데이터 소스에서 스캐닝을 활성화하세요

NetApp Data Classification

NetApp
February 11, 2026

목차

데이터 소스에서 스캐닝을 활성화하세요 . . . 1
NetApp Data Classification 사용하여 데이터 소스 스캔 . . . 1
매핑 스캔과 분류 스캔의 차이점은 무엇입니까? . . . 1
NetApp Data Classification 사용하여 Amazon FSx 에서 ONTAP 볼륨 스캔 . . . 4
시작하기 전에 . . . 5
데이터 분류 인스턴스 배포 . . . 5
시스템에서 데이터 분류를 활성화하세요 . . . 5
데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. . . . 6
볼륨에서 스캔 활성화 및 비활성화 . . . 7
데이터 보호 볼륨 스캔 . . . 8
NetApp Data Classification 사용하여 Azure NetApp Files 볼륨 스캔 . . . 9
검사하려는 Azure NetApp Files 시스템을 검색하세요. . . . 9
데이터 분류 인스턴스 배포 . . . 9
시스템에서 데이터 분류를 활성화하세요 . . . 10
데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. . . . 10
볼륨에서 스캔을 활성화하거나 비활성화합니다. . . . 11
NetApp Data Classification 사용하여 Cloud Volumes ONTAP 및 온프레미스 ONTAP 볼륨 스캔 . . . 12
필수 조건 . . . 12
데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. . . . 13
볼륨에서 스캔을 활성화하거나 비활성화합니다. . . . 14
NetApp Data Classification 사용하여 데이터베이스 스키마 스캔 . . . 15
필수 조건 검토 . . . 15
데이터 분류 인스턴스 배포 . . . 16
데이터베이스 서버 추가 . . . 16
데이터베이스 스키마에 대한 스캔 활성화 및 비활성화 . . . 17
NetApp Data Classification 사용하여 Google Cloud NetApp Volumes 스캔 . . . 18
스캔하려는 Google Cloud NetApp Volumes 시스템을 검색하세요. . . . 18
데이터 분류 인스턴스 배포 . . . 18
시스템에서 데이터 분류를 활성화하세요 . . . 18
데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. . . . 19
볼륨에서 스캔 활성화 및 비활성화 . . . 20
NetApp Data Classification 사용하여 파일 공유 스캔 . . . 21
필수 조건 . . . 21
파일 공유 그룹 만들기 . . . 22
파일 공유 그룹 편집 . . . 23
스캐닝 진행 상황을 추적하세요 . . . 26
NetApp Data Classification 사용하여 StorageGRID 데이터 스캔 . . . 26
StorageGRID 요구 사항 검토 . . . 26
데이터 분류 인스턴스 배포 . . . 26

데이터 분류에 StorageGRID 서비스 추가 26
StorageGRID 버킷에서 스캔 활성화 및 비활성화 27

데이터 소스에서 스캐닝을 활성화하세요

NetApp Data Classification 사용하여 데이터 소스 스캔

NetApp Data Classification 사용자가 선택한 저장소(볼륨, 데이터베이스 스키마 또는 기타 사용자 데이터)의 데이터를 스캔하여 개인 데이터와 민감한 데이터를 식별합니다. 그런 다음 데이터 분류는 조직 데이터를 매핑하고, 각 파일을 분류하고, 데이터에서 미리 정의된 패턴을 식별합니다. 검사 결과는 개인 정보, 민감한 개인 정보, 데이터 범주 및 파일 유형의 인덱스입니다.

초기 스캔 이후, 데이터 분류는 라운드 로빈 방식으로 데이터를 지속적으로 스캔하여 증분적 변경 사항을 감지합니다. 인스턴스를 계속 실행하는 것이 중요한 이유가 여기에 있습니다.

볼륨 수준이나 데이터베이스 스키마 수준에서 검사를 활성화하거나 비활성화할 수 있습니다.

매핑 스캔과 분류 스캔의 차이점은 무엇입니까?

데이터 분류에서는 두 가지 유형의 스캔을 수행할 수 있습니다.

- 매핑 전용 스캔은 데이터에 대한 개략적인 개요만 제공하며 선택된 데이터 소스에서 수행됩니다. 매핑 전용 스캔은 파일에 액세스하여 내부 데이터를 확인하지 않기 때문에 매핑 및 분류 스캔보다 시간이 덜 걸립니다. 연구할 분야를 파악하기 위해 먼저 이 작업을 수행한 다음 해당 분야에 대한 지도 및 분류 검사를 수행하는 것이 좋습니다.
- **Map & Classify** 스캔은 데이터에 대한 심층적인 스캔을 제공합니다.

아래 표는 몇 가지 차이점을 보여줍니다.

특징	스캔 매핑 및 분류	매핑 전용 스캔
스캔 속도	느린	빠른
가격	무료	무료
용량	500TiB*로 제한됨	500TiB*로 제한됨
파일 유형 및 사용 용량 목록	예	예
파일 개수 및 사용 용량	예	예
파일의 나이와 크기	예	예
실행할 수 있는 능력"데이터 매핑 보고서"	예	예
파일 세부 정보를 보려면 데이터 조사 페이지로 이동하세요.	예	아니요
파일 내에서 이름 검색	예	아니요
만들다"저장된 쿼리" 사용자 정의 검색 결과를 제공하는	예	아니요
다른 보고서를 실행하는 기능	예	아니요
파일의 메타데이터를 볼 수 있는 기능**	아니요	예

{별표} 데이터 분류는 스캔할 수 있는 데이터 양에 제한을 두지 않습니다. 각 콘솔 에이전트는 500TiB의 데이터를 스캔하고 표시하는 것을 지원합니다. 500TiB 이상의 데이터를 스캔하려면"다른 콘솔 에이전트를 설치하세요" 그

다음에"다른 데이터 분류 인스턴스 배포" . + 콘솔 UI는 단일 커넥터의 데이터를 표시합니다. 여러 콘솔 에이전트의 데이터를 보는 방법에 대한 팁은 다음을 참조하세요."여러 콘솔 에이전트와 함께 작업" .

{별표}{별표} 매핑 스캔 중에 파일에서 다음 메타데이터가 추출됩니다.

- 체계
- 시스템 유형
- 저장 저장소
- 파일 유형
- 사용된 용량
- 파일 수
- 파일 크기
- 파일 생성
- 파일 마지막 접근
- 파일이 마지막으로 수정되었습니다
- 파일 발견 시간
- 권한 추출

거버넌스 대시보드 차이점:

특징	지도 및 분류	지도
오래된 데이터	예	예
비업무용 데이터	예	예
중복된 파일	예	예
미리 정의된 저장된 쿼리	예	아니요
기본 저장된 쿼리	예	예
DDA 보고서	예	예
매핑 보고서	예	예
감도 수준 감지	예	아니요
광범위한 권한이 있는 민감한 데이터	예	아니요
공개 권한	예	예
데이터의 시대	예	예
데이터 크기	예	예
카테고리	예	아니요
파일 유형	예	예

규정 준수 대시보드 차이점:

특징	지도 및 분류	지도
개인정보	예	아니요
민감한 개인 정보	예	아니요
개인정보 위험 평가 보고서	예	아니요
HIPAA 보고서	예	아니요
PCI DSS 보고서	예	아니요

조사 필터의 차이점은 다음과 같습니다.

특징	지도 및 분류	지도
저장된 쿼리	예	예
시스템 유형	예	예
체계	예	예
저장 저장소	예	예
파일 유형	예	예
파일 크기	예	예
생성 시간	예	예
발견된 시간	예	예
마지막 수정	예	예
마지막 접근	예	예
공개 권한	예	예
파일 디렉토리 경로	예	예
범주	예	아니요
민감도 수준	예	아니요
식별자의 수	예	아니요
개인정보	예	아니요
민감한 개인 데이터	예	아니요
데이터 주체	예	아니요
중복	예	예
분류 상태	예	상태는 항상 "제한된 통찰력"입니다.
스캔 분석 이벤트	예	예
파일 해시	예	예
접근 권한이 있는 사용자 수	예	예
사용자/그룹 권한	예	예
파일 소유자	예	예
디렉토리 유형	예	예

NetApp Data Classification 사용하여 Amazon FSx 에서 ONTAP 볼륨 스캔

NetApp Data Classification 사용하여 Amazon FSx for ONTAP 볼륨을 스캔하려면 몇 가지 단계를 완료하세요.

시작하기 전에

- 데이터 분류를 배포하고 관리하려면 AWS에서 활성 콘솔 에이전트가 필요합니다.
- 시스템을 생성할 때 선택한 보안 그룹은 데이터 분류 인스턴스의 트래픽을 허용해야 합니다. FSx for ONTAP 파일 시스템에 연결된 ENI를 사용하여 연관된 보안 그룹을 찾고 AWS Management Console을 사용하여 편집할 수 있습니다.

  "Linux 인스턴스용 AWS 보안 그룹"

  "Windows 인스턴스용 AWS 보안 그룹"

  "AWS 탄력적 네트워크 인터페이스(ENI)"

- 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요.
  - NFS의 경우 포트 111과 2049.
  - CIFS의 경우 포트 139 및 445.

데이터 분류 인스턴스 배포

"데이터 분류 배포"아직 배포된 인스턴스가 없는 경우.

AWS용 콘솔 에이전트와 스캔하려는 FSx 볼륨과 동일한 AWS 네트워크에 데이터 분류를 배포해야 합니다.

