



개인정보 데이터 보호 파악

Cloud Manager 3.8

NetApp
March 25, 2024

목차

개인정보 데이터 보호 파악	1
클라우드 규정 준수에 대해 알아보십시오	1
시작하십시오	5
프라이빗 데이터에 대한 가시성 및 제어 확보	27
준수 보고서 보기	40
데이터 주체 액세스 요청에 응답	45
클라우드 규정 준수 비활성화	47
클라우드 규정 준수에 대한 FAQ	48

개인정보 데이터 보호 파악

클라우드 규정 준수에 대해 알아보십시오

Cloud Compliance는 Cloud Manager의 데이터 개인 정보 보호 및 규정 준수 서비스로, 볼륨, Amazon S3 버킷 및 데이터베이스를 스캔하여 이러한 파일에 상주하는 개인적이고 민감한 데이터를 식별합니다. Cloud Compliance는 인공 지능(AI) 기반 기술을 사용하여 조직의 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있도록 지원합니다.

["클라우드 규정 준수의 사용 사례에 대해 알아보십시오"](#).

피처

Cloud Compliance는 규정 준수 노력을 지원할 수 있는 여러 가지 툴을 제공합니다. 클라우드 규정 준수를 통해 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

지원되는 작업 환경 및 데이터 소스

Cloud Compliance는 다음 유형의 데이터 소스에서 데이터를 스캔할 수 있습니다.

- AWS의 Cloud Volumes ONTAP
- Azure의 Cloud Volumes ONTAP
- Azure NetApp Files
- Amazon S3
- 데이터베이스가 어디에나 상주하는 데이터베이스(데이터베이스가 작업 환경에 상주할 필요는 없음)
- 참고: * Azure NetApp Files의 경우 Cloud Compliance는 Cloud Manager와 동일한 지역에 있는 모든 볼륨을 스캔할 수 있습니다.

비용

- Cloud Compliance 사용 비용은 스캔 중인 데이터의 양에 따라 다릅니다. 2020년 10월 7일 현재 Cloud Manager 작업 공간에서 Cloud Compliance에서 스캔하는 첫 번째 1TB의 데이터는 무료입니다. 여기에는 Cloud Volumes ONTAP 볼륨, Azure NetApp Files 볼륨, Amazon S3 버킷 및 데이터베이스 스키마의 데이터가 포함됩니다. AWS 또는 Azure Marketplace에 가입해야 해당 시점 이후에 데이터를 계속 스캔할 수 있습니다. 을 참조하십시오 ["가격"](#) 를 참조하십시오.

["구독 방법을 알아보십시오"](#).

- Cloud Compliance를 설치하려면 클라우드 인스턴스를 구축해야 하는데, 클라우드 인스턴스가 배포된 클라우드 공급자가 이를 청구합니다. 를 참조하십시오 [각 클라우드 공급자에 대해 구축된 인스턴스 유형입니다](#)
- Cloud Compliance는 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"](#).

데이터 전송 비용

데이터 전송 비용은 설정에 따라 다릅니다. 클라우드 규정 준수 인스턴스 및 데이터 소스가 동일한 가용성 영역 및 지역에 있는 경우 데이터 전송 비용이 발생하지 않습니다. 하지만 Cloud Volumes ONTAP 클러스터 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"](#)

클라우드 규정 준수 방식

높은 수준에서 클라우드 규정 준수는 다음과 같이 작동합니다.

1. Cloud Manager에서 Cloud Compliance 인스턴스를 구축합니다.
2. 하나 이상의 작업 환경 또는 데이터베이스에서 이 기능을 사용하도록 설정합니다.
3. Cloud Compliance는 AI 학습 프로세스를 사용하여 데이터를 스캔합니다.
4. Cloud Manager에서 * Compliance * 를 클릭하고 제공된 대시보드 및 보고 툴을 사용하여 규정 준수 작업을 지원합니다.

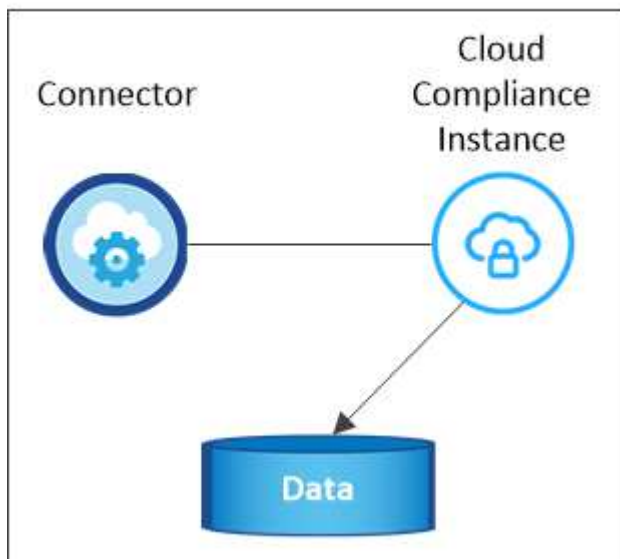
클라우드 규정 준수 인스턴스

Cloud Compliance를 활성화하면 Cloud Manager가 Connector와 동일한 서브넷에 Cloud Compliance 인스턴스를 구축합니다. ["커넥터에 대해 자세히 알아보십시오."](#)



Connector가 내부에 설치된 경우, 요청에 첫 번째 Cloud Volumes ONTAP 시스템과 동일한 VPC 또는 VNET에 클라우드 규정 준수 인스턴스를 배포합니다.

VPC or VNet



인스턴스에 대한 다음 사항에 유의하십시오.

- Azure에서 클라우드 규정 준수는 512GB 디스크가 있는 Standard_D16s_v3 VM에서 실행됩니다.
- AWS에서 Cloud Compliance는 500GB GP2 디스크를 사용하는 m5.4x대용량 인스턴스에서 실행됩니다.

m5.4x4Large를 사용할 수 없는 지역에서는 Cloud Compliance가 대신 m4.4x4대형 인스턴스에서 실행됩니다.



인스턴스/VM 유형의 변경 또는 크기 조정은 지원되지 않습니다. 제공된 크기를 사용해야 합니다.

- 인스턴스의 이름은 *CloudCompliance_*이며 생성된 해시(*UUID*)와 연결됩니다. 예: *_CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Connector당 하나의 Cloud Compliance 인스턴스만 배포됩니다.
- 클라우드 규정 준수 소프트웨어 업그레이드는 자동화되어 있으므로 걱정할 필요가 없습니다.



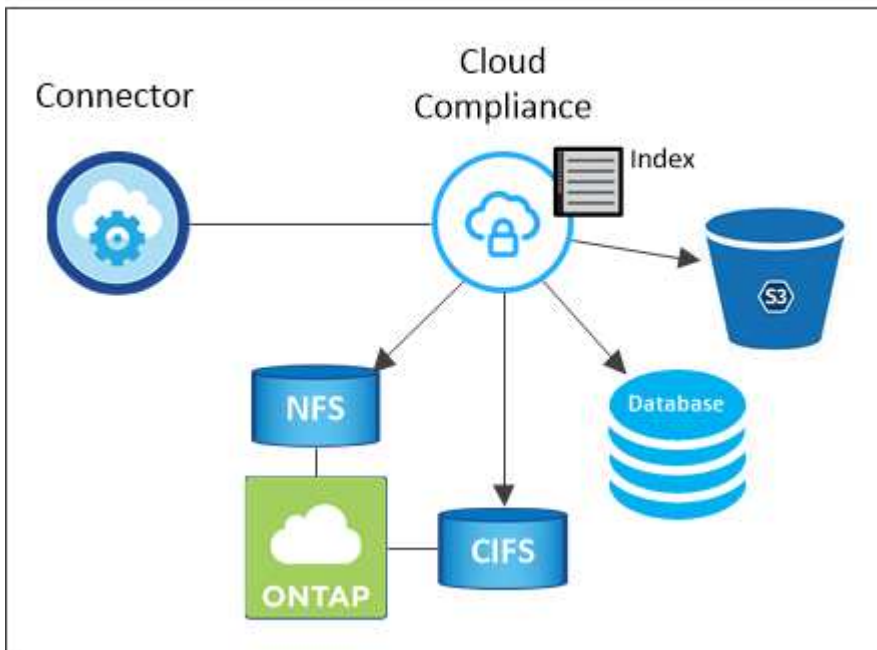
Cloud Compliance는 지속적으로 데이터를 스캔하기 때문에 인스턴스는 항상 실행 상태를 유지해야 합니다.

스캔 작동 방식

Cloud Compliance를 활성화하고 스캔할 볼륨, 버킷 또는 데이터베이스 스키마를 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 및 데이터 범주의 인덱스입니다.

Cloud Compliance는 NFS 및 CIFS 볼륨을 마운트하여 다른 클라이언트와 같은 데이터에 연결합니다. CIFS 볼륨을 스캔하려면 Active Directory 자격 증명을 제공해야 하지만 NFS 볼륨은 읽기 전용으로 자동 액세스됩니다.

VPC or VNet



초기 스캔 후 Cloud Compliance는 각 볼륨을 지속적으로 검사하여 증분 변경 사항을 감지합니다(인스턴스 실행을 유지하는 것이 중요한 이유).

에서 스캔을 활성화 및 비활성화할 수 있습니다 ["볼륨 레벨"](#), 에서 ["버킷 수평"](#), 및 에 있습니다 ["데이터베이스 스키마 수준입니다"](#).

Cloud Compliance에서 인덱싱하는 정보입니다

Cloud Compliance는 비정형 데이터(파일)에 범주를 수집, 인덱스 및 할당합니다. Cloud Compliance가 인덱싱하는 데이터에는 다음이 포함됩니다.

표준 메타데이터

Cloud Compliance는 파일 유형, 크기, 생성 및 수정 날짜 등 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 Compliance는 스캔한 데이터를 다양한 유형의 범주로 나눕니다. 범주는 각 파일의 콘텐츠 및 메타데이터에 대한 AI 분석을 기반으로 하는 주제입니다. ["범주에 대해 자세히 알아보십시오"](#).

이름 요소 인식

Cloud Compliance는 AI를 사용하여 문서에서 자연인의 이름을 추출합니다. ["데이터 주체 액세스 요청에 응답하는 방법에 대해 알아보십시오"](#).

네트워킹 개요

Cloud Manager는 Connector 인스턴스의 인바운드 HTTP 연결을 지원하는 보안 그룹과 함께 Cloud Compliance 인스턴스를 배포합니다.

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

어떤 이유로든 SaaS 사용자 인터페이스 대신 로컬 사용자 인터페이스를 사용해야 하는 경우에도 가능합니다 ["로컬 UI에 액세스합니다"](#).

아웃바운드 규칙은 완전히 열립니다. 클라우드 규정 준수 소프트웨어를 설치 및 업그레이드하고 사용량 메트릭을 전송하려면 인터넷에 액세스해야 합니다.

네트워킹 요구 사항이 엄격하면 ["Cloud Compliance에서 접착하는 엔드포인트에 대해 알아보십시오"](#).

규정 준수 정보에 대한 사용자 액세스

각 사용자에게 할당된 역할은 Cloud Manager 내부 및 클라우드 규정 준수 내에서 서로 다른 기능을 제공합니다.

- *** Account Admins *** 는 모든 작업 환경에 대한 규정 준수 설정을 관리하고 규정 준수 정보를 볼 수 있습니다.
- *** Workspace Admins *** 는 액세스 권한이 있는 시스템에 대해서만 규정 준수 설정을 관리하고 규정 준수 정보를 볼 수 있습니다. 작업 영역 관리자가 Cloud Manager의 작업 환경에 액세스할 수 없는 경우 규정 준수 탭에서 작업

환경에 대한 규정 준수 정보를 볼 수 없습니다.

- Cloud 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.

"[Cloud Manager 역할에 대해 자세히 알아보십시오](#)" 및 [방법](#) 을 참조하십시오 "[특정 역할을 가진 사용자를 추가합니다](#)".

시작하십시오

클라우드 규정 준수 구현

Cloud Manager 작업 공간에 Cloud Compliance 인스턴스를 구축하는 몇 가지 단계를 완료하십시오.

빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션으로 스크롤하여 자세한 내용을 확인하십시오.

1 커넥터를 작성합니다

Connector가 없는 경우 Azure 또는 AWS에서 Connector를 생성합니다. 을 참조하십시오 "[AWS에서 커넥터 생성](#)" 또는 "[Azure에서 커넥터 만들기](#)".

2 사전 요구 사항을 검토합니다

클라우드 환경이 클라우드 규정 준수 인스턴스에 대한 vCPU 16개, 인스턴스에 대한 아웃바운드 인터넷 액세스, 포트 80을 통한 Connector와 Cloud Compliance 간 접속 등 사전 요구 사항을 충족할 수 있는지 확인합니다. [전체 목록을 참조하십시오](#).

3 클라우드 규정 준수 구현

설치 마법사를 시작하여 Cloud Manager에 Cloud Compliance 인스턴스를 구축합니다.

4 클라우드 규정 준수 서비스를 구독하십시오

Cloud Manager에서 Cloud Compliance에서 검사하는 첫 번째 1TB의 데이터는 무료입니다. AWS 또는 Azure Marketplace에 가입해야 해당 시점 이후에 데이터를 계속 스캔할 수 있습니다.

커넥터 작성

Connector가 없는 경우 Azure 또는 AWS에서 Connector를 생성합니다. 을 참조하십시오 "[AWS에서 커넥터 생성](#)" 또는 "[Azure에서 커넥터 만들기](#)". 대부분의 경우, 대부분의 경우 Cloud Compliance 활성화를 시도하기 전에 Connector가 설정되어 있을 수 있습니다 "[Cloud Manager 기능에는 커넥터가 필요합니다](#)"하지만 지금 설정해야 하는 경우가 있습니다.

Cloud Compliance를 위해 AWS 또는 Azure에서 Connector를 사용해야 하는 몇 가지 시나리오가 있습니다.

- AWS 또는 AWS S3 버킷에서 Cloud Volumes ONTAP의 데이터를 스캔할 때는 AWS의 커넥터를 사용합니다.
- Azure 또는 Azure NetApp Files의 Cloud Volumes ONTAP에서 데이터를 스캔할 때 Azure의 커넥터를 사용합니다.
- 커넥터 중 하나를 사용하여 데이터베이스를 스캔할 수 있습니다.

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



Azure NetApp Files를 스캔할 계획이라면 스캔할 볼륨과 동일한 영역에 배포해야 합니다.

사전 요구 사항 검토

Cloud Compliance를 구축하기 전에 다음 필수 구성 요소를 검토하여 지원되는 구성이 있는지 확인하십시오.

아웃바운드 인터넷 액세스를 활성화합니다

클라우드 규정 준수에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 네트워크가 인터넷 액세스에 프록시 서버를 사용하는 경우 클라우드 규정 준수 인스턴스가 다음 엔드포인트에 연결할 아웃바운드 인터넷 액세스를 가지고 있는지 확인합니다. Cloud Manager는 Connector와 동일한 서브넷에 Cloud Compliance 인스턴스를 구축합니다.

엔드포인트	목적
https://cloudmanager.cloud.netapp.com 으로 문의하십시오	Cloud Central 계정을 포함한 Cloud Manager 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com https://auth0.com 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io \ https://dseasb33srrn.cloudfront.net \ https://production.cloudflare.docker.com/	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
https://kinesis.us-east-1.amazonaws.com 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com 으로 문의하십시오	Cloud Compliance에서 매니페스트와 템플릿을 액세스 및 다운로드하고 로그 및 메트릭을 전송할 수 있습니다.

Cloud Manager에 필요한 권한이 있는지 확인합니다

Cloud Manager에 리소스를 구축하고 Cloud Compliance 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.

AWS에서 인스턴스 제품군은 _온디맨드 표준 인스턴스_ 입니다. Azure에서 인스턴스 제품군은 _Standard DSv3 Family_입니다.

vCPU 제한에 대한 자세한 내용은 다음을 참조하십시오.

- "AWS 문서: Amazon EC2 서비스 제한"
- "Azure 설명서: 가상 머신 vCPU 할당량"

Cloud Manager가 클라우드 규정 준수에 액세스할 수 있는지 확인합니다

Connector와 Cloud Compliance 인스턴스 간의 연결을 확인합니다. Connector의 보안 그룹은 포트 80을 통해 클라우드 규정 준수 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다.

이 연결을 통해 Cloud Compliance 인스턴스를 구축하고 Compliance 탭에서 정보를 볼 수 있습니다.

Azure NetApp Files의 검색을 설정합니다

Azure NetApp Files의 볼륨을 스캔하기 전에 "구성을 검색하려면 Cloud Manager를 설정해야 합니다".

클라우드 규정 준수를 지속적으로 실행할 수 있어야 합니다

데이터를 지속적으로 스캔하려면 클라우드 규정 준수 인스턴스가 계속 켜져 있어야 합니다.

클라우드 규정 준수에 대한 웹 브라우저 연결 보장

Cloud Compliance를 활성화한 후 사용자가 Cloud Compliance 인스턴스에 대한 연결이 있는 호스트에서 Cloud Manager 인터페이스에 액세스하는지 확인합니다.

Cloud Compliance 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 AWS 또는 Azure(예: VPN)에 직접 연결되거나 Cloud Compliance 인스턴스와 같은 네트워크 내에 있는 호스트에서 발생할 수 있습니다.

