시작하십시오
BlueXP classification

NetApp
April 03, 2024

목차

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.

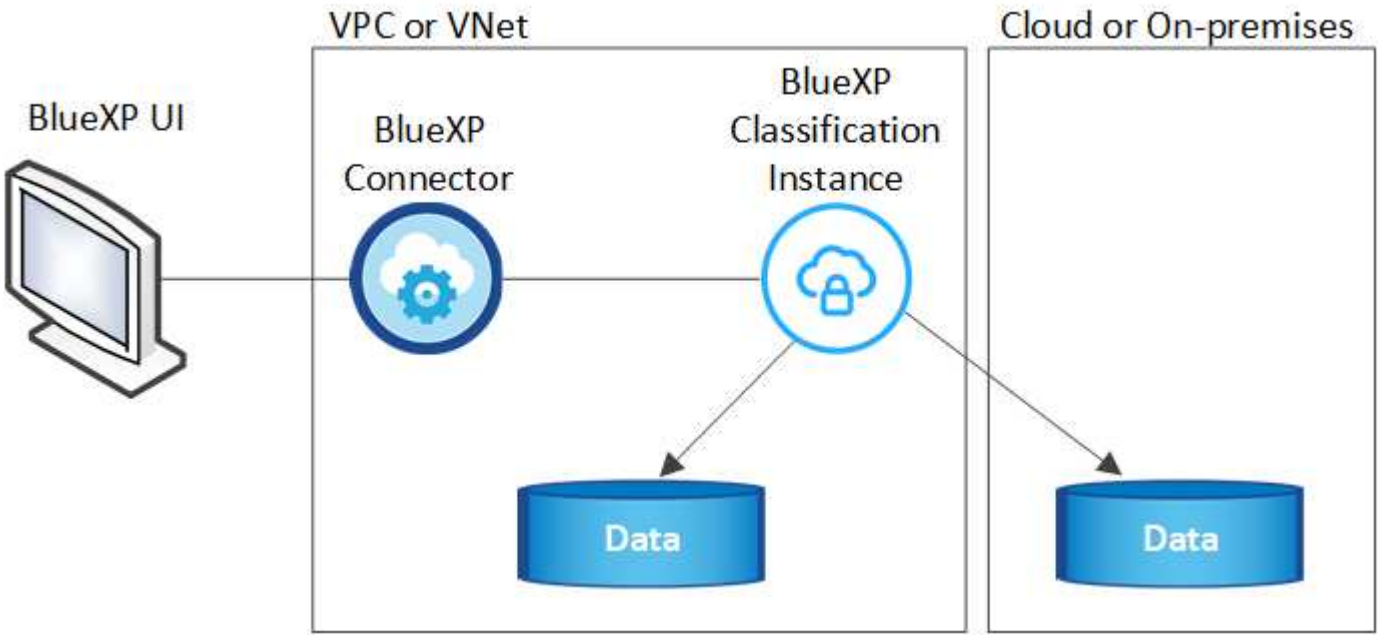
데이터 전송 비용

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

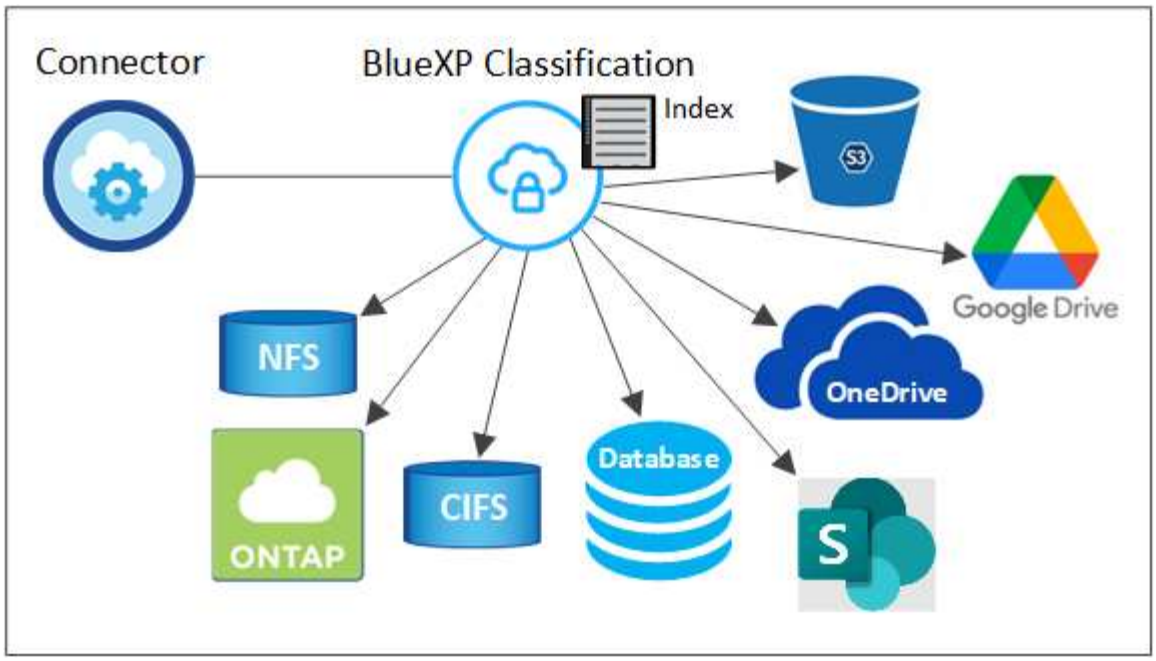
BlueXP 분류는 다음과 같이 작동합니다.

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

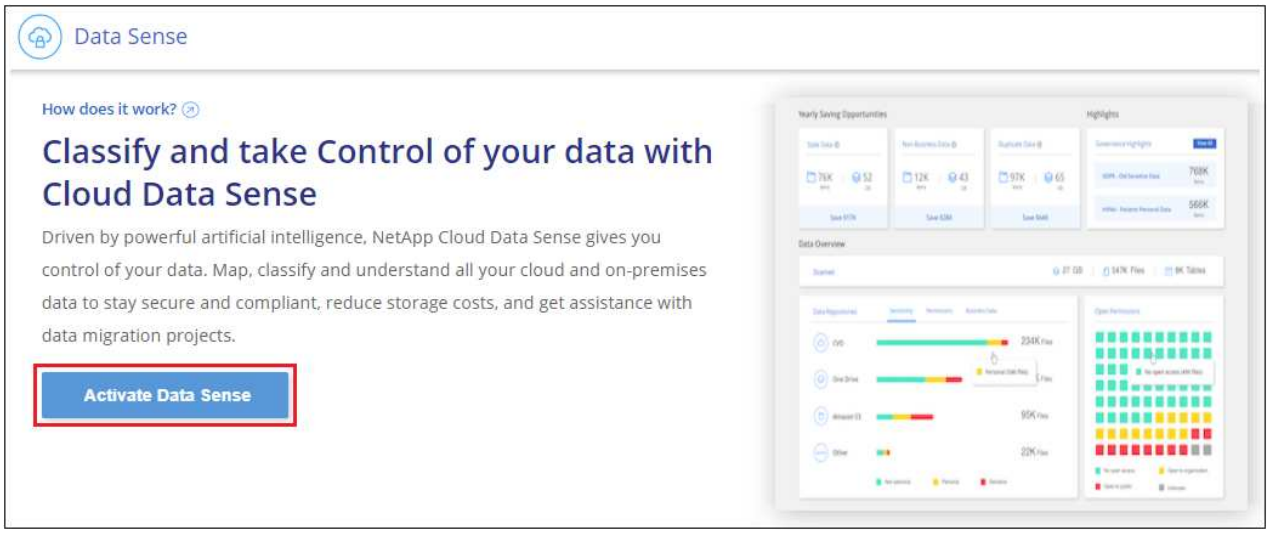
다음 단계에 따라 클라우드에 BlueXP 분류 인스턴스를 배포합니다. Connector는 클라우드에 인스턴스를 배포한 다음 해당 인스턴스에 BlueXP 분류 소프트웨어를 설치합니다.

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.



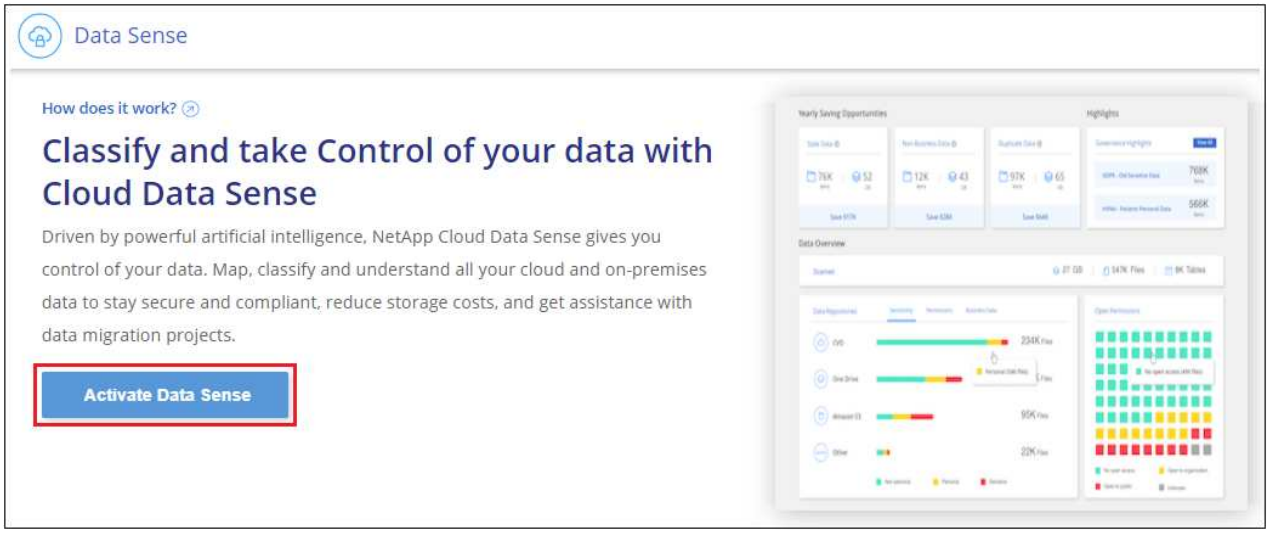
2. Activate Data Sense * 를 클릭합니다.
3. Installation_page에서 * deploy > deploy * 를 클릭하여 "큰" 인스턴스 크기를 사용하고 클라우드 배포 마법사를 시작합니다.
4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

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

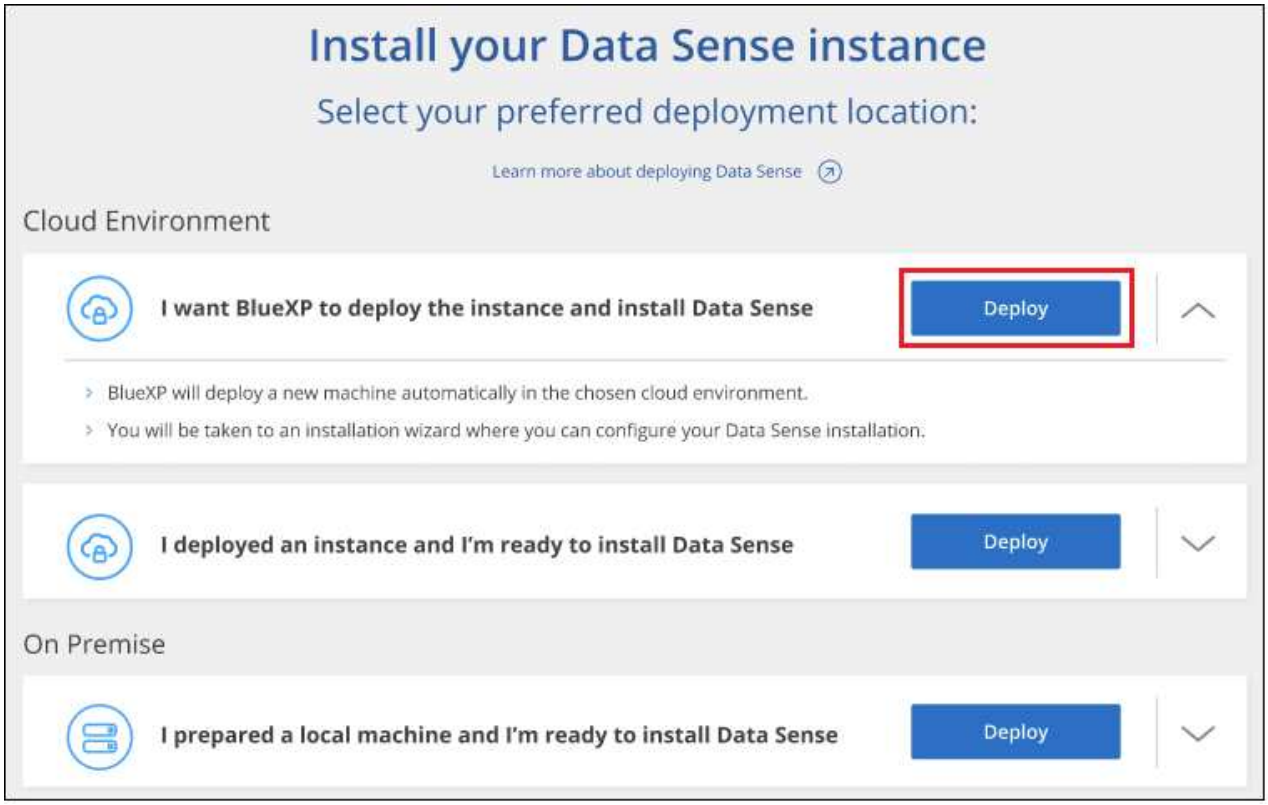
Azure에 구축

단계

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



3. 클라우드 배포 마법사를 시작하려면 * 배포 * 를 클릭합니다.



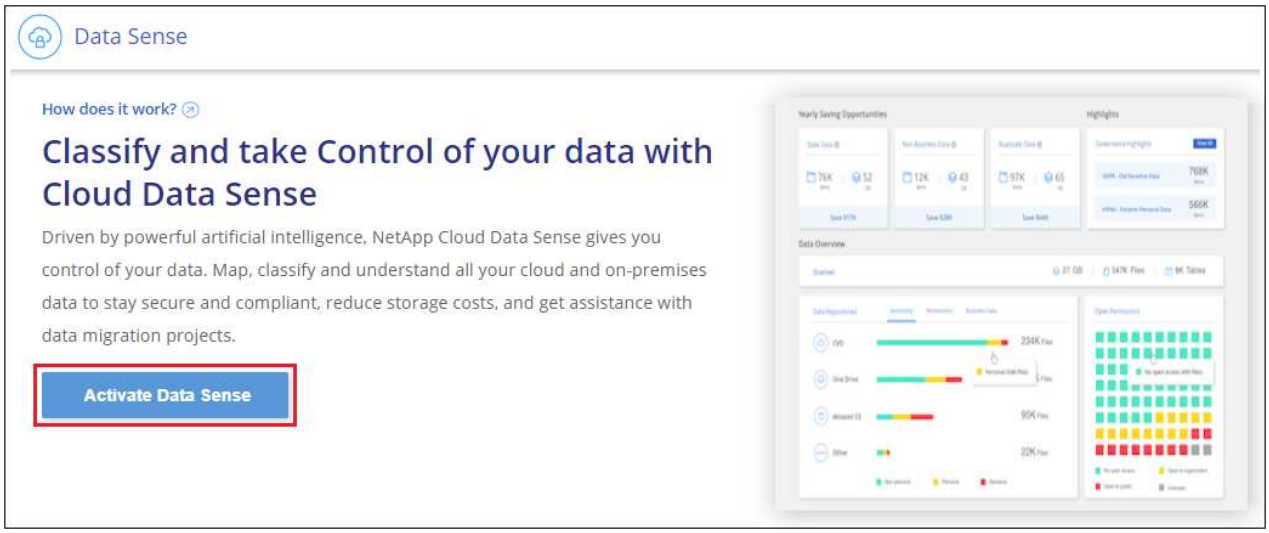
4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생하면 중지하고 입력을 묻는 메시지가 표시됩니다.

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

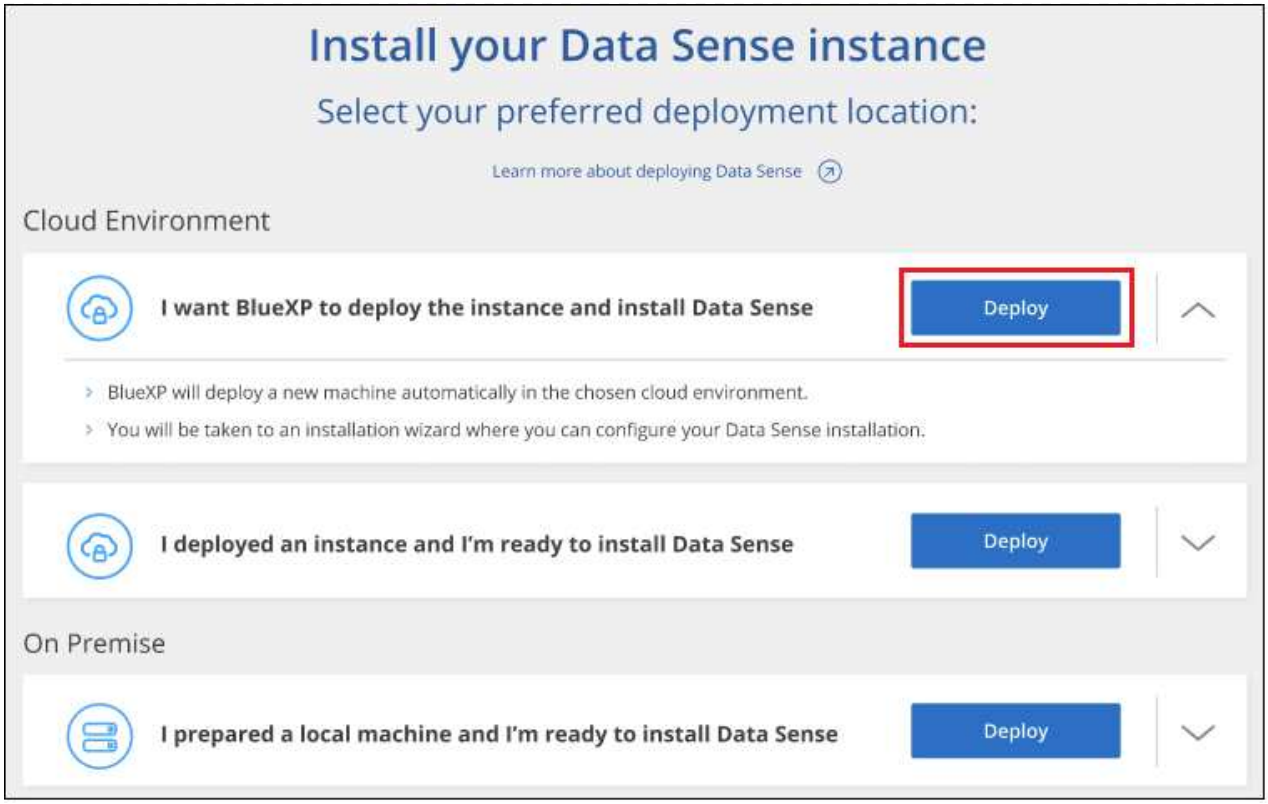
Google Cloud에 배포

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.

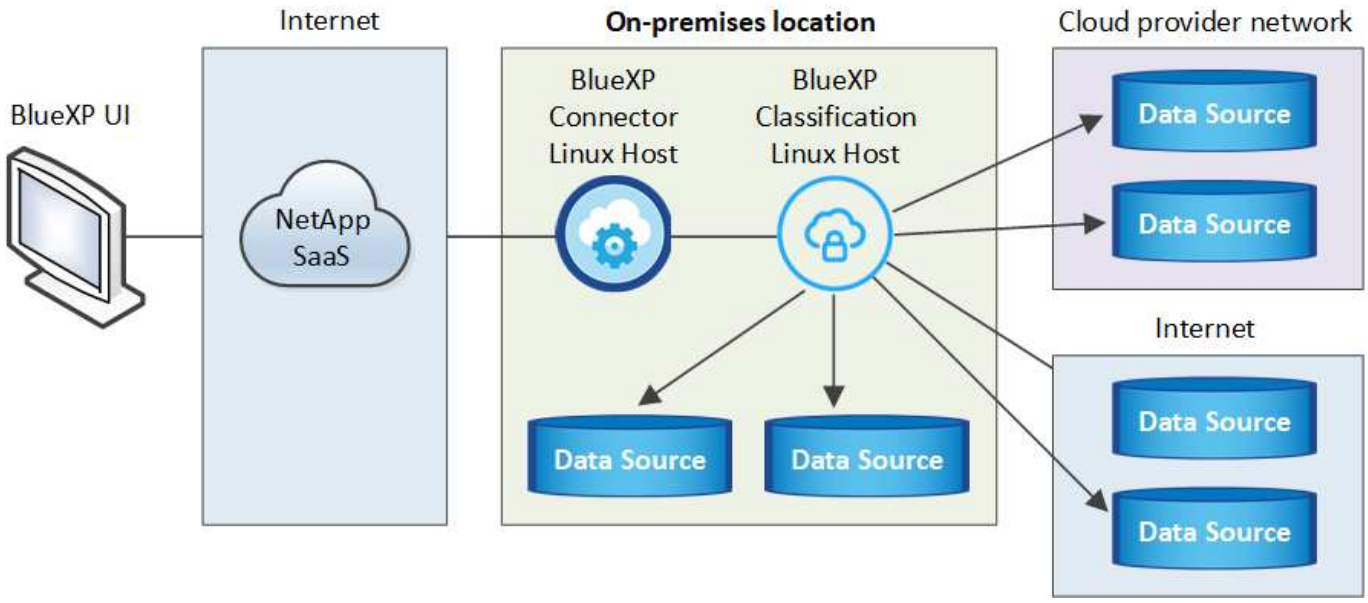
인터넷에 액세스할 수 있는 호스트에 **BlueXP** 분류를 설치합니다

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.

