데이터 소스에서 스캔을 활성화합니다

Cloud Manager 3.8

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/occm38/task_getting_started_compliance.html on March 25, 2024. Always check docs.netapp.com for the latest.

목차

데이터 소스에서 스캔을 활성화합니다 1
- Cloud Volumes ONTAP 및 Azure NetApp Files용 클라우드 규정 준수 시작하기 1
- Amazon S3에 대한 클라우드 규정 준수 시작하기 5
- 데이터베이스 스키마를 검색하는 중입니다 12
- SnapMirror를 사용하여 클라우드 규정 준수 기능을 통해 사내 ONTAP 데이터를 스캔합니다 16

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.

클라우드 규정 준수 인스턴스 구축

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

작업 환경에서 클라우드 규정 준수 지원

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

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 엑스포트 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.

스캔할 볼륨을 구성합니다

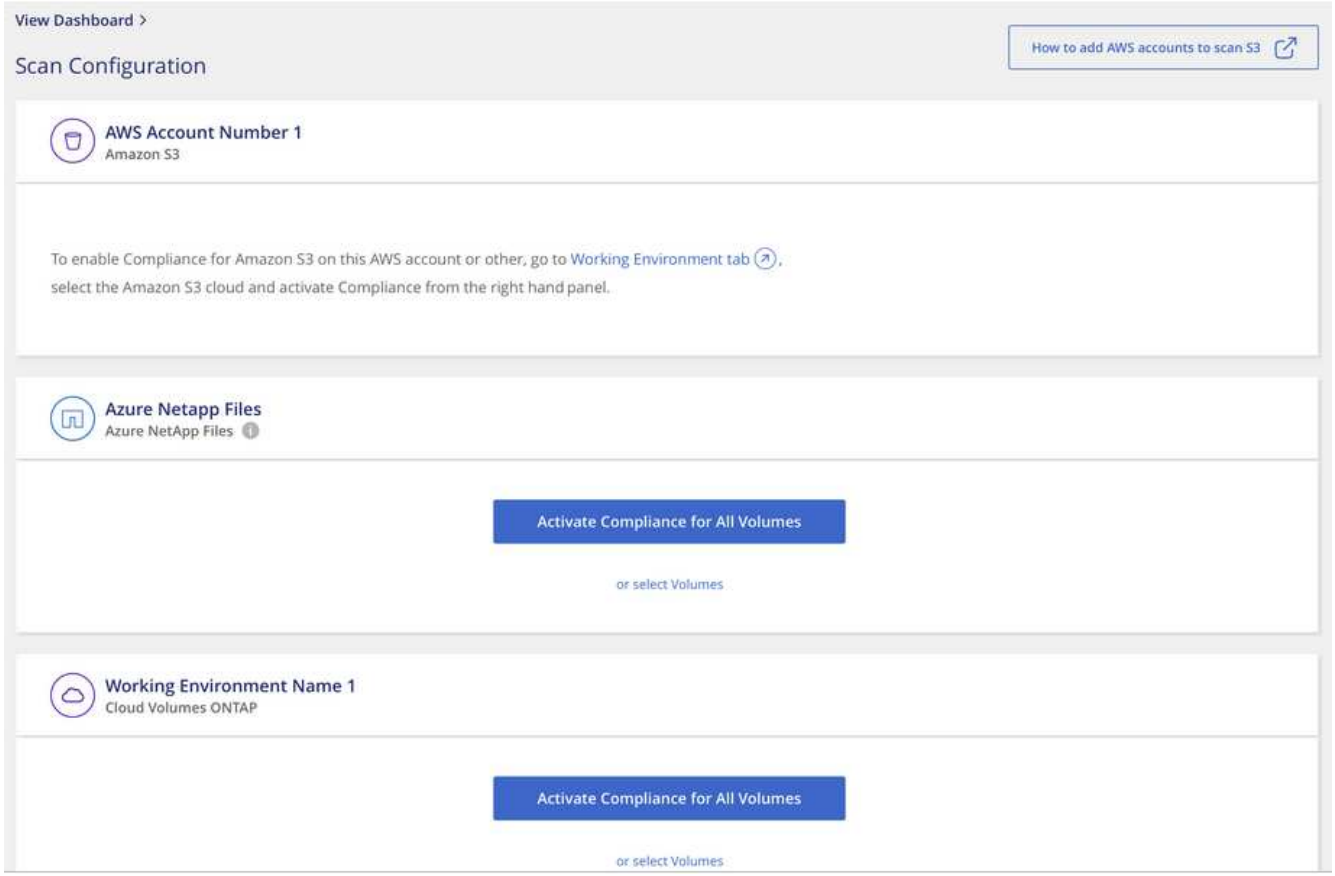
스캔할 볼륨을 선택하면 Cloud Compliance에서 스캔을 시작합니다.

