



Cloud Sync를 사용합니다

Cloud Sync

NetApp
May 02, 2022

목차

Cloud Sync를 사용합니다	1
소스와 타겟 간에 데이터를 동기화합니다	1
무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불합니다	19
동기화 관계 관리	21
데이터 브로커 그룹을 관리합니다	26
구성을 조정하기 위해 보고서 작성 및 보기	33
데이터 브로커를 제거하는 중입니다	36

Cloud Sync를 사용합니다

소스와 타겟 간에 데이터를 동기화합니다

동기화 관계를 생성합니다

동기화 관계를 생성하면 Cloud Sync 서비스는 소스에서 타겟으로 파일을 복사합니다. 초기 복사 후, 서비스는 24시간마다 변경된 데이터를 동기화합니다.

동기화 관계의 일부 유형을 생성하려면 먼저 Cloud Manager에서 작업 환경을 생성해야 합니다.

특정 유형의 작업 환경에 대한 동기화 관계를 생성합니다

다음 중 하나를 위한 동기화 관계를 생성하려면 먼저 작업 환경을 생성하거나 검색해야 합니다.

- ONTAP용 Amazon FSx
- Azure NetApp Files
- Cloud Volumes ONTAP
- 온프레미스 ONTAP 클러스터

단계

1. 작업 환경을 만들거나 검색합니다.
 - ["ONTAP 작업 환경을 위한 Amazon FSx를 생성합니다"](#)
 - ["Azure NetApp Files 설정 및 검색"](#)
 - ["AWS에서 Cloud Volumes ONTAP 실행"](#)
 - ["Azure에서 Cloud Volumes ONTAP 실행"](#)
 - ["Google Cloud에서 Cloud Volumes ONTAP 실행"](#)
 - ["기존 Cloud Volumes ONTAP 시스템 추가"](#)
 - ["ONTAP 클러스터 검색"](#)
2. Canvas * 를 클릭합니다.
3. 위에 나열된 유형과 일치하는 작업 환경을 선택합니다.
4. 동기화 옆에 있는 작업 메뉴를 선택합니다.



5. 이 위치에서 데이터 동기화 * 또는 * 이 위치로 데이터 동기화 * 를 선택하고 프롬프트에 따라 동기화 관계를 설정합니다.

다른 유형의 동기화 관계를 생성합니다

다음 단계를 수행하여 ONTAP, Azure NetApp Files, Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터에 대해 Amazon FSx 이외의 지원되는 스토리지 유형과 데이터를 동기화할 수 있습니다. 아래 단계에서는 NFS 서버에서 S3 버킷으로 동기화 관계를 설정하는 방법을 보여 주는 예를 제공합니다.

1. Cloud Manager에서 * Sync * 를 클릭합니다.
2. 동기화 관계 정의 * 페이지에서 소스 및 대상을 선택합니다.

다음 단계에서는 NFS 서버에서 S3 버킷으로 동기화 관계를 생성하는 방법의 예를 제공합니다.



3. NFS 서버 * 페이지에서 AWS에 동기화할 NFS 서버의 IP 주소 또는 정규화된 도메인 이름을 입력합니다.
4. Data Broker Group * 페이지에서 프롬프트에 따라 AWS, Azure 또는 Google Cloud Platform에서 데이터 브로커 가상 컴퓨터를 만들거나 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치합니다.

자세한 내용은 다음 페이지를 참조하십시오.

- ["AWS에서 데이터 브로커를 생성합니다"](#)
- ["Azure에서 데이터 브로커를 생성합니다"](#)
- ["Google Cloud에서 데이터 브로커를 생성합니다"](#)
- ["Linux 호스트에 데이터 브로커 설치"](#)

5. 데이터 브로커를 설치한 후 * 계속 * 을 클릭합니다.



6. [[FILTER](*) 디렉터리*) 페이지에서 최상위 디렉터리나 하위 디렉터를 선택합니다.

Cloud Sync에서 내보내기를 검색할 수 없는 경우 * 내보내기 수동 추가 * 를 클릭하고 NFS 내보내기 이름을 입력합니다.