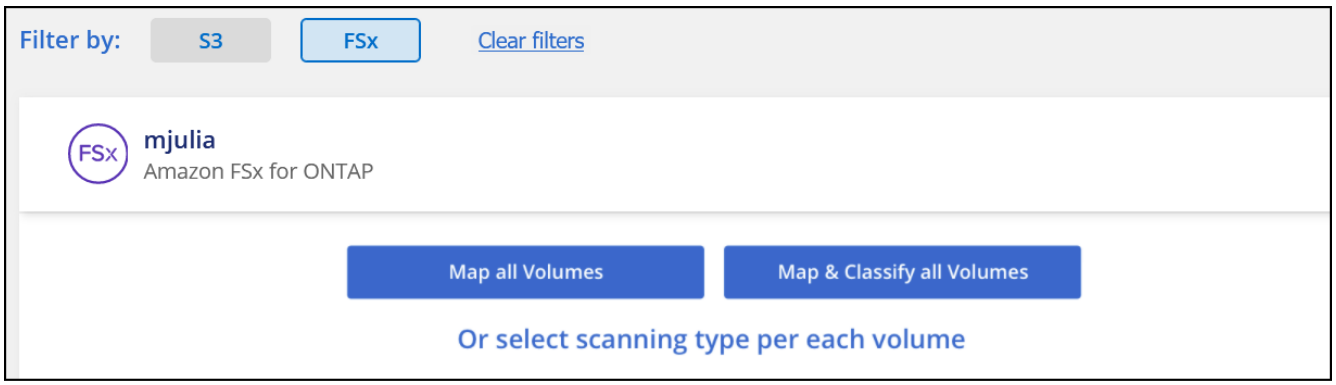
참고: FSx 볼륨을 스캔할 때 온프레미스 위치에 데이터 분류를 배포하는 것은 현재 지원되지 않습니다.

인스턴스에 인터넷 연결이 있는 한 데이터 분류 소프트웨어 업그레이드는 자동으로 수행됩니다.

시스템에서 데이터 분류를 활성화하세요

FSx for ONTAP 볼륨에 대한 데이터 분류를 활성화할 수 있습니다.

1. NetApp Console 에서 *거버넌스 > 분류*를 선택합니다.
2. 데이터 분류 메뉴에서 *구성*을 선택합니다.



3. 각 시스템의 볼륨을 스캔하는 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아보세요":
   - 모든 볼륨을 매핑하려면 *모든 볼륨 매핑*을 선택하세요.
   - 모든 볼륨을 매핑하고 분류하려면 *모든 볼륨 매핑 및 분류*를 선택하세요.

◦ 각 볼륨에 대한 스캐닝을 사용자 지정하려면 *또는 각 볼륨에 대한 스캐닝 유형 선택*을 선택한 다음 매핑 및 /또는 분류하려는 볼륨을 선택합니다.

4. 확인 대화 상자에서 *승인*을 선택하면 데이터 분류가 볼륨 검사를 시작합니다.

결과

데이터 분류는 시스템에서 선택한 볼륨에 대한 스캔을 시작합니다. 데이터 분류가 초기 스캔을 완료하는 즉시 규정 준수 대시보드에서 결과를 확인할 수 있습니다. 걸리는 시간은 데이터 양에 따라 다릅니다. 몇 분이나 몇 시간이 걸릴 수 있습니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 진행률 표시줄에서 각 검사의 진행 상황을 추적하세요. 진행률 표시줄 위에 마우스를 올리면 볼륨의 전체 파일 대비 검사된 파일 수를 확인할 수 있습니다.

- 기본적으로 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우 시스템은 볼륨의 파일을 검사하지 않습니다. 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 마지막 액세스 시간이 재설정되어도 상관없다면 *또는 각 볼륨에 대한 스캐닝 유형을 선택하세요*를 선택하세요. 결과 페이지에는 데이터 분류가 권한에 관계없이 볼륨을 검사하도록 설정할 수 있는 설정이 있습니다.
- 데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한에 대한 자세한 내용을 확인하세요." .

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

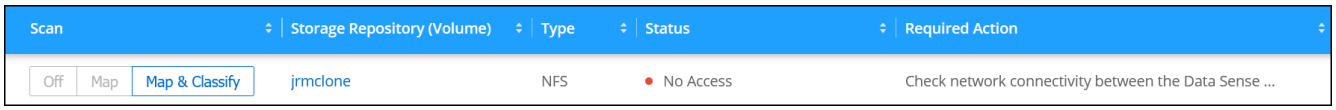
네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

CIFS 볼륨에 액세스할 수 있도록 데이터 분류에 CIFS 자격 증명을 제공해야 합니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 *세부 정보 보기*를 선택하여 상태를 검토하고 오류를 수정하세요.

   예를 들어, 다음 이미지는 데이터 분류 인스턴스와 볼륨 간의 네트워크 연결 문제로 인해 볼륨 데이터 분류가 스캔할 수 없는 상황을 보여줍니다.



3. FSx for ONTAP 볼륨이 포함된 각 네트워크와 데이터 분류 인스턴스 사이에 네트워크 연결이 있는지 확인하세요.

   FSx for ONTAP 의 경우 데이터 분류는 콘솔과 동일한 지역의 볼륨만 스캔할 수 있습니다.

4. NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.
5. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 분류를 제공합니다.

   a. 데이터 분류 메뉴에서 *구성*을 선택합니다.

   b. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택하고 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데

필요한 사용자 이름과 비밀번호를 입력합니다.

자격 증명은 읽기 전용일 수 있지만, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

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

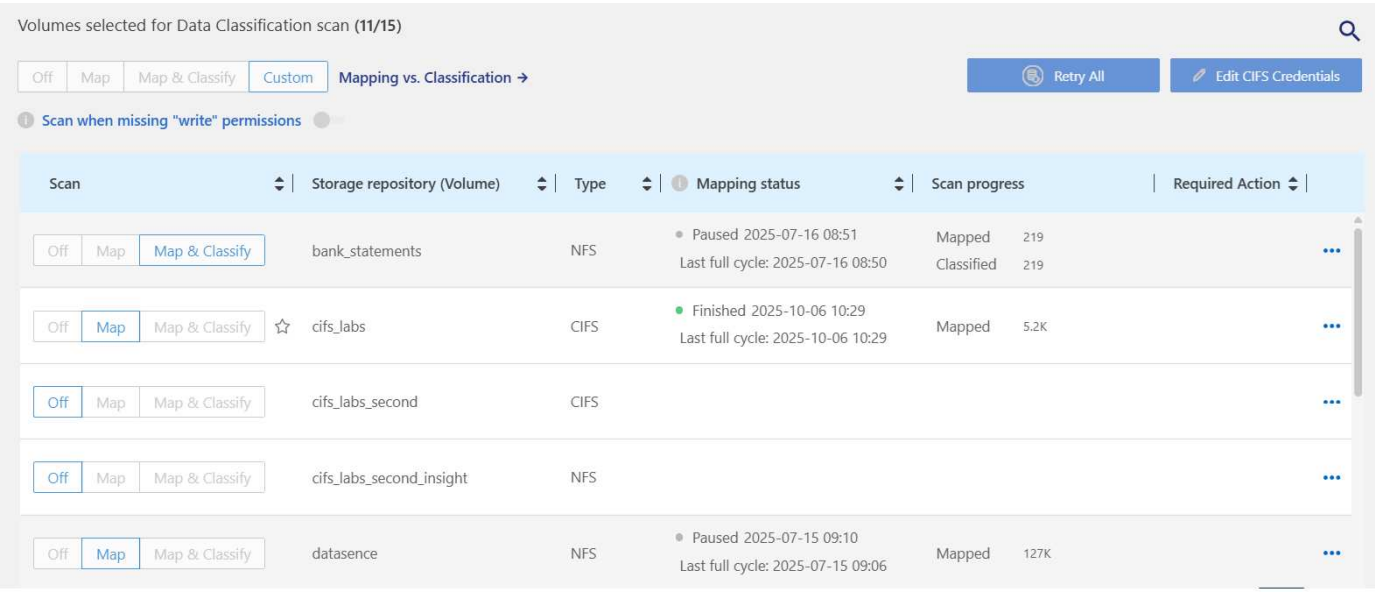
볼륨에서 스캔 활성화 및 비활성화

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.

3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

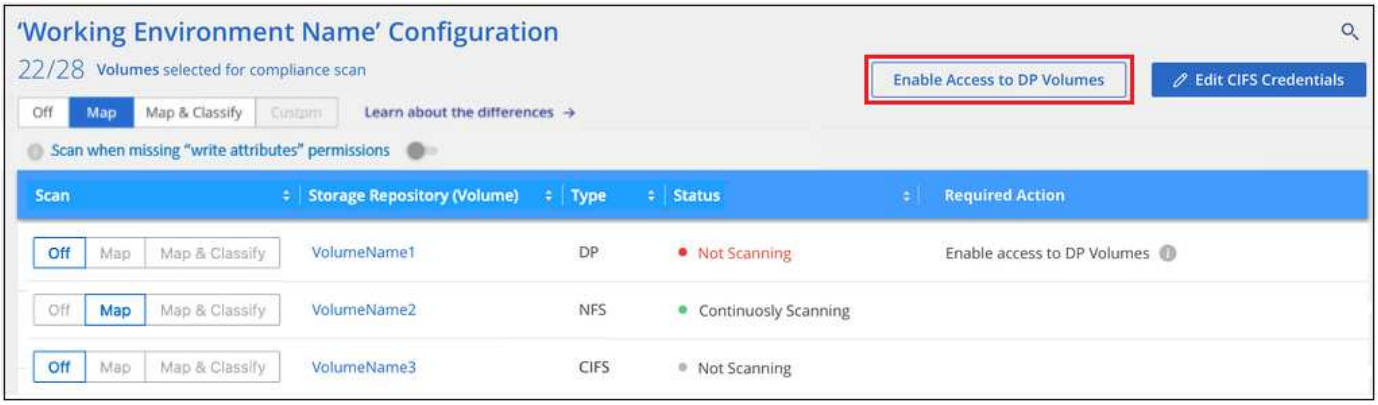
결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

데이터 보호 볼륨 스캔

기본적으로 데이터 보호(DP) 볼륨은 외부에 노출되지 않고 데이터 분류에서 액세스할 수 없으므로 스캔되지 않습니다. 이는 FSx for ONTAP 파일 시스템의 SnapMirror 작업을 위한 대상 볼륨입니다.

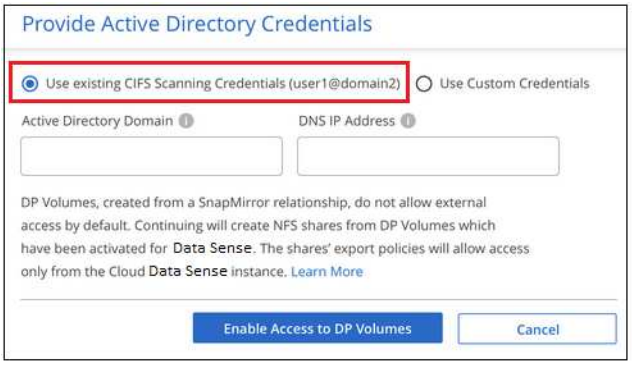
처음에 볼륨 목록은 이러한 볼륨을 유형 **DP**, 상태 스캔 안 함 및 필요한 작업 *DP 볼륨에 대한 액세스 활성화*로 식별합니다.

