개인정보 데이터 보호 파악

Cloud Manager 3.7

NetApp
March 25, 2024

목차

개인정보 데이터 보호 파악

클라우드 규정 준수에 대해 알아보십시오

클라우드 규정 준수 는 AWS 및 Azure의 Cloud Volumes ONTAP를 위한 데이터 개인 정보 보호 및 규정 준수 서비스입니다. 클라우드 규정 준수 는 인공 지능(AI) 중심 기술을 사용하여 조직의 데이터 컨텍스트를 이해하고 Cloud Volumes ONTAP 시스템 전체에서 중요한 데이터를 식별할 수 있도록 지원합니다.

Cloud Compliance는 현재 제어된 가용성 릴리즈로 제공됩니다.

"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

비용

Cloud Compliance는 NetApp에서 추가 비용 없이 제공하는 Cloud Volumes ONTAP용 애드온 서비스입니다. Cloud Compliance를 활성화하려면 클라우드 인스턴스를 배포해야 하며 이 경우 클라우드 공급자가 비용을 부담합니다. 데이터가 네트워크 외부로 흐르지 않기 때문에 데이터 수신 또는 송신에 대한 비용은 없습니다.

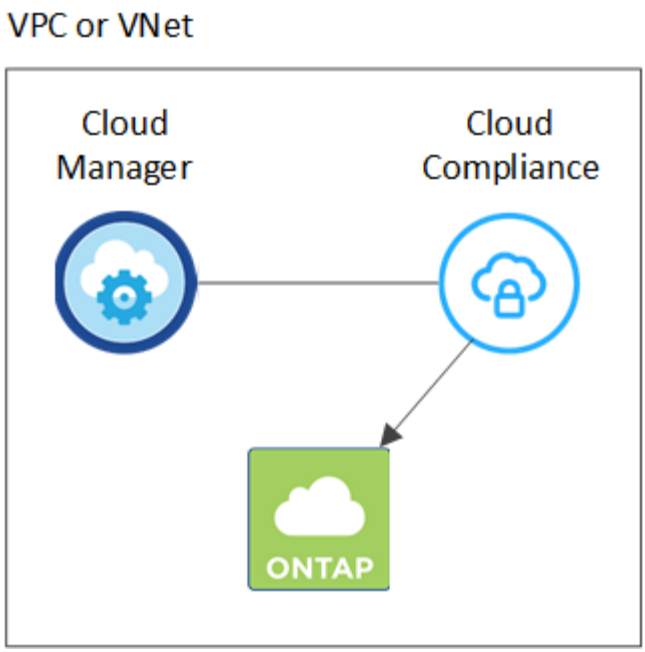
클라우드 규정 준수 방식

높은 수준에서 클라우드 규정 준수는 다음과 같이 작동합니다.

1. 하나 이상의 Cloud Volumes ONTAP 시스템에서 클라우드 규정 준수를 지원합니다.
2. Cloud Compliance는 AI 학습 프로세스를 사용하여 데이터를 스캔합니다.
3. Cloud Manager에서 * Compliance * 를 클릭하고 제공된 대시보드 및 보고 도구를 사용하여 규정 준수 작업을 돕습니다.

클라우드 규정 준수 인스턴스

하나 이상의 Cloud Volumes ONTAP 시스템에서 클라우드 규정 준수를 활성화하면 Cloud Manager가 요청에 따라 첫 번째 Cloud Volumes ONTAP 시스템으로 동일한 VPC 또는 VNET에 클라우드 규정 준수 인스턴스를 배포합니다.



인스턴스에 대한 다음 사항에 유의하십시오.

- Azure에서 클라우드 규정 준수는 512GB 디스크가 있는 Standard_D16s_v3 VM에서 실행됩니다.
- AWS에서 Cloud Compliance는 500GB io1 디스크를 사용하는 m5.4x대용량 인스턴스에서 실행됩니다.

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

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

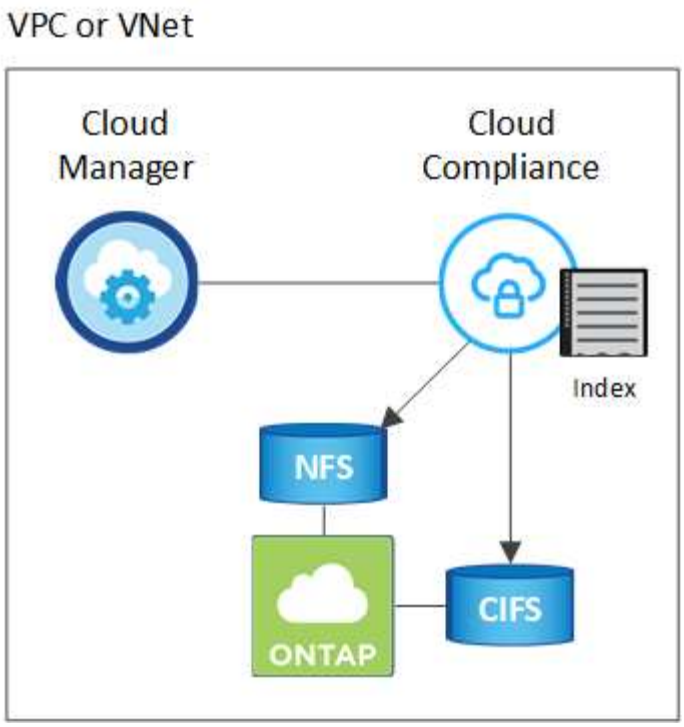
> 클라우드 규정 준수에서 Cloud Volumes ONTAP 시스템의 데이터를 지속적으로 스캔하기 때문에 인스턴스는 항상 실행 상태를 유지해야 합니다.

스캔 작동 방식

Cloud Compliance를 활성화하면 즉시 데이터를 스캔하여 중요한 개인 데이터를 식별합니다.

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

Cloud Compliance는 각 볼륨의 비정형 데이터에서 다양한 개인 정보를 검색합니다. 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.



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

작업 환경 수준에서 스캔을 켜거나 끌 수 있지만 볼륨 수준에서는 설정할 수 없습니다. "자세히 알아보기".

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 알아봅니다".

네트워킹 개요

Cloud Manager는 사설 IP 주소 및 Cloud Manager로부터 인바운드 HTTP 연결을 지원하는 보안 그룹과 함께 Cloud Compliance 인스턴스를 배포합니다. 이 연결을 통해 Cloud Manager 인터페이스에서 Cloud Compliance 대시보드에 액세스할 수 있습니다.