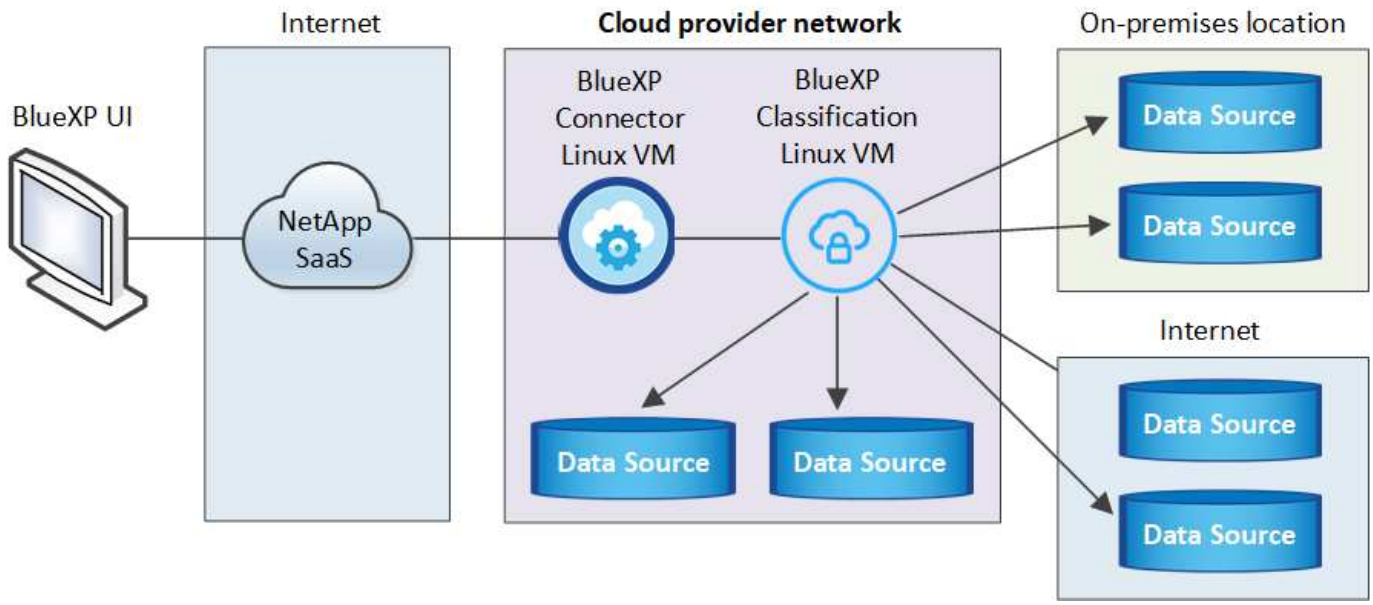
온프레미스에도 위치한 BlueXP 분류 인스턴스를 사용하여 온프레미스 ONTAP 시스템을 스캔하려는 경우 온프레미스 설치가 좋은 옵션이 될 수 있지만, 이는 필수 사항이 아닙니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다.

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.

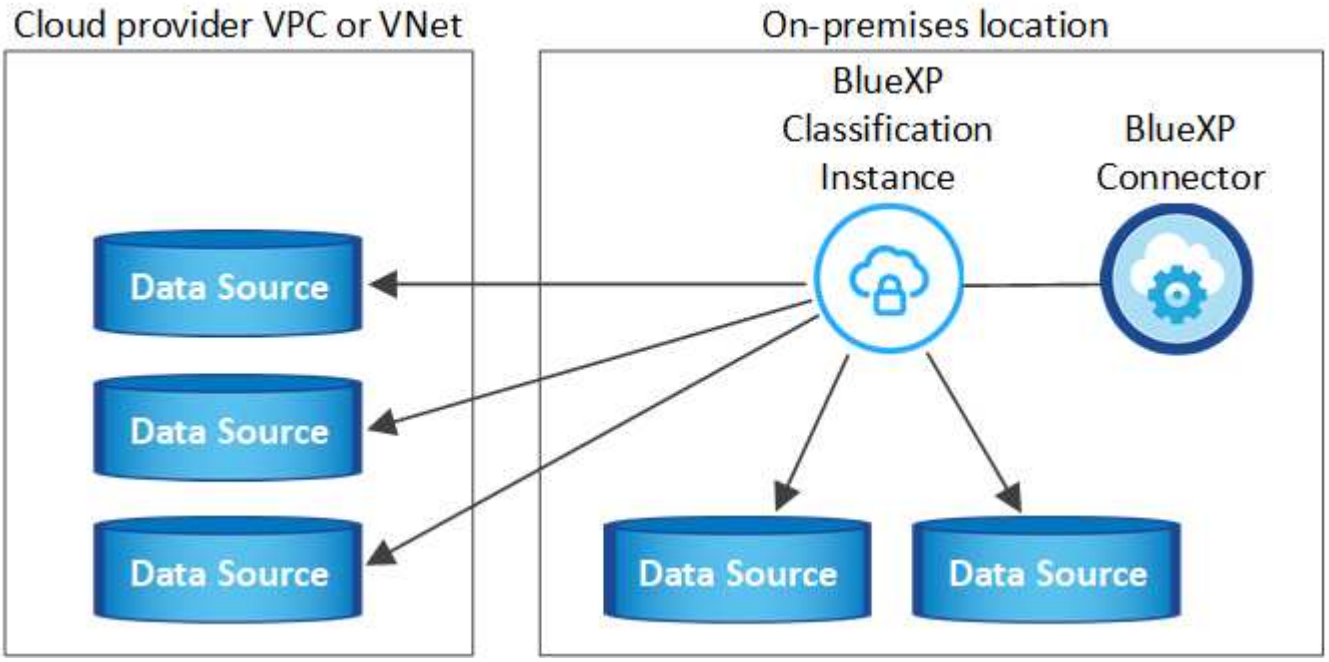
연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 443(TCP) 및 80	Connector의 방화벽 또는 라우팅 규칙은 포트 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 포트 8080이 열려 있는지 확인하여 BlueXP에서 설치 진행률을 확인합니다.

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)

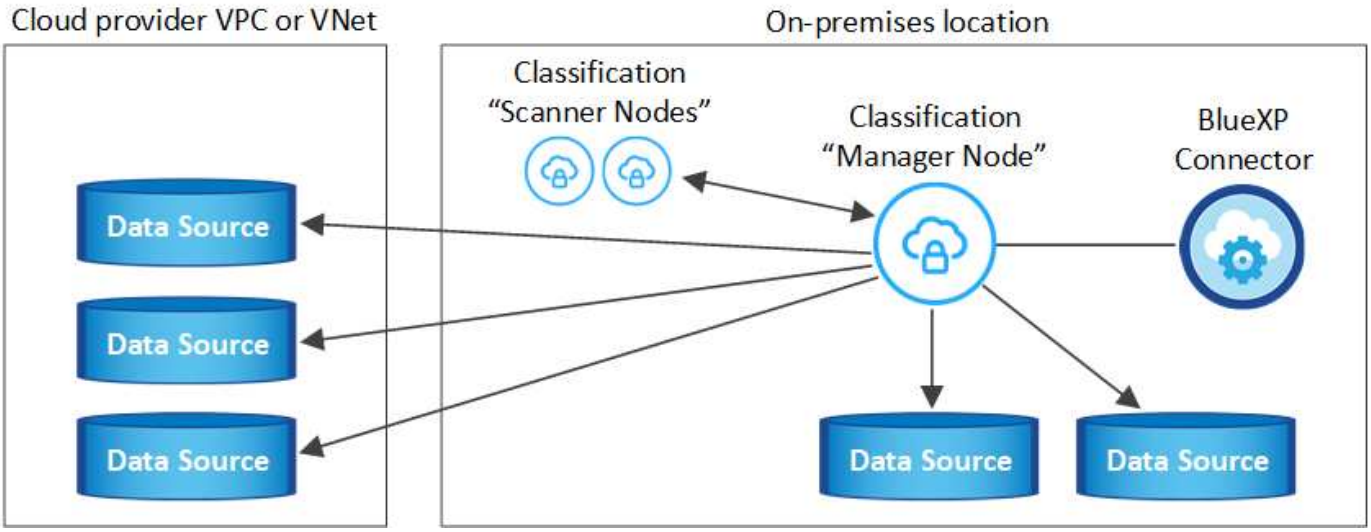
여러 BlueXP 분류 호스트를 사용하여 데이터 소스를 검사하는 추가 처리 기능을 제공하는 경우 추가 포트/프로토콜을 활성화해야 합니다. "추가 포트 요구 사항을 참조하십시오".

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

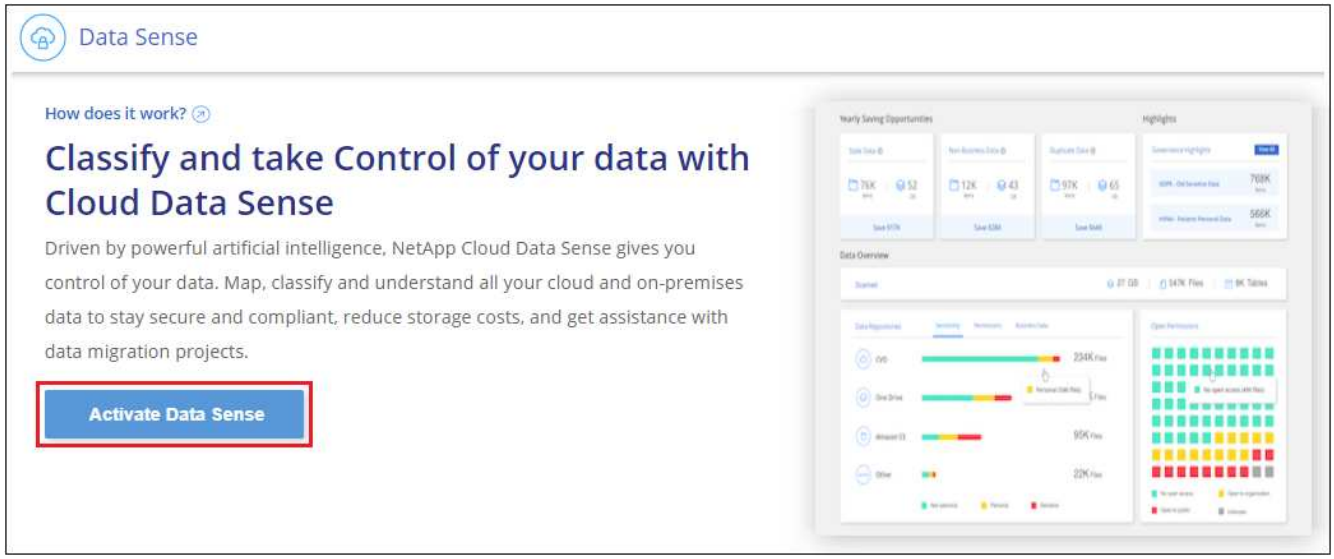
- Linux 시스템이 를 충족하는지 확인합니다 호스트 요구 사항.
- 시스템에 2개의 필수 소프트웨어 패키지(Docker Engine 또는 Podman 및 Python 3)가 설치되어 있는지 확인합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 인터넷 액세스에 프록시를 사용하는 경우:
  - 프록시 서버 정보(IP 주소 또는 호스트 이름, 연결 포트, 연결 스키마: https 또는 http, 사용자 이름 및 암호)가 필요합니다.
  - 프록시가 TLS 가로채기를 수행하는 경우 TLS CA 인증서가 저장된 BlueXP 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

