BlueXP 분류 문서

BlueXP classification

NetApp
April 03, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/bluexp-classification/index.html on April 03, 2024. Always check docs.netapp.com for the latest.

목차

BlueXP 분류 문서 . . . 1
릴리스 정보 . . . 2
- BlueXP 분류의 새로운 기능 . . . 2
- 알려진 제한 사항 . . . 8

시작하십시오 . . . 10
- BlueXP 분류에 대해 알아보십시오 . . . 10
- BlueXP 분류를 배포합니다 . . . 17
- 데이터 소스에서 스캔을 활성화합니다 . . . 62
- Active Directory를 BlueXP 분류와 통합합니다 . . . 106
- BlueXP 분류 라이선스를 설정합니다 . . . 109
- BlueXP 분류에 대한 질문과 대답 . . . 115

BlueXP 분류를 사용합니다 . . . 124
- 조직에 저장된 데이터에 대한 거버넌스 세부 정보를 봅니다 . . . 124
- 조직에 저장된 데이터에 대한 규정 준수 세부 정보를 봅니다 . . . 130
- 개인 데이터의 범주입니다 . . . 136
- 조직에 저장된 데이터를 조사합니다 . . . 142
- 개인 데이터를 구성합니다 . . . 151
- 데이터에 정책을 할당합니다 . . . 160
- 개인 데이터를 관리합니다 . . . 171
- 규정 준수 보고서 보기 . . . 181

BlueXP 분류 관리 . . . 188
- BlueXP 분류 스캔에 개인 데이터 식별자를 추가합니다 . . . 188
- BlueXP 분류 검사에서 특정 디렉토리를 제외합니다 . . . 203
- 준수 작업의 상태 보기 . . . 206
- 추가 그룹 ID를 조직에 공개됨으로 정의합니다 . . . 207
- BlueXP 분류 작업의 이력을 감사합니다 . . . 208
- BlueXP 분류 스캔 속도를 줄입니다 . . . 209
- BlueXP 분류에서 데이터 소스 제거 . . . 210
- BlueXP 분류를 제거하는 중입니다 . . . 212

참조하십시오 . . . 214
- 지원되는 BlueXP 분류 인스턴스 유형 . . . 214
- 데이터 소스에서 수집된 메타데이터 . . . 215
- BlueXP 분류 시스템에 로그인합니다 . . . 216
- BlueXP 분류 API . . . 217

지식 및 지원 . . . 228
- 지원을 위해 등록하십시오 . . . 228
- 도움을 받으십시오 . . . 232

법적 고지 . . . 238
- 저작권 . . . 238

상표 238
특허 238
개인 정보 보호 정책 238
오픈 소스 238

BlueXP 분류 문서

릴리스 정보

BlueXP 분류의 새로운 기능

BlueXP 분류의 새로운 기능 (Cloud Data Sense)을 알아봅니다.

2024년 4월 1일(버전 1.30)

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

이 릴리스는 이전에 지원되는 9.x 외에도 Red Hat Enterprise Linux v8.8 및 v9.3에 대한 지원을 제공하며, Docker 엔진 대신 Podman이 필요합니다. 이는 BlueXP 분류의 수동 온프레미스 설치에 적용할 수 있습니다.

Podman 컨테이너 엔진을 사용해야 하는 운영 체제에는 BlueXP 분류 버전 1.30 이상이 필요합니다. Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3 이상이 필요합니다.

에 대해 자세히 알아보십시오 "BlueXP 분류 구축 개요".

감사 로그 수집을 활성화하는 옵션이 제거되었습니다

감사 로그 수집을 활성화하는 옵션이 비활성화되었습니다.

스캔 속도가 향상되었습니다

보조 스캐너 노드의 스캔 성능이 향상되었습니다. 스캔 처리 능력이 추가로 필요한 경우 스캐너 노드를 더 추가할 수 있습니다. 자세한 내용은 을 참조하십시오 "인터넷에 액세스할 수 있는 호스트에 BlueXP 분류를 설치합니다".

자동 업그레이드

인터넷에 액세스할 수 있는 시스템에 BlueXP 분류를 구축한 경우 시스템이 자동으로 업그레이드됩니다. 이전에는 마지막 사용자 작업 이후 특정 시간이 경과한 후에 업그레이드가 발생했습니다. 이 릴리즈에서는 현지 시간이 오전 1시에서 오전 5시 사이인 경우 BlueXP 분류가 자동으로 업그레이드됩니다. 로컬 시간이 이 시간을 벗어난 경우 마지막 사용자 작업 이후 특정 시간이 경과하면 업그레이드가 수행됩니다. 자세한 내용은 을 참조하십시오 "인터넷에 액세스할 수 있는 Linux 호스트에 설치합니다".

인터넷에 액세스하지 않고 BlueXP 분류를 구축한 경우 수동으로 업그레이드해야 합니다. 자세한 내용은 을 참조하십시오 "인터넷에 액세스할 수 없는 Linux 호스트에 BlueXP 분류를 설치합니다".

2024년 3월 4일(버전 1.29)

이제 특정 데이터 소스 디렉토리에 있는 데이터 검사를 제외할 수 있습니다

BlueXP 분류를 통해 특정 데이터 소스 디렉토리에 있는 스캔 데이터를 제외하려면 이러한 디렉토리 이름을 BlueXP 분류 프로세스를 수행하는 구성 파일에 추가할 수 있습니다. 이 기능을 사용하면 불필요한 디렉터리를 검색하지 않거나 잘못된 개인 데이터 결과를 반환할 수 있습니다.

"자세한 정보".

이제 더 큰 인스턴스 지원이 가능합니다

2억 5천만 개 이상의 파일을 스캔하기 위해 BlueXP 분류가 필요한 경우 클라우드 구축 또는 온프레미스 설치에서 초대형 인스턴스를 사용할 수 있습니다. 이 유형의 시스템은 최대 5억 개의 파일을 스캔할 수 있습니다.

"자세한 정보".

2024년 1월 10일(버전 1.27)

이제 조사 페이지 결과에 총 항목 수와 함께 총 크기가 표시됩니다

이제 조사 페이지의 필터링된 결과에 총 파일 수와 함께 항목의 총 크기가 표시됩니다. 이 기능은 파일 이동, 파일 삭제 등에 도움이 될 수 있습니다.

추가 그룹 **ID**를 **"**조직에 열기**"**로 구성

이제 그룹이 처음에 해당 권한으로 설정되지 않은 경우, NFS의 그룹 ID를 BlueXP 분류에서 직접 "Open to Organization"으로 간주하도록 구성할 수 있습니다. 이러한 그룹 ID가 첨부된 파일 및 폴더는 조사 세부 정보 페이지에서 "조직에 열기"로 표시됩니다. 자세한 내용은 를 참조하십시오 "추가 그룹 ID를 "조직에 열려 있음"으로 추가".

2023년 12월 14일(버전 1.26.6)

이 릴리스에는 몇 가지 사소한 개선 사항이 포함되어 있습니다.

이 릴리스에서는 다음 옵션도 일시적으로 제거되었습니다.

- 감사 로그 수집을 활성화하는 옵션이 비활성화되었습니다. 을 참조하십시오 "파일 액세스 이벤트 모니터링 및 관리".
- 디렉터리 조사 중에는 디렉터리별 개인 식별 정보(PII) 데이터 수를 계산하는 옵션을 사용할 수 없습니다. 을 참조하십시오 "조직에 저장된 데이터를 조사합니다".
- AIP(Azure Information Protection) 레이블을 사용하여 데이터를 통합하는 옵션이 비활성화되었습니다. 을 참조하십시오 "개인 데이터를 구성합니다".

2023년 11월 6일(버전 1.26.3)

이 릴리스에서는 다음 문제가 해결되었습니다

- 시스템에서 스캔된 파일 수를 대시보드에 표시할 때 불일치 문제가 해결되었습니다.
- 이름 및 메타데이터에 특수 문자가 있는 파일과 디렉터리를 처리하고 보고함으로써 검색 동작을 개선했습니다.

2023년 10월 4일(버전 1.26)

RHEL 버전 **9**에서 **BlueXP** 분류의 사내 설치를 지원합니다

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

현재 RHEL 9.x를 사용하는 경우 다크 사이트 설치 또는 분산 스캐닝 환경(마스터 및 원격 스캐너 노드 사용)은 지원되지

않습니다

2023년 9월 5일(버전 1.25)

중소 규모 구축은 일시적으로 사용할 수 없습니다

AWS에 BlueXP 분류의 인스턴스를 구축할 때 * Deploy > Configuration * 을 선택하고 소형 또는 중형 인스턴스를 선택하는 옵션은 현재 사용할 수 없습니다. Deploy > Deploy * 를 선택하여 대규모 인스턴스 크기를 사용하여 인스턴스를 배포할 수 있습니다.

조사 결과 페이지에서 최대 **100,000**개의 항목에 태그를 적용합니다

이전에는 조사 결과 페이지에서 한 번에 한 페이지에만 태그를 적용할 수 있었습니다(20개 항목). 이제 조사 결과 페이지에서 * 모든 * 항목을 선택하고 모든 항목에 태그를 적용할 수 있습니다. 한 번에 최대 100,000개 항목까지 가능합니다. "방법을 확인하십시오".

최소 파일 크기가 **1MB**인 중복 파일을 식별합니다

BlueXP 분류는 파일이 50MB 이상인 경우에만 중복된 파일을 식별하는 데 사용됩니다. 이제 1MB로 시작하는 중복 파일을 식별할 수 있습니다. 조사 페이지에서 "파일 크기"와 "중복 항목"을 필터링하여 사용자 환경에서 특정 크기의 파일이 복제되었는지 확인할 수 있습니다.

2023년 7월 17일(버전 1.24)

BlueXP 분류에서는 두 가지 새로운 유형의 독일 개인 데이터를 식별합니다

BlueXP 분류는 다음과 같은 유형의 데이터가 포함된 파일을 식별하고 분류할 수 있습니다.

- 독일어 ID(Personalausweummer)
- 독일 사회 보장 번호(소지아버서머스무머)

"BlueXP 분류에서 데이터에서 식별할 수 있는 모든 개인 데이터 유형을 확인하십시오".

BlueXP 분류는 제한 모드 및 비공개 모드에서 완전히 지원됩니다

현재 BlueXP 분류는 인터넷 액세스(비공개 모드)가 없는 사이트와 제한된 아웃바운드 인터넷 액세스(제한 모드)에서 완벽하게 지원됩니다. "Connector의 BlueXP 배포 모드에 대해 자세히 알아보십시오".

BlueXP 분류의 비공개 모드 설치를 업그레이드할 때 버전을 건너뛸 수 있습니다

이제 순차적이지 않더라도 최신 버전의 BlueXP 분류로 업그레이드할 수 있습니다. 즉, 한 번에 한 버전씩 BlueXP 분류를 업그레이드할 때 현재 제한이 없어진다는 의미입니다. 이 기능은 버전 1.24 이상부터 관련이 있습니다.

BlueXP 분류 **API**가 이제 제공됩니다

BlueXP 분류 API를 사용하면 작업을 수행하고, 쿼리를 생성하고, 스캔하는 데이터에 대한 정보를 내보낼 수 있습니다. 대화형 설명서는 Swagger를 사용하여 사용할 수 있습니다. 문서는 조사, 규정 준수, 거버넌스 및 구성을 포함한 여러 범주로 구분됩니다. 각 범주는 BlueXP 분류 UI의 탭에 대한 참조입니다.

"BlueXP 분류 API에 관해 자세히 알아보십시오".

2023년 6월 6일(버전 1.23)

이제 데이터 제목 이름을 검색할 때 일본어가 지원됩니다

Data Subject Access Request(SAR)에 대한 응답으로 시험대상자 이름을 검색할 때 일본어 이름을 입력할 수 있습니다. 을 생성할 수 있습니다 "데이터 주체 액세스 요청 보고서" 결과 정보를 사용합니다. 에 일본어 이름을 입력할 수도 있습니다 "데이터 조사 페이지의 "데이터 제목" 필터" 제목 이름이 포함된 파일을 식별합니다.

Ubuntu는 이제 **BlueXP** 분류를 설치할 수 있는 지원되는 **Linux** 배포판입니다

Ubuntu 22.04는 BlueXP 분류에 지원되는 운영 체제로 검증되었습니다. 설치 프로그램의 버전 1.23을 사용하는 경우 네트워크의 Ubuntu Linux 호스트 또는 클라우드의 Linux 호스트에 BlueXP 분류를 설치할 수 있습니다. "Ubuntu가 설치된 호스트에 BlueXP 분류를 설치하는 방법을 참조하십시오".

Red Hat Enterprise Linux 8.6과 **8.7**은 새로운 **BlueXP** 분류 설치에서 더 이상 지원되지 않습니다

Red Hat은 더 이상 Docker를 지원하지 않으므로 이러한 버전은 새로운 배포에서 지원되지 않습니다. RHEL 8.6 또는 8.7에서 기존 BlueXP 분류 시스템을 실행 중인 경우 NetApp는 계속해서 구성을 지원합니다.

ONTAP 시스템에서 **FPolicy** 이벤트를 수신하려면 **BlueXP** 분류를 **FPolicy Collector**로 구성할 수 있습니다

BlueXP 분류 시스템에서 파일 액세스 감사 로그를 수집하여 작업 환경의 볼륨에서 감지된 파일 액세스 이벤트를 처리할 수 있습니다. BlueXP 분류는 다음 유형의 FPolicy 이벤트와 파일에서 작업을 수행한 사용자, 즉 만들기, 읽기, 쓰기, 삭제, 이름 바꾸기, 소유자/권한을 변경하고 SACL/DACL을 변경합니다. "파일 액세스 이벤트를 모니터링하고 관리하는 방법을 확인하십시오".

이제 **Data Sense BYOL** 라이센스가 다크 사이트에서 지원됩니다

이제 데이터 감지 BYOL 라이센스를 어두운 사이트의 BlueXP 디지털 지갑에 업로드하여 라이센스가 낮아지면 알림을 받을 수 있습니다. "Data Sense BYOL 라이센스를 획득하고 업로드하는 방법을 알아보십시오".

2023년 4월 3일(버전 1.22)

새로운 데이터 검색 평가 보고서

데이터 검색 평가 보고서는 스캔한 환경에 대한 상위 수준의 분석을 통해 시스템의 결과를 강조하고 문제 영역 및 잠재적인 개선 단계를 보여줍니다. 이 보고서의 목표는 데이터 거버넌스 문제, 데이터 보안 노출 및 데이터 세트의 데이터 규정 준수 공백에 대한 인식을 높이는 것입니다. "데이터 검색 평가 보고서를 생성하고 사용하는 방법을 확인하십시오".

클라우드 내 소규모 인스턴스에 **BlueXP** 분류 기능을 배포할 수 있습니다

AWS 환경의 BlueXP Connector에서 BlueXP 분류를 배포할 때 이제 기본 인스턴스에서 사용할 수 있는 것보다 두 가지 작은 인스턴스 유형 중에서 선택할 수 있습니다. 소규모 환경을 스캔하면 클라우드 비용을 절감할 수 있습니다. 그러나 더 작은 인스턴스를 사용할 때는 몇 가지 제한 사항이 있습니다. "사용 가능한 인스턴스 유형 및 제한 사항을 참조하십시오".

이제 **BlueXP** 분류 설치 전에 독립 실행형 스크립트를 사용하여 **Linux** 시스템을 검증할 수 있습니다

Linux 시스템이 BlueXP 분류 설치를 실행하는 것과 관계없이 모든 필수 구성 요소를 충족하는지 확인하려면 사전 요구 사항에 대한 테스트만 다운로드할 수 있는 별도의 스크립트가 있습니다. "Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인하는 방법을 참조하십시오".

2023년 3월 7일(버전 1.21)

BlueXP 분류 **UI**에서 사용자 지정 범주를 추가하는 새로운 기능

이제 BlueXP 분류를 통해 사용자 지정 범주를 추가할 수 있으므로 BlueXP 분류에서 해당 범주에 적합한 파일을 식별할 수 있습니다. BlueXP 분류에는 많은 기능이 있습니다 "미리 정의된 범주"따라서 이 기능을 사용하면 사용자 지정 범주를 추가하여 조직에서 고유한 정보를 데이터에서 찾을 위치를 식별할 수 있습니다.

"자세한 정보".

이제 **BlueXP** 분류 **UI**에서 사용자 지정 키워드를 추가할 수 있습니다

BlueXP 분류에서는 BlueXP 분류가 향후 검색에서 식별할 수 있는 사용자 지정 키워드를 추가할 수 있었습니다. 그러나 BlueXP 분류 Linux 호스트에 로그인하고 명령줄 인터페이스를 사용하여 키워드를 추가해야 합니다. 이 릴리스에서 사용자 지정 키워드를 추가하는 기능은 BlueXP 분류 UI에 포함되어 있으므로 이러한 키워드를 쉽게 추가하고 편집할 수 있습니다.

"BlueXP 분류 UI에서 사용자 지정 키워드를 추가하는 방법에 대해 자세히 알아보십시오".

"마지막 액세스 시간**"**이 변경될 때 **BlueXP** 분류 * 파일 * 스캔 기능이 없음

기본적으로 BlueXP 분류에 적절한 "쓰기" 권한이 없으면 BlueXP 분류가 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 볼륨의 파일을 검색하지 않습니다. 그러나 파일의 마지막 액세스 시간이 원래 시간으로 재설정되는 것을 염려하지 않을 경우, BlueXP 분류가 권한에 관계없이 볼륨을 스캔하도록 구성 페이지에서 이 동작을 재정의할 수 있습니다.

이 기능과 함께 "Scan Analysis Event"라는 새 필터가 추가되어 BlueXP 분류로 마지막으로 액세스한 시간을 되돌릴 수 없거나, BlueXP 분류로 마지막으로 액세스한 시간을 되돌릴 수 없는 경우에도 분류된 파일을 볼 수 있습니다.

""마지막 액세스 시간 타임스탬프" 및 BlueXP 분류에 필요한 권한에 대해 자세히 알아보십시오".

BlueXP 분류에서는 세 가지 새로운 유형의 개인 데이터를 식별합니다

BlueXP 분류는 다음과 같은 유형의 데이터가 포함된 파일을 식별하고 분류할 수 있습니다.

- 보츠와나 ID 카드(오만) 번호
- 보츠와나 여권 번호
- 싱가포르 국가 등록 ID 카드(NRIC)

"BlueXP 분류에서 데이터에서 식별할 수 있는 모든 개인 데이터 유형을 확인하십시오".

디렉토리의 기능이 업데이트되었습니다

- 이제 데이터 조사 보고서에 대한 "Light CSV Report(라이트 CSV 보고서)" 옵션에 디렉토리의 정보가 포함됩니다.
- 이제 "마지막 액세스" 시간 필터에 파일과 디렉터리 모두의 마지막 액세스 시간이 표시됩니다.

설치 개선 사항

- 인터넷 접속(다크 사이트)이 없는 사이트의 BlueXP 분류 설치 관리자가 사전 검사를 수행하여 성공적인 설치를 위해 시스템 및 네트워킹 요구 사항이 제대로 갖추어져 있는지 확인합니다.

- 설치 감사 로그 파일은 지금 저장되며 에 기록됩니다 `/ops/netapp/install_logs`.

2023년 2월 5일(버전 1.20)

모든 이메일 주소로 정책 기반 알림 이메일을 보낼 수 있습니다

이전 버전의 BlueXP 분류에서는 특정 중요 정책이 결과를 반환할 때 계정의 BlueXP 사용자에게 전자 메일 알림을 보낼 수 있습니다. 이 기능을 사용하면 온라인 상태가 아닐 때 데이터를 보호하기 위한 알림을 받을 수 있습니다. 이제 BlueXP 계정에 없는 다른 모든 사용자(최대 20개의 이메일 주소)에게 정책의 이메일 알림을 보낼 수 있습니다.

"정책 결과를 기반으로 이메일 알림을 보내는 방법에 대해 자세히 알아보십시오".

이제 **BlueXP** 분류 **UI**에서 개인 패턴을 추가할 수 있습니다

BlueXP 분류에서는 BlueXP 분류가 향후 검색에서 식별할 수 있는 맞춤형 "개인 데이터"를 추가할 수 있었습니다. 그러나 BlueXP 분류 Linux 호스트에 로그인하고 명령줄을 사용하여 사용자 지정 패턴을 추가해야 합니다. 이번 릴리스에서는 BlueXP 분류 UI에 regex를 사용하여 개인 패턴을 추가할 수 있으므로 이러한 사용자 지정 패턴을 쉽게 추가하고 편집할 수 있습니다.

"BlueXP 분류 UI에서 사용자 지정 패턴을 추가하는 방법에 대해 자세히 알아보십시오".

BlueXP 분류를 사용하여 **1500**만 개의 파일을 이동할 수 있습니다

과거에는 BlueXP 분류로 최대 100,000개의 소스 파일을 NFS 공유로 이동할 수 있었습니다. 이제 한 번에 최대 1,500만 개의 파일을 이동할 수 있습니다. "BlueXP 분류를 사용하여 소스 파일을 이동하는 방법에 대해 자세히 알아보십시오".

SharePoint Online 파일에 액세스할 수 있는 사용자 수를 볼 수 있습니다

"액세스 권한이 있는 사용자 수" 필터는 이제 SharePoint Online 리포지토리에 저장된 파일을 지원합니다. 이전에는 CIFS 공유의 파일만 지원되었습니다. Active Directory 기반이 아닌 SharePoint 그룹은 현재 이 필터에서 계산되지 않습니다.

새 **"**부분 성공**"** 상태가 작업 상태 패널에 추가되었습니다

새로운 "부분 성공" 상태는 BlueXP 분류 작업이 완료되었고 일부 항목이 실패했으며 100개의 파일을 이동하거나 삭제하는 등 일부 항목이 성공했음을 나타냅니다. 또한 "완료됨" 상태의 이름이 "성공"으로 변경되었습니다. 과거에는 "완료" 상태에 성공했고 실패한 작업이 나열될 수 있습니다. 이제 "성공" 상태는 모든 작업이 모든 항목에 성공했음을 의미합니다. "작업 상태 패널을 보는 방법을 참조하십시오".

2023년 1월 9일(버전 1.19)

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

Governance 대시보드에는 중요한 데이터(민감한 개인 데이터 및 민감한 개인 데이터 포함)를 포함하고 지나치게 허용적인 파일의 열 지도를 제공하는 새로운 _Sensitive Data 및 Wide Permissions_영역이 추가되었습니다. 이렇게 하면 민감한 데이터와 관련하여 어떤 위험이 있을 수 있는지 확인할 수 있습니다. "자세한 정보".

데이터 조사 페이지에서 **3**개의 새 필터를 사용할 수 있습니다

새 필터를 사용하여 데이터 조사 페이지에 표시되는 결과를 구체화할 수 있습니다.

- "액세스 권한이 있는 사용자 수" 필터는 특정 수의 사용자에게 열려 있는 파일과 폴더를 표시합니다. 숫자 범위를 선택하여 결과를 구체화할 수 있습니다. 예를 들어 51-100명의 사용자가 액세스할 수 있는 파일을 확인할 수 있습니다.
- 이제 "Created Time(생성 시간)", "Discovered Time(검색 시간)", "Last Modified(마지막 수정)" 및 "Last Accessed(마지막 액세스)" 필터를 사용하여 미리 정의된 날짜 범위를 선택하는 대신 사용자 지정 날짜 범위를 만들 수 있습니다. 예를 들어 "만든 시간", "6개월 이전" 또는 "최근 10일" 내의 "마지막으로 수정한 날짜"가 있는 파일을 찾을 수 있습니다.
- 이제 "파일 경로" 필터를 사용하여 필터링된 쿼리 결과에서 제외할 경로를 지정할 수 있습니다. 특정 데이터를 포함 및 제외하기 위한 경로를 입력하면 BlueXP 분류에서 포함된 경로의 모든 파일을 먼저 찾은 다음 제외된 경로에서 파일을 제거한 다음 결과를 표시합니다.

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

BlueXP 분류는 일본어 개인 번호를 식별할 수 있습니다

BlueXP 분류는 일본어 개인 번호(내 번호라고도 함)가 포함된 파일을 식별하고 분류할 수 있습니다. 여기에는 개인 및 회사 내 번호가 모두 포함됩니다. "BlueXP 분류에서 데이터에서 식별할 수 있는 모든 개인 데이터 유형을 확인하십시오".

알려진 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 기능을 식별합니다. 이러한 제한 사항을 주의 깊게 검토하십시오.

BlueXP 분류 릴리즈에서 옵션이 일시적으로 제거되었습니다

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

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

BlueXP 분류 스캔 제한

BlueXP 분류 기능은 볼륨 아래에서 하나의 공유만 검색합니다

단일 볼륨 아래에 여러 파일 공유가 있는 경우 BlueXP 분류는 가장 높은 계층 구조로 공유를 검색합니다. 예를 들어 다음과 같은 공유가 있는 경우

- /A
- /A/B
- /C
- /D/E

그러면 /A의 데이터가 스캔됩니다. /C 및 /D의 데이터는 스캔되지 않습니다.

해결 방법

볼륨에 있는 모든 공유에서 데이터를 스캔하도록 하는 해결 방법이 있습니다. 다음 단계를 수행하십시오.

1. 작업 환경에서 스캔할 볼륨을 추가합니다.
2. BlueXP 분류가 볼륨 스캔을 완료한 후 _Data Investigation_page로 이동하여 어떤 공유가 스캔되고 있는지 확인하기 위한 필터를 생성합니다.

   "작업 환경 이름" 및 "디렉터리 유형 = 공유"로 데이터를 필터링하여 스캔할 공유를 확인할 수 있습니다.

3. 볼륨에 있는 공유의 전체 목록을 받아 스캔하지 않는 공유를 확인할 수 있습니다.
4. "나머지 공유를 공유 그룹에 추가합니다".

   모든 공유를 개별적으로 추가해야 합니다. 예를 들면 다음과 같습니다.

   ```
   /C
   /D
   ```

5. 여러 공유가 있는 작업 환경의 각 볼륨에 대해 다음 단계를 수행합니다.

시작하십시오

BlueXP 분류에 대해 알아보십시오

BlueXP 분류(Cloud Data Sense)는 기업의 온프레미스 및 클라우드 데이터 소스를 검사하여 데이터를 매핑 및 분류하고 프라이빗 정보를 식별하는 BlueXP용 데이터 거버넌스 서비스입니다. 따라서 보안 및 규정 준수 위험을 줄이고 스토리지 비용을 절감하며 데이터 마이그레이션 프로젝트를 지원할 수 있습니다.

피처

BlueXP 분류에서는 인공 지능(AI), 자연어 처리(NLP) 및 머신 러닝(ML)을 사용하여 엔터티를 추출하고 그에 따라 콘텐츠를 범주화하기 위해 검색하는 콘텐츠를 파악합니다. 이를 통해 BlueXP 분류는 다음과 같은 기능 영역을 제공할 수 있습니다.

"BlueXP 분류의 사용 사례에 대해 자세히 알아보십시오".

규정 준수 유지

BlueXP 분류는 규정 준수 노력에 도움이 되는 여러 가지 도구를 제공합니다. BlueXP 분류를 사용하여 다음을 수행할 수 있습니다.

- 개인 식별 정보(PII)를 식별합니다.
- GDPR, CCPA, PCI 및 HIPAA 개인 정보 보호 규정에서 요구하는 광범위한 민감한 개인 정보를 식별합니다.
- 이름 또는 이메일 주소를 기반으로 Data Subject Access Request(SAR)에 응답합니다.
- 데이터베이스의 고유 식별자가 다른 저장소의 파일에 있는지 확인합니다. 기본적으로 BlueXP 분류 검사에서 식별된 "개인 데이터" 목록을 만듭니다.
- 파일에 특정 PII가 포함된 경우 이메일을 통해 특정 사용자에게 알립니다(을 사용하여 이 기준을 정의합니다 "정책") 따라서 실천 계획을 결정할 수 있습니다.

보안 강화

BlueXP 분류는 범죄 목적으로 액세스할 위험이 있는 데이터를 식별할 수 있습니다. BlueXP 분류를 사용하여 다음을 수행할 수 있습니다.

- 전체 조직 또는 공용 에 노출된 공개 권한으로 모든 파일 및 디렉터리(공유 및 폴더)를 식별합니다.
- 초기 전용 위치 외부에 상주하는 중요한 데이터를 식별합니다.
- 데이터 보존 정책 준수
- 정책 _ 을(를) 사용하여 보안 직원에게 새 보안 문제를 자동으로 통지하여 즉시 조치를 취할 수 있습니다.
- 파일에 사용자 지정 태그(예: "이동해야 함")를 추가하고 BlueXP 사용자를 할당하여 사용자가 파일 업데이트를 소유할 수 있도록 합니다.
- 보고 수정합니다 "AIP(Azure Information Protection) 레이블" 파일을 선택합니다.

스토리지 사용을 최적화합니다

BlueXP 분류는 스토리지 TCO(총 소유 비용)에 도움이 되는 도구를 제공합니다. BlueXP 분류를 사용하여 다음을 수행할 수 있습니다.

- 중복 또는 비업무용 데이터를 식별하여 스토리지 효율성 향상 이 정보를 사용하여 특정 파일을 이동하거나 삭제할 것인지 결정할 수 있습니다.
- 안전하지 않거나 위험한 것으로 보이는 파일을 스토리지 시스템에 남겨 두거나 중복으로 식별한 경우 삭제합니다. Policies_를 사용하여 특정 조건에 맞는 파일을 자동으로 삭제할 수 있습니다.
- 더 저렴한 오브젝트 스토리지에 계층화할 수 있는 비활성 데이터를 식별하여 스토리지 비용 절감 "Cloud Volumes ONTAP 시스템의 계층화에 대해 자세히 알아보십시오". "사내 ONTAP 시스템의 계층화에 대해 자세히 알아보십시오".

데이터 마이그레이션을 가속화

BlueXP 분류는 퍼블릭 또는 프라이빗 클라우드로 마이그레이션하기 전에 사내 데이터를 검사하는 데 사용할 수 있습니다. BlueXP 분류를 사용하여 다음을 수행할 수 있습니다.

- 데이터를 이동하기 전에 데이터의 크기와 데이터에 중요한 정보가 포함되어 있는지 여부를 확인합니다.
- 필요한 파일만 대상으로 이동할 수 있도록 소스 데이터(25가지 이상의 조건 유형 기준)를 필터링합니다. 불필요한 데이터는 이동하지 않습니다.
- 필요한 데이터만 클라우드 저장소로 자동, 복사 또는 동기화합니다.

지원되는 데이터 소스

BlueXP 분류는 다음과 같은 유형의 데이터 소스에서 정형 데이터와 비정형 데이터를 스캔 및 분석할 수 있습니다.

- NetApp: *
- Cloud Volumes ONTAP(AWS, Azure 또는 GCP에 구축)
- 온프레미스 ONTAP 클러스터
- StorageGRID
- Azure NetApp Files
- ONTAP용 Amazon FSx
- Google Cloud용 Cloud Volumes Service
- 비 NetApp: *
- Dell EMC Isilon
- Pure Storage 비교
- 말씀해 주십시오
- 기타 스토리지 공급업체
- 클라우드: *
- Amazon S3
- Google 클라우드 스토리지
- OneDrive 를 클릭합니다

- SharePoint Online을 클릭합니다
- SharePoint 사내(SharePoint Server)
- Google 드라이브
- 데이터베이스: *
- Amazon Relational Database Service(Amazon RDS)
- MongoDB
- MySQL
- 오라클
- PostgreSQL
- SAP HANA를 참조하십시오
- SQL Server(MSSQL)

BlueXP 분류는 NFS 버전 3.x와 CIFS 버전 1.x, 2.0, 2.1 및 3.0을 지원합니다.

비용

- BlueXP 분류 사용 비용은 스캔 중인 데이터의 양에 따라 달라집니다. BlueXP 작업 공간에서 BlueXP 분류 검사를 수행하는 첫 1TB의 데이터는 30일간 무료로 제공됩니다. 여기에는 모든 작업 환경 및 데이터 소스의 모든 데이터가 포함됩니다. AWS, Azure 또는 GCP Marketplace에 대한 가입 또는 NetApp의 BYOL 라이센스를 구입해야 하며, 이후 계속해서 데이터를 스캔할 수 있습니다. 을 참조하십시오 "가격" 를 참조하십시오.

  "BlueXP 분류 라이선스를 취득하는 방법을 알아보십시오".

- 클라우드에 BlueXP 분류를 설치하려면 클라우드 인스턴스를 배포해야 하므로 클라우드 인스턴스가 배포된 클라우드 공급자가 비용을 부담합니다. 을 참조하십시오 각 클라우드 공급자에 대해 구축된 인스턴스 유형입니다. BlueXP 분류를 사내 시스템에 설치하면 비용이 들지 않습니다.
- BlueXP 분류에서는 BlueXP 커넥터를 배포해야 합니다. BlueXP에서 사용 중인 다른 스토리지 및 서비스로 인해 이미 커넥터가 있는 경우가 많습니다. Connector 인스턴스를 사용하면 배포된 클라우드 공급자가 비용을 청구합니다. 를 참조하십시오 "각 클라우드 공급자에 대해 구축된 인스턴스 유형입니다". 커넥터를 온프레미스 시스템에 설치하는 경우 비용이 들지 않습니다.

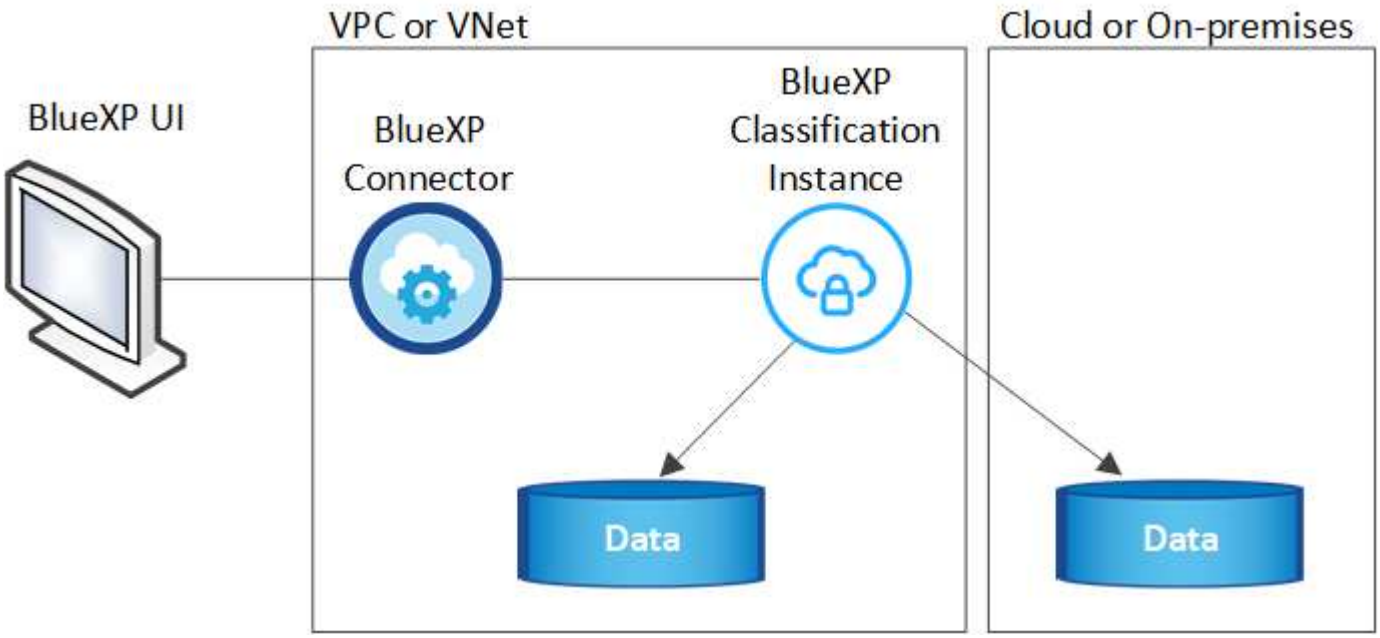
데이터 전송 비용

데이터 전송 비용은 설정에 따라 다릅니다. BlueXP 분류 인스턴스 및 데이터 소스가 동일한 가용성 영역 및 지역에 있는 경우 데이터 전송 비용이 발생하지 않습니다. 하지만 Cloud Volumes ONTAP 시스템 또는 S3 버킷과 같은 데이터 소스가 _different_Availability Zone 또는 지역에 있는 경우 클라우드 공급자가 데이터 전송 비용을 청구합니다. 자세한 내용은 다음 링크를 참조하십시오.

- "AWS: Amazon EC2 가격"
- "Microsoft Azure: 대역폭 가격 세부 정보"
- "Google Cloud: 스토리지 전송 서비스 가격"

BlueXP 분류 인스턴스입니다

BlueXP 분류를 클라우드에 배포하면 BlueXP는 Connector와 동일한 서브넷에 인스턴스를 배포합니다. "커넥터에 대해 자세히 알아보십시오."



기본 인스턴스에 대한 다음 사항에 유의하십시오.

- AWS에서 BlueXP 분류는 에서 실행됩니다 "m6i.4xLarge 인스턴스" 500GiB GP2 디스크 사용. 운영 체제 이미지는 Amazon Linux 2입니다. AWS에 구축할 경우 소량의 데이터를 스캔할 경우 더 작은 인스턴스 크기를 선택할 수 있습니다.
- Azure에서 BlueXP 분류는 에서 실행됩니다 "standard_d16s_v3 vm" 500GiB 디스크 사용 운영 체제 이미지는 CentOS 7.9입니다.
- GCP에서 BlueXP 분류는 에서 실행됩니다 "N2-표준-16 VM" 500GiB 표준 영구 디스크 사용 운영 체제 이미지는 CentOS 7.9입니다.
- 기본 인스턴스를 사용할 수 없는 지역에서는 대체 인스턴스에서 BlueXP 분류가 실행됩니다. "대체 인스턴스 유형을 참조하십시오".
- 인스턴스의 이름은 *CloudCompliance_*이며 생성된 해시*(UUID)*와 연결됩니다. 예*: _CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Connector당 하나의 BlueXP 분류 인스턴스만 배포됩니다.

BlueXP 분류를 사내 Linux 호스트 또는 선호하는 클라우드 공급업체의 호스트에 배포할 수도 있습니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다. 인스턴스에 인터넷 액세스가 가능한 한 BlueXP 분류 소프트웨어의 업그레이드는 자동으로 수행됩니다.

BlueXP 분류는 지속적으로 데이터를 검사하기 때문에 인스턴스가 항상 실행 상태를 유지해야 합니다.

더 작은 인스턴스 유형 사용

CPU가 적고 RAM이 적은 시스템에 BlueXP 분류를 배포할 수 있지만 이러한 덜 강력한 시스템을 사용할 때는 몇 가지 제약이 있습니다.

시스템 크기	사양	제한 사항
매우 크게	32개의 CPU, 128GB RAM, 1TiB SSD	최대 5억 개의 파일을 스캔할 수 있습니다.

시스템 크기	사양	제한 사항
크게(기본값)	CPU 16개, 64GB RAM, 500GiB SSD	최대 2억 5천만 개의 파일을 스캔할 수 있습니다.
중간	CPU 8개, 32GB RAM, 200GiB SSD	스캔 속도가 느리며 최대 100만 개의 파일만 스캔할 수 있습니다.
작은 크기	CPU 8개, 16GB RAM, 100GiB SSD	"중간"과 동일한 제한 사항과 식별 기능을 제공합니다 "데이터 주체 이름" 내부 파일이 비활성화되었습니다.

AWS의 클라우드에 BlueXP 분류를 배포할 때 대규모/중간/소규모 인스턴스를 선택할 수 있습니다. Azure 또는 GCP에서 BlueXP 분류를 구축할 때 이러한 대체 시스템 중 하나를 사용하려면 ng-contact-data-sense@netapp.com 으로 이메일을 보내 지원을 요청하십시오. 이러한 다른 클라우드 구성을 배포하려면 고객과 협력해야 합니다.

BlueXP 분류를 온프레미스에 구축할 경우 대체 사양이 있는 Linux 호스트를 사용하면 됩니다. NetApp에 지원을 요청할 필요가 없습니다.

BlueXP 분류의 작동 방식

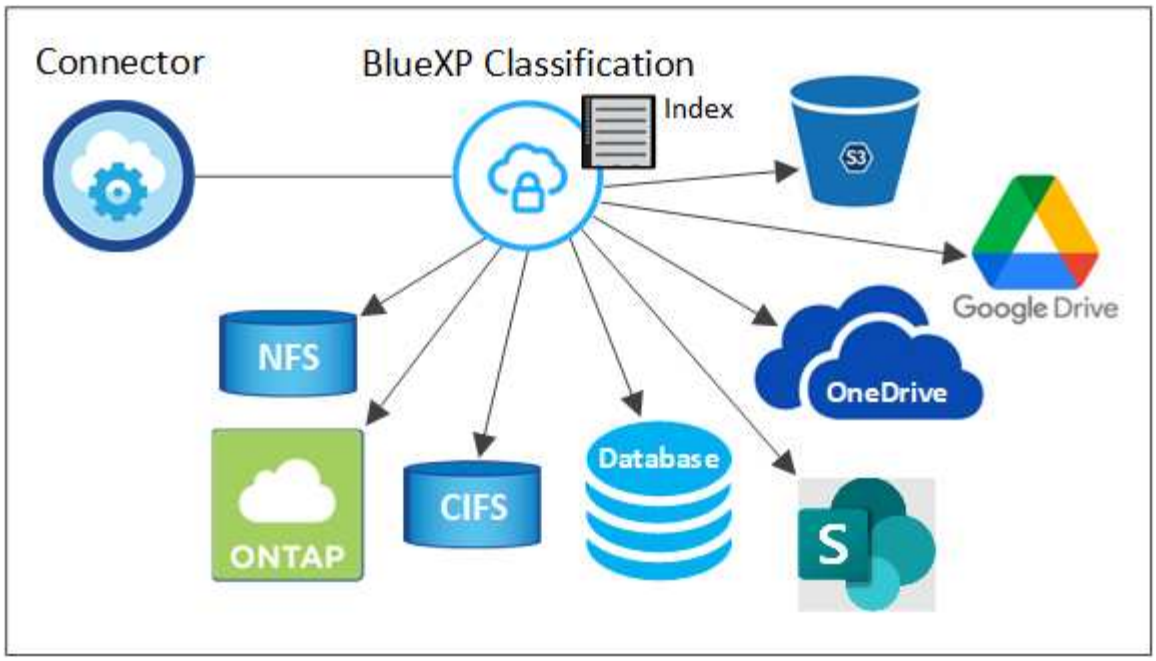
BlueXP 분류는 다음과 같이 작동합니다.

1. BlueXP에서 BlueXP 분류 인스턴스를 배포합니다.
2. 하나 이상의 데이터 소스에서 고급 매핑 또는 심층 스캔을 활성화할 수 있습니다.
3. BlueXP 분류는 AI 학습 프로세스를 사용하여 데이터를 스캔합니다.
4. 제공된 대시보드 및 보고 도구를 사용하여 규정 준수 및 거버넌스 작업에 도움을 줄 수 있습니다.

스캔 작동 방식

BlueXP 분류를 활성화하고 스캔할 저장소(볼륨, 버킷, 데이터베이스 스키마 또는 OneDrive 또는 SharePoint 사용자 데이터)를 선택하면 즉시 데이터 스캔이 시작되어 개인 및 중요 데이터를 식별합니다. 대부분의 경우 백업, 미러 또는 DR 사이트 대신 라이브 운영 데이터를 검사하는 데 집중해야 합니다. 그런 다음 BlueXP 분류를 통해 조직 데이터를 매핑하고, 각 파일을 분류하고, 데이터에서 엔터티와 미리 정의된 패턴을 식별하고 추출합니다. 검사 결과는 개인 정보, 민감한 개인 정보, 데이터 범주 및 파일 형식의 인덱스입니다.

BlueXP 분류는 NFS 및 CIFS 볼륨을 마운트하여 다른 클라이언트와 마찬가지로 데이터에 연결됩니다. CIFS 볼륨을 스캔하려면 Active Directory 자격 증명을 제공해야 하지만 NFS 볼륨은 읽기 전용으로 자동 액세스됩니다.



초기 검사 후 BlueXP 분류는 라운드 로빈 방식으로 데이터를 지속적으로 스캔하여 증분 변경을 감지합니다. 이렇게 했다면 인스턴스를 계속 실행하는 것이 중요합니다.

볼륨 수준, 버킷 수준, 데이터베이스 스키마 수준, OneDrive 사용자 수준 및 SharePoint 사이트 수준에서 스캔을 활성화 및 비활성화할 수 있습니다.

매핑 스캔과 분류 스캔의 차이점은 무엇입니까

BlueXP 분류를 통해 선택한 데이터 소스에서 일반적인 "매핑" 스캔을 실행할 수 있습니다. 매핑은 데이터에 대한 상위 수준의 개요만 제공하는 반면 분류는 데이터에 대한 세부 수준의 스캐닝을 제공합니다. 내부 데이터를 보기 위해 파일에 액세스하지 않기 때문에 데이터 소스에서 매핑을 매우 빠르게 수행할 수 있습니다.

많은 사용자가 데이터를 신속하게 스캔하여 더 많은 연구가 필요한 데이터 소스를 식별하려고 하므로 이 기능을 좋아하고, 그런 다음 필요한 데이터 소스 또는 볼륨에서만 분류 검사를 활성화할 수 있습니다.

아래 표에는 몇 가지 차이점이 나와 있습니다.

피처	분류	매핑
스캔 속도	느림	빠릅니다
파일 유형 및 사용된 용량 목록입니다	예	예
파일 수 및 사용된 용량입니다	예	예
파일의 수명 및 크기	예	예
을 실행하는 기능 "데이터 매핑 보고서"	예	예
파일 세부 정보를 보려면 데이터 조사 페이지 를 참조하십시오	예	아니요
파일 내에서 이름을 검색합니다	예	아니요
생성 "정책" 맞춤형 검색 결과를 제공합니다	예	아니요
AIP 레이블 및 상태 태그를 사용하여 데이터를 분류합니다	예	아니요

피처	분류	매핑
원본 파일을 복사, 삭제 및 이동합니다	예	아니요
다른 보고서를 실행할 수 있습니다	예	아니요

BlueXP 분류 스캔 데이터의 속도

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

- 매핑 스캔을 수행할 때 BlueXP 분류는 스캐너 노드당 하루에 100-150GB의 데이터를 스캔할 수 있습니다.
- 분류 스캔을 수행할 때 BlueXP 분류는 스캐너 노드당 하루에 15-40개의 BB 데이터를 스캔할 수 있습니다.

"데이터를 스캔하기 위해 여러 스캐너 노드를 구축하는 방법에 대해 자세히 알아보십시오".

BlueXP 분류 색인에 대한 정보

BlueXP 분류는 데이터(파일)에 범주를 수집, 색인 및 할당합니다. BlueXP 분류 인덱스의 데이터는 다음과 같습니다.

표준 메타데이터
: BlueXP 분류는 파일 유형, 크기, 생성 및 수정 날짜 등의 파일에 대한 표준 메타데이터를 수집합니다.

개인 데이터
: 이메일 주소, 식별 번호 또는 신용 카드 번호와 같은 개인 식별 정보 "개인 데이터에 대해 자세히 알아보십시오".

민감한 개인 데이터
: GDPR 및 기타 개인 정보 보호 규정에 정의된 의료 데이터, 인종 또는 정치적 의견과 같은 민감한 정보의 특별한 유형. "중요한 개인 데이터에 대해 자세히 알아보십시오".

범주
: BlueXP 분류는 스캔한 데이터를 다른 유형의 범주로 나눕니다. 범주는 각 파일의 콘텐츠 및 메타데이터에 대한 AI 분석을 기반으로 하는 주제입니다. "범주에 대해 자세히 알아보십시오".

유형
: BlueXP 분류는 스캔한 데이터를 파일 유형별로 분류하여 표시합니다. "유형에 대해 자세히 알아보십시오".

이름 요소 인식
: BlueXP 분류에서는 AI를 사용하여 문서에서 자연인의 이름을 추출합니다. "데이터 주체 액세스 요청에 응답하는 방법에 대해 알아봅니다".

네트워킹 개요

BlueXP는 Connector 인스턴스의 인바운드 HTTP 연결을 활성화하는 보안 그룹과 함께 BlueXP 분류 인스턴스를 배포합니다.

SaaS 모드에서 BlueXP에 연결할 때 HTTPS를 통해 BlueXP에 연결되며 브라우저와 BlueXP 분류 인스턴스 간에 전송되는 프라이빗 데이터는 TLS 1.2를 사용하는 엔드 투 엔드 암호화로 보안이 유지됩니다. 즉, NetApp과 타사가 이 데이터를 읽을 수 없습니다.

아웃바운드 규칙은 완전히 열립니다. BlueXP 분류 소프트웨어를 설치 및 업그레이드하고 사용 지표를 전송하려면

인터넷 액세스가 필요합니다.

네트워킹 요구 사항이 엄격하면 "BlueXP 분류 접촉부에 대한 엔드포인트에 대해 알아보십시오".

규정 준수 정보에 대한 사용자 액세스

각 사용자에게 할당된 역할은 BlueXP와 BlueXP 분류 내에서 서로 다른 기능을 제공합니다.

- 계정 관리자 * 는 규정 준수 설정을 관리하고 모든 작업 환경에 대한 규정 준수 정보를 볼 수 있습니다.
- Workspace Admin * 은 액세스 권한이 있는 시스템에 대해서만 준수 설정을 관리하고 준수 정보를 볼 수 있습니다. 작업 영역 관리자가 BlueXP의 작업 환경에 액세스할 수 없는 경우 BlueXP 분류 탭에서 작업 환경에 대한 규정 준수 정보를 볼 수 없습니다.
- Compliance Viewer * 역할의 사용자는 규정 준수 정보를 보고 액세스 권한이 있는 시스템에 대한 보고서만 생성할 수 있습니다. 이러한 사용자는 볼륨, 버킷 또는 데이터베이스 스키마 스캔을 활성화/비활성화할 수 없습니다. 이러한 사용자는 파일을 복사, 이동 또는 삭제할 수 없습니다.

"BlueXP 역할에 대해 자세히 알아보십시오" 및 방법 을 참조하십시오 "특정 역할을 가진 사용자를 추가합니다".

BlueXP 분류를 배포합니다

어떤 BlueXP 분류 구축을 사용해야 합니까?

BlueXP 분류를 다양한 방법으로 구축할 수 있습니다. 어떤 방법이 사용자의 요구를 충족시키는지 알아보십시오.

BlueXP 분류를 다음과 같은 방법으로 구축할 수 있습니다.

- "BlueXP를 사용하여 클라우드에 배포합니다". BlueXP는 BlueXP Connector와 동일한 클라우드 제공업체 네트워크에 BlueXP 분류 인스턴스를 배포합니다.
- "인터넷에 액세스할 수 있는 Linux 호스트에 설치합니다". 네트워크의 Linux 호스트 또는 인터넷에 액세스할 수 있는 클라우드의 Linux 호스트에 BlueXP 분류를 설치합니다. 사내에 있는 BlueXP 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 검사하려는 경우 이러한 설치 유형이 좋은 옵션이 될 수 있지만 반드시 필요한 것은 아닙니다.
- "인터넷 액세스 없이 온-프레미스 사이트에 Linux 호스트에 설치합니다"는 _private 모드라고도 합니다._설치 스크립트를 사용하는 이 유형의 설치는 보안 사이트에 적합합니다.

인터넷에 액세스할 수 있는 Linux 호스트에 설치하고 인터넷에 액세스할 수 없는 Linux 호스트에 온-프레미스 설치 모두 설치 스크립트를 사용합니다. 이 스크립트는 시스템과 환경이 사전 요구 사항을 충족하는지 확인하는 것으로 시작됩니다. 필수 구성 요소가 충족되면 설치가 시작됩니다. BlueXP 분류 설치를 실행하는 것과 별도로 필수 구성 요소를 확인하려면 필수 구성 요소에 대한 테스트만 다운로드할 수 있는 별도의 소프트웨어 패키지가 있습니다.

을 참조하십시오 "Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인합니다".

BlueXP를 사용하여 클라우드에 BlueXP 분류를 배포합니다

클라우드에 BlueXP 분류를 배포하기 위한 몇 가지 단계를 완료합니다. BlueXP는 BlueXP Connector와 동일한 클라우드 제공업체 네트워크에 BlueXP 분류 인스턴스를 배포합니다.

참고: 또한 이 기능을 사용할 수 있습니다 "인터넷에 액세스할 수 있는 Linux 호스트에 BlueXP 분류를 설치합니다". 이 설치 유형은 사내에 위치한 BlueXP 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 스캔하려는 경우 좋은 옵션이 될 수 있지만 반드시 필요한 것은 아닙니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다.

빠른 시작

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

1 커넥터를 작성합니다

아직 커넥터가 없으면 지금 연결선을 작성합니다. 을 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

또한 가능합니다 "Connector On-Premises를 설치합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트

2 사전 요구 사항을 검토합니다

환경이 필수 조건을 충족할 수 있는지 확인합니다. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 커넥터와 BlueXP 분류 간의 연결 등이 포함됩니다. 전체 목록을 참조하십시오.

3 **BlueXP** 분류를 배포합니다

설치 마법사를 시작하여 클라우드에 BlueXP 분류 인스턴스를 배포합니다.

4 **BlueXP** 분류 서비스에 가입합니다

BlueXP의 BlueXP 분류 검사에서 처음 1TB의 데이터는 30일 동안 무료로 제공됩니다. 해당 시점 이후에도 계속해서 데이터를 스캔하려면 클라우드 공급자 마켓플레이스 또는 NetApp의 BYOL 라이센스를 통한 BlueXP 구독이 필요합니다.

커넥터를 작성합니다

Connector가 없는 경우 클라우드 공급자에 Connector를 생성합니다. 을 참조하십시오 "AWS에서 커넥터 생성" 또는 "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다". 대부분의 경우 대부분의 경우 BlueXP 분류를 활성화하기 전에 커넥터가 설정되어 있을 수 있습니다 "BlueXP 기능을 사용하려면 커넥터가 필요합니다"하지만 지금 설정해야 하는 경우도 있습니다.

특정 클라우드 공급자에 배포된 Connector를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP, ONTAP용 Amazon FSx 또는 AWS S3 버킷에서 데이터를 스캔할 때는 AWS의 커넥터를 사용합니다.
- Azure 또는 Azure NetApp Files의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 Azure의 커넥터를 사용합니다.
  - Azure NetApp Files의 경우 스캔하려는 볼륨과 동일한 영역에 배포해야 합니다.
- GCP의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 GCP의 커넥터를 사용합니다.

온프레미스 ONTAP 시스템, NetApp이 아닌 파일 공유, 일반 S3 오브젝트 스토리지, 데이터베이스, OneDrive 폴더,

SharePoint 계정, Google Drive 계정은 이러한 클라우드 커넥터를 사용할 때 검색할 수 있습니다.

참고: 또한 이 기능을 사용할 수 있습니다 "Connector On-Premises를 설치합니다" 네트워크 또는 클라우드의 Linux 호스트 BlueXP 분류를 사내에서 설치하려는 일부 사용자는 Connector를 내부에 설치할 수도 있습니다.

보시다시피 을 사용해야 하는 몇 가지 상황이 있을 수 있습니다 "다중 커넥터".

정부 지역 지원

정부 지역(AWS GovCloud, Azure Gov 또는 Azure DoD)에 Connector를 구축한 경우 BlueXP 분류가 지원됩니다. 이러한 방식으로 배포된 BlueXP 분류에는 다음과 같은 제한 사항이 있습니다.

- OneDrive 계정, SharePoint 계정 및 Google Drive 계정을 검색할 수 없습니다.
- Microsoft Azure 정보 보호(AIP) 레이블 기능은 통합할 수 없습니다.

"정부 지역에서 커넥터 배포에 대한 자세한 내용은 을 참조하십시오".

사전 요구 사항을 검토합니다

클라우드에 BlueXP 분류를 배포하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인합니다. 클라우드에 BlueXP 분류를 배포할 때 Connector와 동일한 서브넷에 위치합니다.

BlueXP 분류에서 아웃바운드 인터넷 액세스를 활성화합니다

BlueXP 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 BlueXP 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다. 프록시는 투명하지 않아야 합니다. 현재 투명 프록시를 지원하지 않습니다.

AWS, Azure 또는 GCP에서 BlueXP 분류를 배포하는지 여부에 따라 아래 적절한 표를 검토하십시오.

AWS에 필요한 엔드포인트

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 및 템플릿에 대한 액세스를 제공합니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
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	BlueXP 분류를 통해 매니페스트와 템플릿을 액세스 및 다운로드하고 로그 및 메트릭을 전송할 수 있습니다.

Azure에 필요한 엔드포인입니다

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

GCP에 필요한 엔드포인입니다

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.

엔드포인트	목적
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

BlueXP에 필요한 권한이 있는지 확인합니다

BlueXP에 리소스를 배포하고 BlueXP 분류 인스턴스에 대한 보안 그룹을 만들 수 있는 권한이 있는지 확인합니다. 최신 BlueXP 사용 권한은 에서 확인할 수 있습니다 "NetApp에서 제공하는 정책".

BlueXP 커넥터가 **BlueXP** 분류에 액세스할 수 있는지 확인합니다

Connector와 BlueXP 분류 인스턴스 간의 연결을 확인합니다. Connector의 보안 그룹은 포트 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 이 연결을 통해 BlueXP 분류 인스턴스를 배포할 수 있으며 규정 준수 및 거버넌스 탭에서 정보를 볼 수 있습니다. BlueXP 분류는 AWS 및 Azure의 정부 지역에서 지원됩니다.

AWS 및 AWS GovCloud 배포에는 추가 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 을 참조하십시오 "AWS의 커넥터 규칙" 를 참조하십시오.

Azure 및 Azure Government 배포에는 추가 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 을 참조하십시오 "Azure의 커넥터 규칙" 를 참조하십시오.

BlueXP 분류를 계속 실행할 수 있는지 확인합니다

데이터를 지속적으로 스캔하려면 BlueXP 분류 인스턴스를 계속 사용해야 합니다.

웹 브라우저가 **BlueXP** 분류에 연결되어 있는지 확인합니다

BlueXP 분류를 사용하도록 설정한 후에는 BlueXP 분류 인스턴스에 연결된 호스트에서 BlueXP 인터페이스에 액세스해야 합니다.

BlueXP 분류 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터에 인터넷에서 액세스할 수 없도록 합니다. 따라서 BlueXP에 액세스하는 데 사용하는 웹 브라우저가 해당 개인 IP 주소에 연결되어 있어야 합니다. 이러한 연결은 클라우드 공급자(예: VPN)에 직접 연결되거나 BlueXP 분류 인스턴스와 동일한 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

vCPU 한도를 확인하십시오

클라우드 공급자의 vCPU 제한에 따라 필요한 수의 코어를 사용하여 인스턴스를 구축할 수 있는지 확인합니다. BlueXP가 실행 중인 지역의 관련 인스턴스 제품군에 대한 vCPU 제한을 확인해야 합니다. "필요한 인스턴스 유형을 참조하십시오".

vCPU 제한에 대한 자세한 내용은 다음 링크를 참조하십시오.

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

참고로, AWS 클라우드 환경에서는 CPU가 적고 RAM이 적은 인스턴스에 BlueXP 분류를 배포할 수 있지만 이러한 시스템을 사용할 때는 한계가 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

클라우드에 **BlueXP** 분류를 배포합니다

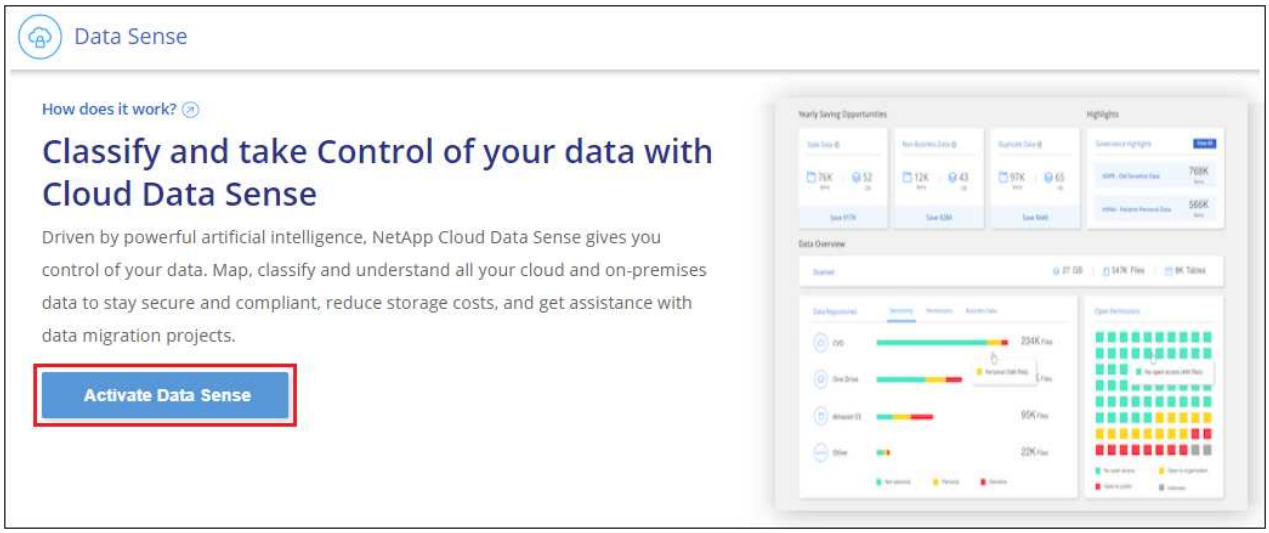
다음 단계에 따라 클라우드에 BlueXP 분류 인스턴스를 배포합니다. Connector는 클라우드에 인스턴스를 배포한 다음 해당 인스턴스에 BlueXP 분류 소프트웨어를 설치합니다.

AWS 환경의 BlueXP Connector에서 BlueXP 분류를 배포할 때 기본 인스턴스 크기를 선택하거나 두 개의 작은 인스턴스 유형 중에서 선택할 수 있습니다. "사용 가능한 인스턴스 유형 및 제한 사항을 참조하십시오". 기본 인스턴스 유형을 사용할 수 없는 지역에서는 BlueXP 분류가 에서 실행됩니다 "대체 인스턴스 유형".

AWS에 구축

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.



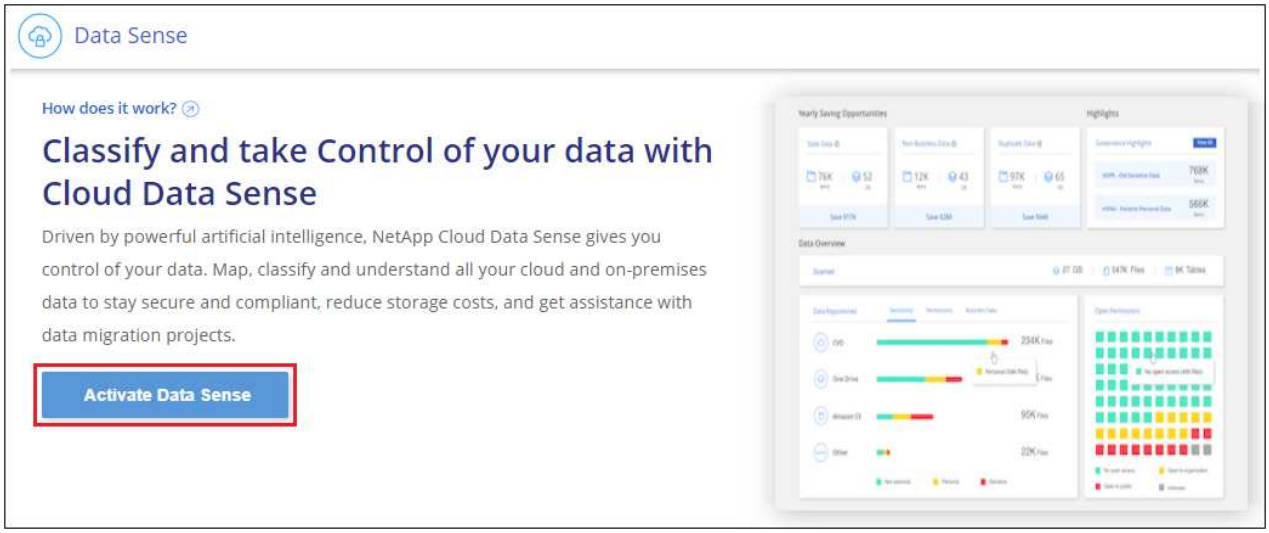
2. Activate Data Sense * 를 클릭합니다.
3. Installation_page에서 * deploy > deploy * 를 클릭하여 "큰" 인스턴스 크기를 사용하고 클라우드 배포 마법사를 시작합니다.
4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

5. 인스턴스가 배포되고 BlueXP 분류가 설치되면 * 구성 계속 * 을 클릭하여 _Configuration_페이지로 이동합니다.

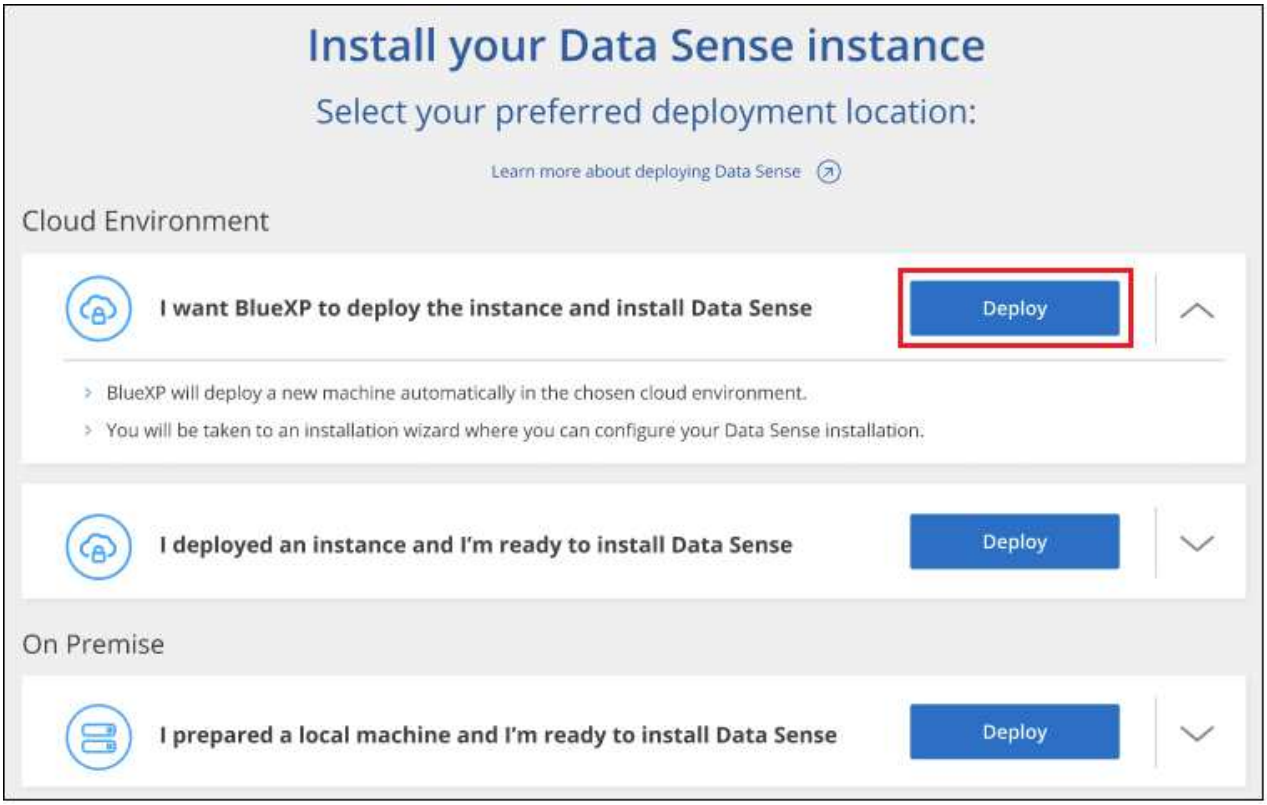
Azure에 구축

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. Activate Data Sense * 를 클릭합니다.



3. 클라우드 배포 마법사를 시작하려면 * 배포 * 를 클릭합니다.



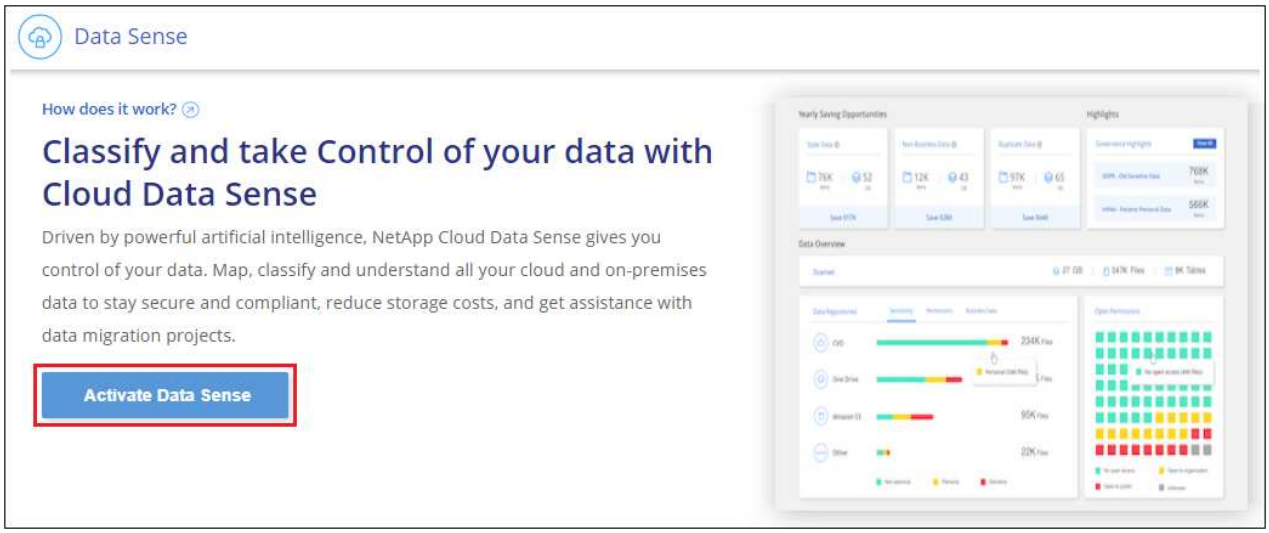
4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

5. 인스턴스가 배포되고 BlueXP 분류가 설치되면 * 구성 계속 * 을 클릭하여 _Configuration_페이지로 이동합니다.

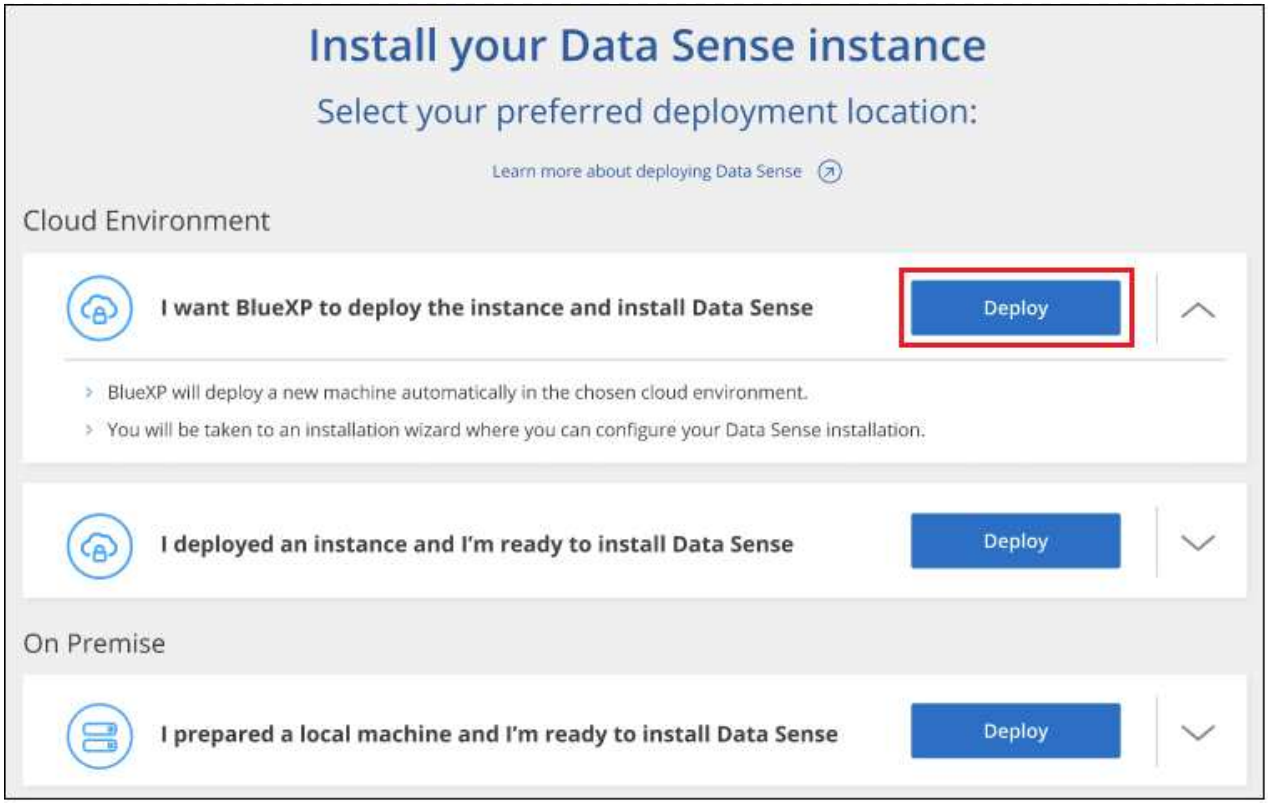
Google Cloud에 배포

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. Activate Data Sense * 를 클릭합니다.



3. 클라우드 배포 마법사를 시작하려면 * 배포 * 를 클릭합니다.



4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

5. 인스턴스가 배포되고 BlueXP 분류가 설치되면 * 구성 계속 * 을 클릭하여 _Configuration_페이지로 이동합니다.

결과

BlueXP는 클라우드 공급업체에 BlueXP 분류 인스턴스를 배포합니다.

인터넷 연결이 가능한 경우 BlueXP Connector 및 BlueXP 분류 소프트웨어에 대한 업그레이드가 자동화됩니다.

다음 단계

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

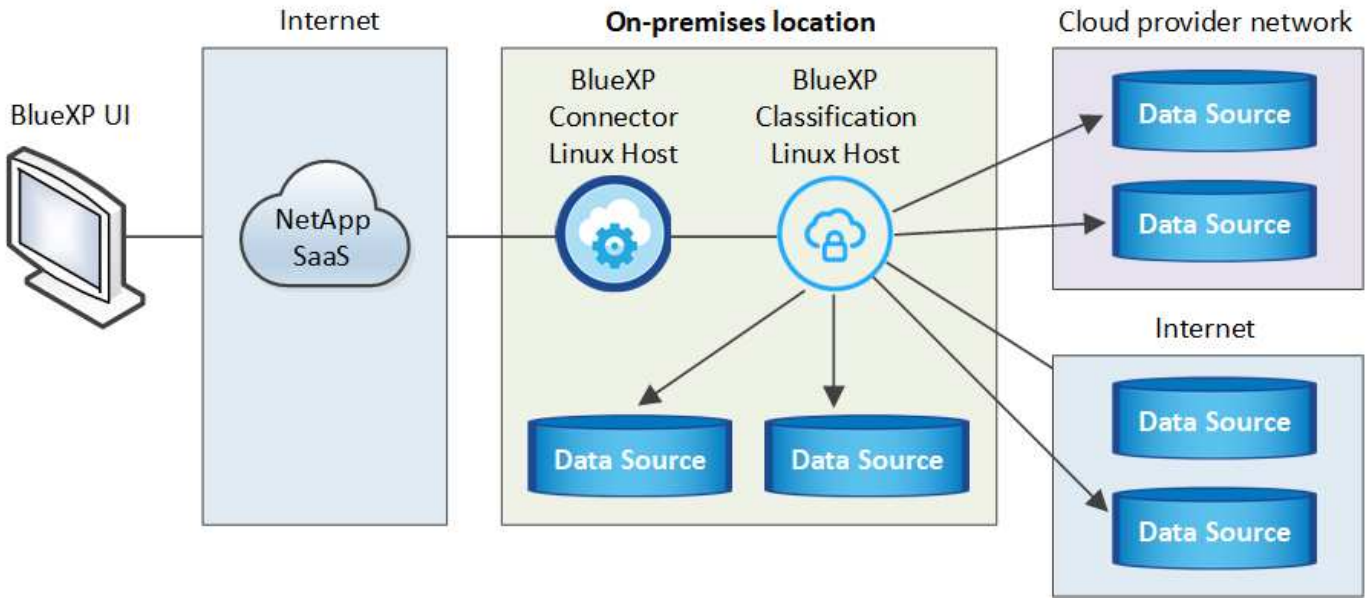
인터넷에 액세스할 수 있는 호스트에 **BlueXP** 분류를 설치합니다

네트워크의 Linux 호스트 또는 인터넷 액세스가 가능한 클라우드의 Linux 호스트에 BlueXP 분류를 설치하려면 몇 가지 단계를 완료하십시오. 이 설치의 일부로 네트워크 또는 클라우드에 Linux 호스트를 수동으로 배포해야 합니다.

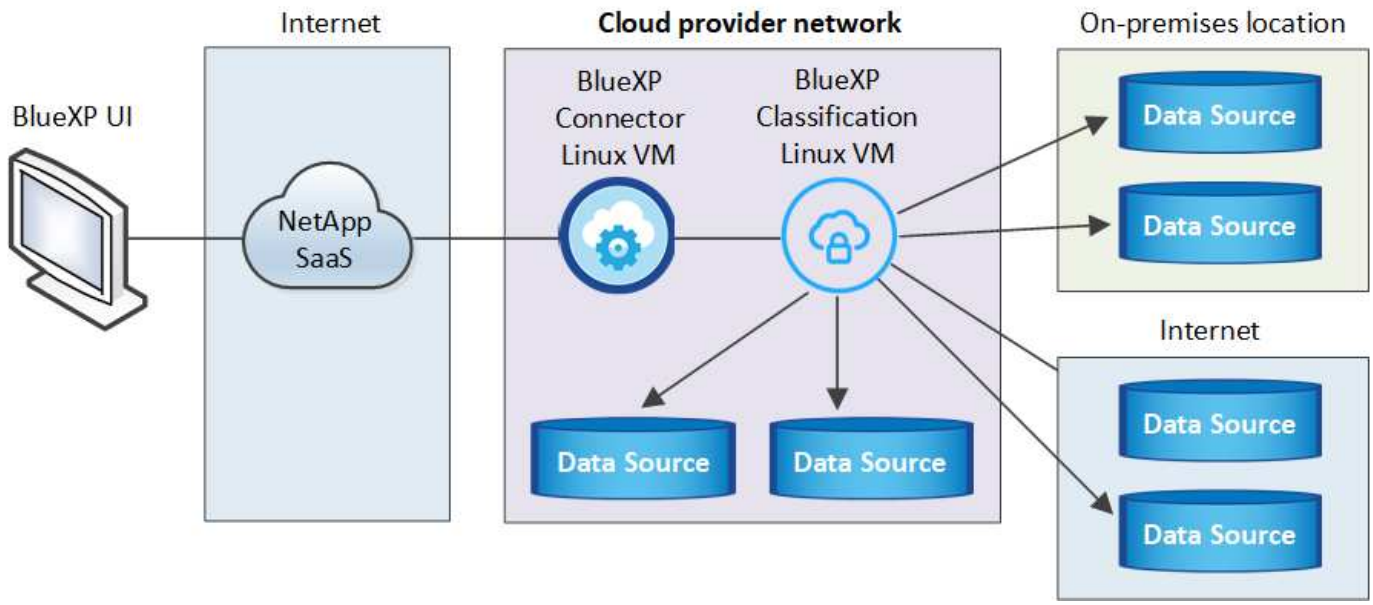
온프레미스에도 위치한 BlueXP 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 스캔하려는 경우 온프레미스 설치가 좋은 옵션이 될 수 있지만, 이는 필수 사항이 아닙니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다.

BlueXP 분류 설치 스크립트는 시스템 및 환경이 필수 전제 조건을 충족하는지 확인하는 것으로 시작됩니다. 필수 구성 요소가 모두 충족되면 설치가 시작됩니다. BlueXP 분류 설치를 실행하는 것과 별도로 필수 구성 요소를 확인하려면 필수 구성 요소에 대한 테스트만 다운로드할 수 있는 별도의 소프트웨어 패키지가 있습니다. "Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인하는 방법을 참조하십시오".

Linux 호스트 _ 의 일반적인 설치 방법은 다음과 같습니다.



클라우드의 Linux 호스트에 _ 을(를) 설치하는 일반적인 구성 요소와 연결은 다음과 같습니다.



페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여러 호스트 시스템을 사용하는 경우 주 시스템을 _Manager node_라고 하며 추가 처리 능력을 제공하는 추가 시스템을 _Scanner nodes_라고 합니다.

참고: 또한 이 기능을 사용할 수 있습니다 "인터넷에 액세스할 수 없는 사내 사이트에 BlueXP 분류를 설치합니다" 완전히 안전한 사이트를 위한 것입니다.

빠른 시작

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

1 커넥터를 작성합니다

커넥터가 없는 경우 "Connector를 온-프레미스에 배포합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트

또한 클라우드 공급자와 커넥터를 생성할 수도 있습니다. 을 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

2 사전 요구 사항을 검토합니다

환경이 필수 조건을 충족할 수 있는지 확인합니다. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 커넥터와 BlueXP 분류 간의 연결 등이 포함됩니다. 전체 목록을 참조하십시오.

또한 을 충족하는 Linux 시스템도 필요합니다 따르는 요구사항.

3 **BlueXP** 분류를 다운로드하고 배포합니다

NetApp Support 사이트에서 클라우드 BlueXP 분류 소프트웨어를 다운로드하고 사용할 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 시작하고 화면의 지시에 따라 BlueXP 분류 인스턴스를 배포합니다.

4 **BlueXP** 분류 서비스에 가입합니다

BlueXP의 BlueXP 분류 검사에서 처음 1TB의 데이터는 30일 동안 무료로 제공됩니다. 해당 시점 이후에도 데이터를 계속 스캔하려면 클라우드 공급자 마켓플레이스 또는 NetApp의 BYOL 라이센스를 구입해야 합니다.

커넥터를 작성합니다

BlueXP 분류를 설치하고 사용하려면 먼저 BlueXP 커넥터가 필요합니다. 대부분의 경우 대부분의 경우 BlueXP 분류를 활성화하기 전에 커넥터가 설정되어 있을 수 있습니다 "BlueXP 기능을 사용하려면 커넥터가 필요합니다"하지만 지금 설정해야 하는 경우도 있습니다.

클라우드 공급자 환경에 하나를 생성하려면 를 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

특정 클라우드 공급자에 배포된 Connector를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS의 Cloud Volumes ONTAP, ONTAP용 Amazon FSx 또는 AWS S3 버킷에서 데이터를 스캔할 때는 AWS의 커넥터를 사용합니다.
- Azure 또는 Azure NetApp Files의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 Azure의 커넥터를 사용합니다.

  Azure NetApp Files의 경우 스캔하려는 볼륨과 동일한 영역에 배포해야 합니다.

- GCP의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 GCP의 커넥터를 사용합니다.

온프레미스 ONTAP 시스템, NetApp이 아닌 파일 공유, 일반 S3 오브젝트 스토리지, 데이터베이스, OneDrive 폴더, SharePoint 계정, Google Drive 계정은 이러한 클라우드 커넥터를 사용하여 스캔할 수 있습니다.

참고: 또한 이 기능을 사용할 수 있습니다 "Connector를 온-프레미스에 배포합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트 BlueXP 분류를 사내에서 설치하려는 일부 사용자는 Connector를 내부에 설치할 수도 있습니다.