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 엑스포트 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.

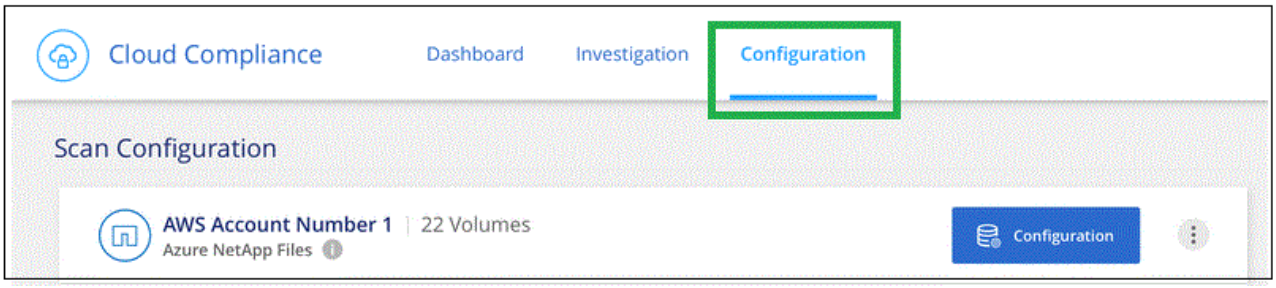
2. Cloud Volumes ONTAP의 보안 그룹이 클라우드 규정 준수 인스턴스의 인바운드 트래픽을 허용하는지 확인합니다.

   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 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 상단에서 * Cloud Compliance * 를 클릭합니다.

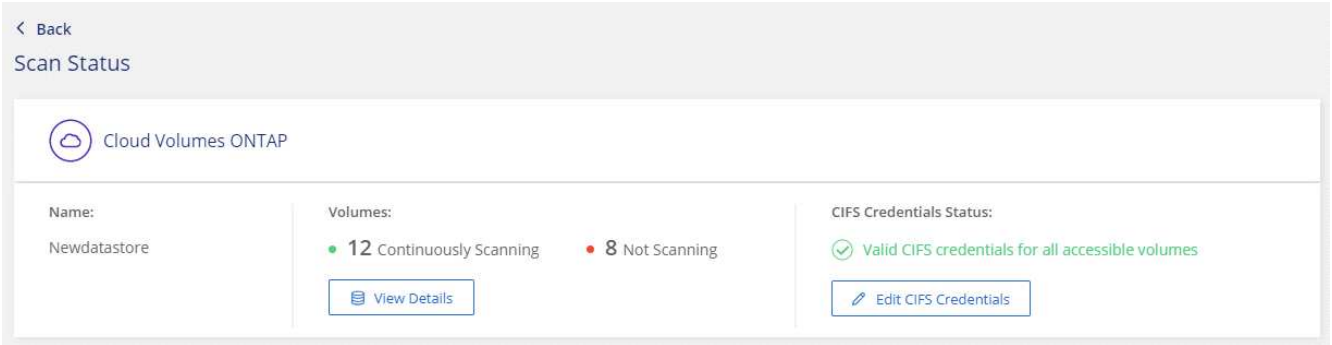
   b. Configuration * 탭을 클릭합니다.



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

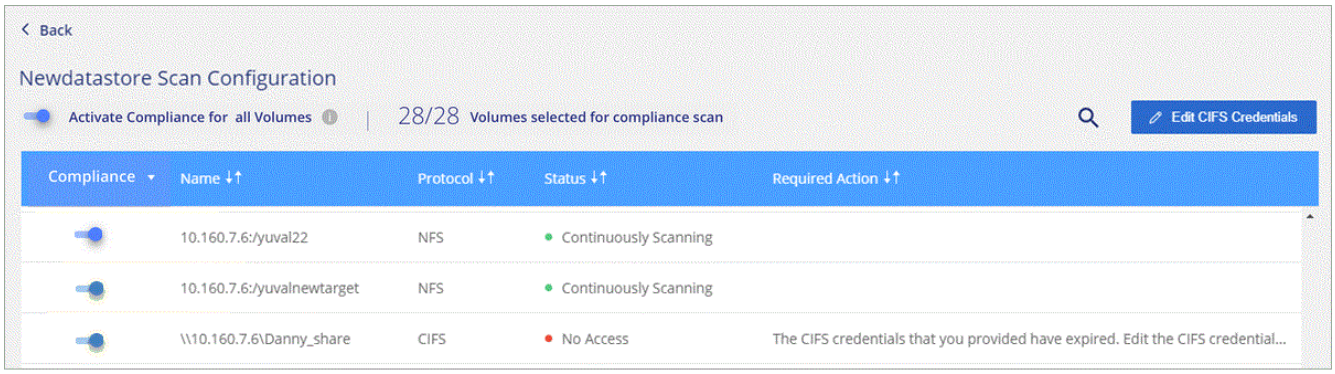
      자격 증명은 읽기 전용일 수 있지만 관리자 자격 증명을 제공하면 Cloud Compliance에서 상승된 사용 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 Cloud Compliance 인스턴스에 저장됩니다.