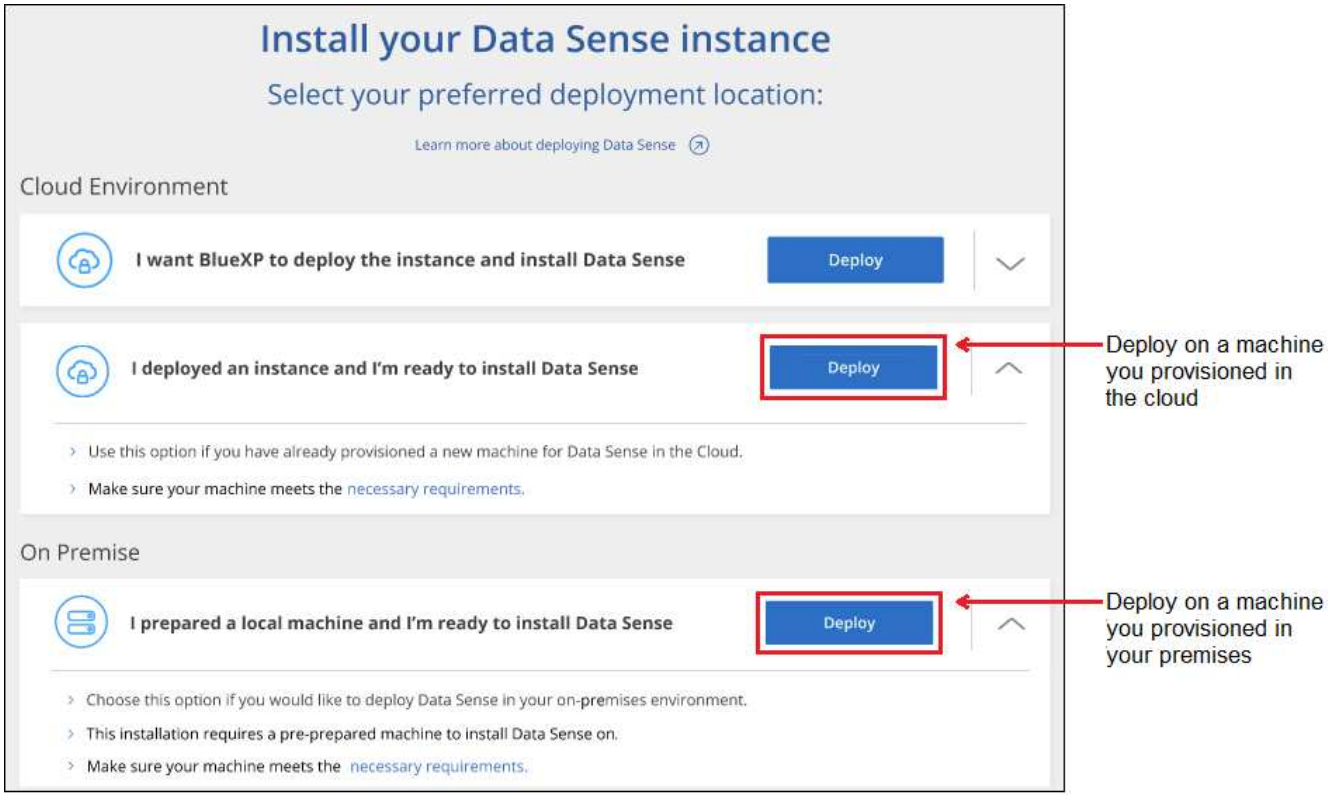
1. 에서 BlueXP 분류 소프트웨어를 다운로드합니다 "NetApp Support 사이트". 선택해야 하는 파일의 이름은 * DATASENSE-INinstaller-<version>.tar.gz * 입니다.
2. 설치 프로그램 파일을 사용하려는 Linux 호스트에 복사합니다(scp 또는 다른 방법 사용).
3. 호스트 시스템에서 설치 프로그램 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

```
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.

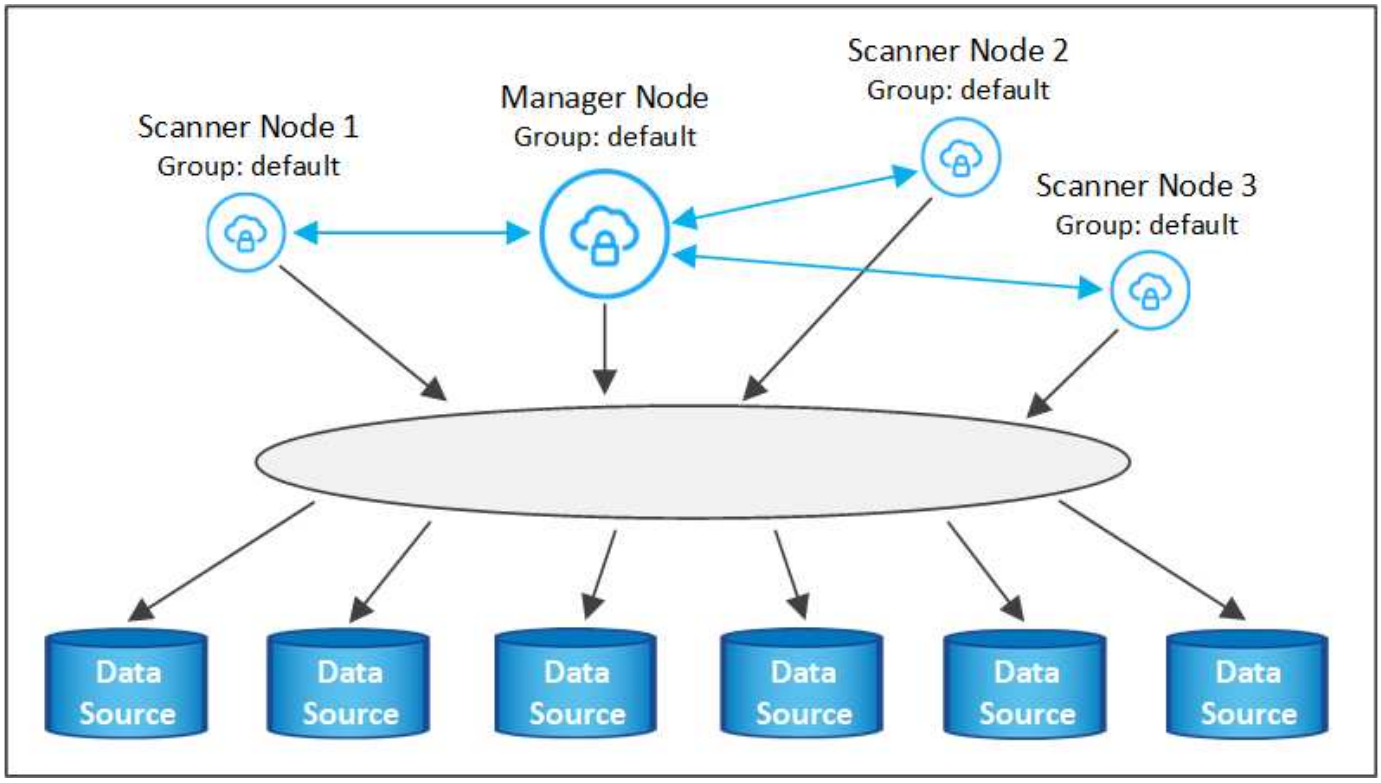
기존 배포에 스캐너 노드를 추가합니다

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

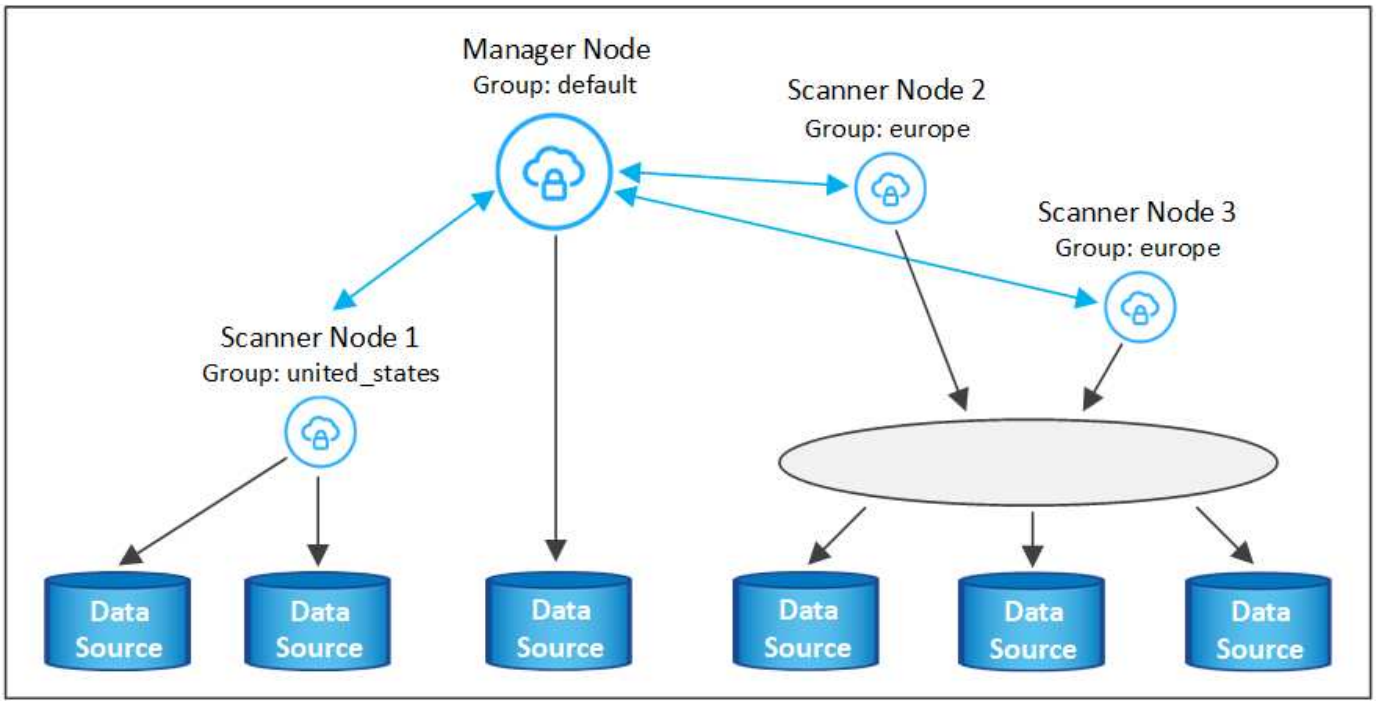
기본적으로 새로 추가한 스캐너 노드는 스캔 리소스의 일반 풀에 추가됩니다. 이를 "기본 스캐너 그룹"이라고 합니다. 아래 이미지의 "기본" 그룹에는 6개 데이터 소스 모두의 스캔 데이터인 1개의 관리자 노드와 3개의 스캐너 노드가 있습니다.



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.

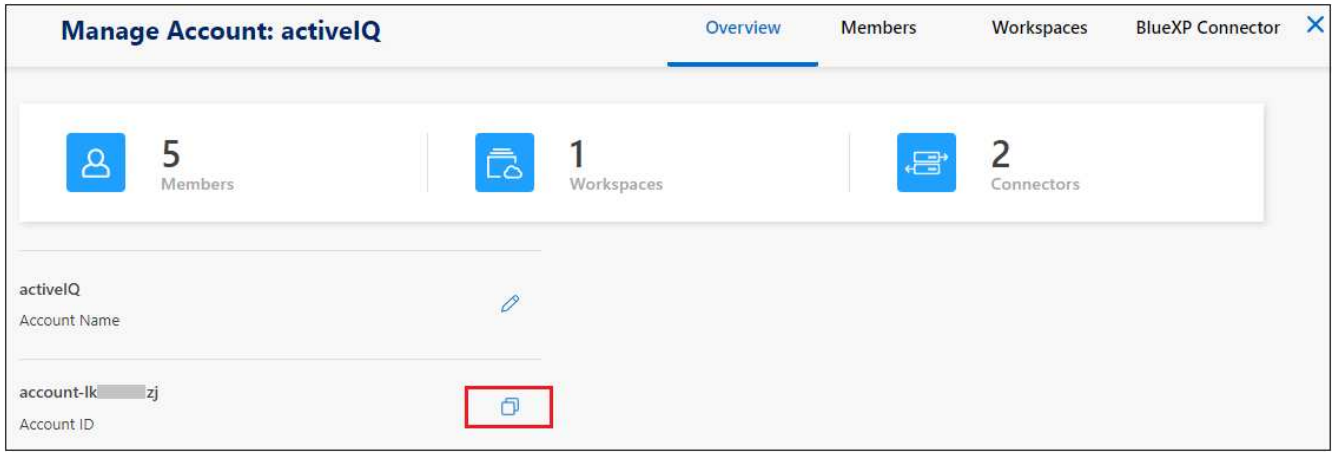
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp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

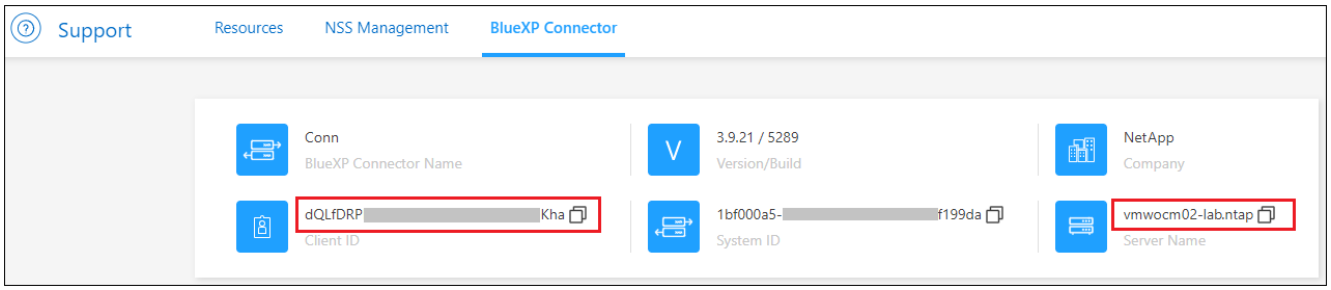
필수 단계

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

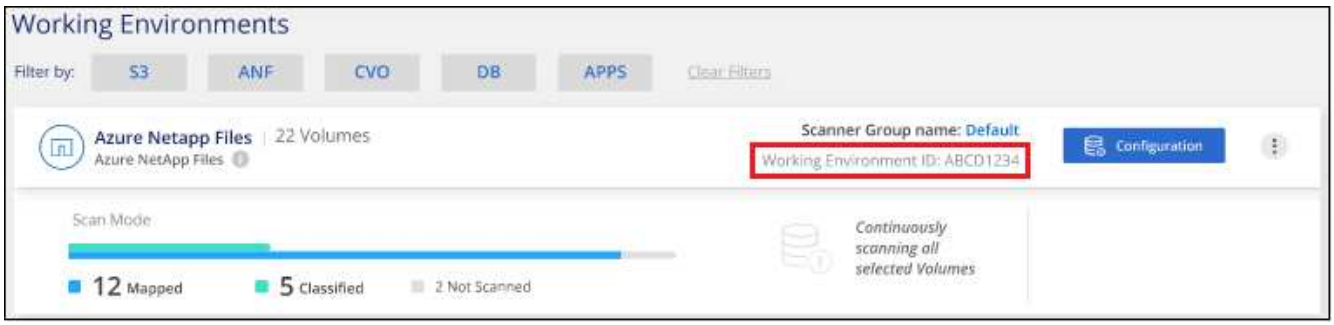
1. BlueXP 메뉴 표시줄에서 * 계정 > 계정 관리 * 를 클릭합니다.



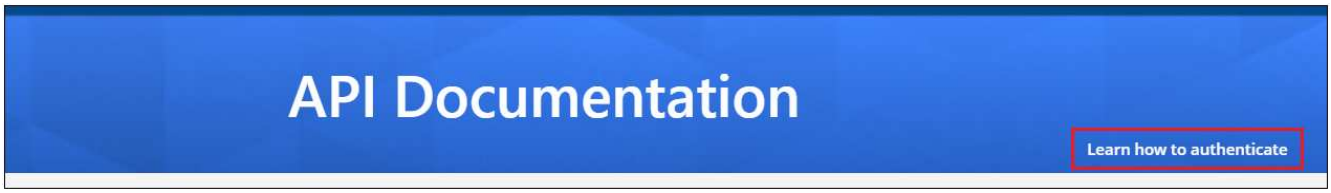
2. 계정 ID _ 을(를) 복사합니다.
3. BlueXP 메뉴 모음에서 * 도움말 > 지원 > BlueXP 커넥터 * 를 클릭합니다.



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`

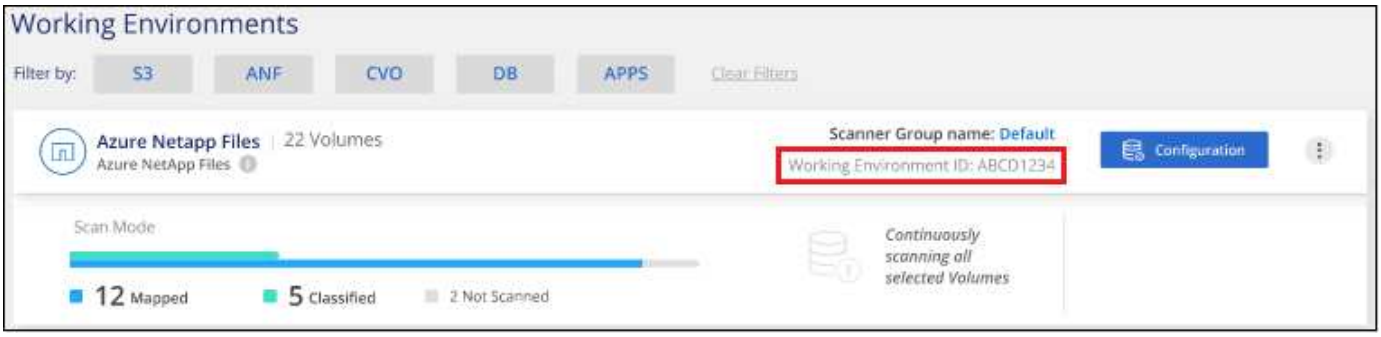
결과

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

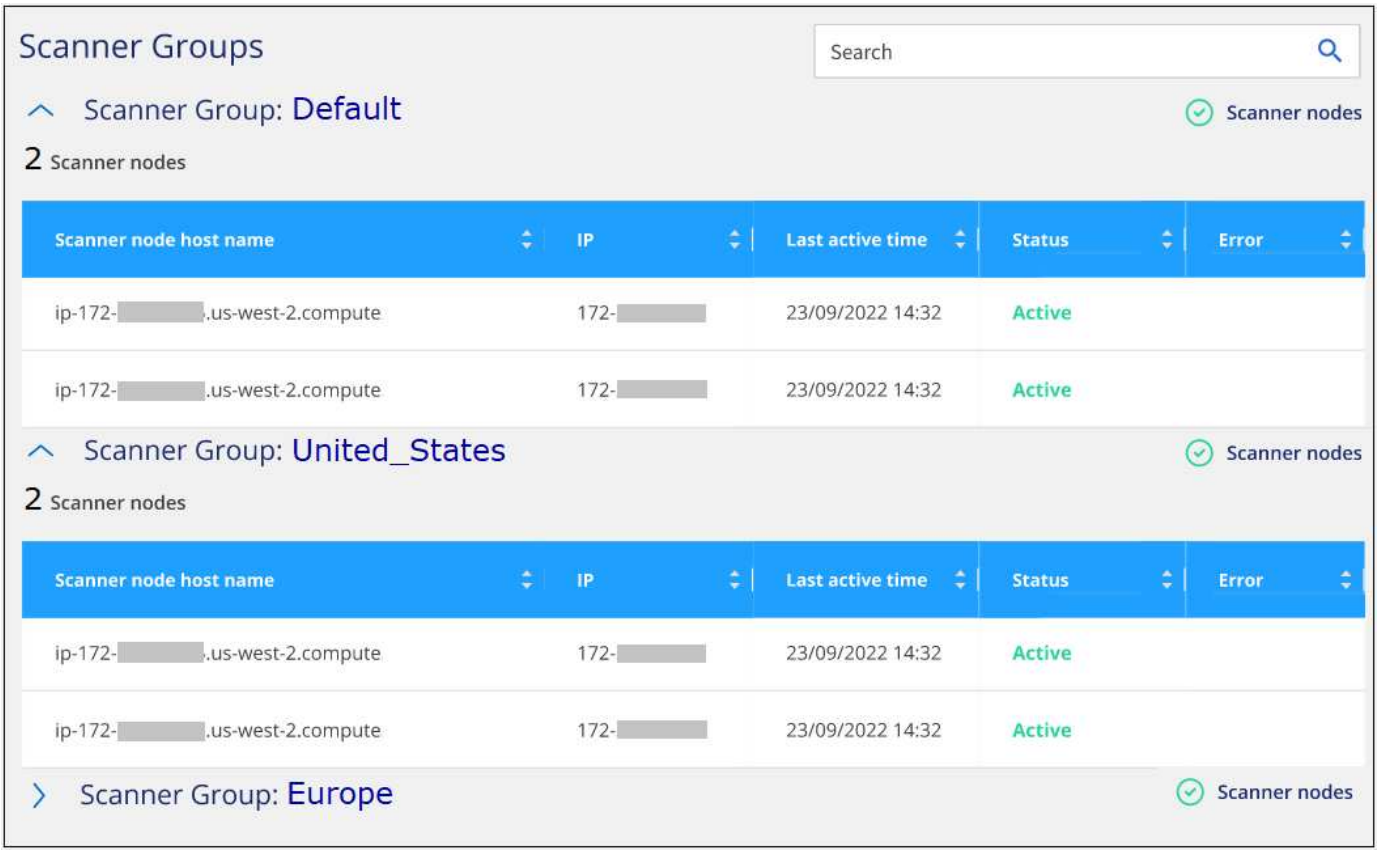
다음 단계

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.

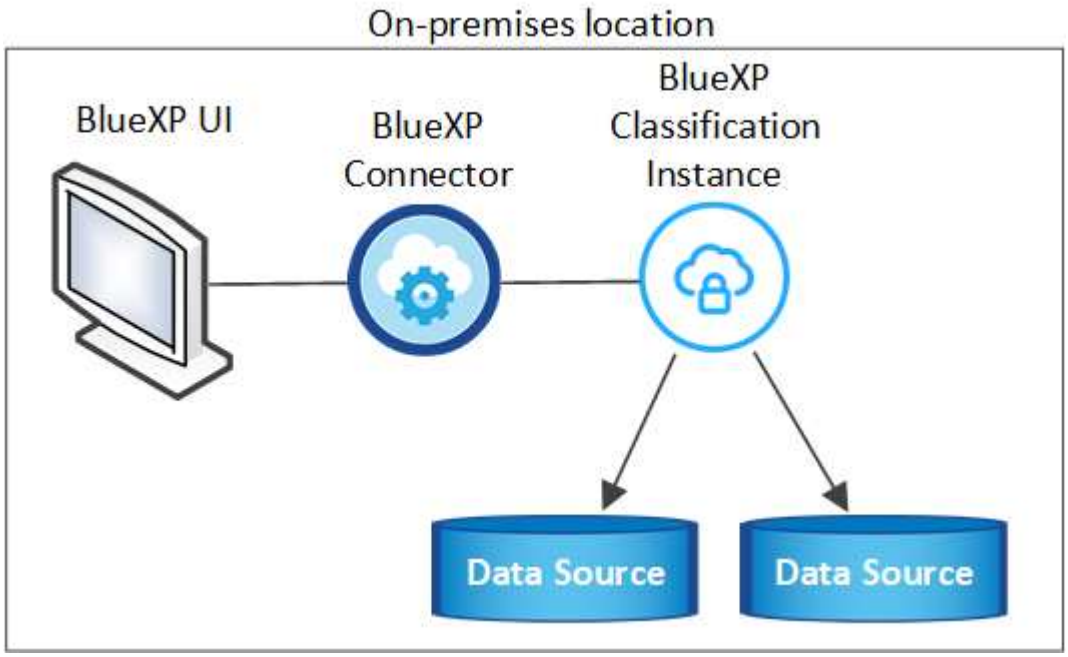
연결 유형	포트	설명
커넥터 <>BlueXP 분류	8080(TCP), 6000(TCP), 443(TCP) 및 80	Connector의 보안 그룹은 포트 6000 및 443을 통해 BlueXP 분류 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. • BlueXP 분류 BYOL 라이센스가 다크 사이트에서 작동하도록 하려면 포트 6000이 필요합니다. • BlueXP에서 설치 진행률을 확인할 수 있도록 포트 8080이 열려 있어야 합니다.
커넥터 <>ONTAP 클러스터(NAS)	443(TCP)	BlueXP는 HTTPS를 사용하여 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)

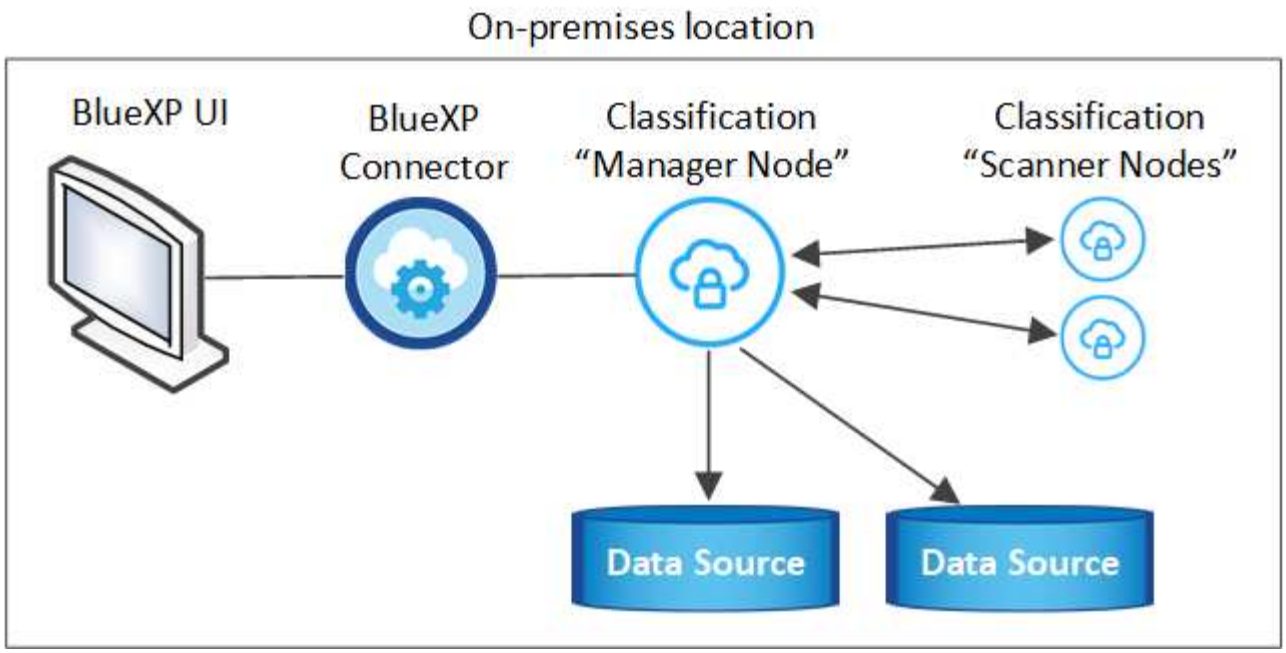
여러 BlueXP 분류 호스트를 사용하여 데이터 소스를 검사하는 추가 처리 기능을 제공하는 경우 추가 포트/프로토콜을 활성화해야 합니다. "추가 포트 요구 사항을 참조하십시오".

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.

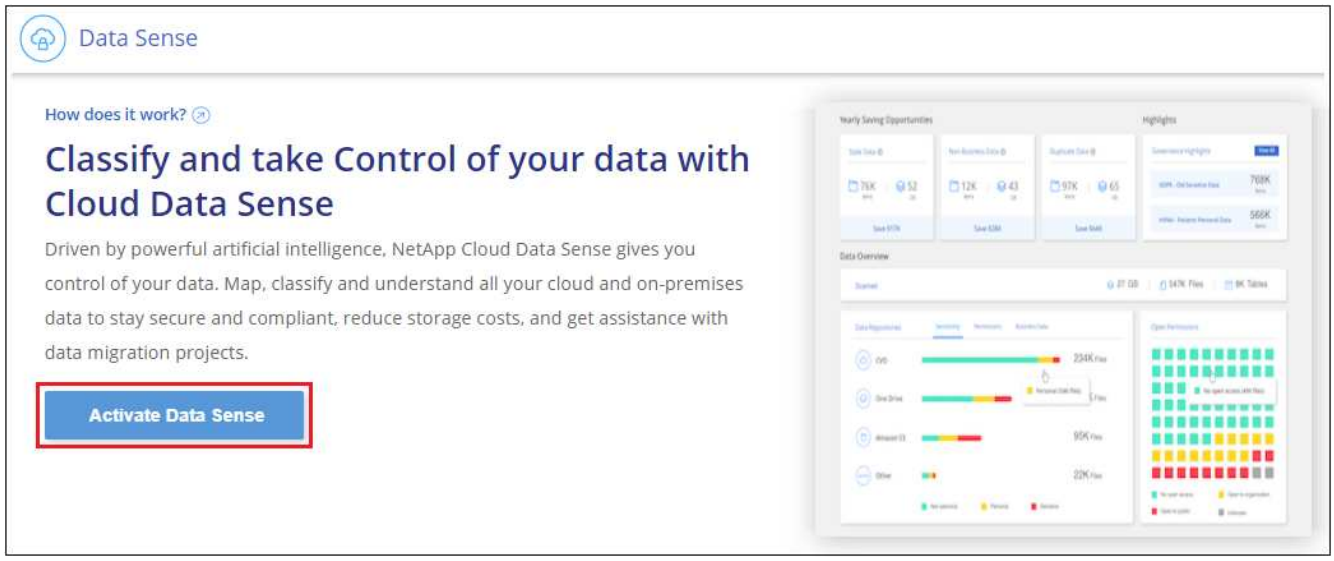
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

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

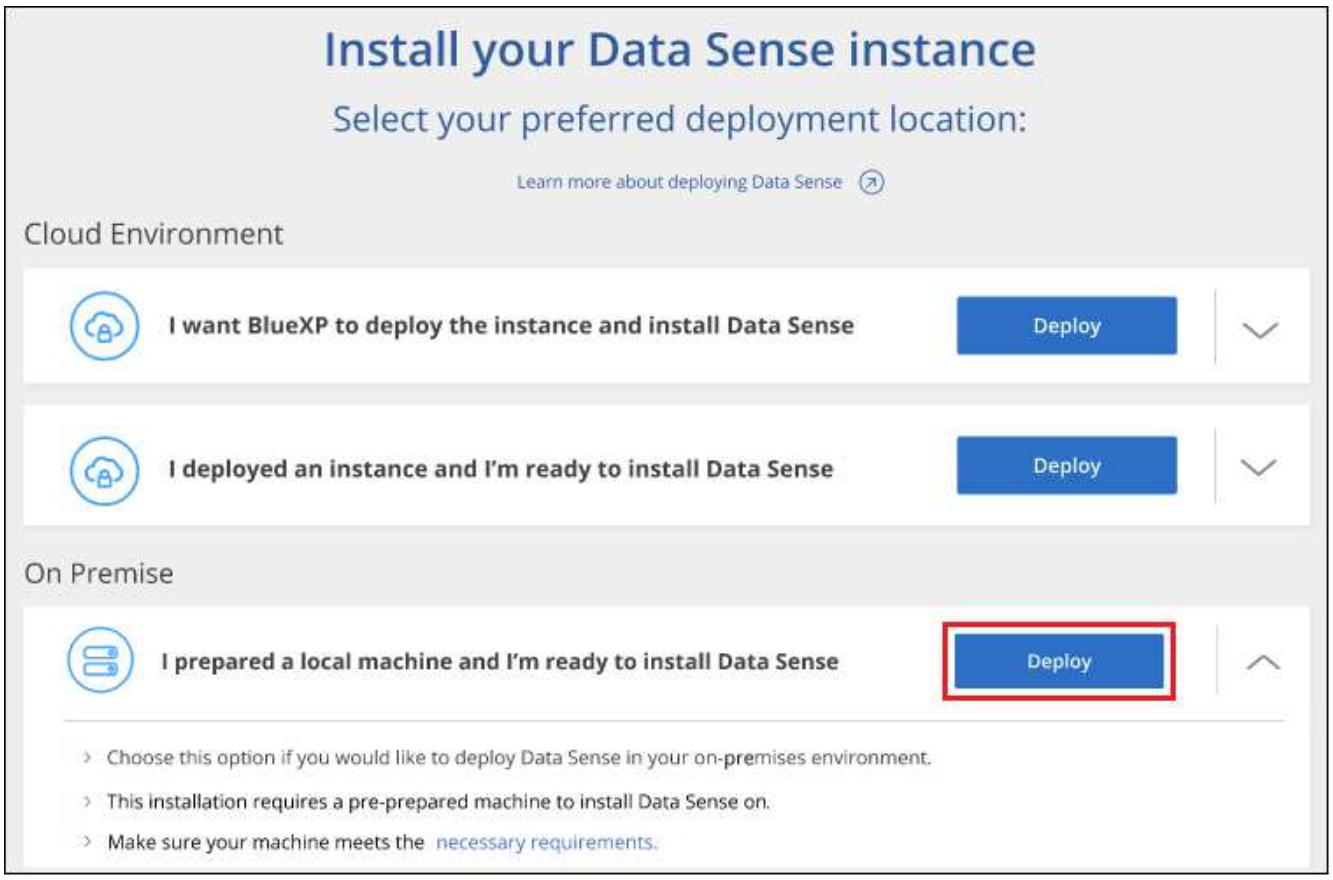
4. 호스트 시스템에서 설치 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

   ```
   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".

