



## 시작하십시오 Cloud Data Sense

NetApp  
April 18, 2022

This PDF was generated from <https://docs.netapp.com/ko-kr/cloud-manager-data-sense/concept-cloud-compliance.html> on April 18, 2022. Always check docs.netapp.com for the latest.

# 목차

시작하십시오 .....	1
클라우드 데이터 센스에 대해 알아보십시오 .....	1
클라우드 데이터 센스를 구축하십시오 .....	7
데이터 소스에서 스캔을 활성화합니다 .....	25
Active Directory를 클라우드 데이터 센스에 통합합니다 .....	62
클라우드 데이터 센스에 대한 라이선스 설정 .....	65
클라우드 데이터 센스에 관한 FAQ .....	71

# 시작하십시오

## 클라우드 데이터 센스에 대해 알아보십시오

Cloud Data Sense는 Cloud Manager를 위한 데이터 거버넌스 서비스로, 회사의 사내 및 클라우드 데이터 소스와 작업 환경을 검사하여 데이터를 매핑 및 분류하고 프라이빗 정보를 식별합니다. 따라서 보안 및 규정 준수 위험을 줄이고 스토리지 비용을 절감하며 데이터 마이그레이션 프로젝트를 지원할 수 있습니다.

["클라우드 데이터 센스의 사용 사례에 대해 알아보십시오"](#).

### 피처

Cloud Data Sense는 규정 준수 작업에 도움이 되는 여러 가지 도구를 제공합니다. 데이터 센스를 사용하여 다음을 수행할 수 있습니다.

- 개인 식별 정보(PII) 식별
- GDPR, CCPA, PCI 및 HIPAA 개인 정보 보호 규정에서 요구하는 광범위한 중요 정보를 식별합니다
- Data Subject Access Request(SAR)에 응답
- 파일에 특정 PII가 포함된 경우 이메일을 통해 Cloud Manager 사용자에게 알립니다(을 사용하여 이 기준을 정의합니다 ["정책"](#))
- 보고 수정합니다 ["AIP\(Azure Information Protection\) 레이블"](#) 파일을 선택합니다
- 파일에 사용자 지정 태그(예: "이동해야 함")를 추가하고 Cloud Manager 사용자를 할당하여 사용자가 파일에 대한 업데이트를 소유할 수 있도록 합니다
- 파일 복사, 이동, 삭제

Cloud Data Sense는 거버넌스 작업에 도움이 되는 툴도 제공합니다. 클라우드 데이터 센스를 사용하여 다음을 수행할 수 있습니다.

- 오래된 데이터, 비업무용 데이터, 중복 파일, 열린 권한이 있는 파일 및 시스템의 대용량 파일을 식별합니다.

이 정보를 사용하여 일부 파일을 보다 저렴한 오브젝트 스토리지로 이동, 삭제 또는 계층화할 것인지 결정할 수 있습니다.

- 데이터를 이동하기 전에 데이터의 크기와 데이터에 중요한 정보가 포함되어 있는지 여부를 확인합니다.

이 기능은 데이터를 사내 위치에서 클라우드로 마이그레이션하려는 경우에 유용합니다.

### 지원되는 작업 환경 및 데이터 소스

Cloud Data Sense는 다음과 같은 유형의 작업 환경 및 데이터 소스에서 데이터를 스캔할 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)
- 데이터베이스를 지원합니다
- OneDrive 계정
- SharePoint 계정

Data Sense는 NFS 버전 3.x, 4.0, 4.1 및 CIFS 버전 1.x, 2.0, 2.1 및 3.0을 지원합니다.

## 비용

- 클라우드 데이터 센스를 사용하는 비용은 스캔하는 데이터의 양에 따라 다릅니다. Cloud Manager 작업 공간에서 Data Sense가 스캔하는 첫 번째 1TB의 데이터는 무료입니다. 여기에는 모든 작업 환경 및 데이터 소스의 모든 데이터가 포함됩니다. AWS, Azure 또는 GCP Marketplace에 대한 가입 또는 NetApp의 BYOL 라이선스를 구입해야 하며, 이후 계속해서 데이터를 스캔할 수 있습니다. 을 참조하십시오 ["가격"](#) 를 참조하십시오.

["Cloud Data Sense에 대한 라이선스 부여 방법을 알아보십시오"](#).

- 클라우드에 Cloud Data Sense를 설치하려면 클라우드 인스턴스를 구축해야 하므로 클라우드 인스턴스가 구축된 클라우드 공급자가 비용을 지불해야 합니다. 을 참조하십시오 [각 클라우드 공급자에 대해 구축된 인스턴스 유형입니다](#). 사내 시스템에 Data Sense를 설치하면 비용이 들지 않습니다.
- Cloud Data Sense를 사용하려면 Connector를 구축해야 합니다. 대부분의 경우 Cloud Manager에서 사용 중인 다른 스토리지 및 서비스로 인해 이미 Connector를 사용하고 있습니다. 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. Cloud Data Sense 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"](#)

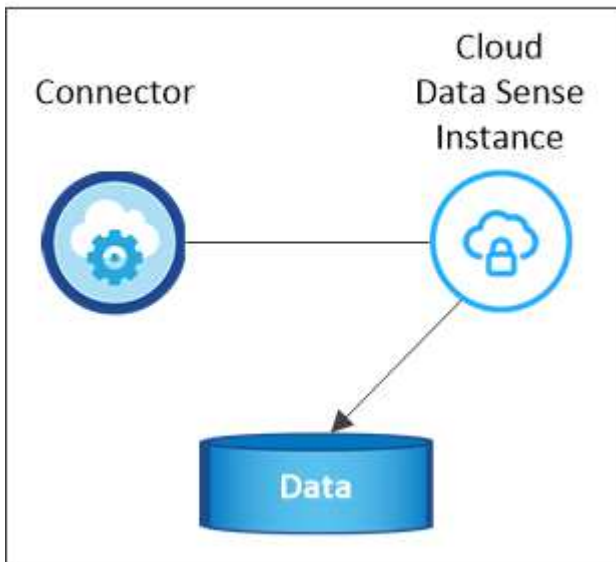
## 클라우드 데이터 감지 인스턴스

클라우드에 Data Sense를 구축하면 Cloud Manager가 Connector와 동일한 서브넷에 인스턴스를 배포합니다. ["커넥터에 대해 자세히 알아보십시오."](#)



Connector가 내부에 설치된 경우, Cloud Data Sense 인스턴스는 요청에 포함된 첫 번째 Cloud Volumes ONTAP 시스템과 동일한 VPC 또는 VNET에 구축됩니다. Data Sense를 온프레미스에 설치할 수도 있습니다.

## VPC or VNet



기본 인스턴스에 대한 다음 사항에 유의하십시오.

- AWS에서 Cloud Data Sense는 에서 실행됩니다 "m5.4xlarge 인스턴스" 500GB GP2 디스크 사용. 운영 체제 이미지는 Amazon Linux 2(Red Hat 7.3.1)입니다.

m5.4xlarge를 사용할 수 없는 지역에서는 데이터 센스를 m4.4xlarge 인스턴스에서 대신 실행합니다.

- Azure에서 Cloud Data Sense는 에서 실행됩니다 "standard\_d16s\_v3 vm" 512GB 디스크 사용 운영 체제 이미지는 CentOS 7.8입니다.
- GCP에서 Cloud Data Sense는 에서 실행됩니다 "N2-표준-16 VM" 512GB 표준 영구 디스크 사용. 운영 체제 이미지는 CentOS 7.9입니다.

n2-standard-16을 사용할 수 없는 지역에서는 n2d-standard-16 또는 n1-standard-16 VM에서 데이터 센스를 대신 실행합니다.

- 인스턴스의 이름은 *CloudCompliance\_*이며 생성된 해시(UUID)와 연결됩니다. 예: *\_CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Connector당 하나의 데이터 감지 인스턴스만 배포됩니다.
- 데이터 감지 소프트웨어의 업그레이드는 인스턴스에 인터넷 액세스 권한이 있는 경우 자동으로 수행됩니다.



Cloud Data Sense는 지속적으로 데이터를 스캔하기 때문에 인스턴스는 항상 실행 상태를 유지해야 합니다.

## 더 작은 인스턴스 유형 사용

CPU가 적고 RAM이 적은 시스템에 데이터 센스를 배포할 수 있지만 이러한 덜 강력한 시스템을 사용할 때는 몇 가지 제한 사항이 있습니다.

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

클라우드에 데이터 센스를 배포할 때 이러한 소형 시스템 중 하나를 사용하려면 [ng-contact-data-sense@netapp.com](mailto:ng-contact-data-sense@netapp.com)으로 이메일을 보내 지원을 요청하십시오. 이러한 소규모 클라우드 구성을 구축하려면 반드시 협력해야 합니다.

온프레미스에 Data Sense를 배포할 때는 작은 사양의 Linux 호스트만 사용하십시오. NetApp에 지원을 요청할 필요가 없습니다.

## 클라우드 데이터 센스의 작동 방식

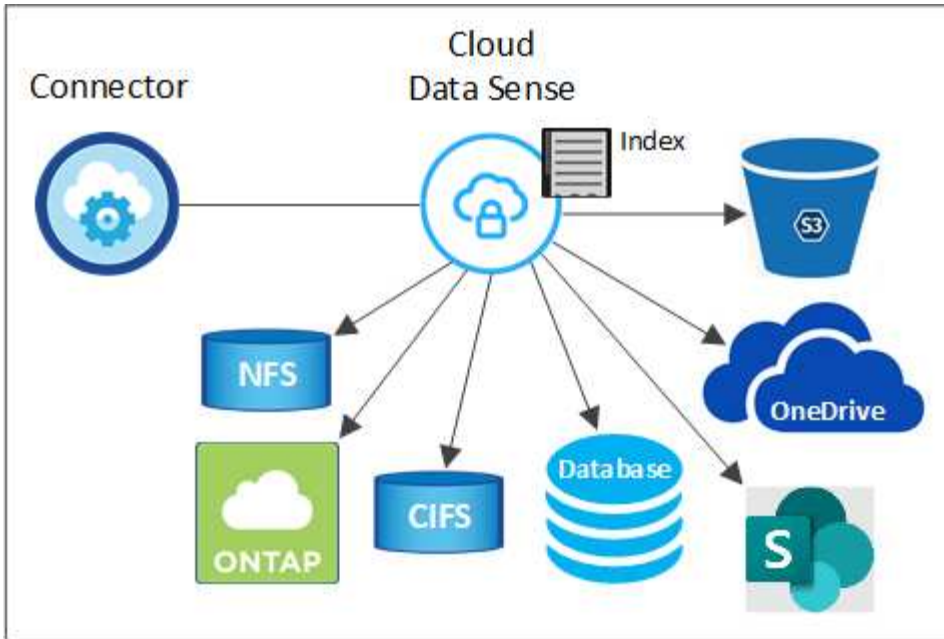
개략적인 Cloud Data Sense는 다음과 같이 작동합니다.

1. Cloud Manager에 데이터 센스의 인스턴스를 배포합니다.
2. 하나 이상의 작업 환경 또는 데이터 소스에서 고급 매핑 또는 심층 스캔을 수행할 수 있습니다.
3. 데이터 센스는 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

Cloud Data Sense를 활성화하고 스캔할 볼륨, 버킷, 데이터베이스 스키마 또는 OneDrive 또는 SharePoint 사용자 데이터를 선택한 후 즉시 데이터를 스캔하여 개인 데이터와 중요한 데이터를 식별합니다. 조직 데이터를 매핑하고 각 파일을 분류하며 데이터에서 엔터티 및 미리 정의된 패턴을 식별 및 추출합니다. 검사 결과는 개인 정보, 민감한 개인 정보, 데이터 범주 및 파일 형식의 인덱스입니다.

Data Sense는 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 스캔 후 데이터 센스에서 지속적으로 데이터를 스캔하여 변동분 변화를 감지합니다(인스턴스 실행을 유지하는 것이 중요한 이유).

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

Cloud Data Sense를 사용하면 선택한 작업 환경 및 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 이러한 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
원본 파일을 복사, 삭제 및 이동합니다	예	아니요

피처	분류	매핑
다른 보고서를 실행할 수 있습니다	예	아니요

## Cloud Data Sense가 인덱싱하는 정보입니다

데이터 센스는 데이터(파일)에 범주를 수집, 색인 및 할당합니다. Data Sense 색인에는 다음과 같은 데이터가 포함됩니다.

### 표준 메타데이터

Cloud Data Sense는 파일 유형, 크기, 생성 및 수정 날짜 등과 같은 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

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

### 유형

Cloud Data Sense는 스캔한 데이터를 파일 형식별로 분해합니다. ["유형에 대해 자세히 알아보십시오"](#).

### 이름 요소 인식

클라우드 데이터 센스(Cloud Data Sense)는 AI를 사용하여 문서에서 자연인의 이름을 추출합니다. ["데이터 주체 액세스 요청에 응답하는 방법에 대해 알아보십시오"](#).

## 네트워킹 개요

Cloud Manager는 Connector 인스턴스의 인바운드 HTTP 연결을 활성화하는 보안 그룹과 함께 Cloud Data Sense 인스턴스를 배포합니다.

SaaS 모드에서 Cloud Manager를 사용할 경우 Cloud Manager에 대한 연결이 HTTPS를 통해 제공되고 브라우저와 Data Sense 인스턴스 간에 전송되는 개인 데이터는 엔드 투 엔드 암호화로 보호됩니다. 즉, NetApp과 타사에서 해당 데이터를 읽을 수 없습니다.

아웃바운드 규칙은 완전히 열립니다. 데이터 감지 소프트웨어를 설치 및 업그레이드하고 사용량 메트릭을 전송하려면 인터넷에 액세스해야 합니다.

네트워킹 요구 사항이 엄격하면 ["Cloud Data Sense가 접속하는 엔드포인트에 대해 알아보십시오"](#).

## 규정 준수 정보에 대한 사용자 액세스

각 사용자에게 할당된 역할은 Cloud Manager 및 Cloud Data Sense 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 Cloud Manager의 작업 환경에 액세스할 수 없는 경우 데이터 감지 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.

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

## 클라우드 데이터 센스를 구축하십시오

클라우드 데이터 센스를 클라우드에 배포합니다

클라우드 데이터 센스를 클라우드에 구축하려면 몇 단계를 완료하십시오.

참고: 또한 이 기능을 사용할 수 있습니다 "인터넷에 액세스할 수 있는 Linux 호스트에 데이터 센스를 배포합니다". 온프레미스에도 있는 데이터 감지 인스턴스를 사용하여 사내 ONTAP 시스템을 스캔하려는 경우 설치 유형이 좋은 옵션이 될 수 있지만 이는 필수 사항이 아닙니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다.

빠른 시작

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

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

또한 가능합니다 "Connector를 온-프레미스에 배포합니다" 네트워크 또는 클라우드의 Linux 호스트

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

기본 구성에는 Cloud Data Sense 인스턴스에 대해 16개의 vCPU가 필요합니다. 을 참조하십시오 "인스턴스 유형에 대한 자세한 내용".

설치 마법사를 시작하여 클라우드에 Cloud Data Sense 인스턴스를 구축합니다.

Cloud Manager에서 Cloud Data Sense를 통해 스캔하는 첫 번째 1TB의 데이터는 무료입니다. 해당 시점 이후에도 데이터를 계속 스캔하려면 클라우드 공급자 마켓플레이스 또는 NetApp의 BYOL 라이선스를 통한 Cloud Manager 가입이 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 Cloud Data Sense를 활성화하려고 시도하기 전에 Connector를 설정했을 것입니다 "Cloud Manager 기능에는 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.
- GCP의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 GCP의 커넥터를 사용합니다.

온프레미스 ONTAP 시스템, 타사 파일 공유, 범용 S3 오브젝트 스토리지, 데이터베이스, OneDrive 폴더, SharePoint 계정을 이러한 클라우드 커넥터를 사용할 때 스캔할 수 있습니다.

참고: 또한 이 기능을 사용할 수 있습니다 "[Connector를 온-프레미스에 배포합니다](#)" 네트워크 또는 클라우드의 Linux 호스트 데이터 센스를 사내에서 설치하려는 일부 사용자는 Connector를 온프레미스에 설치하도록 선택할 수도 있습니다.

보시다시피 을 사용해야 하는 몇 가지 상황이 있을 수 있습니다 "[다중 커넥터](#)".



Azure NetApp Files 볼륨을 스캔할 계획이라면 스캔할 볼륨과 동일한 영역에 를 배포해야 합니다.

사전 요구 사항을 검토합니다

클라우드 데이터 센스를 클라우드에 구축하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

클라우드 데이터 센스에서 아웃바운드 인터넷 액세스를 활성화합니다

클라우드 데이터 센스를 사용하려면 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 데이터 감지 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스가 있는지 확인하십시오. 클라우드에 Data Sense를 구축하면 Connector와 동일한 서브넷에 위치합니다.

AWS, Azure 또는 GCP에서 Cloud Data Sense를 구현하는지 여부에 따라 아래에서 적절한 표를 검토하십시오.

- AWS 구축에 필요한 엔드포인트: \*

엔드포인트	목적
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> 으로 문의하십시오	NetApp 계정을 포함한 Cloud Manager 서비스와 통신합니다.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a> 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
<a href="https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com">https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com</a> \ <a href="https://hub.docker.com">https://hub.docker.com</a> \ <a href="https://auth.docker.io">https://auth.docker.io</a> \ <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> \ <a href="https://index.docker.io/">https://index.docker.io/</a> \ <a href="https://dseasb33srnrn.cloudfront.net">https://dseasb33srnrn.cloudfront.net</a> \ <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a> 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

엔드포인트	목적
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> \ <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> \ <a href="https://user-feedback-store-prod.s3.us-west-2.amazonaws.com">https://user-feedback-store-prod.s3.us-west-2.amazonaws.com</a> \ <a href="https://customer-data-production.s3.us-west-2.amazonaws.com">https://customer-data-production.s3.us-west-2.amazonaws.com</a>	Cloud Data Sense를 통해 매니페스트와 템플릿을 액세스 및 다운로드하고 로그 및 메트릭을 전송할 수 있습니다.

- Azure 및 GCP 구축에 필요한 엔드포인트: \*

엔드포인트	목적
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> 으로 문의하십시오	NetApp 계정을 포함한 Cloud Manager 서비스와 통신합니다.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> \ <a href="https://auth0.com">https://auth0.com</a> 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
<a href="https://support.compliance.cloudmanager.cloud.netapp.com">https://support.compliance.cloudmanager.cloud.netapp.com</a> \ <a href="https://hub.docker.com">https://hub.docker.com</a> \ <a href="https://auth.docker.io">https://auth.docker.io</a> \ <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> \ <a href="https://index.docker.io/">https://index.docker.io/</a> \ <a href="https://dseasb33srrn.cloudfront.net">https://dseasb33srrn.cloudfront.net</a> \ <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	소프트웨어 이미지, 매니페스트, 템플릿에 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
<a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a> 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

#### Cloud Manager에 필요한 권한이 있는지 확인합니다

Cloud Manager에 리소스를 구축하고 Cloud Data Sense 인스턴스에 대한 보안 그룹을 생성할 수 있는 권한이 있는지 확인합니다. 에서 최신 Cloud Manager 사용 권한을 찾을 수 있습니다 "[NetApp에서 제공하는 정책](#)".

#### vCPU 한도를 확인하십시오

클라우드 공급자의 vCPU 제한으로 16개 코어가 있는 인스턴스를 구축할 수 있는지 확인합니다. Cloud Manager가 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](#)"

CPU가 적고 RAM이 적은 시스템에 데이터 센스를 배포할 수 있지만 이러한 시스템을 사용할 때는 한계가 있습니다. 을 참조하십시오 "[더 작은 인스턴스 유형 사용](#)" 를 참조하십시오.

#### Cloud Manager Connector가 클라우드 데이터 센스에 액세스할 수 있는지 확인합니다

Connector와 Cloud Data Sense 인스턴스 간의 연결을 확인합니다. Connector의 보안 그룹은 포트 443을 통해 데이터 감지 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다. 이 연결을 통해 Data Sense 인스턴스를 구축할 수 있으며 규정 준수 및 거버넌스 탭에서 정보를 볼 수 있습니다. Cloud Data Sense는 AWS 및 Azure의 정부 지역에서 지원됩니다.

AWS 및 AWS GovCloud 배포에는 추가 인바운드 및 아웃바운드 규칙이 필요합니다. 을 참조하십시오 ["AWS의 커넥터 규칙"](#) 를 참조하십시오.

Azure 및 Azure Government 배포에는 추가 인바운드 및 아웃바운드 규칙이 필요합니다. 을 참조하십시오 ["Azure의 커넥터 규칙"](#) 를 참조하십시오.

클라우드 데이터 센스를 계속 운영할 수 있는지 확인하십시오

데이터를 지속적으로 스캔하려면 Cloud Data Sense 인스턴스가 켜져 있어야 합니다.

클라우드 데이터 센스에 대한 웹 브라우저 연결을 확인합니다

Cloud Data Sense를 사용하도록 설정한 후에는 사용자가 Data Sense 인스턴스에 연결된 호스트에서 Cloud Manager 인터페이스에 액세스해야 합니다.