클라우드 규정 준수 인스턴스 구축

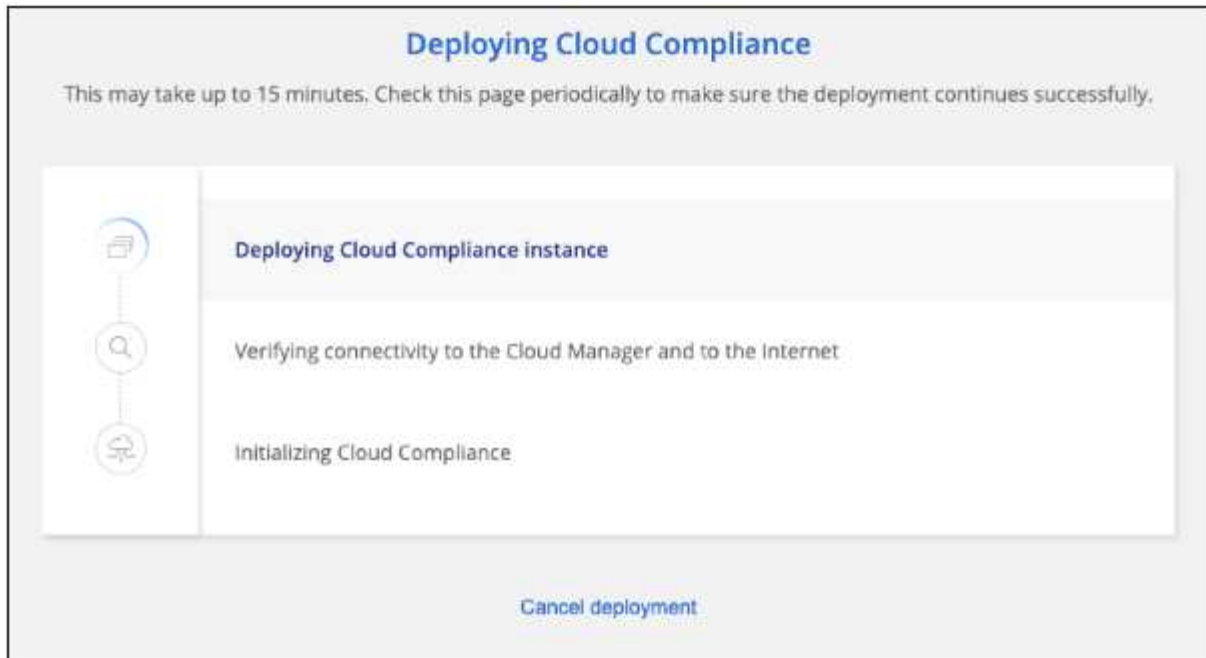
각 Cloud Manager 인스턴스에 대해 Cloud Compliance 인스턴스를 구축합니다.

단계

1. Cloud Manager에서 * Cloud Compliance * 를 클릭합니다.
2. 클라우드 규정 준수 활성화 * 를 클릭하여 구축 마법사를 시작합니다.

The screenshot shows the 'Cloud Compliance' interface. The top navigation bar includes 'Working Environment', 'Compliance', 'Replication', 'Kubernetes', 'Backup & Restore', 'Monitoring', and 'Timeline'. The main content area features a 'Cloud Compliance' header and a 'How does it work?' link. Below this is the heading 'Always-on Privacy & Compliance Controls' and a sub-heading 'Automated controls for data privacy regulations such as the GDPR, CCPA and more. Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready.' A prominent blue button labeled 'Activate Cloud Compliance' is visible. On the right side, there is a 'Compliance Status' dashboard. This dashboard includes a 'Data Distribution' section with a circular progress indicator showing 75% Non-Sensitive, 20% Personal, and 5% Sensitive Personal. Below this, it displays '28,000 Personal Files' and '7,000 Sensitive Personal Files'. A detailed breakdown shows: Email Address (2,700 Files), Credit Card (2,700 Files), Health (2,700 Files), and Ethnicity (2,700 Files). Each category has a corresponding progress bar and a 'View All' link.

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



4. 인스턴스가 배포되면 * Continue to configuration * 을 클릭하여 _Scan Configuration_ 페이지로 이동합니다.

결과

Cloud Manager는 클라우드 공급업체에 클라우드 규정 준수 인스턴스를 구축합니다.

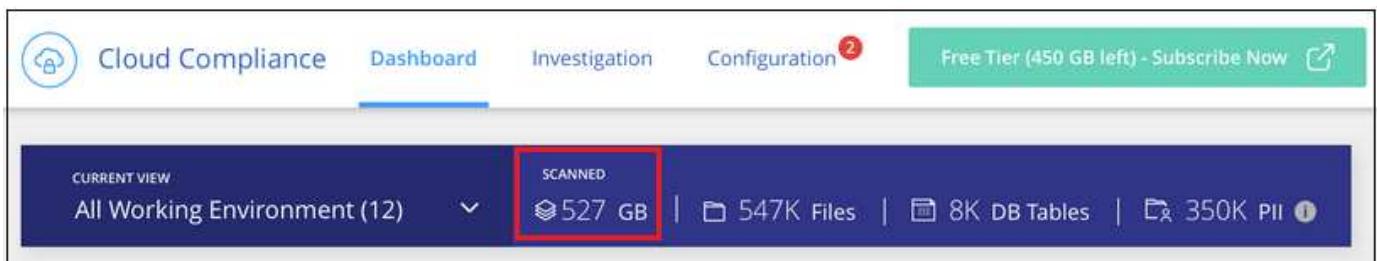
다음 단계

스캔 구성 페이지에서 규정 준수를 검사할 작업 환경, 볼륨 및 버킷을 선택할 수 있습니다. 특정 데이터베이스 스키마를 스캔하기 위해 데이터베이스 서버에 연결할 수도 있습니다. 이러한 데이터 소스에서 클라우드 규정 준수를 활성화합니다.

클라우드 규정 준수 서비스 가입

Cloud Manager 작업 공간에서 Cloud Compliance에서 스캔하는 첫 1TB의 데이터는 무료입니다. AWS 또는 Azure Marketplace에 가입해야 해당 시점 이후에 데이터를 계속 스캔할 수 있습니다.

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

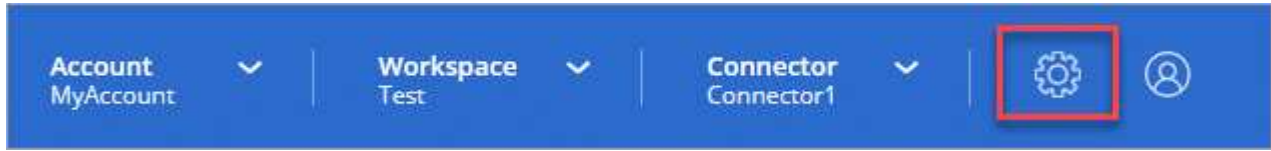


- 참고: * 클라우드 규정 준수(Cloud Compliance)에서 구독하라는 메시지가 나타나지만 이미 Azure 구독을 보유하고 있는 경우 이전 * Cloud Manager * 구독을 사용하고 있는 것이며 새로운 * NetApp Cloud Manager * 구독으로 변경해야 합니다. 을 참조하십시오 Azure에서 새로운 NetApp Cloud Manager 계획으로 변경 를 참조하십시오.

단계

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

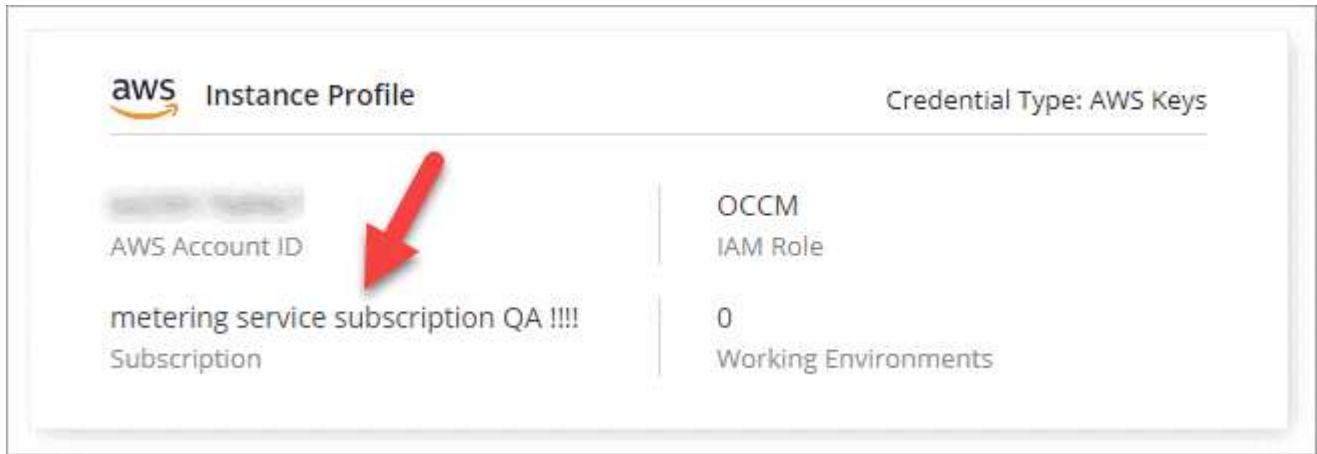
1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 * 자격 증명 * 을 선택합니다.



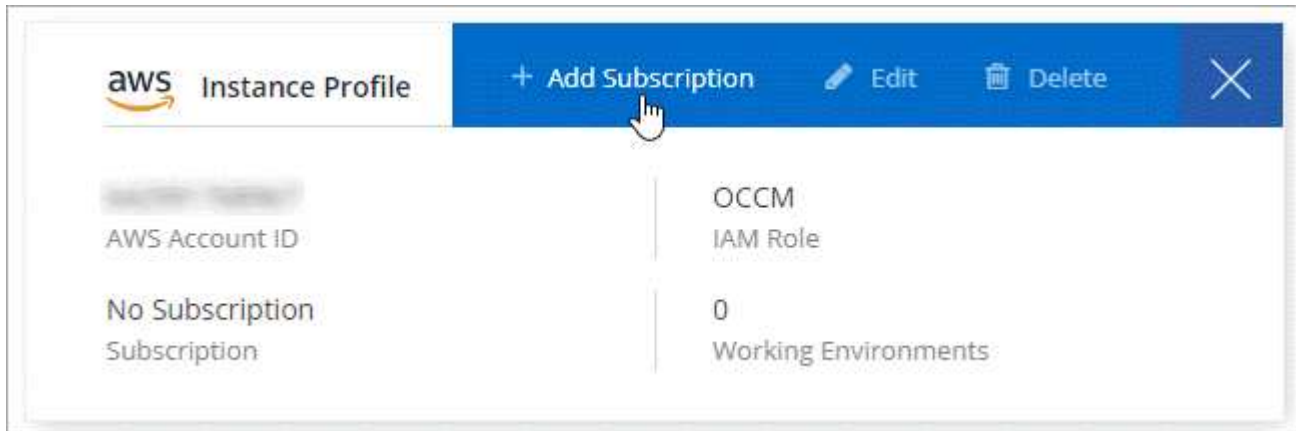
2. AWS 인스턴스 프로파일 또는 Azure 관리 서비스 ID에 대한 자격 증명을 찾습니다.

구독은 인스턴스 프로필 또는 관리 서비스 ID에 추가해야 합니다. 그렇지 않으면 충전이 작동하지 않습니다.

이미 구독이 있는 경우 모든 설정이 완료되며, 다른 작업은 필요하지 않습니다.



3. 구독이 아직 없는 경우 자격 증명 위에 마우스를 올려 놓고 작업 메뉴를 클릭합니다.
4. 구독 추가 * 를 클릭합니다.



5. 구독 추가 * 를 클릭하고 * 계속 * 을 클릭한 다음 단계를 따릅니다.

다음 비디오에서는 마켓플레이스 구독을 AWS 구독에 연결하는 방법을 보여줍니다.

▶ https://docs.netapp.com/ko-kr/occm38//media/video_subscribing_aws.mp4 (video)

다음 비디오에서는 마켓플레이스 구독을 Azure 구독에 연결하는 방법을 보여 줍니다.

▶ https://docs.netapp.com/ko-kr/occm38//media/video_subscribing_azure.mp4 (video)

Azure에서 새로운 Cloud Manager 계획으로 변경

Cloud Compliance는 2020년 10월 7일 * NetApp Cloud Manager * 라는 Azure 마켓플레이스 구독에 추가되었습니다. 원래 Azure * Cloud Manager * 에 이미 가입되어 있으면 Cloud Compliance를 사용할 수 없습니다.

다음 단계를 따라 새로운 * NetApp Cloud Manager * 가입을 선택한 다음, 이전 * Cloud Manager * 가입을 제거해야 합니다.



기존 구독에서 특별 비공개 제안을 받은 경우 NetApp에 연락하여 규정 준수를 포함한 새로운 특별 비공개 제안을 발행해야 합니다.

단계

이러한 단계는 위에서 설명한 대로 새 구독을 추가하는 것과 비슷하지만 몇 가지 면에서 다릅니다.

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 * 자격 증명 * 을 선택합니다.
2. 구독을 변경할 Azure Managed Service Identity에 대한 자격 증명을 찾고 자격 증명 위에 마우스를 올려 놓고 * Associate Subscription * 을 클릭합니다.

현재 마켓플레이스 구독에 대한 세부 정보가 표시됩니다.

3. 구독 추가 * 를 클릭하고 * 계속 * 을 클릭한 다음 단계를 따릅니다. 새 구독을 만들기 위해 Azure 포털로 리디렉션됩니다.
4. Cloud Manager * 가 아닌 클라우드 규정 준수에 대한 액세스를 제공하는 계획 * NetApp Cloud Manager * 를 선택하십시오.
5. 동영상의 단계를 따라 마켓플레이스 구독을 Azure 구독에 연결합니다.

▶ https://docs.netapp.com/ko-kr/occm38//media/video_subscribing_azure.mp4 (video)

6. Cloud Manager로 돌아가서 새 구독을 선택하고 * Associate * 를 클릭합니다.
7. 구독이 변경되었는지 확인하려면 자격 증명 카드의 구독 위에 있는 "I" 위로 마우스를 가져갑니다.

이제 Azure 포털에서 이전 구독을 취소할 수 있습니다.

8. Azure 포털에서 SaaS(Software as a Service)로 이동하여 구독을 선택한 다음 * 구독 취소 * 를 클릭합니다.

데이터 소스에서 스캔을 활성화합니다

Cloud Volumes ONTAP 및 Azure NetApp Files용 클라우드 규정 준수 시작하기

Cloud Volumes ONTAP 또는 Azure NetApp Files용 클라우드 규정 준수를 시작하려면 몇 단계를 완료하십시오.

빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션으로 스크롤하여 자세한 내용을 확인하십시오.

1

클라우드 규정 준수 인스턴스 구축

"Cloud Manager에서 클라우드 규정 준수 구축" 이미 배포된 인스턴스가 없는 경우

2

작업 환경에서 클라우드 규정 준수 지원

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

3

볼륨에 대한 액세스를 확인합니다

이제 Cloud Compliance를 사용하도록 설정했으므로 볼륨에 액세스할 수 있는지 확인합니다.

- 클라우드 규정 준수 인스턴스에는 각 Cloud Volumes ONTAP 서브넷 또는 Azure NetApp Files 서브넷에 대한 네트워크 연결이 필요합니다.
- Cloud Volumes ONTAP의 보안 그룹은 클라우드 규정 준수 인스턴스로부터 인바운드 연결을 허용해야 합니다.
- NFS 볼륨 익스포트 정책은 Cloud Compliance 인스턴스에서 액세스할 수 있어야 합니다.
- Cloud Compliance는 CIFS 볼륨을 검색하려면 Active Directory 자격 증명이 필요합니다.

Cloud Compliance * > * Scan Configuration * > * Edit CIFS Credentials * 를 클릭하고 자격 증명을 입력합니다. 자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Cloud Compliance에서 상승된 권한이 필요한 데이터를 읽을 수 있습니다.

4

스캔할 볼륨을 구성합니다

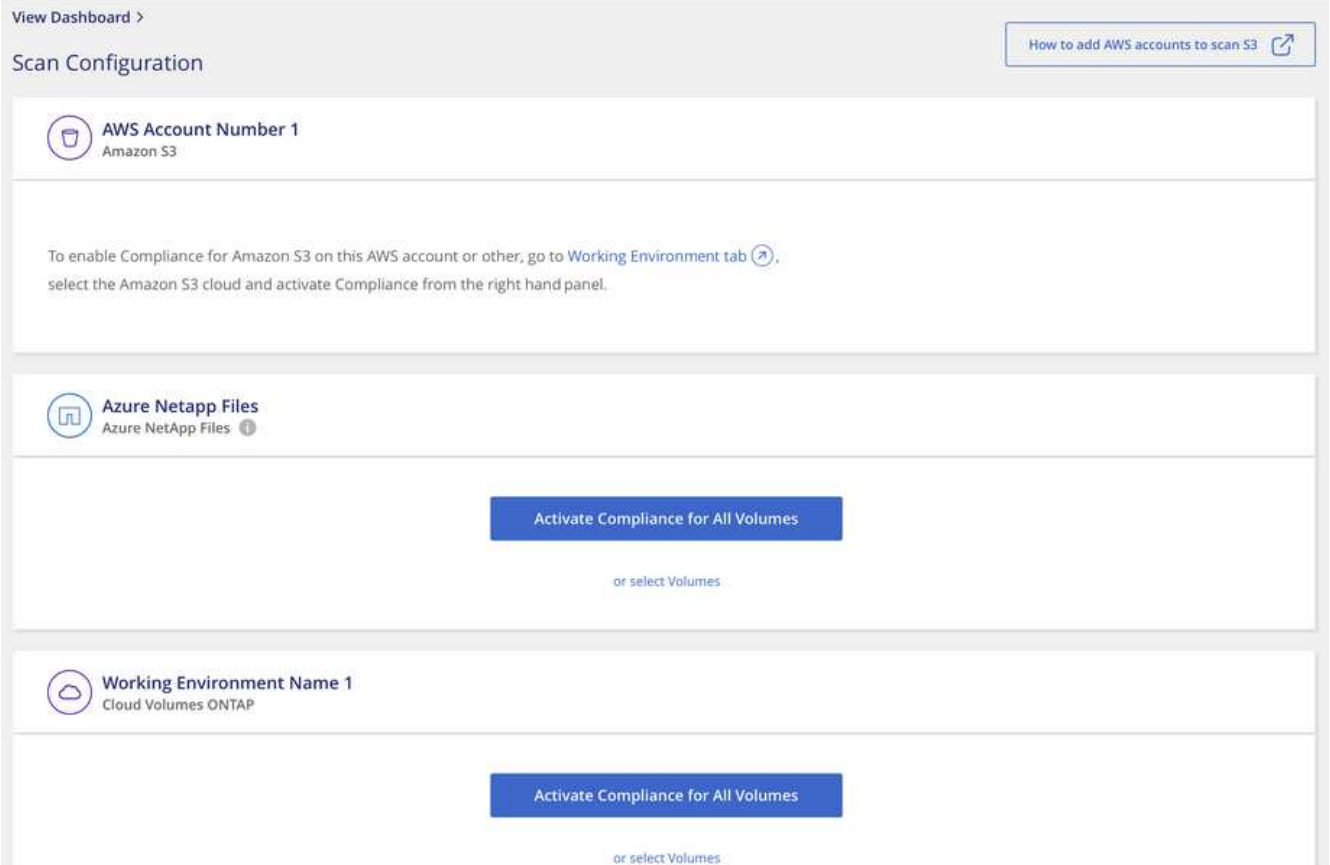
스캔할 볼륨을 선택하면 Cloud Compliance에서 스캔을 시작합니다.