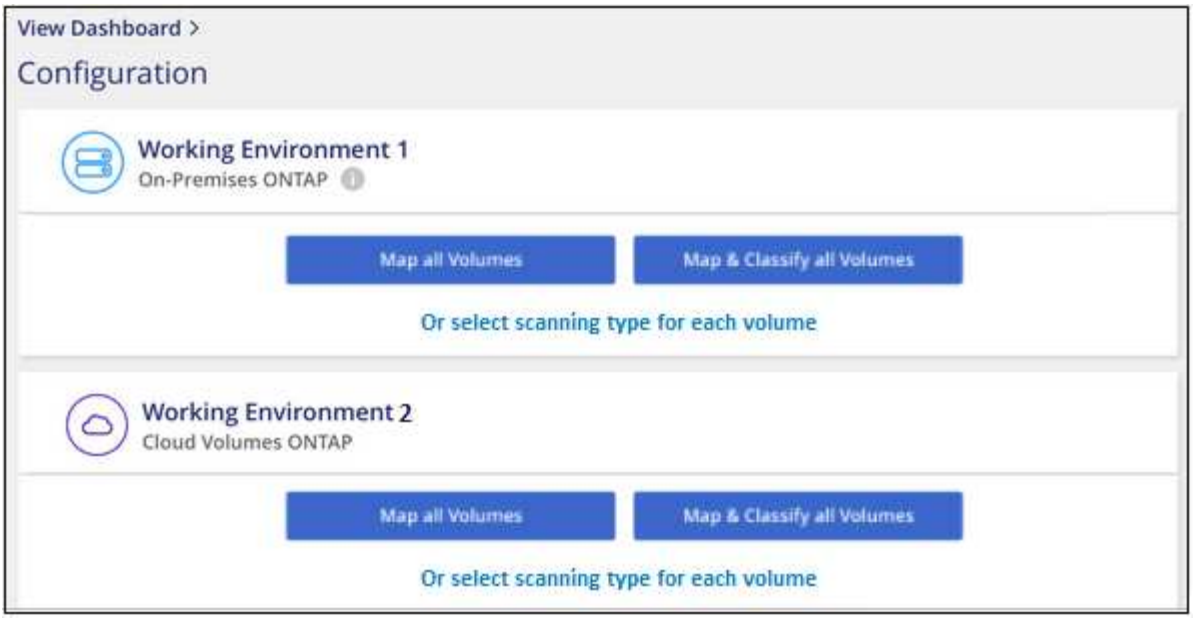
인터넷에 액세스할 수 없는 어두운 사이트에 설치된 온-프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 BlueXP 분류를 배포합니다". 또한 BlueXP Connector를 동일한 사내 위치에 배포해야 합니다.

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

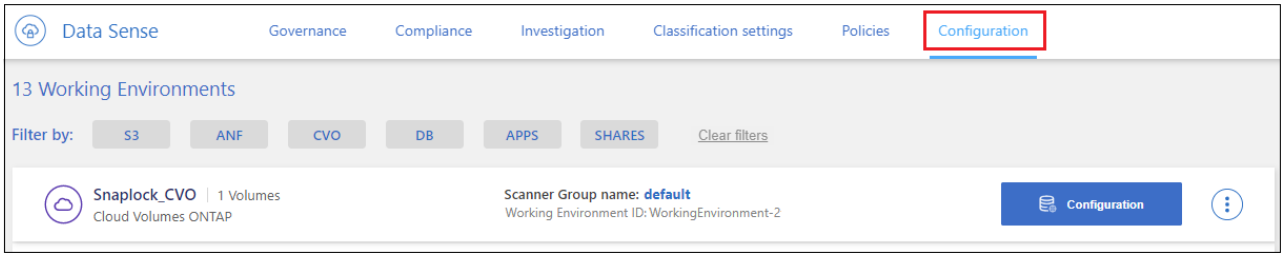
네트워크 사이에 네트워크 연결이 있는지 확인합니다.

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.

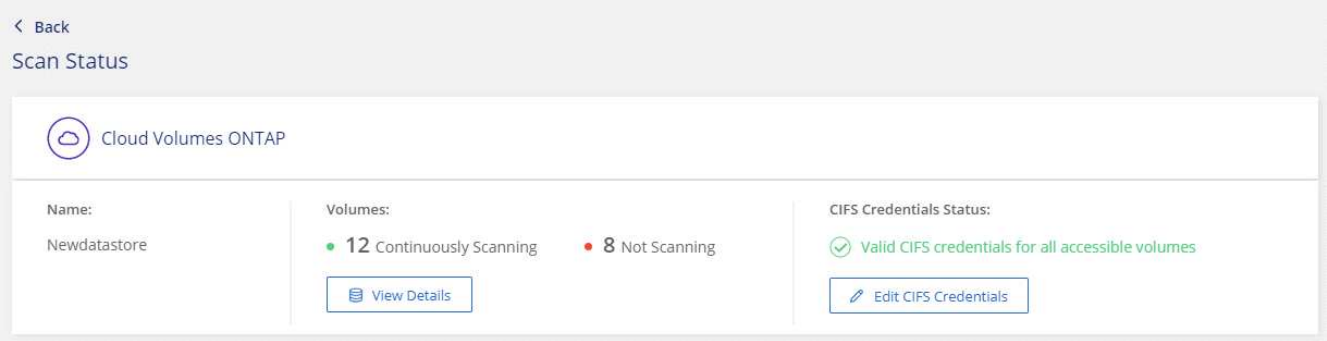


   b. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 BlueXP 분류에서 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

      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.

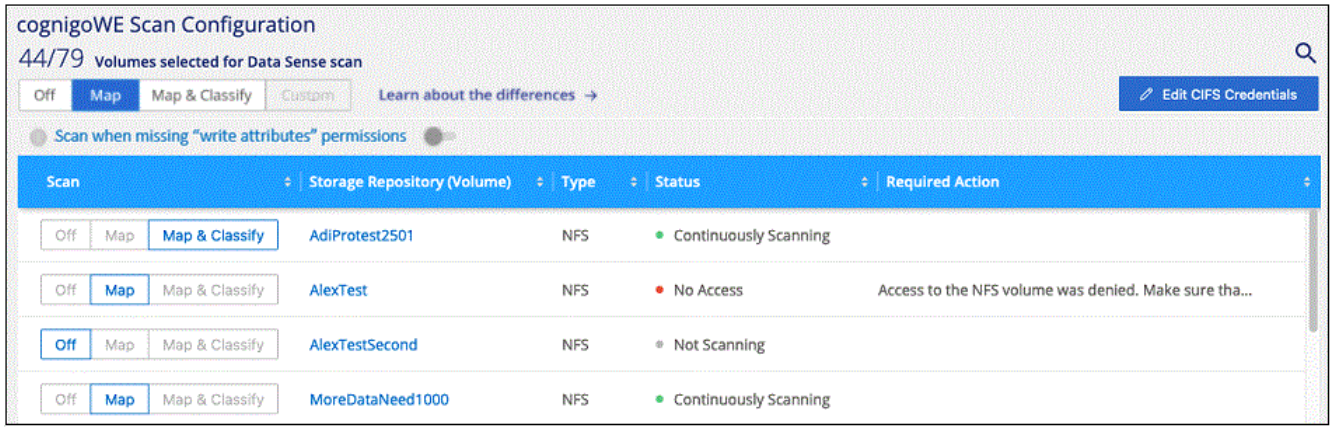
      BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 CIFS에서 쓰기 속성 사용 권한 또는 NFS에서 쓰기 권한이 사용자에게 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

      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.

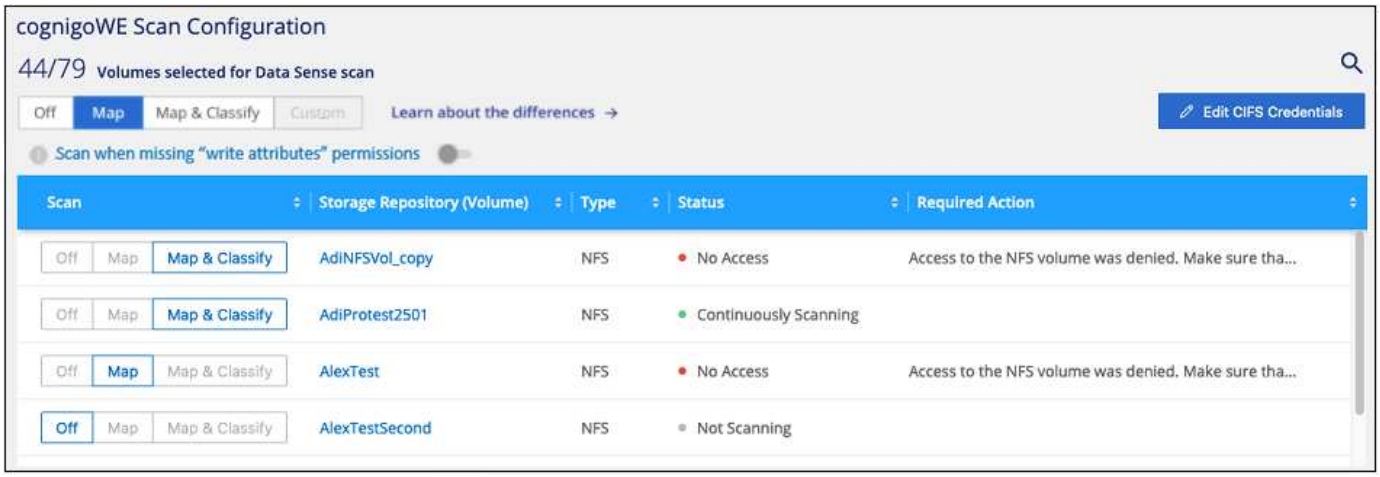
예를 들어 다음 이미지는 네 개의 볼륨을 보여 줍니다. 그 중 하나는 BlueXP 분류 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 BlueXP 분류에서 스캔할 수 없는 볼륨입니다.



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".



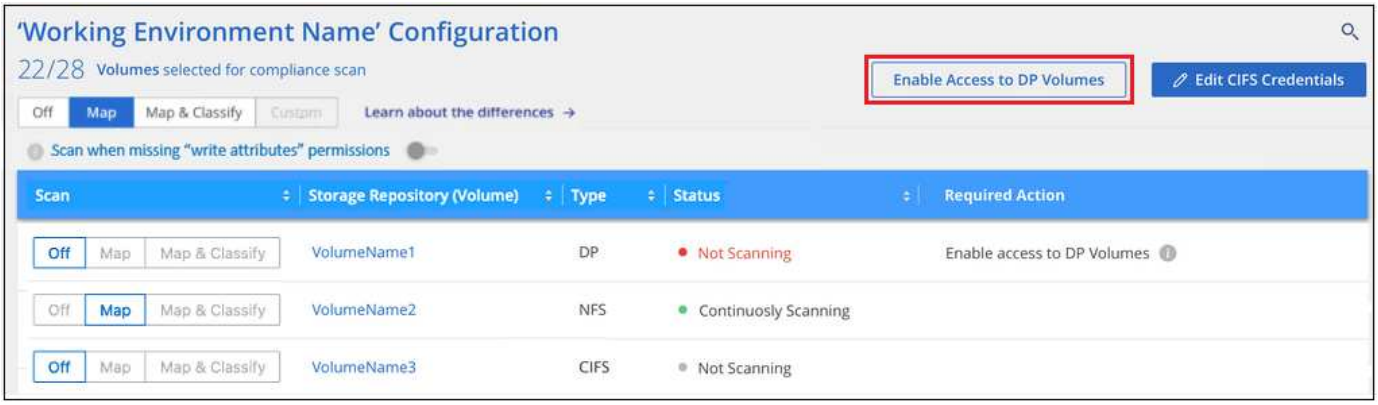
대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다
볼륨에서 스캔을 비활성화합니다	볼륨 영역에서 * Off * 를 클릭합니다
모든 볼륨에서 매핑 전용 스캔을 활성화합니다	제목 영역에서 * Map * 을 클릭합니다
모든 볼륨에서 전체 스캔을 활성화합니다	제목 영역에서 * 지도 및 분류 * 를 클릭합니다
모든 볼륨에서 스캔을 비활성화합니다	제목 영역에서 * Off * 를 클릭합니다

> 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.

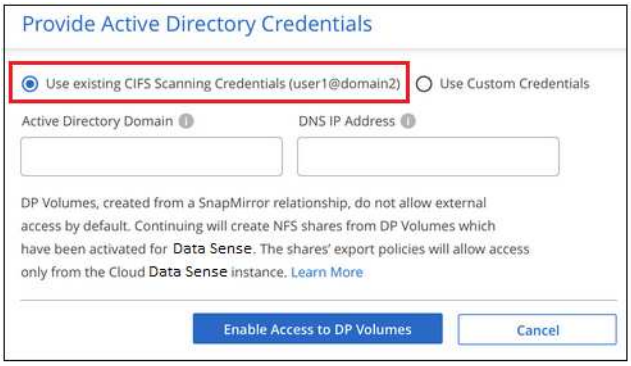
처음에 볼륨 목록은 이러한 볼륨을 *Type* DP*로 식별하며 *Status* Not Scanning* 및 *Required Action* DP 볼륨에 대한 액세스 사용*.

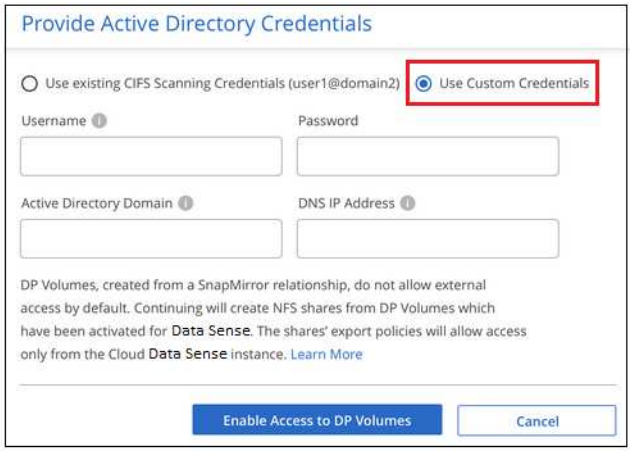


단계

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.

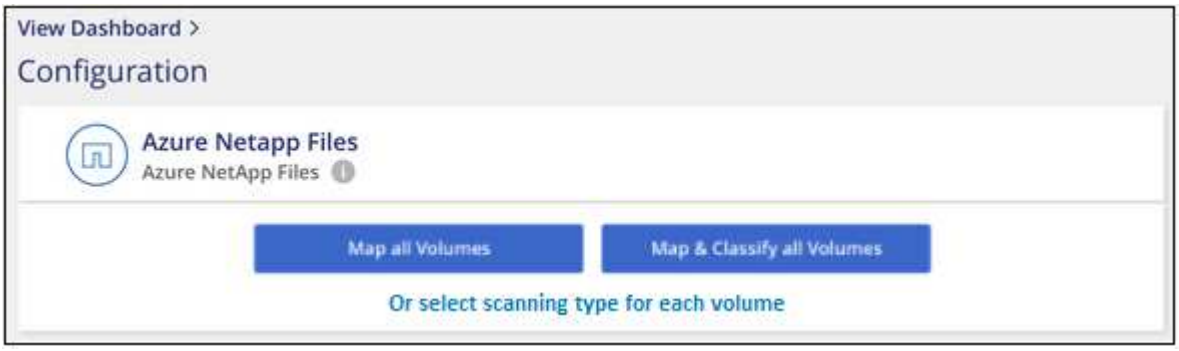
- 참고: * Azure NetApp Files 볼륨을 스캔할 때는 현재 사내 위치에 BlueXP 분류 배포를 지원하지 않습니다.

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.

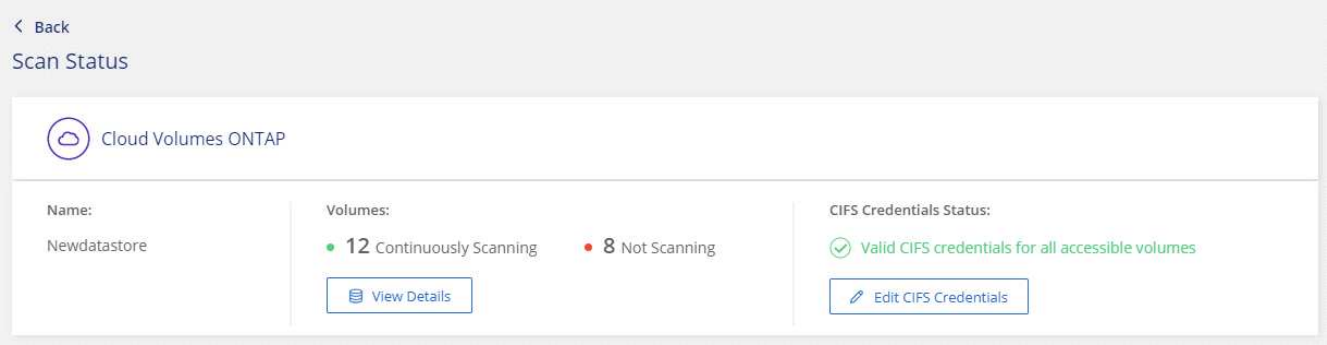
   

   b. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 BlueXP 분류에서 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

   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.

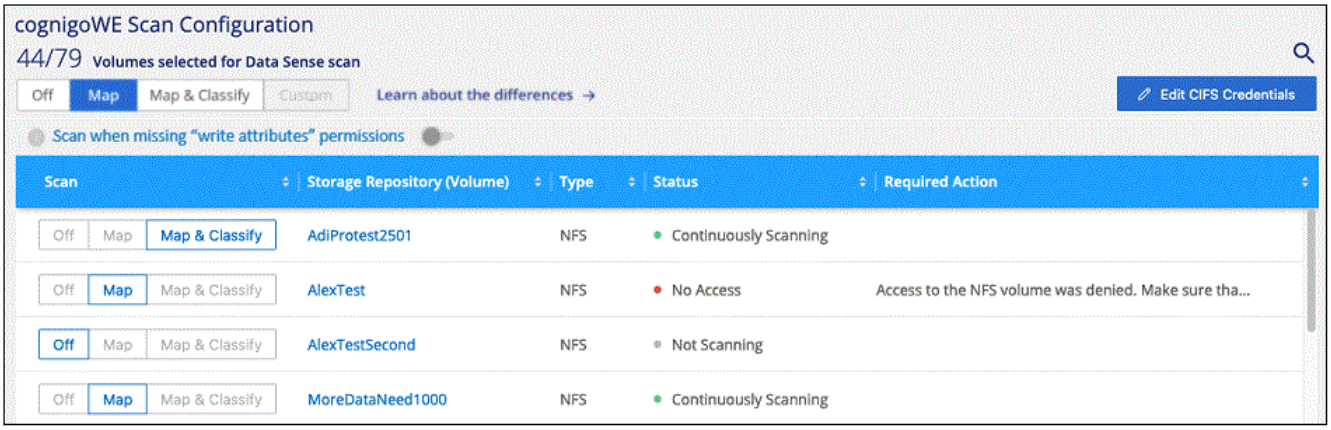
BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 CIFS에서 쓰기 속성 사용 권한 또는 NFS에서 쓰기 권한이 사용자에게 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

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.