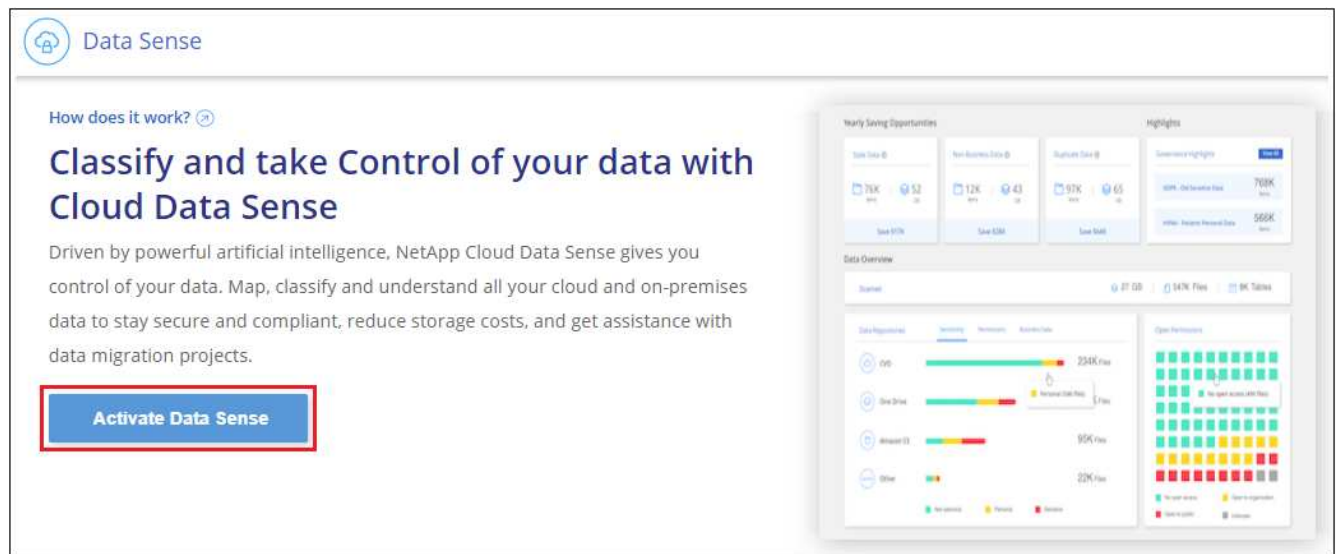
Data Sense 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터에 인터넷에서 액세스할 수 없도록 합니다. 따라서 Cloud Manager에 액세스하는 데 사용하는 웹 브라우저에는 해당 프라이빗 IP 주소에 연결되어 있어야 합니다. 이러한 연결은 클라우드 공급자(예: VPN)에 직접 연결되거나 데이터 감지 인스턴스와 동일한 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

클라우드에 데이터 센스를 구축하십시오

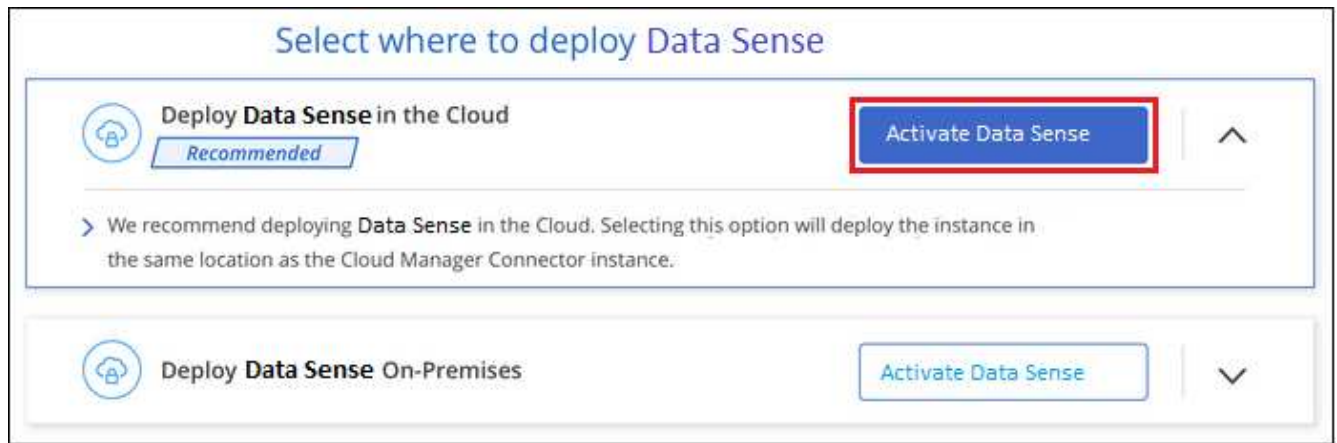
다음 단계에 따라 클라우드 데이터 센스의 인스턴스를 클라우드에 배포합니다.

단계

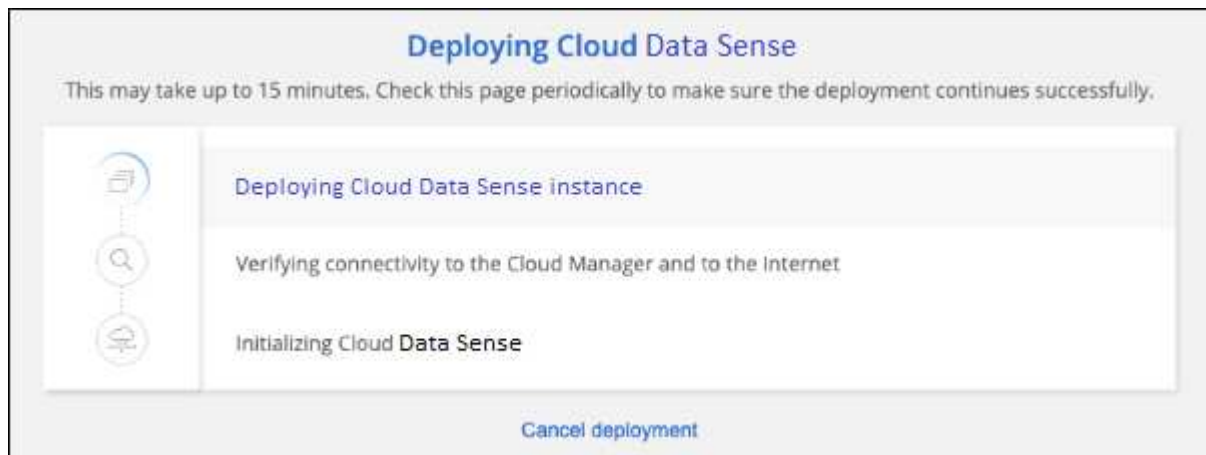
1. Cloud Manager에서 \* 데이터 감지 \* 를 클릭합니다.
2. Activate Data Sense \* 를 클릭합니다.



3. 클라우드 배포 마법사를 시작하려면 \* Activate Data Sense \* 를 클릭합니다.



4. 구축 단계를 진행할 때 마법사가 진행률을 표시합니다. 문제가 발생할 경우 중지하고 입력을 요청합니다.



5. 인스턴스가 배포되면 \* Continue to configuration \* 을 클릭하여 \_Configuration\_ 페이지로 이동합니다.

Cloud Manager는 클라우드 공급업체에 Cloud Data Sense 인스턴스를 구축합니다.

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 ["클라우드 데이터 센스에 대한 라이선스 설정"](#) 현재. 데이터 양이 1TB를 초과할 때까지 비용이 청구되지 않습니다.

인터넷에 액세스할 수 있는 **Linux** 호스트에 클라우드 데이터 센스를 배포합니다

몇 가지 단계를 완료하여 인터넷 액세스가 가능한 네트워크 또는 클라우드의 Linux 호스트에 Cloud Data Sense를 배포합니다.

온프레미스에 있는 데이터 감지 인스턴스를 사용하여 사내 ONTAP 시스템을 스캔하려는 경우 사내 설치가 좋은 옵션이 될 수 있지만, 이것이 요구사항은 아닙니다. 선택한 설치 방법에 관계없이 소프트웨어가 정확히 같은 방식으로 작동합니다.

참고: 또한 이 기능을 사용할 수 있습니다 ["인터넷에 액세스할 수 없는 온프레미스 사이트에 데이터 센스를 구현합니다"](#) 완전히 안전한 사이트를 위한 것입니다.

## 빠른 시작

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

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

또한 가능합니다 ["Connector를 온-프레미스에 배포합니다"](#) 네트워크 또는 클라우드의 Linux 호스트

환경이 필수 조건을 충족할 수 있는지 확인합니다. 여기에는 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 443을 통한 커넥터와 클라우드 데이터 감지 간의 연결 등이 포함됩니다. [전체 목록을 참조하십시오](#).

또한 을 충족하는 Linux 시스템도 필요합니다 [따르는 요구사항](#).

NetApp Support 사이트에서 Cloud Data Sense 소프트웨어를 다운로드하고 사용할 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 시작하고 프롬프트에 따라 Data Sense 인스턴스를 배포합니다.

Cloud Manager에서 Cloud Data Sense를 통해 스캔하는 첫 번째 1TB의 데이터는 무료입니다. 해당 시점 이후에도 데이터를 계속 스캔하려면 클라우드 공급자 마켓플레이스 또는 NetApp의 BYOL 라이선스를 구입해야 합니다.

## 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 Cloud Data Sense를 활성화하려고 시도하기 전에 Connector를 설정했을 것입니다 ["Cloud Manager 기능에는 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.
- 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 계정을 이러한 클라우드 커넥터를 사용하여 스캔할 수 있습니다.

참고: 또한 이 기능을 사용할 수 있습니다 ["Connector를 온-프레미스에 배포합니다"](#) 네트워크 또는 클라우드의 Linux 호스트 데이터 센스를 사내에서 설치하려는 일부 사용자는 Connector를 온프레미스에 설치하도록 선택할 수도 있습니다.

보시다시피 을 사용해야 하는 몇 가지 상황이 있을 수 있습니다 ["다중 커넥터"](#).



Azure NetApp Files 볼륨을 스캔할 계획이라면 스캔할 볼륨과 동일한 영역에 를 배포해야 합니다.

## Linux 호스트 시스템을 준비합니다

Data Sense 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다. 다른 애플리케이션과 공유되는 호스트에서는 데이터 센스를 지원하지 않습니다. 호스트는 전용 호스트여야 합니다.



- 운영 체제: Red Hat Enterprise Linux 또는 CentOS 버전 8.0 또는 8.1
  - 버전 7.8을 사용할 수 있지만 Linux 커널 버전은 4.14 이상이어야 합니다
  - OS에서 Docker 엔진을 설치할 수 있어야 합니다(예: 필요한 경우 `_firewalld_service` 사용 안 함).
- 디스크: 500GiB의 SSD 사용 가능 온/또는
  - 100GiB를 On/OPT에서 사용할 수 있습니다
  - /var에서 400GiB를 사용할 수 있습니다
  - /tmp에 5GiB입니다
- RAM: 64GB(스왑 메모리는 호스트에서 비활성화해야 함)
- CPU: 16코어

CPU가 적고 RAM이 적은 시스템에 데이터 센스를 배포할 수 있지만 이러한 시스템을 사용할 때는 한계가 있습니다. 을 참조하십시오 ["더 작은 인스턴스 유형 사용"](#) 를 참조하십시오.

- Red Hat Enterprise Linux 시스템은 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우 설치 중에 시스템에서 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.
- 다음 소프트웨어가 호스트에 설치되어 있어야 합니다. 호스트에 아직 없는 경우 설치 프로그램이 소프트웨어를 설치합니다.
  - Docker Engine 버전 19 이상 ["설치 지침을 봅니다"](#).
  - Python 3 버전 3.6 이상. ["설치 지침을 봅니다"](#).

## Cloud Manager 및 Data Sense 사전 요구 사항을 확인합니다

Linux 시스템에 Cloud Data Sense를 배포하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

클라우드 데이터 센스에서 아웃바운드 인터넷 액세스를 활성화합니다

클라우드 데이터 센스를 사용하려면 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 데이터 감지 인스턴스에 다음 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스가 있는지 확인하십시오.

엔드포인트	목적
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> 으로 문의하십시오	NetApp 계정을 포함한 Cloud Manager 서비스와 통신합니다.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a> 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
<a href="https://support.compliance.cloudmanager.cloud.netapp.com/https://hub.docker.com/https://auth.docker.io/https://registry-1.docker.io/https://index.docker.io/https://dseasb33srrn.cloudfront.net/https://production.cloudflare.docker.com/">https://support.compliance.cloudmanager.cloud.netapp.com/https://hub.docker.com/https://auth.docker.io/https://registry-1.docker.io/https://index.docker.io/https://dseasb33srrn.cloudfront.net/https://production.cloudflare.docker.com/</a>	소프트웨어 이미지, 매니페스트, 템플릿에 액세스하고 로그 및 메트릭을 보낼 수 있습니다.
<a href="https://support.compliance.cloudmanager.cloud.netapp.com/">https://support.compliance.cloudmanager.cloud.netapp.com/</a> 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.

엔드포인트	목적
<a href="https://github.com/docker">https://github.com/docker</a> <a href="https://download.docker.com">https://download.docker.com</a> <a href="http://mirror.centos.org">http://mirror.centos.org</a> <a href="http://mirrorlist.centos.org">http://mirrorlist.centos.org</a> <a href="http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm">http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm</a> 를 참조하십시오	설치를 위한 필수 패키지를 제공합니다.

### Cloud Manager에 필요한 권한이 있는지 확인합니다

Cloud Manager에 리소스를 구축하고 Cloud Data Sense 인스턴스에 대한 보안 그룹을 생성할 수 있는 권한이 있는지 확인합니다. 에서 최신 Cloud Manager 사용 권한을 찾을 수 있습니다 "[NetApp에서 제공하는 정책](#)".

### Cloud Manager Connector가 클라우드 데이터 센스에 액세스할 수 있는지 확인합니다

Connector와 Cloud Data Sense 인스턴스 간의 연결을 확인합니다. Connector의 보안 그룹은 포트 443을 통해 데이터 감지 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다.

이 연결을 통해 Data Sense 인스턴스를 구축할 수 있으며 규정 준수 및 거버넌스 탭에서 정보를 볼 수 있습니다.

Cloud Manager에서 설치 진행률을 볼 수 있도록 포트 8080이 열려 있는지 확인합니다.

### 클라우드 데이터 센스를 계속 운영할 수 있는지 확인하십시오

데이터를 지속적으로 스캔하려면 Cloud Data Sense 인스턴스가 켜져 있어야 합니다.

### 클라우드 데이터 센스에 대한 웹 브라우저 연결을 확인합니다

Cloud Data Sense를 사용하도록 설정한 후에는 사용자가 Data Sense 인스턴스에 연결된 호스트에서 Cloud Manager 인터페이스에 액세스해야 합니다.

Data Sense 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터에 인터넷에서 액세스할 수 없도록 합니다. 따라서 Cloud Manager에 액세스하는 데 사용하는 웹 브라우저에는 해당 프라이빗 IP 주소에 연결되어 있어야 합니다. 이러한 연결은 클라우드 공급자(예: VPN)에 직접 연결되거나 데이터 감지 인스턴스와 동일한 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

### 온프레미스에서 데이터 센스를 구축합니다

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](#) 클라우드 데이터 센스를 구축하기 전에 필요한 전체 목록을 확인하십시오.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.



소프트웨어가 사내에 설치된 경우 클라우드 데이터 센스에서 현재 Azure NetApp Files용 S3 버킷, ONTAP 또는 FSx를 스캔할 수 없습니다. 이 경우 클라우드 및 에 별도의 Connector와 데이터 센스의 인스턴스를 배포해야 합니다 "[커넥터 사이를 전환합니다](#)" 다양한 데이터 소스에 대해



일반 구성을 위한 단일 호스트 설치

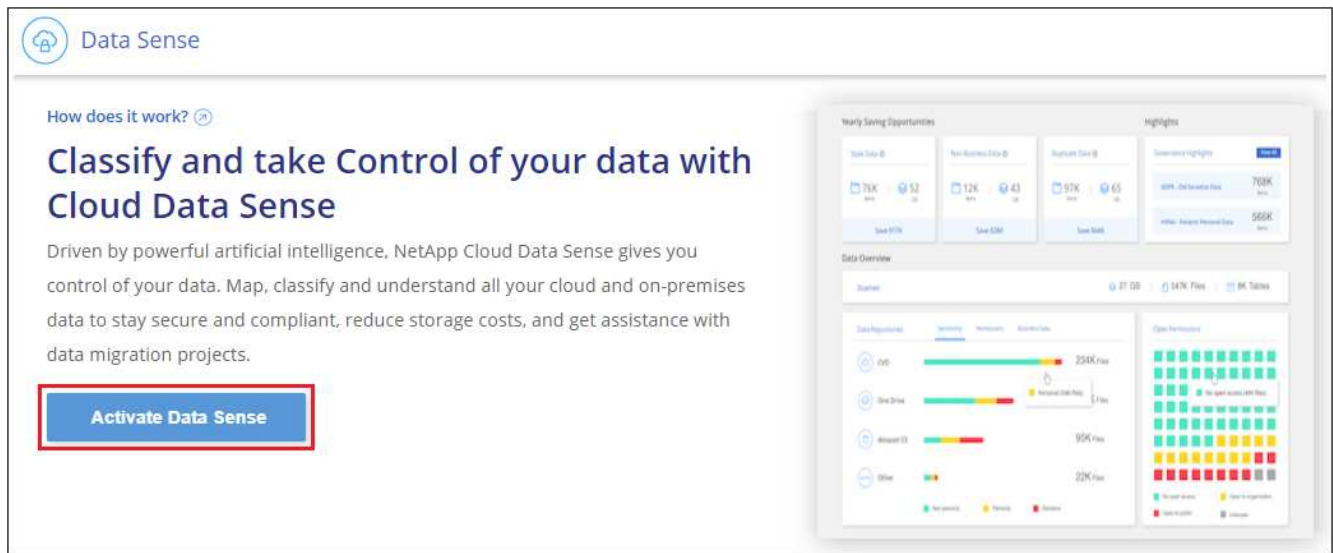
단일 온프레미스 호스트에 Data Sense 소프트웨어를 설치할 때 다음 단계를 따르십시오.

무엇을 '필요로 할거야

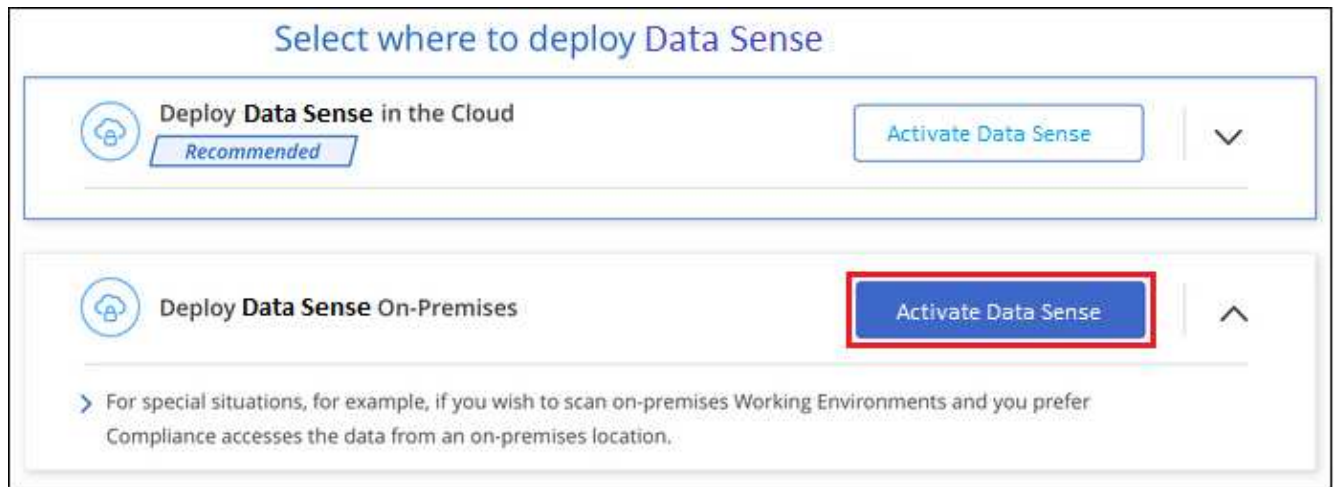
- Linux 시스템이 를 충족하는지 확인합니다 [호스트 요구 사항](#).
- (선택 사항) 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 및 Python 3)가 설치되어 있는지 확인합니다. 시스템에 설치되어 있지 않은 경우 설치 프로그램이 이 소프트웨어를 설치합니다.
- Linux 시스템에 대한 루트 권한이 있는지 확인합니다.
- 프록시를 사용하고 있고 TLS 가로채기를 수행하는 경우 TLS CA 인증서가 저장되는 Data Sense Linux 시스템의 경로를 알아야 합니다.
- 오프라인 환경이 필요한 를 충족하는지 확인합니다 [사용 권한 및 연결](#).

단계

1. 에서 Cloud Data Sense 소프트웨어를 다운로드하십시오 "[NetApp Support 사이트](#)". 선택해야 하는 파일의 이름은 \* cc\_onpremise\_installer\_<version>.tar.gz \* 입니다.
2. 설치 프로그램 파일을 사용하려는 Linux 호스트에 복사합니다(scp 또는 다른 방법 사용).
3. Cloud Manager에서 \* 데이터 감지 \* 를 클릭합니다.
4. Activate Data Sense \* 를 클릭합니다.



