서 파일을 제거한 다음 결과를 표시합니다.

"데이터를 조사하는 데 사용할 수 있는 모든 필터 목록을 확인하세요." .

BlueXP classification 일본 개인 번호를 식별할 수 있습니다**.**

BlueXP classification 일본 개인 번호(마이 넘버라고도 함)가 포함된 파일을 식별하고 분류할 수 있습니다. 여기에는 개인 및 회사 내 번호가 모두 포함됩니다. "BlueXP classification 귀하의 데이터에서 식별할 수 있는 모든 유형의 개인 데이터를 확인하세요." .

NetApp Data Classification 의 알려진 제한 사항

알려진 제한 사항은 이 릴리스에서 지원되지 않거나 올바르게 상호 운용되지 않는 기능을 나타냅니다. 이러한 제한 사항을 주의 깊게 검토하세요.

NetApp Data Classification 비활성화 옵션

2023년 12월(버전 1.26.6) 릴리스에서는 다음 옵션이 제거되었습니다.

- 감사 로그 수집을 활성화하는 옵션이 비활성화되었습니다.
- 디렉토리 조사 중에 디렉토리별 개인 식별 정보(PII) 데이터 수를 계산하는 옵션을 사용할 수 없습니다.
- Azure Information Protection(AIP) 레이블을 사용하여 데이터를 통합하는 옵션이 비활성화되었습니다.

데이터 분류 스캐닝

데이터 분류 스캔에는 다음과 같은 제한 사항이 있습니다.

데이터 분류는 볼륨 아래의 단 하나의 공유만 스캔합니다**.**

단일 볼륨 아래에 여러 개의 파일 공유가 있는 경우 데이터 분류는 계층 구조가 가장 높은 공유를 스캔합니다. 예를 들어, 다음과 같은 주식이 있다고 가정해 보겠습니다.

- /에이
- /A/B
- /기음
- /디/이

이 구성에서는 /A의 데이터만 스캔됩니다. /C와 /D의 데이터는 스캔되지 않습니다.

해결 방법

볼륨의 모든 공유에서 데이터를 스캔하고 있는지 확인하는 해결 방법이 있습니다. 다음 단계를 따르세요.

1. 시스템에서 스캔할 볼륨을 추가합니다.
2. 데이터 분류가 볼륨 스캔을 완료한 후 데이터 조사 페이지로 이동하여 스캔 중인 공유를 확인하기 위한 필터를 만듭니다.

   "시스템 이름"과 "디렉토리 유형 = 공유"로 데이터를 필터링하여 어떤 공유가 스캔되고 있는지 확인하세요.

3. 볼륨에 존재하는 주식의 전체 목록을 가져와서 스캔되지 않은 주식이 무엇인지 확인하세요.
4. "나머지 주식을 공유 그룹에 추가합니다." .

   예를 들어, 모든 주식을 개별적으로 추가합니다.

   ```
   /C
   /D
   ```

5. 여러 공유가 있는 시스템의 각 볼륨에 대해 이 단계를 수행합니다.

마지막으로 액세스한 타임스탬프

데이터 분류가 디렉토리를 스캔할 때, 해당 스캔은 디렉토리의 마지막 액세스 필드에 영향을 미칩니다. 마지막으로 접근한 날짜 필드를 보면 해당 메타데이터는 스캔 날짜와 시간 또는 사용자가 디렉토리에 마지막으로 접근한 시간을 반영합니다.

시작하기

NetApp Data Classification 에 대해 알아보세요

NetApp Data Classification 는 NetApp Console 위한 데이터 거버넌스 서비스로, 기업의 온프레미스 및 클라우드 데이터 소스를 스캔하여 데이터를 매핑하고 분류하며 개인 정보를 식별합니다. 이를 통해 보안 및 규정 준수 위험을 줄이고, 스토리지 비용을 절감하고, 데이터 마이그레이션 프로젝트를 지원할 수 있습니다.

버전 1.31부터 데이터 분류가 NetApp Console 의 핵심 기능으로 제공됩니다. 추가 비용은 없습니다. 분류 라이센스나 구독이 필요하지 않습니다. + 기존 버전 1.30 또는 이전 버전을 사용 중이신 경우, 구독이 만료될 때까지 해당 버전을 사용할 수 있습니다.

NetApp Console

데이터 분류는 NetApp Console 통해 접근할 수 있습니다.

NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경 전반에서 NetApp 스토리지 및 데이터 서비스를 중앙에서 관리할 수 있는 기능을 제공합니다. NetApp 데이터 서비스에 액세스하고 사용하려면 콘솔이 필요합니다. 관리 인터페이스로서, 하나의 인터페이스에서 여러 스토리지 리소스를 관리할 수 있습니다. 콘솔 관리자는 기업 내 모든 시스템의 저장소와 서비스에 대한 액세스를 제어할 수 있습니다.

NetApp Console 사용하려면 라이선스나 구독이 필요하지 않으며, 스토리지 시스템이나 NetApp 데이터 서비스에 대한 연결을 보장하기 위해 클라우드에 Console 에이전트를 배포해야 할 때만 요금이 부과됩니다. 그러나 콘솔에서 액세스할 수 있는 일부 NetApp 데이터 서비스는 라이선스 기반이거나 구독 기반입니다.

자세히 알아보세요"NetApp Console" .

특징

데이터 분류는 인공지능(AI), 자연어 처리(NLP), 머신 러닝(ML)을 사용하여 스캔한 콘텐츠를 이해하고 엔터티를 추출하고 그에 따라 콘텐츠를 분류합니다. 이를 통해 데이터 분류는 다음과 같은 기능 영역을 제공할 수 있습니다.

"데이터 분류 사용 사례에 대해 알아보세요" .

규정 준수 유지

데이터 분류는 규정 준수 노력에 도움이 되는 다양한 도구를 제공합니다. 데이터 분류를 사용하여 다음을 수행할 수 있습니다.

- 개인 식별 정보(PII)를 식별합니다.
- GDPR, CCPA, PCI 및 HIPAA 개인정보 보호 규정에서 요구하는 대로 광범위한 민감한 개인 정보를 식별합니다.
- 이름이나 이메일 주소를 기반으로 데이터 주체 접근 요청(DSAR)에 응답합니다.

보안 강화

데이터 분류를 통해 범죄 목적으로 접근될 위험이 있는 데이터를 식별할 수 있습니다. 데이터 분류를 사용하여 다음을 수행할 수 있습니다.

- 전체 조직이나 대중에게 공개된, 공개 권한이 있는 모든 파일과 디렉토리(공유 및 폴더)를 식별합니다.

- 처음 지정된 위치 외부에 있는 민감한 데이터를 식별합니다.
- 데이터 보존 정책을 준수합니다.
- 정책을 사용하면 새로운 보안 문제를 자동으로 감지하여 보안 직원이 즉시 조치를 취할 수 있습니다.

저장 공간 사용량 최적화

데이터 분류는 스토리지 총 소유 비용(TCO)을 절감하는 데 도움이 되는 도구를 제공합니다. 데이터 분류를 사용하여 다음을 수행할 수 있습니다.

- 중복된 데이터나 업무와 관련 없는 데이터를 식별하여 저장 효율성을 높입니다.
- 비활성 데이터를 식별하여 비용이 덜 드는 개체 스토리지로 계층화하여 스토리지 비용을 절감하세요. "Cloud Volumes ONTAP 시스템의 계층화에 대해 자세히 알아보세요." . "온프레미스 ONTAP 시스템의 계층화에 대해 자세히 알아보세요." .

지원되는 시스템 및 데이터 소스

데이터 분류는 다음 유형의 시스템 및 데이터 소스에서 구조화된 데이터와 구조화되지 않은 데이터를 스캔하고 분석할 수 있습니다.

시스템

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP (AWS, Azure 또는 GCP에 배포됨)
- 온프레미스 ONTAP 클러스터
- StorageGRID
- Google Cloud NetApp Volumes

데이터 출처

- NetApp 파일 공유
- 데이터베이스:
  - Amazon 관계형 데이터베이스 서비스(Amazon RDS)
  - 몽고디비
  - MySQL
  - 신탁
  - 포스트그레스큐엘
  - SAP 하나
  - SQL 서버(MSSQL)

데이터 분류는 NFS 버전 3.x, 4.0, 4.1과 CIFS 버전 1.x, 2.0, 2.1, 3.0을 지원합니다.

비용

데이터 분류는 무료로 사용할 수 있습니다. 분류 라이센스나 유료 구독이 필요하지 않습니다.

인프라 비용

- 클라우드에 데이터 분류를 설치하려면 클라우드 인스턴스를 배포해야 하며, 배포된 클라우드 제공업체에서 요금이 부과됩니다. 보다 각 클라우드 공급자에 배포되는 인스턴스 유형 . 온프레미스 시스템에 데이터 분류를 설치하는 경우 비용이 발생하지 않습니다.
- 데이터 분류를 위해서는 콘솔 에이전트를 배포해야 합니다. 많은 경우 콘솔에서 다른 저장소와 서비스를 사용하고 있기 때문에 이미 콘솔 에이전트가 있는 것입니다. 콘솔 에이전트 인스턴스는 배포된 클라우드 공급자로부터 요금이 부과됩니다. 를 참조하십시오 "각 클라우드 공급자에 배포되는 인스턴스 유형" . 온프레미스 시스템에 콘솔 에이전트를 설치하는 경우 비용이 발생하지 않습니다.

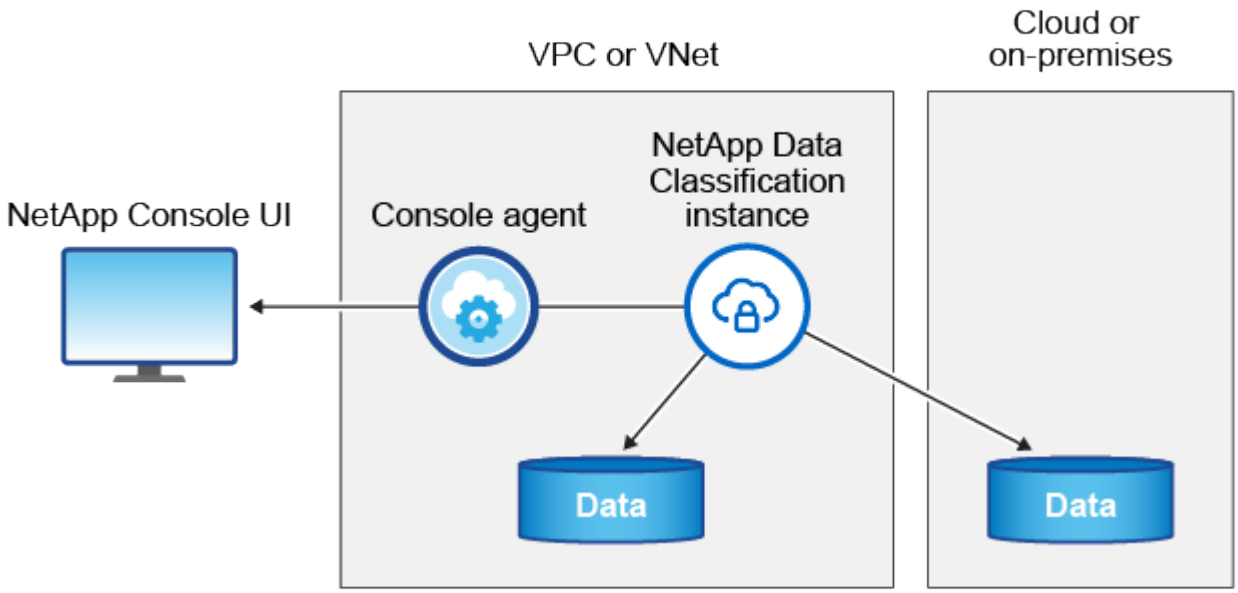
데이터 전송 비용

데이터 전송 비용은 설정에 따라 달라집니다. 데이터 분류 인스턴스와 데이터 소스가 동일한 가용성 영역 및 지역에 있는 경우 데이터 전송 비용이 발생하지 않습니다. 하지만 Cloud Volumes ONTAP 시스템과 같은 데이터 소스가 다른 가용성 영역이나 지역에 있는 경우 클라우드 공급자가 데이터 전송 비용을 청구합니다. 자세한 내용은 다음 링크를 참조하세요.

- "AWS: Amazon Elastic Compute Cloud(Amazon EC2) 가격"
- "Microsoft Azure: 대역폭 가격 세부 정보"
- "Google Cloud: Storage Transfer Service 가격 책정"

데이터 분류 인스턴스

클라우드에 데이터 분류를 배포하면 콘솔은 콘솔 에이전트와 동일한 서브넷에 인스턴스를 배포합니다. "콘솔 에이전트에 대해 자세히 알아보세요."



기본 인스턴스에 대해 다음 사항을 참고하세요.

- AWS에서는 데이터 분류가 실행됩니다. "m6i.4xlarge 인스턴스" 500GiB GP2 디스크 포함. 운영체제 이미지는 Amazon Linux 2입니다. AWS에 배포하는 경우 소량의 데이터를 스캔하는 경우 더 작은 인스턴스 크기를 선택할 수 있습니다.
- Azure에서 데이터 분류는 다음에서 실행됩니다."Standard_D16s_v3 VM" 500GiB 디스크 포함. 운영체제 이미지는 Ubuntu 22.04입니다.

- GCP에서 데이터 분류는 다음에서 실행됩니다."n2-standard-16 VM" 500GiB 표준 영구 디스크를 사용합니다. 운영체제 이미지는 Ubuntu 22.04입니다.
- 기본 인스턴스를 사용할 수 없는 지역에서는 데이터 분류가 대체 인스턴스에서 실행됩니다. "대체 인스턴스 유형을 확인하세요" .
- 인스턴스 이름은 *CloudCompliance_*이고, 생성된 해시*(UUID)*가 여기에 연결됩니다. 예*: _CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- 콘솔 에이전트당 하나의 데이터 분류 인스턴스만 배포됩니다.

사내 Linux 호스트나 선호하는 클라우드 공급업체의 호스트에 데이터 분류를 배포할 수도 있습니다. 어떤 설치 방법을 선택하든 소프트웨어의 기능은 정확히 동일합니다. 인스턴스에 인터넷 접속이 가능한 한 데이터 분류 소프트웨어 업그레이드는 자동화됩니다.

데이터 분류는 지속적으로 데이터를 스캔하므로 인스턴스는 항상 실행 상태를 유지해야 합니다.

다양한 인스턴스 유형에 배포

인스턴스 유형에 대한 다음 사양을 검토하세요.

시스템 크기	명세서	제한 사항
특대	32개 CPU, 128GB RAM, 1TiB SSD	최대 5억 개의 파일을 검색할 수 있습니다.
대형(기본값)	CPU 16개, 64GB RAM, 500GiB SSD	최대 2억 5천만 개의 파일을 스캔할 수 있습니다.

Azure 또는 GCP에서 데이터 분류를 배포할 때 더 작은 인스턴스 유형을 사용하려면 ng-contact-data-sense@netapp.com으로 이메일을 보내 지원을 요청하세요.

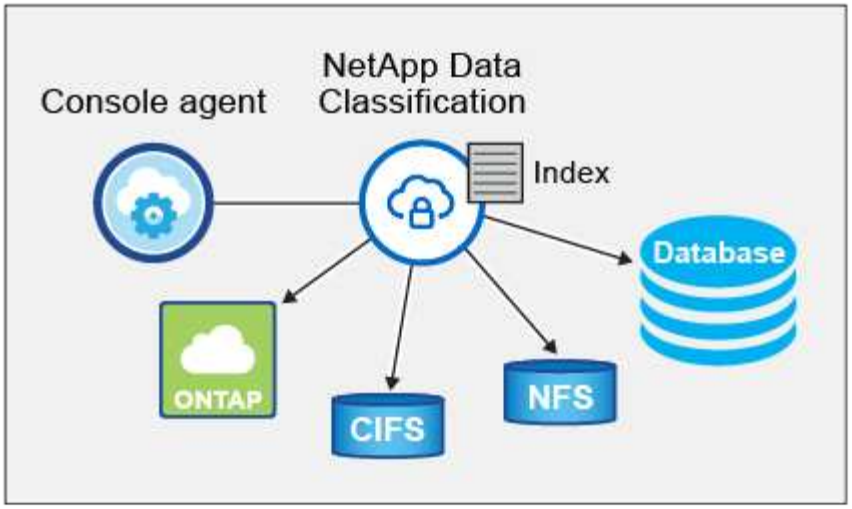
데이터 분류 스캐닝 작동 방식

높은 수준에서 데이터 분류 스캐닝은 다음과 같이 작동합니다.

1. 콘솔에서 데이터 분류 인스턴스를 배포합니다.
2. 하나 이상의 데이터 소스에서 고수준 매핑(매핑 전용 스캔이라고 함) 또는 심층 수준 스캐닝(맵 및 분류 스캔이라고 함)을 활성화합니다.
3. 데이터 분류는 AI 학습 프로세스를 사용하여 데이터를 스캔합니다.
4. 제공된 대시보드와 보고 도구를 사용하면 규정 준수 및 거버넌스 활동에 도움이 됩니다.

데이터 분류를 활성화하고 스캔하려는 저장소(볼륨, 데이터베이스 스키마 또는 기타 사용자 데이터)를 선택하면 즉시 데이터 스캔을 시작하여 개인 및 민감한 데이터를 식별합니다. 대부분의 경우 백업, 미러 또는 DR 사이트 대신 라이브 프로덕션 데이터 스캔에 집중해야 합니다. 그런 다음 데이터 분류는 조직 데이터를 매핑하고, 각 파일을 분류하고, 데이터에서 엔터티와 사전 정의된 패턴을 식별하여 추출합니다. 검사 결과는 개인 정보, 민감한 개인 정보, 데이터 범주 및 파일 유형의 인덱스입니다.

데이터 분류는 NFS 및 CIFS 볼륨을 마운트하여 다른 클라이언트와 마찬가지로 데이터에 연결합니다. NFS 볼륨은 자동으로 읽기 전용으로 액세스되는 반면, CIFS 볼륨을 스캔하려면 Active Directory 자격 증명을 제공해야 합니다.



초기 스캔 이후, 데이터 분류는 라운드 로빈 방식으로 데이터를 지속적으로 스캔하여 증분적 변경 사항을 감지합니다. 인스턴스를 계속 실행하는 것이 중요한 이유가 여기에 있습니다.

볼륨 수준이나 데이터베이스 스키마 수준에서 검사를 활성화하거나 비활성화할 수 있습니다.

데이터 분류는 스캔할 수 있는 데이터 양에 제한을 두지 않습니다. 각 콘솔 에이전트는 500TiB의 데이터를 스캔하고 표시하는 것을 지원합니다. 500TiB 이상의 데이터를 스캔하려면"다른 콘솔 에이전트를 설치하세요" 그 다음에"다른 데이터 분류 인스턴스 배포" . + 콘솔 UI는 단일 커넥터의 데이터를 표시합니다. 여러 콘솔 에이전트의 데이터를 보는 방법에 대한 팁은 다음을 참조하세요."여러 콘솔 에이전트와 함께 작업" .

매핑 스캔과 분류 스캔의 차이점은 무엇입니까?

데이터 분류에서는 두 가지 유형의 스캔을 수행할 수 있습니다.

- 매핑 전용 스캔은 데이터에 대한 개략적인 개요만 제공하며 선택된 데이터 소스에서 수행됩니다. 매핑 전용 스캔은 파일에 액세스하여 내부 데이터를 확인하지 않으므로 매핑 및 분류 스캔보다 시간이 덜 걸립니다. 연구할 분야를 파악하기 위해 먼저 이 작업을 수행한 다음 해당 분야에 대한 지도 및 분류 검사를 수행하는 것이 좋습니다.
- **Map & Classify** 스캔은 데이터에 대한 심층적인 스캔을 제공합니다.

매핑 스캔과 분류 스캔의 차이점에 대한 자세한 내용은 다음을 참조하세요."매핑 스캔과 분류 스캔의 차이점은 무엇인가요?" .

데이터 분류가 분류하는 정보

데이터 분류는 다음 데이터를 수집, 색인화하고 범주를 지정합니다.

- 파일에 대한 표준 메타데이터: 파일 유형, 크기, 생성 및 수정 날짜 등.
- 개인 데이터: 이메일 주소, 신분증 번호 또는 신용 카드 번호와 같은 개인 식별 정보(PII)로, 데이터 분류는 파일에서 특정 단어, 문자열 및 패턴을 사용하여 이를 식별합니다. "개인 데이터에 대해 자세히 알아보세요" .
- 민감한 개인 정보: 건강 데이터, 민족적 기원 또는 정치적 의견과 같은 특수 유형의 민감한 개인 정보(SPII)로, 일반 데이터 보호 규정(GDPR) 및 기타 개인정보 보호 규정에 정의되어 있습니다. "민감한 개인 데이터에 대해 자세히 알아보세요" .
- 범주: 데이터 분류는 스캔한 데이터를 여러 유형의 범주로 분류합니다. 카테고리는 각 파일의 콘텐츠와

메타데이터에 대한 AI 분석을 기반으로 한 주제입니다. "카테고리에 대해 자세히 알아보세요".

- 이름 엔터티 인식: 데이터 분류는 AI를 사용하여 문서에서 사람들의 실제 이름을 추출합니다. "데이터 주체 접근 요청에 응답하는 방법에 대해 알아보세요" .

네트워킹 개요

데이터 분류는 클라우드나 온프레미스 등 원하는 곳에 단일 서버 또는 클러스터를 배포합니다. 서버는 표준 프로토콜을 통해 데이터 소스에 연결하고, 동일한 서버에 배포된 Elasticsearch 클러스터에서 검색 결과를 인덱싱합니다. 이를 통해 멀티 클라우드, 크로스 클라우드, 프라이빗 클라우드 및 온프레미스 환경을 지원할 수 있습니다.

콘솔은 콘솔 에이전트에서 인바운드 HTTP 연결을 활성화하는 보안 그룹과 함께 데이터 분류 인스턴스를 배포합니다.

SaaS 모드에서 콘솔을 사용하는 경우 콘솔 연결은 HTTPS를 통해 제공되고 브라우저와 데이터 분류 인스턴스 간에 전송되는 개인 데이터는 TLS 1.2를 사용하여 종단 간 암호화로 보호되므로 NetApp 과 타사가 해당 데이터를 읽을 수 없습니다.

아웃바운드 규칙은 완전히 공개되어 있습니다. 데이터 분류 소프트웨어를 설치하고 업그레이드하고 사용 지표를 전송하려면 인터넷 접속이 필요합니다.

엄격한 네트워킹 요구 사항이 있는 경우"데이터 분류가 접촉하는 엔드포인트에 대해 알아보세요" .

NetApp Data Classification 액세스

NetApp Console 통해 NetApp Data Classification 액세스할 수 있습니다.

콘솔에 로그인하려면 NetApp 지원 사이트 자격 증명을 사용하거나 이메일과 비밀번호를 사용하여 NetApp Console 로그인에 가입할 수 있습니다. "콘솔에 로그인하는 방법에 대해 자세히 알아보세요" .

특정 작업에는 특정 콘솔 사용자 역할이 필요합니다. "모든 서비스에 대한 콘솔 액세스 역할에 대해 알아보세요." .

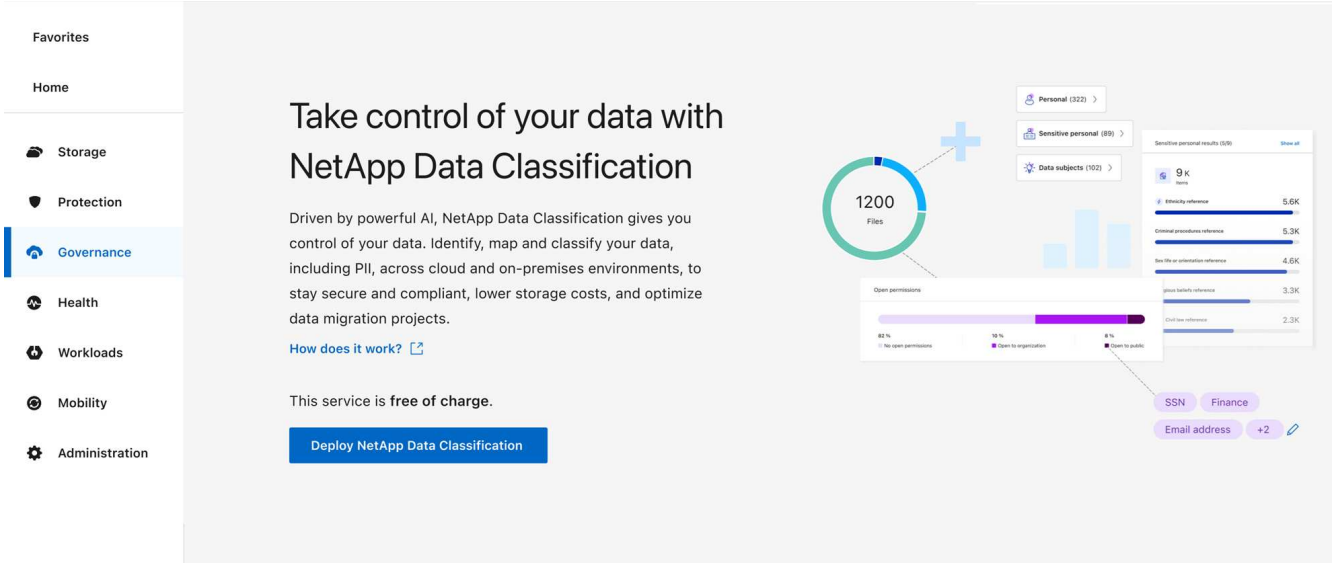
시작하기 전에

- "콘솔 에이전트를 추가해야 합니다."
- "귀하의 작업 부하에 적합한 데이터 분류 배포 스타일을 파악하세요."

단계

1. 웹 브라우저에서 다음으로 이동합니다."콘솔" .
2. 콘솔에 로그인합니다.
3. NetApp Console 의 메인 페이지에서 거버넌스 > *데이터 분류*를 선택합니다.
4. 처음으로 데이터 분류에 접속하는 경우 랜딩 페이지가 나타납니다.

   분류 인스턴스 배포를 시작하려면 *온프레미스 또는 클라우드에 분류 배포*를 선택하세요. 자세한 내용은 다음을 참조하세요."어떤 데이터 분류 배포를 사용해야 합니까?"



그렇지 않으면 데이터 분류 대시보드가 나타납니다.

데이터 분류 배포

어떤 **NetApp Data Classification** 배포를 사용해야 합니까**?**

NetApp Data Classification 다양한 방법으로 배포할 수 있습니다. 어떤 방법이 귀하의 필요에 맞는지 알아보세요.

데이터 분류는 다음과 같은 방법으로 배포될 수 있습니다.

- "콘솔을 사용하여 클라우드에 배포" . 콘솔은 콘솔 에이전트와 동일한 클라우드 공급자 네트워크에 데이터 분류 인스턴스를 배포합니다.
- "인터넷 접속이 가능한 Linux 호스트에 설치" . 인터넷 접속이 가능한 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에 데이터 분류를 설치합니다. 온프레미스 ONTAP 시스템을 온프레미스에 있는 데이터 분류 인스턴스를 사용하여 스캔하려는 경우 이러한 유형의 설치가 좋은 옵션일 수 있지만, 이는 필수 사항은 아닙니다.
- "인터넷 접속이 불가능한 온프레미스 사이트의 Linux 호스트에 설치"_비공개 모드_라고도 합니다. 설치 스크립트를 사용하는 이 유형의 설치는 콘솔 SaaS 계층에 연결할 수 없습니다.

> BlueXP 개인 모드(레거시 BlueXP 인터페이스)는 일반적으로 인터넷 연결이 없고 AWS Secret Cloud, AWS Top Secret Cloud, Azure IL6를 포함하는 보안 클라우드 지역이 있는 온프레미스 환경에서 사용됩니다. NetApp 기존 BlueXP 인터페이스를 통해 이러한 환경을 계속 지원합니다. 레거시 BlueXP 인터페이스의 개인 모드 설명서는 다음을 참조하세요."BlueXP 개인 모드에 대한 PDF 문서" .

인터넷 접속이 가능한 Linux 호스트에 설치하는 경우와 인터넷 접속이 불가능한 Linux 호스트에 온프레미스로 설치하는 경우 모두 설치 스크립트를 사용합니다. 스크립트는 시스템과 환경이 전제 조건을 충족하는지 확인하는 것으로 시작합니다. 필수 구성 요소가 충족되면 설치가 시작됩니다. 데이터 분류 설치를 실행하지 않고도 전제 조건을 독립적으로 확인하려면 전제 조건만 테스트하는 별도의 소프트웨어 패키지를 다운로드할 수 있습니다.

"Linux 호스트가 데이터 분류를 설치할 준비가 되었는지 확인하세요." .

NetApp Console 사용하여 클라우드에 NetApp Data Classification 배포합니다.

NetApp Console 사용하여 클라우드에 NetApp Data Classification 배포할 수 있습니다. 콘솔은 콘솔 에이전트와 동일한 클라우드 공급자 네트워크에 데이터 분류 인스턴스를 배포합니다.

또한 다음을 수행할 수도 있습니다."인터넷 접속이 가능한 Linux 호스트에 데이터 분류 설치" . 온프레미스 ONTAP 시스템을 온프레미스에 있는 데이터 분류 인스턴스를 사용하여 스캔하려는 경우 이러한 유형의 설치가 좋은 옵션일 수 있지만, 이는 필수 사항은 아닙니다. 어떤 설치 방법을 선택하든 소프트웨어의 기능은 정확히 동일합니다.

빠른 시작

다음 단계에 따라 빠르게 시작하거나, 나머지 섹션으로 스크롤하여 자세한 내용을 확인하세요.

1 콘솔 에이전트 만들기

아직 콘솔 에이전트가 없으면 하나 만드세요. 보다 "AWS에서 콘솔 에이전트 만들기" , "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" .

당신도 할 수 있습니다 "온프레미스에 콘솔 에이전트 설치" 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서.

2 필수 조건

귀하의 환경이 전제 조건을 충족하는지 확인하세요. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 콘솔 에이전트와 데이터 분류 간의 연결 등이 포함됩니다. 전체 목록 보기.

3 데이터 분류 배포

설치 마법사를 실행하여 클라우드에 데이터 분류 인스턴스를 배포합니다.

콘솔 에이전트 만들기

아직 콘솔 에이전트가 없다면 클라우드 공급자에서 콘솔 에이전트를 만드세요. 보다 "AWS에서 콘솔 에이전트 만들기" 또는 "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" . 대부분의 경우 데이터 분류를 활성화하기 전에 콘솔 에이전트를 설정했을 가능성이 높습니다. "콘솔 기능에는 콘솔 에이전트가 필요합니다." 하지만 지금 당장 설정해야 하는 경우도 있습니다.

특정 클라우드 공급자에 배포된 콘솔 에이전트를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP 또는 Amazon FSx for ONTAP 버킷에서 데이터를 스캔할 때 AWS의 콘솔 에이전트를 사용합니다.
- Azure의 Cloud Volumes ONTAP 또는 Azure NetApp Files 에서 데이터를 스캔할 때 Azure의 콘솔 에이전트를 사용합니다.
  - Azure NetApp Files 의 경우, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.
- GCP에서 Cloud Volumes ONTAP 의 데이터를 스캔할 때 GCP의 콘솔 에이전트를 사용합니다.

이러한 클라우드 콘솔 에이전트를 사용하면 온프레미스 ONTAP 시스템, NetApp 파일 공유 및 데이터베이스를 검사할 수 있습니다.

또한 다음을 수행할 수도 있습니다. "온프레미스에 콘솔 에이전트 설치" 네트워크나 클라우드 내의 Linux 호스트에서. 온프레미스에 데이터 분류를 설치하려는 일부 사용자는 온프레미스에 콘솔 에이전트를 설치하기로 선택할 수도 있습니다.

보시다시피, 사용해야 하는 상황이 있을 수 있습니다. "여러 콘솔 에이전트" .

데이터 분류는 스캔할 수 있는 데이터 양에 제한을 두지 않습니다. 각 콘솔 에이전트는 500TiB의 데이터를 스캔하고 표시하는 것을 지원합니다. 500TiB 이상의 데이터를 스캔하려면"다른 콘솔 에이전트를 설치하세요" 그 다음에"다른 데이터 분류 인스턴스 배포" . + 콘솔 UI는 단일 커넥터의 데이터를 표시합니다. 여러 콘솔 에이전트의 데이터를 보는 방법에 대한 팁은 다음을 참조하세요."여러 콘솔 에이전트와 함께 작업" .

정부 지역 지원

콘솔 에이전트가 정부 지역(AWS GovCloud, Azure Gov 또는 Azure DoD)에 배포된 경우 데이터 분류가 지원됩니다. 이런 방식으로 배포할 경우 데이터 분류에는 다음과 같은 제한이 있습니다.

"정부 지역에 콘솔 에이전트를 배포하는 방법에 대한 자세한 내용을 확인하세요." .

필수 조건

클라우드에 데이터 분류를 배포하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요. 클라우드에 데이터 분류를 배포하면 콘솔 에이전트와 동일한 서브넷에 위치하게 됩니다.

데이터 분류에서 아웃바운드 인터넷 액세스 활성화

데이터 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 접속을 위해 프록시 서버를 사용하는 경우, 데이터 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 접속 권한이 있는지 확인하세요. 프록시는 투명하지 않아야 합니다. 투명 프록시는 현재 지원되지 않습니다.

AWS, Azure 또는 GCP에서 데이터 분류를 배포하는지에 따라 아래 해당 표를 검토하세요.

AWS에 필요한 엔드포인트

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공합니다.
\ https://kinesis.us-east-1.amazonaws.com	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.
\ https://cognito-idp.us-east-1.amazonaws.com \ https://cognito-identity.us-east-1.amazonaws.com \ https://user-feedback-store-prod.s3.us-west-2.amazonaws.com \ https://customer-data-production.s3.us-west-2.amazonaws.com	데이터 분류를 통해 매니페스트와 템플릿에 액세스하고 다운로드하며, 로그와 메트릭을 전송할 수 있습니다.

Azure에 필요한 엔드포인트

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.console.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.

GCP에 필요한 엔드포인트

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.

엔드포인트	목적
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.console.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.

데이터 분류에 필요한 권한이 있는지 확인하세요.

데이터 분류에 리소스를 배포하고 데이터 분류 인스턴스에 대한 보안 그룹을 생성할 수 있는 권한이 있는지 확인하세요.

- "Google Cloud 권한"
- "AWS 권한"
- "Azure 권한"

콘솔 에이전트가 데이터 분류에 액세스할 수 있는지 확인하세요.

콘솔 에이전트와 데이터 분류 인스턴스 간의 연결을 보장합니다. 콘솔 에이전트의 보안 그룹은 포트 443을 통해 데이터 분류 인스턴스와의 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 이 연결을 통해 데이터 분류 인스턴스를 배포하고 규정 준수 및 거버넌스 탭에서 정보를 볼 수 있습니다. 데이터 분류는 AWS와 Azure의 정부 지역에서 지원됩니다.

AWS 및 AWS GovCloud 배포에는 추가적인 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 보다 "AWS의 콘솔 에이전트에 대한 규칙" 자세한 내용은.

Azure 및 Azure Government 배포에는 추가적인 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 보다 "Azure의 콘솔 에이전트에 대한 규칙" 자세한 내용은.

데이터 분류를 계속 실행할 수 있는지 확인하세요.

데이터 분류 인스턴스는 지속적으로 데이터를 스캔하기 위해 켜져 있어야 합니다.

데이터 분류에 대한 웹 브라우저 연결을 보장합니다.

데이터 분류가 활성화된 후, 사용자가 데이터 분류 인스턴스에 연결된 호스트에서 콘솔 인터페이스에 액세스하는지 확인하세요.

데이터 분류 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터가 인터넷에서 접근되지 않도록 보장합니다. 따라서 콘솔에 접속하는 데 사용하는 웹 브라우저는 해당 개인 IP 주소에 연결되어 있어야 합니다. 해당 연결은 클라우드 공급자(예: VPN)에 대한 직접 연결을 통해 이루어질 수도 있고, 데이터 분류 인스턴스와 동일한 네트워크 내부에 있는 호스트를 통해 이루어질 수도 있습니다.

vCPU 제한을 확인하세요

클라우드 제공업체의 vCPU 한도가 필요한 수의 코어를 갖춘 인스턴스를 배포할 수 있는지 확인하세요. 콘솔이 실행되는 지역에서 해당 인스턴스 패밀리에 대한 vCPU 제한을 확인해야 합니다. "필요한 인스턴스 유형을 확인하세요" .

vCPU 제한에 대한 자세한 내용은 다음 링크를 참조하세요.

- "AWS 설명서: Amazon EC2 서비스 할당량"
- "Azure 설명서: 가상 머신 vCPU 할당량"
- "Google Cloud 문서: 리소스 할당량"

클라우드에 데이터 분류 배포

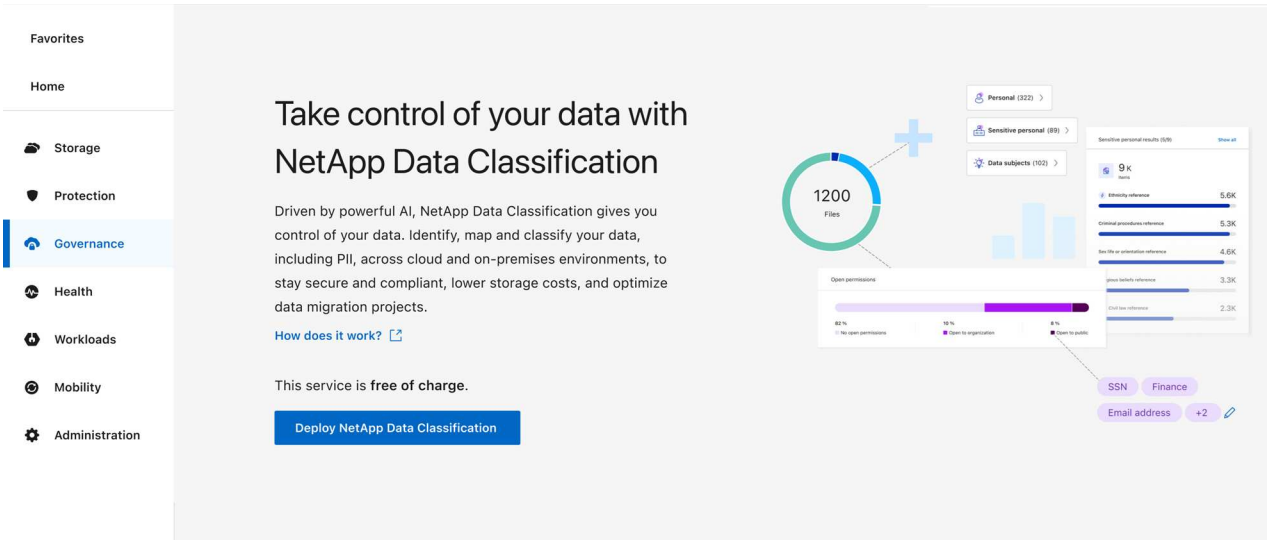
클라우드에 데이터 분류 인스턴스를 배포하려면 다음 단계를 따르세요. 콘솔 에이전트는 클라우드에 인스턴스를 배포한 다음 해당 인스턴스에 데이터 분류 소프트웨어를 설치합니다.

기본 인스턴스 유형을 사용할 수 없는 지역에서는 데이터 분류가 실행됩니다."대체 인스턴스 유형" .

AWS에 배포

단계

1. 데이터 분류의 메인 페이지에서 *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.

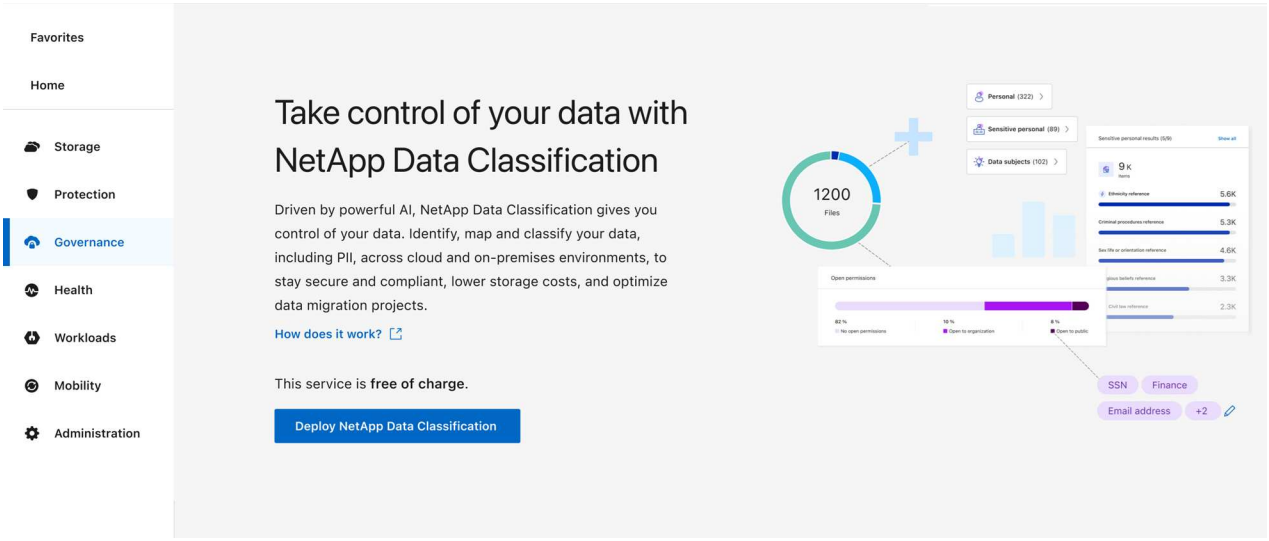


2. 설치 페이지에서 *배포 > 배포*를 선택하여 "대형" 인스턴스 크기를 사용하고 클라우드 배포 마법사를 시작합니다.
3. 마법사는 배포 단계를 진행하면서 진행 상황을 표시합니다. 입력이 필요하거나 문제가 발생하면 메시지가 표시됩니다.
4. 인스턴스가 배포되고 데이터 분류가 설치되면 *구성 계속*을 선택하여 구성 페이지로 이동합니다.