클라우드 규정 준수 인스턴스 구축

"Cloud Manager에서 클라우드 규정 준수 구축" 이미 배포된 인스턴스가 없는 경우

작업 환경에서 클라우드 규정 준수 지원

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭한 다음 * Configuration * 탭을 선택합니다.



2. 작업 환경의 모든 볼륨을 스캔하려면 * Activate Compliance for All Volumes * 를 클릭합니다.

작업 환경의 특정 볼륨만 스캔하려면 * 를 클릭하거나 볼륨 * 을 선택한 다음 스캔할 볼륨을 선택합니다.

을 참조하십시오 [볼륨에서 규정 준수 검사 활성화 및 비활성화](#) 를 참조하십시오.

결과

Cloud Compliance는 각 작업 환경에서 데이터 스캔을 시작합니다. Cloud Compliance에서 초기 스캔을 마치면 Compliance 대시보드에서 결과를 얻을 수 있습니다. 소요되는 시간은 데이터 양에 따라 다릅니다. 몇 분 또는 몇 시간이 걸릴 수도 있습니다.

Cloud Compliance에서 볼륨에 액세스할 수 있는지 확인

네트워킹, 보안 그룹 및 익스포트 정책을 확인하여 Cloud Compliance에서 볼륨에 액세스할 수 있는지 확인합니다. CIFS 볼륨에 액세스할 수 있도록 Cloud Compliance에 CIFS 자격 증명을 제공해야 합니다.

단계

1. 클라우드 규정 준수 인스턴스와 Cloud Volumes ONTAP 또는 Azure NetApp Files용 볼륨이 포함된 각 네트워크 간에 네트워크 연결이 있는지 확인하십시오.

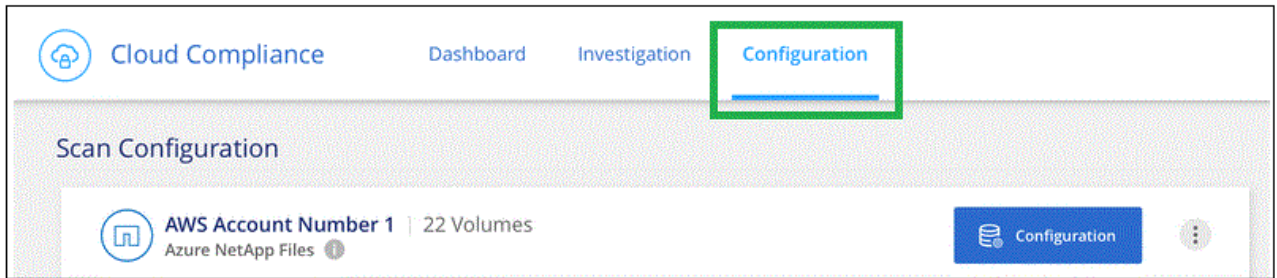


Azure NetApp Files의 경우 Cloud Compliance는 Cloud Manager와 동일한 지역에 있는 볼륨만 스캔할 수 있습니다.

2. Cloud Volumes ONTAP의 보안 그룹이 클라우드 규정 준수 인스턴스의 인바운드 트래픽을 허용하는지 확인합니다.

Cloud Compliance 인스턴스의 IP 주소에 있는 트래픽에 대한 보안 그룹을 열거나 가상 네트워크 내부에서 발생하는 모든 트래픽에 대해 보안 그룹을 열 수 있습니다.

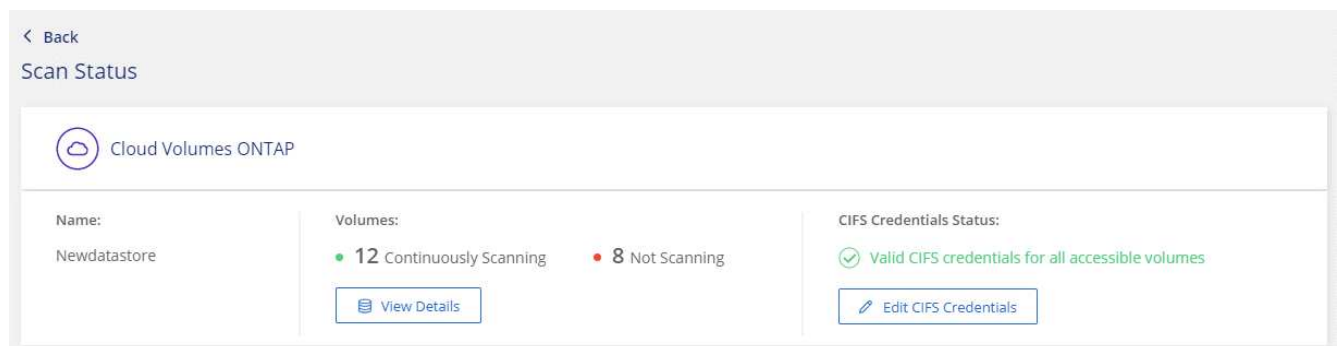
3. NFS 볼륨 익스포트 정책에 Cloud Compliance 인스턴스의 IP 주소가 포함되어 각 볼륨의 데이터에 액세스할 수 있는지 확인합니다.
4. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 Cloud Compliance를 제공합니다.
 - a. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
 - b. Configuration * 탭을 클릭합니다.



- c. 각 작업 환경에서 * CIFS 자격 증명 편집 * 을 클릭하고 Cloud Compliance가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 암호를 입력합니다.

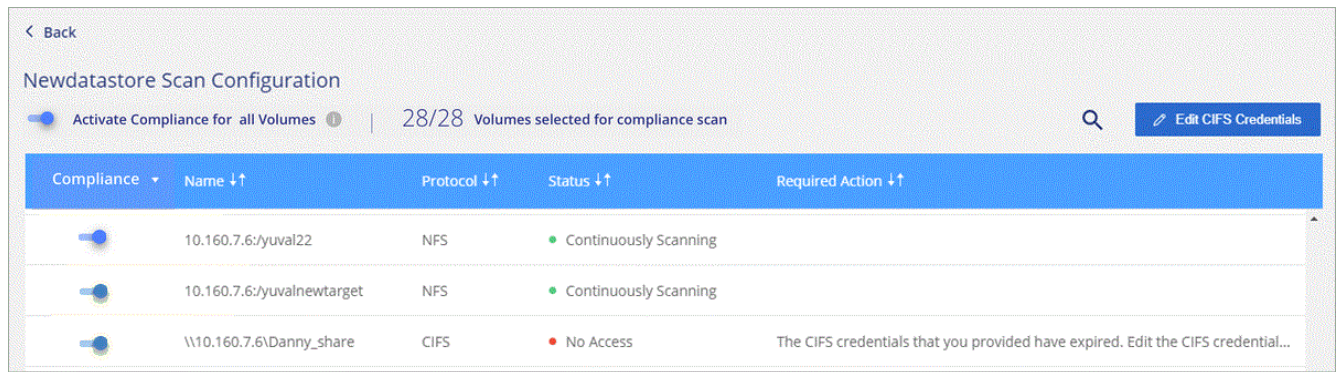
자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Cloud Compliance에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Compliance 인스턴스에 저장됩니다.

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



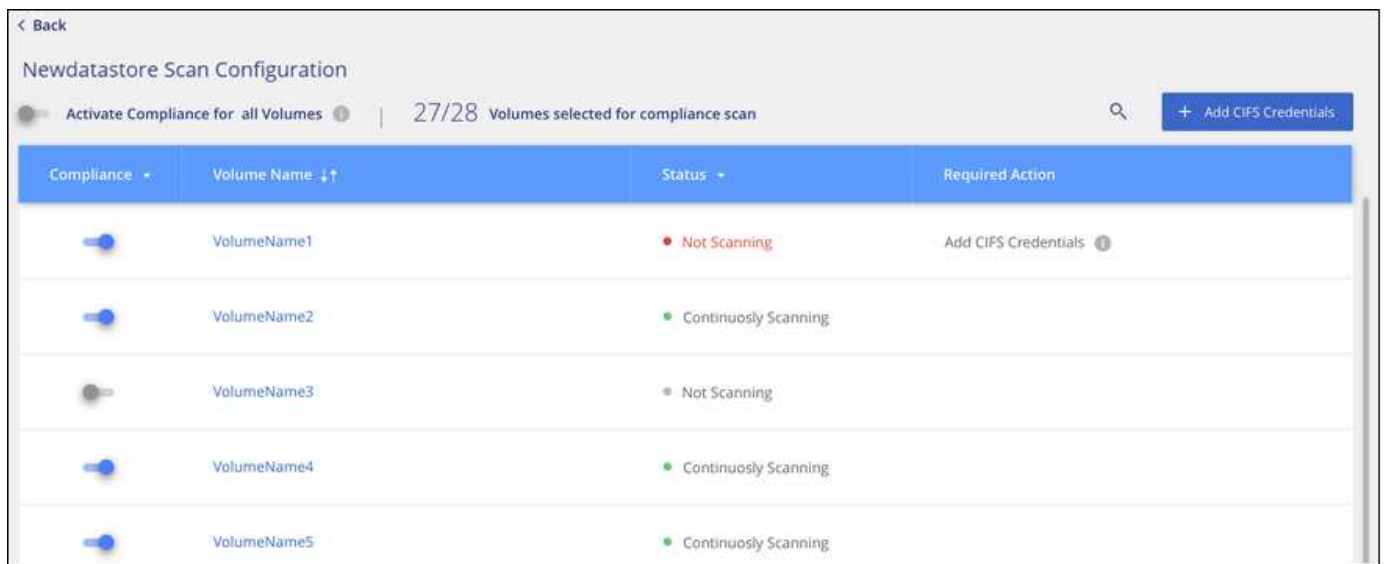
5. Scan Configuration_ 페이지에서 * View Details * 를 클릭하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

예를 들어, 다음 이미지는 3개의 볼륨을 보여 줍니다. 그 중 하나는 Cloud Compliance 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 Cloud Compliance에서 스캔할 수 없는 볼륨입니다.



볼륨에서 규정 준수 검사 활성화 및 비활성화

스캔 구성 페이지에서 언제든지 작업 환경에서 볼륨 스캔을 중지하거나 시작할 수 있습니다. 모든 볼륨을 검사하는 것이 좋습니다.



대상:	방법은 다음과 같습니다.
볼륨 스캔을 비활성화합니다	볼륨 슬라이더를 왼쪽으로 이동합니다
모든 볼륨에 대한 스캔을 비활성화합니다	모든 볼륨에 대해 * 준수 활성화 * 슬라이더를 왼쪽으로 이동합니다
볼륨 스캔을 활성화합니다	볼륨 슬라이더를 오른쪽으로 이동합니다
모든 볼륨 스캔을 활성화합니다	모든 볼륨에 대해 * 준수 활성화 * 슬라이더를 오른쪽으로 이동합니다



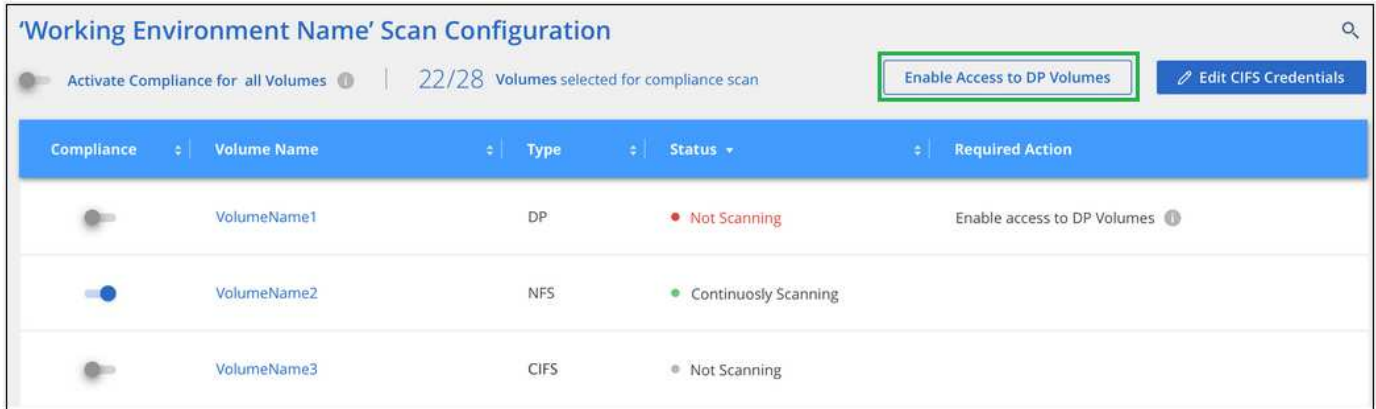
작업 환경에 추가된 새 볼륨은 * Activate Compliance for All Volumes * 설정이 활성화된 경우에만 자동으로 스캔됩니다. 이 설정을 비활성화하면 작업 환경에서 새로 생성한 각 볼륨에 대해 스캐닝을 활성화해야 합니다.

데이터 보호 볼륨을 검색하는 중입니다

기본적으로 데이터 보호(DP) 볼륨은 외부에서 노출되지 않고 Cloud Compliance에서 액세스할 수 없기 때문에 스캔되지 않습니다. 일반적으로 이러한 볼륨은 온프레미스 ONTAP 클러스터에서 SnapMirror 작업을 위한 타겟

볼륨입니다.

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



Compliance	Volume Name	Type	Status	Required Action
<input type="checkbox"/>	VolumeName1	DP	● Not Scanning	Enable access to DP Volumes ⓘ
<input checked="" type="checkbox"/>	VolumeName2	NFS	● Continuously Scanning	
<input type="checkbox"/>	VolumeName3	CIFS	● Not Scanning	

단계

이러한 데이터 보호 볼륨을 스캔하려는 경우:

1. 페이지 맨 위에 있는 * DP 볼륨에 대한 액세스 활성화 * 버튼을 클릭합니다.
2. 스캔할 각 DP 볼륨을 활성화하거나 모든 볼륨 * 컨트롤에 대해 * 규정 준수 활성화 를 사용하여 모든 DP 볼륨을 포함한 모든 볼륨을 활성화합니다.

활성화되면 Cloud Compliance는 규정 준수를 위해 활성화된 각 DP 볼륨에서 NFS 공유를 생성하여 검색할 수 있습니다. 공유 내보내기 정책은 클라우드 규정 준수 인스턴스에서만 액세스를 허용합니다.



소스 ONTAP 시스템에서 처음에 NFS 볼륨으로 생성된 볼륨만 볼륨 목록에 표시됩니다. 처음에 CIFS로 생성된 소스 볼륨은 현재 Cloud Compliance에 표시되지 않습니다.

Amazon S3에 대한 클라우드 규정 준수 시작하기

Cloud Compliance는 Amazon S3 버킷을 스캔하여 S3 오브젝트 스토리지에 상주하는 개인적이고 민감한 데이터를 식별할 수 있습니다. Cloud Compliance는 NetApp 솔루션용으로 제작되었는지에 관계없이 모든 버킷을 스캔할 수 있습니다.

빠른 시작

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



클라우드 환경에서 **S3** 요구사항을 설정합니다

IAM 역할 준비 및 Cloud Compliance에서 S3로 연결 설정 등 클라우드 환경이 클라우드 규정 준수 요구 사항을 충족할 수 있는지 확인합니다. [전체 목록을 참조하십시오.](#)

2

클라우드 규정 준수 인스턴스 구축

"Cloud Manager에서 클라우드 규정 준수 구축" 이미 배포된 인스턴스가 없는 경우

3

S3 작업 환경에서 규정 준수를 활성화합니다

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

4

스캔할 버킷을 선택합니다

스캔하려는 버킷을 선택하면 클라우드 규정 준수 가 해당 버킷을 스캔하기 시작합니다.

S3 사전 요구 사항 검토

다음 요구사항은 S3 버킷 스캔에만 적용됩니다.

Cloud Compliance 인스턴스에 대해 **IAM** 역할을 설정합니다

Cloud Compliance는 계정의 S3 버킷에 연결하고 이를 스캔할 수 있는 권한이 필요합니다. 아래에 나열된 권한을 포함하는 IAM 역할을 설정합니다. Cloud Manager는 Amazon S3 작업 환경에서 Cloud Compliance를 활성화할 때 IAM 역할을 선택하라는 메시지를 표시합니다.

```

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

```

Cloud Compliance에서 Amazon S3로 연결 제공

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

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

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

또는 NAT 게이트웨이를 사용하여 연결을 제공하는 방법도 있습니다.



프록시를 사용하여 인터넷을 통해 S3로 연결할 수는 없습니다.

클라우드 규정 준수 인스턴스 구축

["Cloud Manager에서 클라우드 규정 준수 구축"](#) 이미 배포된 인스턴스가 없는 경우

Cloud Manager가 이 AWS 계정에서 S3 버킷을 자동으로 검색하여 Amazon S3 작업 환경에 표시되도록 AWS Connector에 인스턴스를 구축해야 합니다.

S3 작업 환경에서 규정 준수 활성화

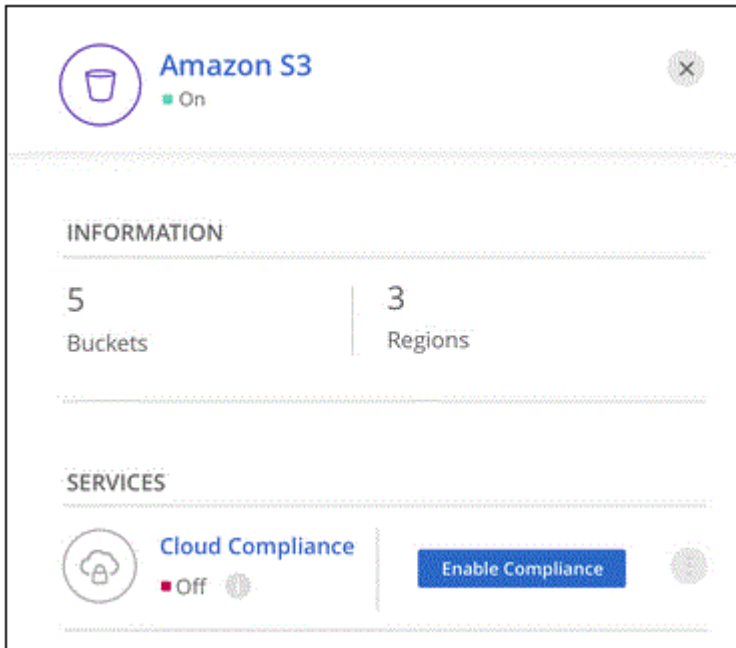
사전 요구 사항을 확인한 후 Amazon S3에서 Cloud Compliance를 활성화합니다.