NFS 서버에 둘 이상의 디렉토리를 동기화하려는 경우 작업을 완료한 후 동기화 관계를 추가로 생성해야 합니다.

7. AWS S3 버킷 * 페이지에서 버킷을 선택합니다.

- 드릴다운하여 버킷 내의 기존 폴더를 선택하거나 버킷 내에서 생성한 새 폴더를 선택합니다.
- 목록에 추가 * 를 클릭하여 AWS 계정과 연결되지 않은 S3 버킷을 선택합니다. "[S3 버킷에 특정 권한을 적용해야 합니다](#)".

8. Bucket 설정 * 페이지에서 Bucket을 설정합니다.

- S3 버킷 암호화를 사용하도록 설정한 다음 AWS KMS 키를 선택하고 KMS 키의 ARN을 입력하거나 AES-256 암호화를 선택합니다.
- S3 스토리지 클래스를 선택합니다. "[지원되는 스토리지 클래스를 봅니다](#)".



9. [[설정] * 설정 * 페이지에서 소스 파일 및 폴더가 대상 위치에서 동기화 및 유지되는 방식을 정의합니다.

스케줄

향후 동기화를 위한 반복 일정을 선택하거나 동기화 일정을 해제합니다. 1분마다 데이터를 동기화하도록 관계를 예약할 수 있습니다.

동기화 시간 초과

동기화가 지정된 시간 또는 일 수에 완료되지 않은 경우 Cloud Sync에서 데이터 동기화를 취소할지 여부를 정의합니다.

알림

클라우드 관리자의 알림 센터에서 Cloud Sync 알림을 수신할지 여부를 선택할 수 있습니다. 성공적인 데이터 동기화, 실패한 데이터 동기화 및 취소된 데이터 동기화를 위한 알림을 활성화할 수 있습니다.

다시 시도

Cloud Sync에서 파일을 건너뛰기 전에 동기화를 재시도할 횟수를 정의합니다.

비교 기준

파일 또는 디렉토리가 변경되었으며 다시 동기화되어야 하는지 여부를 결정할 때 Cloud Sync에서 특정 속성을 비교해야 하는지 여부를 선택합니다.

이 속성을 선택 취소하더라도 Cloud Sync에서는 경로, 파일 크기 및 파일 이름을 확인하여 소스를 타겟과 비교합니다. 변경 사항이 있으면 해당 파일과 디렉토리를 동기화합니다.

Cloud Sync에서 다음 특성을 비교하도록 선택하거나 사용하지 않도록 설정할 수 있습니다.

- * mtime *: 파일의 마지막 수정 시간입니다. 이 속성은 디렉토리에 대해 유효하지 않습니다.
- * uid *, * gid * 및 * 모드 *: Linux용 권한 플래그

개체 복사

오브젝트 스토리지 메타데이터 및 태그를 복사하려면 이 옵션을 활성화하십시오. 사용자가 소스의 메타데이터를 변경하면 Cloud Sync는 다음 동기화 시 이 개체를 복제하지만 사용자가 데이터 자체가 아닌 소스의 태그를 변경하면 Cloud Sync는 다음 동기화 시 개체를 복사하지 않습니다.

관계를 만든 후에는 이 옵션을 편집할 수 없습니다.

태그 복사는 S3 호환 엔드포인트(S3, StorageGRID 또는 IBM 클라우드 오브젝트 스토리지)가 포함된 동기화 관계에서 지원됩니다.

메타데이터 복사는 다음 엔드포인트 간의 '클라우드 간' 관계에서 지원됩니다.

- 설치하고
- Azure Blob
- Google 클라우드 스토리지
- IBM 클라우드 오브젝트 스토리지
- StorageGRID

최근에 수정된 파일

예약된 동기화 전에 최근에 수정된 파일을 제외하도록 선택합니다.

소스에서 파일 삭제

Cloud Sync가 파일을 타겟 위치에 복사한 후 소스 위치에서 파일을 삭제하도록 선택합니다. 이 옵션에는 원본 파일이 복사된 후 삭제되므로 데이터가 손실될 위험이 포함됩니다.