Azure에 배포

단계

1. 데이터 분류의 메인 페이지에서 *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.



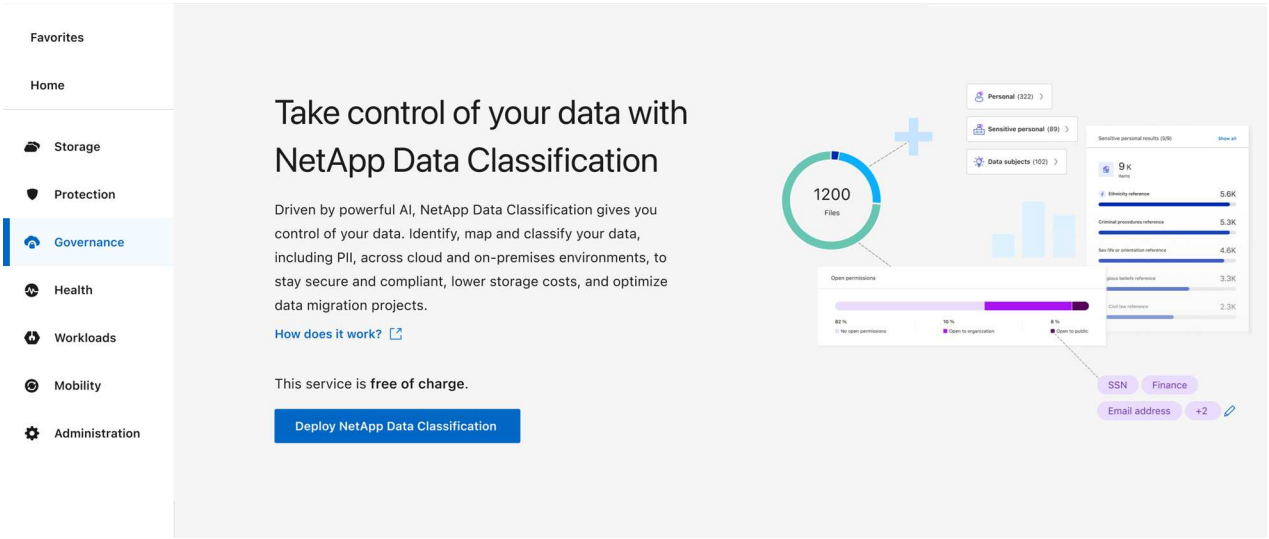
2. 클라우드 배포 마법사를 시작하려면 *배포*를 선택하세요.
3. 마법사는 배포 단계를 진행하면서 진행 상황을 표시합니다. 문제가 발생하면 멈추고 입력을 요청합니다.

4. 인스턴스가 배포되고 데이터 분류가 설치되면 *구성 계속*을 선택하여 구성 페이지로 이동합니다.

Google Cloud에 배포

단계

1. 데이터 분류의 메인 페이지에서 *거버넌스 > 분류*를 선택합니다.
2. *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.



3. 클라우드 배포 마법사를 시작하려면 *배포*를 선택하세요.
4. 마법사는 배포 단계를 진행하면서 진행 상황을 표시합니다. 문제가 발생하면 멈추고 입력을 요청합니다.
5. 인스턴스가 배포되고 데이터 분류가 설치되면 *구성 계속*을 선택하여 구성 페이지로 이동합니다.

결과

콘솔은 클라우드 공급자에 데이터 분류 인스턴스를 배포합니다.

인스턴스가 인터넷에 연결되어 있는 한 콘솔 에이전트와 데이터 분류 소프트웨어의 업그레이드는 자동화됩니다.

다음은 무엇인가

구성 페이지에서 스캔할 데이터 소스를 선택할 수 있습니다.

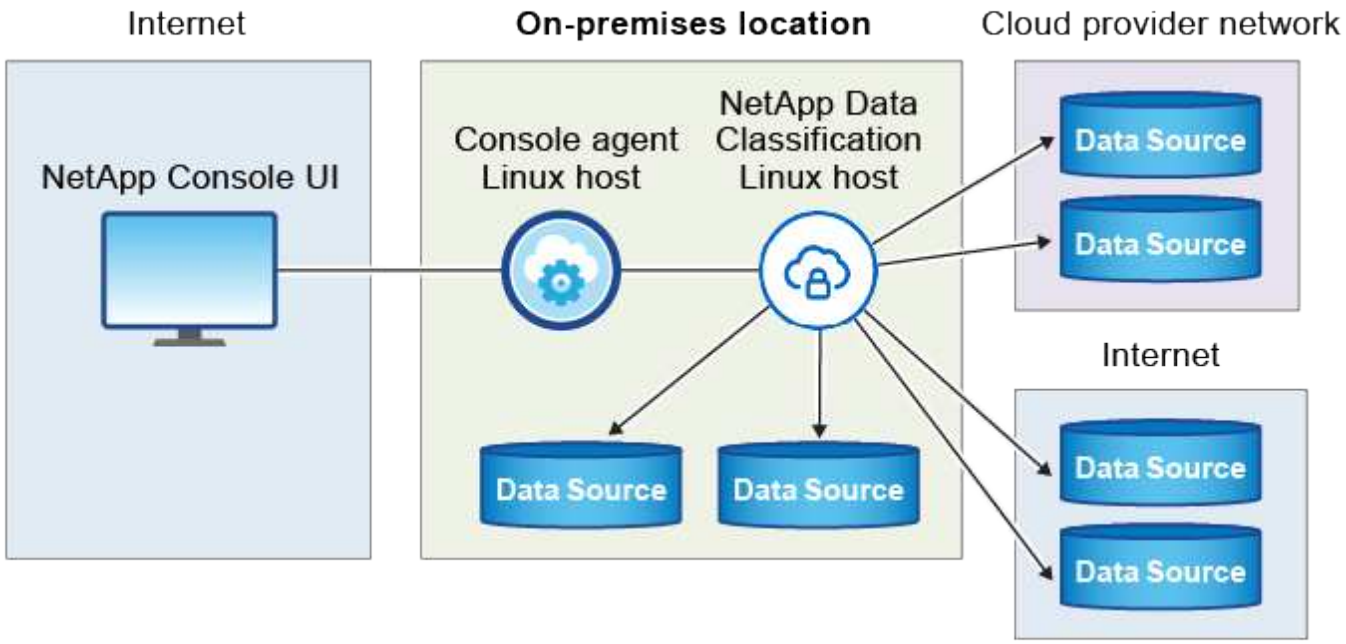
인터넷 접속이 가능한 호스트에 **NetApp Data Classification** 설치

네트워크의 Linux 호스트나 인터넷 접속이 가능한 클라우드의 Linux 호스트에 NetApp Data Classification 배포하려면 네트워크나 클라우드에 Linux 호스트를 수동으로 배포해야 합니다.

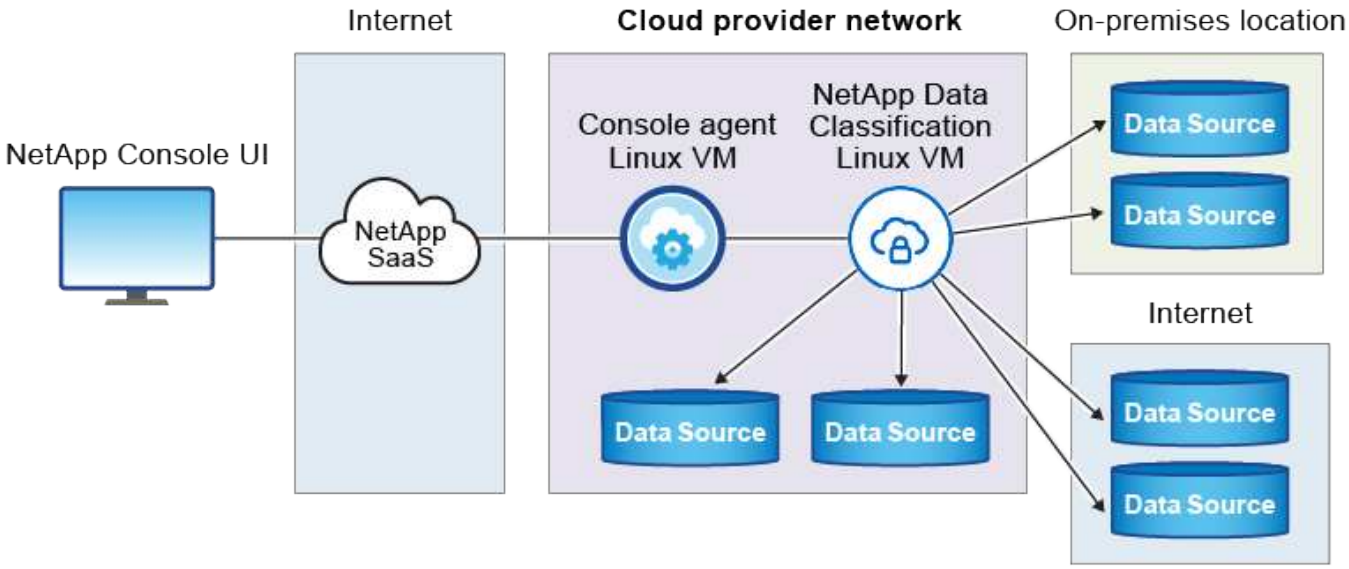
온프레미스 설치는 온프레미스에 있는 데이터 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 스캔하는 것을 선호하는 경우에 좋은 옵션입니다. 이것은 필수사항이 아닙니다. 어떤 설치 방법을 선택하든 소프트웨어의 기능은 동일합니다.

데이터 분류 설치 스크립트는 시스템과 환경이 필수 전제 조건을 충족하는지 확인하는 것으로 시작됩니다. 모든 전제 조건이 충족되면 설치가 시작됩니다. 데이터 분류 설치를 실행하지 않고도 전제 조건을 독립적으로 확인하려면 전제 조건만 테스트하는 별도의 소프트웨어 패키지를 다운로드할 수 있습니다. "Linux 호스트가 데이터 분류를 설치할 준비가 되었는지 확인하는 방법을 알아보세요." .

귀사 구내의 Linux 호스트에 일반적으로 설치되는 구성 요소와 연결은 다음과 같습니다.



클라우드에 있는 Linux 호스트에 일반적으로 설치되는 구성 요소와 연결은 다음과 같습니다.



빠른 시작

다음 단계에 따라 빠르게 시작하거나, 나머지 섹션으로 스크롤하여 자세한 내용을 확인하세요.

1 콘솔 에이전트 만들기

아직 콘솔 에이전트가 없는 경우 "온프레미스에 콘솔 에이전트 배포" 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서.

클라우드 공급자를 사용하여 콘솔 에이전트를 생성할 수도 있습니다. 보다 "AWS에서 콘솔 에이전트 만들기" , "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" .

2 필수 조건 검토

귀하의 환경이 전제 조건을 충족하는지 확인하세요. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 콘솔 에이전트와 데이터 분류 간의 연결 등이 포함됩니다. 전체 목록을 확인하세요 .

또한 다음을 충족하는 Linux 시스템이 필요합니다.다음 요구 사항 .

3 데이터 분류 다운로드 및 배포

NetApp 지원 사이트에서 클라우드 데이터 분류 소프트웨어를 다운로드하고 사용하려는 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 실행하고 메시지에 따라 데이터 분류 인스턴스를 배포합니다.

콘솔 에이전트 만들기

데이터 분류를 설치하고 사용하려면 콘솔 에이전트가 필요합니다. 대부분의 경우 데이터 분류를 활성화하기 전에 콘솔 에이전트를 설정했을 가능성이 높습니다. "콘솔 기능에는 콘솔 에이전트가 필요합니다." 하지만 지금 당장 설정해야 하는 경우도 있습니다.

클라우드 공급자 환경에서 하나를 생성하려면 다음을 참조하세요. "AWS에서 콘솔 에이전트 만들기" , "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" .

특정 클라우드 공급자에 배포된 콘솔 에이전트를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP 또는 Amazon FSx for ONTAP 에서 데이터를 스캔할 때 AWS의 콘솔 에이전트를 사용합니다.
- Azure의 Cloud Volumes ONTAP 또는 Azure NetApp Files 에서 데이터를 스캔할 때 Azure의 콘솔 에이전트를 사용합니다.

  Azure NetApp Files 의 경우, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.

- GCP에서 Cloud Volumes ONTAP 의 데이터를 스캔할 때 GCP의 콘솔 에이전트를 사용합니다.

온프레미스 ONTAP 시스템, NetApp 파일 공유 및 데이터베이스 계정은 이러한 클라우드 콘솔 에이전트를 사용하여 스캔할 수 있습니다.

또한 다음을 수행할 수도 있습니다. "온프레미스에 콘솔 에이전트 배포" 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서. 온프레미스에 데이터 분류를 설치하려는 일부 사용자는 콘솔 에이전트도 온프레미스에 설치하기로 선택할 수도 있습니다.

데이터 분류를 설치할 때 콘솔 에이전트 시스템의 IP 주소나 호스트 이름이 필요합니다. 사내에 콘솔 에이전트를 설치한 경우 이 정보를 얻을 수 있습니다. 콘솔 에이전트가 클라우드에 배포된 경우 콘솔에서 다음 정보를 찾을 수 있습니다. 도움말 아이콘을 선택한 다음 *지원*을 선택하고 콘솔 에이전트를 선택합니다.

Linux 호스트 시스템 준비

데이터 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다. Linux 호스트는 네트워크에 있을 수도 있고 클라우드에 있을 수도 있습니다.

데이터 분류를 계속 실행할 수 있는지 확인하세요. 데이터 분류 머신은 지속적으로 데이터를 스캔하기 위해 계속 켜져 있어야 합니다.

- 다른 애플리케이션과 공유되는 호스트에서는 데이터 분류가 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.
- 사내 호스트 시스템을 구축할 때 데이터 분류를 통해 스캔하려는 데이터 세트의 크기에 따라 다음 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리를 비활성화해야 함**)**	디스크
특대	32개의 CPU	128GB 램	• /에 1TiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker에서 895GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**
크기가 큰	16개의 CPU	64GB 램	• /에 500GiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker 또는 Podman /var/lib/containers에서 400GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**

- 데이터 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 사용하는 것이 좋습니다.
  - **Amazon Elastic Compute Cloud(Amazon EC2)** 인스턴스 유형: "m6i.4xlarge". "추가 AWS 인스턴스 유형 보기" .
  - **Azure VM** 크기: "Standard_D16s_v3". "추가 Azure 인스턴스 유형 보기" .
  - **GCP** 머신 유형: "n2-standard-16". "추가 GCP 인스턴스 유형을 참조하세요." .
- **UNIX** 폴더 권한: 다음과 같은 최소 UNIX 권한이 필요합니다.

접는 사람	최소 권한
/임시	`rwxrwxrwt`
/고르다	`rwxr-xr-x`
/var/lib/도커	`rwx------`
/usr/lib/systemd/시스템	`rwxr-xr-x`

- 운영체제:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9

        - Ubuntu 22.04(데이터 분류 버전 1.23 이상 필요)
        - Ubuntu 24.04(데이터 분류 버전 1.23 이상 필요)
    - 다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, Data Classification 버전 1.30 이상이 필요합니다.
        - Red Hat Enterprise Linux 버전 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 및 9.6.
    - 호스트 시스템에서 고급 벡터 확장(AVX2)을 활성화해야 합니다.
- **Red Hat Subscription Management**: 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우, 설치 중에 시스템은 저장소에 접근하여 필요한 타사 소프트웨어를 업데이트할 수 없습니다.
- 추가 소프트웨어: 데이터 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
    - 사용하는 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
        - Docker Engine 버전 19.3.1 이상. "설치 지침 보기" .
        - Podman 버전 4 이상. Podman을 설치하려면 다음을 입력하세요.(`sudo yum install podman netavark -y`).
- Python 버전 3.6 이상. "설치 지침 보기" .
    - **NTP** 고려 사항: NetApp 데이터 분류 시스템을 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 데이터 분류 시스템과 콘솔 에이전트 시스템 간의 시간은 동기화되어야 합니다.
- 방화벽 고려 사항: 방화벽을 사용하려는 경우 `firewalld` 데이터 분류를 설치하기 전에 해당 기능을 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성하세요. `firewalld` 데이터 분류와 호환되도록:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

추가 데이터 분류 호스트를 스캐너 노드로 사용할 계획이라면 지금 바로 기본 시스템에 다음 규칙을 추가하세요.

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Docker 또는 Podman을 활성화하거나 업데이트할 때마다 다시 시작해야 합니다. `firewalld` 설정.

데이터 분류 호스트 시스템의 IP 주소는 설치 후 변경할 수 없습니다.

데이터 분류에서 아웃바운드 인터넷 액세스 활성화

데이터 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 접속을 위해 프록시

서버를 사용하는 경우, 데이터 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 접속 권한이 있는지 확인하세요.

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함한 콘솔과의 통신.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://support.compliance.api.bluexp.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.console.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.
\ https://github.com/docker \ https://download.docker.com	Docker 설치를 위한 필수 패키지를 제공합니다.
\ http://packages.ubuntu.com/ \ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

모든 필수 포트가 활성화되어 있는지 확인하세요

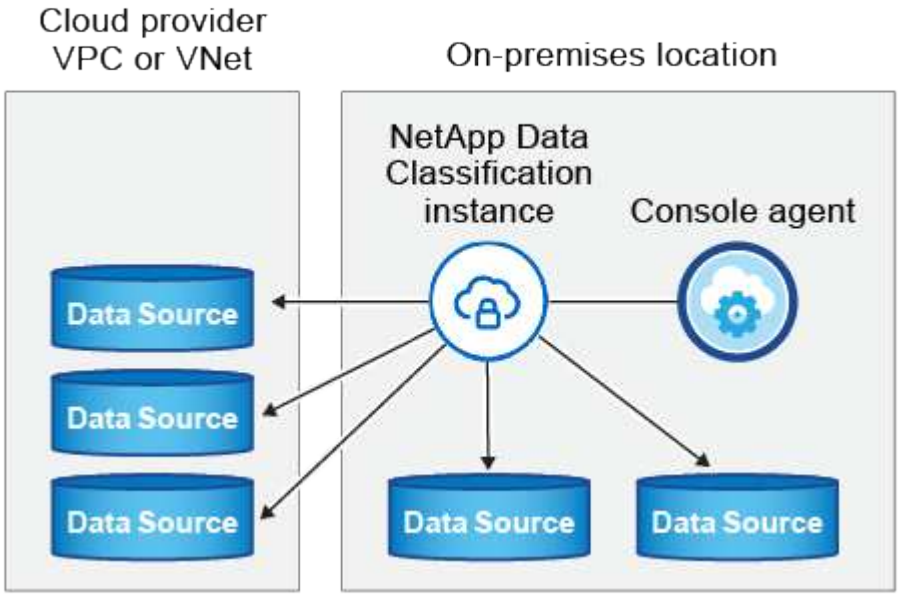
콘솔 에이전트, 데이터 분류, Active Directory 및 데이터 소스 간 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

연결 유형	포트	설명
콘솔 에이전트 <> 데이터 분류	8080(TCP), 443(TCP), 80. 9000	콘솔 에이전트의 방화벽 또는 라우팅 규칙은 포트 443을 통해 데이터 분류 인스턴스로의 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 콘솔에서 설치 진행 상황을 볼 수 있도록 포트 8080이 열려 있는지 확인하세요. Linux 호스트에서 방화벽을 사용하는 경우 Ubuntu 서버 내의 내부 프로세스에는 포트 9000이 필요합니다.

연결 유형	포트	설명
콘솔 에이전트 <> ONTAP 클러스터(NAS)	443(TCP)	콘솔은 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 다음 요구 사항을 충족해야 합니다. • 콘솔 에이전트 호스트는 포트 443을 통해 아웃바운드 HTTPS 액세스를 허용해야 합니다. 콘솔 에이전트가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽이나 라우팅 규칙에 따라 허용됩니다. • ONTAP 클러스터는 포트 443을 통해 인바운드 HTTPS 액세스를 허용해야 합니다. 기본 "mgmt" 방화벽 정책은 모든 IP 주소에서 인바운드 HTTPS 액세스를 허용합니다. 이 기본 정책을 수정했거나 사용자 고유의 방화벽 정책을 만든 경우 HTTPS 프로토콜을 해당 정책과 연결하고 콘솔 에이전트 호스트에서 액세스를 활성화해야 합니다.
데이터 분류 <> ONTAP 클러스터	• NFS의 경우 - 111(TCP\UDP) 및 2049(TCP\UDP) • CIFS의 경우 - 139(TCP\UDP) 및 445(TCP\UDP)	데이터 분류에는 각 Cloud Volumes ONTAP 서브넷이나 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다. Cloud Volumes ONTAP 의 방화벽이나 라우팅 규칙은 데이터 분류 인스턴스에서 인바운드 연결을 허용해야 합니다. 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요. • NFS - 111 및 2049의 경우 • CIFS - 139 및 445의 경우 NFS 볼륨 내보내기 정책은 데이터 분류 인스턴스에서의 액세스를 허용해야 합니다.
데이터 분류 <> Active Directory	389(TCP 및 UDP), 636(TCP), 3268(TCP), 3269(TCP)	회사 사용자를 위해 Active Directory가 이미 설정되어 있어야 합니다. 또한, 데이터 분류에는 CIFS 볼륨을 스캔하기 위한 Active Directory 자격 증명이 필요합니다. Active Directory에 대한 정보가 있어야 합니다. • DNS 서버 IP 주소 또는 여러 IP 주소 • 서버의 사용자 이름 및 비밀번호 • 도메인 이름(Active Directory 이름) • 보안 LDAP(LDAPS)를 사용하든 사용하지 않든 • LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)

Linux 호스트에 데이터 분류 설치

일반적인 구성의 경우 단일 호스트 시스템에 소프트웨어를 설치합니다. 여기에서 해당 단계를 확인하세요 .



보다Linux 호스트 시스템 준비 그리고필수 조건 검토 데이터 분류를 배포하기 전에 필요한 전체 요구 사항 목록을 확인하세요.

인스턴스에 인터넷 연결이 있는 한 데이터 분류 소프트웨어 업그레이드는 자동으로 수행됩니다.

현재 데이터 분류 기능은 온프레미스에 소프트웨어가 설치된 경우 S3 버킷, Azure NetApp Files 또는 FSx for ONTAP 검색할 수 없습니다. 이러한 경우 클라우드에 별도의 콘솔 에이전트와 데이터 분류 인스턴스를 배포해야 합니다. "커넥터 간 전환" 다양한 데이터 소스에 대해.

일반적인 구성을 위한 단일 호스트 설치

단일 온프레미스 호스트에 데이터 분류 소프트웨어를 설치할 때 요구 사항을 검토하고 다음 단계를 따르세요.

"이 영상을 시청하세요"데이터 분류를 설치하는 방법을 알아보세요.

데이터 분류를 설치할 때 모든 설치 활동이 기록됩니다. 설치 중에 문제가 발생하면 설치 감사 로그의 내용을 볼 수 있습니다. 에 쓰여있다 `/opt/netapp/install_logs/` .

시작하기 전에

- Linux 시스템이 다음 사항을 충족하는지 확인하십시오.호스트 요구 사항 .
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman, Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에서 루트 권한이 있는지 확인하세요.
- 인터넷에 접속하기 위해 프록시를 사용하는 경우:
  - 프록시 서버 정보(IP 주소 또는 호스트 이름, 연결 포트, 연결 방식: https 또는 http, 사용자 이름 및 비밀번호)가 필요합니다.
  - 프록시가 TLS 가로채기를 수행하는 경우 TLS CA 인증서가 저장된 Data Classification Linux 시스템의

경로를 알아야 합니다.

- 프록시는 투명하지 않아야 합니다. 데이터 분류는 현재 투명 프록시를 지원하지 않습니다.
- 사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.

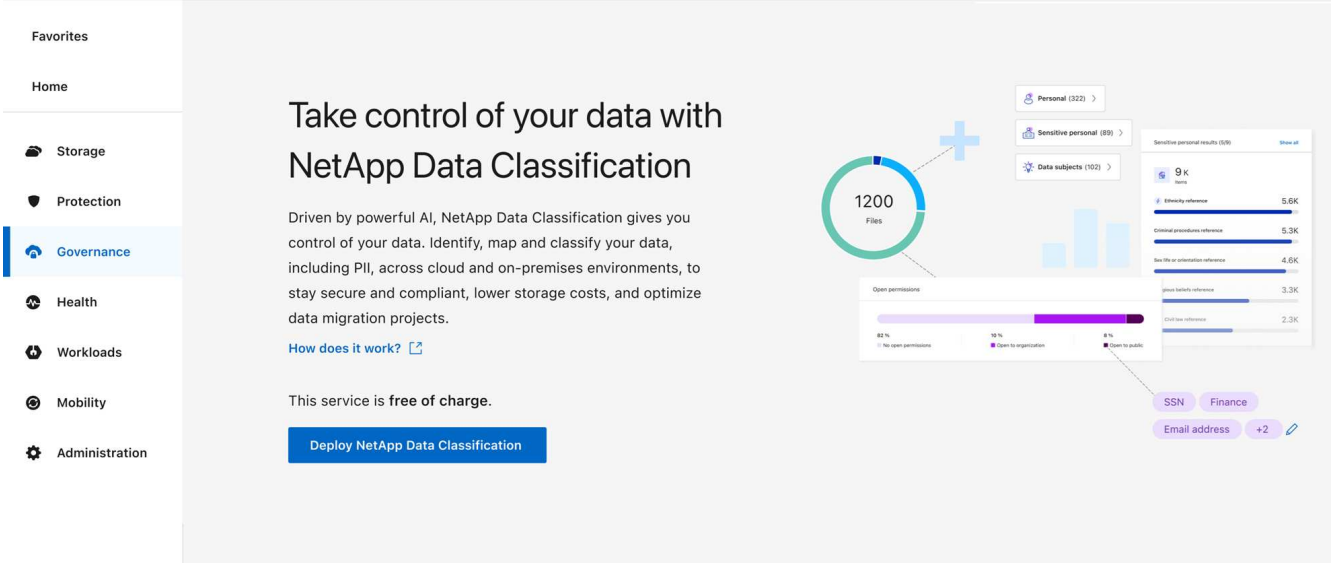
- 오프라인 환경이 요구 사항을 충족하는지 확인하세요.권한 및 연결 .

단계

1. 데이터 분류 소프트웨어를 다운로드하세요. "NetApp 지원 사이트" . 선택해야 하는 파일의 이름은 *DATASENSE-INSTALLER-<버전>.tar.gz*입니다.
2. 사용하려는 Linux 호스트에 설치 프로그램 파일을 복사합니다(사용 `scp` 또는 다른 방법).
3. 호스트 컴퓨터에서 설치 프로그램 파일의 압축을 풉니다. 예:

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. 콘솔에서 *거버넌스 > 분류*를 선택합니다.
5. *온프레미스 또는 클라우드에 분류 배포*를 선택합니다.



6. 클라우드에서 준비한 인스턴스에 데이터 분류를 설치하는지, 아니면 사내에서 준비한 인스턴스에 데이터 분류를 설치하는지에 따라 적절한 배포 옵션을 선택하여 데이터 분류 설치를 시작합니다.
7. 온프레미스에 데이터 분류 배포 대화 상자가 표시됩니다. 제공된 명령을 복사합니다(예: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`)을 텍스트 파일에 붙여넣어 나중에 사용할 수 있습니다. 그런 다음 *닫기*를 선택하여 대화 상자를 닫습니다.
8. 호스트 머신에서 복사한 명령을 입력한 다음 일련의 프롬프트를 따르거나 모든 필수 매개변수를 포함한 전체 명령을 명령줄 인수로 제공할 수 있습니다.

   설치 프로그램은 성공적인 설치를 위해 시스템 및 네트워킹 요구 사항이 충족되는지 사전 점검을 수행합니다. "이 영상을 시청하세요" 사전 확인 메시지와 그 의미를 이해합니다.

프롬프트에 따라 매개변수를 입력하세요.	전체 명령을 입력하세요:
a. 7단계에서 복사한 명령을 붙여넣습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` 클라우드 인스턴스(사내가 아닌)에 설치하는 경우 다음을 추가하세요. `--manual-cloud-install <cloud_provider>` . b. 콘솔 에이전트 시스템에서 액세스할 수 있도록 데이터 분류 호스트 머신의 IP 주소 또는 호스트 이름을 입력하세요. c. 데이터 분류 시스템에서 액세스할 수 있도록 콘솔 에이전트 호스트 머신의 IP 주소 또는 호스트 이름을 입력하세요. d. 지시에 따라 프록시 세부 정보를 입력하세요. 콘솔 에이전트가 이미 프록시를 사용하는 경우 데이터 분류가 자동으로 콘솔 에이전트에서 사용하는 프록시를 사용하므로 여기에 다시 정보를 입력할 필요가 없습니다.	또는 필요한 호스트 및 프록시 매개변수를 제공하여 전체 명령을 미리 만들 수 있습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

변수 값:

- *account_id* = NetApp 계정 ID
- *client_id* = 콘솔 에이전트 클라이언트 ID(클라이언트 ID에 접미사 "clients"가 없으면 추가)
- *user_token* = JWT 사용자 액세스 토큰
- *ds_host* = 데이터 분류 Linux 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm_host* = 콘솔 에이전트 시스템의 IP 주소 또는 호스트 이름입니다.
- *cloud_provider* = 클라우드 인스턴스에 설치하는 경우 클라우드 공급자에 따라 "AWS", "Azure" 또는 "Gcp"를 입력하세요.
- *proxy_host* = 호스트가 프록시 서버 뒤에 있는 경우 프록시 서버의 IP 또는 호스트 이름입니다.
- *proxy_port* = 프록시 서버에 연결할 포트(기본값 80).
- *proxy_scheme* = 연결 방식: https 또는 http(기본값은 http).
- *proxy_user* = 기본 인증이 필요한 경우 프록시 서버에 연결하는 인증된 사용자입니다. 사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.
- *proxy_password* = 지정한 사용자 이름에 대한 비밀번호입니다.
- *ca_cert_dir* = 추가 TLS CA 인증서 번들이 포함된 Data Classification Linux 시스템의 경로입니다. 프록시가 TLS 가로채기를 수행하는 경우에만 필요합니다.

결과

데이터 분류 설치 프로그램은 패키지를 설치하고, 설치를 등록하고, 데이터 분류를 설치합니다. 설치하는 데 10~20분이 걸릴 수 있습니다.

호스트 머신과 콘솔 에이전트 인스턴스 사이에 포트 8080을 통해 연결이 있는 경우 콘솔의 데이터 분류 탭에서 설치

진행률을 볼 수 있습니다.

다음은 무엇인가

구성 페이지에서 스캔할 데이터 소스를 선택할 수 있습니다.

인터넷 접속이 없는 **Linux** 호스트에 **NetApp Data Classification** 설치

인터넷 접속이 불가능한 온프레미스 사이트의 Linux 호스트에 NetApp Data Classification 설치하는 것을 _개인 모드_라고 합니다. 설치 스크립트를 사용하는 이 유형의 설치는 NetApp Console SaaS 계층에 연결되지 않습니다.

BlueXP 개인 모드(레거시 BlueXP 인터페이스)는 일반적으로 인터넷 연결이 없고 AWS Secret Cloud, AWS Top Secret Cloud, Azure IL6를 포함하는 보안 클라우드 지역이 있는 온프레미스 환경에서 사용됩니다. NetApp 기존 BlueXP 인터페이스를 통해 이러한 환경을 계속 지원합니다. 레거시 BlueXP 인터페이스의 개인 모드 설명서는 다음을 참조하세요."BlueXP 개인 모드에 대한 PDF 문서" .

Linux 호스트가 **NetApp Data Classification** 설치할 준비가 되었는지 확인하세요**.**

Linux 호스트에 NetApp Data Classification 수동으로 설치하기 전에 호스트에서 스크립트를 실행하여 Data Classification을 설치하는 데 필요한 모든 전제 조건이 충족되었는지 확인합니다. 이 스크립트는 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서 실행할 수 있습니다. 호스트는 인터넷에 연결되어 있을 수도 있고, 인터넷에 접속할 수 없는 사이트(다크 사이트)에 있을 수도 있습니다.

데이터 분류 설치 스크립트의 일부인 필수 테스트 스크립트도 있습니다. 여기에 설명된 스크립트는 데이터 분류 설치 스크립트를 실행하지 않고도 Linux 호스트를 독립적으로 검증하려는 사용자를 위해 특별히 설계되었습니다.

시작하기

다음 작업을 수행하게 됩니다.

1. 선택적으로, 콘솔 에이전트가 설치되어 있지 않으면 설치하세요. 콘솔 에이전트를 설치하지 않고도 테스트 스크립트를 실행할 수 있지만, 스크립트는 콘솔 에이전트와 데이터 분류 호스트 머신 간의 연결을 확인합니다. 따라서 콘솔 에이전트를 설치하는 것이 좋습니다.
2. 호스트 머신을 준비하고 모든 요구 사항을 충족하는지 확인하세요.
3. 데이터 분류 호스트 머신에서 아웃바운드 인터넷 액세스를 활성화합니다.
4. 모든 시스템에서 필요한 포트가 모두 활성화되어 있는지 확인하세요.
5. 필수 테스트 스크립트를 다운로드하여 실행하세요.

콘솔 에이전트 만들기

데이터 분류를 설치하고 사용하려면 콘솔 에이전트가 필요합니다. 하지만 콘솔 에이전트 없이도 필수 구성 요소 스크립트를 실행할 수 있습니다.

당신은 할 수 있습니다 "온프레미스에 콘솔 에이전트 설치" 네트워크의 Linux 호스트나 클라우드의 Linux 호스트에서. 온프레미스에 데이터 분류를 설치하려는 일부 사용자는 온프레미스에 콘솔 에이전트를 설치하기로 선택할 수도 있습니다.

클라우드 공급자 환경에서 콘솔 에이전트를 생성하려면 다음을 참조하세요. "AWS에서 콘솔 에이전트 만들기" , "Azure에서 콘솔 에이전트 만들기" , 또는 "GCP에서 콘솔 에이전트 만들기" .

필수 구성 요소 스크립트를 실행할 때는 콘솔 에이전트 시스템의 IP 주소나 호스트 이름이 필요합니다. 사내에 콘솔 에이전트를 설치한 경우 이 정보를 얻을 수 있습니다. 콘솔 에이전트가 클라우드에 배포된 경우 콘솔에서 다음 정보를 찾을 수 있습니다. 도움말 아이콘을 선택한 다음 *지원*을 선택하고 *콘솔 에이전트*를 선택합니다.

호스트 요구 사항 확인

데이터 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다.

- 다른 애플리케이션과 공유되는 호스트에서는 데이터 분류가 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.
- 사내 호스트 시스템을 구축할 때 데이터 분류를 통해 스캔하려는 데이터 세트의 크기에 따라 다음 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리를 비활성화해야 함**)**	디스크
특대	32개의 CPU	128GB 램	• /에 1TiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker에서 895GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**
크기가 큰	16개의 CPU	64GB 램	• /에 500GiB SSD, 또는 /opt에 100GiB 사용 가능 • /var/lib/docker 또는 Podman /var/lib/containers에서 400GiB 사용 가능 • /tmp에 5GiB • **Podman**의 경우 **/var/tmp**에 **30GB**

- 데이터 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 사용하는 것이 좋습니다.
  - **Amazon Elastic Compute Cloud(Amazon EC2)** 인스턴스 유형: "m6i.4xlarge". "추가 AWS 인스턴스 유형 보기" .
  - **Azure VM** 크기: "Standard_D16s_v3". "추가 Azure 인스턴스 유형 보기" .
  - **GCP** 머신 유형: "n2-standard-16". "추가 GCP 인스턴스 유형을 참조하세요." .
- **UNIX** 폴더 권한: 다음과 같은 최소 UNIX 권한이 필요합니다.

접는 사람	최소 권한
/임시	`rwxrwxrwt`
/고르다	`rwxr-xr-x`
/var/lib/도커	`rwx------`
/usr/lib/systemd/시스템	`rwxr-xr-x`

- 운영체제:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9
    - Ubuntu 22.04(데이터 분류 버전 1.23 이상 필요)
    - Ubuntu 24.04(데이터 분류 버전 1.23 이상 필요)
  - 다음 운영 체제에서는 Podman 컨테이너 엔진을 사용해야 하며, Data Classification 버전 1.30 이상이 필요합니다.
    - Red Hat Enterprise Linux 버전 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 및 9.6.
  - 호스트 시스템에서 고급 벡터 확장(AVX2)을 활성화해야 합니다.
- **Red Hat Subscription Management**: 호스트는 Red Hat Subscription Management에 등록되어야 합니다. 등록되지 않은 경우, 설치 중에 시스템은 저장소에 접근하여 필요한 타사 소프트웨어를 업데이트할 수 없습니다.
- 추가 소프트웨어: 데이터 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
  - 사용하는 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
    - Docker Engine 버전 19.3.1 이상. "설치 지침 보기" .
    - Podman 버전 4 이상. Podman을 설치하려면 다음을 입력하세요.(`sudo yum install podman netavark -y`).
- Python 버전 3.6 이상. "설치 지침 보기" .
  - **NTP** 고려 사항: NetApp 데이터 분류 시스템을 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 데이터 분류 시스템과 콘솔 에이전트 시스템 간의 시간은 동기화되어야 합니다.
- 방화벽 고려 사항: 방화벽을 사용하려는 경우 `firewalld` 데이터 분류를 설치하기 전에 해당 기능을 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성하세요. `firewalld` 데이터 분류와 호환되도록:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

추가 데이터 분류 호스트를 스캐너 노드로 사용하려는 경우(분산 모델에서), 이때 다음 규칙을 기본 시스템에 추가하세요.

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Docker 또는 Podman을 활성화하거나 업데이트할 때마다 다시 시작해야 합니다. `firewalld` 설정.

데이터 분류에서 아웃바운드 인터넷 액세스 활성화

데이터 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 접속을 위해 프록시 서버를 사용하는 경우, 데이터 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 접속 권한이 있는지 확인하세요.

인터넷 연결이 없는 사이트에 설치된 호스트 시스템에는 이 섹션이 필요하지 않습니다.

엔드포인트	목적
\ https://api.console.netapp.com	NetApp 계정을 포함하는 콘솔 서비스와의 통신입니다.
\ https://netapp-cloud-account.auth0.com \ https://auth0.com	중앙화된 사용자 인증을 위해 콘솔 웹사이트와 통신합니다.
\ https://support.compliance.api.console.netapp.com/ \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트, 템플릿에 대한 액세스를 제공하고 로그와 메트릭을 전송합니다.
\ https://support.compliance.api.console.netapp.com/	NetApp 감사 기록에서 데이터를 스트리밍할 수 있도록 합니다.
\ https://github.com/docker \ https://download.docker.com	Docker 설치를 위한 필수 패키지를 제공합니다.
\ http://packages.ubuntu.com/ \ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

모든 필수 포트가 활성화되어 있는지 확인하세요

콘솔 에이전트, 데이터 분류, Active Directory 및 데이터 소스 간 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

연결 유형	포트	설명
콘솔 에이전트 <> 데이터 분류	8080(TCP), 443(TCP), 80. 9000	콘솔 에이전트의 방화벽 또는 라우팅 규칙은 포트 443을 통해 데이터 분류 인스턴스로의 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 콘솔에서 설치 진행 상황을 볼 수 있도록 포트 8080이 열려 있는지 확인하세요. Linux 호스트에서 방화벽을 사용하는 경우 Ubuntu 서버 내의 내부 프로세스에는 포트 9000이 필요합니다.
콘솔 에이전트 <> ONTAP 클러스터(NAS)	443(TCP)	콘솔은 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 콘솔 에이전트 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. 콘솔 에이전트가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽이나 라우팅 규칙에 따라 허용됩니다.

데이터 분류 필수 조건 스크립트 실행

데이터 분류 필수 조건 스크립트를 실행하려면 다음 단계를 따르세요.

"이 영상을 시청하세요"필수 구성 요소 스크립트를 실행하고 결과를 해석하는 방법을 알아보세요.

시작하기 전에

- Linux 시스템이 다음 사항을 충족하는지 확인하십시오.호스트 요구 사항 .
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman, Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에서 루트 권한이 있는지 확인하세요.

단계

1. 데이터 분류 전제 조건 스크립트를 다운로드하세요. "NetApp 지원 사이트" . 선택해야 하는 파일의 이름은 *standalone-pre-requisite-tester-<version>*입니다.
2. 사용하려는 Linux 호스트에 파일을 복사합니다(사용 `scp` 또는 다른 방법).
3. 스크립트를 실행할 수 있는 권한을 할당합니다.

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. 다음 명령을 사용하여 스크립트를 실행하세요.

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

   인터넷 접속이 불가능한 호스트에서 스크립트를 실행하는 경우에만 "--darksite" 옵션을 추가하세요. 호스트가 인터넷에 연결되어 있지 않으면 특정 필수 테스트가 건너뜁니다.

5. 스크립트는 데이터 분류 호스트 머신의 IP 주소를 입력하라는 메시지를 표시합니다.
   - IP 주소나 호스트 이름을 입력하세요.

6. 스크립트는 콘솔 에이전트가 설치되어 있는지 여부를 묻습니다.
   - 콘솔 에이전트가 설치되어 있지 않으면 *N*을 입력하세요.
   - 콘솔 에이전트가 설치되어 있는 경우 *Y*를 입력하세요. 그런 다음 테스트 스크립트가 이 연결성을 테스트할 수 있도록 콘솔 에이전트의 IP 주소나 호스트 이름을 입력합니다.
7. 스크립트는 시스템에서 다양한 테스트를 실행하고 진행 상황에 따라 결과를 표시합니다. 완료되면 세션 로그를 다음 이름의 파일에 기록합니다. `prerequisites-test-<timestamp>.log` 디렉토리에서 `/opt/netapp/install_logs` .