아웃바운드 규칙은 완전히 열립니다. 이 인스턴스는 Cloud Volumes ONTAP 시스템 및 Cloud Manager의 프록시를 통해 인터넷에 연결됩니다. 클라우드 규정 준수 소프트웨어를 업그레이드하고 사용량 메트릭을 전송하려면 인터넷에 액세스해야 합니다.

네트워킹 요구 사항이 엄격하면 "Cloud Compliance에서 접촉하는 엔드포인트에 대해 알아보십시오".

> 인덱싱된 데이터는 클라우드 규정 준수 인스턴스를 남기지 않습니다. 데이터는 가상 네트워크 외부로 전달되지 않고 Cloud Manager로 전송되지 않습니다.

규정 준수 정보에 대한 사용자 액세스

Cloud Manager 관리자는 모든 작업 환경에 대한 규정 준수 정보를 볼 수 있습니다.

Workspace 관리자는 액세스 권한이 있는 시스템에 대해서만 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 Manager 역할에 대해 자세히 알아보십시오".

Cloud Volumes ONTAP용 클라우드 규정 준수 시작하기

AWS 또는 Azure에서 Cloud Volumes ONTAP용 Cloud Compliance를 시작하려면 몇 단계를 완료하십시오.

빠른 시작

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

1 구성이 요구 사항을 충족할 수 있는지 확인합니다

- 클라우드 규정 준수 인스턴스가 아웃바운드 인터넷 액세스를 가질 수 있는지 확인합니다.

  Cloud Manager는 요청의 첫 번째 Cloud Volumes ONTAP 시스템과 동일한 VPC 또는 VNET에 인스턴스를 배포합니다.

- 사용자가 AWS 또는 Azure에 직접 연결된 호스트 또는 Cloud Compliance 인스턴스와 동일한 네트워크 내의 호스트에서 Cloud Manager 인터페이스에 액세스할 수 있는지 확인합니다(인스턴스에는 프라이빗 IP 주소가 있음).
- 클라우드 규정 준수 인스턴스를 계속 실행할 수 있는지 확인합니다.

Cloud Volumes ONTAP에서 클라우드 규정 준수 지원

- 새로운 작업 환경: 작업 환경을 생성할 때 Cloud Compliance를 사용하도록 설정해야 합니다(기본적으로 활성화됨).
- 기존 작업 환경: * 규정 준수 * 를 클릭하고 작업 환경 목록을 필요에 따라 편집한 다음 * 준수 대시보드 표시 * 를 클릭합니다.

볼륨에 대한 액세스를 확인합니다

이제 Cloud Compliance를 사용하도록 설정했으므로 볼륨에 액세스할 수 있는지 확인합니다.

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

  Compliance * > * CIFS Scan Status * > * 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.

Cloud Manager와 클라우드 규정 준수 간 연결을 보장합니다

- Cloud Manager의 보안 그룹은 포트 80을 통해 클라우드 규정 준수 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용해야 합니다.
- AWS 네트워크에서 인터넷 액세스에 NAT 또는 프록시를 사용하지 않는 경우 Cloud Manager의 보안 그룹은 클라우드 규정 준수 인스턴스에서 TCP 포트 3128을 통한 인바운드 트래픽을 허용해야 합니다.

사전 요구 사항 검토

Cloud Compliance를 설정하기 전에 다음 사전 요구 사항을 검토하여 지원되는 구성이 있는지 확인하십시오. Cloud Compliance를 활성화한 후에는 구성 요소 간의 연결을 확인해야 합니다. 이 내용은 아래에서 다룹니다.

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.

엔드포인트	목적
https://cloudmanager.cloud.netapp.com 으로 문의하십시오	Cloud Central 계정을 포함한 Cloud Manager 서비스와 통신합니다.
https://netapp-cloud-account.auth0.com 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공

엔드포인트	목적
https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com https://hub.docker.com 으로 문의하십시오	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.

웹 브라우저가 **Cloud Compliance**에 연결되어 있는지 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.

> 공용 IP 주소에서 Cloud Manager에 액세스하는 경우 웹 브라우저가 네트워크 내의 호스트에서 실행되고 있지 않을 수 있습니다.

클라우드 규정 준수를 지속적으로 실행

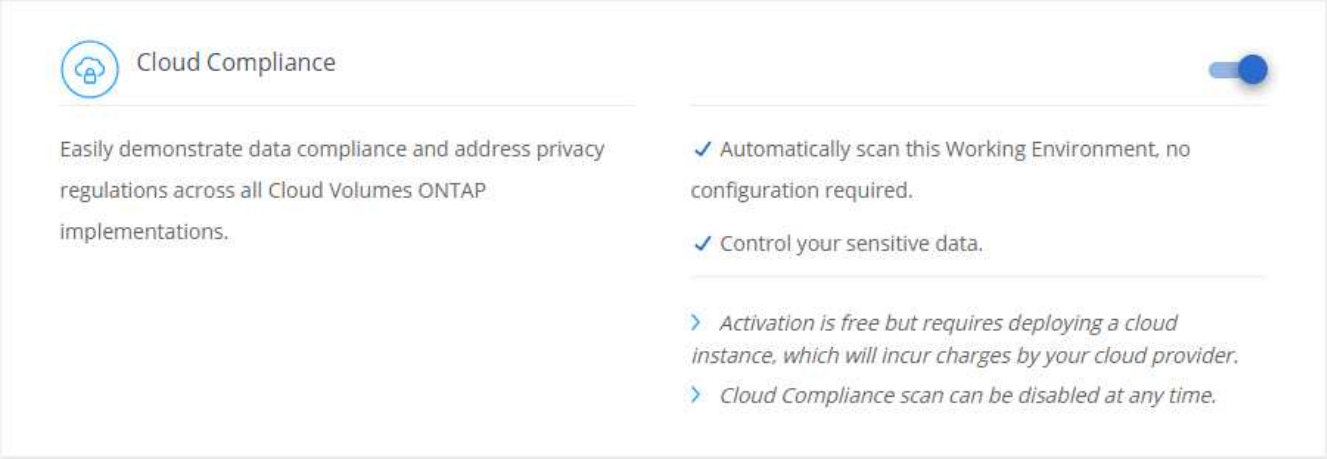
데이터를 지속적으로 스캔하려면 클라우드 규정 준수 인스턴스가 계속 켜져 있어야 합니다.