보시다시피 을 사용해야 하는 몇 가지 상황이 있을 수 있습니다 "다중 커넥터".

BlueXP 분류를 설치할 때 커넥터 시스템의 IP 주소 또는 호스트 이름이 필요합니다. 이 정보는 구내에 Connector를 설치한 경우 확인할 수 있습니다. Connector가 클라우드에 배포된 경우 BlueXP 콘솔에서 이 정보를 찾을 수 있습니다. 도움말 아이콘을 클릭하고 * 지원 * 을 선택한 다음 * BlueXP 커넥터 * 를 클릭합니다.

Linux 호스트 시스템을 준비합니다

BlueXP 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행해야 합니다. Linux 호스트는 네트워크 또는 클라우드에 있을 수 있습니다.

BlueXP 분류를 계속 실행할 수 있는지 확인합니다. 데이터를 지속적으로 스캔하려면 BlueXP 분류 장비가 켜져 있어야 합니다.

- BlueXP 분류는 다른 애플리케이션과 공유되는 호스트에서는 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.
- 구내 호스트 시스템을 구축할 때 BlueXP 분류 검사를 수행할 데이터 세트의 크기에 따라 세 가지 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 초대형 *	32개의 CPU	128GB RAM	/, 또는 의 1TiB SSD /opt에서 -100GiB를 사용할 수 있습니다 -895GiB는 /var/lib/docker에서 사용할 수 있습니다 /tmp에 -5GiB입니다
* 대형 *	CPU 16개	64GB RAM	500GiB SSD 켜짐/또는 /opt에서 -100GiB를 사용할 수 있습니다 /var/lib/docker에서 사용 가능한 395GiB /tmp에 -5GiB입니다
* 중간 *	CPU 8개	32GB RAM	200GiB SSD 켜짐/또는 /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -145GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다
* 소형 *	CPU 8개	16GB RAM	또는 에서 100GiB SSD /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -45GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다

소형 시스템을 사용할 때는 제한이 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

- BlueXP 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때는 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 권장합니다.
  - * AWS EC2 인스턴스 유형 *: "m6i.4xLarge"를 권장합니다. "추가 AWS 인스턴스 유형을 참조하십시오".
  - * Azure VM size *: "Standard_D16s_v3"을 권장합니다. "추가 Azure 인스턴스 유형을 참조하십시오".
  - * GCP 시스템 유형 *: "n2-standard-16"을 권장합니다. "추가 GCP 인스턴스 유형을 참조하십시오".
- UNIX 폴더 권한 *: 다음과 같은 최소 UNIX 권한이 필요합니다.

폴더	최소 권한
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker입니다	`rwx------`
/usr/lib/systemd/system입니다	`rwxr-xr-x`

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

        - CentOS 버전 7.8 및 7.9
        - Ubuntu 22.04(BlueXP 분류 버전 1.23 이상 필요)
    - 다음 운영 체제에는 Podman 컨테이너 엔진을 사용해야 하며 BlueXP 분류 버전 1.30 이상이 필요합니다.
        - Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3

          RHEL 8.x 및 RHEL 9.x를 사용하는 경우 다음 기능은 현재 지원되지 않습니다.

            - 어두운 장소에 설치
            - 분산 스캔, 마스터 스캐너 노드 및 원격 스캐너 노드 사용
- * Red Hat 서브스크립션 관리 *: 호스트는 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 설치 중에 시스템에서 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.
- * 추가 소프트웨어 *: BlueXP 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
    - 사용 중인 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
        - Docker Engine 버전 19.3.1 이상 "설치 지침을 봅니다".

          "이 비디오 시청" CentOS에 Docker를 설치하는 빠른 데모를 보려면

        - Podman 버전 4 이상 Podman을 설치하려면 시스템 패키지를 업데이트하십시오 (`sudo yum update -y`)를 클릭한 다음 Podman을 설치합니다 (`sudo yum install netavark -y`)를 클릭합니다.
- Python 버전 3.6 이상. "설치 지침을 봅니다".
    - * NTP 고려 사항 *: NetApp에서는 NTP(네트워크 시간 프로토콜) 서비스를 사용하도록 BlueXP 분류 시스템을 구성할 것을 권장합니다. BlueXP 분류 시스템과 BlueXP Connector 시스템 간에 시간을 동기화해야 합니다.
    - * Firewalld 고려 사항 *: 사용하려는 경우 `firewalld`BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

      ```
      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 BlueXP 분류 호스트를 스캐너 노드로 사용할 계획이라면 이 규칙을 주 시스템에 추가하십시오.

```
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 활성화 또는 업데이트할 때마다 다시 시작해야 합니다 `firewalld` 설정.

설치 후 BlueXP 분류 호스트 시스템의 IP 주소를 변경할 수 없습니다.

BlueXP 분류에서 아웃바운드 인터넷 액세스를 활성화합니다

BlueXP 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 BlueXP 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다.

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://github.com/docker https://download.docker.com 으로 문의하십시오	Docker 설치를 위한 사전 필수 패키지를 제공합니다.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm 를 참조하십시오	CentOS 설치를 위한 필수 패키지를 제공합니다.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

필요한 모든 포트가 활성화되어 있는지 확인합니다

커넥터, BlueXP 분류, Active Directory 및 데이터 소스 간의 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

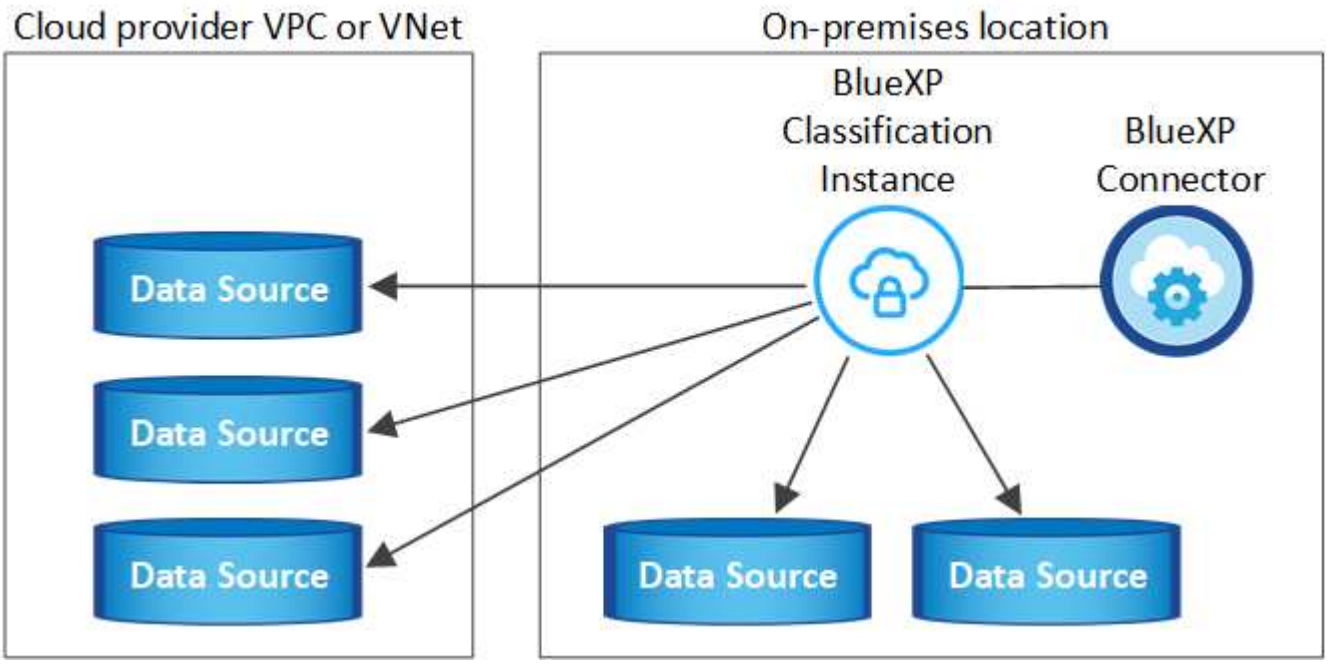
연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 443(TCP) 및 80	Connector의 방화벽 또는 라우팅 규칙은 포트 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 포트 8080이 열려 있는지 확인하여 BlueXP에서 설치 진행률을 확인합니다.

연결 유형	포트	설명
커넥터 <>ONTAP 클러스터(NAS)	443(TCP)	BlueXP는 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 다음 요구 사항을 충족해야 합니다. • 커넥터 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. Connector가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽 또는 라우팅 규칙으로 허용됩니다. • ONTAP 클러스터는 포트 443을 통한 인바운드 HTTPS 액세스를 허용해야 합니다. 기본 "관리" 방화벽 정책은 모든 IP 주소에서 인바운드 HTTPS 액세스를 허용합니다. 이 기본 정책을 수정하거나 자체 방화벽 정책을 만든 경우 HTTPS 프로토콜을 해당 정책에 연결하고 Connector 호스트에서 액세스를 활성화해야 합니다.
BlueXP 분류<>ONTAP 클러스터	• NFS-111(TCP\UDP) 및 2049(TCP\UDP)의 경우 • CIFS-139(TCP\UDP) 및 445(TCP\UDP)의 경우	BlueXP 분류에는 각 Cloud Volumes ONTAP 서브넷 또는 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다. Cloud Volumes ONTAP의 방화벽 또는 라우팅 규칙은 BlueXP 분류 인스턴스에서 인바운드 연결을 허용해야 합니다. 이러한 포트가 BlueXP 분류 인스턴스에 열려 있는지 확인합니다. • NFS-111 및 2049용 • CIFS-139 및 445의 경우 NFS 볼륨 내보내기 정책은 BlueXP 분류 인스턴스에서 액세스를 허용해야 합니다.
BlueXP 분류<>Active Directory	389(TCP 및 UDP), 636(TCP), 3268(TCP) 및 3269(TCP)	회사의 사용자에 대해 Active Directory가 이미 설정되어 있어야 합니다. 또한 BlueXP 분류에는 CIFS 볼륨을 스캔하기 위해 Active Directory 자격 증명이 필요합니다. Active Directory에 대한 정보가 있어야 합니다. • DNS 서버 IP 주소 또는 여러 IP 주소 • 서버의 사용자 이름 및 암호 • 도메인 이름(Active Directory 이름) • 보안 LDAP(LDAPS) 사용 여부 • LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)

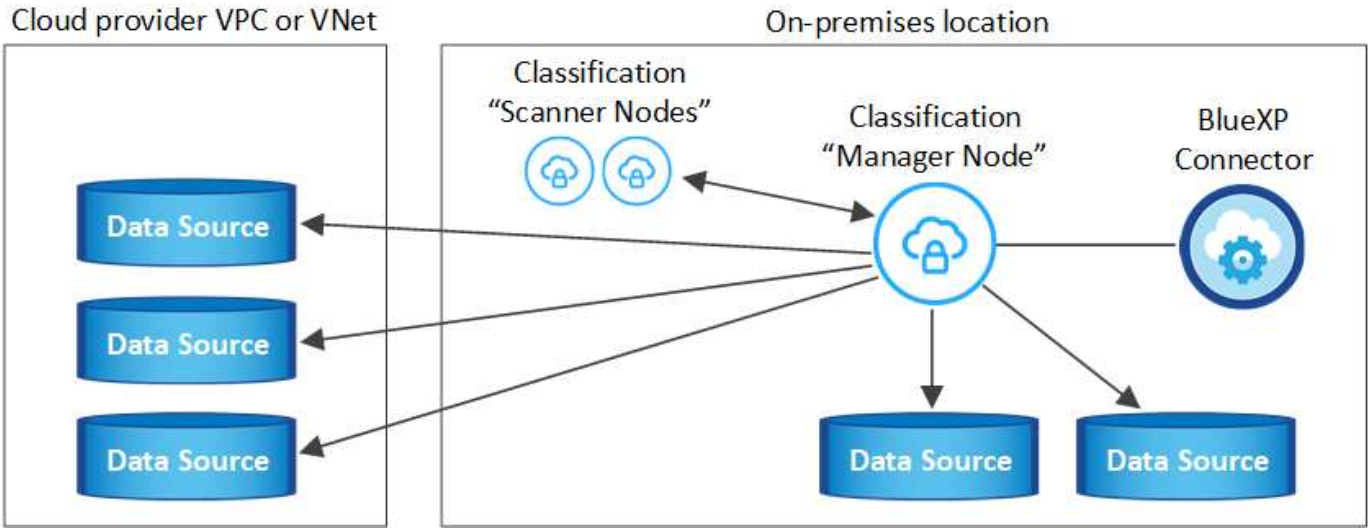
여러 BlueXP 분류 호스트를 사용하여 데이터 소스를 검사하는 추가 처리 기능을 제공하는 경우 추가 포트/프로토콜을 활성화해야 합니다. "추가 포트 요구 사항을 참조하십시오".

Linux 호스트에 BlueXP 분류를 설치합니다

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



페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여기에서 해당 단계를 확인하십시오.



을 참조하십시오 Linux 호스트 시스템 준비 및 사전 요구 사항 검토 BlueXP 분류를 배포하기 전에 필요한 전체 목록을 확인하십시오.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

> BlueXP 분류는 소프트웨어가 사내에 설치된 경우 현재 ONTAP용 S3 버킷, Azure NetApp Files 또는 FSx를 스캔할 수 없습니다. 이러한 경우 클라우드 및 에 별도의 Connector 및 BlueXP 분류 인스턴스를 배포해야 합니다 "커넥터 사이를 전환합니다" 다양한 데이터 소스에 대해

단일 온-프레미스 호스트에 BlueXP 분류 소프트웨어를 설치할 때 요구 사항을 검토하고 다음 단계를 따르십시오.

"이 비디오 시청" BlueXP 분류 설치 방법을 확인합니다.

모든 설치 작업은 BlueXP 분류를 설치할 때 기록됩니다. 설치 중에 문제가 발생하면 설치 감사 로그의 내용을 볼 수 있습니다. 에 기록됩니다 `/opt/netapp/install_logs/`. "자세한 내용은 여기에서 확인하십시오.".

필요한 것

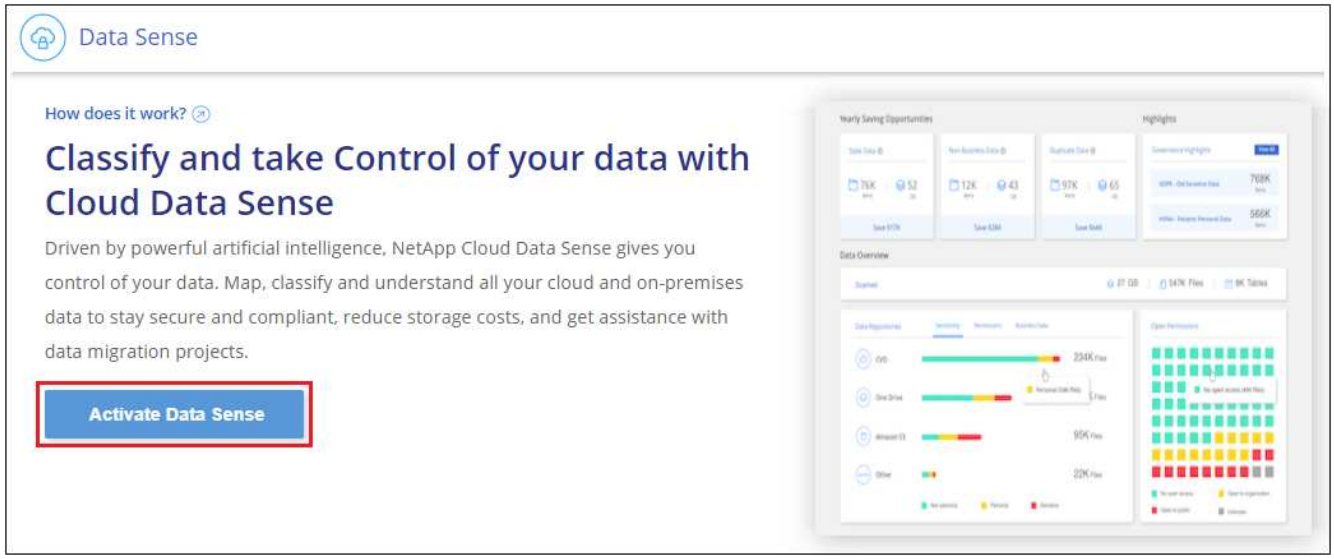
- Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 2개의 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 인터넷 액세스에 프록시를 사용하는 경우:
  - 프록시 서버 정보(IP 주소 또는 호스트 이름, 연결 포트, 연결 스키마: https 또는 http, 사용자 이름 및 암호)가 필요합니다.
  - 프록시가 TLS 가로채기를 수행하는 경우 TLS CA 인증서가 저장된 BlueXP 분류 Linux 시스템의 경로를 알아야 합니다.
  - 프록시는 투명하지 않아야 합니다. 현재 투명 프록시를 지원하지 않습니다.
  - 사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.
- 오프라인 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.

단계

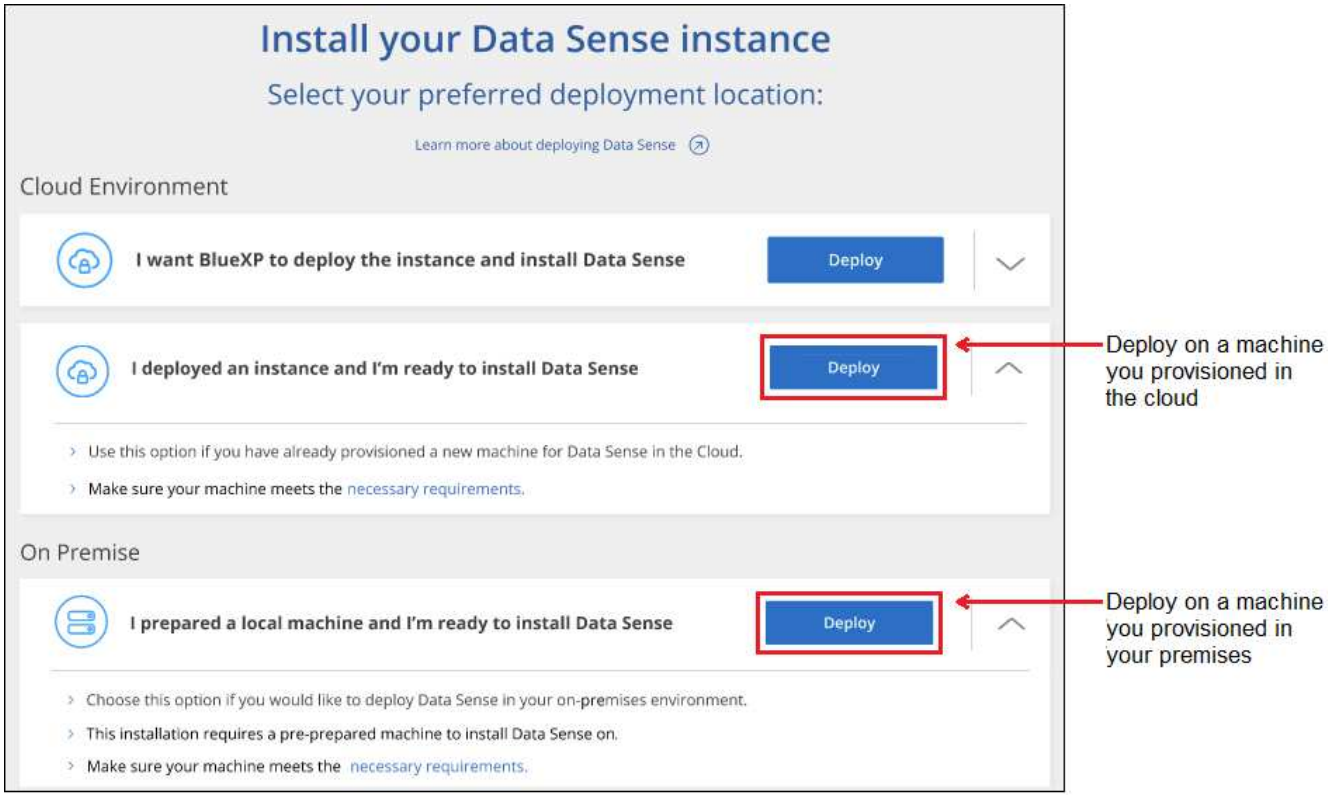
1. 에서 BlueXP 분류 소프트웨어를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * DATASENSE-INinstaller-<version>.tar.gz * 입니다.
2. 설치 프로그램 파일을 사용하려는 Linux 호스트에 복사합니다(scp 또는 다른 방법 사용).
3. 호스트 시스템에서 설치 프로그램 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

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

4. BlueXP에서 * 거버넌스 > 분류 * 를 선택합니다.
5. Activate Data Sense * 를 클릭합니다.



6. 클라우드에서 준비한 인스턴스 또는 사내에서 준비한 인스턴스에 BlueXP 분류를 설치할 것인지 여부에 따라 해당 * deploy * 버튼을 클릭하여 BlueXP 분류 설치를 시작합니다.



7. Deploy Data Sense on Premises_대화 상자가 표시됩니다. 제공된 명령을 복사합니다(예: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`)를 사용하여 텍스트 파일에 붙여 넣어 나중에 사용할 수 있습니다. 그런 다음 * 닫기 * 를 클릭하여 대화 상자를 닫습니다.

8. 호스트 시스템에서 복사한 명령을 입력한 다음 일련의 프롬프트를 따르거나 필요한 모든 매개 변수를 명령줄 인수로 포함하여 전체 명령을 제공할 수 있습니다.

   설치 프로그램은 사전 검사를 수행하여 시스템 및 네트워킹 요구 사항이 제대로 설치되어 있는지 확인합니다. "이 비디오 시청" 사전 점검 메시지 및 의미를 이해합니다.

프롬프트가 나타나면 매개 변수를 입력합니다.	전체 명령 입력:
a. 7단계에서 복사한 명령을 붙여 넣습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` 구내에 설치하지 않고 클라우드 인스턴스에 설치하는 경우 를 추가합니다 `--manual-cloud -install <cloud_provider>`. b. BlueXP 분류 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 Connector 시스템에서 액세스할 수 있도록 합니다. c. BlueXP 커넥터 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 BlueXP 분류 시스템에서 액세스할 수 있습니다. d. 메시지가 나타나면 프록시 세부 정보를 입력합니다. BlueXP Connector가 이미 프록시를 사용하고 있는 경우 BlueXP 분류가 자동으로 Connector에서 사용하는 프록시를 사용하기 때문에 이 정보를 다시 입력할 필요가 없습니다.	또는 필요한 호스트 및 프록시 매개 변수를 제공하여 전체 명령을 미리 생성할 수도 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 ID입니다
- *client_id*=커넥터 클라이언트 ID(클라이언트 ID에 접미어 "clients"가 없으면 추가)
- *USER_TOKEN*= JWT 사용자 액세스 토큰
- *DS_HOST*= BlueXP 분류 Linux 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm_host*= BlueXP 커넥터 시스템의 IP 주소 또는 호스트 이름입니다.
- *cloud_provider*= 클라우드 인스턴스에 설치할 때 클라우드 공급자에 따라 "AWS", "Azure" 또는 "GCP"를 입력하십시오.
- *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 체계: https 또는 http(기본값 http).
- *proxy_user*= 기본 인증이 필요한 경우 프록시 서버에 연결할 인증된 사용자입니다. 사용자는 로컬 사용자여야 합니다. - 도메인 사용자는 지원되지 않습니다.
- *proxy_password*=지정한 사용자 이름의 암호입니다.
- *ca_cert_dir*=추가 TLS CA 인증서 번들을 포함하는 BlueXP 분류 Linux 시스템의 경로입니다. 프록시가 TLS 가로채기를 수행하는 경우에만 필요합니다.

결과

BlueXP 분류 설치 프로그램은 패키지를 설치하고, 설치를 등록하고, BlueXP 분류를 설치합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

호스트 시스템과 커넥터 인스턴스 간에 포트 8080을 통해 연결되어 있는 경우 BlueXP의 BlueXP 분류 탭에서 설치

진행 상황을 확인할 수 있습니다.

다음 단계

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

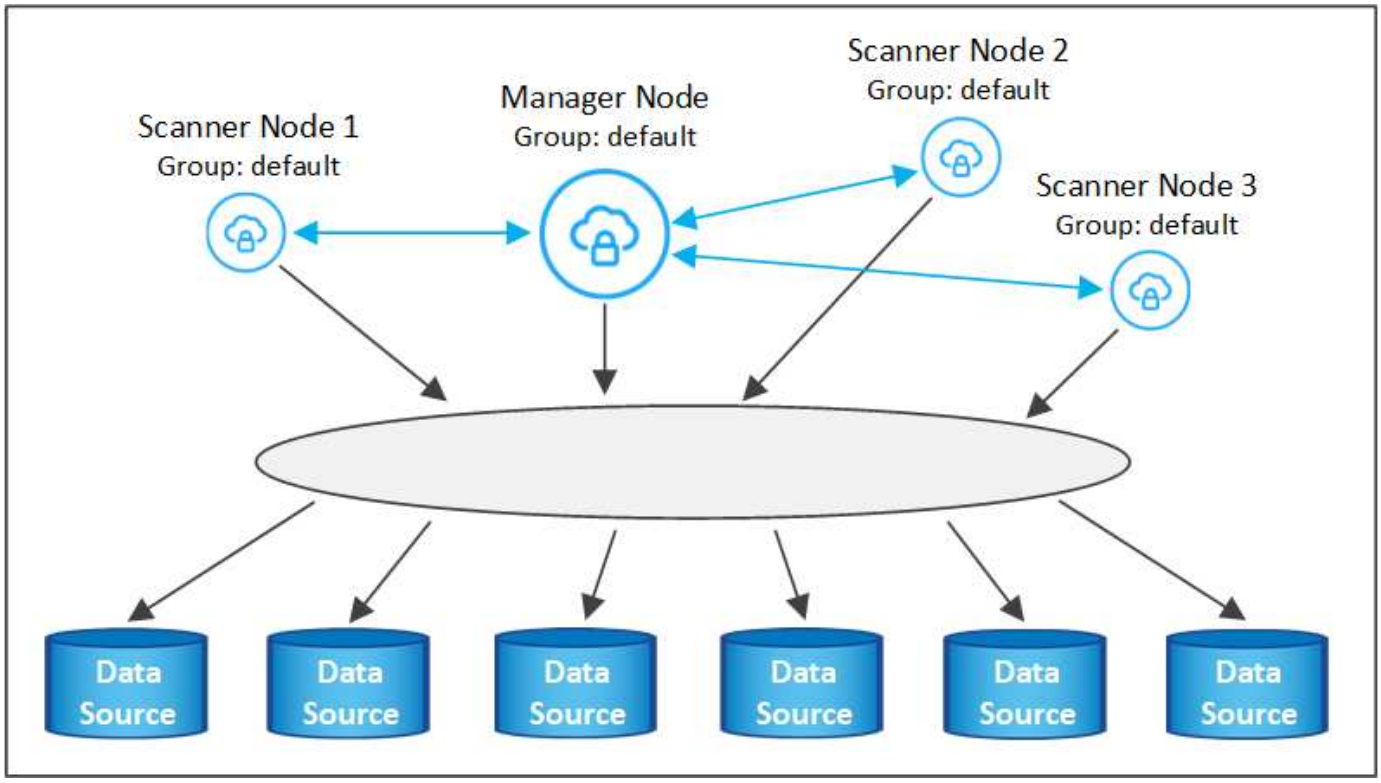
기존 배포에 스캐너 노드를 추가합니다

데이터 원본을 스캔하기 위해 스캔 처리 성능이 더 필요한 경우 스캐너 노드를 더 추가할 수 있습니다. 관리자 노드를 설치한 직후 스캐너 노드를 추가하거나 나중에 스캐너 노드를 추가할 수 있습니다. 예를 들어 데이터 소스 중 하나에 있는 데이터의 양이 6개월 후 두 배 또는 세 배 증가했다는 사실을 알고 있는 경우 데이터 스캔을 지원하기 위해 새 스캐너 노드를 추가할 수 있습니다.

다음 두 가지 방법으로 스캐너 노드를 추가할 수 있습니다.

- 노드를 추가하여 모든 데이터 소스 스캔에 도움을 줍니다
- 특정 데이터 소스 또는 특정 데이터 소스 그룹(일반적으로 위치에 따라 다름)을 스캔하는 데 도움이 되는 노드 추가

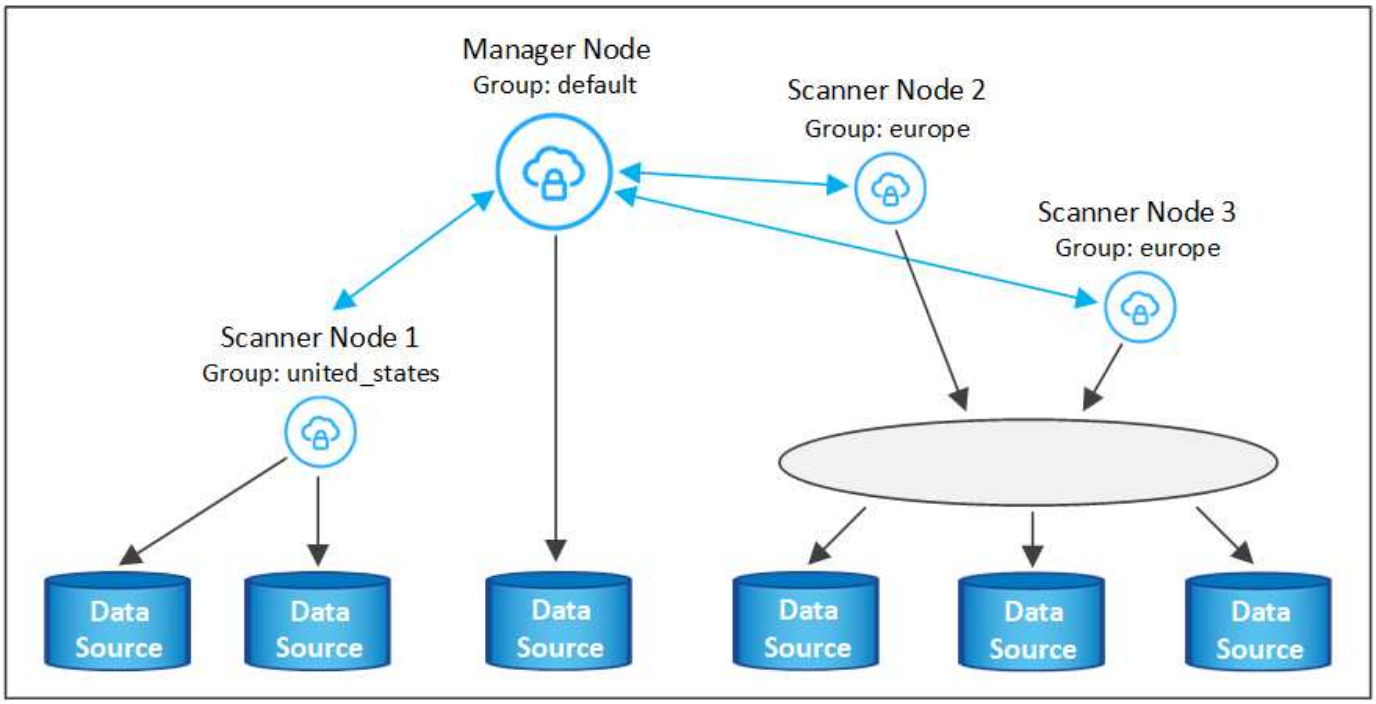
기본적으로 새로 추가한 스캐너 노드는 스캔 리소스의 일반 풀에 추가됩니다. 이를 "기본 스캐너 그룹"이라고 합니다. 아래 이미지의 "기본" 그룹에는 6개 데이터 소스 모두의 스캔 데이터인 1개의 관리자 노드와 3개의 스캐너 노드가 있습니다.



데이터 원본에 물리적으로 가까운 스캐너 노드에서 스캔할 특정 데이터 원본이 있는 경우 스캐너 노드 또는 스캐너 노드 그룹을 정의하여 특정 데이터 원본 또는 데이터 원본 그룹을 스캔할 수 있습니다. 아래 이미지에는 관리자 노드 1개와 스캐너 노드 3개가 있습니다.

- Manager 노드는 "기본" 그룹에 있으며 1개의 데이터 소스를 스캔하고 있습니다

- 스캐너 노드 1은 "United_states" 그룹에 있으며 2개의 데이터 소스를 스캔하고 있습니다
- 스캐너 노드 2와 3은 "유럽" 그룹에 속하며 3개의 데이터 원본에 대한 스캔 작업을 공유합니다



BlueXP 분류 스캐너 그룹은 데이터가 저장되는 별도의 지리적 영역으로 정의할 수 있습니다. 여러 BlueXP 분류 스캐너 노드를 전 세계에 배포하고 각 노드에 대해 스캐너 그룹을 선택할 수 있습니다. 이렇게 하면 각 스캐너 노드가 가장 가까운 데이터를 스캔합니다. 스캐너 노드가 데이터에 가까울수록 데이터 스캔 시 네트워크 대기 시간이 최대한 줄어들기 때문에 성능이 향상됩니다.

BlueXP 분류에 추가할 스캐너 그룹을 선택하고 이름을 선택할 수 있습니다. BlueXP 분류에서는 "유럽"이라는 스캐너 그룹에 매핑된 노드가 유럽에 배치되도록 강제하지 않습니다.

다음 단계에 따라 추가 BlueXP 분류 스캐너 노드를 설치합니다.

1. 스캐너 노드로 사용할 Linux 호스트 시스템을 준비합니다
2. 이 Linux 시스템에 Data Sense 소프트웨어를 다운로드하십시오
3. Manager 노드에서 명령을 실행하여 스캐너 노드를 식별합니다
4. 스캐너 노드에 소프트웨어를 배포하려면 다음 단계를 따르십시오(특정 스캐너 노드에 대해 "스캐너 그룹"을 선택적으로 정의).
5. 스캐너 그룹을 정의한 경우 관리자 노드에서 다음을 수행합니다.
   a. "working_environment_to_scanner_group_config.yml" 파일을 열고 각 스캐너 그룹이 스캔할 작업 환경을 정의합니다
   b. 다음 스크립트를 실행하여 이 매핑 정보를 모든 스캐너 노드에 등록합니다.
   `update_we_scanner_group_from_config_file.sh`

필요한 것

- 스캐너 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)가 설치되어 있는지 확인합니다.

- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 사용 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.
- 추가하려는 스캐너 노드 호스트의 IP 주소가 있어야 합니다.
- BlueXP 분류 관리자 노드 호스트 시스템의 IP 주소가 있어야 합니다
- 커넥터 시스템의 IP 주소 또는 호스트 이름, NetApp 계정 ID, 커넥터 클라이언트 ID 및 사용자 액세스 토큰이 있어야 합니다. 스캐너 그룹을 사용하려는 경우 계정의 각 데이터 원본에 대한 작업 환경 ID를 알아야 합니다. 이 정보를 보려면 아래의 *필수 단계 * 를 참조하십시오.
- 모든 호스트에서 다음 포트 및 프로토콜을 활성화해야 합니다.

포트	프로토콜	설명
2377	TCP	클러스터 관리 통신
7946	TCP, UDP	노드 간 통신
4789	UDP입니다	오버레이 네트워크 트래픽
50	ESP	암호화된 IPsec 오버레이 네트워크(ESP) 트래픽
111	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)
2049	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)

- 를 사용하는 경우 `firewalld` BlueXP 분류 시스템에서 BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

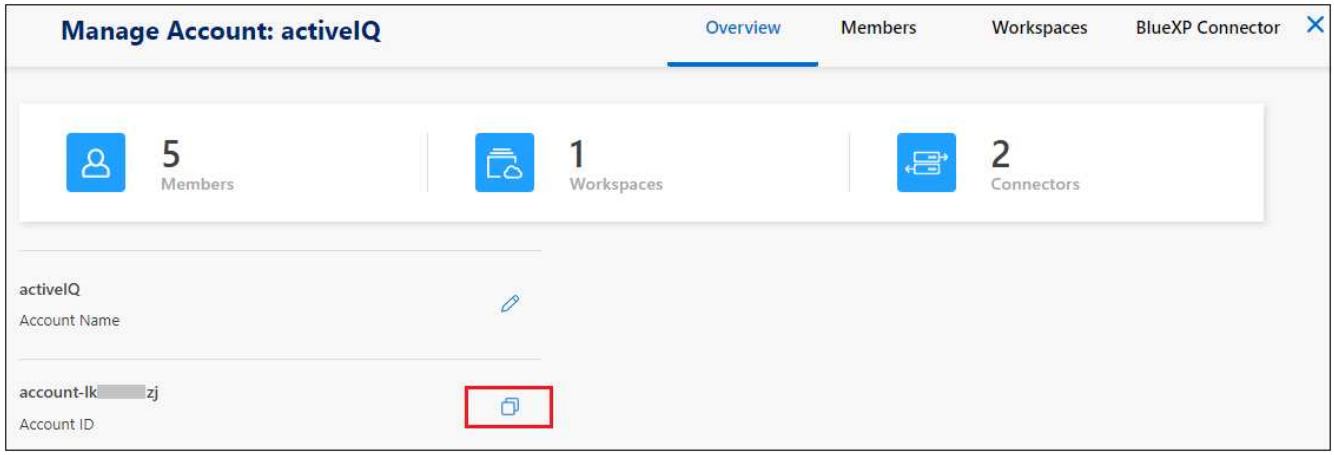
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

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

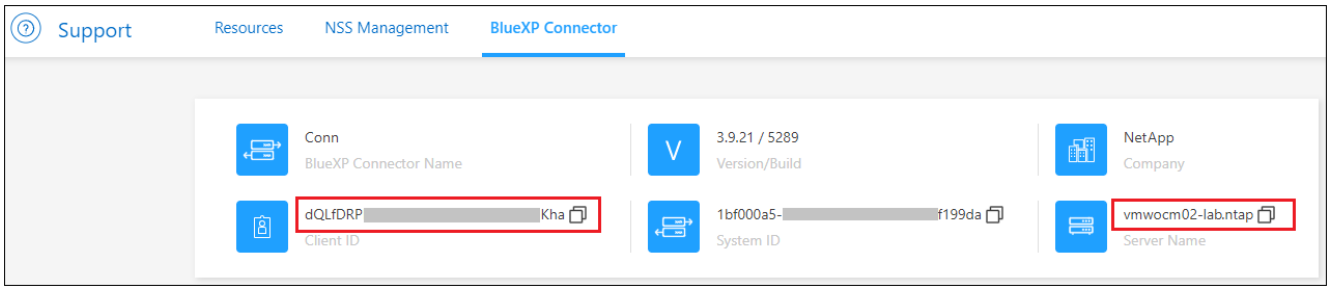
필수 단계

다음 단계에 따라 스캐너 노드를 추가하는 데 필요한 NetApp 계정 ID, 커넥터 클라이언트 ID, 커넥터 서버 이름 및 사용자 액세스 토큰을 얻습니다.

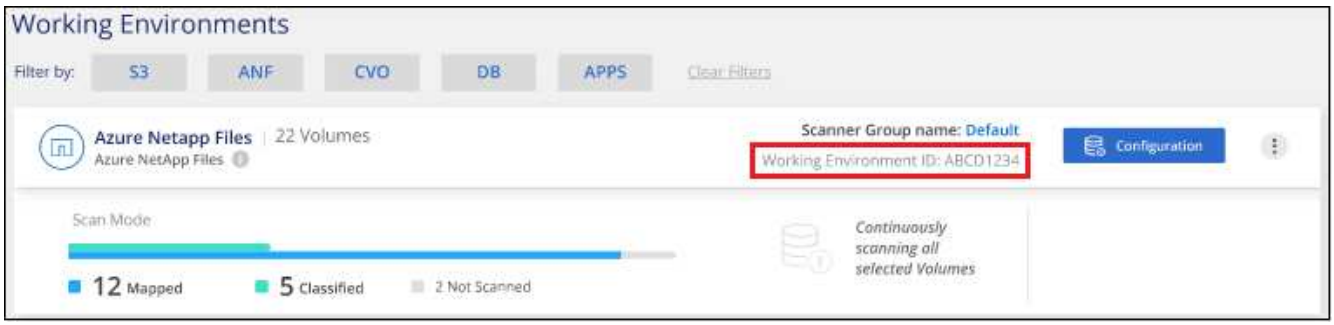
1. BlueXP 메뉴 표시줄에서 * 계정 > 계정 관리 * 를 클릭합니다.



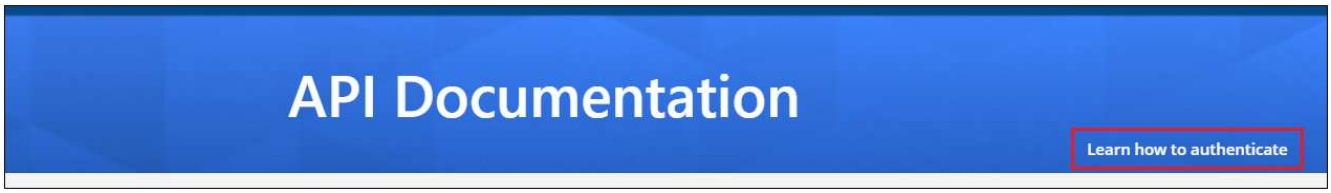
2. 계정 ID _ 을(를) 복사합니다.
3. BlueXP 메뉴 모음에서 * 도움말 > 지원 > BlueXP 커넥터 * 를 클릭합니다.



4. 커넥터_클라이언트 ID_ 및 _서버 이름_을 복사합니다.
5. 스캐너 그룹을 사용하려는 경우 BlueXP 분류 구성 탭에서 스캐너 그룹에 추가할 각 작업 환경의 작업 환경 ID를 복사합니다.



6. 로 이동합니다 "API 설명서 개발자 허브" 를 클릭하고 * 인증 방법 알아보기 * 를 클릭합니다.



7. "사용자 이름" 및 "암호" 매개 변수에서 계정 관리자의 사용자 이름과 암호를 사용하여 인증 지침을 따릅니다.
8. 그런 다음 응답에서 _ACCESS TOKEN_을 복사합니다.

단계

1. BlueXP 분류 관리자 노드에서 "add_scanner_node.sh" 스크립트를 실행합니다. 예를 들어, 이 명령은 두 개의 스캐너 노드를 추가합니다.

   ```
   sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h
   <ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
   ```

   변수 값:

   - *ACCOUNT_ID*= NetApp 계정 ID입니다
   - *client_id*=커넥터 클라이언트 ID(필수 조건 단계에서 복사한 클라이언트 ID에 접미사 "clients" 추가)
   - *cm_host*= 커넥터 시스템의 IP 주소 또는 호스트 이름입니다
   - *DS_MANAGER_IP*= BlueXP 분류 관리자 노드 시스템의 전용 IP 주소입니다
   - *node_private_ip*= BlueXP 분류 스캐너 노드 시스템의 IP 주소(여러 스캐너 노드 IP는 쉼표로 구분)
   - *USER_TOKEN*= JWT 사용자 액세스 토큰

2. add_scanner_node 스크립트가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사합니다(예: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`)를 입력하고 텍스트 파일에 저장합니다.

3. 켜짐 * 각 * 스캐너 노드 호스트:

   a. 데이터 감지 설치 프로그램 파일(* DATASENSE-INinstaller-<version>.tar.gz*)을 호스트 컴퓨터('scp' 또는 다른 방법 사용)에 복사합니다.

   b. 설치 프로그램 파일의 압축을 풉니다.

   c. 2단계에서 복사한 명령을 붙여 넣고 실행합니다.

   d. 스캐너 노드를 "scanner group"에 추가하려면 * -r <scanner_group_name> * 매개 변수를 명령에 추가합니다. 그렇지 않으면 스캐너 노드가 "기본" 그룹에 추가됩니다.

      모든 스캐너 노드에서 설치가 완료되고 관리자 노드에 연결된 경우 "add_scanner_node.sh" 스크립트도 완료됩니다. 설치하는 데 10-20분이 소요될 수 있습니다.

4. 스캐너 그룹에 스캐너 노드를 추가한 경우 관리자 노드로 돌아가 다음 두 가지 작업을 수행합니다.

   a. "/opt/netapp/config/custom_configuration/working_environment_to_scanner_group_config.yml" 파일을 열고 특정 작업 환경을 스캔할 스캐너 그룹의 매핑을 입력합니다. 각 데이터 소스에 대해 _Working Environment ID_가 있어야 합니다. 예를 들어 다음 항목은 "유럽" 스캐너 그룹에 작업 환경 2개를 추가하고 "United_states" 스캐너 그룹에 작업 환경 2개를 추가합니다.

```
scanner_groups:
 europe:
   working_environments:
     - "working_environment_id1"
     - "working_environment_id2"
 united_states:
   working_environments:
     - "working_environment_id3"
     - "working_environment_id4"
```

목록에 추가되지 않은 모든 작업 환경은 "기본" 그룹에 의해 스캔됩니다. "기본" 그룹에 하나 이상의 관리자 또는 스캐너 노드가 있어야 합니다.

b. 다음 스크립트를 실행하여 이 매핑 정보를 모든 스캐너 노드에 등록합니다.
`/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh`

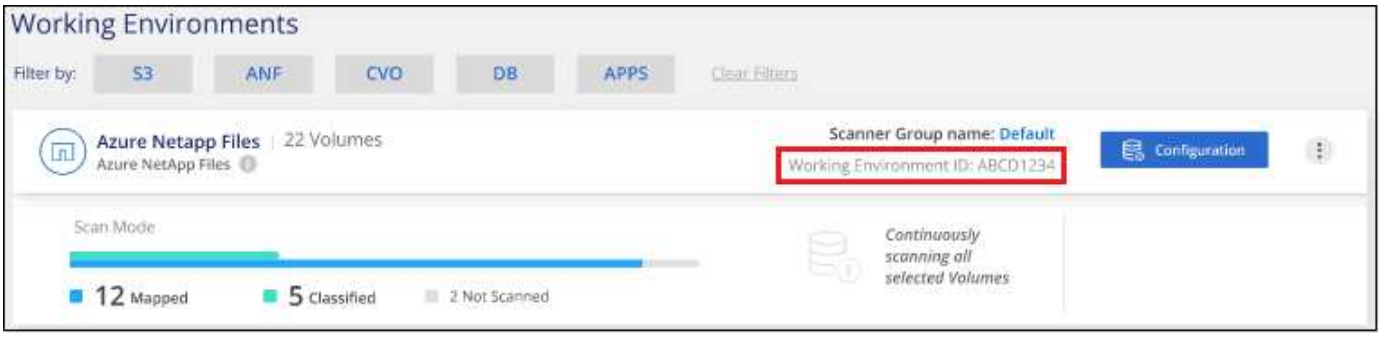
결과

BlueXP 분류는 모든 데이터 소스를 스캔하기 위해 관리자 및 스캐너 노드와 함께 설정됩니다.

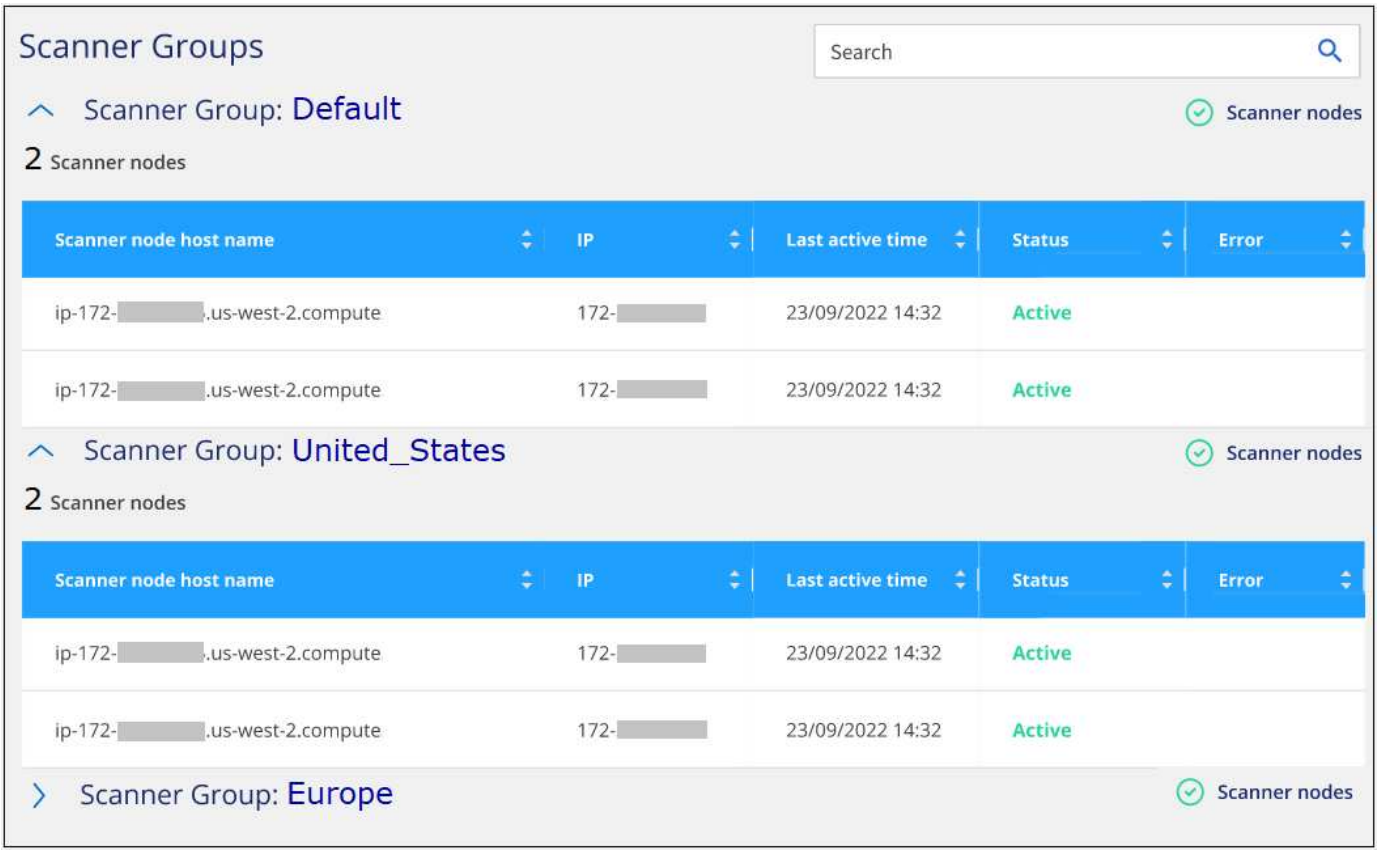
다음 단계

아직 선택하지 않은 경우 구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다. 스캐너 그룹을 생성한 경우 각 데이터 소스는 해당 그룹의 스캐너 노드에 의해 스캔됩니다.

구성 페이지에서 각 작업 환경에 대한 스캐너 그룹 이름을 볼 수 있습니다.



또한 구성 페이지 아래쪽에 있는 그룹의 각 스캐너 노드에 대한 IP 주소 및 상태와 함께 모든 스캐너 그룹 목록을 볼 수 있습니다.



가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

대규모 구성을 위한 다중 호스트 설치

페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여러 호스트 시스템을 사용하는 경우 주 시스템을 _Manager node_라고 하며 추가 처리 능력을 제공하는 추가 시스템을 _Scanner nodes_라고 합니다.

여러 온-프레미스 호스트에 BlueXP 분류 소프트웨어를 동시에 설치할 경우 다음 단계를 따르십시오. 이러한 방식으로 여러 호스트를 배포할 때는 "스캐너 그룹"을 사용할 수 없습니다.

필요한 것

- Manager 및 Scanner 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 두 가지 필수 소프트웨어 패키지(Docker 또는 Podman Engine 및 Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 사용 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.
- 사용하려는 스캐너 노드 호스트의 IP 주소가 있어야 합니다.
- 모든 호스트에서 다음 포트 및 프로토콜을 활성화해야 합니다.

포트	프로토콜	설명
2377	TCP	클러스터 관리 통신
7946	TCP, UDP	노드 간 통신

포트	프로토콜	설명
4789	UDP입니다	오버레이 네트워크 트래픽
50	ESP	암호화된 IPsec 오버레이 네트워크(ESP) 트래픽
111	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)
2049	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)

단계

1. 에서 1단계부터 7단계까지 수행합니다 단일 호스트 설치 관리자 노드에서.
2. 8단계에서 설명한 것처럼 설치 프로그램에서 메시지를 표시하면 일련의 프롬프트에 필요한 값을 입력하거나 설치 프로그램에 명령줄 인수로 필요한 매개 변수를 제공할 수 있습니다.

   단일 호스트 설치에 사용할 수 있는 변수 외에도 새 옵션 * -n<node_ip> * 를 사용하여 스캐너 노드의 IP 주소를 지정할 수 있습니다. 여러 스캐너 노드 IP는 쉼표로 구분됩니다.

   예를 들어, 이 명령은 다음과 같이 3개의 스캐너 노드를 추가합니다.
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy
   -host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme>
   --proxy-user <proxy_user> --proxy-password <proxy_password>
   ```
3. 관리자 노드 설치가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사합니다(예: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`)를 입력하고 텍스트 파일에 저장합니다.
4. 켜짐 * 각 * 스캐너 노드 호스트:
   a. 데이터 감지 설치 프로그램 파일(* DATASENSE-INinstaller-<version>.tar.gz*)을 호스트 컴퓨터('scp' 또는 다른 방법 사용)에 복사합니다.
   b. 설치 프로그램 파일의 압축을 풉니다.
   c. 3단계에서 복사한 명령을 붙여 넣고 실행합니다.

      모든 스캐너 노드에서 설치가 완료되고 관리자 노드에 연결되었으면 관리자 노드 설치도 완료됩니다.

결과

BlueXP 분류 설치 프로그램이 패키지 설치를 완료하고 설치를 등록합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

다음 단계

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 "BlueXP 분류 라이선스를 설정합니다" 현재. 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

인터넷에 액세스할 수 없는 **Linux** 호스트에 **BlueXP** 분류를 설치합니다

인터넷에 액세스할 수 없는 온프레미스 사이트의 Linux 호스트에 BlueXP 분류를 설치하려면 몇 단계를 완료하십시오. _ private mode _ 라고도 합니다. 이러한 유형의 설치는 보안 사이트에 적합합니다.

"BlueXP Connector 및 BlueXP 분류의 다양한 배포 모드에 대해 알아보십시오".

참고: 또한 이 기능을 사용할 수 있습니다 "인터넷에 액세스할 수 있는 사내 사이트에 BlueXP 분류를 배포합니다".

BlueXP 분류 설치 스크립트는 시스템 및 환경이 필수 전제 조건을 충족하는지 확인하는 것으로 시작됩니다. 필수 구성 요소가 모두 충족되면 설치가 시작됩니다. BlueXP 분류 설치를 실행하는 것과 별도로 필수 구성 요소를 확인하려면 필수 구성 요소에 대한 테스트만 다운로드할 수 있는 별도의 소프트웨어 패키지가 있습니다. "Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인하는 방법을 참조하십시오".

지원되는 데이터 소스

비공개 모드("오프라인" 또는 "다크" 사이트라고도 함)를 설치할 경우 BlueXP 분류는 사내 사이트에 로컬인 데이터 소스에서만 데이터를 스캔할 수 있습니다. 현재 BlueXP 분류는 다음 * 로컬 * 데이터 소스를 검사할 수 있습니다.

- 온프레미스 ONTAP 시스템
- 데이터베이스 스키마
- SharePoint 사내 계정(SharePoint Server)
- 비NetApp NFS 또는 CIFS 파일 공유
- S3(Simple Storage Service) 프로토콜을 사용하는 오브젝트 스토리지

현재 Cloud Volumes ONTAP, Azure NetApp Files, FSx for ONTAP, AWS S3 또는 Google Drive 스캔을 지원하지 않습니다. BlueXP 분류가 개인 모드로 배포되는 경우 OneDrive 또는 SharePoint Online 계정

제한 사항

대부분의 BlueXP 분류 기능은 인터넷에 액세스할 수 없는 사이트에 배포할 때 작동합니다. 그러나 인터넷 액세스가 필요한 특정 기능은 지원되지 않습니다. 예를 들면 다음과 같습니다.

- Microsoft Azure 정보 보호(AIP) 레이블 관리
- 특정 중요 정책이 결과를 반환할 때 BlueXP 사용자에게 전자 메일 알림을 보냅니다
- 여러 사용자에 대한 BlueXP 역할 설정(예: 계정 관리자 또는 규정 준수 뷰어)
- BlueXP 복사 및 동기화를 사용하여 소스 파일 복사 및 동기화
- 사용자 피드백을 받는 중입니다
- BlueXP에서 소프트웨어 자동 업그레이드

  BlueXP 커넥터와 BlueXP 분류 모두 새로운 기능을 사용하려면 정기적인 수동 업그레이드가 필요합니다. BlueXP 분류 UI 페이지 하단에서 BlueXP 분류 버전을 확인할 수 있습니다. 를 확인하십시오 "BlueXP 분류 릴리스 정보" 각 릴리스의 새로운 기능과 해당 기능을 원하는지 여부를 확인합니다. 그런 다음 의 단계를 수행할 수 있습니다 "BlueXP 커넥터를 업그레이드합니다" 및 BlueXP 분류 소프트웨어를 업그레이드합니다.

빠른 시작

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

1 **BlueXP** 커넥터를 설치합니다

아직 비공개 모드로 커넥터가 설치되어 있지 않은 경우 "커넥터를 배포합니다" 이제 Linux 호스트에서

2 **BlueXP** 분류 사전 요구 사항을 검토합니다

Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항필요한 모든 소프트웨어가 설치되어 있고 오프라인 환경이 필요한 를 충족한다는 것을 나타냅니다 사용 권한 및 연결.

3 **BlueXP** 분류를 다운로드하고 배포합니다

NetApp Support 사이트에서 BlueXP 분류 소프트웨어를 다운로드하고 사용할 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 시작하고 화면의 지시에 따라 BlueXP 분류 인스턴스를 배포합니다.

4 **BlueXP** 분류 서비스에 가입합니다

BlueXP의 BlueXP 분류 검사에서 처음 1TB의 데이터는 30일 동안 무료로 제공됩니다. 이 시점 이후에 데이터를 계속 스캔하려면 NetApp의 BYOL 라이센스가 필요합니다.

BlueXP 커넥터를 설치합니다

BlueXP 커넥터가 아직 비공개 모드로 설치되어 있지 않은 경우 "커넥터를 배포합니다" 오프라인 사이트의 Linux 호스트

Linux 호스트 시스템을 준비합니다

BlueXP 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행해야 합니다.

- BlueXP 분류는 다른 애플리케이션과 공유되는 호스트에서는 지원되지 않습니다. 호스트는 전용 호스트여야 합니다.
- 구내 호스트 시스템을 구축할 때 BlueXP 분류 검사를 수행할 데이터 세트의 크기에 따라 세 가지 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 초대형 *	32개의 CPU	128GB RAM	/, 또는 의 1TiB SSD /opt에서 -100GiB를 사용할 수 있습니다 -895GiB는 /var/lib/docker에서 사용할 수 있습니다 /tmp에 -5GiB입니다

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 대형 *	CPU 16개	64GB RAM	500GiB SSD 켜짐/또는 /opt에서 -100GiB를 사용할 수 있습니다 /var/lib/docker에서 사용 가능한 395GiB /tmp에 -5GiB입니다
* 중간 *	CPU 8개	32GB RAM	200GiB SSD 켜짐/또는 /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -145GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다
* 소형 *	CPU 8개	16GB RAM	또는 에서 100GiB SSD /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -45GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다

소형 시스템을 사용할 때는 제한이 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

- BlueXP 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때는 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 권장합니다.
  - * AWS EC2 인스턴스 유형 *: "m6i.4xLarge"를 권장합니다. "추가 AWS 인스턴스 유형을 참조하십시오".
  - * Azure VM size *: "Standard_D16s_v3"을 권장합니다. "추가 Azure 인스턴스 유형을 참조하십시오".
  - * GCP 시스템 유형 *: "n2-standard-16"을 권장합니다. "추가 GCP 인스턴스 유형을 참조하십시오".
- UNIX 폴더 권한 *: 다음과 같은 최소 UNIX 권한이 필요합니다.

폴더	최소 권한
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker입니다	`rwx------`
/usr/lib/systemd/system입니다	`rwxr-xr-x`

- * 운영 체제 *:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9
    - CentOS 버전 7.8 및 7.9
    - Ubuntu 22.04(BlueXP 분류 버전 1.23 이상 필요)
  - 다음 운영 체제에는 Podman 컨테이너 엔진을 사용해야 하며 BlueXP 분류 버전 1.30 이상이 필요합니다.
    - Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3

RHEL 8.x 및 RHEL 9.x를 사용하는 경우 다음 기능은 현재 지원되지 않습니다.

  - 어두운 장소에 설치
  - 분산 스캔, 마스터 스캐너 노드 및 원격 스캐너 노드 사용

- * Red Hat 서브스크립션 관리 *: 호스트는 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 설치 중에 시스템에서 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.
- * 추가 소프트웨어 *: BlueXP 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
  - 사용 중인 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
    - Docker Engine 버전 19.3.1 이상 "설치 지침을 봅니다".

      "이 비디오 시청" CentOS에 Docker를 설치하는 빠른 데모를 보려면

    - Podman 버전 4 이상 Podman을 설치하려면 시스템 패키지를 업데이트하십시오 (`sudo yum update -y`)를 클릭한 다음 Podman을 설치합니다 (`sudo yum install netavark -y`)를 클릭합니다.
- Python 버전 3.6 이상. "설치 지침을 봅니다".
  - * NTP 고려 사항 *: NetApp에서는 NTP(네트워크 시간 프로토콜) 서비스를 사용하도록 BlueXP 분류 시스템을 구성할 것을 권장합니다. BlueXP 분류 시스템과 BlueXP Connector 시스템 간에 시간을 동기화해야 합니다.
  - * Firewalld 고려 사항 *: 사용하려는 경우 `firewalld`BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

```
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
```

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

설치 후 BlueXP 분류 호스트 시스템의 IP 주소를 변경할 수 없습니다.

BlueXP 및 **BlueXP** 분류 사전 요구 사항을 확인합니다

BlueXP 분류를 배포하기 전에 다음 전제 조건을 검토하여 지원되는 구성이 있는지 확인합니다.

- Connector에 리소스를 배포하고 BlueXP 분류 인스턴스에 대한 보안 그룹을 만들 수 있는 권한이 있는지 확인합니다. 최신 BlueXP 사용 권한은 에서 확인할 수 있습니다 "NetApp에서 제공하는 정책".
- BlueXP 분류를 계속 실행할 수 있는지 확인합니다. 데이터를 지속적으로 스캔하려면 BlueXP 분류 인스턴스를 계속 사용해야 합니다.
- 웹 브라우저가 BlueXP 분류에 연결되어 있는지 확인합니다. BlueXP 분류를 사용하도록 설정한 후에는 BlueXP 분류 인스턴스에 연결된 호스트에서 BlueXP 인터페이스에 액세스해야 합니다.

  BlueXP 분류 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터에 다른 사용자가 액세스할 수 없도록 합니다. 따라서 BlueXP에 액세스하는 데 사용하는 웹 브라우저가 해당 개인 IP 주소에 연결되어 있어야 합니다. 이러한

연결은 BlueXP 분류 인스턴스와 동일한 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

필요한 모든 포트가 활성화되어 있는지 확인합니다

커넥터, BlueXP 분류, Active Directory 및 데이터 소스 간의 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

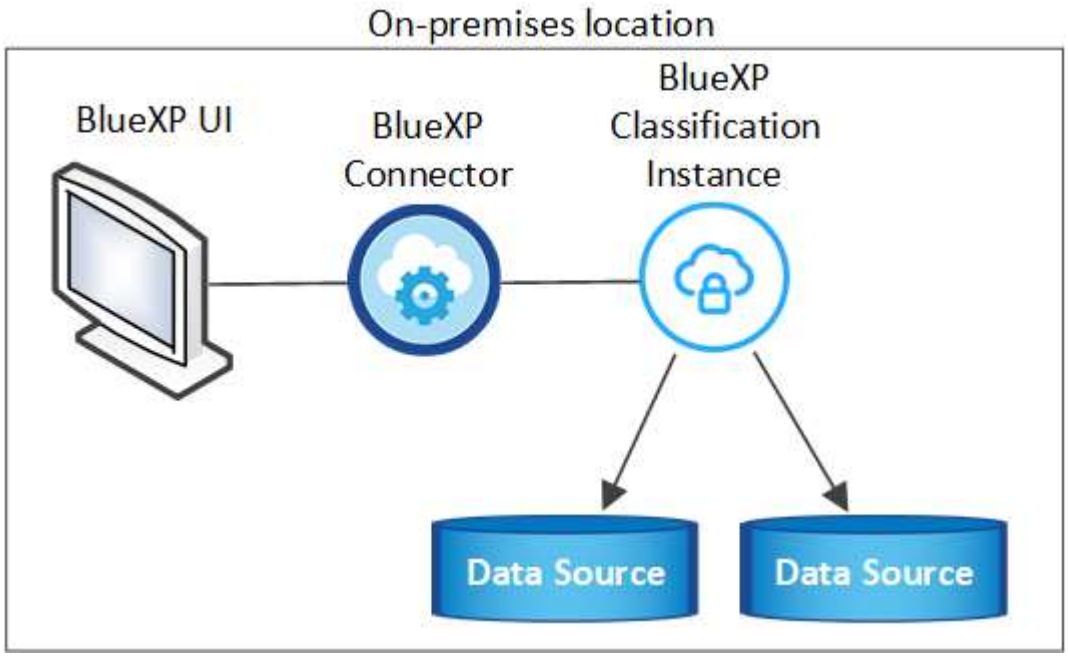
연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 6000(TCP), 443(TCP) 및 80	Connector의 보안 그룹은 포트 6000 및 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. • BlueXP 분류 BYOL 라이센스가 다크 사이트에서 작동하도록 하려면 포트 6000이 필요합니다. • BlueXP에서 설치 진행률을 확인할 수 있도록 포트 8080이 열려 있어야 합니다.
커넥터 <>ONTAP 클러스터(NAS)	443(TCP)	BlueXP는 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 다음 요구 사항을 충족해야 합니다. • 커넥터 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. Connector가 클라우드에 있는 경우 모든 아웃바운드 통신은 미리 정의된 보안 그룹에서 허용됩니다. • ONTAP 클러스터는 포트 443을 통한 인바운드 HTTPS 액세스를 허용해야 합니다. 기본 "관리" 방화벽 정책은 모든 IP 주소에서 인바운드 HTTPS 액세스를 허용합니다. 이 기본 정책을 수정하거나 자체 방화벽 정책을 만든 경우 HTTPS 프로토콜을 해당 정책에 연결하고 Connector 호스트에서 액세스를 활성화해야 합니다.
BlueXP 분류<>ONTAP 클러스터	• NFS-111(TCP\UDP) 및 2049(TCP\UDP)의 경우 • CIFS-139(TCP\UDP) 및 445(TCP\UDP)의 경우	BlueXP 분류에는 각 Cloud Volumes ONTAP 서브넷 또는 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다. Cloud Volumes ONTAP의 보안 그룹은 BlueXP 분류 인스턴스에서 인바운드 연결을 허용해야 합니다. 이러한 포트가 BlueXP 분류 인스턴스에 열려 있는지 확인합니다. • NFS-111 및 2049용 • CIFS-139 및 445의 경우 NFS 볼륨 내보내기 정책은 BlueXP 분류 인스턴스에서 액세스를 허용해야 합니다.

연결 유형	포트	설명
BlueXP 분류<>Active Directory	389(TCP 및 UDP), 636(TCP), 3268(TCP) 및 3269(TCP)	회사의 사용자에 대해 Active Directory가 이미 설정되어 있어야 합니다. 또한 BlueXP 분류에는 CIFS 볼륨을 스캔하기 위해 Active Directory 자격 증명이 필요합니다. Active Directory에 대한 정보가 있어야 합니다. • DNS 서버 IP 주소 또는 여러 IP 주소 • 서버의 사용자 이름 및 암호 • 도메인 이름(Active Directory 이름) • 보안 LDAP(LDAPS) 사용 여부 • LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)

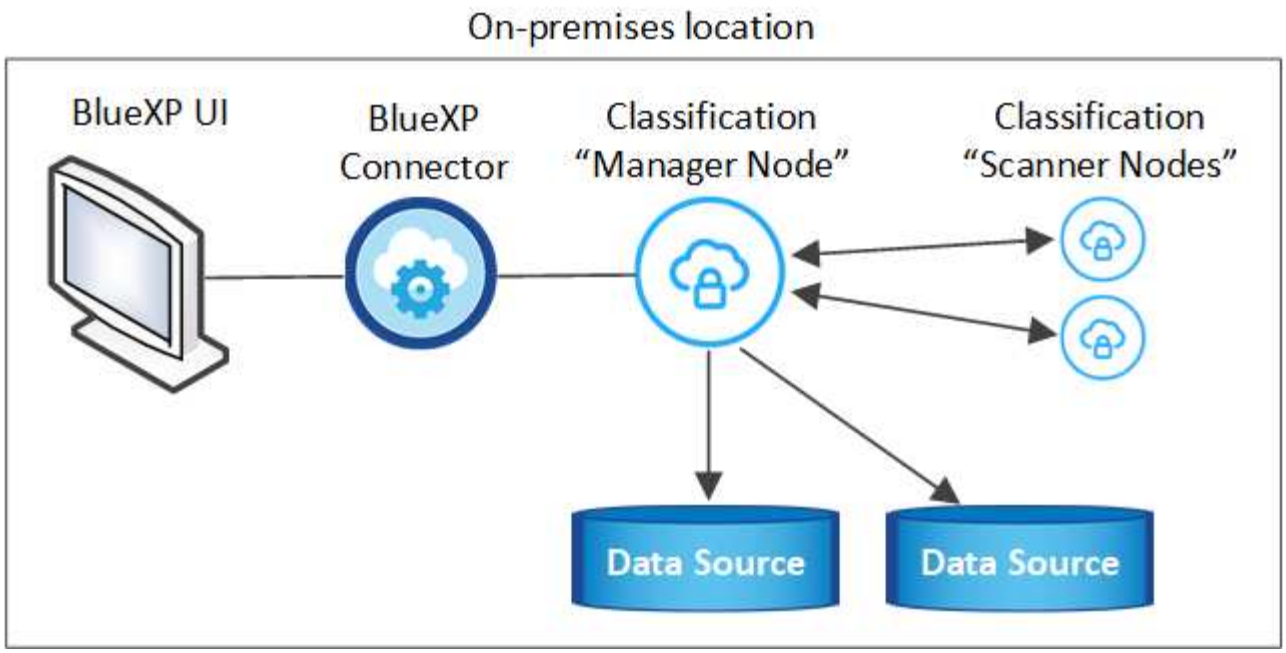
여러 BlueXP 분류 호스트를 사용하여 데이터 소스를 검사하는 추가 처리 기능을 제공하는 경우 추가 포트/프로토콜을 활성화해야 합니다. "추가 포트 요구 사항을 참조하십시오".

사내 **Linux** 호스트에 **BlueXP** 분류를 설치합니다

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



페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. "여기에서 해당 단계를 확인하십시오".



일반 구성을 위한 단일 호스트 설치

오프라인 환경의 단일 사내 호스트에 BlueXP 분류 소프트웨어를 설치할 때는 다음 단계를 따르십시오.

모든 설치 작업은 BlueXP 분류를 설치할 때 기록됩니다. 설치 중에 문제가 발생하면 설치 감사 로그의 내용을 볼 수 있습니다. 에 기록됩니다 `/opt/netapp/install_logs/`. "자세한 내용은 여기에서 확인하십시오.".

필요한 것

- Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항.
- 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)를 설치했는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 오프라인 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.

단계

1. 인터넷 구성 시스템의 경우 에서 BlueXP 분류 소프트웨어를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * DataSense-offline-bundle-<version>.tar.gz * 입니다.
2. 개인 모드에서 사용할 Linux 호스트에 설치 프로그램 번들을 복사합니다.
3. 호스트 시스템에서 설치 프로그램 번들의 압축을 풉니다. 예를 들면 다음과 같습니다.

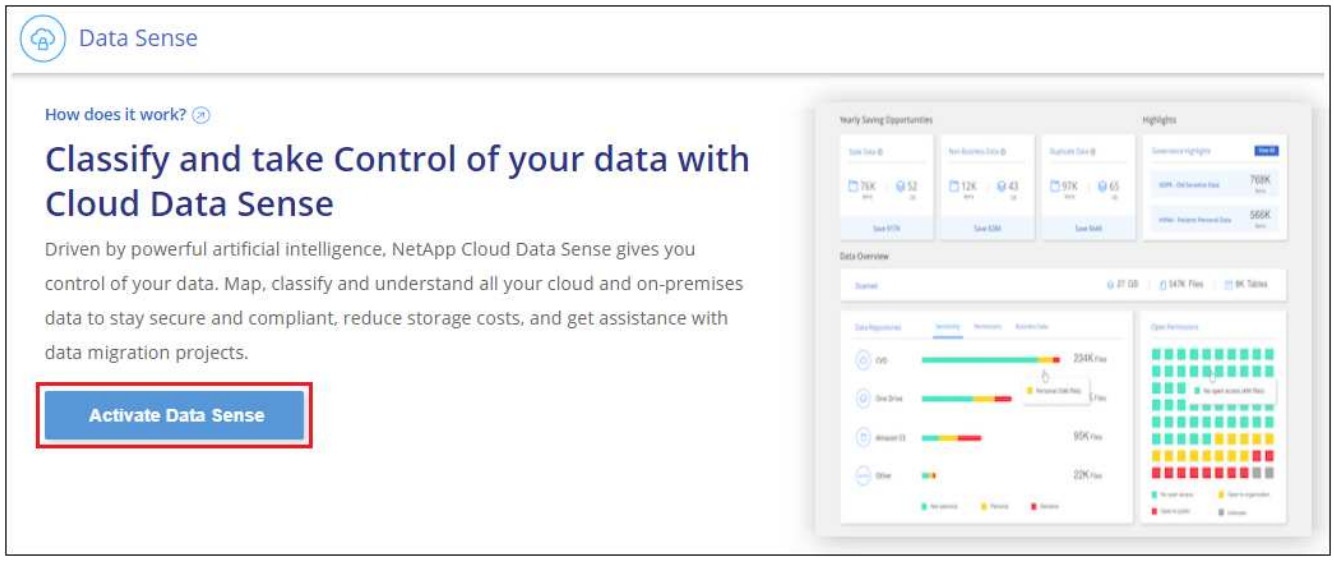
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   필요한 소프트웨어와 실제 설치 파일 * cc_onprem_installer.tar.gz * 를 추출합니다.

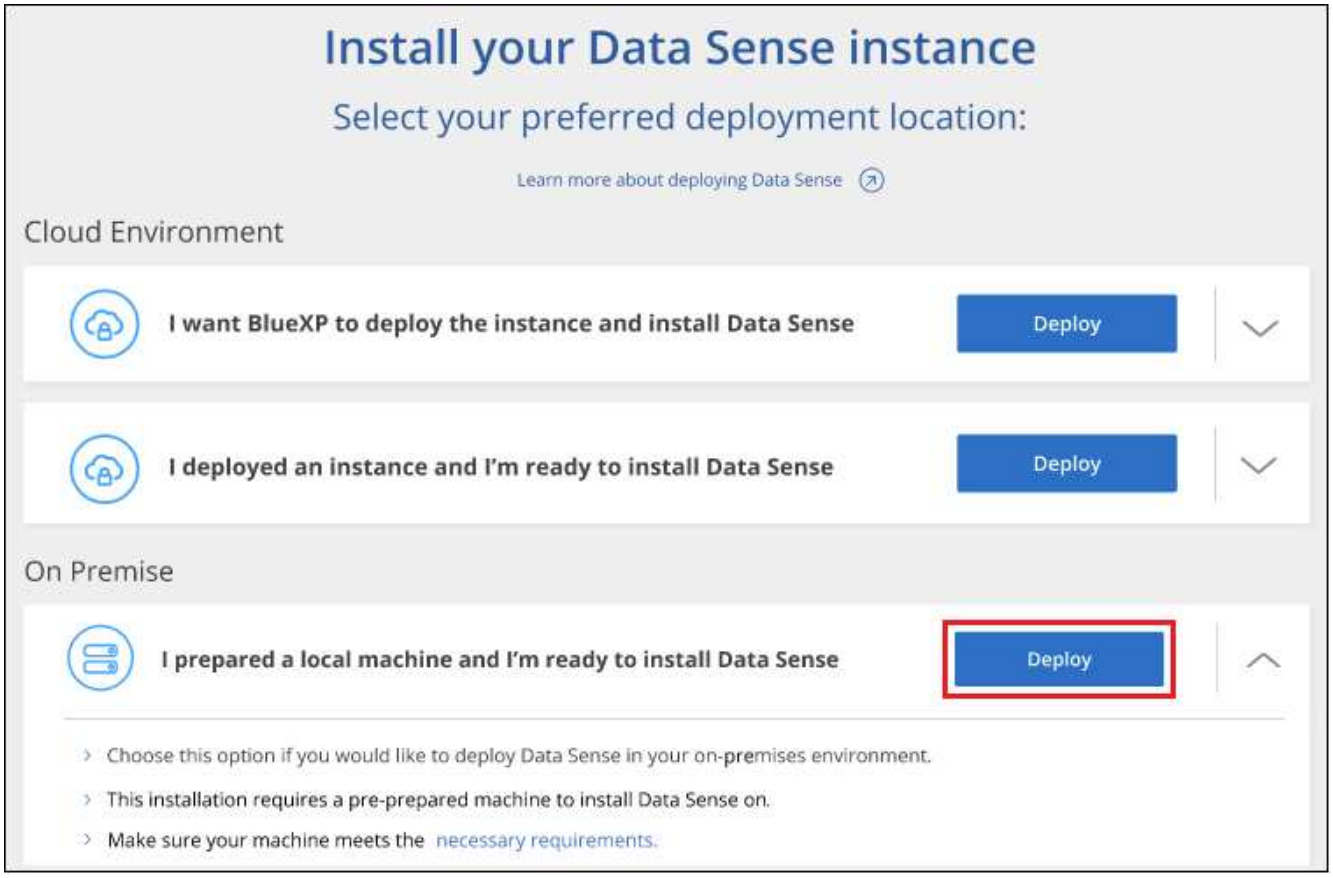
4. 호스트 시스템에서 설치 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

5. BlueXP를 시작하고 * Governance > Classification * 을 선택합니다.
6. Activate Data Sense * 를 클릭합니다.



7. 사내 설치를 시작하려면 * deploy * 를 클릭합니다.



8. Deploy Data Sense on Premises_대화 상자가 표시됩니다. 제공된 명령을 복사합니다(예: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`)를 사용하여 텍스트 파일에 붙여 넣어 나중에 사용할 수 있습니다. 그런 다음 * 닫기 * 를 클릭하여 대화 상자를 닫습니다.
9. 호스트 시스템에서 복사한 명령을 입력한 다음 일련의 프롬프트를 따르거나 필요한 모든 매개 변수를 명령줄 인수로

포함하여 전체 명령을 제공할 수 있습니다.

설치 프로그램은 사전 검사를 수행하여 시스템 및 네트워킹 요구 사항이 제대로 설치되어 있는지 확인합니다.

프롬프트가 나타나면 매개 변수를 입력합니다.	전체 명령 입력:
a. 8단계에서 복사한 정보를 붙여 넣습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. BlueXP 분류 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 Connector 시스템에서 액세스할 수 있도록 합니다. c. BlueXP 커넥터 호스트 시스템의 IP 주소 또는 호스트 이름을 입력하여 BlueXP 분류 시스템에서 액세스할 수 있습니다.	또는 필요한 호스트 매개 변수를 제공하여 전체 명령을 미리 생성할 수도 있습니다. `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

변수 값:

- *ACCOUNT_ID*= NetApp 계정 ID입니다
- *client_id*=커넥터 클라이언트 ID(클라이언트 ID에 접미어 "clients"가 없으면 추가)
- *USER_TOKEN*= JWT 사용자 액세스 토큰
- *DS_HOST*= BlueXP 분류 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm_host*= BlueXP 커넥터 시스템의 IP 주소 또는 호스트 이름입니다.

결과

BlueXP 분류 설치 프로그램은 패키지를 설치하고, 설치를 등록하고, BlueXP 분류를 설치합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

호스트 시스템과 커넥터 인스턴스 간에 포트 8080을 통해 연결되어 있는 경우 BlueXP의 BlueXP 분류 탭에서 설치 진행 상황을 확인할 수 있습니다.

다음 단계

구성 페이지에서 로컬 을 선택할 수 있습니다 "온프레미스 ONTAP 클러스터" 및 "데이터베이스를 지원합니다" 선택합니다.

또한 가능합니다 "BlueXP 분류에 대한 BYOL 라이센스 설정" 현재 BlueXP 디지털 전자지갑에서 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

대규모 구성을 위한 다중 호스트 설치

페타바이트 단위의 데이터를 스캐닝할 대규모 구성의 경우 여러 호스트를 포함하여 추가적인 처리 성능을 제공할 수 있습니다. 여러 호스트 시스템을 사용하는 경우 주 시스템을 _Manager node_라고 하며 추가 처리 능력을 제공하는 추가 시스템을 _Scanner nodes_라고 합니다.

오프라인 환경의 여러 사내 호스트에 BlueXP 분류 소프트웨어를 설치할 때는 다음 단계를 따르십시오.

필요한 것

- Manager 및 Scanner 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 호스트 요구 사항.
- 두 가지 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)를 설치했는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 오프라인 환경이 필요한 를 충족하는지 확인합니다 사용 권한 및 연결.
- 사용하려는 스캐너 노드 호스트의 IP 주소가 있어야 합니다.
- 모든 호스트에서 다음 포트 및 프로토콜을 활성화해야 합니다.

포트	프로토콜	설명
2377	TCP	클러스터 관리 통신
7946	TCP, UDP	노드 간 통신
4789	UDP입니다	오버레이 네트워크 트래픽
50	ESP	암호화된 IPsec 오버레이 네트워크(ESP) 트래픽
111	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)
2049	TCP, UDP	호스트 간 파일 공유를 위한 NFS 서버(각 스캐너 노드에서 관리자 노드로 필요)

단계

1. 에서 1단계부터 8단계까지 수행합니다 "단일 호스트 설치" 관리자 노드에서.
2. 9단계에서 설명한 것처럼 설치 관리자가 메시지를 표시하면 일련의 프롬프트에 필요한 값을 입력하거나 설치 프로그램에 명령줄 인수로 필요한 매개 변수를 제공할 수 있습니다.

   단일 호스트 설치에 사용할 수 있는 변수 외에도 새 옵션 * -n<node_ip> * 를 사용하여 스캐너 노드의 IP 주소를 지정할 수 있습니다. 여러 노드 IP는 쉼표로 구분됩니다.