결과

모든 필수 테스트가 성공적으로 실행되었다면 준비가 되면 호스트에 데이터 분류를 설치할 수 있습니다.

문제가 발견되면 "권장" 또는 "필수"로 분류하여 수정합니다. 권장되는 문제는 일반적으로 데이터 분류 스캐닝 및 분류 작업의 실행 속도를 느리게 만드는 항목입니다. 이러한 항목은 수정할 필요가 없지만 해결하는 것이 좋습니다.

"필수" 문제가 있는 경우 문제를 해결하고 필수 구성 요소 테스트 스크립트를 다시 실행해야 합니다.

데이터 소스에서 스캐닝을 활성화하세요

NetApp Data Classification 사용하여 데이터 소스 스캔

NetApp Data Classification 사용자가 선택한 저장소(볼륨, 데이터베이스 스키마 또는 기타 사용자 데이터)의 데이터를 스캔하여 개인 데이터와 민감한 데이터를 식별합니다. 그런 다음 데이터 분류는 조직 데이터를 매핑하고, 각 파일을 분류하고, 데이터에서 미리 정의된 패턴을 식별합니다. 검사 결과는 개인 정보, 민감한 개인 정보, 데이터 범주 및 파일 유형의 인덱스입니다.

초기 스캔 이후, 데이터 분류는 라운드 로빈 방식으로 데이터를 지속적으로 스캔하여 증분적 변경 사항을 감지합니다. 인스턴스를 계속 실행하는 것이 중요한 이유가 여기에 있습니다.

볼륨 수준이나 데이터베이스 스키마 수준에서 검사를 활성화하거나 비활성화할 수 있습니다.

매핑 스캔과 분류 스캔의 차이점은 무엇입니까?

데이터 분류에서는 두 가지 유형의 스캔을 수행할 수 있습니다.

- 매핑 전용 스캔은 데이터에 대한 개략적인 개요만 제공하며 선택된 데이터 소스에서 수행됩니다. 매핑 전용 스캔은 파일에 액세스하여 내부 데이터를 확인하지 않기 때문에 매핑 및 분류 스캔보다 시간이 덜 걸립니다. 연구할 분야를 파악하기 위해 먼저 이 작업을 수행한 다음 해당 분야에 대한 지도 및 분류 검사를 수행하는 것이 좋습니다.
- **Map & Classify** 스캔은 데이터에 대한 심층적인 스캔을 제공합니다.

아래 표는 몇 가지 차이점을 보여줍니다.

특징	스캔 매핑 및 분류	매핑 전용 스캔
스캔 속도	느린	빠른
가격	무료	무료
용량	500TiB*로 제한됨	500TiB*로 제한됨

특징	스캔 매핑 및 분류	매핑 전용 스캔
파일 유형 및 사용 용량 목록	예	예
파일 개수 및 사용 용량	예	예
파일의 나이와 크기	예	예
실행할 수 있는 능력"데이터 매핑 보고서"	예	예
파일 세부 정보를 보려면 데이터 조사 페이지로 이동하세요.	예	아니요
파일 내에서 이름 검색	예	아니요
만들다"저장된 쿼리" 사용자 정의 검색 결과를 제공하는	예	아니요
다른 보고서를 실행하는 기능	예	아니요
파일의 메타데이터를 볼 수 있는 기능**	아니요	예

{별표} 데이터 분류는 스캔할 수 있는 데이터 양에 제한을 두지 않습니다. 각 콘솔 에이전트는 500TiB의 데이터를 스캔하고 표시하는 것을 지원합니다. 500TiB 이상의 데이터를 스캔하려면"다른 콘솔 에이전트를 설치하세요" 그 다음에"다른 데이터 분류 인스턴스 배포" . + 콘솔 UI는 단일 커넥터의 데이터를 표시합니다. 여러 콘솔 에이전트의 데이터를 보는 방법에 대한 팁은 다음을 참조하세요."여러 콘솔 에이전트와 함께 작업" .

{별표}{별표} 매핑 스캔 중에 파일에서 다음 메타데이터가 추출됩니다.

- 체계
- 시스템 유형
- 저장 저장소
- 파일 유형
- 사용된 용량
- 파일 수
- 파일 크기
- 파일 생성
- 파일 마지막 접근
- 파일이 마지막으로 수정되었습니다
- 파일 발견 시간
- 권한 추출

거버넌스 대시보드 차이점:

특징	지도 및 분류	지도
오래된 데이터	예	예
비업무용 데이터	예	예
중복된 파일	예	예
미리 정의된 저장된 쿼리	예	아니요
기본 저장된 쿼리	예	예
DDA 보고서	예	예
매핑 보고서	예	예
감도 수준 감지	예	아니요
광범위한 권한이 있는 민감한 데이터	예	아니요
공개 권한	예	예
데이터의 시대	예	예
데이터 크기	예	예
카테고리	예	아니요
파일 유형	예	예

규정 준수 대시보드 차이점:

특징	지도 및 분류	지도
개인정보	예	아니요
민감한 개인 정보	예	아니요
개인정보 위험 평가 보고서	예	아니요
HIPAA 보고서	예	아니요
PCI DSS 보고서	예	아니요

조사 필터의 차이점은 다음과 같습니다.

특징	지도 및 분류	지도
저장된 쿼리	예	예
시스템 유형	예	예
체계	예	예
저장 저장소	예	예
파일 유형	예	예
파일 크기	예	예
생성 시간	예	예
발견된 시간	예	예
마지막 수정	예	예
마지막 접근	예	예
공개 권한	예	예
파일 디렉토리 경로	예	예
범주	예	아니요
민감도 수준	예	아니요
식별자의 수	예	아니요
개인정보	예	아니요
민감한 개인 데이터	예	아니요
데이터 주체	예	아니요
중복	예	예
분류 상태	예	상태는 항상 "제한된 통찰력 "입니다.
스캔 분석 이벤트	예	예
파일 해시	예	예
접근 권한이 있는 사용자 수	예	예
사용자/그룹 권한	예	예
파일 소유자	예	예
디렉토리 유형	예	예

데이터 분류는 얼마나 빨리 데이터를 스캔합니까?

검사 속도는 네트워크 지연 시간, 디스크 지연 시간, 네트워크 대역폭, 환경 크기 및 파일 배포 크기의 영향을 받습니다.

- 매핑 전용 스캔을 수행하는 경우 데이터 분류는 하루에 100~150TiB의 데이터를 스캔할 수 있습니다.
- Map & Classify 스캔을 수행할 때, Data Classification은 하루에 15~40TiB의 데이터를 스캔할 수 있습니다.

NetApp Data Classification 사용하여 Amazon FSx 에서 ONTAP 볼륨 스캔

NetApp Data Classification 사용하여 Amazon FSx for ONTAP 볼륨을 스캔하려면 몇 가지 단계를 완료하세요.

시작하기 전에

- 데이터 분류를 배포하고 관리하려면 AWS에서 활성 콘솔 에이전트가 필요합니다.
- 시스템을 생성할 때 선택한 보안 그룹은 데이터 분류 인스턴스의 트래픽을 허용해야 합니다. FSx for ONTAP 파일 시스템에 연결된 ENI를 사용하여 연관된 보안 그룹을 찾고 AWS Management Console을 사용하여 편집할 수 있습니다.

  "Linux 인스턴스용 AWS 보안 그룹"

  "Windows 인스턴스용 AWS 보안 그룹"

  "AWS 탄력적 네트워크 인터페이스(ENI)"

- 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요.
  - NFS의 경우 포트 111과 2049.
  - CIFS의 경우 포트 139 및 445.

데이터 분류 인스턴스 배포

"데이터 분류 배포"아직 배포된 인스턴스가 없는 경우.

AWS용 콘솔 에이전트와 스캔하려는 FSx 볼륨과 동일한 AWS 네트워크에 데이터 분류를 배포해야 합니다.

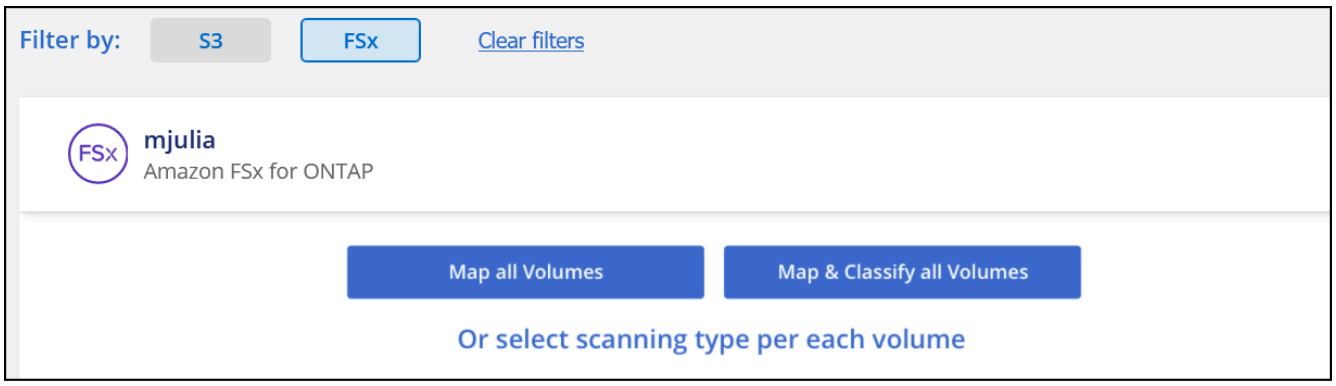
참고: FSx 볼륨을 스캔할 때 온프레미스 위치에 데이터 분류를 배포하는 것은 현재 지원되지 않습니다.

인스턴스에 인터넷 연결이 있는 한 데이터 분류 소프트웨어 업그레이드는 자동으로 수행됩니다.

시스템에서 데이터 분류를 활성화하세요

FSx for ONTAP 볼륨에 대한 데이터 분류를 활성화할 수 있습니다.

1. NetApp Console 에서 *거버넌스 > 분류*를 선택합니다.
2. 데이터 분류 메뉴에서 *구성*을 선택합니다.



3. 각 시스템의 볼륨을 스캔하는 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아보세요":
   - 모든 볼륨을 매핑하려면 *모든 볼륨 매핑*을 선택하세요.
   - 모든 볼륨을 매핑하고 분류하려면 *모든 볼륨 매핑 및 분류*를 선택하세요.
   - 각 볼륨에 대한 스캐닝을 사용자 지정하려면 *또는 각 볼륨에 대한 스캐닝 유형 선택*을 선택한 다음 매핑 및/또는 분류하려는 볼륨을 선택합니다.
4. 확인 대화 상자에서 *승인*을 선택하면 데이터 분류가 볼륨 검사를 시작합니다.

결과

데이터 분류는 시스템에서 선택한 볼륨에 대한 스캔을 시작합니다. 데이터 분류가 초기 스캔을 완료하는 즉시 규정 준수 대시보드에서 결과를 확인할 수 있습니다. 걸리는 시간은 데이터 양에 따라 다릅니다. 몇 분이나 몇 시간이 걸릴 수 있습니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 진행률 표시줄에서 각 검사의 진행 상황을 추적하세요. 진행률 표시줄 위에 마우스를 올리면 볼륨의 전체 파일 대비 검사된 파일 수를 확인할 수 있습니다.

- 기본적으로 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우 시스템은 볼륨의 파일을 검사하지 않습니다. 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 마지막 액세스 시간이 재설정되어도 상관없다면 *또는 각 볼륨에 대한 스캐닝 유형을 선택하세요*를 선택하세요. 결과 페이지에는 데이터 분류가 권한에 관계없이 볼륨을 검사하도록 설정할 수 있는 설정이 있습니다.
- 데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한에 대한 자세한 내용을 확인하세요." .

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

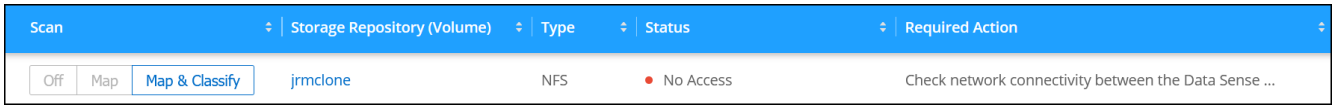
네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

CIFS 볼륨에 액세스할 수 있도록 데이터 분류에 CIFS 자격 증명을 제공해야 합니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 *세부 정보 보기*를 선택하여 상태를 검토하고 오류를 수정하세요.

   예를 들어, 다음 이미지는 데이터 분류 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 볼륨 데이터 분류가 스캔할 수 없는 상황을 보여줍니다.



3. FSx for ONTAP 볼륨이 포함된 각 네트워크와 데이터 분류 인스턴스 사이에 네트워크 연결이 있는지 확인하세요.

   FSx for ONTAP 의 경우 데이터 분류는 콘솔과 동일한 지역의 볼륨만 스캔할 수 있습니다.

4. NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.
5. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 분류를

제공합니다.

a. 데이터 분류 메뉴에서 *구성*을 선택합니다.

b. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택하고 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 비밀번호를 입력합니다.

   자격 증명은 읽기 전용일 수 있지만, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

   데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

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

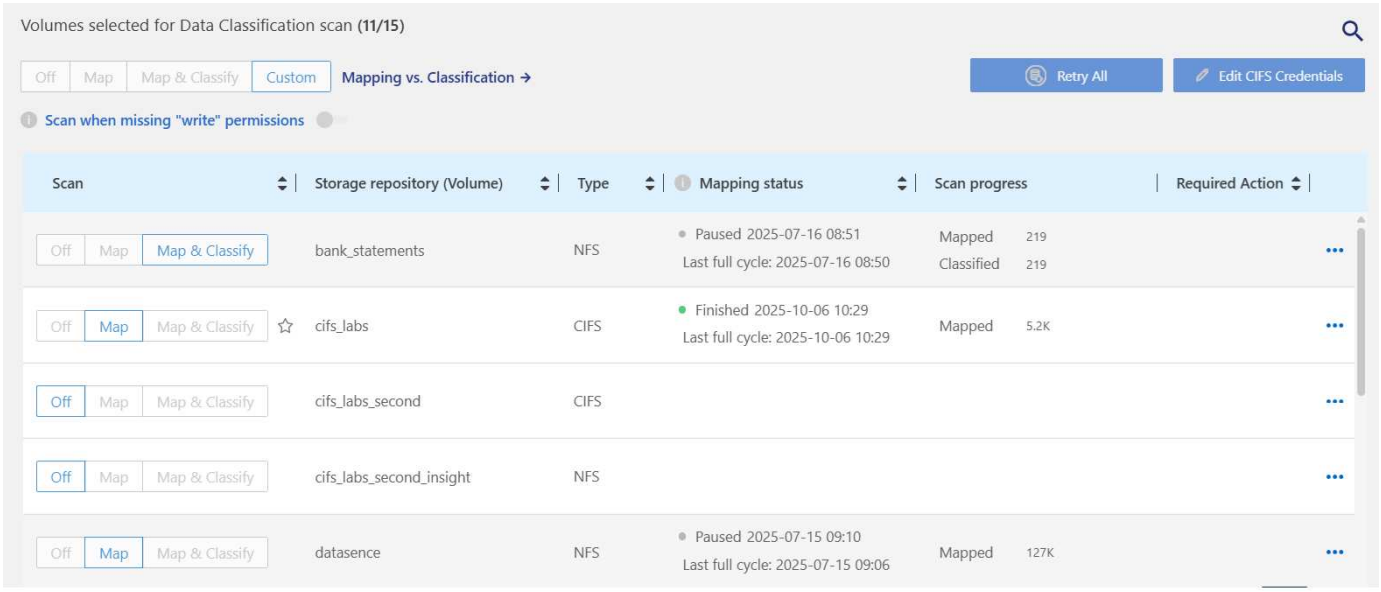
볼륨에서 스캔 활성화 및 비활성화

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.
3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

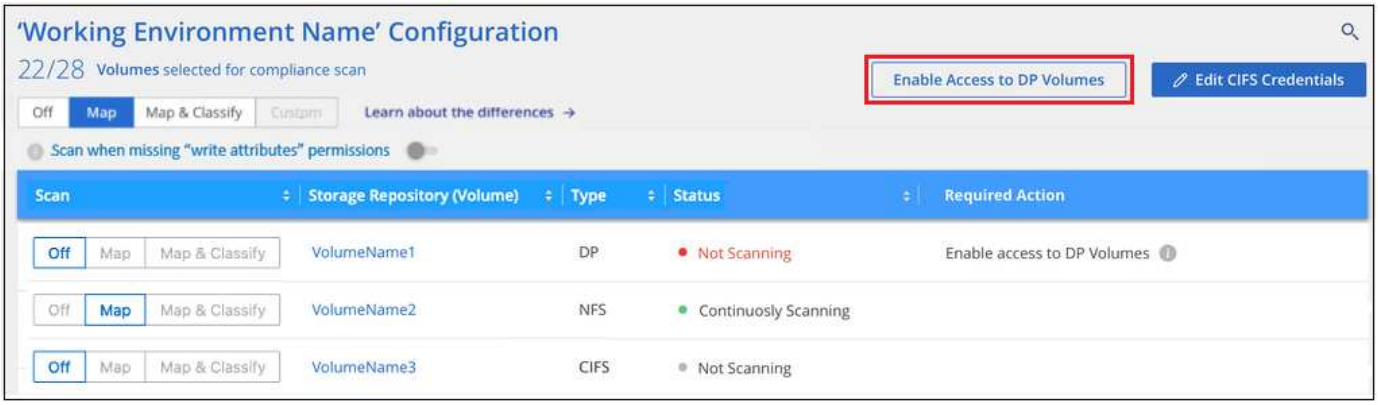
결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

데이터 보호 볼륨 스캔

기본적으로 데이터 보호(DP) 볼륨은 외부에 노출되지 않고 데이터 분류에서 액세스할 수 없으므로 스캔되지 않습니다. 이는 FSx for ONTAP 파일 시스템의 SnapMirror 작업을 위한 대상 볼륨입니다.

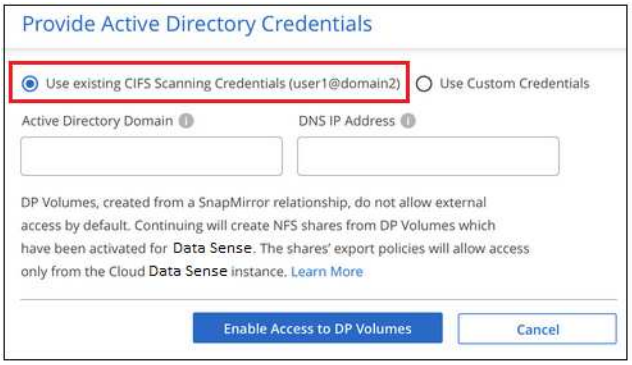
처음에 볼륨 목록은 이러한 볼륨을 유형 **DP**, 상태 스캔 안 함 및 필요한 작업 *DP 볼륨에 대한 액세스 활성화*로 식별합니다.

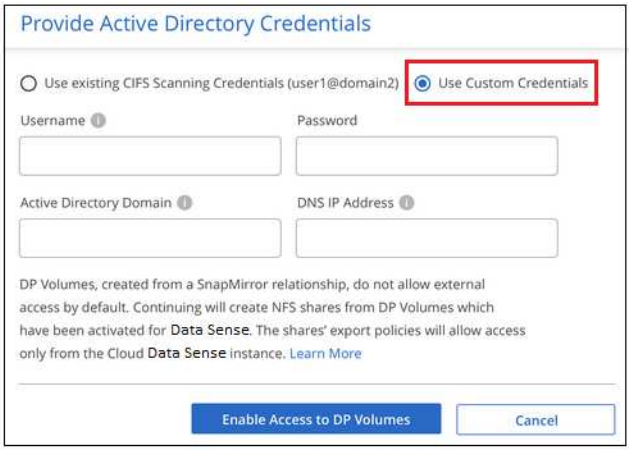


단계

다음 데이터 보호 볼륨을 스캔하려면 다음을 수행하세요.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 페이지 상단에서 *DP 볼륨에 대한 액세스 활성화*를 선택합니다.
3. 확인 메시지를 검토하고 *DP 볼륨에 대한 액세스 활성화*를 다시 선택합니다.
   - ONTAP 파일 시스템용 소스 FSx에서 원래 NFS 볼륨으로 생성된 볼륨이 활성화됩니다.
   - ONTAP 파일 시스템용 소스 FSx에서 CIFS 볼륨으로 처음 생성된 볼륨의 경우 해당 DP 볼륨을 스캔하려면 CIFS 자격 증명을 입력해야 합니다. 데이터 분류가 CIFS 볼륨을 검색할 수 있도록 이미 Active Directory 자격 증명을 입력한 경우 해당 자격 증명을 사용하거나 다른 관리자 자격 증명 집합을 지정할 수 있습니다.





4. 스캔하려는 각 DP 볼륨을 활성화합니다.

결과

데이터 분류가 활성화되면 스캐닝을 위해 활성화된 각 DP 볼륨에서 NFS 공유가 생성됩니다. 공유 내보내기 정책은 데이터 분류 인스턴스에서만 액세스를 허용합니다.

처음에 DP 볼륨에 대한 액세스를 활성화했을 때 CIFS 데이터 보호 볼륨이 없었고 나중에 볼륨을 추가한 경우, 구성 페이지 상단에 **CIFS DP**에 대한 액세스 활성화 버튼이 나타납니다. 이 버튼을 선택하고 CIFS 자격 증명을 추가하여 이러한 CIFS DP 볼륨에 대한 액세스를 활성화합니다.

Active Directory 자격 증명은 첫 번째 CIFS DP 볼륨의 스토리지 VM에만 등록되므로 해당 SVM의 모든 DP 볼륨이 검사됩니다. 다른 SVM에 있는 볼륨에는 Active Directory 자격 증명이 등록되지 않으므로 해당 DP 볼륨은 검사되지 않습니다.

NetApp Data Classification 사용하여 Azure NetApp Files 볼륨 스캔

Azure NetApp Files 에 대한 NetApp Data Classification 시작하려면 몇 가지 단계를 완료하세요.

검사하려는 **Azure NetApp Files** 시스템을 검색하세요**.**

검사하려는 Azure NetApp Files 시스템이 시스템으로 NetApp Console 에 아직 없는 경우"시스템 페이지에 추가하세요" .

데이터 분류 인스턴스 배포

"데이터 분류 배포"아직 배포된 인스턴스가 없는 경우.

Azure NetApp Files 볼륨을 스캔할 때는 데이터 분류를 클라우드에 배포해야 하며, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.

참고**:** Azure NetApp Files 볼륨을 스캔할 때 온-프레미스 위치에 데이터 분류를 배포하는 것은 현재 지원되지 않습니다.

시스템에서 데이터 분류를 활성화하세요

Azure NetApp Files 볼륨에서 데이터 분류를 활성화할 수 있습니다.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.

2. 각 시스템의 볼륨을 스캔하는 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아보세요":
   - 모든 볼륨을 매핑하려면 *모든 볼륨 매핑*을 선택하세요.
   - 모든 볼륨을 매핑하고 분류하려면 *모든 볼륨 매핑 및 분류*를 선택하세요.
   - 각 볼륨에 대한 스캐닝을 사용자 지정하려면 *또는 각 볼륨에 대한 스캐닝 유형 선택*을 선택한 다음 매핑하거나 매핑하고 분류하려는 볼륨을 선택합니다.

     보다볼륨에서 스캔을 활성화하거나 비활성화합니다. 자세한 내용은.

3. 확인 대화 상자에서 *승인*을 선택합니다.

결과

데이터 분류는 시스템에서 선택한 볼륨에 대한 스캔을 시작합니다. 데이터 분류가 초기 스캔을 완료하면 규정 준수 대시보드에서 결과를 확인할 수 있습니다. 걸리는 시간은 데이터 양에 따라 다릅니다. 몇 분이나 몇 시간이 걸릴 수 있습니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 데이터 분류에서는 각 스캔에 대한 진행률 표시줄이 표시됩니다. 볼륨에 있는 전체 파일 수에 대한 검사된 파일 수를 확인하려면 진행률 표시줄 위에 마우스를 올려놓으세요.

- 기본적으로 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우 시스템은 볼륨의 파일을 검사하지 않습니다. 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 마지막 액세스 시간이 재설정되어도 상관없다면 *또는 각 볼륨에 대한 스캐닝 유형을 선택하세요*를 선택하세요. 결과 페이지에는 데이터 분류가 권한에 관계없이 볼륨을 검사하도록 설정할 수 있는 설정이 있습니다.
- 데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한 사항에 대해 알아보세요" .

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. CIFS 볼륨에 액세스할 수 있도록 데이터 분류에 CIFS 자격 증명을 제공해야 합니다.

Azure NetApp Files 의 경우 데이터 분류는 콘솔과 동일한 지역의 볼륨만 검색할 수 있습니다.

체크리스트

- 데이터 분류 인스턴스와 Azure NetApp Files 볼륨이 포함된 각 네트워크 간에 네트워크 연결이 있는지 확인하세요.
- 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요.
  - NFS의 경우 포트 111과 2049.

◦ CIFS의 경우 포트 139 및 445.

- NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.

단계

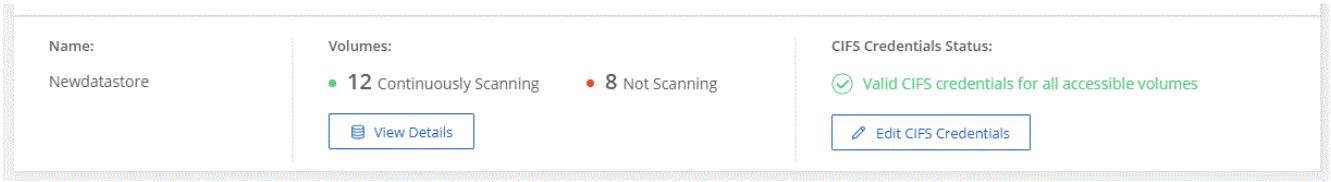
1. 데이터 분류 메뉴에서 *구성*을 선택합니다.

   a. CIFS(SMB)를 사용하는 경우 Active Directory 자격 증명이 올바른지 확인하세요. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택한 다음 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 비밀번호를 입력합니다.

      자격 증명은 읽기 전용일 수 있으며, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

      데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

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



2. 구성 페이지에서 *세부 정보 보기*를 선택하여 각 CIFS 및 NFS 볼륨의 상태를 검토합니다. 필요한 경우 네트워크 연결 문제 등의 오류를 수정하세요.

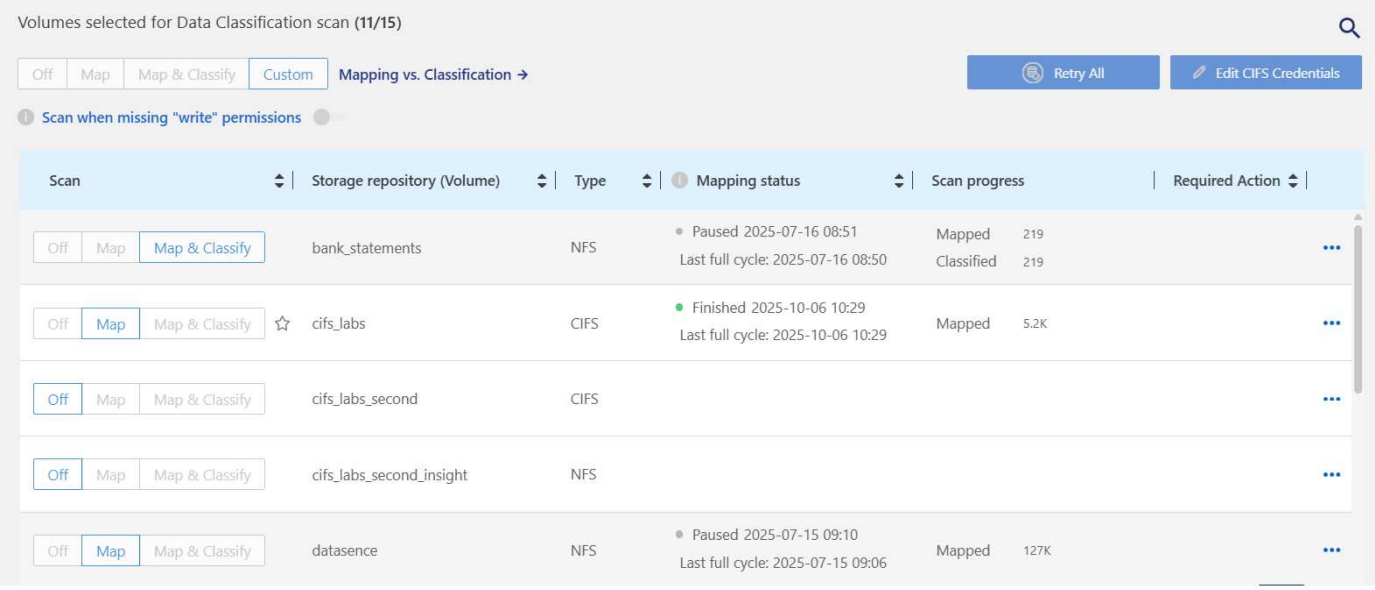
볼륨에서 스캔을 활성화하거나 비활성화합니다.

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.
3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

NetApp Data Classification 사용하여 Cloud Volumes ONTAP 및 온프레미스 ONTAP 볼륨 스캔

NetApp Data Classification 사용하여 Cloud Volumes ONTAP 및 온프레미스 ONTAP 볼륨 스캔을 시작하려면 몇 가지 단계를 완료하세요.

필수 조건

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하세요.

- 인터넷을 통해 액세스할 수 있는 Cloud Volumes ONTAP 및 온프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행할 수 있습니다."클라우드에 데이터 분류 배포" 또는"인터넷 접속이 가능한 사내 위치에서" .
- 인터넷 접속이 불가능한 다크 사이트에 설치된 온프레미스 ONTAP 시스템을 스캔하는 경우 다음이 필요합니다. "인터넷 접속이 없는 동일한 온프레미스 위치에 데이터 분류를 배포합니다." . 이렇게 하려면 콘솔 에이전트를 동일한 온프레미스 위치에 배포해야 합니다.

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. CIFS 볼륨에 액세스할 수 있도록 데이터 분류에 CIFS 자격 증명을 제공해야 합니다.

체크리스트

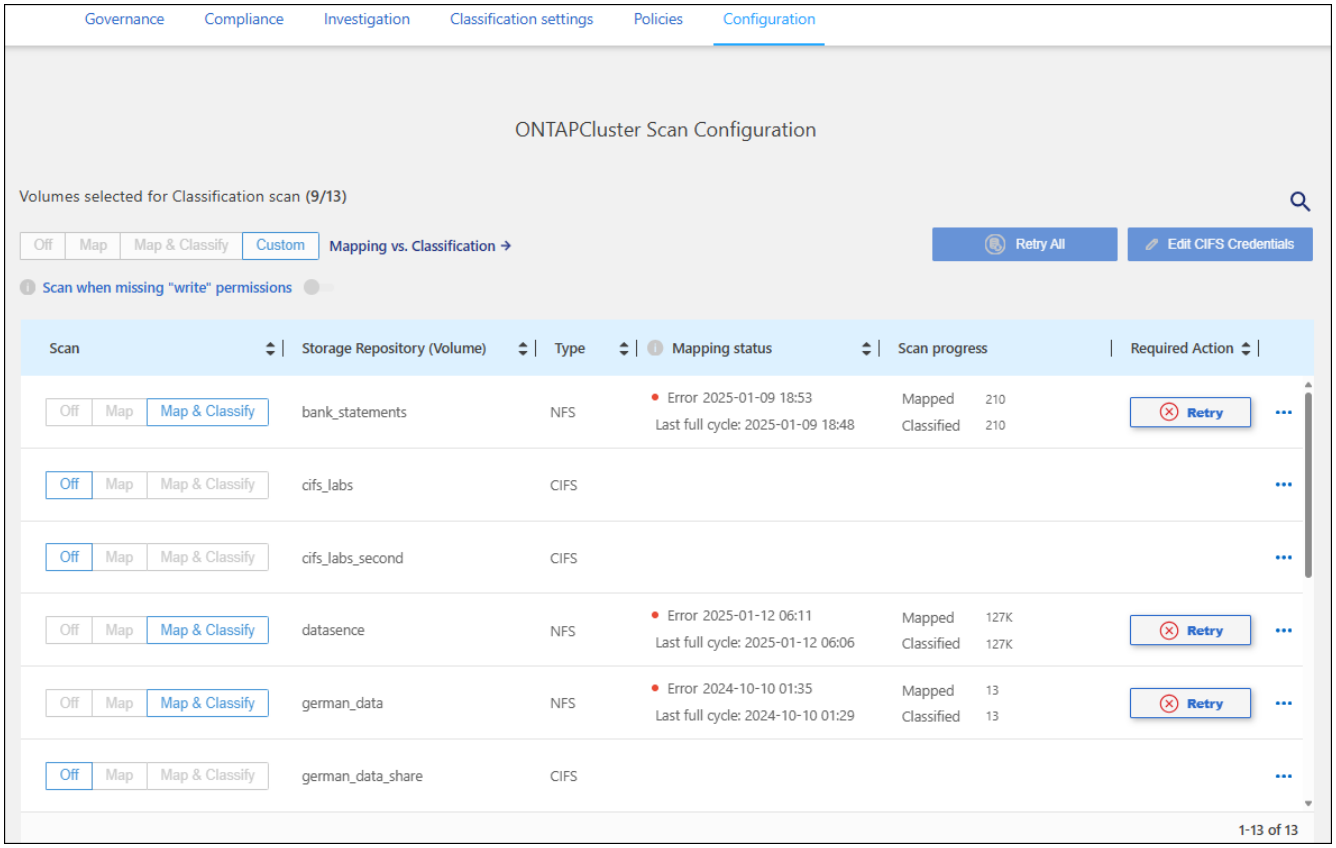
- 데이터 분류 인스턴스와 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터의 볼륨이 포함된 각 네트워크 간에 네트워크 연결이 있는지 확인하세요.
- Cloud Volumes ONTAP 의 보안 그룹이 데이터 분류 인스턴스에서 들어오는 트래픽을 허용하는지 확인하세요.

  데이터 분류 인스턴스의 IP 주소에서 발생하는 트래픽에 대해 보안 그룹을 열거나, 가상 네트워크 내부의 모든 트래픽에 대해 보안 그룹을 열 수 있습니다.

- NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.



2. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 분류를 제공합니다. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택하고 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 비밀번호를 입력합니다.

   자격 증명은 읽기 전용일 수 있지만, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

   데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기

속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

자격 증명을 올바르게 입력한 경우 모든 CIFS 볼륨이 성공적으로 인증되었음을 확인하는 메시지가 표시됩니다.

3. 구성 페이지에서 *구성*을 선택하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

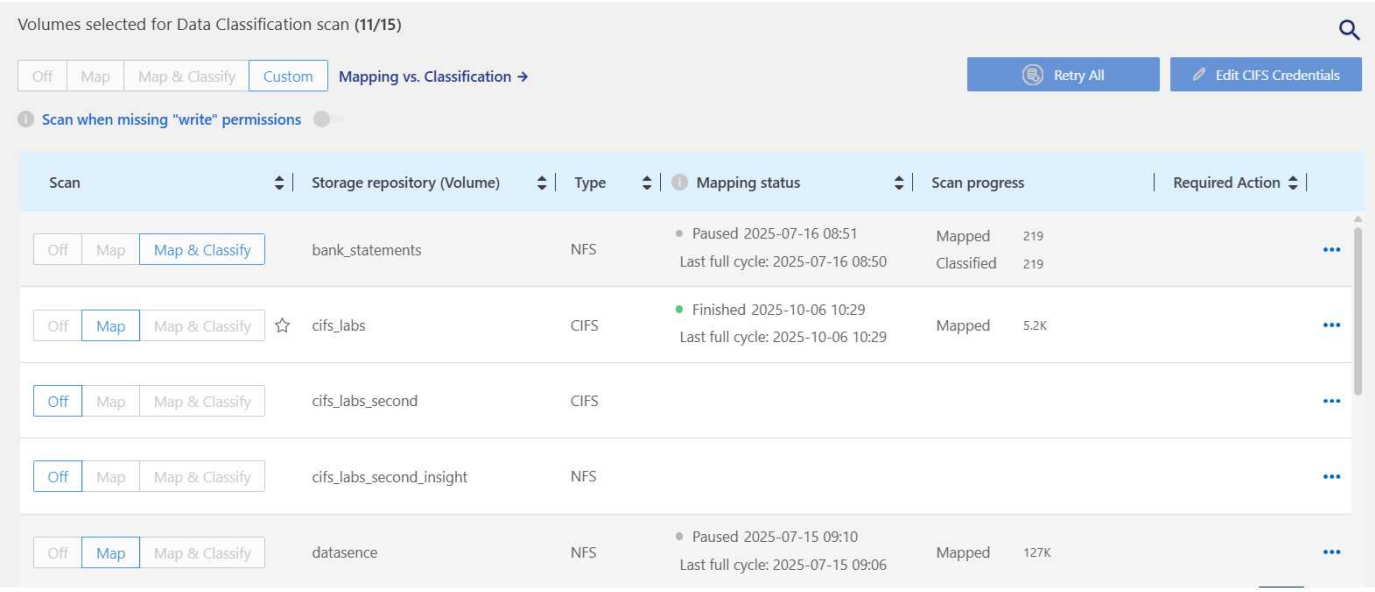
볼륨에서 스캔을 활성화하거나 비활성화합니다.

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.
3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한에 대한 자세한 내용을 확인하세요." .

NetApp Data Classification 사용하여 데이터베이스 스키마 스캔

NetApp Data Classification 사용하여 데이터베이스 스키마 스캔을 시작하려면 몇 가지 단계를 완료하세요.

필수 조건 검토

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요.

지원되는 데이터베이스

데이터 분류는 다음 데이터베이스에서 스키마를 스캔할 수 있습니다.

- Amazon 관계형 데이터베이스 서비스(Amazon RDS)
- 몽고디비
- MySQL
- 신탁
- 포스트그레스큐엘
- SAP 하나
- SQL 서버(MSSQL)

데이터베이스에서 통계 수집 기능을 *활성화*해야 합니다.

데이터베이스 요구 사항

데이터 분류 인스턴스에 연결된 모든 데이터베이스는 호스팅 위치에 관계없이 스캔할 수 있습니다. 데이터베이스에 연결하려면 다음 정보가 필요합니다.

- IP 주소 또는 호스트 이름
- 포트
- 서비스 이름(Oracle 데이터베이스에 액세스하는 경우에만 해당)
- 스키마에 대한 읽기 액세스를 허용하는 자격 증명

  사용자 이름과 비밀번호를 선택할 때는 스캔하려는 모든 스키마와 테이블에 대한 전체 읽기 권한이 있는 것을 선택하는 것이 중요합니다. 데이터 분류 시스템에 필요한 모든 권한을 갖춘 전담 사용자를 만드는 것이 좋습니다.

MongoDB의 경우 읽기 전용 관리자 역할이 필요합니다.

데이터 분류 인스턴스 배포

아직 배포된 인스턴스가 없으면 데이터 분류를 배포합니다.

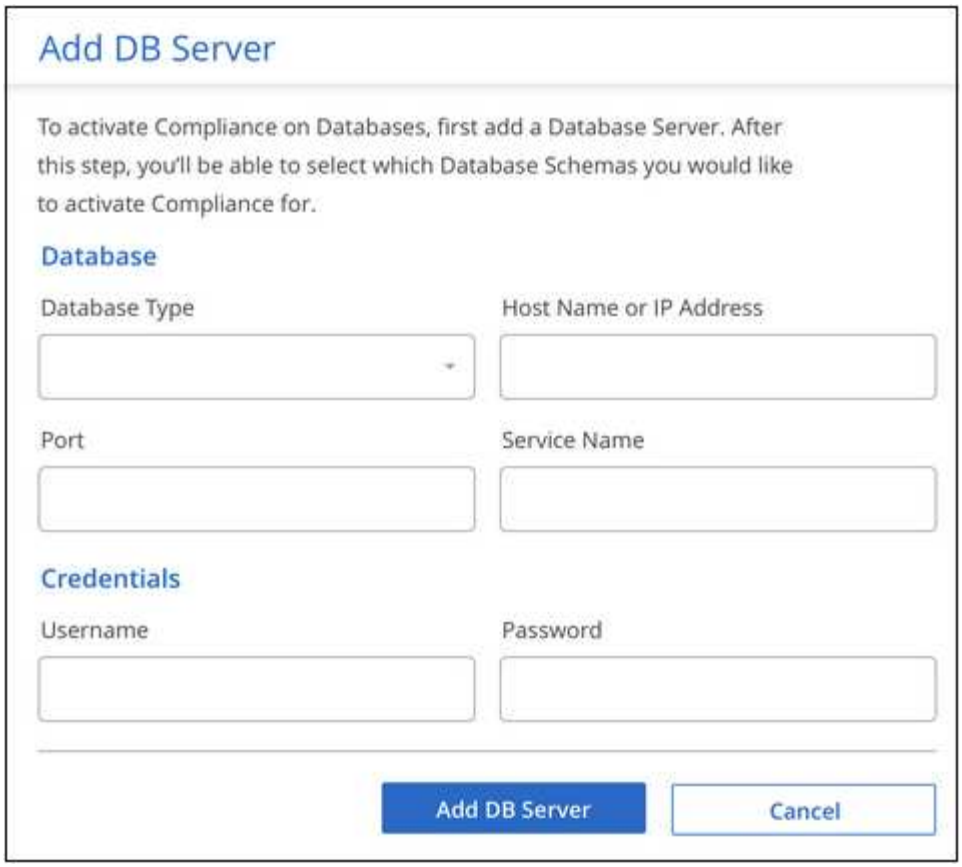
인터넷을 통해 접근 가능한 데이터베이스 스키마를 스캔하는 경우 다음을 수행할 수 있습니다."클라우드에 데이터 분류 배포" 또는"인터넷 접속이 가능한 온프레미스 위치에 데이터 분류를 배포합니다." .