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



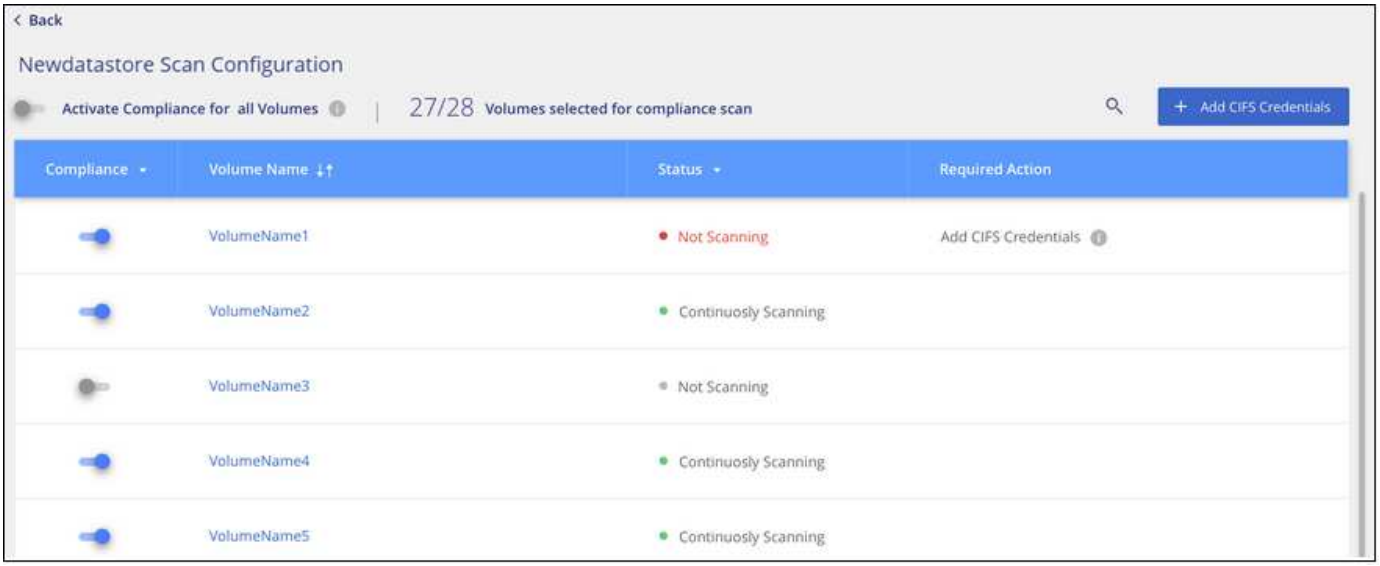
5. Scan Configuration_ 페이지에서 * View Details * 를 클릭하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

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.