새로운 작업 환경에서 클라우드 규정 준수 지원

작업 환경 마법사에서는 기본적으로 클라우드 규정 준수를 사용하도록 설정되어 있습니다. 옵션을 활성 상태로 유지해야 합니다.

단계

1. Create Cloud Volumes ONTAP * 를 클릭합니다.
2. 클라우드 공급자로 Amazon Web Services 또는 Microsoft Azure를 선택하고 단일 노드 또는 HA 시스템을 선택합니다.
3. 세부 정보 및 자격 증명 페이지를 입력합니다.
4. 서비스 페이지에서 클라우드 규정 준수 를 활성화된 상태로 두고 * 계속 * 을 클릭합니다.



5. 마법사의 페이지를 완료하여 시스템을 구축합니다.

   자세한 내용은 을 참조하십시오 "AWS에서 Cloud Volumes ONTAP 실행" 및 "Azure에서 Cloud Volumes ONTAP 실행".

결과

Cloud Volumes ONTAP 시스템에서 클라우드 규정 준수를 지원합니다. Cloud Compliance를 처음 활성화한 경우 Cloud Manager는 클라우드 공급자에 Cloud Compliance 인스턴스를 배포합니다. 인스턴스를 사용할 수 있게 되면 생성한 각 볼륨에 기록된 데이터를 스캔하기 시작합니다.

기존 작업 환경에서 클라우드 규정 준수 지원

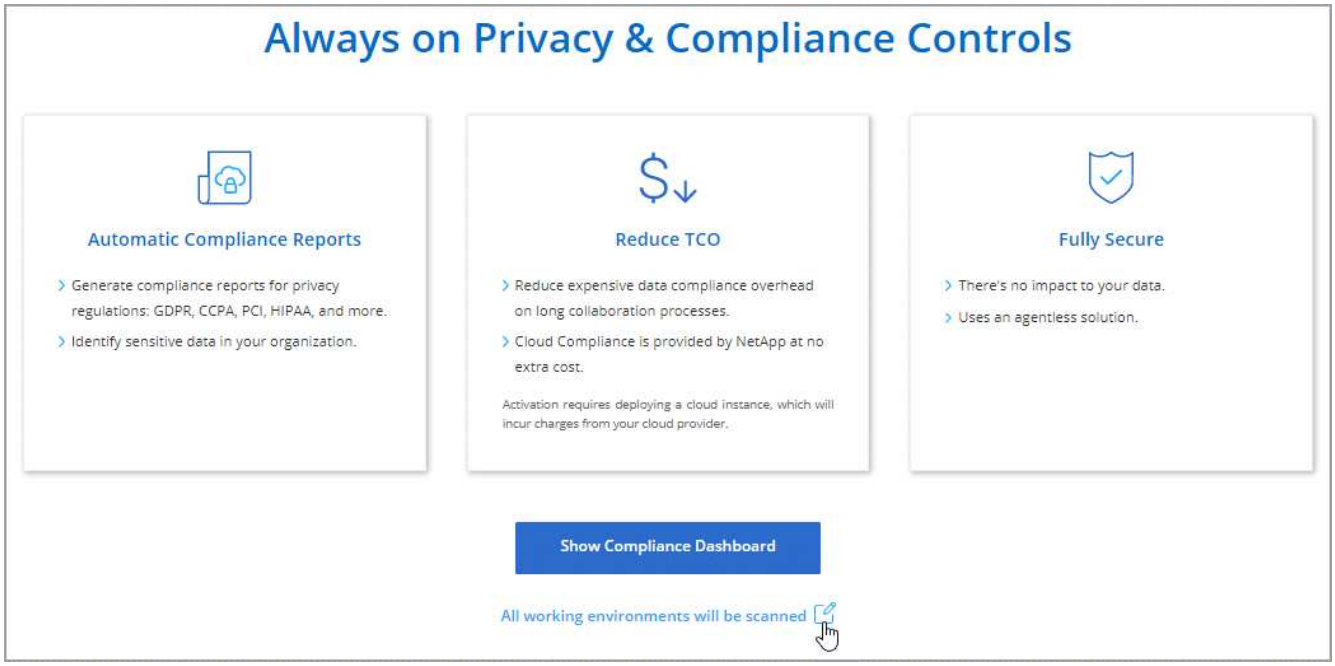
Cloud Manager의 * Compliance * 탭에서 기존 Cloud Volumes ONTAP 시스템에서 클라우드 규정 준수를 지원합니다.

또 다른 옵션은 각 작업 환경을 개별적으로 선택하여 * 작업 환경 * 탭에서 클라우드 규정 준수를 활성화하는 것입니다. 단 하나의 시스템만 있는 경우를 제외하고 완료하는 데 시간이 더 오래 걸립니다.

여러 작업 환경을 위한 단계

1. Cloud Manager 맨 위에서 * 규정 준수 * 를 클릭합니다.
2. 특정 작업 환경에서 클라우드 규정 준수를 활성화하려면 편집 아이콘을 클릭합니다.

   그렇지 않으면 Cloud Manager가 액세스 권한이 있는 모든 작업 환경에서 Cloud Compliance를 사용하도록 설정됩니다.

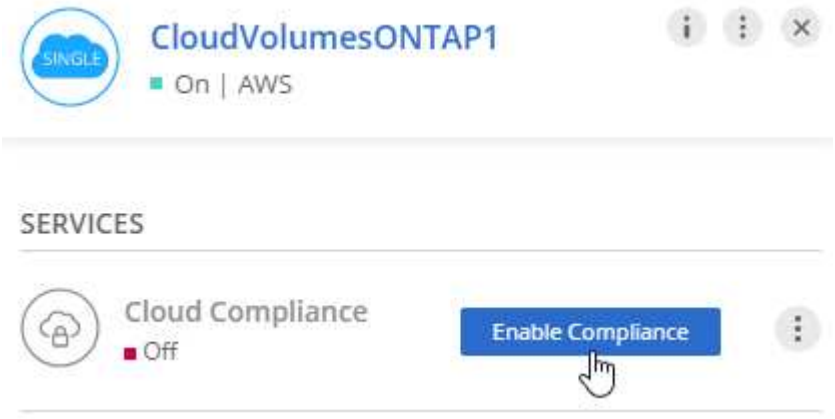


3. 준수 대시보드 표시 * 를 클릭합니다.

단일 작업 환경을 위한 단계

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

3. 오른쪽 창에서 * 준수 활성화 * 를 클릭합니다.