이 옵션을 활성화하면 데이터 브로커에서 local.json 파일의 매개 변수도 변경해야 합니다. 파일을 열고 다음과 같이 업데이트합니다.

```
{
  "workers": {
    "transferrer": {
      "delete-on-source": true
    }
  }
}
```

대상에서 파일 삭제

파일이 소스에서 삭제된 경우 대상 위치에서 파일을 삭제하도록 선택합니다. 기본값은 대상 위치에서 파일을 삭제하지 않는 것입니다.

파일 형식

파일, 디렉토리 및 심볼 링크 등 각 동기화에 포함할 파일 유형을 정의합니다.

파일 확장명 제외

파일 확장명을 입력하고 * Enter * 를 눌러 동기화에서 제외할 파일 확장명을 지정합니다. 예를 들어, *.log 파일을 제외하려면 _log_ 또는 .log_를 입력합니다. 여러 확장자에 대해 구분 기호가 필요하지 않습니다. 다음 비디오는 짧은 데모를 제공합니다.

▶ https://docs.netapp.com/ko-kr/cloud-manager-sync//media/video_file_extensions.mp4 (video)

파일 크기

파일 크기나 특정 크기 범위에 있는 파일에 관계없이 모든 파일을 동기화하도록 선택합니다.

수정한 날짜

마지막으로 수정한 날짜, 특정 날짜 이후 수정된 파일, 특정 날짜 이전 또는 시간 범위 사이에 관계없이 모든 파일을 선택합니다.

만든 날짜

SMB 서버가 소스인 경우 이 설정을 사용하면 특정 날짜 이후, 특정 날짜 이전 또는 특정 시간 범위 간에 생성된 파일을 동기화할 수 있습니다.

ACL - 액세스 제어 목록

SMB 서버에서 ACL 복사 - 관계를 생성할 때 또는 관계를 생성한 후에 설정을 사용합니다.

10. 태그/메타데이터 * 페이지에서 S3 버킷으로 전송된 모든 파일에 키 값 쌍을 태그로 저장할지 또는 모든 파일에 메타데이터 키 값 쌍을 할당할지 여부를 선택합니다.

Relationship Tags

Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket.

This enables you to search for the transferred files by using the tag values.

☒ Save on Object's Tags ☐ Save On Object's Metadata

Tag Key: Up to 128 characters

Tag Value: Up to 256 characters

+ Add Relationship Tag

Optional Field | [Up to 5]



StorageGRID 및 IBM 클라우드 오브젝트 스토리지로 데이터를 동기화할 때도 동일한 기능을 사용할 수 있습니다. Azure 및 Google Cloud Storage의 경우 메타데이터 옵션만 사용할 수 있습니다.

11. 동기화 관계에 대한 세부 정보를 검토한 다음 * 관계 생성 * 을 클릭합니다.

결과 *

Cloud Sync가 소스와 타겟 간의 데이터 동기화를 시작합니다.

클라우드 데이터 센스에서 동기화 관계를 생성합니다

Cloud Sync는 클라우드 데이터 센스에 통합되어 있습니다. 데이터 감지 내에서 Cloud Sync를 사용하여 타겟 위치에 동기화할 소스 파일을 선택할 수 있습니다.

Cloud Data Sense에서 데이터 동기화를 시작한 후에는 모든 소스 정보가 한 번에 포함되고 몇 가지 키 세부 정보만 입력하면 됩니다. 그런 다음 새 동기화 관계의 타겟 위치를 선택합니다.

Sync Relationship

1 Data Sense Integration 2 Data Broker Group 3 NFS Server 4 Directory

How does it work?

Selected Data Sense Source

Azure NetApp Files /cifs1 Source 1.1.1.1 Host cifs Working Environment \\1.1.1.1\\cifs1 Volume

A few more things before we continue

Define SMB Credentials:

User Name Password Domain (Optional)

"클라우드 데이터 센스에서 동기식 관계를 시작하는 방법을 알아보십시오".