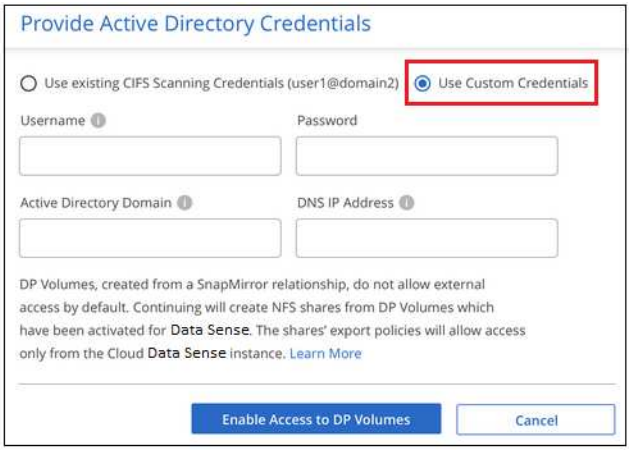


단계

다음 데이터 보호 볼륨을 스캔하려면 다음을 수행하세요.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 페이지 상단에서 *DP 볼륨에 대한 액세스 활성화*를 선택합니다.
3. 확인 메시지를 검토하고 *DP 볼륨에 대한 액세스 활성화*를 다시 선택합니다.
   - ONTAP 파일 시스템용 소스 FSx에서 원래 NFS 볼륨으로 생성된 볼륨이 활성화됩니다.
   - ONTAP 파일 시스템용 소스 FSx에서 CIFS 볼륨으로 처음 생성된 볼륨의 경우 해당 DP 볼륨을 스캔하려면 CIFS 자격 증명을 입력해야 합니다. 데이터 분류가 CIFS 볼륨을 검색할 수 있도록 이미 Active Directory 자격 증명을 입력한 경우 해당 자격 증명을 사용하거나 다른 관리자 자격 증명 집합을 지정할 수 있습니다.





4. 스캔하려는 각 DP 볼륨을 활성화합니다.

결과

데이터 분류가 활성화되면 스캐닝을 위해 활성화된 각 DP 볼륨에서 NFS 공유가 생성됩니다. 공유 내보내기 정책은 데이터 분류 인스턴스에서만 액세스를 허용합니다.

처음에 DP 볼륨에 대한 액세스를 활성화했을 때 CIFS 데이터 보호 볼륨이 없었고 나중에 볼륨을 추가한 경우, 구성 페이지 상단에 **CIFS DP**에 대한 액세스 활성화 버튼이 나타납니다. 이 버튼을 선택하고 CIFS 자격 증명을 추가하여 이러한 CIFS DP 볼륨에 대한 액세스를 활성화합니다.

Active Directory 자격 증명은 첫 번째 CIFS DP 볼륨의 스토리지 VM에만 등록되므로 해당 SVM의 모든 DP 볼륨이 검사됩니다. 다른 SVM에 있는 볼륨에는 Active Directory 자격 증명이 등록되지 않으므로 해당 DP 볼륨은 검사되지 않습니다.

NetApp Data Classification 사용하여 Azure NetApp Files 볼륨 스캔

Azure NetApp Files 에 대한 NetApp Data Classification 시작하려면 몇 가지 단계를 완료하세요.

검사하려는 **Azure NetApp Files** 시스템을 검색하세요.

검사하려는 Azure NetApp Files 시스템이 시스템으로 NetApp Console 에 아직 없는 경우"시스템 페이지에 추가하세요" .

데이터 분류 인스턴스 배포

"데이터 분류 배포"아직 배포된 인스턴스가 없는 경우.

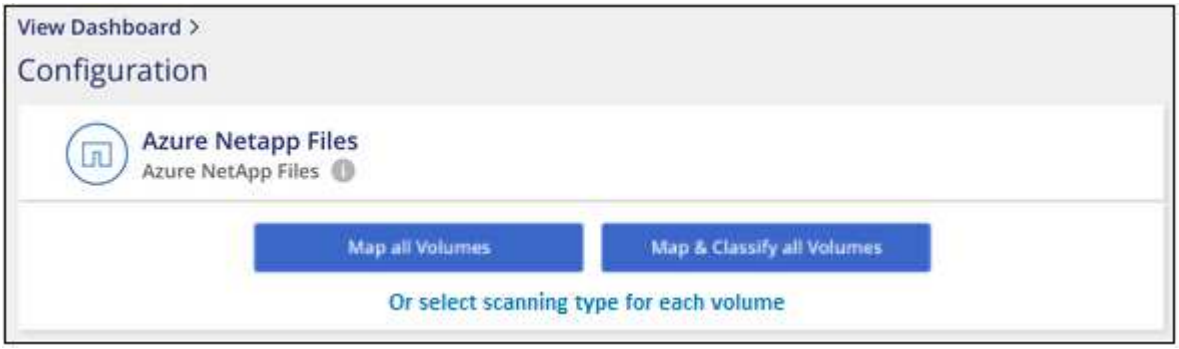
Azure NetApp Files 볼륨을 스캔할 때는 데이터 분류를 클라우드에 배포해야 하며, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.

참고: Azure NetApp Files 볼륨을 스캔할 때 온-프레미스 위치에 데이터 분류를 배포하는 것은 현재 지원되지 않습니다.

시스템에서 데이터 분류를 활성화하세요

Azure NetApp Files 볼륨에서 데이터 분류를 활성화할 수 있습니다.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.



2. 각 시스템의 볼륨을 스캔하는 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아보세요":
   - 모든 볼륨을 매핑하려면 *모든 볼륨 매핑*을 선택하세요.
   - 모든 볼륨을 매핑하고 분류하려면 *모든 볼륨 매핑 및 분류*를 선택하세요.
   - 각 볼륨에 대한 스캐닝을 사용자 지정하려면 *또는 각 볼륨에 대한 스캐닝 유형 선택*을 선택한 다음 매핑하거나 매핑하고 분류하려는 볼륨을 선택합니다.

     보다볼륨에서 스캔을 활성화하거나 비활성화합니다. 자세한 내용은.

3. 확인 대화 상자에서 *승인*을 선택합니다.

결과

데이터 분류는 시스템에서 선택한 볼륨에 대한 스캔을 시작합니다. 데이터 분류가 초기 스캔을 완료하면 규정 준수 대시보드에서 결과를 확인할 수 있습니다. 걸리는 시간은 데이터 양에 따라 다릅니다. 몇 분이나 몇 시간이 걸릴 수 있습니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 데이터 분류에서는 각 스캔에 대한 진행률 표시줄이 표시됩니다. 볼륨에 있는 전체 파일 수에 대한 검사된 파일 수를 확인하려면 진행률 표시줄 위에 마우스를 올려놓으세요.

- 기본적으로 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우 시스템은 볼륨의 파일을 검사하지 않습니다. 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 마지막 액세스 시간이 재설정되어도 상관없다면 *또는 각 볼륨에 대한 스캐닝 유형을 선택하세요*를 선택하세요. 결과 페이지에는 데이터 분류가 권한에 관계없이 볼륨을 검사하도록 설정할 수 있는 설정이 있습니다.
- 데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한 사항에 대해 알아보세요" .

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. CIFS 볼륨에 액세스할 수 있도록 데이터 분류에 CIFS 자격 증명을 제공해야 합니다.

Azure NetApp Files 의 경우 데이터 분류는 콘솔과 동일한 지역의 볼륨만 검색할 수 있습니다.

체크리스트

- 데이터 분류 인스턴스와 Azure NetApp Files 볼륨이 포함된 각 네트워크 간에 네트워크 연결이 있는지 확인하세요.
- 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요.
  - NFS의 경우 포트 111과 2049.
  - CIFS의 경우 포트 139 및 445.
- NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.

단계

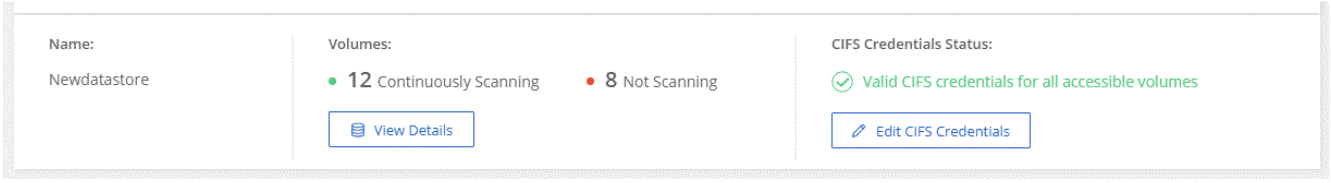
1. 데이터 분류 메뉴에서 *구성*을 선택합니다.

   a. CIFS(SMB)를 사용하는 경우 Active Directory 자격 증명이 올바른지 확인하세요. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택한 다음 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 비밀번호를 입력합니다.

      자격 증명은 읽기 전용일 수 있으며, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

      데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

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



2. 구성 페이지에서 *세부 정보 보기*를 선택하여 각 CIFS 및 NFS 볼륨의 상태를 검토합니다. 필요한 경우 네트워크 연결 문제 등의 오류를 수정하세요.