   예를 들어, 이 명령은 다음과 같이 3개의 스캐너 노드를 추가합니다.
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no
   -proxy --darksite
   ```
3. 관리자 노드 설치가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사합니다(예: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`)를 입력하고 텍스트 파일에 저장합니다.
4. 켜짐 * 각 * 스캐너 노드 호스트:
   a. Data Sense 설치 프로그램 파일(* cc_onpremise_installer.tar.gz *)을 호스트 컴퓨터에 복사합니다.
   b. 설치 프로그램 파일의 압축을 풉니다.
   c. 3단계에서 복사한 명령을 붙여 넣고 실행합니다.

      모든 스캐너 노드에서 설치가 완료되고 관리자 노드에 연결되었으면 관리자 노드 설치도 완료됩니다.

결과

BlueXP 분류 설치 프로그램이 패키지 설치를 완료하고 설치를 등록합니다. 설치에는 15 ~ 25분이 소요될 수 있습니다.

다음 단계

구성 페이지에서 로컬 을 선택할 수 있습니다 "온프레미스 ONTAP 클러스터" 및 로컬 "데이터베이스를 지원합니다" 선택합니다.

또한 가능합니다 "BlueXP 분류에 대한 BYOL 라이센스 설정" 현재 BlueXP 디지털 전자지갑에서 30일 무료 평가판이 종료될 때까지 요금이 부과되지 않습니다.

BlueXP 분류 소프트웨어를 업그레이드합니다

BlueXP 분류 소프트웨어는 정기적으로 새로운 기능으로 업데이트되므로 정기적으로 새로운 버전을 확인하여 최신 소프트웨어와 기능을 사용하고 있는지 확인해야 합니다. 업그레이드를 자동으로 수행하기 위한 인터넷 연결이 없기 때문에 BlueXP 분류 소프트웨어를 수동으로 업그레이드해야 합니다.

시작하기 전에

- BlueXP Connector 소프트웨어를 최신 버전으로 업그레이드하는 것이 좋습니다. "커넥터 업그레이드 단계를 참조하십시오".
- BlueXP 분류 버전 1.24부터 향후 모든 소프트웨어 버전으로 업그레이드할 수 있습니다.

  BlueXP 분류 소프트웨어가 1.24 이전 버전을 실행 중인 경우 한 번에 하나의 주요 버전만 업그레이드할 수 있습니다. 예를 들어, 버전 1.21.x가 설치되어 있는 경우 1.22.x로 업그레이드할 수 있습니다 몇 가지 주요 버전이 뒤쳐지면 소프트웨어를 여러 번 업그레이드해야 합니다.

단계

1. 인터넷 구성 시스템의 경우 에서 BlueXP 분류 소프트웨어를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * DataSense-offline-bundle-<version>.tar.gz * 입니다.
2. 소프트웨어 번들을 Linux 호스트에 복사하면 BlueXP 분류가 다크 사이트에 설치됩니다.
3. 호스트 시스템에서 소프트웨어 번들의 압축을 풉니다. 예를 들면 다음과 같습니다.

   ```
   tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   그러면 설치 파일 * cc_onpremise_installer.tar.gz * 가 추출됩니다.

4. 호스트 시스템에서 설치 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

   그러면 업그레이드 스크립트 * start_darsite_upgrade.sh * 와 필요한 타사 소프트웨어가 추출됩니다.

5. 호스트 시스템에서 업그레이드 스크립트를 실행합니다. 예를 들면 다음과 같습니다.

   ```
   start_darksite_upgrade.sh
   ```

결과

BlueXP 분류 소프트웨어가 호스트에서 업그레이드됩니다. 업데이트는 5분에서 10분 정도 소요될 수 있습니다.

대규모 구성을 스캔하기 위해 여러 호스트 시스템에 BlueXP 분류를 배포한 경우에는 스캐너 노드에 업그레이드가 필요하지 않습니다.

BlueXP 분류 UI 페이지 하단에 있는 버전을 확인하여 소프트웨어가 업데이트되었는지 확인할 수 있습니다.

Linux 호스트가 BlueXP 분류를 설치할 준비가 되었는지 확인합니다

Linux 호스트에 수동으로 BlueXP 분류를 설치하기 전에 호스트에서 스크립트를 실행하여 BlueXP 분류를 설치하기 위한 모든 필수 구성 요소가 준비되어 있는지 확인할 수 있습니다. 이 스크립트는 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트에서 실행할 수 있습니다. 호스트를 인터넷에 연결하거나 호스트가 인터넷에 액세스할 수 없는 사이트(A_Dark site_)에 상주할 수 있습니다.

BlueXP 분류 설치 스크립트의 일부인 필수 테스트 스크립트도 있습니다. 여기에 설명된 스크립트는 BlueXP 분류 설치 스크립트를 실행하는 것과 독립적으로 Linux 호스트를 확인하려는 사용자를 위해 특별히 설계되었습니다.

시작하기

다음 작업을 수행합니다.

1. BlueXP 커넥터가 아직 설치되지 않은 경우 설치할 수도 있습니다. Connector를 설치하지 않고 테스트 스크립트를 실행할 수 있지만 스크립트는 Connector와 BlueXP 분류 호스트 시스템 간의 연결을 검사하므로 Connector를 사용하는 것이 좋습니다.
2. 호스트 시스템을 준비하고 모든 요구 사항을 충족하는지 확인합니다.
3. BlueXP 분류 호스트 시스템에서 아웃바운드 인터넷 액세스를 활성화합니다.
4. 모든 시스템에서 필요한 포트가 활성화되어 있는지 확인합니다.
5. 사전 필수 테스트 스크립트를 다운로드하고 실행합니다.

커넥터를 작성합니다

BlueXP 분류를 설치하고 사용하려면 먼저 BlueXP 커넥터가 필요합니다. 그러나 커넥터 없이 필수 구성 요소 스크립트를 실행할 수 있습니다.

가능합니다 "Connector On-Premises를 설치합니다" 네트워크의 Linux 호스트 또는 클라우드의 Linux 호스트 BlueXP 분류를 사내에서 설치하려는 일부 사용자는 Connector를 내부에 설치할 수도 있습니다.

클라우드 공급자 환경에 Connector를 만들려면 를 참조하십시오 "AWS에서 커넥터 생성", "Azure에서 커넥터 만들기", 또는 "GCP에서 커넥터를 생성하는 중입니다".

필수 구성 요소 스크립트를 실행할 때는 커넥터 시스템의 IP 주소 또는 호스트 이름이 필요합니다. 이 정보는 구내에 Connector를 설치한 경우 확인할 수 있습니다. Connector가 클라우드에 배포된 경우 BlueXP 콘솔에서 이 정보를 찾을 수 있습니다. 도움말 아이콘을 클릭하고 * 지원 * 을 선택한 다음 * BlueXP 커넥터 * 를 클릭합니다.

호스트 요구 사항을 확인합니다

BlueXP 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행해야 합니다.

- BlueXP 분류는 다른 애플리케이션과 공유되는 호스트에서는 지원되지 않습니다. 호스트는 전용 호스트여야

합니다.

- 구내 호스트 시스템을 구축할 때 BlueXP 분류 검사를 수행할 데이터 세트의 크기에 따라 세 가지 시스템 크기 중에서 선택할 수 있습니다.

시스템 크기	**CPU**	**RAM(**스왑 메모리는 비활성화 상태여야 함**)**	디스크
* 초대형 *	32개의 CPU	128GB RAM	/, 또는 의 1TiB SSD /opt에서 -100GiB를 사용할 수 있습니다 -895GiB는 /var/lib/docker에서 사용할 수 있습니다 /tmp에 -5GiB입니다
* 대형 *	CPU 16개	64GB RAM	500GiB SSD 켜짐/또는 /opt에서 -100GiB를 사용할 수 있습니다 /var/lib/docker에서 사용 가능한 395GiB /tmp에 -5GiB입니다
* 중간 *	CPU 8개	32GB RAM	200GiB SSD 켜짐/또는 /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -145GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다
* 소형 *	CPU 8개	16GB RAM	또는 에서 100GiB SSD /opt에서 -50GiB를 사용할 수 있습니다 /var/lib/docker에서 -45GiB를 사용할 수 있습니다 /tmp에 -5GiB입니다

소형 시스템을 사용할 때는 제한이 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

- BlueXP 분류 설치를 위해 클라우드에 컴퓨팅 인스턴스를 배포할 때는 위의 "대규모" 시스템 요구 사항을 충족하는 시스템을 권장합니다.
  - * AWS EC2 인스턴스 유형 *: "m6i.4xLarge"를 권장합니다. "추가 AWS 인스턴스 유형을 참조하십시오".
  - * Azure VM size *: "Standard_D16s_v3"을 권장합니다. "추가 Azure 인스턴스 유형을 참조하십시오".
  - * GCP 시스템 유형 *: "n2-standard-16"을 권장합니다. "추가 GCP 인스턴스 유형을 참조하십시오".
- UNIX 폴더 권한 *: 다음과 같은 최소 UNIX 권한이 필요합니다.

폴더	최소 권한
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/docker입니다	`rwx------`
/usr/lib/systemd/system입니다	`rwxr-xr-x`

- * 운영 체제 *:
  - 다음 운영 체제에서는 Docker 컨테이너 엔진을 사용해야 합니다.
    - Red Hat Enterprise Linux 버전 7.8 및 7.9
    - CentOS 버전 7.8 및 7.9
    - Ubuntu 22.04(BlueXP 분류 버전 1.23 이상 필요)
  - 다음 운영 체제에는 Podman 컨테이너 엔진을 사용해야 하며 BlueXP 분류 버전 1.30 이상이 필요합니다.
    - Red Hat Enterprise Linux 버전 8.8, 9.0, 9.1, 9.2 및 9.3

      RHEL 8.x 및 RHEL 9.x를 사용하는 경우 다음 기능은 현재 지원되지 않습니다.

      - 어두운 장소에 설치
      - 분산 스캔, 마스터 스캐너 노드 및 원격 스캐너 노드 사용
- * Red Hat 서브스크립션 관리 *: 호스트는 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 설치 중에 시스템에서 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.
- * 추가 소프트웨어 *: BlueXP 분류를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.
  - 사용 중인 OS에 따라 컨테이너 엔진 중 하나를 설치해야 합니다.
    - Docker Engine 버전 19.3.1 이상 "설치 지침을 봅니다".

      "이 비디오 시청" CentOS에 Docker를 설치하는 빠른 데모를 보려면

    - Podman 버전 4 이상 Podman을 설치하려면 시스템 패키지를 업데이트하십시오 (`sudo yum update -y`)를 클릭한 다음 Podman을 설치합니다 (`sudo yum install netavark -y`)를 클릭합니다.
- Python 버전 3.6 이상. "설치 지침을 봅니다".
  - * NTP 고려 사항 *: NetApp에서는 NTP(네트워크 시간 프로토콜) 서비스를 사용하도록 BlueXP 분류 시스템을 구성할 것을 권장합니다. BlueXP 분류 시스템과 BlueXP Connector 시스템 간에 시간을 동기화해야 합니다.
  - * Firewalld 고려 사항 *: 사용하려는 경우 `firewalld`BlueXP 분류를 설치하기 전에 활성화하는 것이 좋습니다. 다음 명령을 실행하여 구성합니다 `firewalld` 따라서 BlueXP 분류와 호환됩니다.