SMB 공유에서 ACL 복사

Cloud Sync는 소스 SMB 공유와 타겟 SMB 공유 간에 또는 소스 SMB 공유에서 오브젝트 스토리지(ONTAP S3 제외)로 액세스 제어 목록(ACL)을 복사할 수 있습니다. 필요한 경우 Robo-Copy를 사용하여 SMB 공유 간의 ACL을 수동으로 보존할 수도 있습니다.



Cloud Sync는 오브젝트 스토리지에서 SMB 공유로 ACL을 다시 복사할 수 없습니다.

선택

- [ACL을 자동으로 복제하도록 Cloud Sync를 설정합니다](#)
- [SMB 공유 간에 ACL을 수동으로 복사합니다](#)

SMB 서버에서 ACL을 복제하도록 Cloud Sync 설정

SMB 서버에서 ACL 복사 - 관계를 생성할 때 또는 관계를 생성한 후에 설정을 사용합니다.

이 기능은 AWS, Azure, Google Cloud Platform 또는 온프레미스 데이터 브로커 등 `_any_` 유형의 데이터 브로커와 연동됩니다. 온프레미스 데이터 브로커를 실행할 수 있습니다 "[지원되는 모든 운영 체제](#)".

새로운 관계를 위한 단계

1. Cloud Sync에서 * 새 동기화 생성 * 을 클릭합니다.
2. SMB 서버 * 를 소스에 끌어다 놓고 타겟으로 SMB 서버 또는 오브젝트 스토리지를 선택한 다음 * 계속 * 을 클릭합니다.
3. SMB 서버 * 페이지에서 다음을 수행합니다.
 - a. 새 SMB 서버를 입력하거나 기존 서버를 선택하고 * 계속 * 을 클릭합니다.
 - b. SMB 서버의 자격 증명을 입력합니다.
 - c. 대상에 대한 액세스 제어 목록 복사 * 를 선택하고 * 계속 * 을 클릭합니다.

Select an SMB Source

SMB Version : 2.1 ▼



Selected SMB Server:

10.20.30.152

Define SMB Credentials:

User Name

user1

Password

Domain (Optional)

ACL - Access Control List

☒ Copy Access Control Lists to the target

Notice: Copying ACLs can affect sync performance.
You can change this setting after you create the relationship.

4. 나머지 프롬프트에 따라 동기화 관계를 생성합니다.

SMB에서 오브젝트 스토리지로 ACL을 복사할 때 대상에 따라 ACL을 오브젝트의 태그 또는 오브젝트의 메타데이터에 복사하도록 선택할 수 있습니다. Azure 및 Google Cloud Storage의 경우 메타데이터 옵션만 사용할 수 있습니다.

다음 스크린샷에서는 이 옵션을 선택할 수 있는 단계의 예를 보여 줍니다.

<
AWS S3 Bucket
Settings
6 Tags/Metadata
7 Review

Relationship Metadata

Cloud Sync assigns the relationship metadata to all of the files transferred to the S3 bucket.

☐ Save on Object's Tags
 ☒ Save On Object's Metadata

Metadata Key

Up to 128 characters

Metadata Value

Up to 256 characters

+ Add Relationship Metadata Optional Field | [Up to 5]

기존 관계에 대한 단계

1. 동기화 관계 위로 마우스를 이동하고 작업 메뉴를 클릭합니다.
2. 설정 * 을 클릭합니다.
3. 대상에 대한 액세스 제어 목록 복사 * 를 선택합니다.
4. 설정 저장 * 을 클릭합니다.

데이터를 동기화할 때 Cloud Sync는 소스 및 타겟 SMB 공유 간 또는 소스 SMB 공유에서 오브젝트 스토리지까지의 ACL을 보존합니다.

SMB 공유 간에 ACL을 수동으로 복제합니다

Windows Robo-copy 명령을 사용하여 SMB 공유 간의 ACL을 수동으로 보존할 수 있습니다.

단계

1. 두 SMB 공유에 대한 모든 액세스 권한이 있는 Windows 호스트를 식별합니다.
2. 두 끝점 중 하나에 인증이 필요한 경우 * net use * 명령을 사용하여 Windows 호스트의 끝점에 연결합니다.

로봇 복사를 사용하기 전에 이 단계를 수행해야 합니다.