5. Activate Data Sense \* 를 클릭하여 온프레미스 배포 마법사를 시작합니다.



6. deploy Data Sense on premises\_dialog에서 제공된 명령을 복사하여 나중에 사용할 수 있도록 텍스트 파일에 붙여넣은 다음 \* Close \* 를 클릭합니다. 예를 들면 다음과 같습니다.

```
'SUDO./install.sh - A 12345-c 27AG75-t 2198qq'
```

7. 호스트 시스템에서 설치 프로그램 파일의 압축을 풉니다. 예를 들면 다음과 같습니다.

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

8. 설치 프로그램에서 프롬프트가 표시되면 일련의 프롬프트에 필요한 값을 입력하거나 설치 프로그램에 명령줄 인수로 필요한 매개 변수를 제공할 수 있습니다.

프롬프트가 나타나면 매개 변수를 입력합니다.	전체 명령 입력:
<p>a. 6 단계:'SUDO./install.sh -a&lt;account_id&gt; -c&lt;agent_id&gt;-t&lt;token&gt;'에서 복사한 정보를 붙여 넣습니다</p> <p>b. Connector 인스턴스에서 액세스할 수 있도록 Data Sense 호스트 시스템의 IP 주소 또는 호스트 이름을 입력합니다.</p> <p>c. Data Sense 인스턴스에서 액세스할 수 있도록 Cloud Manager Connector 호스트 시스템의 IP 주소 또는 호스트 이름을 입력합니다.</p> <p>d. 메시지가 나타나면 프록시 세부 정보를 입력합니다. Cloud Manager에서 이미 프록시를 사용하고 있는 경우, Data Sense에서 Cloud Manager에서 사용하는 프록시를 자동으로 사용하기 때문에 이 정보를 다시 입력할 필요가 없습니다.</p>	<p>또는 필요한 호스트 및 프록시 매개 변수</p> <pre>'sudo./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt;--host &lt;ds_host&gt;--manager -host &lt;cm_host&gt;--proxy-host &lt;proxy_host&gt;--proxy scheme -port &lt;proxy_port&gt; -proxy -proxy -proxy -dir'</pre> <p>를 제공하여 전체 명령을 미리 생성할 수 있습니다</p>

변수 값:

- *ACCOUNT\_ID*= NetApp 계정 ID입니다
- *agent\_id*=커넥터 ID입니다

- *token*= JWT 사용자 토큰
- *DS\_HOST*= Data Sense Linux 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm\_host*= Cloud Manager Connector 시스템의 IP 주소 또는 호스트 이름입니다.
- *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.
- *proxy\_password*=지정한 사용자 이름의 암호입니다.
- *ca\_cert\_dir*=추가 TLS CA 인증서 번들이 포함된 Data Sense Linux 시스템의 경로입니다. 프록시가 TLS 가로채기를 수행하는 경우에만 필요합니다.

Cloud Data Sense 설치 프로그램은 패키지를 설치하고, Docker를 설치하고, 설치를 등록하고, Data Sense를 설치합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

호스트 시스템과 Connector 인스턴스 간에 포트 8080을 통해 연결되어 있는 경우 Cloud Manager의 Data Sense 탭에서 설치 진행률을 확인할 수 있습니다.

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 ["클라우드 데이터 센스에 대한 라이선스 설정"](#) 현재. 데이터 양이 1TB를 초과할 때까지 비용이 청구되지 않습니다.

대규모 구성을 위한 다중 호스트 설치

페타바이트 단위의 데이터를 스캔할 수 있는 대규모 구성의 경우 여러 호스트를 포함하여 처리 능력을 높일 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 Data Sense 소프트웨어를 설치할 때 다음 단계를 따르십시오.

무엇을 '필요로 할거야

- Manager 및 Scanner 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 [호스트 요구 사항](#).
- (선택 사항) 시스템에 두 가지 필수 소프트웨어 패키지(Docker Engine 및 Python 3)가 설치되어 있는지 확인합니다. 시스템에 설치되어 있지 않은 경우 설치 프로그램이 이 소프트웨어를 설치합니다.
- 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
4789	UDP입니다	오버레이 네트워크 트래픽

포트	프로토콜	설명
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

- 에서 1단계부터 7단계까지 수행합니다 [단일 호스트 설치](#) 관리자 노드에서.
- 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 scanner 노드 3개를 추가합니다. `sudo./install.sh -a <account_id> -c <agent_id> -t <token>--host <DS_host>--manager -host <cm_host> * -n <node_IP1>, <node_ip2>, <node_ip2>, <node_proxy scheme> -proxy -proxy -proxy -host < 프록시 포트 프록시> -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -proxy -port -proxy -proxy -host <`

- 관리자 노드 설치가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사하여 텍스트 파일에 저장합니다. 예를 들면 다음과 같습니다.

'`SUDO./node_install.sh -m 10.11.12.13 -t abcdef-1-3u69m1-1s35212`'를 참조하십시오

- 켜짐 \* 각 \* 스캐너 노드 호스트:
  - Data Sense 설치 프로그램 파일(\* `cc_onpremise_installer_<version>.tar.gz` \*)을 호스트 시스템('scp' 또는 기타 다른 방법 사용)에 복사합니다.
  - 설치 프로그램 파일의 압축을 풉니다.
  - 3단계에서 복사한 명령을 붙여 넣고 실행합니다.

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

Cloud Data Sense 설치 프로그램이 패키지, Docker 설치를 완료하고 설치를 등록합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

구성 페이지에서 스캔할 데이터 원본을 선택할 수 있습니다.

또한 가능합니다 ["클라우드 데이터 센스에 대한 라이선스 설정"](#) 현재. 데이터 양이 1TB를 초과할 때까지 비용이 청구되지 않습니다.

인터넷에 액세스하지 않고 클라우드 데이터 센스를 내부에 구축할 수 있습니다

인터넷 액세스가 없는 사내 사이트의 호스트에 클라우드 데이터 센스를 배포하려면 몇 단계를 완료하십시오. 이러한 유형의 설치 는 보안 사이트에 적합합니다.

참고: 또한 이 기능을 사용할 수 있습니다 ["인터넷에 액세스할 수 있는 온프레미스 사이트에 데이터 센스를 구현합니다"](#).

## 지원되는 데이터 소스

이러한 방식으로 설치할 경우("오프라인" 또는 "다크" 사이트라고도 함) 데이터 센스(Data Sense)는 사내 사이트에도 로컬인 데이터 소스의 데이터만 스캔할 수 있습니다. 현재 Data Sense는 다음과 같은 로컬 데이터 소스를 스캔할 수 있습니다.

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

매우 안전한 Cloud Manager 설치에 필요하지만 OneDrive 계정 또는 SharePoint 계정에서 로컬 데이터를 스캔하려는 특수한 상황에서는 Data Sense 오프라인 설치 프로그램을 사용하여 몇 개의 선택 끝점에 대한 인터넷 액세스를 제공할 수 있습니다. 을 참조하십시오 [SharePoint 및 OneDrive 특별 요구 사항](#) 을 참조하십시오.

현재 Cloud Volumes ONTAP, Azure NetApp Files, FSx for ONTAP 또는 AWS S3 계정을 스캔할 수 없습니다.

## 제한 사항

대부분의 데이터 감지 기능은 인터넷에 연결되지 않은 사이트에 구축할 때 작동합니다. 그러나 인터넷 액세스가 필요한 특정 기능은 지원되지 않습니다. 예를 들면 다음과 같습니다.

- Microsoft Azure 정보 보호(AIP) 레이블 관리
- 특정 중요 정책에서 결과를 반환하는 경우 Cloud Manager 사용자에게 이메일 알림을 보냅니다
- 여러 사용자에게 대한 Cloud Manager 역할 설정(예: 계정 관리자 또는 규정 준수 뷰어)
- Cloud Sync를 사용하여 소스 파일 복사 및 동기화
- 사용자 피드백을 받는 중입니다
- Cloud Manager에서 소프트웨어 업그레이드 자동화

Cloud Manager Connector와 데이터 센스 모두 새로운 기능을 사용하기 위해 정기적인 수동 업그레이드가 필요합니다. 데이터 감지 UI 페이지 하단에 데이터 감지 버전이 표시됩니다. 를 확인하십시오 ["클라우드 데이터 감지 릴리스 정보"](#) 각 릴리스의 새로운 기능과 해당 기능을 원하는지 여부를 확인합니다. 그런 다음 의 단계를 수행할 수 있습니다 [데이터 감지 소프트웨어를 업그레이드하십시오](#).

## 빠른 시작

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

오프라인 온-프레미스 사이트에 커넥터가 아직 설치되어 있지 않은 경우 ["커넥터를 배포합니다"](#) 이제 Linux 호스트에서

Linux 시스템이 를 충족하는지 확인합니다 [호스트 요구 사항](#)필요한 모든 소프트웨어가 설치되어 있고 오프라인 환경이 필요한 를 충족한다는 것을 나타냅니다 [사용 권한 및 연결](#).

NetApp Support 사이트에서 Cloud Data Sense 소프트웨어를 다운로드하고 사용할 Linux 호스트에 설치 프로그램 파일을 복사합니다. 그런 다음 설치 마법사를 시작하고 화면의 지시에 따라 Cloud Data Sense 인스턴스를 구축합니다.

Cloud Manager에서 Cloud Data Sense를 통해 스캔하는 첫 번째 1TB의 데이터는 무료입니다. 이 시점 이후에 데이터를 계속 스캔하려면 NetApp의 BYOL 라이선스가 필요합니다.

## Cloud Manager Connector를 설치합니다

오프라인 사내 사이트에 Cloud Manager Connector가 아직 설치되지 않은 경우 ["커넥터를 배포합니다"](#) 오프라인 사이트의 Linux 호스트

### Linux 호스트 시스템을 준비합니다

Data Sense 소프트웨어는 특정 운영 체제 요구 사항, RAM 요구 사항, 소프트웨어 요구 사항 등을 충족하는 호스트에서 실행되어야 합니다. 다른 애플리케이션과 공유되는 호스트에서는 데이터 센스를 지원하지 않습니다. 호스트는 전용 호스트여야 합니다.

- 운영 체제: Red Hat Enterprise Linux 또는 CentOS 버전 8.0 또는 8.1
  - 버전 7.8을 사용할 수 있지만 Linux 커널 버전은 4.14 이상이어야 합니다
  - OS에서 Docker Engine을 설치할 수 있어야 합니다(예: 필요한 경우 `_firewalld_service` 사용 안 함).
- 디스크: 500GiB의 SSD 사용 가능 온/또는
  - 100GiB를 On/OPT에서 사용할 수 있습니다
  - /var에서 400GiB를 사용할 수 있습니다
  - /tmp에 5GiB입니다
- RAM: 64GB(스왑 메모리는 호스트에서 비활성화해야 함)
- CPU: 16코어

CPU가 적고 RAM이 적은 시스템에 데이터 센스를 배포할 수 있지만 이러한 시스템을 사용할 때는 한계가 있습니다. 을 참조하십시오 ["더 작은 인스턴스 유형 사용"](#) 를 참조하십시오.

Data Sense를 설치하기 전에 호스트에 다음 소프트웨어를 설치해야 합니다.

- Docker Engine 버전 19 이상 ["설치 지침을 봅니다"](#).
- Python 3 버전 3.6 이상. ["설치 지침을 봅니다"](#).

### Cloud Manager 및 Data Sense 사전 요구 사항을 확인합니다

Cloud Data Sense를 구축하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

- Cloud Manager에 리소스를 구축하고 Cloud Data Sense 인스턴스에 대한 보안 그룹을 생성할 수 있는 권한이 있는지 확인합니다.
- Cloud Manager Connector가 데이터 감지 인스턴스에 액세스할 수 있는지 확인합니다. Connector의 보안 그룹은 포트 443을 통해 데이터 감지 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다.

이 연결을 통해 Data Sense 인스턴스를 구축할 수 있으며 규정 준수 및 거버넌스 정보를 볼 수 있습니다.

Cloud Manager에서 설치 진행률을 볼 수 있도록 포트 8080이 열려 있는지 확인합니다.

- 클라우드 데이터 센스를 계속 운영할 수 있는지 확인하십시오. 데이터를 지속적으로 스캔하려면 Cloud Data Sense 인스턴스가 켜져 있어야 합니다.
- 클라우드 데이터 센스에 대한 웹 브라우저 연결을 확인합니다. Cloud Data Sense를 사용하도록 설정한 후에는 사용자가 Data Sense 인스턴스에 연결된 호스트에서 Cloud Manager 인터페이스에 액세스해야 합니다.

Data Sense 인스턴스는 개인 IP 주소를 사용하여 인덱싱된 데이터에 다른 사용자가 액세스할 수 없도록 합니다. 따라서 Cloud Manager에 액세스하는 데 사용하는 웹 브라우저에는 해당 프라이빗 IP 주소에 연결되어 있어야 합니다. 이 연결은 Data Sense 인스턴스와 동일한 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

## SharePoint 및 OneDrive 특별 요구 사항

인터넷에 액세스할 수 없는 사이트에 Cloud Manager 및 Data Sense를 배포하는 경우, 몇 개의 선택 엔드포인트에 대한 인터넷 액세스를 제공하여 SharePoint 및 OneDrive 계정의 로컬 파일을 검색할 수 있습니다.

엔드포인트	목적
login.microsoft.com \graph.microsoft.com 으로 문의하십시오	Microsoft 서버와 통신하여 선택한 온라인 서비스에 로그인합니다.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> 으로 문의하십시오	NetApp 계정을 포함한 Cloud Manager 서비스와 통신합니다.

이러한 외부 서비스에 처음 연결하는 동안에만 *cloudmanager.cloud.netapp.com* 에 액세스해야 합니다.

데이터 센스를 구축합니다

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 Data Sense 소프트웨어를 설치할 때는 다음 단계를 따르십시오.

무엇을 '필요로 할거야

- Linux 시스템이 를 충족하는지 확인합니다 [호스트 요구 사항](#).
- 필수 소프트웨어 패키지 2개(Docker Engine 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 클라우드 데이터 감지 소프트웨어를 다운로드합니다 "[NetApp Support 사이트](#)". 선택해야 하는 파일의 이름은 \* DataSense-offline-bundle-<version>.tar.gz \* 입니다.
2. 설치 프로그램 번들을 다크 사이트에서 사용할 Linux 호스트에 복사합니다.
3. 호스트 시스템에서 설치 프로그램 번들의 압축을 풉니다. 예를 들면 다음과 같습니다.

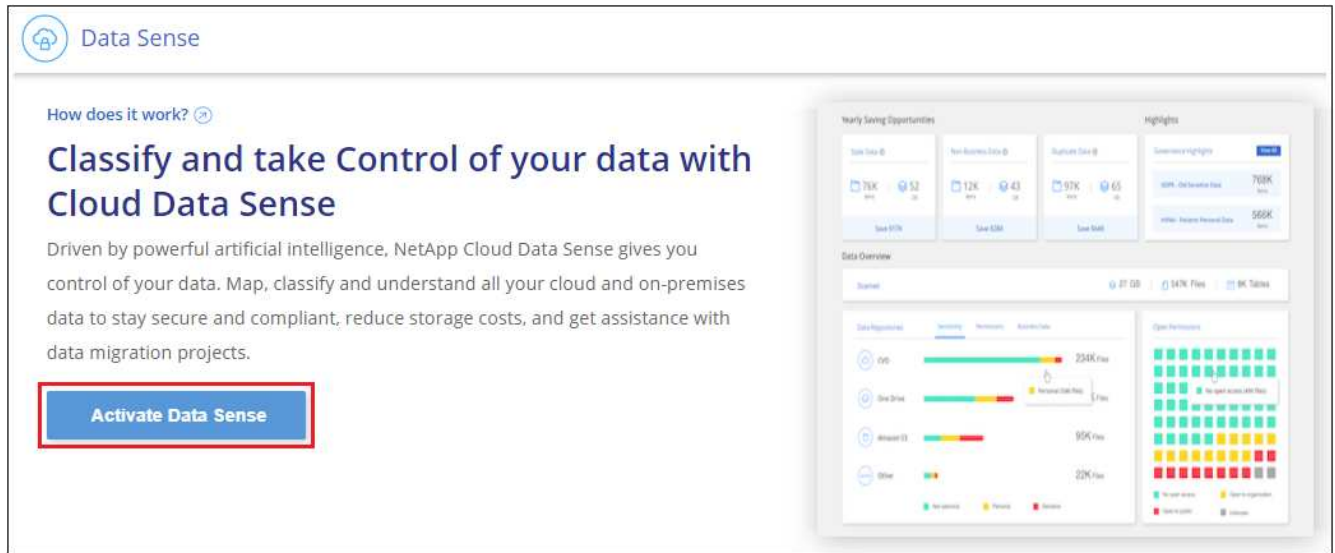
```
tar -xzf DataSense-offline-bundle-v1.10.0.tar.gz
```

필요한 소프트웨어와 실제 설치 파일 \* cc\_onprem\_installer\_<version>.tar.gz \* 를 추출합니다.

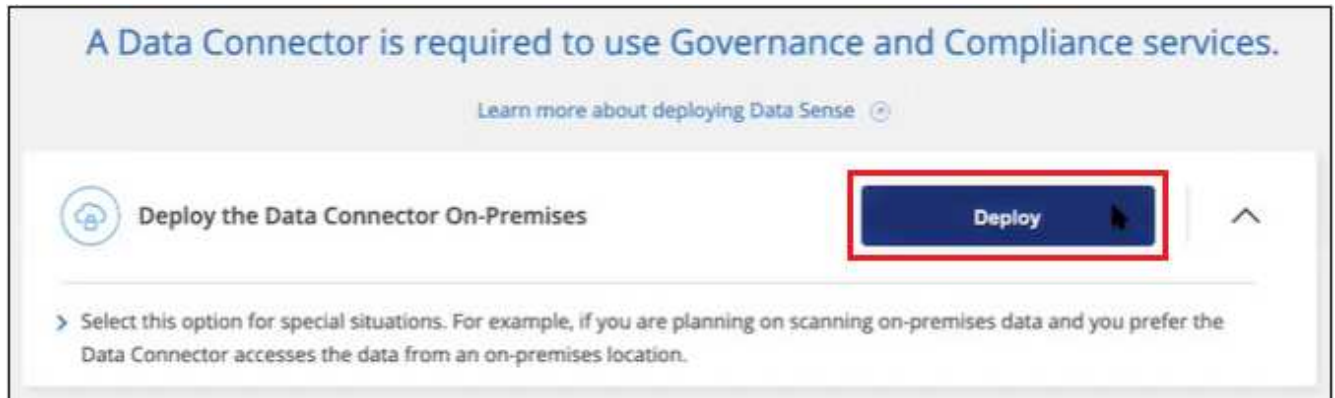
4. Cloud Manager를 시작하고 \* Data Sense \* 탭을 클릭합니다.



5. Activate Data Sense \* 를 클릭합니다.



6. 구축 \* 을 클릭하여 온프레미스 구축 마법사를 시작합니다.



7. deploy Data Sense on premises\_dialog에서 제공된 명령을 복사하여 나중에 사용할 수 있도록 텍스트 파일에 붙여넣은 다음 \* Close \* 를 클릭합니다. 예를 들면 다음과 같습니다.

'SUDO./install.sh -a 12345-c 27AG75-t 2198qq—암막'

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

```
tar -xzf cc_onprem_installer_1.10.0.tar.gz
```

9. 설치 프로그램에서 프롬프트가 표시되면 일련의 프롬프트에 필요한 값을 입력하거나 설치 프로그램에 명령줄 인수로 필요한 매개 변수를 제공할 수 있습니다.



프롬프트가 나타나면 매개 변수를 입력합니다.	전체 명령 입력:
a. 7단계:'SUDO./install.sh -a<account_id> -c<agent_id> -t<token>--darsite'에서 복사한 정보를 붙여 넣습니다 b. Connector 인스턴스에서 액세스할 수 있도록 Data Sense 호스트 시스템의 IP 주소 또는 호스트 이름을 입력합니다. c. Data Sense 인스턴스에서 액세스할 수 있도록 Cloud Manager Connector 호스트 시스템의 IP 주소 또는 호스트 이름을 입력합니다.	또는 필요한 호스트 매개 변수 'sudo./install.sh -a <account_id> -c <agent_id> -t <token>--host <DS_host>--manager-host <cm_host>--no-proxy--dar사이트'를 제공하여 전체 명령을 미리 생성할 수 있습니다

변수 값:

- *ACCOUNT\_ID*= NetApp 계정 ID입니다
- *agent\_id*=커넥터 ID입니다
- *token*= JWT 사용자 토큰
- *DS\_HOST*= Data Sense Linux 시스템의 IP 주소 또는 호스트 이름입니다.
- *cm\_host*= Cloud Manager Connector 시스템의 IP 주소 또는 호스트 이름입니다.

Data Sense 설치 프로그램은 패키지를 설치하고, 설치를 등록하고, Data Sense를 설치합니다. 설치는 10분에서 20분 정도 걸릴 수 있습니다.

호스트 시스템과 Connector 인스턴스 간에 포트 8080을 통해 연결되어 있는 경우 Cloud Manager의 Data Sense 탭에서 설치 진행률을 확인할 수 있습니다.