결과

Cloud Compliance를 처음 활성화한 경우 Cloud Manager는 클라우드 공급자에 Cloud Compliance 인스턴스를 배포합니다.

Cloud Compliance는 각 작업 환경에서 데이터 스캔을 시작합니다. Cloud Compliance에서 초기 스캔을 마치면 Compliance 대시보드에서 데이터를 사용할 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 엑스포트 정책을 확인하여 Cloud Compliance에서 Cloud Volumes ONTAP의 볼륨에 액세스할 수 있는지 확인합니다. CIFS 볼륨에 액세스할 수 있도록 Cloud Compliance에 CIFS 자격 증명을 제공해야 합니다.

단계

1. 클라우드 규정 준수 인스턴스와 각 Cloud Volumes ONTAP 서브넷 사이에 네트워크 연결이 있는지 확인하십시오.

   Cloud Manager는 요청에 따라 첫 번째 Cloud Volumes ONTAP 시스템과 동일한 VPC 또는 VNET에 클라우드 규정 준수 인스턴스를 구축합니다. 따라서 일부 Cloud Volumes ONTAP 시스템이 다른 서브넷 또는 가상 네트워크에 있는 경우 이 단계가 중요합니다.

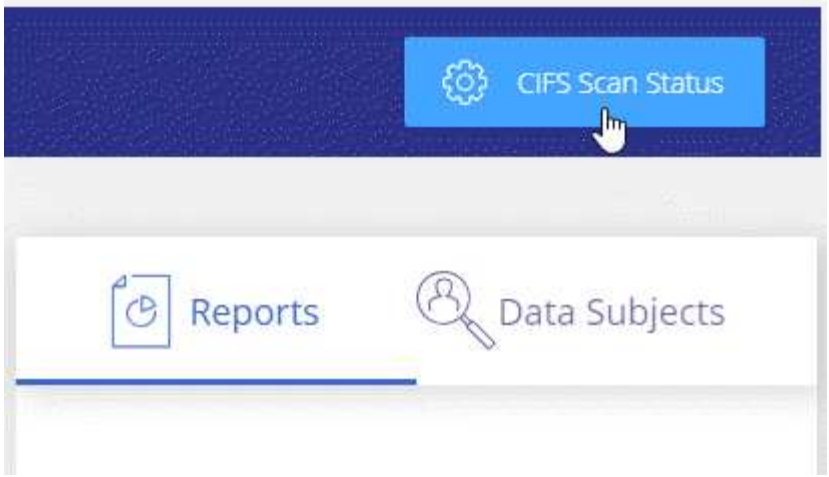
2. Cloud Volumes ONTAP의 보안 그룹이 클라우드 규정 준수 인스턴스의 인바운드 트래픽을 허용하는지 확인합니다.

   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 엑스포트 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 맨 위에서 * 규정 준수 * 를 클릭합니다.

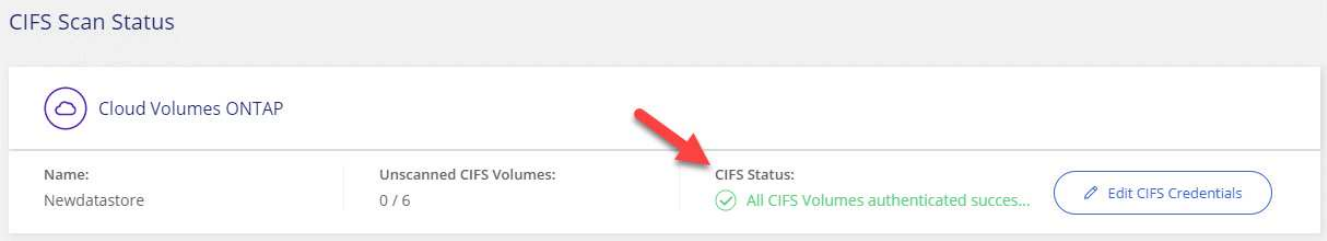
   b. 오른쪽 상단에서 * CIFS Scan Status * 를 클릭합니다.



c. 각 Cloud Volumes ONTAP 시스템에서 * 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.



Cloud Manager가 Cloud Compliance에 액세스할 수 있는지 검증

Cloud Manager와 클라우드 규정 준수 간의 연결을 보장하므로 클라우드 규정 준수에 대한 규정 준수 인사이트를 확인할 수 있습니다.

단계

1. Cloud Manager의 보안 그룹이 포트 80을 통해 클라우드 규정 준수 인스턴스 간에 인바운드 및 아웃바운드 트래픽을 허용하는지 확인합니다.

   이 연결을 통해 준수 탭에서 정보를 볼 수 있습니다.

2. AWS 네트워크가 인터넷 액세스에 NAT 또는 프록시를 사용하지 않는 경우 Cloud Manager의 보안 그룹을 수정하여 클라우드 규정 준수 인스턴스에서 TCP 포트 3128을 통한 인바운드 트래픽을 허용합니다.

   Cloud Compliance 인스턴스가 Cloud Manager를 프록시로 사용하여 인터넷에 액세스하기 때문에 이 작업이 필요합니다.

   > 이 포트는 버전 3.7.5부터 시작하는 모든 새로운 Cloud Manager 인스턴스에서 기본적으로 열립니다. 해당 버전 이전에 생성된 Cloud Manager 인스턴스에서는 열 수 없습니다.

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.