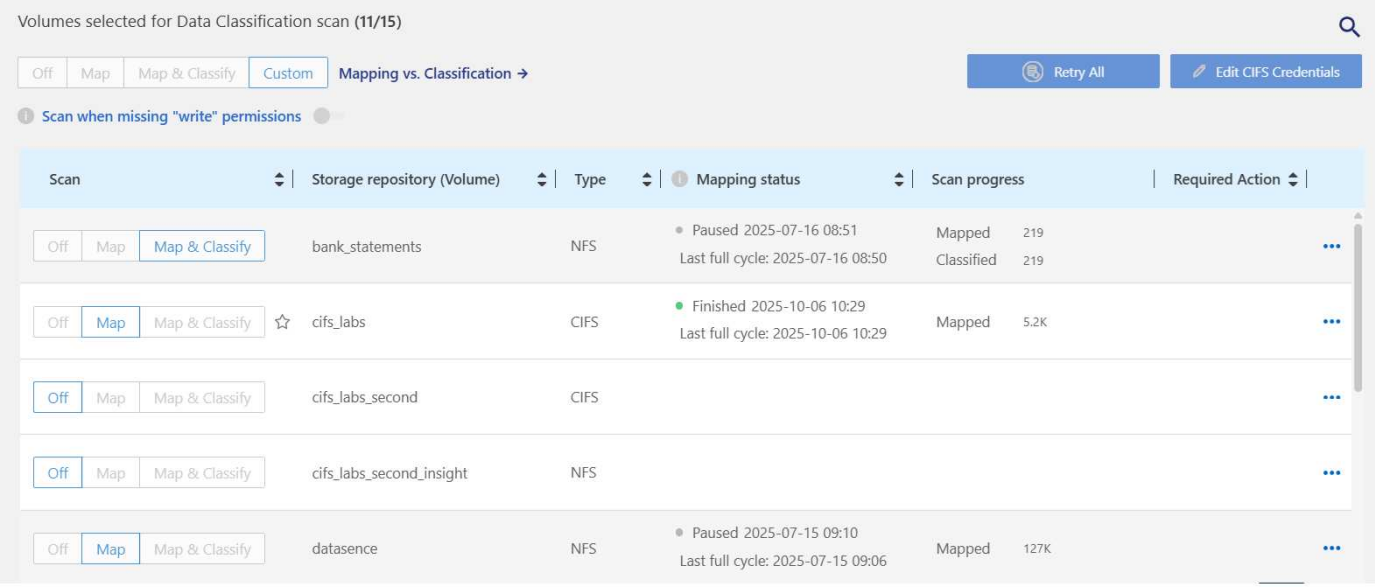
볼륨에서 스캔을 활성화하거나 비활성화합니다.

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.
3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

NetApp Data Classification 사용하여 Cloud Volumes ONTAP 및 온프레미스 ONTAP 볼륨 스캔

NetApp Data Classification 사용하여 Cloud Volumes ONTAP 및 온프레미스 ONTAP 볼륨 스캔을 시작하려면 몇 가지 단계를 완료하세요.

필수 조건

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하세요.

- 인터넷을 통해 액세스할 수 있는 Cloud Volumes ONTAP 및 온프레미스 ONTAP 시스템을 스캔하는 경우 다음을 수행할 수 있습니다."클라우드에 데이터 분류 배포" 또는"인터넷 접속이 가능한 사내 위치에서" .
- 인터넷 접속이 불가능한 다크 사이트에 설치된 온프레미스 ONTAP 시스템을 스캔하는 경우 다음이 필요합니다. "인터넷 접속이 없는 동일한 온프레미스 위치에 데이터 분류를 배포합니다." . 이렇게 하려면 콘솔 에이전트를 동일한 온프레미스 위치에 배포해야 합니다.

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. CIFS 볼륨에 액세스할 수 있도록 데이터 분류에 CIFS 자격 증명을 제공해야 합니다.

체크리스트

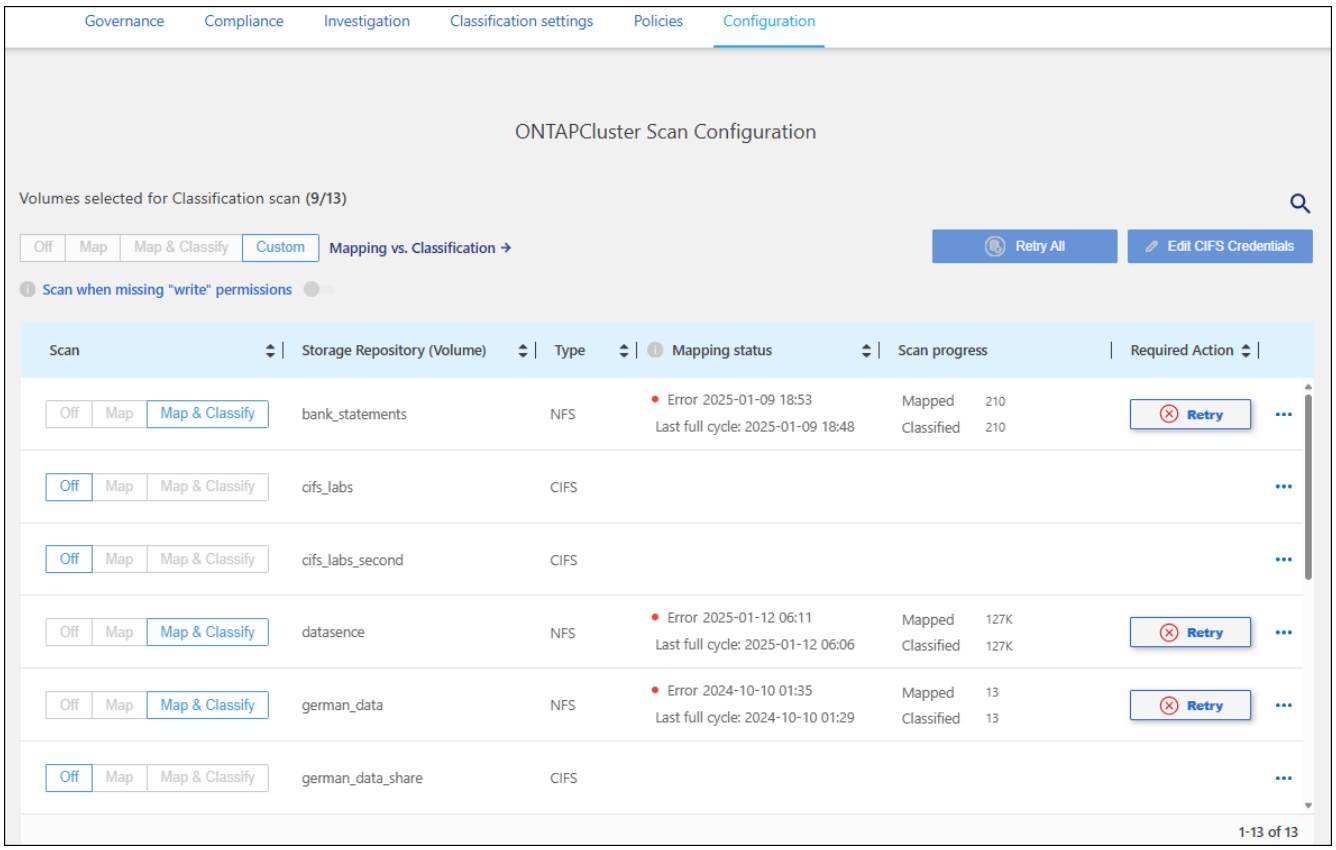
- 데이터 분류 인스턴스와 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터의 볼륨이 포함된 각 네트워크 간에 네트워크 연결이 있는지 확인하세요.
- Cloud Volumes ONTAP 의 보안 그룹이 데이터 분류 인스턴스에서 들어오는 트래픽을 허용하는지 확인하세요.

  데이터 분류 인스턴스의 IP 주소에서 발생하는 트래픽에 대해 보안 그룹을 열거나, 가상 네트워크 내부의 모든 트래픽에 대해 보안 그룹을 열 수 있습니다.

- NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.



2. CIFS를 사용하는 경우 CIFS 볼륨을 스캔할 수 있도록 Active Directory 자격 증명을 사용하여 데이터 분류를 제공합니다. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택하고 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 비밀번호를 입력합니다.

   자격 증명은 읽기 전용일 수 있지만, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

   데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기

속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

자격 증명을 올바르게 입력한 경우 모든 CIFS 볼륨이 성공적으로 인증되었음을 확인하는 메시지가 표시됩니다.

3. 구성 페이지에서 *구성*을 선택하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

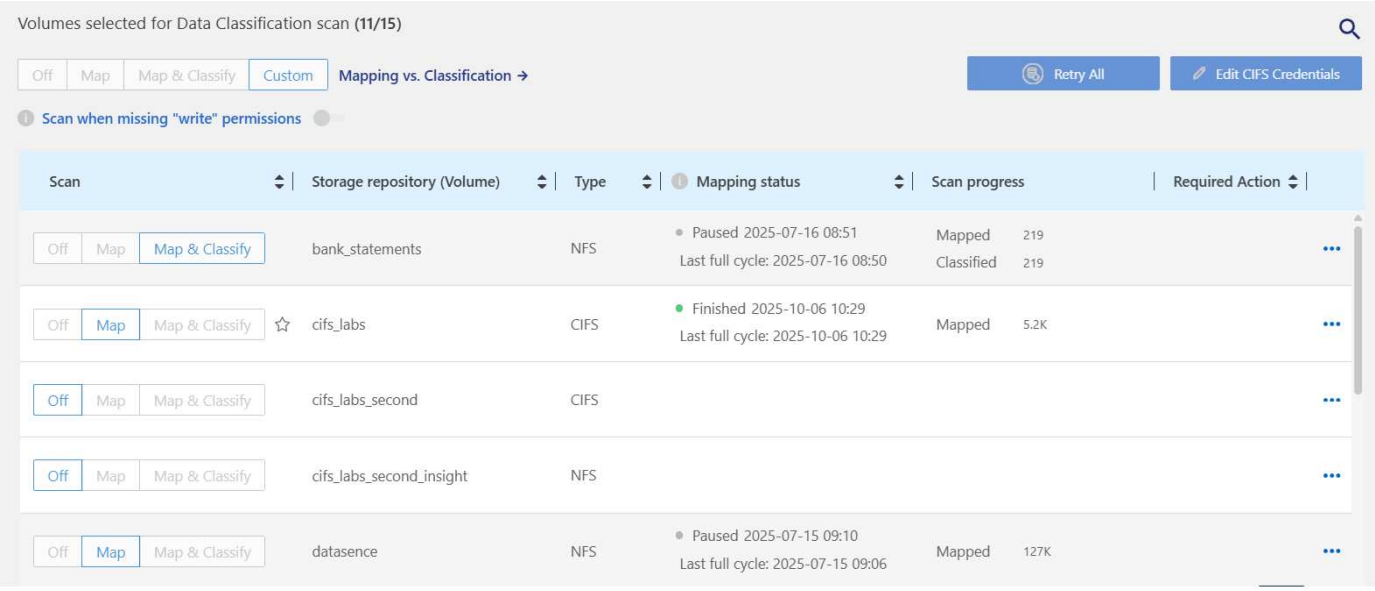
볼륨에서 스캔을 활성화하거나 비활성화합니다.