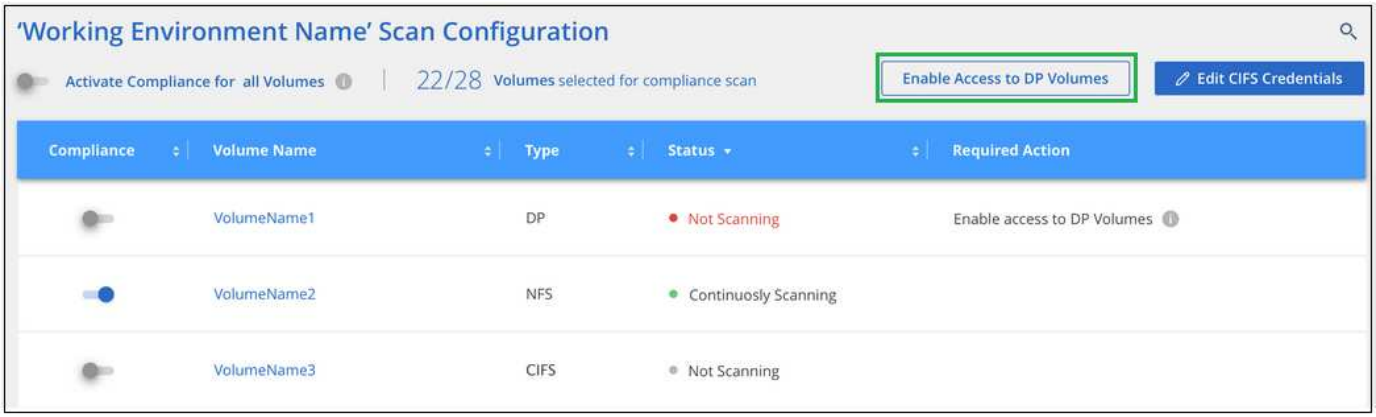
대상:	방법은 다음과 같습니다.
볼륨 스캔을 비활성화합니다	볼륨 슬라이더를 왼쪽으로 이동합니다
모든 볼륨에 대한 스캔을 비활성화합니다	모든 볼륨에 대해 * 준수 활성화 * 슬라이더를 왼쪽으로 이동합니다
볼륨 스캔을 활성화합니다	볼륨 슬라이더를 오른쪽으로 이동합니다
모든 볼륨 스캔을 활성화합니다	모든 볼륨에 대해 * 준수 활성화 * 슬라이더를 오른쪽으로 이동합니다

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.



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.

클라우드 규정 준수 인스턴스 구축

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

S3 작업 환경에서 규정 준수를 활성화합니다

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

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 S3**로 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.

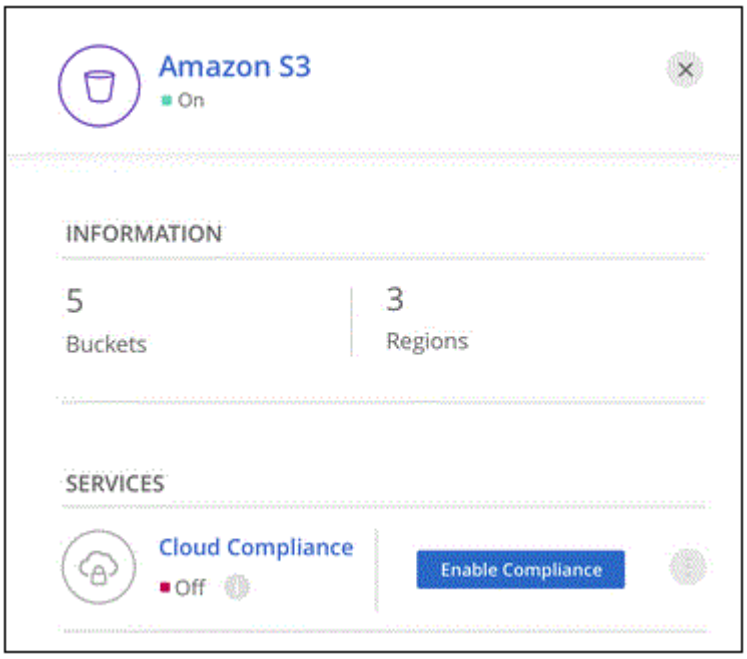
S3 작업 환경에서 규정 준수 활성화

사전 요구 사항을 확인한 후 Amazon S3에서 Cloud Compliance를 활성화합니다.