단계

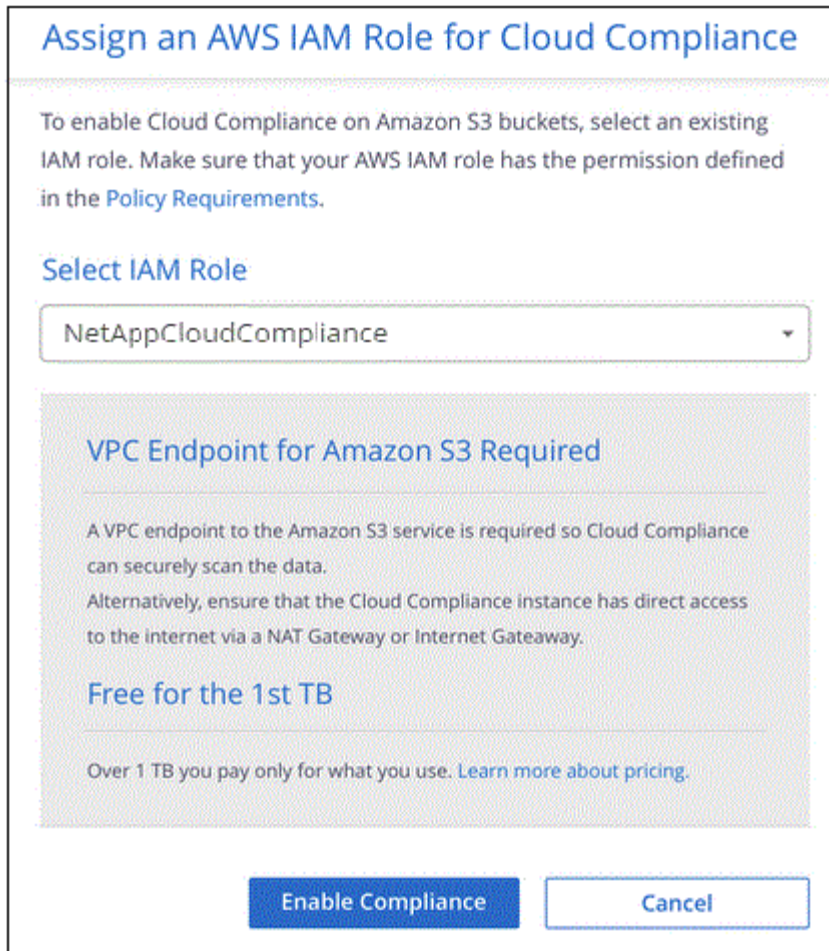
1. Cloud Manager 상단에서 * 작업 환경 * 을 클릭합니다.
2. Amazon S3 작업 환경을 선택합니다.



3. 오른쪽 창에서 * 준수 활성화 * 를 클릭합니다.



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



5. 준수 활성화 * 를 클릭합니다.



스캔 구성 페이지에서 을 클릭하여 작업 환경에 대한 규정 준수 스캔을 활성화할 수도 있습니다 버튼을 클릭하고 * 규정 준수 활성화 * 를 선택합니다.



결과

Cloud Manager는 IAM 역할을 인스턴스에 할당합니다.

S3 버킷에서 규정 준수 스캔 활성화 및 비활성화

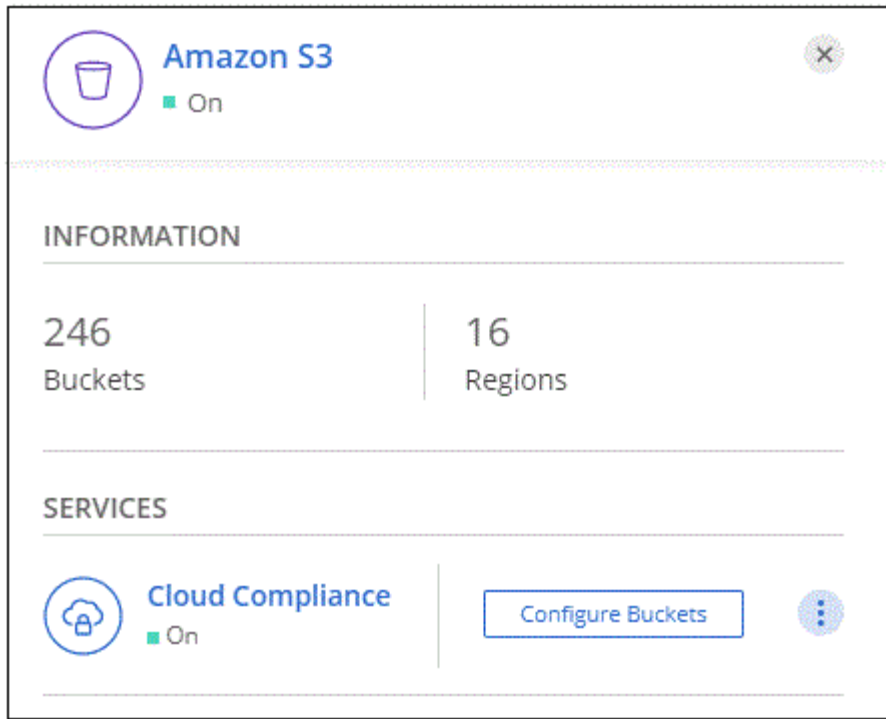
Cloud Manager를 사용하여 Amazon S3에서 Cloud Compliance를 사용하도록 설정한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다.

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

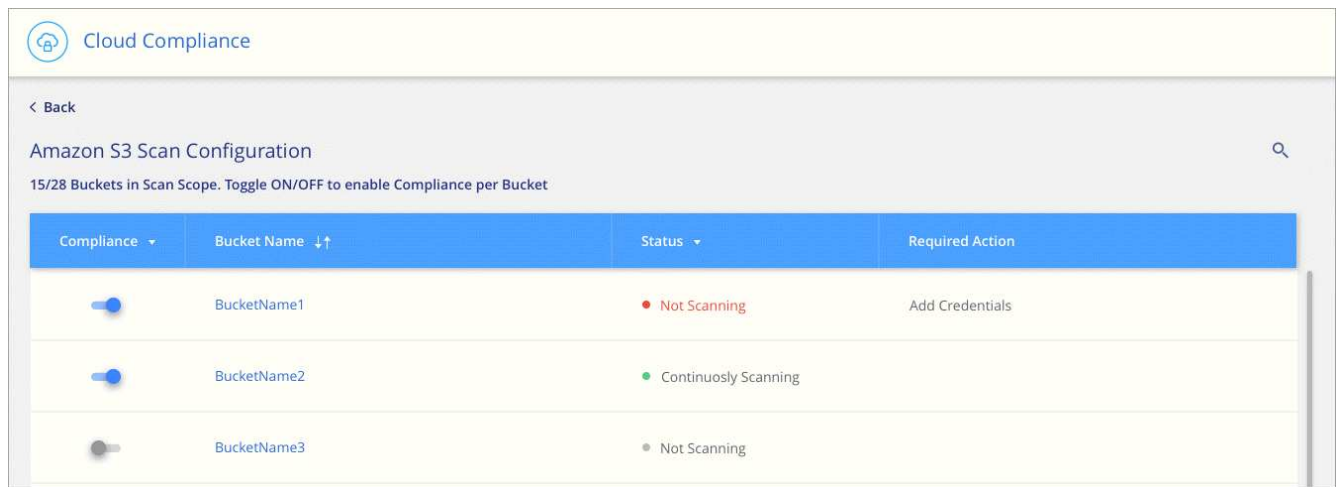
클라우드 규정 준수도 가능합니다 서로 다른 AWS 계정에 있는 S3 버킷을 스캔합니다.

단계

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



3. 스캔할 버킷의 규정 준수를 활성화합니다.



결과

Cloud Compliance는 사용자가 활성화한 S3 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

추가 **AWS** 계정에서 버킷 스캔

해당 계정에서 역할을 할당하여 기존 Cloud Compliance 인스턴스에 액세스함으로써 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



Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation 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 Compliance 인스턴스가 있는 계정의 ID를 입력합니다.
- 최대 CLI/API 세션 지속 시간 * 을 1시간에서 12시간으로 변경하고 변경 사항을 저장합니다.
- Cloud Compliance IAM 정책을 연결합니다. 필요한 권한이 있는지 확인합니다.

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

2. Cloud Compliance 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" 작업과 대상 계정에서 생성한 역할의 ARN을 포함하는 정책을 생성합니다.

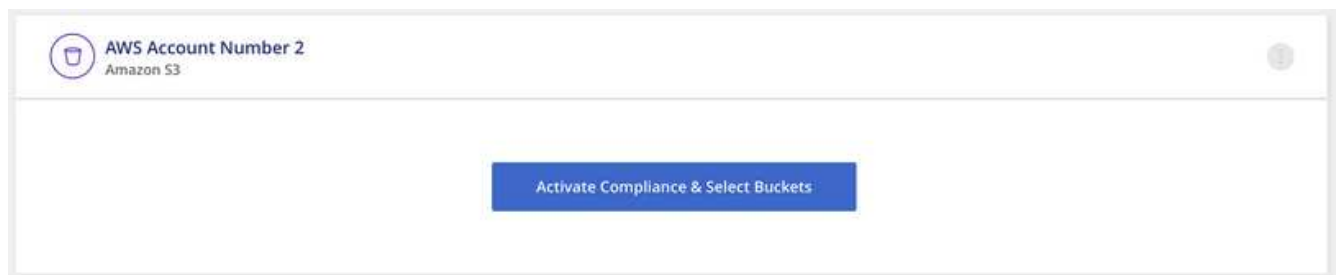
```

{
  "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/*"
      ]
    }
  ]
}

```

Cloud Compliance 인스턴스 프로파일 계정이 이제 추가 AWS 계정에 액세스할 수 있습니다.

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



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

결과

Cloud Compliance는 귀사가 활성화한 새로운 S3 버킷을 스캔합니다.

데이터베이스 스키마를 검색하는 중입니다

Cloud Compliance를 사용하여 데이터베이스 스키마 스캔을 시작하려면 몇 가지 단계를 완료하십시오.

빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션으로 스크롤하여 자세한 내용을 확인하십시오.

1 데이터베이스 사전 요구 사항을 검토합니다

데이터베이스가 지원되고 데이터베이스에 연결하는 데 필요한 정보가 있는지 확인합니다.

2 클라우드 규정 준수 인스턴스 구축

"Cloud Manager에서 클라우드 규정 준수 구축" 이미 배포된 인스턴스가 없는 경우

3 데이터베이스 서버를 추가합니다

액세스할 데이터베이스 서버를 추가합니다.

4 스키마를 선택합니다

스캔할 스키마를 선택합니다.

사전 요구 사항 검토

Cloud Compliance를 설정하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오.

지원되는 데이터베이스

Cloud Compliance는 다음 데이터베이스에서 스키마를 스캔할 수 있습니다.

- MongoDB
- 오라클
- PostgreSQL
- SAP HANA를 참조하십시오
- SQL Server(MSSQL)

i 데이터베이스에서 통계 수집 기능 * 을 활성화해야 합니다.

데이터베이스 요구 사항

Cloud Compliance 인스턴스에 연결할 수 있는 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 클라우드 규정 준수 시스템에 대한 전용 사용자를 생성하는 것이 좋습니다.

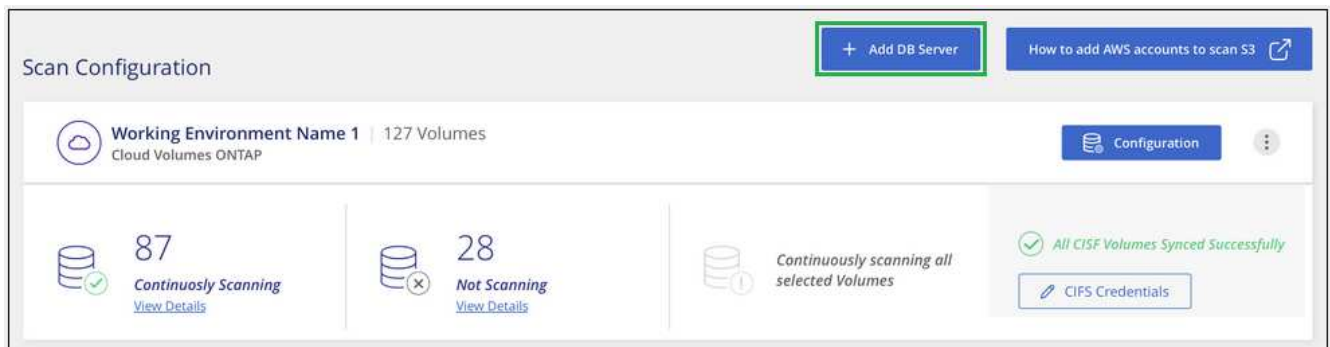
- 참고: * MongoDB의 경우 읽기 전용 관리자 역할이 필요합니다.

데이터베이스 서버 추가

이(가) 있어야 합니다 "Cloud Manager에 이미 클라우드 규정 준수 인스턴스를 배포했습니다".

스키마가 있는 데이터베이스 서버를 추가합니다.

1. Scan Configuration_ 페이지에서 * DB 서버 추가 * 버튼을 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 규정 준수 가 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

Port Service Name

Credentials

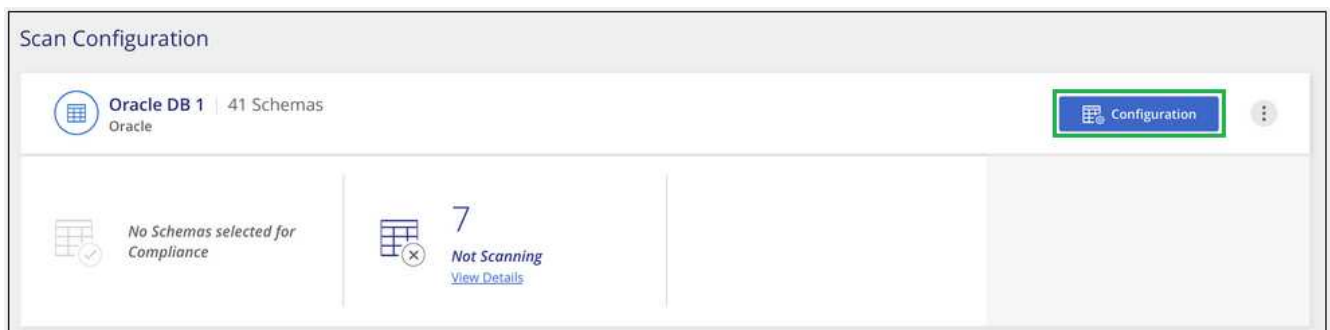
Username Password

데이터베이스가 작업 디렉토리 목록에 추가됩니다.

데이터베이스 스키마에서 규정 준수 검사를 활성화 및 비활성화합니다

언제든지 스키마 스캔을 중지하거나 시작할 수 있습니다.

1. Scan Configuration_ 페이지에서 구성하려는 데이터베이스의 * Configuration * 버튼을 클릭합니다.



2. 슬라이더를 오른쪽으로 이동하여 스캔할 스키마를 선택합니다.

Compliance	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

결과

Cloud Compliance는 사용자가 활성화한 데이터베이스 스키마 스캔을 시작합니다. 오류가 있는 경우 오류를 해결하는데 필요한 작업과 함께 상태 열에 표시됩니다.

Cloud Manager에서 데이터베이스 제거

특정 데이터베이스를 더 이상 스캔하지 않으려는 경우 Cloud Manager 인터페이스에서 해당 데이터베이스를 삭제하고 모든 스캔을 중지할 수 있습니다.

Scan Configuration_ 페이지에서 을 클릭합니다  단추를 클릭한 다음 * DB 서버 제거 * 를 클릭합니다.



SnapMirror를 사용하여 클라우드 규정 준수 기능을 통해 사내 **ONTAP** 데이터를 스캔합니다

온프레미스 NFS 또는 CIFS 데이터를 Cloud Volumes ONTAP 작업 환경에 복제하고 규정 준수를 설정하여 온프레미스 ONTAP 데이터를 클라우드 규정 준수 로 스캔할 수 있습니다. 온-프레미스 ONTAP 작업 환경에서 직접 데이터를 스캔하는 것은 지원되지 않습니다.

이(가) 있어야 합니다 "Cloud Manager에 이미 클라우드 규정 준수 인스턴스를 배포했습니다".

단계

1. Cloud Manager에서 사내 ONTAP 클러스터와 Cloud Volumes ONTAP 간에 SnapMirror 관계를 생성합니다.
 - a. "Cloud Manager에서 사내 클러스터를 검색합니다".
 - b. "Cloud Manager에서 사내 ONTAP 클러스터와 Cloud Volumes ONTAP 간에 SnapMirror 복제를 생성합니다".

2. SMB 소스 볼륨에서 생성된 DP 볼륨의 경우, ONTAP CLI에서 데이터 액세스를 위한 SMB 대상 볼륨을 구성합니다. (Cloud Compliance를 통해 데이터 액세스가 자동으로 설정되므로 NFS 볼륨에는 이 작업이 필요하지 않습니다.)
 - a. "타겟 볼륨에 SMB 공유를 생성합니다".
 - b. "대상 볼륨의 SMB 공유에 적절한 ACL을 적용합니다".
3. Cloud Manager에서 SnapMirror 데이터가 포함된 Cloud Volumes ONTAP 작업 환경에서 클라우드 규정 준수를 활성화합니다.
 - a. 작업 환경 * 을 클릭합니다.
 - b. SnapMirror 데이터가 포함된 작업 환경을 선택하고 * 규정 준수 활성화 * 를 클릭합니다.