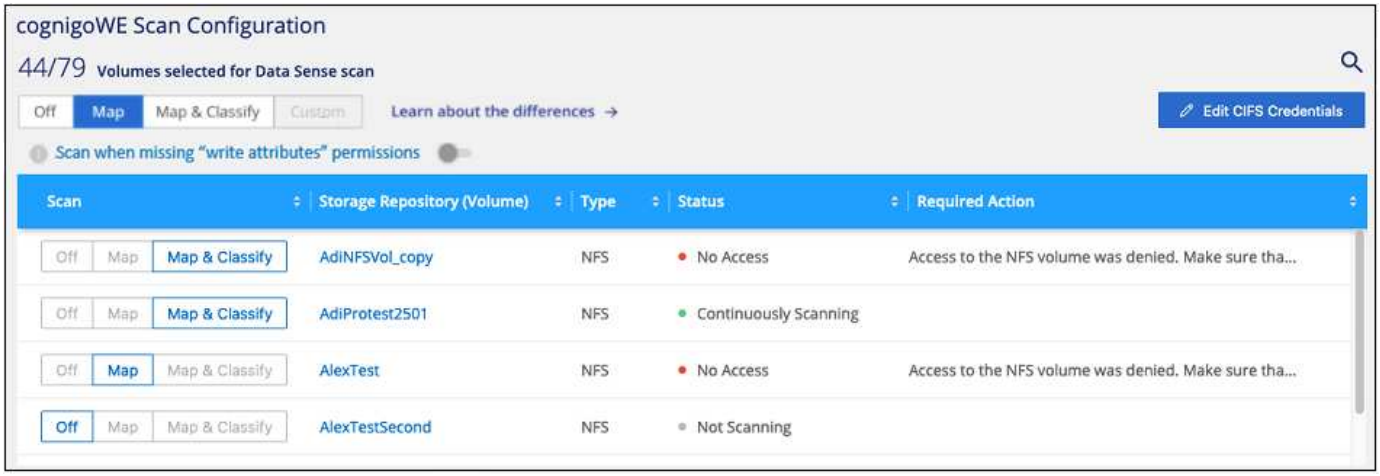
   예를 들어 다음 이미지는 네 개의 볼륨을 보여 줍니다. 그 중 하나는 BlueXP 분류 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 BlueXP 분류에서 스캔할 수 없는 볼륨입니다.



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.

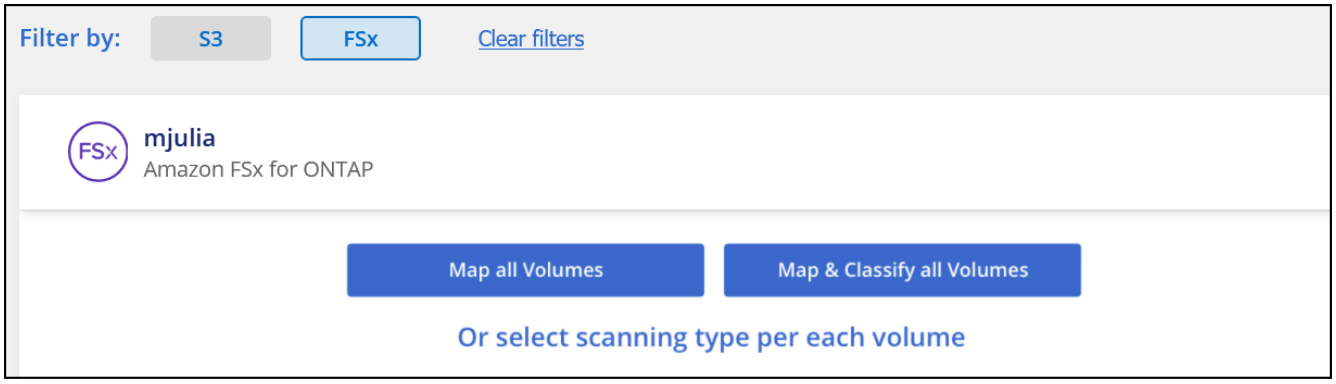
- 참고: * FSx 볼륨을 스캔할 때는 현재 온-프레미스 위치에서 BlueXP 분류 배포를 지원하지 않습니다.

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.

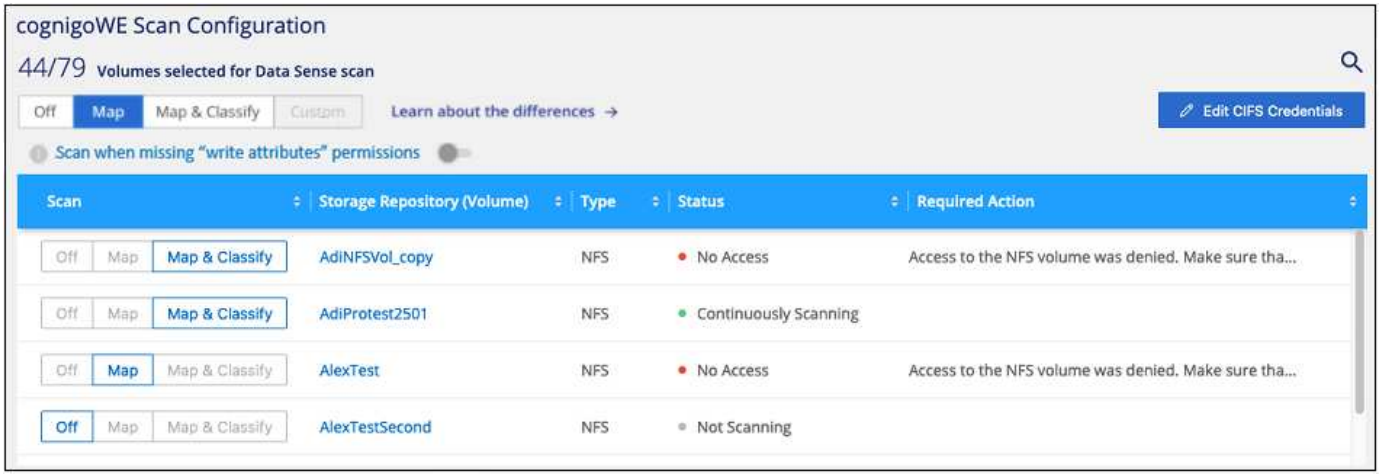
      BlueXP 분류 검사에서 파일 "마지막 액세스 시간"이 변경되지 않도록 하려면 CIFS에서 쓰기 속성 사용 권한 또는 NFS에서 쓰기 권한이 사용자에게 있는 것이 좋습니다. 가능하면 Active Directory 구성 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹에 구성하는 것이 좋습니다.

   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".



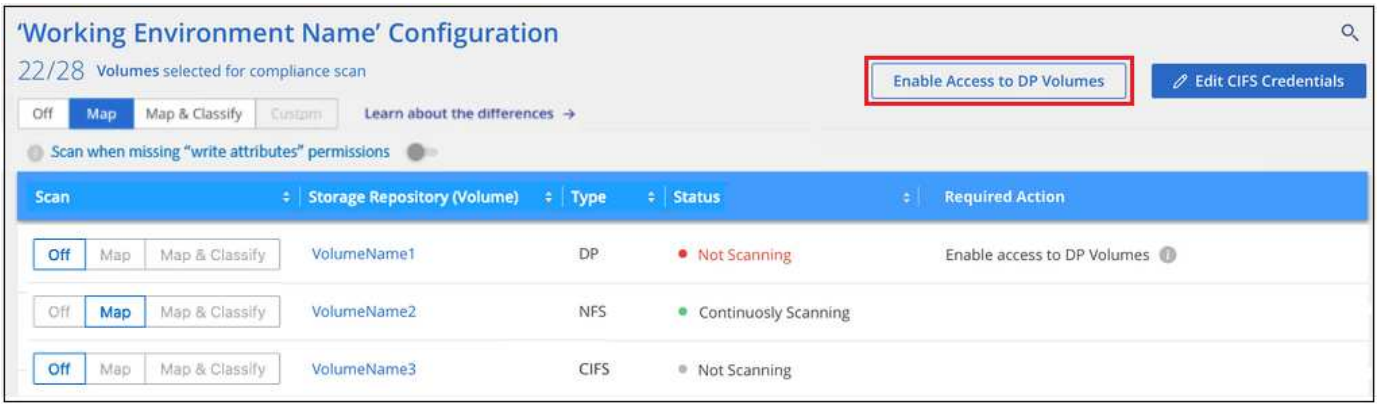
대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다
볼륨에서 스캔을 비활성화합니다	볼륨 영역에서 * Off * 를 클릭합니다
모든 볼륨에서 매핑 전용 스캔을 활성화합니다	제목 영역에서 * Map * 을 클릭합니다
모든 볼륨에서 전체 스캔을 활성화합니다	제목 영역에서 * 지도 및 분류 * 를 클릭합니다
모든 볼륨에서 스캔을 비활성화합니다	제목 영역에서 * Off * 를 클릭합니다

> 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.

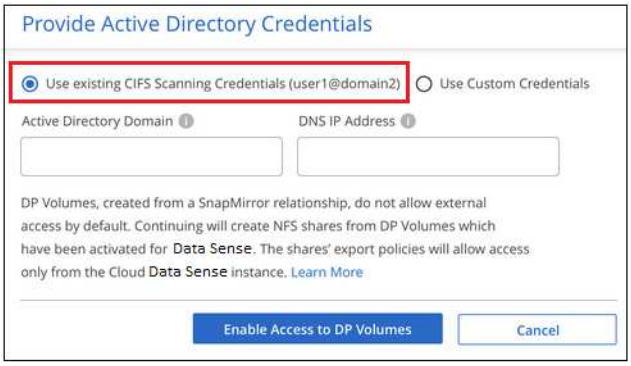
처음에 볼륨 목록은 이러한 볼륨을 *Type** DP*로 식별하며 *Status** Not Scanning* 및 *Required Action** DP 볼륨에 대한 액세스 사용*.

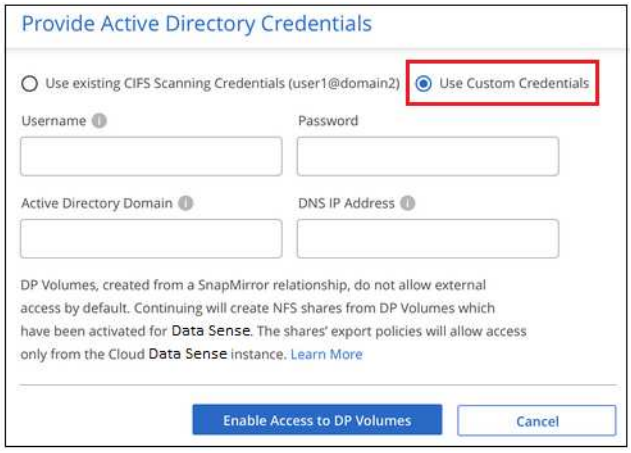


단계

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.

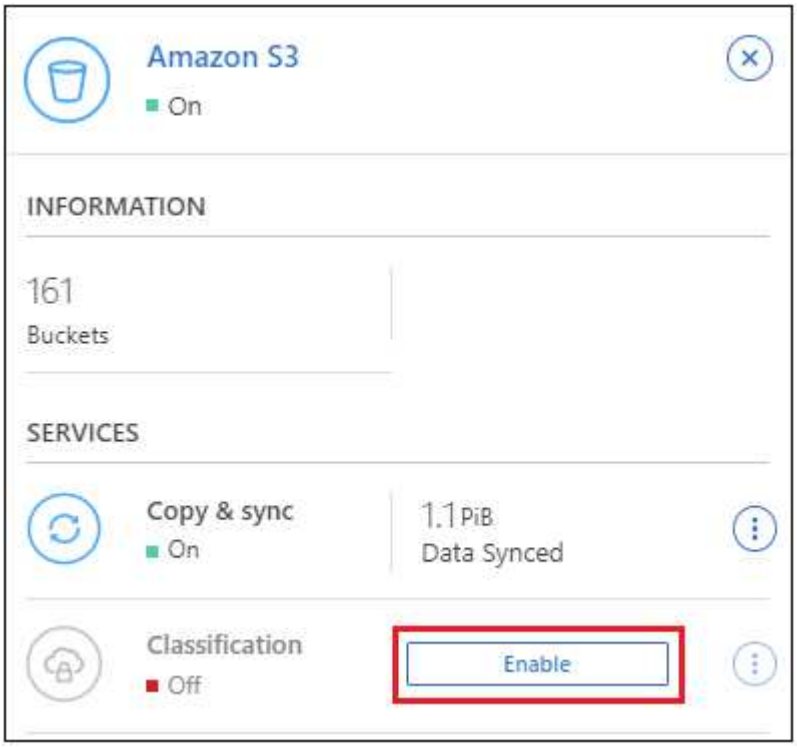
S3 작업 환경에서 **BlueXP** 분류 활성화

사전 요구 사항을 확인한 후 Amazon S3에서 BlueXP 분류를 활성화합니다.

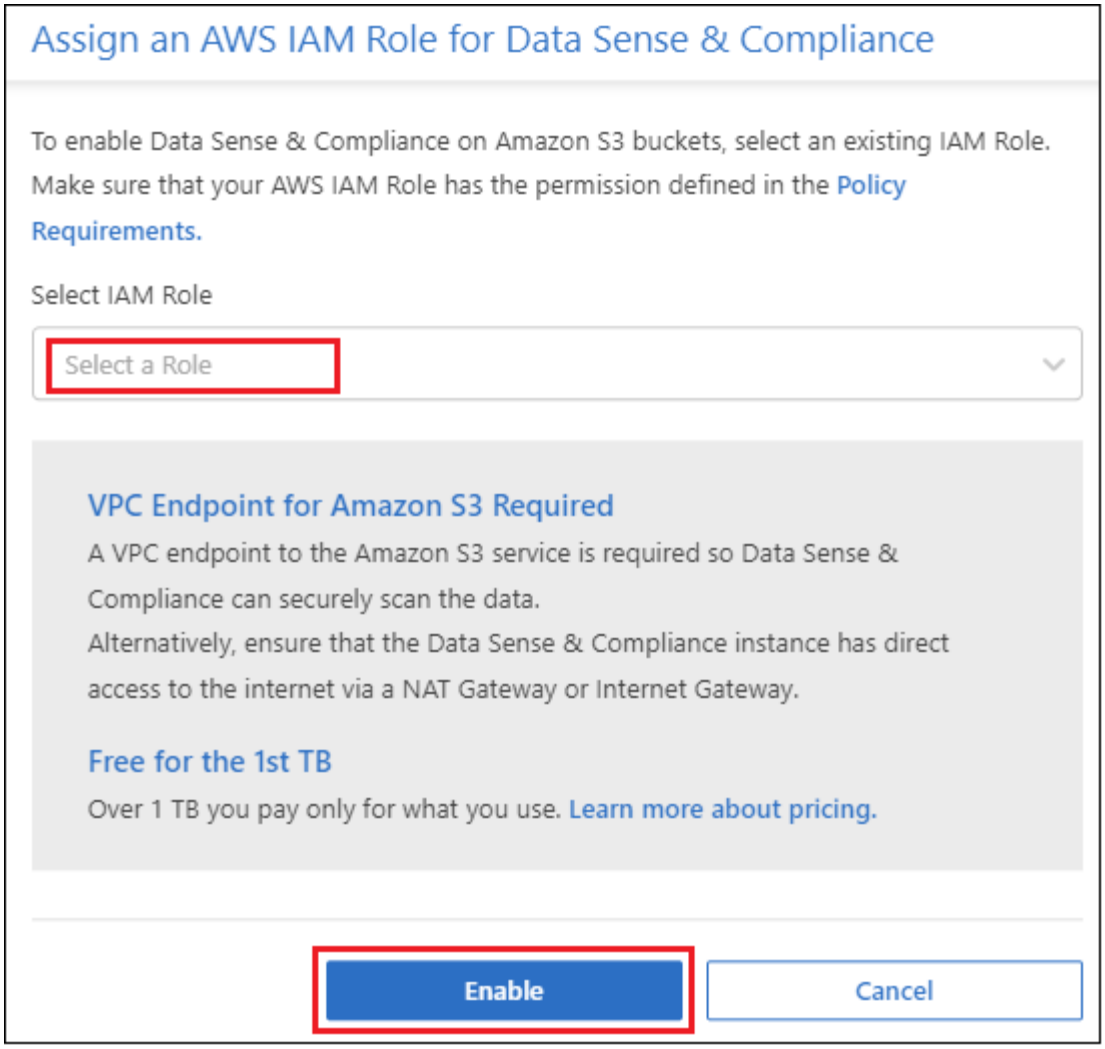
단계

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

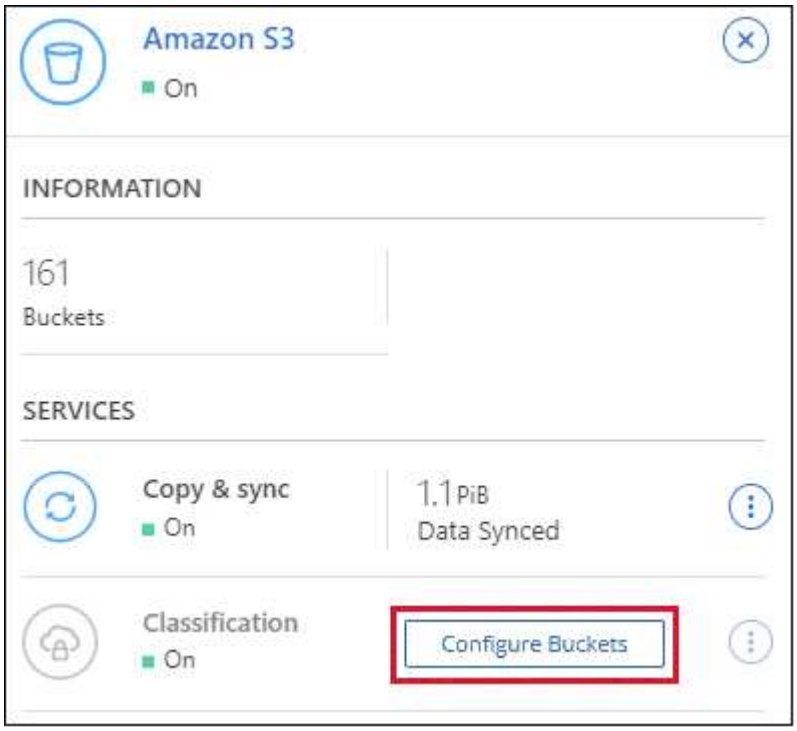
BlueXP에서 Amazon S3에서 BlueXP 분류를 사용하도록 설정한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다.

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

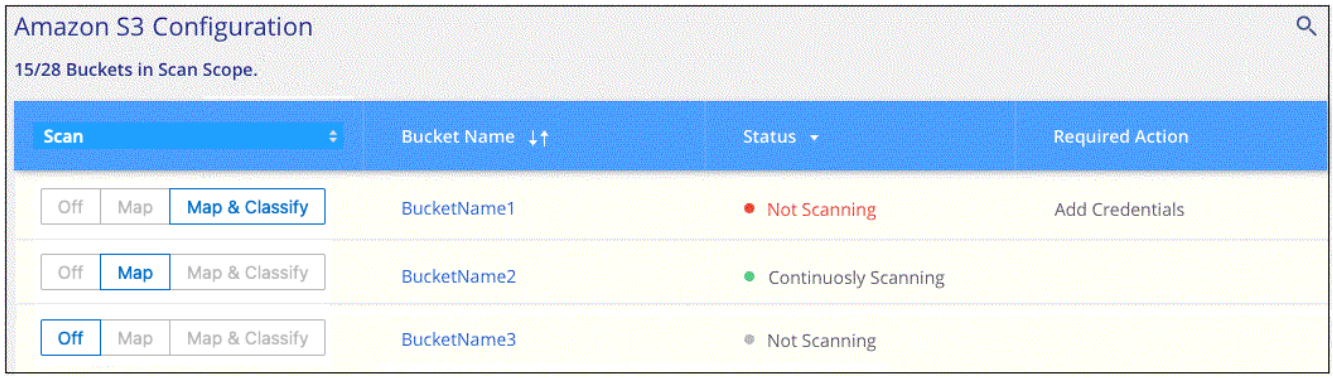
BlueXP 분류도 가능합니다 서로 다른 AWS 계정에 있는 S3 버킷을 스캔합니다.