인터넷 접속이 불가능한 다크 사이트에 설치된 데이터베이스 스키마를 스캔하는 경우 다음이 필요합니다."인터넷 접속이 없는 동일한 온프레미스 위치에 데이터 분류를 배포합니다." . 이를 위해서는 콘솔 에이전트가 동일한 온프레미스 위치에 배포되어야 합니다.

데이터베이스 서버 추가

스키마가 있는 데이터베이스 서버를 추가합니다.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 시스템 추가 > *데이터베이스 서버 추가*를 선택합니다.
3. 데이터베이스 서버를 식별하는 데 필요한 정보를 입력하세요.
    a. 데이터베이스 유형을 선택하세요.
    b. 데이터베이스에 연결하려면 포트와 호스트 이름 또는 IP 주소를 입력하세요.
    c. Oracle 데이터베이스의 경우 서비스 이름을 입력합니다.
    d. 데이터 분류가 서버에 액세스할 수 있도록 자격 증명을 입력하세요.
    e. *DB 서버 추가*를 선택합니다.



데이터베이스가 시스템 목록에 추가되었습니다.

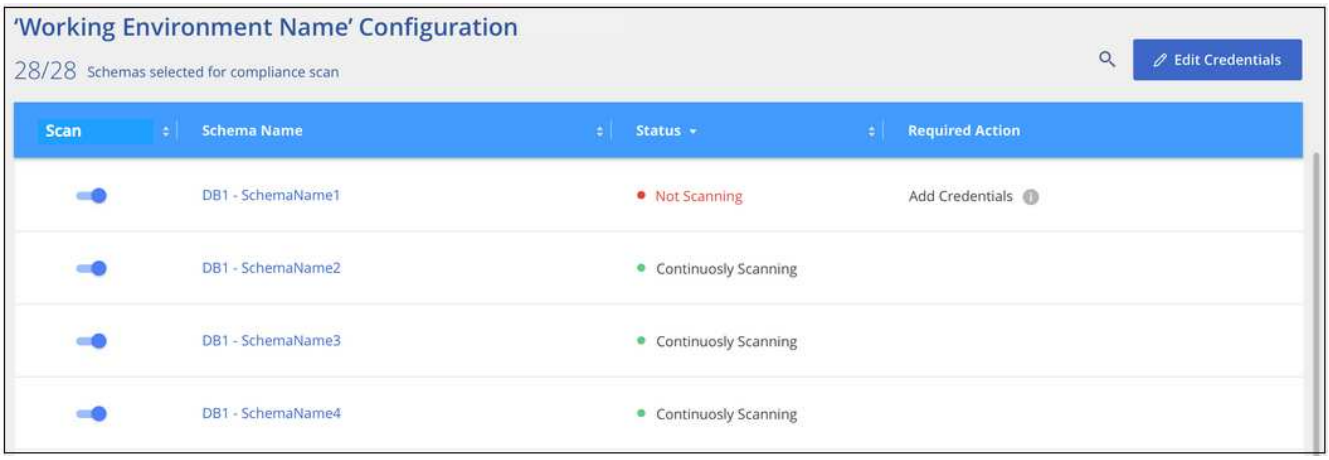
데이터베이스 스키마에 대한 스캔 활성화 및 비활성화

언제든지 스키마 전체 스캐닝을 중지하거나 시작할 수 있습니다.

데이터베이스 스키마에 대해 매핑 전용 스캔을 선택하는 옵션은 없습니다.

1. 구성 페이지에서 구성하려는 데이터베이스에 대한 구성 버튼을 선택합니다.

2. 슬라이더를 오른쪽으로 움직여 검사할 스키마를 선택합니다.



결과

데이터 분류는 활성화된 데이터베이스 스키마를 스캔하기 시작합니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 각 스캔의 진행 상황은 진행률 표시줄로 표시됩니다. 진행률 표시줄 위에 마우스를 올려 놓으면 볼륨에 있는 전체 파일 수에 대한 검사된 파일 수를 확인할 수 있습니다. 오류가 있는 경우 오류 수정에 필요한 작업과 함께 상태 열에 오류가 표시됩니다.

데이터 분류는 하루에 한 번씩 데이터베이스를 스캔합니다. 데이터베이스는 다른 데이터 소스처럼 지속적으로 스캔되지 않습니다.

NetApp Data Classification 사용하여 Google Cloud NetApp Volumes 스캔

NetApp Data Classification 시스템으로서 Google Cloud NetApp Volumes 지원합니다. Google Cloud NetApp Volumes 시스템을 스캔하는 방법을 알아보세요.

스캔하려는 **Google Cloud NetApp Volumes** 시스템을 검색하세요**.**

스캔하려는 Google Cloud NetApp Volumes 시스템이 NetApp Console 에 시스템으로 아직 없는 경우"시스템 페이지에 추가하세요" .

데이터 분류 인스턴스 배포

"데이터 분류 배포"아직 배포된 인스턴스가 없는 경우.

Google Cloud NetApp Volumes 스캔할 때는 데이터 분류를 클라우드에 배포해야 하며, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.

참고**:** 현재 Google Cloud NetApp Volumes 스캔할 때 온프레미스 위치에 데이터 분류를 배포하는 것은 지원되지 않습니다.

시스템에서 데이터 분류를 활성화하세요

Google Cloud NetApp Volumes 시스템에서 데이터 분류를 활성화할 수 있습니다.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 각 시스템의 볼륨을 스캔하는 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아보세요":
   - 모든 볼륨을 매핑하려면 *모든 볼륨 매핑*을 선택하세요.

- 모든 볼륨을 매핑하고 분류하려면 *모든 볼륨 매핑 및 분류*를 선택하세요.
- 각 볼륨에 대한 스캐닝을 사용자 지정하려면 *또는 각 볼륨에 대한 스캐닝 유형 선택*을 선택한 다음 매핑 및/또는 분류하려는 볼륨을 선택합니다.

  보다볼륨에서 규정 준수 검사 활성화 및 비활성화 자세한 내용은.

3. 확인 대화 상자에서 *승인*을 선택합니다.

결과

데이터 분류는 시스템에서 선택한 볼륨에 대한 스캔을 시작합니다. 데이터 분류가 초기 스캔을 완료하면 규정 준수 대시보드에서 결과를 확인할 수 있습니다. 걸리는 시간은 데이터 양에 따라 다릅니다. 몇 분에서 몇 시간까지 걸립니다. 구성 메뉴의 시스템 구성 섹션에서 초기 검사의 진행 상황을 추적할 수 있습니다. 데이터 분류에서는 각 스캔에 대한 진행률 표시줄이 표시됩니다. 진행률 표시줄 위에 마우스를 올려 놓으면 볼륨의 전체 파일 대비 검사된 파일 수를 확인할 수 있습니다.

- 기본적으로 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우 시스템은 볼륨의 파일을 검사하지 않습니다. 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 마지막 액세스 시간이 재설정되어도 상관없다면 *또는 각 볼륨에 대한 스캐닝 유형을 선택하세요*를 선택하세요. 결과 페이지에는 데이터 분류가 권한에 관계없이 볼륨을 검사하도록 설정할 수 있는 설정이 있습니다.
- 데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한 사항에 대해 알아보세요".

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. CIFS 볼륨의 경우 CIFS 자격 증명을 사용하여 데이터 분류를 제공해야 합니다.

Google Cloud NetApp Volumes 의 경우 데이터 분류는 콘솔과 동일한 지역의 볼륨만 스캔할 수 있습니다.

체크리스트

- Google Cloud NetApp Volumes 대한 볼륨이 포함된 각 네트워크와 데이터 분류 인스턴스 사이에 네트워크 연결이 있는지 확인하세요.
- 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요.
  - NFS의 경우 포트 111과 2049.
  - CIFS의 경우 포트 139 및 445.
- NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.

단계

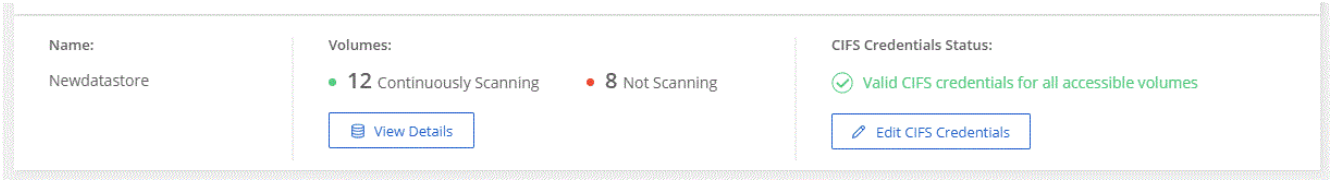
1. 데이터 분류 메뉴에서 *구성*을 선택합니다.

   a. CIFS(SMB)를 사용하는 경우 Active Directory 자격 증명이 올바른지 확인하세요. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택한 다음 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 비밀번호를 입력합니다.

      자격 증명은 읽기 전용일 수 있지만, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

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



2. 구성 페이지에서 *세부 정보 보기*를 선택하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

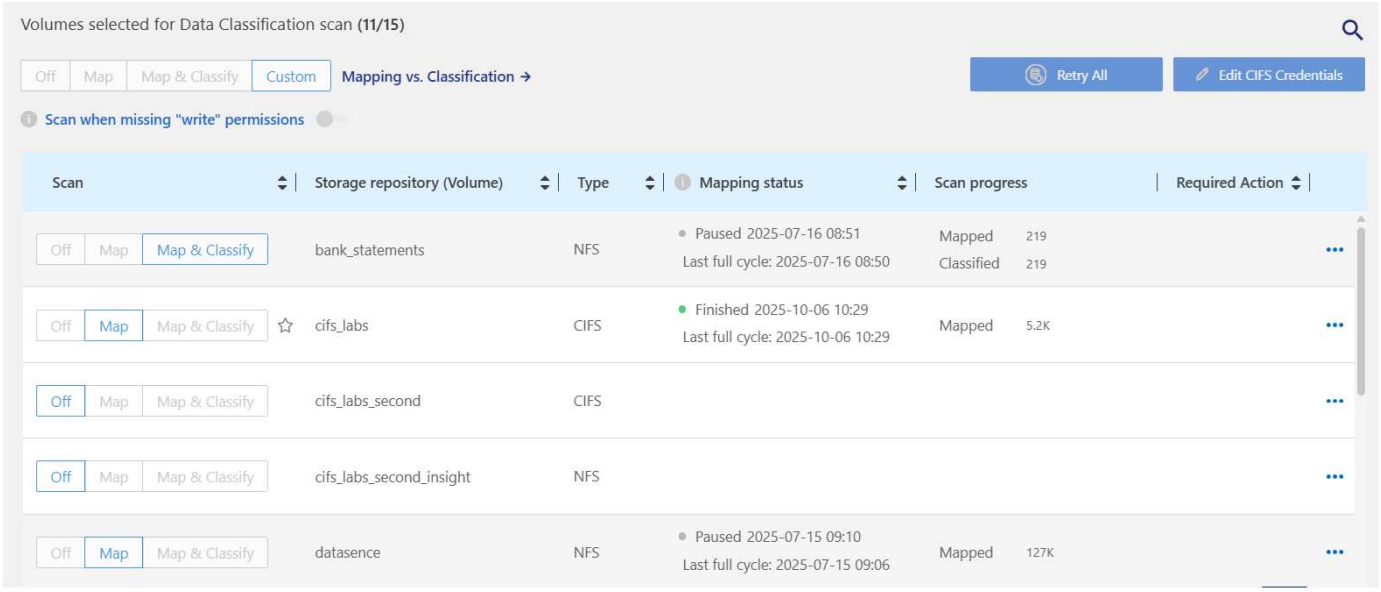
볼륨에서 스캔 활성화 및 비활성화

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.
3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

NetApp Data Classification 사용하여 파일 공유 스캔

파일 공유를 스캔하려면 먼저 NetApp Data Classification 에서 파일 공유 그룹을 만들어야 합니다. 파일 공유 그룹은 온프레미스 또는 클라우드에서 호스팅되는 NFS 또는 CIFS(SMB) 공유를 위한 것입니다.

데이터 분류 핵심 버전에서는 NetApp 아닌 파일 공유에서 데이터를 스캔하는 기능이 지원되지 않습니다.

필수 조건

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요.

- 공유는 클라우드나 온프레미스 등 어디에서나 호스팅될 수 있습니다. 이전 NetApp 7-Mode 스토리지 시스템의 CIFS 공유는 파일 공유로 스캔될 수 있습니다.
  - 데이터 분류는 7-Mode 시스템에서 권한이나 "마지막 액세스 시간"을 추출할 수 없습니다.
  - 7-Mode 시스템에서 일부 Linux 버전과 CIFS 공유 간에 알려진 문제로 인해 NTLM 인증이 활성화된 SMBv1만 사용하도록 공유를 구성해야 합니다.
- 데이터 분류 인스턴스와 공유 간에 네트워크 연결이 필요합니다.
- DFS(분산 파일 시스템) 공유를 일반 CIFS 공유로 추가할 수 있습니다. 데이터 분류에서는 공유가 단일 CIFS 공유로 결합된 여러 서버/볼륨에 기반을 두고 있다는 사실을 인식하지 못하기 때문에 메시지가 실제로는 다른 서버/볼륨에 있는 폴더/공유 중 하나에만 적용되는 경우에도 공유에 대한 권한 또는 연결 오류가 발생할 수 있습니다.
- CIFS(SMB) 공유의 경우 공유에 대한 읽기 액세스 권한을 제공하는 Active Directory 자격 증명이 있는지 확인하세요. 데이터 분류에서 높은 권한이 필요한 데이터를 스캔해야 하는 경우 관리자 자격 증명이 선호됩니다.

  데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.
- 그룹 내의 모든 CIFS 파일 공유는 동일한 Active Directory 자격 증명을 사용해야 합니다.
- NFS와 CIFS(Kerberos 또는 NTLM 사용) 공유를 혼합할 수 있습니다. 그룹에 주식을 별도로 추가해야 합니다. 즉, 프로토콜당 한 번씩, 총 두 번 프로세스를 완료해야 합니다.

◦ CIFS 인증 유형(Kerberos 및 NTLM)을 혼합하여 파일 공유 그룹을 만들 수 없습니다.

- Kerberos 인증을 사용하는 CIFS를 사용하는 경우 제공된 IP 주소가 데이터 분류에 액세스할 수 있는지 확인하세요. IP 주소에 접근할 수 없으면 파일 공유를 추가할 수 없습니다.

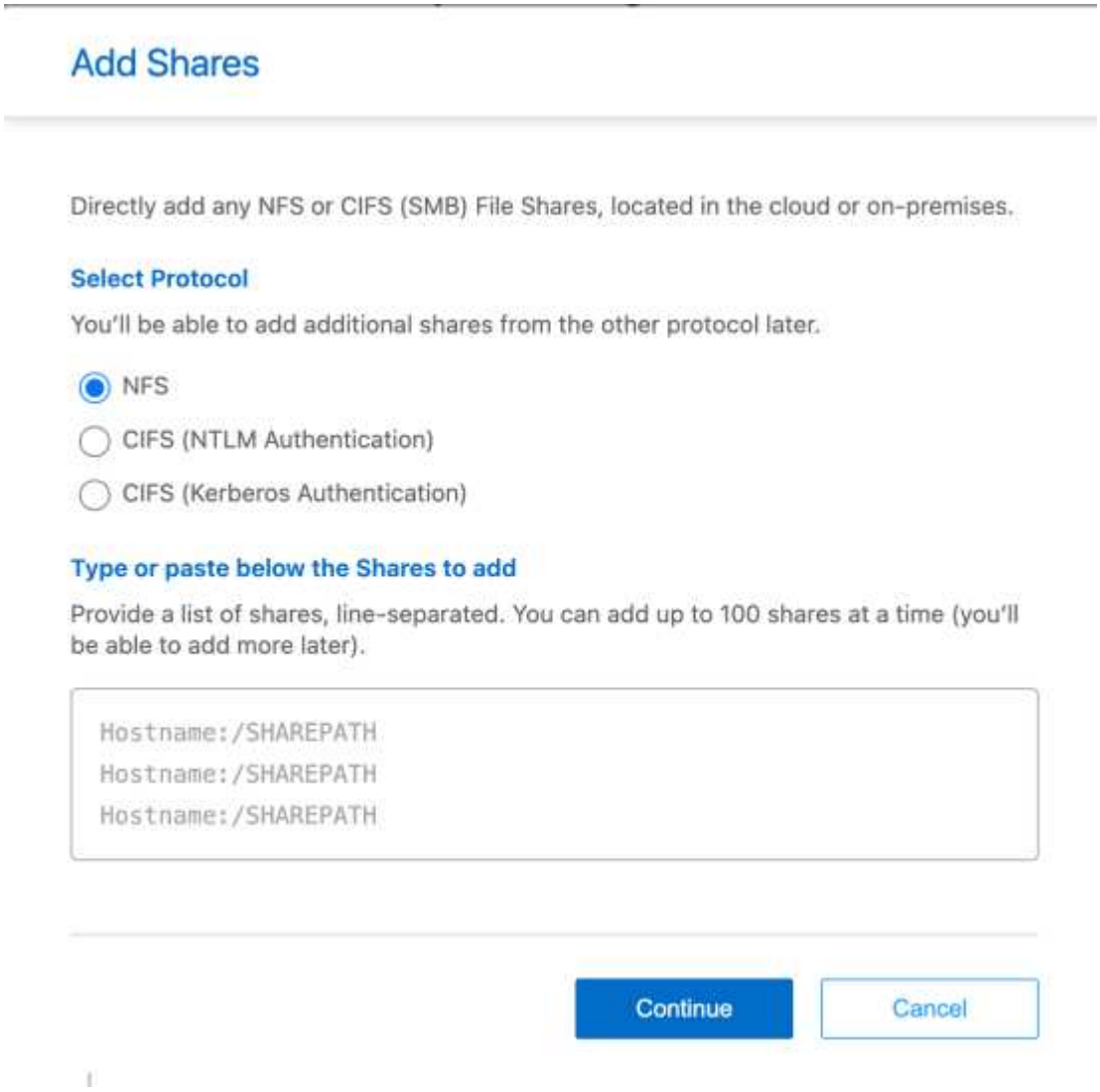
파일 공유 그룹 만들기

그룹에 파일 공유를 추가할 때는 다음 형식을 사용해야 합니다. `<host_name>:/<share_path>` .

파일 공유를 개별적으로 추가할 수도 있고, 검사하려는 파일 공유를 줄로 구분하여 나열하여 입력할 수도 있습니다. 한 번에 최대 100개의 주식을 추가할 수 있습니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 시스템 추가 > *파일 공유 그룹 추가*를 선택합니다.
3. 파일 공유 그룹 추가 대화 상자에서 공유 그룹의 이름을 입력한 다음 *계속*을 선택합니다.
4. 추가할 파일 공유에 대한 프로토콜을 선택하세요.



a. NTLM 인증을 사용하여 CIFS 공유를 추가하는 경우 Active Directory 자격 증명을 입력하여 CIFS 볼륨에

액세스합니다. 읽기 전용 자격 증명도 지원되지만 관리자 자격 증명을 사용하여 전체 액세스 권한을 제공하는 것이 좋습니다. 저장을 선택하세요.

5. 검사하려는 파일 공유를 추가합니다(한 줄에 파일 공유 하나씩). 그런 다음 계속을 선택하세요.
6. 확인 대화 상자에는 추가된 주식 수가 표시됩니다.

   대화 상자에 추가할 수 없는 공유가 나열되면 이 정보를 캡처하여 문제를 해결하세요. 문제가 명명 규칙과 관련된 경우, 수정된 이름으로 공유를 다시 추가할 수 있습니다.

7. 볼륨에 대한 스캐닝을 구성합니다.
   - 파일 공유에서 매핑 전용 검사를 활성화하려면 *매핑*을 선택합니다.
   - 파일 공유에 대한 전체 검사를 활성화하려면 *매핑 및 분류*를 선택하세요.
   - 파일 공유에서 스캐닝을 비활성화하려면 *끄기*를 선택하세요.

> 기본적으로 페이지 상단의 **"쓰기 속성"** 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. + "쓰기 속성" 권한이 없는 경우 검사*를 *켜기*로 전환하면 검사에서 마지막으로 액세스한 시간을 재설정하고 권한에 관계없이 모든 파일을 검사합니다. + 마지막으로 액세스한 타임스탬프에 대해 자세히 알아보려면 다음을 참조하세요."데이터 분류의 데이터 소스에서 수집된 메타데이터" .

결과

데이터 분류는 추가한 파일 공유에 있는 파일의 스캔을 시작합니다. 당신은 할 수 있습니다스캐닝 진행 상황을 추적하세요 대시보드에서 검사 결과를 확인하세요.

> Kerberos 인증을 사용하는 CIFS 구성에 대한 스캔이 성공적으로 완료되지 않으면 구성 탭에서 오류를 확인하세요.

파일 공유 그룹 편집

파일 공유 그룹을 만든 후에는 CIFS 프로토콜을 편집하거나 파일 공유를 추가 및 제거할 수 있습니다.

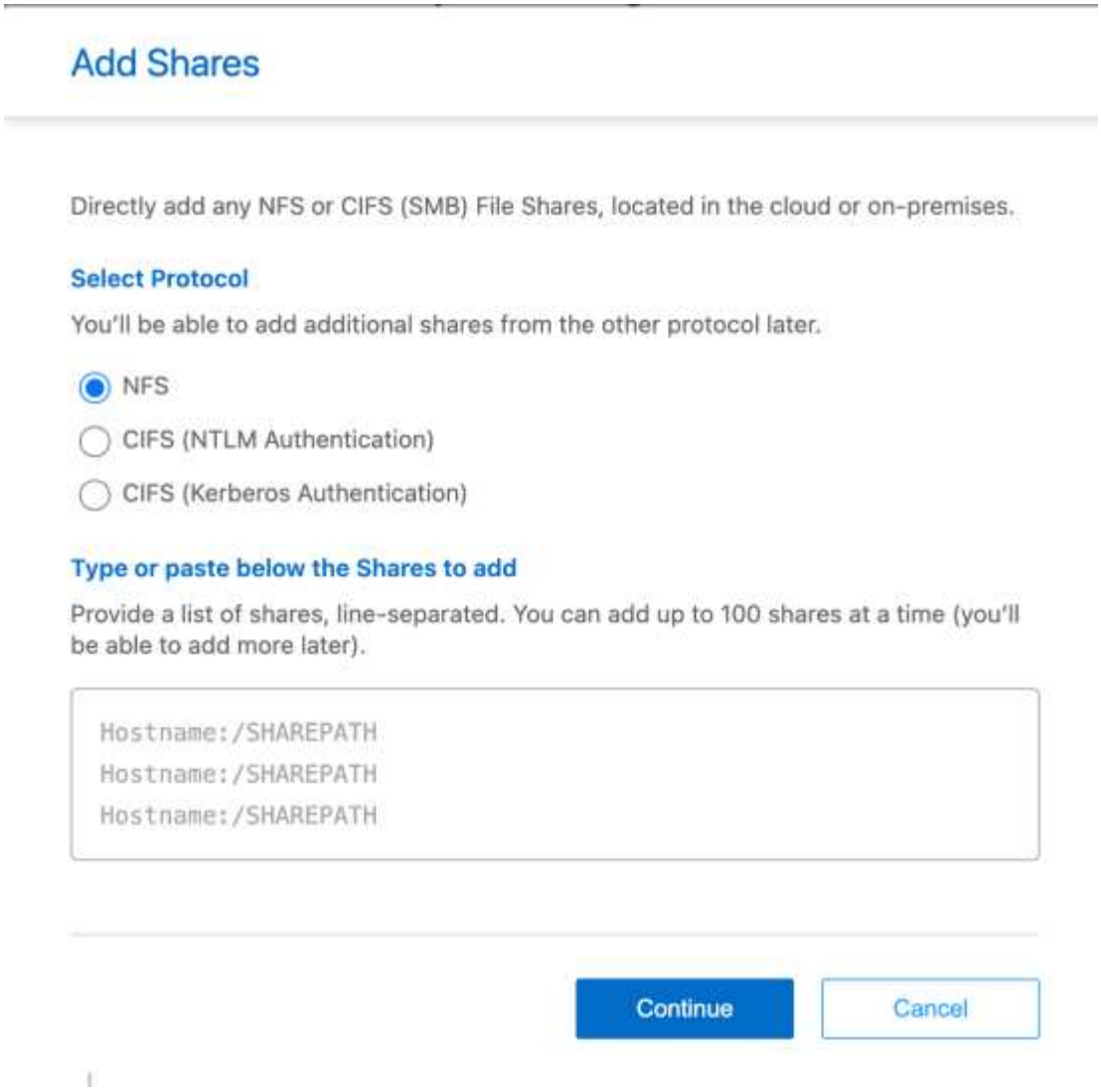
CIFS 프로토콜 구성 편집

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 수정하려는 파일 공유 그룹을 선택합니다.
3. **CIFS** 자격 증명 편집을 선택합니다.

4. 인증 방법을 선택하세요: **NTLM** 또는 **Kerberos**.
5. Active Directory 사용자 이름과 암호를 입력합니다.
6. 저장을 선택하여 프로세스를 완료하세요.

스캔에 파일 공유 추가

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 수정하려는 파일 공유 그룹을 선택합니다.
3. **+** 공유 추가를 선택하세요.
4. 추가할 파일 공유에 대한 프로토콜을 선택하세요.



이미 구성한 프로토콜에 파일 공유를 추가하는 경우 변경할 필요가 없습니다.

두 번째 프로토콜을 사용하여 파일 공유를 추가하는 경우 다음에서 자세히 설명한 대로 인증을 올바르게 구성했는지 확인하십시오."전제 조건" .

5. 형식을 사용하여 검사하려는 파일 공유를 추가합니다(줄당 파일 공유 하나). `<host_name>:/<share_path>` .
6. 계속을 선택하여 파일 공유 추가를 완료합니다.

스캔에서 파일 공유 제거

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 파일 공유를 제거할 시스템을 선택하세요.
3. *구성*을 선택하세요.
4. 구성 페이지에서 작업을 선택하세요. ••• 제거하려는 파일 공유에 대해.
5. 작업 메뉴에서 *공유 제거*를 선택합니다.

스캐닝 진행 상황을 추적하세요

초기 스캔의 진행 상황을 추적할 수 있습니다.

1. 구성 메뉴를 선택하세요.
2. 시스템 구성을 선택하세요.
3. 저장소의 경우, 검사 진행률 열을 확인하여 상태를 확인하세요.

NetApp Data Classification 사용하여 StorageGRID 데이터 스캔

NetApp Data Classification 사용하여 StorageGRID 내에서 직접 데이터 스캔을 시작하려면 몇 가지 단계를 완료하세요.

StorageGRID 요구 사항 검토

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요.

- 개체 스토리지 서비스에 연결하려면 엔드포인트 URL이 필요합니다.
- 데이터 분류가 버킷에 액세스할 수 있도록 StorageGRID 에서 액세스 키와 비밀 키가 필요합니다.

데이터 분류 인스턴스 배포

아직 배포된 인스턴스가 없으면 데이터 분류를 배포합니다.

인터넷을 통해 액세스할 수 있는 StorageGRID 의 데이터를 스캔하는 경우 다음을 수행할 수 있습니다."클라우드에 데이터 분류 배포" 또는"인터넷 접속이 가능한 온프레미스 위치에 데이터 분류를 배포합니다." .

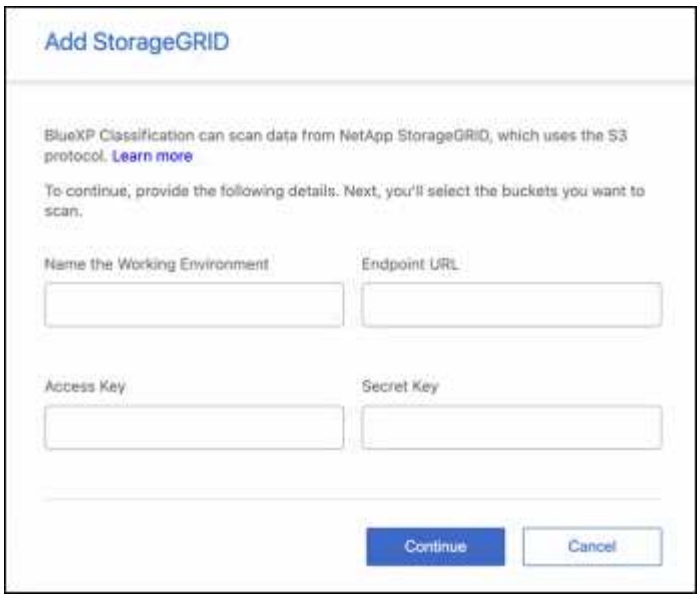
인터넷 접속이 불가능한 어두운 장소에 설치된 StorageGRID 에서 데이터를 스캔하는 경우 다음이 필요합니다."인터넷 접속이 없는 동일한 온프레미스 위치에 데이터 분류를 배포합니다." . 이를 위해서는 콘솔 에이전트가 동일한 온프레미스 위치에 배포되어야 합니다.

데이터 분류에 StorageGRID 서비스 추가

StorageGRID 서비스를 추가합니다.

단계

1. 데이터 분류 메뉴에서 구성 옵션을 선택합니다.
2. 구성 페이지에서 시스템 추가 > * StorageGRID 추가*를 선택합니다.
3. StorageGRID 서비스 추가 대화 상자에서 StorageGRID 서비스에 대한 세부 정보를 입력하고 *계속*을 선택합니다.
   a. 시스템에 사용할 이름을 입력하세요. 이 이름은 연결하려는 StorageGRID 서비스의 이름을 반영해야 합니다.
   b. 개체 스토리지 서비스에 액세스하려면 Endpoint URL을 입력하세요.
   c. Data Classification이 StorageGRID 의 버킷에 액세스할 수 있도록 액세스 키와 비밀 키를 입력하세요.



결과

StorageGRID 시스템 목록에 추가되었습니다.

StorageGRID 버킷에서 스캔 활성화 및 비활성화

StorageGRID 에서 데이터 분류를 활성화한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다. 데이터 분류는 해당 버킷을 검색하여 사용자가 만든 시스템에 표시합니다.

단계

1. 구성 페이지에서 StorageGRID 시스템을 찾으세요.
2. StorageGRID 시스템 타일에서 *구성*을 선택합니다.
3. 다음 단계 중 하나를 완료하여 스캐닝을 활성화하거나 비활성화하세요.
   - 버킷에서 매핑 전용 스캔을 활성화하려면 *맵*을 선택합니다.
   - 버킷에 대한 전체 검사를 활성화하려면 *매핑 및 분류*를 선택합니다.
   - 버킷에서 스캐닝을 비활성화하려면 *끄기*를 선택하세요.

결과

데이터 분류는 활성화된 버킷을 스캔하기 시작합니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 각 스캔의 진행 상황은 진행률 표시줄로 표시됩니다. 진행률 표시줄 위에 마우스를 올려 놓으면 볼륨의 전체 파일 대비 검사된 파일 수를 확인할 수 있습니다. 오류가 있는 경우 오류는 상태 열에 표시되고 오류를 수정하는 데 필요한 작업도 함께 표시됩니다.

Active Directory를 NetApp Data Classification 와 통합하세요

NetApp Data Classification 와 글로벌 Active Directory를 통합하면 데이터 분류 보고서에서 파일 소유자와 파일에 액세스할 수 있는 사용자 및 그룹에 대한 결과를 더욱 향상시킬 수 있습니다.

특정 데이터 소스(아래 나열됨)를 설정하는 경우 데이터 분류가 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격

증명을 입력해야 합니다. 이 통합은 데이터 분류에 해당 데이터 소스에 있는 데이터의 파일 소유자 및 권한 세부 정보를 제공합니다. 해당 데이터 소스에 대해 입력한 Active Directory는 여기에 입력한 글로벌 Active Directory 자격 증명과 다를 수 있습니다. 데이터 분류는 모든 통합 Active Directory에서 사용자 및 권한 세부 정보를 찾습니다.

이 통합은 데이터 분류의 다음 위치에 추가 정보를 제공합니다.

- "파일 소유자"를 사용할 수 있습니다"필터" 조사 창에서 파일 메타데이터에서 결과를 확인하세요. SID(보안 식별자)를 포함하는 파일 소유자 대신 실제 사용자 이름이 채워집니다.

  파일 소유자에 대한 자세한 정보(계정 이름, 이메일 주소, SAM 계정 이름)를 보거나 해당 사용자가 소유한 항목을 볼 수도 있습니다.

- 당신은 볼 수 있습니다"전체 파일 권한" "모든 권한 보기" 버튼을 클릭하면 각 파일과 디렉토리에 대한 권한이 표시됩니다.
- 에서"거버넌스 대시보드" , 공개 권한 패널에는 데이터에 대한 더 자세한 정보가 표시됩니다.

로컬 사용자 SID와 알 수 없는 도메인의 SID는 실제 사용자 이름으로 변환되지 않습니다.

지원되는 데이터 소스

데이터 분류와 Active Directory를 통합하면 다음 데이터 소스에서 데이터를 식별할 수 있습니다.

- 온프레미스 ONTAP 시스템
- Cloud Volumes ONTAP
- Azure NetApp Files
- ONTAP 용 FSx

Active Directory 서버에 연결

데이터 분류를 배포하고 데이터 소스에 대한 스캐닝을 활성화한 후에는 데이터 분류를 Active Directory와 통합할 수 있습니다. Active Directory는 DNS 서버 IP 주소나 LDAP 서버 IP 주소를 사용하여 액세스할 수 있습니다.

Active Directory 자격 증명은 읽기 전용일 수 있지만, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

CIFS 볼륨/파일 공유의 경우 데이터 분류 검사에서 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 쓰기 속성 권한이 있어야 합니다. 가능하다면 Active Directory로 구성된 사용자를 모든 파일에 대한 권한이 있는 조직 내 상위 그룹에 포함하는 것이 좋습니다.

요구 사항

- 회사 사용자를 위해 Active Directory가 이미 설정되어 있어야 합니다.
- Active Directory에 대한 정보가 있어야 합니다.
  - DNS 서버 IP 주소 또는 여러 IP 주소

    또는

  LDAP 서버 IP 주소 또는 여러 IP 주소

- 서버에 접속하기 위한 사용자 이름과 비밀번호
- 도메인 이름(Active Directory 이름)
- 보안 LDAP(LDAPS)를 사용하든 사용하지 않든
- LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)

- 다음 포트는 데이터 분류 인스턴스의 아웃바운드 통신을 위해 열려 있어야 합니다.

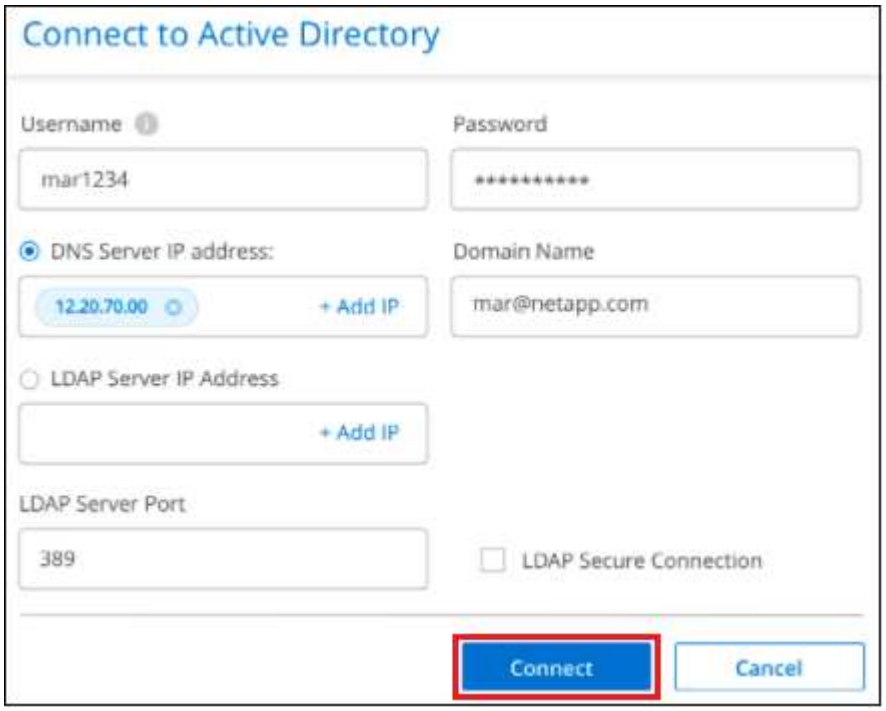
규약	포트	목적지	목적
TCP 및 UDP	389	액티브 디렉토리	LDAP
TCP	636	액티브 디렉토리	SSL을 통한 LDAP
TCP	3268	액티브 디렉토리	글로벌 카탈로그
TCP	3269	액티브 디렉토리	SSL을 통한 글로벌 카탈로그

단계

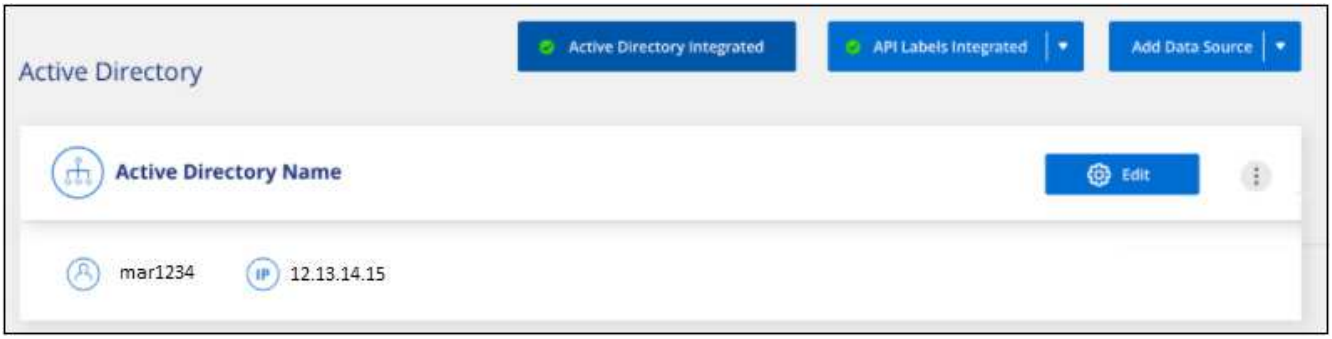
1. 데이터 분류 구성 페이지에서 *Active Directory 추가*를 클릭합니다.

2. Active Directory에 연결 대화 상자에서 Active Directory 세부 정보를 입력하고 *연결*을 클릭합니다.

   필요한 경우 *IP 추가*를 선택하여 여러 개의 IP 주소를 추가할 수 있습니다.



   데이터 분류가 Active Directory에 통합되었으며, 구성 페이지에 새로운 섹션이 추가되었습니다.



Active Directory 통합 관리

Active Directory 통합에서 값을 수정해야 하는 경우 편집 버튼을 클릭하고 변경합니다.

통합을 선택하여 삭제할 수도 있습니다. 버튼을 클릭한 다음 *Active Directory 제거*를 클릭합니다.

데이터 분류 사용

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

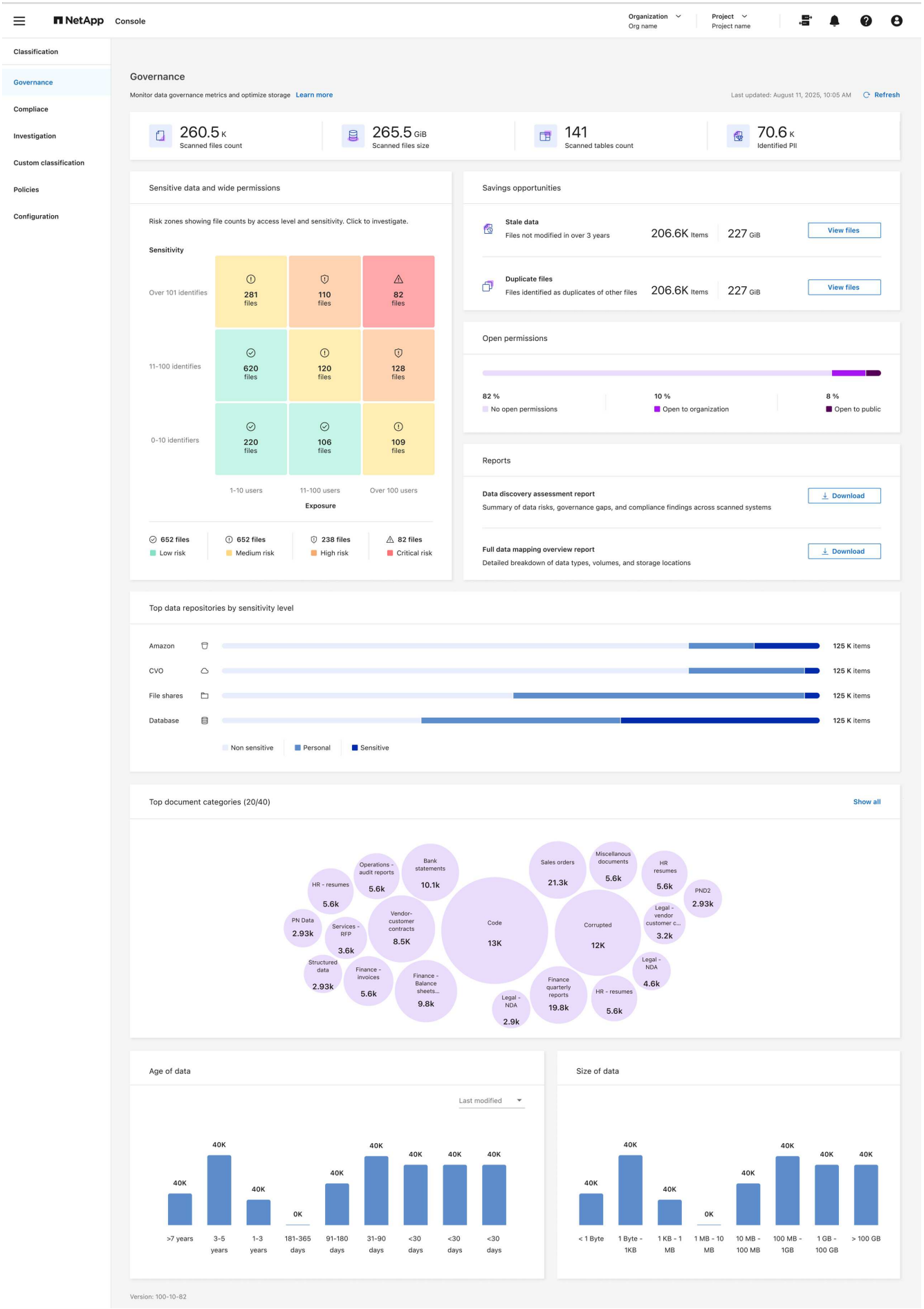
조직의 스토리지 리소스에 있는 데이터와 관련된 비용을 제어하세요. NetApp Data Classification 시스템에서 오래된 데이터, 중복 파일, 매우 큰 파일의 양을 파악하여 일부 파일을 제거할지 아니면 비용이 덜 드는 개체 스토리지로 계층화할지 결정할 수 있도록 도와줍니다.