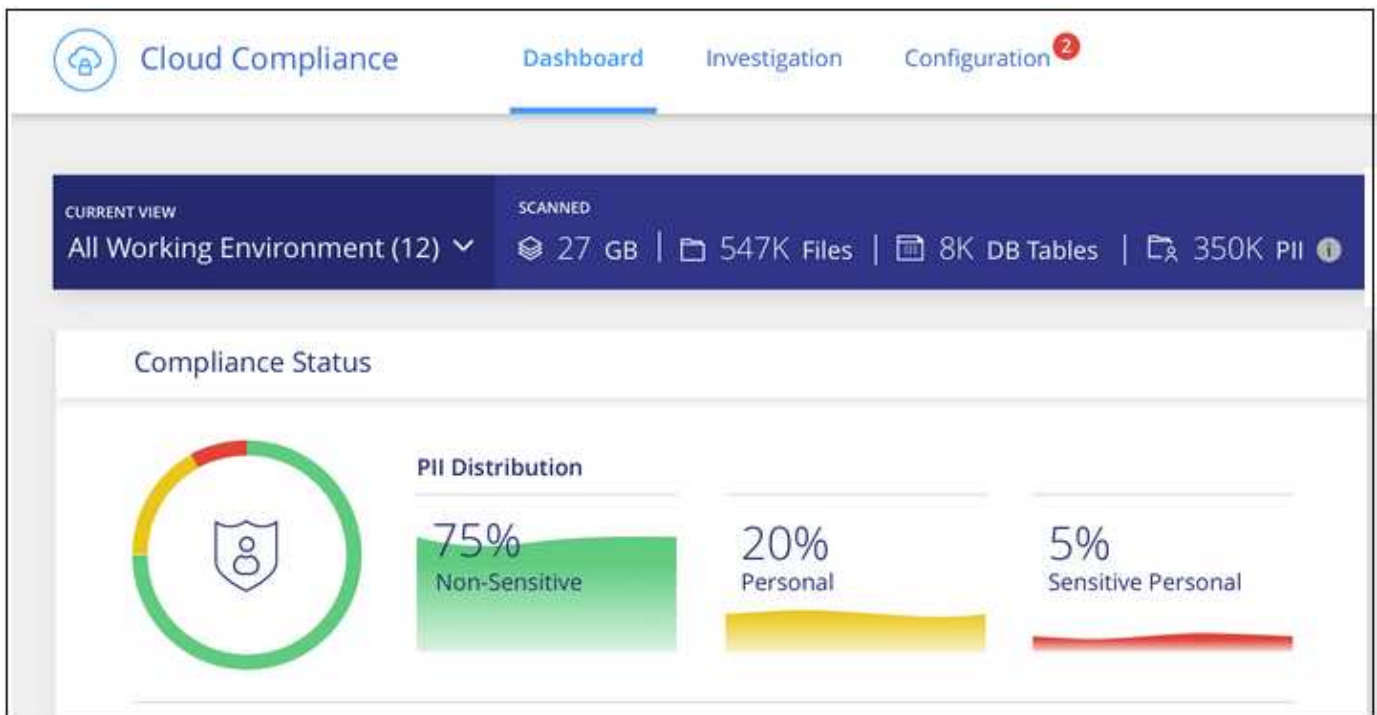
 "Cloud Volumes ONTAP 시스템에서 클라우드 규정 준수를 지원하는 데 도움이 필요한 경우 여기를 클릭하십시오".
 - c. Scan Configuration_page 상단의 * Enable Access to DP volumes * 버튼을 클릭합니다.
 - d. 스캔할 각 DP 볼륨을 활성화하거나 모든 볼륨 * 컨트롤에 대해 * 규정 준수 활성화 를 사용하여 모든 DP 볼륨을 포함한 모든 볼륨을 활성화합니다.

을 참조하십시오 "데이터 보호 볼륨을 검색하는 중입니다" DP 볼륨 스캔에 대한 자세한 내용은 를 참조하십시오.

프라이빗 데이터에 대한 가시성 및 제어 확보

조직의 개인 데이터 및 민감한 개인 데이터에 대한 세부 정보를 확인하여 개인 데이터를 제어할 수 있습니다. Cloud Compliance에서 데이터에 제공하는 범주 및 파일 형식을 검토하여 가시성을 확보할 수도 있습니다.

기본적으로 Cloud Compliance 대시보드에는 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터가 표시됩니다.



일부 작업 환경에 대한 데이터만 보려면 [작업 환경을 선택합니다](#).

개인 데이터

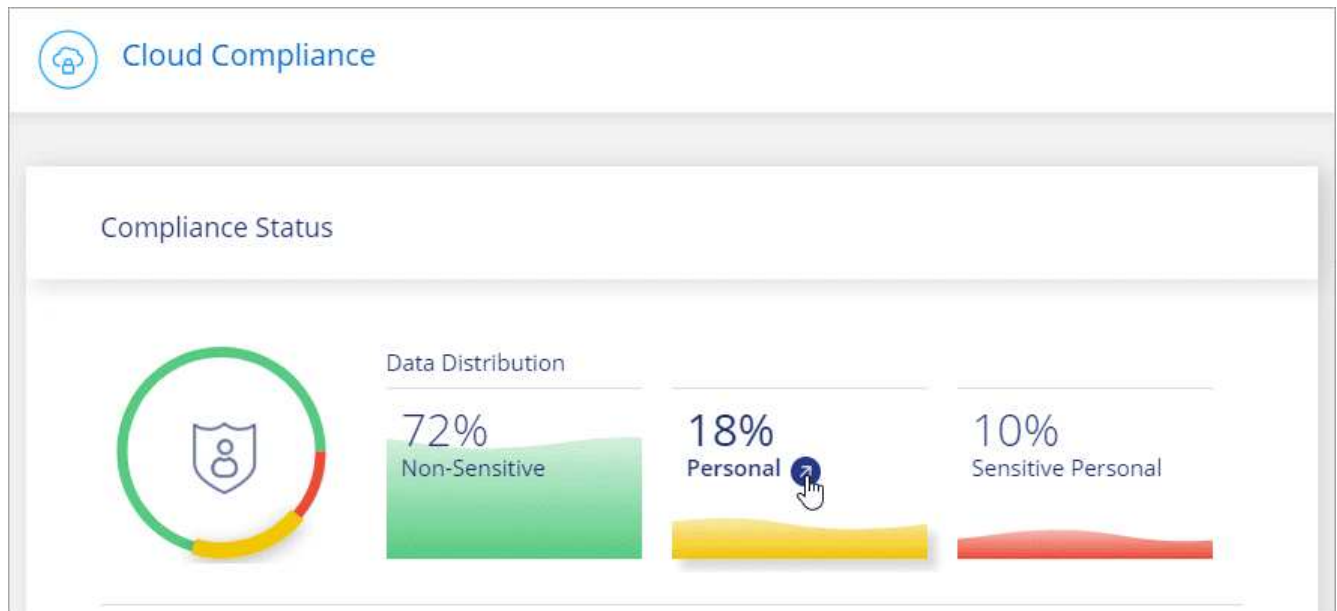
Cloud Compliance는 데이터 내에서 특정 단어, 문자열 및 패턴(Regex)을 자동으로 식별합니다. 예를 들어 개인 식별 정보(PII), 신용 카드 번호, 주민 등록 번호, 은행 계좌 번호 등이 있습니다. [전체 목록을 참조하십시오](#).

일부 유형의 개인 데이터에 대해 Cloud Compliance는 근접성 검증_을 사용하여 결과를 검증합니다. 유효성 검사는 발견된 개인 데이터 근처에서 하나 이상의 미리 정의된 키워드를 찾는 방식으로 수행됩니다. 예를 들어, *Cloud Compliance*는 미국 주민등록번호(SSN) 옆에 근접 단어가 있는 경우 주민등록번호로 사용 — 예: *_SSN_OR_Social security*. [아래 목록](#) Cloud Compliance에서 근접 유효성 검사를 사용하는 경우를 표시합니다.

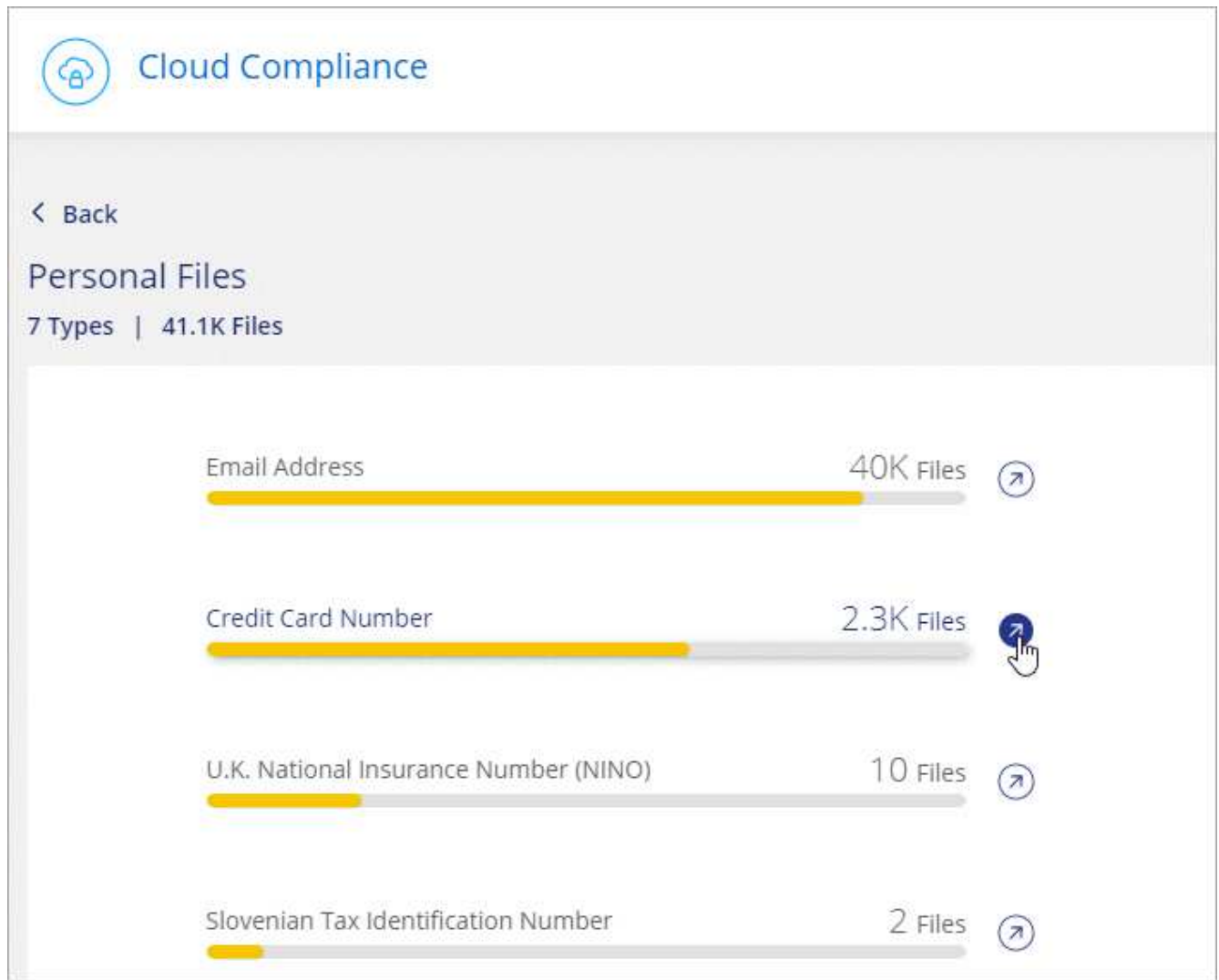
개인 데이터가 포함된 파일 보기

단계

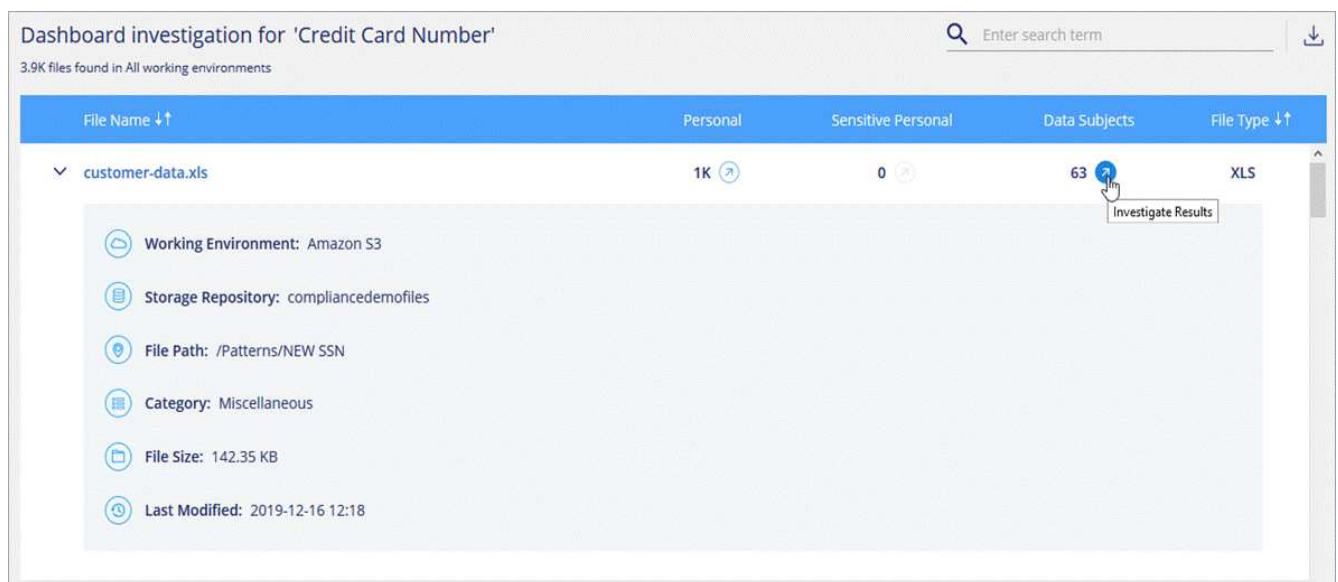
1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭하고 * Dashboard * 탭을 클릭합니다.
2. 모든 개인 데이터에 대한 세부 정보를 조사하려면 개인 데이터 백분율 옆에 있는 아이콘을 클릭합니다.



3. 특정 유형의 개인 데이터에 대한 세부 정보를 조사하려면 * 모두 보기 * 를 클릭한 다음 특정 유형의 개인 데이터에 대한 * 조사 결과 * 아이콘을 클릭합니다.



4. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을 다운로드하여 데이터를 조사합니다.



5. 조사 페이지의 내용을 필터링하여 원하는 결과만 표시할 수도 있습니다. 최상위 탭을 사용하면 파일(비정형 데이터)

또는 데이터베이스(구조화된 데이터)의 데이터를 볼 수 있습니다.

작업 환경, 스토리지 저장소, 범주, 개인 데이터, 파일 유형, 마지막으로 수정한 날짜 및 S3 오브젝트의 사용 권한이 공개 액세스에 대해 열려 있는지 여부를 나타냅니다.

Dashboard Investigation		Unstructured (32K Files)		Structured (323 DB Tables)		
FILTERS: Clear All		File Name	Personal	Sensitive Personal	Data Subjects	File Type
Working Environment 4 +	>	Expense Report EXP-TPO-10603888765435 cvo	6	3	16	PDF
Storage Repository +	>	Expense Report EXP-TPO-10603888765435 cvo	6	3	16	PDF
Category +	>	Expense Report EXP-TPO-10603888765435 cvo	6	3	16	PDF
Private Data 6 +	>	Expense Report EXP-TPO-10603888765435 cvo	6	3	16	PDF
File Type +	>	Expense Report EXP-TPO-10603888765435 cvo	6	3	16	PDF
	>	Expense Report EXP-TPO-10603888765435 cvo	6	3	16	PDF

개인 데이터의 유형입니다

파일에서 발견된 개인 데이터는 일반 개인 데이터 또는 국가 식별자일 수 있습니다. 세 번째 열에는 Cloud Compliance가 사용되는지 여부가 표시됩니다. [근접 확인](#) 식별자에 대한 결과를 검증합니다.

유형	ID입니다	근접성 검증?
일반	이메일 주소입니다	아니요
	신용 카드 번호입니다	아니요
	IBAN 번호(국제 은행 계좌 번호)	아니요

유형	ID입니다	근접성 검증?
국가 식별자	벨기에 iD(Numero National)	예
	브라질 ID(CPF)	예
	불가리아어 ID(UCN)	예
	캘리포니아 운전면허증	예
	크로아티아어 ID(OIB)	예
	키프로스 세금 식별 번호(TIC)	예
	체코어/슬로바키아어 ID	예
	덴마크어 ID(CPR)	예
	네덜란드어 ID(BSN)	예
	에스토니아어 ID	예
	핀란드 iD(HETU)	예
	프랑스어 세금 식별 번호(SPI)	예
	독일 세금 식별 번호(슈테루리체 식별 번호)	예
	그리스어 ID	예
	헝가리 세금 식별 번호	예
	아일랜드 ID(PPS)	예
	이스라엘 iD	예
	이탈리아 세금 식별 번호	예
	라트비아어 ID	예
	리투아니아어 ID	예
	룩셈부르크 ID입니다	예
	몰타 ID	예
	폴란드어 ID(PESEL)	예
	포르투갈어 세금 식별 번호(NIF)	예
	루마니아어 ID(CNP)	예
	슬로베니아어 ID(EMSO)	예
	남아프리카 ID	예
	스페인어 세금 식별 번호	예
	스웨덴 iD	예
	영국 ID(Nino)	예
미국 주민등록번호	예	

민감한 개인 데이터

Cloud Compliance는 와 같은 개인 정보 보호 규정에 정의된 대로 민감한 개인 정보의 특정 유형을 자동으로 식별합니다 "GDPR 9조 및 10조". 예를 들어, 개인의 건강, 인증 또는 성적 취향과 관련된 정보를 제공합니다. [전체 목록을 참조하십시오.](#)

Cloud Compliance는 인공 지능(AI), 자연어 처리(NLP), 머신 러닝(ML) 및 코그니티브 컴퓨팅(CC)을 사용하여 엔터티를 추출하고 그에 따라 범주화하기 위해 검색하는 내용의 의미를 파악합니다.

예를 들어, 중요한 GDPR 데이터 범주 중 하나는 인증입니다. 클라우드 규정 준수(Cloud Compliance)는 NLP 기능으로 인해 "George is Mexican"(GDPR 제9조에 명시된 민감한 데이터 표시)과 "George is eating Mexican food"라는 문장의 차이를 구별할 수 있습니다.