3. Cloud Sync에서 소스 및 타겟 SMB 공유 간에 새 관계를 생성하거나 기존 관계를 동기화합니다.
4. 데이터 동기화가 완료되면 Windows 호스트에서 다음 명령을 실행하여 ACL 및 소유권을 동기화합니다.

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots  
/UNILOG:"[logfilepath]
```

UNC 형식을 사용하여 _source_와 _target_을 모두 지정해야 합니다. 예: \\<server>\<share>\<path>

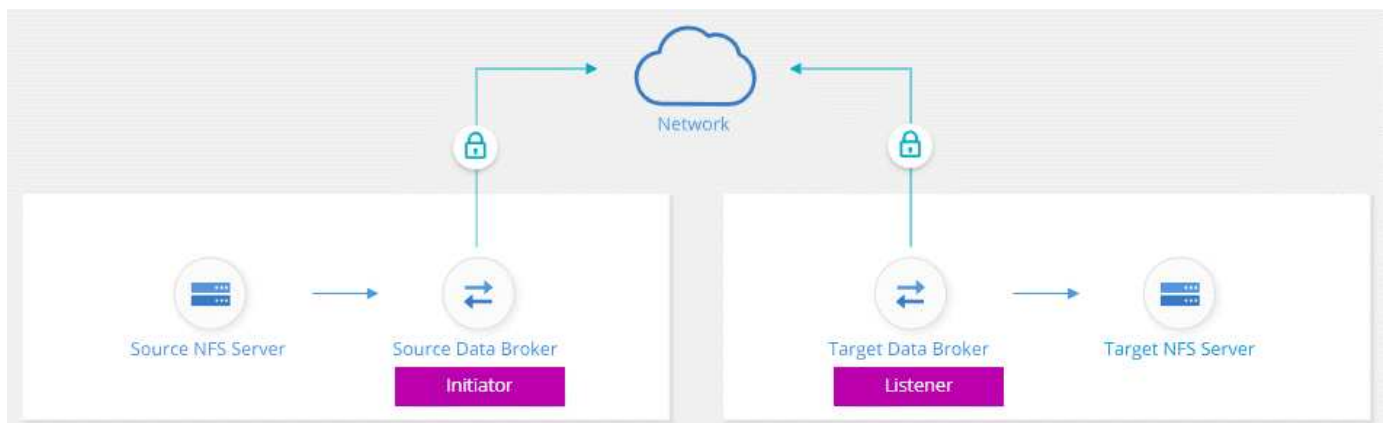
전송 중 데이터 암호화를 사용하여 NFS 데이터 동기화

회사에 엄격한 보안 정책이 있는 경우 전송 중인 데이터 암호화를 사용하여 NFS 데이터를 동기화할 수 있습니다. 이 기능은 NFS 서버에서 다른 NFS 서버로, Azure NetApp Files에서 Azure NetApp Files로 지원됩니다.

예를 들어, 서로 다른 네트워크에 있는 두 NFS 서버 간에 데이터를 동기화할 수 있습니다. 또는 서브넷 또는 영역 간에 Azure NetApp Files의 데이터를 안전하게 전송해야 할 수 있습니다.

전송 중 데이터 암호화 작동 방식

전송 중인 데이터 암호화는 두 데이터 브로커 간에 네트워크를 통해 전송되는 NFS 데이터를 암호화합니다. 다음 이미지는 두 NFS 서버와 두 데이터 브로커 간의 관계를 보여 줍니다.



하나의 데이터 브로커가 _initiator_로 작동합니다. 데이터를 동기화할 시간이 되면 다른 데이터 브로커, 즉 _listener_로

연결 요청을 보냅니다. 이 데이터 브로커는 포트 443에서 요청을 수신합니다. 필요한 경우 다른 포트를 사용할 수 있지만 포트가 다른 서비스에서 사용되고 있지 않은지 확인해야 합니다.

예를 들어, 온프레미스 NFS 서버의 데이터를 클라우드 기반 NFS 서버로 동기화하는 경우 연결 요청을 수신 대기하는 데이터 브로커를 선택할 수 있습니다.

전송 중 암호화 방식은 다음과 같습니다.

1. 동기화 관계를 생성한 후 이니시에이터는 다른 데이터 브로커와 암호화된 연결을 시작합니다.
2. 소스 데이터 브로커는 TLS 1.3을 사용하여 소스에서 데이터를 암호화합니다.
3. 그런 다음 데이터를 네트워크를 통해 타겟 데이터 브로커로 전송합니다.
4. 대상 데이터 브로커는 데이터를 타겟으로 전송하기 전에 해독합니다.
5. 초기 복사 후, 서비스는 24시간마다 변경된 데이터를 동기화합니다. 동기화할 데이터가 있는 경우 이니시에이터에서 다른 데이터 브로커와 암호화된 연결을 여는 것으로 프로세스가 시작됩니다.