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 - 3년 전에 마지막으로 수정된 데이터입니다.
   - 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.

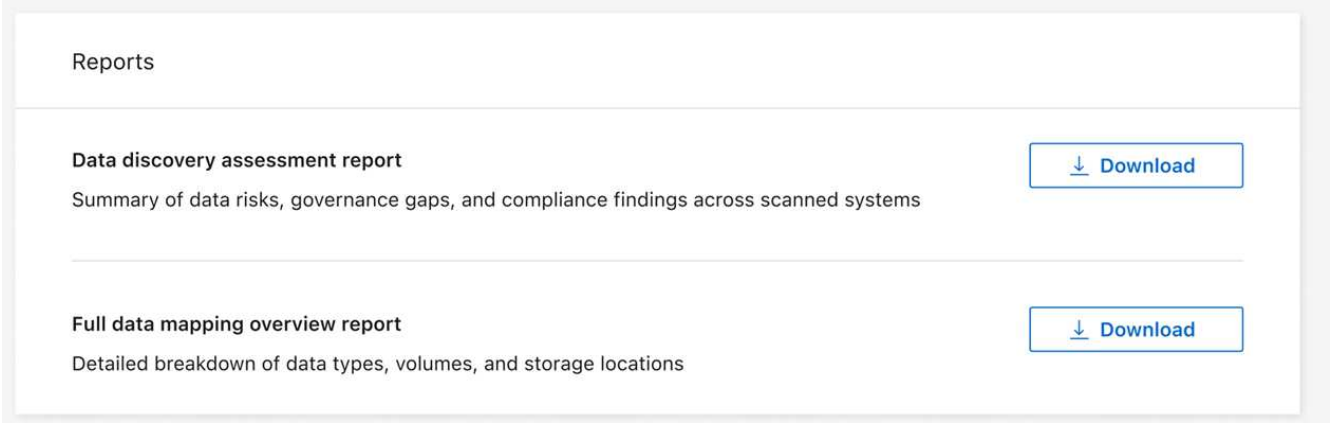
보고서를 사용하면 다음과 같은 작업을 수행할 수 있습니다.

- 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

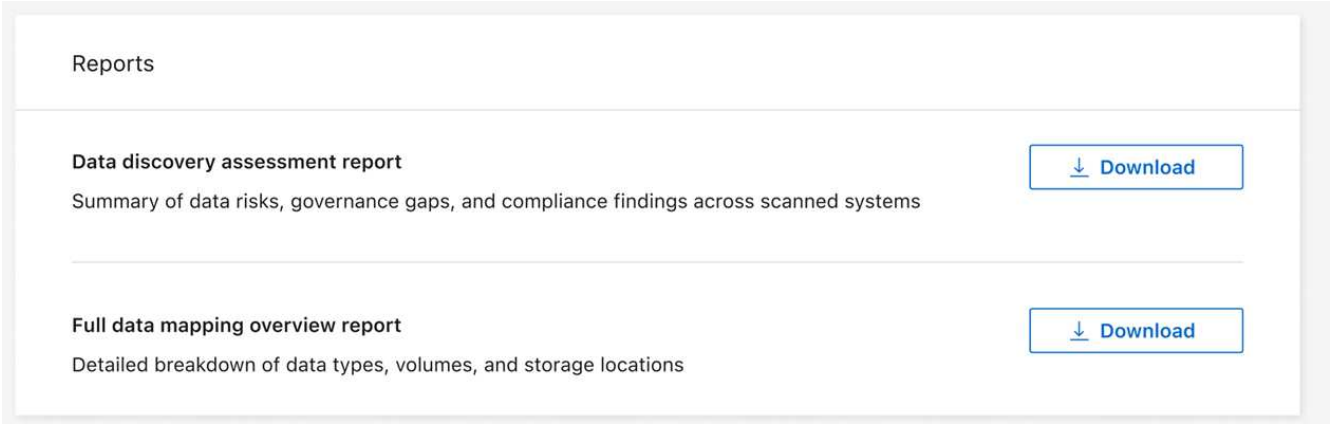
데이터 매핑 개요 보고서는 마이그레이션, 백업, 보안 및 규정 준수 프로세스에 대한 결정을 내리는 데 도움이 되도록 회사 데이터 소스에 저장된 데이터에 대한 개요를 제공합니다. 이 보고서는 모든 시스템과 데이터 소스를 요약합니다. 또한 각 시스템에 대한 분석도 제공합니다.

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.

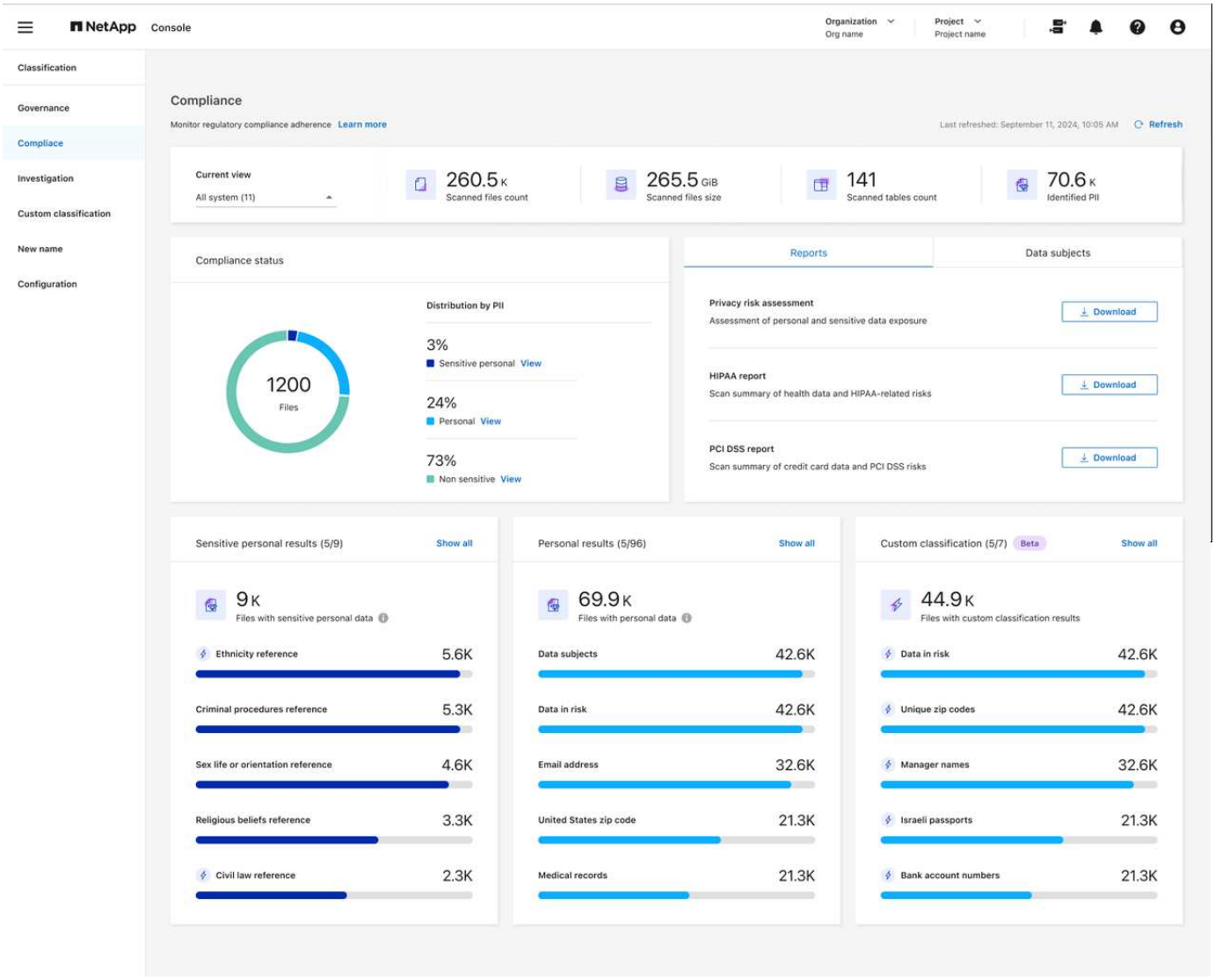
데이터 소스 중 하나라도 데이터 계층화를 구현하는 경우 개체 스토리지에 이미 있는 오래된 데이터는 데이터 연령 그래프에서 식별될 수 있습니다.

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.

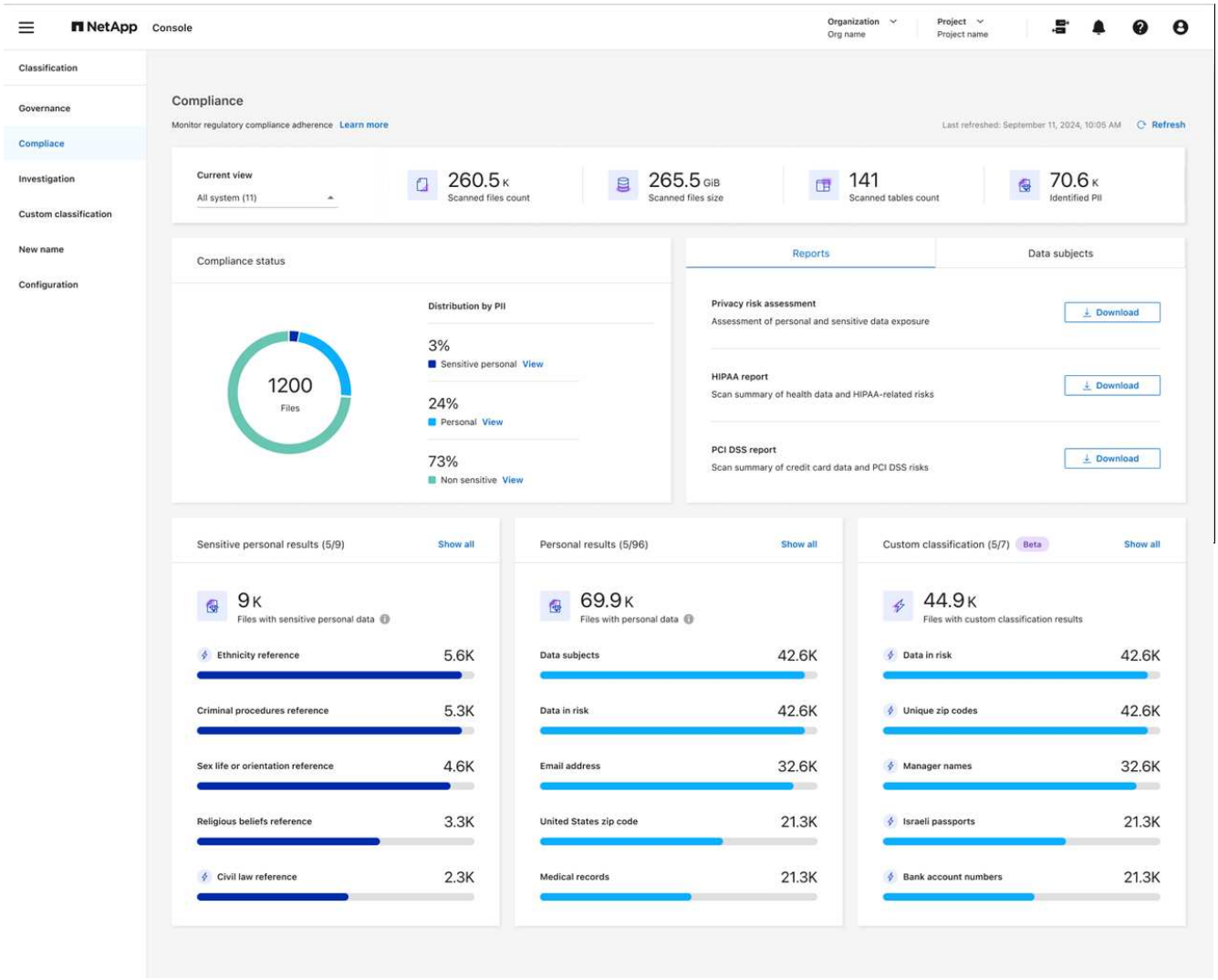
귀하의 조직과 관련된 개인 데이터를 식별하기 위해 사용자 정의 검색어를 만들 수도 있습니다. 자세한 내용은 다음을 참조하세요. "사용자 정의 분류 만들기" .

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.

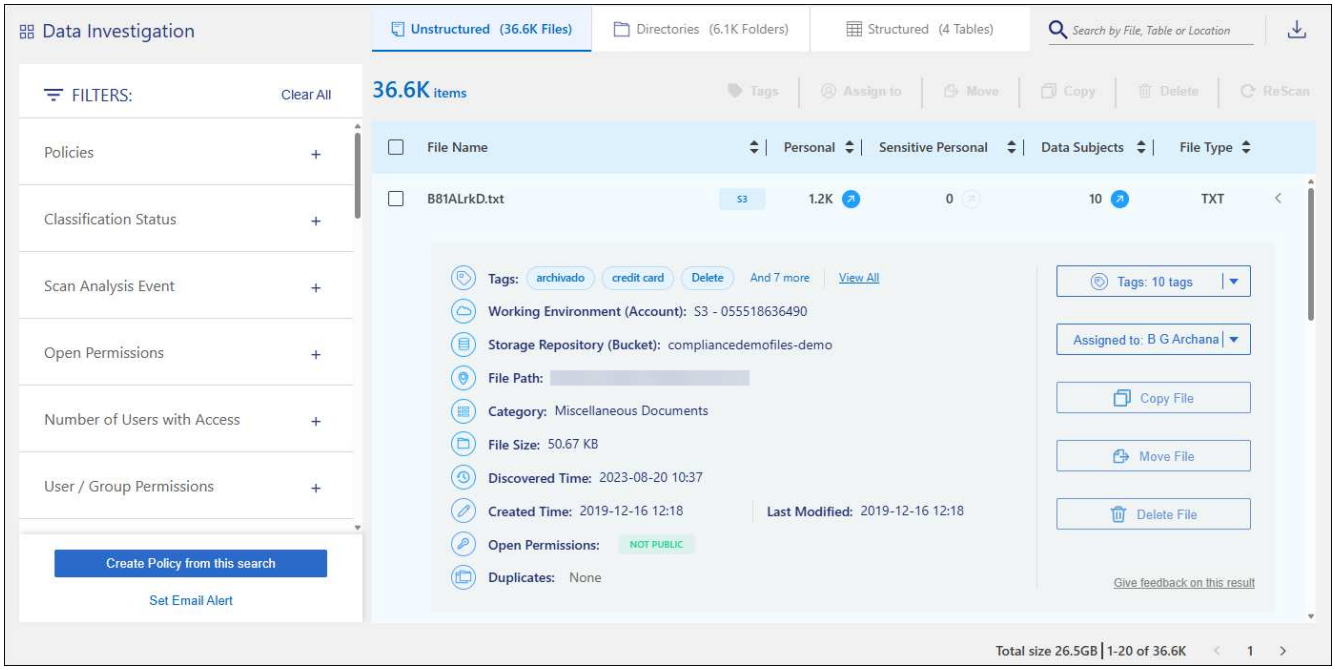
2. 모든 개인 데이터의 세부 정보를 조사하려면 개인 데이터 비율 옆에 있는 아이콘을 선택하세요.

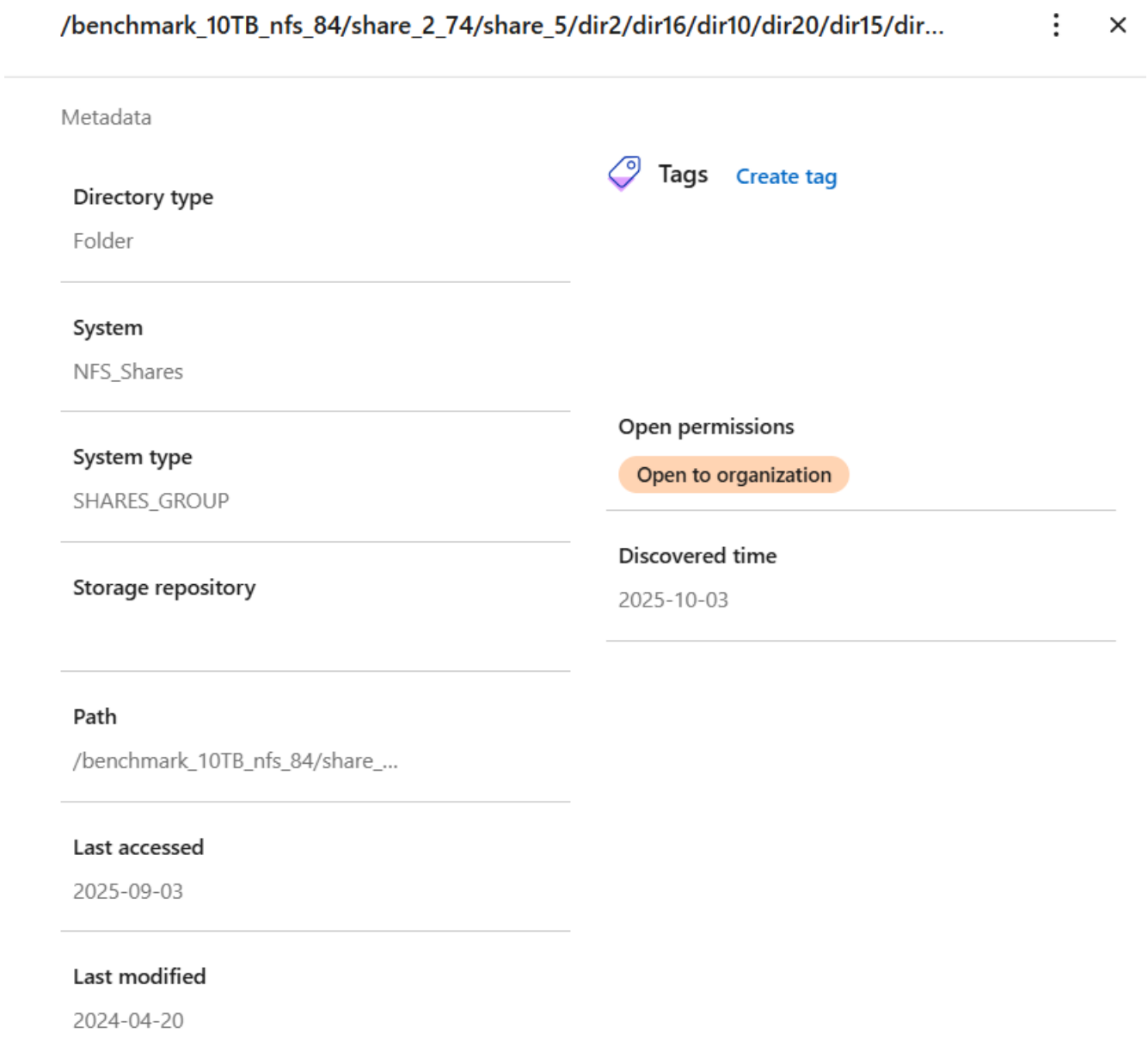


3. 특정 유형의 개인 데이터에 대한 세부 정보를 조사하려면 모두 보기*를 선택한 다음 특정 유형의 개인 데이터(예: 이메일 주소)에 대한 *조사 결과 화살표 아이콘을 선택합니다.

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.

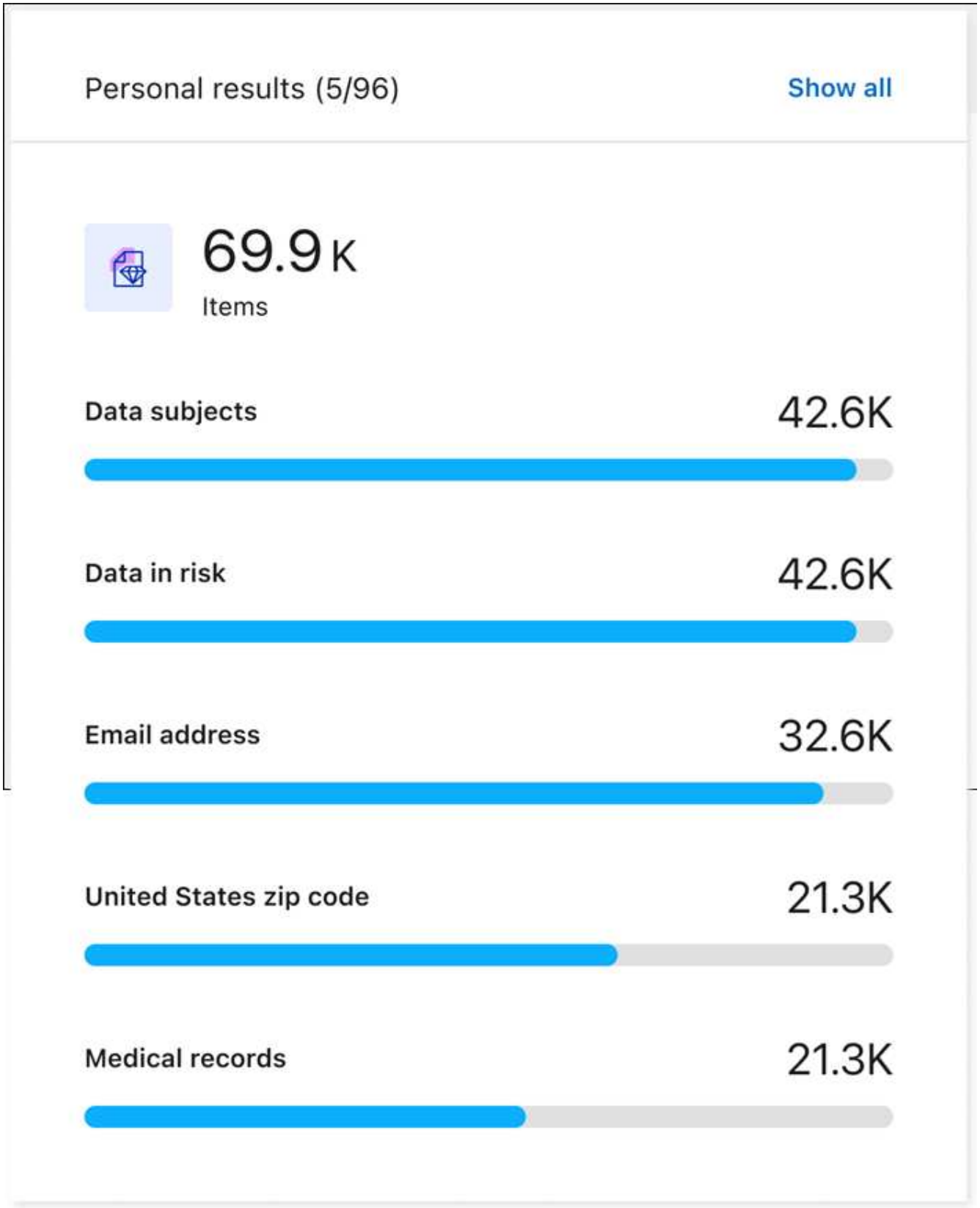
데이터 분류는 AI, 자연어 처리(NLP), 머신 러닝(ML), 인지 컴퓨팅(CC)을 사용하여 스캔하는 콘텐츠의 의미를 이해하고 엔터티를 추출하여 그에 따라 분류합니다.

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 사용하면 민감한 정보에 대한 사용자 정의 검색을 만들 수 있습니다. 검색 범위는 정규 표현식(regex)으로 지정될 수 있습니다.

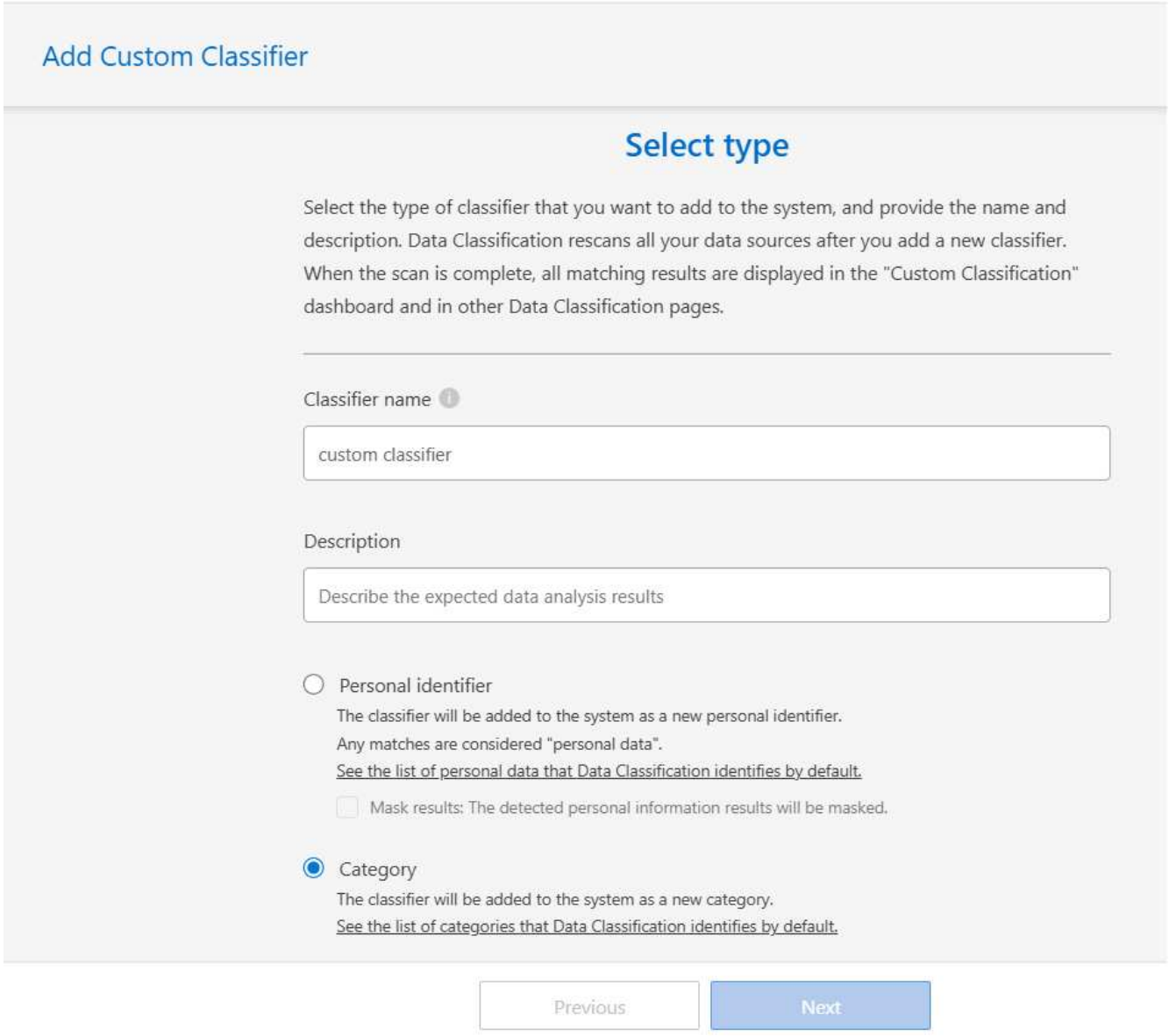
사용자 정의 분류 만들기

사용자 정의 분류는 매핑 전용 스캔이 아닌 맵 및 분류 스캔에만 사용할 수 있습니다. 이 기능은 현재 미리보기 단계에 있습니다.

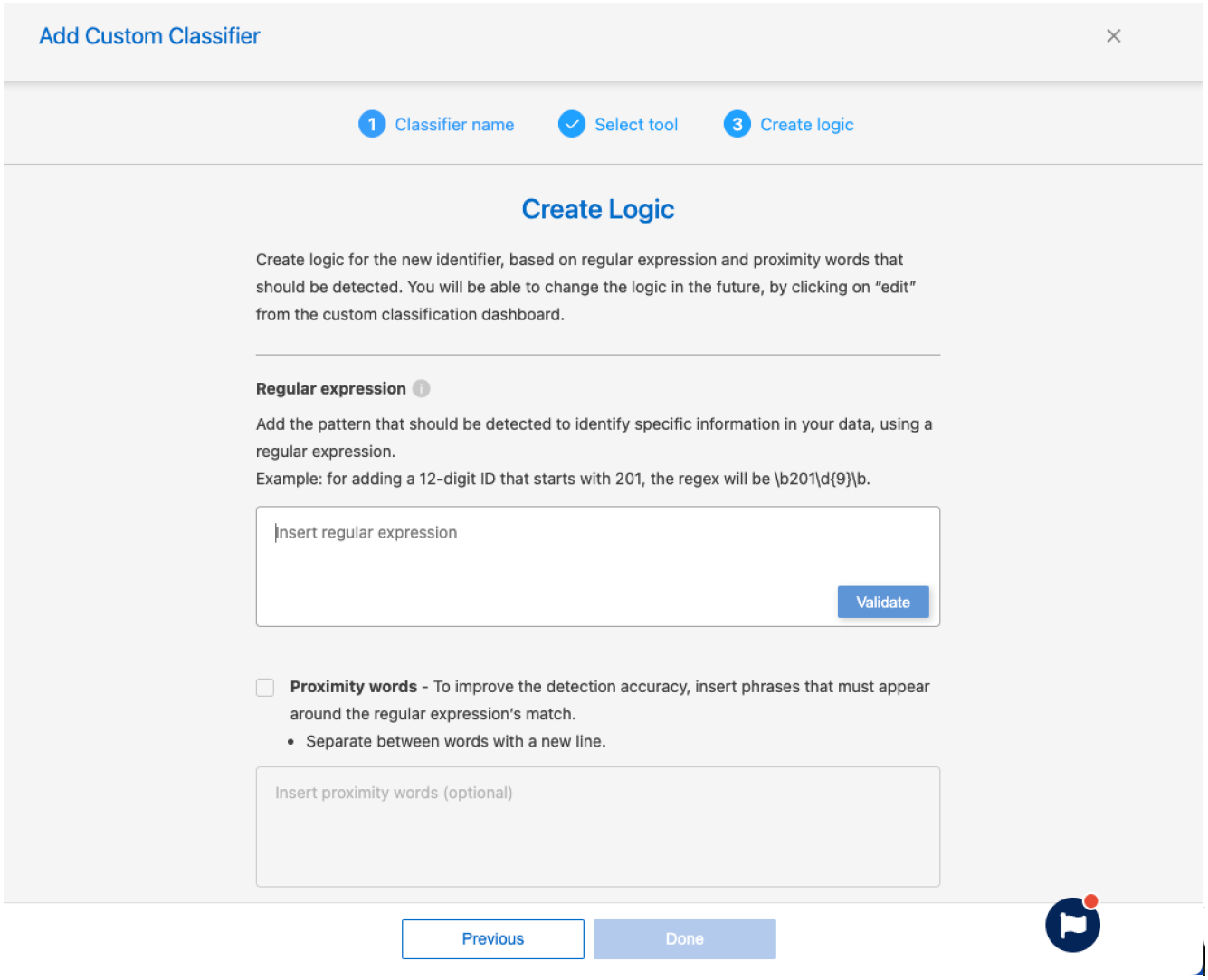
단계

1. 사용자 정의 분류 탭을 선택합니다.
2. 새로운 분류자 추가 버튼을 선택합니다.

3. 새로운 분류기에 대한 분류기 이름과 설명을 추가합니다.
4. 분류자를 개인 식별자 또는 *범주*로 추가하도록 선택합니다.



5. *다음*을 선택하세요.
6. 사용자 정의를 정규 표현식으로 추가하려면 사용자 정의 정규 표현식을 선택한 후 다음을 선택합니다.
7. 데이터의 특정 정보를 감지하기 위한 패턴을 추가합니다. 검증을 선택하여 항목의 구문을 확인하세요
.



8. 완료를 선택하여 사용자 정의 분류를 만듭니다.

새로운 사용자 정의는 다음 예약된 스캔에서 캡처됩니다. 결과를 보려면 다음을 참조하세요.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

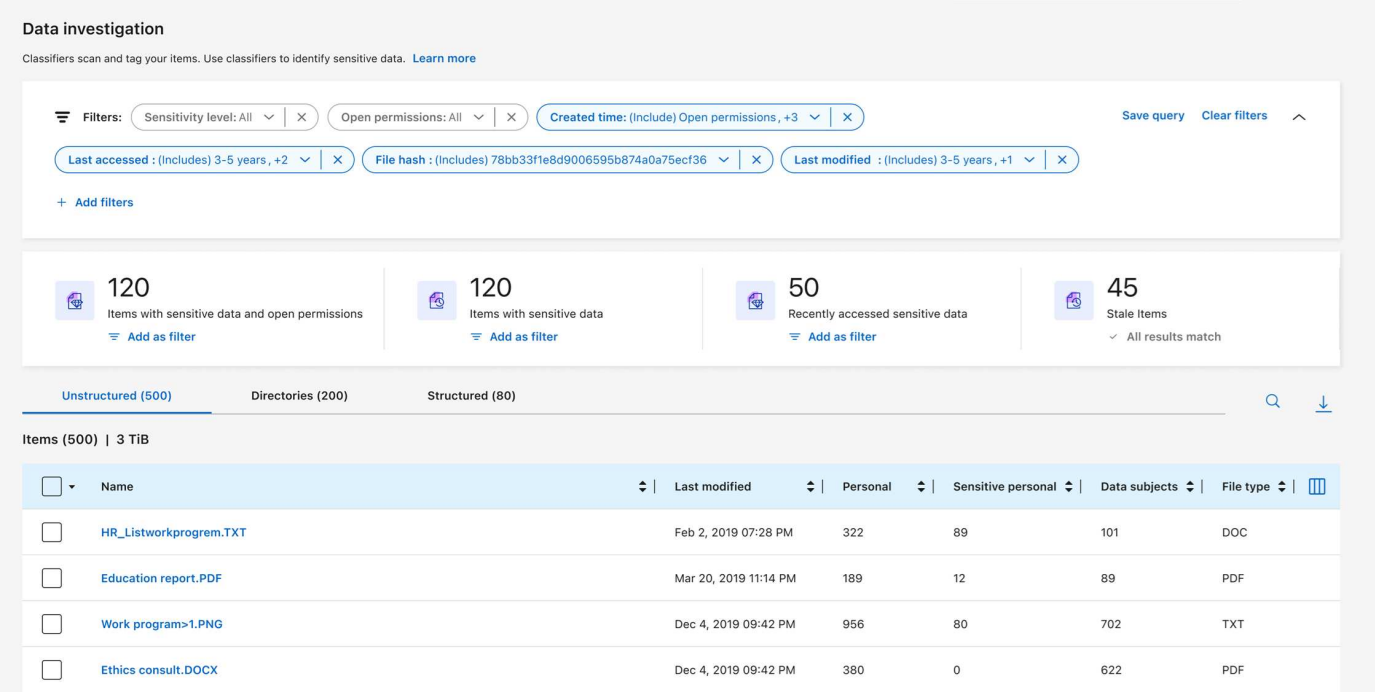
데이터 조사 페이지는 데이터를 세 개의 탭으로 분류합니다.

- 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" .

필터	세부
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.
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.

필터	세부
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.
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.

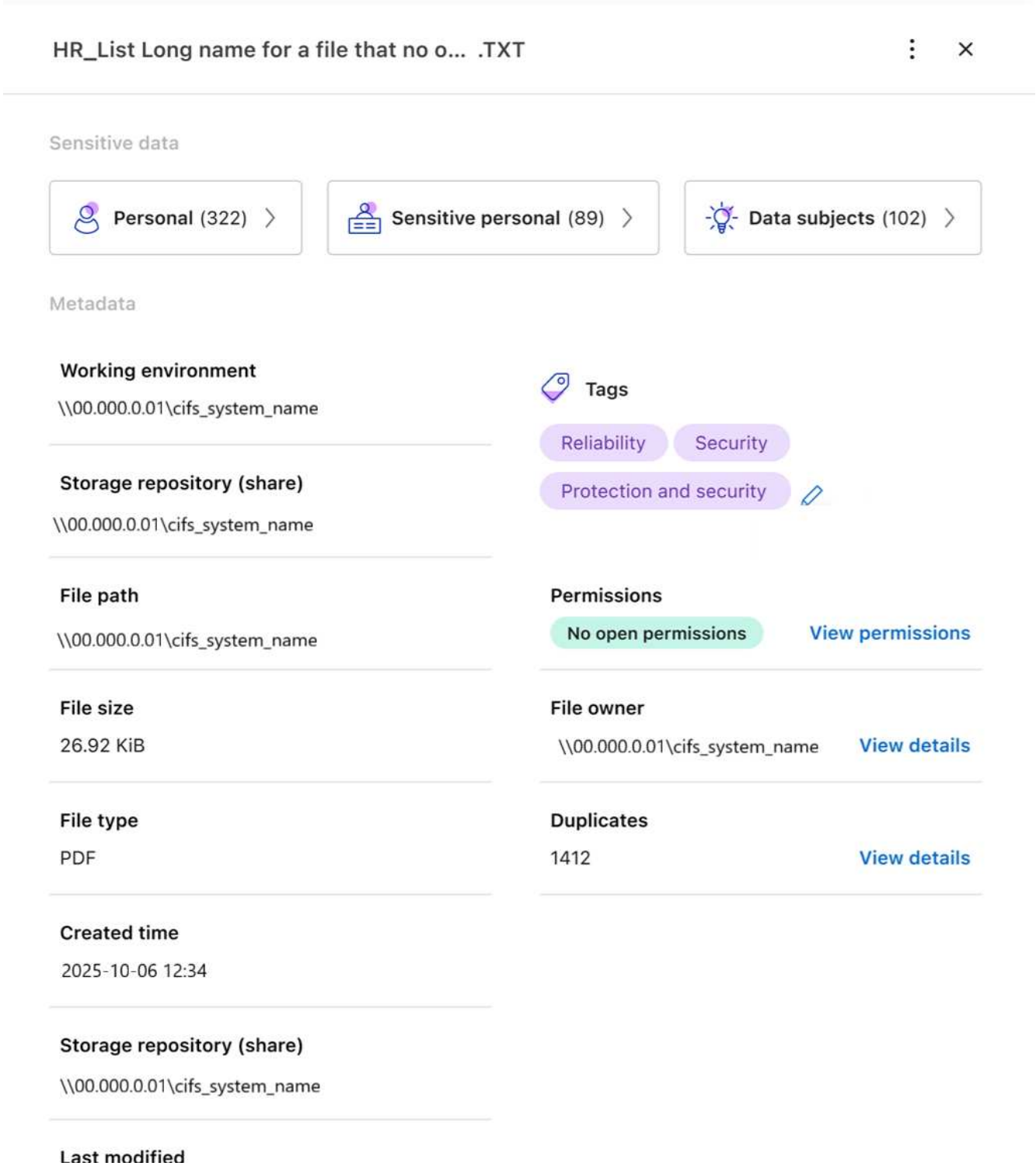
파일 메타데이터 보기

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.

1MB 이상이거나 개인 정보나 민감한 개인 정보가 포함된 모든 파일(데이터베이스 제외)을 비교하여 중복이 있는지 확인합니다.

데이터 분류는 해싱 기술을 사용하여 중복 파일을 확인합니다. 어떤 파일이 다른 파일과 동일한 해시 코드를 가지고 있다면, 파일 이름이 다르더라도 그 파일이 정확히 중복된 파일이라는 것을 100% 확신할 수 있습니다.