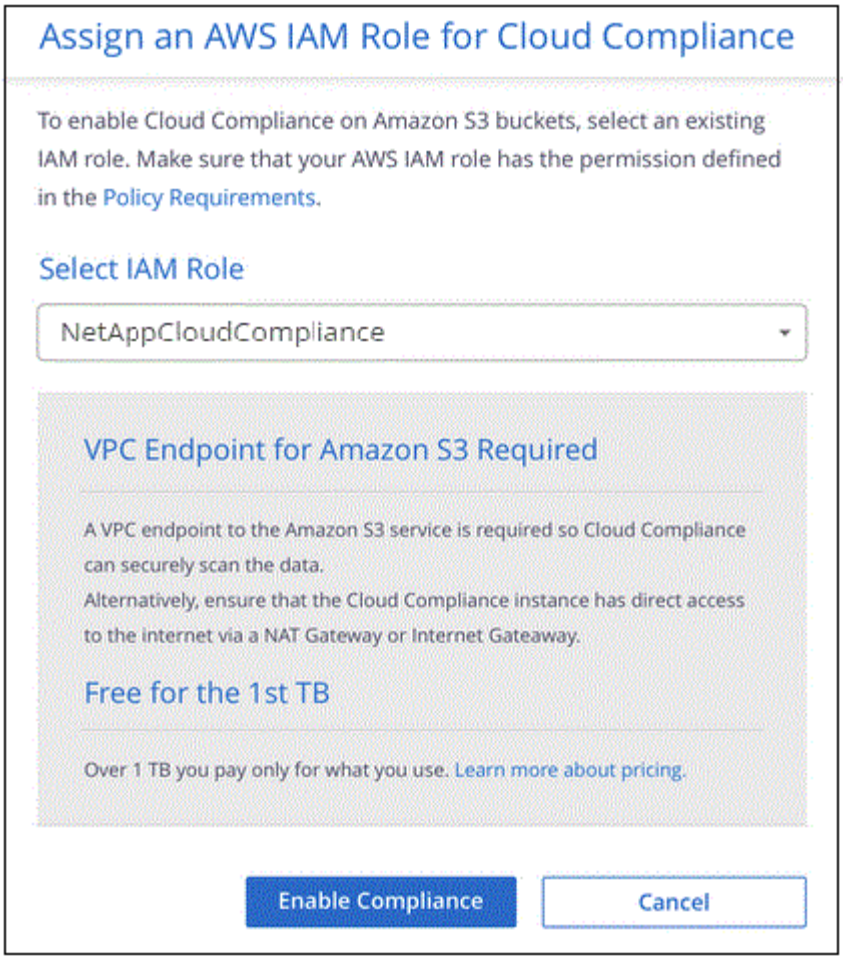
단계

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

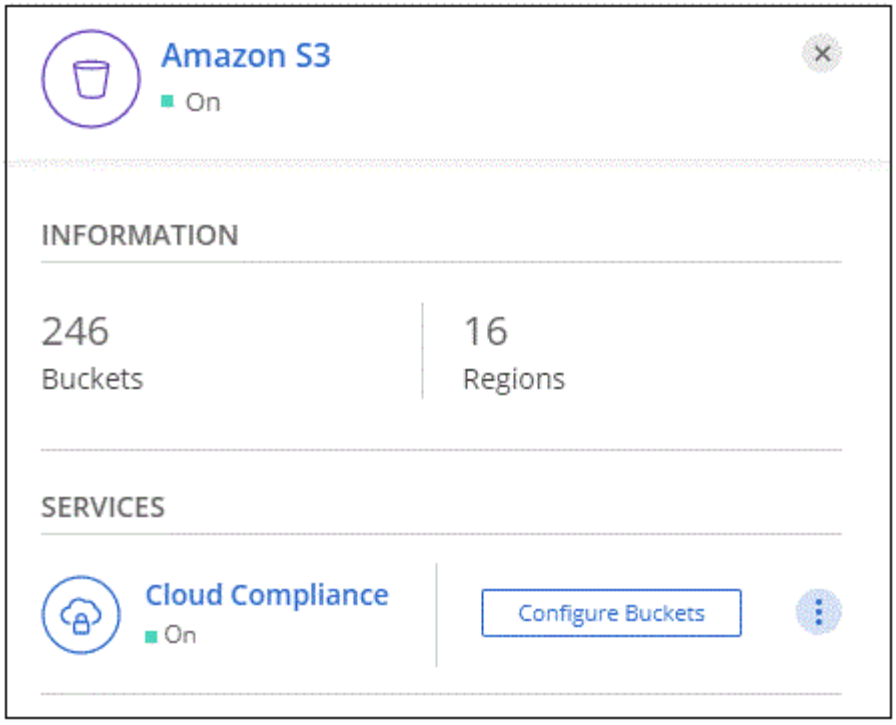
Cloud Manager를 사용하여 Amazon S3에서 Cloud Compliance를 사용하도록 설정한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다.