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

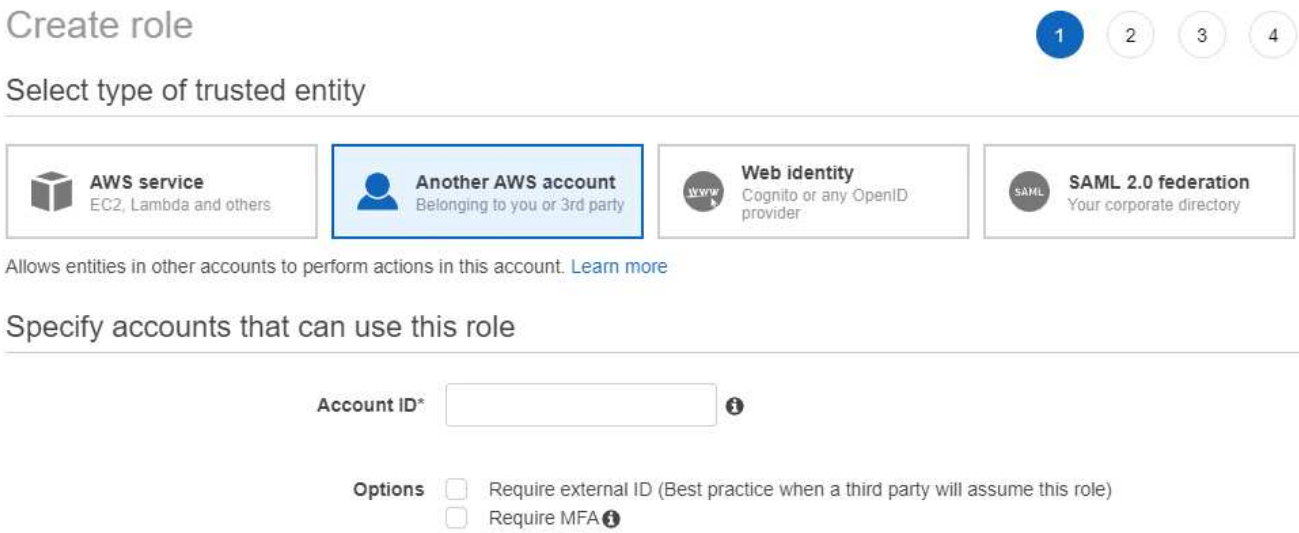
BlueXP 분류는 활성화한 S3 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

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.

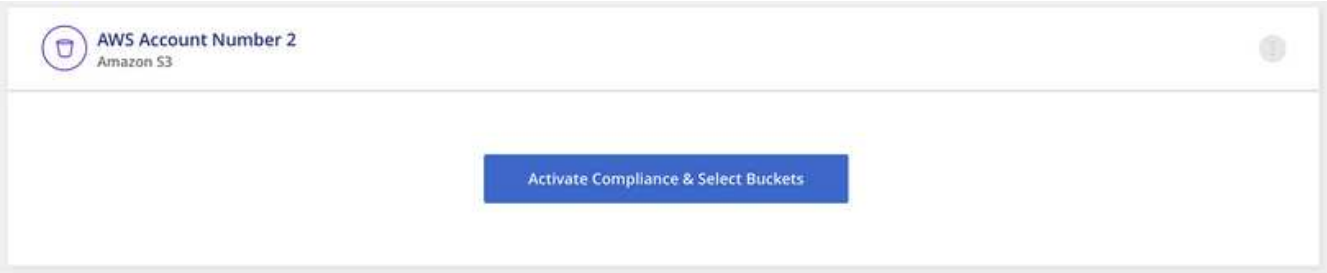
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

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".

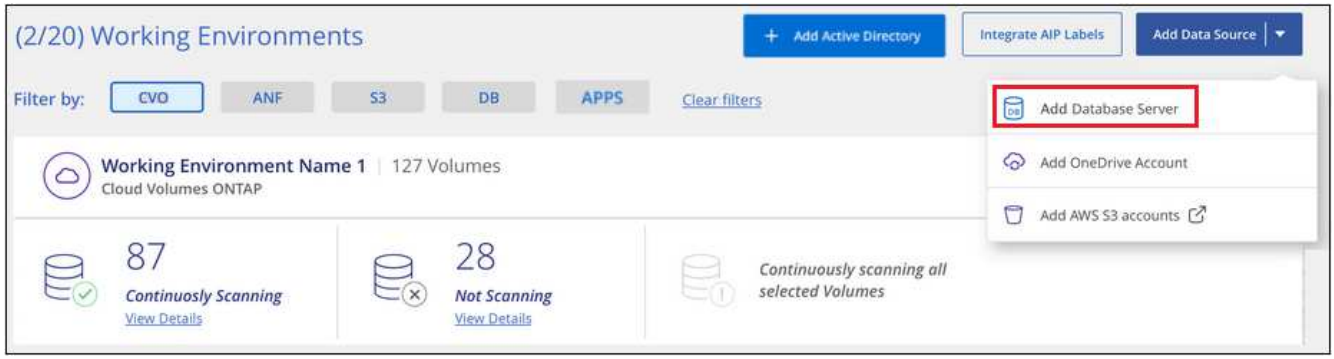
인터넷에 액세스할 수 없는 어두운 사이트에 설치된 데이터베이스 스키마를 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 BlueXP 분류를 배포합니다". 또한 BlueXP Connector를 동일한 사내 위치에 배포해야 합니다.

인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

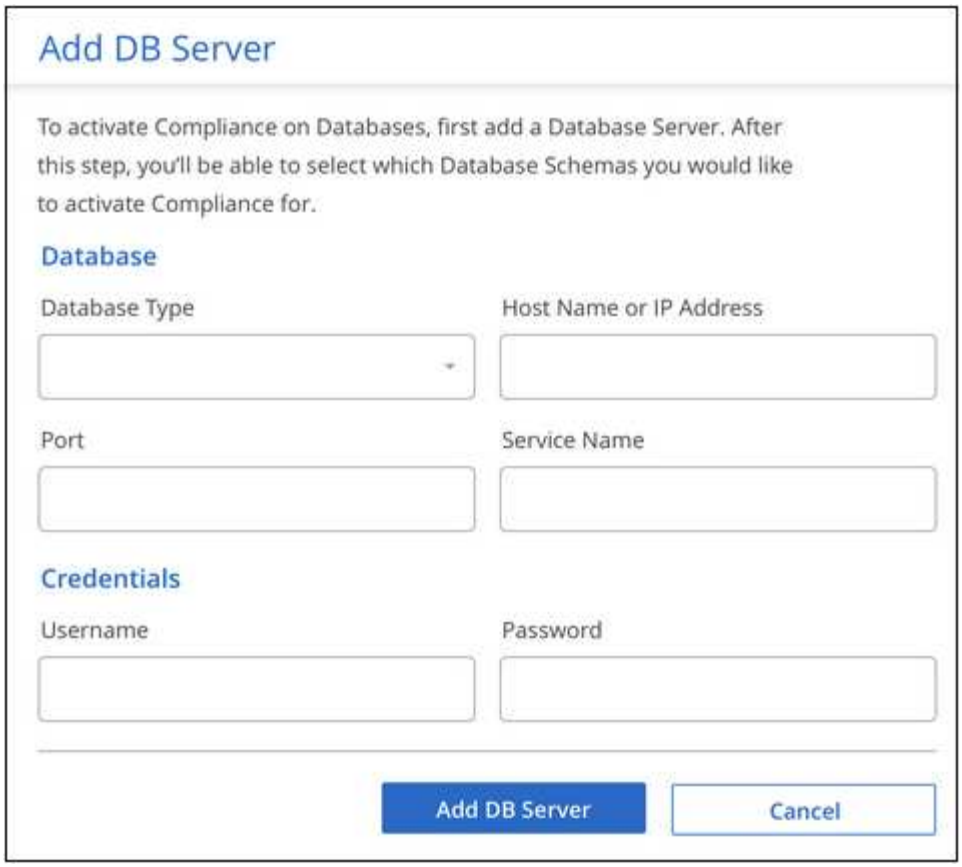
데이터베이스 서버를 추가합니다

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.

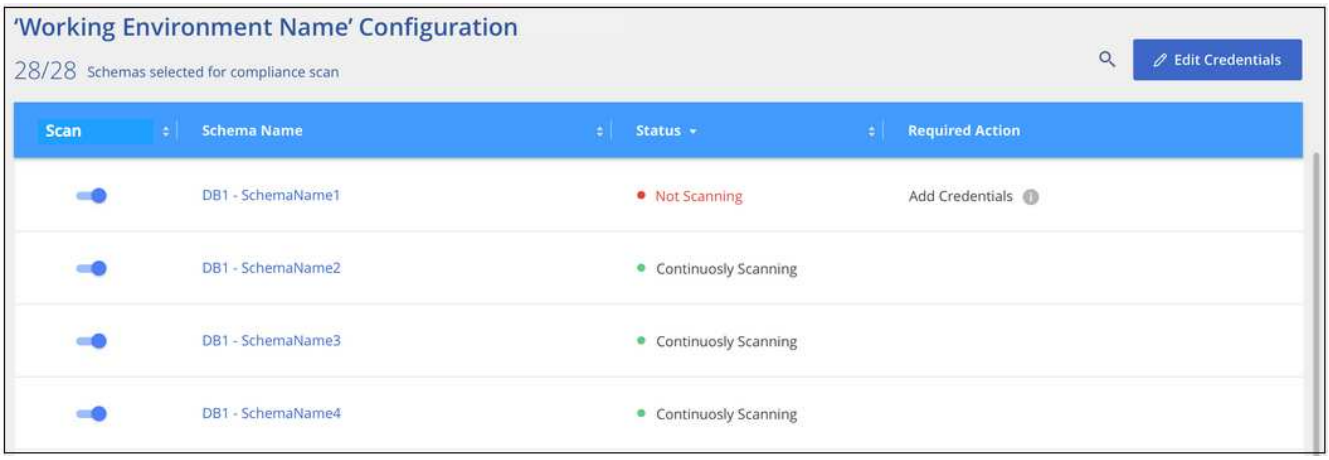
데이터베이스 스키마에서 규정 준수 검사를 활성화 및 비활성화합니다

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".

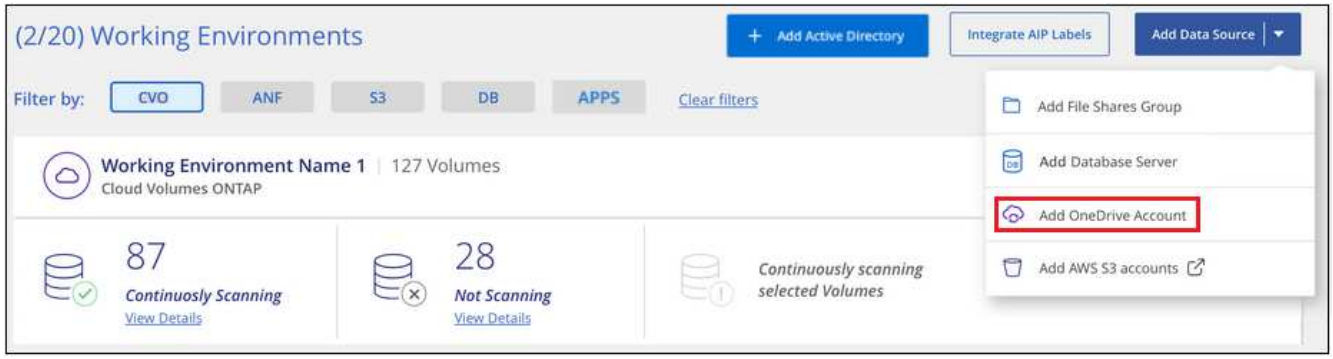
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

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.

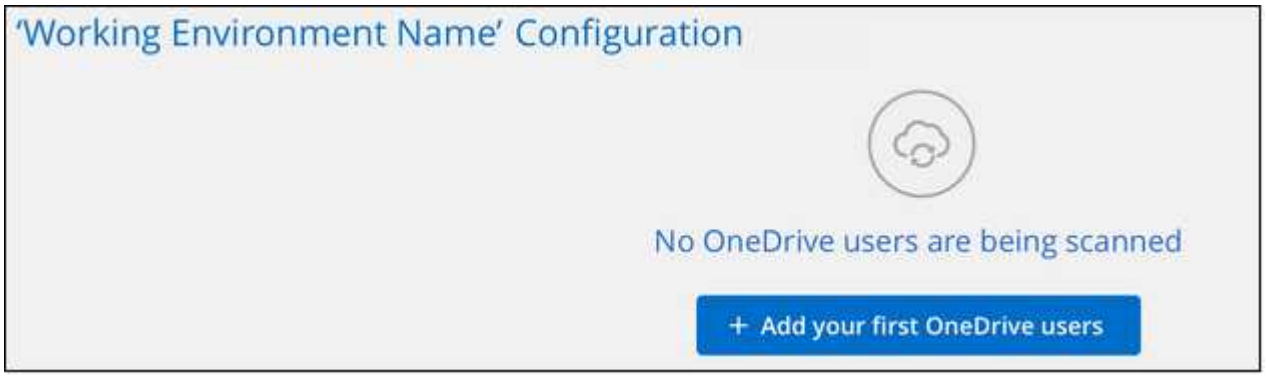
규정 준수 검사에 OneDrive 사용자 추가

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

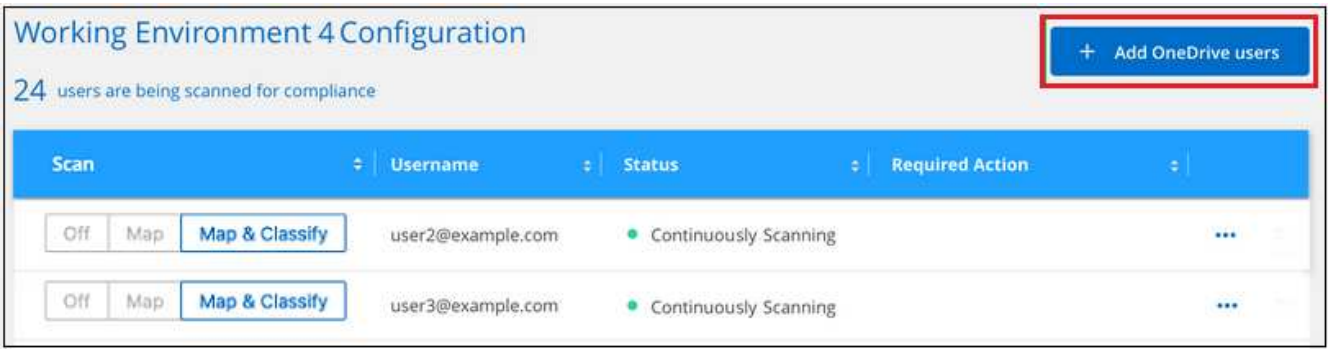
단계

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

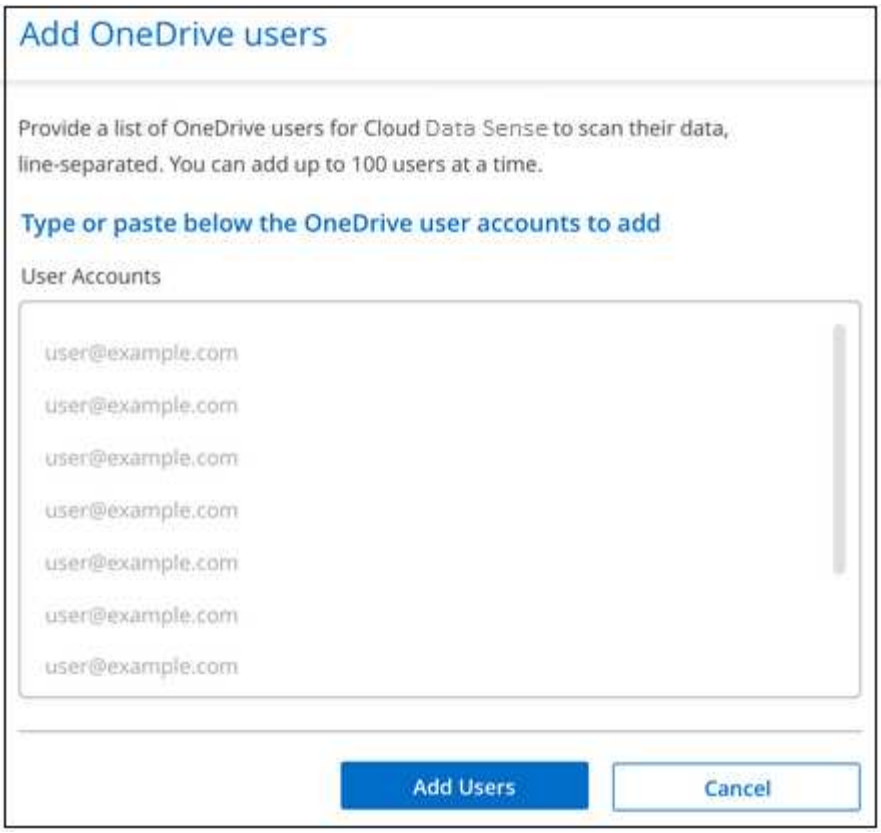
2. 이 OneDrive 계정에 사용자를 처음으로 추가하는 경우 * 첫 번째 OneDrive 사용자 추가 * 를 클릭합니다.



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.

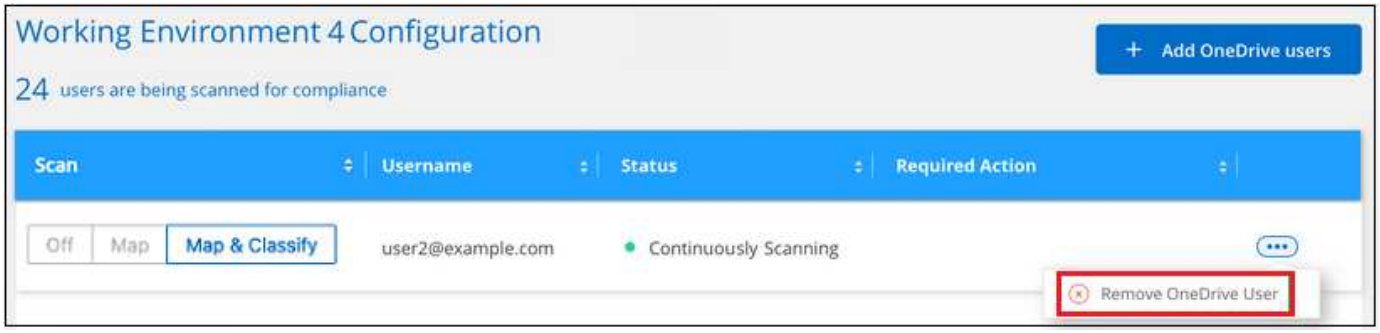
대상:	방법은 다음과 같습니다.
사용자 파일에 대한 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
사용자 파일에 대한 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
사용자 파일 스캔을 비활성화합니다	Off * 를 클릭합니다

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".

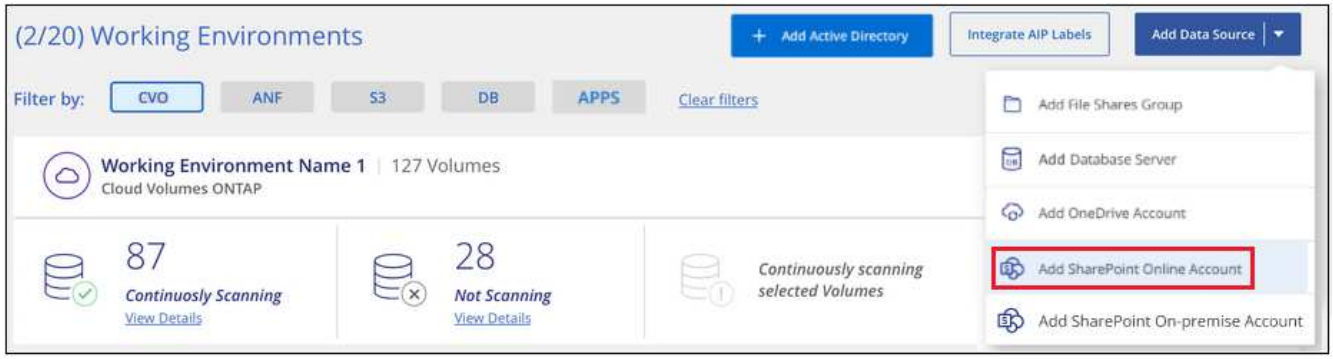
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

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.

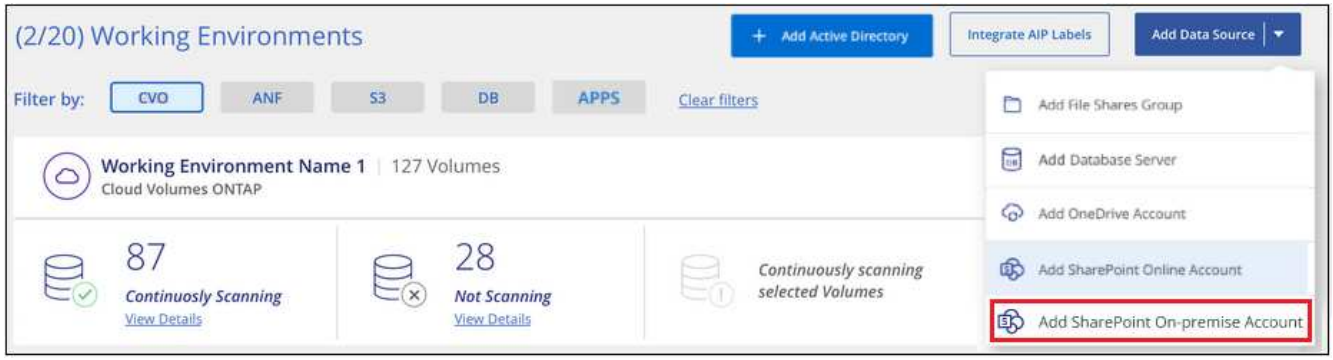
SharePoint Online 계정이 작업 환경 목록에 추가됩니다.