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

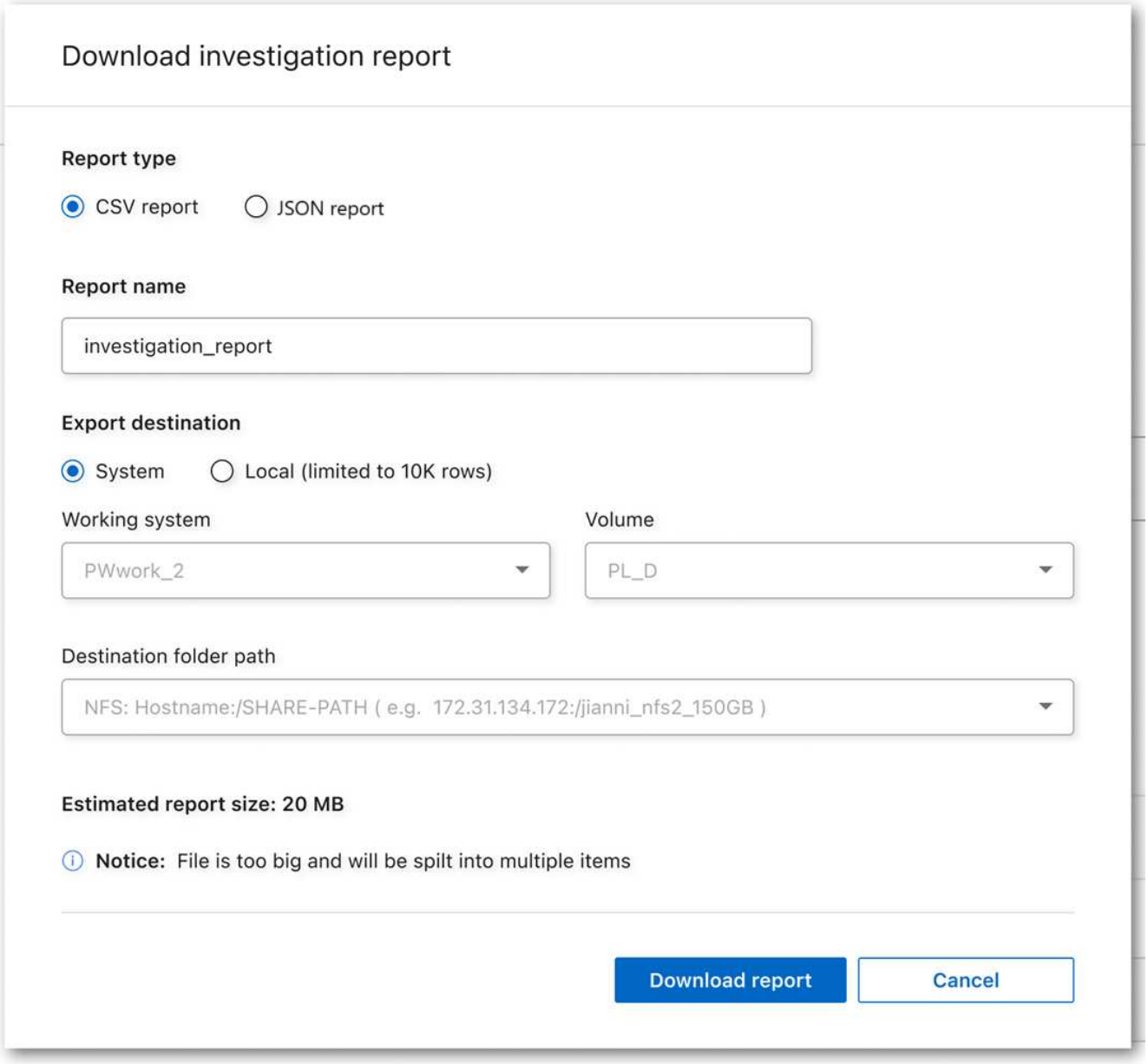
보고서 생성 단계

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.



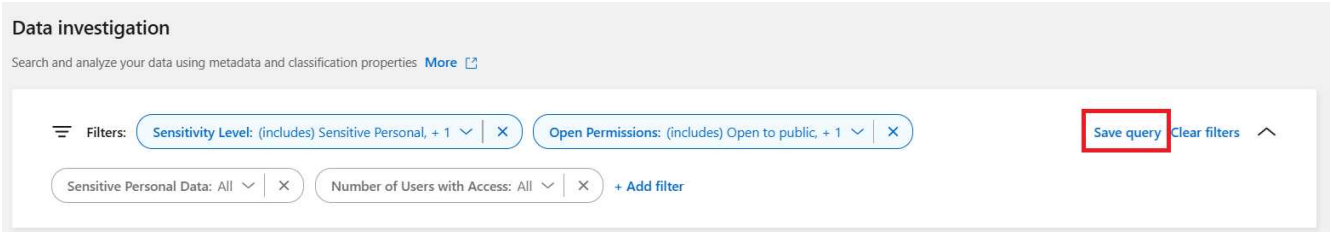
결과

보고서를 다운로드 중이라는 메시지가 대화 상자에 표시됩니다.

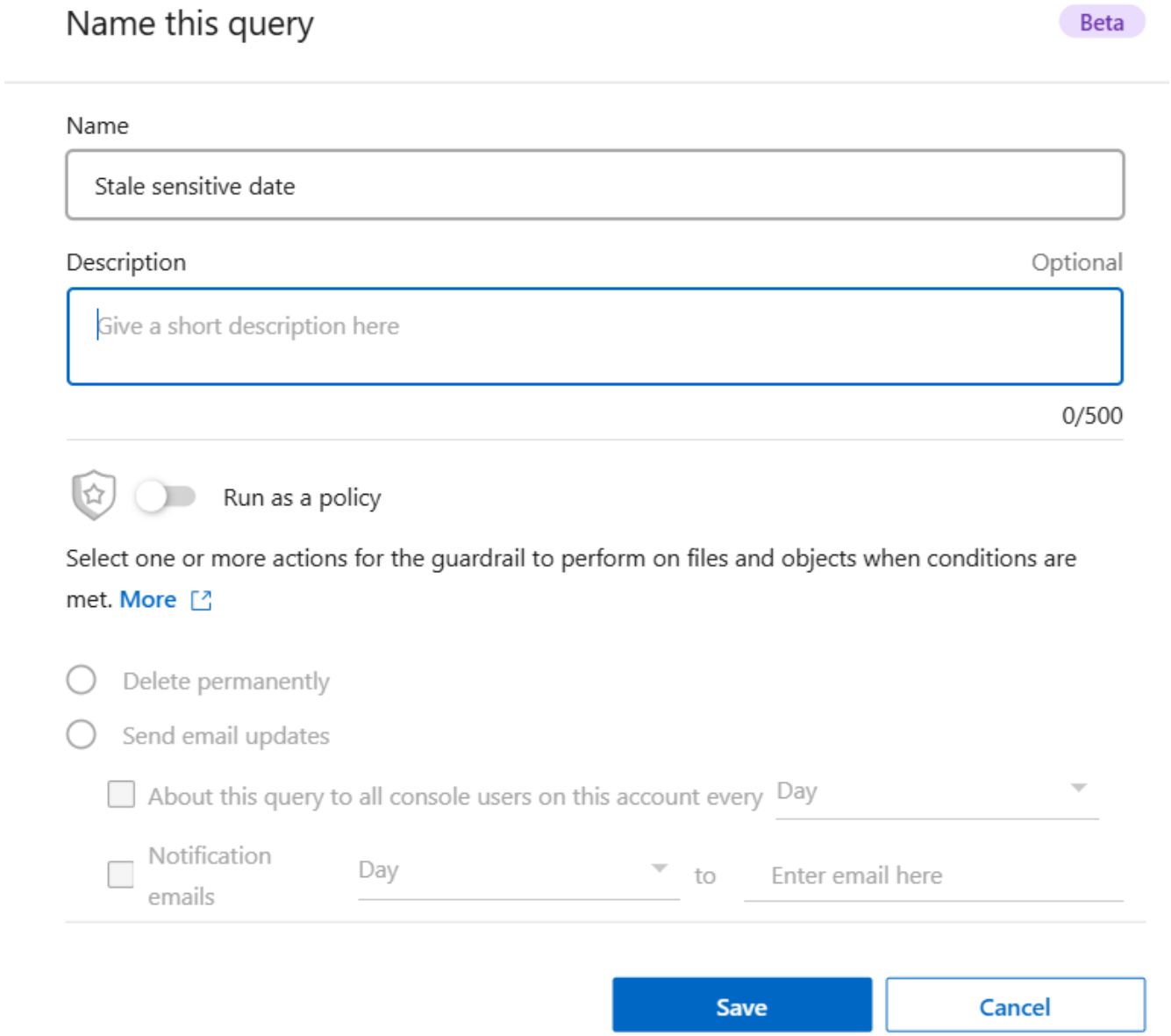
선택한 필터를 기반으로 저장된 쿼리를 만듭니다.

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.

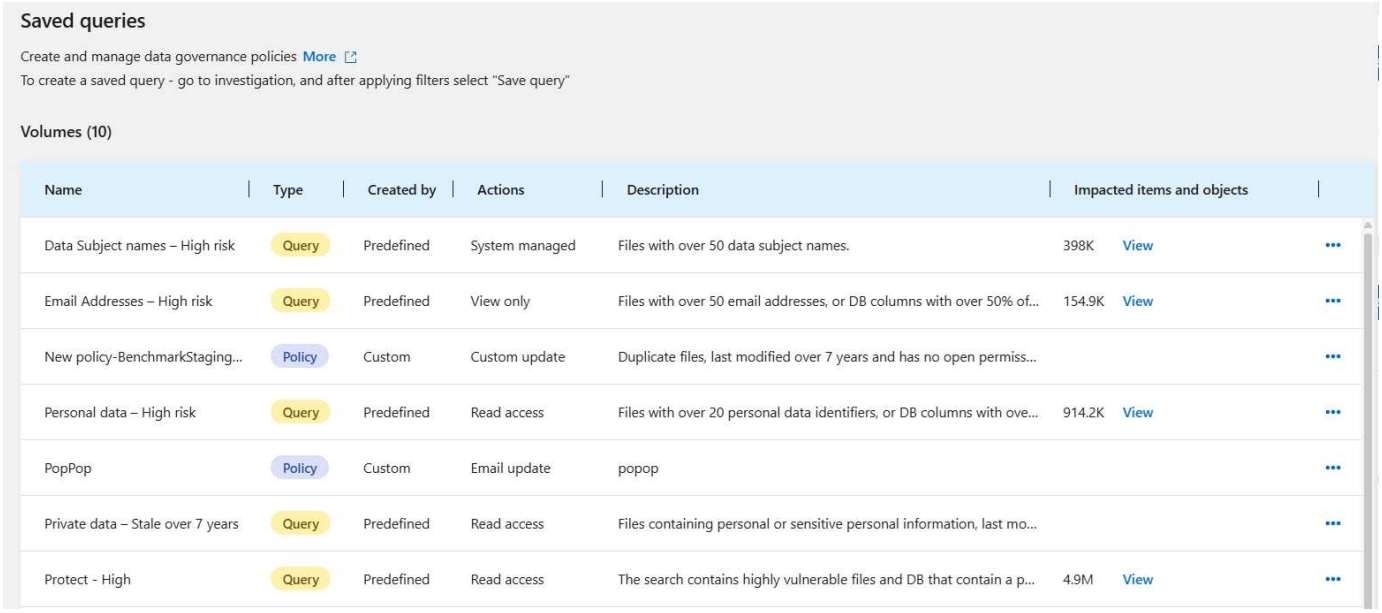
NetApp Data Classification 사용하여 저장된 쿼리 관리

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

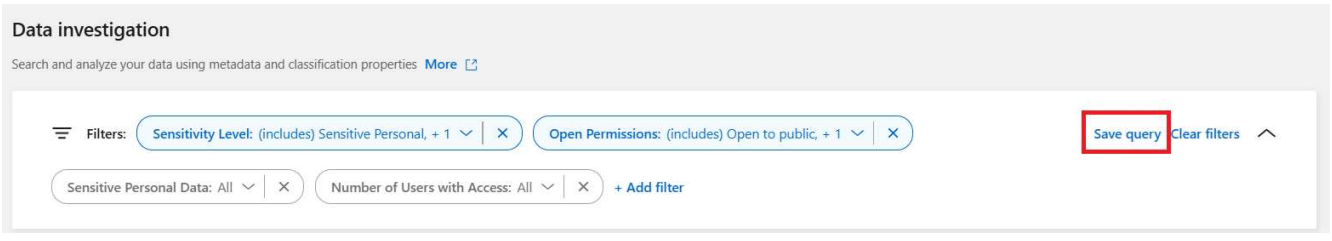
조사 페이지에서 저장된 쿼리에 대한 결과를 표시하려면 다음을 선택하십시오. 특정 검색에 대한 버튼을 클릭한 다음 *결과 조사*를 선택하세요.

저장된 쿼리 및 정책 생성

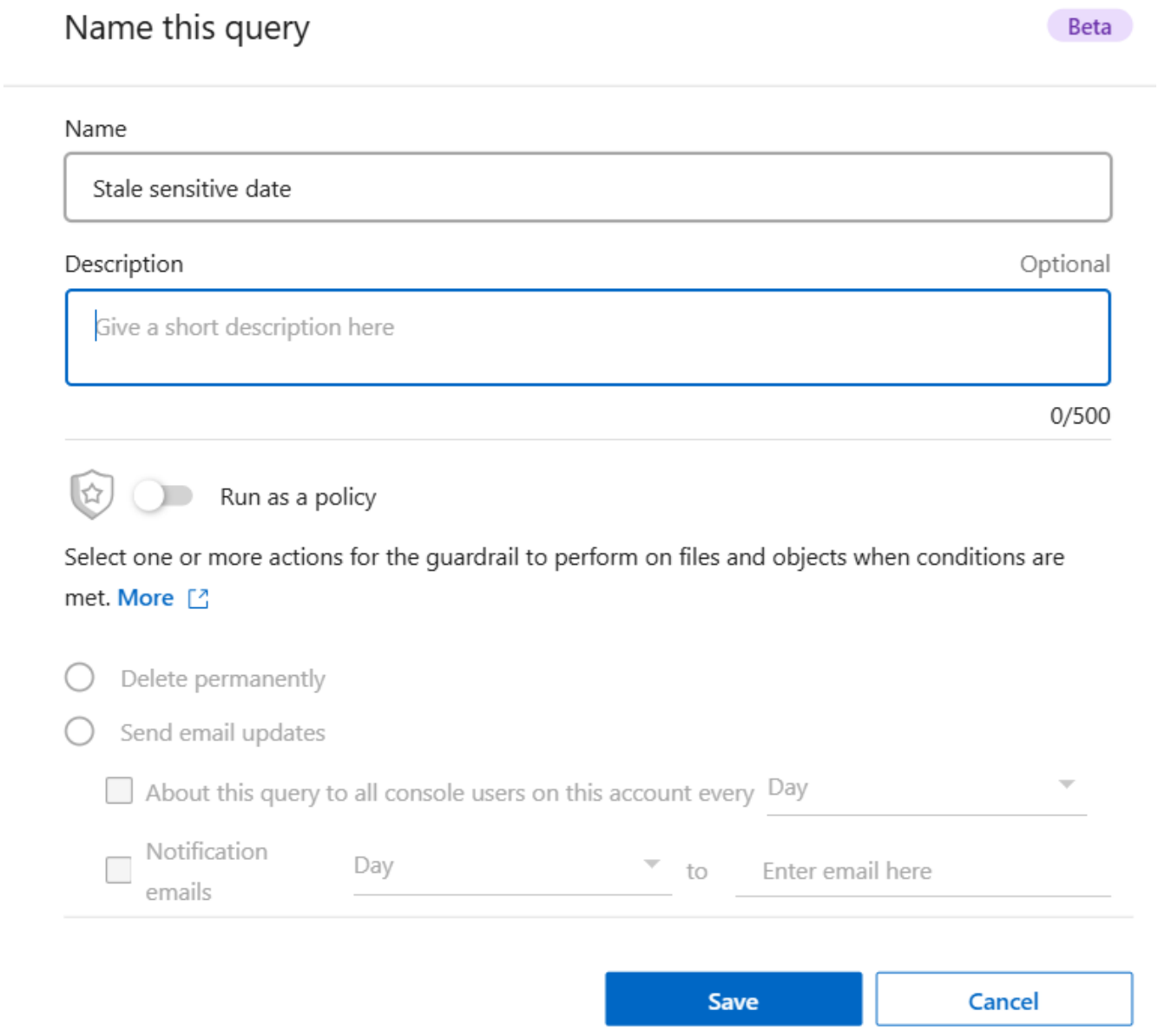
귀하의 조직에 맞는 특정 쿼리에 대한 결과를 제공하는 사용자 정의 저장된 쿼리를 만들 수 있습니다. 검색 기준과 일치하는 모든 파일과 디렉토리(공유 및 폴더)에 대한 결과가 반환됩니다.

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.

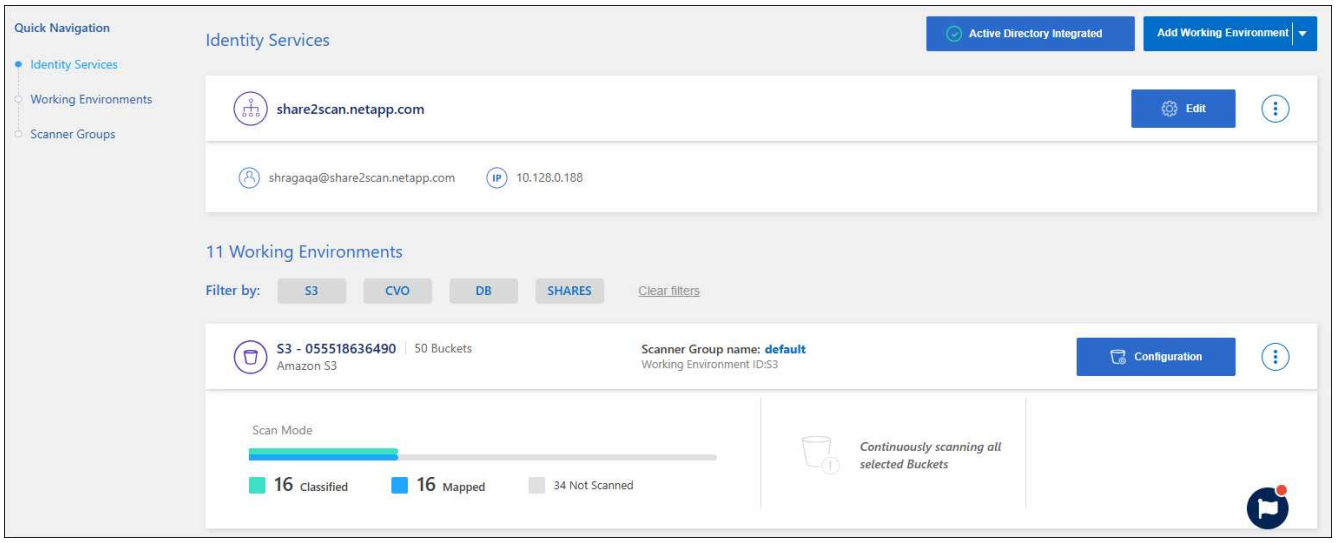
각 작업 환경의 스캐닝 상태는 구성 페이지에서 볼 수 있습니다.

- 초기화 (밝은 파란색 점): 지도 또는 분류 구성이 활성화되었습니다. 이는 "대기 대기열" 상태가 시작되기 전 몇 초 동안 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 중지하려면 "일시 중지" 옵션을 선택했습니다. 볼륨의 변화는 시스템에 표시되지 않지만, 스캔된 통찰력은 여전히 표시됩니다.
- 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.

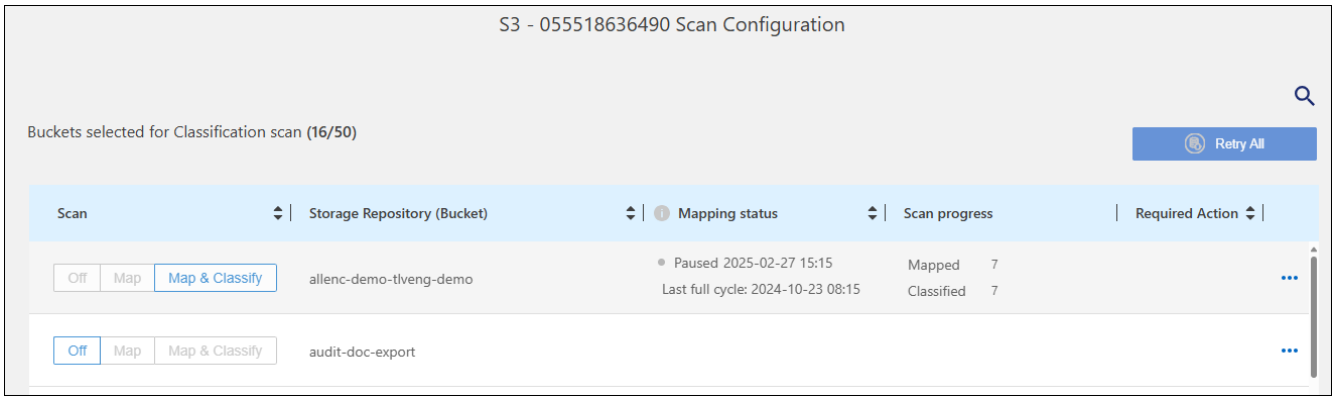
- 스캔 안 함: 볼륨 구성이 "끄기"로 선택되어 시스템이 볼륨을 스캔하지 않습니다.

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. 매핑 상태 열의 차트 위에 커서를 올려 놓으면 각 저장소(이 예에서는 버킷)에서 매핑 또는 분류되어야 하는 파일 수가 표시됩니다.

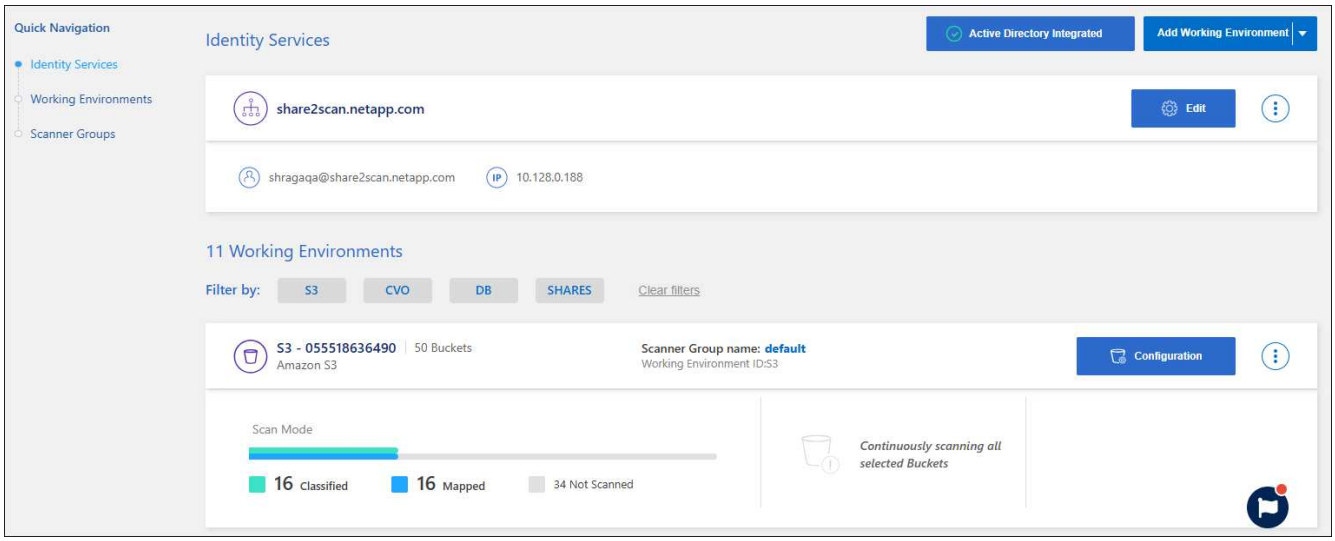
저장소 스캐닝 유형 변경

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.

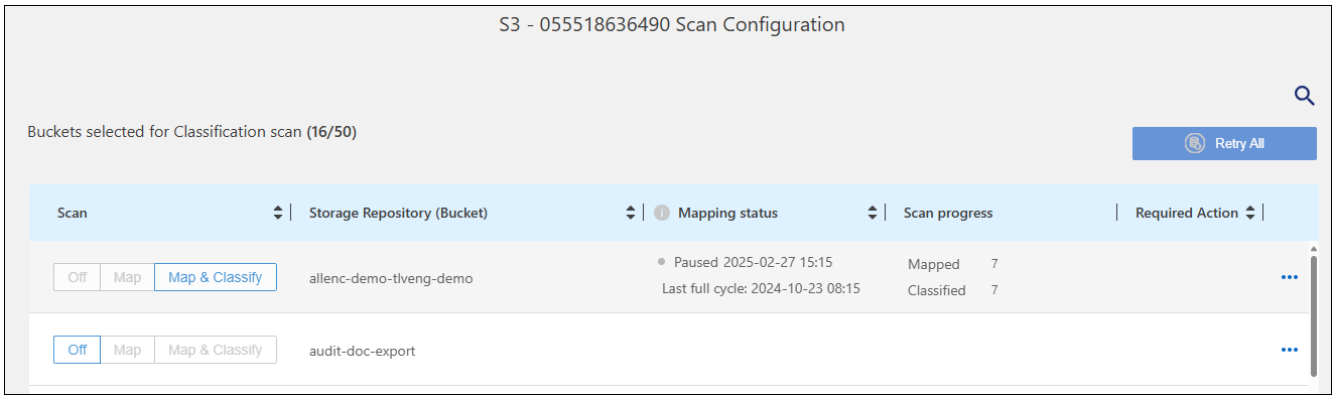
데이터베이스는 매핑 전용 스캔으로 설정할 수 없습니다. 데이터베이스 스캐닝은 켜거나 끌 수 있습니다. 켜짐은 맵 및 분류와 동일합니다.

단계

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

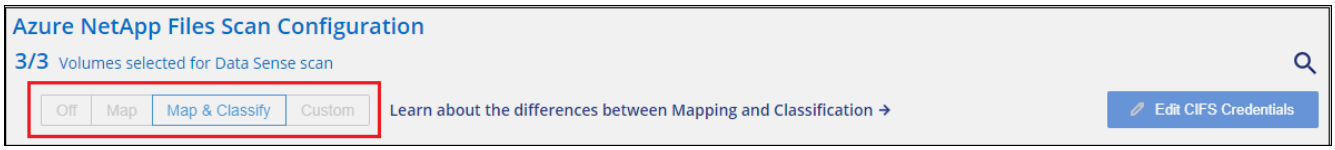


3. 스캔 구성 페이지에서 저장소(이 예에서는 버킷)를 변경하여 매핑 또는 매핑 및 분류 스캔을 수행합니다.



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

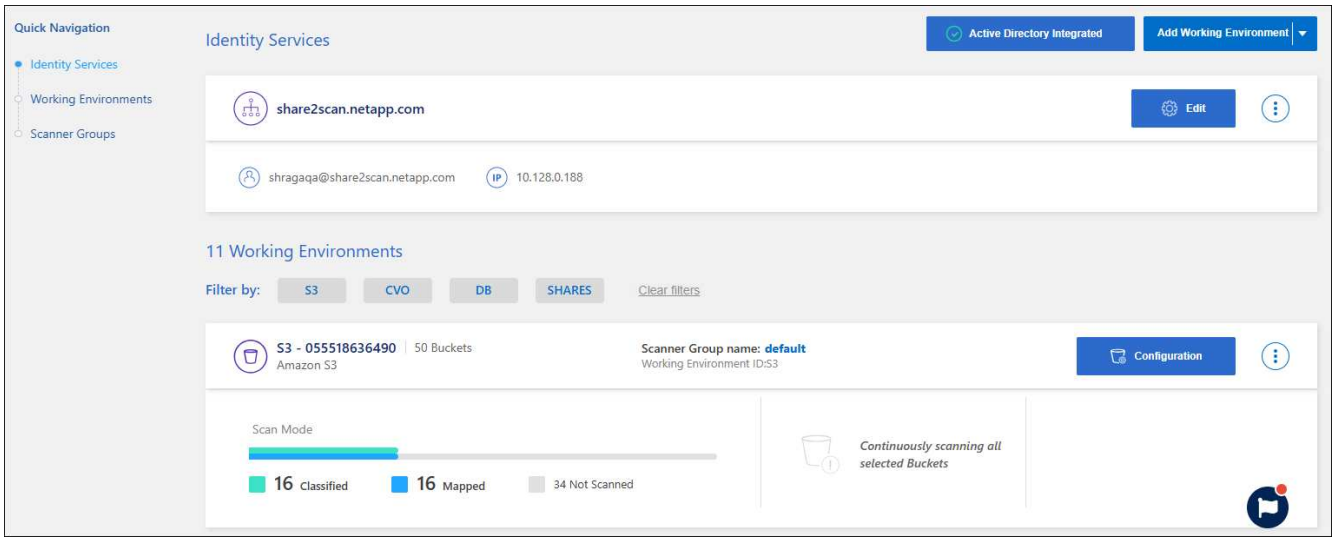
1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 우선순위를 지정할 리소스를 선택하세요.
3. 행동으로부터 ... 옵션에서 *스캔 우선 순위*를 선택하세요.

저장소 스캔 중지

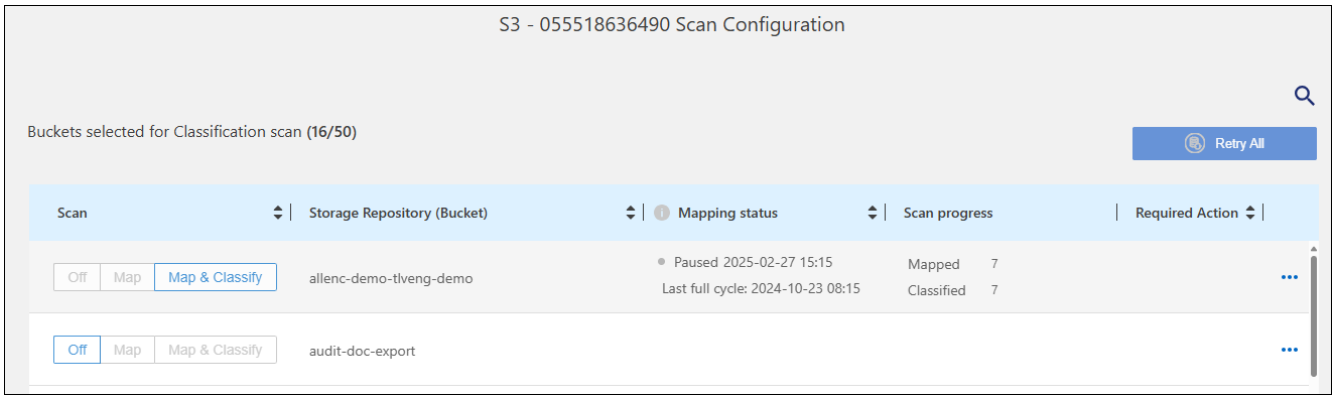
더 이상 규정 준수 여부를 모니터링할 필요가 없으면 저장소(예: 볼륨) 스캔을 중지할 수 있습니다. 스캐닝을 "끄면" 됩니다. 스캐닝을 끄면 해당 볼륨에 대한 모든 인덱싱 및 정보가 시스템에서 제거되고, 데이터 스캐닝에 대한 요금 청구도 중단됩니다.

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

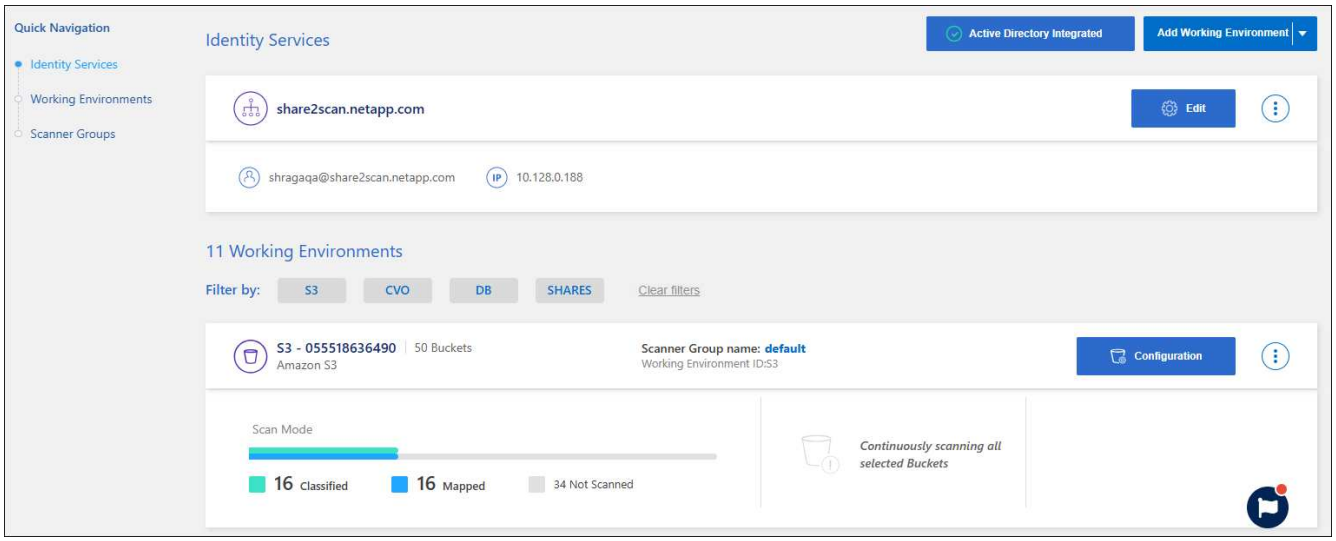
특정 콘텐츠 스캔을 일시적으로 중지하려면 저장소에서 스캔을 "일시 중지"할 수 있습니다. 스캐닝을 일시 중지하면 데이터 분류가 저장소의 변경 사항이나 추가 사항에 대해 향후 스캐닝을 수행하지 않지만, 현재 결과는 모두 시스템에

계속 표시됩니다. 스캔을 일시 중지해도 스캔한 데이터에 대한 요금 청구는 중단되지 않습니다. 왜냐하면 데이터는 여전히 존재하기 때문입니다.

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.

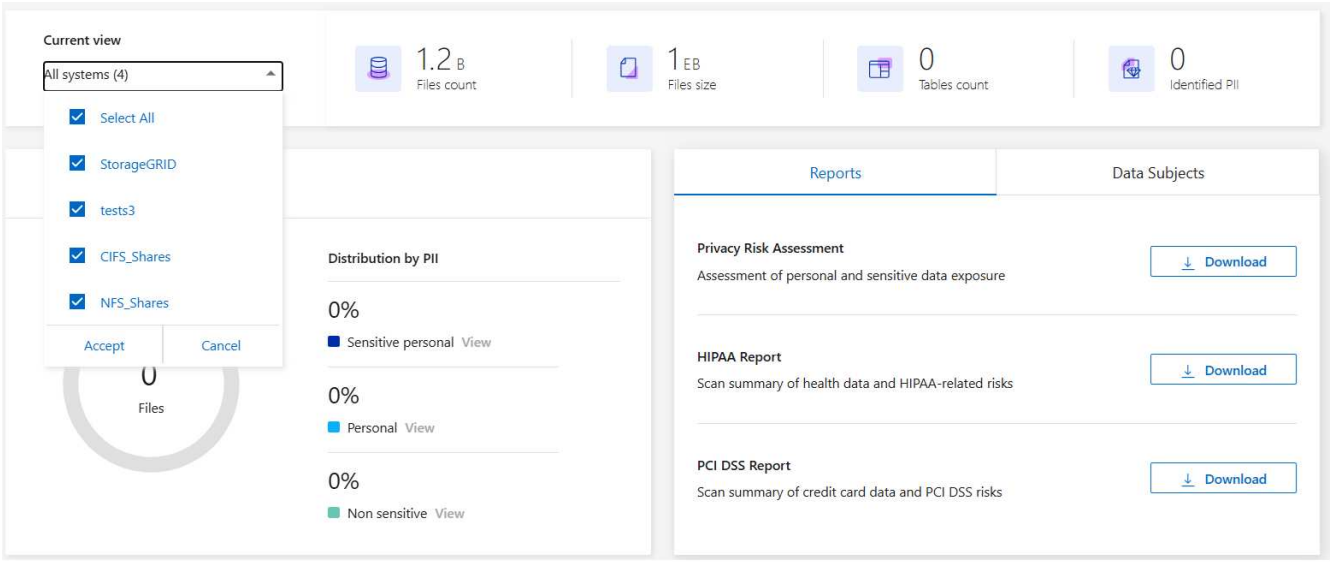
보고서를 위한 시스템을 선택하세요

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.

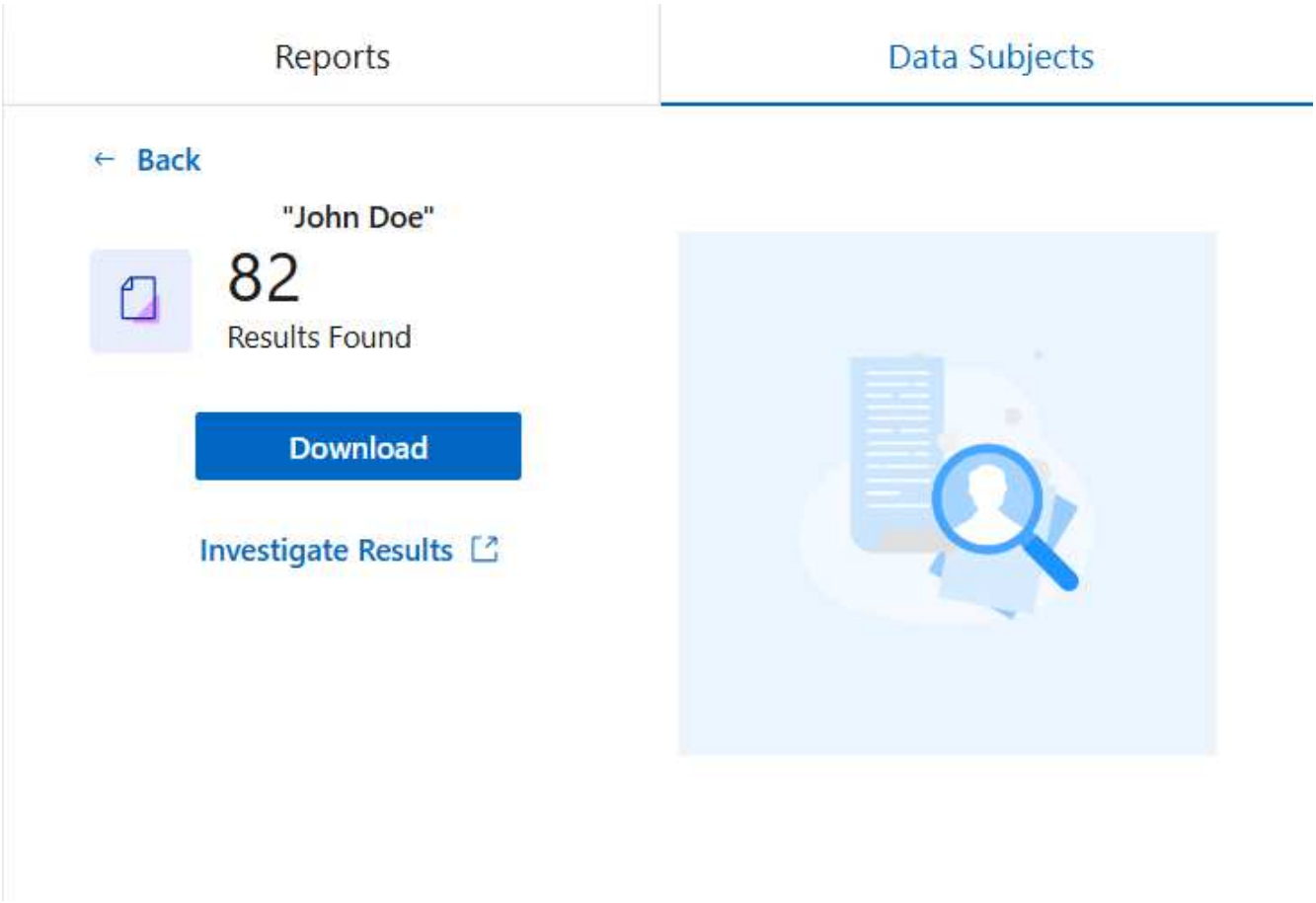
데이터 주체 검색 및 보고서 다운로드

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.

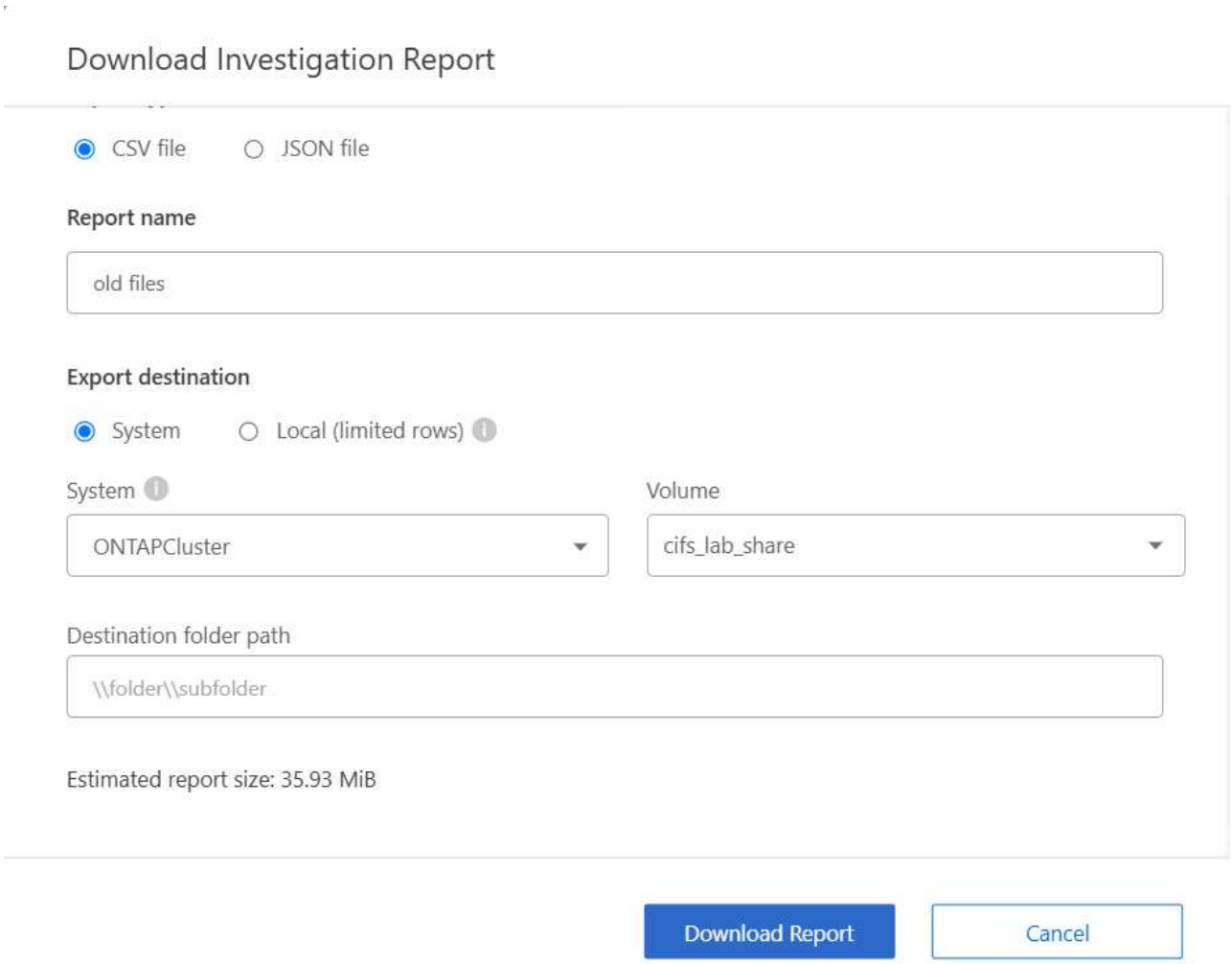
      - 영화 형식을 선택하세요: CSV 또는 JSON
      - *보고서 이름*을 입력하세요
      - 내보내기 대상을 선택하세요: 시스템 또는 로컬 컴퓨터.