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

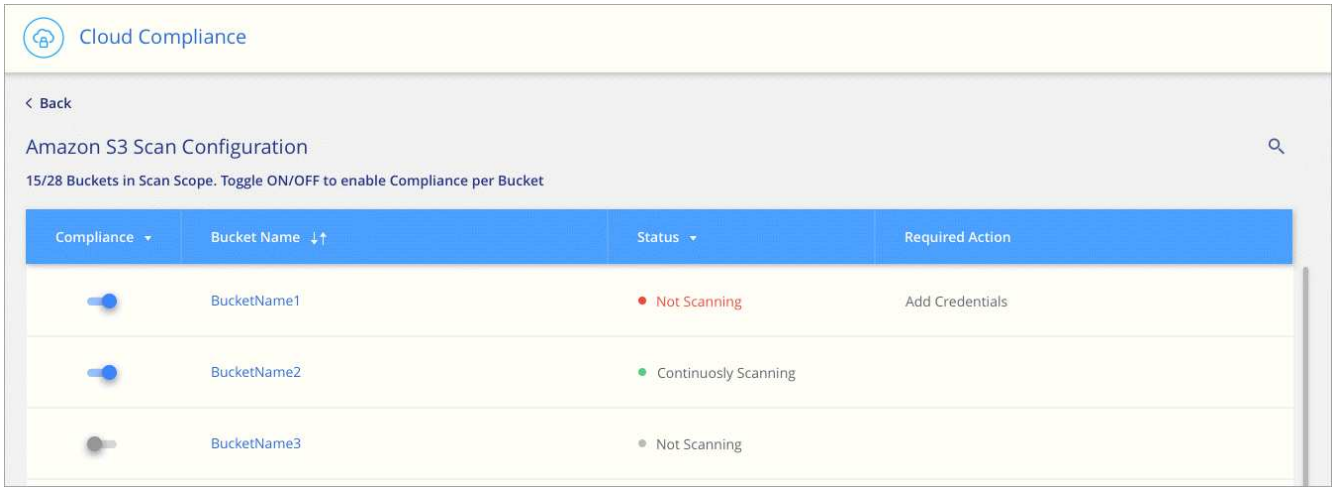
클라우드 규정 준수도 가능합니다 서로 다른 AWS 계정에 있는 S3 버킷을 스캔합니다.

단계

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



3. 스캔할 버킷의 규정 준수를 활성화합니다.



결과

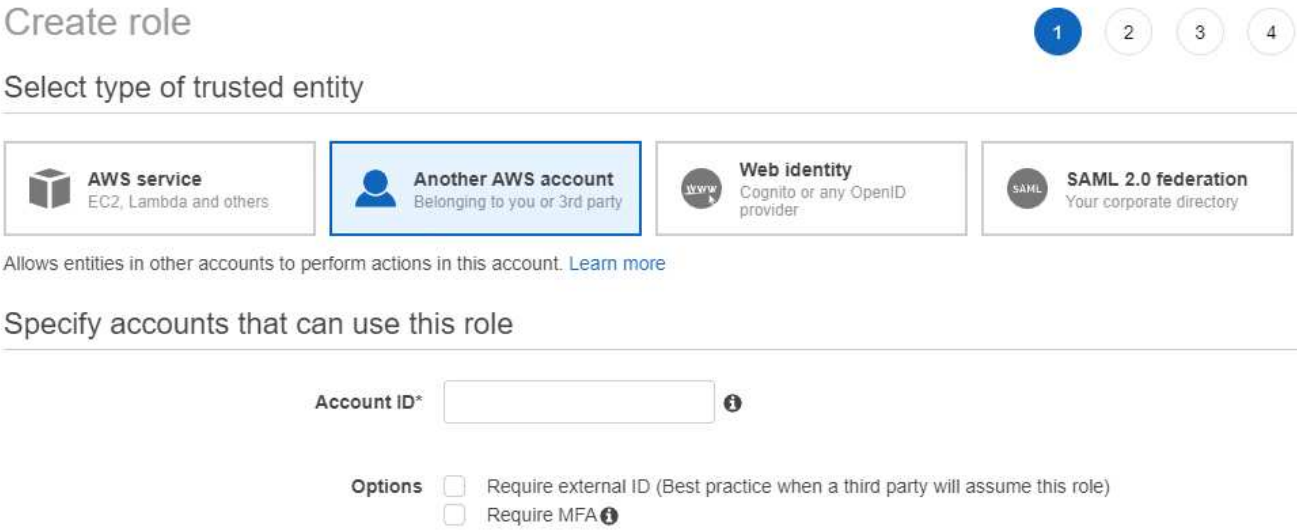
Cloud Compliance는 사용자가 활성화한 S3 버킷을 스캔하기 시작합니다. 오류가 있는 경우 오류를 해결하는 데 필요한 작업과 함께 상태 열에 표시됩니다.

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.



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.