구성 페이지에서 로컬 을 선택할 수 있습니다 ["온프레미스 ONTAP 클러스터"](#) 및 ["데이터베이스를 지원합니다"](#) 선택합니다.

또한 가능합니다 ["Cloud Data Sense에 대한 BYOL 라이선싱 설정"](#) 현재 Digital Wallet 페이지에서 확인할 수 있습니다. 데이터 양이 1TB를 초과할 때까지 비용이 청구되지 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 Data Sense 소프트웨어를 설치할 때는 다음 단계를 따르십시오.

무엇을 '필요로 할거야

- Manager 및 Scanner 노드의 모든 Linux 시스템이 을 충족하는지 확인합니다 [호스트 요구 사항](#).
- 필수 소프트웨어 패키지 2개(Docker Engine 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 3개의 스캐너 노드(`sudo./install.sh -a <account_id> -c <agent_id> -t <token>--host <DS_host>--manager-host <cm_host> * -n <node_IP1>, <node_IP2>, <node_ip3> * --no-proxy-site`)를 추가합니다

3. 관리자 노드 설치가 완료되기 전에 스캐너 노드에 필요한 설치 명령이 대화 상자에 표시됩니다. 명령을 복사하여 텍스트 파일에 저장합니다. 예를 들면 다음과 같습니다.

'`SUDO./node_install.sh -m 10.11.12.13 -t abcdef-1-3u69m1-1s35212`'를 참조하십시오

4. 커짐 \* 각 \* 스캐너 노드 호스트:
  - a. Data Sense 설치 프로그램 파일(\* `cc_onpremise_installer_<version>.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.

Cloud Data Sense 설치 프로그램이 패키지 설치를 완료하고 설치를 등록합니다. 설치에는 15 ~ 25분이 소요될 수 있습니다.

구성 페이지에서 로컬 을 선택할 수 있습니다 "[온프레미스 ONTAP 클러스터](#)" 및 로컬 "[데이터베이스를 지원합니다](#)" 선택합니다.

또한 가능합니다 "[Cloud Data Sense에 대한 BYOL 라이선싱 설정](#)" 현재 Digital Wallet 페이지에서 확인할 수 있습니다. 데이터 양이 1TB를 초과할 때까지 비용이 청구되지 않습니다.

## 데이터 감지 소프트웨어를 업그레이드합니다

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

### 시작하기 전에

- Data Sense 소프트웨어는 한 번에 하나의 주요 버전으로 업그레이드할 수 있습니다. 예를 들어, 버전 1.9.x가 설치되어 있는 경우 1.10.x로 업그레이드할 수 있습니다. 몇 가지 주요 버전이 뒤쳐지면 소프트웨어를 여러 번 업그레이드해야 합니다.
- 온프레미스 커넥터 소프트웨어가 최신 버전으로 업그레이드되었는지 확인합니다. "[커넥터 업그레이드 단계를 참조하십시오](#)".

### 단계

1. 인터넷 구성 시스템의 경우 에서 클라우드 데이터 감지 소프트웨어를 다운로드합니다 "[NetApp Support 사이트](#)". 선택해야 하는 파일의 이름은 \* DataSense-offline-bundle-<version>.tar.gz \* 입니다.
2. Data Sense가 설치된 Linux 호스트에 소프트웨어 번들을 복사합니다.
3. 호스트 시스템에서 소프트웨어 번들의 압축을 풉니다. 예를 들면 다음과 같습니다.

```
tar -xvf DataSense-offline-bundle-v1.10.0.tar.gz
```

그러면 설치 파일 \* cc\_onpremise\_installer\_<version>.tar.gz \* 가 추출됩니다.

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

```
tar -xzf cc_onprem_installer_1.10.0.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
```

Data Sense 소프트웨어가 호스트에서 업그레이드됩니다. 업데이트는 5분에서 10분 정도 소요될 수 있습니다.

매우 큰 구성을 스캔하기 위해 여러 호스트 시스템에 Data Sense를 구축한 경우 스캐너 노드에는 업그레이드가 필요하지 않습니다.

데이터 감지 UI 페이지 하단에 있는 버전을 확인하여 소프트웨어가 업데이트되었는지 확인할 수 있습니다.

## 데이터 소스에서 스캔을 활성화합니다

## Cloud Volumes ONTAP 및 사내 ONTAP에 대한 클라우드 데이터 센스를 시작하십시오

클라우드 데이터 센스를 사용하여 Cloud Volumes ONTAP 및 온프레미스 ONTAP 볼륨을 스캔하려면 몇 단계를 완료하십시오.

### 빠른 시작

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

볼륨을 스캔하려면 먼저 Cloud Manager에서 시스템을 작업 환경으로 추가해야 합니다.

- Cloud Volumes ONTAP 시스템의 경우, 이러한 작업 환경을 Cloud Manager에서 이미 사용할 수 있어야 합니다
- 사내 ONTAP 시스템의 경우, ["Cloud Manager가 ONTAP 클러스터를 검색해야 합니다"](#)

["클라우드 데이터 센스를 구축하십시오"](#) 이미 배포된 인스턴스가 없는 경우

데이터 감지 \* 를 클릭하고 \* 구성 \* 탭을 선택한 다음 특정 작업 환경의 볼륨에 대한 규정 준수 스캔을 활성화합니다.

이제 Cloud Data Sense가 활성화되었으므로 모든 볼륨에 액세스할 수 있는지 확인하십시오.

- 클라우드 데이터 감지 인스턴스에는 각 Cloud Volumes ONTAP 서버넷 또는 온프레미스 ONTAP 시스템에 대한 네트워크 연결이 필요합니다.
- Cloud Volumes ONTAP의 보안 그룹은 데이터 감지 인스턴스의 인바운드 연결을 허용해야 합니다.
- 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 익스포트 정책은 데이터 감지 인스턴스에서 액세스할 수 있어야 합니다.
- CIFS 볼륨을 검색하려면 Data Sense에 Active Directory 자격 증명이 필요합니다.

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

스캔할 볼륨을 선택하거나 선택 취소하면 Cloud Data Sense에서 스캔을 시작하거나 중지합니다.

### 스캔할 데이터 소스 검색

스캔할 데이터 원본이 Cloud Manager 환경에 없으면 현재 캔버스에 추가할 수 있습니다.

Cloud Volumes ONTAP 시스템은 클라우드 관리자의 Canvas에서 이미 사용 가능해야 합니다. 사내 ONTAP 시스템의 경우 가 있어야 합니다 ["Cloud Manager가 이러한 클러스터를 검색합니다"](#).

### Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 Cloud Volumes ONTAP 및 온-프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행할 수 있습니다 ["클라우드 데이터 센스를 클라우드에 배포합니다"](#) 또는 ["인터넷 액세스가 가능한 사내 위치"](#).

인터넷에 액세스할 수 없는 어두운 사이트에 설치된 온-프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행해야

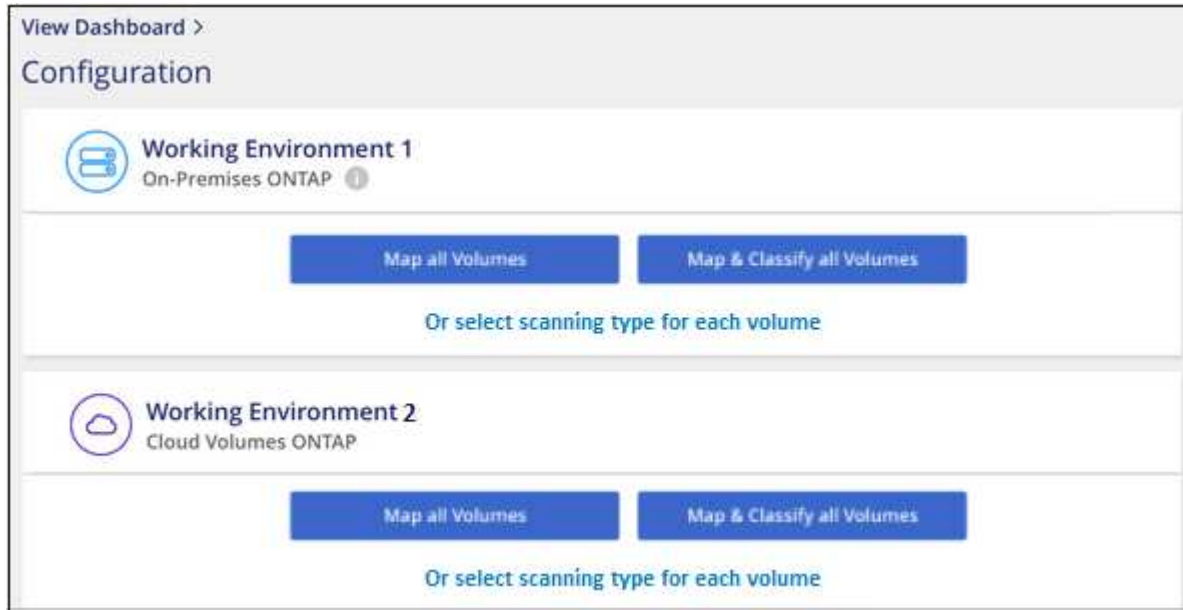
합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

작업 환경에서 클라우드 데이터 센스를 활성화합니다

Cloud Volumes ONTAP 시스템(AWS, Azure 및 GCP) 및 온프레미스 ONTAP 클러스터에서 클라우드 데이터 센스를 활성화할 수 있습니다.

1. Cloud Manager 상단에서 \* 데이터 감지 \* 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 \* Approve \* (승인 \*)를 클릭하여 데이터 센스에서 체적 스캔을 시작하도록 합니다.

Cloud Data Sense는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. Cloud Data Sense에서 초기 스캔을 마치면 Compliance 대시보드에서 결과를 얻을 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

#### Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인

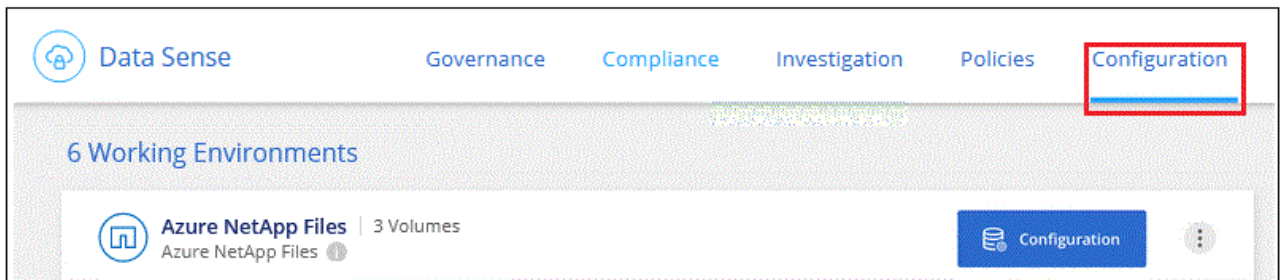
네트워킹, 보안 그룹 및 익스포트 정책을 확인하여 Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인하십시오. CIFS 볼륨에 액세스할 수 있도록 CIFS 자격 증명을 사용하여 데이터 센스를 제공해야 합니다.

단계

1. 클라우드 데이터 감지 인스턴스와 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터용 볼륨이 포함된 각 네트워크 사이에 네트워크 연결이 있는지 확인하십시오.
2. Cloud Volumes ONTAP용 보안 그룹이 데이터 감지 인스턴스의 인바운드 트래픽을 허용하는지 확인합니다.

Data Sense 인스턴스의 IP 주소에서 오는 트래픽에 대한 보안 그룹을 열거나 가상 네트워크 내부의 모든 트래픽에 대한 보안 그룹을 열 수 있습니다.

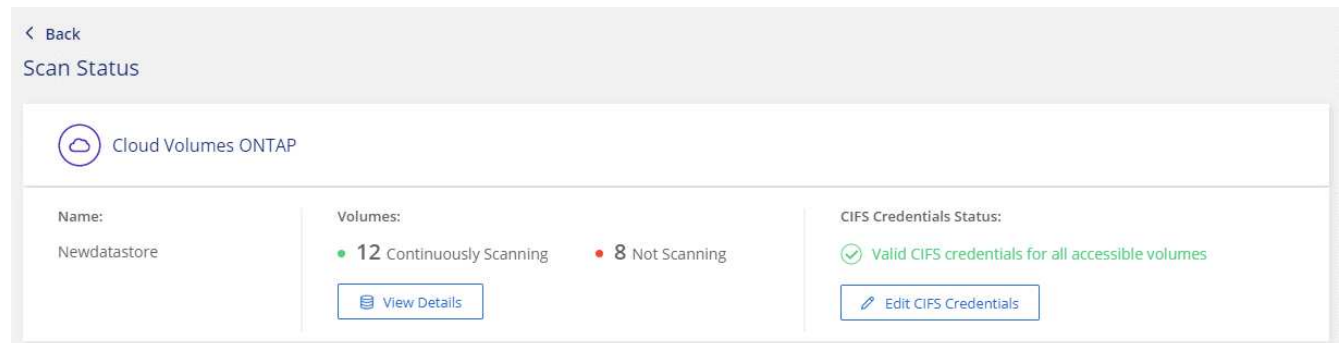
3. 데이터 감지 인스턴스에 대해 다음 포트가 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
4. NFS 볼륨 내보내기 정책에 각 볼륨의 데이터에 액세스할 수 있도록 Data Sense 인스턴스의 IP 주소가 포함되어 있는지 확인합니다.
5. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 센스를 제공합니다.
  - a. Cloud Manager 상단에서 \* 데이터 감지 \* 를 클릭합니다.
  - b. Configuration \* 탭을 클릭합니다.



- c. 각 작업 환경에서 \* CIFS 자격 증명 편집 \* 을 클릭하고 Data Sense가 시스템의 CIFS 볼륨을 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Data Sense에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Data Sense 인스턴스에 저장됩니다.

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 이미지에는 4개의 볼륨이 나와 있습니다. 이 중 하나는 Data Sense 인스턴스와 볼륨 간의 네트워크



연결 문제로 인해 Cloud Data Sense가 스캔할 수 없는 볼륨입니다.

cognitoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

Off

Map

Map & Classify

Custom

Learn about the differences →

Edit CIFS Credentials

Scan	Storage Repository (Volume)	Type	Status	Required Action
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	AdiProtest2501	NFS	Continuously Scanning	
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	AlexTestSecond	NFS	Not Scanning	
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	MoreDataNeed1000	NFS	Continuously Scanning	

## 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.

cognitoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

Off

Map

Map & Classify

Custom

Learn about the differences →

Edit CIFS Credentials

Scan	Storage Repository (Volume)	Type	Status	Required Action
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	AdiProtest2501	NFS	Continuously Scanning	
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	AlexTestSecond	NFS	Not Scanning	
<div>Off</div> <div>Map</div> <div>Map &amp; Classify</div>	MoreDataNeed1000	NFS	Continuously Scanning	

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 Cloud Data Sense에서 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\*.

Scan	Storage Repository (Volume)	Type	Status	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map &amp; Classify"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map &amp; Classify"/>	VolumeName2	NFS	Continuously Scanning	
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map &amp; Classify"/>	VolumeName3	CIFS	Not Scanning	

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. Cloud Data Sense가 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 이미 입력한 경우 해당 자격 증명을 사용하거나 다른 관리자 자격 증명 세트를 지정할 수 있습니다.

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

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

활성화되면 Cloud Data Sense는 스캔을 위해 활성화된 각 DP 볼륨에서 NFS 공유를 생성합니다. 공유 내보내기 정책은 데이터 감지 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 증명에 등록되지 않으므로 DP 볼륨이 검색되지 않습니다.

## Azure NetApp Files용 클라우드 데이터 센스를 시작하십시오

Azure NetApp Files용 클라우드 데이터 센스를 시작하려면 몇 단계를 완료하십시오.

### 빠른 시작

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

Azure NetApp Files 볼륨을 스캔하기 전에 ["구성을 검색하려면 Cloud Manager를 설정해야 합니다"](#).

["Cloud Manager에 클라우드 데이터 센스를 구축하십시오"](#) 이미 배포된 인스턴스가 없는 경우

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

이제 Cloud Data Sense가 활성화되었으므로 모든 볼륨에 액세스할 수 있는지 확인하십시오.

- 클라우드 데이터 감지 인스턴스에는 각 Azure NetApp Files 서브넷에 대한 네트워크 연결이 필요합니다.
- 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 익스포트 정책은 데이터 감지 인스턴스에서 액세스할 수 있어야 합니다.
- CIFS 볼륨을 검색하려면 Data Sense에 Active Directory 자격 증명이 필요합니다.

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

스캔할 볼륨을 선택하거나 선택 취소하면 Cloud Data Sense에서 스캔을 시작하거나 중지합니다.

### 스캔할 Azure NetApp Files 시스템 검색

스캔할 Azure NetApp Files 시스템이 Cloud Manager에 작업 환경으로 설정되어 있지 않으면 현재 캔버스에 추가할 수 있습니다.

["Cloud Manager에서 Azure NetApp Files 시스템을 검색하는 방법을 알아보십시오"](#).

### Cloud Data Sense 인스턴스 구축

["클라우드 데이터 센스를 구축하십시오"](#) 이미 배포된 인스턴스가 없는 경우

Azure NetApp Files 볼륨을 스캔할 때는 클라우드에 데이터 센스를 구축해야 하며 스캔하려는 볼륨과 동일한 영역에 구축해야 합니다.

- 참고: \* Azure NetApp Files 볼륨을 스캔할 때는 현재 사내 위치에 클라우드 데이터 센스를 배포하는 것이 지원되지 않습니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

작업 환경에서 클라우드 데이터 센스를 활성화합니다

Azure NetApp Files 볼륨에서 클라우드 데이터 센스를 활성화할 수 있습니다.

1. Cloud Manager 상단에서 \* 데이터 감지 \* 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 \* Approve \* (승인 \*)를 클릭하여 데이터 센스에서 체적 스캔을 시작하도록 합니다.

Cloud Data Sense는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. Cloud Data Sense에서 초기 스캔을 마치면 Compliance 대시보드에서 결과를 얻을 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

### Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인

네트워킹, 보안 그룹 및 익스포트 정책을 확인하여 Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인하십시오. CIFS 볼륨에 액세스할 수 있도록 CIFS 자격 증명을 사용하여 데이터 센스를 제공해야 합니다.

#### 단계

1. 클라우드 데이터 감지 인스턴스와 Azure NetApp Files용 볼륨이 포함된 각 네트워크 사이에 네트워크 연결이 있는지 확인하십시오.

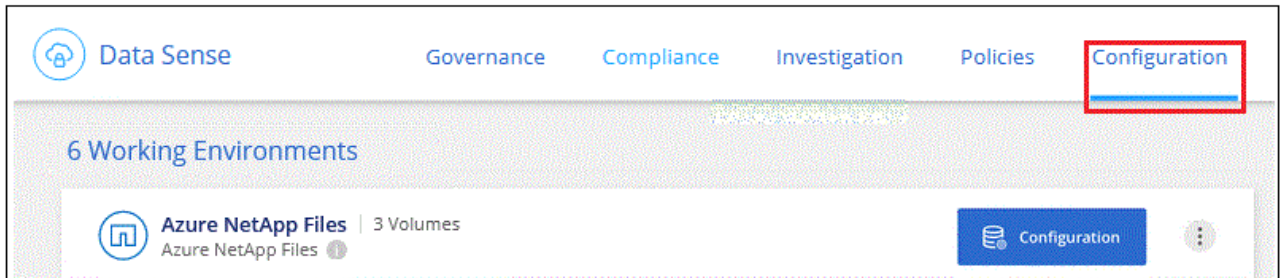


Azure NetApp Files의 경우 클라우드 데이터 감지는 Cloud Manager와 같은 영역에 있는 볼륨만 스캔할 수 있습니다.

2. 데이터 감지 인스턴스에 대해 다음 포트가 열려 있는지 확인합니다.

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

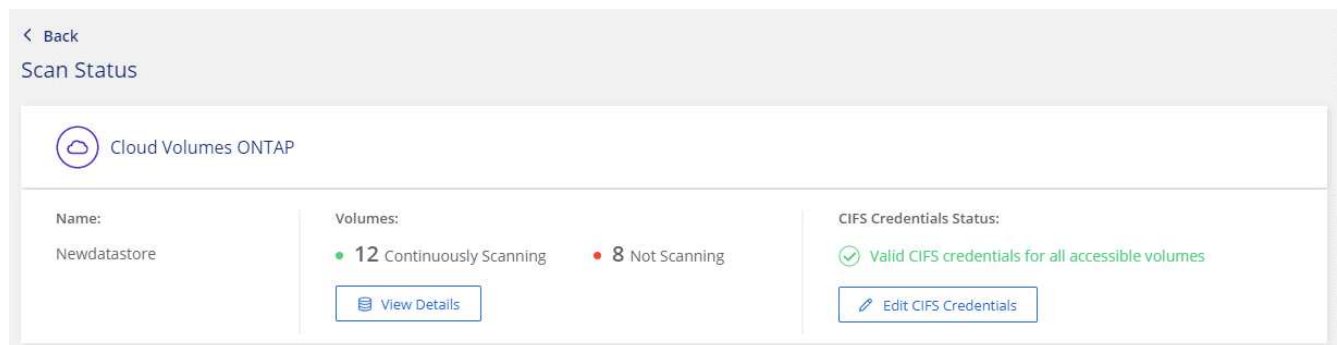
3. NFS 볼륨 내보내기 정책에 각 볼륨의 데이터에 액세스할 수 있도록 Data Sense 인스턴스의 IP 주소가 포함되어 있는지 확인합니다.
4. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 센스를 제공합니다.
  - a. Cloud Manager 상단에서 \* 데이터 감지 \* 를 클릭합니다.
  - b. Configuration \* 탭을 클릭합니다.