    ```
    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 BlueXP 분류 호스트를 스캐너 노드(분산 모델)로 사용할 계획이라면 이 규칙을 주 시스템에 추가하십시오.

```
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 활성화 또는 업데이트할 때마다 다시 시작해야 합니다 `firewalld` 설정.

BlueXP 분류에서 아웃바운드 인터넷 액세스를 활성화합니다

BlueXP 분류에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 BlueXP 분류 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다.

인터넷에 연결되지 않은 사이트에 설치된 호스트 시스템에는 이 섹션이 필요하지 않습니다.

엔드포인트	목적
https://api.bluexp.netapp.com 으로 문의하십시오	NetApp 계정을 포함한 BlueXP 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	BlueXP 웹 사이트와 통신하여 중앙 집중식 사용자 인증.
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 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
https://support.compliance.api.bluexp.netapp.com/ 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://github.com/docker https://download.docker.com 으로 문의하십시오	Docker 설치를 위한 사전 필수 패키지를 제공합니다.
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm 를 참조하십시오	CentOS 설치를 위한 필수 패키지를 제공합니다.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntu 설치를 위한 필수 패키지를 제공합니다.

필요한 모든 포트가 활성화되어 있는지 확인합니다

커넥터, BlueXP 분류, Active Directory 및 데이터 소스 간의 통신에 필요한 모든 포트가 열려 있는지 확인해야 합니다.

연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 443(TCP) 및 80	Connector의 방화벽 또는 라우팅 규칙은 포트 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 포트 8080이 열려 있는지 확인하여 BlueXP에서 설치 진행률을 확인합니다.
커넥터 <>ONTAP 클러스터(NAS)	443(TCP)	BlueXP는 HTTPS를 사용하여 ONTAP 클러스터를 검색합니다. 사용자 지정 방화벽 정책을 사용하는 경우 커넥터 호스트는 포트 443을 통한 아웃바운드 HTTPS 액세스를 허용해야 합니다. Connector가 클라우드에 있는 경우 모든 아웃바운드 통신은 사전 정의된 방화벽 또는 라우팅 규칙으로 허용됩니다.

BlueXP 분류 필수 구성 요소 스크립트를 실행합니다

다음 단계에 따라 BlueXP 분류 전제 조건 스크립트를 실행합니다.

"이 비디오 시청" 필수 구성 요소 스크립트를 실행하고 결과를 해석하는 방법을 확인합니다.

필요한 것

- Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 2개의 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.

단계

1. 에서 BlueXP 분류 필수 구성 요소 스크립트를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * standalone-pre-requised-tester-<version> * 입니다.
2. 사용할 Linux 호스트에 파일을 복사합니다(사용) `scp` 또는 다른 방법 참조).
3. 스크립트를 실행할 권한을 할당합니다.

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

4. 다음 명령을 사용하여 스크립트를 실행합니다.

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

   인터넷 액세스가 없는 호스트에서 스크립트를 실행하는 경우에만 "--car사이트" 옵션을 추가합니다. 호스트가 인터넷에 연결되어 있지 않으면 특정 필수 구성 요소 테스트를 건너뜁니다.

5. 이 스크립트는 BlueXP 분류 호스트 시스템의 IP 주소를 묻는 메시지를 표시합니다.
   - IP 주소 또는 호스트 이름을 입력합니다.
6. 이 스크립트에는 BlueXP Connector가 설치되어 있는지 여부를 묻는 메시지가 표시됩니다.

- 커넥터가 설치되어 있지 않으면 * N * 을 입력하십시오.
- 커넥터가 설치된 경우 * Y * 를 입력합니다. 그런 다음 테스트 스크립트가 이 연결을 테스트할 수 있도록 BlueXP Connector의 IP 주소 또는 호스트 이름을 입력합니다.

7. 이 스크립트는 시스템에서 다양한 테스트를 실행하고 진행되면서 결과를 표시합니다. 작업이 완료되면 세션 로그를 라는 파일에 씁니다 `prerequisites-test-<timestamp>.log` 디렉토리에 있습니다 `/opt/netapp/install_logs`.

결과

모든 필수 구성 요소 테스트가 성공적으로 실행된 경우 준비가 되면 호스트에 BlueXP 분류를 설치할 수 있습니다.

발견된 문제가 있는 경우 "권장" 또는 "필수"로 분류하여 해결합니다. 권장 문제는 일반적으로 BlueXP 분류 검사 및 분류 작업의 실행 속도를 느리게 만드는 항목입니다. 이러한 항목은 수정할 필요가 없지만, 이를 해결할 수 있습니다.

"필수" 문제가 있는 경우 문제를 해결하고 사전 요구 사항 테스트 스크립트를 다시 실행해야 합니다.

데이터 소스에서 스캔을 활성화합니다

Cloud Volumes ONTAP 및 온-프레미스 **ONTAP**에 대한 **BlueXP** 분류를 시작합니다

BlueXP 분류를 사용하여 Cloud Volumes ONTAP 및 온-프레미스 ONTAP 볼륨을 스캔하려면 몇 단계를 완료하십시오.

빠른 시작

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

1 스캔할 데이터 원본을 검색합니다

볼륨을 스캔하려면 먼저 시스템을 BlueXP의 작업 환경으로 추가해야 합니다.

- Cloud Volumes ONTAP 시스템의 경우 BlueXP에서 이러한 작업 환경을 사용할 수 있어야 합니다
- 사내 ONTAP 시스템의 경우, "BlueXP는 ONTAP 클러스터를 검색해야 합니다"

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 **BlueXP** 분류를 활성화하고 스캔할 볼륨을 선택합니다

Configuration * 탭을 선택하고 특정 작업 환경의 볼륨에 대한 규정 준수 검사를 활성화합니다.

4 볼륨에 대한 액세스를 확인합니다

이제 BlueXP 분류를 사용하도록 설정했으므로 모든 볼륨에 액세스할 수 있는지 확인합니다.

- BlueXP 분류 인스턴스에는 각 Cloud Volumes ONTAP 서브넷 또는 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다.
- Cloud Volumes ONTAP의 보안 그룹은 BlueXP 분류 인스턴스에서 인바운드 연결을 허용해야 합니다.
- 이러한 포트가 BlueXP 분류 인스턴스에 열려 있는지 확인합니다.
  - NFS 포트 111 및 2049의 경우
  - CIFS-포트 139 및 445의 경우
- NFS 볼륨 내보내기 정책은 BlueXP 분류 인스턴스에서 액세스를 허용해야 합니다.
- BlueXP 분류에는 CIFS 볼륨을 스캔하기 위해 Active Directory 자격 증명이 필요합니다.

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

5 스캔할 볼륨을 관리합니다

스캔할 볼륨을 선택하거나 선택 취소하면 BlueXP 분류가 시작 또는 스캔을 중지합니다.

스캔할 데이터 소스 검색

검사할 데이터 소스가 BlueXP 환경에 아직 없는 경우 현재 캔버스에 추가할 수 있습니다.

Cloud Volumes ONTAP 시스템은 BlueXP의 Canvas에서 이미 사용 가능해야 합니다. 사내 ONTAP 시스템의 경우 가 있어야 합니다 "BlueXP는 이러한 클러스터를 검색합니다".

BlueXP 분류 인스턴스 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

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

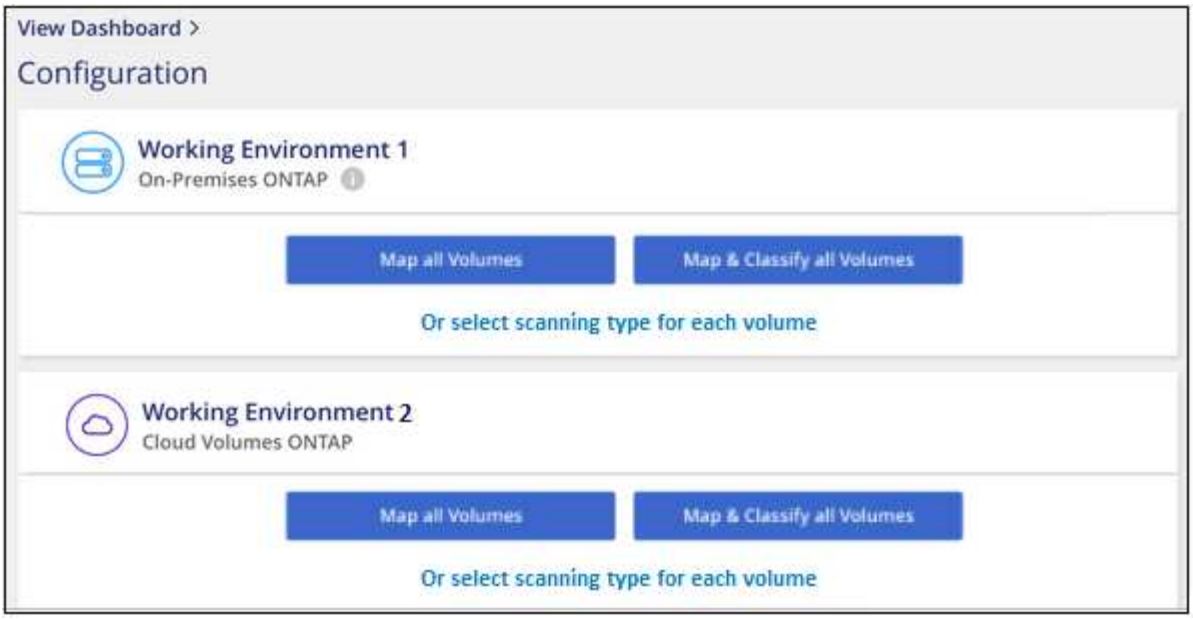
인터넷에 액세스할 수 없는 어두운 사이트에 설치된 온-프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 BlueXP 분류를 배포합니다". 또한 BlueXP Connector를 동일한 사내 위치에 배포해야 합니다.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

작업 환경에서 **BlueXP** 분류 활성화

지원되는 모든 클라우드 공급자 및 온프레미스 ONTAP 클러스터의 Cloud Volumes ONTAP 시스템에서 BlueXP 분류를 사용하도록 설정할 수 있습니다.

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.



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

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

3. 확인 대화 상자에서 * 승인 * 을 클릭하여 BlueXP 분류가 볼륨 스캔을 시작하도록 합니다.

결과

BlueXP 분류는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. BlueXP 분류가 초기 스캔을 마치면 준수 대시보드에서 결과를 확인할 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

- 기본적으로 BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 볼륨의 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우 * 를 클릭하거나 각 볼륨에 대한 스캐닝 유형을 선택하십시오 *. 결과 페이지에는 BlueXP 분류가 권한에 관계없이 볼륨을 스캔하도록 설정할 수 있는 설정이 있습니다.
- BlueXP 분류는 한 볼륨에서 하나의 파일 공유만 검사합니다. 볼륨에 여러 공유가 있는 경우 해당 다른 공유를 공유 그룹으로 별도로 스캔해야 합니다. "이 BlueXP 분류 제한에 대한 자세한 내용은 을 참조하십시오".

BlueXP 분류에서 볼륨에 액세스할 수 있는지 확인합니다

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

단계

1. BlueXP 분류 인스턴스와 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터의 볼륨을 포함하는 각

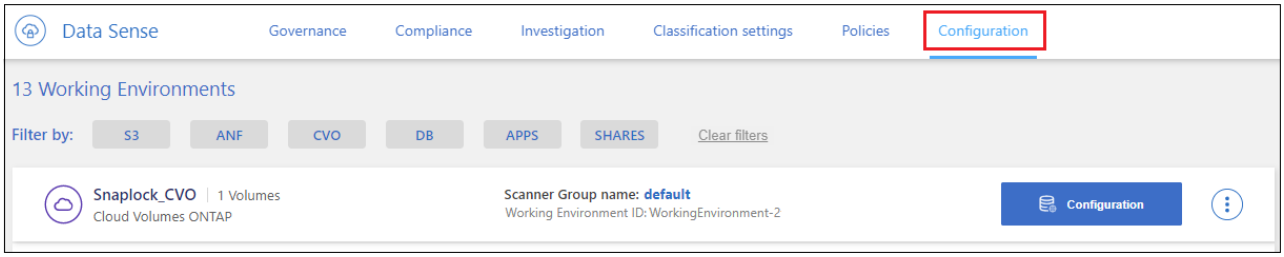
네트워크 사이에 네트워크 연결이 있는지 확인합니다.

2. Cloud Volumes ONTAP용 보안 그룹이 BlueXP 분류 인스턴스에서 들어오는 트래픽을 허용하는지 확인합니다.

   BlueXP 분류 인스턴스의 IP 주소에서 오는 트래픽에 대해 보안 그룹을 열거나 가상 네트워크 내부에서 발생하는 모든 트래픽에 대해 보안 그룹을 열 수 있습니다.

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

   a. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.

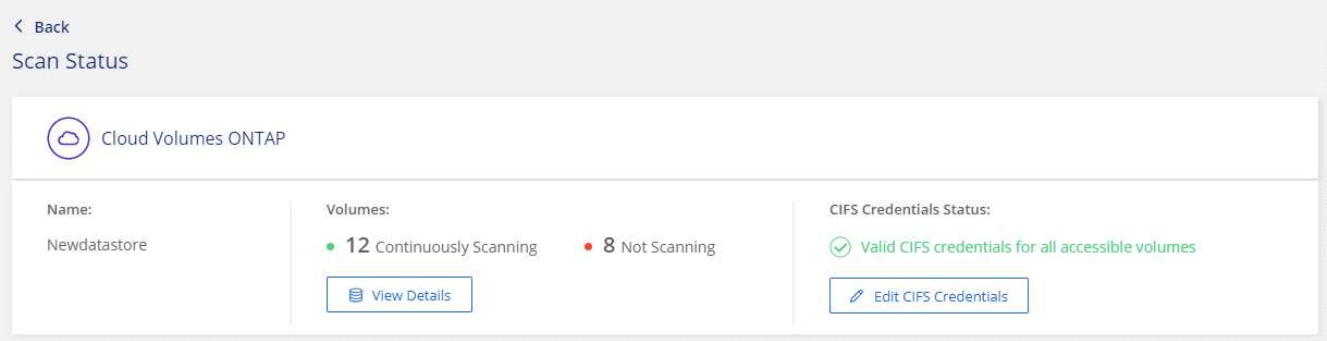


   b. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 BlueXP 분류에서 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

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

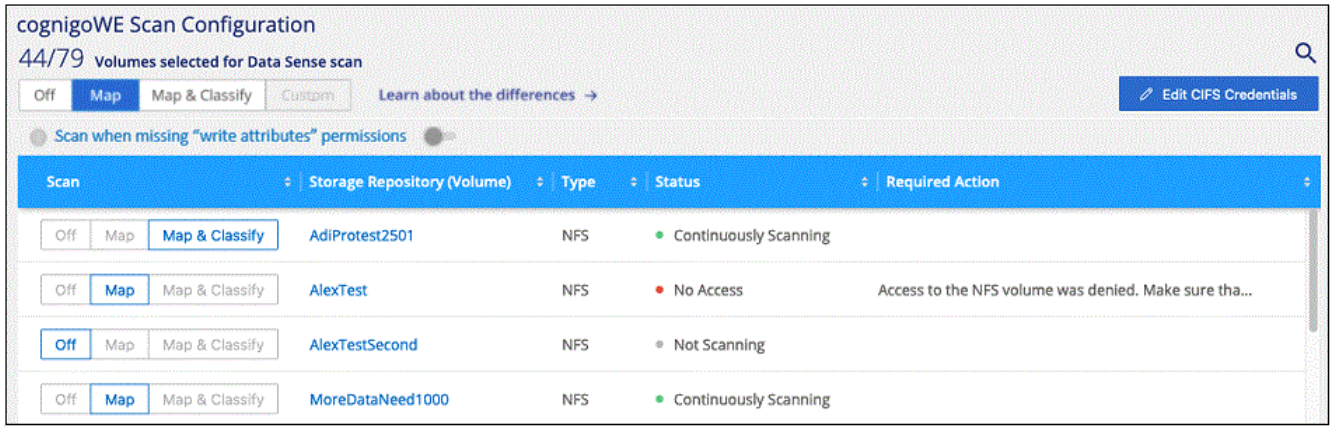
      BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 CIFS에서 쓰기 속성 사용 권한 또는 NFS에서 쓰기 권한이 사용자에게 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

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



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

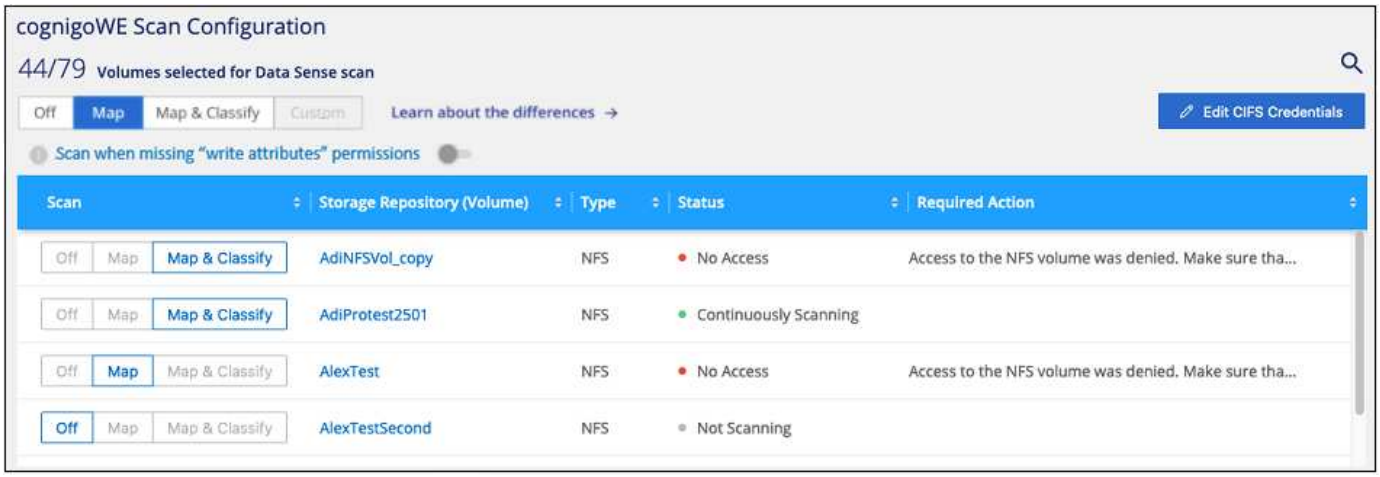
예를 들어 다음 이미지는 네 개의 볼륨을 보여 줍니다. 그 중 하나는 BlueXP 분류 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 BlueXP 분류에서 스캔할 수 없는 볼륨입니다.



볼륨에서 규정 준수 검사 활성화 및 비활성화

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

페이지 상단의 * "쓰기 속성" 권한 * 이 누락된 경우 * 스캔 에 대한 스위치는 기본적으로 비활성화되어 있습니다. 즉, BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우, 스위치를 켜면 사용 권한에 관계없이 모든 파일이 스캔됩니다. "자세한 정보".



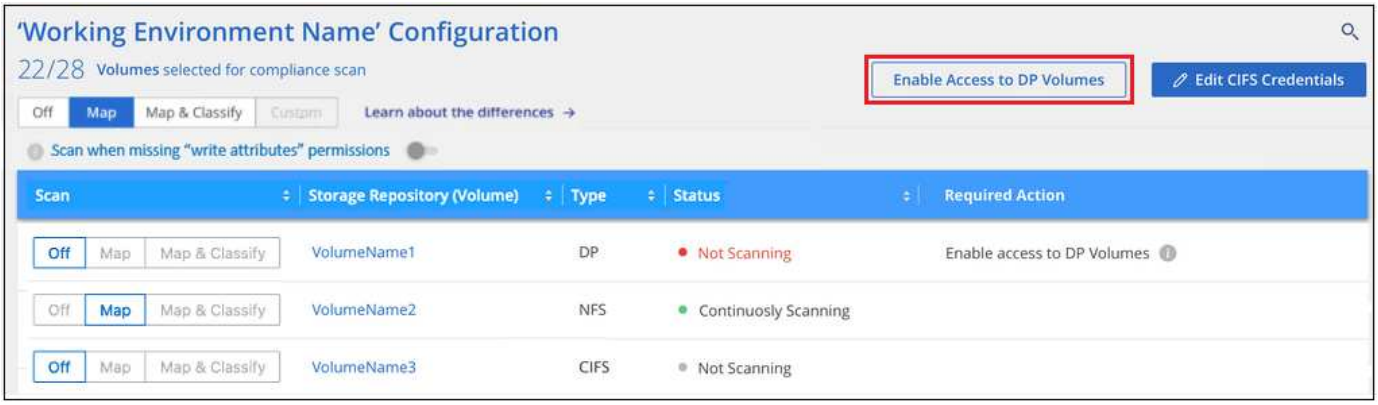
대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다
볼륨에서 스캔을 비활성화합니다	볼륨 영역에서 * Off * 를 클릭합니다
모든 볼륨에서 매핑 전용 스캔을 활성화합니다	제목 영역에서 * Map * 을 클릭합니다
모든 볼륨에서 전체 스캔을 활성화합니다	제목 영역에서 * 지도 및 분류 * 를 클릭합니다
모든 볼륨에서 스캔을 비활성화합니다	제목 영역에서 * Off * 를 클릭합니다

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

데이터 보호 볼륨을 검색하는 중입니다

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

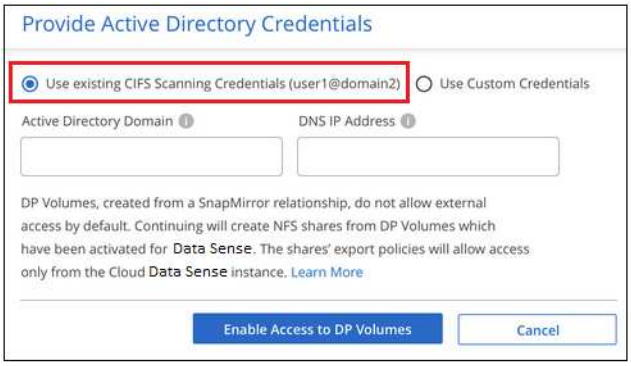
처음에 볼륨 목록은 이러한 볼륨을 *Type** DP*로 식별하며 *Status** Not Scanning* 및 *Required Action** DP 볼륨에 대한 액세스 사용*.

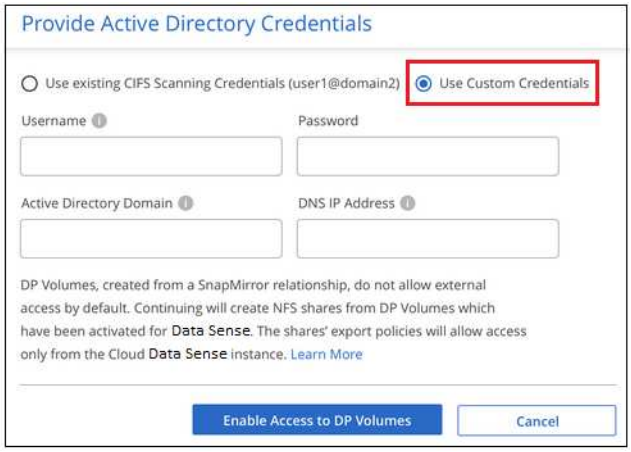


단계

이러한 데이터 보호 볼륨을 스캔하려는 경우:

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





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

결과

활성화되면 BlueXP 분류는 스캔을 위해 활성화된 각 DP 볼륨에서 NFS 공유를 생성합니다. 공유 내보내기 정책은 BlueXP 분류 인스턴스에서만 액세스를 허용합니다.

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

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

Azure NetApp Files에 대한 BlueXP 분류 시작

Azure NetApp Files용 BlueXP 분류를 시작하려면 몇 가지 단계를 완료하십시오.

빠른 시작

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

1 검사할 **Azure NetApp Files** 시스템을 검색합니다

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

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP에서 BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 **BlueXP** 분류를 활성화하고 스캔할 볼륨을 선택합니다

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

4 볼륨에 대한 액세스를 확인합니다

이제 BlueXP 분류를 사용하도록 설정했으므로 모든 볼륨에 액세스할 수 있는지 확인합니다.

- BlueXP 분류 인스턴스에는 각 Azure NetApp Files 서브넷에 대한 네트워크 연결이 필요합니다.
- 이러한 포트가 BlueXP 분류 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 내보내기 정책은 BlueXP 분류 인스턴스에서 액세스를 허용해야 합니다.
- BlueXP 분류에는 CIFS 볼륨을 스캔하기 위해 Active Directory 자격 증명이 필요합니다.

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

5 스캔할 볼륨을 관리합니다

스캔할 볼륨을 선택하거나 선택 취소하면 BlueXP 분류가 시작 또는 스캔을 중지합니다.

스캔할 **Azure NetApp Files** 시스템 검색

검사할 Azure NetApp Files 시스템이 BlueXP에 작업 환경으로 포함되어 있지 않은 경우 이 때 캔버스에 추가할 수 있습니다.

"BlueXP에서 Azure NetApp Files 시스템을 검색하는 방법을 확인하십시오".

BlueXP 분류 인스턴스 배포

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

BlueXP 분류는 Azure NetApp Files 볼륨을 스캔할 때 클라우드에 배포해야 하며 스캔할 볼륨과 동일한 영역에 배포되어야 합니다.

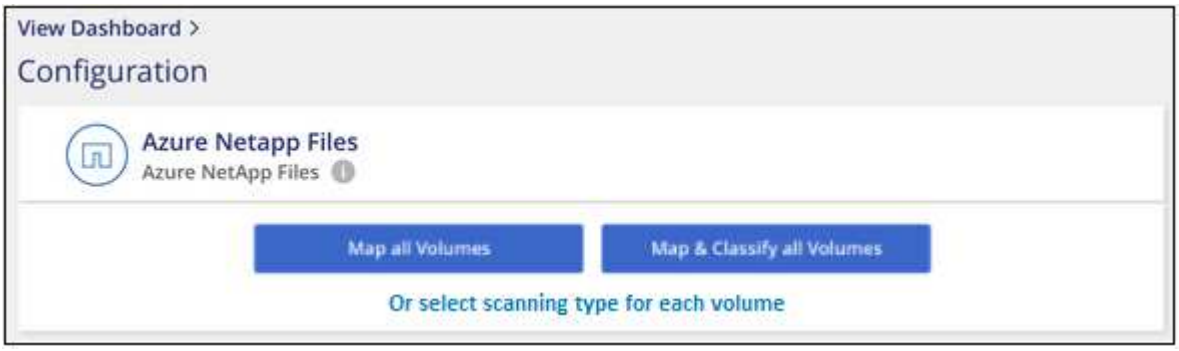
- 참고: * Azure NetApp Files 볼륨을 스캔할 때는 현재 사내 위치에 BlueXP 분류 배포를 지원하지 않습니다.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

작업 환경에서 **BlueXP** 분류 활성화

Azure NetApp Files 볼륨에서 BlueXP 분류를 활성화할 수 있습니다.

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.



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

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

3. 확인 대화 상자에서 * 승인 * 을 클릭하여 BlueXP 분류가 볼륨 스캔을 시작하도록 합니다.

결과

BlueXP 분류는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. BlueXP 분류가 초기 스캔을 마치면 준수 대시보드에서 결과를 확인할 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

- 기본적으로 BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 볼륨의 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우 * 를 클릭하거나 각 볼륨에 대한 스캐닝 유형을 선택하십시오 *. 결과 페이지에는 BlueXP 분류가 권한에 관계없이 볼륨을 스캔하도록 설정할 수 있는 설정이 있습니다.
- BlueXP 분류는 한 볼륨에서 하나의 파일 공유만 검사합니다. 볼륨에 여러 공유가 있는 경우 해당 다른 공유를 공유 그룹으로 별도로 스캔해야 합니다. "이 BlueXP 분류 제한에 대한 자세한 내용은을 참조하십시오".

BlueXP 분류에서 볼륨에 액세스할 수 있는지 확인합니다

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

단계

1. BlueXP 분류 인스턴스와 Azure NetApp Files 볼륨을 포함하는 각 네트워크 사이에 네트워크 연결이 있는지 확인합니다.

   Azure NetApp Files의 경우 BlueXP 분류는 BlueXP와 동일한 영역에 있는 볼륨만 스캔할 수 있습니다.

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

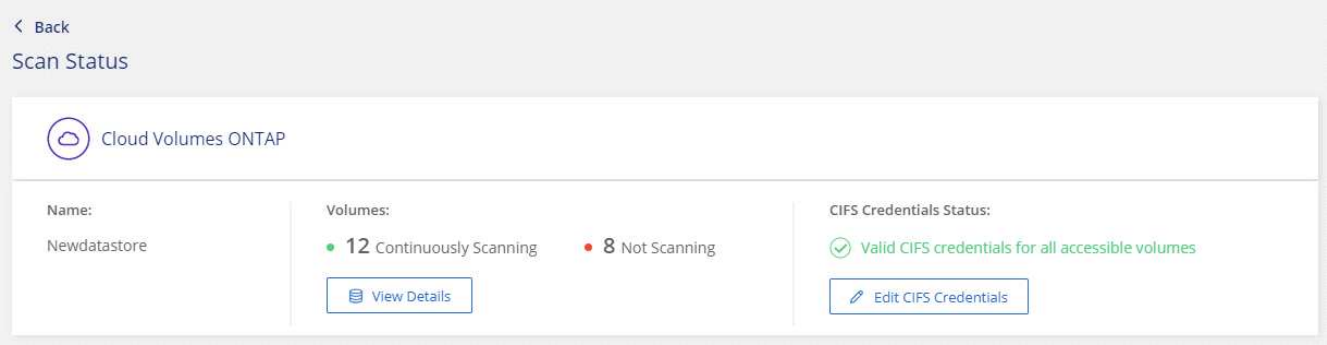
   a. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.

   b. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 BlueXP 분류에서 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

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

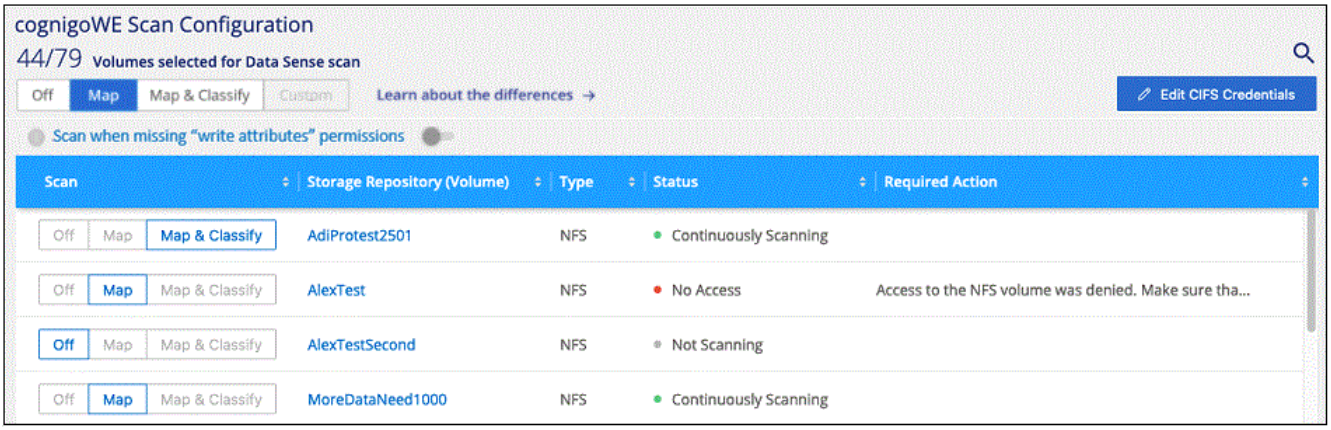
BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 CIFS에서 쓰기 속성 사용 권한 또는 NFS에서 쓰기 권한이 사용자에게 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

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



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

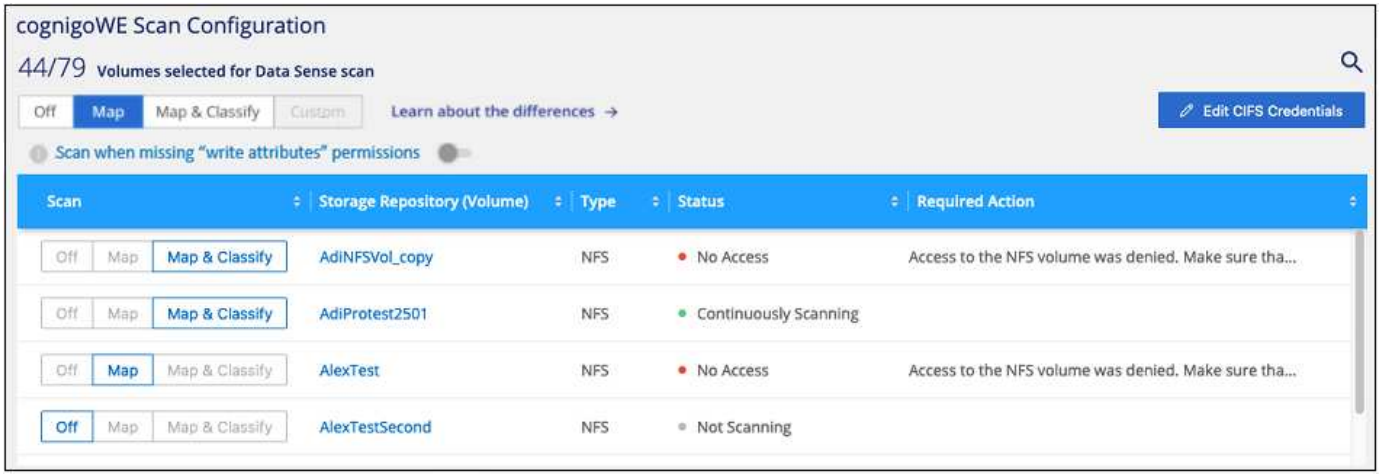
   예를 들어 다음 이미지는 네 개의 볼륨을 보여 줍니다. 그 중 하나는 BlueXP 분류 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 BlueXP 분류에서 스캔할 수 없는 볼륨입니다.



볼륨에서 규정 준수 검사 활성화 및 비활성화

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

페이지 상단의 * "쓰기 속성" 권한 * 이 누락된 경우 * 스캔 에 대한 스위치는 기본적으로 비활성화되어 있습니다. 즉, BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우, 스위치를 켜면 사용 권한에 관계없이 모든 파일이 스캔됩니다. "자세한 정보".



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

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

ONTAP용 Amazon FSx에 대한 BlueXP 분류를 시작하십시오

BlueXP 분류를 사용하여 ONTAP 볼륨에 대한 Amazon FSx 스캔을 시작하려면 몇 단계를 완료하십시오.

시작하기 전에

- BlueXP 분류를 구축 및 관리하려면 AWS에 활성 커넥터가 필요합니다.
- 작업 환경을 생성할 때 선택한 보안 그룹은 BlueXP 분류 인스턴스의 트래픽을 허용해야 합니다. ONTAP용 FSx 파일 시스템에 연결된 ENI를 사용하여 관련 보안 그룹을 찾은 다음 AWS 관리 콘솔을 사용하여 편집할 수 있습니다.

  "Linux 인스턴스용 AWS 보안 그룹"

  "Windows 인스턴스용 AWS 보안 그룹"

  "AWS의 탄력적인 네트워크 인터페이스(ENI)"

빠른 시작

다음 단계를 따라 빠르게 시작하거나 아래로 스크롤하여 자세한 내용을 확인하십시오.

1 검사할 **ONTAP** 파일 시스템용 **FSx**를 검색합니다

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

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP에서 BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 **BlueXP** 분류를 활성화하고 스캔할 볼륨을 선택합니다

Configuration * 탭을 선택하고 특정 작업 환경의 볼륨에 대한 규정 준수 검사를 활성화합니다.

4 볼륨에 대한 액세스를 확인합니다

이제 BlueXP 분류를 사용하도록 설정했으므로 모든 볼륨에 액세스할 수 있는지 확인합니다.

- BlueXP 분류 인스턴스에는 ONTAP 서브넷을 위해 각 FSx에 대한 네트워크 연결이 필요합니다.
- BlueXP 분류 인스턴스에 대해 다음 포트가 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 내보내기 정책은 BlueXP 분류 인스턴스에서 액세스를 허용해야 합니다.
- BlueXP 분류에는 CIFS 볼륨을 스캔하기 위해 Active Directory 자격 증명이 필요합니다. + * Compliance * > * Configuration * > * Edit CIFS Credentials * 를 클릭하고 자격 증명을 입력합니다.

5 스캔할 볼륨을 관리합니다

스캔할 볼륨을 선택하거나 선택 취소하면 BlueXP 분류가 스캔을 시작하거나 중지합니다.

검사할 **ONTAP** 파일 시스템용 **FSx** 검색

검사할 ONTAP 파일 시스템용 FSx가 BlueXP에 작업 환경으로 설정되어 있지 않은 경우 이 파일을 캔버스에 추가할 수 있습니다.

"BlueXP에서 ONTAP 파일 시스템용 FSx를 검색 또는 생성하는 방법을 확인하십시오".

BlueXP 분류 인스턴스 배포

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

BlueXP 분류를 AWS용 커넥터 및 스캔할 FSx 볼륨과 동일한 AWS 네트워크에 배포해야 합니다.

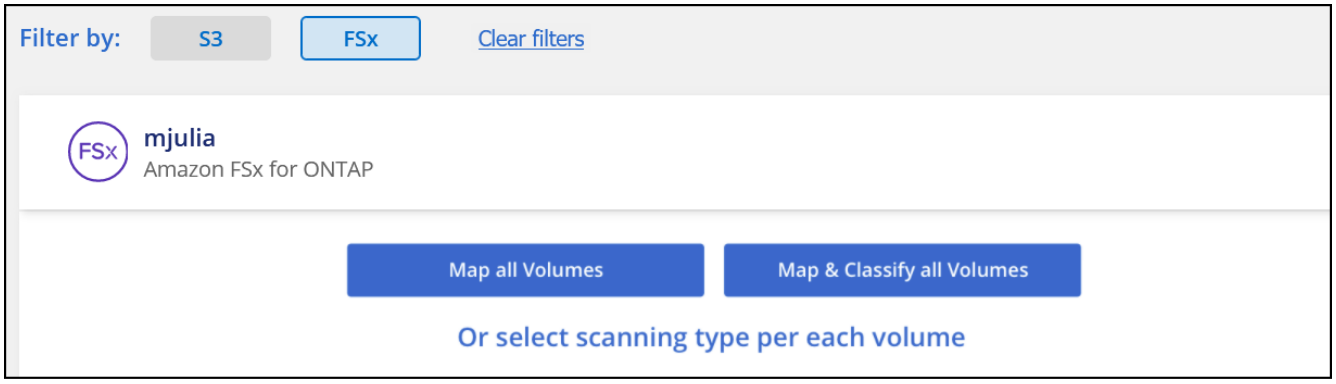
- 참고: * FSx 볼륨을 스캔할 때는 현재 온-프레미스 위치에서 BlueXP 분류 배포를 지원하지 않습니다.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

작업 환경에서 **BlueXP** 분류 활성화

ONTAP 볼륨에 대해 FSx에 대해 BlueXP 분류를 활성화할 수 있습니다.

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.



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

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

3. 확인 대화 상자에서 * 승인 * 을 클릭하여 BlueXP 분류가 볼륨 스캔을 시작하도록 합니다.

결과

BlueXP 분류는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. BlueXP 분류가 초기 스캔을 마치면 준수 대시보드에서 결과를 확인할 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

- 기본적으로 BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 볼륨의 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우 * 를 클릭하거나 각 볼륨에 대한 스캐닝 유형을 선택하십시오 *. 결과 페이지에는 BlueXP 분류가 권한에 관계없이 볼륨을 스캔하도록 설정할 수 있는 설정이 있습니다.
- BlueXP 분류는 한 볼륨에서 하나의 파일 공유만 검사합니다. 볼륨에 여러 공유가 있는 경우 해당 다른 공유를 공유 그룹으로 별도로 스캔해야 합니다. "이 BlueXP 분류 제한에 대한 자세한 내용은 을 참조하십시오".

BlueXP 분류에서 볼륨에 액세스할 수 있는지 확인합니다

네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 BlueXP 분류가 볼륨에 액세스할 수 있는지 확인합니다.

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

단계

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

   예를 들어, 다음 이미지는 BlueXP 분류 인스턴스와 볼륨 사이의 네트워크 연결 문제로 인해 BlueXP 분류에서 스캔할 수 없는 볼륨을 보여 줍니다.

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

2. BlueXP 분류 인스턴스와 ONTAP용 FSx 볼륨을 포함하는 각 네트워크 사이에 네트워크 연결이 있는지 확인합니다.

   ONTAP용 FSx의 경우 BlueXP 분류는 BlueXP와 동일한 영역에서만 볼륨을 스캔할 수 있습니다.

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

   a. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 구성 * 탭을 선택합니다.

   b. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 BlueXP 분류에서 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

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

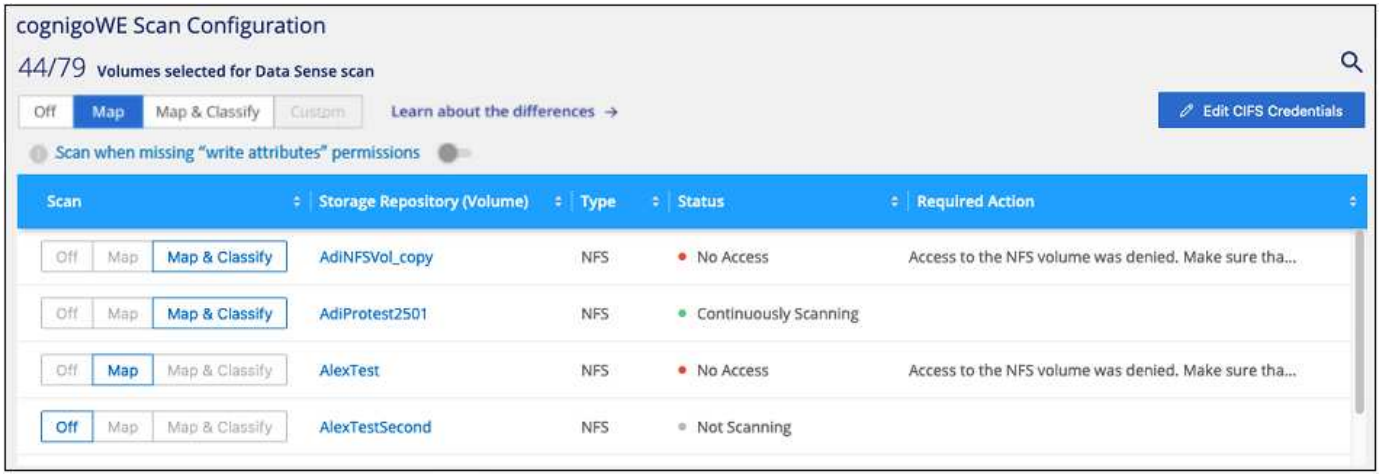
      BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 CIFS에서 쓰기 속성 사용 권한 또는 NFS에서 쓰기 권한이 사용자에게 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

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

볼륨에서 규정 준수 검사 활성화 및 비활성화

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

페이지 상단의 * "쓰기 속성" 권한 * 이 누락된 경우 * 스캔 에 대한 스위치는 기본적으로 비활성화되어 있습니다. 즉, BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우, 스위치를 켜면 사용 권한에 관계없이 모든 파일이 스캔됩니다. "자세한 정보".



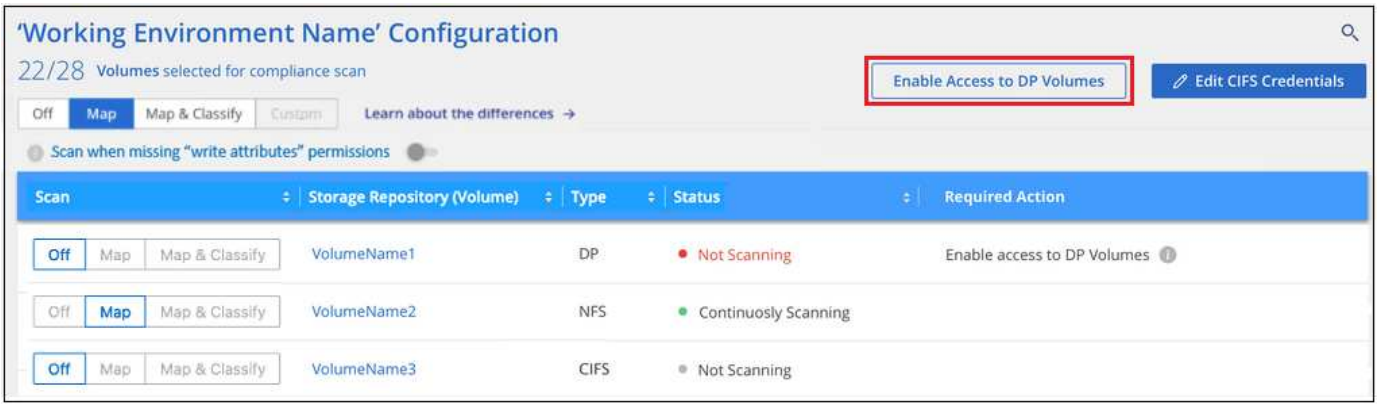
대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다
볼륨에서 스캔을 비활성화합니다	볼륨 영역에서 * Off * 를 클릭합니다
모든 볼륨에서 매핑 전용 스캔을 활성화합니다	제목 영역에서 * Map * 을 클릭합니다
모든 볼륨에서 전체 스캔을 활성화합니다	제목 영역에서 * 지도 및 분류 * 를 클릭합니다
모든 볼륨에서 스캔을 비활성화합니다	제목 영역에서 * Off * 를 클릭합니다

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

데이터 보호 볼륨을 검색하는 중입니다

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

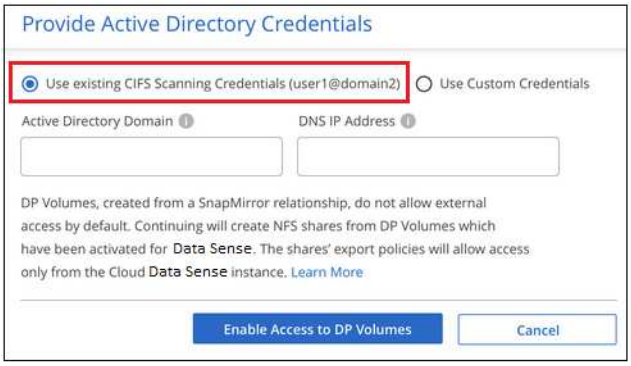
처음에 볼륨 목록은 이러한 볼륨을 *Type** DP*로 식별하며 *Status** Not Scanning* 및 *Required Action** DP 볼륨에 대한 액세스 사용*.

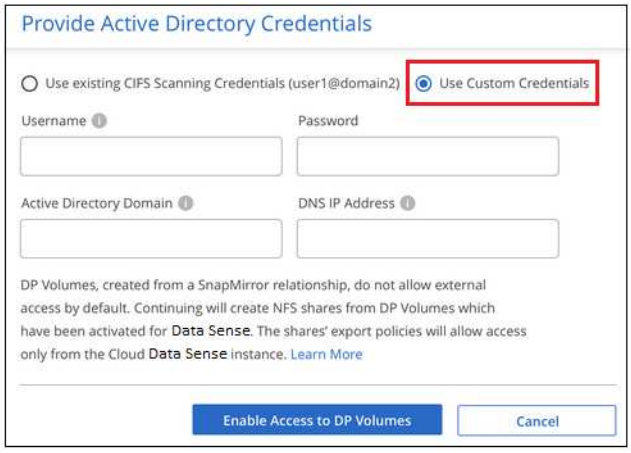


단계

이러한 데이터 보호 볼륨을 스캔하려는 경우:

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





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

결과

활성화되면 BlueXP 분류는 스캔을 위해 활성화된 각 DP 볼륨에서 NFS 공유를 생성합니다. 공유 내보내기 정책은 BlueXP 분류 인스턴스에서만 액세스를 허용합니다.

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

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

Amazon S3에 대한 BlueXP 분류 시작

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

빠른 시작

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

1. 클라우드 환경에서 **S3** 요구사항을 설정합니다

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

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 **S3** 작업 환경에서 **BlueXP** 분류를 활성화합니다

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

4 스캔할 버킷을 선택합니다

스캔하려는 버킷을 선택하면 BlueXP 분류가 스캔을 시작합니다.

S3 사전 요구 사항 검토

다음 요구사항은 S3 버킷 스캔에만 적용됩니다.

BlueXP 분류 인스턴스에 대해 **IAM** 역할을 설정합니다

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

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

BlueXP 분류에서 **Amazon S3**로 연결을 제공합니다

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

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

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

또는 NAT 게이트웨이를 사용하여 연결을 제공하는 방법도 있습니다.

> 프록시를 사용하여 인터넷을 통해 S3로 연결할 수는 없습니다.

BlueXP 분류 인스턴스 배포

"BlueXP에서 BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

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

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

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

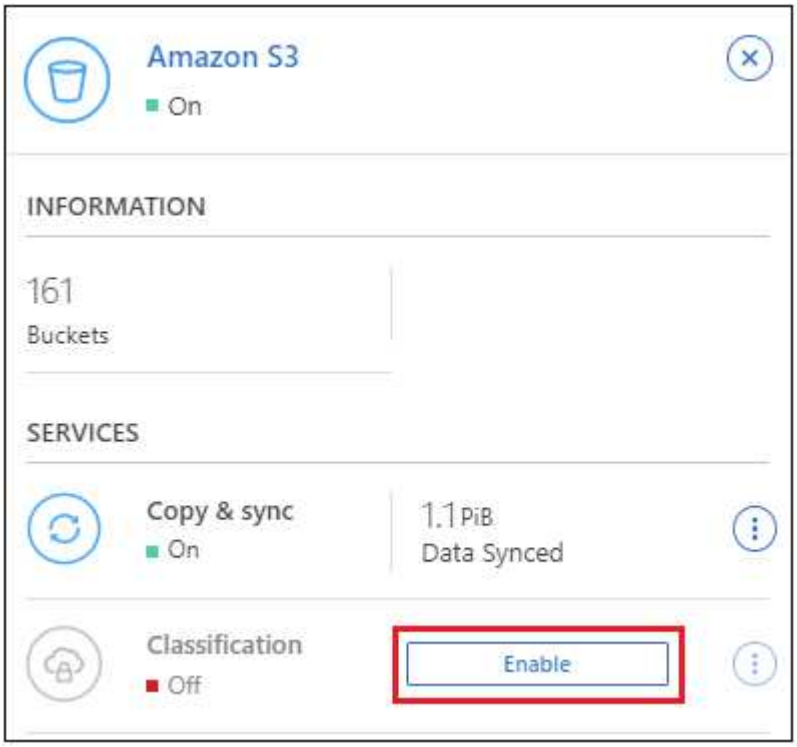
S3 작업 환경에서 **BlueXP** 분류 활성화

사전 요구 사항을 확인한 후 Amazon S3에서 BlueXP 분류를 활성화합니다.

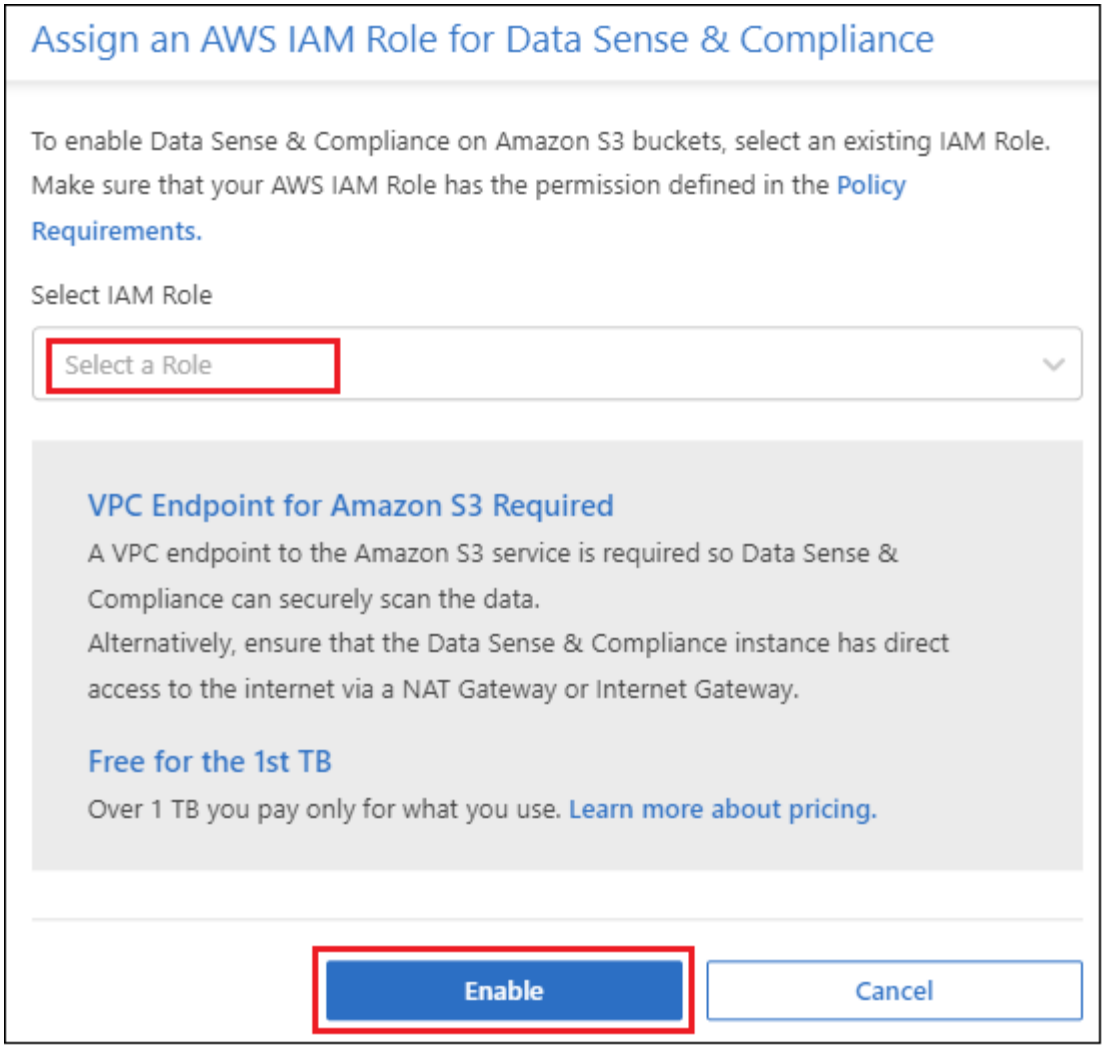
단계

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

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



4. 메시지가 표시되면 의 BlueXP 분류 인스턴스에 IAM 역할을 할당합니다 필요한 권한.



5. 사용 * 을 클릭합니다.

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

결과

BlueXP는 인스턴스에 IAM 역할을 할당합니다.

S3 버킷에서 규정 준수 스캔 활성화 및 비활성화

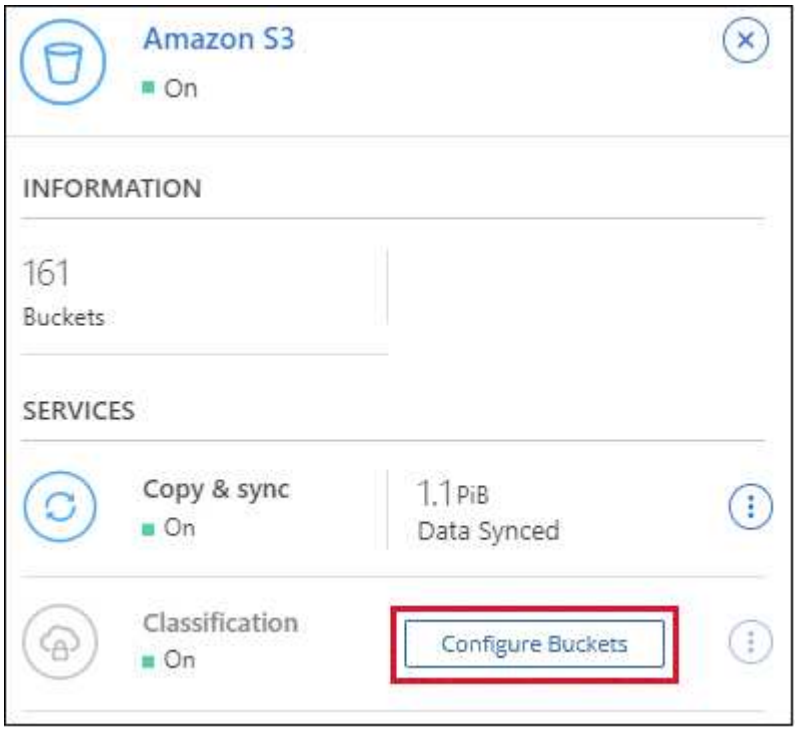
BlueXP에서 Amazon S3에서 BlueXP 분류를 사용하도록 설정한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다.

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

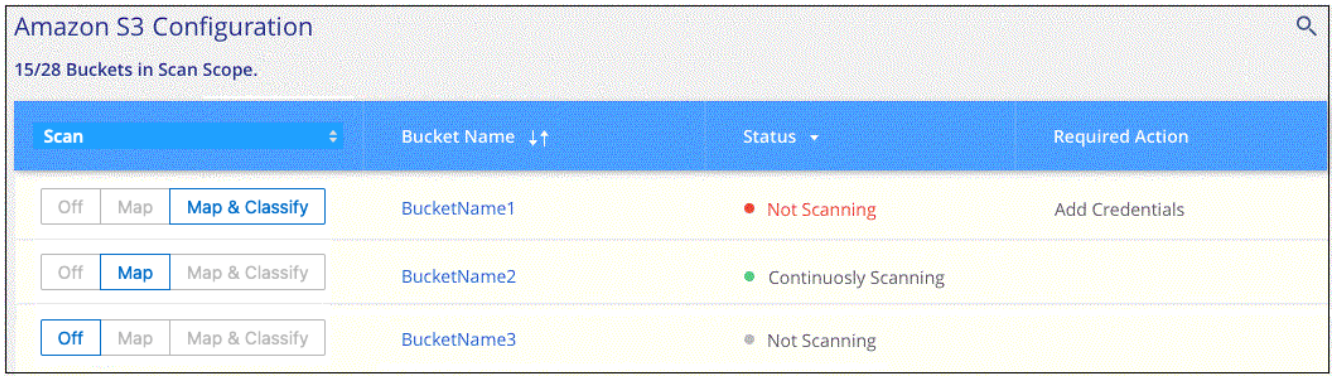
BlueXP 분류도 가능합니다 서로 다른 AWS 계정에 있는 S3 버킷을 스캔합니다.

단계

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



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



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

결과

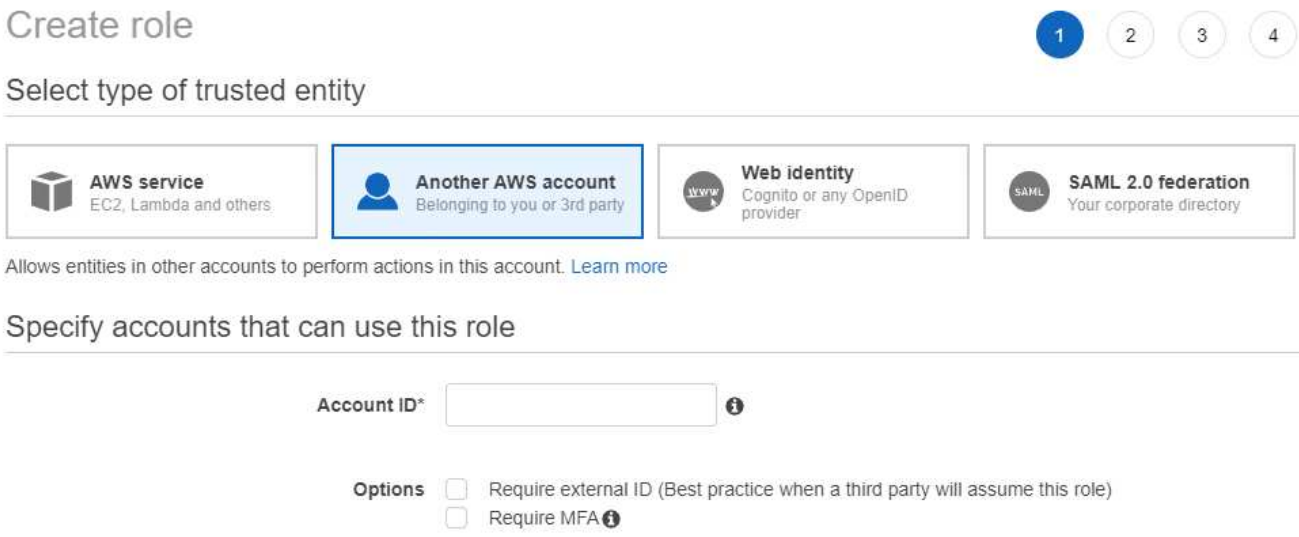
BlueXP 분류는 활성화한 S3 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

추가 **AWS** 계정에서 버킷 스캔

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

단계

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



다음을 수행하십시오.

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

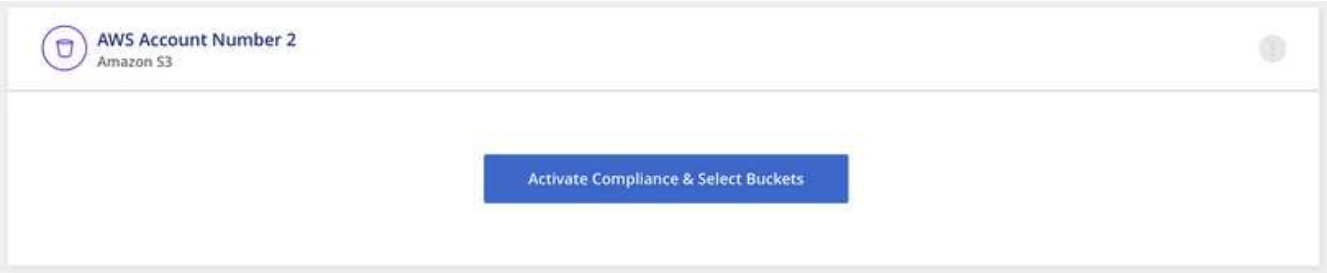
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

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

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

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

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



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

결과

BlueXP 분류는 사용자가 활성화한 새 S3 버킷을 스캔하기 시작합니다.

데이터베이스 스키마를 스캔합니다

BlueXP 분류를 사용하여 데이터베이스 스키마 스캔을 시작하려면 몇 단계를 완료하십시오.

데이터베이스 검사를 사용하도록 설정한 후에는 BlueXP 분류가 데이터베이스의 특정 열을 기반으로 모든 데이터 원본에서 식별하는 고유 식별자를 추가할 수 있습니다. 이를 _Data Fusion_피처라고 합니다. "데이터베이스에서 사용자 지정 개인 데이터 식별자를 추가하는 방법에 대해 알아봅니다".

빠른 시작

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

1. 데이터베이스 사전 요구 사항을 검토합니다

데이터베이스가 지원되고 데이터베이스에 연결하는 데 필요한 정보가 있는지 확인합니다.

2. **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3. 데이터베이스 서버를 추가합니다

액세스할 데이터베이스 서버를 추가합니다.

4. 스키마를 선택합니다

스캔할 스키마를 선택합니다.

사전 요구 사항을 검토합니다

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

지원되는 데이터베이스

BlueXP 분류는 다음 데이터베이스에서 스키마를 검사할 수 있습니다.

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

> ! 데이터베이스에서 통계 수집 기능 * 을 활성화해야 합니다.

데이터베이스 요구 사항

BlueXP 분류 인스턴스에 연결된 모든 데이터베이스는 호스팅 위치에 관계없이 검색할 수 있습니다. 데이터베이스에 연결하려면 다음 정보만 필요합니다.

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

  사용자 이름과 암호를 선택할 때는 검사할 모든 스키마와 테이블에 대한 읽기 권한이 있는 스키마를 선택해야 합니다. 필요한 모든 권한을 사용하여 BlueXP 분류 시스템에 대한 전용 사용자를 생성하는 것이 좋습니다.

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

BlueXP 분류 인스턴스를 배포합니다

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

인터넷을 통해 액세스할 수 있는 데이터베이스 스키마를 스캔하는 경우 를 사용할 수 있습니다 "클라우드에 BlueXP 분류를 배포합니다" 또는 "인터넷 액세스가 가능한 사내 위치에 BlueXP 분류를 배포합니다".

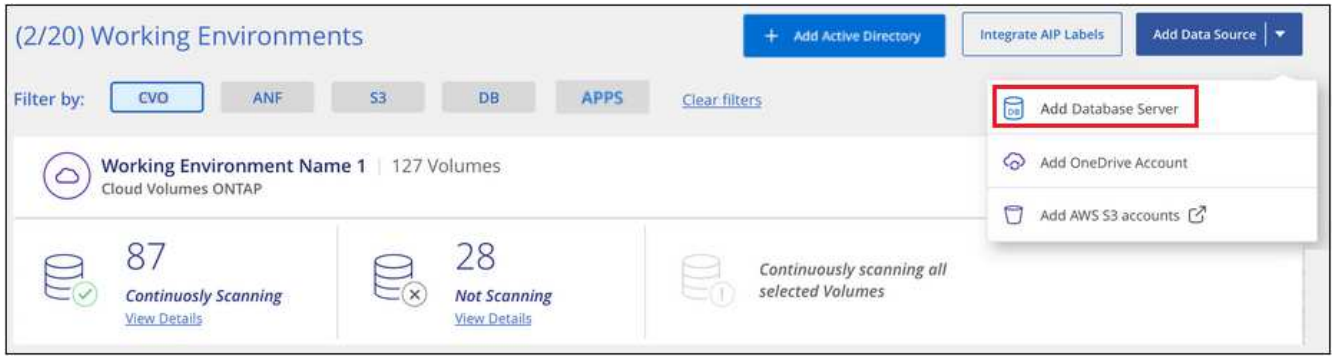
인터넷에 액세스할 수 없는 어두운 사이트에 설치된 데이터베이스 스키마를 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 BlueXP 분류를 배포합니다". 또한 BlueXP Connector를 동일한 사내 위치에 배포해야 합니다.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

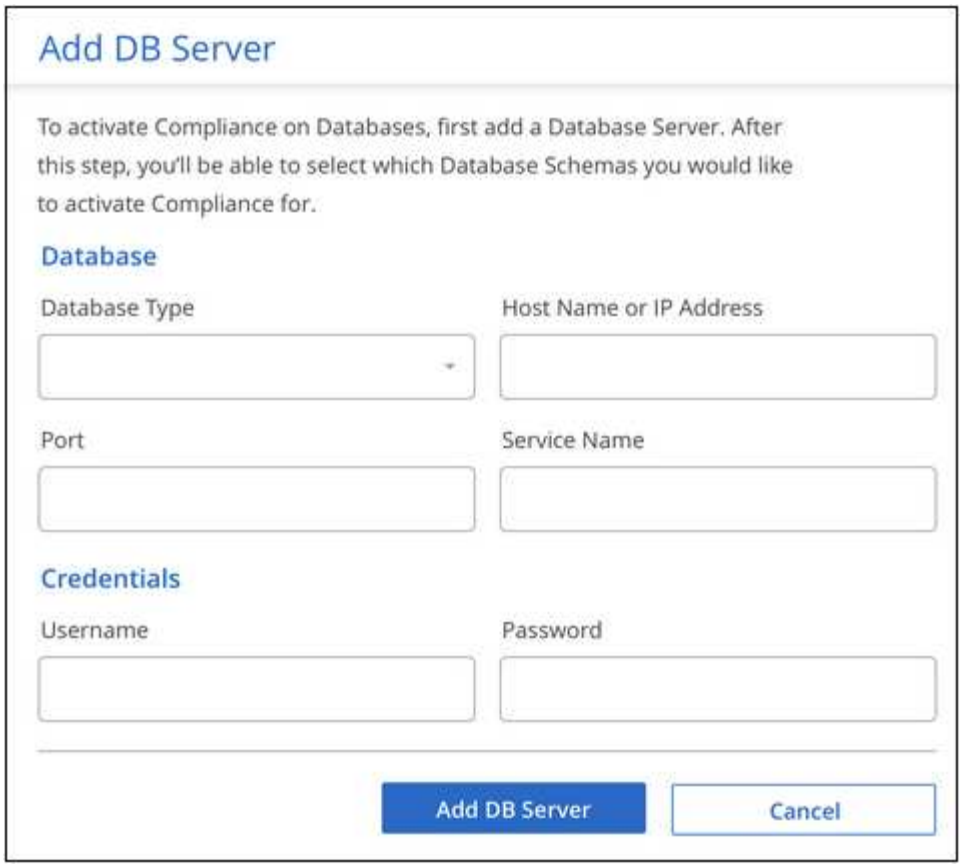
데이터베이스 서버를 추가합니다

스키마가 있는 데이터베이스 서버를 추가합니다.

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



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



데이터베이스가 작업 환경 목록에 추가됩니다.

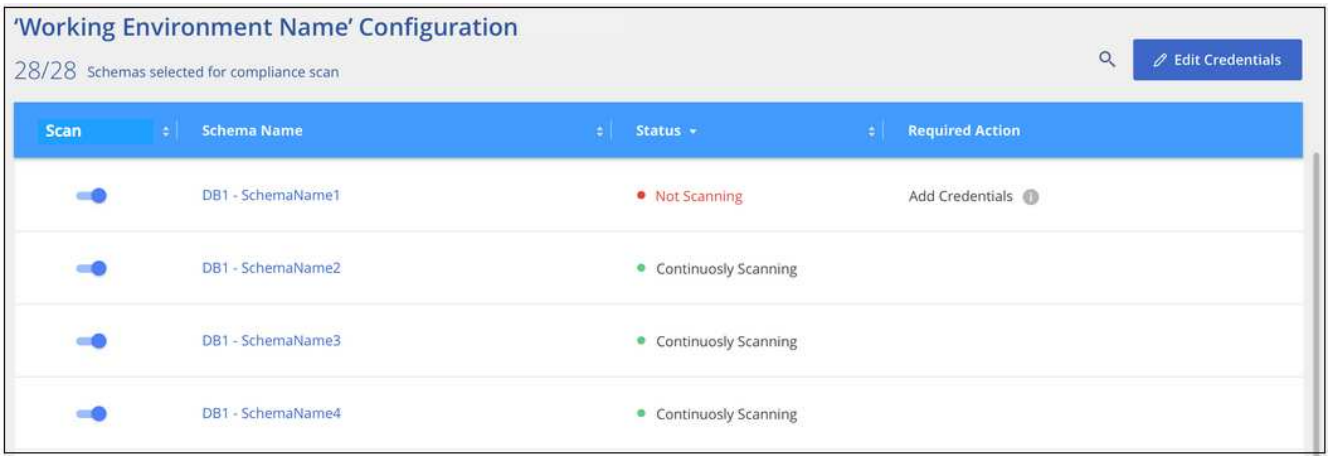
데이터베이스 스키마에서 규정 준수 검사를 활성화 및 비활성화합니다

언제든지 스키마를 중지하거나 전체 스캔을 시작할 수 있습니다.

데이터베이스 스키마에 대한 매핑 전용 검사를 선택하는 옵션은 없습니다.

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

2. 슬라이더를 오른쪽으로 이동하여 스캔할 스키마를 선택합니다.



결과

BlueXP 분류는 사용자가 활성화한 데이터베이스 스키마를 검사하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

BlueXP 분류는 하루에 한 번 데이터베이스를 검사하므로 다른 데이터 소스와 마찬가지로 데이터베이스를 지속적으로 스캔하지 않습니다.

OneDrive 계정 스캔 중

BlueXP 분류를 사용하여 사용자의 OneDrive 폴더에 있는 파일을 스캔하려면 몇 단계를 완료하십시오.

빠른 시작

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

1 **OneDrive** 사전 요구 사항을 검토합니다

OneDrive 계정에 로그인할 수 있는 관리자 자격 증명이 있는지 확인합니다.

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 **OneDrive** 계정을 추가합니다

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

4 사용자를 추가하고 스캔 유형을 선택합니다

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

OneDrive 요구 사항 검토

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

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

BlueXP 분류 인스턴스 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

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

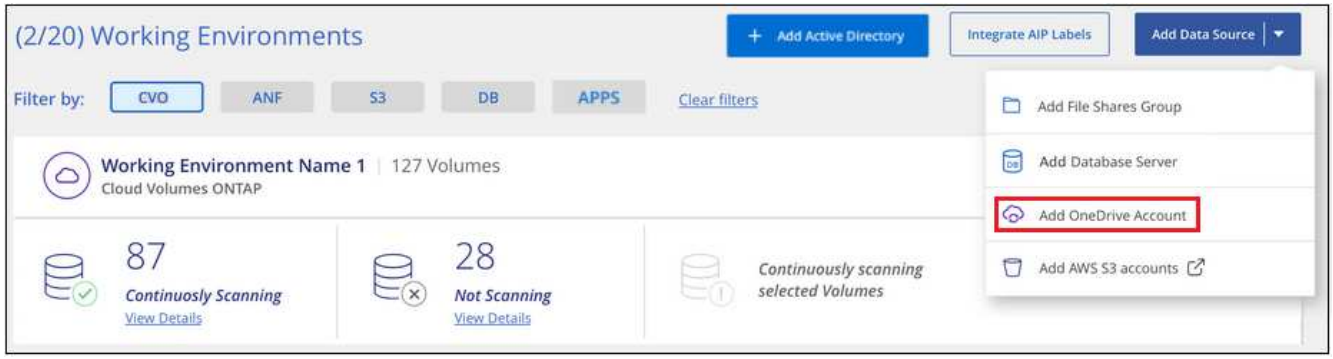
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

OneDrive 계정 추가

사용자 파일이 있는 OneDrive 계정을 추가합니다.

단계

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



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

OneDrive 계정이 작업 환경 목록에 추가됩니다.

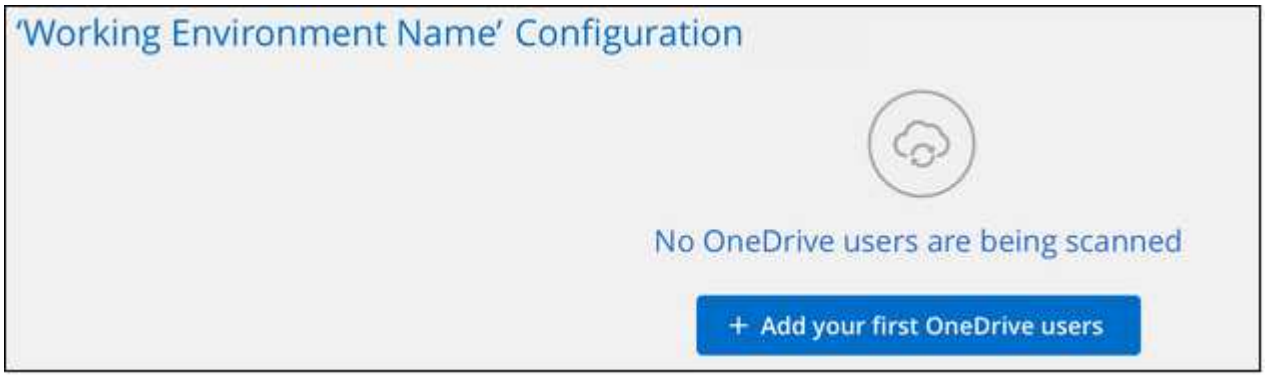
규정 준수 검사에 OneDrive 사용자 추가

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

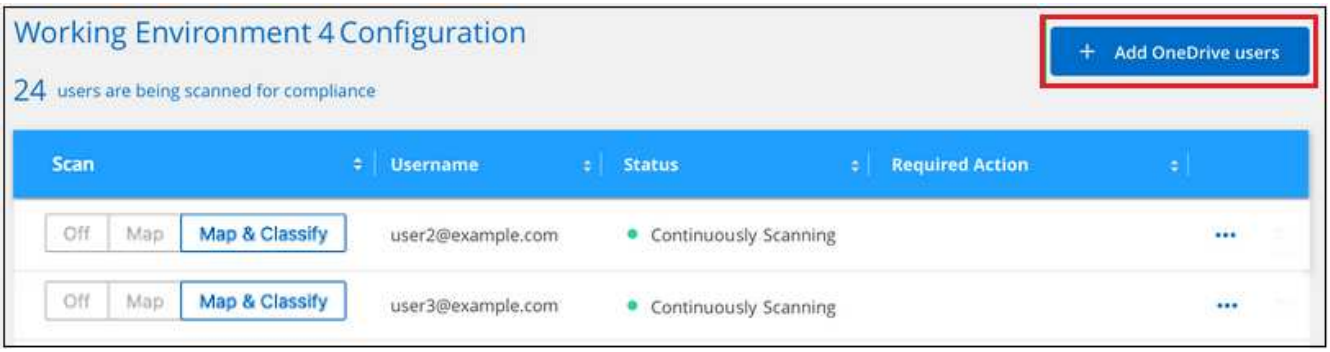
단계

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

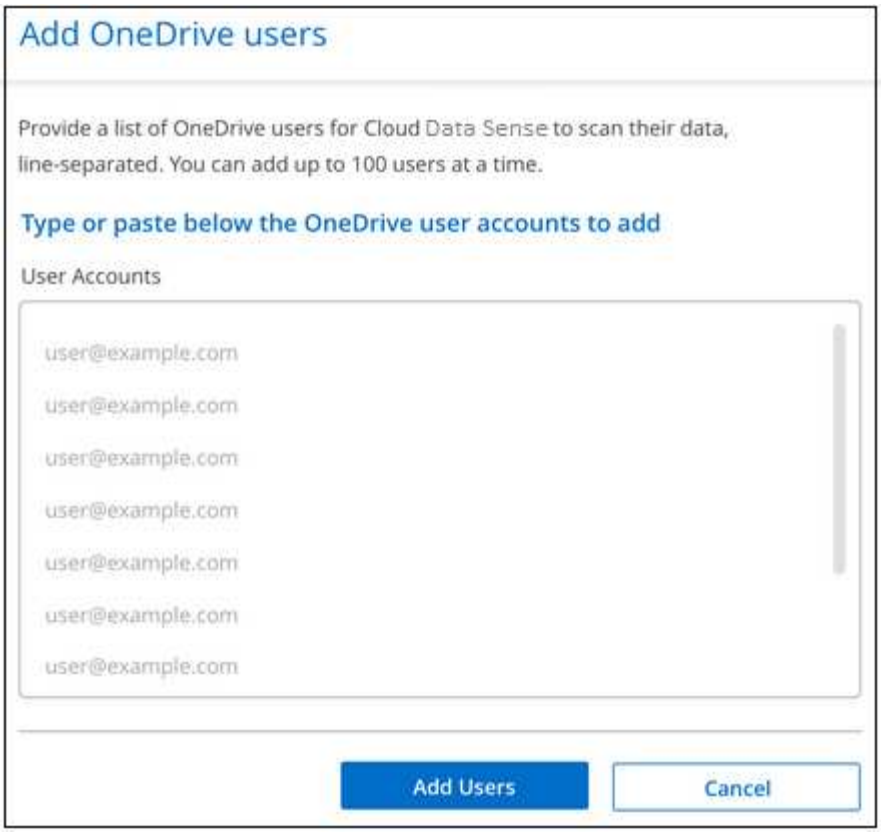
2. 이 OneDrive 계정에 사용자를 처음으로 추가하는 경우 * 첫 번째 OneDrive 사용자 추가 * 를 클릭합니다.



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



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



확인 대화 상자에 추가된 사용자 수가 표시됩니다.

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

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

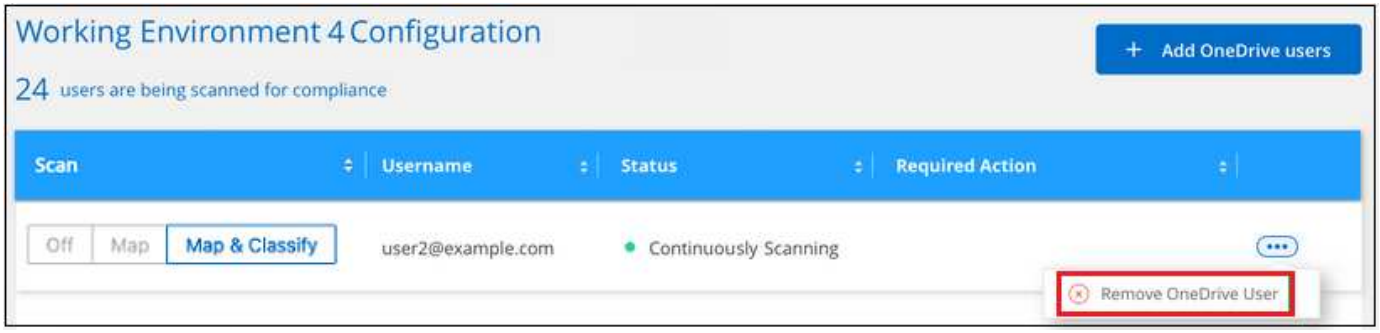
대상:	방법은 다음과 같습니다.
사용자 파일에 대한 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
사용자 파일에 대한 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
사용자 파일 스캔을 비활성화합니다	Off * 를 클릭합니다

결과

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

규정 준수 검사에서 **OneDrive** 사용자 제거

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



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

SharePoint 계정 스캔 중

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

빠른 시작

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

1 **SharePoint** 사전 요구 사항을 검토합니다

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

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 **SharePoint** 계정에 로그인합니다

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

4 검사할 **SharePoint** 사이트 **URL**을 추가합니다

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

SharePoint 요구 사항 검토

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

- 모든 SharePoint 사이트에 읽기 권한을 제공하는 SharePoint 계정에 대한 관리자 사용자 로그인 자격 증명이 있어야 합니다.
  - SharePoint Online의 경우 관리자가 아닌 계정을 사용할 수 있지만 해당 사용자는 검색할 모든 SharePoint

사이트에 액세스할 수 있는 권한이 있어야 합니다.

- SharePoint 온-프레미스의 경우 SharePoint Server의 URL도 필요합니다.
- 검색할 모든 데이터에 대해 SharePoint 사이트 URL의 줄 구분 목록이 필요합니다.

BlueXP 분류 인스턴스 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

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

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

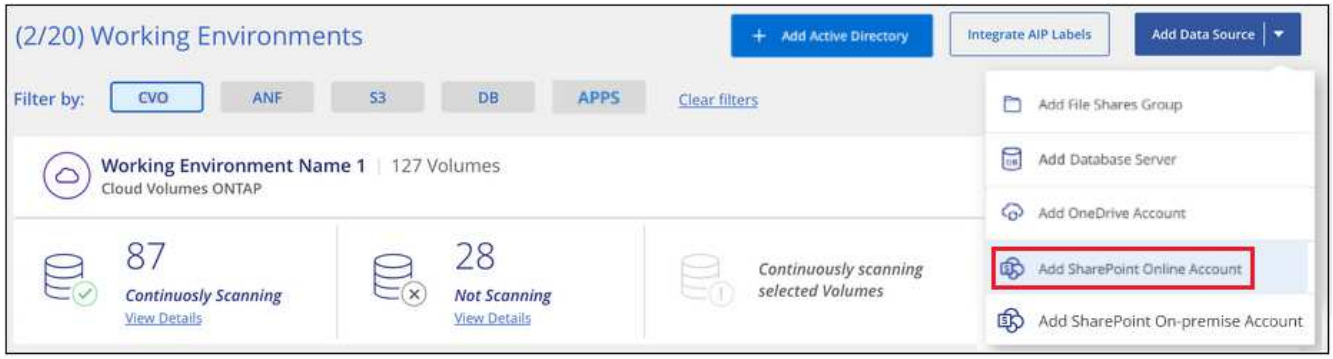
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

SharePoint Online 계정 추가

사용자 파일이 있는 SharePoint Online 계정을 추가합니다.

단계

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



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

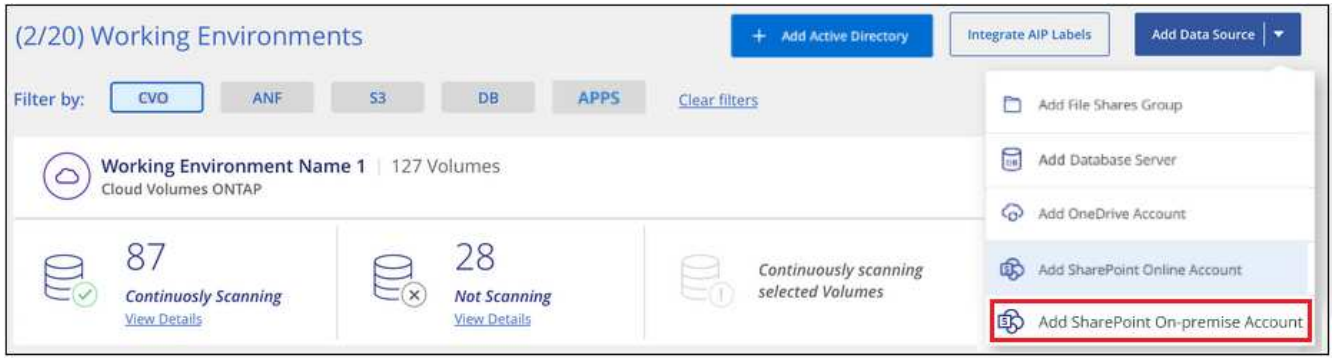
SharePoint Online 계정이 작업 환경 목록에 추가됩니다.

SharePoint 온-프레미스 계정 추가

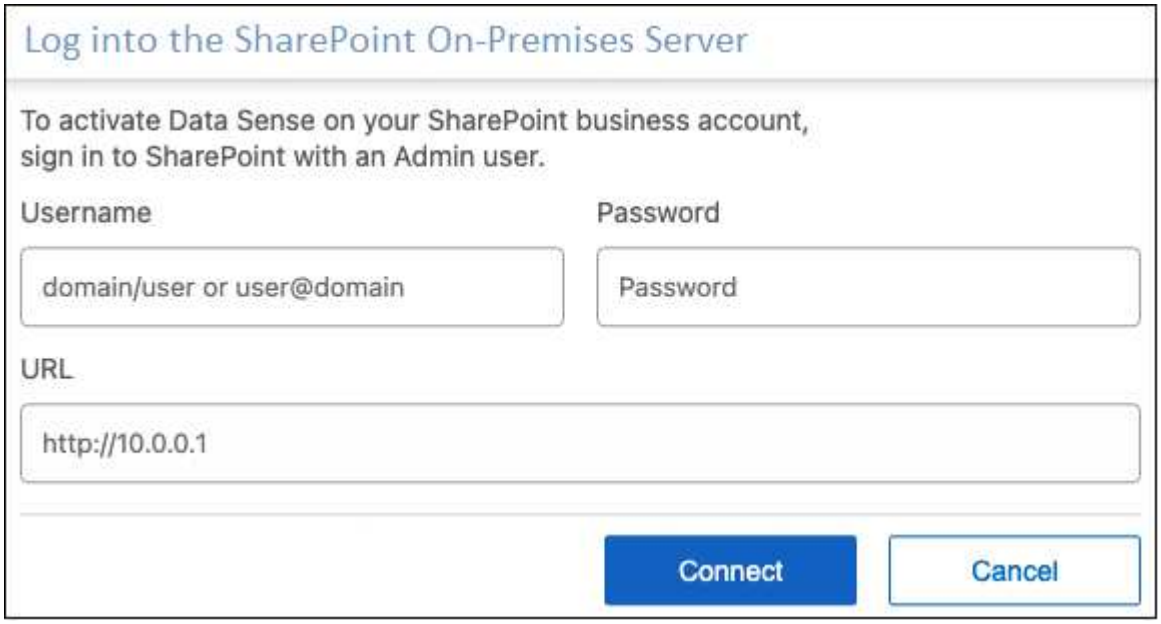
사용자 파일이 있는 SharePoint 온-프레미스 계정을 추가합니다.

단계

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



2. SharePoint 온-프레미스 서버에 로그인 대화 상자에서 다음 정보를 입력합니다.
   - "domain/user" 또는 "user@domain" 형식의 admin 사용자 및 admin 암호
   - SharePoint Server의 URL입니다



3. 연결 * 을 클릭합니다.

SharePoint 온-프레미스 계정이 작업 환경 목록에 추가됩니다.

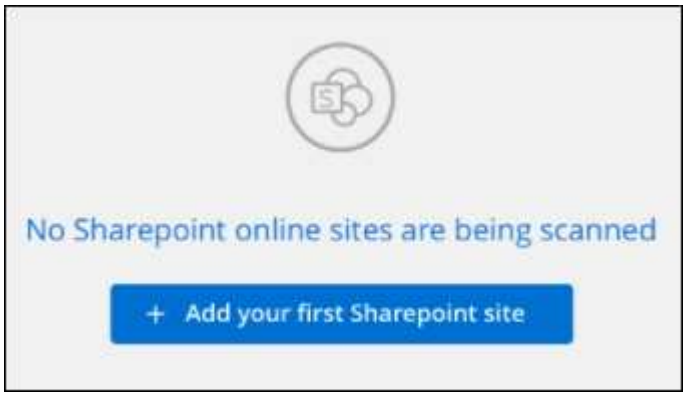
규정 준수 검사에 **SharePoint** 사이트 추가

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

단계

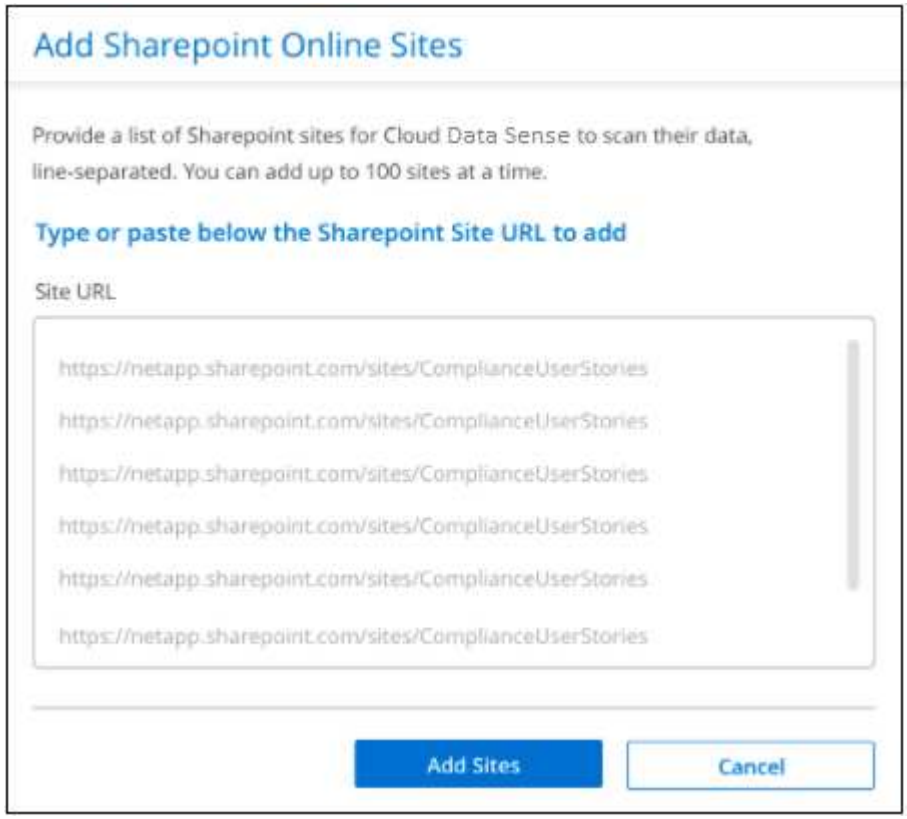
1. Configuration_ 페이지에서 SharePoint 계정의 * Configuration * 버튼을 클릭합니다.

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



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

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



확인 대화 상자에 추가된 사이트 수가 표시됩니다.

대화 상자에 추가할 수 없는 사이트가 나열되어 있으면 이 정보를 캡처하여 문제를 해결할 수 있습니다. 경우에 따라

수정된 URL을 사용하여 사이트를 다시 추가할 수 있습니다.

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

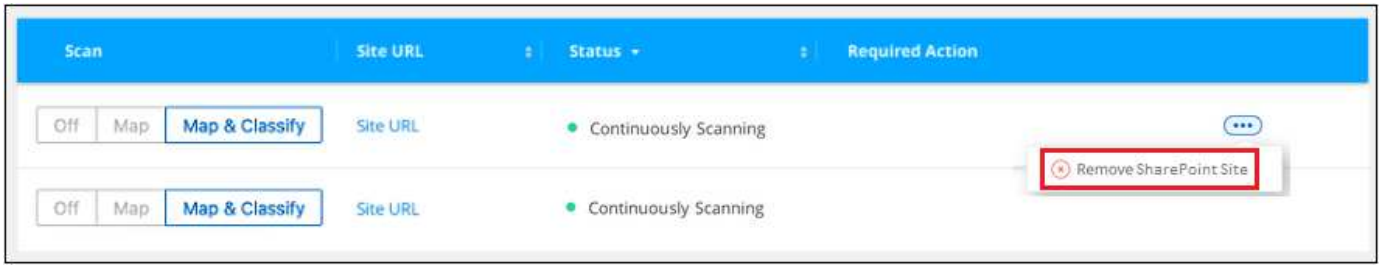
대상:	방법은 다음과 같습니다.
파일에서 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
파일에 대한 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
파일 스캔을 비활성화합니다	Off * 를 클릭합니다

결과

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

규정 준수 검사에서 **SharePoint** 사이트 제거

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



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

Google Drive 계정을 검색하는 중입니다

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

빠른 시작

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

1 **Google Drive** 사전 요구 사항을 검토합니다

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

2 **BlueXP** 분류를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 **Google Drive** 계정에 로그인합니다

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

4 사용자 파일에 대한 스캔 유형을 선택합니다

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

Google Drive 요구 사항 검토

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

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

현재 제한 사항

다음 BlueXP 분류 기능은 현재 Google 드라이브 파일에서 지원되지 않습니다.

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

BlueXP 분류 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

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

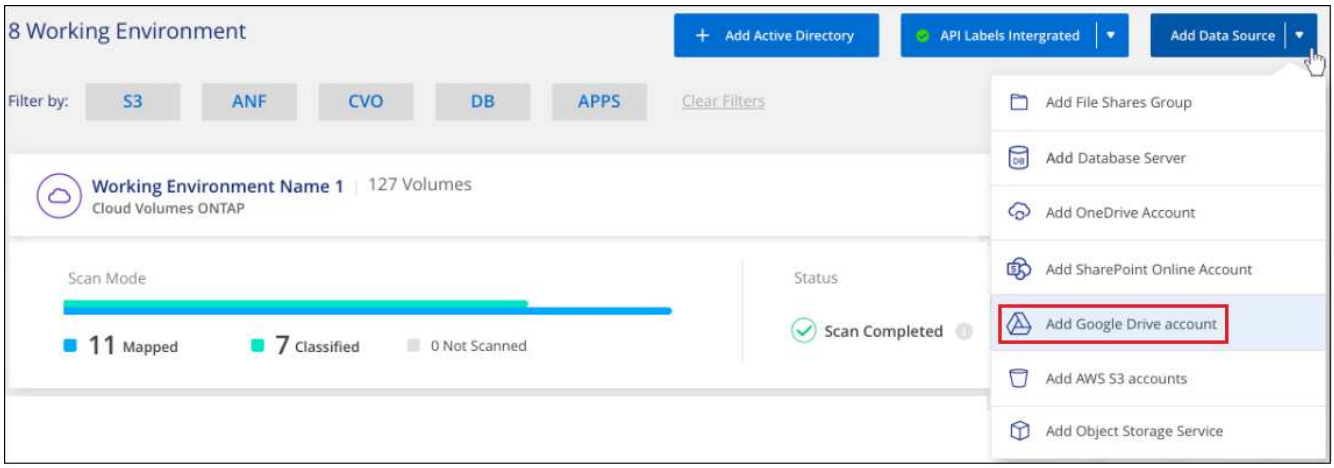
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

Google Drive 계정을 추가하는 중입니다

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

단계

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



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

Google Drive 계정이 작업 환경 목록에 추가됩니다.

사용자 데이터에 대한 스캔 유형을 선택합니다

BlueXP 분류가 사용자 데이터에 대해 수행할 스캔 유형을 선택합니다.

단계

1. Configuration_ 페이지에서 Google Drive 계정의 * Configuration * 버튼을 클릭합니다.

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

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

결과

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

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

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

파일 공유를 검색하는 중입니다

몇 가지 단계를 완료하여 BlueXP 분류와 직접 비NetApp NFS 또는 CIFS 파일 공유 스캔을 시작하십시오. 이러한 파일 공유는 사내 또는 클라우드에 상주할 수 있습니다.

빠른 시작

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

1 파일 공유 사전 요구 사항을 검토합니다

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

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 파일 공유를 보관할 그룹을 생성합니다

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

4 그룹에 파일 공유를 추가합니다

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

파일 공유 요구 사항 검토

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

- 공유는 클라우드 또는 온프레미스 등 어디서나 호스팅할 수 있습니다. 대부분의 경우 이는 NetApp이 아닌 스토리지 시스템에 상주하는 파일 공유입니다. 하지만 이전 NetApp 7-Mode 스토리지 시스템의 CIFS 공유를 파일 공유로 스캔할 수 있습니다.

  BlueXP 분류는 7-Mode 시스템에서 사용 권한 또는 "마지막 액세스 시간"을 추출할 수 없습니다. 또한 일부 Linux 버전과 7-Mode 시스템의 CIFS 공유 사이에서 알려진 문제로 인해 NTLM 인증이 활성화된 SMB v1만 사용하도록 공유를 구성해야 합니다.

- BlueXP 분류 인스턴스와 공유 사이에 네트워크 연결이 있어야 합니다.
- 이러한 포트가 BlueXP 분류 인스턴스에 열려 있는지 확인합니다.

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

- DFS(Distributed File System) 공유를 일반 CIFS 공유로 추가할 수 있습니다. 그러나 BlueXP 분류에서는 공유가 단일 CIFS 공유로 결합된 여러 서버/볼륨에 구축되어 있음을 인식하지 못하기 때문에 메시지가 실제로 다른 서버/볼륨에 있는 폴더/공유 중 하나에만 적용되는 경우 공유에 대한 권한 또는 연결 오류가 발생할 수 있습니다.
- CIFS(SMB) 공유의 경우 공유에 대한 읽기 액세스를 제공하는 Active Directory 자격 증명이 있는지 확인합니다. BlueXP 분류에서 상승된 권한이 필요한 데이터를 검색해야 하는 경우 관리자 자격 증명이 권장됩니다.

  BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 CIFS에서 쓰기 속성 사용 권한 또는 NFS에서 쓰기 권한이 사용자에게 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

- '<host_name>:/<share_path>' 형식으로 추가하려는 공유 목록이 필요합니다. 공유를 개별적으로 입력하거나 스캔하려는 파일 공유의 라인 분리 목록을 제공할 수 있습니다.

BlueXP 분류 인스턴스 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

인터넷을 통해 액세스할 수 있는 비NetApp NFS 또는 CIFS 파일 공유를 스캔하는 경우 다음을 수행할 수 있습니다 "클라우드에 BlueXP 분류를 배포합니다" 또는 "인터넷 액세스가 가능한 사내 위치에 BlueXP 분류를 배포합니다".

인터넷에 액세스할 수 없는 어두운 사이트에 설치된 비 NetApp NFS 또는 CIFS 파일 공유를 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 BlueXP 분류를 배포합니다". 또한 BlueXP Connector를 동일한 사내 위치에 배포해야 합니다.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

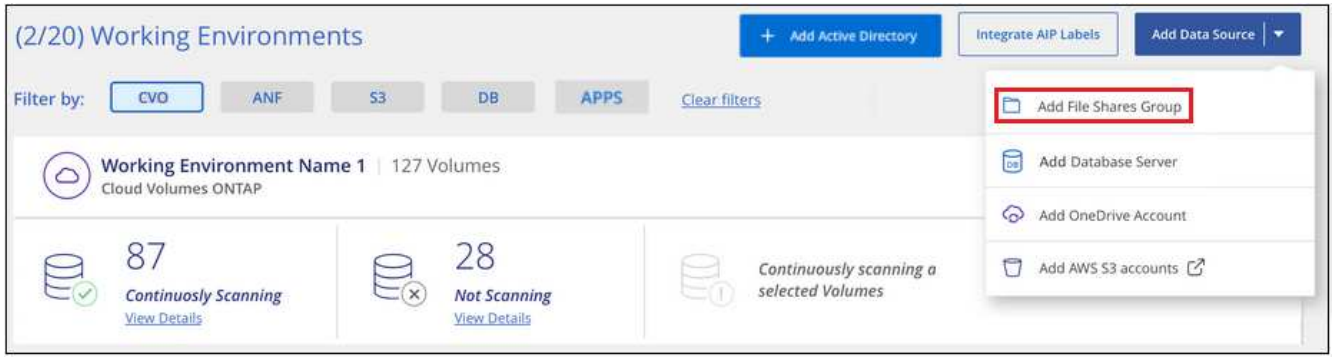
파일 공유에 대한 그룹을 생성하는 중입니다

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

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

단계

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



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

새 파일 공유 그룹이 작업 환경 목록에 추가됩니다.

그룹에 파일 공유를 추가하는 중입니다

파일 공유 그룹에 파일 공유를 추가하면 해당 공유의 파일이 BlueXP 분류에서 검사됩니다. 형식으로 공유를 추가합니다 `<host_name>:/<share_path>`.

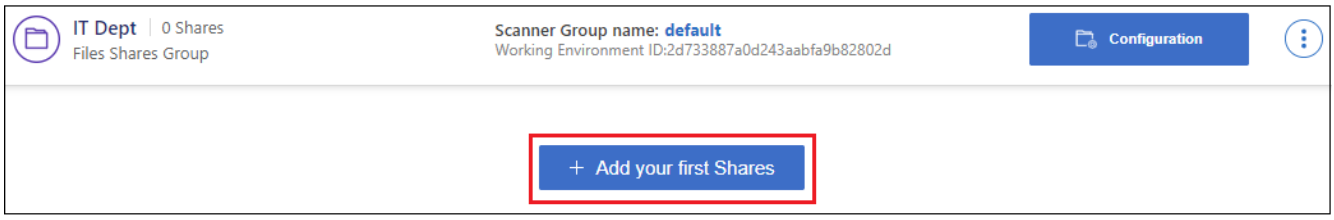
개별 파일 공유를 추가하거나 스캔할 파일 공유의 줄별 목록을 제공할 수 있습니다. 한 번에 최대 100개의 공유를 추가할 수 있습니다.

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

단계

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

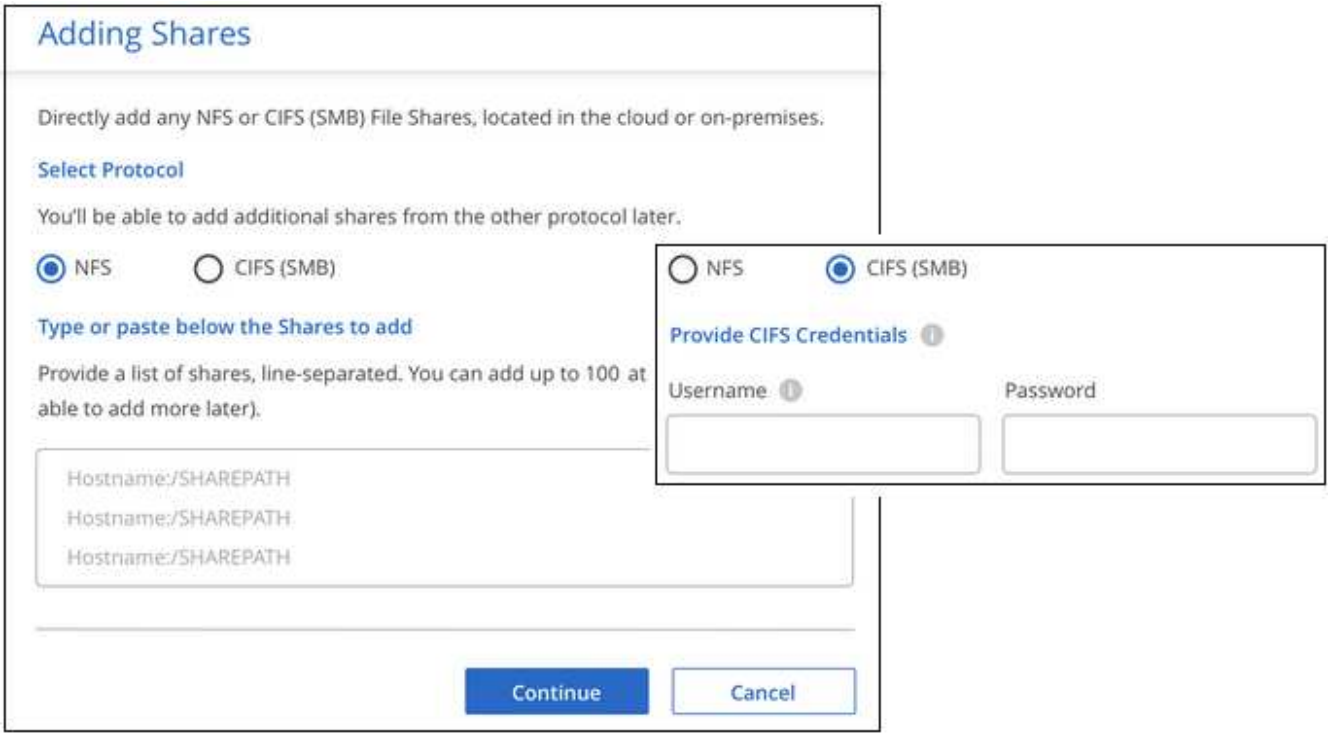
2. 이 파일 공유 그룹에 대한 파일 공유를 처음으로 추가하는 경우 * 첫 번째 공유 추가 * 를 클릭합니다.



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

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

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



확인 대화 상자에 추가된 공유 수가 표시됩니다.

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

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

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

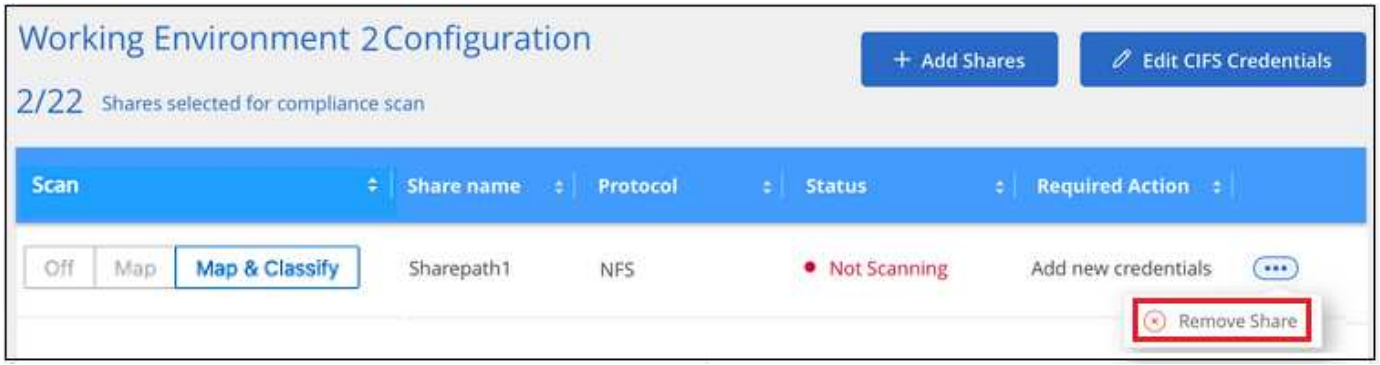
페이지 상단의 * "쓰기 속성" 권한 * 이 누락된 경우 * 스캔 에 대한 스위치는 기본적으로 비활성화되어 있습니다. 즉, BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우, 스위치를 켜면 사용 권한에 관계없이 모든 파일이 스캔됩니다. "자세한 정보".

결과

BlueXP 분류는 사용자가 추가한 파일 공유의 파일을 검사하기 시작하고 그 결과는 대시보드와 다른 위치에 표시됩니다.

규정 준수 검사에서 파일 공유를 제거합니다

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



S3 프로토콜을 사용하는 오브젝트 스토리지 스캔

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

빠른 시작

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

1 오브젝트 스토리지의 사전 요구 사항을 검토합니다

객체 스토리지 서비스에 연결하려면 엔드포인트 URL이 있어야 합니다.

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

2 **BlueXP** 분류 인스턴스를 배포합니다

"BlueXP 분류를 배포합니다" 이미 배포된 인스턴스가 없는 경우

3 오브젝트 스토리지 서비스를 추가합니다

BlueXP 분류에 오브젝트 스토리지 서비스를 추가합니다.

4 스캔할 버킷을 선택합니다

스캔하려는 버킷을 선택하면 BlueXP 분류가 스캔을 시작합니다.

오브젝트 스토리지의 요구사항 검토

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

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

BlueXP 분류 인스턴스 배포

배포된 인스턴스가 없으면 BlueXP 분류를 배포합니다.

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

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

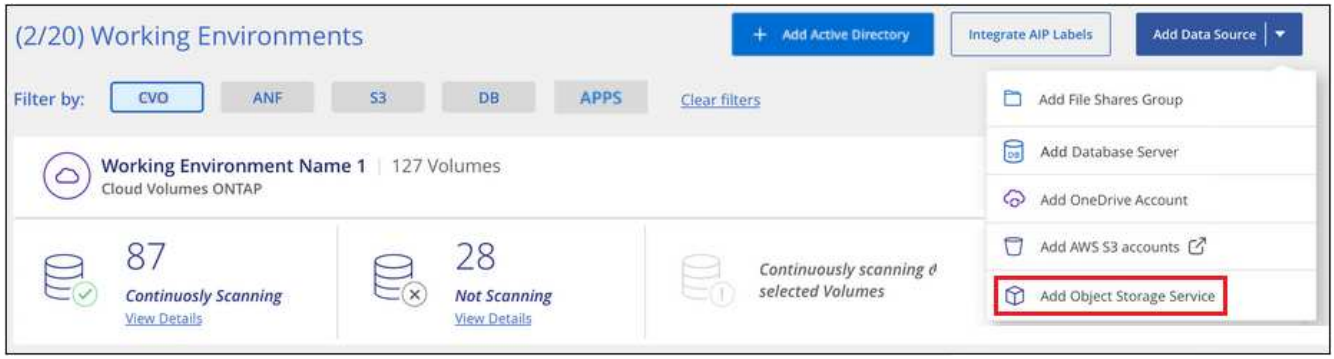
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

BlueXP 분류에 오브젝트 스토리지 서비스 추가

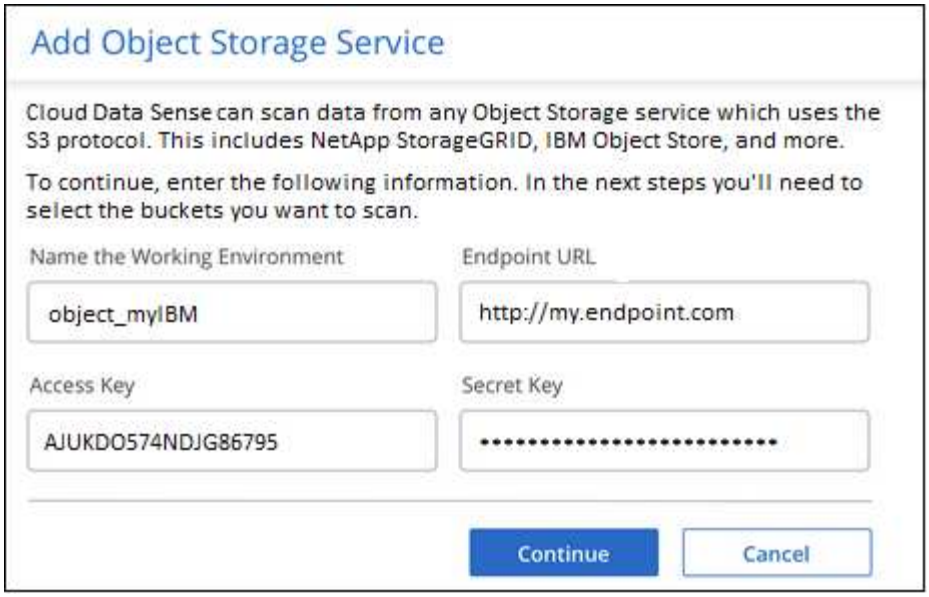
오브젝트 스토리지 서비스를 추가합니다.

단계

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



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



결과

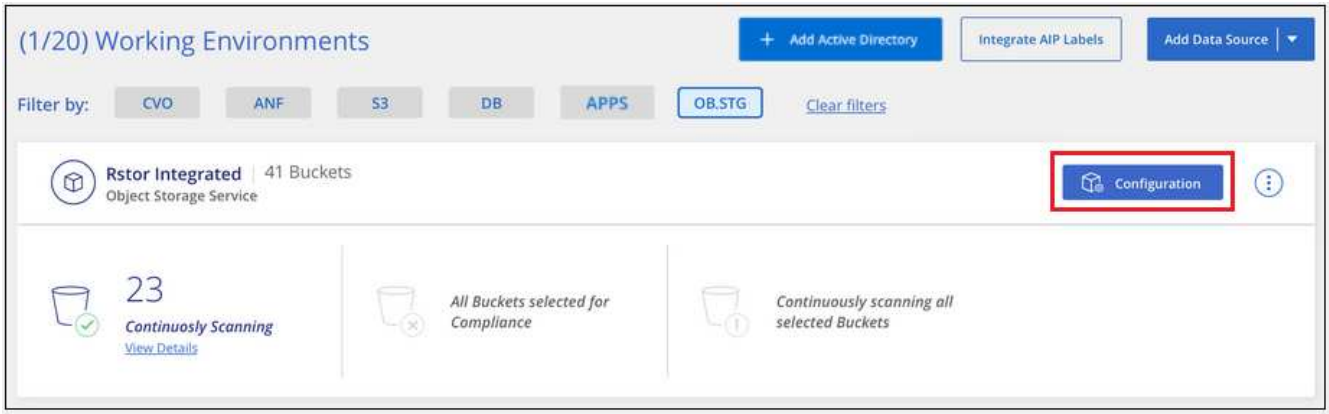
새로운 오브젝트 스토리지 서비스가 작업 환경 목록에 추가됩니다.

오브젝트 스토리지 버킷에 대한 규정 준수 검사 설정 및 해제

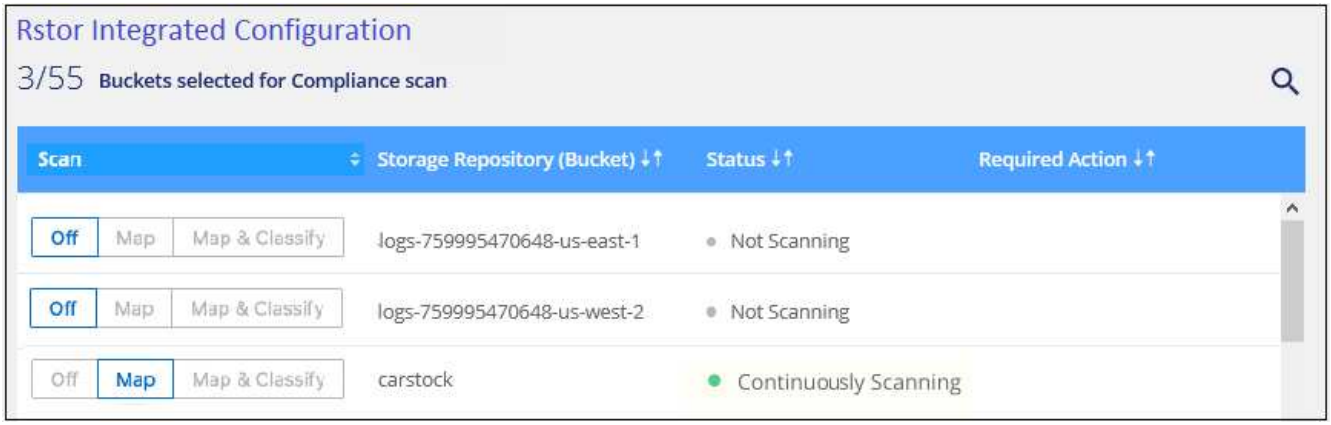
오브젝트 스토리지 서비스에서 BlueXP 분류를 활성화한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다. BlueXP 분류는 이러한 버킷을 검색하여 사용자가 만든 작업 환경에 표시합니다.

단계

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



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



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

결과

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

Active Directory를 BlueXP 분류와 통합합니다

글로벌 Active Directory를 BlueXP 분류와 통합하여 파일 소유자 및 파일에 액세스할 수 있는 사용자 및 그룹에 대한 BlueXP 분류 보고서의 결과를 개선할 수 있습니다.

아래 나열된 특정 데이터 소스를 설정할 때 BlueXP에서 CIFS 볼륨을 스캔하려면 Active Directory 자격 증명을 입력해야 합니다. 이러한 통합을 통해 파일 소유자와 BlueXP 분류를 수행하고 해당 데이터 소스에 있는 데이터에 대한 사용 권한 세부 정보를 확인할 수 있습니다. 이러한 데이터 원본에 대해 입력한 Active Directory가 여기에 입력한 글로벌 Active Directory 자격 증명과 다를 수 있습니다. BlueXP 분류는 모든 통합 Active Directory에서 사용자 및 권한 세부 정보를 확인할 수 있습니다.

이러한 통합은 BlueXP 분류의 다음 위치에 추가 정보를 제공합니다.

- "파일 소유자"를 사용할 수 있습니다. "필터" 그리고 조사 창에서 파일의 메타데이터에서 결과를 확인합니다. SID(보안 식별자)가 포함된 파일 소유자 대신 실제 사용자 이름으로 채워집니다.
- 확인할 수 있습니다 "전체 파일 권한" "모든 권한 보기" 버튼을 클릭하면 각 파일 및 디렉토리에 대해 이 작업을 수행할 수 있습니다.
- 에 있습니다 "거버넌스 대시보드"의 '사용 권한 열기' 패널에 데이터에 대한 자세한 정보가 표시됩니다.

ⓘ 로컬 사용자 SID 및 알 수 없는 도메인의 SID는 실제 사용자 이름으로 변환되지 않습니다.

지원되는 데이터 소스

BlueXP 분류와 Active Directory를 통합하면 다음 데이터 소스 내에서 데이터를 식별할 수 있습니다.

- 온프레미스 ONTAP 시스템
- Cloud Volumes ONTAP
- Azure NetApp Files
- ONTAP용 FSX
- 비 NetApp CIFS 파일 공유(NFS 파일 공유 아님)
- OneDrive 계정
- SharePoint 계정

데이터베이스 스키마, Google Drive 계정, Amazon S3 계정 또는 S3(Simple Storage Service) 프로토콜을 사용하는 오브젝트 스토리지에서 사용자 및 권한 정보를 식별할 수 있는 기능은 없습니다.

Active Directory 서버에 연결합니다

BlueXP 분류를 배포하고 데이터 소스에서 스캔을 활성화한 후 BlueXP 분류를 Active Directory와 통합할 수 있습니다. Active Directory는 DNS 서버 IP 주소 또는 LDAP 서버 IP 주소를 사용하여 액세스할 수 있습니다.

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

CIFS 볼륨/파일 공유의 경우 BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 사용자에게 쓰기 속성 권한이 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

요구 사항

- 회사의 사용자에 대해 Active Directory가 이미 설정되어 있어야 합니다.
- Active Directory에 대한 정보가 있어야 합니다.
  - DNS 서버 IP 주소 또는 여러 IP 주소

    또는

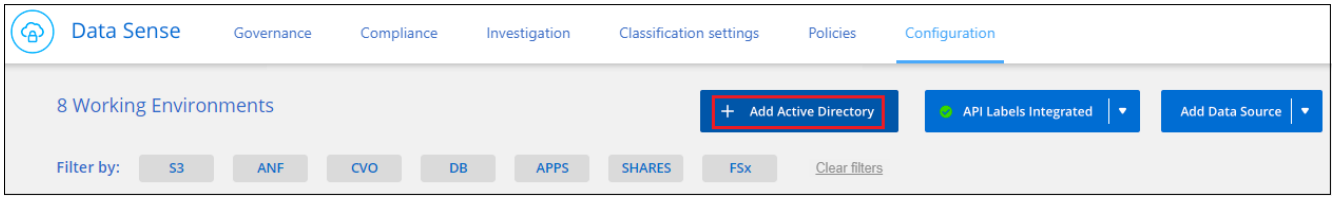
  LDAP 서버 IP 주소 또는 여러 IP 주소