        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.

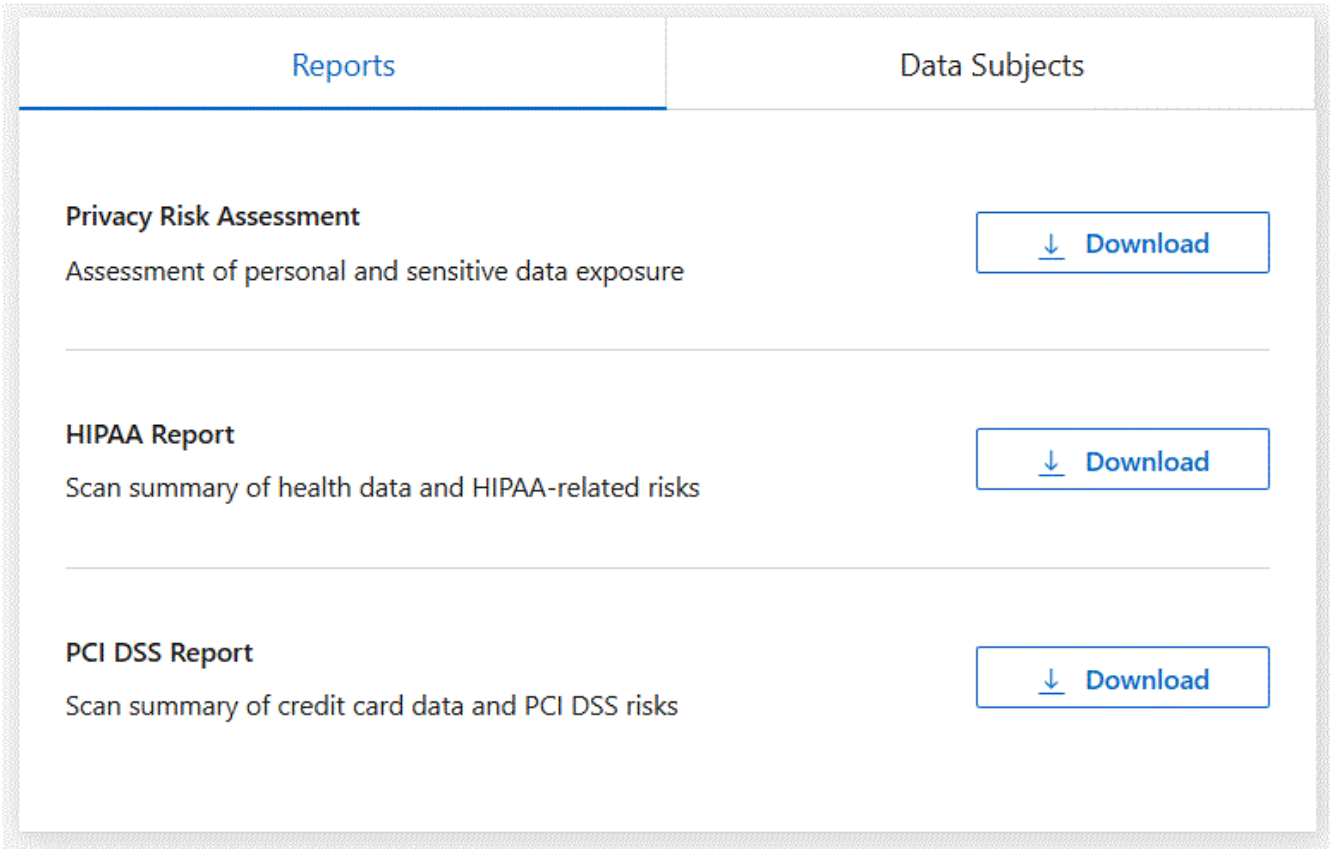
- 보존 기간: 파일이 마지막으로 수정된 기간입니다. 이는 건강 정보를 처리하는 데 필요한 기간 이상으로 보관하면 안 되기 때문에 유용합니다.
- 건강 정보 배포: 건강 정보가 발견된 시스템과 암호화 및 랜섬웨어 보호가 활성화되어 있는지 여부.

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.

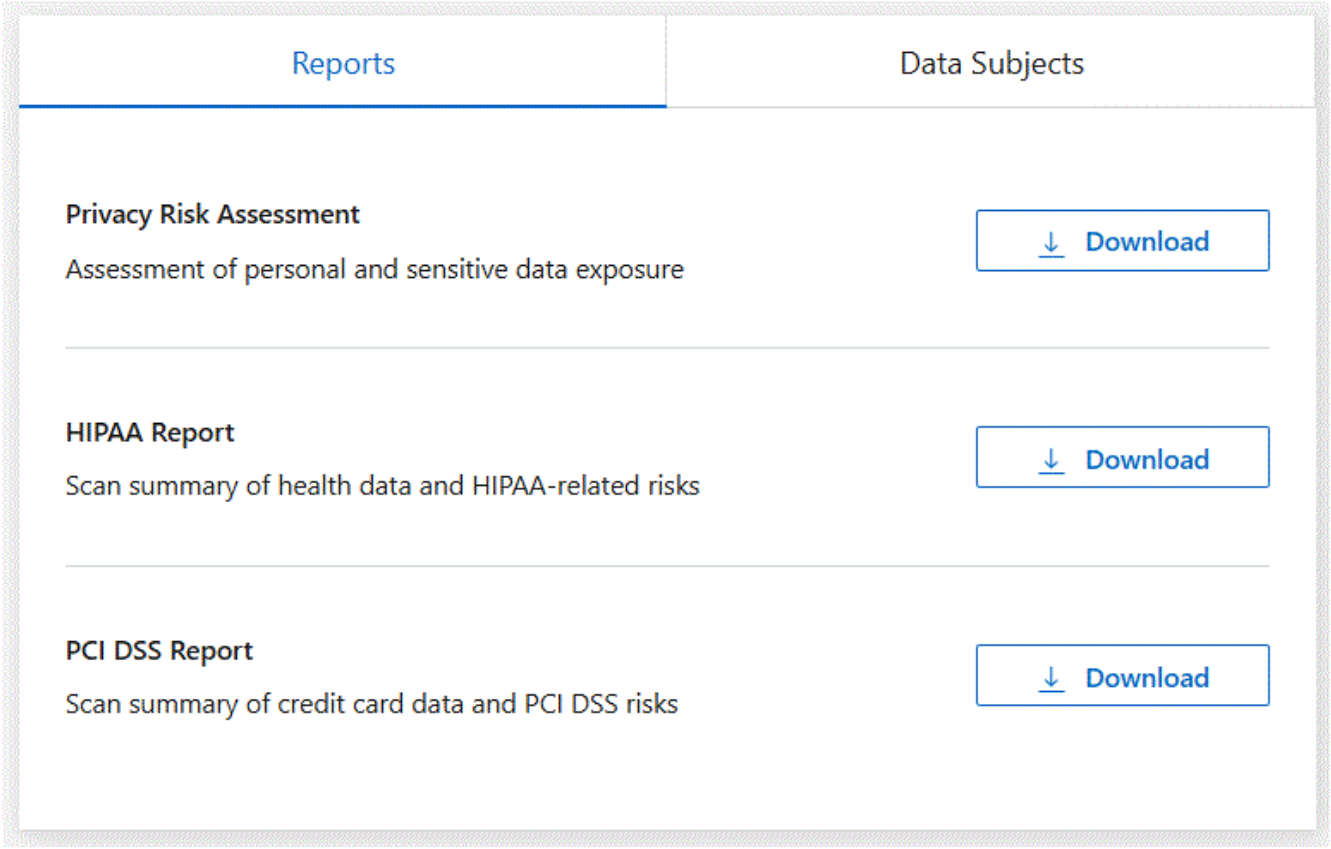
- 랜섬웨어 보호: 랜섬웨어 보호가 활성화되어 있거나 활성화되어 있지 않은 시스템에 있는 신용카드 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP 에만 해당됩니다.
- 보존 기간: 파일이 마지막으로 수정된 기간입니다. 이는 신용카드 정보를 처리하는 데 필요한 기간 이상으로 보관하면 안 되기 때문에 유용합니다.
- 신용카드 정보 배포: 신용카드 정보가 발견된 시스템과 암호화 및 랜섬웨어 보호가 활성화되어 있는지 여부.

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)

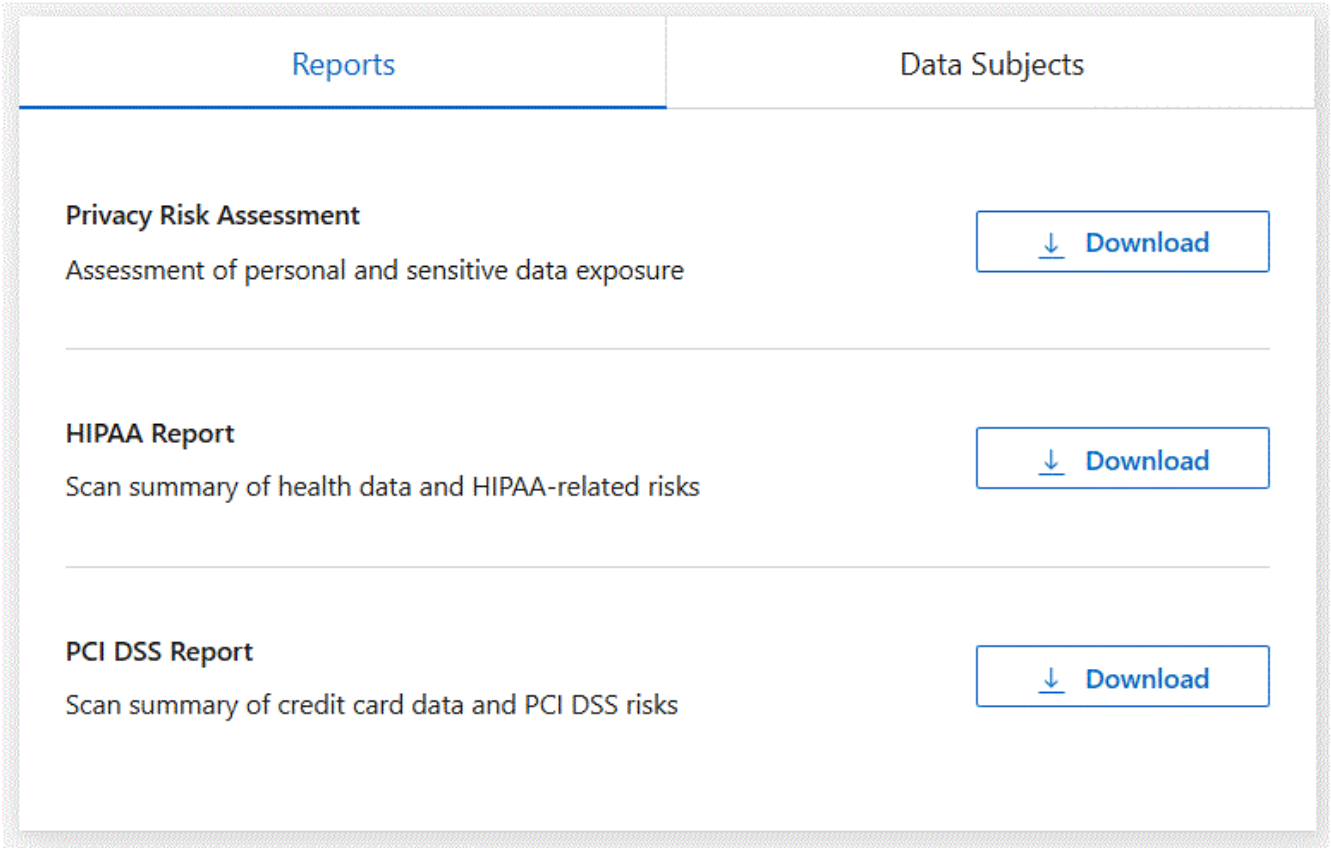
- 평가 개요: 발견된 개인 데이터 유형과 데이터 범주에 대한 분석입니다.
- 이 평가에서 데이터 주체는 다음과 같습니다. 국가 식별자가 발견된 위치별 사람의 수입니다.

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.

데이터 분류 관리

NetApp Data Classification 검사에서 특정 디렉토리 제외

NetApp Data Classification 특정 디렉토리를 검사에서 제외하려면 이러한 디렉토리 이름을 구성 파일에 추가할 수 있습니다. 이 변경 사항을 적용하면 데이터 분류 엔진이 해당 디렉토리를 검사에서 제외합니다.

기본적으로 데이터 분류 스캔에서는 볼륨의 소스와 동일한 볼륨 스냅샷 데이터는 제외됩니다.

지원되는 데이터 소스

다음 데이터 소스의 NFS 및 CIFS 공유에 대해 데이터 분류 검사에서 특정 디렉토리를 제외하는 기능이 지원됩니다.

- 온프레미스 ONTAP
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- 일반 파일 공유

스캔에서 제외할 디렉토리를 정의합니다.

디렉토리를 분류 스캐닝에서 제외하려면 먼저 데이터 분류 시스템에 로그인하여 구성 파일을 편집하고 스크립트를 실행해야 합니다. 방법을 확인하세요"데이터 분류 시스템에 로그인하세요" Linux 시스템에 소프트웨어를 수동으로 설치했는지, 아니면 클라우드에 인스턴스를 배포했는지에 따라 다릅니다.

고려 사항

- 데이터 분류 시스템당 최대 50개의 디렉토리 경로를 제외할 수 있습니다.
- 디렉토리 경로를 제외하면 스캔 시간에 영향을 미칠 수 있습니다.

단계

1. 데이터 분류 시스템에서 "/opt/netapp/config/custom_configuration"으로 이동한 다음 파일을 엽니다. `data_provider.yaml` .
2. "data_providers" 섹션의 "exclude:" 줄에 제외할 디렉토리 경로를 입력합니다. 예를 들어:

   ```
   exclude:
   - "folder1"
   - "folder2"
   ```

   이 파일의 다른 내용은 수정하지 마세요.
3. 파일의 변경 사항을 저장합니다.
4. "/opt/netapp/Datasense/tools/customer_configuration/data_providers"로 이동하여 다음 스크립트를

실행합니다.

```
update_data_providers_from_config_file.sh
```

+ 이 명령은 스캐닝에서 제외할 디렉토리를 분류 엔진에 커밋합니다.

결과

이후의 모든 데이터 검사에서는 해당 지정된 디렉토리 검사가 제외됩니다.

동일한 단계를 사용하여 제외 목록에서 항목을 추가, 편집 또는 삭제할 수 있습니다. 스크립트를 실행하여 변경 사항을 커밋한 후 개정된 제외 목록이 업데이트됩니다.

예시

구성 **1:**

이름에 "folder1"이 포함된 모든 폴더는 모든 데이터 소스에서 제외됩니다.

```
data_providers:
   exclude:
   - "folder1"
```

제외될 경로에 대한 예상 결과:

- /CVO1/폴더1
- /CVO1/폴더1이름
- /CVO1/폴더10
- /CVO1/*폴더1
- /CVO1/+폴더1이름
- /CVO1/notfolder10
- /CVO22/폴더1
- /CVO22/폴더1이름
- /CVO22/폴더10

제외되지 않는 경로의 예:

- /CVO1/*폴더
- /CVO1/폴더 이름
- /CVO22/*폴더20

구성 **2:**

이름 앞에 "*folder1"만 포함된 모든 폴더는 제외됩니다.

```
data_providers:
   exclude:
   - "\\*folder1"
```

제외될 경로에 대한 예상 결과:

- /CVO/*폴더1
- /CVO/*폴더1이름
- /CVO/*폴더10

제외되지 않는 경로의 예:

- /CVO/폴더1
- /CVO/폴더1이름
- /CVO/not*folder10

구성 **3:**

이름에 "folder1"이 포함된 데이터 소스 "CVO22"의 모든 폴더는 제외됩니다.

```
data_providers:
   exclude:
   - "CVO22/folder1"
```

제외될 경로에 대한 예상 결과:

- /CVO22/폴더1
- /CVO22/폴더1이름
- /CVO22/폴더10

제외되지 않는 경로의 예:

- /CVO1/폴더1
- /CVO1/폴더1이름
- /CVO1/폴더10

폴더 이름에서 특수 문자 이스케이프

다음 특수 문자 중 하나가 포함된 폴더 이름이 있고 해당 폴더의 데이터를 검사에서 제외하려면 폴더 이름 앞에 이스케이프 시퀀스 \\를 사용해야 합니다.

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
```

예를 들어:

소스의 경로: `/project/*not_to_scan`

제외 파일의 구문: "*not_to_scan"

현재 제외 목록 보기

내용의 경우 가능합니다. data_provider.yaml 실행 후 실제로 커밋된 내용과 다르게 구성 파일을 작성합니다. update_data_providers_from_config_file.sh 스크립트. 데이터 분류 검사에서 제외한 디렉토리의 현재 목록을 보려면 "/opt/netapp/Datasense/tools/customer_configuration/data_providers"에서 다음 명령을 실행하세요.

```
get_data_providers_configuration.sh
```

NetApp Data Classification 에서 조직에 공개된 추가 그룹 ID 정의

NFS 파일 공유의 파일이나 폴더에 그룹 ID(GID)가 추가되면 파일이나 폴더에 대한 사용 권한이 정의됩니다. 예를 들어, "조직에 공개"할지 여부가 정의됩니다. 일부 GID가 처음에 "조직에 공개" 권한 수준으로 설정되지 않은 경우 해당 권한을 GID에 추가하여 해당 GID가 첨부된 모든 파일과 폴더가 "조직에 공개"된 것으로 간주되도록 할 수 있습니다.

이 변경을 하고 NetApp Data Classification 파일과 폴더를 다시 검사하면 이러한 그룹 ID가 첨부된 모든 파일과 폴더에 조사 세부 정보 페이지에 이 권한이 표시되고 파일 권한을 표시하는 보고서에도 나타납니다.

이 기능을 활성화하려면 데이터 분류 시스템에 로그인하여 구성 파일을 편집하고 스크립트를 실행해야 합니다. 방법을 확인하세요"데이터 분류 시스템에 로그인하세요" Linux 시스템에 소프트웨어를 수동으로 설치했는지, 아니면 클라우드에 인스턴스를 배포했는지에 따라 다릅니다.

그룹 ID에 "조직에 공개" 권한 추가

이 작업을 시작하기 전에 그룹 ID 번호(GID)가 필요합니다.

단계

1. 데이터 분류 시스템에서 "/opt/netapp/config/custom_configuration"으로 이동하여 파일을 엽니다. data_provider.yaml .
2. "organization_group_ids: []" 줄에 그룹 ID를 추가합니다. 예를 들어:

   ```
   organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
   ```

   이 파일의 다른 내용은 변경하지 마세요.
3. 파일의 변경 사항을 저장합니다.
4. "/opt/netapp/Datasense/tools/customer_configuration/data_providers"로 이동하여 다음 스크립트를 실행합니다.

   ```
   update_data_providers_from_config_file.sh
   ```

   이 명령은 수정된 그룹 ID 권한을 분류 엔진에 커밋합니다.

결과

이후의 모든 데이터 스캔에서는 이러한 그룹 ID가 "조직에 공개됨"으로 첨부된 파일이나 폴더를 식별합니다.

동일한 단계를 사용하여 그룹 ID 목록을 편집하고 과거에 추가한 그룹 ID를 삭제할 수 있습니다. 스크립트를 실행하여 변경 사항을 커밋한 후 수정된 그룹 ID 목록이 업데이트됩니다.

현재 그룹 ID 목록 보기

내용의 경우 가능합니다. `data_provider.yaml` 실행 후 실제로 커밋된 내용과 다르게 구성 파일을 설정합니다. `update_data_providers_from_config_file.sh` 스크립트. 데이터 분류에 추가한 그룹 ID의 현재 목록을 보려면 "/opt/netapp/Datasense/tools/customer_configuration/data_providers"에서 다음 명령을 실행하세요.

```
get_data_providers_configuration.sh
```

NetApp Data Classification 에서 데이터 소스 제거

필요한 경우 NetApp Data Classification 하나 이상의 시스템, 데이터베이스 또는 파일 공유 그룹을 스캔하는 것을 중지할 수 있습니다.

시스템 검사 비활성화

검사를 비활성화하면 데이터 분류가 더 이상 시스템의 데이터를 검사하지 않으며 데이터 분류 인스턴스에서 인덱싱된 통찰력을 제거합니다. 시스템 자체의 데이터는 삭제되지 않습니다.

1. 구성 페이지에서 다음을 선택하세요. 시스템 행에 있는 버튼을 클릭한 다음 *데이터 분류 비활성화*를 클릭합니다.

시스템을 선택하면 서비스 패널에서 시스템 검사를 비활성화할 수도 있습니다.

데이터 분류에서 데이터베이스 제거

더 이상 특정 데이터베이스를 스캔할 필요가 없다면 데이터 분류 인터페이스에서 해당 데이터베이스를 삭제하고 모든 스캔을 중지할 수 있습니다.

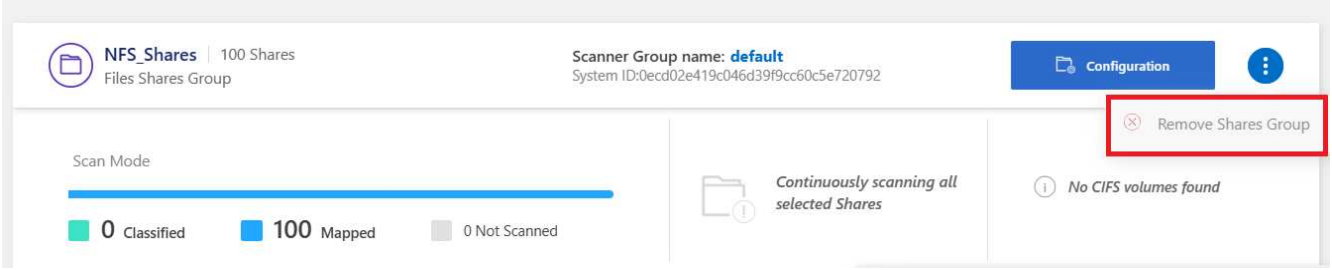
1. 구성 페이지에서 다음을 선택하세요. 데이터베이스 행에 있는 버튼을 클릭한 다음 *DB 서버 제거*를 클릭합니다.

데이터 분류에서 파일 공유 그룹 제거

더 이상 파일 공유 그룹에서 사용자 파일을 검사하지 않으려면 데이터 분류 인터페이스에서 파일 공유 그룹을 삭제하고 모든 검사를 중지할 수 있습니다.

단계

1. 구성 페이지에서 다음을 선택하세요. 파일 공유 그룹 행에 있는 버튼을 클릭한 다음 *파일 공유 그룹 제거*를 선택합니다.



2. 확인 대화 상자에서 *공유 그룹 삭제*를 선택합니다.

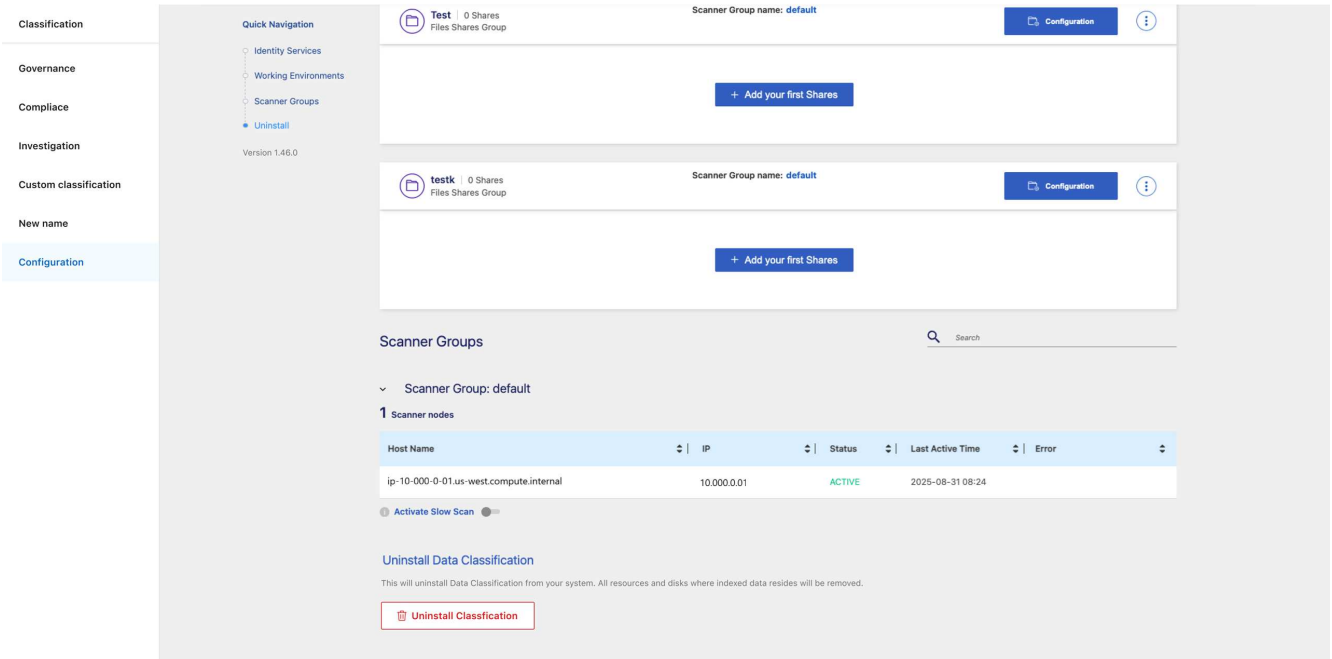
NetApp Data Classification 제거

문제를 해결하거나 호스트에서 소프트웨어를 영구적으로 제거하려면 NetApp Data Classification 제거할 수 있습니다. 인스턴스를 삭제하면 인덱싱된 데이터가 있는 관련 디스크도 삭제되므로 데이터 분류에서 스캔한 모든 정보가 영구적으로 삭제됩니다.

사용해야 하는 단계는 데이터 분류를 클라우드에 배포했는지, 아니면 온프레미스 호스트에 배포했는지에 따라 달라집니다.

클라우드 공급자로부터 데이터 분류 제거

1. 데이터 분류에서 구성을 선택합니다.
2. 구성 페이지 하단에서 분류 제거를 선택합니다.

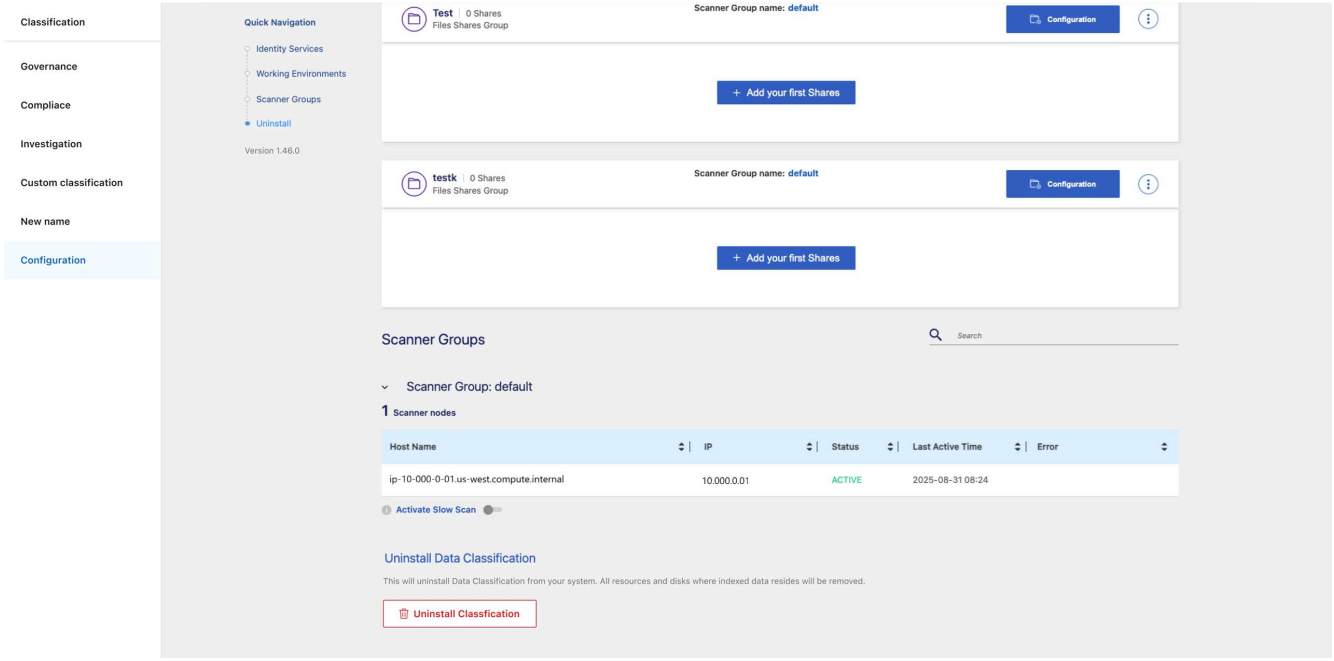


3. 대화 상자에서 "제거"를 입력하여 콘솔 에이전트에서 데이터 분류 인스턴스의 연결을 끊습니다. 제거를 선택하여 확인하세요.
4. 분류 제거 대화 상자에서 *uninstall*을 입력하여 콘솔 에이전트에서 데이터 분류 인스턴스의 연결을 끊으려는 것을 확인한 다음 *제거*를 선택합니다.
5. 제거 프로세스를 마무리하려면 클라우드 공급자의 콘솔로 이동하여 데이터 분류 인스턴스를 삭제하세요. 인스턴스

이름은 *CloudCompliance_*이고, 생성된 해시*(UUID)*가 여기에 연결됩니다. 예: *_CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

온프레미스 배포에서 데이터 분류 제거

1. 데이터 분류에서 구성을 선택합니다.
2. 구성 페이지 하단에서 분류 제거를 선택합니다.



3. 대화 상자에서 "제거"를 입력하여 콘솔 에이전트에서 데이터 분류 인스턴스의 연결을 끊습니다. 제거를 선택하여 확인하세요.
4. 호스트에서 소프트웨어를 제거하려면 다음을 실행하세요. `cleanup.sh` 예를 들어, 데이터 분류 호스트 머신의 스크립트:

```
cleanup.sh
```

스크립트는 다음 위치에 있습니다. `/install/light_probe/onprem_installer/cleanup.sh` 예배 규칙서. 방법을 확인하세요"데이터 분류 호스트 머신에 로그인합니다." .

참조

지원되는 NetApp Data Classification 인스턴스 유형

NetApp Data Classification 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다. 클라우드에서 데이터 분류를 배포할 때 모든 기능을 활용하려면 "대규모" 특성을 갖춘 시스템을 사용하는 것이 좋습니다.

CPU와 RAM이 적은 시스템에도 데이터 분류를 배포할 수 있지만, 이러한 덜 강력한 시스템을 사용할 경우 몇 가지 제한 사항이 있습니다. "이러한 제한 사항에 대해 알아보세요" .

다음 표에서 "기본"으로 표시된 시스템을 데이터 분류를 설치하는 지역에서 사용할 수 없는 경우 표의 다음 시스템이 배포됩니다.

AWS 인스턴스 유형

시스템 크기	명세서	인스턴스 유형
특대	32개 CPU, 128GB RAM, 1TiB gp3 SSD	"m6i.8xlarge"(기본)
크기가 큰	CPU 16개, 64GB RAM, 500GiB SSD	"m6i.4xlarge"(기본값) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
중간	CPU 8개, 32GB RAM, 200GiB SSD	"m6i.2xlarge"(기본값) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
작은	CPU 8개, 16GB RAM, 100GiB SSD	"c6a.2xlarge"(기본값) c5a.2xlarge c5.2xlarge c4.2xlarge

Azure 인스턴스 유형

시스템 크기	명세서	인스턴스 유형
특대	32개 CPU, 128GB RAM, OS 디스크(2,048GiB, 최소 250MB/s 처리량), 데이터 디스크(1TiB SSD, 최소 750MB/s 처리량)	"Standard_D32_v3"(기본)
크기가 큰	CPU 16개, 64GB RAM, 500GiB SSD	"Standard_D16s_v3"(기본)

GCP 인스턴스 유형

시스템 크기	명세서	인스턴스 유형
크기가 큰	CPU 16개, 64GB RAM, 500GiB SSD	"n2-표준-16"(기본값) n2d-standard-16 n1-standard-16

NetApp Data Classification 데이터 소스에서 수집된 메타데이터

NetApp Data Classification 데이터 소스와 시스템의 데이터에 대한 분류 스캔을 수행할 때 특정 메타데이터를 수집합니다. 데이터 분류는 데이터 분류에 필요한 대부분의 메타데이터에 접근할 수 있지만, 필요한 데이터에 접근할 수 없는 일부 소스도 있습니다.

	메타데이터	CIFS	NFS
타임스탬프	생성 시간	사용 가능	사용할 수 없음(Linux에서는 지원되지 않음)
	마지막 접속 시간	사용 가능	사용 가능
	마지막 수정 시간	사용 가능	사용 가능
권한	열기 권한	"EVERYONE" 그룹이 파일에 액세스할 수 있는 경우 해당 파일은 "조직에 공개"로 간주됩니다.	"기타"가 파일에 액세스할 수 있는 경우 해당 파일은 "조직에 공개됨"으로 간주됩니다.
	사용자/그룹 액세스	사용자 및 그룹 정보는 LDAP에서 가져옵니다.	사용할 수 없음(NFS 사용자는 일반적으로 서버에서 로컬로 관리되므로 동일한 개인이 각 서버에서 다른 UID를 가질 수 있음)

- 데이터 분류는 데이터베이스 데이터 소스에서 "마지막 액세스 시간"을 추출하지 않습니다.
- 이전 버전의 Windows OS(예: Windows 7 및 Windows 8)는 시스템 성능에 영향을 줄 수 있으므로 기본적으로 "마지막 액세스 시간" 특성 수집을 비활성화합니다. 이 속성이 수집되지 않으면 "마지막 액세스 시간"을 기반으로 하는 데이터 분류 분석에 영향을 미칩니다. 필요한 경우 이러한 이전 Windows 시스템에서 마지막 액세스 시간 수집을 활성화할 수 있습니다.

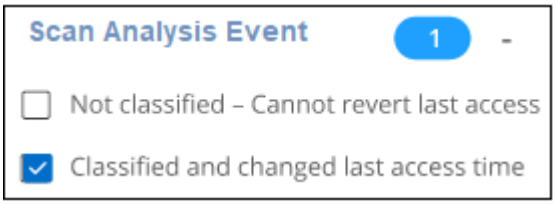
마지막 액세스 시간 타임스탬프

데이터 분류가 파일 공유에서 데이터를 추출할 때, 운영 체제는 이를 데이터에 액세스하는 것으로 간주하고 그에 따라 "마지막 액세스 시간"을 변경합니다. 스캐닝 후, 데이터 분류는 마지막 액세스 시간을 원래 타임스탬프로 되돌리려고 시도합니다. 데이터 분류에 CIFS의 쓰기 속성 권한이 없거나 NFS의 쓰기 권한이 없는 경우 시스템은 마지막 액세스 시간을 원래 타임스탬프로 되돌릴 수 없습니다. SnapLock 으로 구성된 ONTAP 볼륨은 읽기 전용 권한을 가지며 마지막 액세스 시간을 원래 타임스탬프로 되돌릴 수 없습니다.

기본적으로 데이터 분류에 이러한 권한이 없으면 시스템은 볼륨에서 해당 파일을 검사하지 않습니다. 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 하지만 파일의 마지막 액세스 시간이 원래 시간으로 재설정되는 것이 문제가 되지 않는다면 구성 페이지 하단의 **"쓰기 속성"** 권한이 없는 경우 검사 스위치를 선택하면 데이터 분류가 권한에 관계없이 볼륨을 검사합니다.

이 기능은 온프레미스 ONTAP 시스템, Cloud Volumes ONTAP, Azure NetApp Files, Amazon FSx for NetApp ONTAP 관리 및 타사 파일 공유에 적용할 수 있습니다.

조사 페이지에는 _스캔 분석 이벤트_라는 필터가 있는데, 이를 사용하면 데이터 분류가 마지막 액세스 시간을 되돌릴 수 없어 분류되지 않은 파일이나 데이터 분류가 마지막 액세스 시간을 되돌릴 수 없어도 분류된 파일을 표시할 수 있습니다.



필터 선택은 다음과 같습니다.

- "분류되지 않음 - 마지막 액세스 시간을 되돌릴 수 없음" - 쓰기 권한이 없어 분류되지 않은 파일을 표시합니다.
- "분류 및 업데이트된 마지막 액세스 시간" - 이는 분류된 파일을 보여주며, 데이터 분류는 마지막 액세스 시간을 원래 날짜로 재설정하지 못했습니다. 이 필터는 *"쓰기 속성" 권한이 없는 경우 검사*를 켜둔 환경에만 적용됩니다.

필요한 경우 이러한 결과를 보고서로 내보내어 권한 때문에 어떤 파일이 검사되고 있는지, 검사되지 않고 있는지 확인할 수 있습니다. "데이터 조사 보고서에 대해 자세히 알아보세요".

NetApp Data Classification 시스템에 로그인하세요

로그 파일에 액세스하거나 구성 파일을 편집하려면 NetApp Data Classification 시스템에 로그인해야 합니다.

데이터 분류가 사내 Linux 머신이나 클라우드에 배포한 Linux 머신에 설치된 경우 구성 파일과 스크립트에 직접 액세스할 수 있습니다.

데이터 분류가 클라우드에 배포되는 경우 데이터 분류 인스턴스에 SSH를 사용해야 합니다. 사용자 이름과 비밀번호를 입력하거나 콘솔 에이전트 설치 중에 제공한 SSH 키를 사용하여 시스템에 SSH를 실행합니다. SSH 명령은 다음과 같습니다.

```
ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
```

- `<path_to_the_ssh_key>`= ssh 인증 키의 위치
- `<machine_user>`:
  - AWS의 경우: <ec2-user>를 사용하세요.

    - Azure의 경우: 콘솔 인스턴스에 대해 생성된 사용자를 사용합니다.
    - GCP의 경우: 콘솔 인스턴스에 대해 생성된 사용자를 사용합니다.
- `<datasense_ip>`= 가상 머신 인스턴스의 IP 주소

클라우드 시스템에 액세스하려면 보안 그룹 인바운드 규칙을 수정해야 합니다. 자세한 내용은 다음을 참조하세요.

- "AWS의 보안 그룹 규칙"
- "Azure의 보안 그룹 규칙"
- "Google Cloud의 방화벽 규칙"

NetApp Data Classification API

웹 UI를 통해 제공되는 NetApp Data Classification 기능은 REST API를 통해서도 사용할 수 있습니다.

UI의 탭에 해당하는 데이터 분류에는 4가지 범주가 정의되어 있습니다.

- 조사
- 규정 준수
- 통치
- 구성

Swagger 문서의 API를 사용하면 검색, 데이터 집계, 스캔 추적이 가능하며 복사, 이동, 삭제 등의 작업을 수행할 수 있습니다.

개요

API를 사용하면 다음 기능을 수행할 수 있습니다.

- 수출 정보
    - UI에서 사용 가능한 모든 것은 API를 통해 내보낼 수 있습니다(보고서 제외)
    - 데이터는 JSON 형식으로 내보내집니다(Splunk와 같은 타사 애플리케이션에 쉽게 구문 분석하고 푸시할 수 있음)
- "AND" 및 "OR" 문을 사용하여 쿼리를 만들고, 정보를 포함하거나 제외하는 등의 작업을 수행합니다.

  예를 들어, 특정 개인 식별 정보(PII)가 없는 파일을 찾을 수 있습니다(이 기능은 UI에서 사용할 수 없습니다). 내보내기 작업에서 특정 필드를 제외할 수도 있습니다.

- 작업 수행
    - CIFS 자격 증명 업데이트
    - 작업 보기 및 취소
    - 디렉토리 재스캔
    - 데이터 내보내기

API는 안전하며 UI와 동일한 인증 방법을 사용합니다. 인증에 대한 정보는 다음에서 찾을 수 있습니다."REST API 설명서" .

Swagger API 참조에 액세스하기

Swagger에 들어가려면 데이터 분류 인스턴스의 IP 주소가 필요합니다. 클라우드에 배포하는 경우 공용 IP 주소를 사용합니다. 그러면 다음 엔드포인트로 이동해야 합니다.

https://<분류_IP>/문서

API를 사용한 예

다음 예제는 파일을 복사하는 API 호출을 보여줍니다.

API 요청

조사 탭의 모든 필터를 보려면 먼저 시스템에 필요한 모든 관련 필드와 옵션을 확보해야 합니다.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

응답

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
}
{
  "options": [
```

```
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
      "name": "Open Permissions",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
```

```
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT_TYPE",
      "name": "system-type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
```

```
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "system",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
      "name": "Category",
      "operators": [
        "IN",
        "NOT_IN"
      ],
```

```
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_SENSITIVITY_LEVEL",
    "name": "Sensitivity Level",
    "operators": [
      "IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "NUMBER_OF_IDENTIFIERS",
    "name": "Number of identifiers",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_PERSONAL",
    "name": "Personal Data",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_SENSITIVE",
    "name": "Sensitive Personal Data",
    "operators": [
      "IN",
      "NOT_IN"
```

```
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_TYPE",
      "name": "File Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
```

```
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_MODIFICATION_RETENTION",
      "name": "Last Modified",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
      "name": "Last Accessed",
      "operators": [
        "IN"
```

```
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "USER_DEFINED_STATUS",
      "name": "Tags",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
```

```
          "IN",
          "NOT_IN"
        ],
        "server_data": true,
        "type": "SELECT"
      }
    ]
}
```

우리는 복사하려는 원하는 파일을 필터링하기 위해 요청 매개변수에서 해당 응답을 사용할 것입니다.