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.
3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한에 대한 자세한 내용을 확인하세요." .

NetApp Data Classification 사용하여 데이터베이스 스키마 스캔

NetApp Data Classification 사용하여 데이터베이스 스키마 스캔을 시작하려면 몇 가지 단계를 완료하세요.

필수 조건 검토

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요.

지원되는 데이터베이스

데이터 분류는 다음 데이터베이스에서 스키마를 스캔할 수 있습니다.

- Amazon 관계형 데이터베이스 서비스(Amazon RDS)
- 몽고디비
- MySQL
- 신탁
- 포스트그레스큐엘
- SAP 하나
- SQL 서버(MSSQL)

데이터베이스에서 통계 수집 기능을 *활성화*해야 합니다.

데이터베이스 요구 사항

데이터 분류 인스턴스에 연결된 모든 데이터베이스는 호스팅 위치에 관계없이 스캔할 수 있습니다. 데이터베이스에 연결하려면 다음 정보가 필요합니다.

- IP 주소 또는 호스트 이름
- 포트
- 서비스 이름(Oracle 데이터베이스에 액세스하는 경우에만 해당)
- 스키마에 대한 읽기 액세스를 허용하는 자격 증명

  사용자 이름과 비밀번호를 선택할 때는 스캔하려는 모든 스키마와 테이블에 대한 전체 읽기 권한이 있는 것을 선택하는 것이 중요합니다. 데이터 분류 시스템에 필요한 모든 권한을 갖춘 전담 사용자를 만드는 것이 좋습니다.

MongoDB의 경우 읽기 전용 관리자 역할이 필요합니다.

데이터 분류 인스턴스 배포

아직 배포된 인스턴스가 없으면 데이터 분류를 배포합니다.

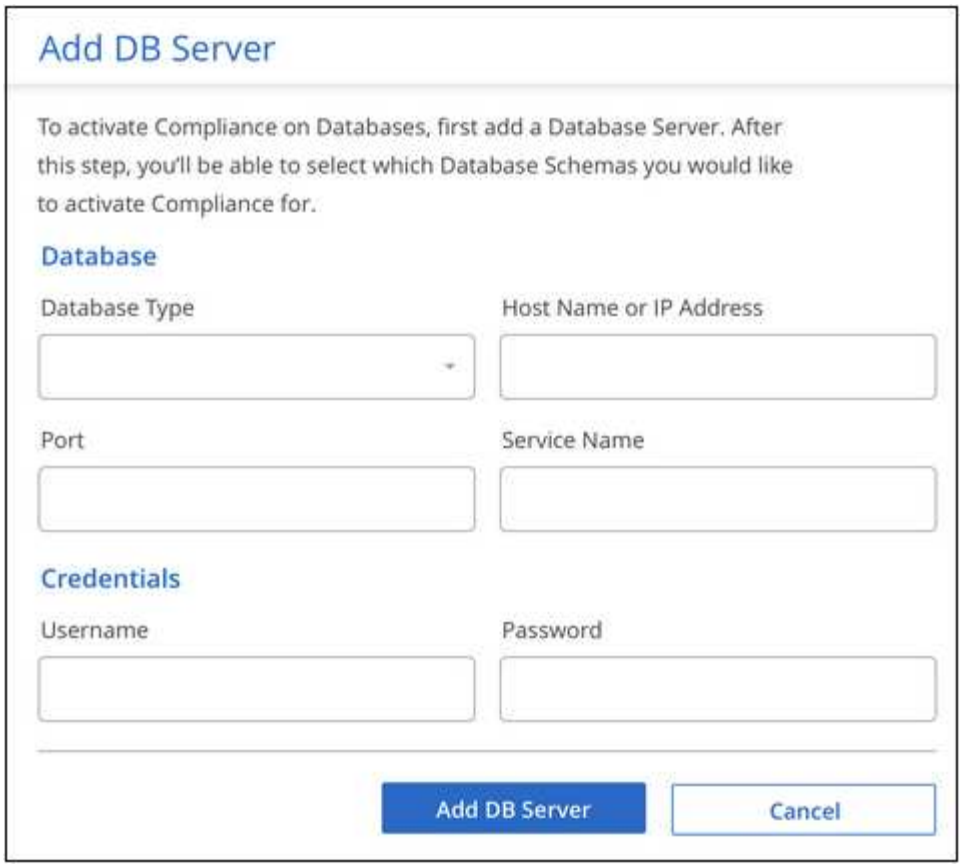
인터넷을 통해 접근 가능한 데이터베이스 스키마를 스캔하는 경우 다음을 수행할 수 있습니다."클라우드에 데이터 분류 배포" 또는"인터넷 접속이 가능한 온프레미스 위치에 데이터 분류를 배포합니다." .

인터넷 접속이 불가능한 다크 사이트에 설치된 데이터베이스 스키마를 스캔하는 경우 다음이 필요합니다."인터넷 접속이 없는 동일한 온프레미스 위치에 데이터 분류를 배포합니다." . 이를 위해서는 콘솔 에이전트가 동일한 온프레미스 위치에 배포되어야 합니다.

데이터베이스 서버 추가

스키마가 있는 데이터베이스 서버를 추가합니다.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 시스템 추가 > *데이터베이스 서버 추가*를 선택합니다.
3. 데이터베이스 서버를 식별하는 데 필요한 정보를 입력하세요.
    a. 데이터베이스 유형을 선택하세요.
    b. 데이터베이스에 연결하려면 포트와 호스트 이름 또는 IP 주소를 입력하세요.
    c. Oracle 데이터베이스의 경우 서비스 이름을 입력합니다.
    d. 데이터 분류가 서버에 액세스할 수 있도록 자격 증명을 입력하세요.
    e. *DB 서버 추가*를 선택합니다.



데이터베이스가 시스템 목록에 추가되었습니다.

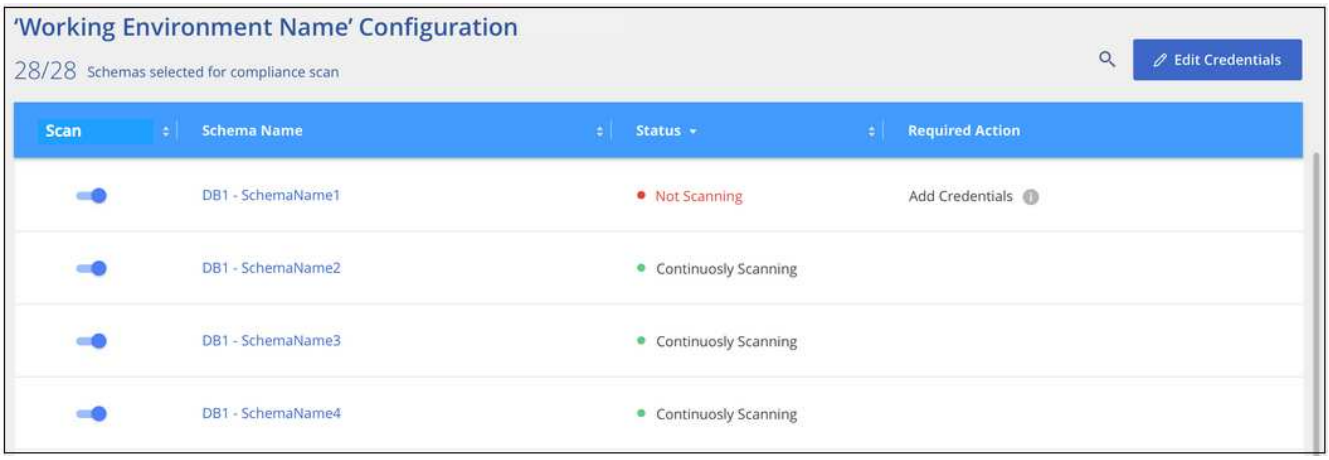
데이터베이스 스키마에 대한 스캔 활성화 및 비활성화

언제든지 스키마 전체 스캐닝을 중지하거나 시작할 수 있습니다.

데이터베이스 스키마에 대해 매핑 전용 스캔을 선택하는 옵션은 없습니다.

1. 구성 페이지에서 구성하려는 데이터베이스에 대한 구성 버튼을 선택합니다.

2. 슬라이더를 오른쪽으로 움직여 검사할 스키마를 선택합니다.



결과

데이터 분류는 활성화된 데이터베이스 스키마를 스캔하기 시작합니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 각 스캔의 진행 상황은 진행률 표시줄로 표시됩니다. 진행률 표시줄 위에 마우스를 올려 놓으면 볼륨에 있는 전체 파일 수에 대한 검사된 파일 수를 확인할 수 있습니다. 오류가 있는 경우 오류 수정에 필요한 작업과 함께 상태 열에 오류가 표시됩니다.

데이터 분류는 하루에 한 번씩 데이터베이스를 스캔합니다. 데이터베이스는 다른 데이터 소스처럼 지속적으로 스캔되지 않습니다.

NetApp Data Classification 사용하여 Google Cloud NetApp Volumes 스캔

NetApp Data Classification 시스템으로서 Google Cloud NetApp Volumes 지원합니다. Google Cloud NetApp Volumes 시스템을 스캔하는 방법을 알아보세요.

스캔하려는 **Google Cloud NetApp Volumes** 시스템을 검색하세요.

스캔하려는 Google Cloud NetApp Volumes 시스템이 NetApp Console 에 시스템으로 아직 없는 경우"시스템 페이지에 추가하세요" .

데이터 분류 인스턴스 배포

"데이터 분류 배포"아직 배포된 인스턴스가 없는 경우.

Google Cloud NetApp Volumes 스캔할 때는 데이터 분류를 클라우드에 배포해야 하며, 스캔하려는 볼륨과 동일한 지역에 배포해야 합니다.

참고: 현재 Google Cloud NetApp Volumes 스캔할 때 온프레미스 위치에 데이터 분류를 배포하는 것은 지원되지 않습니다.

시스템에서 데이터 분류를 활성화하세요

Google Cloud NetApp Volumes 시스템에서 데이터 분류를 활성화할 수 있습니다.

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.