개인 데이터

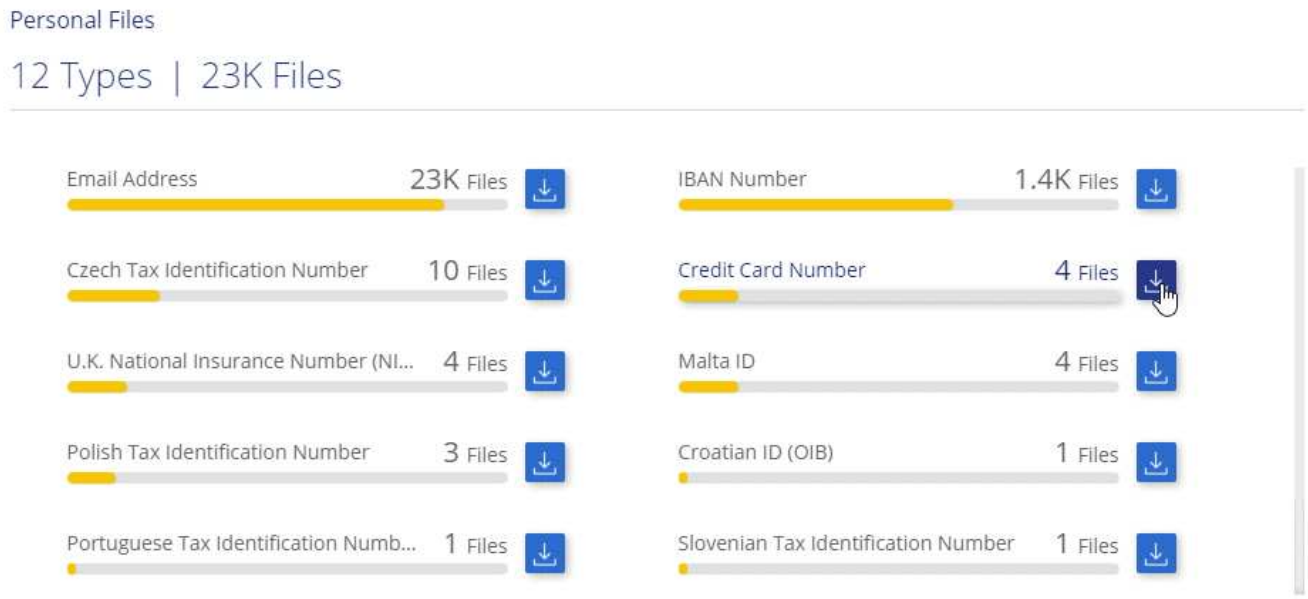
Cloud Compliance는 데이터 내에서 특정 단어, 문자열 및 패턴(Regex)을 자동으로 식별합니다. 예를 들어 개인 식별 정보(PII), 신용 카드 번호, 주민 등록 번호, 은행 계좌 번호 등이 있습니다. 전체 목록을 참조하십시오.

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 맨 위에서 * 규정 준수 * 를 클릭합니다.
2. 기본 화면에서 상위 2개 파일 유형 중 하나에 대한 세부 정보를 직접 다운로드하거나 * 모두 보기 * 를 클릭한 다음 찾은 개인 데이터 유형에 대한 목록을 다운로드합니다.



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	**ID**입니다	근접성 검증**?**
일반	이메일 주소입니다	아니요
	신용 카드 번호입니다	아니요
	IBAN 번호(국제 은행 계좌 번호)	아니요
	IP 주소입니다	예
국가 식별자	벨기에 iD(Numero National)	예
	불가리아어 ID(통합 민수)	예
	키프로스 세금 식별 번호(TIC)	예
	덴마크 세금 식별 번호(CPR)	예
	에스토니아어 ID(이시쿠목)	예
	핀란드 iD(henkilötunnus)	예
	프랑스어 세금 식별 번호(SPI)	예
	독일 세금 식별 번호(슈테루리체 식별 번호)	예
	헝가리 세금 식별 번호(Adóazonosító jel)	예
	아일랜드 ID(PPS)	예
	이스라엘 iD	예
	이탈리아어 ID(코주사위 파이스케일급)	예
	라트비아어 세금 식별 번호	예
	리투아니아어 ID(Asmens kodas)	예
	룩셈부르크 ID입니다	예
	몰타 ID	예
	네덜란드 ID(BSN)	예
	폴란드 세금 식별 번호	예
	포르투갈어 세금 식별 번호(NIF)	예
	루마니아어 세금 식별 번호	예
	슬로바키아어 세금 식별 번호	예
	슬로베니아어 세금 식별 번호	예
	남아프리카 ID	예
	스페인어 세금 식별 번호	예
	스웨덴 납세 식별 번호	예
	영국 국민 보험 번호(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, 인종 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.

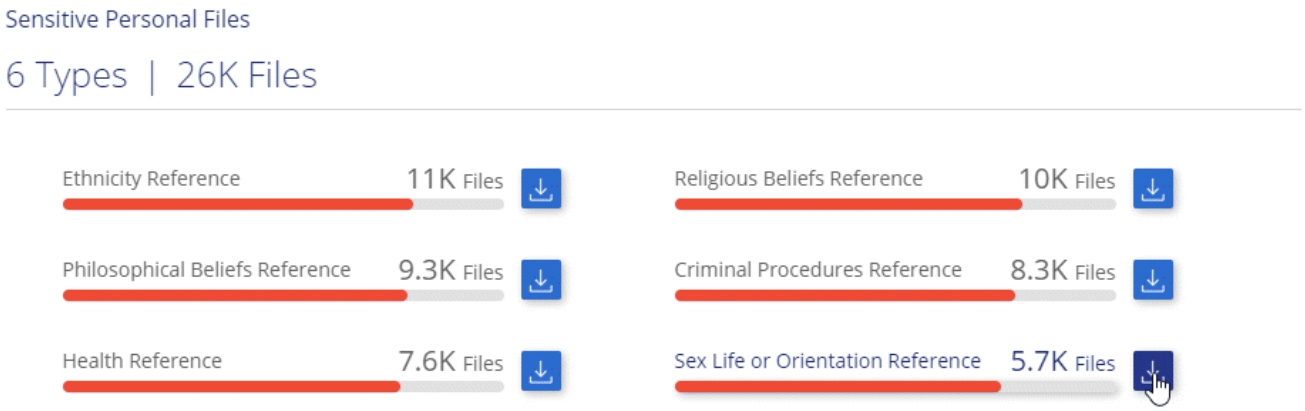
예를 들어, 중요한 GDPR 데이터 범주 중 하나는 인종입니다. 클라우드 규정 준수(Cloud Compliance)는 NLP 기능으로 인해 "George is Mexican"(GDPR 제9조에 명시된 민감한 데이터 표시)과 "George is eating Mexican food"라는 문장의 차이를 구별할 수 있습니다.

> 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 맨 위에서 * 규정 준수 * 를 클릭합니다.
2. 기본 화면에서 상위 2개 파일 유형 중 하나에 대한 세부 정보를 직접 다운로드하거나 * 모두 보기 * 를 클릭한 다음 발견된 민감한 개인 데이터 유형에 대한 목록을 다운로드합니다.



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.

인종 참조
: 자연인의 인종 또는 민족에 관한 데이터.

상태 참조
: 자연인의 건강에 관한 데이터.

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.