여러 항목에 작업을 적용할 수 있습니다. 지원되는 작업 유형에는 이동, 삭제, 복사가 있습니다.

복사 작업을 생성합니다.

API 요청

다음 API는 액션 API이며 이를 통해 여러 액션을 생성할 수 있습니다.

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

응답

응답에서는 작업 객체가 반환되므로 get 및 delete API를 사용하여 작업에 대한 상태를 얻거나 작업을 취소할 수 있습니다.

```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

지식과 지원

NetApp Console 지원에 등록하세요

NetApp Console 과 해당 스토리지 솔루션, 데이터 서비스에 대한 기술 지원을 받으려면 지원 등록이 필요합니다. Cloud Volumes ONTAP 시스템의 주요 워크플로를 활성화하려면 지원 등록도 필요합니다.

지원에 등록해도 클라우드 공급자 파일 서비스에 대한 NetApp 지원은 제공되지 않습니다. 클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품 설명서의 "도움말 받기 "를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

지원 등록 개요

지원 자격을 활성화하기 위한 등록 방법은 두 가지가 있습니다.

- NetApp Console 계정 일련 번호를 등록합니다(콘솔의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호).

  이는 콘솔 내의 모든 서비스에 대한 단일 지원 구독 ID 역할을 합니다. 각 콘솔 계정을 등록해야 합니다.

- 클라우드 공급업체의 마켓플레이스에서 구독과 관련된 Cloud Volumes ONTAP 일련 번호를 등록합니다(20자리 909201xxxxxxxx 일련 번호).

  이러한 일련 번호는 일반적으로 _PAYGO 일련 번호_라고 하며 Cloud Volumes ONTAP 배포 시 NetApp Console 에서 생성됩니다.

두 가지 유형의 일련 번호를 모두 등록하면 지원 티켓 개설 및 자동 사례 생성과 같은 기능을 사용할 수 있습니다. 아래 설명된 대로 콘솔에 NetApp 지원 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

NetApp 지원을 위해 NetApp Console 등록

지원을 등록하고 지원 자격을 활성화하려면 NetApp Console 계정의 한 사용자가 NetApp 지원 사이트 계정을 콘솔 로그인과 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp 지원 사이트(NSS) 계정이 있는지 여부에 따라 달라집니다.

NSS 계정이 있는 기존 고객

NSS 계정이 있는 NetApp 고객이라면 콘솔을 통해 지원을 등록하기만 하면 됩니다.

단계

1. 관리 > *자격 증명*을 선택합니다.
2. *사용자 자격 증명*을 선택하세요.

3. *NSS 자격 증명 추가*를 선택하고 NetApp 지원 사이트(NSS) 인증 프롬프트를 따릅니다.
4. 등록 과정이 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택하고 *지원*을 선택하세요.

   리소스 페이지에는 귀하의 콘솔 계정이 지원을 위해 등록되어 있다는 내용이 표시됩니다.

   다른 콘솔 사용자는 NetApp 지원 사이트 계정을 로그인과 연결하지 않은 경우 동일한 지원 등록 상태를 볼 수 없습니다. 하지만 그렇다고 해서 귀하의 계정이 지원을 위해 등록되지 않았다는 의미는 아닙니다. 조직 내 한 명의 사용자가 이러한 단계를 따랐다면 귀하의 계정은 등록되었습니다.

기존 고객이지만 **NSS** 계정이 없습니다.

기존 라이선스와 일련 번호는 있지만 NSS 계정이 없는 기존 NetApp 고객인 경우 NSS 계정을 만들고 콘솔 로그인과 연결해야 합니다.

단계

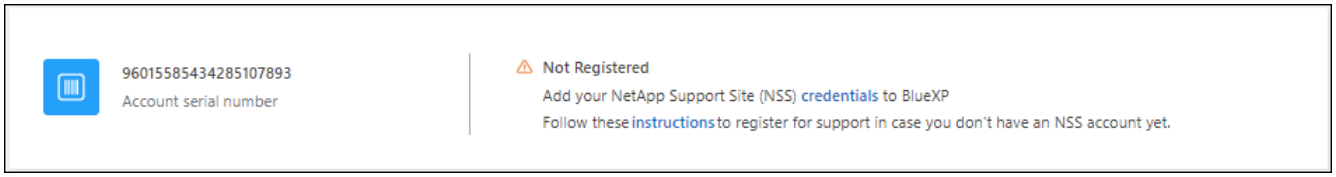
1. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
   b. 위에 사용된 콘솔 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 계정 처리가 빨라집니다.
2. 다음 단계를 완료하여 새 NSS 계정을 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

NetApp 의 새로운 기능

NetApp 처음 사용하시고 NSS 계정이 없으신 경우 아래의 각 단계를 따르세요.

단계

1. 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.
2. 지원 등록 페이지에서 계정 ID 일련 번호를 찾으세요.



3. 로 이동 "NetApp 지원 등록 사이트" *저는 등록된 NetApp 고객이 아닙니다*를 선택하세요.
4. 필수 입력란(빨간색 별표가 있는 항목)을 작성해 주세요.
5. 제품군 필드에서 *클라우드 관리자*를 선택한 다음 해당 청구 제공자를 선택하세요.
6. 위의 2단계에서 계정 일련번호를 복사하고 보안 검사를 완료한 다음 NetApp의 글로벌 데이터 개인정보 보호정책을 읽었는지 확인하세요.

   이 안전한 거래를 마무리하기 위해 제공된 사서함으로 이메일이 즉시 전송됩니다. 몇 분 안에 인증 이메일이 도착하지 않으면 스팸 폴더를 확인하세요.

7. 이메일 내에서 작업을 확인하세요.

   확인을 클릭하면 귀하의 요청이 NetApp 에 제출되고 NetApp 지원 사이트 계정을 만드는 것이 좋습니다.

8. 다음을 완료하여 NetApp 지원 사이트 계정을 만드십시오. "NetApp 지원 사이트 사용자 등록 양식"
    a. 일반적으로 * NetApp 고객/최종 사용자*인 적절한 사용자 수준을 선택하세요.
    b. 위에 사용된 계정 일련번호(960xxxx)를 일련번호 필드에 꼭 복사해 두세요. 이렇게 하면 처리 속도가 빨라집니다.

당신이 완료한 후

이 과정에서 NetApp 귀하에게 연락을 드릴 것입니다. 이는 신규 사용자를 대상으로 한 일회성 온보딩 과정입니다.

NetApp 지원 사이트 계정이 있으면 아래 단계를 완료하여 계정을 콘솔 로그인과 연결하세요.NSS 계정이 있는 기존 고객 .

Cloud Volumes ONTAP 지원을 위한 NSS 자격 증명 연결

Cloud Volumes ONTAP 에 대한 다음 주요 워크플로를 활성화하려면 NetApp 지원 사이트 자격 증명을 콘솔 계정과 연결해야 합니다.

- 지원을 위해 Pay-as-you-go Cloud Volumes ONTAP 시스템 등록

  시스템 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스하려면 NSS 계정을 제공해야 합니다.

- BYOL(Bring Your Own License)을 사용할 때 Cloud Volumes ONTAP 배포

  콘솔에서 라이선스 키를 업로드하고 구매한 기간 동안 구독을 활성화하려면 NSS 계정을 제공해야 합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리스로 업그레이드

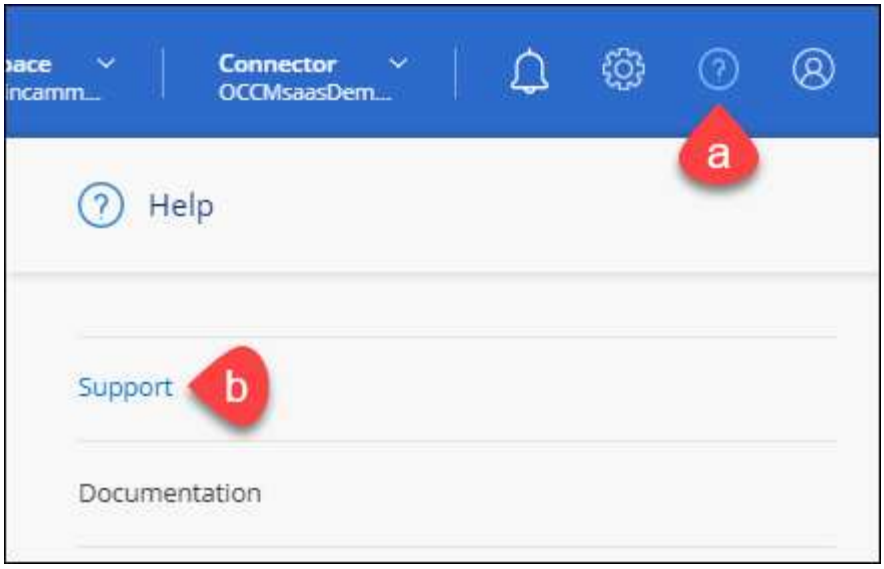
NSS 자격 증명을 NetApp Console 계정과 연결하는 것은 콘솔 사용자 로그인과 연결된 NSS 계정과 다릅니다.

이러한 NSS 자격 증명은 특정 콘솔 계정 ID와 연결됩니다. 콘솔 조직에 속한 사용자는 *지원 > NSS 관리*에서 이러한 자격 증명에 액세스할 수 있습니다.

- 고객 수준 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있습니다.
- 파트너 또는 리셀러 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 *지원*을 선택하세요.



2. *NSS 관리 > NSS 계정 추가*를 선택하세요.
3. 메시지가 표시되면 *계속*을 선택하여 Microsoft 로그인 페이지로 이동합니다.

   NetApp 지원 및 라이선싱에 특화된 인증 서비스를 위한 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 NetApp 지원 사이트에 등록된 이메일 주소와 비밀번호를 입력하여 인증 과정을 진행합니다.

   이러한 작업을 통해 콘솔은 라이선스 다운로드, 소프트웨어 업그레이드 확인, 향후 지원 등록과 같은 작업에 NSS 계정을 사용할 수 있습니다.

   다음 사항에 유의하세요.

   - NSS 계정은 고객 수준 계정이어야 합니다(게스트나 임시 계정이어서는 안 됩니다). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
   - 해당 계정이 파트너 수준 계정인 경우 NSS 계정은 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하는데 파트너 수준 계정이 이미 있는 경우 다음과 같은 오류 메시지가 표시됩니다.

     "이 계정에는 다른 유형의 NSS 사용자가 이미 있으므로 NSS 고객 유형이 허용되지 않습니다."

   기존 고객 수준 NSS 계정이 있고 파트너 수준 계정을 추가하려는 경우에도 마찬가지입니다.

   - 로그인에 성공하면 NetApp NSS 사용자 이름을 저장합니다.

     이는 귀하의 이메일에 매핑되는 시스템 생성 ID입니다. **NSS** 관리 페이지에서 이메일을 표시할 수 있습니다. ••• 메뉴.

   - 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 자격 증명 업데이트 옵션도 있습니다. ••• 메뉴.

     이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이 계정의 토큰은 90일 후에 만료됩니다. 이에 대한 알림이 게시됩니다.

NetApp Data Classification 에 대한 도움말 받기

NetApp 다양한 방법으로 NetApp Console 과 클라우드 서비스에 대한 지원을 제공합니다. 지식 기반(KB) 문서와 커뮤니티 포럼 등 광범위한 무료 셀프 지원 옵션을 24시간 연중무휴로 이용할 수 있습니다. 지원 등록 시 웹 티켓팅을 통한 원격 기술 지원이 제공됩니다.

클라우드 공급자 파일 서비스에 대한 지원을 받으세요

클라우드 공급자 파일 서비스, 해당 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원에 대해서는 해당 제품의 설명서를 참조하세요.

- "ONTAP 용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

NetApp 과 해당 스토리지 솔루션, 데이터 서비스에 대한 특정 기술 지원을 받으려면 아래에 설명된 지원 옵션을 사용하세요.

셀프 지원 옵션 사용

다음 옵션은 주 7일, 하루 24시간 무료로 이용 가능합니다.

- 설명서

  현재 보고 있는 NetApp Console 문서입니다.

- "지식 기반"

  NetApp 지식 기반을 검색하여 문제 해결에 도움이 되는 문서를 찾아보세요.

- "커뮤니티"

  NetApp Console 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새로운 토론을 만들어 보세요.

NetApp 지원을 통해 사례 만들기

위에 나열된 셀프 지원 옵션 외에도, 지원을 활성화한 후 NetApp 지원 전문가와 협력하여 문제를 해결할 수 있습니다.

시작하기 전에

- 사례 만들기 기능을 사용하려면 먼저 NetApp 지원 사이트 자격 증명을 콘솔 로그인과 연결해야 합니다. "콘솔 로그인과 관련된 자격 증명을 관리하는 방법을 알아보세요." .
- 일련 번호가 있는 ONTAP 시스템에 대한 사례를 개설하는 경우 NSS 계정은 해당 시스템의 일련 번호와 연결되어야 합니다.

단계

1. NetApp Console 에서 *도움말 > 지원*을 선택합니다.
2. 리소스 페이지에서 기술 지원 아래에 있는 사용 가능한 옵션 중 하나를 선택하세요.

a. 전화로 상담원과 통화하고 싶으시면 *전화하기*를 선택하세요. netapp.com에서 전화할 수 있는 전화번호가 나열된 페이지로 이동하게 됩니다.

b. NetApp 지원 전문가에게 티켓을 열려면 *사례 만들기*를 선택하세요.

   - 서비스: 문제와 관련된 서비스를 선택하세요. 예를 들어, * NetApp Console*은 콘솔 내 워크플로 또는 기능과 관련된 기술 지원 문제에 대한 구체적인 내용입니다.
   - 시스템: 스토리지에 해당되는 경우 * Cloud Volumes ONTAP* 또는 *온프레미스*를 선택한 다음 연관된 작업 환경을 선택합니다.

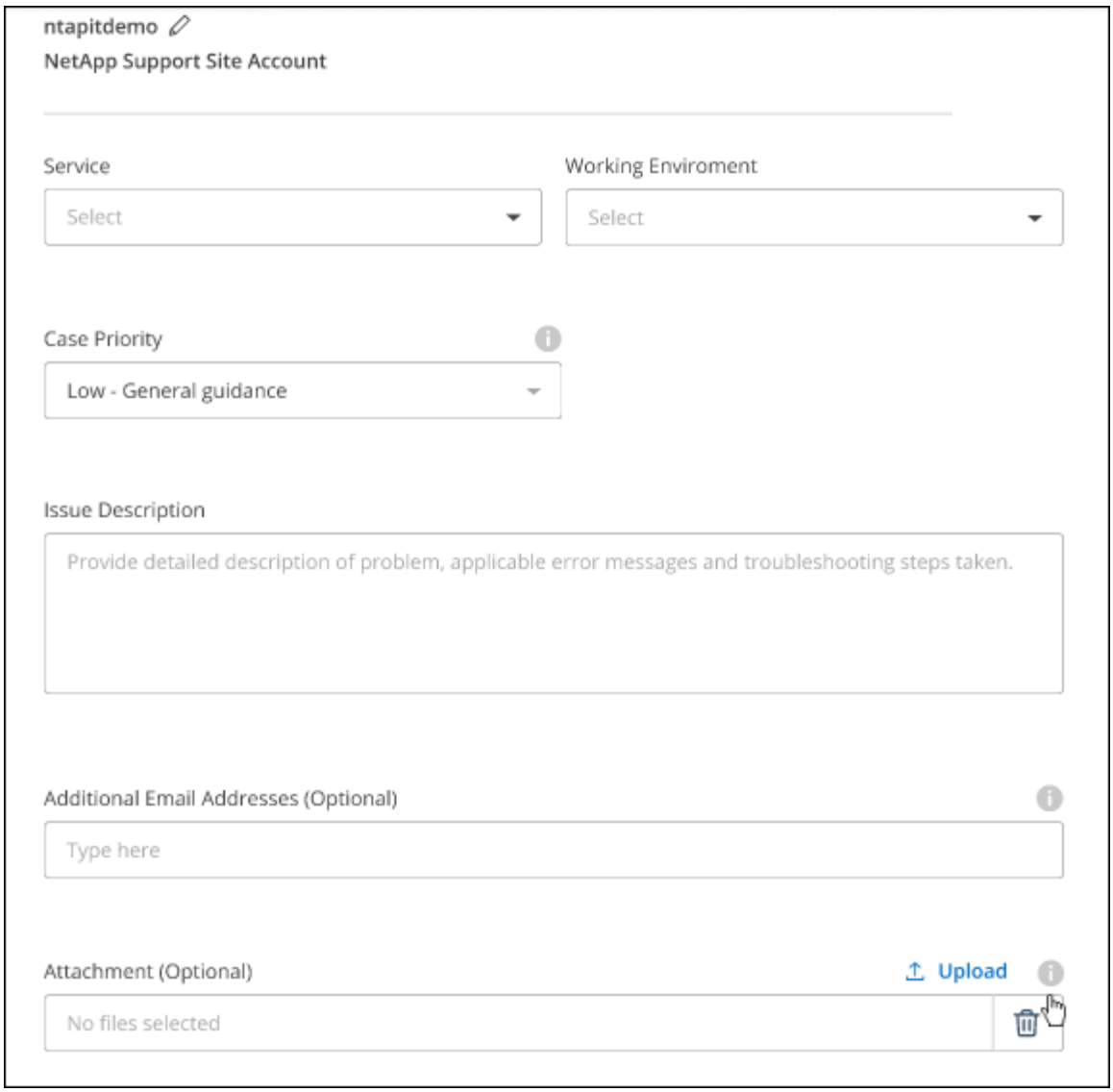
     시스템 목록은 콘솔 조직 범위 내에 있으며, 상단 배너에서 선택한 콘솔 에이전트입니다.

   - 사례 우선순위: 낮음, 보통, 높음 또는 중요로 사례의 우선순위를 선택합니다.

     이러한 우선순위에 대한 자세한 내용을 알아보려면 필드 이름 옆에 있는 정보 아이콘 위에 마우스를 올려놓으세요.

   - 문제 설명: 해당 오류 메시지나 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공하세요.
   - 추가 이메일 주소: 이 문제를 다른 사람에게 알리려면 추가 이메일 주소를 입력하세요.
   - 첨부파일(선택사항): 최대 5개의 첨부파일을 한 번에 하나씩 업로드하세요.

     첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.



당신이 완료한 후

지원 사례 번호가 포함된 팝업이 나타납니다. NetApp 지원 전문가가 귀하의 사례를 검토하고 곧 연락드릴 것입니다.

지원 사례 기록을 보려면 *설정 > 타임라인*을 선택하고 "지원 사례 만들기"라는 이름의 작업을 찾으세요. 가장 오른쪽에 있는 버튼을 누르면 동작을 확장하여 자세한 내용을 볼 수 있습니다.

사례를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대해 사례를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 해당 계정과 연결된 기록상 회사가 NetApp Console 계정 일련 번호에 대한 기록상 회사와 동일하지 않다는 것을 의미할 수 있습니다(예: 960xxxx) 또는 작업 환경 일련 번호. 다음 옵션 중 하나를 사용하여 도움을 요청할 수 있습니다.

- 비기술적 사례를 제출하세요 https://mysupport.netapp.com/site/help

지원 사례 관리

콘솔에서 직접 활성화된 지원 사례와 해결된 지원 사례를 보고 관리할 수 있습니다. 귀하의 NSS 계정 및 회사와 관련된

사례를 관리할 수 있습니다.

다음 사항에 유의하세요.

- 페이지 상단의 사례 관리 대시보드는 두 가지 보기를 제공합니다.
  - 왼쪽 보기는 귀하가 제공한 NSS 계정 사용자에 의해 지난 3개월 동안 열린 총 사례를 보여줍니다.
  - 오른쪽 보기는 사용자 NSS 계정을 기준으로 지난 3개월 동안 회사 수준에서 열린 총 사례를 보여줍니다.

  표의 결과는 귀하가 선택한 보기와 관련된 사례를 반영합니다.
- 관심 있는 열을 추가하거나 제거할 수 있으며, 우선순위 및 상태와 같은 열의 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

  자세한 내용은 아래 단계를 참조하세요.
- 사례별로 사례 메모를 업데이트하거나 아직 닫힘 또는 닫힘 보류 상태가 아닌 사례를 닫는 기능을 제공합니다.

단계

1. NetApp Console 에서 *도움말 > 지원*을 선택합니다.
2. *사례 관리*를 선택하고 메시지가 표시되면 콘솔에 NSS 계정을 추가합니다.

   사례 관리 페이지는 콘솔 사용자 계정과 연결된 NSS 계정과 관련된 미해결 사례를 표시합니다. 이는 **NSS** 관리 페이지 상단에 표시되는 NSS 계정과 동일합니다.
3. 필요에 따라 표에 표시되는 정보를 수정합니다.
   - *조직 사례*에서 *보기*를 선택하면 회사와 관련된 모든 사례를 볼 수 있습니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정하세요.
   - 열의 내용을 필터링합니다.
   - 표에 나타나는 열을 변경하려면 다음을 선택하세요. 그런 다음 표시하려는 열을 선택합니다.
4. 기존 사례를 선택하여 관리하세요. 그리고 사용 가능한 옵션 중 하나를 선택하세요:
   - 사례 보기: 특정 사례에 대한 전체 세부 정보를 확인하세요.
   - 사례 메모 업데이트: 문제에 대한 추가 세부 정보를 제공하거나 *파일 업로드*를 선택하여 최대 5개의 파일을 첨부하세요.

     첨부파일은 파일당 25MB로 제한됩니다. 다음 파일 확장자가 지원됩니다: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv.
   - 사건 종결: 사건을 종결하는 이유를 자세히 입력하고 *사건 종결*을 선택하세요.

NetApp Data Classification 에 대한 자주 묻는 질문

이 FAQ는 질문에 대한 빠른 답변을 찾는 데 도움이 될 수 있습니다.

NetApp Data Classification

다음 질문은 데이터 분류에 대한 일반적인 이해를 제공합니다.

데이터 분류는 어떻게 작동하나요?

데이터 분류는 NetApp Console 시스템 및 스토리지 시스템과 함께 또 다른 계층의 AI를 배포합니다. 그런 다음 볼륨, 버킷, 데이터베이스 및 기타 스토리지 계정의 데이터를 스캔하고 발견된 데이터 통찰력을 인덱싱합니다. 데이터 분류는 일반적으로 정규 표현식과 패턴 매칭을 중심으로 구축되는 대체 솔루션과 달리 인공 지능과 자연어 처리를 모두 활용합니다.

데이터 분류는 AI를 사용하여 데이터에 대한 맥락적 이해를 제공하여 정확한 탐지 및 분류를 제공합니다. 최신 데이터 유형과 규모에 맞춰 설계되었기 때문에 AI를 기반으로 합니다. 또한 강력하고 정확한 검색 및 분류를 제공하기 위해 데이터 컨텍스트를 이해합니다.

"데이터 분류가 작동하는 방식에 대해 자세히 알아보세요" .

데이터 분류에 **REST API**가 있나요? 타사 도구와도 호환되나요?

네, 데이터 분류에는 콘솔 핵심 플랫폼의 일부인 데이터 분류 버전의 지원되는 기능에 대한 REST API가 있습니다. 보다 "API 문서" .

클라우드 마켓플레이스를 통해 데이터 분류를 이용할 수 있나요?

데이터 분류는 NetApp Console 핵심 기능의 일부이므로 이 서비스를 위해 마켓플레이스를 사용할 필요가 없습니다.

데이터 분류 스캐닝 및 분석

다음 질문은 데이터 분류 스캐닝 성능과 분석과 관련이 있습니다.

데이터 분류는 얼마나 자주 데이터를 스캔합니까?

데이터를 처음 검사하는 데는 시간이 조금 걸릴 수 있지만, 이후 검사에서는 증분적인 변경 사항만 검사하므로 시스템 검사 시간이 줄어듭니다. 데이터 분류는 한 번에 6개의 저장소에서 라운드 로빈 방식으로 데이터를 지속적으로 스캔하므로 변경된 모든 데이터가 매우 빠르게 분류됩니다.

"스캔 작동 방식 알아보기" .

데이터 분류는 하루에 한 번만 데이터베이스를 스캔합니다. 데이터베이스는 다른 데이터 소스처럼 지속적으로 스캔되지 않습니다.

데이터 스캔은 저장 시스템과 데이터에 미치는 영향이 미미합니다.

스캔 성능은 다양합니까?

검사 성능은 네트워크 대역폭과 사용자 환경의 평균 파일 크기에 따라 달라질 수 있습니다. 또한 호스트 시스템(클라우드 또는 온프레미스)의 크기 특성에 따라 달라질 수 있습니다. 다음을 참조하세요. "데이터 분류 인스턴스" 그리고 "데이터 분류 배포" 자세한 내용은.

처음에 새로운 데이터 소스를 추가할 때 전체 "분류"(맵 및 분류) 스캔 대신 "매핑"(매핑만) 스캔만 수행하도록 선택할 수도 있습니다. 데이터 내부에 있는 데이터를 보기 위해 파일에 접근하지 않기 때문에 데이터 소스에서 매우 빠르게 매핑을 수행할 수 있습니다. "매핑 스캔과 분류 스캔의 차이점을 확인하세요" .

데이터 분류를 사용하여 데이터를 검색할 수 있나요?

데이터 분류는 모든 연결된 소스에서 특정 파일이나 데이터를 쉽게 검색할 수 있는 광범위한 검색 기능을 제공합니다. 데이터 분류를 통해 사용자는 메타데이터가 반영하는 것 이상의 심층적인 검색을 수행할 수 있습니다. 이름, ID 등 다양한 민감한 데이터 유형을 읽고 분석할 수 있는 언어에 구애받지 않는 서비스입니다. 예를 들어, 사용자는 구조화된 데이터 저장소와 구조화되지 않은 데이터 저장소를 모두 검색하여 회사 정책을 위반하여 데이터베이스에서 사용자 파일로 유출되었을 수 있는 데이터를 찾을 수 있습니다. 검색 결과는 나중에 사용할 수 있도록 저장할 수 있으며, 정책을 만들어서 일정 빈도로 검색 결과를 검색하고 조치를 취할 수 있습니다.

관심 있는 파일을 찾으면 태그, 시스템 계정, 버킷, 파일 경로, 범주(분류에서 가져옴), 파일 크기, 마지막 수정, 권한 상태, 중복, 민감도 수준, 개인 데이터, 파일 내의 민감한 데이터 유형, 소유자, 파일 유형, 파일 크기, 생성 시간, 파일 해시, 데이터가 주의를 끌기 위해 누군가에게 할당되었는지 여부 등의 특성을 나열할 수 있습니다. 필터를 적용하면 관련성이 없는 특성을 걸러낼 수 있습니다.

데이터 분류에는 역할 기반 액세스 제어(RBAC) 기능도 있어 적절한 권한이 있는 경우 파일을 이동하거나 삭제할 수 있습니다. 적절한 권한이 없는 경우, 해당 작업은 조직 내에서 적절한 권한이 있는 사람에게 할당될 수 있습니다.

데이터 분류 관리 및 개인 정보 보호

다음 질문은 데이터 분류 및 개인정보 보호 설정을 관리하는 방법에 대한 정보를 제공합니다.

데이터 분류를 활성화하거나 비활성화하려면 어떻게 해야 하나요?

먼저 콘솔이나 온프레미스 시스템에 데이터 분류 인스턴스를 배포해야 합니다. 인스턴스가 실행되면 구성 탭에서 또는 특정 시스템을 선택하여 기존 시스템, 데이터베이스 및 기타 데이터 소스에서 서비스를 활성화할 수 있습니다. "시작하는 방법을 알아보세요" .

> 데이터 소스에서 데이터 분류를 활성화하면 즉각적인 초기 검사가 수행됩니다. 검사 결과는 곧 표시됩니다.

데이터 분류 구성 페이지에서 개별 시스템, 데이터베이스 또는 파일 공유 그룹을 스캔하는 데이터 분류를 비활성화할 수 있습니다. 보다 "데이터 분류에서 데이터 소스 제거" .

데이터 분류 인스턴스를 완전히 제거하려면 클라우드 공급자의 포털이나 온프레미스 위치에서 데이터 분류 인스턴스를 수동으로 제거하세요.

이 서비스는 특정 디렉토리의 스캐닝 데이터를 제외할 수 있나요?

네. 특정 데이터 소스 디렉토리에 있는 스캐닝 데이터를 데이터 분류에서 제외하려면 분류 엔진에 해당 목록을 제공하면 됩니다. 해당 변경 사항을 적용하면 데이터 분류에서 지정된 디렉토리의 스캐닝 데이터가 제외됩니다. "자세히 알아보기" .

ONTAP 볼륨에 있는 스냅샷이 스캔되나요?

아니요. 데이터 분류는 스냅샷을 스캔하지 않습니다. 콘텐츠가 볼륨의 콘텐츠와 동일하기 때문입니다.

ONTAP 볼륨에서 데이터 계층화가 활성화되면 어떻게 되나요?

데이터 분류가 매핑 전용 스캔을 사용하여 개체 스토리지에 계층화된 콜드 데이터가 있는 볼륨을 스캔하는 경우 로컬 디스크에 있는 데이터와 개체 스토리지에 계층화된 콜드 데이터를 포함한 모든 데이터를 스캔합니다. 이는 계층화를 구현하는 NetApp 이외의 제품에도 해당됩니다.

매핑 전용 스캔은 콜드 데이터를 가열하지 않습니다. 콜드 데이터는 그대로 유지되며 개체 스토리지에 남아 있습니다. 반면, Map & Classify 스캔을 수행하는 경우 일부 구성에서 콜드 데이터가 가열될 수 있습니다.

소스 시스템 및 데이터 유형의 유형

다음 질문은 스캔할 수 있는 저장소 유형과 스캔되는 데이터 유형과 관련이 있습니다.

정부 지역에 배치될 때 제한 사항이 있나요?

콘솔 에이전트가 정부 지역(AWS GovCloud, Azure Gov 또는 Azure DoD)에 배포된 경우 데이터 분류가 지원됩니다. 이를 "제한 모드"라고도 합니다.

인터넷 접속이 불가능한 사이트에 데이터 분류를 설치하면 어떤 데이터 소스를 스캔할 수 있나요?

> BlueXP 개인 모드(레거시 BlueXP 인터페이스)는 일반적으로 인터넷 연결이 없고 AWS Secret Cloud, AWS Top Secret Cloud, Azure IL6를 포함하는 보안 클라우드 지역이 있는 온프레미스 환경에서 사용됩니다. NetApp 기존 BlueXP 인터페이스를 통해 이러한 환경을 계속 지원합니다. 레거시 BlueXP 인터페이스의 개인 모드 설명서는 다음을 참조하세요."BlueXP 개인 모드에 대한 PDF 문서" .

데이터 분류는 온프레미스 사이트의 로컬 데이터 소스에서만 데이터를 스캔할 수 있습니다. 현재 데이터 분류는 다음과 같은 로컬 데이터 소스를 "비공개 모드"(다크 사이트라고도 함)에서 스캔할 수 있습니다.

- 온프레미스 ONTAP 시스템
- 데이터베이스 스키마
- S3(Simple Storage Service) 프로토콜을 사용하는 개체 스토리지

어떤 파일 형식이 지원되나요?

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
```

데이터 분류는 어떤 종류의 데이터와 메타데이터를 수집합니까?

데이터 분류를 사용하면 데이터 소스에 대한 일반적인 "매핑" 스캔이나 전체 "분류" 스캔을 실행할 수 있습니다. 매핑은 데이터에 대한 개략적인 개요만 제공하는 반면, 분류는 데이터에 대한 심층적인 스캐닝을 제공합니다. 데이터 내부에 있는 데이터를 보기 위해 파일에 접근하지 않기 때문에 데이터 소스에서 매우 빠르게 매핑을 수행할 수 있습니다.

- 데이터 매핑 스캔(매핑 전용 스캔): 데이터 분류는 메타데이터만 스캔합니다. 이는 전반적인 데이터 관리 및 거버넌스, 신속한 프로젝트 범위 설정, 대규모 자산 및 우선 순위 지정에 유용합니다. 데이터 매핑은 메타데이터를 기반으로 하며 빠른 스캔으로 간주됩니다.

  빠른 검사 후 데이터 매핑 보고서를 생성할 수 있습니다. 이 보고서는 기업 데이터 소스에 저장된 데이터에 대한 개요를 제공하며, 이를 통해 리소스 활용, 마이그레이션, 백업, 보안 및 규정 준수 프로세스에 대한 의사 결정을 내리는 데 도움이 됩니다.

- 데이터 분류 심층 스캔(맵 및 분류 스캔): 데이터 분류는 표준 프로토콜과 사용자 환경 전반의 읽기 전용 권한을 사용하여 데이터를 스캔합니다. 민감한 비즈니스 관련 데이터, 개인 정보, 랜섬웨어 관련 문제를 확인하기 위해 일부 파일을 열어서 검사합니다.

  전체 검사 후에는 데이터 조사 페이지에서 데이터 보기 및 세분화, 파일 내에서 이름 검색, 소스 파일 복사, 이동 및 삭제 등 데이터에 적용할 수 있는 추가 데이터 분류 기능이 많이 있습니다.

데이터 분류는 파일 이름, 권한, 생성 시간, 마지막 액세스, 마지막 수정과 같은 메타데이터를 캡처합니다. 여기에는 데이터 조사 세부 정보 페이지와 데이터 조사 보고서에 나타나는 모든 메타데이터가 포함됩니다.

데이터 분류를 통해 개인 정보(PII) 및 민감한 개인 정보(SPII) 등 다양한 유형의 비공개 데이터를 식별할 수 있습니다. 개인 정보에 대한 자세한 내용은 다음을 참조하세요.데이터 분류가 스캔하는 개인 데이터 범주 .

데이터 분류 정보를 특정 사용자에게만 제한할 수 있나요?

네, 데이터 분류는 NetApp Console 과 완벽하게 통합되어 있습니다. NetApp Console 사용자는 자신의 권한에 따라 볼 수 있는 시스템에 대한 정보만 볼 수 있습니다.

또한, 특정 사용자가 데이터 분류 설정을 관리할 수 없도록 데이터 분류 검사 결과만 볼 수 있도록 허용하려면 해당 사용자에게 분류 뷰어 역할(NetApp Console 표준 모드로 사용하는 경우) 또는 규정 준수 뷰어 역할(NetApp Console 제한 모드로 사용하는 경우)을 할당할 수 있습니다. "자세히 알아보기" .

내 브라우저와 데이터 분류 간에 전송되는 개인 데이터에 누구든지 접근할 수 있나요?

아니요. 브라우저와 데이터 분류 인스턴스 간에 전송되는 개인 데이터는 TLS 1.2를 사용하여 종단 간 암호화로 보호되므로 NetApp 과 비 NetApp 당사자는 해당 데이터를 읽을 수 없습니다. 데이터 분류는 귀하가 액세스를 요청하고 승인하지 않는 한 NetApp 과 어떠한 데이터나 결과도 공유하지 않습니다.

스캔된 데이터는 사용자 환경 내에 유지됩니다.

민감한 데이터는 어떻게 처리되나요?

NetApp 민감한 데이터에 액세스할 수 없으며 이를 UI에 표시하지 않습니다. 민감한 데이터는 가려집니다. 예를 들어, 신용카드 정보의 경우 마지막 4자리 숫자가 표시됩니다.

데이터는 어디에 저장되나요?

검사 결과는 데이터 분류 인스턴스 내의 Elasticsearch에 저장됩니다.

데이터에 어떻게 접근하나요?

데이터 분류는 API 호출을 통해 Elasticsearch에 저장된 데이터에 액세스하는데, 이 때 인증이 필요하고 AES-128을 사용하여 암호화됩니다. Elasticsearch에 직접 액세스하려면 루트 액세스가 필요합니다.

라이센스 및 비용

다음 질문은 데이터 분류 사용에 따른 라이선스 및 비용과 관련이 있습니다.

데이터 분류 비용은 얼마인가요?

데이터 분류는 NetApp Console 핵심 기능입니다. 충전되지 않았습니다.

콘솔 에이전트 배포

다음 질문은 콘솔 에이전트와 관련이 있습니다.

콘솔 에이전트란 무엇인가요?

콘솔 에이전트는 클라우드 계정 내부 또는 온프레미스의 컴퓨팅 인스턴스에서 실행되는 소프트웨어로, NetApp Console 클라우드 리소스를 안전하게 관리할 수 있도록 해줍니다. 데이터 분류를 사용하려면 콘솔 에이전트를 배포해야 합니다.

콘솔 에이전트는 어디에 설치해야 합니까?

데이터를 스캔할 때 NetApp Console 에이전트를 다음 위치에 설치해야 합니다.

- AWS의 Cloud Volumes ONTAP 또는 Amazon FSx for ONTAP 의 경우: 콘솔 에이전트가 AWS에 있습니다.
- Azure 또는 Azure NetApp Files 의 Cloud Volumes ONTAP 의 경우: 콘솔 에이전트가 Azure에 있습니다.
- GCP의 Cloud Volumes ONTAP 의 경우: 콘솔 에이전트가 GCP에 있습니다.
- 온프레미스 ONTAP 시스템의 경우: 콘솔 에이전트는 온프레미스에 있습니다.

이러한 위치에 데이터가 있는 경우 다음을 사용해야 할 수 있습니다. "여러 콘솔 에이전트" .

데이터 분류에 자격 증명에 대한 액세스가 필요합니까?

데이터 분류 자체는 저장소 자격 증명을 검색하지 않습니다. 대신 콘솔 에이전트에 저장됩니다.

데이터 분류는 스캔하기 전에 공유를 마운트하기 위해 CIFS 자격 증명과 같은 데이터 플레인 자격 증명을 사용합니다.

서비스와 콘솔 에이전트 간의 통신은 **HTTP**를 사용합니까?

네, 데이터 분류는 HTTP를 사용하여 콘솔 에이전트와 통신합니다.

데이터 분류 배포

다음 질문은 별도의 데이터 분류 인스턴스와 관련이 있습니다.

데이터 분류는 어떤 배포 모델을 지원합니까?

NetApp Console 사용하면 사용자는 온프레미스, 클라우드, 하이브리드 환경을 포함한 거의 모든 곳에서 시스템을 검사하고 보고할 수 있습니다. 데이터 분류는 일반적으로 SaaS 모델을 사용하여 배포됩니다. 즉, 서비스는 콘솔 인터페이스를 통해 활성화되며 하드웨어나 소프트웨어를 설치할 필요가 없습니다. 이러한 클릭 앤 런 배포 모드에서도 데이터 저장소가 온프레미스에 있든 퍼블릭 클라우드에 있든 관계없이 데이터 관리를 수행할 수 있습니다.

데이터 분류에는 어떤 유형의 인스턴스 또는 VM이 필요합니까?

언제"클라우드에 배포됨" :

- AWS에서 데이터 분류는 500GiB GP2 디스크가 있는 m6i.4xlarge 인스턴스에서 실행됩니다. 배포 중에 더 작은 인스턴스 유형을 선택할 수 있습니다.
- Azure에서 데이터 분류는 500GiB 디스크가 있는 Standard_D16s_v3 VM에서 실행됩니다.
- GCP에서 데이터 분류는 500GiB Standard 영구 디스크가 있는 n2-standard-16 VM에서 실행됩니다.

"데이터 분류가 작동하는 방식에 대해 자세히 알아보세요" .

내 호스트에 데이터 분류를 배포할 수 있나요?

네. 네트워크나 클라우드에서 인터넷 접속이 가능한 Linux 호스트에 데이터 분류 소프트웨어를 설치할 수 있습니다. 모든 것이 동일하게 작동하며 콘솔을 통해 스캔 구성과 결과를 계속 관리할 수 있습니다. 보다"온프레미스에 데이터 분류 배포" 시스템 요구 사항 및 설치 세부 정보를 확인하세요.

인터넷 접속이 불가능한 보안 사이트는 어떻게 되나요?

네, 그것도 지원됩니다. 당신은 할 수 있습니다"인터넷 접속이 불가능한 온프레미스 사이트에 데이터 분류 배포" 완벽하게 안전한 사이트를 위해.

법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인정보 보호정책

"https://www.netapp.com/company/legal/privacy-policy/"

오픈소스

공지 파일은 NetApp 소프트웨어에서 사용되는 타사 저작권 및 라이선스에 대한 정보를 제공합니다.

- "NetApp Console 에 대한 알림"
- "NetApp Data Classification 에 대한 공지"