2. 각 시스템의 볼륨을 스캔하는 방법을 선택합니다. "매핑 및 분류 스캔에 대해 알아보세요":
   - 모든 볼륨을 매핑하려면 *모든 볼륨 매핑*을 선택하세요.
   - 모든 볼륨을 매핑하고 분류하려면 *모든 볼륨 매핑 및 분류*를 선택하세요.
   - 각 볼륨에 대한 스캐닝을 사용자 지정하려면 *또는 각 볼륨에 대한 스캐닝 유형 선택*을 선택한 다음 매핑 및/또는 분류하려는 볼륨을 선택합니다.

     보다볼륨에서 스캔 활성화 및 비활성화 자세한 내용은.
3. 확인 대화 상자에서 *승인*을 선택합니다.

결과

데이터 분류는 시스템에서 선택한 볼륨에 대한 스캔을 시작합니다. 데이터 분류가 초기 스캔을 완료하면 규정 준수 대시보드에서 결과를 확인할 수 있습니다. 걸리는 시간은 데이터 양에 따라 다릅니다. 몇 분에서 몇 시간까지 걸립니다. 구성 메뉴의 시스템 구성 섹션에서 초기 검사의 진행 상황을 추적할 수 있습니다. 데이터 분류에서는 각 스캔에 대한 진행률 표시줄이 표시됩니다. 진행률 표시줄 위에 마우스를 올려 놓으면 볼륨의 전체 파일 대비 검사된 파일 수를 확인할 수 있습니다.

- 기본적으로 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우 시스템은 볼륨의 파일을 검사하지 않습니다. 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문입니다. 마지막 액세스 시간이 재설정되어도 상관없다면 *또는 각 볼륨에 대한 스캐닝 유형을 선택하세요*를 선택하세요. 결과 페이지에는 데이터 분류가 권한에 관계없이 볼륨을 검사하도록 설정할 수 있는 설정이 있습니다.
- 데이터 분류는 볼륨 아래의 파일 공유를 하나만 스캔합니다. 볼륨에 여러 개의 주식이 있는 경우 다른 주식을 주식 그룹으로 별도로 스캔해야 합니다. "이 데이터 분류 제한 사항에 대해 알아보세요".

데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요.

네트워킹, 보안 그룹 및 내보내기 정책을 확인하여 데이터 분류가 볼륨에 액세스할 수 있는지 확인하세요. CIFS 볼륨의 경우 CIFS 자격 증명을 사용하여 데이터 분류를 제공해야 합니다.

Google Cloud NetApp Volumes 의 경우 데이터 분류는 콘솔과 동일한 지역의 볼륨만 스캔할 수 있습니다.

체크리스트

- Google Cloud NetApp Volumes 대한 볼륨이 포함된 각 네트워크와 데이터 분류 인스턴스 사이에 네트워크 연결이 있는지 확인하세요.
- 다음 포트가 데이터 분류 인스턴스에 열려 있는지 확인하세요.
  - NFS의 경우 포트 111과 2049.
  - CIFS의 경우 포트 139 및 445.
- NFS 볼륨 내보내기 정책에 데이터 분류 인스턴스의 IP 주소가 포함되어 있는지 확인하여 각 볼륨의 데이터에 액세스할 수 있도록 합니다.

단계

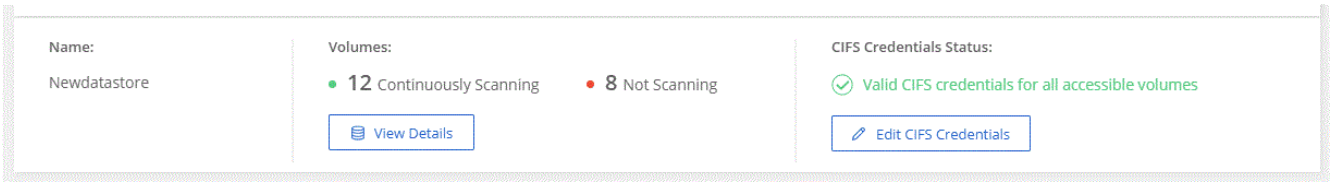
1. 데이터 분류 메뉴에서 *구성*을 선택합니다.

   a. CIFS(SMB)를 사용하는 경우 Active Directory 자격 증명이 올바른지 확인하세요. 각 시스템에 대해 *CIFS 자격 증명 편집*을 선택한 다음 데이터 분류가 시스템의 CIFS 볼륨에 액세스하는 데 필요한 사용자 이름과 비밀번호를 입력합니다.

자격 증명은 읽기 전용일 수 있지만, 관리자 자격 증명을 제공하면 데이터 분류에서 높은 권한이 필요한 모든 데이터를 읽을 수 있습니다. 자격 증명은 데이터 분류 인스턴스에 저장됩니다.

데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

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



2. 구성 페이지에서 *세부 정보 보기*를 선택하여 각 CIFS 및 NFS 볼륨의 상태를 검토하고 오류를 수정합니다.

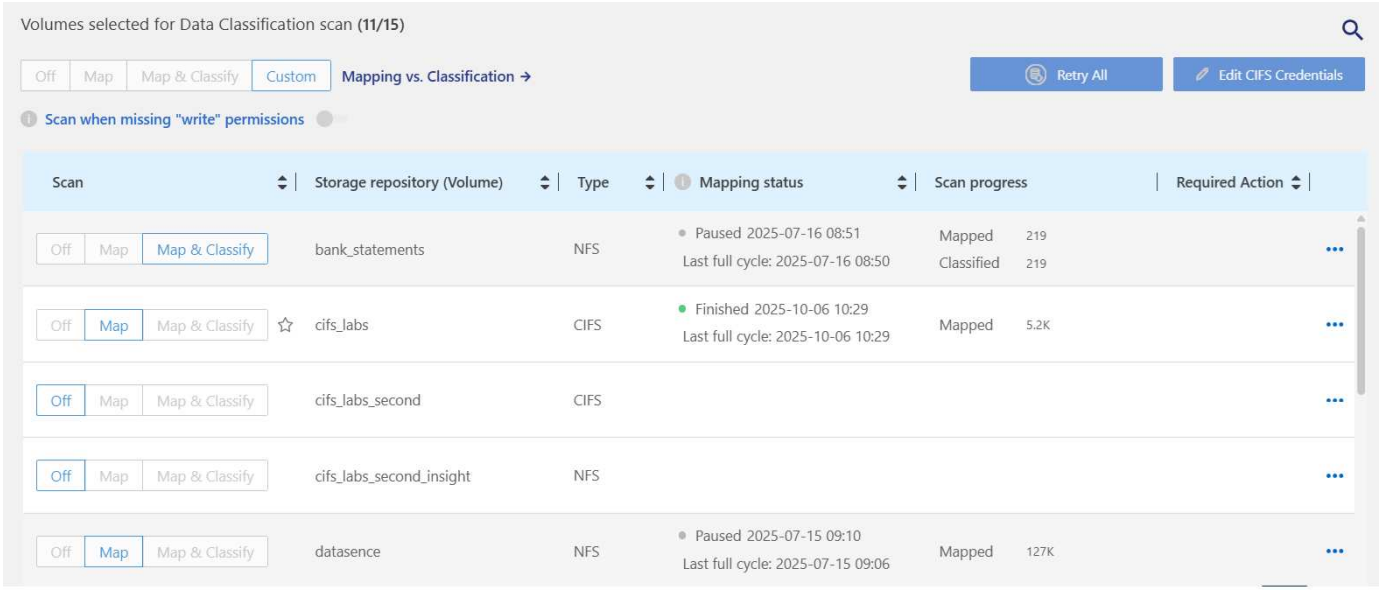
볼륨에서 스캔 활성화 및 비활성화

구성 페이지에서 언제든지 모든 시스템의 검사를 시작하거나 중지할 수 있습니다. 매핑 전용 스캔에서 매핑 및 분류 스캔으로 전환할 수도 있고, 그 반대로도 가능합니다. 시스템의 모든 볼륨을 스캔하는 것이 좋습니다.

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 선택한 경우에만 자동으로 스캔됩니다. 제목 영역에서 사용자 지정 또는 *끄기*로 설정하면 시스템에 추가하는 각 새 볼륨에 대해 매핑 및/또는 전체 스캐닝을 활성화해야 합니다.

기본적으로 페이지 상단의 쓰기 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. 마지막 접근 시간이 재설정되어도 상관없다면 스위치를 켜면 권한에 관계없이 모든 파일이 검사됩니다. "자세히 알아보기".

시스템에 추가된 새 볼륨은 제목 영역에서 지도 또는 지도 및 분류 설정을 지정한 경우에만 자동으로 스캔됩니다. 모든 볼륨에 대한 설정이 사용자 지정 또는 *끄기*인 경우, 새로 추가하는 각 볼륨에 대해 수동으로 스캐닝을 활성화해야 합니다.



단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 시스템을 선택한 다음 *구성*을 선택하세요.
3. 모든 볼륨에 대한 검사를 활성화하거나 비활성화하려면 모든 볼륨 위의 제목에서 맵, 맵 및 분류 또는 끄기를 선택합니다.

   개별 볼륨에 대한 검사를 활성화하거나 비활성화하려면 목록에서 볼륨을 찾은 다음 볼륨 이름 옆에 있는 매핑, 매핑 및 분류 또는 끄기를 선택합니다.

결과

스캐닝을 활성화하면 데이터 분류가 시스템에서 선택한 볼륨을 스캐닝하기 시작합니다. 데이터 분류가 스캔을 시작하자마자 규정 준수 대시보드에 결과가 나타나기 시작합니다. 검사 완료 시간은 데이터 양에 따라 달라지며, 몇 분에서 몇 시간까지 걸릴 수 있습니다.

NetApp Data Classification 사용하여 파일 공유 스캔

파일 공유를 스캔하려면 먼저 NetApp Data Classification 에서 파일 공유 그룹을 만들어야 합니다. 파일 공유 그룹은 온프레미스 또는 클라우드에서 호스팅되는 NFS 또는 CIFS(SMB) 공유를 위한 것입니다.

데이터 분류 핵심 버전에서는 NetApp 아닌 파일 공유에서 데이터를 스캔하는 기능이 지원되지 않습니다.

필수 조건

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요.