- c. 각 작업 환경에서 \* CIFS 자격 증명 편집 \* 을 클릭하고 Data Sense가 시스템의 CIFS 볼륨을 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Data Sense에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Data Sense 인스턴스에 저장됩니다.

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 이미지에는 4개의 볼륨이 나와 있습니다. 이 중 하나는 Data Sense 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 Cloud Data Sense가 스캔할 수 없는 볼륨입니다.

cognigoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map &amp; Classify Custom </div> <a href="#">Learn about the differences →</a> <div>Edit CIFS Credentials</div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning	
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

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.

cognigoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div> Off Map Map &amp; Classify Custom </div> <a href="#">Learn about the differences →</a> <div>Edit CIFS Credentials</div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning	
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning	
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

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 클라우드 데이터 센스를 시작해 보십시오

클라우드 데이터 센스를 사용하여 ONTAP 볼륨에 대한 Amazon FSx 스캔을 시작하려면 몇

단계를 완료하십시오.

시작하기 전에

- 데이터 센스를 구축 및 관리하려면 AWS에 액티브 커넥터가 필요합니다.
- 작업 환경을 생성할 때 선택한 보안 그룹은 Cloud Data Sense 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.

ONTAP 볼륨에 대해 FSx를 스캔하기 전에 ["볼륨이 구성된 FSx 작업 환경이 있어야 합니다"](#).

["Cloud Manager에 클라우드 데이터 센스를 구축하십시오"](#) 이미 배포된 인스턴스가 없는 경우

데이터 감지 \* 를 클릭하고 \* 구성 \* 탭을 선택한 다음 특정 작업 환경의 볼륨에 대한 규정 준수 스캔을 활성화합니다.

이제 Cloud Data Sense가 활성화되었으므로 모든 볼륨에 액세스할 수 있는지 확인하십시오.

- 클라우드 데이터 감지 인스턴스에는 ONTAP 서브넷을 위해 각 FSx에 대한 네트워크 연결이 필요합니다.
- 데이터 감지 인스턴스에 대해 다음 포트가 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 익스포트 정책은 데이터 감지 인스턴스에서 액세스할 수 있어야 합니다.
- CIFS 볼륨을 검색하려면 Data Sense에 Active Directory 자격 증명이 필요합니다. + \* Compliance \* > \* Configuration \* > \* Edit CIFS Credentials \* 를 클릭하고 자격 증명을 입력합니다.

스캔할 볼륨을 선택하거나 선택 취소하면 Cloud Data Sense에서 스캔을 시작하거나 중지합니다.

검사할 **ONTAP** 파일 시스템용 **FSx** 검색

스캔할 ONTAP 파일 시스템용 FSx가 Cloud Manager에 작업 환경으로 설정되어 있지 않은 경우 이 파일을 캔버스에 추가할 수 있습니다.

["Cloud Manager에서 ONTAP 파일 시스템용 FSx를 검색 또는 생성하는 방법을 확인하십시오"](#).

**Cloud Data Sense** 인스턴스 구축

["클라우드 데이터 센스를 구축하십시오"](#) 이미 배포된 인스턴스가 없는 경우

AWS용 커넥터 및 스캔하려는 FSx 볼륨과 동일한 AWS 네트워크에 데이터 센스를 구축해야 합니다.

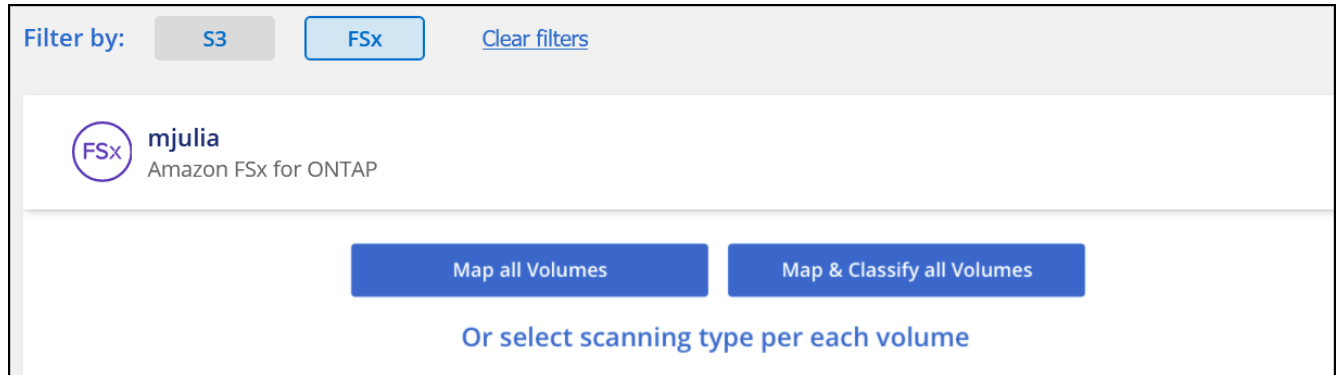
- 참고: \* FSx 볼륨을 스캔할 때는 현재 온-프레미스 위치에 클라우드 데이터 감지 배포를 지원하지 않습니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

작업 환경에서 클라우드 데이터 센스를 활성화합니다

ONTAP 볼륨에 대해 FSx에 대한 클라우드 데이터 센스를 활성화할 수 있습니다.

1. Cloud Manager 상단에서 \* 데이터 감지 \* 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 \* Approve \* (승인 \*)를 클릭하여 데이터 센스에서 체적 스캔을 시작하도록 합니다.

Cloud Data Sense는 작업 환경에서 선택한 볼륨을 스캔하기 시작합니다. Cloud Data Sense에서 초기 스캔을 마치면 Compliance 대시보드에서 결과를 얻을 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

### Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인

네트워킹, 보안 그룹 및 익스포트 정책을 확인하여 Cloud Data Sense가 볼륨에 액세스할 수 있는지 확인하십시오.

CIFS 볼륨에 액세스할 수 있도록 CIFS 자격 증명을 사용하여 데이터 센스를 제공해야 합니다.

단계

1. Configuration\_페이지에서 \* View Details \* 를 클릭하여 상태를 검토하고 오류를 수정합니다.

예를 들어, 다음 이미지는 Data Sense 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 Cloud Data Sense에서 스캔할 수 없는 볼륨을 보여 줍니다.

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off   Map   <b>Map &amp; Classify</b>	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...



- 클라우드 데이터 감지 인스턴스와 ONTAP용 FSx 볼륨을 포함하는 각 네트워크 사이에 네트워크 연결이 있는지 확인합니다.



ONTAP용 FSx의 경우 Cloud Data Sense는 Cloud Manager와 동일한 영역에서만 볼륨을 스캔할 수 있습니다.

- 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- NFS 볼륨 내보내기 정책에 데이터 감지 인스턴스의 IP 주소가 포함되어 각 볼륨의 데이터에 액세스할 수 있는지 확인합니다.
- CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 센스를 제공합니다.
  - Cloud Manager 상단에서 \* 데이터 감지 \* 를 클릭합니다.
  - Configuration \* 탭을 클릭합니다.
  - 각 작업 환경에서 \* CIFS 자격 증명 편집 \* 을 클릭하고 Data Sense가 시스템의 CIFS 볼륨을 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Data Sense에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Data Sense 인스턴스에 저장됩니다.

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.

cognitoWE Scan Configuration					
44/79 Volumes selected for Data Sense scan					
<div> <span>Off</span> <span>Map</span> <span>Map &amp; Classify</span> <span>Custom</span> <a href="#">Learn about the differences →</a> <span>Edit CIFS Credentials</span> </div>					
Scan	Storage Repository (Volume)	Type	Status	Required Action	
<span>Off</span> <span>Map</span> <span>Map &amp; Classify</span>	AdiNFVoI_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...	
<span>Off</span> <span>Map</span> <span>Map &amp; Classify</span>	AdiProtest2501	NFS	Continuously Scanning		
<span>Off</span> <span>Map</span> <span>Map &amp; Classify</span>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...	
<span>Off</span> <span>Map</span> <span>Map &amp; Classify</span>	AlexTestSecond	NFS	Not Scanning		
<span>Off</span> <span>Map</span> <span>Map &amp; Classify</span>	MoreDataNeed1000	NFS	Continuously Scanning		

대상:	방법은 다음과 같습니다.
볼륨에서 매핑 전용 스캔을 활성화합니다	볼륨 영역에서 * Map * 을 클릭합니다
볼륨에서 전체 스캔을 활성화합니다	볼륨 영역에서 * Map & Classify * 를 클릭합니다

대상:	방법은 다음과 같습니다.
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 Cloud Data Sense에서 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\**.

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. Cloud Data Sense가 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 이미 입력한 경우 해당 자격 증명을 사용하거나 다른 관리자 자격 증명 세트를 지정할 수 있습니다.



3. 스캔할 각 DP 볼륨을 활성화합니다 **다른 볼륨을 활성화해도 마찬가지로입니다.**

활성화되면 Cloud Data Sense는 스캔을 위해 활성화된 각 DP 볼륨에서 NFS 공유를 생성합니다. 공유 내보내기 정책은 데이터 감지 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 증명 등록되지 않으므로 DP 볼륨이 검색되지 않습니다.

## Amazon S3에 대한 Cloud Data Sense 시작하기

Cloud Data Sense는 Amazon S3 버킷을 스캔하여 S3 오브젝트 스토리지에 상주하는 개인적이고 민감한 데이터를 식별할 수 있습니다. Cloud Data Sense는 NetApp 솔루션용으로 만든 버킷에 관계없이 고객의 모든 버킷을 스캔할 수 있습니다.

### 빠른 시작

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

IAM 역할 준비 및 데이터 센스에서 S3까지 연결 설정을 포함하여 클라우드 환경이 클라우드 데이터 센스에 대한 요구 사항을 충족할 수 있는지 확인합니다. [전체 목록을 참조하십시오.](#)

["클라우드 데이터 센스를 구축하십시오"](#) 이미 배포된 인스턴스가 없는 경우

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

스캔하려는 버킷을 선택하면 Cloud Data Sense에서 스캔을 시작합니다.

### S3 사전 요구 사항 검토

다음 요구사항은 S3 버킷 스캔에만 적용됩니다.

## Cloud Data Sense 인스턴스에 대해 IAM 역할을 설정합니다

Cloud Data Sense는 계정의 S3 버킷에 연결하고 이를 스캔할 수 있는 권한이 필요합니다. 아래에 나열된 권한을 포함하는 IAM 역할을 설정합니다. Amazon S3 작업 환경에서 Data Sense를 활성화하면 Cloud Manager에서 IAM 역할을 선택하라는 메시지가 표시됩니다.

```
{
  "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/*"
      ]
    }
  ]
}
```

## Cloud Data Sense에서 Amazon S3로 연결할 수 있습니다

클라우드 데이터 센스에 Amazon S3에 대한 연결이 필요합니다. 이 연결을 제공하는 가장 좋은 방법은 VPC 엔드포인트를 통해 S3 서비스로 연결하는 것입니다. 자세한 내용은 [AWS 설명서: 게이트웨이 엔드포인트 생성](#).

VPC 엔드포인트를 생성할 때 Cloud Data Sense 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 데이터 센스를 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 [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.

## Cloud Data Sense 인스턴스 구축

"Cloud Manager에 클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

- 참고: \* S3 버킷을 스캔할 때는 현재 사내 위치에 클라우드 데이터 센스를 구축하는 것이 지원되지 않습니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

## S3 작업 환경에서 데이터 센스를 활성화합니다

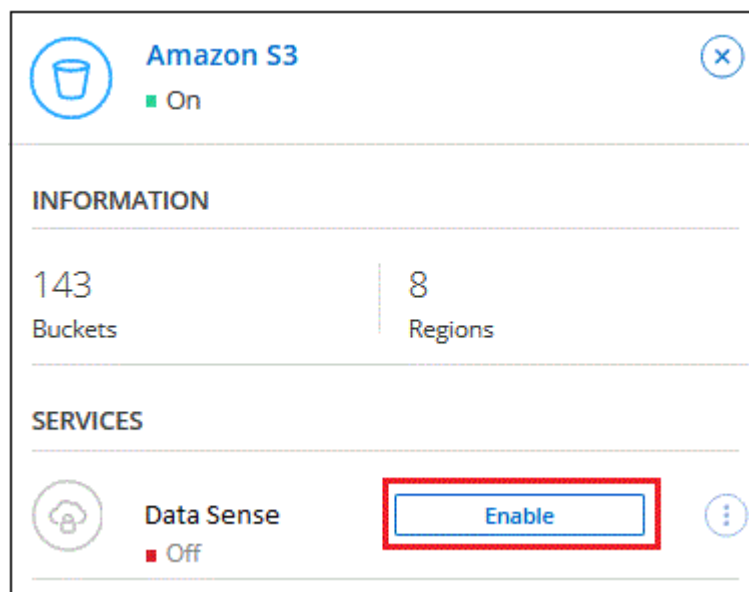
사전 요구 사항을 확인한 후 Amazon S3에서 클라우드 데이터 센스를 활성화합니다.

단계

1. Cloud Manager 상단에서 \* Canvas \* 를 클릭합니다.
2. Amazon S3 작업 환경을 선택합니다.



3. 오른쪽의 데이터 감지 창에서 \* 활성화 \* 를 클릭합니다.



4. 메시지가 표시되면 가 있는 Cloud Data Sense 인스턴스에 IAM 역할을 할당합니다 [필요한 권한](#).

### Assign an AWS IAM Role for Cloud Data Sense

To enable **Cloud Data Sense** on Amazon S3 buckets, select an existing IAM Role.  
Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

occm

#### VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so **Data Sense** can securely scan the data.

Alternatively, ensure that the **Data Sense** instance has direct access to the internet via a NAT Gateway or Internet Gateway.

#### Free for the 1st TB


Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable

Cancel

5. 사용 \* 을 클릭합니다.



를 클릭하여 구성 페이지에서 작업 환경에 대한 규정 준수 검사를 활성화할 수도 있습니다  버튼을 클릭하고 \* 데이터 감지 활성화 \* 를 선택합니다.

Cloud Manager는 IAM 역할을 인스턴스에 할당합니다.

### S3 버킷에서 규정 준수 스캔 활성화 및 비활성화

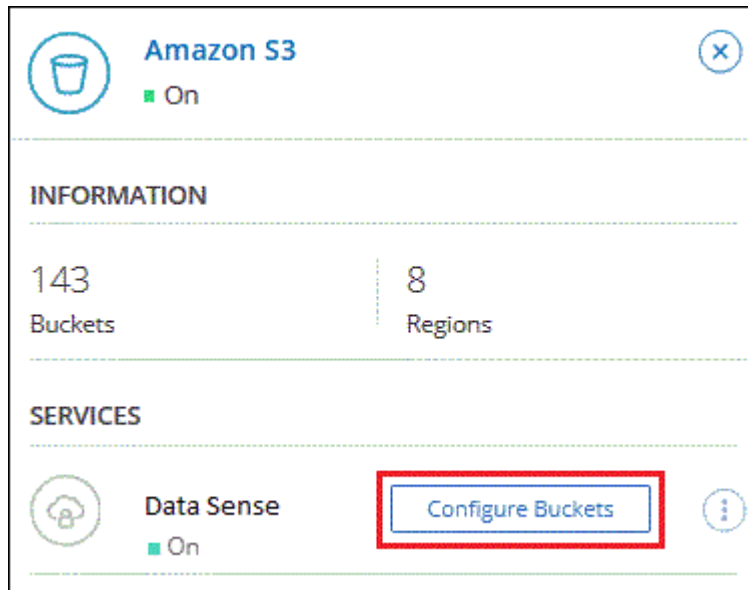
Cloud Manager를 사용하여 Amazon S3에서 Cloud Data Sense를 사용하도록 설정한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다.

Cloud Manager가 검사할 S3 버킷이 있는 AWS 계정에서 실행 중인 경우 해당 버킷을 검색하고 Amazon S3 작업 환경에 표시합니다.

클라우드 데이터 센스도 가능합니다 [서로 다른 AWS 계정에 있는 S3 버킷을 스캔합니다](#).

단계

1. Amazon S3 작업 환경을 선택합니다.
2. 오른쪽 창에서 \* 버킷 구성 \* 을 클릭합니다.



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

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map <b>Map &amp; Classify</b>	BucketName1	Not Scanning	Add Credentials
Off <b>Map</b> Map & Classify	BucketName2	Continuously Scanning	
<b>Off</b> Map Map & Classify	BucketName3	Not Scanning	

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

Cloud Data Sense는 활성화한 S3 버킷을 검색하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

추가 **AWS** 계정에서 버킷 스캔

기존 Cloud Data Sense 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.

## Create role

1

2

3

4


### Select type of trusted entity

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
  - ☐ Require MFA 

다음을 수행하십시오.

- Cloud Data Sense 인스턴스가 있는 계정의 ID를 입력합니다.
- 최대 CLI/API 세션 지속 시간 \* 을 1시간에서 12시간으로 변경하고 변경 사항을 저장합니다.
- Cloud Data Sense IAM 정책을 연결합니다. 필요한 권한이 있는지 확인합니다.

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

2. Data Sense 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 Cloud Data Sense 인스턴스 프로파일 계정이 추가 AWS 계정에 액세스할 수 있습니다.

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



4. Activate Data Sense & Select Bucket \* 을 클릭하고 스캔할 버킷을 선택합니다.

Cloud Data Sense는 사용자가 활성화한 새로운 S3 버킷을 스캔하기 시작합니다.

데이터베이스 스키마를 검색하는 중입니다

클라우드 데이터 센스를 사용하여 데이터베이스 스키마 스캔을 시작하려면 몇 단계를 완료하십시오.



## 빠른 시작

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

데이터베이스가 지원되고 데이터베이스에 연결하는 데 필요한 정보가 있는지 확인합니다.

["클라우드 데이터 센스를 구축하십시오"](#) 이미 배포된 인스턴스가 없는 경우

액세스할 데이터베이스 서버를 추가합니다.

스캔할 스키마를 선택합니다.

## 사전 요구 사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

지원되는 데이터베이스

Cloud Data Sense는 다음 데이터베이스에서 스키마를 검색할 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

Cloud Data Sense 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 Cloud Data Sense 시스템의 전용 사용자를 생성하는 것이 좋습니다.

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

## Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 데이터베이스 스키마를 스캔하는 경우 를 사용할 수 있습니다 "클라우드 데이터 센스를 클라우드에 배포합니다" 또는 "인터넷에 액세스할 수 있는 온프레미스 위치에 데이터 센스를 배포하십시오".

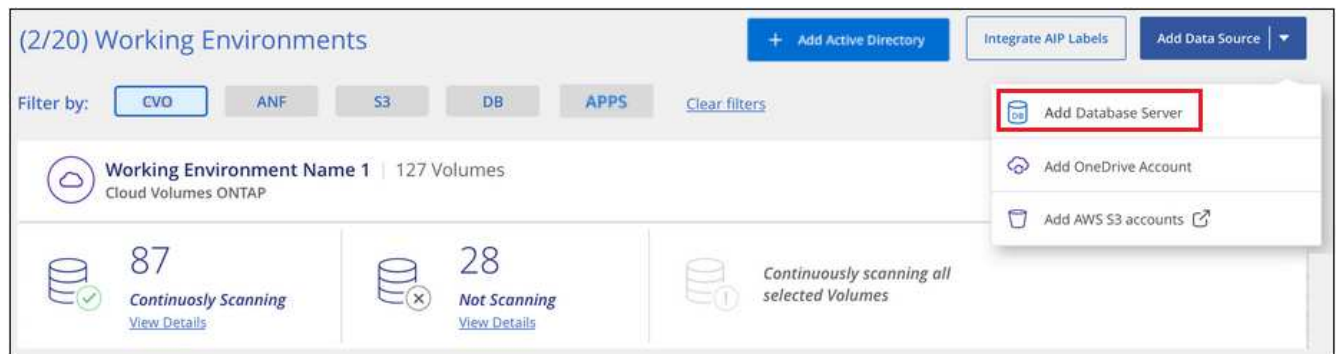
인터넷에 액세스할 수 없는 어두운 사이트에 설치된 데이터베이스 스키마를 스캔하는 경우 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

## 데이터베이스 서버 추가

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. 클라우드 데이터 센스에서 서버에 액세스할 수 있도록 자격 증명을 입력합니다.
  - e. DB 서버 추가 \* 를 클릭합니다.

### Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

#### Database

Database Type	Host Name or IP Address
<input type="text"/>	<input type="text"/>
Port	Service Name
<input type="text"/>	<input type="text"/>

#### Credentials

Username	Password
<input type="text"/>	<input type="text"/>

데이터베이스가 작업 환경 목록에 추가됩니다.