데이터를 더 자주 동기화하려는 경우 ["관계를 만든 후에는 일정을 변경할 수 있습니다"](#).

지원되는 **NFS** 버전입니다

- NFS 서버의 경우 NFS 버전 3, 4.0, 4.1 및 4.2에서 전송 중인 데이터 암호화가 지원됩니다.
- Azure NetApp Files의 경우, NFS 버전 3 및 4.1에서 전송 중인 데이터 암호화가 지원됩니다.

프록시 서버 제한

암호화된 동기화 관계를 만들면 암호화된 데이터가 HTTPS를 통해 전송되며 프록시 서버를 통해 라우팅할 수 없습니다.

시작하는 데 필요한 사항

다음 사항을 확인하십시오.

- 충족하는 NFS 서버 2대 ["소스 및 타겟 요구 사항"](#) 또는 두 개의 서브넷 또는 영역의 Azure NetApp Files.
- 서버의 IP 주소 또는 정규화된 도메인 이름입니다.
- 2개의 데이터 브로커를 위한 네트워크 위치.

기존 데이터 브로커를 선택할 수 있지만 이니시에이터로 작동해야 합니다. 수신기 데이터 브로커는 `_new_data` 브로커여야 합니다.

기존 데이터 브로커 그룹을 사용하려면 그룹에 데이터 브로커가 하나만 있어야 합니다. 암호화된 동기화 관계를 사용하면 한 그룹의 여러 데이터 브로커가 지원되지 않습니다.

데이터 브로커를 아직 구축하지 않은 경우 데이터 브로커 요구사항을 검토하십시오. 엄격한 보안 정책이 있으므로 포트 443과 의 아웃바운드 트래픽을 포함하는 네트워킹 요구 사항을 검토하십시오 ["인터넷 엔드포인트"](#) 데이터 브로커가 연결합니다.

- ["AWS 설치를 검토합니다"](#)
- ["Azure 설치를 검토합니다"](#)
- ["Google Cloud 설치를 검토합니다"](#)

◦ "Linux 호스트 설치를 검토합니다"

전송 중 데이터 암호화를 사용하여 **NFS** 데이터 동기화

두 NFS 서버 간 또는 Azure NetApp Files 간에 새 동기화 관계를 생성하고 전송 중 암호화 옵션을 설정한 다음 화면의 지시를 따릅니다.

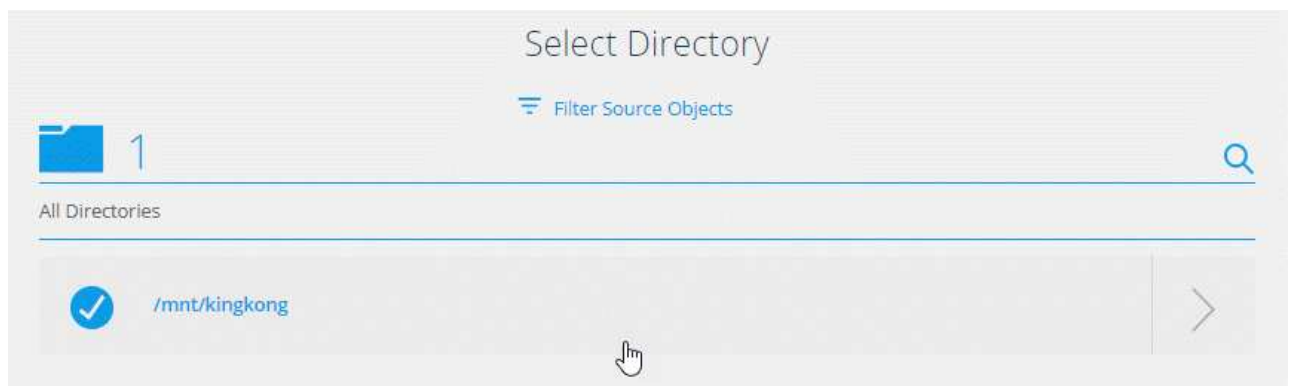
단계

1. 새 동기화 만들기 * 를 클릭합니다.
2. 소스 및 타겟 위치로 * NFS 서버 * 를 끌어다 놓거나 * Azure NetApp Files * 를 소스 및 타겟 위치로 끈 후 * 예 * 를 선택하여 전송 중인 데이터 암호화를 활성화합니다.
3. 프롬프트에 따라 관계를 생성합니다.