  - 사용자 이름 및 암호 를 클릭하여 서버에 액세스합니다
  - 도메인 이름(Active Directory 이름)
  - 보안 LDAP(LDAPS) 사용 여부
  - LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)
- BlueXP 분류 인스턴스에서 아웃바운드 통신을 위해 다음 포트가 열려 있어야 합니다.

프로토콜	포트	목적지	목적
TCP 및 UDP	389	Active Directory를 클릭합니다	LDAP를 지원합니다
TCP	636	Active Directory를 클릭합니다	SSL을 통한 LDAP
TCP	3268	Active Directory를 클릭합니다	글로벌 카탈로그
TCP	3269	Active Directory를 클릭합니다	SSL을 통한 글로벌 카탈로그

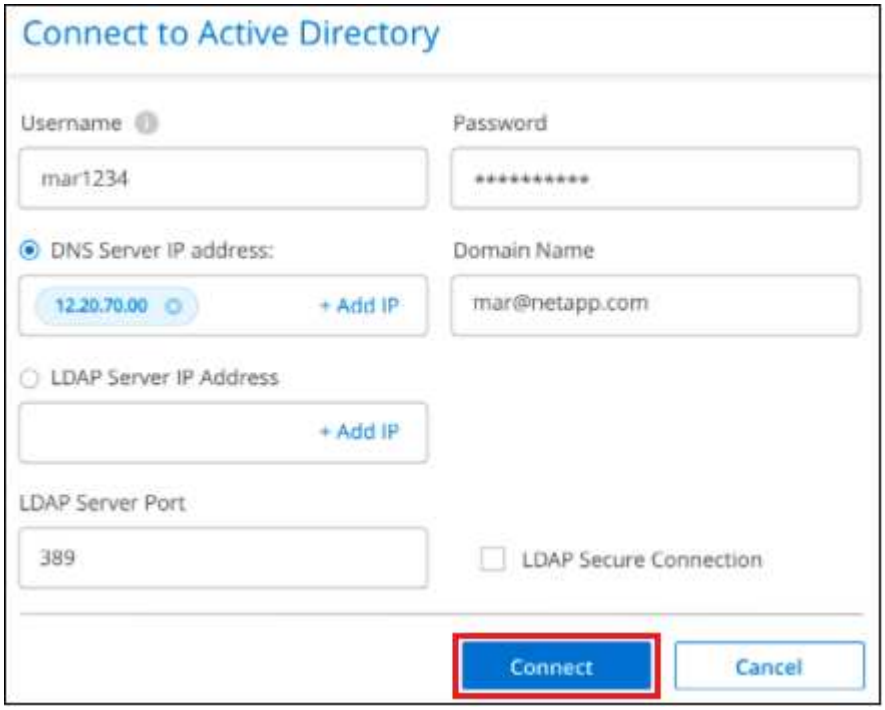
단계

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

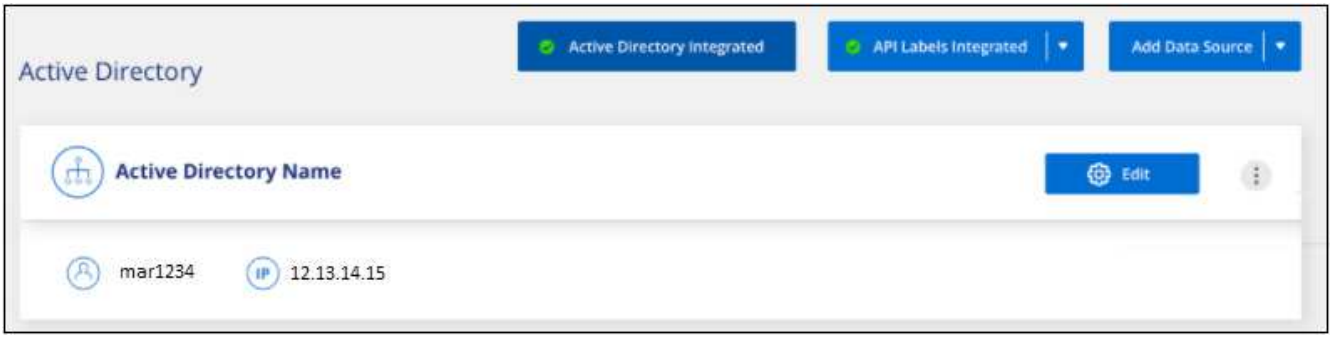


2. Active Directory에 연결 대화 상자에서 Active Directory 세부 정보를 입력하고 * Connect * 를 클릭합니다.

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



   BlueXP 분류는 Active Directory에 통합되며 새 섹션이 구성 페이지에 추가됩니다.



Active Directory 통합을 관리합니다

Active Directory 통합에서 값을 수정해야 하는 경우 * Edit * (편집 *) 버튼을 클릭하여 변경합니다.

통합을 더 이상 필요로 하지 않는 경우 을 클릭하여 삭제할 수도 있습니다 ⋮ 단추를 클릭한 다음 * Active Directory 제거 * 를 클릭합니다.

BlueXP 분류 라이선스를 설정합니다

BlueXP 작업 공간에서 BlueXP 분류 검사를 수행하는 첫 1TB의 데이터는 30일간 무료로 제공됩니다. 해당 시점 이후에도 데이터를 계속 스캔하려면 NetApp의 BYOL 라이센스 또는 클라우드 공급자 마켓플레이스의 가입형 라이센스가 필요합니다.

추가 내용을 읽기 전에 몇 가지 참고 사항을 확인하십시오.

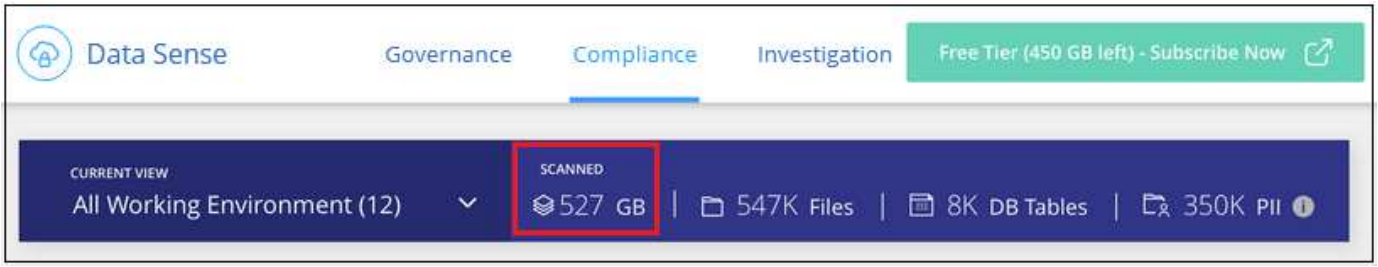
- 클라우드 공급자의 마켓플레이스에서 이미 BlueXP PAYGO(pay-as-you-go) 구독을 신청했다면 BlueXP 분류에도 자동으로 가입됩니다. 다시 가입하지 않아도 됩니다.
- BlueXP 분류(데이터 감지) BYOL(Bring-Your-Own-License)은 작업 공간의 모든 작업 환경과 데이터 소스에서 스캔할 수 있는 _floating_license입니다. BlueXP 디지털 지갑에 활성 구독이 표시됩니다.
- 스캔되는 데이터의 양은 스토리지 효율성 없이 논리적 파일 크기를 기준으로 계산됩니다.

"BlueXP 분류와 관련된 라이센스 및 비용에 대해 자세히 알아보십시오".

30일 무료 평가판

BlueXP 작업 공간에서 BlueXP 분류 검사를 수행하는 최대 1TB의 데이터에 대해 30일 무료 평가판을 사용할 수 있습니다. 이후 데이터 검색을 계속하려면 NetApp에서 BYOL 라이센스를 구입하거나 클라우드 공급자의 마켓플레이스에서 구독을 신청해야 합니다.

언제든지 구독할 수 있으며 30일 평가판이 종료되거나 데이터 양이 1TB를 초과할 때까지 요금이 청구되지 않습니다. BlueXP 분류 거버넌스 대시보드에서 스캔되는 데이터의 총 양을 항상 확인할 수 있습니다. 지금 가입(*Subscribe Now*) 단추를 사용하면 준비가 되면 쉽게 가입할 수 있습니다.



BlueXP 분류 PAYGO 구독을 사용합니다

클라우드 공급자의 마켓플레이스에서 용량제 구독을 통해 Cloud Volumes ONTAP 시스템 및 BlueXP 분류와 같은 많은 BlueXP 서비스 사용에 대한 라이센스를 등록할 수 있습니다. 단일 구독에서 시간 단위로 BlueXP 분류를 검사하는 데이터의 양에 대한 비용을 클라우드 공급자에게 지불하게 됩니다.

구독하면 무료 평가판이 종료된 후에도 서비스가 중단되지 않습니다. 평가판이 종료되면 스캔하는 데이터의 양에 따라 매시간 요금이 부과됩니다. 무료 평가판 사용 중에는 구독에 대한 요금이 부과되지 않습니다.

단계

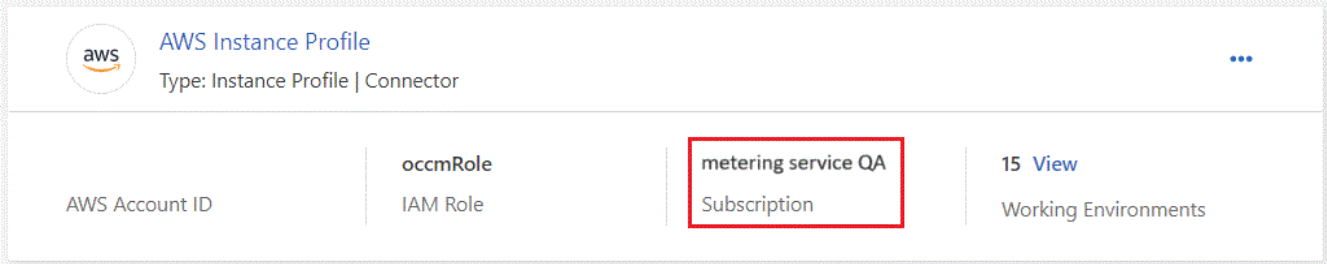
이러한 단계는 _ 계정 관리자 _ 역할을 가진 사용자가 완료해야 합니다.

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 * 자격 증명 * 을 선택합니다.

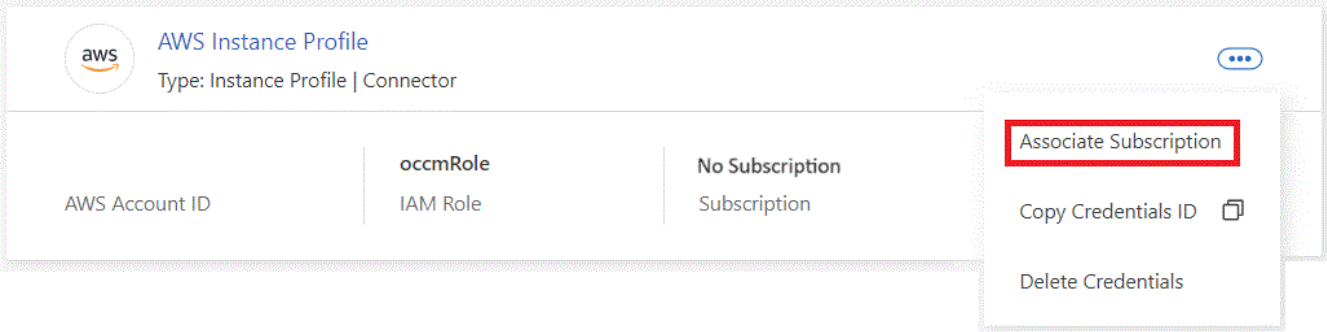
2. 자격 증명 * 을 클릭한 다음 AWS 인스턴스 프로필, Azure Managed Service Identity 또는 Google Project에 대한 자격 증명을 찾습니다.

   구독은 인스턴스 프로필, 관리 서비스 ID 또는 Google Project에 추가해야 합니다. 그렇지 않으면 충전이 작동하지 않습니다.

   AWS용 아래 표시된 것처럼 이미 BlueXP에 가입되어 있다면 모두 준비가 완료된 것입니다. 더 필요한 것은 없습니다.



3. 아직 구독이 없는 경우 작업 메뉴를 클릭하고 * 가입 연계 * 를 클릭합니다.



4. 기존 구독을 선택하고 * Associate * 를 클릭하거나 * Add Subscription * 을 클릭하고 단계를 따릅니다.

   다음 비디오에서는 을 연결하는 방법을 보여줍니다 "AWS 마켓플레이스 를 참조하십시오" AWS 구독:

   ▶ https://docs.netapp.com/ko-kr/bluexp-classification//media/video_subscribing_aws.mp4 *(video)*

   다음 비디오에서는 을 연결하는 방법을 보여줍니다 "Azure 마켓플레이스 를 참조하십시오" Azure 구독 신청:

   ▶ https://docs.netapp.com/ko-kr/bluexp-classification//media/video_subscribing_azure.mp4 *(video)*

   다음 비디오에서는 을 연결하는 방법을 보여줍니다 "Google Cloud 마켓플레이스 를 참조하십시오" GCP 구독 신청:

   ▶ https://docs.netapp.com/ko-kr/bluexp-classification//media/video_subscribing_gcp.mp4 *(video)*

연간 계약을 사용합니다

연간 계약을 구매하여 BlueXP 분류에 대한 비용을 매년 지불합니다. 1년, 2년 또는 3년 기간으로 제공됩니다.

마켓플레이스에서 연간 계약을 체결한 경우 모든 BlueXP 분류 데이터 스캔 비용이 해당 계약에 대해 청구됩니다. BYOL은 연간 시장 계약을 혼합 및 일치시킬 수 없습니다.

- AWS: "가격 세부 정보는 BlueXP Marketplace 오퍼링으로 이동하십시오".
- Azure(Azure): "가격 세부 정보는 BlueXP Marketplace 오퍼링으로 이동하십시오".
- Google Cloud: 연간 계약을 구매하려면 NetApp 세일즈 담당자에게 문의하십시오. 이 계약은 Google Cloud Marketplace에서 프라이빗 오퍼로 제공됩니다. NetApp이 전용 혜택을 공유하고 나면 BlueXP 분류 활성화 중에 Google Cloud Marketplace를 구독할 때 연간 계획을 선택할 수 있습니다.

BlueXP 분류 BYOL 라이센스 사용

NetApp에서 제공하는 자체 라이센스는 1년, 2년 또는 3년간 제공됩니다. BYOL BlueXP 분류(Data Sense) 라이센스는 작업 환경 및 데이터 소스의 * 전체 * 간에 전체 용량을 공유하는 _ floating_license로 초기 라이센스 및 갱신을 간편하게 수행할 수 있습니다.

BlueXP 분류 라이센스가 없는 경우 다음 연락처로 문의해 주십시오.

- mailto:ng-contact-data-sense@netapp.com?subject=Licensing [라이센스 구매를 위해 이메일 보내기].
- 라이센스를 요청하려면 BlueXP 오른쪽 하단의 채팅 아이콘을 클릭하십시오.

선택적으로 사용하지 않을 Cloud Volumes ONTAP에 대해 할당되지 않은 노드 기반 라이센스가 있는 경우 동일한 달러 당량 및 만료 날짜가 있는 BlueXP 분류 라이센스로 변환할 수 있습니다. "자세한 내용을 보려면 여기를 클릭하십시오".

BlueXP 디지털 지갑을 사용하여 BlueXP 분류 BYOL 라이센스를 관리할 수 있습니다. BlueXP 디지털 지갑에서 새 라이센스를 추가하고 기존 라이센스를 업데이트하고 라이센스 상태를 볼 수 있습니다.

BlueXP 분류 라이센스 파일을 얻습니다

BlueXP 분류(데이터 감지) 라이센스를 구매한 후에는 BlueXP 분류 일련 번호 및 NSS(NetApp Support 사이트) 계정을 입력하거나 NetApp 라이센스 파일(NLF)을 업로드하여 BlueXP에서 라이센스를 활성화합니다. 아래 단계에서는 NLF 라이센스 파일을 가져오는 방법을 보여 줍니다(해당 방법을 사용하려는 경우).

인터넷에 액세스할 수 없는 온프레미스 사이트의 호스트에 BlueXP 분류를 구축한 경우, BlueXP Connector를 에 구축한 것입니다 "비공개 모드", 인터넷에 연결된 시스템에서 라이센스 파일을 얻어야 합니다. 개인 모드 설치에서는 제품 번호 및 NSS 계정을 사용하여 라이센스를 활성화할 수 없습니다.

시작하기 전에

시작하기 전에 다음 정보가 필요합니다.

- BlueXP 분류 일련 번호

  판매 주문에서 이 번호를 찾거나 계정 팀에 문의하여 이 정보를 확인하십시오.

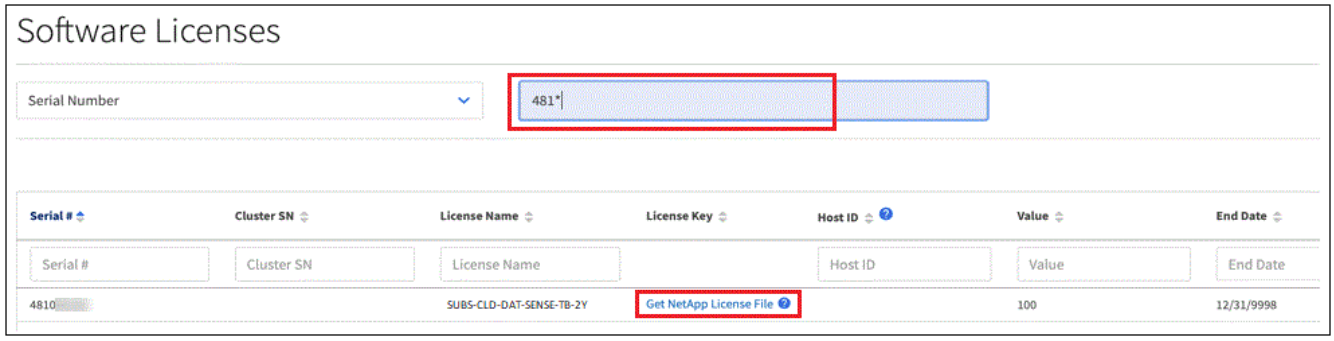
- BlueXP 계정 ID

  BlueXP의 상단에서 * 계정 * 드롭다운을 선택한 다음 계정 옆의 * 계정 관리 * 를 클릭하여 BlueXP 계정 ID를 찾을 수 있습니다. 계정 ID는 개요 탭에 있습니다. 인터넷에 액세스할 수 없는 개인 모드 사이트의 경우 * ACCOUNT-

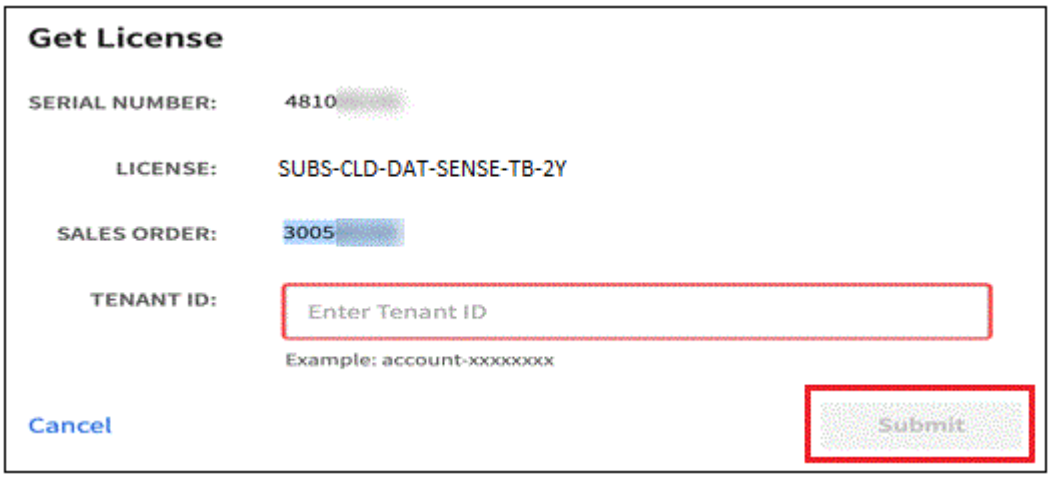
DARKSITE1 * 을 사용하십시오.

단계

1. 에 로그인합니다 "NetApp Support 사이트" 시스템 > 소프트웨어 라이센스 * 를 클릭합니다.
2. BlueXP 분류 라이센스 일련 번호를 입력합니다.



3. 라이센스 키 * 열에서 * NetApp 라이센스 파일 가져오기 * 를 클릭합니다.
4. BlueXP 계정 ID(지원 사이트에서 테넌트 ID라고 함)를 입력하고 * 제출 * 을 클릭하여 라이센스 파일을 다운로드합니다.



BlueXP 분류 **BYOL** 라이센스를 계정에 추가합니다

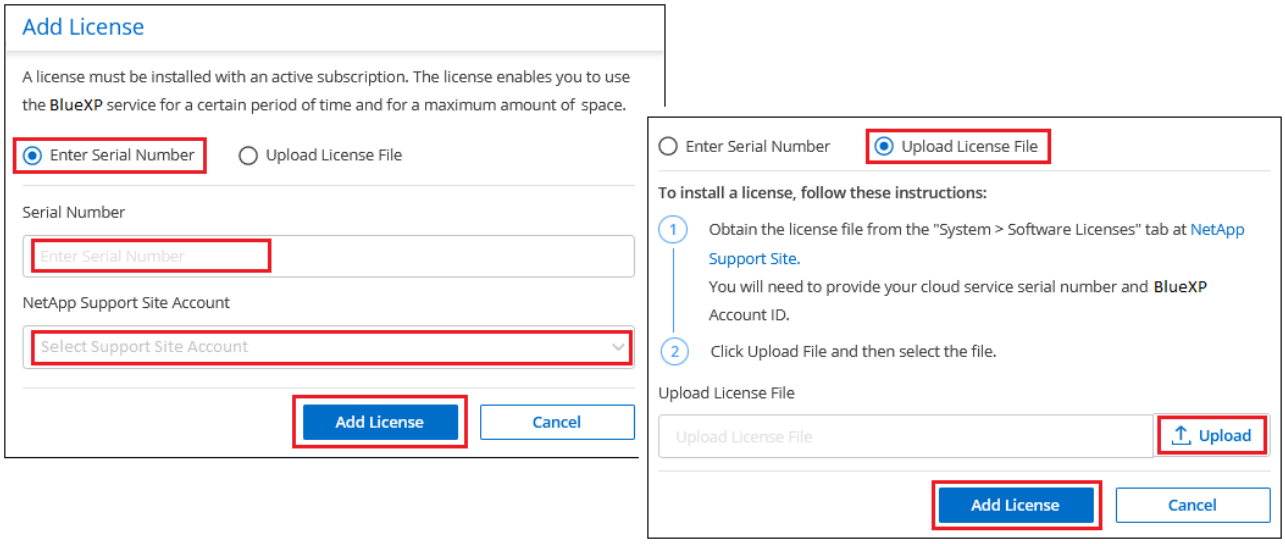
BlueXP 계정에 대한 BlueXP 분류(데이터 감지) 라이센스를 구입한 후 BlueXP 분류 서비스를 사용하려면 BlueXP에 라이센스를 추가해야 합니다.

단계

1. BlueXP 메뉴에서 * Governance > Digital Wallet * 을 클릭한 다음 * Data Services Licenses * 탭을 선택합니다.
2. 라이선스 추가 * 를 클릭합니다.
3. Add License_대화 상자에서 라이센스 정보를 입력하고 * Add License * 를 클릭합니다.
   - BlueXP 분류 라이선스 일련 번호가 있고 NSS 계정을 알고 있는 경우 * 일련 번호 입력 * 옵션을 선택하고 해당 정보를 입력합니다.

     드롭다운 목록에서 NetApp Support 사이트 계정을 사용할 수 없는 경우 "NSS 계정을 BlueXP에 추가합니다".

- BlueXP 분류 라이센스 파일(어두운 사이트에 설치할 때 필요)이 있는 경우 * 라이센스 파일 업로드 * 옵션을 선택하고 메시지에 따라 파일을 첨부합니다.



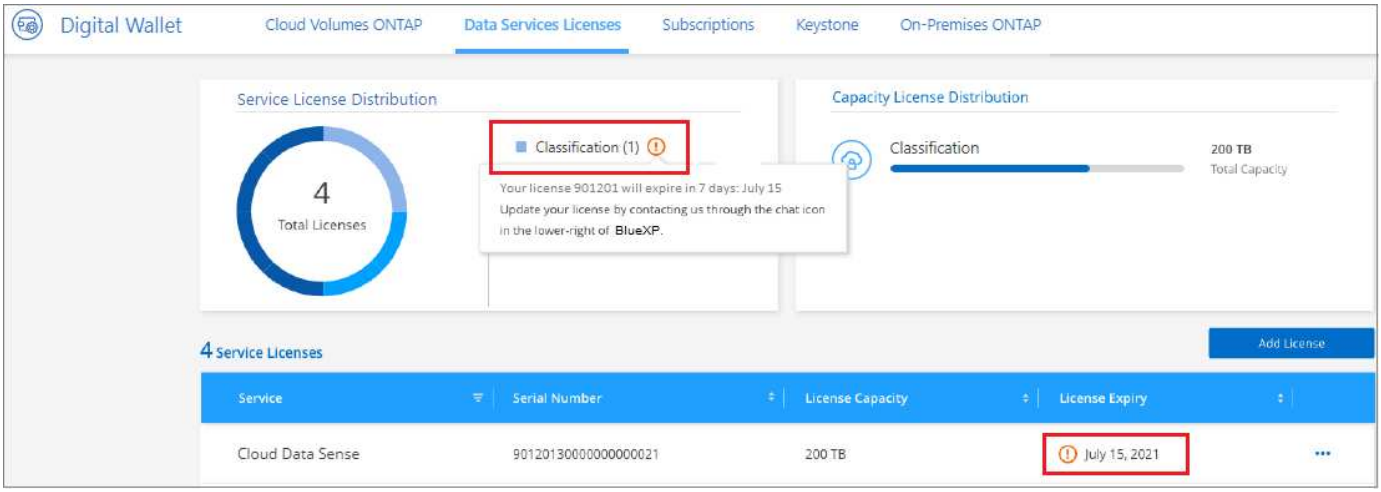
결과

BlueXP는 BlueXP 분류 서비스가 활성화되도록 라이센스를 추가합니다.

BlueXP 분류 BYOL 라이센스를 업데이트합니다

라이센스 기간이 만료일에 가까워졌거나 라이센스 용량이 제한에 도달한 경우 분류 UI에서 알림을 받게 됩니다.

이 상태는 BlueXP 디지털 지갑과 에도 표시됩니다 "알림".



BlueXP 분류 라이센스가 만료되기 전에 업데이트하여 스캔한 데이터에 액세스할 수 없도록 할 수 있습니다.

단계

1. BlueXP의 오른쪽 하단에 있는 채팅 아이콘을 클릭하여 특정 일련 번호에 대한 Cloud Data Sense 라이센스의 기간

연장 또는 추가 용량을 요청합니다. 또한 라이센스 업데이트를 요청하려면 이메일을 보내십시오을 사용할 수 있습니다.

라이센스 비용을 지불하고 NetApp Support 사이트에 등록한 후 BlueXP는 BlueXP 디지털 지갑의 라이센스를 자동으로 업데이트하고 데이터 서비스 라이센스 페이지에 변경 내용이 5-10분 내에 반영됩니다.

2. BlueXP에서 라이센스를 자동으로 업데이트할 수 없는 경우(예: 어두운 사이트에 설치된 경우) 라이센스 파일을 수동으로 업로드해야 합니다.
   a. 가능합니다 NetApp Support 사이트에서 라이센스 파일을 받으십시오.
   b. BlueXP 디지털 전자지갑의 _Data Services Licenses_탭에서 를 클릭합니다 ••• 업데이트하는 서비스 일련 번호에 대해 * Update License * 를 클릭합니다.

   c. Update License_page에서 라이센스 파일을 업로드하고 * Update License * 를 클릭합니다.

결과

BlueXP는 BlueXP 분류 서비스가 계속 활성화되도록 라이센스를 업데이트합니다.

BYOL 라이센스 고려사항

BlueXP 분류(Data Sense) BYOL 라이센스를 사용하는 경우, 검사 중인 모든 데이터의 크기가 용량 제한에 도달하거나 라이센스 만료 날짜가 임박한 경우 BlueXP 분류 UI와 BlueXP 디지털 지갑 UI에 경고가 표시됩니다. 다음과 같은 경고가 표시됩니다.

- 스캔 중인 데이터의 양이 라이센스 용량의 80%에 도달한 경우, 제한에 도달하면 다시 한 번 표시됩니다
- 라이센스가 만료되기 30일 전에 라이센스가 만료되고 라이센스가 만료되면 다시 만료됩니다

이러한 경고가 표시되면 BlueXP 인터페이스 오른쪽 아래에 있는 채팅 아이콘을 사용하여 라이센스를 갱신하십시오.

라이센스가 만료되거나 BYOL 제한에 도달한 경우 BlueXP 분류는 계속 실행되지만, 스캔한 데이터에 대한 정보를 볼 수 없도록 대시보드에 대한 액세스가 차단됩니다. 라이센스 한도 내에서 용량 사용을 잠재적으로 가져오기 위해 스캔되는 볼륨 수를 줄이려는 경우 *Configuration* 페이지만 사용할 수 있습니다.

BYOL 라이센스를 갱신하면 BlueXP 디지털 지갑에서 라이센스를 자동으로 업데이트하고 모든 대시보드에 대한 모든 액세스 권한을 제공합니다. BlueXP가 보안 인터넷 연결(예: 어두운 사이트에 설치된 경우)을 통해 라이센스 파일에 액세스할 수 없는 경우 직접 파일을 얻고 BlueXP에 수동으로 업로드할 수 있습니다. 자세한 내용은 을 참조하십시오 BlueXP 분류 라이센스를 업데이트하는 방법.

> 사용 중인 계정에 BYOL 라이센스와 PAYGO 가입이 모두 있는 경우 BYOL 라이센스가 만료되면 BlueXP classification_은 PAYGO 구독으로 전환할 수 없습니다. BYOL 라이센스를 갱신해야 합니다.

BlueXP 분류에 대한 질문과 대답

이 FAQ는 질문에 대한 간단한 답변을 찾는 경우에 도움이 될 수 있습니다.

BlueXP 분류 서비스

다음 질문은 BlueXP 분류에 대한 일반적인 이해를 제공합니다.

BlueXP 분류란 무엇입니까?

BlueXP 분류는 인공 지능(AI) 기반 기술을 사용하는 클라우드 오퍼링으로, 데이터 컨텍스트를 이해하고 스토리지 시스템 전반에 걸쳐 중요한 데이터를 식별하는 데 도움을 줍니다. 시스템은 BlueXP Canvas에 추가한 작업 환경과 BlueXP 분류가 네트워크를 통해 액세스할 수 있는 다양한 유형의 데이터 소스가 될 수 있습니다. "아래 전체 목록을 참조하십시오".

BlueXP 분류는 GDPR, CCPA, HIPAA 등과 같은 데이터 개인 정보 보호 및 민감성에 대한 새로운 데이터 규정 준수 규정을 해결하기 위해 미리 정의된 매개변수(예: 민감한 정보 유형 및 범주)를 제공합니다.

BlueXP 분류는 어떻게 작동합니까?

BlueXP 분류는 BlueXP 시스템 및 스토리지 시스템과 함께 또 다른 인공 지능 계층을 구축합니다. 그런 다음 볼륨, 버킷, 데이터베이스 및 기타 스토리지 계정의 데이터를 검색하고 검색된 데이터 인사이트를 인덱싱합니다. BlueXP 분류는 정규식과 패턴 일치를 기반으로 일반적으로 구축되는 대체 솔루션과 달리 인공 지능과 자연어 처리를 모두 활용합니다.

BlueXP 분류에서는 AI를 사용하여 정확한 탐지 및 분류를 위해 데이터에 대한 상황별 이해를 제공합니다. AI는 최신 데이터 유형과 규모에 맞게 설계되었으므로 AI를 중심으로 구동됩니다. 또한 데이터 컨텍스트를 이해하여 강력하고 정확한 검색 및 분류를 제공합니다.

"BlueXP 분류의 작동 방식에 대해 자세히 알아보십시오".

BlueXP 분류의 일반적인 사용 사례는 무엇입니까?

- 개인 식별 정보(PII)를 식별합니다.
- GDPR, CCPA, HIPAA 및 기타 데이터 개인 정보 보호 규정에 따라 데이터 주체에 대응하여 특정 데이터를 쉽게 찾고 보고할 수 있습니다.
- 새로운 데이터 개인 정보 보호 규정 및 예정된 데이터 개인 정보 보호 규정을 준수합니다.
- 데이터 규정 준수 및 개인정보 보호 규정 준수
- 기존 시스템에서 클라우드로 데이터 마이그레이션
- 데이터 보존 정책 준수

"BlueXP 분류의 사용 사례에 대해 자세히 알아보십시오".

BlueXP 분류의 아키텍처는 어떻습니까?

BlueXP 분류는 클라우드 또는 온프레미스 등 어느 곳에서든 단일 서버 또는 클러스터를 배포합니다. 서버는 표준 프로토콜을 통해 데이터 소스에 연결하고 동일한 서버에 배포되는 Elasticsearch 클러스터에서 결과를 인덱싱합니다. 따라서 멀티 클라우드, 교차 클라우드, 프라이빗 클라우드 및 온프레미스 환경을 지원할 수 있습니다.

지원되는 클라우드 공급자는 무엇입니까?

BlueXP 분류는 BlueXP의 일부로 작동하며 AWS, Azure 및 GCP를 지원합니다. 이를 통해 조직은 다양한 클라우드 공급자 전반에서 통합된 개인 정보 보호 가시성을 확보할 수 있습니다.

BlueXP 분류에는 **REST API**가 있으며 타사 도구와 작동합니까?

BlueXP는 서비스에 대한 REST API 기능을 지원합니다. BlueXP가 선호하는 관리 지점이 아닌 경우 REST API를 통해 BlueXP 분류 등의 서비스를 사용할 수도 있습니다. 모든 사용자 동작에는 타사 시스템과 통합할 수 있는 REST API가 있습니다. 을 참조하십시오 "BlueXP 분류 API" 를 참조하십시오.

시장에서 **BlueXP** 분류를 사용할 수 있습니까?

예. BlueXP 및 BlueXP 분류는 AWS, Azure 및 GCP 마켓플레이스에서 이용할 수 있습니다.

BlueXP 분류 스캔 및 분석

다음 질문은 BlueXP 분류 스캔 성능 및 사용자가 사용할 수 있는 분석과 관련이 있습니다.

BlueXP 분류는 내 데이터를 얼마나 자주 검사합니까?

데이터의 초기 스캔에는 시간이 다소 걸릴 수 있지만 후속 스캔에서는 증분 변경 내용만 검사하므로 시스템 검사 시간이 단축됩니다. BlueXP 분류는 데이터를 라운드 로빈 방식으로 지속적으로 스캔하므로 변경된 모든 데이터를 매우 빠르게 분류할 수 있습니다.

"스캔 작동 방식에 대해 알아보십시오".

BlueXP 분류는 데이터베이스를 하루에 한 번만 스캔합니다. 데이터베이스는 다른 데이터 소스와 마찬가지로 지속적으로 스캔되지 않습니다.

데이터 스캔은 스토리지 시스템과 데이터에 경미한 영향을 줍니다. 그러나 매우 작은 충격에도 신경 쓰면 BlueXP 분류를 구성하여 "느린" 스캔을 수행할 수 있습니다. "스캔 속도를 줄이는 방법을 참조하십시오".

BlueXP 분류를 사용하여 데이터를 검색할 수 있습니까?

BlueXP 분류는 연결된 모든 소스에서 특정 파일 또는 데이터 조각을 쉽게 검색할 수 있는 광범위한 검색 기능을 제공합니다. BlueXP 분류는 메타데이터의 반사보다 더 깊이 있는 검색을 가능하게 합니다. 또한 파일을 읽고 이름 및 ID와 같은 여러 가지 중요한 데이터 형식을 분석할 수 있는 언어 독립적인 서비스입니다. 예를 들어, 사용자는 정형 데이터 저장소와 비정형 데이터 저장소 모두를 검색하여 데이터베이스에서 사용자 파일로 유출되었을 수 있는 데이터를 찾을 수 있습니다. 이는 기업 정책에 위배됩니다. 검색을 나중에 저장할 수 있으며, 설정된 빈도로 검색 및 결과에 대한 조치를 취하기 위해 정책을 생성할 수 있습니다.

관심 파일이 발견되면 태그, 작업 환경 계정, 버킷, 파일 경로, 범주(분류 기준), 파일 크기, 마지막 수정, 권한 상태, 중복, 감도 수준, 개인 데이터, 파일 내 중요 데이터 유형, 소유자, 파일 유형, 파일 크기, 생성 시간, 파일 해시, 해당 데이터가 관심을 원하는 사람에게 할당되었는지 여부 등 필터는 관련이 없는 특성을 선별하는 데 적용할 수 있습니다. BlueXP 분류에는 적절한 권한이 있는 경우 파일을 이동하거나 삭제할 수 있도록 하는 RBAC 컨트롤도 있습니다. 올바른 사용 권한이 없으면 조직에 있는 사용자에게 적절한 사용 권한이 있는 작업을 할당할 수 있습니다.

BlueXP 분류는 어떤 종류의 분석을 제공합니까?

데이터 소스는 시각적으로 표현될 수 있으며 관계를 그래픽으로 정의하고 표현할 수 있습니다. 예를 들어, 관리자는 온프레미스 시스템, 데이터베이스, 파일 공유, S3 저장소, OneDrive, 등). 그런 다음 데이터를 복사, 이동, 삭제,

관리하여 스토리지 비용을 최적화하고 위험을 줄일 수 있습니다. 사용자는 중요한 데이터가 노출될 수 있는 것을 보고 위험을 줄일 수 있으며 강력한 데이터 보호를 위한 사용 권한을 관리하는 작업을 만들 수 있습니다. 또한 BlueXP 분류는 모든 다양한 유형의 데이터를 분류하므로 관리자가 데이터를 유형별로 조사하고 데이터에 대해 수행된 작업과 시기를 확인할 수 있습니다.

BlueXP 분류 제공 보고서가 있습니까**?**

예. BlueXP 분류에서 제공하는 정보는 조직의 다른 이해 관계자와 관련이 있을 수 있으므로 보고서를 생성하여 통찰력을 공유할 수 있습니다. BlueXP 분류에 대해 다음 보고서를 사용할 수 있습니다.

개인 정보 보호 위험 평가 보고서

개인 정보 보호 관련 정보와 개인 정보 보호 위험 점수를 제공합니다. "자세한 정보".

데이터 주체 액세스 요청 보고서

데이터 주체의 특정 이름 또는 개인 식별자와 관련된 정보가 포함된 모든 파일의 보고서를 추출할 수 있습니다. "자세한 정보".

PCI DSS 보고서

파일 전체에서 신용 카드 정보의 배포를 식별하는 데 도움이 됩니다. "자세한 정보".

HIPAA 보고서

파일에 대한 상태 정보 배포를 식별하는 데 도움이 됩니다. "자세한 정보".

데이터 매핑 보고서

작업 환경의 파일 크기 및 수에 대한 정보를 제공합니다. 여기에는 사용 용량, 데이터 사용 기간, 데이터 크기 및 파일 유형이 포함됩니다. "자세한 정보".

데이터 검색 평가 보고서

스캔한 환경에 대한 상위 수준의 분석을 통해 시스템 결과를 강조하고 문제 영역 및 잠재적인 개선 단계를 보여줍니다. "학습 모드".

특정 정보 유형에 대한 보고서입니다

개인 데이터와 민감한 개인 데이터가 포함된 식별된 파일에 대한 세부 정보가 포함된 보고서를 사용할 수 있습니다. 범주 및 파일 유형별로 분류된 파일도 볼 수 있습니다. "자세한 정보".

스캔 성능이 달라집니까**?**

스캔 성능은 네트워크 대역폭 및 환경의 평균 파일 크기에 따라 달라질 수 있습니다. 또한 호스트 시스템의 크기 특성(클라우드 또는 온프레미스)에 따라 달라질 수 있습니다. 을 참조하십시오 "BlueXP 분류 인스턴스입니다" 및 "BlueXP 분류 배포" 를 참조하십시오.

처음에 새 데이터 소스를 추가할 때 전체 "분류" 스캔이 아닌 "매핑" 스캔만 수행하도록 선택할 수도 있습니다. 내부 데이터를 보기 위해 파일에 액세스하지 않기 때문에 데이터 소스에서 매핑을 매우 빠르게 수행할 수 있습니다. "매핑 스캔과 분류 스캔의 차이를 확인하십시오".

BlueXP 분류 관리 및 개인 정보 보호

다음 질문에서는 BlueXP 분류 및 개인 정보 보호 설정을 관리하는 방법에 대한 정보를 제공합니다.

BlueXP 분류를 활성화하려면 어떻게 해야 합니까**?**

먼저 BlueXP 또는 사내 시스템에 BlueXP 분류 인스턴스를 배포해야 합니다. 인스턴스가 실행되면 * Configuration * 탭에서 기존 작업 환경, 데이터베이스 및 기타 데이터 원본에 대한 서비스를 활성화하거나 특정 작업 환경을 선택할 수 있습니다.

"시작하는 방법을 알아보십시오".

> 데이터 소스에서 BlueXP 분류를 활성화하면 즉시 초기 검사가 이루어집니다. 스캔 결과는 잠시 후에 표시됩니다.

BlueXP 분류를 비활성화하려면 어떻게 합니까**?**

BlueXP 분류 구성 페이지에서 개별 작업 환경, 데이터베이스, 파일 공유 그룹, OneDrive 계정 또는 SharePoint 계정을 검색하지 못하도록 BlueXP 분류를 비활성화할 수 있습니다.

"자세한 정보".

> BlueXP 분류 인스턴스를 완전히 제거하려면 클라우드 공급자의 포털 또는 사내 위치에서 BlueXP 분류 인스턴스를 수동으로 제거할 수 있습니다.

조직의 요구에 맞게 서비스를 사용자 정의할 수 있습니까**?**

BlueXP 분류는 데이터에 대한 즉각적인 통찰력을 제공합니다. 이러한 통찰력을 추출하여 조직의 요구에 활용할 수 있습니다.

또한 BlueXP 분류에서는 여러 가지 방법으로 BlueXP 분류에서 검사할 때 식별할 수 있는 "개인 데이터" 사용자 지정 목록을 추가할 수 있으므로 중요한 데이터가 조직의 _ All_ 파일에 있는 위치에 대한 전체 정보를 얻을 수 있습니다.

- 검색 중인 데이터베이스의 특정 열을 기준으로 고유 식별자를 추가할 수 있습니다. 이를 데이터 Fusion*라고 합니다.
- 텍스트 파일에서 사용자 지정 키워드를 추가할 수 있습니다.
- 정규식(regex)을 사용하여 사용자 지정 패턴을 추가할 수 있습니다.

"자세한 정보".

특정 디렉터리에서 스캔 데이터를 제외하도록 서비스를 지시할 수 있습니까**?**

예. BlueXP 분류를 통해 특정 데이터 소스 디렉토리에 있는 스캔 데이터를 제외하려면 해당 목록을 분류 엔진에 제공할 수 있습니다. 변경 사항을 적용하면 BlueXP 분류에서 지정된 디렉토리에 있는 검사 데이터를 제외합니다.

"자세한 정보".

ONTAP 볼륨에 있는 스냅샷 복사본이 검사됩니까**?**

아니요 BlueXP 분류는 볼륨의 콘텐츠와 동일하므로 스냅샷을 스캔하지 않습니다.

ONTAP 볼륨에서 데이터 계층화가 활성화된 경우 어떻게 됩니까**?**

BlueXP 분류는 오브젝트 스토리지에 콜드 데이터가 계층화된 볼륨을 검사할 때 로컬 디스크에 있는 모든 데이터와 오브젝트 스토리지에 계층화된 콜드 데이터를 검사합니다. 이는 계층화를 구현하는 NetApp 제품이 아닌 경우에도

마찬가지입니다.

스캔으로 콜드 데이터가 가열되지 않으며 오브젝트 스토리지에 보관되어 차갑게 유지됩니다.

BlueXP 분류가 조직에 알림을 보낼 수 있습니까**?**

예. 정책 기능과 함께 정책이 결과를 반환하면 데이터를 보호하기 위한 알림을 받을 수 있도록 BlueXP 사용자(매일, 매주 또는 매월) 또는 기타 전자 메일 주소로 전자 메일 알림을 보낼 수 있습니다. 에 대해 자세히 알아보십시오 "정책".

또한 조직에서 내부적으로 공유할 수 있는 관리 페이지 및 조사 페이지에서 상태 보고서를 다운로드할 수도 있습니다.

BlueXP 분류는 내 파일에 포함된 **AIP** 레이블과 함께 사용할 수 있습니까**?**

예. 에 가입한 경우 BlueXP 분류에서 검색하는 파일의 AIP 레이블을 관리할 수 있습니다 "AIP(Azure Information Protection)". 파일에 이미 할당된 레이블을 보고, 파일에 레이블을 추가하고, 기존 레이블을 변경할 수 있습니다.

"자세한 정보".

소스 시스템 및 데이터 유형의 유형입니다

다음 질문은 스캔할 수 있는 스토리지 유형 및 스캔할 데이터 유형과 관련되어 있습니다.

BlueXP 분류로 스캔할 수 있는 데이터 소스는 무엇입니까**?**

BlueXP 분류는 BlueXP Canvas에 추가한 작업 환경과 BlueXP 분류가 네트워크를 통해 액세스할 수 있는 다양한 유형의 정형 및 비정형 데이터 소스에서 데이터를 검색할 수 있습니다.

- 작업 환경: *
- Cloud Volumes ONTAP(AWS, Azure 또는 GCP에 구축)
- 온프레미스 ONTAP 클러스터
- Azure NetApp Files
- ONTAP용 Amazon FSx
- Amazon S3
- 데이터 소스: *
- 비 NetApp 파일 공유
- 오브젝트 스토리지(S3 프로토콜 사용)
- 데이터베이스(Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL Server)
- OneDrive 계정
- SharePoint Online 및 온-프레미스 계정
- Google Drive 계정

BlueXP 분류는 NFS 버전 3.x와 CIFS 버전 1.x, 2.0, 2.1 및 3.0을 지원합니다.

정부 지역에 배포할 때 제한 사항이 있습니까?

커넥터가 정부 지역(AWS GovCloud, Azure Gov 또는 Azure DoD)에 배포되어 "제한 모드"라고도 하는 경우 BlueXP 분류가 지원됩니다. 이러한 방식으로 배포된 BlueXP 분류에는 다음과 같은 제한 사항이 있습니다.

- OneDrive 계정, SharePoint 계정 및 Google Drive 계정을 검색할 수 없습니다.
- Microsoft Azure 정보 보호(AIP) 레이블 기능은 통합할 수 없습니다.

인터넷 액세스 없이 사이트에 **BlueXP** 분류를 설치할 경우 어떤 데이터 소스를 검색할 수 있습니까?

BlueXP 분류는 사내 사이트에 로컬인 데이터 소스에서만 데이터를 스캔할 수 있습니다. 현재 BlueXP 분류는 "비공개 모드"에서 "다크" 사이트라고도 하는 다음 로컬 데이터 소스를 검사할 수 있습니다.

- 온프레미스 ONTAP 시스템
- 데이터베이스 스키마
- SharePoint 사내 계정(SharePoint Server)
- 비NetApp NFS 또는 CIFS 파일 공유
- S3(Simple Storage Service) 프로토콜을 사용하는 오브젝트 스토리지

지원되는 파일 유형은 무엇입니까?

BlueXP 분류는 모든 파일에서 범주 및 메타데이터 정보를 검색하고 대시보드의 파일 형식 섹션에 모든 파일 형식을 표시합니다.

BlueXP 분류에서 PII(개인 식별 정보)를 감지하거나 DSAR 검색을 수행할 때 다음 파일 형식만 지원됩니다.

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

BlueXP 분류 체계는 어떤 종류의 데이터와 메타데이터를 캡처합니까?

BlueXP 분류를 통해 데이터 소스에서 일반적인 "매핑" 스캔 또는 전체 "분류" 스캔을 실행할 수 있습니다. 매핑은 데이터에 대한 상위 수준의 개요만 제공하는 반면 분류는 데이터에 대한 세부 수준의 스캐닝을 제공합니다. 내부 데이터를 보기 위해 파일에 액세스하지 않기 때문에 데이터 소스에서 매핑을 매우 빠르게 수행할 수 있습니다.

- 데이터 매핑 스캔.

  BlueXP 분류는 메타데이터만 스캔합니다. 이 기능은 전체 데이터 관리 및 거버넌스, 빠른 프로젝트 범위 지정, 대규모 부동산 및 우선순위 지정에 유용합니다. 데이터 매핑은 메타데이터를 기반으로 하며 * 빠른 * 스캔으로 간주됩니다.

  고속 스캔 후 데이터 매핑 보고서를 생성할 수 있습니다. 이 보고서는 리소스 활용도, 마이그레이션, 백업, 보안 및 규정 준수 프로세스에 대한 의사 결정을 돕기 위해 기업 데이터 소스에 저장된 데이터에 대한 개요입니다.

- 데이터 분류(딥) 스캔.

  BlueXP 분류 검사는 표준 프로토콜 및 사용자 환경 전체에서 읽기 전용 권한을 사용하여 수행합니다. Select 파일은 랜섬웨어 관련 중요 비즈니스 관련 데이터, 개인 정보 및 문제를 대상으로 열렸다 스캔됩니다.

  전체 스캔 후에는 데이터 조사 페이지의 데이터 보기 및 구체화, 파일 내 이름 검색, 복사, 이동, 원본 파일 삭제 등 데이터에 적용할 수 있는 여러 가지 BlueXP 분류 기능이 추가로 있습니다.

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

BlueXP 분류는 개인 데이터 및 중요 개인 데이터와 같은 다양한 유형의 프라이빗 데이터를 식별할 수 있습니다. 개인 데이터에 대한 자세한 내용은 을 참조하십시오 "BlueXP 분류가 검사하는 프라이빗 데이터의 범주입니다".

특정 사용자에게 **BlueXP** 분류 정보를 제한할 수 있습니까**?**

예. BlueXP 분류는 BlueXP와 완전히 통합되어 있습니다. BlueXP 사용자는 작업 영역 권한에 따라 볼 수 있는 작업 환경에 대한 정보만 볼 수 있습니다.

또한 특정 사용자가 BlueXP 분류 설정을 관리할 수 없는 상태에서 BlueXP 분류 검사 결과만 볼 수 있도록 하려면 해당 사용자에게 Cloud Compliance Viewer 역할을 할당할 수 있습니다.

"자세한 정보".

내 브라우저와 **BlueXP** 분류 간에 전송되는 개인 데이터에 누구나 액세스할 수 있습니까**?**

아니요 브라우저와 BlueXP 분류 인스턴스 간에 전송되는 프라이빗 데이터는 TLS 1.2를 사용하여 엔드 투 엔드 암호화로 보안이 유지됩니다. 즉, NetApp과 타사가 이 데이터를 읽을 수 없습니다. BlueXP 분류는 액세스를 요청하고 승인하지 않는 한 NetApp과 데이터 또는 결과를 공유하지 않습니다.

스캔되는 데이터는 사용자 환경 내에 유지됩니다.

중요 데이터는 어떻게 처리됩니까**?**

NetApp는 중요한 데이터에 액세스할 수 없으며 UI에 이를 표시하지 않습니다. 중요한 데이터는 마스킹됩니다. 예를 들어, 마지막 4개의 숫자는 신용 카드 정보로 표시됩니다.

데이터가 어디에 저장됩니까**?**

스캔 결과는 BlueXP 분류 인스턴스 내의 Elasticsearch에 저장됩니다.

데이터에 어떻게 액세스됩니까**?**

BlueXP 분류는 API 호출을 통해 Elasticsearch에 저장된 데이터에 액세스하며, 인증이 필요하며 AES-128을 사용하여 암호화됩니다. Elasticsearch에 직접 액세스하려면 루트 액세스가 필요합니다.

추가 수익 실적을

다음 질문은 BlueXP 분류 사용과 관련된 라이센스 및 비용에 관한 것입니다.

BlueXP 분류 비용은 얼마입니까**?**

BlueXP 분류 사용 비용은 스캔 중인 데이터의 양에 따라 달라집니다. BlueXP 작업 공간에서 BlueXP 분류 검사를 수행하는 첫 1TB의 데이터는 30일간 무료로 제공됩니다. 두 한계 중 하나에 도달한 후 데이터 스캔을 계속하려면 다음 중 하나가 필요합니다.

- 클라우드 공급업체의 BlueXP Marketplace 목록 가입 또는
- BYOL(Bring-Your-Own-License) 방식으로 NetApp의 BYOL(Bring-Your-License

을 참조하십시오 "가격" 를 참조하십시오.

BYOL 용량 제한에 도달하면 어떻게 됩니까**?**

BYOL 용량 제한에 도달하면 BlueXP 분류가 계속 실행되지만 스캔된 데이터에 대한 정보를 볼 수 없도록 대시보드에 대한 액세스가 차단됩니다. 라이센스 한도 내에서 용량 사용을 잠재적으로 가져오기 위해 스캔되는 볼륨 수를 줄이려는 경우 구성 페이지만 사용할 수 있습니다. BlueXP 분류에 대한 전체 액세스 권한을 회복하려면 BYOL 라이센스를 갱신해야 합니다.

커넥터 전개

다음 질문은 BlueXP 커넥터와 관련이 있습니다.

커넥터란 무엇입니까**?**

Connector는 클라우드 계정 또는 온프레미스 컴퓨팅 인스턴스에서 실행되는 소프트웨어로, BlueXP에서 클라우드 리소스를 안전하게 관리할 수 있도록 지원합니다. BlueXP 분류를 사용하려면 커넥터를 배포해야 합니다.

커넥터를 어디에 설치해야 합니까**?**

- AWS의 Cloud Volumes ONTAP, ONTAP용 Amazon FSx 또는 AWS S3 버킷에서 데이터를 스캔할 때는 AWS의 커넥터를 사용합니다.
- Azure 또는 Azure NetApp Files의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 Azure의 커넥터를 사용합니다.
- GCP의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 GCP의 커넥터를 사용합니다.
- 사내 ONTAP 시스템, 타사 파일 공유, 범용 S3 오브젝트 스토리지, 데이터베이스, OneDrive 폴더, SharePoint 계정, Google Drive 계정에서 데이터를 스캔할 경우 이러한 클라우드 위치 중 아무 곳에서나 커넥터를 사용할 수 있습니다.

따라서 여러 위치에 데이터가 있는 경우 를 사용해야 할 수 있습니다 "다중 커넥터".

BlueXP 분류를 수행하려면 자격 증명에 액세스해야 합니까**?**

BlueXP 분류 자체는 스토리지 자격 증명을 검색하지 않습니다. BlueXP Connector에 저장됩니다.

BlueXP 분류에서는 스캔 전에 CIFS 자격 증명을 사용하여 공유를 마운트하는 등의 데이터 플레인 자격 증명을 사용합니다.

내 호스트에 커넥터를 배포할 수 있습니까**?**

예. 가능합니다 "Connector를 온-프레미스에 배포합니다" 네트워크의 Linux 호스트 또는 클라우드의 호스트 BlueXP 분류를 사내 배포하려는 경우 Connector를 온-프레미스에도 설치할 수 있지만 반드시 필요한 것은 아닙니다.

서비스와 커넥터 간의 통신이 **HTTP**를 사용합니까**?**

예, BlueXP 분류는 HTTP를 사용하여 BlueXP Connector와 통신합니다.

인터넷에 연결되지 않은 보안 사이트는 어떻게 됩니까**?**

예, 지원합니다. 가능합니다 "인터넷에 액세스할 수 없는 온프레미스 Linux 호스트에 커넥터를 배포합니다". "이를

"비공개 모드"라고도 합니다.". 그런 다음 사내 ONTAP 클러스터와 기타 로컬 데이터 소스를 검색하고 BlueXP 분류를 사용하여 데이터를 검색할 수 있습니다.

BlueXP 분류 구축

다음 질문은 별도의 BlueXP 분류 인스턴스와 관련이 있습니다.

BlueXP 분류 기능은 어떤 배포 모델을 지원합니까**?**

BlueXP를 사용하면 온프레미스, 클라우드 및 하이브리드 환경을 비롯한 거의 모든 곳에서 시스템을 검색하고 보고할 수 있습니다. 일반적으로 BlueXP 분류는 서비스를 BlueXP 인터페이스를 통해 사용할 수 있고 하드웨어나 소프트웨어를 설치할 필요가 없는 SaaS 모델을 사용하여 배포됩니다. 이처럼 클릭-앤-런 구축 모드에서도 데이터 저장소가 온프레미스에 있든 퍼블릭 클라우드에 있든 상관없이 데이터 관리를 수행할 수 있습니다.

BlueXP 분류에 필요한 인스턴스 또는 **VM** 유형은 무엇입니까**?**

시기 "클라우드에 구축":

- AWS에서 BlueXP 분류는 500GiB GP2 디스크가 있는 m6i.4xLarge 인스턴스에서 실행됩니다. 배포 중에 더 작은 인스턴스 유형을 선택할 수 있습니다.
- Azure에서 BlueXP 분류는 500GiB 디스크를 사용하는 Standard_D16s_v3 VM에서 실행됩니다.
- GCP에서 BlueXP 분류는 500GiB 표준 영구 디스크를 사용하는 n2-standard-16 VM에서 실행됩니다.

CPU가 적고 RAM이 적은 시스템에 BlueXP 분류를 배포할 수 있지만 이러한 시스템을 사용할 때는 한계가 있습니다. 을 참조하십시오 "더 작은 인스턴스 유형 사용" 를 참조하십시오.

"BlueXP 분류의 작동 방식에 대해 자세히 알아보십시오".

자체 호스트에 **BlueXP** 분류를 배포할 수 있습니까**?**

예. 네트워크 또는 클라우드에서 인터넷에 액세스할 수 있는 Linux 호스트에 BlueXP 분류 소프트웨어를 설치할 수 있습니다. 모든 기능이 동일하며 BlueXP를 통해 스캔 구성 및 결과를 계속 관리할 수 있습니다. 을 참조하십시오 "구내 BlueXP 분류 배포" 시스템 요구 사항 및 설치 세부 정보를 확인하십시오.

인터넷에 연결되지 않은 보안 사이트는 어떻게 됩니까**?**

예, 지원합니다. 가능합니다 "인터넷에 액세스할 수 없는 사내 사이트에 BlueXP 분류를 배포합니다" 완전히 안전한 사이트를 위한 것입니다.

BlueXP 분류를 사용합니다

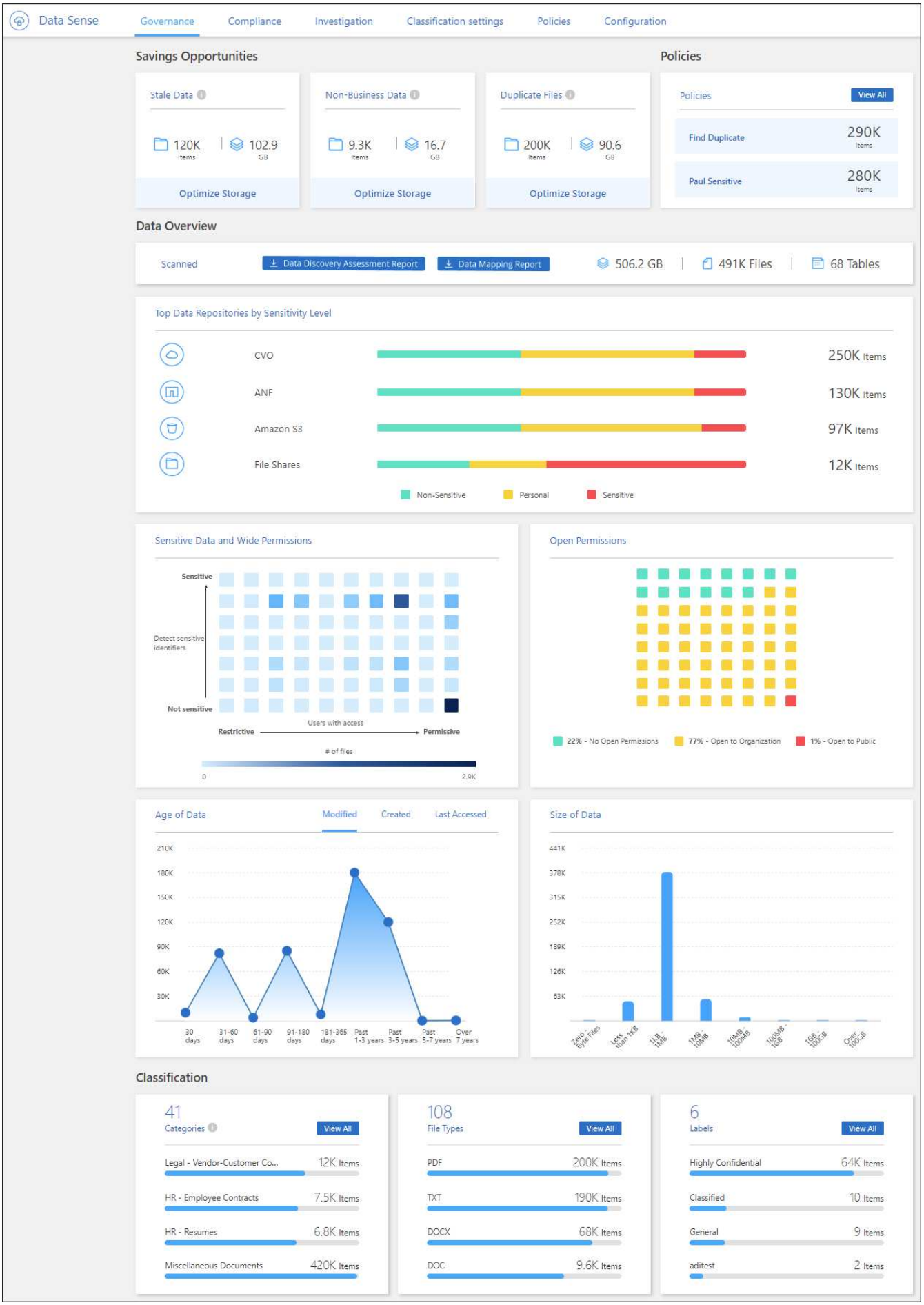
조직에 저장된 데이터에 대한 거버넌스 세부 정보를 봅니다

조직의 스토리지 리소스에 있는 데이터와 관련된 비용을 제어할 수 있습니다. BlueXP 분류는 시스템에 있는 오래된 데이터, 비업무용 데이터, 중복 파일 및 대용량 파일의 양을 식별하므로 일부 파일을 제거하거나 더 저렴한 오브젝트 스토리지에 계층화할 것인지 결정할 수 있습니다.

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

Governance 대시보드

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


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate 290K Items
Paul Sensitive 280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO 250K Items
ANF 130K Items
Amazon S3 97K Items
File Shares 12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co... 12K Items
HR - Employee Contracts 7.5K Items
HR - Resumes 6.8K Items
Miscellaneous Documents 420K Items
108
File Types
View All
PDF 200K Items
TXT 190K Items
DOCX 68K Items
DOC 9.6K Items
6
Labels
View All
Highly Confidential 64K Items
Classified 10 Items
General 9 Items
aditest 2 Items

기회 저장

삭제할 데이터가 있는지 또는 더 저렴한 오브젝트 스토리지에 계층화해야 하는지 여부를 확인하려면 *Saving Opportunities* 영역의 항목을 조사하십시오. 조사 페이지에서 필터링된 결과를 보려면 각 항목을 클릭합니다.

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

  참고

  데이터 소스 중 하나라도 데이터 계층화를 구현하는 경우 오브젝트 스토리지에 이미 있는 이전 데이터를 _st오래된 Data_category에서 식별할 수 있습니다.

결과 수가 가장 많은 정책입니다

Policies_영역에서 결과 수가 가장 많은 정책이 목록 맨 위에 나타납니다. 정책 이름을 클릭하여 조사 페이지에 결과를 표시합니다. 사용 가능한 모든 정책 목록을 보려면 * 모두 보기 * 를 클릭합니다.

을 클릭합니다 "여기" 정책에 대해 자세히 알아보십시오.

데이터 개요

Data Overview_ 섹션에서는 스캔되는 모든 데이터에 대한 간단한 개요를 제공합니다. 버튼을 클릭하여 모든 작업 환경 및 데이터 소스에 대한 사용 용량, 데이터 수명, 데이터 크기 및 파일 유형이 포함된 전체 데이터 매핑 보고서를 다운로드합니다. 을 참조하십시오 데이터 매핑 보고서 이 보고서에 대한 자세한 내용은 를 참조하십시오.

데이터 민감도에 따라 나열된 상위 데이터 리포지토리

Sensitivity Level_영역별 상위 데이터 리포지토리는 가장 중요한 항목을 포함하는 상위 4개의 데이터 저장소(작업 환경 및 데이터 원본)를 나열합니다. 각 작업 환경의 막대 차트는 다음과 같이 구분됩니다.

- 중요하지 않은 데이터입니다
- 개인 데이터
- 민감한 개인 데이터

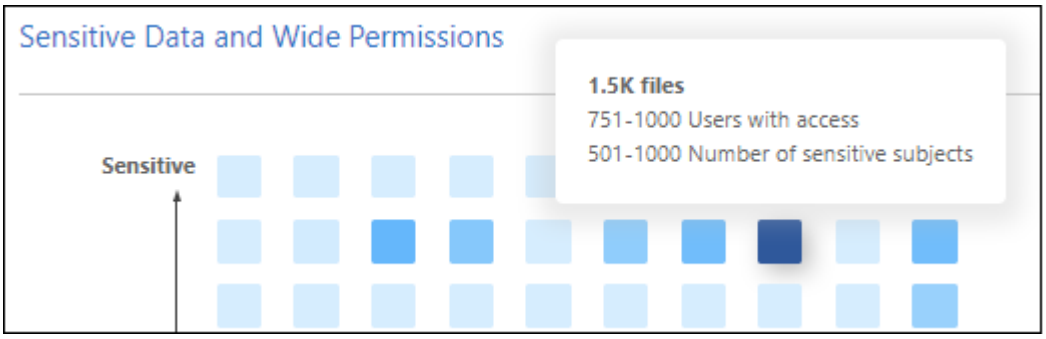
각 섹션 위로 마우스를 가져가면 각 범주의 총 항목 수를 볼 수 있습니다.

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

민감도 및 넓은 권한으로 나열된 데이터

중요한 데이터 및 광범위한 권한 영역 은 중요한 데이터(민감한 개인 데이터 및 민감한 개인 데이터 포함)를 포함하고 지나치게 허용적인 파일의 히트 맵을 제공합니다. 이렇게 하면 민감한 데이터와 관련하여 어떤 위험이 있을 수 있는지 확인할 수 있습니다.

파일 등급은 X축에 있는 파일에 액세스할 수 있는 권한이 있는 사용자 수(가장 낮음에서 가장 높음)와 Y축에 있는 파일 내의 중요한 식별자 수(가장 낮음에서 가장 높음)를 기준으로 합니다. 블럭은 X 및 Y 축의 항목과 일치하는 파일 수를 나타냅니다. 밝은 색상의 블록이 적합합니다. 더 적은 수의 사용자가 파일에 액세스할 수 있고 파일당 중요한 식별자는 더 적습니다. 어두운 블럭은 조사하려는 항목입니다. 예를 들어 아래 화면에는 짙은 파란색 블록의 호버 텍스트가 표시됩니다. 이 그림은 751-100명의 사용자가 액세스할 수 있는 1,500개의 파일이 있으며, 파일당 501-100개의 민감한 식별자가 있다는 것을 보여 줍니다.



원하는 블록을 클릭하여 조사 페이지에서 영향을 받는 파일의 필터링된 결과를 확인하여 더 자세히 조사할 수 있습니다.

BlueXP 분류와 ID 서비스를 통합하지 않은 경우 이 패널에 데이터가 표시되지 않습니다. "Active Directory 서비스를 BlueXP 분류와 통합하는 방법을 확인하십시오".

이 패널은 CIFS 공유, OneDrive 및 SharePoint 데이터 소스의 파일을 지원합니다. 현재 데이터베이스, Google Drive, Amazon S3, 일반 오브젝트 스토리지는 지원되지 않습니다.

열기 권한 유형별로 나열된 데이터

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

- 열기 권한이 없습니다
- 조직에 열기
- 공개
- 알 수 없는 액세스

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

데이터 기간 및 데이터 크기 그래프

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

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

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

참고

데이터 소스 중 하나라도 데이터 계층화를 구현하는 경우 오브젝트 스토리지에 이미 있는 이전 데이터를 _ Age of Data_graph에서 식별할 수 있습니다.

가장 많이 식별된 데이터 분류

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

범주

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

을 참조하십시오 "범주별로 파일 보기" 를 참조하십시오.

파일 형식

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

을 참조하십시오 "파일 형식 보기" 를 참조하십시오.

AIP 레이블

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

을 참조하십시오 "AIP 레이블" 를 참조하십시오.

데이터 매핑 보고서

데이터 매핑 보고서는 마이그레이션, 백업, 보안 및 규정 준수 프로세스를 결정하는 데 도움이 되도록 기업 데이터 소스에 저장되는 데이터에 대한 개요를 제공합니다. 이 보고서에는 먼저 모든 작업 환경 및 데이터 소스가 요약되어 있는 개요가 나열되며, 각 작업 환경에 대한 분석 정보가 제공됩니다.

보고서에는 다음 정보가 포함됩니다.

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

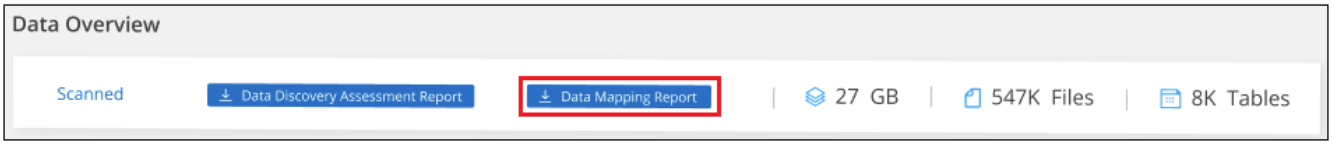
범주	설명
데이터 사용 기간	파일이 생성되거나, 마지막으로 수정되거나, 마지막으로 액세스된 시간에 대한 3개의 차트와 그래프를 제공합니다. 특정 날짜 범위를 기준으로 파일 수와 사용된 용량을 나열합니다.
데이터 크기	작업 환경의 특정 크기 범위 내에 있는 파일 수를 나열합니다.
파일 형식	에는 작업 환경에 저장되는 각 파일 유형의 총 파일 수와 사용된 용량이 나와 있습니다.

데이터 매핑 보고서를 생성합니다

BlueXP 분류의 Governance 탭에서 이 보고서를 생성합니다.

단계

1. BlueXP 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. Governance * 를 클릭한 다음 * Data Mapping Report * 버튼을 클릭합니다.



결과

BlueXP 분류는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

보고서가 1MB 이상인 경우 PDF 파일이 BlueXP 분류 인스턴스에 유지되고 정확한 위치에 대한 팝업 메시지가 표시됩니다. BlueXP 분류가 사내 Linux 시스템이나 클라우드에 배포한 Linux 시스템에 설치되어 있는 경우 PDF 파일로 직접 이동할 수 있습니다. 클라우드에 BlueXP 분류를 배포할 때 PDF 파일을 다운로드하려면 BlueXP 분류 인스턴스에 SSH를 사용해야 합니다. "Classification 인스턴스의 데이터에 액세스하는 방법을 확인하십시오".

참고: 을 클릭하여 보고서의 첫 페이지에 나타나는 회사 이름을 BlueXP 분류 페이지 상단에서 사용자 지정할 수 있습니다 ⋮ 그런 다음 * 회사 이름 변경 * 을 클릭합니다. 다음에 보고서를 생성할 때 새 이름이 포함됩니다.

데이터 검색 평가 보고서

Data Discovery Assessment Report는 스캔한 환경에 대한 상위 수준의 분석을 통해 시스템 결과를 강조하고 문제 영역 및 잠재적인 개선 단계를 보여 줍니다. 결과는 데이터의 매핑과 분류를 기반으로 합니다. 이 보고서의 목표는 데이터 세트의 다음과 같은 세 가지 중요한 측면에 대한 인식을 높이는 것입니다.

피처	설명
데이터 거버넌스 문제	소유하고 있는 모든 데이터와 비용을 절감할 수 있는 영역을 상세하게 보여줍니다.
데이터 보안 노출	광범위한 액세스 권한으로 내부 또는 외부 공격에 데이터에 액세스할 수 있는 영역입니다.
데이터 규정 준수 격차	개인 정보 또는 민감한 개인 정보가 보안 및 DSAR(데이터 주체 액세스 요청)을 위해 위치한 경우

평가 후에 이 보고서는 다음과 같은 분야를 식별합니다.

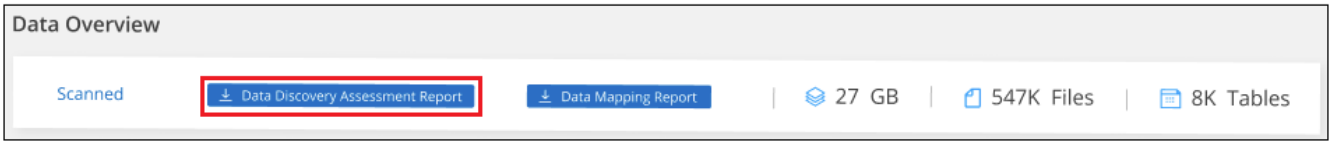
- 보존 정책을 변경하거나 특정 데이터(오래된 데이터, 중복 데이터 또는 비업무용 데이터)를 이동 또는 삭제하여 스토리지 비용 절감
- 전역 그룹 관리 정책을 수정하여 광범위한 사용 권한이 있는 데이터를 보호합니다
- PII를 보다 안전한 데이터 저장소로 이동하여 개인 또는 민감한 개인 정보가 있는 데이터를 보호합니다

데이터 검색 평가 보고서를 생성합니다

BlueXP 분류의 Governance 탭에서 이 보고서를 생성합니다.

단계

1. BlueXP 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. Governance * 를 클릭한 다음 * Data Discovery Assessment Report * 버튼을 클릭합니다.



결과

BlueXP 분류는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

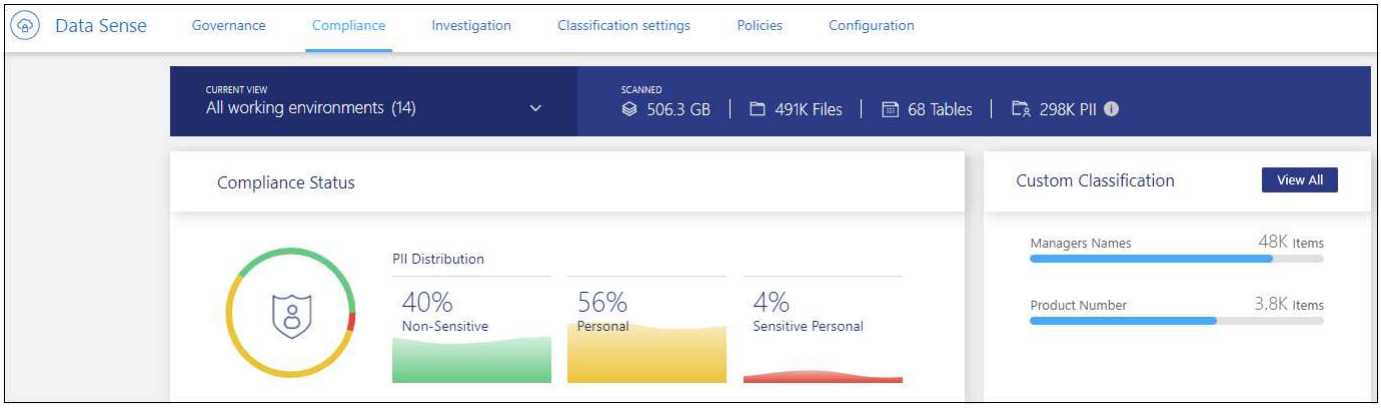
참고: 을 클릭하여 보고서의 첫 페이지에 나타나는 회사 이름을 BlueXP 분류 페이지 상단에서 사용자 지정할 수 있습니다 ⋮ 그런 다음 * 회사 이름 변경 * 을 클릭합니다. 다음에 보고서를 생성할 때 새 이름이 포함됩니다.

조직에 저장된 데이터에 대한 규정 준수 세부 정보를 봅니다

조직의 개인 데이터 및 민감한 개인 데이터에 대한 세부 정보를 확인하여 개인 데이터를 제어할 수 있습니다. 또한 데이터에 있는 BlueXP 분류의 범주 및 파일 형식을 검토하여 가시성을 확보할 수도 있습니다.

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

기본적으로 BlueXP 분류 대시보드에는 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터가 표시됩니다.



일부 작업 환경에 대한 데이터만 보려면 작업 환경을 선택합니다.

또한 데이터 조사 페이지에서 결과를 필터링하고 결과 보고서를 CSV 파일로 다운로드할 수도 있습니다. 을 참조하십시오 "데이터 조사 페이지의 데이터 필터링" 를 참조하십시오.

개인 데이터가 포함된 파일을 봅니다

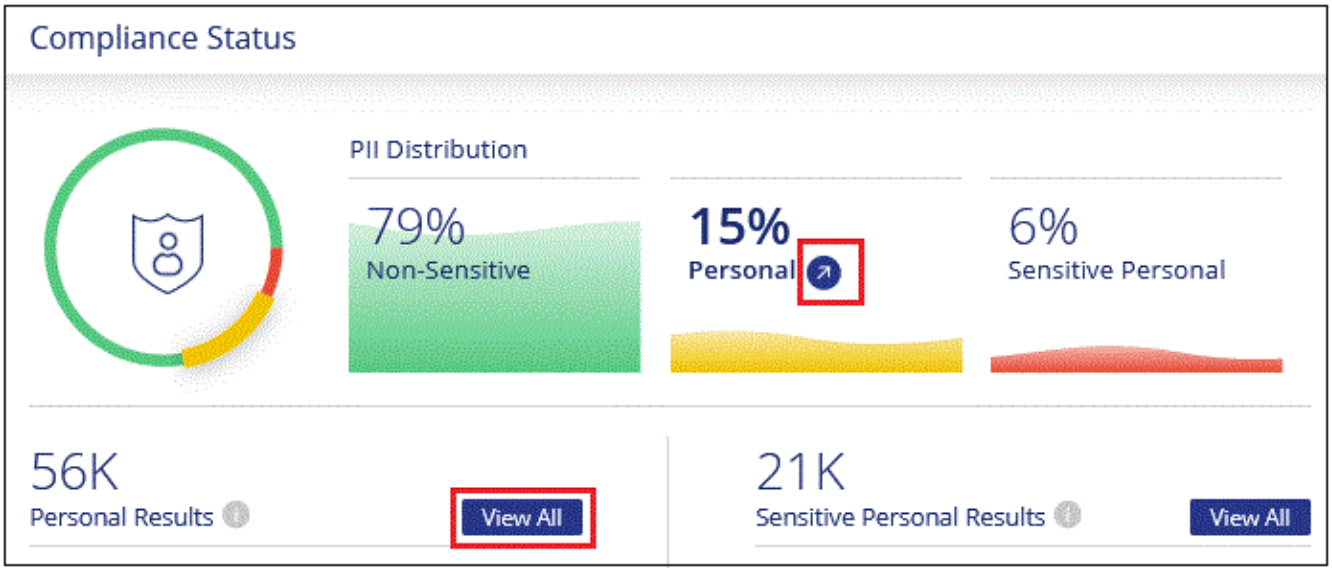
BlueXP 분류는 데이터 내에서 특정 단어, 문자열 및 패턴(Regex)을 자동으로 식별합니다. 예를 들어 개인 식별 정보(PII), 신용 카드 번호, 주민 등록 번호, 은행 계좌 번호, 암호, 있습니다. "전체 목록을 참조하십시오". BlueXP 분류는 디렉터리(공유 및 폴더) 내의 파일 및 데이터베이스 테이블에서 이러한 유형의 정보를 개별 파일에 식별합니다.

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

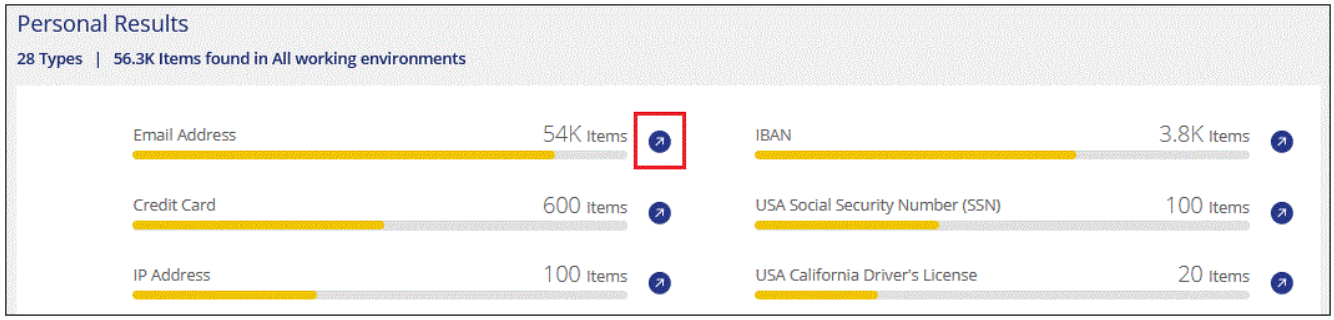
BlueXP 분류에서는 일부 유형의 개인 데이터에 대해 근접 검증_을 사용하여 결과를 검증합니다. 유효성 검사는 발견된 개인 데이터 근처에서 하나 이상의 미리 정의된 키워드를 찾는 방식으로 수행됩니다. 예를 들어, *BlueXP* 분류는 미국을 식별합니다 주민등록번호*(SSN)* 옆에 근접 단어가 있는 경우 주민등록번호로 사용 — 예*: _SSN_OR_Social security*. "개인 데이터 표" BlueXP 분류에서 근접 유효성 검사를 사용할 때 표시됩니다.

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 규정 준수 * 탭을 클릭합니다.
2. 모든 개인 데이터에 대한 세부 정보를 조사하려면 개인 데이터 백분율 옆에 있는 아이콘을 클릭합니다.

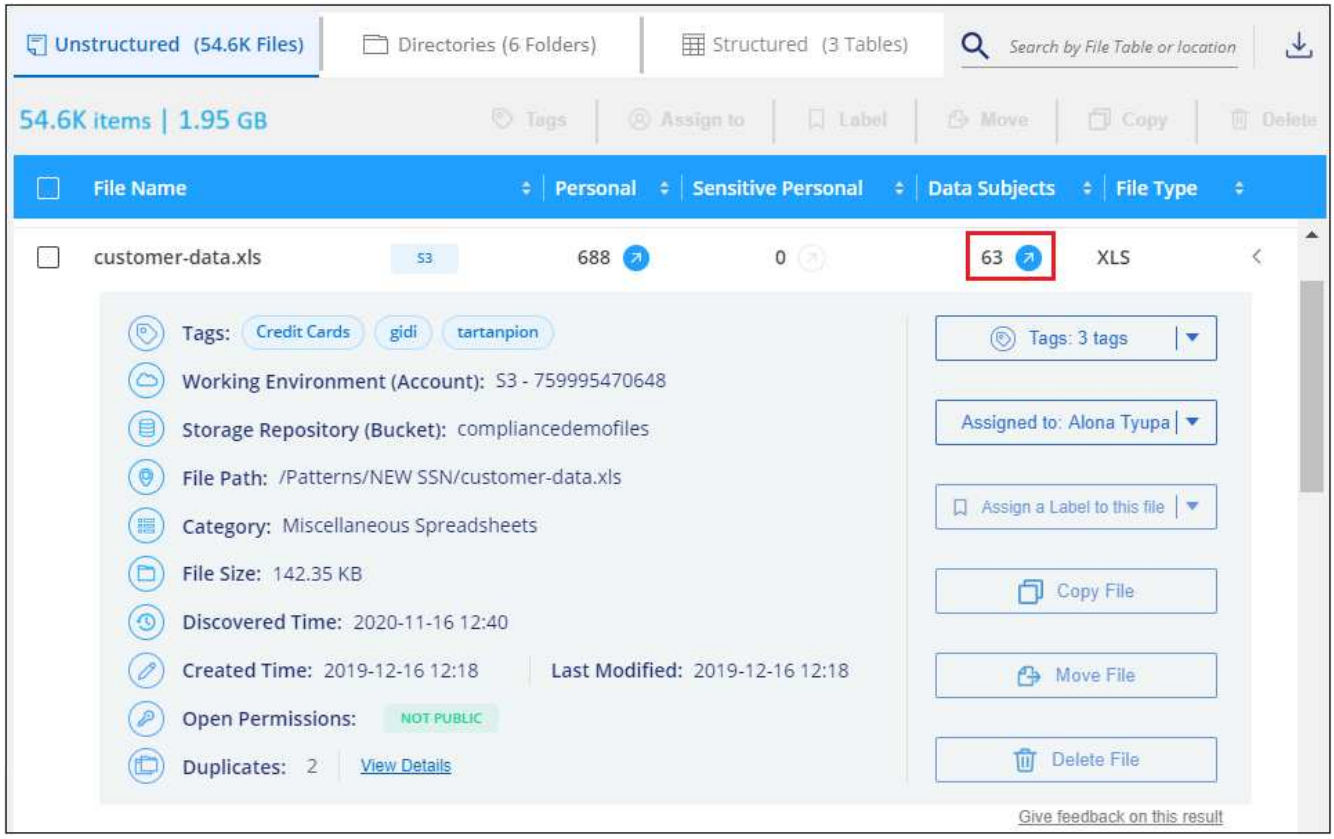


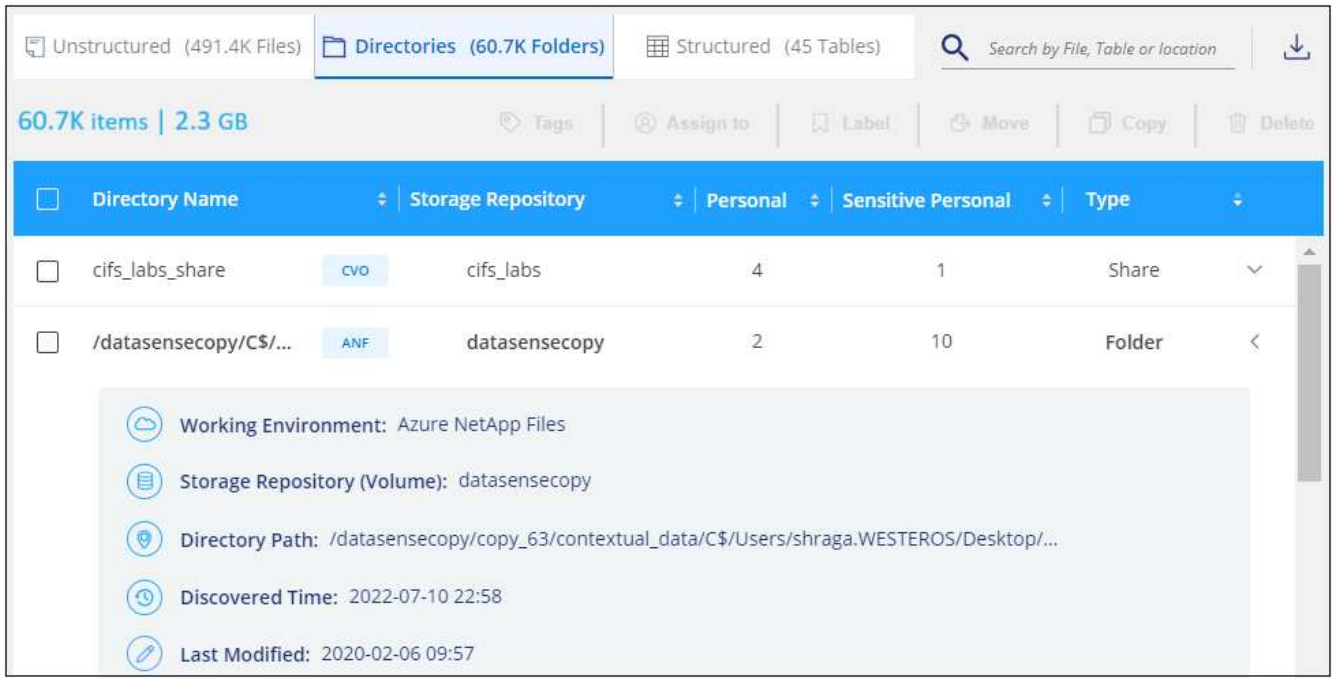
3. 특정 유형의 개인 데이터에 대한 세부 정보를 조사하려면 * 모두 보기 * 를 클릭한 다음 특정 유형의 개인 데이터(예: 전자 메일 주소)에 대한 * 조사 결과 * 아이콘을 클릭합니다.



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

   아래 스크린샷 2개는 개별 파일에서 찾은 개인 데이터를 보여 주고 디렉터리(공유 및 폴더) 내의 파일에서 찾을 수 있습니다. 또한 * Structured * (구조적 *) 탭을 선택하여 데이터베이스에서 찾은 개인 데이터를 볼 수도 있습니다.





중요한 개인 데이터가 포함된 파일을 봅니다

BlueXP 분류는 와 같은 개인 정보 보호 규정에 따라 민감한 개인 정보의 특수한 유형을 자동으로 식별합니다 "GDPR 9조 및 10조". 예를 들어, 개인의 건강, 인종 또는 성적 취향과 관련된 정보를 제공합니다. "전체 목록을 참조하십시오". BlueXP 분류는 디렉터리(공유 및 폴더) 내의 파일 및 데이터베이스 테이블에서 이러한 유형의 정보를 개별 파일에 식별합니다.

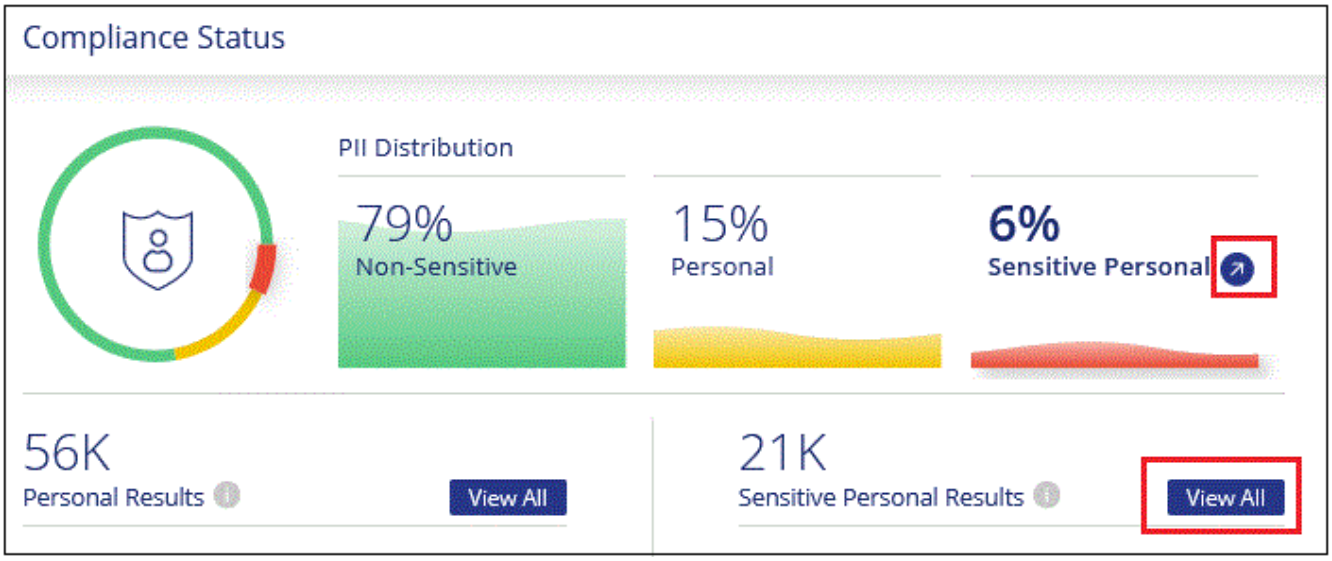
BlueXP 분류에서는 인공 지능(AI), 자연어 처리(NLP), 머신 러닝(ML) 및 인지 컴퓨팅(CC)을 사용하여 엔터티를 추출하고 그에 따라 범주화하기 위해 검색하는 내용의 의미를 파악합니다.

예를 들어, 중요한 GDPR 데이터 범주 중 하나는 인종입니다. BlueXP 분류는 NLP 기능으로 인해 "George is Mexican"(GDPR 제9조에 명시된 민감한 데이터를 나타냄)이라는 문장과 "George is Mexican food"라는 문장의 차이를 구별할 수 있습니다.

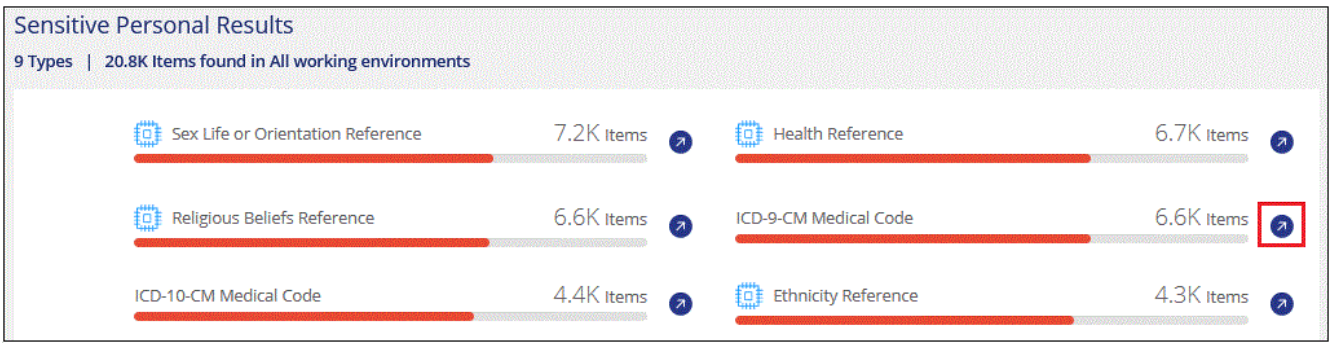
> 민감한 개인 데이터를 검색할 때는 영어로만 지원됩니다. 더 많은 언어에 대한 지원은 나중에 추가됩니다.

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 규정 준수 * 탭을 클릭합니다.
2. 중요한 모든 개인 데이터에 대한 세부 정보를 조사하려면 중요한 개인 데이터 백분율 옆에 있는 아이콘을 클릭합니다.



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



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

범주별로 파일을 봅니다

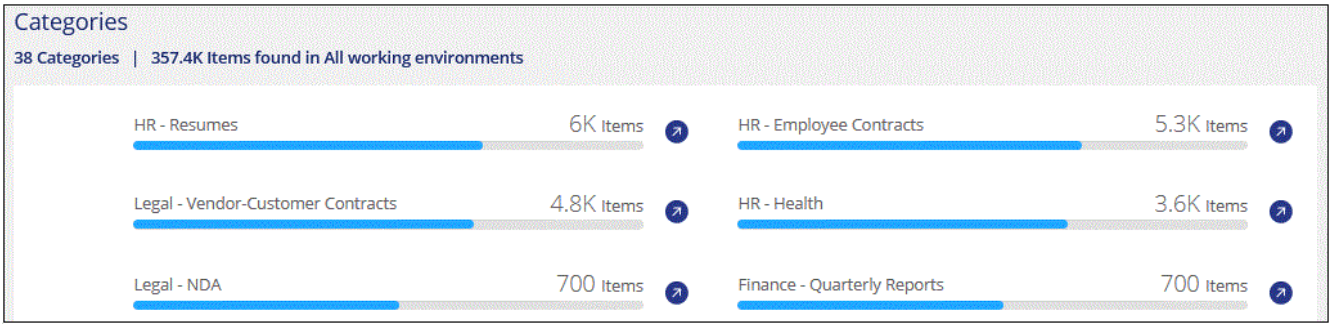
BlueXP 분류는 스캔한 데이터를 다른 유형의 범주로 나눕니다. 범주는 각 파일의 콘텐츠 및 메타데이터에 대한 AI 분석을 기반으로 하는 주제입니다. "범주 목록을 참조하십시오".

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

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

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 규정 준수 * 탭을 클릭합니다.
2. 기본 화면에서 직접 상위 4개 범주 중 하나에 대한 * 조사 결과 * 아이콘을 클릭하거나 * 모두 보기 * 를 클릭한 다음 범주 중 하나에 대한 아이콘을 클릭합니다.



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

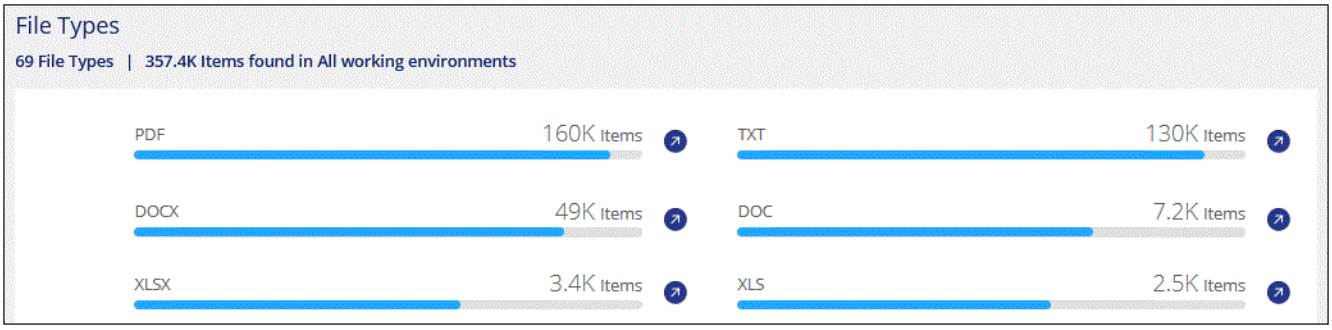
파일 형식별로 파일을 봅니다

BlueXP 분류는 스캔한 데이터를 파일 유형별로 분류하여 표시합니다. 파일 형식을 검토하면 특정 파일 형식이 올바르게 저장되지 않은 것을 발견할 수 있으므로 중요한 데이터를 제어하는 데 도움이 됩니다. "파일 형식 목록을 참조하십시오".

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

단계

1. BlueXP 왼쪽 탐색 메뉴에서 * 거버넌스 > 분류 * 를 클릭한 다음 * 규정 준수 * 탭을 클릭합니다.
2. 기본 화면에서 직접 상위 4개 파일 유형 중 하나에 대한 * 조사 결과 * 아이콘을 클릭하거나 * 모두 보기 * 를 클릭한 다음 파일 유형에 대한 아이콘을 클릭합니다.



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

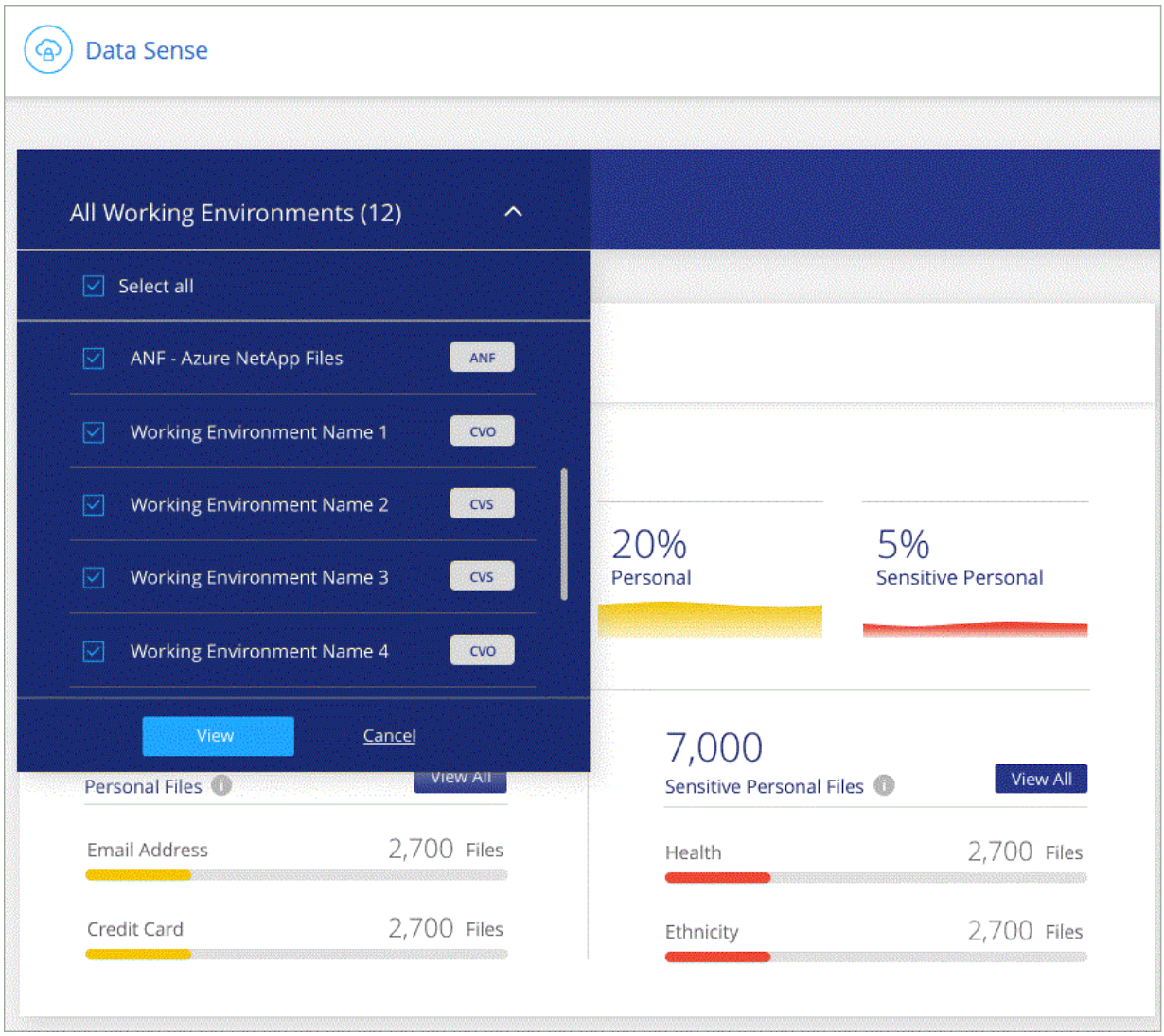
특정 작업 환경에 대한 대시보드 데이터를 봅니다

BlueXP 분류 대시보드의 내용을 필터링하여 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터를 보거나 특정 작업 환경에 대한 규정 준수 데이터를 확인할 수 있습니다.

대시보드를 필터링할 때 BlueXP 분류는 규정 준수 데이터와 보고서를 선택한 작업 환경에만 설정합니다.

단계

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



개인 데이터의 범주입니다

볼륨, Amazon S3 버킷, 데이터베이스, OneDrive 폴더, SharePoint 계정에서 BlueXP 분류가 식별할 수 있는 여러 유형의 개인 데이터가 있습니다. Google Drive 계정을 만듭니다. 아래 범주를 참조하십시오.

> 다른 개인 데이터 유형(예: 추가 국가 ID 번호 또는 의료 식별자)을 식별하기 위해 BlueXP 분류가 필요한 경우, 요청 시 ng-contact-data-sense@netapp.com 으로 이메일을 보내십시오.

개인 데이터의 유형입니다

파일에서 발견된 개인 데이터는 일반 개인 데이터 또는 국가 식별자일 수 있습니다. 아래 표의 세 번째 열은 BlueXP 분류의 사용 여부를 나타냅니다 "근접 확인" 식별자에 대한 결과를 검증합니다.

이러한 항목을 인식할 수 있는 언어는 테이블에서 식별됩니다.

참고: 파일에 있는 개인 데이터 목록에 추가할 수 있습니다. 데이터베이스 서버를 검색하는 경우, *Data Fusion* 기능을 사용하면 데이터베이스 테이블에서 열을 선택하여 BlueXP 분류에서 검색할 추가 식별자를 선택할 수 있습니다. 텍스트

파일의 사용자 지정 키워드를 추가하거나 정규식을 사용하여 사용자 지정 패턴을 추가할 수도 있습니다. 을 참조하십시오 "BlueXP 분류 스캔에 개인 데이터 ID를 추가합니다" 를 참조하십시오.

유형	**ID**입니다	근접성 검증**?**	영어	독일어	스페인어	프랑스어	일본어
일반	신용 카드 번호입니다	아니요	✓	✓	✓		✓
	데이터 제목	아니요	✓	✓	✓		
	이메일 주소	아니요	✓	✓	✓		✓
	IBAN 번호(국제 은행 계좌 번호)	아니요	✓	✓	✓		✓
	IP 주소	아니요	✓	✓	✓		✓
	암호	예	✓	✓	✓		✓

유형	**ID**입니다	근접성 검증**?**	영어	독일어	스페인어	프랑스어	일본어
국가 식별자							
138							

유형	ID입니다	근접성 검증?	영어	독일어	스페인어	프랑스어	일본어
	이탈리아 세금 식별 번호	예	✓	✓	✓		
	일본 개인 식별 번호(개인 및 법인)	예	✓	✓	✓		✓
	라트비아어 ID	예	✓	✓	✓		
	리투아니아어 ID	예	✓	✓	✓		
	룩셈부르크 ID입니다	예	✓	✓	✓		
	몰타 ID	예	✓	✓	✓		
	NHS(National Health Service) 번호	예	✓	✓	✓		
	뉴질랜드 은행 계좌	예	✓	✓	✓		
	뉴질랜드 운전면허증	예	✓	✓	✓		
	뉴질랜드 IRD 번호(세금 ID)	예	✓	✓	✓		
	뉴질랜드 NHI(National Health Index) 번호	예	✓	✓	✓		
	뉴질랜드 여권 번호	예	✓	✓	✓		
	폴란드어 ID(PESEL)	예	✓	✓	✓		
	포르투갈어 세금 식별 번호(NIF)	예	✓	✓	✓		
	루마니아어 ID(CNP)	예	✓	✓	✓		
	싱가포르 국가 등록 ID 카드(NRIC)	예	✓	✓	✓		
	슬로베니아어 ID(EMSO)	예	✓	✓	✓		
	남아프리카 ID	예	✓	✓	✓		
	스페인어 세금 식별 번호	예	✓	✓	✓		
	스웨덴 iD	예	✓	✓	✓		
	Texas Driver의 라이센스	예	✓	✓	✓		
	영국 ID(Nino)	예	✓	✓	✓		
	미국 캘리포니아 운전면허증	예	✓	✓	✓		
	미국 인디애나 운전면허증	예	✓	✓	✓		
	미국 뉴욕 운전면허증	예	✓	✓	✓		
	미국 주민등록번호	예	✓	✓	✓		

중요한 개인 데이터의 유형

BlueXP 분류가 파일에서 찾을 수 있는 중요한 개인 데이터에는 다음 목록이 포함됩니다.

이 범주의 항목은 현재 영어로만 인식할 수 있습니다.

형사 절차 참조

자연인의 범죄 소신 및 범죄에 관한 데이터.

인종 참조
: 자연인의 인종 또는 민족에 관한 데이터.

상태 참조
: 자연인의 건강에 관한 데이터.

ICD-9-cm 의료 코드
: 의료 및 의료 산업에서 사용되는 코드.

ICD-10-CM 의료 코드
: 의료 및 의료 산업에서 사용되는 코드.

철학적 신념 기준
: 자연인의 철학적 신념에 관한 데이터.

정치적 견해 참조
: 자연인의 정치적 의견에 관한 자료.

종교적 신념 참조
: 자연인의 종교적 신념에 관한 데이터.

성생활 또는 오리엔테이션 참조
: 자연인의 성생활 또는 성적 취향과 관련된 데이터.

범주 유형

BlueXP 분류는 다음과 같이 데이터를 분류합니다.

이러한 범주의 대부분은 영어, 독일어 및 스페인어로 인정될 수 있습니다.

범주	유형	영어	독일어	스페인어
재무	밸런스 시트	✓	✓	✓
	구매 주문	✓	✓	✓
	인보이스	✓	✓	✓
	분기별 보고서	✓	✓	✓
시간	배경 확인	✓		✓
	보상 계획	✓	✓	✓
	직원 계약	✓		✓
	직원 검토	✓		✓
	상태	✓		✓
	다시 시작합니다	✓	✓	✓
법적 고지	NDAS	✓	✓	✓
	공급업체 - 고객 계약	✓	✓	✓

범주	유형	영어	독일어	스페인어
마케팅	캠페인	✓	✓	✓
	회의	✓	✓	✓
운영	감사 보고서	✓	✓	✓
판매	판매 주문	✓	✓	
서비스	RFI	✓		✓
	RFP	✓		✓
	SOW	✓	✓	✓
	교육	✓	✓	✓
지원	불만 및 티켓	✓	✓	✓

다음 메타데이터도 분류되어 동일한 지원 언어로 식별됩니다.

- 애플리케이션 데이터
- 파일 보관
- 오디오
- 비즈니스 애플리케이션 데이터
- CAD 파일
- 코드
- 손상되었습니다
- 데이터베이스 및 인덱스 파일
- BlueXP 분류 브레드크럼입니다
- 설계 파일
- 이메일 애플리케이션 데이터
- 암호화(엔트로피 점수가 높은 파일)
- 실행 파일
- 재무 애플리케이션 데이터
- 상태 응용 프로그램 데이터
- 이미지
- 로그
- 기타 문서
- 기타 프레젠테이션
- 기타 스프레드시트
- 기타 "알 수 없음"
- 암호로 보호된 파일
- 정형 데이터

- 비디오
- 0바이트 파일

파일 유형

BlueXP 분류는 모든 파일에서 범주 및 메타데이터 정보를 검색하고 대시보드의 파일 형식 섹션에 모든 파일 형식을 표시합니다.

그러나 BlueXP 분류에서 PII(개인 식별 정보)를 감지하거나 DSAR 검색을 수행할 때는 다음 파일 형식만 지원됩니다.

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

정보가 정확합니다

NetApp은 BlueXP의 분류 체계에서 식별할 수 있는 개인 데이터와 민감한 개인 데이터의 100% 정확성을 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 확인해야 합니다.

테스트를 기준으로 아래 표는 BlueXP 분류에서 발견한 정보의 정확성을 보여줍니다. 정밀 _ 및 _ 리콜 _ 을(를) 통해 분해합니다.

정밀도

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

리콜

BlueXP 분류 시 필요한 사항을 찾을 수 있는 확률입니다. 예를 들어, 개인 데이터의 리콜 비율이 70%이면 BlueXP 분류에서 조직에 개인 정보가 실제로 포함된 10개 파일 중 7개를 식별할 수 있습니다. BlueXP 분류는 데이터의 30%를 놓칠 수 있으며 대시보드에 표시되지 않습니다.

우리는 결과의 정확성을 지속적으로 개선하고 있습니다. 이러한 개선 사항은 향후 BlueXP 분류 릴리스에서 자동으로 제공됩니다.

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

조직에 저장된 데이터를 조사합니다

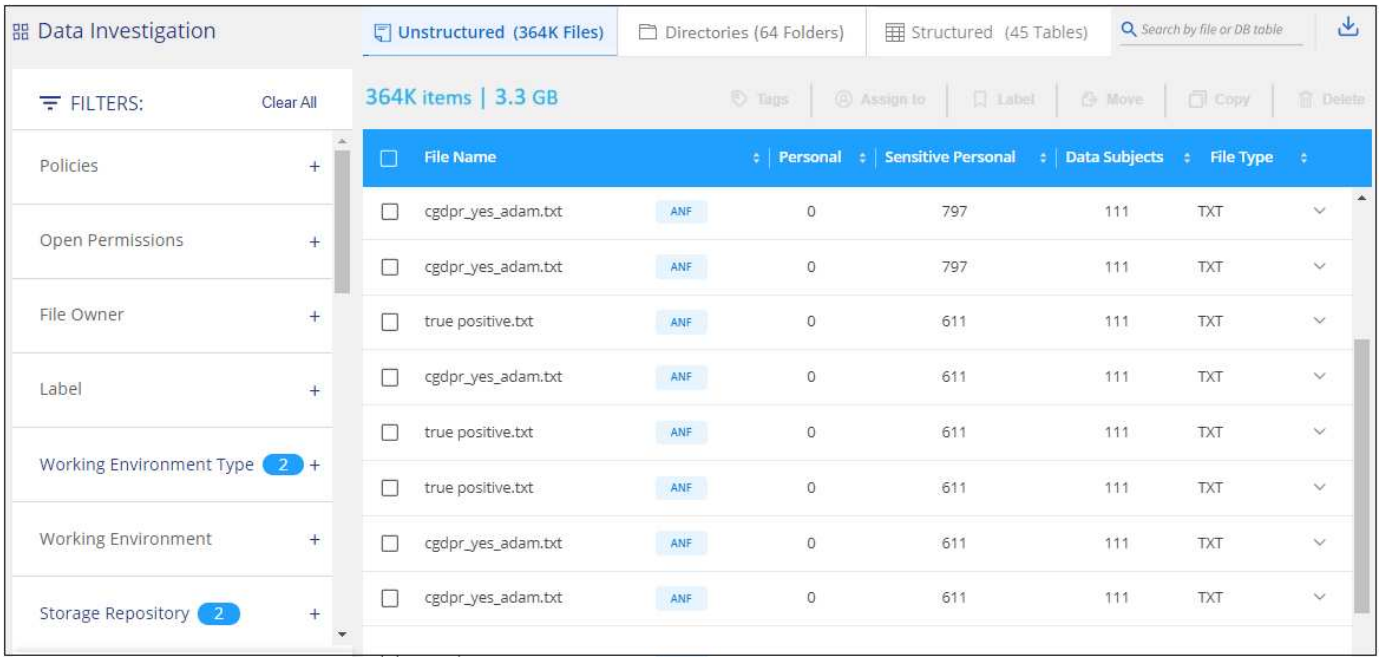
데이터 조사 페이지에서 세부 정보를 확인하여 조직의 데이터를 조사할 수 있습니다. Governance and Compliance 대시보드를 비롯한 BlueXP 분류 UI의 여러 영역에서 이 페이지로 이동할 수 있습니다.

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

데이터 조사 페이지에서 데이터를 필터링합니다

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

페이지 내용을 구체화한 후 보고서로 다운로드하려면 을 클릭합니다 단추를 클릭합니다. 데이터 조사 보고서에 대한 자세한 내용은 여기 를 참조하십시오.



- 최상위 탭을 사용하면 파일(비정형 데이터), 디렉토리(폴더 및 파일 공유) 또는 데이터베이스(정형 데이터)에서 데이터를 볼 수 있습니다.
- 각 열의 맨 위에 있는 컨트롤을 사용하여 결과를 숫자 또는 알파벳 순서로 정렬할 수 있습니다.
- 왼쪽 창 필터를 사용하면 다음 섹션에서 설명하는 속성을 선택하여 결과를 구체화할 수 있습니다.

민감도와 내용별로 데이터를 필터링합니다

다음 필터를 사용하여 데이터에 포함된 중요한 정보의 양을 확인할 수 있습니다.

필터	세부 정보
범주	를 선택합니다 "범주 유형".
감도 수준	감도 수준(개인, 민감한 개인 또는 민감하지 않음)을 선택합니다.

필터	세부 정보
식별자 수입니다	파일당 감지된 중요 식별자의 범위를 선택합니다. 개인 데이터 및 민감한 개인 데이터가 포함됩니다. 디렉터리에서 필터링할 때 BlueXP 분류는 각 폴더(및 하위 폴더)의 모든 파일에서 일치하는 항목의 합계를 구합니다. 참고: 2023년 12월(버전 1.26.6) 릴리스는 디렉토리에서 PII(개인 식별 정보) 데이터의 수를 계산하는 옵션을 일시적으로 제거했습니다.