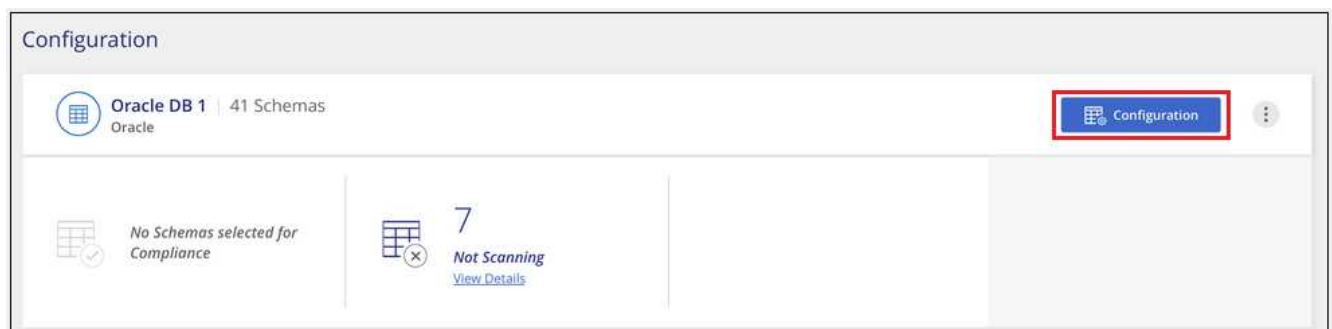
데이터베이스 스키마에서 규정 준수 검사를 활성화 및 비활성화합니다

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.

'Working Environment Name' Configuration			
28/28 Schemas selected for compliance scan		<input type="text"/> <a href="#">Edit Credentials</a>	
Scan	Schema Name	Status	Required Action
<input type="checkbox"/>	DB1 - SchemaName1	Not Scanning	<a href="#">Add Credentials</a>
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

클라우드 데이터 센스가 활성화한 데이터베이스 스키마를 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

## OneDrive 계정 스캔 중

Cloud Data Sense를 사용하여 사용자의 OneDrive 폴더에 있는 파일을 스캔하려면 몇 단계를 완료하십시오.

빠른 시작

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

OneDrive 계정에 로그인할 수 있는 관리자 자격 증명이 있는지 확인합니다.

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

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

## OneDrive 요구 사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

- 모든 사용자 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.

## Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

데이터 센스 가능 "클라우드에 구축" 또는 "인터넷 액세스가 가능한 사내 위치".

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

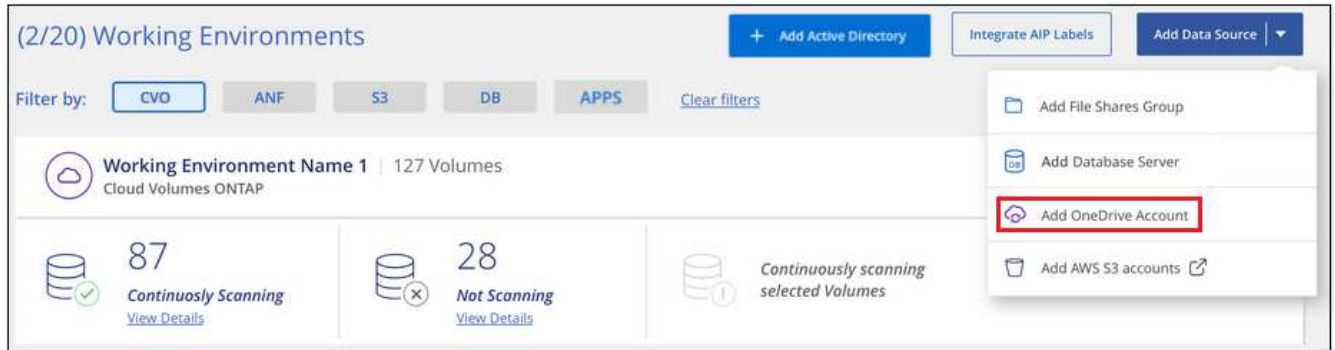
데이터 센스도 가능합니다 "인터넷에 액세스할 수 없는 온프레미스 위치에 배포되었습니다". 하지만 로컬 OneDrive 파일을 검색하려면 몇 개의 선택 끝점에 인터넷 액세스를 제공해야 합니다. "필요한 엔드포인트 목록은 [여기](#) 를 참조하십시오".

## 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. Microsoft 페이지가 나타나면 OneDrive 계정을 선택하고 필요한 관리자 사용자 및 암호를 입력한 다음 \* 수락 \* 을 클릭하여 Cloud Data Sense가 이 계정에서 데이터를 읽을 수 있도록 합니다.

OneDrive 계정이 작업 환경 목록에 추가됩니다.

규정 준수 검사에 **OneDrive** 사용자 추가

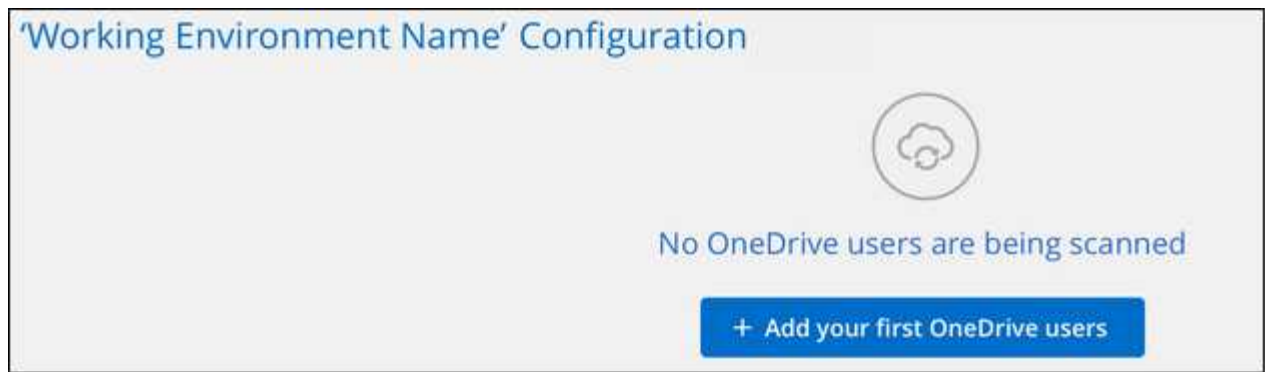
개별 OneDrive 사용자 또는 모든 OneDrive 사용자를 추가하여 Cloud Data Sense에서 파일을 검색할 수 있습니다.

단계

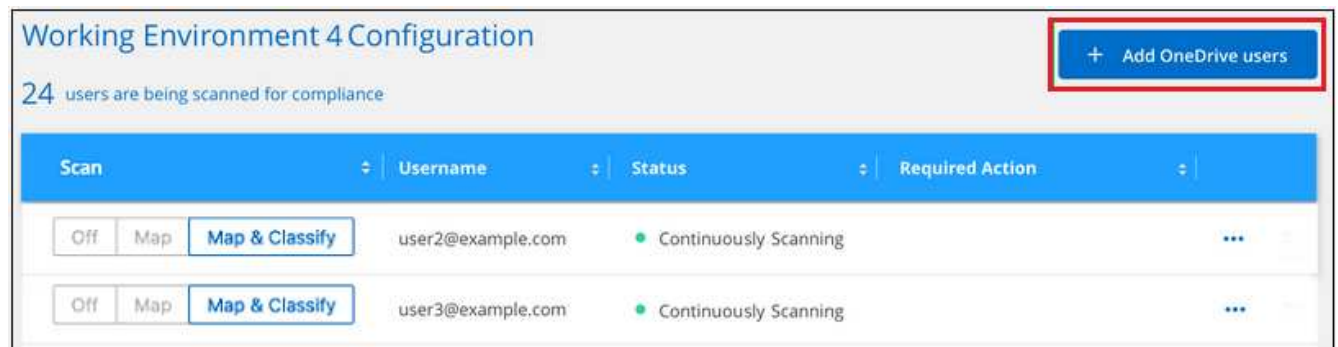
1. Configuration\_ 페이지에서 OneDrive 계정의 \* Configuration \* 버튼을 클릭합니다.



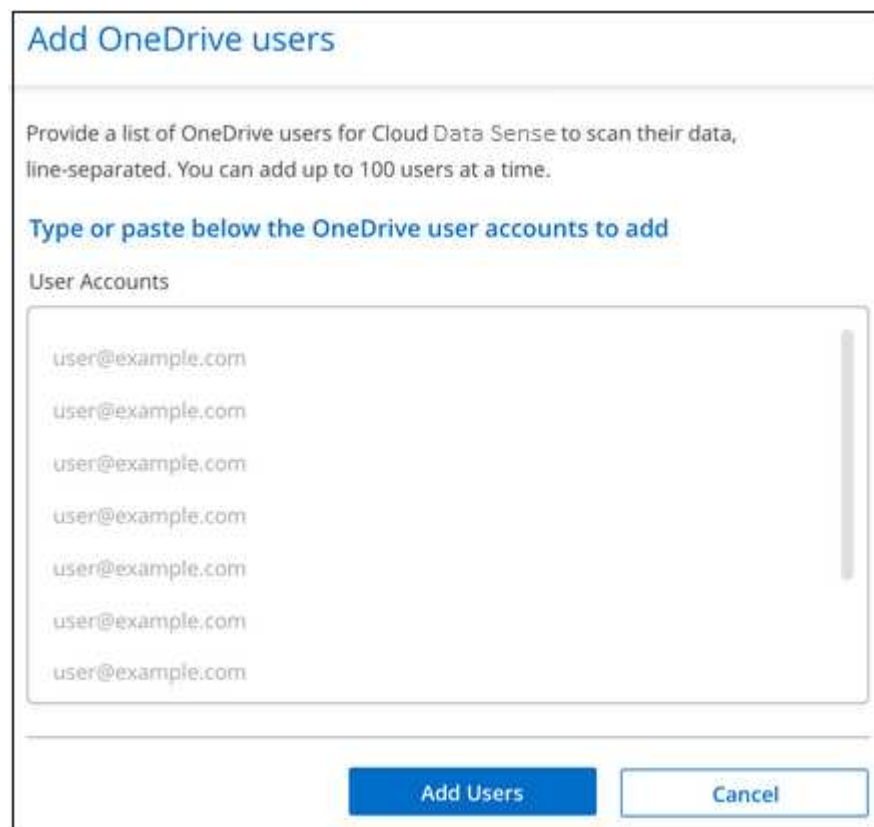
2. 이 OneDrive 계정에 사용자를 처음으로 추가하는 경우 \* 첫 번째 OneDrive 사용자 추가 \* 를 클릭합니다.



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.

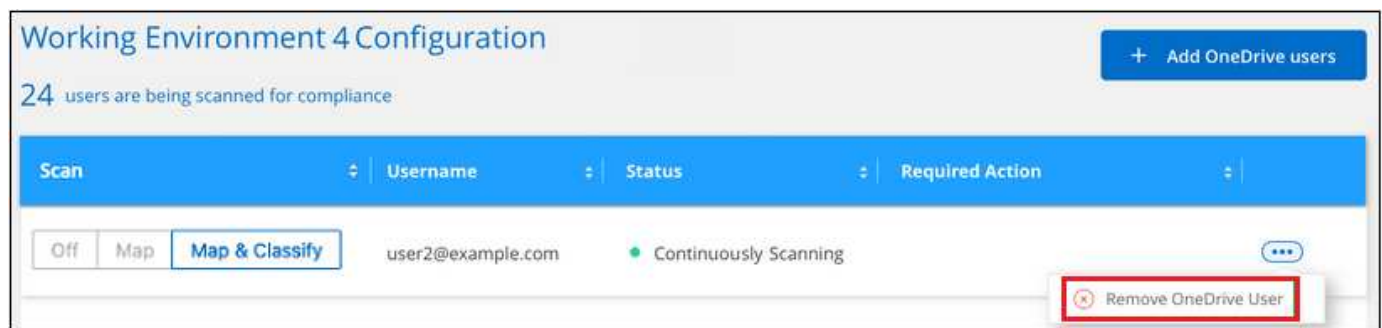
4. 사용자 파일에서 매핑 전용 스캔 또는 매핑 및 분류 스캔을 활성화합니다.

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

Cloud Data Sense는 추가한 사용자의 파일 스캔을 시작하고, 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.



## SharePoint 계정 스캔 중

Cloud Data Sense를 사용하여 SharePoint 계정의 파일 스캔을 시작하려면 몇 단계를 완료하십시오.

빠른 시작

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

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

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

SharePoint 계정에서 검색할 SharePoint 사이트 URL 목록을 추가하고 검색 유형을 선택합니다. 한 번에 최대 100개의 URL을 추가할 수 있습니다.

## SharePoint 요구 사항 검토

다음 필수 구성 요소를 검토하여 SharePoint 계정에서 Cloud Data Sense를 활성화할 준비가 되었는지 확인합니다.



- 모든 SharePoint 사이트에 읽기 권한을 제공하는 SharePoint 계정에 대한 관리자 로그인 자격 증명이 있어야 합니다.
- 검색할 모든 데이터에 대해 SharePoint 사이트 URL의 줄 구분 목록이 필요합니다.

## Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

데이터 센스 가능 ["클라우드에 구축"](#) 또는 ["인터넷 액세스가 가능한 사내 위치"](#).

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

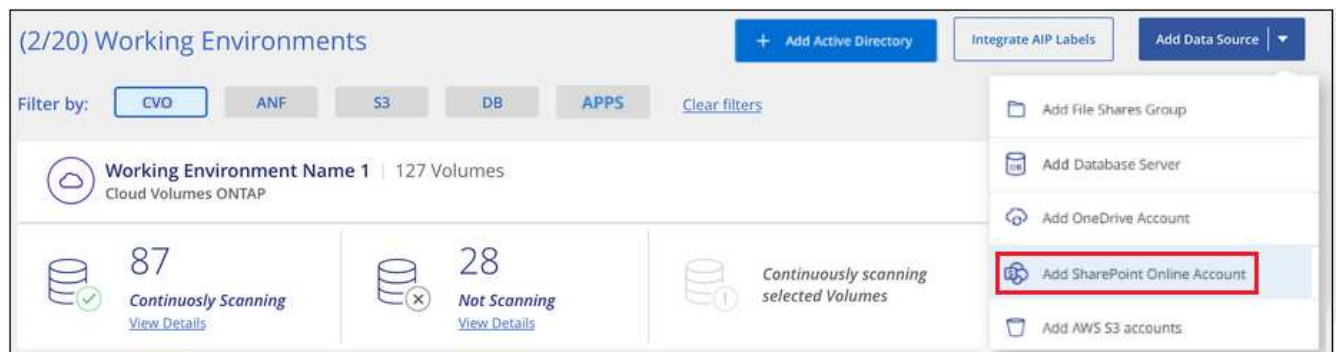
데이터 센스도 가능합니다 ["인터넷에 액세스할 수 없는 온프레미스 위치에 배포되었습니다"](#). 그러나 로컬 SharePoint 파일을 검색하려면 몇 개의 선택 끝점에 인터넷 액세스를 제공해야 합니다. ["필요한 엔드포인트 목록은 여기 를 참조하십시오"](#).

## SharePoint 계정을 추가하는 중입니다

사용자 파일이 있는 SharePoint 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 필요한 관리자 사용자 및 암호를 입력한 다음 \* 수락 \* 을 클릭하여 Cloud Data Sense가 이 계정에서 데이터를 읽을 수 있도록 합니다.

SharePoint 계정이 작업 환경 목록에 추가됩니다.

## 규정 준수 검사에 SharePoint 사이트 추가

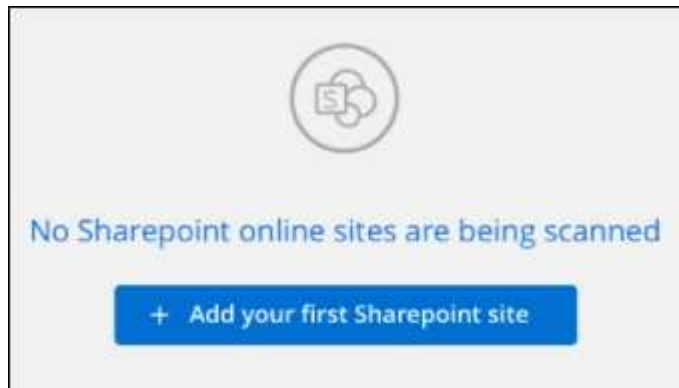
Cloud Data Sense에서 연결된 파일을 검사하도록 개별 SharePoint 사이트 또는 계정의 모든 SharePoint 사이트를 추가할 수 있습니다.

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.

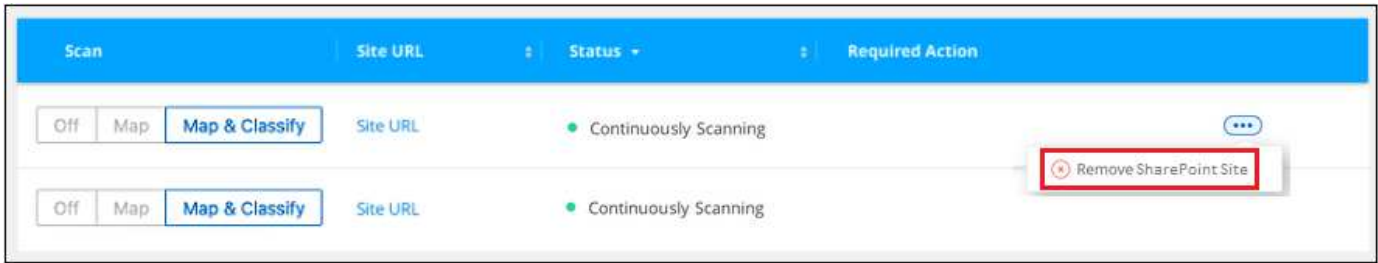
4. SharePoint 사이트의 파일에서 매핑 전용 스캔 또는 매핑 및 분류 검사를 사용하도록 설정합니다.

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

Cloud Data Sense는 추가한 SharePoint 사이트의 파일을 스캔하기 시작하며, 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.



## 파일 공유를 검색하는 중입니다

Cloud Data Sense를 사용하여 NetApp이 아닌 NFS 또는 CIFS 파일 공유 스캔을 시작하려면 몇 가지 단계를 완료하십시오. 이러한 파일 공유는 사내 또는 클라우드에 상주할 수 있습니다.

### 빠른 시작

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

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

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

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

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

### 파일 공유 요구 사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

- 공유는 클라우드 또는 온프레미스 등 어디서나 호스팅할 수 있습니다. 이는 타사 스토리지 시스템에 상주하는 파일 공유입니다.
- Data Sense 인스턴스와 공유 사이에 네트워크 연결이 있어야 합니다.
- 다음 포트가 Data Sense 인스턴스에 열려 있는지 확인합니다.
  - NFS – 포트 111 및 2049의 경우
  - CIFS – 포트 139 및 445의 경우
- '<host\_name>:/<share\_path>' 형식으로 추가하려는 공유 목록이 필요합니다. 공유를 개별적으로 입력하거나 스캔하려는 파일 공유의 라인 분리 목록을 제공할 수 있습니다.
- CIFS(SMB) 공유의 경우 공유에 대한 읽기 액세스를 제공하는 Active Directory 자격 증명이 있는지 확인합니다. Cloud Data Sense에서 상승된 권한이 필요한 데이터를 검색해야 하는 경우 관리자 자격 증명이 선호됩니다.

### Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 비NetApp NFS 또는 CIFS 파일 공유를 스캔하는 경우 다음을 수행할 수 있습니다 "클라우드 데이터 센스를 클라우드에 배포합니다" 또는 "인터넷에 액세스할 수 있는 온프레미스 위치에 데이터 센스를 배포하십시오".

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 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

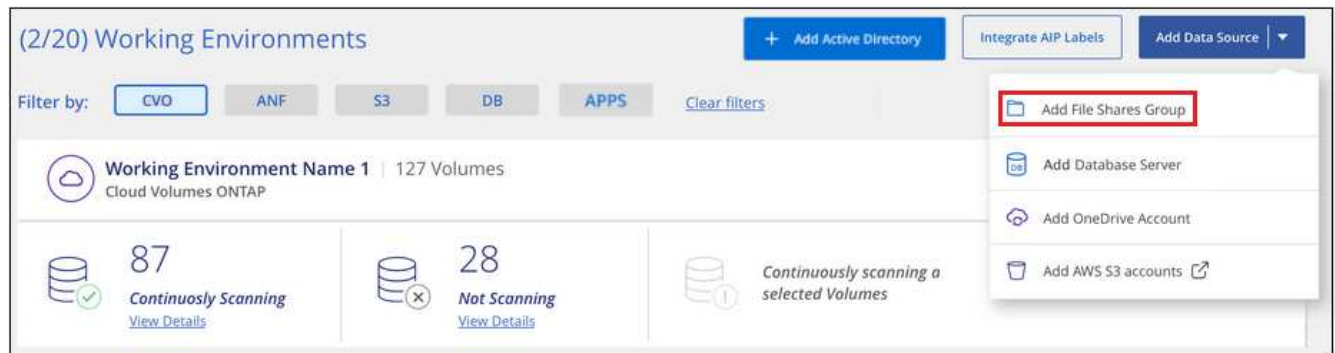
파일 공유에 대한 그룹을 생성하는 중입니다

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 공유를 파일 공유 그룹에 추가하면 해당 공유의 파일이 Cloud Data Sense에 의해 스캔됩니다. '<host\_name>:/<share\_path>' 형식으로 공유를 추가합니다.