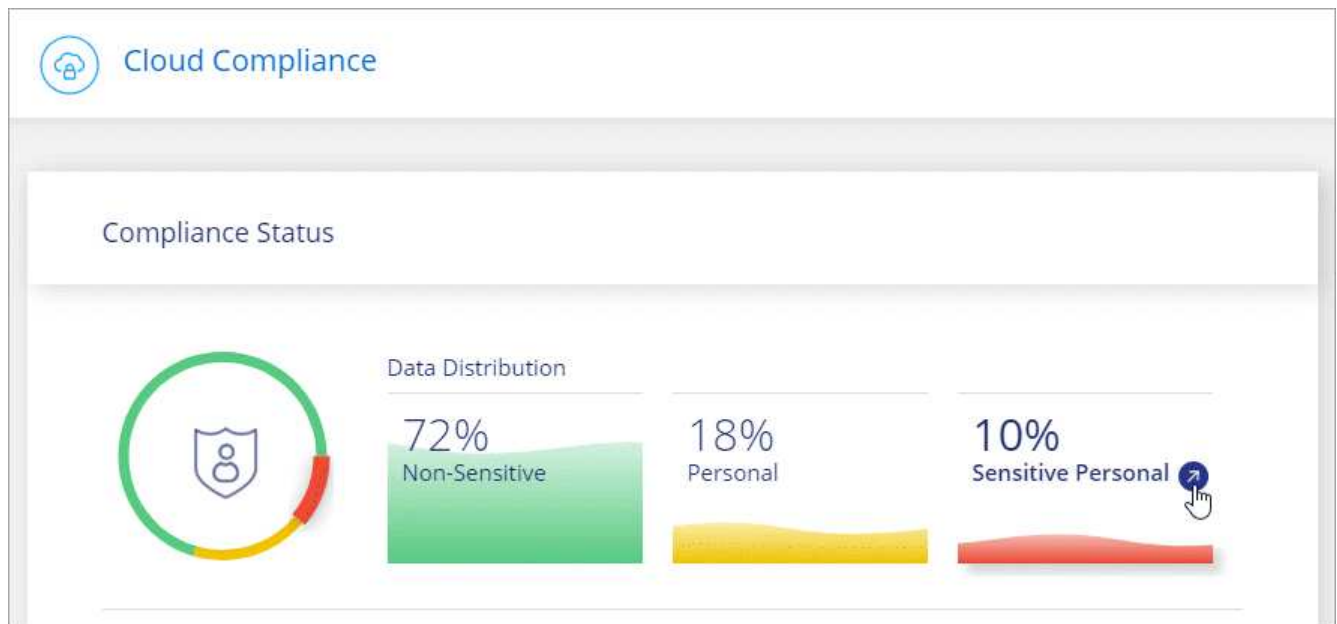


민감한 개인 데이터를 검색할 때는 영어로만 지원됩니다. 더 많은 언어에 대한 지원은 나중에 추가됩니다.

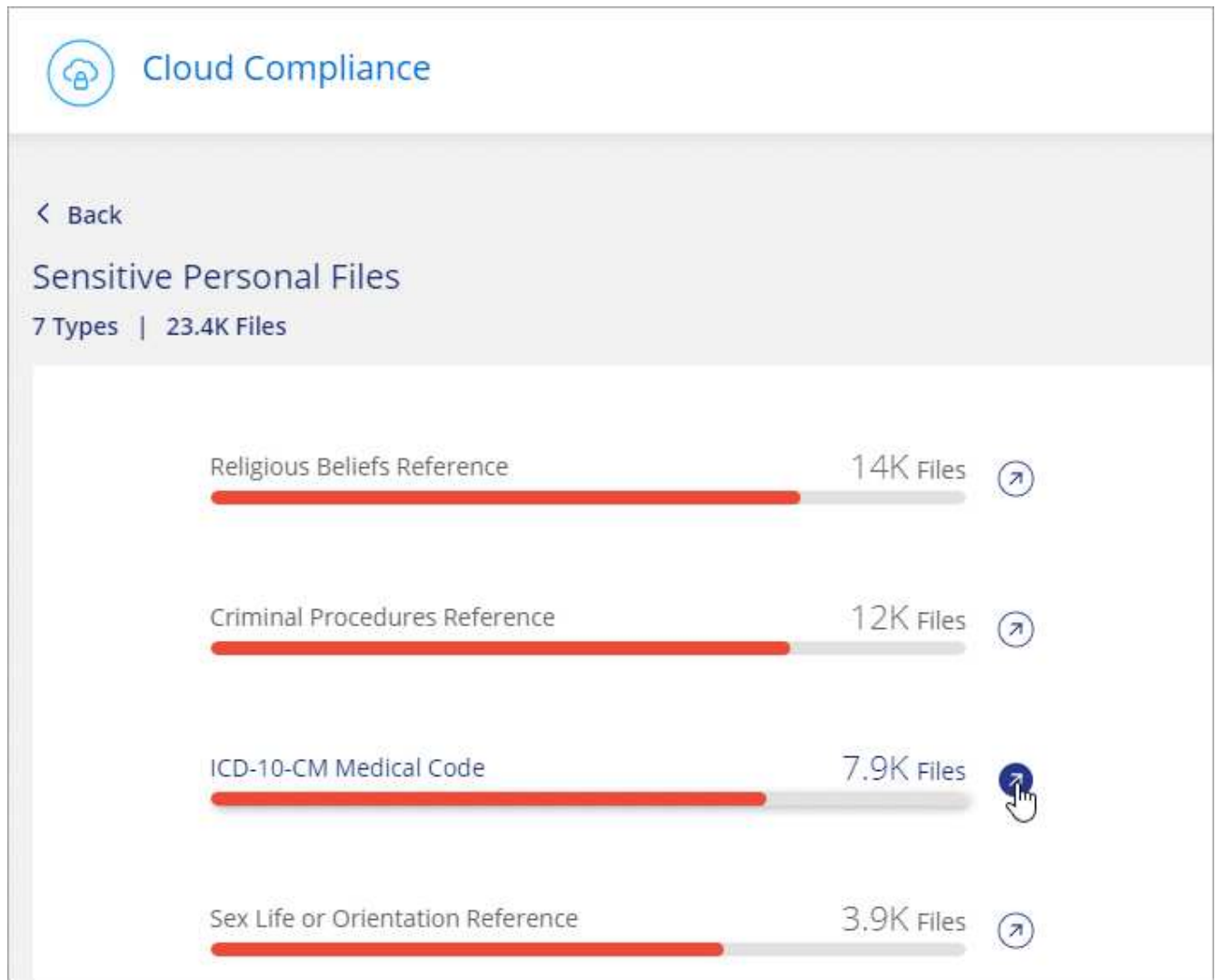
중요한 개인 데이터가 들어 있는 파일 보기

단계

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
2. 중요한 모든 개인 데이터에 대한 세부 정보를 조사하려면 중요한 개인 데이터 백분율 옆에 있는 아이콘을 클릭합니다.



3. 특정 유형의 중요한 개인 데이터에 대한 세부 정보를 조사하려면 * 모두 보기 * 를 클릭한 다음 특정 유형의 중요한 개인 데이터에 대해 * 결과 조사 * 아이콘을 클릭합니다.



4. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을 다운로드하여 데이터를 조사합니다.

중요한 개인 데이터의 유형

Cloud Compliance가 파일에서 찾을 수 있는 중요한 개인 데이터에는 다음이 포함됩니다.

형사 절차 참조

자연인의 범죄 소신 및 범죄에 관한 데이터.

인증 참조

자연인의 인증 또는 민족에 관한 데이터.

상태 참조

자연인의 건강에 관한 데이터.

ICD-9-cm 의료 코드

의료 및 의료 산업에서 사용되는 코드.

ICD-10-CM 의료 코드

의료 및 의료 산업에서 사용되는 코드.

철학적 신념 기준

자연인의 철학적 신념에 관한 데이터.

종교적 신념 참조

자연인의 종교적 신념에 관한 데이터.

성생활 또는 오리엔테이션 참조

자연인의 성생활 또는 성적 취향과 관련된 데이터.

범주

Cloud Compliance는 스캔한 데이터를 다양한 유형의 범주로 나눕니다. 범주는 각 파일의 콘텐츠 및 메타데이터에 대한 AI 분석을 기반으로 하는 주제입니다. [범주 목록을 참조하십시오.](#)

범주는 보유한 정보의 유형을 표시하여 데이터의 상태를 이해하는 데 도움이 됩니다. 예를 들어 이력서 또는 직원 계약과 같은 범주에는 중요한 데이터가 포함될 수 있습니다. 결과를 조사할 때 직원 계약이 안전하지 않은 위치에 저장되어 있는 것을 발견할 수 있습니다. 그런 다음 해당 문제를 해결할 수 있습니다.

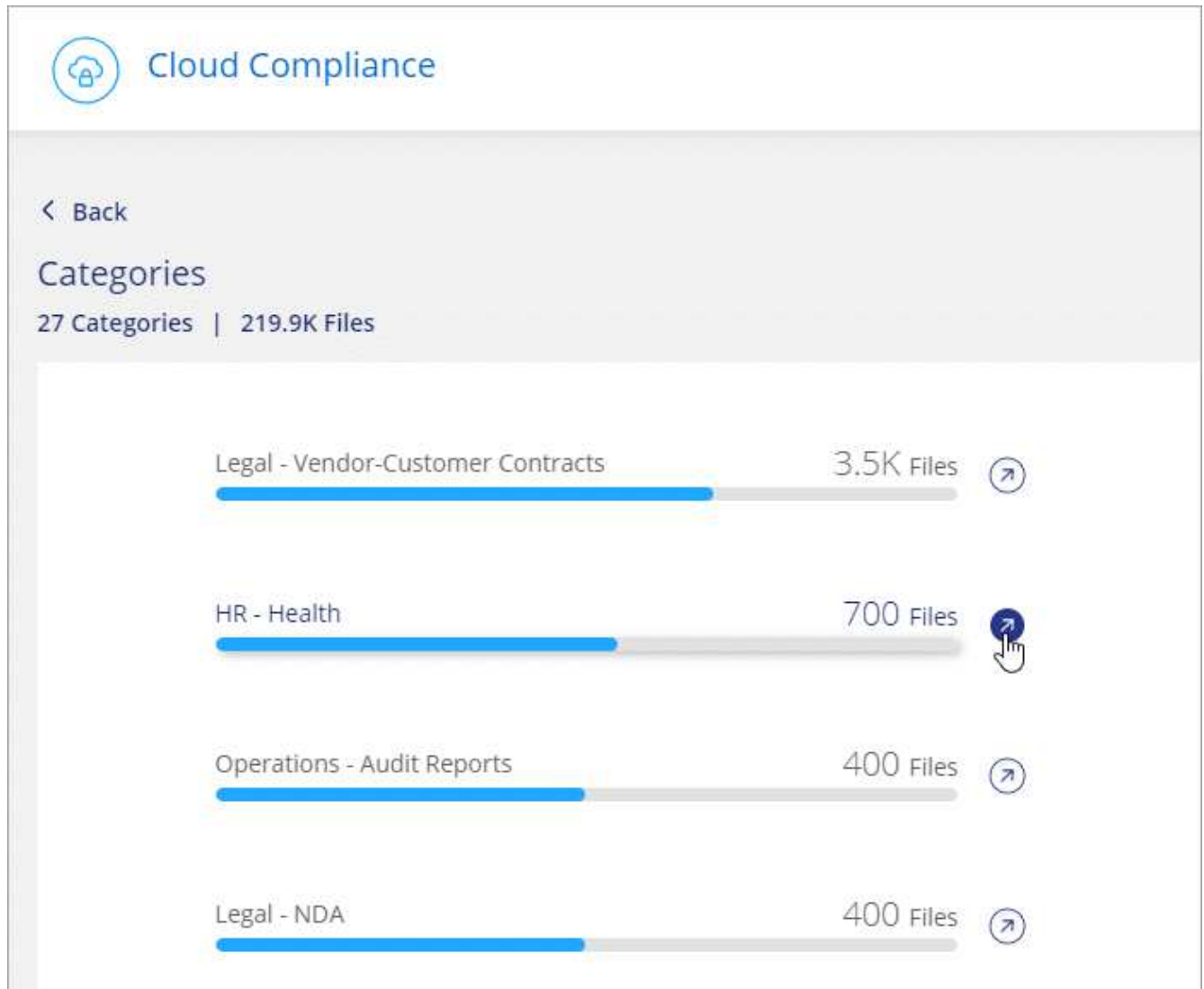


카테고리에는 영어만 지원됩니다. 더 많은 언어에 대한 지원은 나중에 추가됩니다.

범주별로 파일 보기

단계

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
2. 기본 화면에서 직접 상위 4개 범주 중 하나에 대한 * 조사 결과 * 아이콘을 클릭하거나 * 모두 보기 * 를 클릭한 다음 범주 중 하나에 대한 아이콘을 클릭합니다.



3. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을 다운로드하여 데이터를 조사합니다.

범주 유형

Cloud Compliance는 데이터를 다음과 같이 분류합니다.

재무

- 밸런스 시트
- 구매 주문
- 인보이스
- 분기별 보고서

시간

- 배경 확인
- 보상 계획
- 직원 계약

- 직원 검토
- 상태
- 다시 시작합니다

법적 고지

- NDAS
- 공급업체 - 고객 계약

마케팅

- 캠페인
- 회의

운영

- 감사 보고서

판매

- 판매 주문

서비스

- RFI
- RFP
- SOW
- 교육

지원

- 불만 및 티켓

메타데이터 범주입니다

- 애플리케이션 데이터
- 파일 보관
- 오디오
- 비즈니스 애플리케이션 데이터
- CAD 파일
- 코드
- 데이터베이스 및 인덱스 파일
- 설계 파일
- 이메일 애플리케이션 데이터
- 실행 파일
- 재무 애플리케이션 데이터
- 상태 응용 프로그램 데이터
- 이미지

- 로그
- 기타 문서
- 기타 프레젠테이션
- 기타 스프레드시트
- 비디오

파일 형식

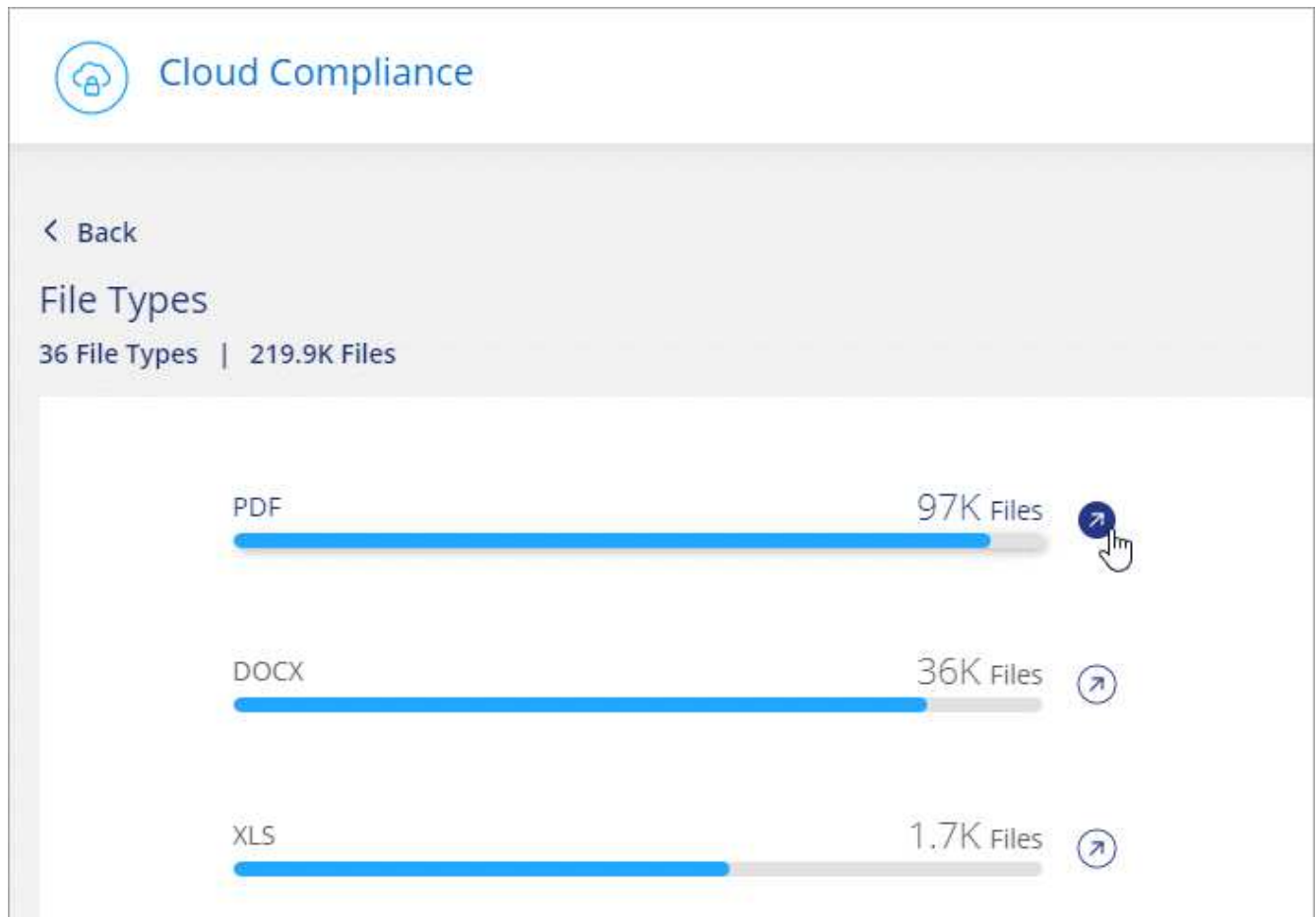
Cloud Compliance는 스캔한 데이터를 파일 유형에 따라 분해합니다. 파일 형식을 검토하면 특정 파일 형식이 올바르게 저장되지 않은 것을 발견할 수 있으므로 중요한 데이터를 제어하는 데 도움이 됩니다. [파일 형식 목록을 참조하십시오.](#)

예를 들어 조직에 대한 매우 중요한 정보가 포함된 CAD 파일을 저장할 수 있습니다. 보안이 설정되지 않은 경우 사용 권한을 제한하거나 파일을 다른 위치로 이동하여 중요한 데이터를 제어할 수 있습니다.

파일 형식 보기

단계

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
2. 기본 화면에서 직접 상위 4개 파일 유형 중 하나에 대한 * 조사 결과 * 아이콘을 클릭하거나 * 모두 보기 * 를 클릭한 다음 파일 유형에 대한 아이콘을 클릭합니다.



3. 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 * 결과 조사 * 를 클릭하여 마스킹된 정보를 보거나 파일 목록을

다운로드하여 데이터를 조사합니다.

파일 유형

Cloud Compliance는 모든 파일에서 범주 및 메타데이터 정보를 검색하고 대시보드의 파일 유형 섹션에 모든 파일 유형을 표시합니다.

그러나 클라우드 규정 준수에서 PII(개인 식별 정보)를 감지하거나 DSAR 검색을 수행할 경우 .pdf, .DOCX, .DOC, .PPTX, .XLS, XLSX, .csv, .TXT, .rtf 및 .JSON.