개인 데이터	를 선택합니다 "개인 데이터의 유형입니다".
민감한 개인 데이터	를 선택합니다 "중요한 개인 데이터의 유형".
데이터 제목	데이터 주체의 전체 이름 또는 알려진 식별자를 입력합니다. "여기에서 데이터 주제에 대해 자세히 알아보십시오".

사용자 소유자 및 사용자 권한별로 데이터를 필터링합니다

다음 필터를 사용하여 파일 소유자 및 데이터 액세스 권한을 볼 수 있습니다.

필터	세부 정보
사용 권한을 엽니다	데이터 및 폴더/공유 내에서 사용 권한 유형을 선택합니다.
사용자/그룹 권한	하나 이상의 사용자 이름 및/또는 그룹 이름을 선택하거나 부분 이름을 입력합니다.
파일 소유자	파일 소유자 이름을 입력합니다.
액세스 권한이 있는 사용자 수입니다	특정 수의 사용자에게 열려 있는 파일과 폴더를 표시하려면 하나 이상의 범주 범위를 선택합니다.

시간별 데이터 필터링

다음 필터를 사용하여 시간 기준에 따라 데이터를 봅니다.

필터	세부 정보
만든 시간	파일이 생성된 시간 범위를 선택합니다. 또한 사용자 지정 시간 범위를 지정하여 검색 결과를 더욱 구체화할 수도 있습니다.
검색된 시간	BlueXP 분류에서 파일을 검색할 시간 범위를 선택합니다. 또한 사용자 지정 시간 범위를 지정하여 검색 결과를 더욱 구체화할 수도 있습니다.
마지막 수정	파일을 마지막으로 수정한 시간 범위를 선택합니다. 또한 사용자 지정 시간 범위를 지정하여 검색 결과를 더욱 구체화할 수도 있습니다.
마지막 액세스	파일 또는 디렉토리(CIFS 또는 NFS만 해당)를 마지막으로 액세스한 시간 범위를 선택합니다. 또한 사용자 지정 시간 범위를 지정하여 검색 결과를 더욱 구체화할 수도 있습니다. BlueXP 분류 검사에서 검사하는 파일 유형의 경우, BlueXP 분류에서 파일을 마지막으로 검사한 것입니다. BlueXP 분류는 SharePoint Online, SharePoint 온-프레미스(SharePoint Server), OneDrive, Google Drive 및 Amazon S3의 데이터 원본에서 "마지막 액세스 시간"을 추출하지 않습니다.

메타데이터를 기준으로 데이터를 필터링합니다

다음 필터를 사용하여 위치, 크기, 디렉터리 또는 파일 형식에 따라 데이터를 볼 수 있습니다.

필터	세부 정보
파일 경로	쿼리에서 포함하거나 제외할 부분 경로 또는 전체 경로를 최대 20개까지 입력합니다. 경로 포함 및 제외 경로를 모두 입력하면 BlueXP 분류에서 포함된 경로의 모든 파일을 먼저 찾은 다음 제외된 경로에서 파일을 제거한 다음 결과를 표시합니다. 이 필터에서 " * "를 사용하면 아무런 영향이 없으며 검색에서 특정 폴더를 제외할 수 없습니다. 구성된 공유 아래에 있는 모든 디렉토리와 파일이 검색됩니다.
디렉터리 유형	"공유" 또는 "폴더"와 같은 디렉토리 유형을 선택합니다.
파일 형식	를 선택합니다 "파일 유형".
파일 크기	파일 크기 범위를 선택합니다.
파일 해시	파일 해시를 입력하여 이름이 다르더라도 특정 파일을 찾습니다.

스토리지 유형별로 데이터를 필터링합니다

다음 필터를 사용하여 스토리지 유형별로 데이터를 봅니다.

필터	세부 정보
작업 환경 유형	작업 환경의 유형을 선택합니다. OneDrive, SharePoint 및 Google Drive는 "앱"으로 분류됩니다.
작업 환경 이름	특정 작업 환경을 선택합니다.
저장소 저장소	볼륨 또는 스키마와 같은 스토리지 리포지토리를 선택합니다.

태그, 레이블, 할당된 사용자 및 정책을 기준으로 데이터를 필터링합니다

다음 필터를 사용하여 AIP 레이블 또는 태그로 데이터를 봅니다.

필터	세부 정보
정책	정책 또는 정책을 선택합니다. 이동 "여기" 기존 정책 목록을 보고 고유한 사용자 지정 정책을 만들려면
라벨	를 선택합니다 "AIP 레이블" 파일에 할당됩니다.
태그	를 선택합니다 "태그 또는 태그" 파일에 할당됩니다.
할당 대상	파일이 할당된 사람의 이름을 선택합니다.

분석 상태별로 데이터를 필터링합니다

다음 필터를 사용하여 BlueXP 분류 스캔 상태별 데이터를 봅니다.

필터	세부 정보
분석 상태	옵션을 선택하여 보류 중인 첫 번째 스캔, 완료된 스캔, 보류 중인 재스캔 또는 스캔하지 않은 파일 목록을 표시합니다.

필터	세부 정보
스캔 분석 이벤트	BlueXP 분류로 마지막으로 액세스한 시간을 되돌릴 수 없어 분류되지 않은 파일을 볼 것인지, 아니면 BlueXP 분류로 마지막으로 액세스한 시간을 되돌릴 수 없더라도 분류된 파일을 볼 것인지 선택합니다.

""마지막 액세스 시간" 타임스탬프에 대한 세부 정보를 봅니다" 스캔 분석 이벤트를 사용하여 필터링할 때 조사 페이지에 표시되는 항목에 대한 자세한 내용은 을 참조하십시오.

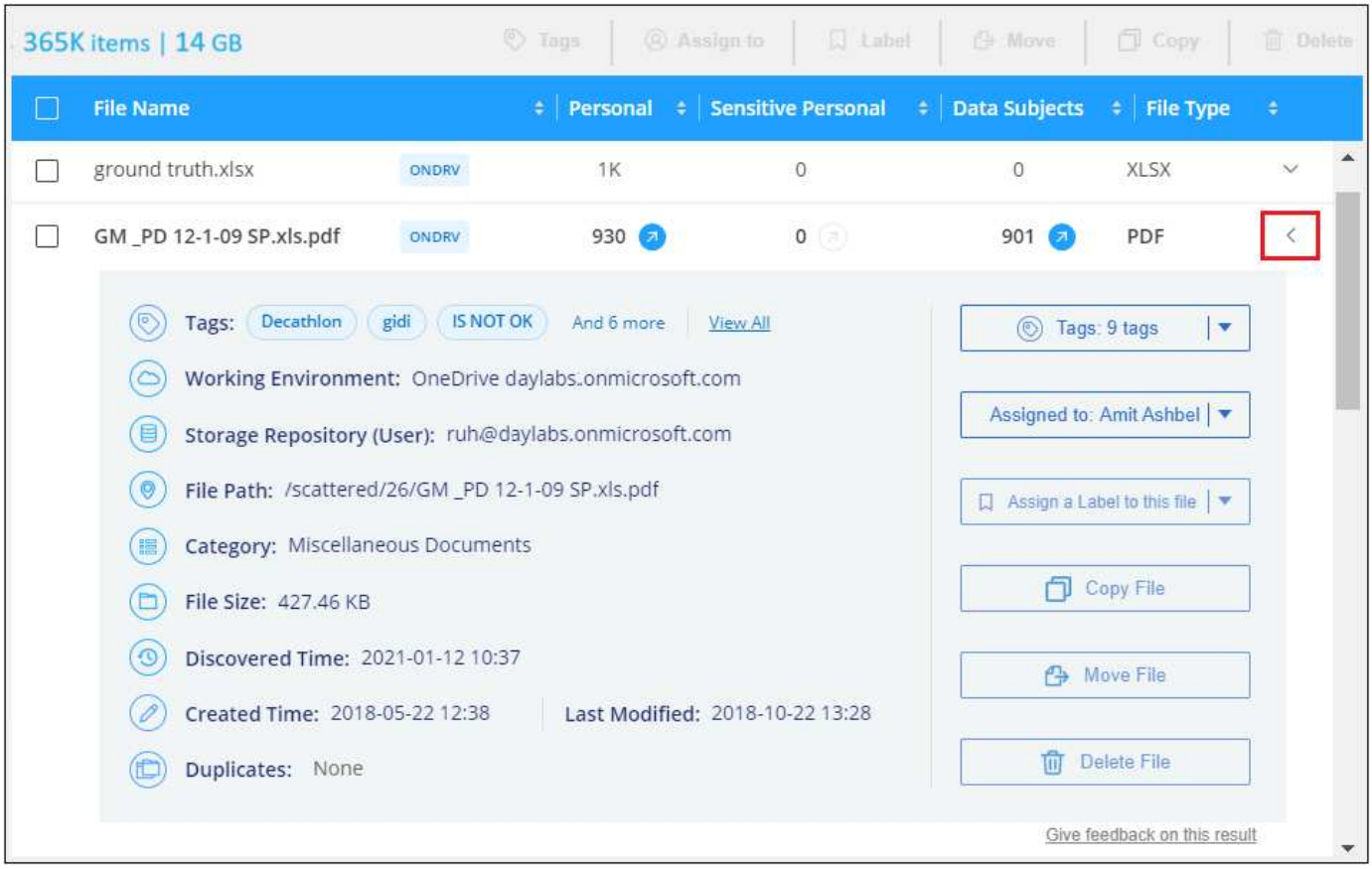
데이터를 중복으로 필터링합니다

다음 필터를 사용하여 스토리지에 복제된 파일을 봅니다.

필터	세부 정보
중복	파일이 리포지토리에서 복제되는지 여부를 선택합니다.

파일 메타데이터 보기

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



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

모든 데이터 원본에 대해 모든 정보를 사용할 수 있는 것은 아니며 해당 데이터 원본에 적합한 정보일 뿐입니다. 예를

들어 볼륨 이름, 권한 및 AIP 레이블은 데이터베이스 파일과 관련이 없습니다.

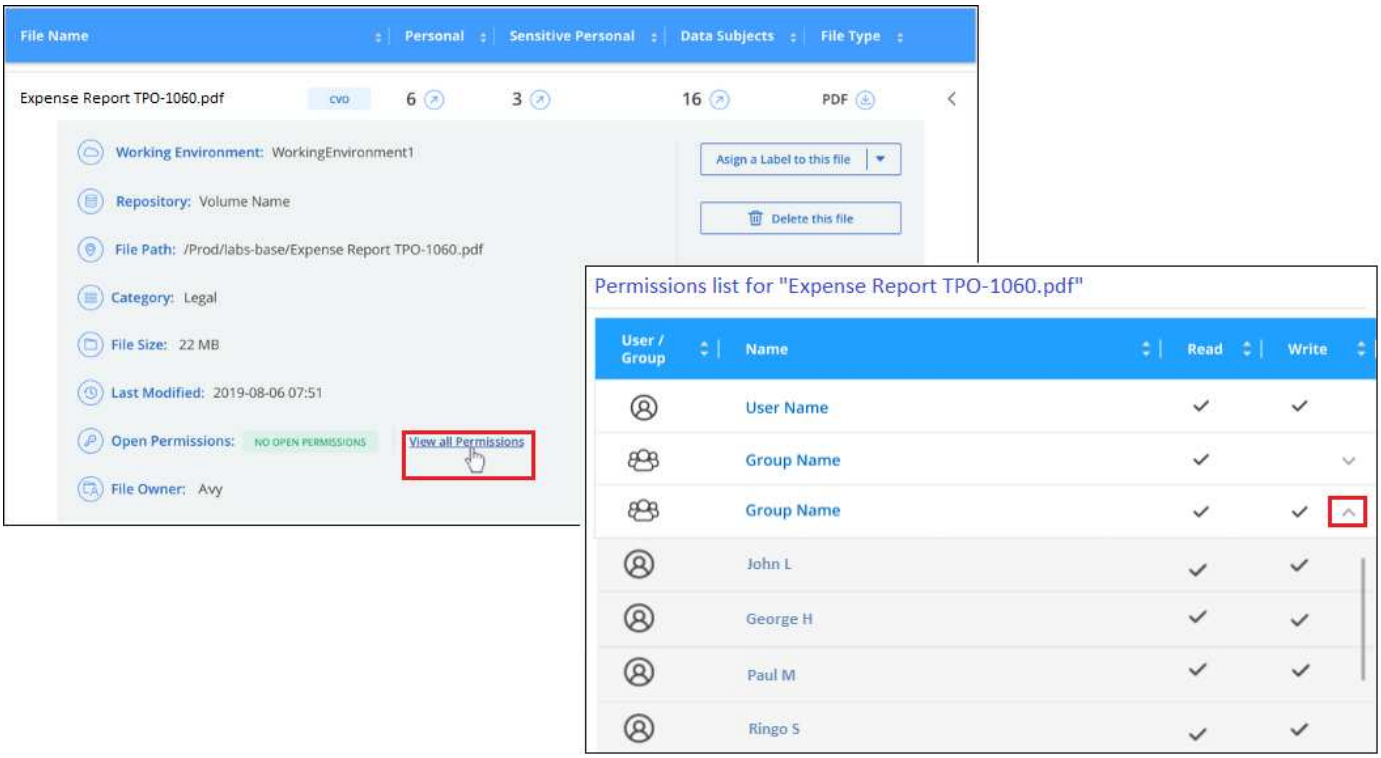
단일 파일의 세부 정보를 볼 때 파일에 대해 수행할 수 있는 몇 가지 작업이 있습니다.

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

파일 및 디렉터리에 대한 사용 권한을 봅니다

파일이나 디렉터리에 액세스할 수 있는 모든 사용자 또는 그룹의 목록과 해당 권한이 있는 권한 유형을 보려면 * 모든 권한 보기 * 를 클릭합니다. 이 단추는 CIFS 공유, SharePoint Online, SharePoint On-Premise 및 OneDrive의 데이터에만 사용할 수 있습니다.

사용자 및 그룹 이름 대신 SID(보안 식별자)가 표시되는 경우 Active Directory를 BlueXP 분류에 통합해야 합니다. "이 작업을 수행하는 방법을 확인하십시오".



를 클릭할 수 있습니다 ⌄ 모든 그룹에 대해 그룹에 속한 사용자 목록을 표시합니다.

또한, 사용자 또는 그룹의 이름을 클릭하면 "사용자/그룹 권한" 필터에 입력된 사용자 또는 그룹의 이름과 함께 조사 페이지가 표시되어 사용자 또는 그룹이 액세스할 수 있는 모든 파일 및 디렉터리를 볼 수 있습니다.

스토리지 시스템에 중복된 파일이 있는지 확인합니다

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

1MB 이상의 개인 정보나 중요한 개인 정보가 포함된 모든 파일(데이터베이스 제외)을 비교하여 중복된 파일이 있는지 확인합니다. 조사 페이지에서 "파일 크기" 필터와 "중복 항목"을 사용하여 사용자 환경에서 특정 크기 범위의 파일이 복제되었는지 확인할 수 있습니다.

BlueXP 분류는 해시 기술을 사용하여 중복 파일을 결정합니다. 파일에 다른 파일과 동일한 해시 코드가 있으면 파일 이름이 다르더라도 파일이 정확하게 중복되었는지 100% 확인할 수 있습니다.

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

모든 중복 파일을 봅니다

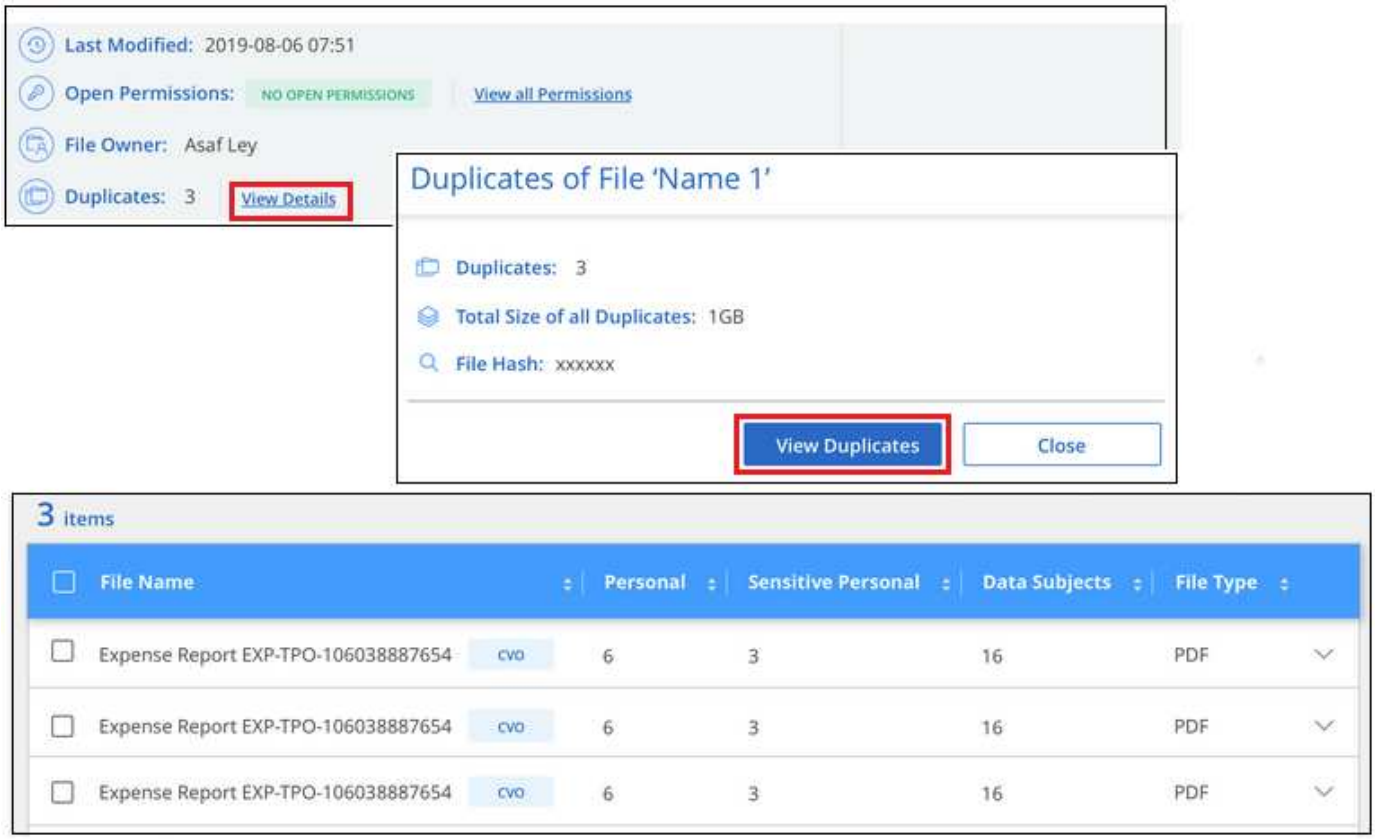
작업 환경 및 스캔할 데이터 원본에 중복되는 모든 파일의 목록을 보려면 데이터 조사 페이지에서 * 중복 > 중복 항목 있음 * 이라는 필터를 사용하면 됩니다.

모든 중복 파일이 결과 페이지에 표시됩니다.

특정 파일이 복제되었는지 확인합니다

단일 파일에 중복이 있는지 확인하려면 데이터 조사 결과 창에서 을(를) 클릭합니다 ⌄ 모든 단일 파일에서 파일 메타데이터를 볼 수 있습니다. 특정 파일의 복제본이 있는 경우 이 정보는 *Duplicates* 필드 옆에 표시됩니다.

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



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

데이터 조사 보고서

데이터 조사 보고서는 데이터 조사 페이지의 필터링된 콘텐츠를 다운로드하는 것입니다.

보고서는 두 가지 형식으로 제공됩니다.

- 로컬 컴퓨터에 저장할 수 있는 .csv 파일

  이 보고서에는 최대 10,000개의 데이터 행이 포함될 수 있습니다.

- NFS 공유로 내보내는 .JSON 파일

  데이터가 250,000행이 넘는 경우 .JSON 파일이 추가로 생성됩니다.

  파일 공유로 내보낼 때 BlueXP 분류에 내보내기 액세스에 대한 올바른 권한이 있는지 확인합니다.

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

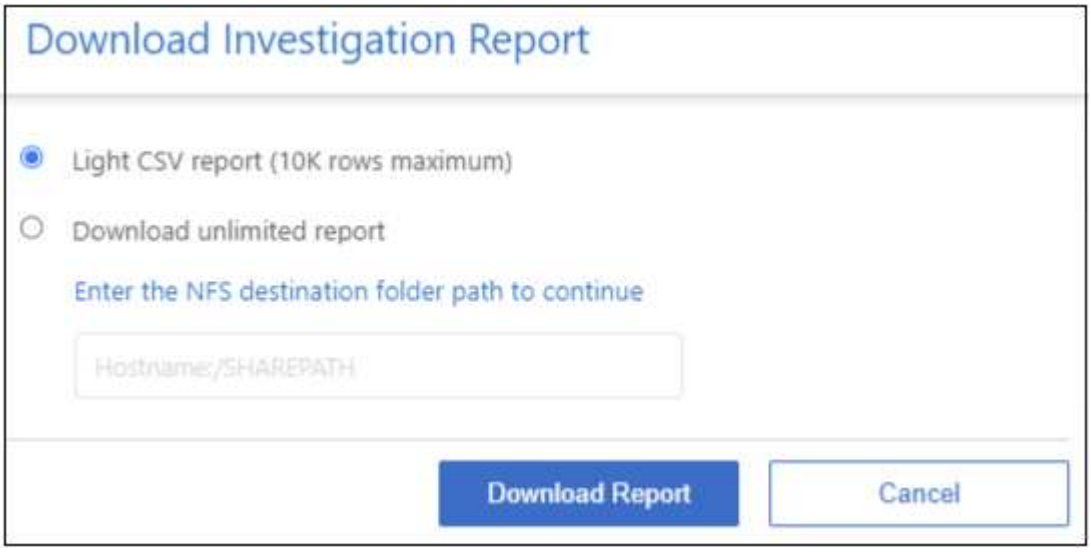
데이터 조사 보고서를 생성합니다

단계

1. 데이터 조사 페이지에서 을 클릭합니다 버튼을 클릭합니다.

2. 데이터의 .csv 보고서 또는 .JSON 보고서를 다운로드할지 여부를 선택하고 * 보고서 다운로드 * 를 클릭합니다.

   JSON 보고서를 선택할 때 보고서를 다운로드할 NFS 공유의 이름을 '<host_name>:/<share_path>' 형식으로 입력합니다.



결과

대화 상자에 보고서가 다운로드되고 있다는 메시지가 표시됩니다.

에서 JSON 보고서 생성 진행률을 볼 수 있습니다 "작업 상태 창".

각 데이터 조사 보고서에 포함되는 사항

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

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

- 민감한 개인 정보
- 권한을 엽니다
- 스캔 분석 오류
- 삭제 감지 날짜입니다

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

비정형 디렉터리 데이터 보고서 * 에는 폴더 및 파일 공유에 대한 다음 정보가 포함되어 있습니다.

- 작업 환경 유형입니다
- 작업 환경 이름입니다
- 디렉토리 이름
- 스토리지 저장소(예: 폴더 또는 파일 공유)
- 디렉토리 소유자
- 만든 시간
- 검색된 시간
- 마지막 수정
- 마지막 액세스
- 권한을 엽니다
- 디렉터리 유형입니다

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

- DB 테이블 이름입니다
- 위치 유형
- 작업 환경 이름입니다
- 스토리지 저장소(예: 스키마)
- 열 개수
- 행 수
- 개인 정보
- 민감한 개인 정보

개인 데이터를 구성합니다

BlueXP 분류는 개인 데이터를 관리하고 구성할 수 있는 다양한 방법을 제공합니다. 따라서 가장 중요한 데이터를 더 쉽게 볼 수 있습니다.

- 에 가입되어 있는 경우 "AIP(Azure Information Protection)" 파일을 분류하고 보호하려면 BlueXP 분류를

사용하여 해당 AIP 레이블을 관리할 수 있습니다.

> 2023년 12월(v1.26.6) 릴리즈에서는 AIP(Azure Information Protection) 레이블을 사용하여 데이터를 통합하는 옵션이 일시적으로 제거되었습니다.

- 조직 또는 일부 유형의 추가 작업에 대해 표시할 파일에 태그를 추가할 수 있습니다.
- BlueXP 사용자를 특정 파일 또는 여러 파일에 할당하여 파일 관리를 책임질 수 있습니다.
- "정책" 기능을 사용하면 버튼 하나를 클릭하여 결과를 쉽게 볼 수 있도록 사용자 지정 검색 쿼리를 직접 만들 수 있습니다.
- 특정 중요 정책이 결과를 반환할 때 BlueXP 사용자 또는 기타 전자 메일 주소로 전자 메일 알림을 보낼 수 있습니다.

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

태그나 라벨을 사용해야 합니까?

다음은 BlueXP 분류 태깅 및 Azure 정보 보호 라벨과 비교한 것입니다.

태그	라벨
파일 태그는 BlueXP 분류의 통합된 부분입니다.	Azure 정보 보호(AIP)에 가입해야 합니다.
이 태그는 BlueXP 분류 데이터베이스에만 보관되며, 파일에는 기록되지 않습니다. 파일 또는 액세스되거나 수정된 파일은 변경되지 않습니다.	레이블은 파일의 일부이며 레이블이 변경되면 파일이 변경됩니다. 또한 이 변경 사항은 액세스 및 수정된 파일 시간도 변경합니다.
한 파일에 여러 개의 태그를 지정할 수 있습니다.	단일 파일에 하나의 레이블이 있을 수 있습니다.
태그는 복사, 이동, 삭제, 정책 실행 등의 내부 BlueXP 분류 작업에 사용할 수 있습니다. 등	파일을 읽을 수 있는 다른 시스템은 추가 자동화에 사용할 수 있는 레이블을 볼 수 있습니다.
단일 API 호출만 사용하여 파일에 태그가 있는지 확인합니다.	

AIP 레이블을 사용하여 데이터를 분류합니다

에 가입한 경우 BlueXP 분류에서 검색하는 파일의 AIP 레이블을 관리할 수 있습니다 "AIP(Azure Information Protection)". AIP를 사용하면 콘텐츠에 레이블을 적용하여 문서와 파일을 분류하고 보호할 수 있습니다. BlueXP 분류를 사용하면 파일에 이미 할당된 레이블을 보고, 파일에 레이블을 추가하고, 레이블이 이미 있는 경우 레이블을 변경할 수 있습니다.

BlueXP 분류는 .DOC, .DOCX, .PDF, .PPTX, .XLS 파일 형식 내에서 AIP 레이블을 지원합니다. XLSX

> - 현재 30MB를 초과하는 파일의 레이블은 변경할 수 없습니다. OneDrive, SharePoint 및 Google Drive 계정의 경우 최대 파일 크기는 4MB입니다.
> - 파일에 AIP에 더 이상 존재하지 않는 레이블이 있는 경우 BlueXP 분류에서는 레이블이 없는 파일로 간주합니다.
> - 정부 지역 또는 인터넷 액세스가 없는 온프레미스 위치(어두운 사이트라고도 함)에 BlueXP 분류를 배포한 경우에는 AIP 레이블 기능을 사용할 수 없습니다.

작업 공간에 **AIP** 레이블을 통합합니다

AIP 레이블을 관리하려면 기존 Azure 계정에 로그인하여 AIP 레이블 기능을 BlueXP 분류에 통합해야 합니다. 활성화되면 모든 파일의 AIP 레이블을 관리할 수 있습니다 "데이터 소스" BlueXP 작업 영역에서

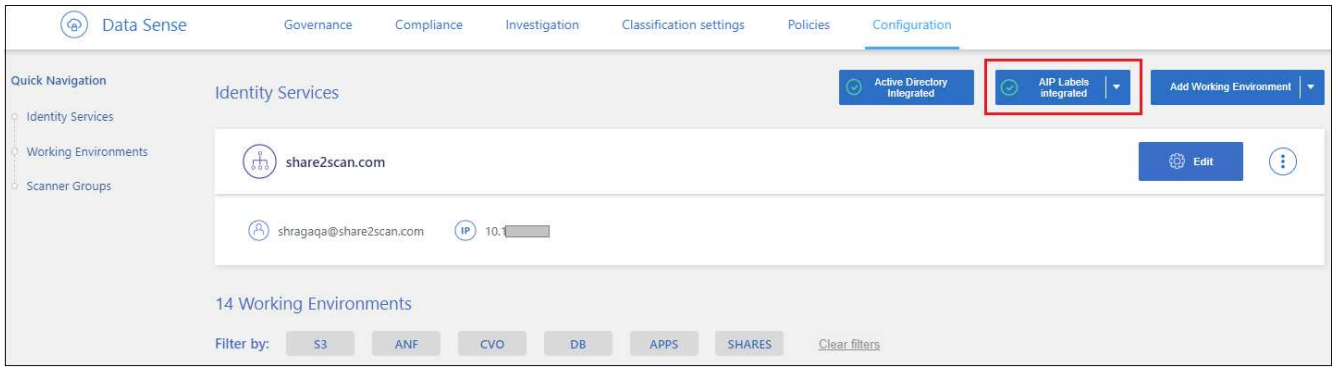
요구 사항

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

단계

1. BlueXP 분류 구성 페이지에서 * AIP 레이블 통합 * 을 클릭합니다.

2. AIP 레이블 통합 대화 상자에서 * Azure에 로그인 * 을 클릭합니다.
3. Microsoft 페이지가 나타나면 계정을 선택하고 필요한 자격 증명을 입력합니다.
4. BlueXP 분류 탭으로 돌아가면 "*AIP* 라벨이 *<account_name>* 계정과 성공적으로 통합되었습니다."라는 메시지가 나타납니다.
5. 닫기 * 를 클릭하면 페이지 상단에 _AIP 라벨 통합 _ 이라는 텍스트가 표시됩니다.



결과

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

파일에서 **AIP** 레이블을 봅니다

파일에 할당된 현재 AIP 레이블을 볼 수 있습니다.

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

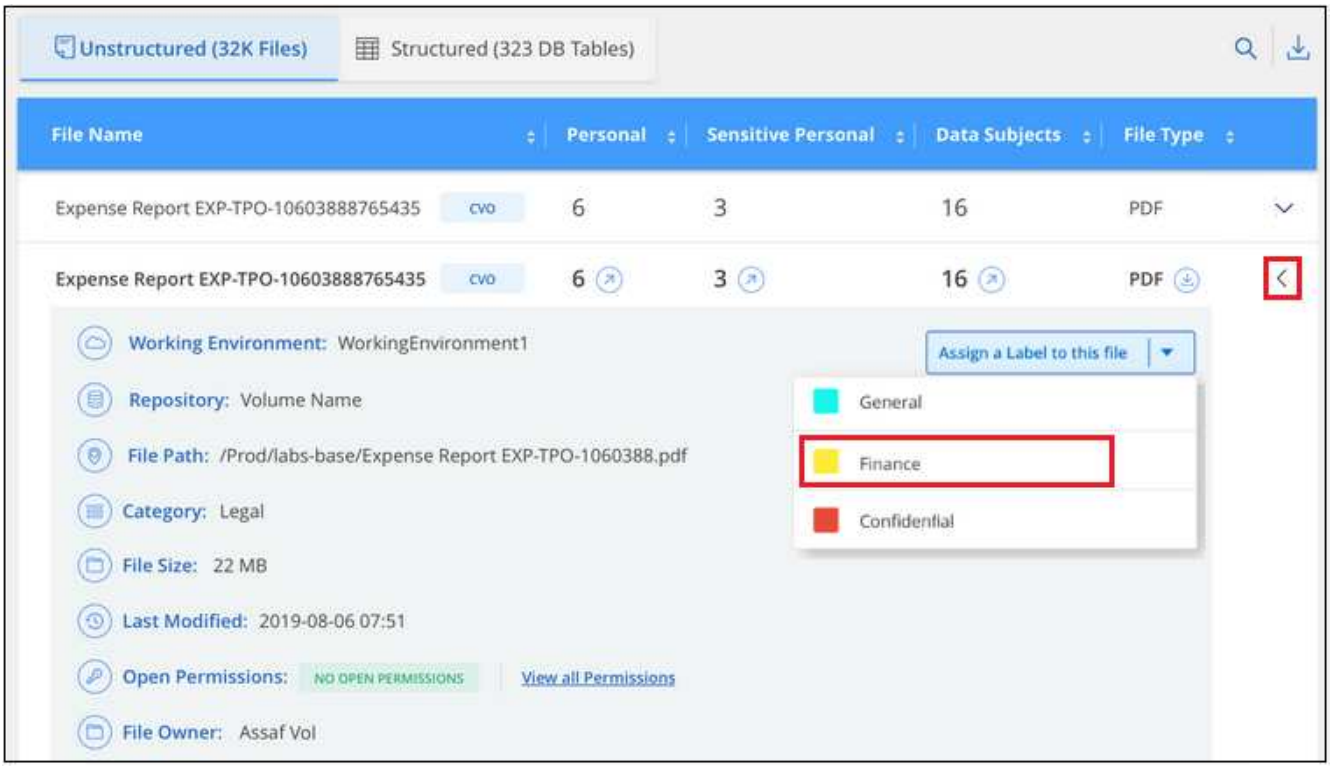
AIP 레이블을 수동으로 할당합니다

BlueXP 분류를 사용하여 파일에서 AIP 레이블을 추가, 변경 및 제거할 수 있습니다.

다음 단계에 따라 AIP 레이블을 단일 파일에 할당합니다.

단계

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



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

   파일 메타데이터에 레이블이 나타납니다.

다음 단계에 따라 여러 파일에 AIP 레이블을 할당합니다. AIP 레이블을 한 번에 최대 20개의 파일(UI에서 한 페이지)에 할당할 수 있습니다.

단계

1. 데이터 조사 결과 창에서 레이블을 지정할 파일을 선택합니다.

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

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

선택한 모든 파일의 메타데이터에 AIP 레이블이 추가됩니다.

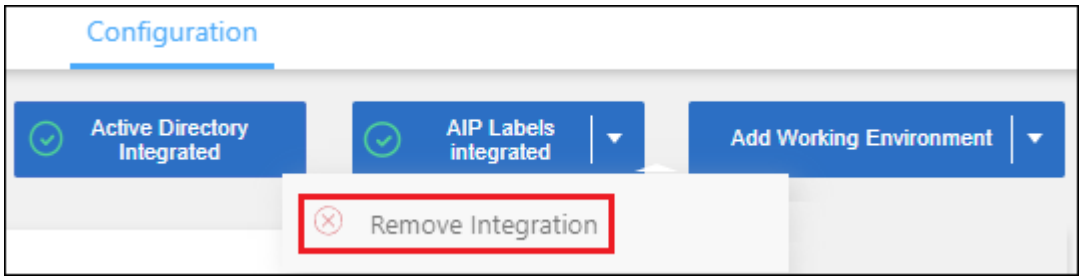
AIP 통합을 제거합니다

파일의 AIP 레이블을 더 이상 관리할 수 없는 경우 BlueXP 분류 인터페이스에서 AIP 계정을 제거할 수 있습니다.

BlueXP 분류를 사용하여 추가한 레이블은 변경되지 않습니다. 파일에 있는 레이블은 현재 있는 그대로 유지됩니다.

단계

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



2. 확인 대화 상자에서 * 통합 제거 * 를 클릭합니다.

태그를 적용하여 스캔한 파일을 관리합니다

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

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

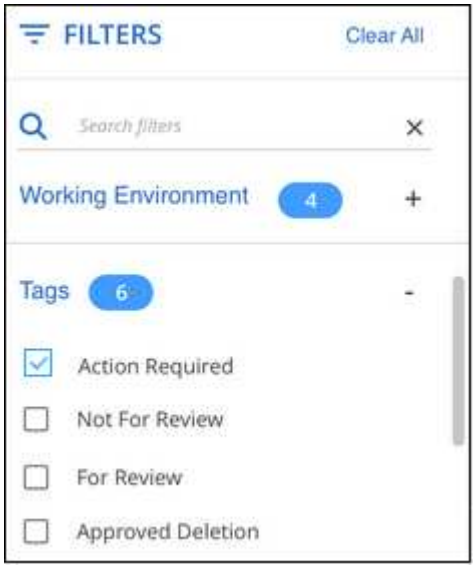
AIP 레이블과 같은 방식으로 태그가 파일에 추가되지 않습니다. BlueXP 사용자는 BlueXP 분류를 사용하여 태그를 볼 수 있으므로 일부 유형의 후속 작업을 위해 파일을 삭제하거나 확인해야 하는지 확인할 수 있습니다.

> BlueXP 분류에서 파일에 할당된 태그는 볼륨 또는 가상 시스템 인스턴스 같은 리소스에 추가할 수 있는 태그와 관련이 없습니다. 파일 수준에서 BlueXP 분류 태그가 적용됩니다.

특정 태그가 적용된 파일을 봅니다

특정 태그가 지정된 모든 파일을 볼 수 있습니다.

1. BlueXP 분류에서 * Investigation * (조사 *) 탭을 클릭합니다.
2. 데이터 조사 페이지의 필터 창에서 * 태그 * 를 클릭한 다음 필요한 태그를 선택합니다.



조사 결과 창에는 해당 태그가 지정된 모든 파일이 표시됩니다.

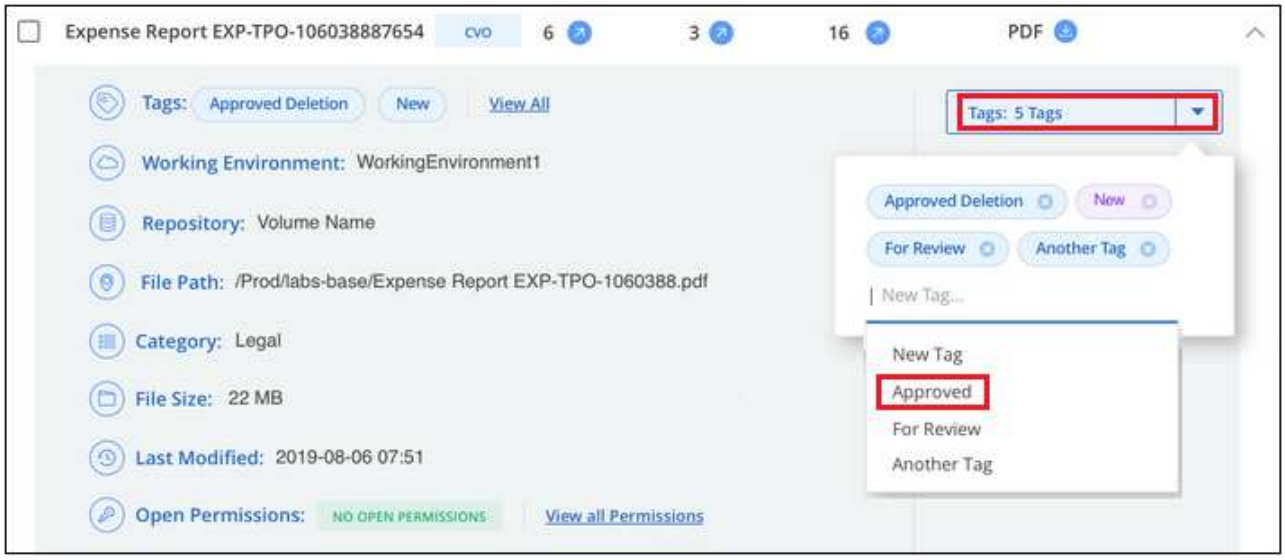
파일에 태그를 지정합니다

단일 파일 또는 파일 그룹에 태그를 추가할 수 있습니다.

단일 파일에 태그 추가하기:

단계

1. 데이터 조사 결과 창에서 을 클릭합니다 ⌄ 파일 메타데이터 세부 정보를 확장합니다.
2. 태그 * 필드를 클릭하면 현재 할당된 태그가 표시됩니다.
3. 태그 또는 태그 추가:
   - 기존 태그를 지정하려면 * 새 태그… * 필드를 클릭하고 태그 이름을 입력합니다. 찾고 있는 태그가 나타나면 해당 태그를 선택하고 * Enter * 를 누릅니다.
   - 새 태그를 만들어 파일에 할당하려면 * 새 태그… * 필드를 클릭하고 새 태그의 이름을 입력한 다음 * Enter * 를 누릅니다.



태그가 파일 메타데이터에 나타납니다.

여러 파일에 태그 추가하기:

단계

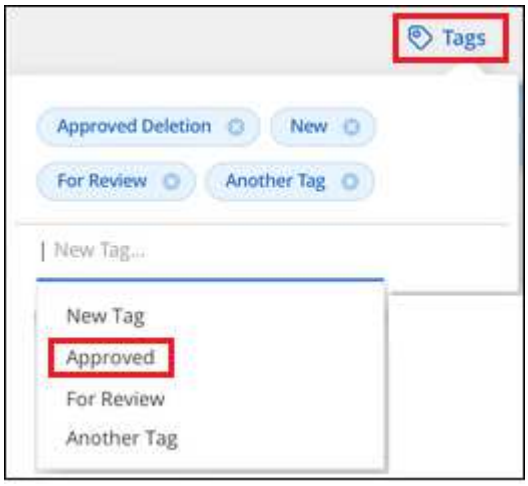
1. 데이터 조사 결과 창에서 태그를 지정할 파일을 선택합니다.

   - 개별 파일을 선택하려면 각 파일(Volume_1)를 클릭합니다.
   - 현재 페이지의 모든 파일을 선택하려면 제목 행(File Name)를 클릭합니다.
   - 모든 페이지의 모든 파일을 선택하려면 제목 행(File Name)를 클릭한 다음 팝업 메시지에서 를

클릭합니다 All 20 Items on this page selected Select all Items in list (63K Items)목록에서 * 모든 항목 선택(xxx개 항목) * 을 클릭합니다.

한 번에 최대 100,000개의 파일에 태그를 적용할 수 있습니다.

2. 버튼 모음에서 * 태그 * 를 클릭하면 현재 할당된 태그가 표시됩니다.
3. 태그 또는 태그 추가:
   - 기존 태그를 지정하려면 * 새 태그… * 필드를 클릭하고 태그 이름을 입력합니다. 찾고 있는 태그가 나타나면 해당 태그를 선택하고 * Enter * 를 누릅니다.
   - 새 태그를 만들어 파일에 할당하려면 * 새 태그… * 필드를 클릭하고 새 태그의 이름을 입력한 다음 * Enter * 를 누릅니다.



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

파일에서 태그를 삭제합니다

더 이상 사용하지 않아도 되는 태그는 삭제할 수 있습니다.

기존 태그에 대해 * x * 를 클릭하기만 하면 됩니다.

여러 파일을 선택한 경우 태그가 모든 파일에서 제거됩니다.

특정 파일을 관리할 사용자를 지정합니다

BlueXP 사용자를 특정 파일 또는 여러 파일에 할당하면 해당 파일에 대해 수행해야 하는 모든 후속 작업을 사용자가 책임질 수 있습니다. 이 기능은 종종 기능과 함께 사용되어 파일에 사용자 정의 상태 태그를 추가합니다.

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

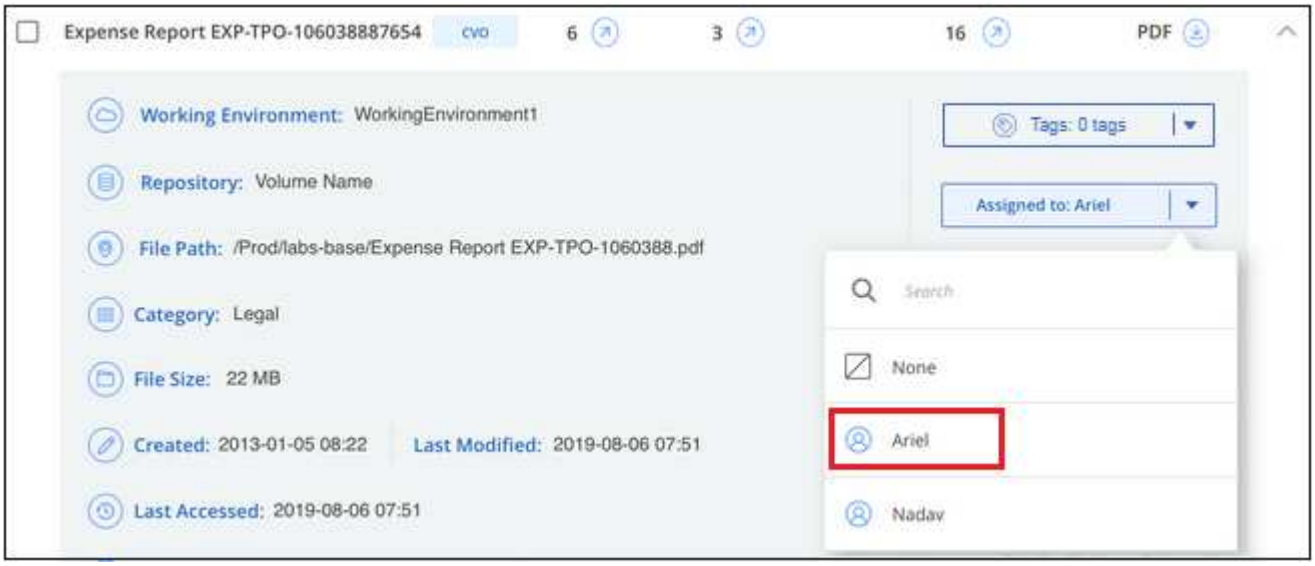
사용자 이름은 파일 메타데이터의 일부로 파일에 추가되지 않습니다. BlueXP 사용자는 BlueXP 분류를 사용할 때 이 이름을 볼 수 있습니다.

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

사용자를 단일 파일에 할당하려면 다음 단계를 수행하십시오.

단계

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



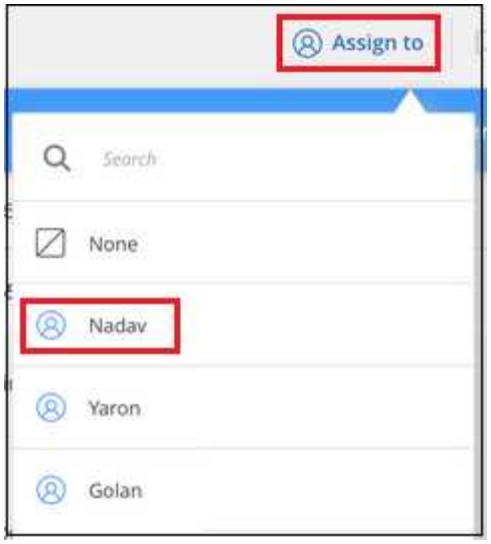
사용자 이름이 파일 메타데이터에 나타납니다.

사용자를 여러 파일에 할당하려면 다음 단계를 수행하십시오. 사용자를 한 번에 최대 20개의 파일(UI에서 한 페이지)에 할당할 수 있습니다.

단계

1. 데이터 조사 결과 창에서 사용자에게 할당할 파일을 선택합니다.

   - 개별 파일을 선택하려면 각 파일(Volume_1)를 클릭합니다.
   - 현재 페이지의 모든 파일을 선택하려면 제목 행(File Name)를 클릭합니다.
2. 버튼 모음에서 * Assign to * (할당 대상 *)를 클릭하고 사용자 이름을 선택합니다.



선택한 모든 파일의 메타데이터에 사용자가 추가됩니다.

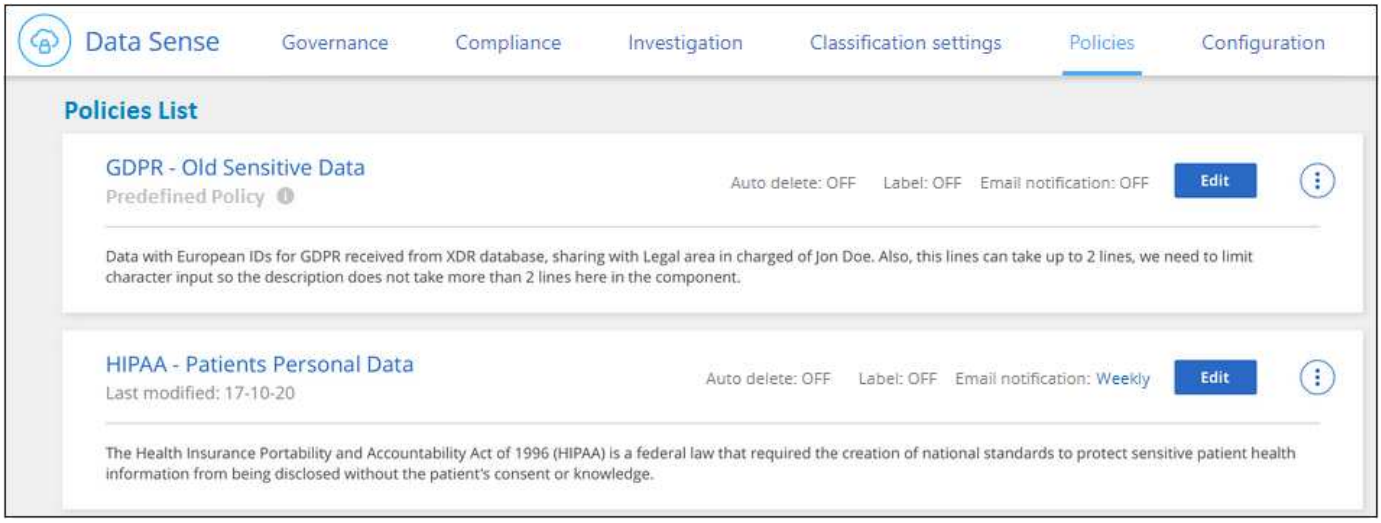
데이터에 정책을 할당합니다

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

정책은 다음과 같은 기능을 제공합니다.

- 사전 정의된 정책 구성하는 방법에 대해 설명합니다
- 고유한 사용자 지정 정책을 만들 수 있습니다
- 클릭 한 번으로 정책의 결과가 포함된 조사 페이지를 시작합니다
- 특정 중요 정책이 결과를 반환하면 데이터를 보호하기 위한 알림을 받을 수 있도록 BlueXP 사용자 또는 기타 전자 메일 주소로 전자 메일 알림을 보냅니다
- AIP(Azure Information Protection) 레이블을 정책에 정의된 조건과 일치하는 모든 파일에 자동으로 할당합니다
- 특정 정책이 결과를 반환하면 데이터를 자동으로 보호할 수 있도록 파일을 자동으로 삭제합니다(하루에 한 번)

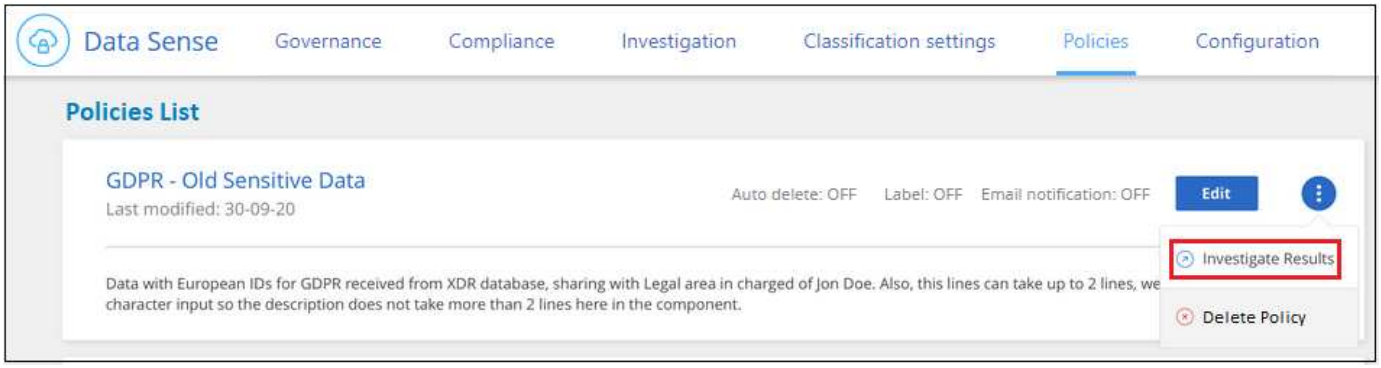
Compliance Dashboard의 * Policies * 탭에는 이 BlueXP 분류 인스턴스에서 사용할 수 있는 사전 정의된 정책과 사용자 지정 정책이 모두 나열됩니다.



또한 조사 페이지의 필터 목록에 정책이 표시됩니다.

조사 페이지에서 정책 결과를 봅니다

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



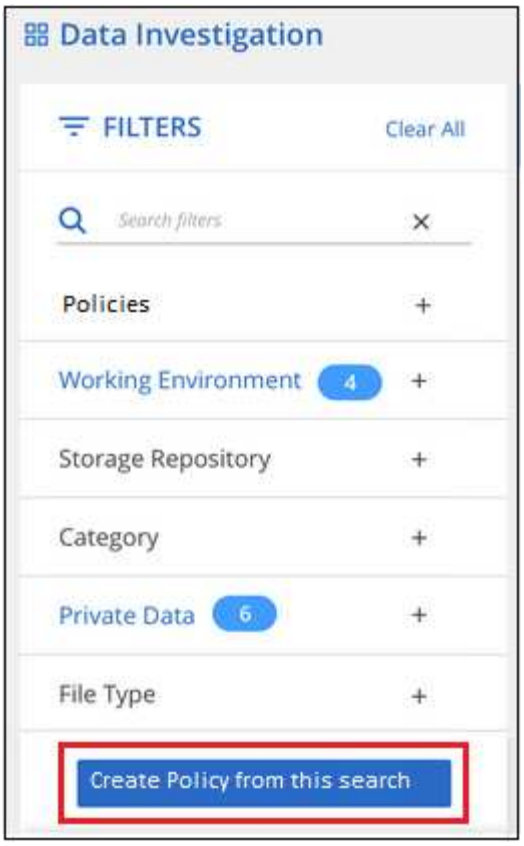
사용자 지정 정책을 만듭니다

조직에 맞는 검색 결과를 제공하는 사용자 지정 정책을 만들 수 있습니다. 검색 기준과 일치하는 모든 파일 및 디렉토리(공유 및 폴더)에 대한 결과가 반환됩니다.

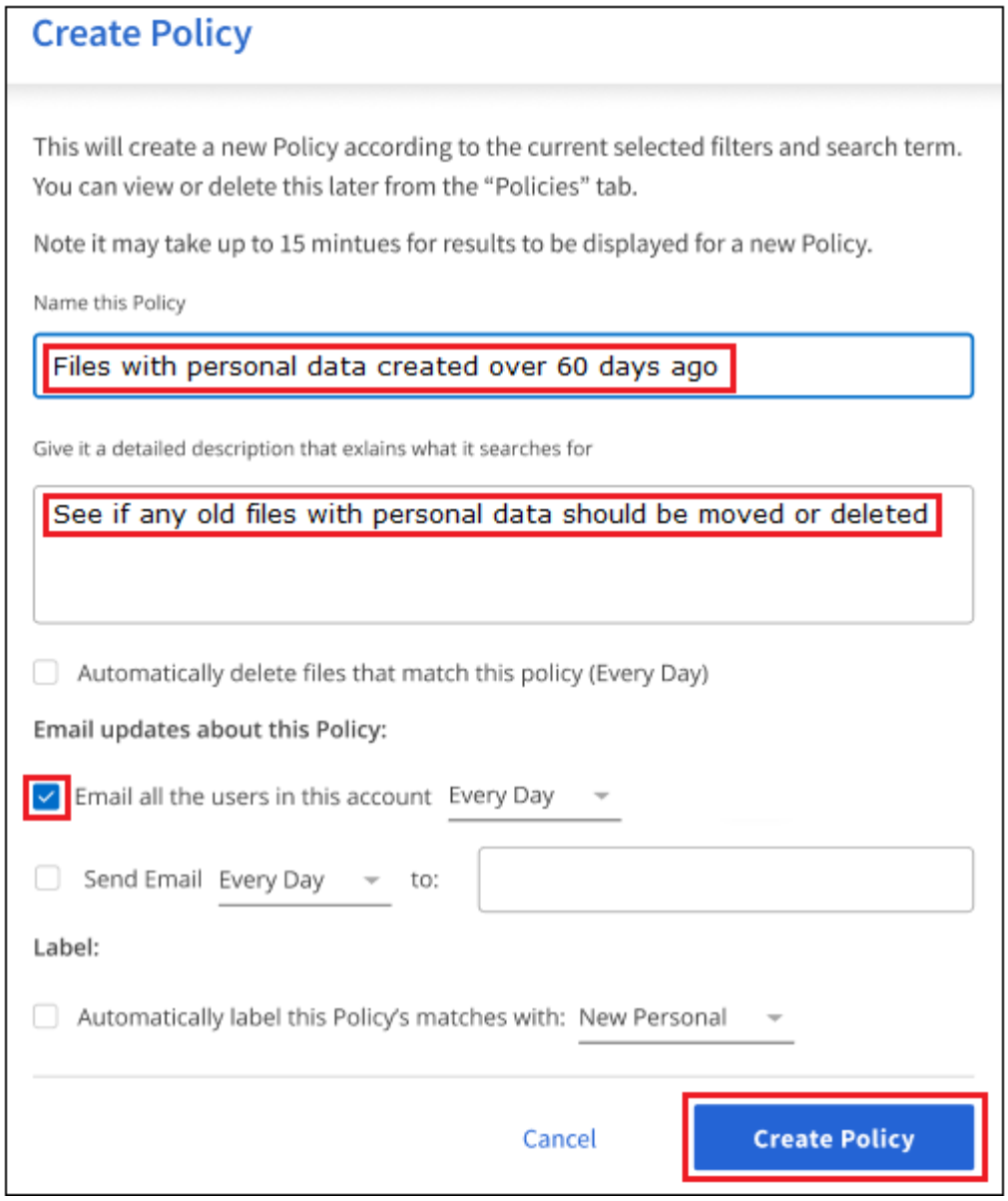
정책 결과에 따라 데이터를 삭제하고 AIP 레이블을 할당하는 작업은 파일에만 유효합니다. 검색 기준과 일치하는 디렉토리는 자동으로 삭제하거나 할당 AIP 레이블을 지정할 수 없습니다.

단계

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



3. 정책의 이름을 지정하고 정책에서 수행할 수 있는 다른 작업을 선택합니다.
   a. 고유한 이름과 설명을 입력합니다.
   b. 필요한 경우 정책 매개 변수와 일치하는 파일을 자동으로 삭제하려면 확인란을 선택합니다. 에 대해 자세히 알아보십시오 정책을 사용하여 소스 파일을 삭제하는 중입니다.
   c. 필요에 따라 계정의 BlueXP 사용자에게 알림 이메일을 보내려면 확인란을 선택하고 이메일을 보낼 간격을 선택합니다. 에 대해 자세히 알아보십시오 정책 결과에 따라 이메일 알림을 보냅니다.
   d. 필요에 따라 다른 사용자에게 알림 이메일을 보내려면 확인란을 선택하고 최대 20개의 이메일 주소를 입력한 다음 이메일을 보낼 간격을 선택합니다.
   e. 필요한 경우 정책 매개 변수와 일치하는 파일에 AIP 레이블을 자동으로 할당하려면 확인란을 선택하고 레이블을 선택합니다. (이미 AIP 레이블을 통합한 경우에만 해당됩니다. 에 대해 자세히 알아보십시오 "AIP 레이블"참조)
   f. Create Policy * 를 클릭합니다.



결과

새 정책이 정책 탭에 나타납니다.

비준수 데이터가 발견되면 이메일 알림을 보냅니다

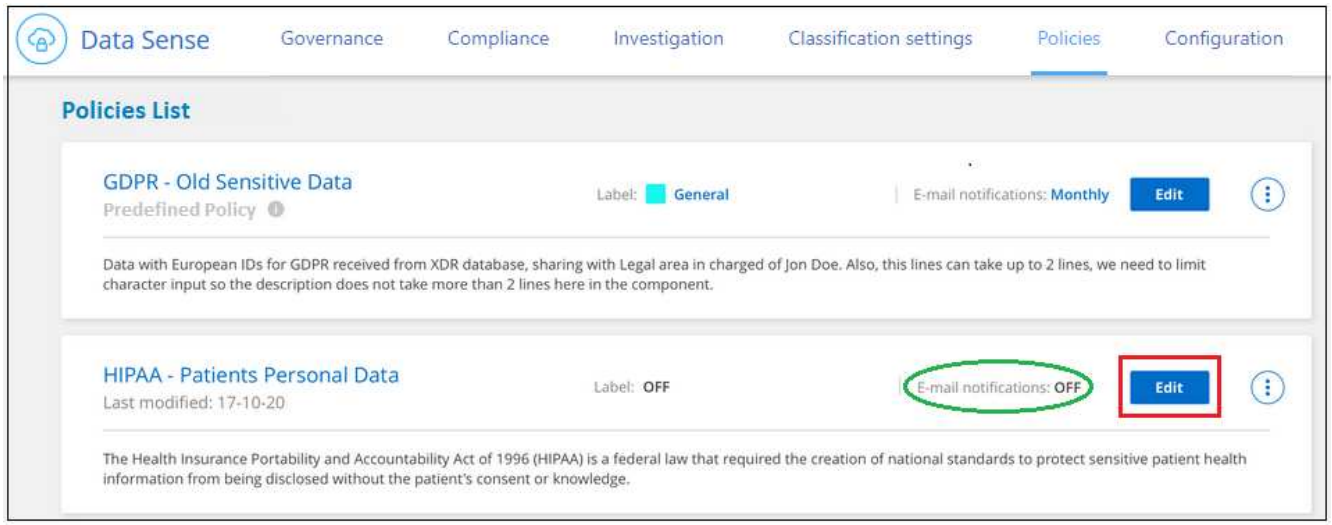
BlueXP 분류는 특정 중요 정책이 결과를 반환할 때 계정의 BlueXP 사용자에게 이메일 경고를 보내 데이터를 보호할 수 있도록 알림을 받을 수 있습니다. 매일, 매주 또는 매월 이메일 알림을 보내도록 선택할 수 있습니다. 또한 BlueXP 계정이 아닌 최대 20개의 전자 메일 주소로 다른 전자 메일 주소로 전자 메일 알림을 보내도록 선택할 수 있습니다.

정책을 만들거나 정책을 편집할 때 이 설정을 구성할 수 있습니다.

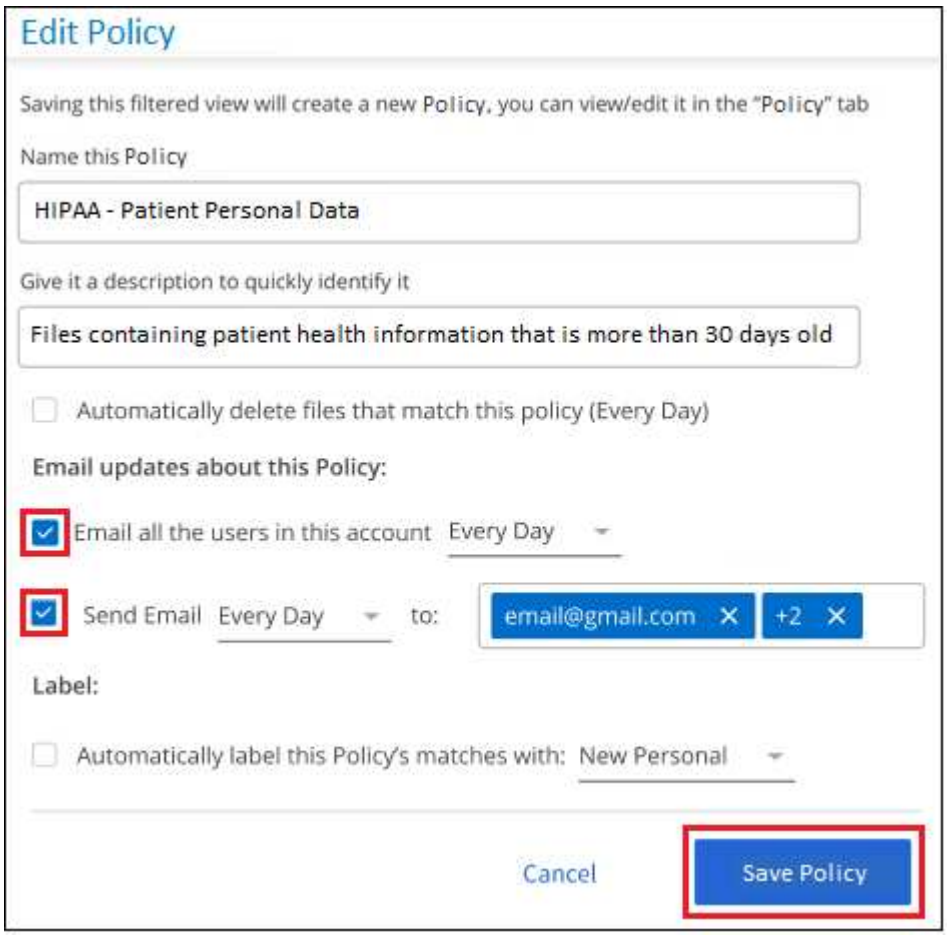
기존 정책에 전자 메일 업데이트를 추가하려면 다음 단계를 따릅니다.

단계

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



2. 정책 편집 페이지에서 다음을 수행합니다.
   a. BlueXP 계정의 사용자에게 알림 이메일을 보내려면 "이 계정의 모든 사용자에게 이메일 보내기" 확인란을 선택하고 이메일을 보낼 간격을 선택합니다(예: * 매일 *).
   b. 추가 사용자에게 알림 이메일을 보내려면 "이메일 보내기" 확인란을 선택하고 이메일 발송 간격을 선택한 후 최대 20개의 이메일 주소를 입력합니다.



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

결과

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

정책을 사용하여 소스 파일을 자동으로 삭제합니다

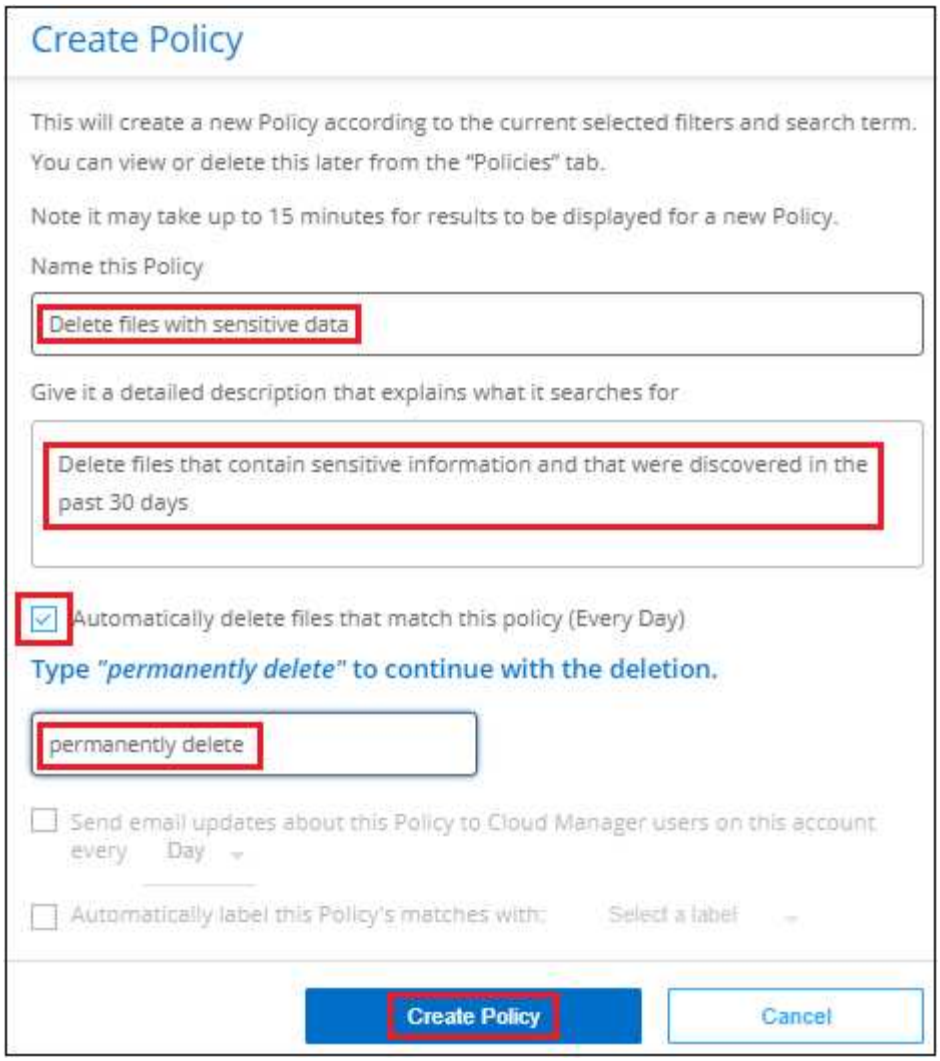
사용자 지정 정책을 만들어 정책과 일치하는 파일을 삭제할 수 있습니다. 예를 들어, 지난 30일 동안 BlueXP 분류에서 발견된 중요한 정보가 포함된 파일을 삭제할 수 있습니다.

계정 관리자만 파일을 자동으로 삭제하는 정책을 만들 수 있습니다.

> 정책과 일치하는 모든 파일이 하루에 한 번 영구적으로 삭제됩니다.

단계

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



결과

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

에서 삭제된 파일 목록을 볼 수 있습니다 "작업 상태 창".

정책을 사용하여 AIP 레이블을 자동으로 할당합니다

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

BlueXP 분류에서 파일을 검사하면 파일에 레이블이 계속 추가되거나 업데이트됩니다.

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

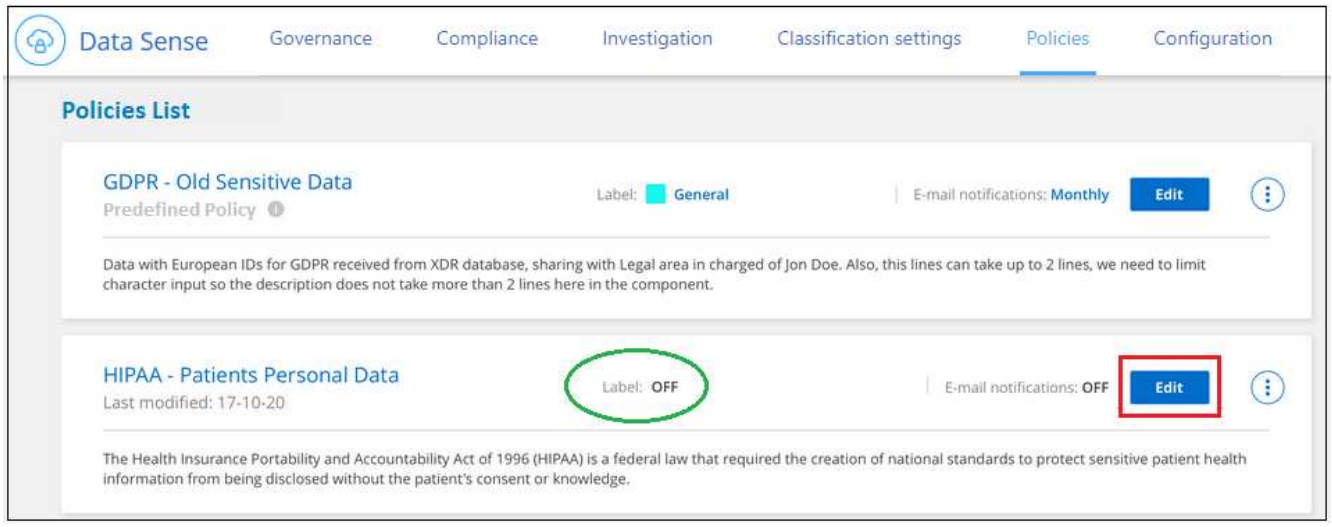
파일이...	그러면...
레이블이 없습니다	라벨이 추가됩니다
낮은 수준의 분류에 대한 기존 레이블이 있습니다	더 높은 수준의 라벨이 추가됩니다
더 높은 수준의 분류에 대한 기존 레이블이 있습니다	더 높은 수준의 레이블이 유지됩니다

파일이...	그러면...
는 수동으로 또는 정책에 의해 레이블이 할당됩니다	더 높은 수준의 라벨이 추가됩니다
는 두 정책에 의해 두 개의 서로 다른 레이블을 할당합니다	더 높은 수준의 라벨이 추가됩니다

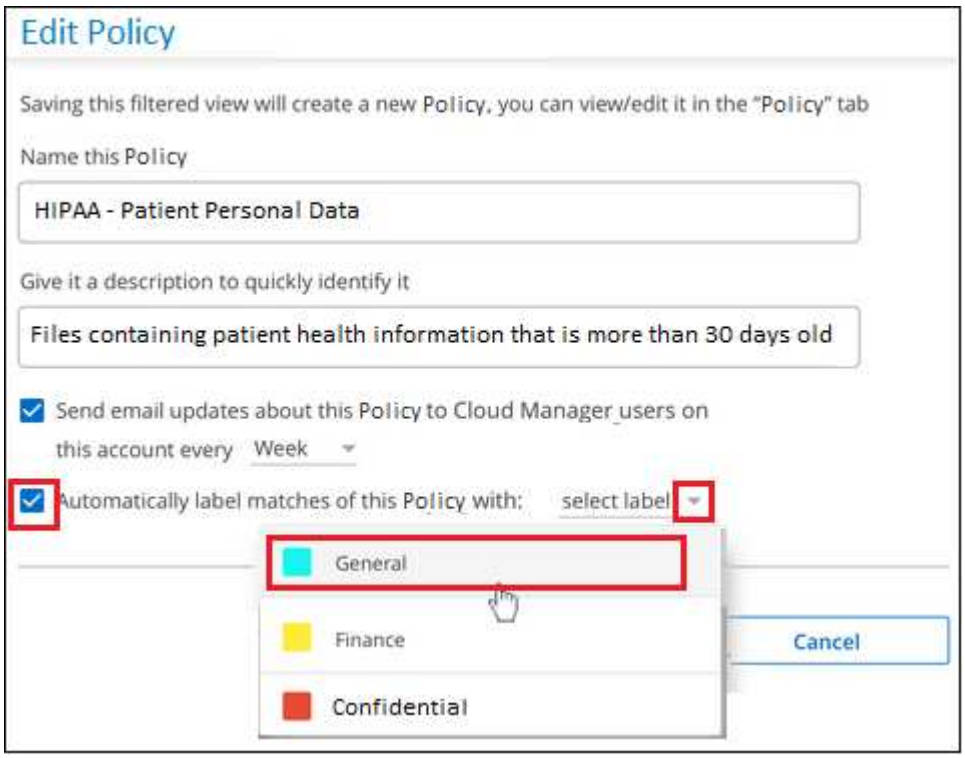
기존 정책에 AIP 레이블을 추가하려면 다음 단계를 따르십시오.

단계

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



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



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

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

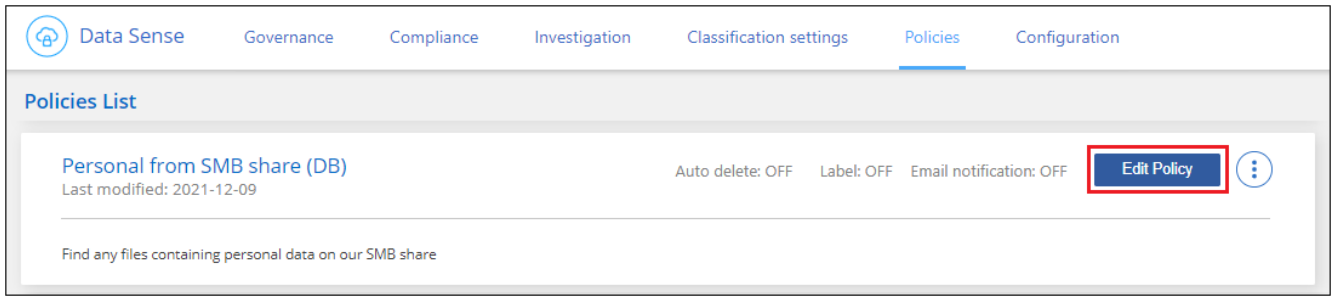
정책을 편집합니다

이전에 만든 기존 정책의 조건을 수정할 수 있습니다. 이 기능은 특정 매개 변수를 추가하거나 제거하기 위해 쿼리(필터를 사용하여 정의한 항목)를 변경하려는 경우에 특히 유용합니다.

사전 정의된 정책의 경우 이메일 알림의 전송 여부와 AIP 레이블 추가 여부만 수정할 수 있습니다. 다른 값은 변경할 수 없습니다.

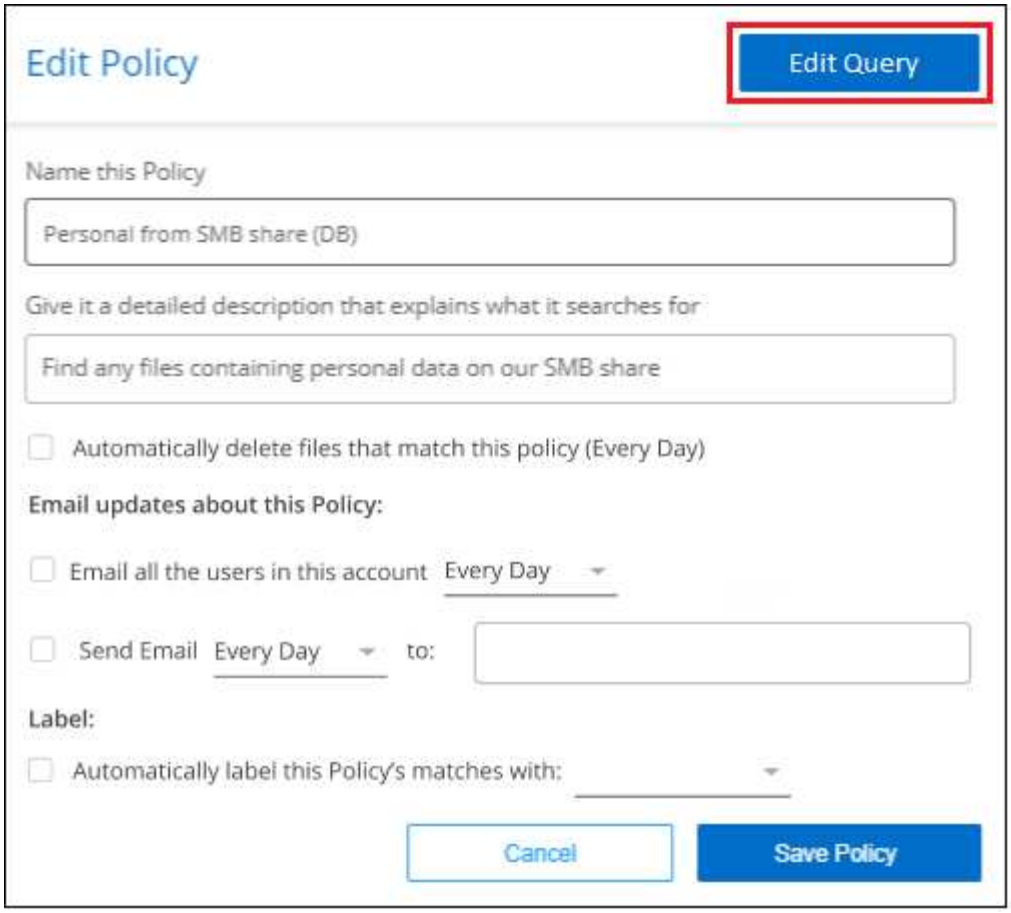
단계

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

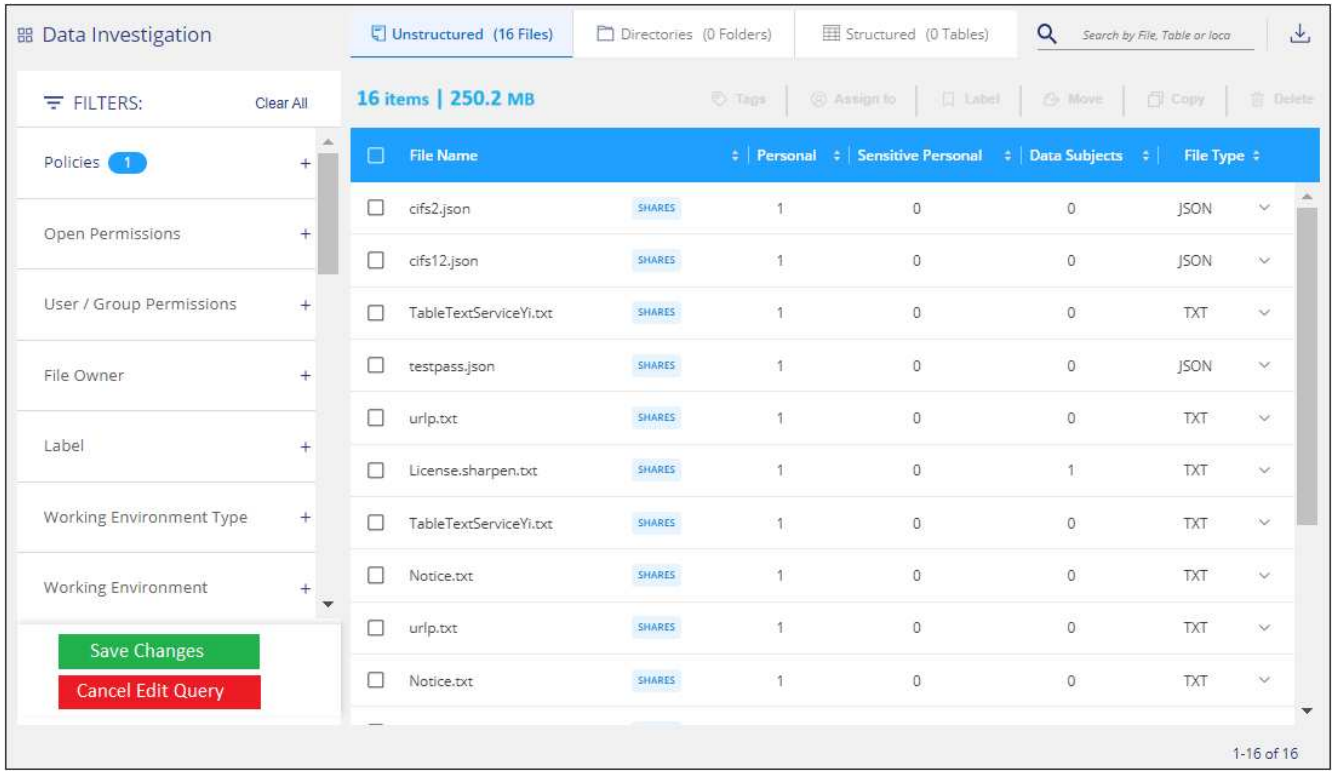


2. 이 페이지의 항목(이름, 설명, 이메일 알림 전송 여부 및 AIP 레이블 추가 여부)만 변경하려면 변경하고 * 정책 저장 * 을 클릭합니다.

   저장된 쿼리의 필터를 변경하려면 * 쿼리 편집 * 을 클릭합니다.



3. 해당 쿼리를 정의하는 조사 페이지에서 필터를 추가, 제거 또는 사용자 지정하여 쿼리를 편집하고 * 변경 내용 저장 * 을 클릭합니다.



결과

정책이 즉시 변경됩니다. 이메일을 보내거나 AIP 레이블을 추가하거나 파일을 삭제하기 위해 해당 정책에 정의된 모든 작업은 다음 내부에서도 수행됩니다.

정책을 삭제합니다

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

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

사전 정의된 정책 목록입니다

BlueXP 분류는 다음과 같은 시스템 정의 정책을 제공합니다.

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

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

개인 데이터를 관리합니다

BlueXP 분류는 개인 데이터를 관리하는 여러 가지 방법을 제공합니다. 일부 기능을 사용하면 데이터 마이그레이션을 쉽게 준비할 수 있을 뿐만 아니라 다른 기능도 데이터를 변경할 수 있습니다.

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

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

원본 파일을 복사합니다

BlueXP 분류에서 스캔 중인 모든 원본 파일을 복사할 수 있습니다. 달성하려는 목표에 따라 세 가지 유형의 복사 작업이 있습니다.

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

  특정 데이터의 복사본을 만들어 다른 NFS 위치로 이동하려는 경우 유용합니다.

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

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

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

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

소스 파일을 **NFS** 공유에 복사합니다

BlueXP 분류에서 스캔 중인 소스 파일을 모든 NFS 공유로 복사할 수 있습니다. NFS 공유를 BlueXP 분류와 통합할 필요가 없습니다. NFS 공유의 이름을 알아야 선택한 모든 파일이 형식으로 복사됩니다 `<host_name>:/<share_path>`.

데이터베이스에 있는 파일은 복사할 수 없습니다.

요구 사항

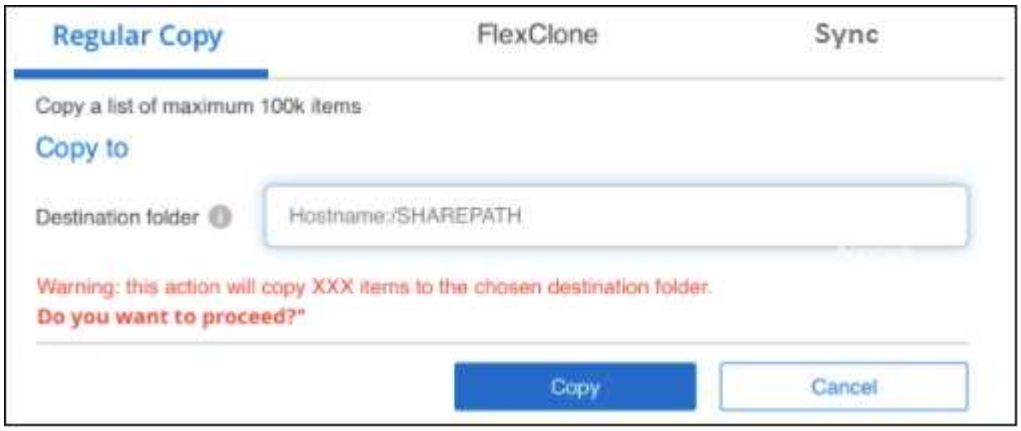
- 파일을 복사하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 파일을 복사하려면 대상 NFS 공유가 BlueXP 분류 인스턴스에서 액세스할 수 있어야 합니다.
- 한 번에 1에서 100,000개 파일 간에 복사할 수 있습니다.

단계

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

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

2. 파일 복사 대화 상자에서 * 일반 복사 * 탭을 선택합니다.



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

   복사 작업 상태와 함께 대화 상자가 나타납니다.

에서 복사 작업의 진행률을 볼 수 있습니다 "작업 상태 창".

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

볼륨 데이터를 새 볼륨에 복제합니다

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

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

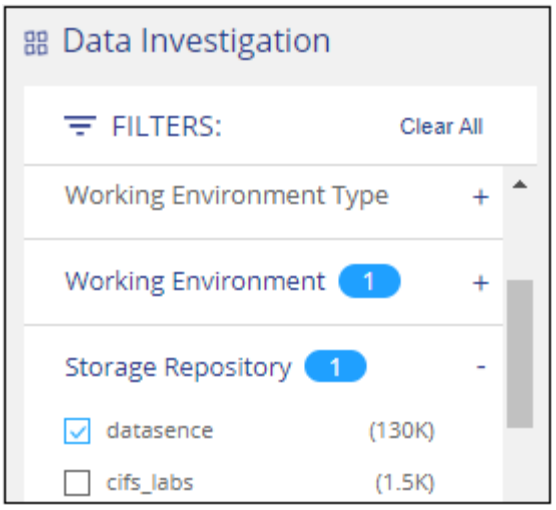
- 참고: * FlexGroup 볼륨은 FlexClone에서 지원하지 않으므로 복제할 수 없습니다.

요구 사항

- 파일을 복사하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 최소 20개의 파일을 선택해야 합니다.
- 선택한 모든 파일은 동일한 볼륨에서 가져온 것이어야 하며 볼륨이 온라인 상태여야 합니다.
- 볼륨은 Cloud Volumes ONTAP 또는 사내 ONTAP 시스템이어야 합니다. 현재 다른 데이터 원본은 지원되지 않습니다.
- FlexClone 라이센스가 클러스터에 설치되어 있어야 합니다. 이 라이센스는 Cloud Volumes ONTAP 시스템에 기본적으로 설치됩니다.

단계

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

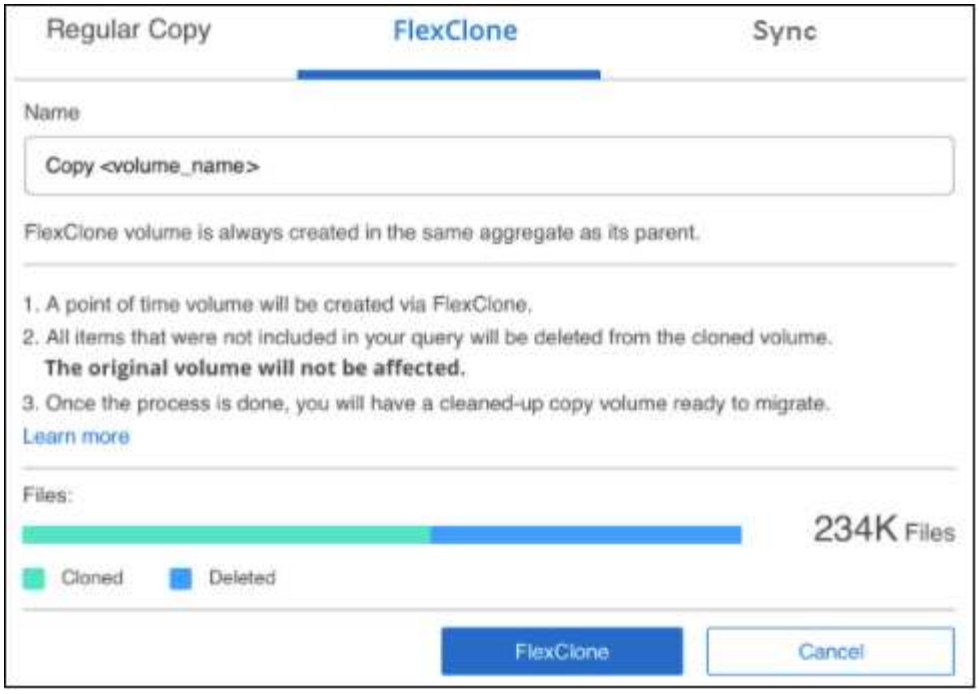


새 볼륨에 복제할 파일만 표시되도록 다른 필터를 적용합니다.

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

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

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



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

   클론 작업의 상태가 표시된 대화 상자가 나타납니다.

결과

클론 복제된 새 볼륨은 소스 볼륨과 동일한 애그리게이트에 생성됩니다.

에서 클론 작업의 진행률을 볼 수 있습니다 "작업 상태 창".

소스 볼륨이 있는 작업 환경에 대해 BlueXP 분류를 사용하도록 설정한 * 모든 볼륨 매핑 * 또는 * 모든 볼륨 매핑 및 분류 * 를 처음 선택한 경우 BlueXP 분류는 복제된 새 볼륨을 자동으로 스캔합니다. 처음에 이러한 선택 항목을 사용하지 않은 경우 이 새 볼륨을 스캔하려면 가 필요합니다 "수동으로 볼륨에서 스캔을 활성화합니다".

소스 파일을 타겟 시스템에 복사하고 동기화합니다

BlueXP 분류에서 검색하는 소스 파일을 지원되는 비정형 데이터 소스에서 특정 대상 위치의 디렉토리로 복사할 수 있습니다 ("BlueXP 복사 및 동기화가 지원되는 대상 위치입니다")를 클릭합니다. 초기 복제 후에는 구성한 일정에 따라 파일에서 변경된 모든 데이터가 동기화됩니다.

이 기능은 소스 시스템 간에 데이터를 마이그레이션하는 경우에 유용합니다. 이 작업은 를 사용합니다 "NetApp BlueXP 복사 및 동기화" 소스에서 타겟으로 데이터를 복제 및 동기화하는 기능

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

요구 사항

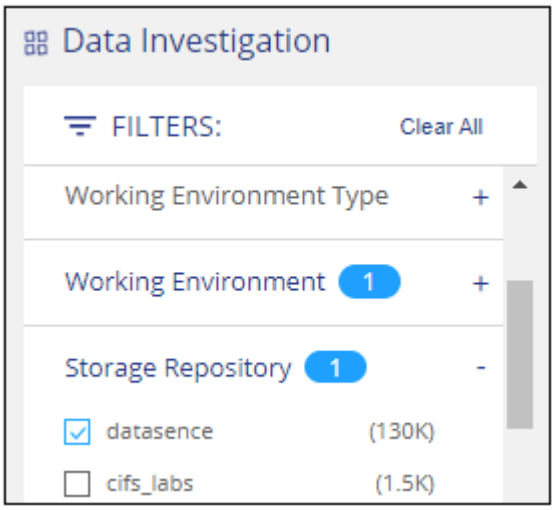
- 파일을 복사 및 동기화하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 최소 20개의 파일을 선택해야 합니다.
- 선택한 모든 파일은 동일한 소스 저장소(ONTAP 볼륨, S3 버킷, NFS 또는 CIFS 공유 등)에서 가져온 것이어야 합니다.

- BlueXP 복사 및 동기화 서비스를 활성화하고 소스 시스템과 대상 시스템 간에 파일을 전송하는 데 사용할 수 있는 최소 하나의 데이터 브로커를 구성해야 합니다. 부터 BlueXP 복사 및 동기화 요구 사항을 검토합니다 "빠른 시작 설명".

  BlueXP 복사 및 동기화 서비스에는 동기화 관계에 대한 별도의 서비스 요금이 부과되며 클라우드에 데이터 브로커를 배포할 경우 리소스 요금이 발생합니다.

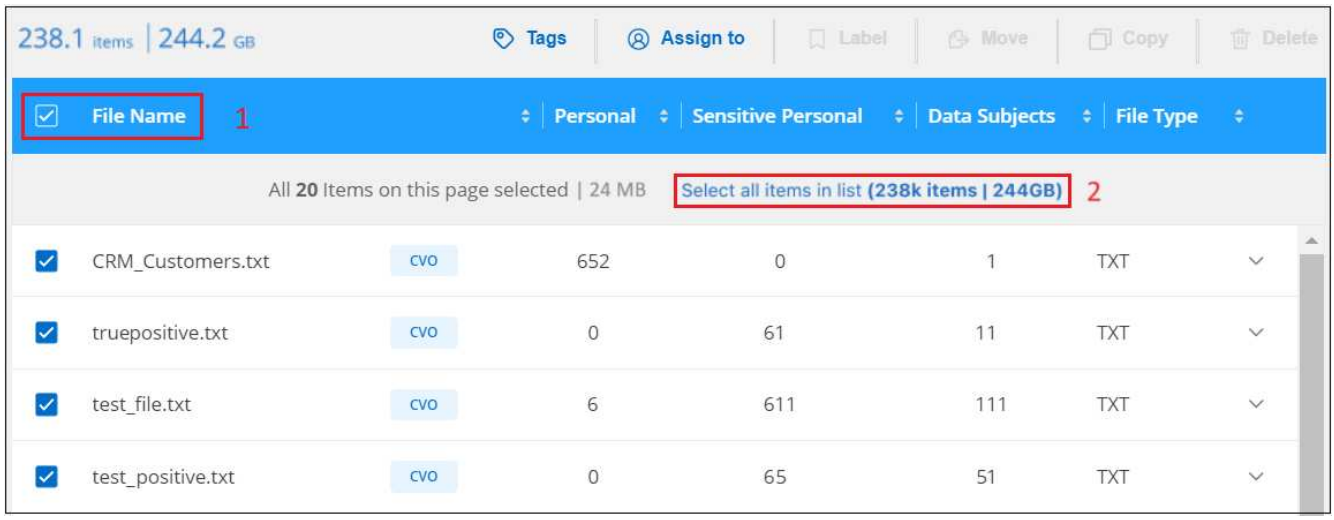
단계

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

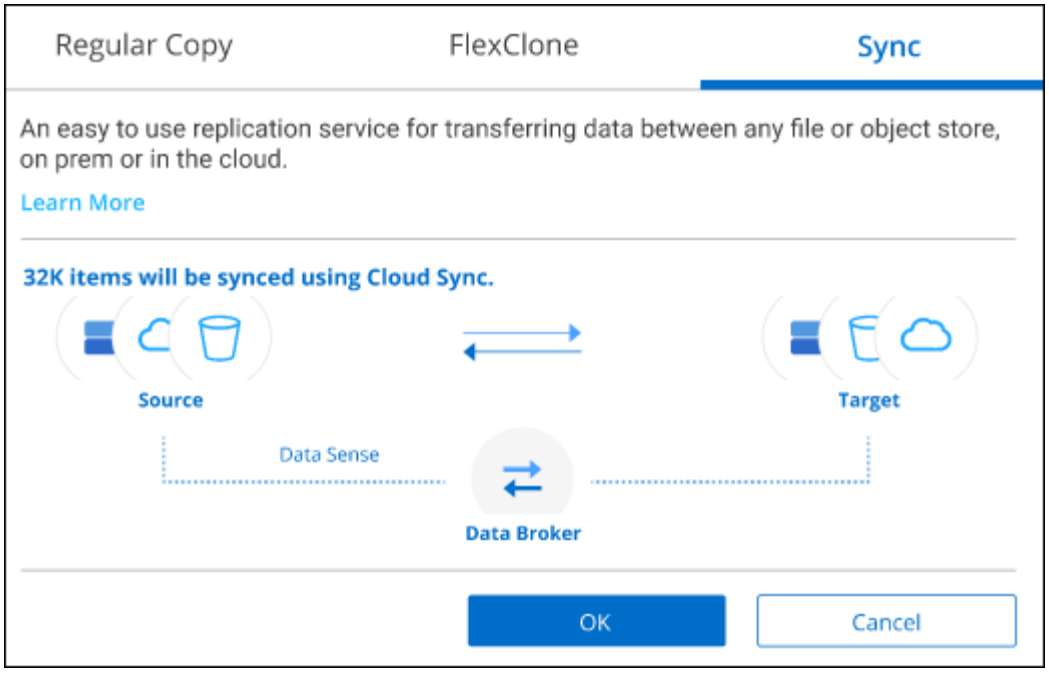


   대상 시스템에 복사 및 동기화할 파일만 표시되도록 다른 필터를 적용합니다.

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



3. 파일 복사 대화 상자에서 * 동기화 * 탭을 선택합니다.



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

   BlueXP 복사 및 동기화 UI는 BlueXP에서 열립니다.

   동기화 관계를 정의하라는 메시지가 표시됩니다. 소스 시스템은 BlueXP 분류에서 이미 선택한 리포지토리와 파일을 기반으로 미리 채워집니다.

5. 대상 시스템을 선택한 다음 사용하려는 데이터 브로커를 선택(또는 생성)해야 합니다. 부터 BlueXP 복사 및 동기화 요구 사항을 검토합니다 "빠른 시작 설명".

결과

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

BlueXP 분류에서 호출되면 일반적인 BlueXP 복사 및 동기화 작업 중 일부가 비활성화됩니다.

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

소스 파일을 **NFS** 공유로 이동합니다

BlueXP 분류에서 스캔 중인 소스 파일을 모든 NFS 공유로 이동할 수 있습니다. NFS 공유를 BlueXP 분류와 통합할 필요가 없습니다.

필요한 경우 이동 파일 위치에 이동 경로 파일을 그대로 둘 수 있습니다. Breadcrumb 파일을 사용하면 파일이 원래 위치에서 이동된 이유를 쉽게 이해할 수 있습니다. 이동된 각 파일에 대해 시스템은 "<filename> -breadcrumb -<date>.txt"라는 소스 위치에 Breadcrumb 파일을 만듭니다. Breadcrumb 파일에 추가될 대화 상자에서 텍스트를 추가하여 파일이 이동된 위치와 파일을 이동한 사용자를 나타낼 수 있습니다.

파일을 이동할 때 소스 파일의 하위 디렉토리 구조가 대상 공유에서 다시 생성되므로 파일이 이동된 위치를 쉽게 파악할 수 있습니다. 대상 위치에 같은 이름의 파일이 있으면 파일이 이동하지 않습니다.

데이터베이스에 있는 파일은 이동할 수 없습니다.

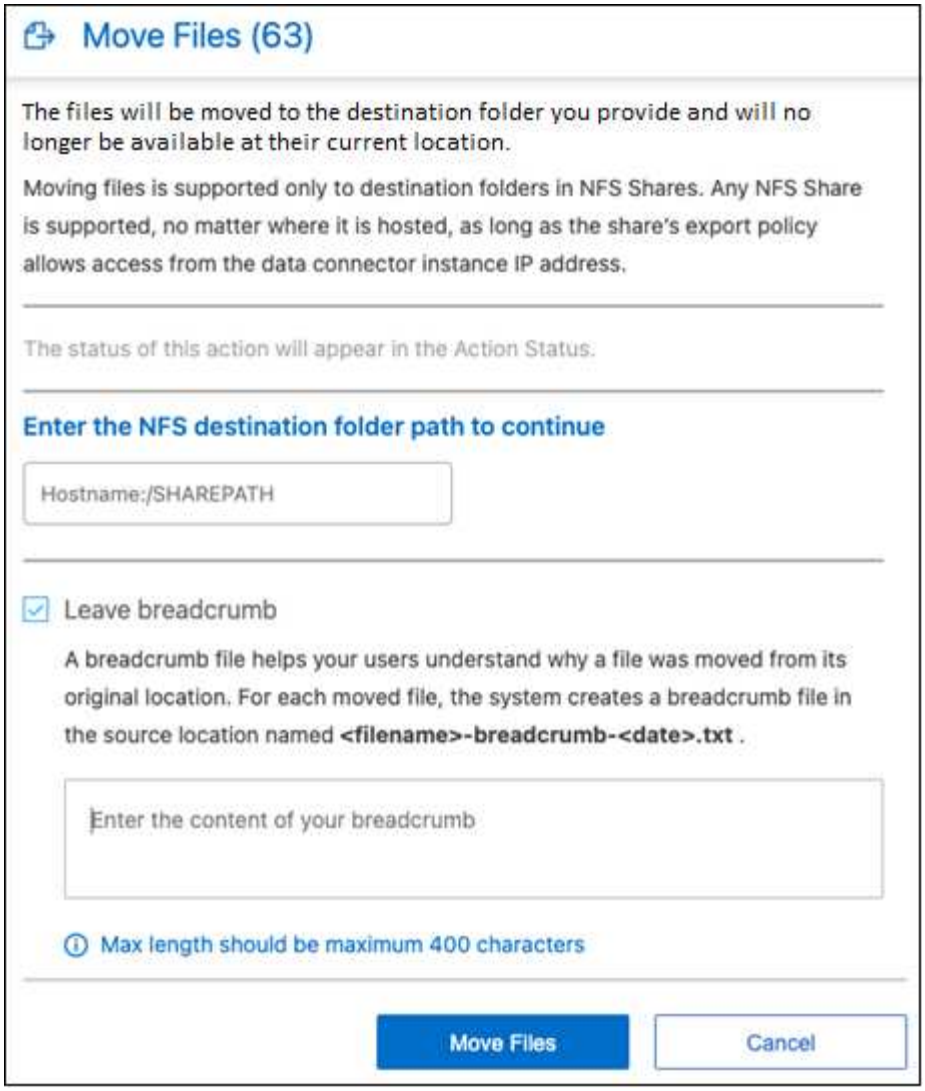
요구 사항

- 파일을 이동하려면 계정 관리자 또는 작업 영역 관리자 역할이 있어야 합니다.
- 소스 파일은 온-프레미스 ONTAP, Cloud Volumes ONTAP, Azure NetApp Files, 파일 공유 및 SharePoint Online 데이터 원본에 위치할 수 있습니다.
- 한 번에 최대 1500만 개의 파일을 이동할 수 있습니다.
- 50MB 이하의 파일만 이동됩니다.
- 대상 NFS 공유에서 BlueXP 분류 인스턴스 IP 주소에서 액세스할 수 있어야 합니다.

단계

1. 데이터 조사 결과 창에서 이동할 파일을 선택합니다.

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



3. Move Files_ 대화 상자에서 선택한 모든 파일이 "<host_name>:/<share_path>" 형식으로 이동될 NFS 공유의 이름을 입력합니다.
4. Breadcrumb 파일을 그대로 두려면 _Breadcrumb_상자를 선택합니다. 대화 상자에 텍스트를 입력하여 파일이 이동된 위치, 파일을 이동한 사용자 및 파일이 이동된 이유와 같은 기타 정보를 나타낼 수 있습니다.
5. 파일 이동 * 을 클릭합니다.

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

원본 파일을 삭제합니다

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

조사 창 또는 에서 파일을 수동으로 삭제할 수 있습니다 "정책을 자동으로 사용합니다".

데이터베이스에 있는 파일은 삭제할 수 없습니다. 다른 모든 데이터 원본은 지원됩니다.

파일을 삭제하려면 다음 권한이 필요합니다.

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

소스 파일을 수동으로 삭제합니다

요구 사항

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

단계

1. 데이터 조사 결과 창에서 삭제할 파일을 선택합니다.

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

2. 버튼 모음에서 * 삭제 * 를 클릭합니다.
3. 삭제 작업은 영구적이므로 후속 _Delete File_대화 상자에 " * 영구 삭제 * "를 입력하고 * 파일 삭제 * 를 클릭해야 합니다.

에서 삭제 작업의 진행률을 볼 수 있습니다 "작업 상태 창".

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

규정 준수 보고서 보기

BlueXP 분류는 조직의 데이터 개인 정보 보호 프로그램 상태를 보다 잘 이해하기 위해 사용할 수 있는 보고서를 제공합니다.

기본적으로 BlueXP 분류 대시보드에는 모든 작업 환경, 데이터베이스 및 데이터 소스에 대한 규정 준수 및 거버넌스 데이터가 표시됩니다. 일부 작업 환경에 대한 데이터만 포함된 보고서를 보려면 작업 환경을 선택합니다.

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

개인 정보 보호 위험 평가 보고서

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

준수 상태

A 심각도 점수 또한 데이터가 중요하지 않거나 개인적이거나 민감한 개인이든 상관없이 배포할 수 있습니다.

평가 개요

발견된 개인 데이터 유형 및 데이터 범주에 대한 분석.

이 평가의 데이터 주체

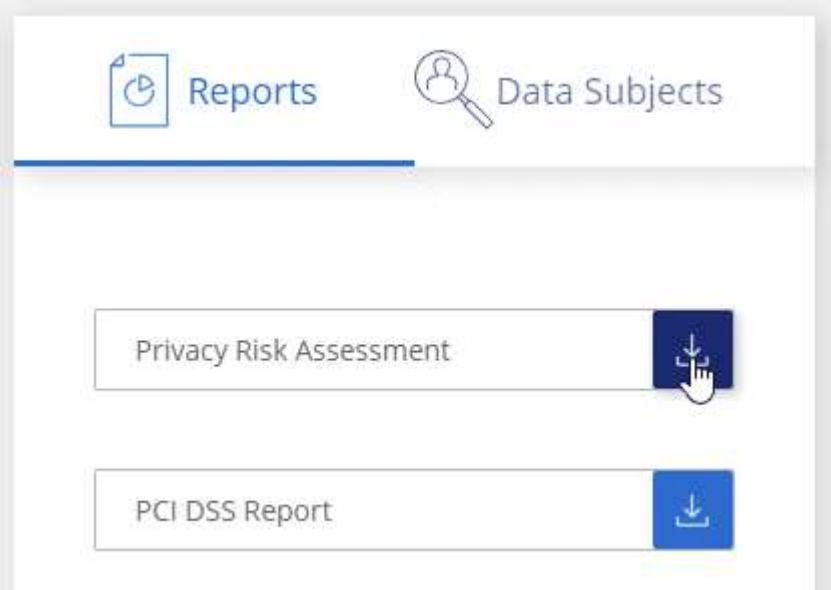
국가 식별자가 발견된 위치별 사람 수.

개인정보 보호 위험 평가 보고서를 생성합니다

준수 탭으로 이동하여 보고서를 생성합니다.

단계

1. BlueXP 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. Compliance * 를 클릭한 다음 * Reports * 에서 * Privacy Risk Assessment * 옆에 있는 다운로드 아이콘을 클릭합니다.



결과

BlueXP 분류는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

심각도 점수

BlueXP 분류는 세 가지 변수를 기준으로 개인 정보 보호 위험 평가 보고서의 심각도 점수를 계산합니다.

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

점수를 결정하는 데 사용되는 논리는 다음과 같습니다.

심각도 점수	논리
0	세 가지 변수는 모두 정확히 0%입니다
1	변수 중 하나가 0%보다 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	변수 중 두 개가 15%보다 큽니다
10	세 개의 변수가 15%보다 큽니다

PCI DSS 보고서

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

개요

신용 카드 정보와 작업 환경이 포함된 파일 수

암호화

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

랜섬웨어 보호

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

보존

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

신용 카드 정보 배포

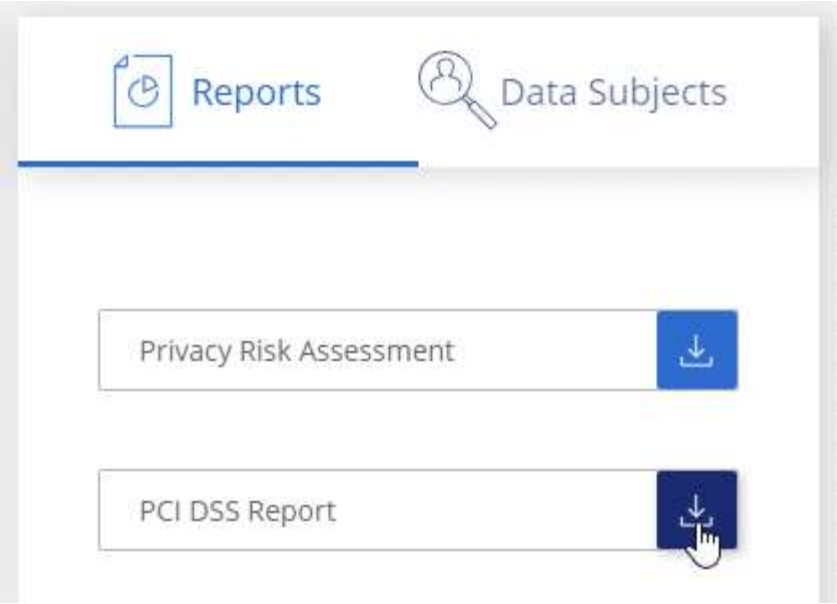
신용 카드 정보가 발견된 작업 환경 및 암호화 및 랜섬웨어 방지 기능이 활성화되어 있는지 여부

PCI DSS 보고서를 생성합니다

준수 탭으로 이동하여 보고서를 생성합니다.

단계

1. BlueXP 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. 규정 준수 * 를 클릭한 다음 * 보고서 * 에서 * PCI DSS 보고서 * 옆에 있는 다운로드 아이콘을 클릭합니다.



결과

BlueXP 분류는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

HIPAA 보고서

HIPAA(Health Insurance Portability and Accountability Act) 보고서를 통해 건강 정보가 포함된 파일을 확인할 수 있습니다. HIPAA 데이터 개인 정보 보호 법률을 준수하기 위한 조직의 요구 사항을 지원하도록 설계되었습니다. BlueXP 분류에서 확인할 수 있는 정보는 다음과 같습니다.

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

보고서에는 다음 정보가 포함됩니다.

개요

상태 정보가 포함된 파일 수와 작업 환경이 포함된 파일 수

암호화

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

랜섬웨어 보호

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

보존

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

유용합니다.

건강 정보 배포

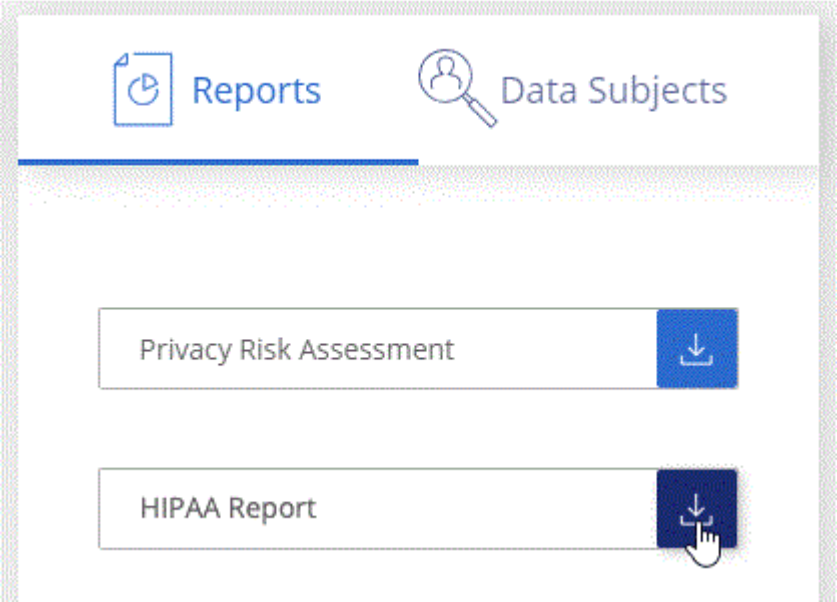
상태 정보가 발견된 작업 환경 및 암호화 및 랜섬웨어 방지 기능이 활성화되어 있는지 여부

HIPAA 보고서를 생성합니다

준수 탭으로 이동하여 보고서를 생성합니다.

단계

1. BlueXP 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. 규정 준수 * 를 클릭한 다음 * 보고서 * 에서 * HIPAA 보고서 * 옆에 있는 다운로드 아이콘을 클릭합니다.



결과

BlueXP 분류는 PDF 보고서를 생성하여 필요에 따라 다른 그룹에 검토 및 전송할 수 있습니다.

데이터 주체 액세스 요청이란 무엇입니까?

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

피험자의 전체 이름 또는 알려진 식별자(예: 이메일 주소)를 검색한 다음 보고서를 다운로드하여 DSAR에 응답할 수 있습니다. 이 보고서는 GDPR 또는 이와 유사한 데이터 개인 정보 보호 법률을 준수하기 위한 조직의 요구 사항을 지원하도록 설계되었습니다.

BlueXP 분류는 **SAR**에 대응하는 데 어떤 도움이 됩니까**?**

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

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

> 현재 데이터베이스 내에서 데이터 주제 검색이 지원되지 않습니다.

데이터 주제를 검색하고 보고서를 다운로드합니다

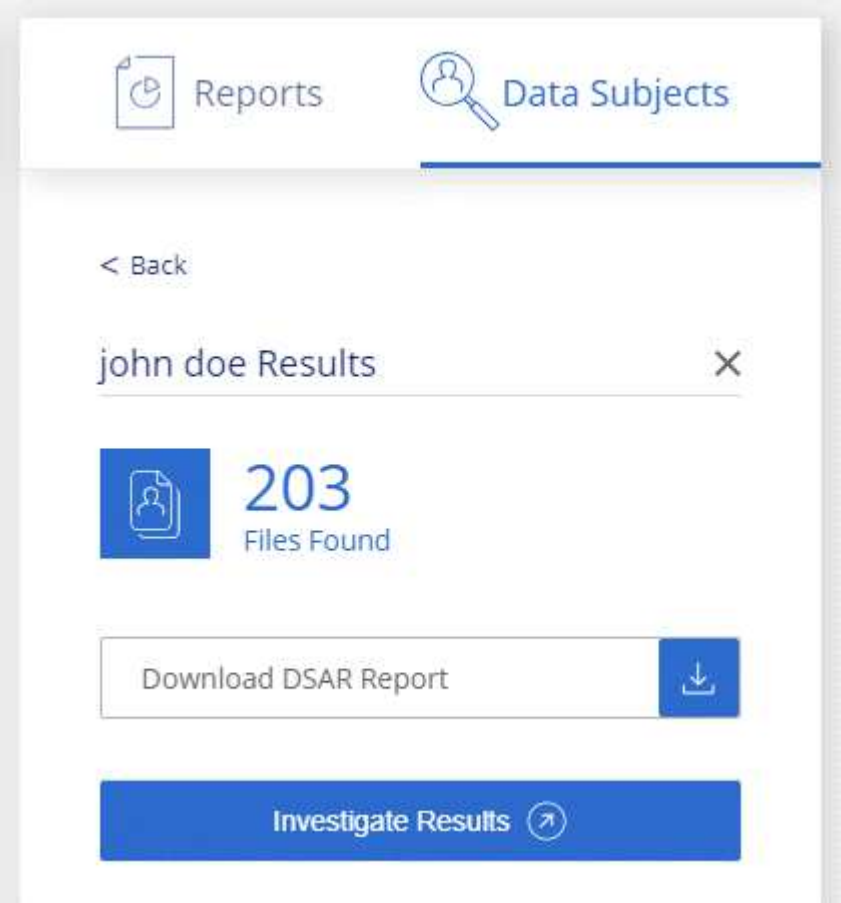
데이터 주체의 전체 이름 또는 알려진 식별자를 검색한 다음 파일 목록 보고서 또는 DSAR 보고서를 다운로드합니다. 검색할 수 있는 기준 "모든 개인 정보 유형입니다".

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

단계

1. BlueXP 메뉴에서 * 거버넌스 > 분류 * 를 클릭합니다.
2. 데이터 제목 * 을 클릭합니다.
3. 데이터 제목의 전체 이름 또는 알려진 식별자를 검색합니다.

   다음은 name_john doe_에 대한 검색을 보여 주는 예입니다.



4. 사용 가능한 옵션 중 하나를 선택합니다.
   - * DSAR 보고서 다운로드 *: 데이터 주체에 전송할 수 있는 액세스 요청에 대한 공식 응답입니다. 이 보고서에는 데이터 주체에 있는 BlueXP 분류 데이터를 기반으로 자동으로 생성된 정보가 포함되며 템플릿으로 사용하도록

설계되었습니다. 양식을 작성하여 내부적으로 검토한 후 데이터 제목으로 보내야 합니다.

- * 결과 조사 *: 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 파일 목록을 다운로드하여 데이터를 조사할 수 있는 페이지입니다.

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

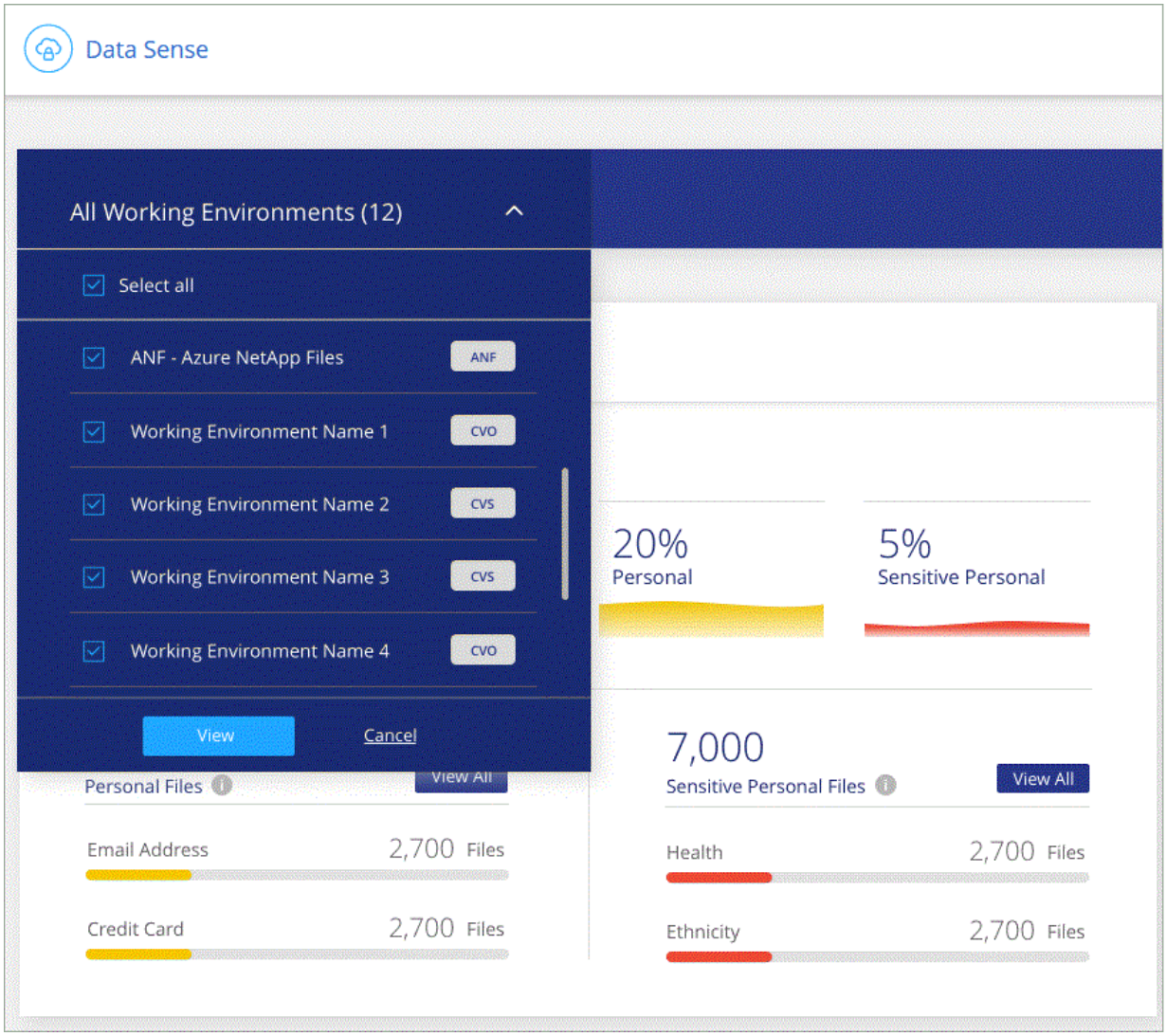
보고서의 작업 환경을 선택합니다

BlueXP 분류 준수 대시보드의 내용을 필터링하여 모든 작업 환경 및 데이터베이스의 규정 준수 데이터를 확인하거나 특정 작업 환경에 대한 규정 준수 데이터를 확인할 수 있습니다.

대시보드를 필터링할 때 BlueXP 분류는 규정 준수 데이터와 보고서를 선택한 작업 환경에만 설정합니다.

단계

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



BlueXP 분류 관리

BlueXP 분류 스캔에 개인 데이터 식별자를 추가합니다

BlueXP 분류는 BlueXP 분류가 향후 검색에서 식별할 수 있는 "개인 데이터"의 사용자 지정 목록을 추가할 수 있는 여러 가지 방법을 제공하므로, 중요한 데이터가 _ALL_귀하의 조직 파일에 있는 위치에 대한 전체적인 정보를 얻을 수 있습니다.

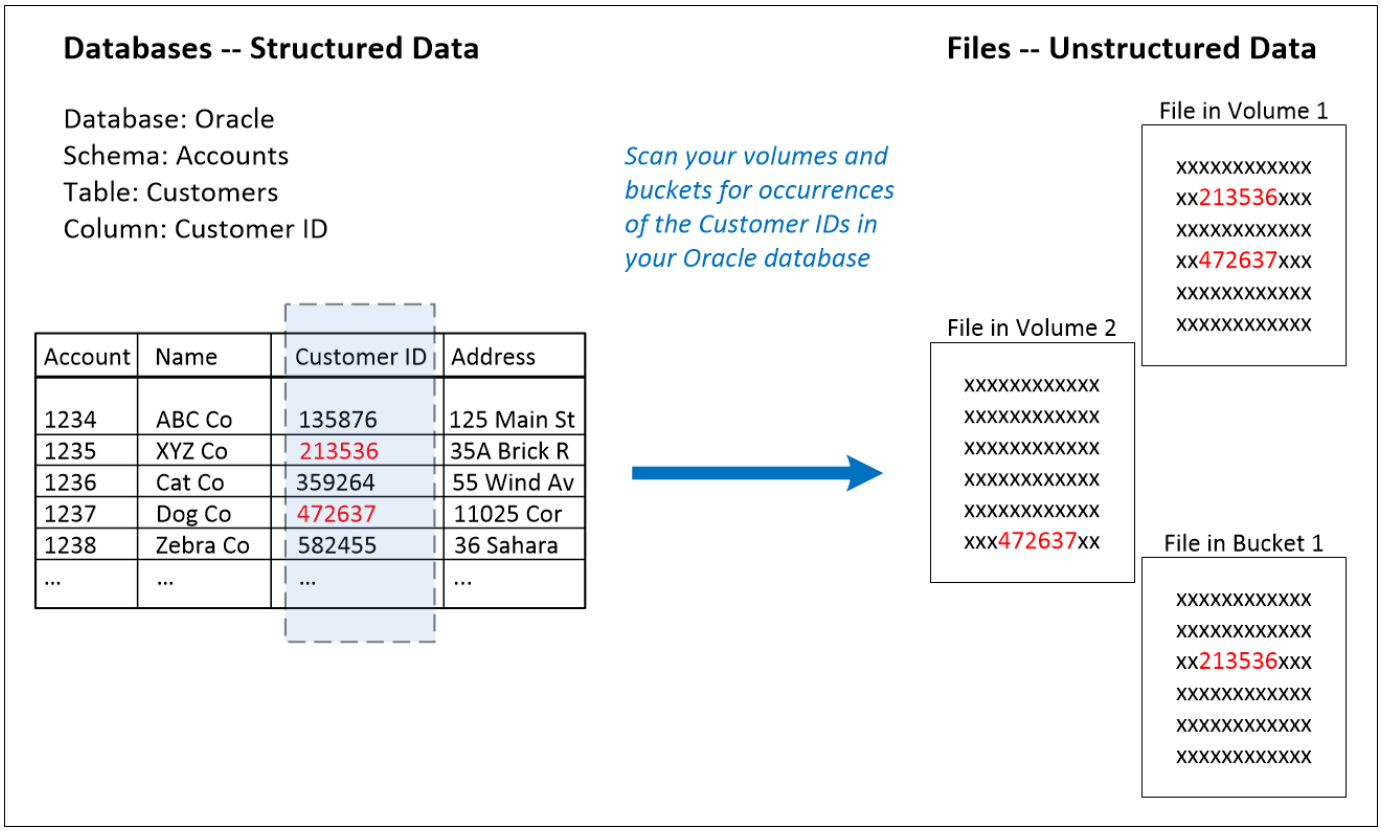
- 검색 중인 데이터베이스의 특정 열을 기준으로 고유 식별자를 추가할 수 있습니다.
- 텍스트 파일에서 사용자 지정 키워드를 추가할 수 있습니다. — 이러한 단어는 데이터 내에서 식별됩니다.
- 정규식(regex)을 사용하여 개인 패턴을 추가할 수 있습니다. regex는 기존의 미리 정의된 패턴에 추가됩니다.
- 사용자 지정 범주를 추가하여 데이터에서 특정 범주의 정보를 찾을 위치를 식별할 수 있습니다.

사용자 정의 검색 기준을 추가하는 이러한 모든 메커니즘은 모든 언어에서 지원됩니다.

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

데이터베이스에서 사용자 지정 개인 데이터 식별자를 추가합니다

Data Fusion _ 라는 기능을 사용하면 조직의 데이터를 스캔하여 데이터베이스에서 고유한 식별자가 다른 데이터 소스에서 검색되는지 여부를 확인할 수 있습니다. 데이터베이스 테이블에서 특정 열 또는 열을 선택하여 BlueXP 분류에서 검색할 추가 식별자를 선택할 수 있습니다. 예를 들어, 아래 다이어그램은 Data Fusion를 사용하여 볼륨, 버킷 및 데이터베이스를 검사하여 Oracle 데이터베이스에서 모든 고객 ID를 확인하는 방법을 보여 줍니다.



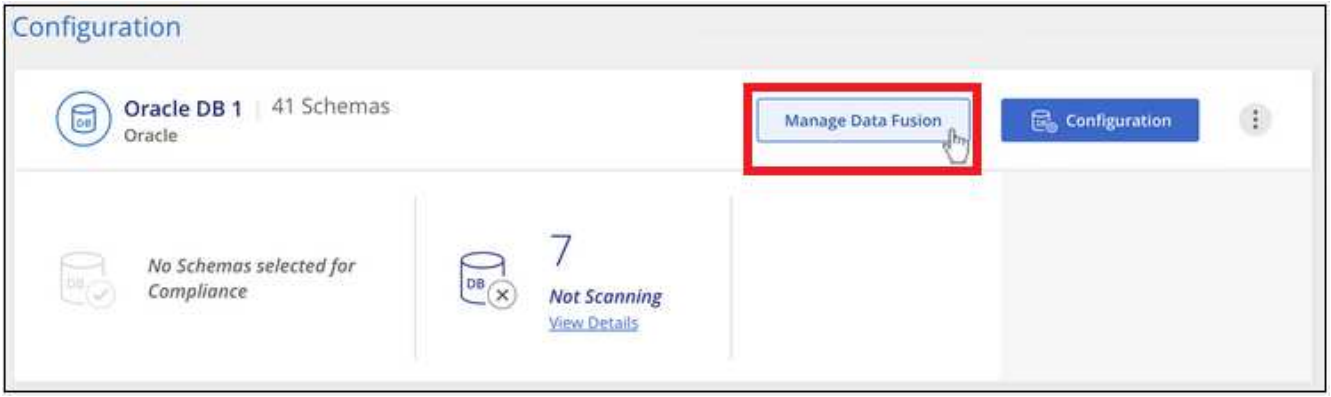
보시다시피, 2개의 볼륨과 1개의 S3 버킷에서 2개의 고유 고객 ID가 발견되었습니다. 데이터베이스 테이블의 모든 일치 항목도 식별됩니다.

자신의 데이터베이스를 스캔하기 때문에 데이터가 저장된 언어는 향후 BlueXP 분류 검사에서 데이터를 식별하는 데 사용됩니다.

단계

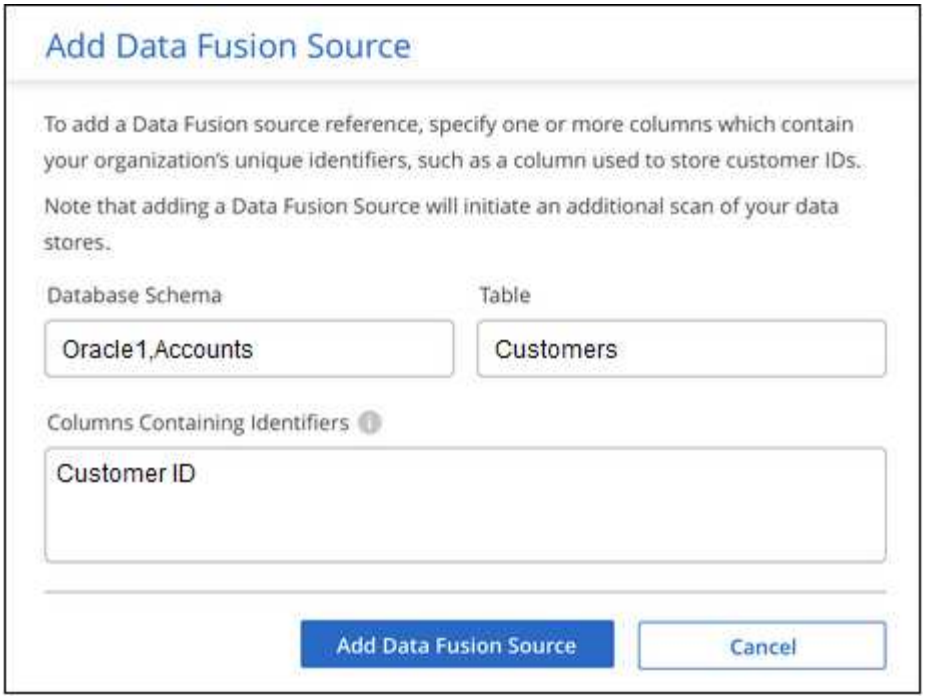
이(가) 있어야 합니다 "하나 이상의 데이터베이스 서버가 추가되었습니다" 데이터 Fusion 소스를 추가하기 전에 BlueXP 분류를 수행합니다.

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

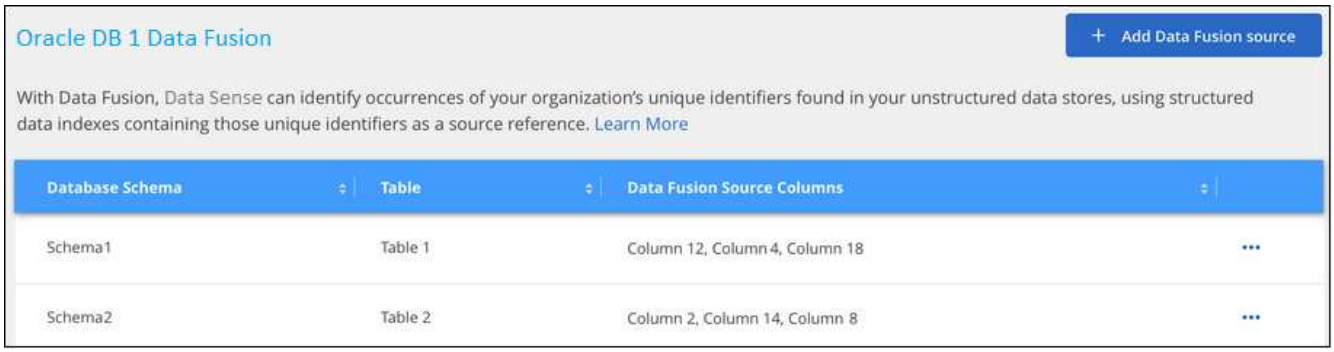


2. 다음 페이지에서 * 데이터 Fusion 소스 추가 * 를 클릭합니다.
3. Add Data Fusion Source _ 페이지에서 다음을 수행합니다.
   a. 드롭다운 메뉴에서 데이터베이스 스키마를 선택합니다.
   b. 해당 스키마에 테이블 이름을 입력합니다.
   c. 사용할 고유 식별자가 포함된 열 또는 열을 입력합니다.

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

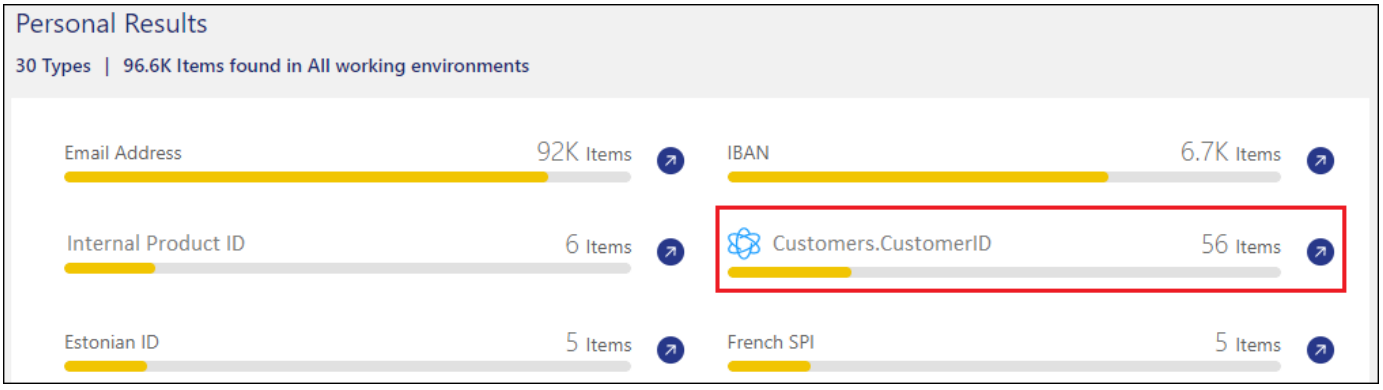


4. 데이터 Fusion 소스 추가 * 를 클릭합니다.



결과

다음 검사 후 결과에는 이 새 정보가 "개인 결과" 섹션의 준수 대시보드 및 "개인 데이터" 필터의 조사 페이지에 포함됩니다. 분류자에 사용한 이름이 필터 목록에 나타납니다(예:) `Customers.CustomerID`.



Data Fusion 소스를 삭제합니다

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

단어 목록에서 사용자 지정 키워드를 추가합니다

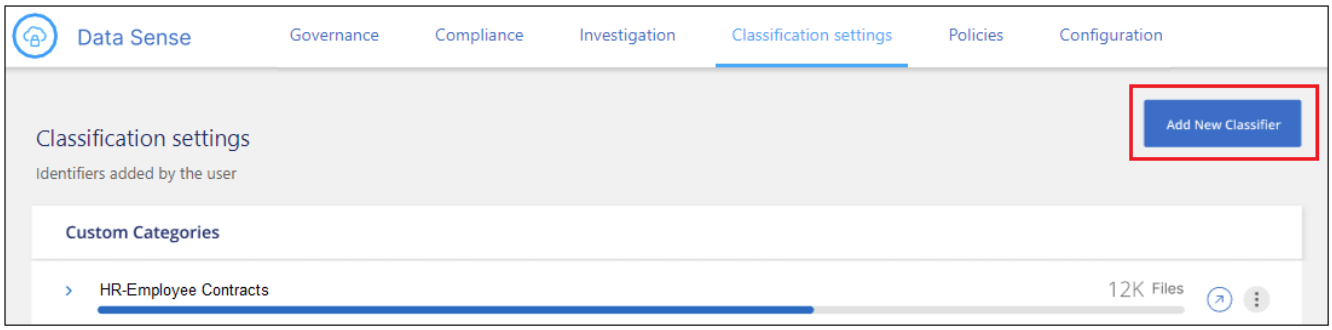
사용자 지정 키워드를 BlueXP 분류에 추가하여 데이터에서 해당 정보가 있는 위치를 식별할 수 있습니다. BlueXP 분류를 인식할 각 단어를 입력하여 키워드를 추가합니다. 키워드는 BlueXP 분류에서 이미 사용하는 기존의 미리 정의된 키워드에 추가되며, 결과는 개인 패턴 섹션 아래에 표시됩니다.

예를 들어, 안전하지 않은 위치에서 이러한 이름에 액세스할 수 없도록 모든 파일에서 내부 제품 이름이 언급된 위치를 확인할 수 있습니다.

사용자 지정 키워드를 업데이트한 후 BlueXP 분류는 모든 데이터 소스 스캔을 다시 시작합니다. 검사가 완료되면 "개인 결과" 섹션 아래의 BlueXP 분류 준수 대시보드와 "개인 데이터" 필터의 조사 페이지에 새 결과가 나타납니다.

단계

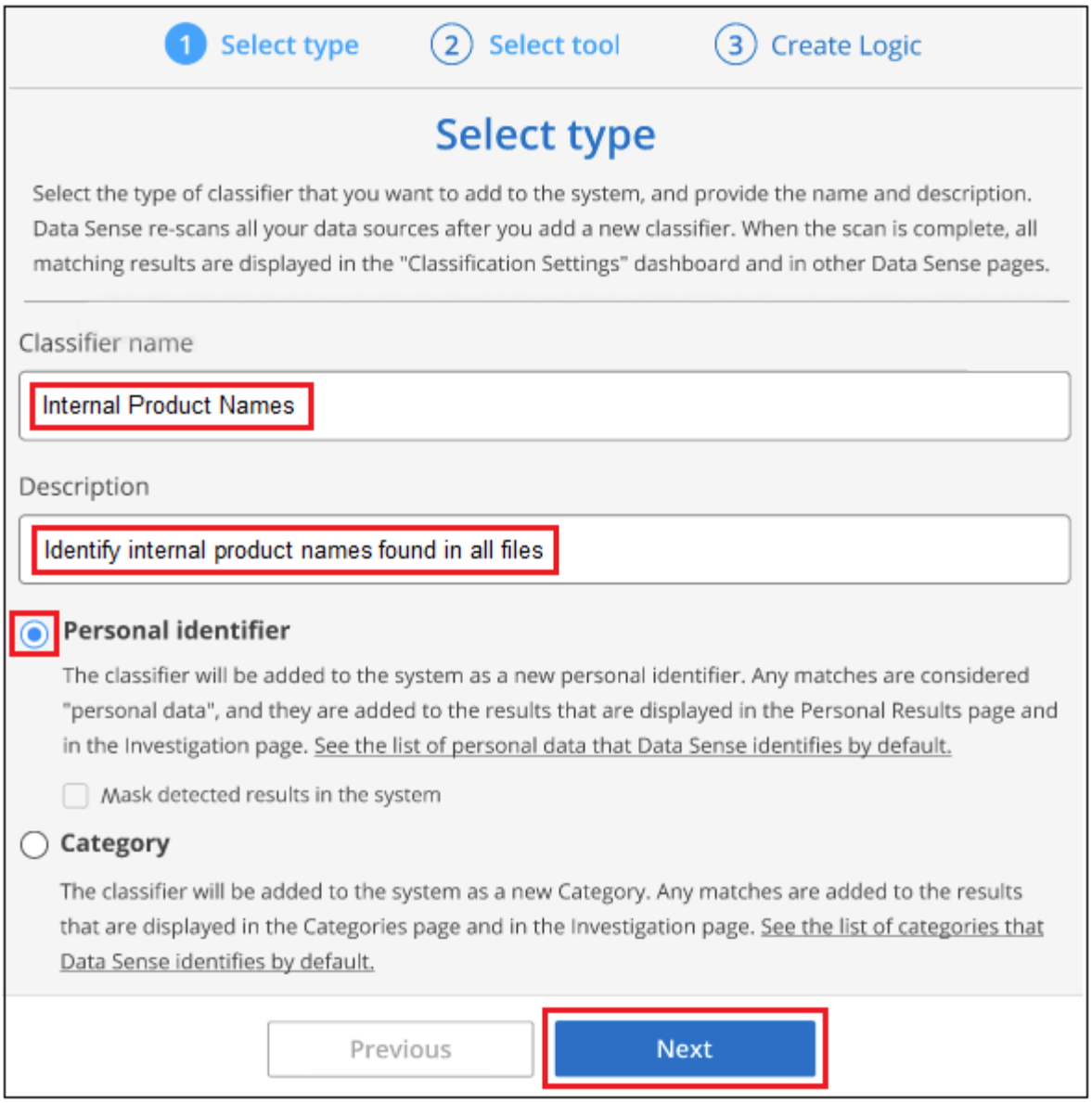
1. Classification settings_tab에서 * Add New Classifier * 를 클릭하여 _Add Custom Classifier_wizard를 실행합니다.



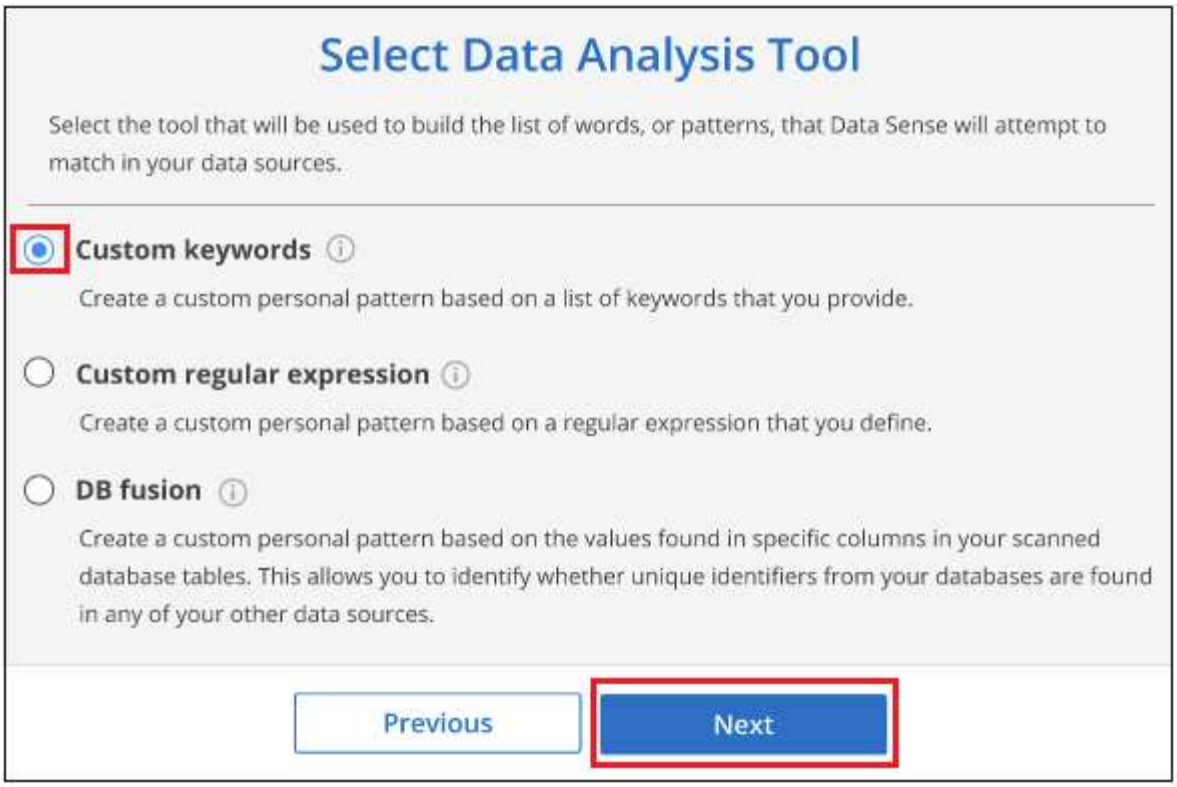
2. 종류 선택_페이지에서 분류자의 이름을 입력하고 간단한 설명을 입력한 다음 * 개인 식별자 * 를 선택하고 * 다음 * 을 클릭합니다.

   입력한 이름은 BlueXP 분류 UI에 분류자 요구 사항과 일치하는 스캔된 파일의 머리글로, 조사 페이지의 필터 이름으로 표시됩니다.

   "시스템에서 검색된 결과 마스크" 확인란을 선택하여 UI에 전체 결과가 나타나지 않도록 할 수도 있습니다. 예를 들어, 전체 신용 카드 번호나 비슷한 개인 데이터를 숨기려면 이 작업을 수행할 수 있습니다. 이러한 마스크는 UI에 "**** **** ****" 3434).

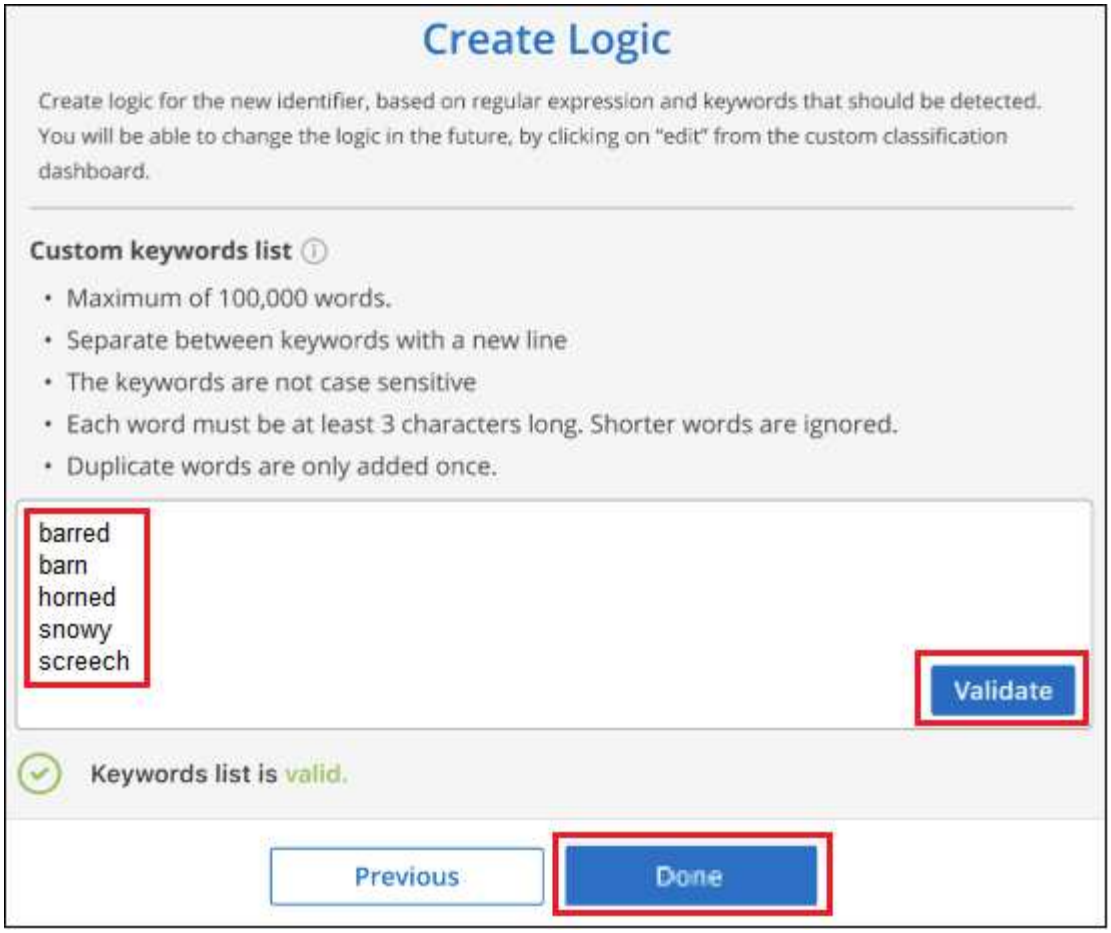


3. 데이터 분석 선택 도구_페이지에서 분류자를 정의하는 데 사용할 방법으로 * 사용자 정의 키워드 * 를 선택한 후 * 다음 * 을 클릭합니다.



4. Create Logic_page에서 인식하려는 키워드(각 단어를 별도의 줄에 입력)를 입력하고 * Validate * 를 클릭합니다.

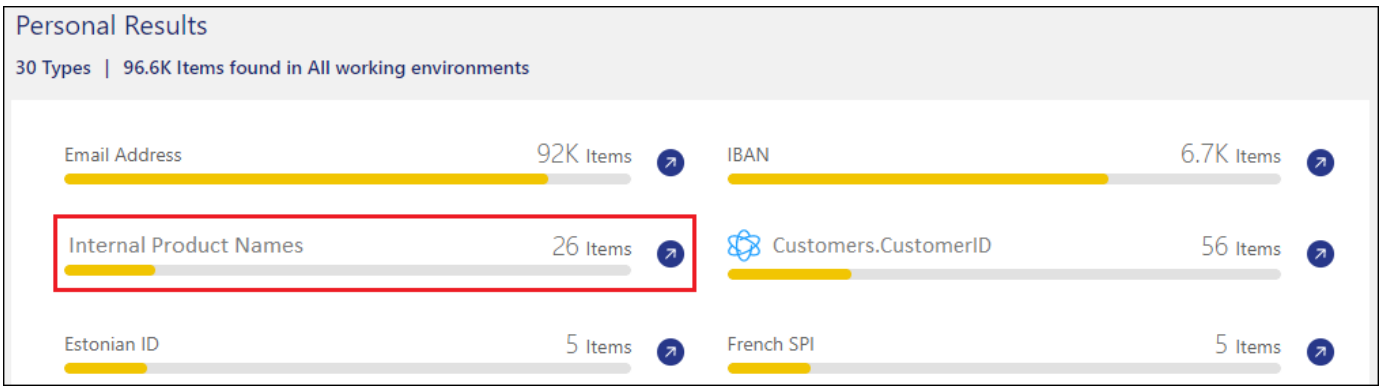
   아래 스크린샷은 내부 제품 이름(부엉이의 여러 유형)을 보여줍니다. 이러한 항목에 대한 BlueXP 분류 검색은 대/소문자를 구분하지 않습니다.



5. Done(완료) * 을 클릭하면 BlueXP 분류가 시작되어 데이터를 다시 검색합니다.

결과

검사가 완료되면 "개인 결과" 섹션의 준수 대시보드 및 "개인 데이터" 필터의 조사 페이지에 이 새로운 정보가 결과에 포함됩니다.



보시다시피 분류자의 이름은 개인 결과 패널에서 이름으로 사용됩니다. 이러한 방식으로 여러 키워드 그룹을 활성화하고 각 그룹의 결과를 볼 수 있습니다.

regex를 사용하여 사용자 지정 개인 데이터 식별자를 추가합니다

사용자 지정 정규식(regex)을 사용하여 개인 패턴을 추가하여 데이터의 특정 정보를 식별할 수 있습니다. 이렇게 하면 새 사용자 지정 regex를 만들어 시스템에 아직 존재하지 않는 새로운 개인 정보 요소를 식별할 수 있습니다. regex는

BlueXP 분류에서 이미 사용하는 기존의 사전 정의된 패턴에 추가되며, 결과는 개인 패턴 섹션에서 볼 수 있습니다.

예를 들어 모든 파일에서 내부 제품 ID가 언급된 위치를 확인할 수 있습니다. 예를 들어 제품 ID가 명확한 구조를 갖는 경우 201로 시작하는 12자리 숫자입니다. 사용자 지정 regex 기능을 사용하여 파일에서 검색할 수 있습니다. 이 예제의 정규식은 *\b201\d{9}\b * 입니다.

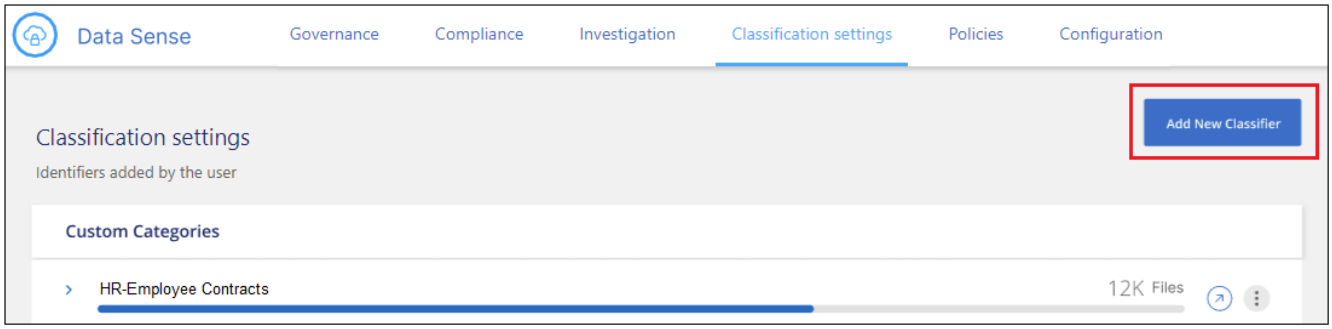
regex를 추가한 후 BlueXP 분류는 모든 데이터 소스 스캔을 다시 시작합니다. 검사가 완료되면 "개인 결과" 섹션 아래의 BlueXP 분류 준수 대시보드와 "개인 데이터" 필터의 조사 페이지에 새 결과가 나타납니다.

정규식을 작성하는 데 도움이 필요한 경우 을 참조하십시오 "정규식 101". 원하는 맛을 내려면 * Python * 을 선택하여 BlueXP 분류가 정규식에서 일치하는 결과의 유형을 확인하십시오. 를 클릭합니다 "Python Regex 테스터 페이지입니다" 또한 패턴의 그래픽 표현을 표시할 때 유용합니다.

현재 정규식 생성 시 패턴 플래그 사용을 허용하지 않습니다. 즉, "/"를 사용하면 안 됩니다.

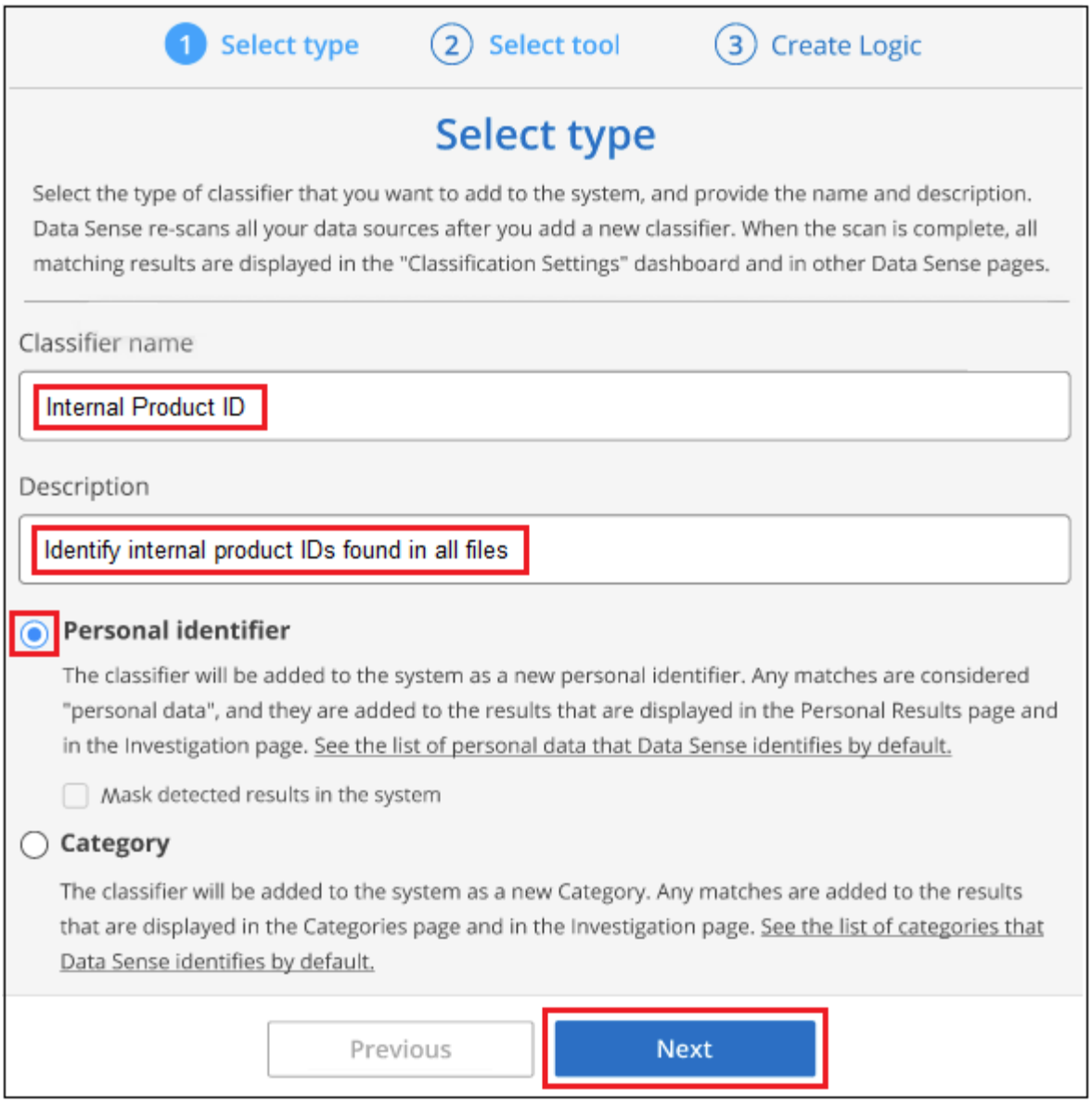
단계

1. Classification settings_tab에서 * Add New Classifier * 를 클릭하여 _Add Custom Classifier_wizard를 실행합니다.

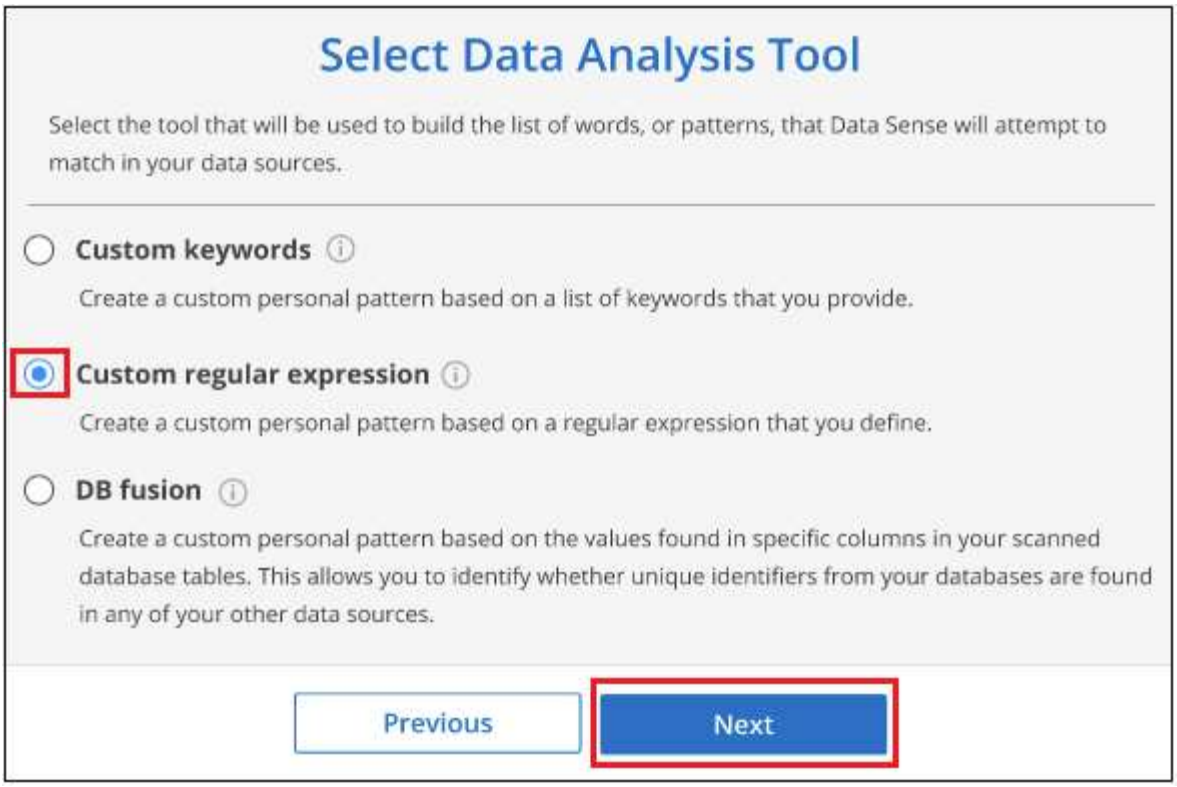


2. 종류 선택_페이지에서 분류자의 이름을 입력하고 간단한 설명을 입력한 다음 * 개인 식별자 * 를 선택하고 * 다음 * 을 클릭합니다.

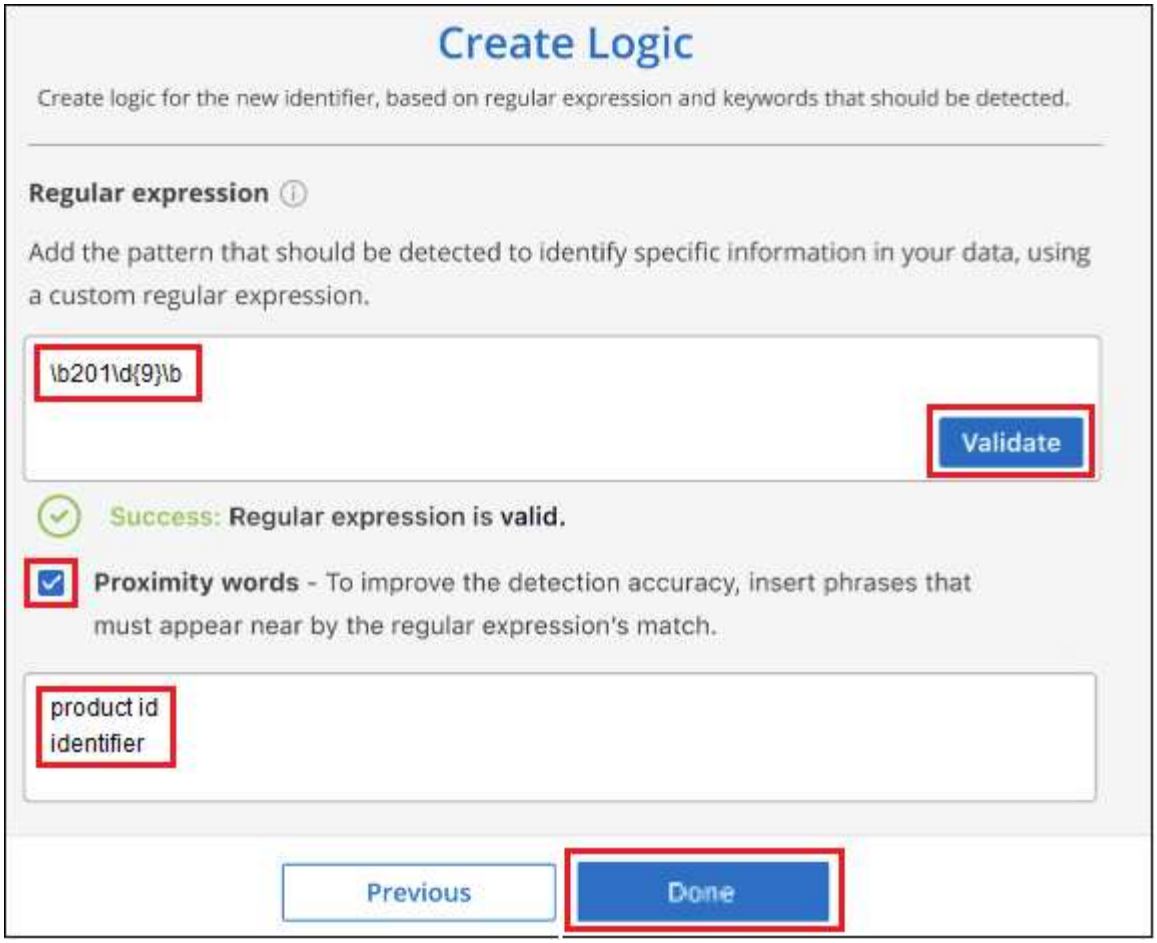
   입력한 이름은 BlueXP 분류 UI에 분류자 요구 사항과 일치하는 스캔된 파일의 머리글로, 조사 페이지의 필터 이름으로 표시됩니다. "시스템에서 검색된 결과 마스크" 확인란을 선택하여 UI에 전체 결과가 나타나지 않도록 할 수도 있습니다. 예를 들어 전체 신용 카드 번호나 이와 유사한 개인 데이터를 숨기려면 이 작업을 수행할 수 있습니다.



3. Select Data Analysis Tool_page에서 분류자를 정의하는 데 사용할 방법으로 * 사용자 지정 정규식 * 을 선택한 후 * 다음 * 을 클릭합니다.

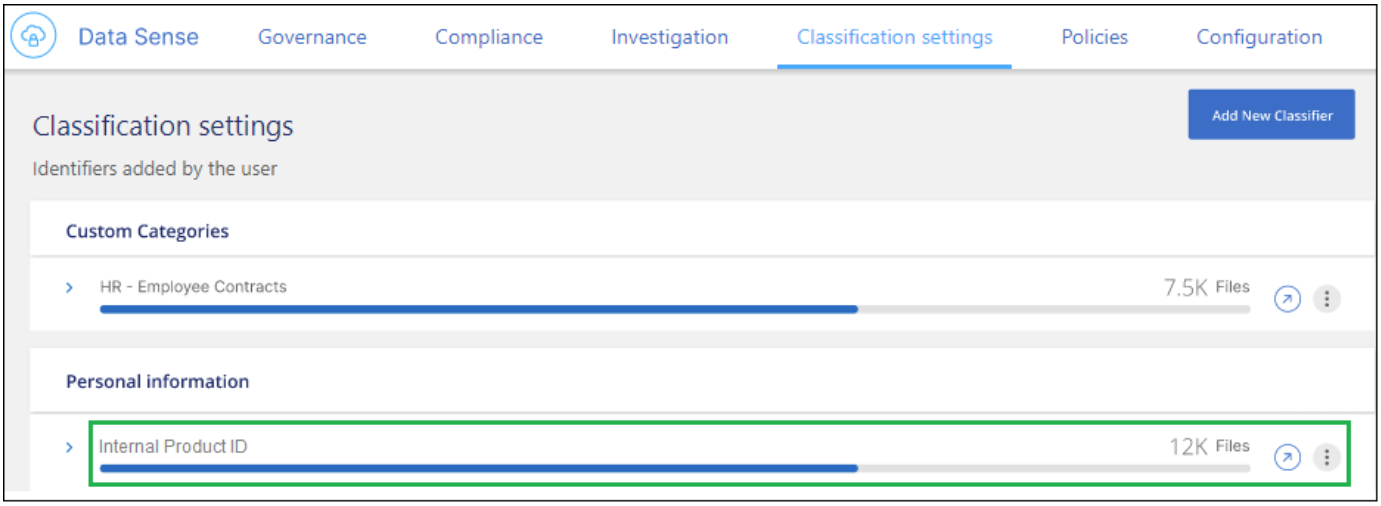


4. Create Logic_page에서 정규식과 근접 단어를 입력하고 * Done * 을 클릭합니다.
   a. 임의의 법적 정규식을 입력할 수 있습니다. BlueXP 분류에 따라 * Validate * 버튼을 클릭하여 정규식이 유효한지, 정규식이 너무 광범위하지 않은지 확인합니다. 즉, 너무 많은 결과가 반환됩니다.
   b. 선택적으로 근접 단어를 입력하여 결과의 정확도를 높일 수 있습니다. 일반적으로 검색하는 패턴의 300자 이내(찾은 패턴 이전 또는 이후)에 있는 단어입니다. 각 단어 또는 구를 별도의 줄에 입력합니다.



결과

분류자가 추가되고 BlueXP 분류가 모든 데이터 원본을 다시 검색합니다. 사용자 지정 분류자 페이지로 돌아가 새 분류자에 맞는 파일 수를 볼 수 있습니다. 모든 데이터 원본을 스캔하여 얻은 결과는 스캔해야 하는 파일 수에 따라 다소 시간이 걸릴 수 있습니다.



사용자 지정 범주를 추가합니다

BlueXP 분류는 스캔한 데이터를 다양한 유형의 범주로 나눕니다. 범주는 각 파일의 콘텐츠 및 메타데이터에 대한 인공지능 분석을 기반으로 하는 주제입니다. "미리 정의된 범주 목록을 참조하십시오".

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

사용자 지정 범주를 BlueXP 분류에 추가하여 데이터 자산에 고유한 정보 범주를 데이터에서 찾을 수 있도록 할 수 있습니다. 식별하려는 데이터 범주가 포함된 "교육" 파일을 만들어 각 범주를 추가한 다음 BlueXP 분류 기능이 해당 파일을 스캔하여 AI를 통해 "학습"하여 데이터 소스에서 해당 데이터를 식별하도록 합니다. 범주는 BlueXP 분류에서 이미 식별한 기존의 미리 정의된 범주에 추가되며, 결과는 범주 섹션 아래에 표시됩니다.

예를 들어, 필요한 경우 제거할 수 있도록 .gz 형식의 압축된 설치 파일이 파일에서 어디에 있는지 확인할 수 있습니다.

사용자 지정 범주를 업데이트한 후 BlueXP 분류는 모든 데이터 소스 스캔을 다시 시작합니다. 검사가 완료되면 새 결과가 "범주" 섹션의 BlueXP 분류 준수 대시보드 및 "범주" 필터의 조사 페이지에 나타납니다. "범주별로 파일을 보는 방법을 확인하십시오".

필요한 것

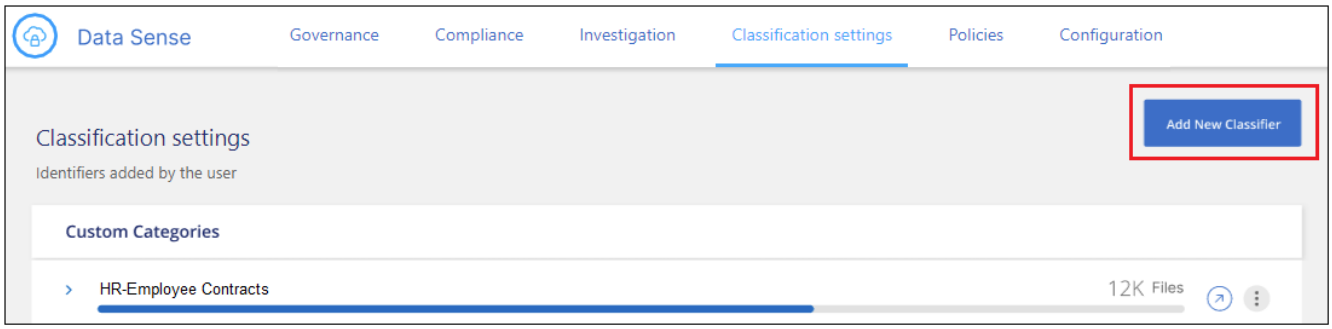
BlueXP 분류에서 인식할 데이터 범주의 샘플이 포함된 최소 25개의 교육 파일을 만들어야 합니다. 지원되는 파일 형식은 다음과 같습니다.

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

파일은 최소 100바이트여야 하며 BlueXP 분류에서 액세스할 수 있는 폴더에 있어야 합니다.

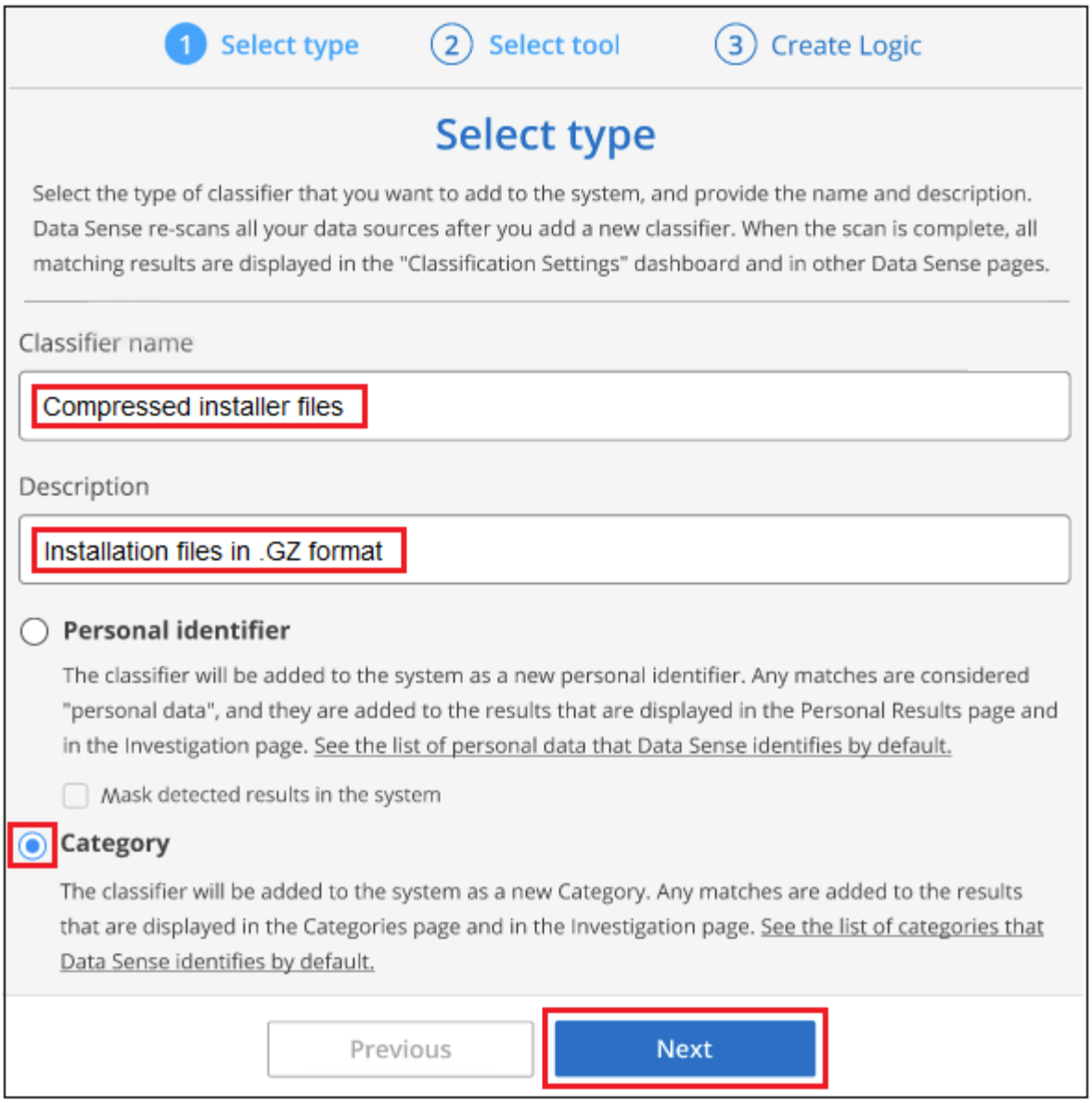
단계

1. Classification settings_tab에서 * Add New Classifier * 를 클릭하여 _Add Custom Classifier_wizard를 실행합니다.

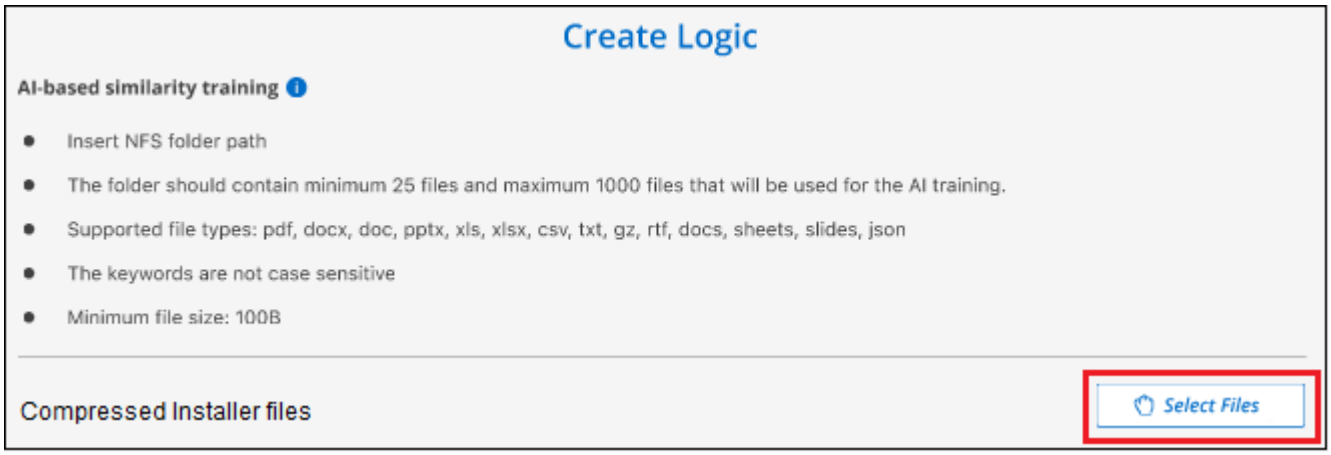


2. Select type_page에서 분류자의 이름을 입력하고 간단한 설명을 입력한 다음 * Category * 를 선택하고 * Next * 를 클릭합니다.

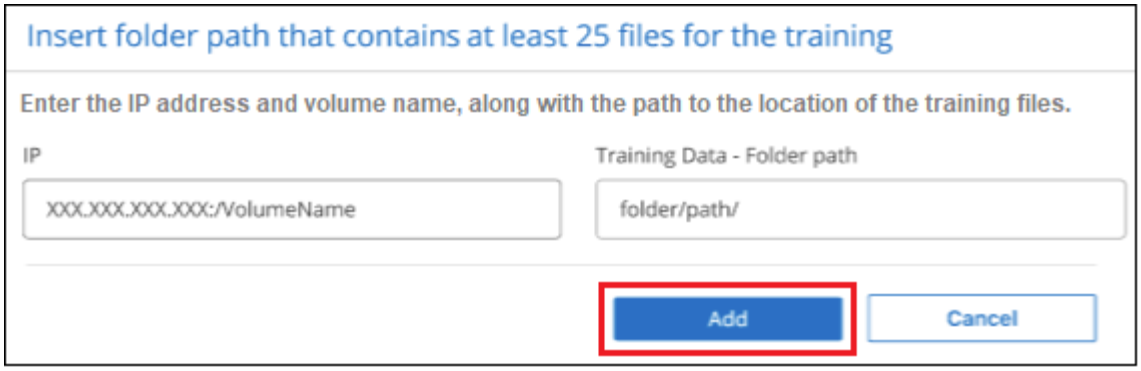
   입력하는 이름은 BlueXP 분류 UI에 정의하는 데이터 범주와 일치하는 스캔된 파일의 머리글로, 조사 페이지의 필터 이름으로 표시됩니다.



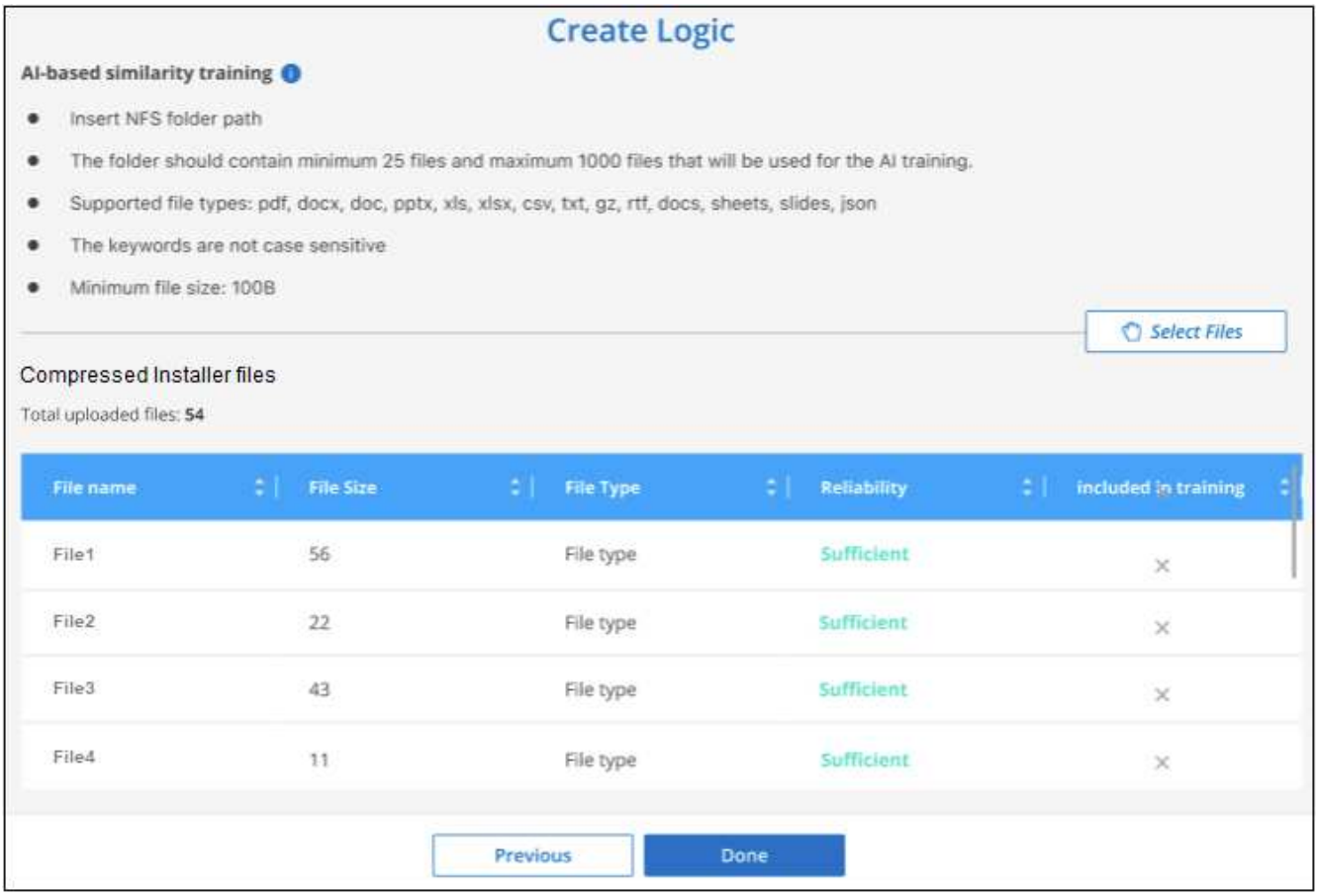
3. Create Logic_page에서 학습 파일이 준비되었는지 확인한 다음 * Select files * 를 클릭합니다.



4. 볼륨의 IP 주소와 교육 파일이 있는 경로를 입력하고 * 추가 * 를 클릭합니다.



5. 교육 파일이 BlueXP 분류에서 인식되었는지 확인합니다. x * 를 클릭하여 요구 사항을 충족하지 않는 교육 파일을 제거합니다. 그런 다음 * 완료 * 를 클릭합니다.

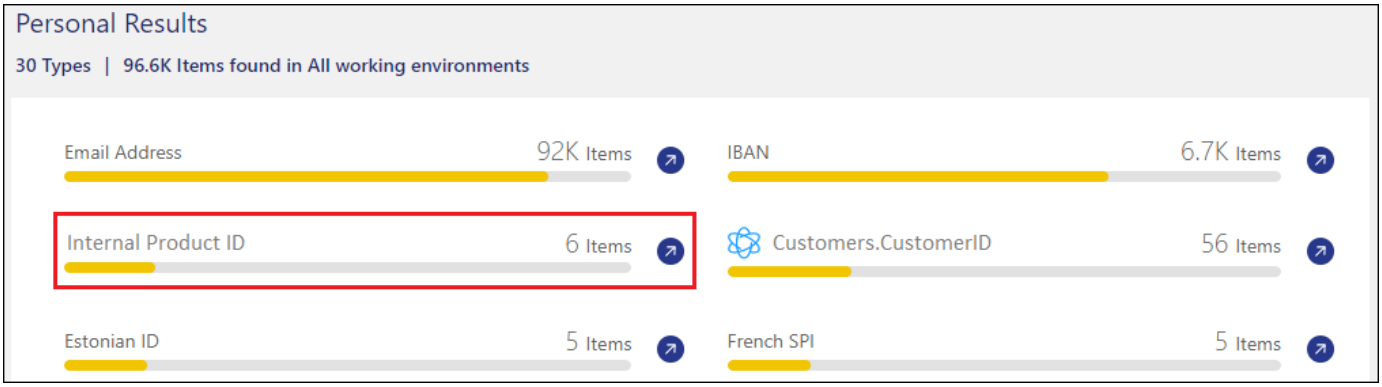


결과

새 범주는 교육 파일에 정의된 대로 생성되며 BlueXP 분류에 추가됩니다. 그런 다음 BlueXP 분류는 모든 데이터 원본을 다시 검색하여 이 새 범주에 적합한 파일을 식별합니다. 사용자 지정 분류자 페이지로 돌아가 새 범주와 일치하는 파일 수를 볼 수 있습니다. 모든 데이터 원본을 스캔하여 얻은 결과는 스캔해야 하는 파일 수에 따라 다소 시간이 걸릴 수 있습니다.

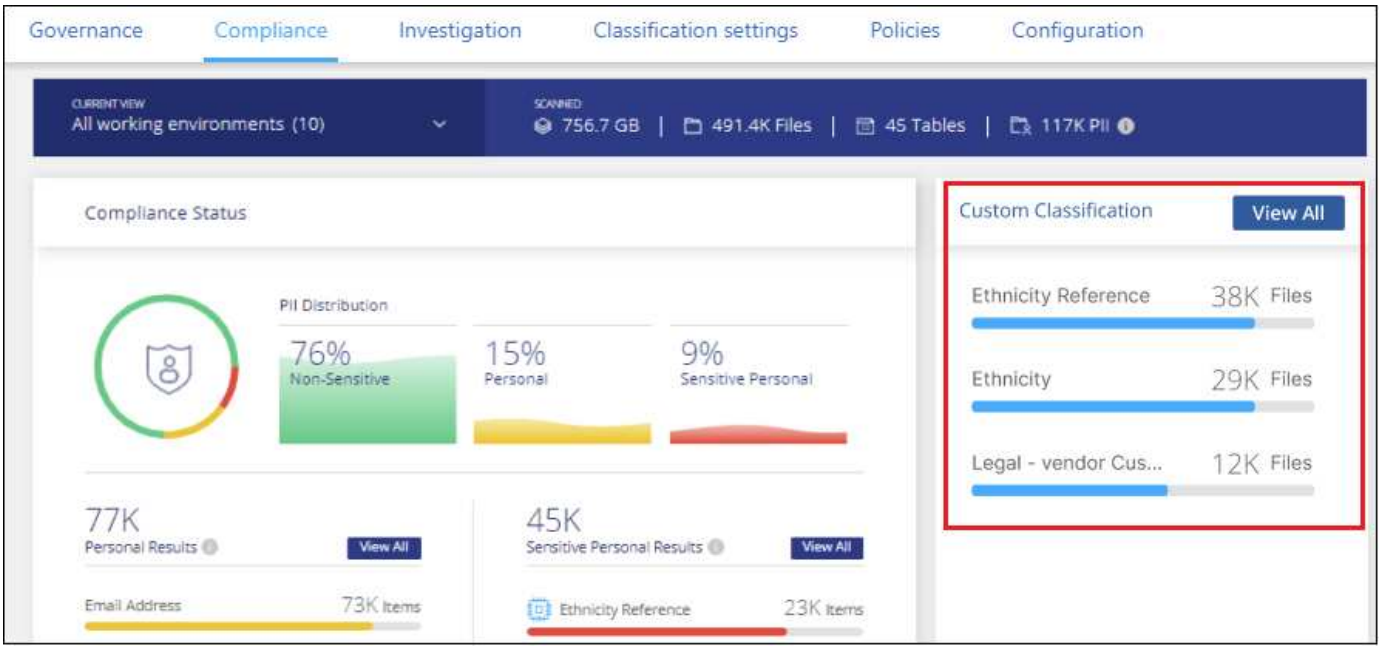
사용자 지정 분류자의 결과를 봅니다

준수 대시보드 및 조사 페이지에서 사용자 지정 분류자의 결과를 볼 수 있습니다. 예를 들어 이 스크린샷은 "개인 결과" 섹션 아래의 준수 대시보드에서 일치하는 정보를 보여 줍니다.



를 클릭합니다 ↗ 버튼을 눌러 조사 페이지에서 자세한 결과를 확인합니다.

또한 모든 사용자 지정 분류자 결과가 사용자 지정 분류자 탭에 나타나고, 아래와 같이 상위 6개의 사용자 지정 분류자 결과가 준수 대시보드에 표시됩니다.

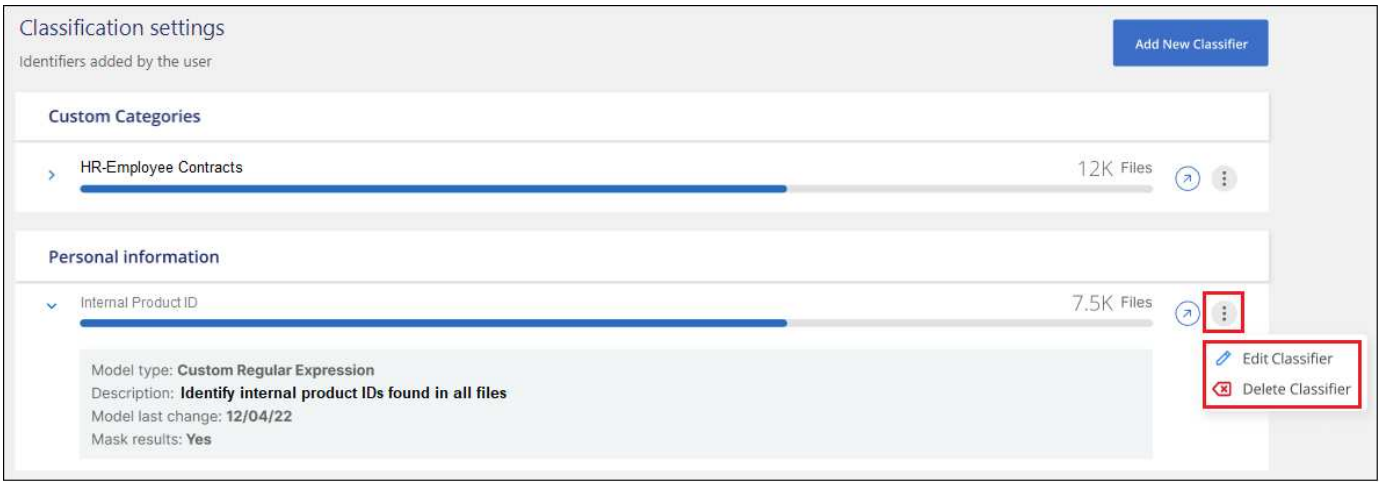


사용자 지정 분류자를 관리합니다

분류자 편집 * 단추를 사용하여 만든 사용자 지정 분류자를 변경할 수 있습니다.

> 지금은 Data Fusion 분류자를 편집할 수 없습니다.

그리고 나중에 추가한 사용자 정의 패턴을 식별하기 위해 BlueXP 분류가 필요하지 않다고 판단될 경우 * 분류자 삭제 * 버튼을 사용하여 각 항목을 제거할 수 있습니다.



BlueXP 분류 검사에서 특정 디렉토리를 제외합니다

BlueXP 분류를 통해 특정 데이터 소스 디렉토리에 있는 스캔 데이터를 제외하려면 이러한 디렉토리 이름을 구성 파일에 추가할 수 있습니다. 이 변경 사항을 적용하면 BlueXP 분류 엔진에서 해당 디렉토리에서 검사 데이터를 제외합니다.

BlueXP 분류는 기본적으로 볼륨 스냅샷 데이터의 검사가 볼륨 내의 콘텐츠와 동일하기 때문에 볼륨 스냅샷 데이터 검사를 제외하도록 구성됩니다.

이 기능은 BlueXP 분류 버전 1.29 이상에서 사용할 수 있습니다(2024년 3월부터).

지원되는 데이터 소스

BlueXP 분류 검사에서 특정 디렉토리를 제외하면 다음 데이터 소스에서 NFS 및 CIFS 공유에 대해 지원됩니다.

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

스캔에서 제외할 디렉토리를 정의합니다

디렉토리를 분류 스캔에서 제외하려면 먼저 BlueXP 분류 시스템에 로그인해야 구성 파일을 편집하고 스크립트를 실행할 수 있습니다. 자세한 내용은 를 참조하십시오 "BlueXP 분류 시스템에 로그인합니다" Linux 시스템에 소프트웨어를 수동으로 설치했는지 아니면 클라우드에 인스턴스를 배포했는지에 따라 다릅니다.

- BlueXP 분류 시스템별로 최대 50개의 디렉토리 경로를 제외할 수 있습니다.
- 디렉터리 경로를 제외하면 검색 시간에 영향을 줄 수 있습니다.

단계

1. BlueXP 분류 시스템에서 "/opt/netapp/config/custom_configuration"으로 이동하여 파일을 엽니다 `data_provider.yaml`.

2. "data_providers" 섹션의 "exclude:" 줄에 제외할 디렉토리 경로를 입력합니다. 예를 들면 다음과 같습니다.

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

   이 파일의 다른 내용은 변경하지 마십시오.

3. 변경 내용을 파일에 저장합니다.
4. "/opt/netapp/datasense/tools/customer_configuration/data_providers"로 이동하여 다음 스크립트를 실행합니다.