SharePoint 온-프레미스 계정 추가

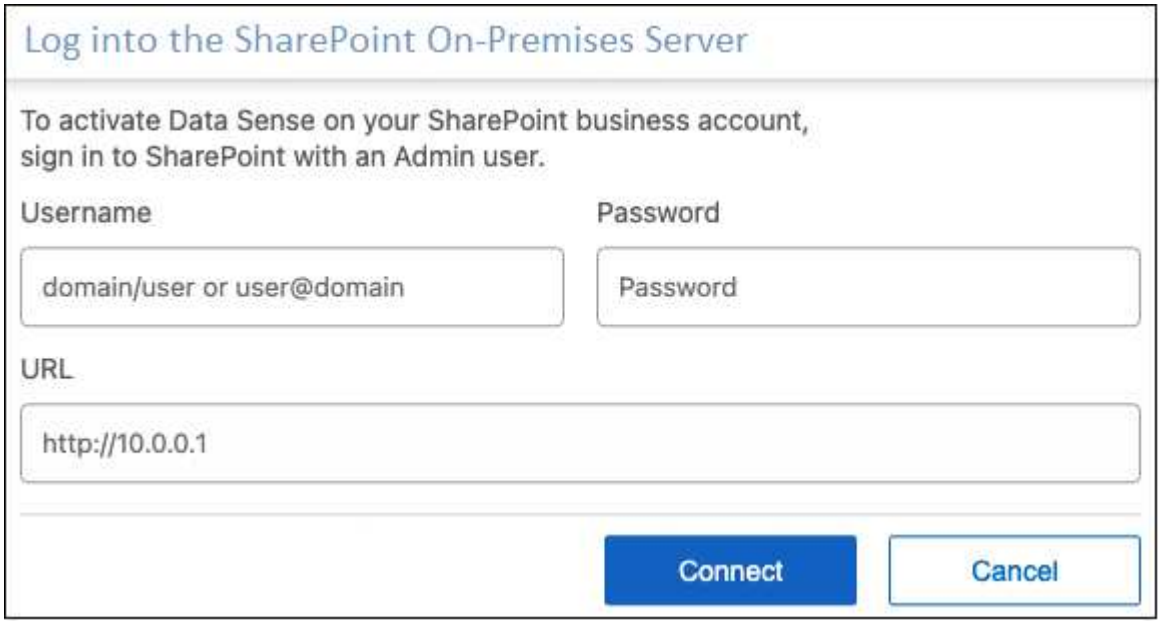
사용자 파일이 있는 SharePoint 온-프레미스 계정을 추가합니다.

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.

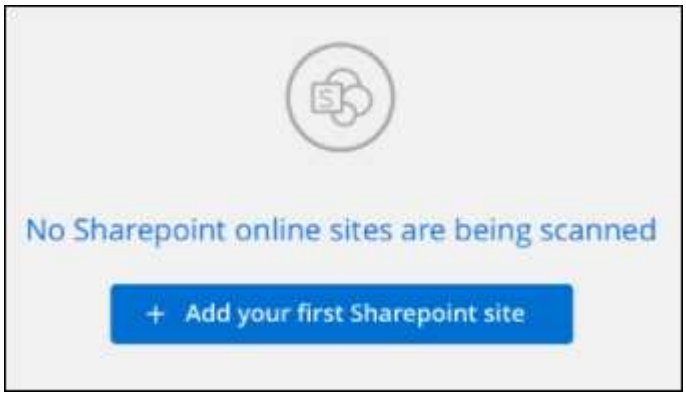
규정 준수 검사에 **SharePoint** 사이트 추가

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

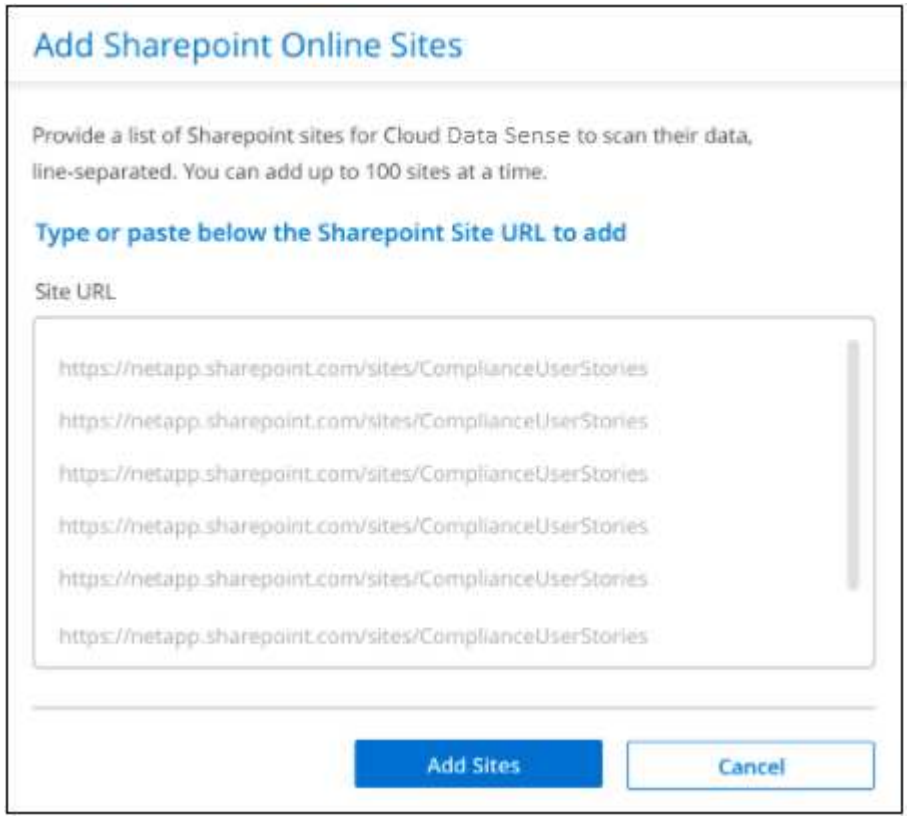
1. Configuration_ 페이지에서 SharePoint 계정의 * Configuration * 버튼을 클릭합니다.

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.

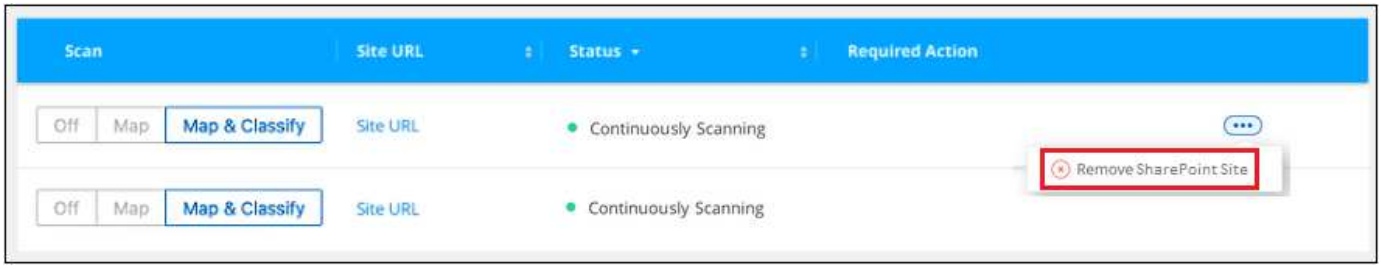
대상:	방법은 다음과 같습니다.
파일에서 매핑 전용 스캔을 활성화합니다	Map * 을 클릭합니다
파일에 대한 전체 스캔을 활성화합니다	지도 및 분류 * 를 클릭합니다
파일 스캔을 비활성화합니다	Off * 를 클릭합니다

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".

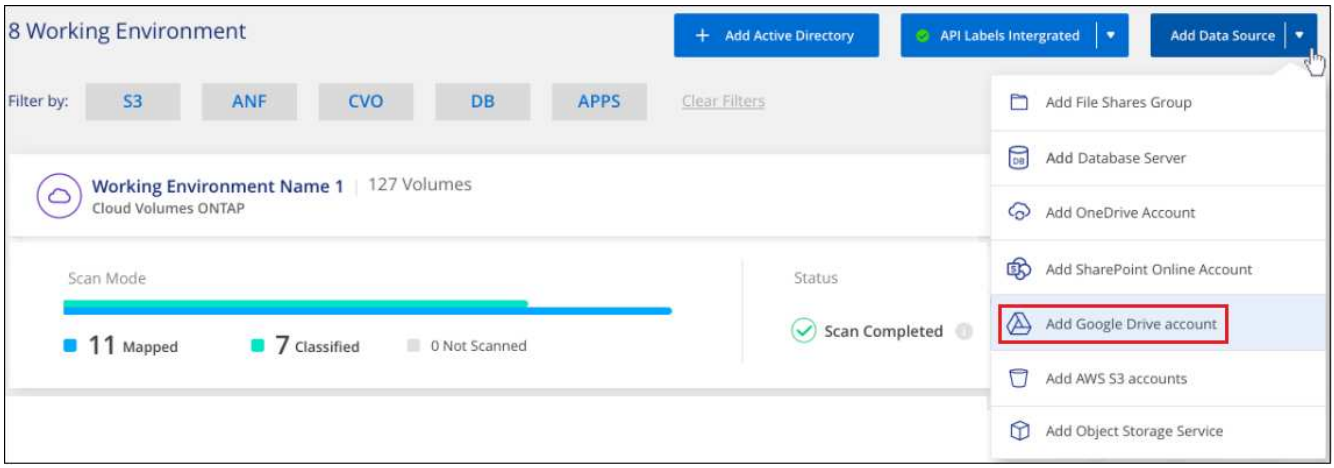
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

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.

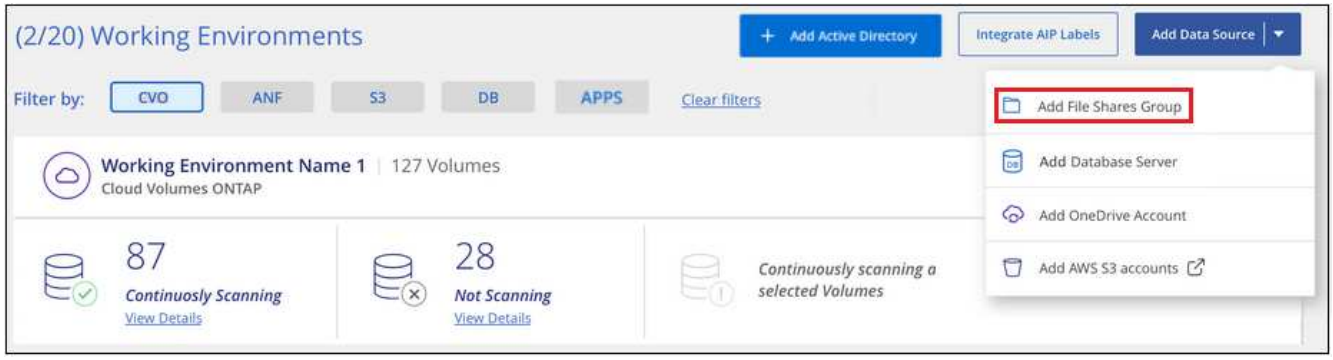
파일 공유에 대한 그룹을 생성하는 중입니다

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>`.

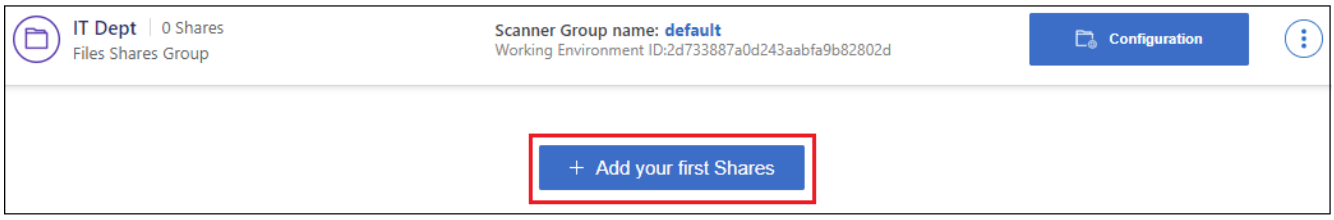
개별 파일 공유를 추가하거나 스캔할 파일 공유의 줄별 목록을 제공할 수 있습니다. 한 번에 최대 100개의 공유를 추가할 수 있습니다.

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.

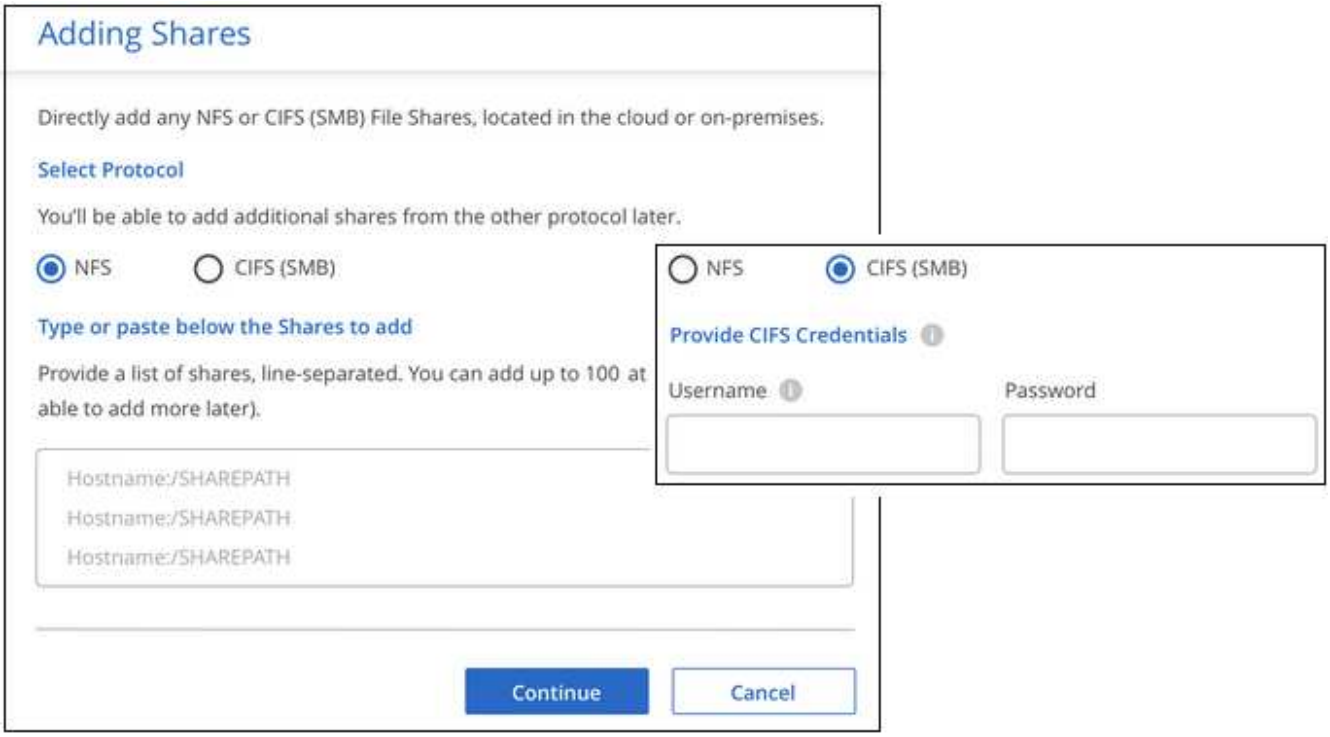
2. 이 파일 공유 그룹에 대한 파일 공유를 처음으로 추가하는 경우 * 첫 번째 공유 추가 * 를 클릭합니다.



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

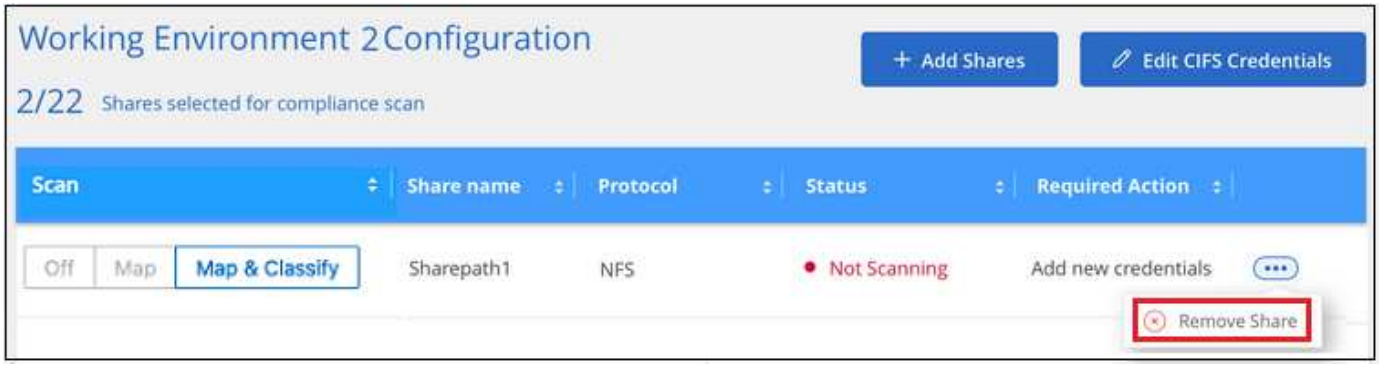
페이지 상단의 * "쓰기 속성" 권한 * 이 누락된 경우 * 스캔 에 대한 스위치는 기본적으로 비활성화되어 있습니다. 즉, BlueXP 분류에 CIFS의 쓰기 속성 권한이나 NFS의 쓰기 권한이 없는 경우 BlueXP 분류는 "마지막 액세스 시간"을 원래 타임 스탬프로 되돌릴 수 없기 때문에 시스템에서 파일을 검색하지 않습니다. 마지막 액세스 시간이 재설정되는 것을 염려하지 않을 경우, 스위치를 켜면 사용 권한에 관계없이 모든 파일이 스캔됩니다. "자세한 정보".

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.

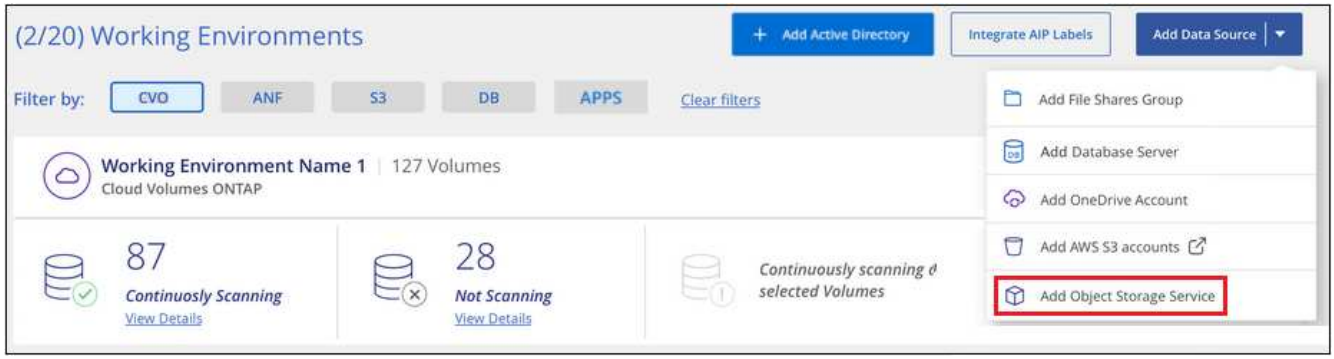
인스턴스가 인터넷에 연결되어 있는 경우 BlueXP 분류 소프트웨어로의 업그레이드가 자동화됩니다.

BlueXP 분류에 오브젝트 스토리지 서비스 추가

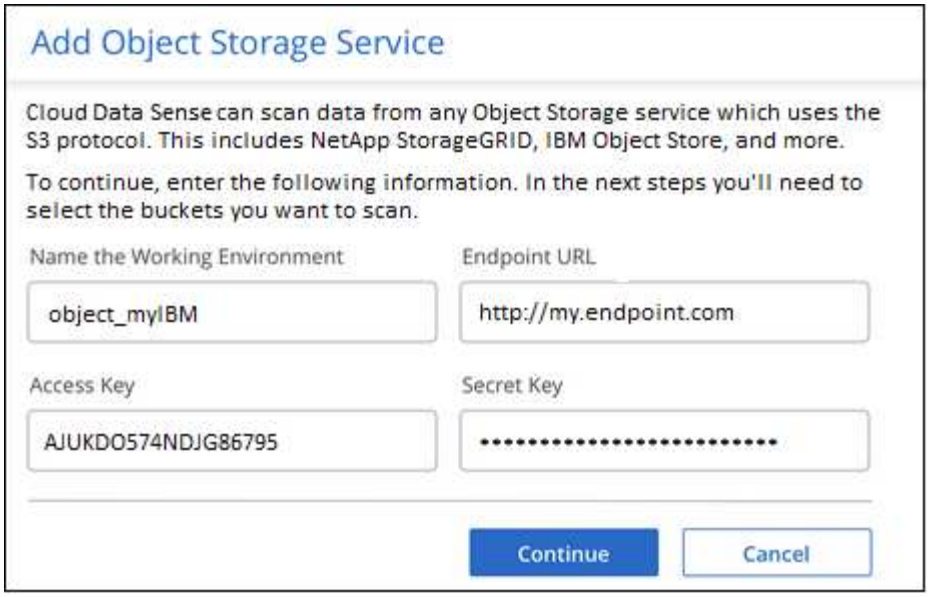
오브젝트 스토리지 서비스를 추가합니다.