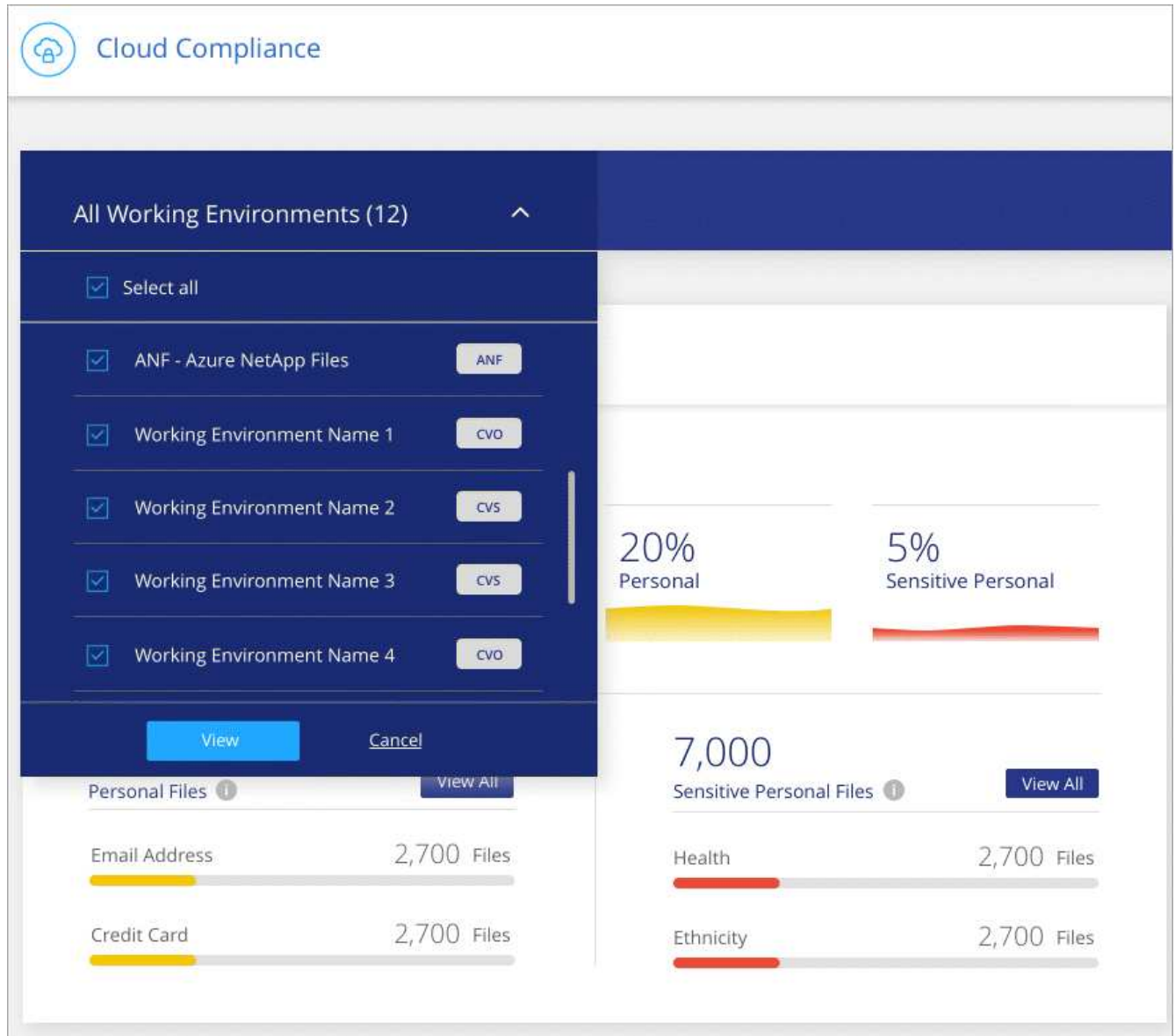
특정 작업 환경의 데이터 보기

Cloud Compliance 대시보드의 내용을 필터링하여 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터를 보거나 특정 작업 환경에 대한 규정 준수 데이터를 볼 수 있습니다.

대시보드를 필터링할 때 Cloud Compliance는 규정 준수 데이터와 보고서를 선택한 작업 환경만 표시하도록 지정합니다.

단계

1. 필터 드롭다운을 클릭하고 데이터를 보려는 작업 환경을 선택한 다음 * 보기 * 를 클릭합니다.



정보가 정확합니다

NetApp은 Cloud Compliance에서 식별한 개인 데이터 및 중요한 개인 데이터의 100% 정확성을 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 확인해야 합니다.

테스트를 기준으로 아래 표는 Cloud Compliance에서 찾은 정보의 정확성을 보여줍니다. 정밀 _ 및 _ 리콜 _ 을(를) 통해 분해합니다.

정밀도

Cloud Compliance가 발견한 가능성이 올바르게 식별되었습니다. 예를 들어, 개인 데이터의 정밀도가 90%이면 개인 정보가 포함된 것으로 확인된 10개 파일 중 9개가 개인 정보를 포함하고 있음을 의미합니다. 10개 파일 중 1개는 위양성입니다.

리콜

클라우드 규정 준수에서 필요한 것을 찾을 수 있는 가능성 예를 들어, 개인 데이터의 리콜 비율이 70%인 경우 Cloud Compliance는 사용자 조직의 개인 정보가 실제로 포함된 10개 파일 중 7개를 식별할 수 있습니다. Cloud Compliance는 데이터의 30%를 놓치게 되며 대시보드에 표시되지 않습니다.

Cloud Compliance는 제어된 가용성 릴리스에 들어 있으며 결과의 정확성을 지속적으로 개선하고 있습니다. 이러한 개선 사항은 향후 클라우드 규정 준수 릴리스에서 자동으로 제공됩니다.

유형	정밀도	리콜
개인 데이터 - 일반	90% - 95%	60%~80%
개인 데이터 - 국가 식별자	30% ~ 60%	40% ~ 60%
민감한 개인 데이터	80% - 95%	20% - 30%
범주	90% - 97%	60%~80%

각 파일 목록 보고서(CSV 파일)에 포함된 내용

각 조사 페이지에서 식별된 파일에 대한 세부 정보가 포함된 파일 목록(CSV 형식)을 다운로드할 수 있습니다. 10,000개가 넘는 결과가 있는 경우 최상위 10,000개만 목록에 표시됩니다.

각 파일 목록에는 다음 정보가 포함됩니다.

- 파일 이름입니다
- 위치 유형
- 작업 환경
- 저장소 저장소
- 프로토콜
- 파일 경로
- 파일 형식
- 범주
- 개인 정보
- 민감한 개인 정보
- 삭제 감지 날짜입니다

삭제 감지 날짜는 파일이 삭제되거나 이동된 날짜를 나타냅니다. 이렇게 하면 중요한 파일이 이동된 시기를 식별할 수 있습니다. 삭제된 파일은 대시보드나 조사 페이지에 나타나는 파일 번호 개수에 포함되지 않습니다. 파일은 CSV 보고서에만 나타납니다.

준수 보고서 보기

Cloud Compliance는 조직의 데이터 개인 정보 보호 프로그램 상태를 더 잘 이해하는 데 사용할 수 있는 보고서를 제공합니다.

기본적으로 Cloud Compliance 대시보드에는 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터가 표시됩니다. 일부 작업 환경에 대한 데이터만 포함된 보고서를 보려면 [작업 환경을 선택합니다](#).



NetApp은 Cloud Compliance에서 식별한 개인 데이터 및 중요한 개인 데이터의 100% 정확성을 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 확인해야 합니다.

개인 정보 보호 위험 평가 보고서

개인 정보 보호 위험 평가 보고서는 GDPR 및 CCPA와 같은 개인 정보 보호 규정에 따라 조직의 개인 정보 보호 위험 상태에 대한 개요를 제공합니다. 보고서에는 다음 정보가 포함됩니다.

준수 상태

A **심각도 점수** 또한 데이터가 중요하지 않거나 개인적이거나 민감한 개인이든 상관없이 배포할 수 있습니다.

평가 개요

발견된 개인 데이터 유형 및 데이터 범주에 대한 분석.

이 평가의 데이터 주체

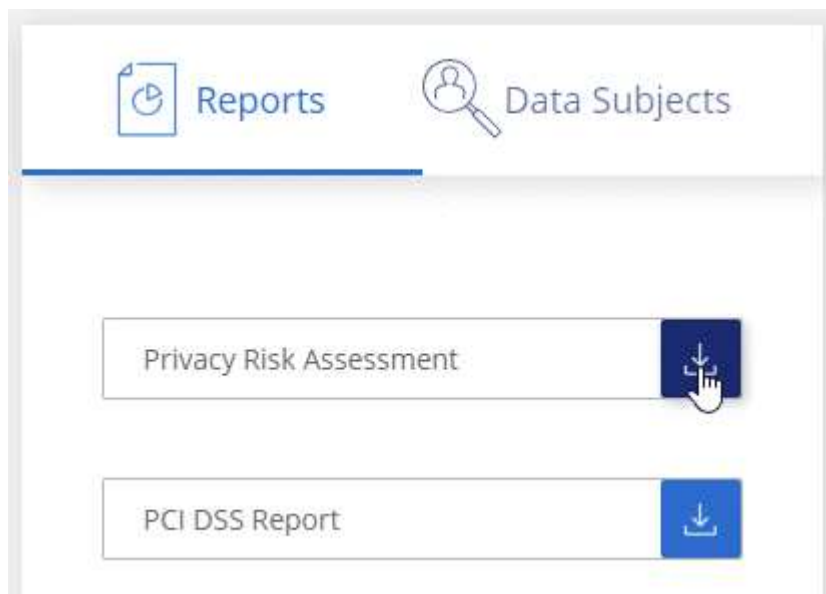
국가 식별자가 발견된 위치별 사람 수.

개인 정보 보호 위험 평가 보고서 생성

준수 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
2. 보고서 * 에서 * 개인 정보 위험 평가 * 옆에 있는 다운로드 아이콘을 클릭합니다.



결과

Cloud Compliance는 PDF 보고서를 생성하여 필요한 경우 다른 그룹에 검토 및 전송할 수 있습니다.

심각도 점수

클라우드 규정 준수 는 세 가지 변수를 기준으로 개인 정보 보호 위험 평가 보고서의 심각도 점수를 계산합니다.

- 모든 데이터 중 개인 데이터의 비율입니다.
- 모든 데이터 중 중요한 개인 데이터의 비율입니다.

- 국가 ID, 사회 보장 번호 및 세금 ID 번호와 같은 국가 식별자에 의해 결정되는 데이터 주제가 포함된 파일의 비율입니다.

점수를 결정하는 데 사용되는 논리는 다음과 같습니다.

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

PCI DSS 보고서

PCI DSS(Payment Card Industry Data Security Standard) 보고서를 통해 파일 전체에서 신용 카드 정보의 분포를 확인할 수 있습니다. 보고서에는 다음 정보가 포함됩니다.

개요

신용 카드 정보와 작업 환경이 포함된 파일 수

암호화

암호화 또는 암호화되지 않은 작업 환경에 있는 신용 카드 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

랜섬웨어 보호

랜섬웨어 보호가 활성화된 작업 환경에 있는 신용 카드 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

보존

파일이 마지막으로 수정된 기간. 이 기능은 신용 카드 정보를 처리하는 데 필요한 것보다 더 오래 보관해서는 안 되기 때문에 유용합니다.

신용 카드 정보 배포

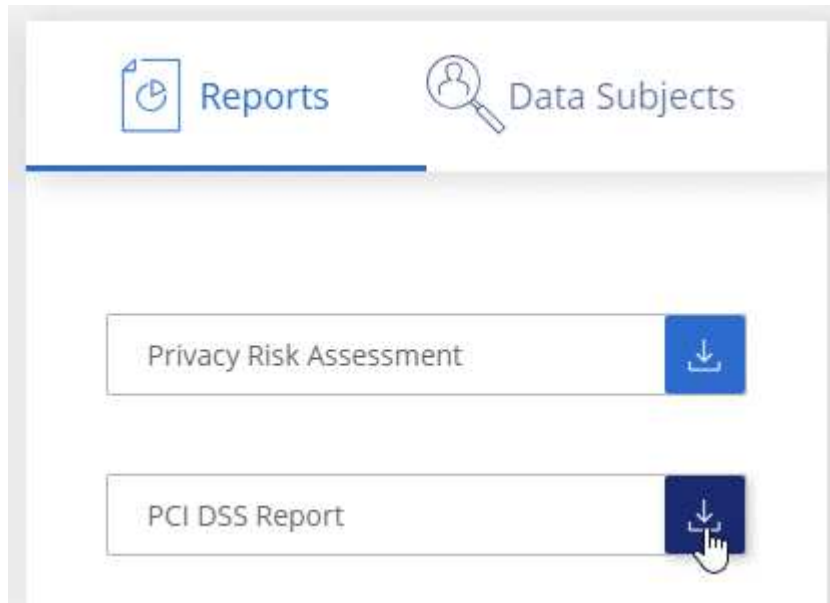
신용 카드 정보가 발견된 작업 환경 및 암호화 및 랜섬웨어 방지 기능이 활성화되어 있는지 여부

PCI DSS 보고서 생성

준수 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
2. 보고서 * 에서 * PCI DSS 보고서 * 옆에 있는 다운로드 아이콘을 클릭합니다.



결과

Cloud Compliance는 PDF 보고서를 생성하여 필요한 경우 다른 그룹에 검토 및 전송할 수 있습니다.

HIPAA 보고서

HIPAA(Health Insurance Portability and Accountability Act) 보고서를 통해 건강 정보가 포함된 파일을 확인할 수 있습니다. 이 솔루션은 HIPAA 데이터 개인 정보 보호법을 준수하기 위한 조직의 요구 사항을 지원하도록 설계되었습니다. Cloud Compliance에서 찾는 정보는 다음과 같습니다.

- 상태 참조 패턴
- ICD-10-cm 의료 코드
- ICD-9-cm 의료 코드
- HR – 건강 범주
- 상태 응용 프로그램 데이터 범주입니다

보고서에는 다음 정보가 포함됩니다.

개요

상태 정보가 포함된 파일 수와 작업 환경이 포함된 파일 수

암호화

암호화 또는 암호화되지 않은 작업 환경에 있는 상태 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

랜섬웨어 보호

랜섬웨어 보호가 활성화된 작업 환경에 대한 상태 정보가 포함된 파일의 비율입니다. 이 정보는 Cloud Volumes ONTAP에만 해당됩니다.

보존

파일이 마지막으로 수정된 기간. 이 기능은 건강 정보를 처리하는 데 필요한 것보다 오래 보관할 필요가 없기 때문에 유용합니다.

건강 정보 배포

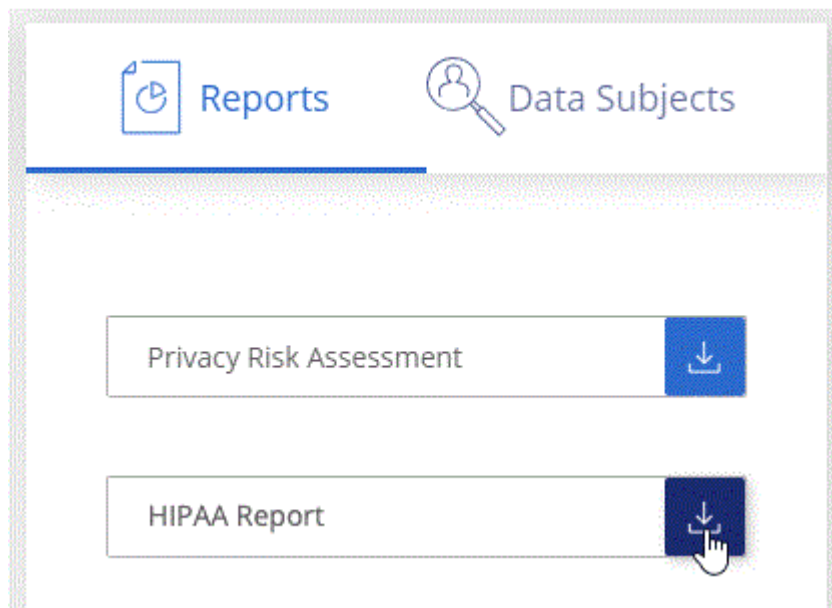
상태 정보가 발견된 작업 환경 및 암호화 및 랜섬웨어 방지 기능이 활성화되어 있는지 여부

HIPAA 보고서 생성

준수 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
2. 보고서 * 에서 * HIPAA 보고서 * 옆에 있는 다운로드 아이콘을 클릭합니다.



결과

Cloud Compliance는 PDF 보고서를 생성하여 필요한 경우 다른 그룹에 검토 및 전송할 수 있습니다.

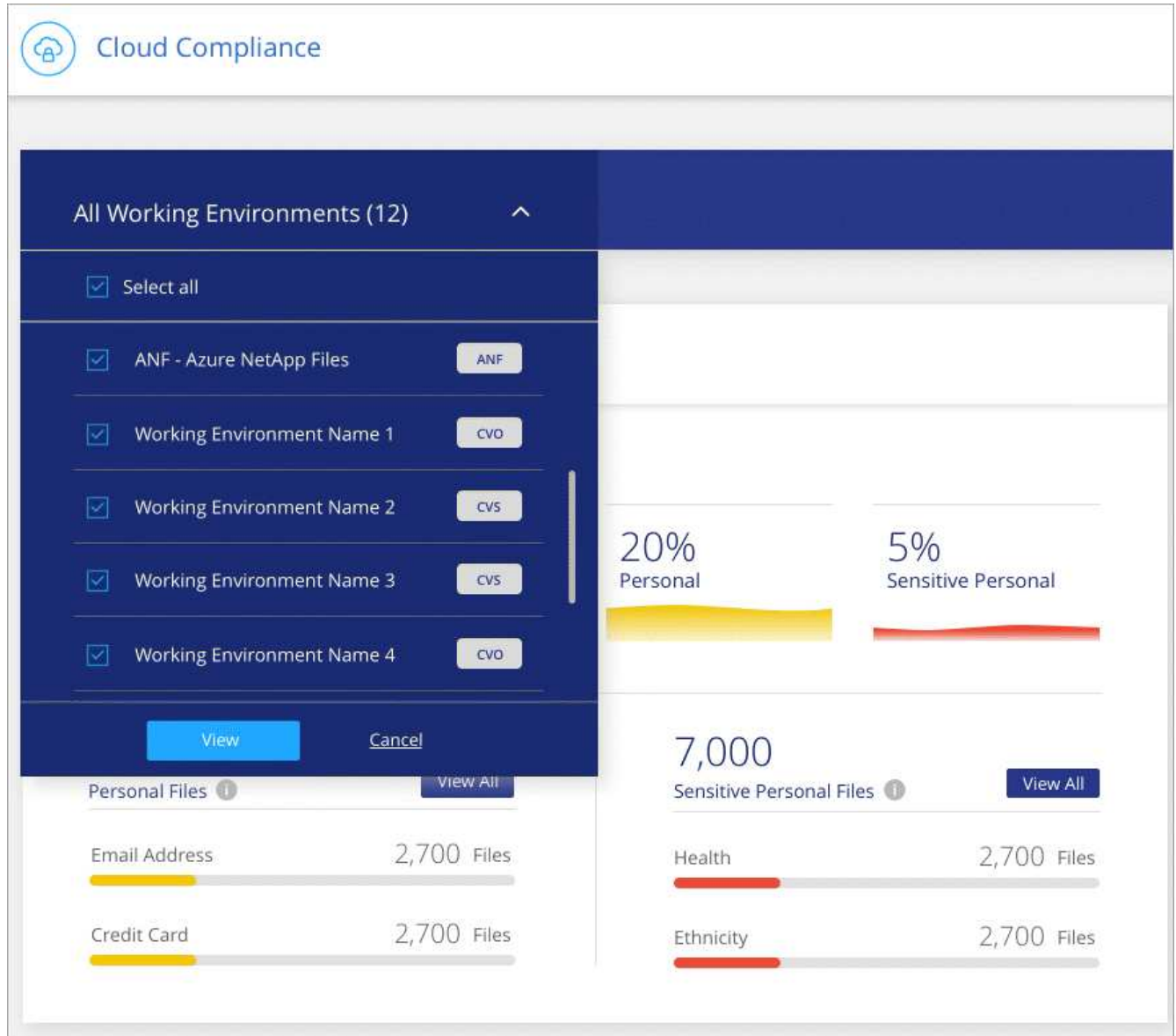
보고서에 사용할 작업 환경 선택

Cloud Compliance 대시보드의 내용을 필터링하여 모든 작업 환경 및 데이터베이스에 대한 규정 준수 데이터를 보거나 특정 작업 환경에 대한 규정 준수 데이터를 볼 수 있습니다.