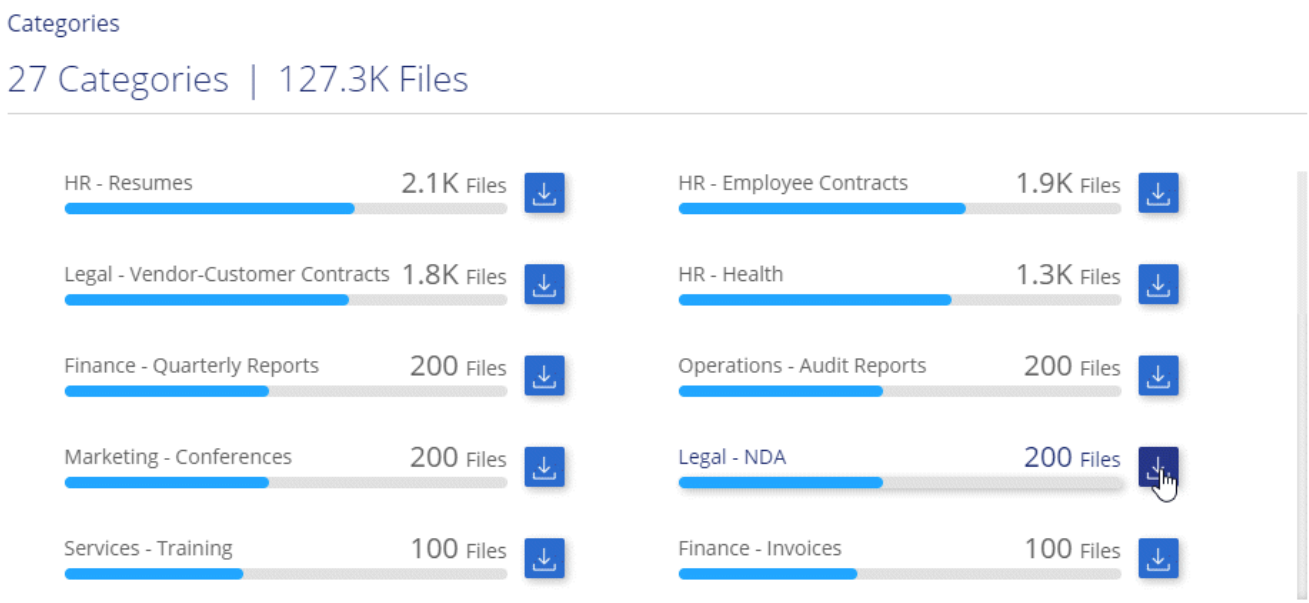
범주는 보유한 정보의 유형을 표시하여 데이터의 상태를 이해하는 데 도움이 됩니다. 예를 들어 이력서 또는 직원 계약과 같은 범주에는 중요한 데이터가 포함될 수 있습니다. CSV 보고서를 다운로드할 때 직원 계약이 안전하지 않은 위치에 저장되어 있는 것을 확인할 수 있습니다. 그런 다음 해당 문제를 해결할 수 있습니다.

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

범주별로 파일 보기

단계

1. Cloud Manager 맨 위에서 * 규정 준수 * 를 클릭합니다.
2. 기본 화면에서 상위 4개 파일 유형 중 하나에 대한 세부 정보를 직접 다운로드하거나 * 모두 보기 * 를 클릭한 다음 모든 범주의 목록을 다운로드합니다.



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

- NDA를 체결합니다
- 공급업체 - 고객 계약

마케팅

- 캠페인
- 회의

운영

- 감사 보고서

판매

- 판매 주문

서비스

- RFI
- RFP
- 교육

지원

- 불만 및 티켓

기타

- 파일 보관
- 오디오
- CAD 파일
- 코드

- 실행 파일
- 이미지

파일 형식

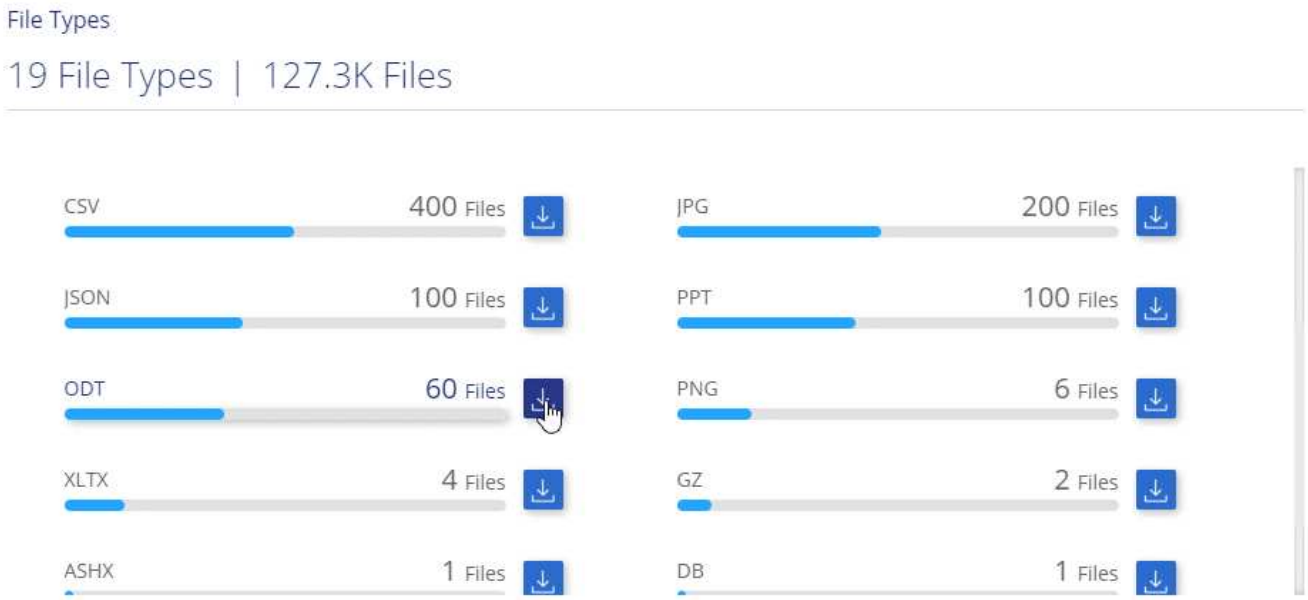
Cloud Compliance는 스캔한 데이터를 파일 유형에 따라 분해합니다. Cloud Compliance는 검사에서 발견된 모든 파일 유형을 표시할 수 있습니다.