- 공유는 클라우드나 온프레미스 등 어디에서나 호스팅될 수 있습니다. 이전 NetApp 7-Mode 스토리지 시스템의 CIFS 공유는 파일 공유로 스캔될 수 있습니다.
  - 데이터 분류는 7-Mode 시스템에서 권한이나 "마지막 액세스 시간"을 추출할 수 없습니다.
  - 7-Mode 시스템에서 일부 Linux 버전과 CIFS 공유 간에 알려진 문제로 인해 NTLM 인증이 활성화된 SMBv1만 사용하도록 공유를 구성해야 합니다.
- 데이터 분류 인스턴스와 공유 간에 네트워크 연결이 필요합니다.
- DFS(분산 파일 시스템) 공유를 일반 CIFS 공유로 추가할 수 있습니다. 데이터 분류에서는 공유가 단일 CIFS 공유로 결합된 여러 서버/볼륨에 기반을 두고 있다는 사실을 인식하지 못하기 때문에 메시지가 실제로는 다른 서버/볼륨에 있는 폴더/공유 중 하나에만 적용되는 경우에도 공유에 대한 권한 또는 연결 오류가 발생할 수 있습니다.
- CIFS(SMB) 공유의 경우 공유에 대한 읽기 액세스 권한을 제공하는 Active Directory 자격 증명이 있는지 확인하세요. 데이터 분류에서 높은 권한이 필요한 데이터를 스캔해야 하는 경우 관리자 자격 증명이 선호됩니다.

  데이터 분류 검사를 통해 파일의 "마지막 액세스 시간"이 변경되지 않았는지 확인하려면 사용자에게 CIFS에서 쓰기 속성 권한이나 NFS에서 쓰기 권한이 있는 것이 좋습니다. 가능하다면 Active Directory 사용자를 모든 파일에 대한 권한이 있는 조직의 상위 그룹의 일부로 구성하세요.

- 그룹 내의 모든 CIFS 파일 공유는 동일한 Active Directory 자격 증명을 사용해야 합니다.
- NFS와 CIFS(Kerberos 또는 NTLM 사용) 공유를 혼합할 수 있습니다. 그룹에 주식을 별도로 추가해야 합니다. 즉,

프로토콜당 한 번씩, 총 두 번 프로세스를 완료해야 합니다.

- CIFS 인증 유형(Kerberos 및 NTLM)을 혼합하여 파일 공유 그룹을 만들 수 없습니다.

- Kerberos 인증을 사용하는 CIFS를 사용하는 경우 제공된 IP 주소가 데이터 분류에 액세스할 수 있는지 확인하세요. IP 주소에 접근할 수 없으면 파일 공유를 추가할 수 없습니다.

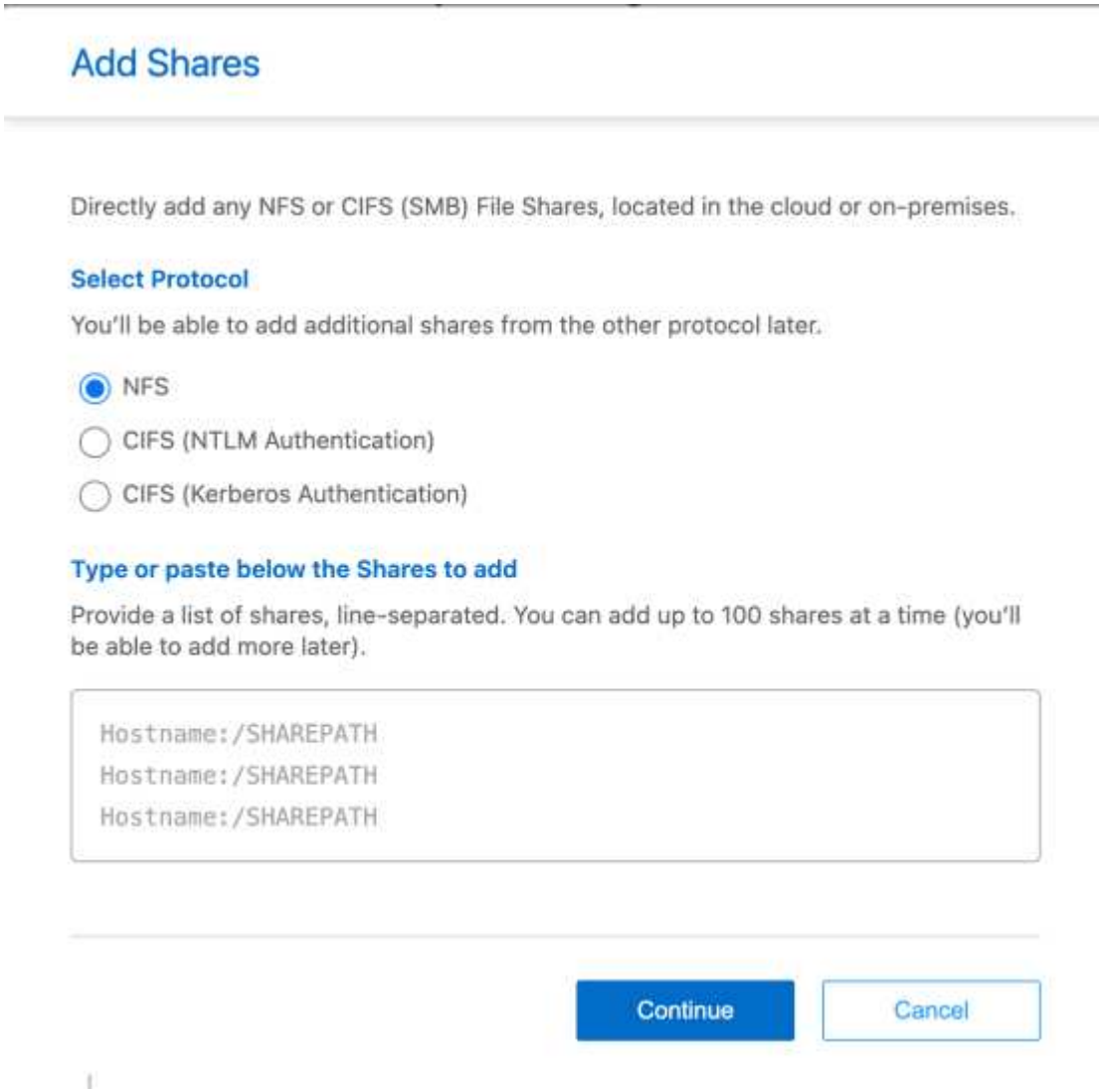
파일 공유 그룹 만들기

그룹에 파일 공유를 추가할 때는 다음 형식을 사용해야 합니다. `<host_name>:/<share_path>` .

파일 공유를 개별적으로 추가할 수도 있고, 검사하려는 파일 공유를 줄로 구분하여 나열하여 입력할 수도 있습니다. 한 번에 최대 100개의 주식을 추가할 수 있습니다.

단계

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 시스템 추가 > *파일 공유 그룹 추가*를 선택합니다.
3. 파일 공유 그룹 추가 대화 상자에서 공유 그룹의 이름을 입력한 다음 *계속*을 선택합니다.
4. 추가할 파일 공유에 대한 프로토콜을 선택하세요.



a. NTLM 인증을 사용하여 CIFS 공유를 추가하는 경우 Active Directory 자격 증명을 입력하여 CIFS 볼륨에 액세스합니다. 읽기 전용 자격 증명도 지원되지만 관리자 자격 증명을 사용하여 전체 액세스 권한을 제공하는 것이 좋습니다. 저장을 선택하세요.

5. 검사하려는 파일 공유를 추가합니다(한 줄에 파일 공유 하나씩). 그런 다음 계속을 선택하세요.
6. 확인 대화 상자에는 추가된 주식 수가 표시됩니다.

   대화 상자에 추가할 수 없는 공유가 나열되면 이 정보를 캡처하여 문제를 해결하세요. 문제가 명명 규칙과 관련된 경우, 수정된 이름으로 공유를 다시 추가할 수 있습니다.

7. 볼륨에 대한 스캐닝을 구성합니다.
   - 파일 공유에서 매핑 전용 검사를 활성화하려면 *매핑*을 선택합니다.
   - 파일 공유에 대한 전체 검사를 활성화하려면 *매핑 및 분류*를 선택하세요.
   - 파일 공유에서 스캐닝을 비활성화하려면 *끄기*를 선택하세요.

> 기본적으로 페이지 상단의 **"쓰기 속성"** 권한이 없는 경우 검사 스위치는 비활성화되어 있습니다. 즉, 데이터 분류에 CIFS에서 쓰기 속성 권한이 없거나 NFS에서 쓰기 권한이 없는 경우, 데이터 분류는 "마지막 액세스 시간"을 원래 타임스탬프로 되돌릴 수 없기 때문에 시스템은 파일을 검사하지 않습니다. + "쓰기 속성" 권한이 없는 경우 검사*를 *켜기*로 전환하면 검사에서 마지막으로 액세스한 시간을 재설정하고 권한에 관계없이 모든 파일을 검사합니다. + 마지막으로 액세스한 타임스탬프에 대해 자세히 알아보려면 다음을 참조하세요."데이터 분류의 데이터 소스에서 수집된 메타데이터" .

결과

데이터 분류는 추가한 파일 공유에 있는 파일의 스캔을 시작합니다. 당신은 할 수 있습니다스캐닝 진행 상황을 추적하세요 대시보드에서 검사 결과를 확인하세요.

> Kerberos 인증을 사용하는 CIFS 구성에 대한 스캔이 성공적으로 완료되지 않으면 구성 탭에서 오류를 확인하세요.

파일 공유 그룹 편집

파일 공유 그룹을 만든 후에는 CIFS 프로토콜을 편집하거나 파일 공유를 추가 및 제거할 수 있습니다.