대시보드를 필터링할 때 Cloud Compliance는 규정 준수 데이터와 보고서를 선택한 작업 환경만 표시하도록 지정합니다.

단계

1. 필터 드롭다운을 클릭하고 데이터를 보려는 작업 환경을 선택한 다음 * 보기 * 를 클릭합니다.



데이터 주체 액세스 요청에 응답

피해자의 전체 이름 또는 알려진 식별자(예: 이메일 주소)를 검색한 다음 보고서를 다운로드하여 Data Subject Access Request(SAR)에 응답합니다. 이 보고서는 GDPR 또는 이와 유사한 데이터 개인 정보 보호 법률을 준수하기 위한 조직의 요구 사항을 지원하도록 설계되었습니다.



NetApp은 Cloud Compliance에서 식별한 개인 데이터 및 중요한 개인 데이터의 100% 정확성을 보장할 수 없습니다. 항상 데이터를 검토하여 정보의 유효성을 확인해야 합니다.

데이터 주체 액세스 요청이란 무엇입니까?

유럽 GDPR과 같은 개인 정보 보호 규정은 데이터 주체(고객 또는 직원 등)에게 개인 데이터에 액세스할 수 있는 권한을 부여합니다. 데이터 피해자가 이 정보를 요청하는 경우 이를 SAR(데이터 주체 액세스 요청)이라고 합니다. 조직은 이러한 요청에 대해 "부당한 지연 없이", 그리고 수령일로부터 1개월 이내에 응답해야 합니다.

SAR에 대응하는 데 클라우드 규정 준수는 어떻게 도움이 됩니까?

데이터 주체 검색을 수행할 때 Cloud Compliance는 해당 사용자의 이름이나 식별자가 포함된 모든 파일을 찾습니다. Cloud Compliance는 이름 또는 식별자에 대해 사전 인덱싱된 최신 데이터를 확인합니다. 새 스캔은 시작되지 않습니다.

검색이 완료되면 데이터 주체 액세스 요청 보고서에 대한 파일 목록을 다운로드할 수 있습니다. 이 보고서는 데이터에서 얻은 통찰력을 집계하여 해당 사람에게 다시 보낼 수 있는 법적 용어로 저장합니다.

데이터 주체 검색 및 보고서 다운로드

데이터 주체의 전체 이름 또는 알려진 식별자를 검색한 다음 파일 목록 보고서 또는 DSAR 보고서를 다운로드합니다. 검색할 수 있는 기준 "모든 개인 정보 유형입니다".

데이터 제목 이름을 검색할 때는 영어로만 지원됩니다. 더 많은 언어에 대한 지원은 나중에 추가됩니다.

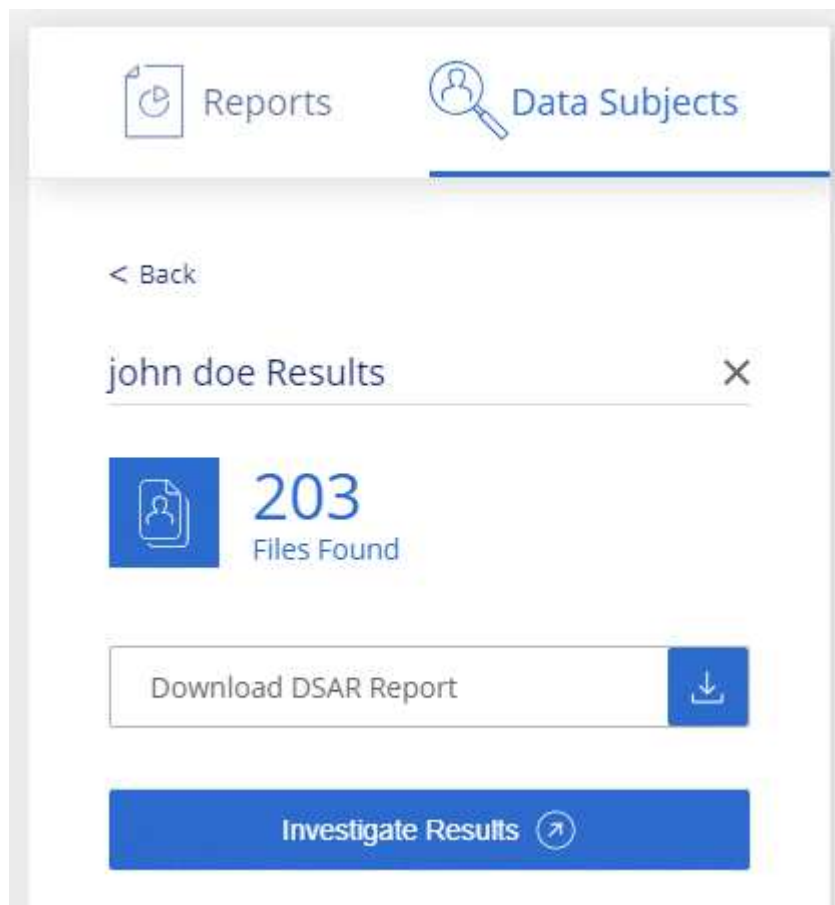


현재 데이터베이스 내에서 데이터 주체 검색이 지원되지 않습니다.

단계

1. Cloud Manager 상단에서 * Cloud Compliance * 를 클릭합니다.
2. 데이터 제목 * 을 클릭합니다.
3. 데이터 제목의 전체 이름 또는 알려진 식별자를 검색합니다.

다음은 name_john doe_에 대한 검색을 보여 주는 예입니다.



4. 사용 가능한 옵션 중 하나를 선택합니다.

- * DSAR 보고서 다운로드 *: 데이터 주체에 전송할 수 있는 액세스 요청에 대한 공식 응답입니다. 이 보고서에는 데이터 주체에 대해 Cloud Compliance에서 찾아 템플릿으로 사용하도록 설계된 데이터를 기반으로 자동으로 생성된 정보가 포함됩니다. 양식을 작성하여 내부적으로 검토한 후 데이터 제목으로 보내야 합니다.
- * 결과 조사 *: 특정 파일에 대한 세부 정보를 검색, 정렬, 확장하고 파일 목록을 다운로드하여 데이터를 조사할 수 있는 페이지입니다.



10,000개가 넘는 결과가 있을 경우 파일 목록에 최상위 10,000개만 표시됩니다.

클라우드 규정 준수 비활성화

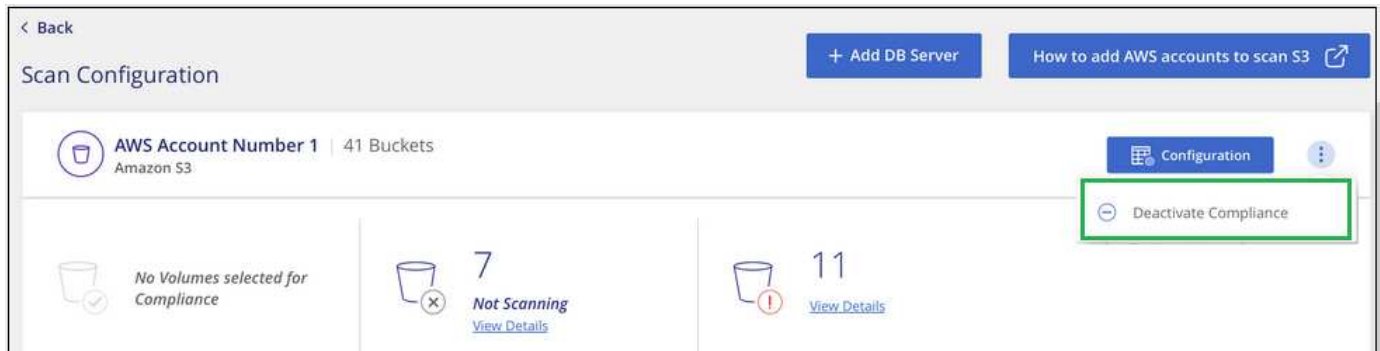
필요한 경우 클라우드 규정 준수가 하나 이상의 작업 환경 또는 데이터베이스를 스캐닝하지 못하도록 할 수 있습니다. 또한 작업 환경에서 Cloud Compliance를 더 이상 사용하지 않으려는 경우 Cloud Compliance 인스턴스를 삭제할 수 있습니다.

작업 환경에 대한 규정 준수 검사 비활성화

스캔을 비활성화하면 Cloud Compliance는 더 이상 시스템의 데이터를 스캔하지 않고 Cloud Compliance 인스턴스에서 인덱싱된 규정 준수 정보를 제거합니다(작업 환경 또는 데이터베이스 자체의 데이터는 삭제되지 않음).

단계

Scan Configuration_ 페이지에서 을 클릭합니다  단추를 클릭한 다음 * 준수 비활성화 * 를 클릭합니다.



작업 환경을 선택할 때 서비스 패널에서 작업 환경에 대한 준수 검사를 비활성화할 수도 있습니다.

Cloud Compliance 인스턴스 삭제

Cloud Compliance를 더 이상 사용하지 않으려면 Cloud Compliance 인스턴스를 삭제할 수 있습니다. 인스턴스를 삭제하면 인덱싱된 데이터가 있는 연결된 디스크도 삭제됩니다.

단계

1. 클라우드 공급자의 콘솔로 이동하여 Cloud Compliance 인스턴스를 삭제합니다.

인스턴스의 이름은 *CloudCompliance_*이며 생성된 해시(UUID)와 연결됩니다. 예: *_CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*

클라우드 규정 준수에 대한 FAQ

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

클라우드 규정 준수란?

클라우드 규정 준수는 인공지능(AI) 기반 기술을 사용하는 클라우드 오퍼링으로, 조직에서 Azure NetApp Files 구성, AWS 또는 Azure에서 호스팅되는 Cloud Volumes ONTAP 시스템, Amazon S3 버킷 및 데이터베이스 전반의 중요 데이터를 파악하고 데이터 컨텍스트를 이해하는 데 도움을 줍니다.

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

클라우드 규정 준수를 사용해야 하는 이유는 무엇입니까?

Cloud Compliance는 데이터를 통해 다음과 같은 이점을 제공합니다.

- 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.

클라우드 규정 준수의 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 규정 준수 사용 사례에 대해 자세히 알아보십시오"](#).

Cloud Compliance로 스캔할 수 있는 데이터 유형은 무엇입니까?

Cloud Compliance는 Cloud Volumes ONTAP 및 Azure NetApp Files에서 관리하는 NFS 및 CIFS 프로토콜을 통해 비정형 데이터 스캔을 지원합니다. Cloud Compliance는 Amazon S3 버킷에 저장된 데이터도 스캔할 수 있습니다.

또한 Cloud Compliance는 Cloud Manager로 관리할 필요가 없는 데이터베이스를 어디서나 스캔할 수 있습니다.

["스캔 작동 방식에 대해 알아보십시오"](#).

지원되는 클라우드 공급자는 무엇입니까?

Cloud Compliance는 Cloud Manager의 일부로 작동하며 현재 AWS 및 Azure를 지원합니다. 이를 통해 조직은 다양한 클라우드 공급자 전반에서 통합된 개인 정보 보호 가시성을 확보할 수 있습니다. Google Cloud Platform(GCP) 지원이 곧 추가될 예정입니다.

클라우드 규정 준수에 어떻게 액세스합니까?

Cloud Manager를 통해 클라우드 규정 준수를 운영 및 관리합니다. Cloud Manager의 * 규정 준수 * 탭에서 클라우드 규정 준수 기능에 액세스할 수 있습니다.

클라우드 규정 준수는 어떻게 작동합니까?

Cloud Compliance는 Cloud Manager 시스템 및 스토리지 시스템과 함께 또 다른 인공지능 계층을 구축합니다. 그런 다음 볼륨, 버킷 및 데이터베이스의 데이터를 검색하고 검색된 데이터 인사이트를 인덱싱합니다.

["클라우드 규정 준수 방식에 대해 자세히 알아보십시오"](#).

클라우드 규정 준수 비용은 얼마입니까?

Cloud Compliance 사용 비용은 스캔 중인 데이터의 양에 따라 다릅니다. Cloud Manager 작업 공간에서 Cloud Compliance에서 스캔하는 첫 1TB의 데이터는 무료입니다. AWS 또는 Azure Marketplace에 가입해야 해당 시점 이후에 데이터를 계속 스캔할 수 있습니다. 을 참조하십시오 ["가격"](#) 를 참조하십시오.

Cloud Compliance는 내 데이터를 얼마나 자주 스캔합니까?

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

["스캔 작동 방식에 대해 알아보십시오"](#).

클라우드 규정 준수에서 보고서를 제공합니까?

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

클라우드 규정 준수에 대한 다음 보고서가 제공됩니다.

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"](#).

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"](#).

클라우드 규정 준수에 필요한 인스턴스 또는 VM 유형은 무엇입니까?

- Azure에서 클라우드 규정 준수는 512GB 디스크가 있는 Standard_D16s_v3 VM에서 실행됩니다.
- AWS에서 Cloud Compliance는 500GB GP2 디스크를 사용하는 m5.4x대용량 인스턴스에서 실행됩니다.
m5.4x4Large를 사용할 수 없는 지역에서는 Cloud Compliance가 대신 m4.4x4대형 인스턴스에서 실행됩니다.



인스턴스/VM 유형의 변경 또는 크기 조정은 지원되지 않습니다. 제공된 기본 크기를 사용해야 합니다.

"클라우드 규정 준수 방식에 대해 자세히 알아보십시오".

스캔 성능이 달라집니까?

스캔 성능은 클라우드 환경의 네트워크 대역폭과 평균 파일 크기에 따라 달라질 수 있습니다.

지원되는 파일 유형은 무엇입니까?

Cloud Compliance는 모든 파일에서 범주 및 메타데이터 정보를 검색하고 대시보드의 파일 유형 섹션에 모든 파일 유형을 표시합니다.

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

클라우드 규정 준수를 어떻게 활성화합니까?

먼저 Cloud Manager에서 Cloud Compliance 인스턴스를 구축해야 합니다. 인스턴스가 실행 중이면 * Compliance * 탭에서 기존 작업 환경 및 데이터베이스에서 활성화하거나 특정 작업 환경을 선택할 수 있습니다.

"시작하는 방법을 알아보십시오".



Cloud Compliance를 활성화하면 즉시 초기 스캔이 됩니다. 준수 결과는 잠시 후에 표시됩니다.

클라우드 규정 준수를 비활성화하려면 어떻게 해야 합니까?

개별 작업 환경을 선택한 후 작업 환경 페이지에서 클라우드 규정 준수를 비활성화할 수 있습니다.

"자세한 정보".



Cloud Compliance 인스턴스를 완전히 제거하려면 클라우드 공급자의 포털에서 Cloud Compliance 인스턴스를 수동으로 제거해야 합니다.

Cloud Volumes ONTAP에서 데이터 계층화를 활성화하면 어떻게 됩니까?

오브젝트 스토리지에 콜드 데이터를 계층화하는 Cloud Volumes ONTAP 시스템에서 클라우드 규정 준수를 활성화할 수 있습니다. 데이터 계층화를 사용할 경우 Cloud Compliance는 디스크에 있는 데이터와 오브젝트 스토리지에 대한 콜드 데이터 등 모든 데이터를 검사합니다.

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

클라우드 규정 준수를 사용하여 사내 **ONTAP** 스토리지를 검색할 수 있습니까?

온-프레미스 ONTAP 작업 환경에서 직접 데이터를 스캔하는 것은 지원되지 않습니다. 하지만 사내 NFS 또는 CIFS 데이터를 Cloud Volumes ONTAP 작업 환경에 복제하고 해당 볼륨에 대한 규정 준수를 활성화하여 온프레미스 ONTAP 데이터를 스캔할 수 있습니다. NetApp은 Cloud Volumes Service와 같은 추가 클라우드 오퍼링을 통해 클라우드 규정 준수를 지원할 계획입니다.

["자세한 정보"](#).

Cloud Compliance는 내 조직에 알림을 전송할 수 있습니까?

아니요. 하지만 조직 내부에서 공유할 수 있는 상태 보고서를 다운로드할 수 있습니다.

조직의 필요에 맞게 서비스를 사용자 정의할 수 있습니까?

Cloud Compliance는 즉각적인 데이터 통찰력을 제공합니다. 이러한 통찰력을 추출하여 조직의 요구에 활용할 수 있습니다.

클라우드 규정 준수 정보를 특정 사용자로 제한할 수 있습니까?

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

또한 특정 사용자가 클라우드 규정 준수 설정을 관리할 수 없는 상태에서 클라우드 규정 준수 검사 결과만 볼 수 있도록 허용하려면 해당 사용자에게 `_Cloud Compliance Viewer_` 역할을 할당할 수 있습니다.

["자세한 정보"](#).

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.