파일 형식을 검토하면 특정 파일 형식이 올바르게 저장되지 않은 것을 발견할 수 있으므로 중요한 데이터를 제어하는 데 도움이 됩니다. 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 맨 위에서 * 규정 준수 * 를 클릭합니다.
2. 기본 화면에서 상위 4개 파일 유형 중 하나에 대한 세부 정보를 직접 다운로드하거나 * 모두 보기 * 를 클릭한 다음 파일 유형에 대한 목록을 다운로드합니다.



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

대시보드를 사용하면 식별된 파일에 대한 세부 정보가 포함된 파일 목록(CSV 형식)을 다운로드할 수 있습니다. 결과가 10,000개를 초과하는 경우 상위 10,000개만 목록에 표시됩니다(더 많은 에 대한 지원은 나중에 추가됨).

각 파일 목록에는 다음 정보가 포함됩니다.

- 파일 이름입니다
- 위치 유형
- 위치
- 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 대시보드에 나타나는 파일 번호 개수에 포함되지 않습니다. 파일은 CSV 보고서에만 나타납니다.

개인 정보 보호 위험 평가 보고서 보기

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

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

보고서에는 다음 정보가 포함됩니다.

준수 상태
: 심각성 점수(자세한 내용은 아래 참조) 및 데이터의 분포(민감하지 않거나 개인적이거나 민감한 개인 정보)

평가 개요
: 발견된 개인 데이터 유형 및 데이터 범주에 대한 분석.

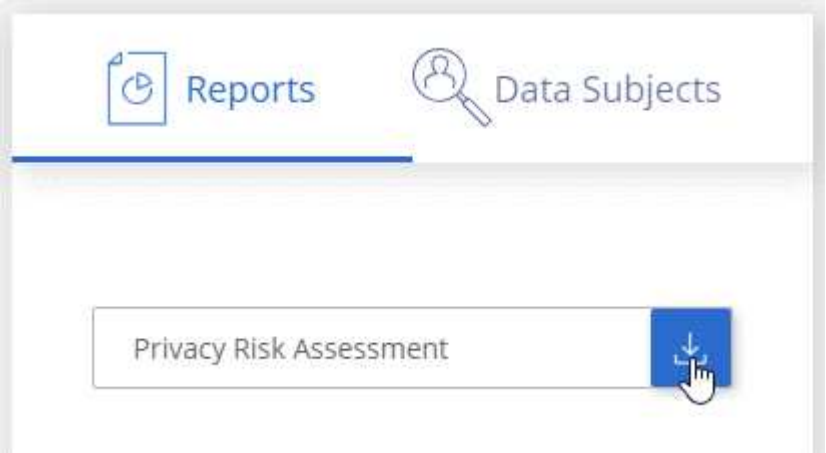
이 평가의 데이터 주체
: 국가 식별자가 발견된 위치별 사용자 수.

개인 정보 보호 위험 평가 보고서 생성

준수 탭으로 이동하여 보고서를 생성합니다.

단계

1. Cloud Manager 맨 위에서 * 규정 준수 * 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 큽니다
2	변수 중 하나가 3%보다 큽니다
3	변수 중 두 개가 3%보다 큽니다
4	변수 중 3개가 3%보다 큽니다
5	변수 중 하나가 6% 더 큽니다
6	변수 중 두 개가 6% 더 큽니다
7	변수 중 3개는 6%가 더 큽니다
8	변수 중 하나가 15% 더 큽니다
9	변수 중 두 개가 15% 더 큽니다
10	세 개의 변수가 15% 더 큽니다

데이터 주체 액세스 요청에 응답

피험자의 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 피험자가 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 파일 목록 또는 데이터 주체 액세스 요청 보고서를 다운로드할 수 있습니다. 이 보고서는 데이터에서 얻은 통찰력을 집계하여 해당 사람에게 다시 보낼 수 있는 법적 용어로 저장합니다.

데이터 주체 검색 및 보고서 다운로드

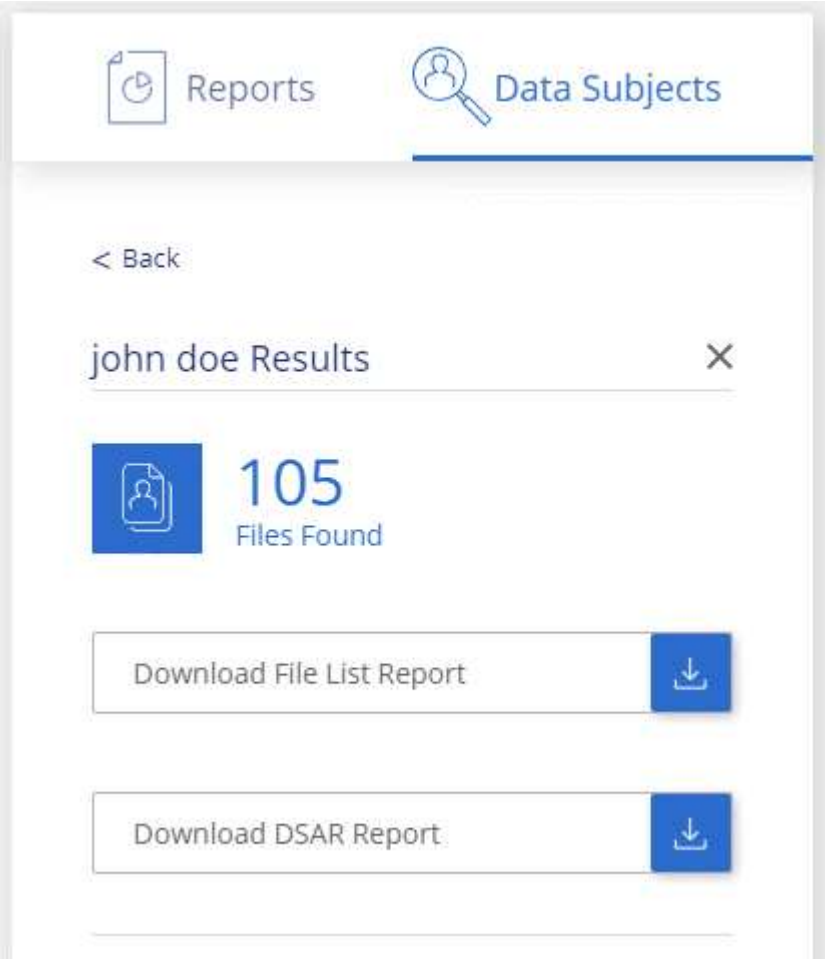
데이터 주체의 전체 이름 또는 알려진 식별자를 검색한 다음 파일 목록 보고서 또는 DSAR 보고서를 다운로드합니다. 검색할 수 있는 기준 "모든 개인 정보 유형입니다".