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

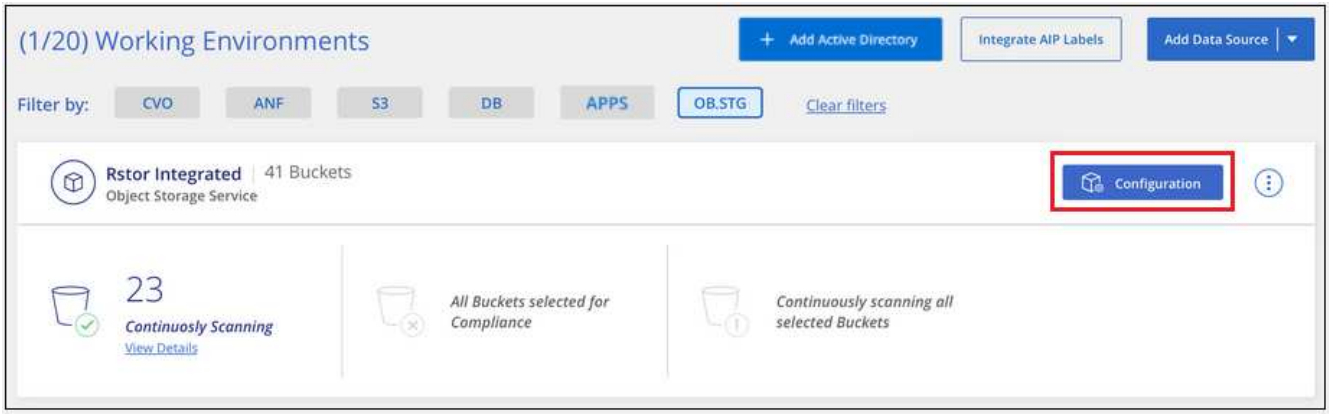
새로운 오브젝트 스토리지 서비스가 작업 환경 목록에 추가됩니다.

오브젝트 스토리지 버킷에 대한 규정 준수 검사 설정 및 해제

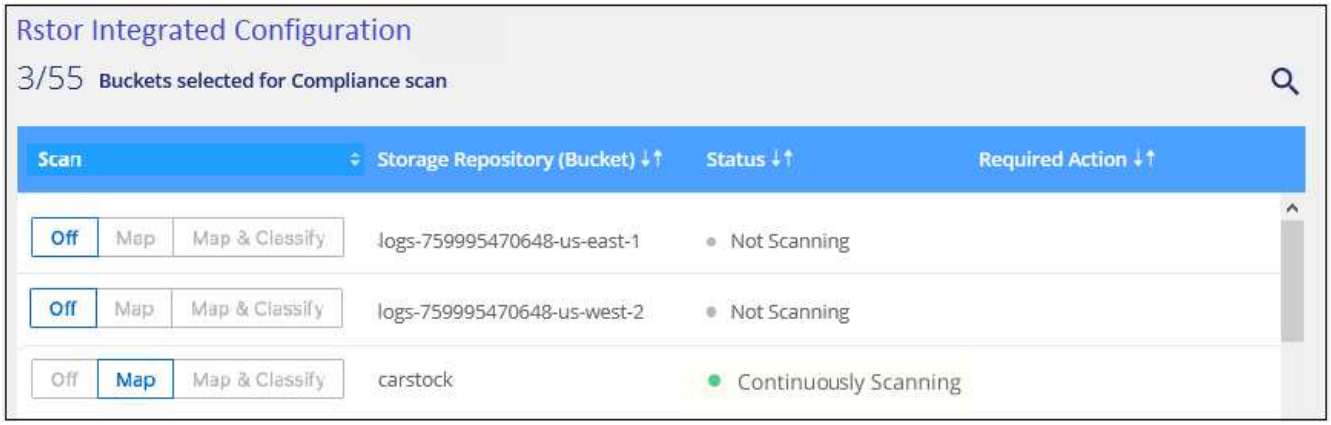
오브젝트 스토리지 서비스에서 BlueXP 분류를 활성화한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다. BlueXP 분류는 이러한 버킷을 검색하여 사용자가 만든 작업 환경에 표시합니다.

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

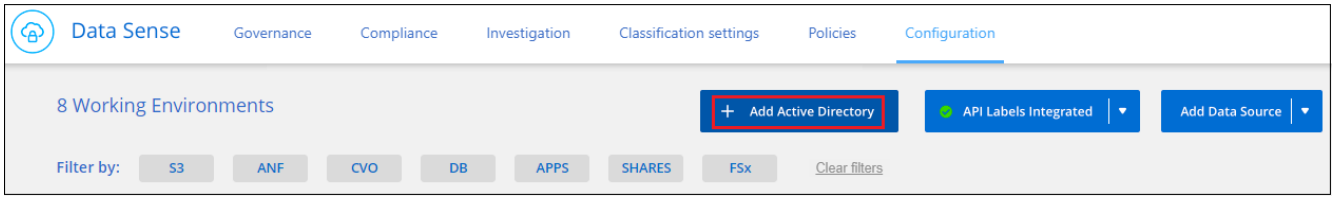
  LDAP 서버 IP 주소 또는 여러 IP 주소

  - 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

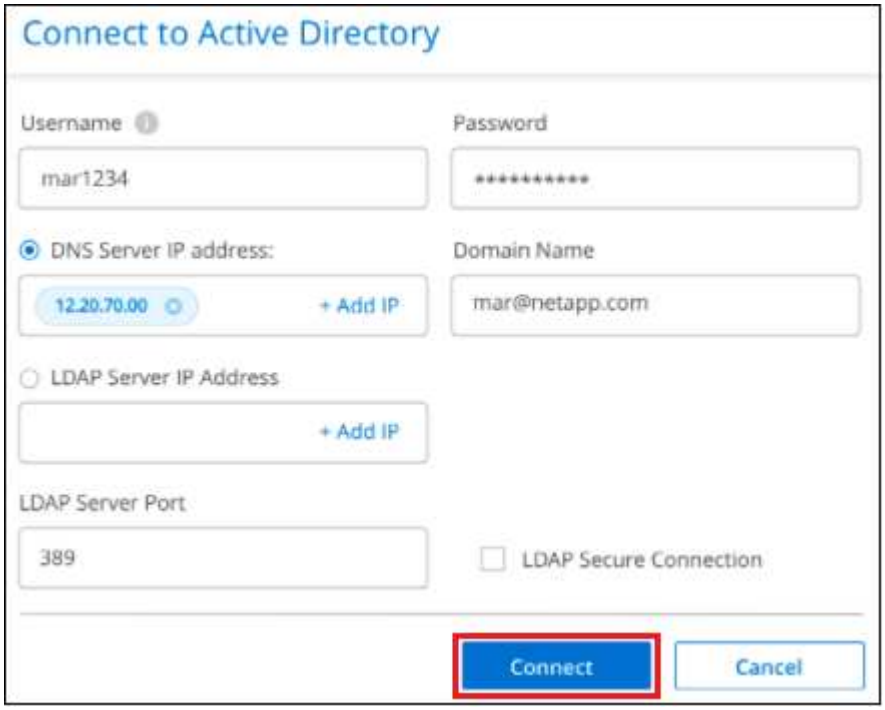
단계

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

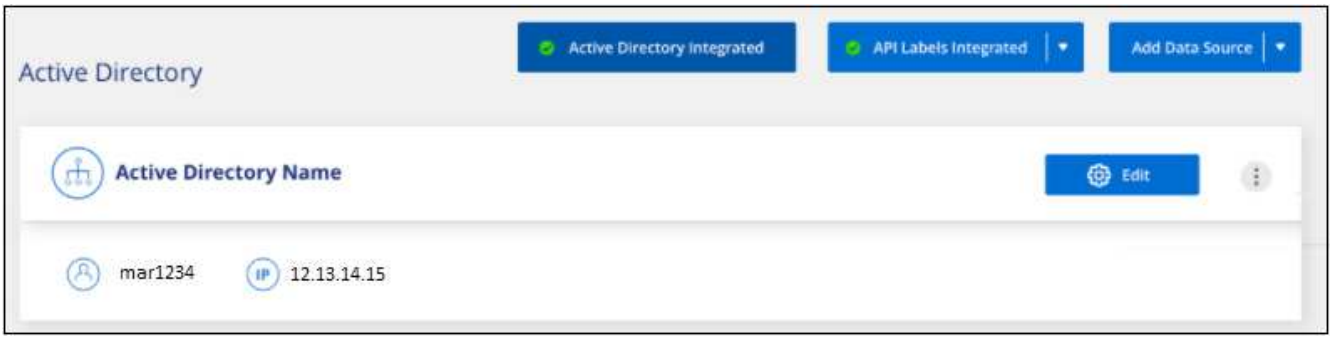


2. Active Directory에 연결 대화 상자에서 Active Directory 세부 정보를 입력하고 * Connect * 를 클릭합니다.

   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.

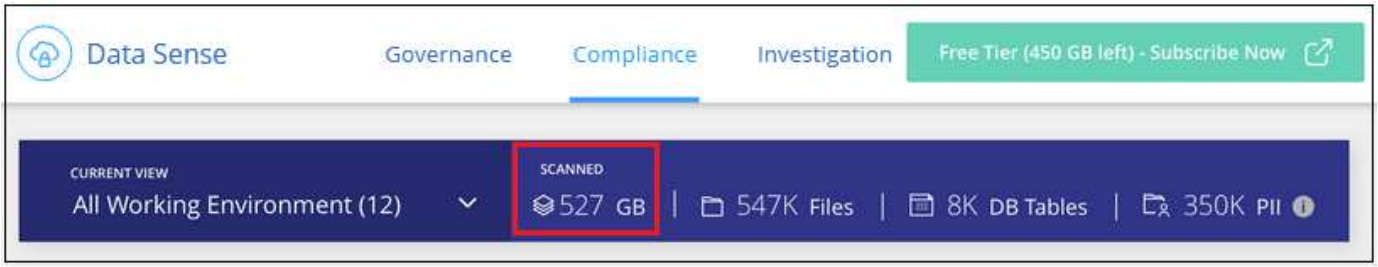
- 클라우드 공급자의 마켓플레이스에서 이미 BlueXP PAYGO(pay-as-you-go) 구독을 신청했다면 BlueXP 분류에도 자동으로 가입됩니다. 다시 가입하지 않아도 됩니다.
- BlueXP 분류(데이터 감지) BYOL(Bring-Your-Own-License)은 작업 공간의 모든 작업 환경과 데이터 소스에서 스캔할 수 있는 _floating_license입니다. BlueXP 디지털 지갑에 활성 구독이 표시됩니다.
- 스캔되는 데이터의 양은 스토리지 효율성 없이 논리적 파일 크기를 기준으로 계산됩니다.

"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

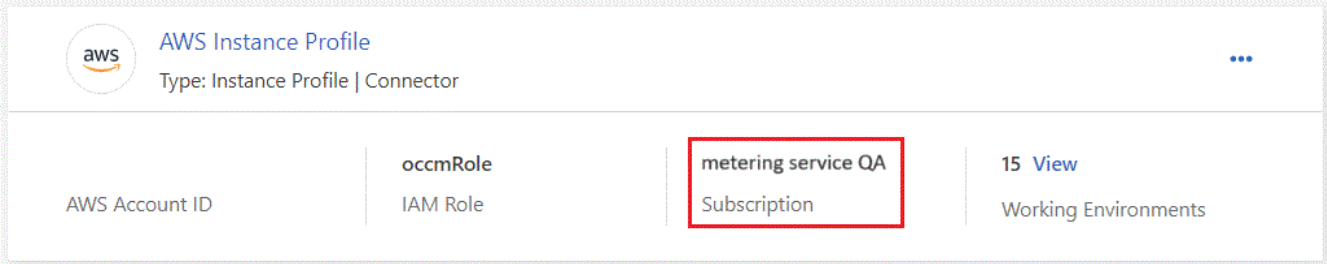
이러한 단계는 _ 계정 관리자 _ 역할을 가진 사용자가 완료해야 합니다.

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

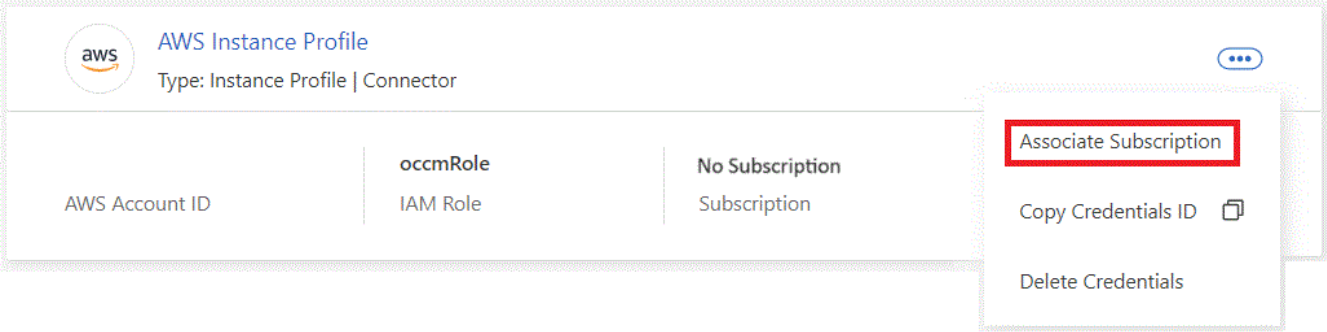
2. 자격 증명 * 을 클릭한 다음 AWS 인스턴스 프로필, Azure Managed Service Identity 또는 Google Project에 대한 자격 증명을 찾습니다.

   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.

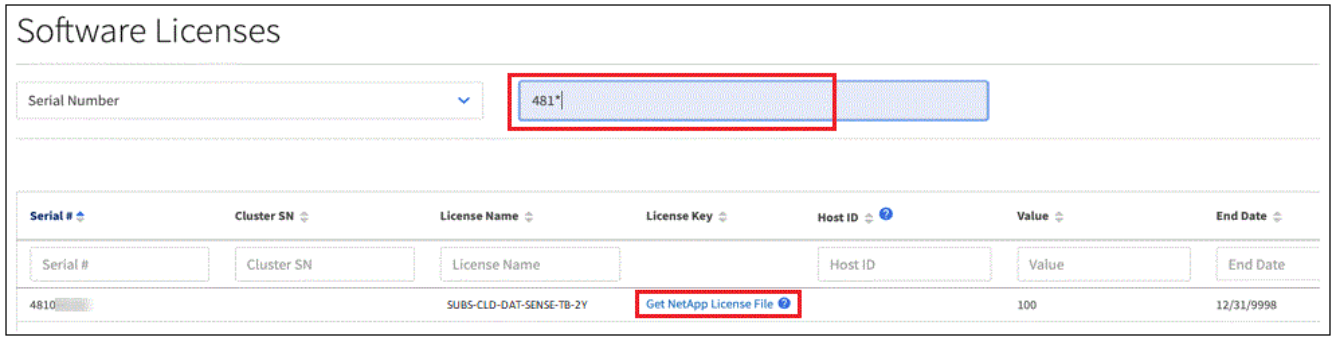
- BlueXP 계정 ID

  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-

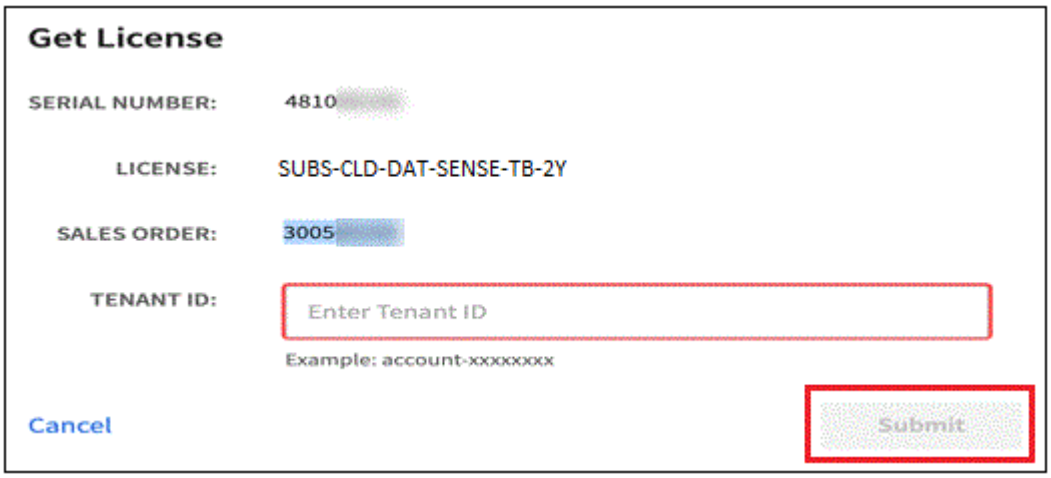
DARKSITE1 * 을 사용하십시오.

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

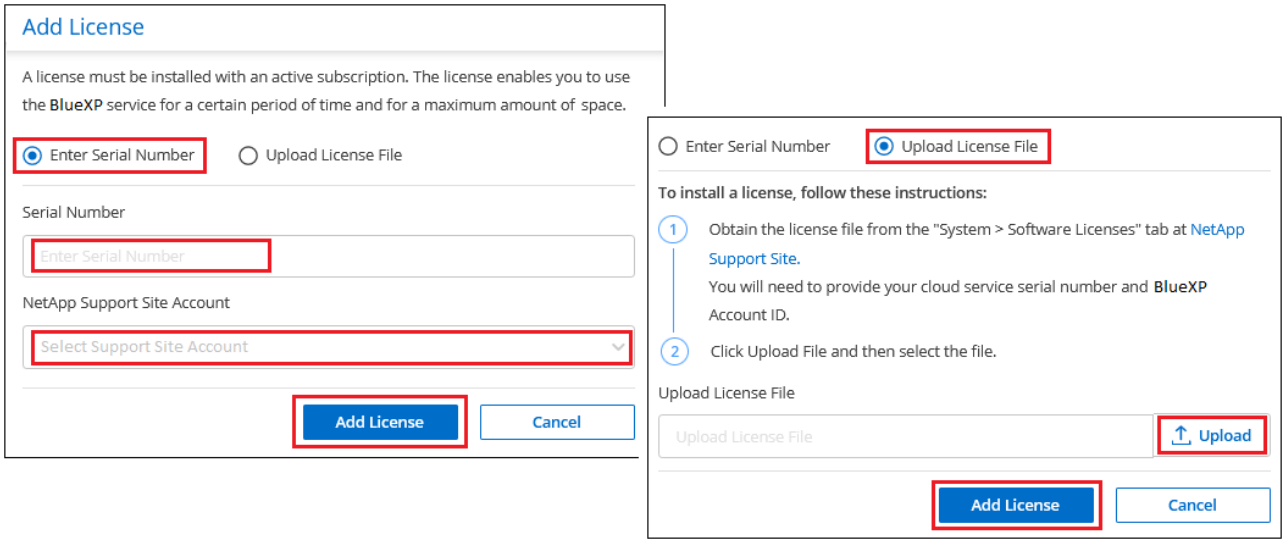
BlueXP 계정에 대한 BlueXP 분류(데이터 감지) 라이센스를 구입한 후 BlueXP 분류 서비스를 사용하려면 BlueXP에 라이센스를 추가해야 합니다.

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.



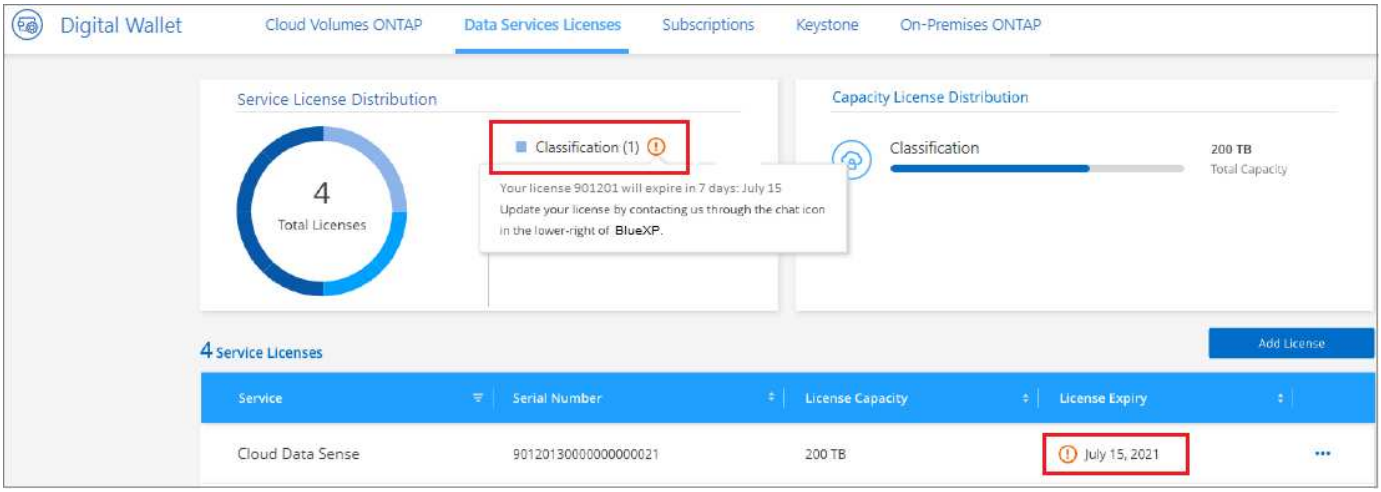
결과

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.