```
update_data_providers_from_config_file.sh
```

   이 명령은 스캔에서 제외할 디렉토리를 분류 엔진으로 커밋합니다.

결과

이후의 모든 데이터 스캔은 지정된 디렉토리의 스캔을 제외합니다.

이와 동일한 단계를 사용하여 제외 목록에서 항목을 추가, 편집 또는 삭제할 수 있습니다. 수정된 제외 목록은 스크립트를 실행하여 변경 내용을 커밋한 후 업데이트됩니다.

예

구성 **1:**

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

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

제외할 경로에 대한 예상 결과**:**

- /CVO1/폴더1
- /CVO1/folder1name 을 입력합니다
- /CVO1/폴더10
- /CVO1/ * 폴더1
- /CVO1/+folder1name
- /CVO1/notfolder10 을 참조하십시오
- /CVO22/폴더1
- /CVO22/folder1name 을 입력합니다

- /CVO22/Folder10 을 참조하십시오

제외되지 않을 경로의 예:

- /CVO1/* 폴더
- /CVO1/Foldername 을 입력합니다
- /CVO22/ * folder20

구성 **2:**

이름 시작 부분에만 "* folder1"이 포함된 모든 폴더는 제외됩니다.

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

제외할 경로에 대한 예상 결과:

- /CVO/ * 폴더1
- /CVO/ * folder1name
- /CVO/ * folder10

제외되지 않을 경로의 예:

- /CVO/폴더1
- /CVO/folder1name 을 참조하십시오
- /CVO/Not * folder10

구성 **3:**

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

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

제외할 경로에 대한 예상 결과:

- /CVO22/폴더1
- /CVO22/folder1name 을 입력합니다
- /CVO22/Folder10 을 참조하십시오

제외되지 않을 경로의 예:

- /CVO1/폴더1
- /CVO1/folder1name 을 입력합니다
- /CVO1/폴더10

폴더 이름의 특수 문자를 이스케이프하는 중입니다

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

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
예를 들면 다음과 같습니다.
```