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

Cloud Data Sense는 추가한 파일 공유의 파일 스캔을 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

Cloud Data Sense를 사용하여 오브젝트 스토리지 내에서 직접 데이터 스캔을 시작하려면 몇 가지 단계를 완료하십시오. Data Sense는 S3(Simple Storage Service) 프로토콜을 사용하는 오브젝트 스토리지 서비스에서 데이터를 스캔할 수 있습니다. 여기에는 NetApp StorageGRID, IBM Cloud Object Store, Azure Blob(MinIO 사용), Linode, B2 클라우드 스토리지, Amazon S3 등이 포함됩니다.

### 빠른 시작

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

객체 스토리지 서비스에 연결하려면 엔드포인트 URL이 있어야 합니다.

Cloud Data Sense가 버킷에 액세스할 수 있도록 오브젝트 스토리지 공급자로부터 액세스 키 및 비밀 키가 있어야 합니다.

"클라우드 데이터 센스를 구축하십시오" 이미 배포된 인스턴스가 없는 경우

클라우드 데이터 센스에 오브젝트 스토리지 서비스를 추가합니다.

스캔하려는 버킷을 선택하면 Cloud Data Sense에서 스캔을 시작합니다.

### 오브젝트 스토리지의 요구사항 검토

Cloud Data Sense를 활성화하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

- 객체 스토리지 서비스에 연결하려면 엔드포인트 URL이 있어야 합니다.
- 데이터 센스에서 버킷에 액세스할 수 있도록 오브젝트 스토리지 공급자로부터 액세스 키 및 비밀 키가 있어야 합니다.
- Azure Blob을 지원하려면 을 사용해야 합니다 "MinIO 서비스".

### Cloud Data Sense 인스턴스 구축

이미 구축된 인스턴스가 없으면 Cloud Data Sense를 구축하십시오.

인터넷을 통해 액세스할 수 있는 S3 오브젝트 스토리지에서 데이터를 스캔하는 경우 "클라우드 데이터 센스를 클라우드에 배포합니다" 또는 "인터넷에 액세스할 수 있는 온프레미스 위치에 데이터 센스를 배포하십시오".

인터넷에 액세스할 수 없는 어두운 사이트에 설치된 S3 오브젝트 스토리지에서 데이터를 스캔하는 경우, 다음을 수행해야 합니다 "인터넷에 액세스할 수 없는 동일한 사내 위치에 클라우드 데이터 센스를 배포합니다". 또한 Cloud Manager Connector를 동일한 사내 위치에 구축해야 합니다.

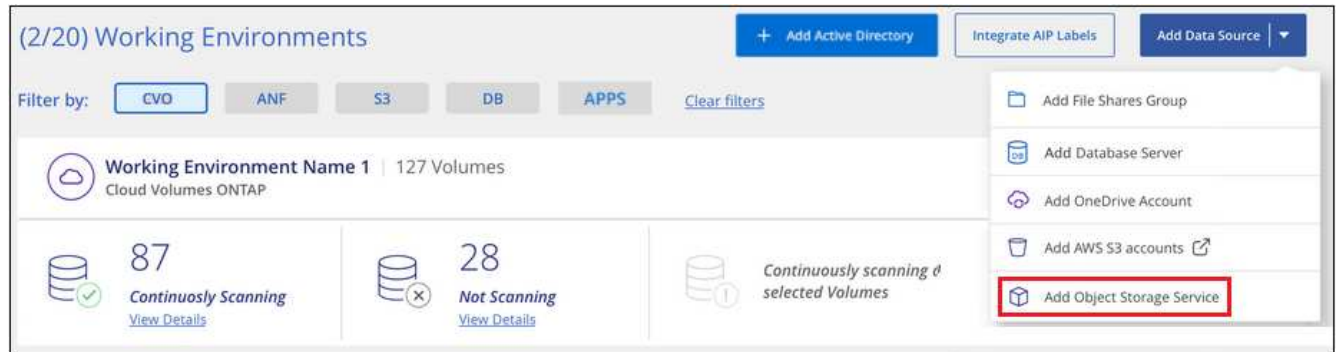
데이터 감지 소프트웨어로 업그레이드하는 것은 인스턴스에 인터넷 연결이 있는 한 자동으로 수행됩니다.

클라우드 데이터 센스에 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. 클라우드 데이터 센스에서 오브젝트 스토리지에 있는 버킷에 액세스할 수 있도록 액세스 키와 비밀 키를 입력합니다.

### Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKDO574NDJG86795"/>	<input type="password" value="....."/>

ContinueCancel

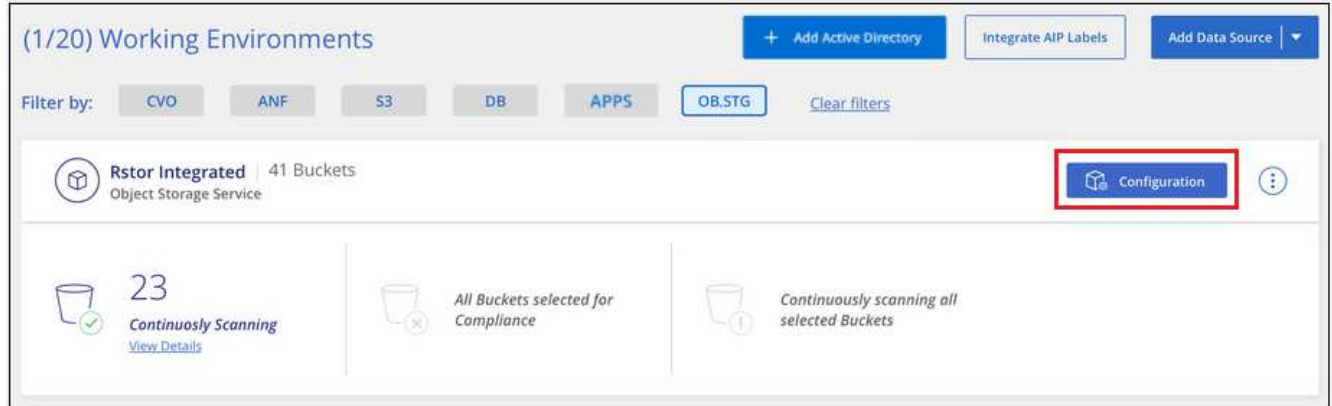
새로운 오브젝트 스토리지 서비스가 작업 환경 목록에 추가됩니다.

## 오브젝트 스토리지 버킷에 대한 규정 준수 검사 설정 및 해제

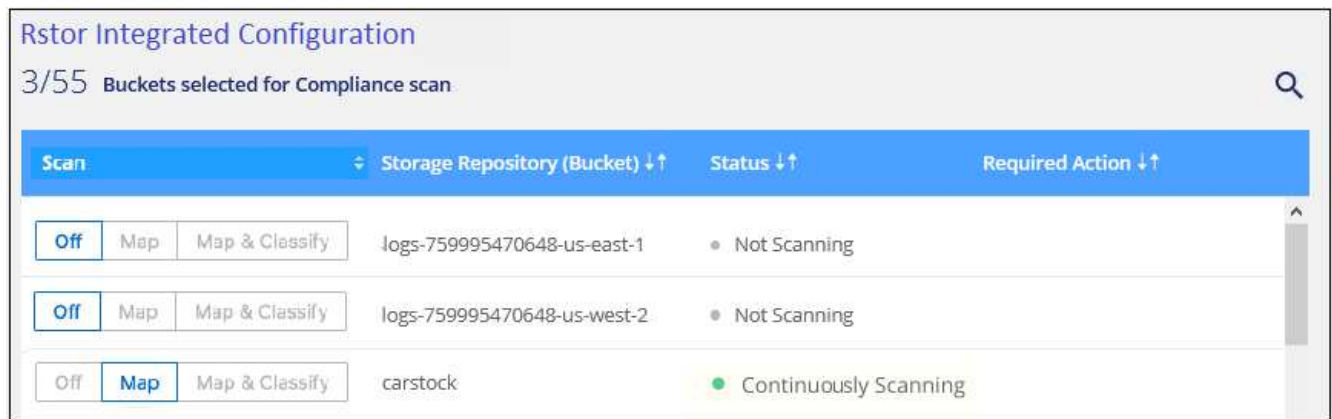
오브젝트 스토리지 서비스에서 클라우드 데이터 센스를 활성화한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다. Data Sense는 이러한 버킷을 검색하여 사용자가 만든 작업 환경에 표시합니다.

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

Cloud Data Sense는 사용자가 활성화한 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 옆에 표시됩니다.

## Active Directory를 클라우드 데이터 센스에 통합합니다

글로벌 Active Directory를 클라우드 데이터 센스와 통합하여 데이터 센스에서 파일 소유자와 파일에 액세스할 수 있는 사용자 및 그룹에 대해 보고하는 결과를 개선할 수 있습니다.

아래에 나열된 특정 데이터 소스를 설정할 때 Data Sense에서 CIFS 볼륨을 스캔하려면 Active Directory 자격 증명을 입력해야 합니다. 이러한 통합은 데이터 소스에 있는 데이터에 대한 파일 소유자 및 사용 권한 세부 정보와 함께 데이터 센스를 제공합니다. 이러한 데이터 원본에 대해 입력한 Active Directory가 여기에 입력한 글로벌 Active Directory 자격 증명과 다를 수 있습니다. 데이터 센스(Data Sense)는 모든 통합 Active Directory에서 사용자 및 권한 세부 정보를 찾습니다.

이러한 통합으로 데이터 센스의 다음 위치에 추가 정보가 제공됩니다.

- "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"** 각 파일에 대해 "모든 권한 보기" 버튼을 클릭합니다.
- 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

Active Directory와 클라우드 데이터 센스를 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 제외)

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

## Active Directory 서버에 연결하는 중입니다

데이터 센스를 배포하고 데이터 소스에서 스캔을 활성화한 후에는 데이터 센스를 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 Data Sense에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Data Sense 인스턴스에 저장됩니다.

### 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

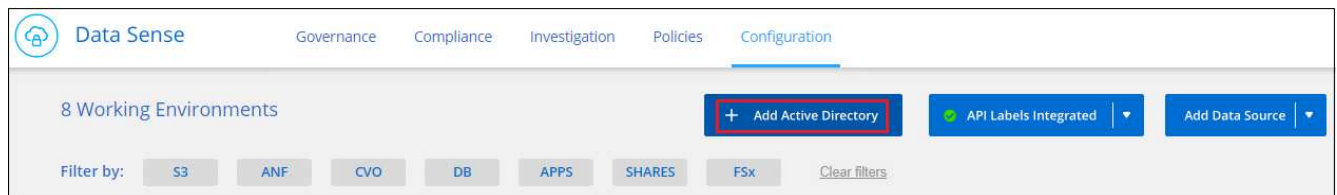
- 사용자 이름 및 암호 를 클릭하여 서버에 액세스합니다

- 도메인 이름(Active Directory 이름)
- 보안 LDAP(LDAPS) 사용 여부
- LDAP 서버 포트(일반적으로 LDAP의 경우 389, 보안 LDAP의 경우 636)
- 다음 포트는 Data Sense 인스턴스에 의한 아웃바운드 통신을 위해 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

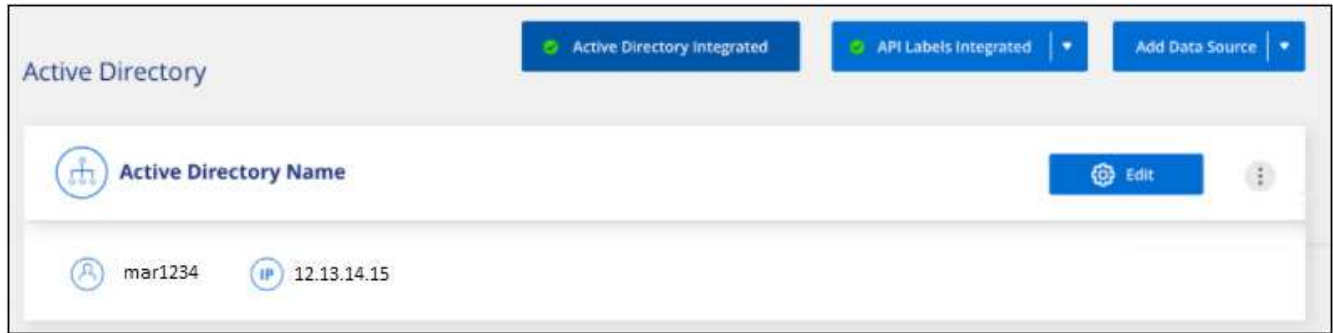
1. 클라우드 데이터 감지 구성 페이지에서 \* Active Directory 추가 \* 를 클릭합니다.



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.

Data Sense는 Active Directory에 통합되며 새 섹션이 구성 페이지에 추가됩니다.



## Active Directory 통합 관리

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.

## 클라우드 데이터 센스에 대한 라이선스 설정

Cloud Manager 작업 공간에서 Cloud Data Sense가 검색하는 첫 번째 1TB의 데이터는 무료입니다. 해당 시점 이후에도 데이터를 계속 스캔하려면 NetApp의 BYOL 라이선스 또는 클라우드 공급자의 Cloud Manager 가입이 필요합니다.

추가 내용을 읽기 전에 몇 가지 참고 사항을 확인하십시오.

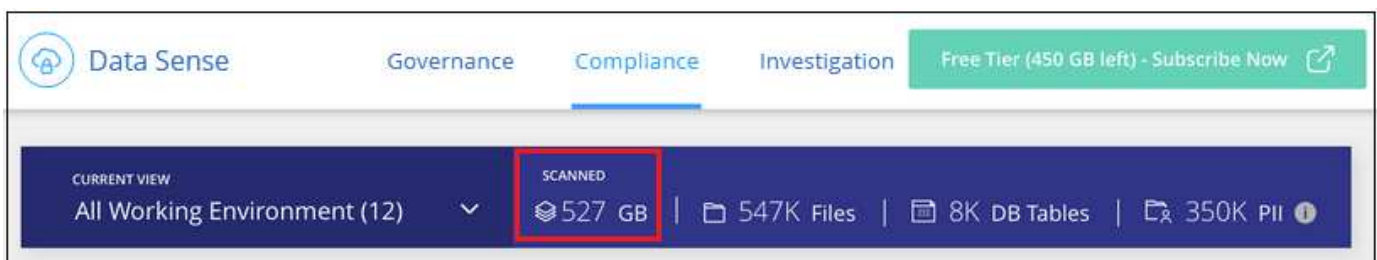
- 클라우드 공급자 마켓플레이스에서 이미 Cloud Manager PAYGO(Pay-as-you-Go) 구독을 구독한 경우 Cloud Data Sense도 자동으로 구독됩니다. 다시 가입하지 않아도 됩니다.
- Cloud Data Sense BYOL(Bring-Your-Own-License)은 스캔할 작업 영역의 모든 작업 환경과 데이터 소스에서 사용할 수 있는 \_floating\_license입니다. 디지털 지갑에 활성 구독이 표시됩니다.

"클라우드 데이터 센스와 관련된 라이선스 및 비용에 대해 자세히 알아보십시오".

## Cloud Data Sense PAYGO 구독을 사용합니다

클라우드 공급자 마켓플레이스에서 용량제 구독을 통해 Cloud Volumes ONTAP 시스템과 클라우드 데이터 센스와 같은 다양한 클라우드 데이터 서비스를 사용할 수 있습니다.

언제든지 구독할 수 있으며 데이터 양이 1TB를 초과할 때까지 요금이 청구되지 않습니다. 항상 데이터 감지 대시보드에서 스캔되는 데이터의 총 양을 볼 수 있습니다. 지금 가입(*Subscribe Now*) 단추를 사용하면 준비가 되면 쉽게 가입할 수 있습니다.





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

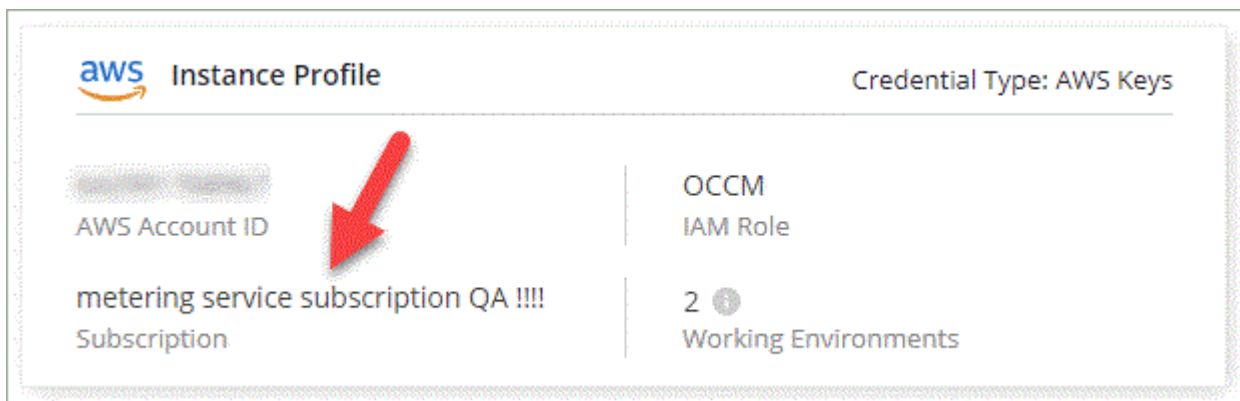
1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.



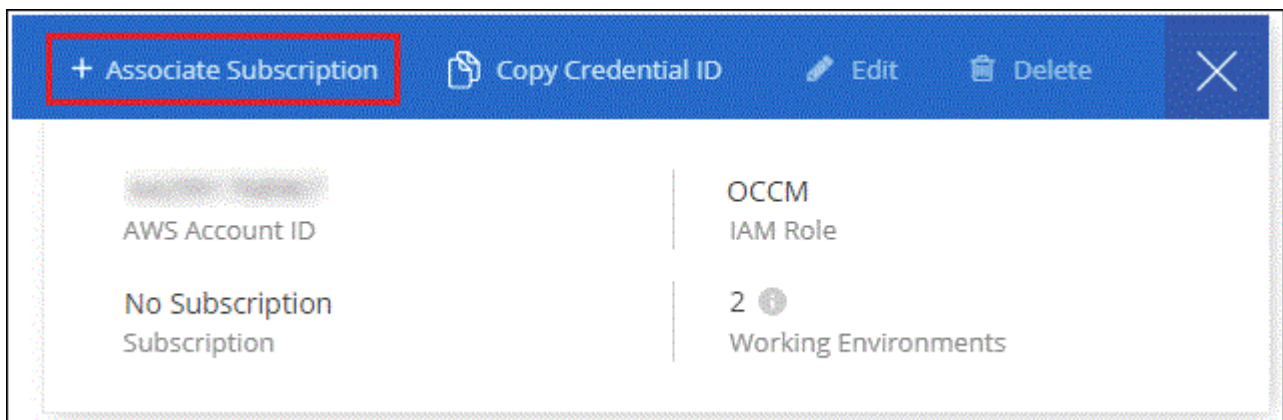
2. AWS 인스턴스 프로필, Azure 관리 서비스 ID 또는 Google Project에 대한 자격 증명을 찾습니다.

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

AWS에 대한 아래 표시된 것처럼 이미 구독을 사용 중인 경우에는 모두 설정된 것이므로 다른 작업은 필요하지 않습니다.



3. 구독이 아직 없는 경우 자격 증명 위에 마우스를 올려 놓고 작업 메뉴를 클릭한 다음 \* 가입 연결 \* 을 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/cloud-manager-data-sense//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/ko-kr/cloud-manager-data-sense//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/cloud-manager-data-sense//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/ko-kr/cloud-manager-data-sense//media/video_subscribing_azure.mp4) (video)



다음 비디오에서는 을 연결하는 방법을 보여줍니다 ["GCP 마켓플레이스" GCP 구독 신청](#):

▶ [https://docs.netapp.com/ko-kr/cloud-manager-data-sense//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/ko-kr/cloud-manager-data-sense//media/video_subscribing_gcp.mp4) (video)

## Cloud Data Sense BYOL 라이선스 사용

NetApp에서 제공하는 자체 라이선스는 1년, 2년 또는 3년간 제공됩니다. BYOL \* Cloud Data Sense \* 라이선스는 전체 용량이 \* 모든 \* 작업 환경 및 데이터 소스 \* 간에 공유되는 \_floating\_license로, 초기 라이선스 등록 및 갱신이 용이합니다.

Cloud Data Sense 라이선스가 없는 경우 다음 연락처로 문의해 주십시오.

- <mailto:ng-contact-data-sense@netapp.com?subject=Licensing> [라이선스 구매를 위해 이메일 보내기].
- Cloud Manager의 오른쪽 하단에 있는 채팅 아이콘을 클릭하여 라이선스를 요청하십시오.

선택적으로 사용하지 않을 Cloud Volumes ONTAP에 대해 할당되지 않은 노드 기반 라이선스가 있는 경우 동일한 달러 당량 및 만료 날짜가 있는 클라우드 데이터 감지 라이선스로 전환할 수 있습니다. ["자세한 내용을 보려면 여기를 클릭하십시오"](#).