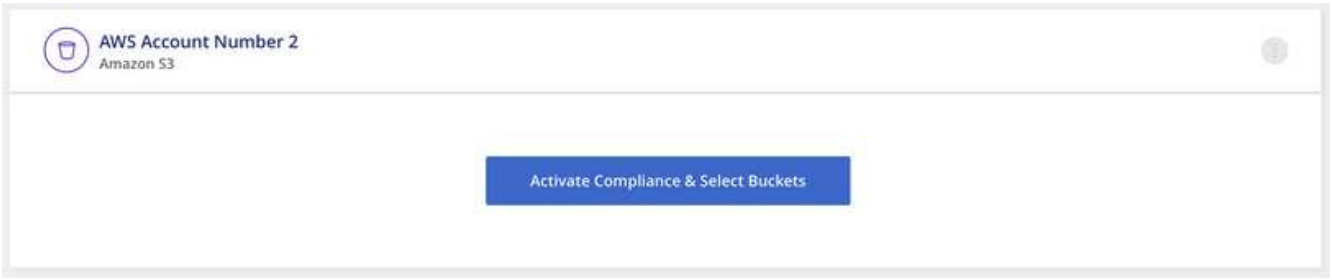
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

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 프로필 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.

데이터베이스 사전 요구 사항을 검토합니다

데이터베이스가 지원되고 데이터베이스에 연결하는 데 필요한 정보가 있는지 확인합니다.

클라우드 규정 준수 인스턴스 구축

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

데이터베이스 서버를 추가합니다

액세스할 데이터베이스 서버를 추가합니다.

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)

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.

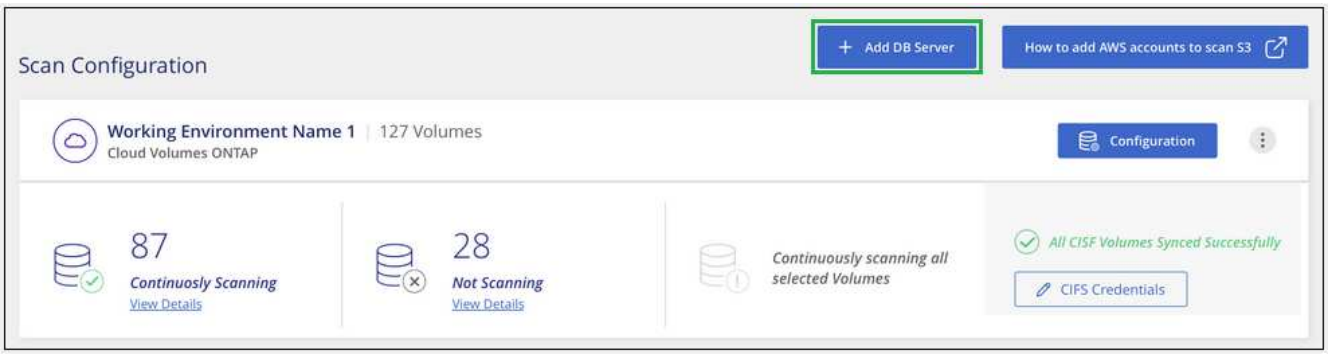
- 참고: * MongoDB의 경우 읽기 전용 관리자 역할이 필요합니다.