소스의 경로: `/project/*not_to_scan`

제외 파일의 구문: `"\\*not_to_scan"`

현재 제외 목록을 봅니다

의 내용에 사용할 수 있습니다 `data_provider.yaml` 를 실행한 후 실제로 커밋된 구성 파일과 다른 구성 파일 `update_data_providers_from_config_file.sh` 스크립트. BlueXP 분류 검사에서 제외된 디렉토리의 현재 목록을 보려면 "/opt/netapp/datasense/tools/customer_configuration/data_providers"에서 다음 명령을 실행합니다.

```
get_data_providers_configuration.sh
```

준수 작업의 상태 보기

100개의 파일을 이동하거나 삭제하는 등 여러 파일에 걸쳐 조사 결과 창에서 비동기 작업을 실행할 경우 프로세스에 시간이 걸릴 수 있습니다. 이러한 작업의 상태를 _Action Status_창에서 모니터링할 수 있으므로 모든 파일에 적용된 시기를 알 수 있습니다.

이를 통해 성공적으로 완료된 작업, 현재 진행 중인 작업 및 실패한 작업을 볼 수 있으므로 문제를 진단하고 해결할 수 있습니다. 단일 파일 이동과 같이 빠르게 완료되는 짧은 작업은 작업 상태 창에 나타나지 않습니다.

상태는 다음과 같습니다.

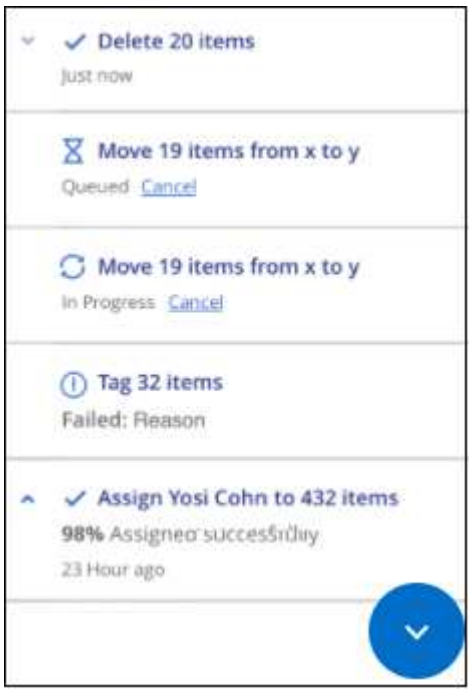
- 성공 - BlueXP 분류 작업이 완료되고 모든 항목이 성공했습니다.
- 부분 성공 - BlueXP 분류 작업이 완료되고 일부 항목이 실패하여 일부 항목이 성공했습니다.
- 진행 중 - 작업이 아직 진행 중입니다.
- 대기열에 있음 - 작업이 시작되지 않았습니다.
- 취소됨 - 작업이 취소되었습니다.
- 실패 - 작업이 실패했습니다.

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

단계

1. BlueXP 분류 UI의 오른쪽 하단에 * 작업 상태 * 버튼이 있습니다 .

2. 이 버튼을 클릭하면 최근 20개 작업이 나열됩니다.



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

추가 그룹 ID를 조직에 공개됨으로 정의합니다

그룹 ID(GID)가 NFS 파일 공유의 파일 또는 폴더에 첨부되면 파일 또는 폴더에 대한 사용 권한을 정의합니다(예: 해당 GID가 "조직에 열려 있는지"). 일부 GID(그룹 ID)가 처음에 "Open to Organization" 권한 수준으로 설정되지 않은 경우 GID에 해당 권한을 추가하여 GID가 첨부된 모든 파일 및 폴더가 "Open to the Organization"으로 간주되도록 할 수 있습니다.

이렇게 변경하고 BlueXP 분류에서 파일과 폴더를 다시 검사하면 이러한 그룹 ID가 첨부된 모든 파일 및 폴더가 조사 세부 정보 페이지에 이 권한을 표시하고 파일 권한을 표시하는 보고서에도 표시됩니다.

이 기능을 활성화하려면 BlueXP 분류 시스템에 로그인하여 구성 파일을 편집하고 스크립트를 실행해야 합니다. 자세한 내용은 를 참조하십시오 "BlueXP 분류 시스템에 로그인합니다" Linux 시스템에 소프트웨어를 수동으로 설치했는지 아니면 클라우드에 인스턴스를 배포했는지에 따라 다릅니다.

그룹 ID에 "조직에 열기" 권한을 추가합니다

이 작업을 시작하기 전에 그룹 ID 번호(GID)가 있어야 합니다.

단계

1. BlueXP 분류 시스템에서 "/opt/netapp/config/custom_configuration"으로 이동하여 파일을 엽니다 `data_provider.yaml`.
2. "organization_group_ids:[]" 줄에 그룹 ID를 추가합니다. 예를 들면 다음과 같습니다.

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

이 파일의 다른 내용은 변경하지 마십시오.

3. 변경 내용을 파일에 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 검사는 이러한 그룹 ID가 "조직 공개"로 첨부된 파일 또는 폴더를 식별합니다.

이와 동일한 단계를 사용하여 그룹 ID 목록을 편집하고 이전에 추가한 그룹 ID를 삭제할 수 있습니다. 수정된 그룹 ID 목록은 스크립트를 실행하여 변경 내용을 커밋한 후에 업데이트됩니다.

현재 그룹 ID 목록을 봅니다

의 내용에 사용할 수 있습니다 `data_provider.yaml` 를 실행한 후 실제로 커밋된 구성 파일과 다른 구성 파일 `update_data_providers_from_config_file.sh` 스크립트. BlueXP 분류에 추가한 그룹 ID의 현재 목록을 보려면 "/opt/netapp/datasense/tools/customer_configuration/data_providers"에서 다음 명령을 실행하십시오.

```
get_data_providers_configuration.sh
```

BlueXP 분류 작업의 이력을 감사합니다

BlueXP 분류는 BlueXP 분류가 검색하는 모든 작업 환경 및 데이터 소스의 파일에 대해 수행된 관리 작업을 기록합니다. 또한 BlueXP 분류는 BlueXP 분류 인스턴스를 배포할 때 작업을 기록합니다.

BlueXP 분류 감사 로그 파일의 내용을 보거나 다운로드하여 어떤 파일 변경 사항이 발생했는지, 언제 변경되었는지 확인할 수 있습니다. 예를 들어, 어떤 요청이 실행되었는지, 요청 시간, 파일이 삭제된 경우 소스 위치 등의 세부 정보 또는 파일이 이동된 경우 소스 및 대상 위치를 확인할 수 있습니다.

로그 파일 내용

감사 로그의 각 줄에는 다음 형식의 정보가 포함되어 있습니다.

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- 날짜 및 시간 - 이벤트의 전체 타임 스탬프입니다

- 상태 - 정보, 경고
- 작업 유형(삭제, 복사, 이동, 정책 생성, 정책 업데이트, 파일 재검색, JSON 보고서 다운로드 등)
- 파일 이름(작업이 파일과 관련된 경우)
- 작업에 대한 세부 정보 - 수행한 작업: 작업에 따라 다릅니다
  - 정책 이름입니다
  - 이동 - 원본 및 대상
  - 복사 - 원본 및 대상
  - 태그-태그 이름용
  - 사용자 이름으로 할당
  - 전자 메일 알림의 경우 - 전자 메일 주소/계정입니다

예를 들어, 로그 파일의 다음 줄은 성공적인 복사 작업과 실패한 복제 작업을 보여 줍니다.

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 |
49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device
10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports
(NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file |
239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from
device 10.31.133.183 (type: SMB_SHARE) to device
10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

로그 파일 위치

관리 감사 로그 파일은 BlueXP 분류 시스템의 다음 위치에 있습니다. `/opt/netapp/audit_logs/`

설치 감사 로그 파일은 에 기록됩니다 `/opt/netapp/install_logs/`

각 로그 파일의 크기는 최대 10MB입니다. 이 제한에 도달하면 새 로그 파일이 시작됩니다. 로그 파일의 이름은 "DataSense_audit.log", "DataSense_audit.log.1", "DataSense_audit.log.2" 등으로 지정됩니다. 시스템에 최대 100개의 로그 파일이 보존됩니다. 오래된 로그 파일은 최대 로그 수에 도달하면 자동으로 삭제됩니다.

로그 파일에 액세스합니다

로그 파일에 액세스하려면 BlueXP 분류 시스템에 로그인해야 합니다. 자세한 내용은 를 참조하십시오 "BlueXP 분류 시스템에 로그인합니다" Linux 시스템에 소프트웨어를 수동으로 설치했는지 아니면 클라우드에 인스턴스를 배포했는지에 따라 다릅니다.

BlueXP 분류 스캔 속도를 줄입니다

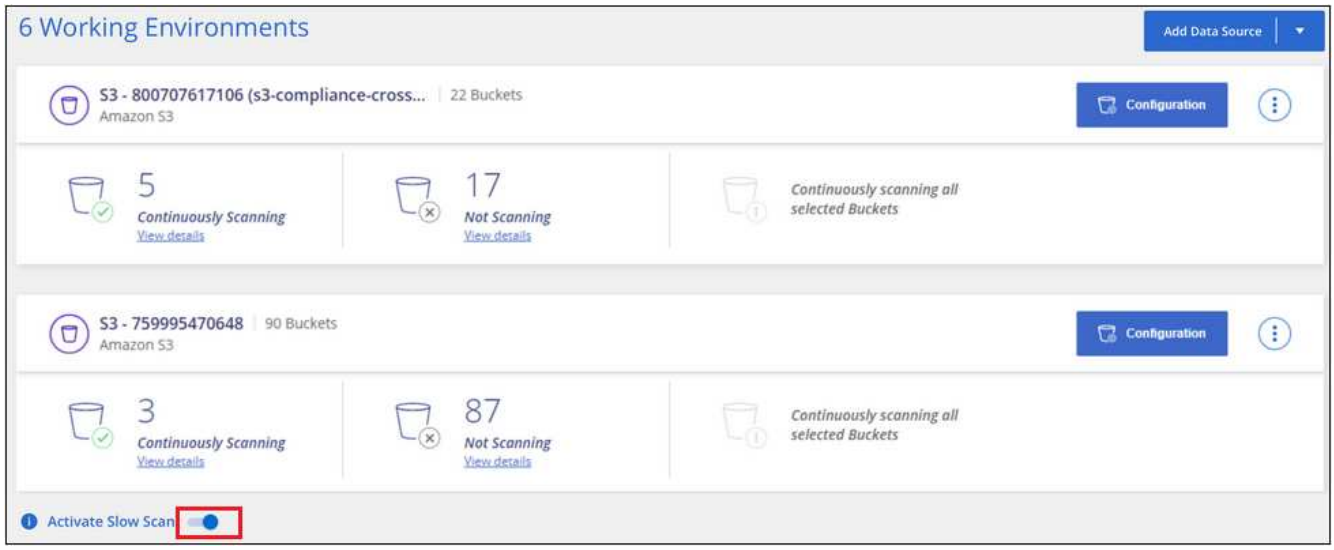
데이터 스캔은 스토리지 시스템과 데이터에 경미한 영향을 줍니다. 그러나 매우 작은 충격에도 신경 쓰면 BlueXP 분류를 구성하여 "느린" 스캔을 수행할 수 있습니다.

이 옵션을 설정하면 모든 데이터 소스에서 느린 스캔이 사용됩니다. 단일 작업 환경 또는 데이터 원본에 대해 느린 스캔을 구성할 수 없습니다.

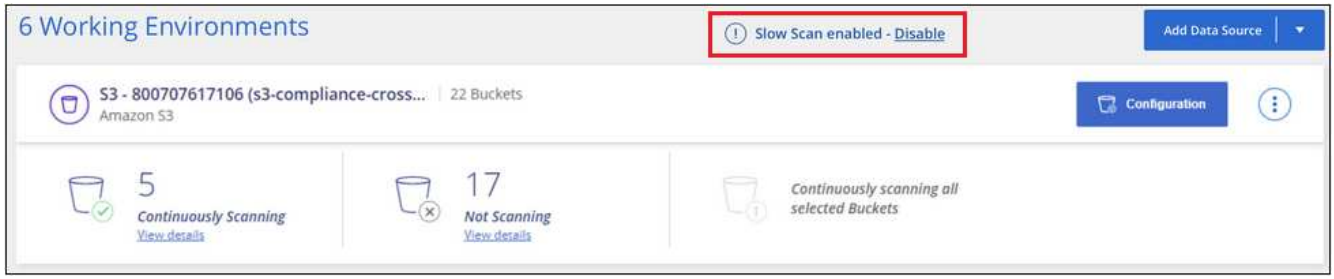
데이터베이스를 스캔할 때는 스캔 속도를 줄일 수 없습니다.

단계

1. Configuration_page 하단에서 슬라이더를 오른쪽으로 이동하여 저속 스캔을 활성화합니다.



구성 페이지 맨 위에는 저속 스캔이 활성화되어 있습니다.



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

BlueXP 분류에서 데이터 소스 제거

필요한 경우 하나 이상의 작업 환경, 데이터베이스, 파일 공유 그룹, OneDrive 계정, Google Drive 계정, SharePoint 계정을 사용할 수 있습니다.

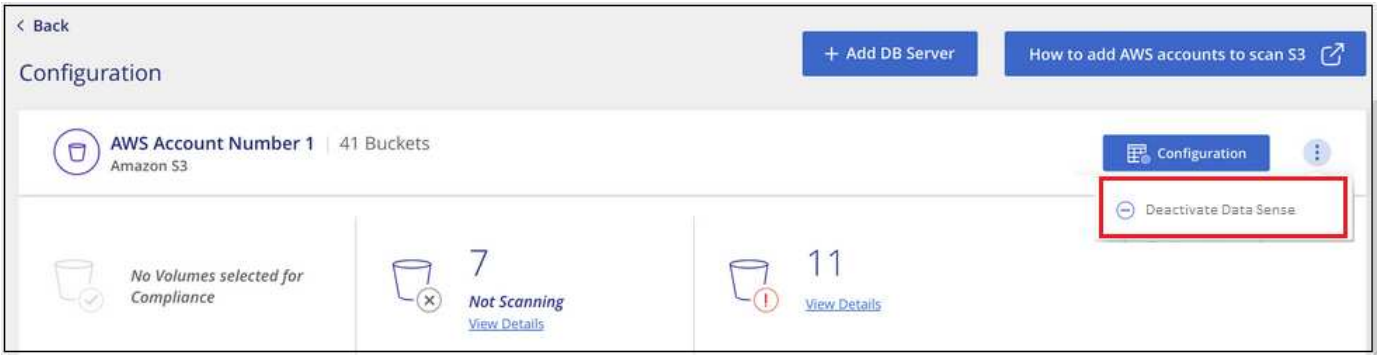
데이터 소스가 제거되면 데이터 스캔 충전이 중지됩니다.

작업 환경에 대한 규정 준수 검사 비활성화

스캔을 비활성화하면 BlueXP 분류는 작업 환경의 데이터를 더 이상 스캔하지 않고 BlueXP 분류 인스턴스에서 인덱싱된 규정 준수 정보를 제거합니다(작업 환경 자체의 데이터는 삭제되지 않음).

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

를 클릭합니다.



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

BlueXP 분류에서 데이터베이스 제거

특정 데이터베이스를 더 이상 스캔하지 않으려면 BlueXP 분류 인터페이스에서 해당 데이터베이스를 삭제하고 모든 스캔을 중지할 수 있습니다.

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

BlueXP 분류에서 OneDrive, SharePoint 또는 Google Drive 계정 제거

특정 OneDrive 계정, 특정 SharePoint 계정 또는 Google Drive 계정에서 사용자 파일을 더 이상 스캔하지 않으려는 경우 BlueXP 분류 인터페이스에서 계정을 삭제하고 모든 스캔을 중지할 수 있습니다.

단계

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

2. 확인 대화 상자에서 * 계정 삭제 * 를 클릭합니다.

BlueXP 분류에서 파일 공유 그룹을 제거합니다

더 이상 파일 공유 그룹에서 사용자 파일을 스캔하지 않으려는 경우 BlueXP 분류 인터페이스에서 파일 공유 그룹을 삭제하고 모든 검사를 중지할 수 있습니다.

단계

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

2. 확인 대화 상자에서 * 공유 그룹 삭제 * 를 클릭합니다.

BlueXP 분류를 제거하는 중입니다

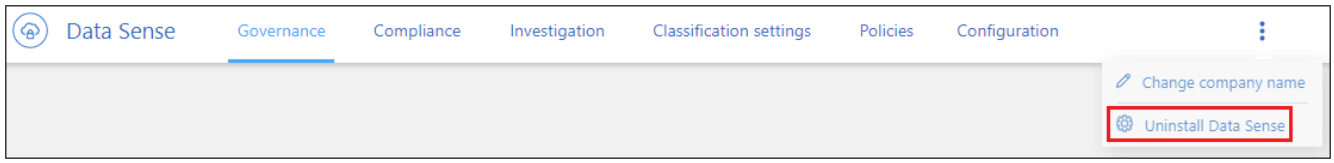
문제를 해결하거나 호스트에서 소프트웨어를 영구적으로 제거하기 위해 BlueXP 분류 소프트웨어를 제거할 수 있습니다. 또한 인스턴스를 삭제하면 인덱싱된 데이터가 있는 연결된 디스크도 삭제됩니다. BlueXP 분류에서 검색한 모든 정보는 영구적으로 삭제됩니다.

필요한 단계는 클라우드에 BlueXP 분류를 배포했는지 또는 온프레미스 호스트에 배포했는지에 따라 달라집니다.

클라우드 배포에서 BlueXP 분류를 제거합니다

BlueXP 분류를 더 이상 사용하지 않으려는 경우 클라우드 공급자 환경에서 BlueXP 분류 인스턴스를 제거하고 삭제할 수 있습니다.

1. BlueXP 분류 페이지 상단에서 을 클릭합니다 ⋮ 그런 다음 * 데이터 감지 제거 * 를 클릭합니다.



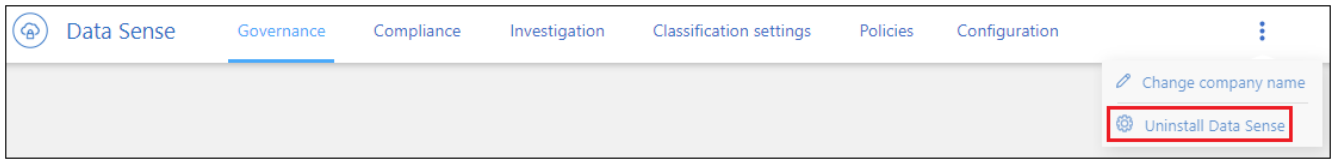
2. 데이터 감지 제거 대화 상자에서 * 제거 * 를 입력하여 BlueXP 커넥터에서 BlueXP 분류 인스턴스를 분리할지 확인한 다음 * 제거 * 를 클릭합니다.
3. 클라우드 공급자의 콘솔로 이동하여 BlueXP 분류 인스턴스를 삭제합니다. 인스턴스의 이름은 *CloudCompliance_*이며 생성된 해시*(UUID)*와 연결됩니다. 예*: _CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*

그러면 인스턴스 및 BlueXP 분류에서 수집한 모든 관련 데이터가 삭제됩니다.

온-프레미스 배포에서 **BlueXP** 분류를 제거합니다

BlueXP 분류를 더 이상 사용하지 않거나 재설치가 필요한 문제가 있는 경우 호스트에서 BlueXP 분류를 제거할 수 있습니다.

1. BlueXP 분류 페이지 상단에서 을 클릭합니다 ⋮ 그런 다음 * 데이터 감지 제거 * 를 클릭합니다.



2. 데이터 감지 제거 대화 상자에서 * 제거 * 를 입력하여 BlueXP 커넥터에서 BlueXP 분류 인스턴스를 분리할지 확인한 다음 * 제거 * 를 클릭합니다.
3. 호스트에서 소프트웨어를 제거하려면 를 실행합니다 `cleanup.sh` 호스트 시스템의 스크립트(예:

```
cleanup.sh
```

자세한 내용은 를 참조하십시오 "BlueXP 분류 호스트 시스템에 로그인합니다".

참조하십시오

지원되는 BlueXP 분류 인스턴스 유형

BlueXP 분류 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행해야 합니다. 클라우드에 BlueXP 분류를 배포할 때는 모든 기능을 위해 "큰" 특성을 가진 시스템을 사용하는 것이 좋습니다.

CPU가 적고 RAM이 적은 시스템에 BlueXP 분류를 배포할 수 있지만 이러한 덜 강력한 시스템을 사용할 때는 몇 가지 제약이 있습니다. "이러한 제한 사항에 대해 자세히 알아보십시오".

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

AWS 인스턴스 유형

시스템 크기	사양	인스턴스 유형
매우 크게	32개의 CPU, 128GB RAM, 1TiB GP3 SSD	"m6i.8x 대형" (기본값)
대형	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 크기	CPU 8개, 16GB RAM, 100GiB SSD	"c6a.2xLarge" (기본값) C5A.2xLarge c5.2xLarge c4.2xLarge

Azure 인스턴스 유형

시스템 크기	사양	인스턴스 유형
매우 크게	32개의 CPU, 128GB RAM, OS 디스크(2,048GiB, 최소 250MB/s 처리량) 및 데이터 디스크(1TiB SSD, 최소 750MB/s 처리량)	"Standard_D32_v3" (기본값)
대형	CPU 16개, 64GB RAM, 500GiB SSD	"standard_d16s_v3" (기본값)

GCP 인스턴스 유형

시스템 크기	사양	인스턴스 유형
대형	CPU 16개, 64GB RAM, 500GiB SSD	"N2-표준-16" (기본값) n2d-standard-16 n1-standard-16

데이터 소스에서 수집된 메타데이터

BlueXP 분류는 데이터 소스 및 작업 환경의 데이터에 대한 분류 검사를 수행할 때 특정 메타데이터를 수집합니다. BlueXP 분류는 데이터를 분류하는 데 필요한 대부분의 메타데이터에 액세스할 수 있지만 필요한 데이터에 액세스할 수 없는 소스가 있습니다.

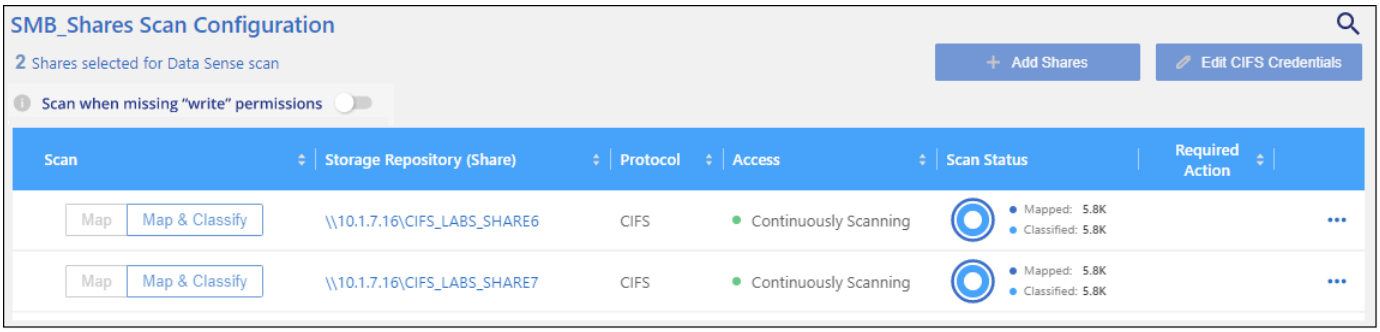
	* 메타데이터 *	**CIFS ***	*** NFS ***
* 타임 스탬프 *	_작성 시간 _	사용 가능	사용할 수 없음(Linux에서는 지원되지 않음)
	_마지막 액세스 시간 _	사용 가능	사용 가능
	_마지막 수정 시간 _	사용 가능	사용 가능
* 권한 *	_권한 열기 _	"Everyone" 그룹이 파일에 액세스할 수 있는 경우 "조직에 열기"로 간주됩니다.	"기타"가 파일에 액세스할 수 있는 경우 "조직에 열기"로 간주됩니다.
	_ 사용자/그룹 액세스 _	사용자 및 그룹 정보는 LDAP에서 가져옵니다	사용할 수 없음(NFS 사용자는 일반적으로 서버에서 로컬로 관리되므로 동일한 개인이 각 서버에서 다른 UID를 가질 수 있음)

- BlueXP 분류는 SharePoint Online, SharePoint 온프레미스(SharePoint Server), OneDrive, Google Drive, Amazon S3, 데이터베이스의 데이터 소스에서는 "마지막 액세스 시간"을 추출하지 않습니다.
- Windows OS의 이전 버전(예: Windows 7 및 Windows 8)은 시스템 성능에 영향을 줄 수 있으므로 기본적으로 "마지막 액세스 시간" 속성의 컬렉션을 사용하지 않습니다. 이 속성을 수집하지 않으면 "마지막 액세스 시간"을 기반으로 하는 BlueXP 분류 분석에 영향을 줍니다. 필요한 경우 이러한 이전 Windows 시스템에서 마지막 액세스 시간 모음을 활성화할 수 있습니다.

마지막 액세스 시간 타임 스탬프입니다

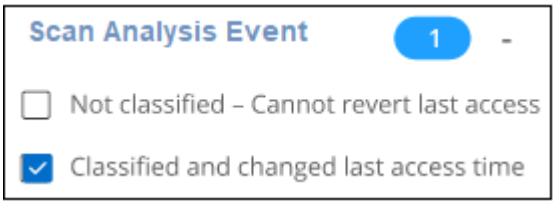
BlueXP 분류는 파일 공유에서 데이터를 추출할 때 운영 체제는 이를 데이터에 액세스하는 것으로 간주하고 그에 따라 "마지막 액세스 시간"을 변경합니다. 검사 후 BlueXP 분류는 마지막 액세스 시간을 원래 타임 스탬프로 되돌려줍니다. BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 시스템은 마지막 액세스 시간을 원래 타임 스탬프로 되돌릴 수 없습니다. SnapLock로 구성된 ONTAP 볼륨은 읽기 전용 권한을 가지며 마지막 액세스 시간을 원래 타임 스탬프로 되돌릴 수도 없습니다.

기본적으로 BlueXP 분류에 이러한 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 볼륨의 해당 파일을 검색하지 않습니다. 그러나 파일의 마지막 액세스 시간이 원래 시간으로 재설정되는 것을 염려하지 않을 경우, BlueXP 분류가 권한에 관계없이 볼륨을 스캔하도록 구성 페이지 하단에 있는 * "쓰기 속성" 권한 * 스위치가 없을 때 * 스캔 을 클릭할 수 있습니다.



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

조사 페이지에 *Scan Analysis Event* 라는 필터가 있어 BlueXP 분류로 마지막 액세스 시간을 되돌릴 수 없기 때문에 분류되지 않은 파일을 표시할 수 있습니다. 또는 BlueXP 분류로 마지막 액세스 시간을 되돌릴 수 없지만 분류된 파일을 사용할 수 있습니다.



필터 선택 항목은 다음과 같습니다.

- "분류되지 않음 — 마지막 액세스 시간을 되돌릴 수 없음" - 쓰기 권한이 없어 분류되지 않은 파일을 표시합니다.
- "마지막 액세스 시간 분류 및 업데이트" - 분류된 파일과 BlueXP 분류에서 마지막 액세스 시간을 원래 날짜로 다시 설정할 수 없는 파일을 표시합니다. 이 필터는 에서 "쓰기 속성" 권한이 없을 때 * 스캔 을 설정한 환경에만 적용됩니다.

필요한 경우 이러한 결과를 보고서로 내보내면 권한 때문에 어떤 파일이 스캔되고 있는지 또는 스캔되지 않았는지 확인할 수 있습니다. "데이터 조사 보고서에 대해 자세히 알아보십시오".

BlueXP 분류 시스템에 로그인합니다

때때로 BlueXP 분류 시스템에 로그인하여 로그 파일에 액세스하거나 구성 파일을 편집해야 할 수 있습니다.

BlueXP 분류가 온프레미스의 Linux 머신 또는 클라우드에 구축한 Linux 시스템에 설치되면 구성 파일 및 스크립트에 직접 액세스할 수 있습니다.

클라우드에 BlueXP 분류를 배포할 때는 BlueXP 분류 인스턴스에 SSH를 사용해야 합니다. 사용자 및 암호를 입력하거나 BlueXP Connector 설치 중에 제공한 SSH 키를 사용하여 시스템에 SSH를 수행합니다. SSH 명령은 다음과 같습니다.

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* path_to_the_ssh_key> = ssh 인증 키의 위치입니다
* machine_user>:
```

+
AWS의 경우 **<EC2-USER>**를 사용합니다
Azure의 경우: BlueXP 인스턴스에 대해 생성한 사용자를 사용합니다
** GCP의 경우: BlueXP 인스턴스에 대해 생성한 사용자를 사용합니다

- datasense_ip> = 가상 시스템 인스턴스의 IP 주소입니다

클라우드의 시스템에 액세스하려면 보안 그룹 인바운드 규칙을 수정해야 합니다. 자세한 내용은 다음을 참조하십시오.

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

BlueXP 분류 API

웹 UI를 통해 사용할 수 있는 BlueXP 분류 기능은 Swagger API를 통해서도 사용할 수 있습니다.

BlueXP 분류 안에는 UI의 탭에 해당하는 4가지 범주가 정의되어 있습니다.

- 조사
- 규정 준수
- 기대치를 설정합니다
- 구성

Swagger 문서의 API를 사용하여 데이터를 검색, 집계, 스캔 추적 및 복사, 이동 등의 작업을 생성할 수 있습니다.

개요

API를 사용하여 다음 기능을 수행할 수 있습니다.

- 정보를 내보냅니다
  - UI에서 사용할 수 있는 모든 것을 API를 통해 내보낼 수 있습니다(보고서 제외).
  - 데이터를 JSON 형식으로 내보내기(분석 및 Splunk와 같은 타사 애플리케이션으로 푸시)
- "AND" AND "OR" 문을 사용하여 쿼리를 만들고, 정보를 포함 및 제외하는 등의 작업을 수행할 수 있습니다.

  예를 들어 FILES_Without_specific 개인 식별 정보(PII)를 찾을 수 있습니다(UI에서는 사용할 수 없는 기능). 내보내기 작업에 대한 특정 필드를 제외할 수도 있습니다.

- 작업을 수행합니다
  - CIFS 자격 증명을 업데이트합니다
  - 작업을 보고 취소합니다
  - 디렉토리를 다시 스캔합니다
  - 데이터를 삭제, 복사, 레이블 지정 및 할당합니다

- 파일 복제 및 복사
- 데이터를 내보냅니다

API는 안전하고 UI와 동일한 인증 방법을 사용합니다. 인증에 대한 자세한 내용은 다음을 참조하십시오. https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Swagger API 참조에 액세스

Swagger로 이동하려면 BlueXP 분류 인스턴스의 IP 주소가 필요합니다. 클라우드 배포의 경우 공용 IP 주소를 사용합니다. 그런 다음 이 끝점에 도달해야 합니다.

https://<classification_ip>/documentation 을 참조하십시오

API 사용 예

다음 예제는 파일을 복사하기 위한 API 호출을 보여 줍니다.

API 요청

처음에는 작업 환경에 대한 모든 관련 필드 및 옵션을 가져와서 조사 탭의 모든 필터를 확인해야 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": "Working Environment Type",
      "operators": [
        "IN",
        "NOT_IN"
```

```
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "Working Environment",
      "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"
    }
  ]
}
```

요청 매개 변수에서 해당 응답을 사용하여 복사하려는 파일을 필터링합니다.

여러 항목에 작업을 적용할 수 있습니다. 지원되는 작업 유형은 이동, 삭제, 복사, 할당, FlexClone, 데이터 내보내기, 재스캔 및 레이블

다음과 같이 복사 작업을 생성합니다.

API 요청

다음 API는 해당 API이며, 이를 통해 여러 작업을 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

응답은 동작 객체를 반환하므로 API 가져오기 및 삭제 를 사용하여 동작에 대한 상태를 얻거나 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"
}
```

지식 및 지원

지원을 위해 등록하십시오

BlueXP 및 해당 스토리지 솔루션 및 서비스와 관련된 기술 지원을 받으려면 지원을 등록해야 합니다. Cloud Volumes ONTAP 시스템의 주요 워크플로우를 사용하려면 지원 등록도 필요합니다.

지원을 등록한다고 해서 클라우드 공급자 파일 서비스에 대한 NetApp 지원이 활성화되지 않습니다. 클라우드 공급자의 파일 서비스, 자체 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원은 해당 제품의 BlueXP 설명서에서 "도움말 얻기"를 참조하십시오.

- "ONTAP용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud용 Cloud Volumes Service"

지원 등록 개요

지원 권한을 활성화하려면 두 가지 형태의 등록이 있습니다.

- BlueXP 계정 ID 지원 가입 등록(BlueXP의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호)

  이는 BlueXP 내의 모든 서비스에 대한 단일 지원 가입 ID의 역할을 합니다. 각 BlueXP 계정 수준 지원 구독을 등록해야 합니다.

- 클라우드 공급자 마켓플레이스의 구독과 연결된 Cloud Volumes ONTAP 일련 번호 등록(20자리 909201xxxxxxxx 일련 번호)

  이러한 일련 번호는 일반적으로 _PAYGO 일련 번호_라고 하며 Cloud Volumes ONTAP 배포 시 BlueXP에서 생성됩니다.

두 가지 유형의 일련 번호를 등록하면 지원 티켓 열기와 자동 케이스 생성 등의 기능을 사용할 수 있습니다. 아래 설명과 같이 BlueXP에 NetApp Support 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

NetApp 지원을 위해 **BlueXP** 계정을 등록합니다

지원을 등록하고 지원 권한을 활성화하려면 BlueXP 계정의 한 사용자가 NetApp Support 사이트 계정을 BlueXP 로그인에 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp Support 사이트(NSS) 계정이 이미 있는지 여부에 따라 다릅니다.

NSS 계정이 있는 기존 고객

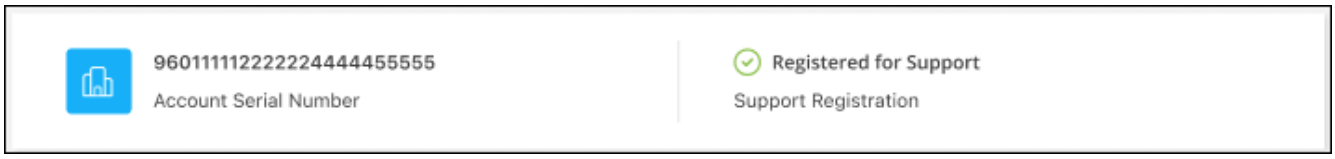
NSS 계정을 가지고 있는 NetApp 고객은 BlueXP를 통해 지원을 받기 위해 등록하기만 하면 됩니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 * 자격 증명 * 을 선택합니다.
2. 사용자 자격 증명 * 을 선택합니다.

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

   리소스 * 페이지에 계정이 지원을 위해 등록되었다는 내용이 표시됩니다.



   다른 BlueXP 사용자는 BlueXP 로그인과 NetApp Support 사이트 계정을 연결하지 않은 경우 동일한 지원 등록 상태를 볼 수 없습니다. 그러나 BlueXP 계정이 지원을 위해 등록되지 않은 것은 아닙니다. 계정에 있는 한 사용자가 이 단계를 따랐을 경우 계정이 등록되었습니다.

기존 고객이지만 **NSS** 계정은 없습니다

기존 사용권 및 제품 번호가 _NO_NSS인 기존 NetApp 고객인 경우 NSS 계정을 만들어 BlueXP 로그인과 연결해야 합니다.

단계

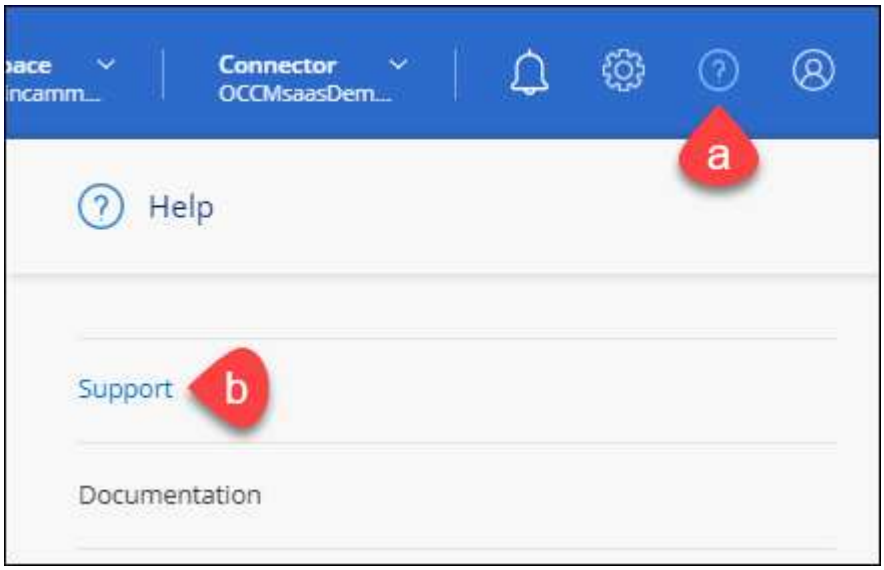
1. 를 완료하여 NetApp Support 사이트 계정을 생성합니다 "NetApp Support 사이트 사용자 등록 양식"
   a. 적절한 사용자 레벨(일반적으로 * NetApp 고객/최종 사용자 *)을 선택해야 합니다.
   b. 위에 사용된 BlueXP 계정 일련 번호(960xxxx)를 일련 번호 필드에 복사해야 합니다. 이렇게 하면 계정 처리 속도가 빨라집니다.
2. 의 단계를 완료하여 새 NSS 계정을 BlueXP 로그인에 연결합니다 NSS 계정이 있는 기존 고객.

NetApp이 처음이었습니다

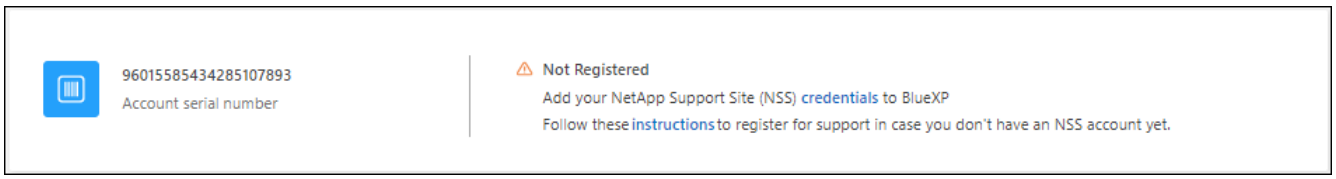
NetApp의 새로운 브랜드이고 NSS 계정이 없는 경우 아래의 각 단계를 수행하십시오.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.



2. 지원 등록 페이지에서 계정 ID 일련 번호를 찾습니다.



3. 로 이동합니다 "NetApp의 지원 등록 사이트" 를 선택하고 * 등록된 NetApp 고객이 아닙니다 * 를 선택합니다.
4. 필수 필드(빨간색 별표가 있는 필드)를 입력합니다.
5. [제품 라인] * 필드에서 * Cloud Manager * 를 선택한 다음 해당 청구 공급자를 선택합니다.
6. 위의 2단계에서 계정의 일련 번호를 복사하고 보안 검색을 완료한 다음 NetApp의 글로벌 데이터 개인 정보 보호 정책을 읽는지 확인합니다.

   이 보안 트랜잭션을 완료하기 위해 제공된 사서함으로 즉시 이메일이 전송됩니다. 몇 분 내에 확인 이메일이 도착하지 않으면 스팸 폴더를 확인해야 합니다.

7. 이메일 내에서 작업을 확인합니다.

   확인 시 NetApp에 요청이 제출되고 NetApp Support 사이트 계정을 만들 것을 권장합니다.

8. 를 완료하여 NetApp Support 사이트 계정을 생성합니다 "NetApp Support 사이트 사용자 등록 양식"
   a. 적절한 사용자 레벨(일반적으로 * NetApp 고객/최종 사용자 *)을 선택해야 합니다.
   b. 일련 번호 필드에 위에서 사용된 계정 일련 번호(960xxxx)를 복사해 주십시오. 이렇게 하면 계정 처리 속도가 빨라집니다.

작업을 마친 후

이 과정에서 NetApp이 연락을 드릴 것입니다. 신규 사용자를 위한 일회성 온보딩 연습입니다.

NetApp Support 사이트 계정이 있으면 의 단계를 완료하여 계정을 BlueXP 로그인에 연결합니다 NSS 계정이 있는 기존 고객.

Cloud Volumes ONTAP 지원을 위해 NSS 자격 증명을 연결합니다

Cloud Volumes ONTAP에 대해 다음 주요 워크플로를 사용하려면 NetApp Support 사이트 자격 증명을 BlueXP 계정과 연결해야 합니다.

- 지원을 위해 선불 종량제 Cloud Volumes ONTAP 시스템을 등록합니다

  NSS 계정을 제공하면 시스템에 대한 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스할 수 있습니다.

- BYOL(Bring Your Own License) 방식으로 Cloud Volumes ONTAP 구축

  BlueXP에서 사용권 키를 업로드하고 구입한 용어에 대한 구독을 활성화하려면 NSS 계정을 제공해야 합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리즈로 업그레이드하는 중입니다

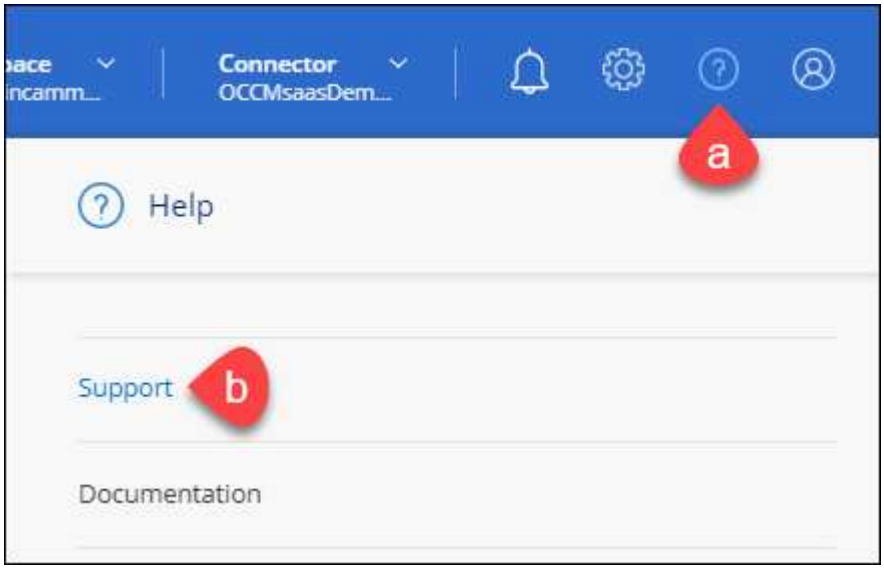
NSS 자격 증명을 BlueXP 계정과 연결하는 것은 BlueXP 사용자 로그인과 연결된 NSS 계정과 다릅니다.

이러한 NSS 자격 증명은 특정 BlueXP 계정 ID와 연결됩니다. BlueXP 계정에 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 NSS 계정을 하나 이상 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 * 지원 * 을 선택합니다.



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

   NetApp는 지원 및 라이센스와 관련된 인증 서비스의 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

   이러한 작업을 통해 BlueXP는 NSS 계정을 사용하여 라이선스 다운로드, 소프트웨어 업그레이드 확인 및 향후 지원 등록과 같은 작업을 수행할 수 있습니다.

   다음 사항에 유의하십시오.

   - NSS 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
   - NSS 계정은 파트너 수준 계정인 경우 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하면 파트너 수준 계정이 있으면 다음 오류 메시지가 나타납니다.

     "NSS 고객 유형은 이미 다른 유형의 NSS 사용자가 있으므로 이 계정에 허용되지 않습니다."

   기존 고객 수준 NSS 계정이 있는 경우에도 마찬가지이며 파트너 수준 계정을 추가하려고 합니다.

   - 로그인에 성공하면 NetApp은 NSS 사용자 이름을 저장합니다.

이 ID는 이메일에 매핑되는 시스템 생성 ID입니다. NSS 관리 * 페이지의 에서 이메일을 표시할 수 있습니다 ••• 메뉴.

- 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 에 * 자격 증명 업데이트 * 옵션이 있습니다 ••• 메뉴.

  이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이러한 계정의 토큰은 90일 후에 만료됩니다. 이를 알리는 알림이 게시됩니다.

도움을 받으십시오

NetApp은 다양한 방법으로 BlueXP 및 클라우드 서비스를 지원합니다. 기술 자료(KB) 기사 및 커뮤니티 포럼과 같은 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. 지원 등록에는 웹 티켓팅을 통한 원격 기술 지원이 포함됩니다.

클라우드 공급자의 파일 서비스에 대한 지원을 받습니다

클라우드 공급자의 파일 서비스, 자체 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원은 해당 제품의 BlueXP 설명서에서 "도움말 얻기"를 참조하십시오.

- "ONTAP용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud용 Cloud Volumes Service"

BlueXP 및 해당 스토리지 솔루션 및 서비스에 관한 기술 지원을 받으려면 아래에 설명된 지원 옵션을 사용하십시오.

자체 지원 옵션을 사용합니다

이 옵션은 하루 24시간, 주 7일 동안 무료로 사용할 수 있습니다.

- 문서화

  현재 보고 있는 BlueXP 문서입니다.

- "기술 자료"

  문제를 해결하는 데 도움이 되는 문서를 찾으려면 BlueXP 기술 자료를 검색하십시오.

- "커뮤니티"

  BlueXP 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새 토론을 만드십시오.

NetApp Support로 케이스 생성

위의 자체 지원 옵션 외에도 NetApp 지원 전문가와 협력하여 지원을 활성화한 이후의 모든 문제를 해결할 수 있습니다.

시작하기 전에

- 케이스 생성 * 기능을 사용하려면 먼저 NetApp Support 사이트 자격 증명을 BlueXP 로그인에 연결해야 합니다. "BlueXP 로그인과 관련된 자격 증명을 관리하는 방법에 대해 알아봅니다".

- 일련 번호가 있는 ONTAP 시스템의 케이스를 여는 경우 NSS 계정은 해당 시스템의 일련 번호와 연결되어 있어야 합니다.

단계

1. BlueXP에서 * 도움말 > 지원 * 을 선택합니다.
2. 리소스 * 페이지의 기술 지원 아래에서 사용 가능한 옵션 중 하나를 선택합니다.

   a. 전화로 통화하려면 * 전화 * 를 선택하십시오. 전화를 걸 수 있는 전화 번호가 나열된 netapp.com 페이지로 연결됩니다.

   b. NetApp 지원 전문가와 함께 티켓을 열려면 * 케이스 생성 * 을 선택하십시오.

      - * 서비스 *: 문제와 관련된 서비스를 선택합니다. 예를 들어, 서비스 내의 워크플로우 또는 기능과 관련된 기술 지원 문제에 해당하는 BlueXP를 예로 들 수 있습니다.
      - * 작업 환경 *: 스토리지에 적용 가능한 경우 * Cloud Volumes ONTAP * 또는 * On-Premise * 를 선택한 다음 관련 작업 환경을 선택합니다.

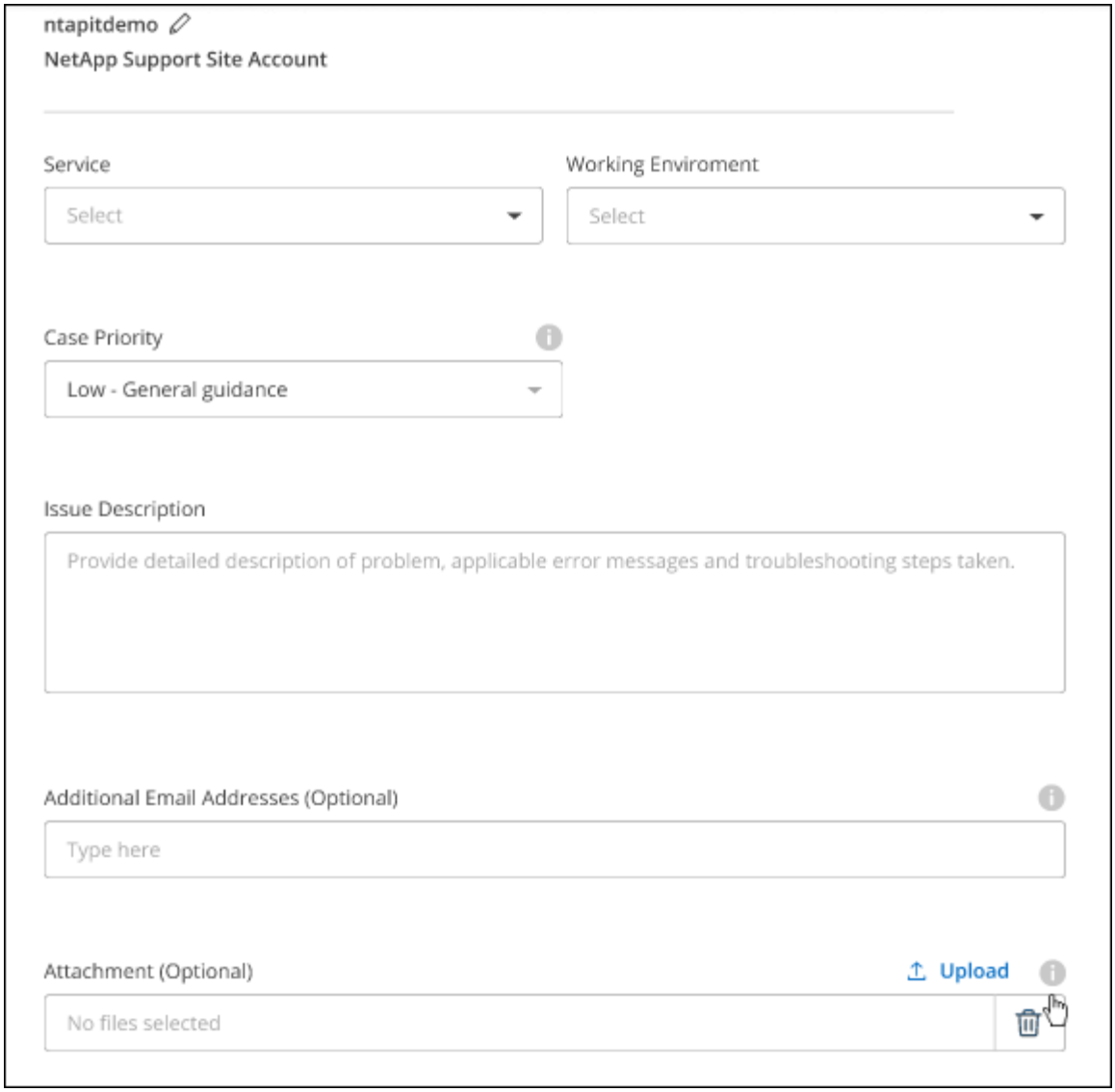
        작업 환경 목록은 서비스의 상단 배너에서 선택한 BlueXP 계정, 작업 영역 및 커넥터의 범위 내에 있습니다.

      - * 케이스 우선 순위 *: 케이스의 우선 순위를 선택합니다. 우선 순위는 낮음, 중간, 높음 또는 긴급입니다.

        이러한 우선 순위에 대한 자세한 내용을 보려면 필드 이름 옆에 있는 정보 아이콘 위로 마우스를 가져갑니다.

      - * 문제 설명 * : 해당 오류 메시지 또는 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공합니다.
      - * 추가 이메일 주소 *: 다른 사람에게 이 문제를 알고자 할 경우 추가 이메일 주소를 입력하십시오.
      - * 첨부 파일(선택 사항) *: 한 번에 하나씩 최대 5개의 첨부 파일을 업로드합니다.

        첨부 파일은 파일당 25MB로 제한됩니다. txt, log, pdf, jpg/jpeg, rtf, DOC/docx, xls/xlsx 및 CSV.



작업을 마친 후

지원 케이스 번호와 함께 팝업이 나타납니다. NetApp 지원 전문가가 귀사의 사례를 검토하고 곧 다시 연결해 드릴 것입니다.

지원 케이스 내역을 보려면 * 설정 > 타임라인 * 을 선택하고 "지원 케이스 생성"이라는 이름의 작업을 찾습니다. 오른쪽 끝에 있는 버튼을 사용하여 작업을 확장하여 세부 정보를 볼 수 있습니다.

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

"선택한 서비스에 대해 케이스를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 연결된 레코드 회사가 BlueXP 계정 일련 번호(960xxxx) 또는 작동 환경 일련 번호 다음 옵션 중 하나를 사용하여 지원을 요청할 수 있습니다.

- 제품 내 채팅을 사용합니다
- 에서 비기술 케이스를 제출하십시오 https://mysupport.netapp.com/site/help

지원 사례 관리(Preview)

BlueXP에서 직접 활성 및 해결된 지원 사례를 보고 관리할 수 있습니다. NSS 계정 및 회사와 관련된 케이스를 관리할 수 있습니다.

케이스 관리를 미리 보기로 사용할 수 있습니다. NetApp은 이 경험을 개선하고 다음 릴리즈에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 사용하여 피드백을 보내주십시오.

다음 사항에 유의하십시오.

- 페이지 상단의 케이스 관리 대시보드에서는 두 가지 보기를 제공합니다.
  - 왼쪽 보기에는 사용자가 제공한 NSS 계정으로 지난 3개월 동안 개설된 총 케이스가 표시됩니다.
  - 오른쪽 보기에는 사용자 NSS 계정을 기준으로 회사 수준에서 지난 3개월 동안 개설된 총 사례가 표시됩니다.

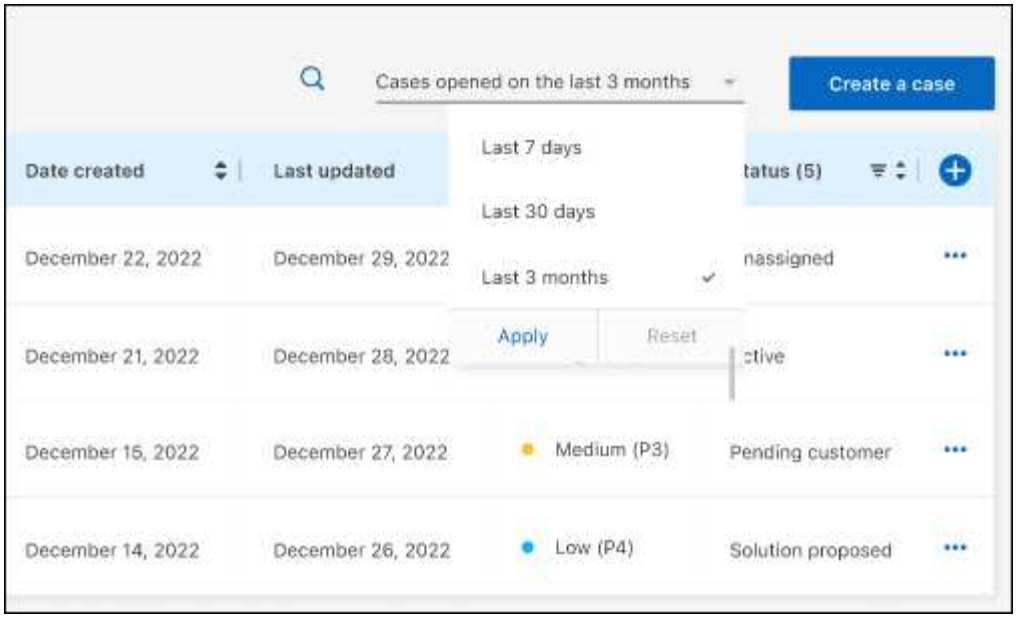
  테이블의 결과에는 선택한 보기와 관련된 사례가 반영됩니다.
- 관심 있는 열을 추가 또는 제거할 수 있으며 우선 순위 및 상태 등의 열 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

  자세한 내용은 아래 단계를 참조하십시오.
- 케이스 수준별로 케이스 메모를 업데이트하거나 아직 종결 또는 미결 종결 상태가 아닌 케이스를 종결할 수 있습니다.

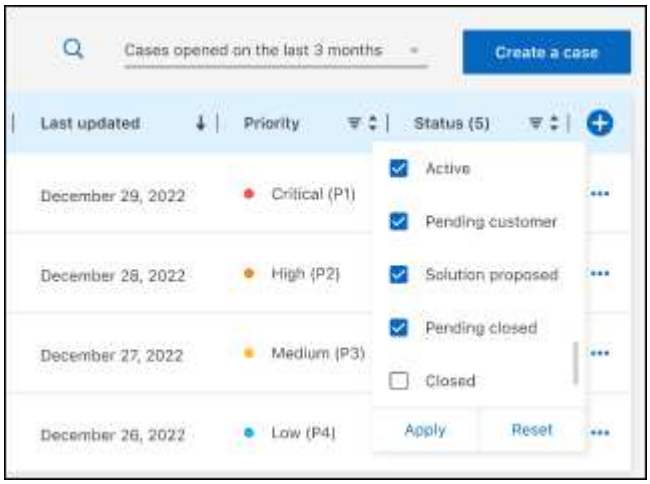
단계

1. BlueXP에서 * 도움말 > 지원 * 을 선택합니다.
2. Case Management * 를 선택하고 메시지가 표시되면 NSS 계정을 BlueXP에 추가합니다.

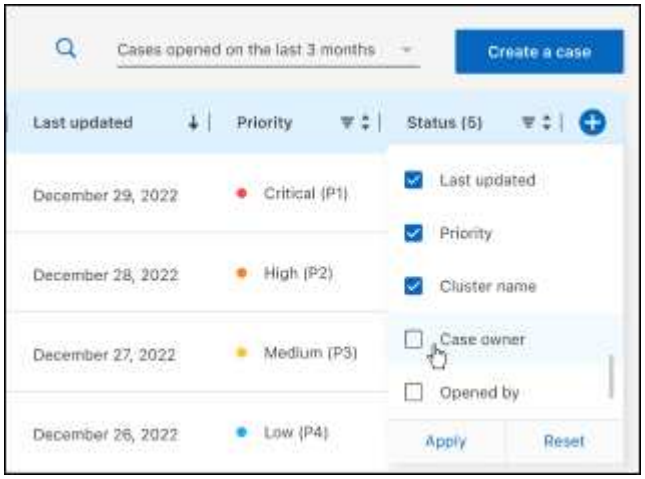
   케이스 관리 * 페이지에는 BlueXP 사용자 계정과 연결된 NSS 계정과 관련된 미해결 케이스가 표시됩니다. NSS 관리 * 페이지 상단에 나타나는 것과 동일한 NSS 계정입니다.
3. 필요한 경우 테이블에 표시되는 정보를 수정합니다.
   - 조직의 케이스 * 에서 * 보기 * 를 선택하여 회사와 관련된 모든 케이스를 봅니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정합니다.



◦ 열의 내용을 필터링합니다.



◦ 를 선택하여 테이블에 표시되는 열을 변경합니다 ⊕ 표시할 열을 선택합니다.

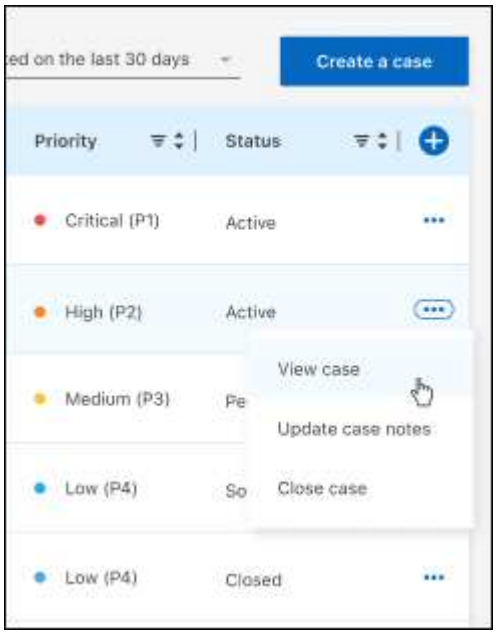


4. 를 선택하여 기존 케이스를 관리합니다 ••• 사용 가능한 옵션 중 하나를 선택합니다.

- * 사례 보기 *: 특정 케이스에 대한 전체 세부 정보를 봅니다.
- * 케이스 메모 업데이트 *: 문제에 대한 추가 세부 정보를 제공하거나 * 파일 업로드 * 를 선택하여 최대 5개의 파일을 첨부할 수 있습니다.

  첨부 파일은 파일당 25MB로 제한됩니다. txt, log, pdf, jpg/jpeg, rtf, DOC/docx, xls/xlsx 및 CSV.

- * 케이스 종료 *: 케이스를 종료하는 이유에 대한 세부 정보를 제공하고 * 케이스 닫기 * 를 선택합니다.



법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

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

상표

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

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

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

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

개인 정보 보호 정책

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

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

- "BlueXP에 대한 고지 사항"
- "BlueXP 분류 고지 사항"

저작권 정보

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

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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