Cloud Manager의 Digital Wallet 페이지를 사용하여 Cloud Data Sense BYOL 라이선스를 관리할 수 있습니다. 새 라이선스를 추가하고 기존 라이선스를 업데이트할 수 있습니다.

## Cloud Data Sense 라이선스 파일을 받으십시오

Cloud Data Sense 라이선스를 구입한 후에는 Cloud Data Sense 일련 번호 및 NSS 계정을 입력하거나 NLF 라이선스 파일을 업로드하여 Cloud Manager에서 라이선스를 활성화합니다. 아래 단계에서는 NLF 라이선스 파일을 가져오는 방법을 보여 줍니다(해당 방법을 사용하려는 경우).

인터넷에 액세스할 수 없는 온프레미스 사이트의 호스트에 Cloud Data Sense를 배포한 경우 인터넷에 연결된 시스템에서 라이선스 파일을 얻어야 합니다. 일련 번호 및 NSS 계정을 사용하여 라이선스를 활성화하는 것은 다크 사이트 설치에 사용할 수 없습니다.

단계

1. 에 로그인합니다 ["NetApp Support 사이트"](#) 시스템 > 소프트웨어 라이선스 \* 를 클릭합니다.
2. Cloud Data Sense 라이선스 일련 번호를 입력합니다.

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		SUBS-CLD-DAT-SENSE-TB-2Y	Get NetApp License File		100	12/31/9998

3. 라이선스 키 \* 에서 \* NetApp 라이선스 파일 가져오기 \* 를 클릭합니다.
4. Cloud Manager 계정 ID(지원 사이트에서 테넌트 ID라고 함)를 입력하고 \* 제출 \* 을 클릭하여 라이선스 파일을 다운로드합니다.

**Get License**

SERIAL NUMBER: 4810

LICENSE: SUBS-CLD-DAT-SENSE-TB-2Y

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

[Cancel](#) [Submit](#)

Cloud Manager 상단의 \* Account \* (계정 \*) 드롭다운을 선택한 다음 계정 옆의 \* Manage Account \* 를 클릭하여 Cloud Manager 계정 ID를 찾을 수 있습니다. 계정 ID는 개요 탭에 있습니다.

### Cloud Data Sense BYOL 라이선스를 계정에 추가

Cloud Manager 계정에 대한 Cloud Data Sense 라이선스를 구입한 후 Data Sense 서비스를 사용하려면 Cloud Manager에 라이선스를 추가해야 합니다.

단계

1. 모든 서비스 > 디지털 지갑 > 데이터 서비스 라이선스 \* 를 클릭합니다.
2. 라이선스 추가 \* 를 클릭합니다.
3. Add License\_대화 상자에서 라이선스 정보를 입력하고 \* Add License \* 를 클릭합니다.
  - 데이터 감지 사용권 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 Cloud Manager에 추가합니다"](#).
  - 데이터 감지 라이선스 파일(어두운 사이트에 설치할 때 필요)이 있는 경우 \* 라이선스 파일 업로드 \* 옵션을 선택하고 메시지에 따라 파일을 첨부합니다.

**Add License**

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

☒ Enter Serial Number ☐ Upload License File

Serial Number

NetApp Support Site Account

☐ Enter Serial Number ☒ Upload License File

To install a license, follow these instructions:

- 1 Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- 2 Click Upload File and then select the file.

Upload License File

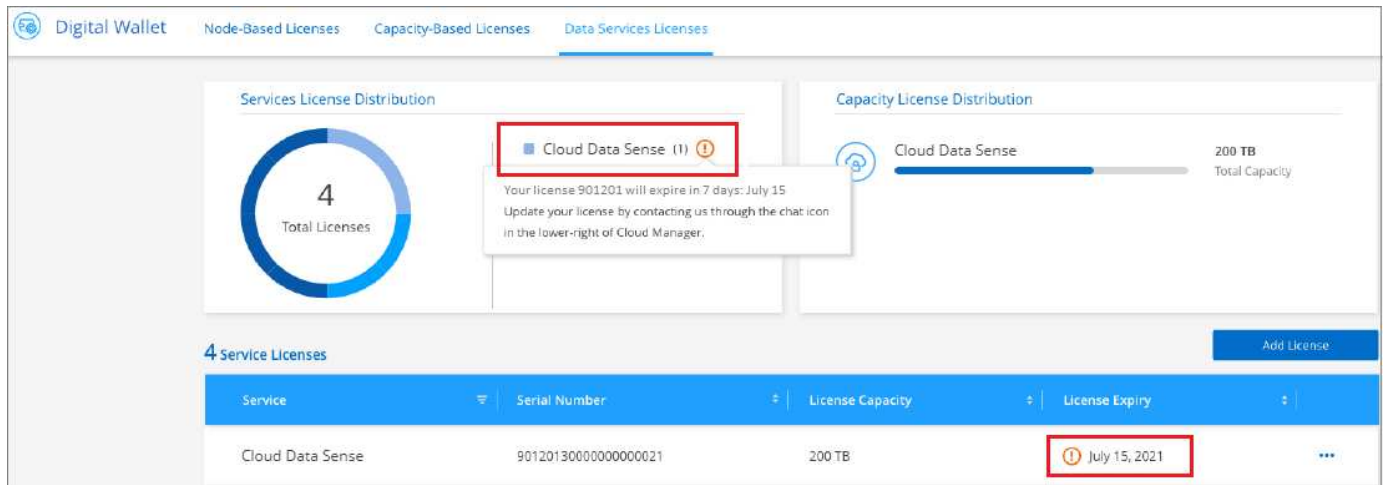
Cloud Manager에서 라이선스를 추가하므로 Cloud Data Sense 서비스가 활성화됩니다.

### Cloud Data Sense BYOL 라이선스 업데이트

라이선스가 부여된 기간이 만료일이 다가오고 있거나 라이선스가 부여된 용량이 한도에 도달한 경우 Cloud Data Sense에서 알림을 받게 됩니다.



이 상태는 디지털 지갑에도 표시됩니다.



Cloud Data Sense 라이선스가 만료되기 전에 업데이트하여 스캔한 데이터에 대한 액세스 중단이 발생하지 않도록 할 수 있습니다.

단계

1. Cloud Manager의 오른쪽 하단에 있는 채팅 아이콘을 클릭하여 특정 일련 번호에 대한 Cloud Data Sense 라이선스에서 기간 연장 또는 추가 용량을 요청합니다. 또한 [라이선스 업데이트를 요청하려면 이메일을 보내십시오](#)를 사용할 수 있습니다.

라이선스 비용을 지불하고 NetApp Support 사이트에 등록된 Cloud Manager는 Digital Wallet의 라이선스를 자동으로 업데이트하며, 데이터 서비스 라이선스 페이지에는 변경 사항이 5~10분 안에 반영됩니다.

2. Cloud Manager에서 라이선스를 자동으로 업데이트할 수 없는 경우(예: 어두운 사이트에 설치된 경우) 라이선스 파일을 수동으로 업로드해야 합니다.
  - a. 가능합니다 [NetApp Support 사이트에서 라이선스 파일을 받으십시오.](#)
  - b. Data Services Licenses\_탭의 Digital Wallet 페이지에서 을 클릭합니다 ... 업데이트하는 서비스 일련 번호에 대해 \* Update License \* 를 클릭합니다.



- c. Update License\_page에서 라이선스 파일을 업로드하고 \* Update License \* 를 클릭합니다.

Cloud Manager가 라이선스를 업데이트하여 Cloud Data Sense 서비스가 계속 활성화될 수 있도록 합니다.

## BYOL 라이선스 고려사항

Cloud Data Sense BYOL 라이선스를 사용하는 경우, 스캔 중인 모든 데이터의 크기가 용량 제한에 근접하거나 라이선스 만료 날짜가 임박한 경우 Cloud Manager는 Data Sense UI 및 Digital Wallet UI에 경고를 표시합니다. 다음과 같은 경고가 표시됩니다.

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

이러한 경고가 표시되면 Cloud Manager 인터페이스 오른쪽 아래에 있는 채팅 아이콘을 사용하여 라이선스를 갱신하십시오.

라이선스가 만료되면 Data Sense는 계속 실행되지만, 스캔된 데이터에 대한 정보를 볼 수 없도록 대시보드에 대한 액세스가 차단됩니다. 라이선스 한도 내에서 용량 사용을 잠재적으로 가져오기 위해 스캔되는 볼륨 수를 줄이려는 경우 *Configuration* 페이지만 사용할 수 있습니다.

BYOL 라이선스를 갱신하면 Cloud Manager가 Digital Wallet에서 라이선스를 자동으로 업데이트하고 모든 대시보드에 대한 모든 액세스를 제공합니다. Cloud Manager가 보안 인터넷 연결을 통해 라이선스 파일에 액세스할 수 없는 경우(예: 어두운 사이트에 설치된 경우) 직접 파일을 얻고 Cloud Manager에 수동으로 업로드할 수 있습니다. 자세한 내용은 [참조하십시오 Cloud Data Sense 라이선스를 업데이트하는 방법.](#)



사용 중인 계정에 BYOL 라이선스와 PAYGO 구독이 모두 있는 경우, BYOL 라이선스가 만료되면 Data Sense\_NOT\_SHIFT가 PAYGO 구독으로 전환됩니다. BYOL 라이선스를 갱신해야 합니다.

# 클라우드 데이터 센스에 관한 FAQ

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

## 클라우드 데이터 센스의 정의

Cloud Data Sense는 인공 지능(AI) 기반 기술을 사용하는 클라우드 오퍼링으로, 조직이 데이터 컨텍스트를 이해하고 스토리지 시스템 전체에서 중요한 데이터를 식별할 수 있도록 도와줍니다. 시스템은 Azure NetApp Files 구성, ONTAP용 Amazon FSx, Cloud Volumes ONTAP 시스템(AWS, Azure 또는 GCP에서 호스팅), Amazon S3 버킷, 온프레미스 ONTAP 시스템일 수 있습니다. 비 NetApp 파일 공유, 일반 S3 오브젝트 스토리지, 데이터베이스, OneDrive 계정 및 SharePoint 계정.

Cloud Data Sense는 GDPR, CCPA, HIPAA 등과 같은 데이터 개인 정보 보호 및 민감도에 대한 새로운 데이터 규정 준수 규정을 해결하기 위해 미리 정의된 매개 변수(예: 중요한 정보 유형 및 범주)를 제공합니다.

## Cloud Data Sense를 사용해야 하는 이유는 무엇입니까?

클라우드 데이터 센스를 통해 다음과 같은 이점을 얻을 수 있습니다.

- 데이터 규정 준수 및 개인정보 보호 규정 준수
- 데이터 보존 정책 준수
- GDPR, CCPA, HIPAA 및 기타 데이터 개인 정보 보호 규정에 따라 데이터 주체에 대응하여 특정 데이터를 쉽게 찾고 보고할 수 있습니다.

## Cloud Data Sense의 일반적인 사용 사례는 무엇입니까?

- 개인 식별 정보(PII)를 식별합니다.
- GDPR 및 CCPA 개인 정보 보호 규정에서 요구하는 광범위한 중요 정보를 식별합니다.
- 새로운 데이터 개인 정보 보호 규정 및 예정된 데이터 개인 정보 보호 규정을 준수합니다.

["클라우드 데이터 센스의 사용 사례에 대해 자세히 알아보십시오."](#)

## Cloud Data Sense를 사용하여 어떤 유형의 데이터를 스캔할 수 있습니까?

Cloud Data Sense는 Cloud Volumes ONTAP, Azure NetApp Files, Amazon FSx for ONTAP, 온프레미스 ONTAP 시스템 및 타사 파일 공유에 의해 관리되는 NFS 및 CIFS 프로토콜을 통한 비정형 데이터 스캔을 지원합니다. Data Sense는 NFS 버전 3.x, 4.0, 4.1 및 CIFS 버전 1.x, 2.0, 2.1 및 3.0을 지원합니다.

또한 Data Sense는 Amazon S3 버킷과 일반 S3 오브젝트 스토리지에 저장된 데이터를 스캔할 수 있습니다.

또한, 데이터 센스를 사용하면 어디서나 있는 데이터베이스와 OneDrive 및 SharePoint 계정의 사용자 파일을 검색할 수 있습니다.

["스캔 작동 방식에 대해 알아보십시오."](#)

## 지원되는 클라우드 공급자는 무엇입니까?

Cloud Data Sense는 Cloud Manager의 일부로 작동하며 AWS, Azure 및 GCP를 지원합니다. 이를 통해 조직은

다양한 클라우드 공급자 전반에서 통합된 개인 정보 보호 가시성을 확보할 수 있습니다.

## 클라우드 데이터 센스에 어떻게 액세스합니까?

Cloud Data Sense는 Cloud Manager를 통해 작동 및 관리됩니다. Cloud Manager의 \* 데이터 감지 \* 탭에서 데이터 감지 기능에 액세스할 수 있습니다.

## Cloud Data Sense는 어떻게 작동합니까?

Cloud Data Sense는 Cloud Manager 시스템 및 스토리지 시스템과 함께 또 다른 인공 지능 계층을 구축합니다. 그런 다음 볼륨, 버킷, 데이터베이스 및 OneDrive 계정의 데이터를 검색하고 검색된 데이터 인사이트를 인덱싱합니다.

["클라우드 데이터 센스의 작동 방식에 대해 자세히 알아보십시오"](#).

## Cloud Data Sense 비용은 얼마입니까?

클라우드 데이터 센스를 사용하는 비용은 스캔하는 데이터의 양에 따라 다릅니다. Cloud Manager 작업 공간에서 Data Sense가 스캔하는 첫 번째 1TB의 데이터는 무료입니다. AWS, Azure 또는 GCP Marketplace에 대한 가입 또는 NetApp의 BYOL 라이선스를 구입해야 하며, 이후 계속해서 데이터를 스캔할 수 있습니다. 을 참조하십시오 ["가격"](#) 를 참조하십시오.

## 클라우드 데이터 센스에 필요한 인스턴스 또는 VM 유형은 무엇입니까?

시기 ["클라우드에 구축"](#):

- AWS에서 Cloud Data Sense는 500GB GP2 디스크가 있는 m5.4x대용량 인스턴스에서 실행됩니다.
- Azure에서 클라우드 데이터 센스(Cloud Data Sense)는 512GB 디스크가 있는 Standard\_D16s\_v3 VM에서 실행됩니다.
- GCP에서 Cloud Data Sense는 512GB의 표준 영구 디스크가 있는 n2-standard-16 VM에서 실행됩니다.

네트워크 또는 클라우드에서 인터넷에 액세스할 수 있는 Linux 호스트에 Data Sense 소프트웨어를 설치할 수 있습니다. 모든 기능이 동일하게 작동하며 Cloud Manager를 통해 스캔 구성과 결과를 지속적으로 관리할 수 있습니다. 을 참조하십시오 ["온프레미스에서 클라우드 데이터 센스를 구축하는 중입니다"](#) 시스템 요구 사항 및 설치 세부 정보를 확인하십시오.

또한, 할 수 있습니다 ["인터넷에 액세스할 수 없는 온프레미스 사이트에 데이터 센스를 구현합니다"](#) 완전히 안전한 사이트를 위한 것입니다.

CPU가 적고 RAM이 적은 시스템에 데이터 센스를 배포할 수 있지만 이러한 시스템을 사용할 때는 한계가 있습니다. 을 참조하십시오 ["더 작은 인스턴스 유형 사용"](#) 를 참조하십시오.

["클라우드 데이터 센스의 작동 방식에 대해 자세히 알아보십시오"](#).

## Cloud Data Sense는 내 데이터를 얼마나 자주 스캔합니까?

데이터는 자주 변경되므로 Cloud Data Sense는 데이터에 영향을 주지 않고 데이터를 지속적으로 검색합니다. 초기 데이터 스캔에는 시간이 오래 걸릴 수 있지만 후속 스캔에서는 증분 변경 사항만 스캔하므로 시스템 스캔 시간이 줄어듭니다.

["스캔 작동 방식에 대해 알아보십시오"](#).

데이터 스캔은 스토리지 시스템과 데이터에 경미한 영향을 줍니다. 그러나 아주 작은 충격에도 신경 쓰면 데이터 센스를 구성하여 "느린" 스캔을 수행할 수 있습니다. ["스캔 속도를 줄이는 방법을 참조하십시오"](#).

## 클라우드 데이터 센스에서 보고서를 제공합니까?

예. Cloud Data Sense에서 제공하는 정보는 조직의 다른 이해 관계자와 관련이 있을 수 있으므로 보고서를 생성하여 통찰력을 공유할 수 있습니다.

데이터 센스에 사용할 수 있는 보고서는 다음과 같습니다.

### 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 식별자에 관한 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"](#).

### 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 ["클라우드 데이터 감지 인스턴스"](#) 및 ["클라우드 데이터 센스를 구축하는 중입니다"](#) 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"](#).

## 지원되는 파일 유형은 무엇입니까?

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

데이터 센스에서 PII(개인 식별 정보)를 감지하거나 DSAR 검색을 수행할 때 .csv, .dcm, .dicom, .DOC, .DOCX, .JSON, .pdf, .PPTX, .rtf, .TXT, XLS 및 .XLSX.



## 클라우드 데이터 센스를 활성화하려면 어떻게 해야 하나요?

먼저 Cloud Manager에 Cloud Data Sense의 인스턴스를 배포해야 합니다. 인스턴스가 실행 중이면 \* Data Sense \* 탭에서 기존 작업 환경 및 데이터베이스에 대한 서비스를 활성화하거나 특정 작업 환경을 선택할 수 있습니다.

"시작하는 방법을 알아보십시오".



클라우드 데이터 센스를 활성화하면 즉시 초기 스캔이 됩니다. 스캔 결과는 잠시 후에 표시됩니다.

## 클라우드 데이터 센스를 비활성화하려면 어떻게 해야 하나요?

데이터 감지 구성 페이지에서 개별 작업 환경, 데이터베이스, 파일 공유 그룹, OneDrive 계정 또는 SharePoint 계정을 검색할 때 Cloud Data Sense를 사용하지 않도록 설정할 수 있습니다.

"자세한 정보".



Cloud Data Sense 인스턴스를 완전히 제거하려면 클라우드 공급자의 포털 또는 사내 위치에서 Data Sense 인스턴스를 수동으로 제거해야 합니다.

## ONTAP 볼륨에서 데이터 계층화가 활성화된 경우 어떻게 됩니까?

콜드 데이터를 오브젝트 스토리지에 계층화하는 ONTAP 시스템에서 클라우드 데이터 센스를 활성화할 수도 있습니다. 데이터 계층화가 활성화된 경우 데이터 센스(Data Sense)는 디스크에 있는 데이터와 오브젝트 스토리지에 대한 콜드 데이터 등 모든 데이터를 검색합니다.

규정 준수 검사에서는 콜드 데이터를 가열하지 않으며 오브젝트 스토리지까지 차갑게 유지됩니다.

## 클라우드 데이터 센스를 사용하여 사내 ONTAP 스토리지를 스캔할 수 있습니까?

예. Cloud Manager에서 사내 ONTAP 클러스터를 작업 환경으로 검색한 경우 볼륨 데이터를 검색할 수 있습니다.

## Cloud Data Sense는 내 조직에 알림을 전송할 수 있습니까?

예. 정책 기능과 함께 정책이 결과를 반환할 때 Cloud Manager 사용자(매일, 매주 또는 매월)에게 이메일 경고를 보내 데이터를 보호하기 위한 알림을 받을 수 있습니다. 예 대해 자세히 알아보십시오 "정책".

또한 조직에서 내부적으로 공유할 수 있는 관리 페이지 및 조사 페이지에서 상태 보고서를 다운로드할 수도 있습니다.

## 조직의 요구에 맞게 서비스를 사용자 정의할 수 있습니까?

클라우드 데이터 센스를 통해 즉각적인 데이터 인사이트를 얻을 수 있습니다. 이러한 통찰력을 추출하여 조직의 요구에 활용할 수 있습니다.

또한 \* Data Fusion \* 기능을 사용하여 스캔 중인 데이터베이스의 특정 열에 있는 기준에 따라 데이터 센스를 통해 모든 데이터를 검색할 수 있습니다. 기본적으로 사용자 지정 개인 데이터 유형을 만들 수 있습니다.

"자세한 정보".

## Cloud Data Sense는 내 파일에 포함된 AIP 레이블과 함께 사용할 수 있습니까?

예. 구독한 경우 Cloud Data Sense에서 검색 중인 파일에서 AIP 레이블을 관리할 수 있습니다 "[AIP\(Azure Information Protection\)](#)". 파일에 이미 할당된 레이블을 보고, 파일에 레이블을 추가하고, 기존 레이블을 변경할 수 있습니다.

["자세한 정보"](#).

## 클라우드 데이터 감지 정보를 특정 사용자로 제한할 수 있습니까?

예, Cloud Data Sense는 Cloud Manager와 완벽하게 통합됩니다. Cloud Manager 사용자는 작업 영역 권한에 따라 볼 수 있는 작업 환경에 대한 정보만 볼 수 있습니다.

또한 특정 사용자가 데이터 감지 설정을 관리할 수 없는 상태에서 데이터 감지 스캔 결과만 볼 수 있도록 하려면 해당 사용자에게 \_Cloud Compliance Viewer\_ 역할을 할당할 수 있습니다.

["자세한 정보"](#).

## Copyright Information

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

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

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

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

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

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

## Trademark Information

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