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

단계

1. Cloud Manager 맨 위에서 * 규정 준수 * 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.
   - * 파일 목록 보고서 다운로드 *: 데이터 주제에 대한 정보가 포함된 파일 목록입니다.

     10,000개가 넘는 결과가 있을 경우 보고서에 상위 10,000개만 표시됩니다(더 많은 에 대한 지원은 나중에 추가됨).

   - * DSAR 보고서 다운로드 *: 데이터 주체에 전송할 수 있는 액세스 요청에 대한 공식 응답입니다. 이 보고서에는 데이터 주제에 대해 Cloud Compliance에서 찾아 템플릿으로 사용하도록 설계된 데이터를 기반으로 자동으로 생성된 정보가 포함됩니다. 양식을 작성하여 내부적으로 검토한 후 데이터 제목으로 보내야 합니다.

클라우드 규정 준수 비활성화

필요한 경우 클라우드 규정 준수 가 하나 이상의 작업 환경을 스캐닝하지 못하도록 할 수 있습니다. Cloud Volumes ONTAP 시스템에서 클라우드 규정 준수를 더 이상 사용하지

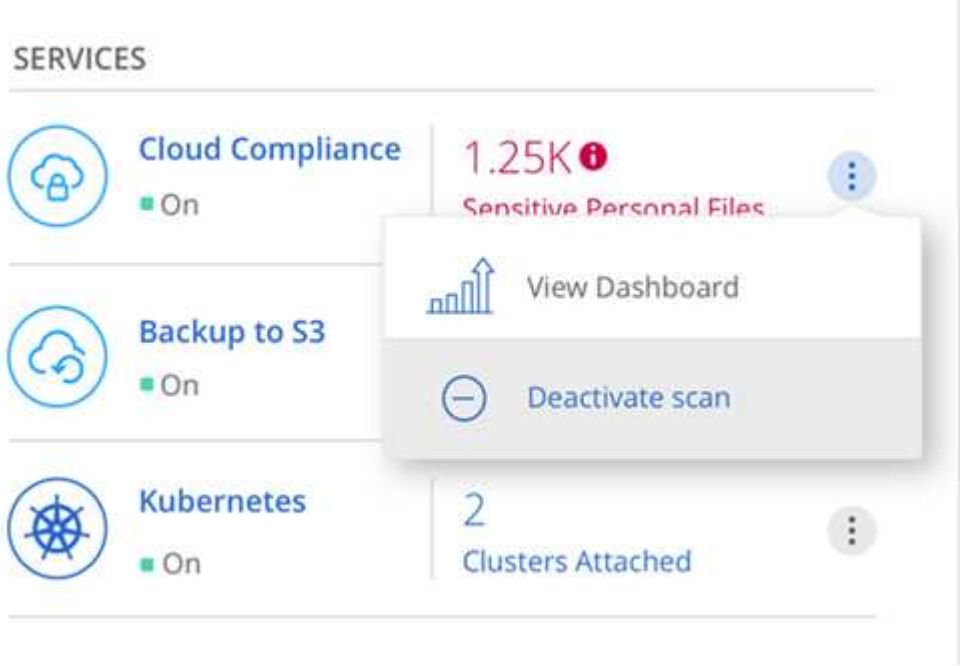
않으려는 경우 클라우드 규정 준수 인스턴스를 삭제할 수도 있습니다.

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 자체의 데이터는 삭제되지 않음).

단계

1. Cloud Manager 상단에서 * 작업 환경 * 을 클릭합니다.
2. 작업 환경을 선택합니다.
3. 오른쪽 패널에서 클라우드 규정 준수 서비스의 작업 아이콘을 클릭하고 * 스캔 비활성화 * 를 선택합니다.



Cloud Compliance 인스턴스 삭제

Cloud Volumes ONTAP에서 더 이상 클라우드 규정 준수를 사용하지 않으려는 경우 클라우드 규정 준수 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 새로운 NetApp 클라우드 오퍼링입니다. 클라우드 규정 준수 는 인공 지능(AI) 중심 기술을 사용하여 AWS 또는 Azure에서 호스팅되는 Cloud Volumes ONTAP 시스템 전반에서 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있도록 지원합니다.

Cloud Compliance는 GDPR, CCPA 등과 같은 데이터 개인 정보 보호 및 민감도에 대한 새로운 데이터 규정 준수 규제를 해결할 수 있도록 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 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 NFS 및 CIFS 프로토콜을 통해 비정형 데이터 스캔을 지원합니다. 현재 클라우드 규정 준수 는 Cloud Volumes ONTAP에서 관리하는 데이터를 검색합니다.

"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 Cloud Volumes ONTAP 인스턴스와 함께 또 다른 인공 지능 계층을 구축합니다. 그런 다음 Cloud Volumes ONTAP의 데이터를 검색하고 검색된 데이터 통찰력을 인덱싱합니다.

"클라우드 규정 준수 방식에 대해 자세히 알아보십시오".

클라우드 규정 준수 비용은 얼마입니까?

클라우드 규정 준수는 Cloud Volumes ONTAP의 일부로 제공되며 추가 비용이 필요하지 않습니다. 향후 맞춤형 기능에 추가 비용이 필요할 수 있습니다.

> Cloud Compliance는 클라우드 공급자에 인스턴스를 구축해야 하는데, 이 경우 클라우드 공급자가 이를 유료로 제공합니다.

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".

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 io1 디스크를 사용하는 m5.4x대용량 인스턴스에서 실행됩니다.

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

"클라우드 규정 준수 방식에 대해 자세히 알아보십시오".

스캔 성능이 달라집니까?

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

클라우드 규정 준수를 어떻게 활성화합니까?

새로운 작업 환경을 생성할 때 클라우드 규정 준수를 활성화할 수 있습니다. Compliance * (규정 준수 *) 탭(첫 번째 활성화에만 해당)이나 특정 작업 환경을 선택하여 기존 작업 환경에서 사용할 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?

아니요 Cloud Compliance는 현재 Cloud Manager의 일부로 제공되며 Cloud Volumes ONTAP를 지원합니다. NetApp은 Cloud Volumes Service 및 Azure NetApp Files와 같은 추가 클라우드 오퍼링을 통해 클라우드 규정 준수를 지원할 계획입니다.

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.

"자세한 정보".