데이터베이스 서버 추가

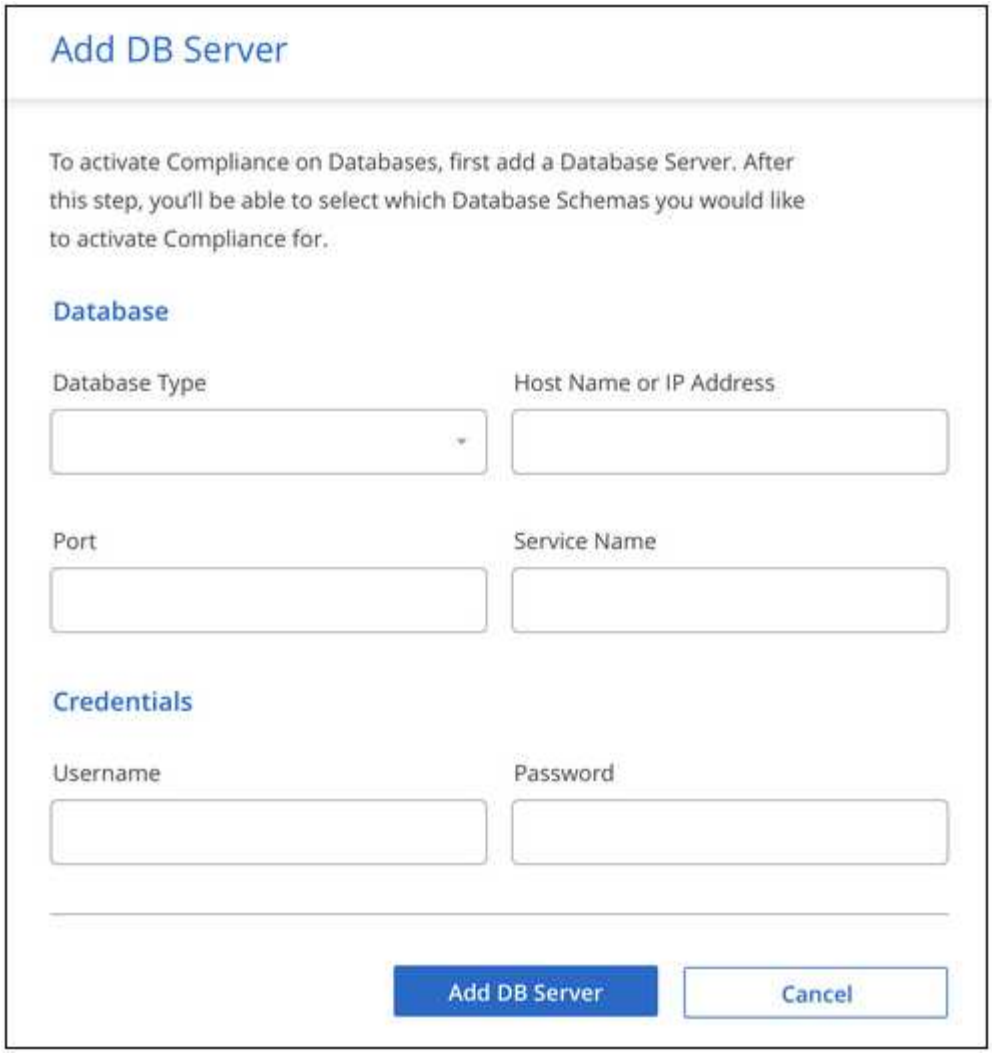
이(가) 있어야 합니다 "Cloud Manager에 이미 클라우드 규정 준수 인스턴스를 배포했습니다".

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.



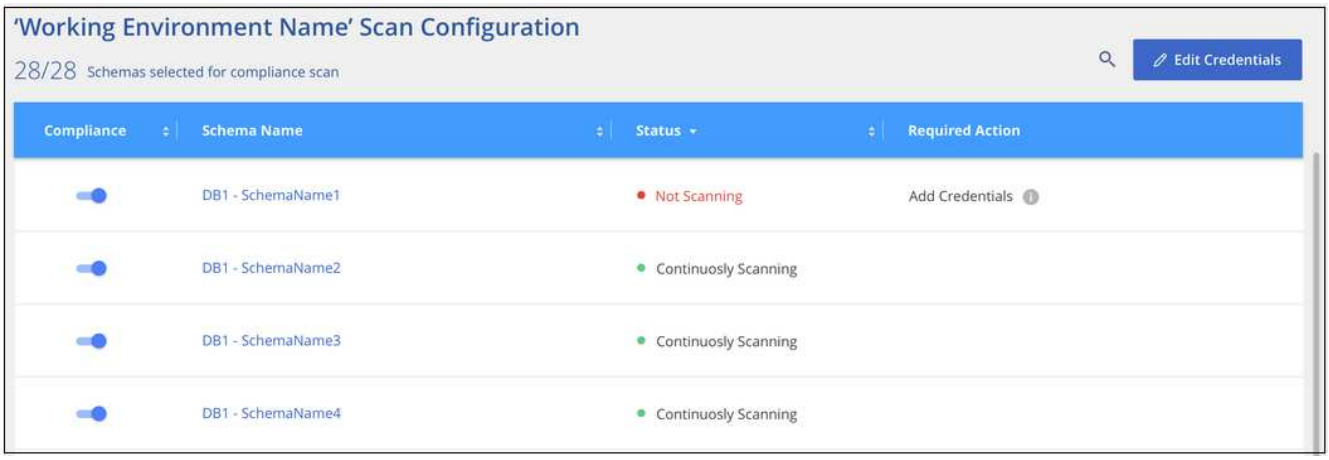
데이터베이스가 작업 디렉토리 목록에 추가됩니다.

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.



결과

Cloud Compliance는 사용자가 활성화한 데이터베이스 스키마 스캔을 시작합니다. 오류가 있는 경우 오류를 해결하는 데 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.

저작권 정보

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

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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