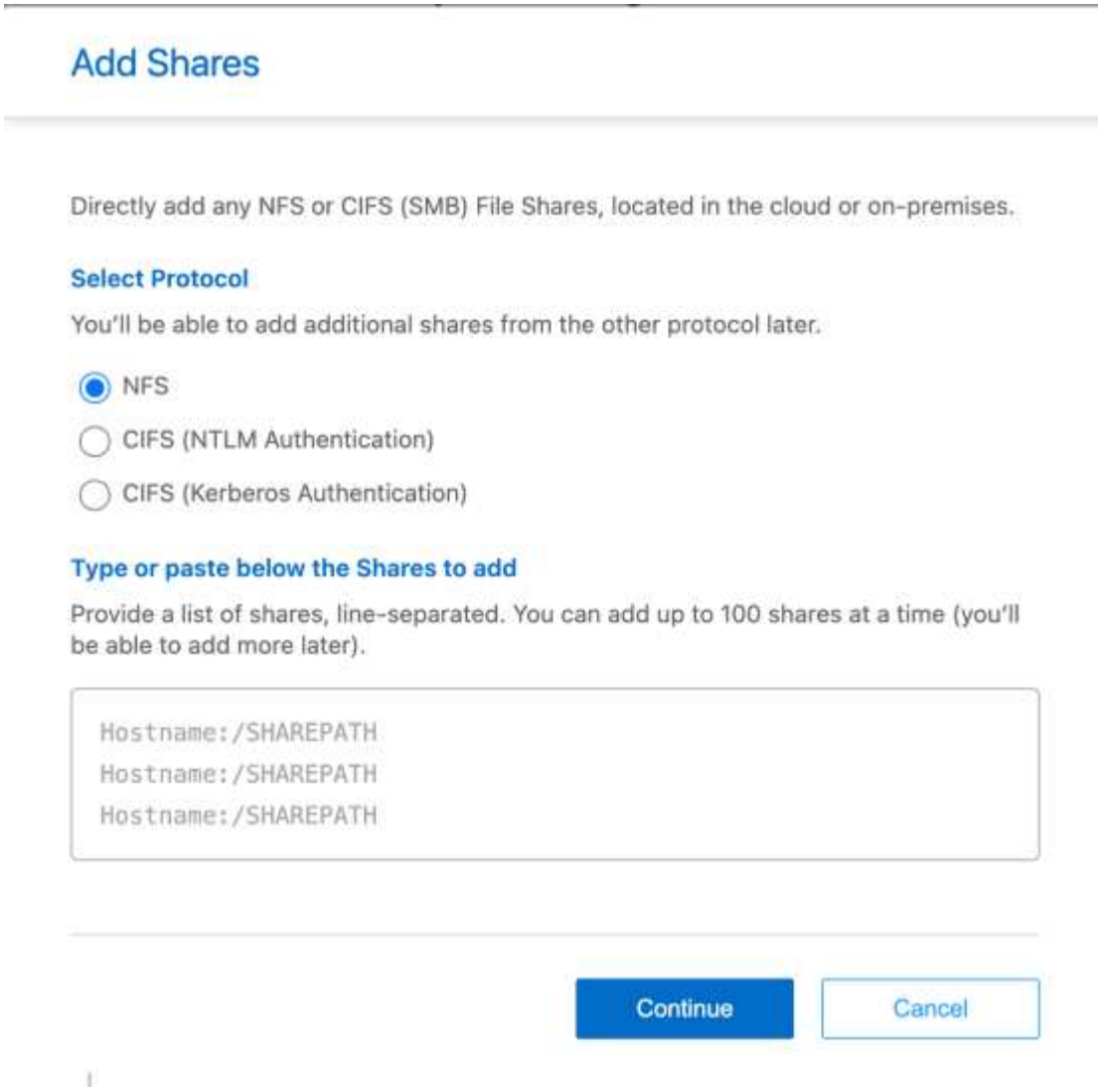
CIFS 프로토콜 구성 편집

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 수정하려는 파일 공유 그룹을 선택합니다.
3. **CIFS** 자격 증명 편집을 선택합니다.

4. 인증 방법을 선택하세요: **NTLM** 또는 **Kerberos**.
5. Active Directory 사용자 이름과 암호를 입력합니다.
6. 저장을 선택하여 프로세스를 완료하세요.

스캔에 파일 공유 추가

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 구성 페이지에서 수정하려는 파일 공유 그룹을 선택합니다.
3. **+** 공유 추가를 선택하세요.
4. 추가할 파일 공유에 대한 프로토콜을 선택하세요.



이미 구성한 프로토콜에 파일 공유를 추가하는 경우 변경할 필요가 없습니다.

두 번째 프로토콜을 사용하여 파일 공유를 추가하는 경우 다음에서 자세히 설명한 대로 인증을 올바르게 구성했는지 확인하십시오."전제 조건" .

5. 형식을 사용하여 검사하려는 파일 공유를 추가합니다(줄당 파일 공유 하나). `<host_name>:/<share_path>` .
6. 계속을 선택하여 파일 공유 추가를 완료합니다.

스캔에서 파일 공유 제거

1. 데이터 분류 메뉴에서 *구성*을 선택합니다.
2. 파일 공유를 제거할 시스템을 선택하세요.
3. *구성*을 선택하세요.
4. 구성 페이지에서 작업을 선택하세요. ••• 제거하려는 파일 공유에 대해.
5. 작업 메뉴에서 *공유 제거*를 선택합니다.

스캐닝 진행 상황을 추적하세요

초기 스캔의 진행 상황을 추적할 수 있습니다.

1. 구성 메뉴를 선택하세요.
2. 시스템 구성을 선택하세요.
3. 저장소의 경우, 검사 진행률 열을 확인하여 상태를 확인하세요.

NetApp Data Classification 사용하여 StorageGRID 데이터 스캔

NetApp Data Classification 사용하여 StorageGRID 내에서 직접 데이터 스캔을 시작하려면 몇 가지 단계를 완료하세요.

StorageGRID 요구 사항 검토

데이터 분류를 활성화하기 전에 지원되는 구성이 있는지 확인하려면 다음 필수 구성 요소를 검토하세요.

- 개체 스토리지 서비스에 연결하려면 엔드포인트 URL이 필요합니다.
- 데이터 분류가 버킷에 액세스할 수 있도록 StorageGRID 에서 액세스 키와 비밀 키가 필요합니다.

데이터 분류 인스턴스 배포

아직 배포된 인스턴스가 없으면 데이터 분류를 배포합니다.

인터넷을 통해 액세스할 수 있는 StorageGRID 의 데이터를 스캔하는 경우 다음을 수행할 수 있습니다."클라우드에 데이터 분류 배포" 또는"인터넷 접속이 가능한 온프레미스 위치에 데이터 분류를 배포합니다." .

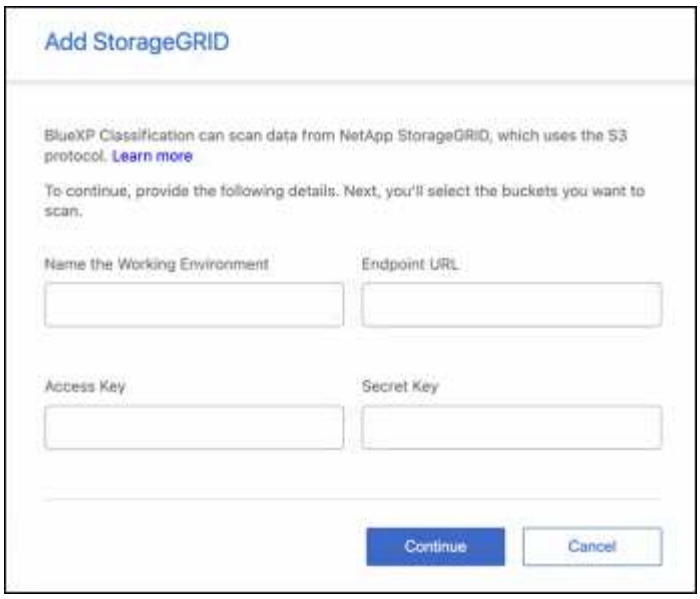
인터넷 접속이 불가능한 어두운 장소에 설치된 StorageGRID 에서 데이터를 스캔하는 경우 다음이 필요합니다."인터넷 접속이 없는 동일한 온프레미스 위치에 데이터 분류를 배포합니다." . 이를 위해서는 콘솔 에이전트가 동일한 온프레미스 위치에 배포되어야 합니다.

데이터 분류에 StorageGRID 서비스 추가

StorageGRID 서비스를 추가합니다.

단계

1. 데이터 분류 메뉴에서 구성 옵션을 선택합니다.
2. 구성 페이지에서 시스템 추가 > * StorageGRID 추가*를 선택합니다.
3. StorageGRID 서비스 추가 대화 상자에서 StorageGRID 서비스에 대한 세부 정보를 입력하고 *계속*을 선택합니다.
   a. 시스템에 사용할 이름을 입력하세요. 이 이름은 연결하려는 StorageGRID 서비스의 이름을 반영해야 합니다.
   b. 개체 스토리지 서비스에 액세스하려면 Endpoint URL을 입력하세요.
   c. Data Classification이 StorageGRID 의 버킷에 액세스할 수 있도록 액세스 키와 비밀 키를 입력하세요.



결과

StorageGRID 시스템 목록에 추가되었습니다.

StorageGRID 버킷에서 스캔 활성화 및 비활성화

StorageGRID 에서 데이터 분류를 활성화한 후 다음 단계는 스캔할 버킷을 구성하는 것입니다. 데이터 분류는 해당 버킷을 검색하여 사용자가 만든 시스템에 표시합니다.

단계

1. 구성 페이지에서 StorageGRID 시스템을 찾으세요.
2. StorageGRID 시스템 타일에서 *구성*을 선택합니다.
3. 다음 단계 중 하나를 완료하여 스캐닝을 활성화하거나 비활성화하세요.
   - 버킷에서 매핑 전용 스캔을 활성화하려면 *맵*을 선택합니다.
   - 버킷에 대한 전체 검사를 활성화하려면 *매핑 및 분류*를 선택합니다.
   - 버킷에서 스캐닝을 비활성화하려면 *끄기*를 선택하세요.

결과

데이터 분류는 활성화된 버킷을 스캔하기 시작합니다. 구성 메뉴로 이동한 다음 시스템 구성을 선택하면 초기 검사의 진행 상황을 추적할 수 있습니다. 각 스캔의 진행 상황은 진행률 표시줄로 표시됩니다. 진행률 표시줄 위에 마우스를 올려 놓으면 볼륨의 전체 파일 대비 검사된 파일 수를 확인할 수 있습니다. 오류가 있는 경우 오류는 상태 열에 표시되고 오류를 수정하는 데 필요한 작업도 함께 표시됩니다.