 - a. * NFS Server * / * Azure NetApp Files *: NFS 버전을 선택한 다음 새 NFS 소스를 지정하거나 기존 서버를 선택합니다.
 - b. * 데이터 브로커 기능 정의 *: 포트에서 연결 요청을 처리하는 데이터 브로커_listen_과 연결을 시작하는 데이터 브로커를 정의합니다. 네트워킹 요구 사항에 따라 선택할 수 있습니다.
 - c. * Data Broker *: 프롬프트에 따라 새 소스 데이터 브로커를 추가하거나 기존 데이터 브로커를 선택합니다.

다음 사항에 유의하십시오.

- 기존 데이터 브로커 그룹을 사용하려면 그룹에 데이터 브로커가 하나만 있어야 합니다. 암호화된 동기화 관계를 사용하면 한 그룹의 여러 데이터 브로커가 지원되지 않습니다.
 - 소스 데이터 브로커가 수신기 역할을 하는 경우 새로운 데이터 브로커가 되어야 합니다.
 - 새 데이터 브로커가 필요한 경우 Cloud Sync에 설치 지침이 표시됩니다. 클라우드에 데이터 브로커를 구축하거나 자체 Linux 호스트에 대한 설치 스크립트를 다운로드할 수 있습니다.
- d. * 디렉터리 *: 모든 디렉터리를 선택하거나 드릴다운 및 하위 디렉터리를 선택하여 동기화할 디렉터리를 선택합니다.

소스 파일 및 폴더가 대상 위치에서 동기화 및 유지 관리되는 방식을 정의하는 설정을 수정하려면 * 소스 개체 필터 * 를 클릭합니다.



- e. * 타겟 NFS 서버 * / * 타겟 Azure NetApp Files *: NFS 버전을 선택한 다음 새 NFS 타겟을 입력하거나 기존 서버를 선택합니다.
- f. * 대상 데이터 브로커 *: 프롬프트에 따라 새 소스 데이터 브로커를 추가하거나 기존 데이터 브로커를 선택합니다.

대상 데이터 브로커가 수신기 역할을 하는 경우 새 데이터 브로커가 되어야 합니다.

다음은 대상 데이터 브로커가 수신기로 작동할 때의 프롬프트의 예입니다. 포트를 지정하는 옵션을 확인합니다.

- a. * 대상 디렉터리 *: 최상위 디렉터리를 선택하거나 드릴다운하여 기존 하위 디렉터리를 선택하거나 내보내기 내에 새 폴더를 만듭니다.
- b. * 설정 *: 원본 파일과 폴더가 대상 위치에서 동기화 및 유지되는 방식을 정의합니다.
- c. * 검토 *: 동기화 관계의 세부 정보를 검토한 다음 * 관계 생성 * 을 클릭합니다.



Cloud Sync에서 새 동기화 관계 생성을 시작합니다. 완료되면 * Dashboard * 에서 View를 클릭하여 새 관계에 대한 세부 정보를 봅니다.

외부 HashCorp Vault를 사용하도록 데이터 브로커 그룹을 설정합니다

Amazon S3, Azure 또는 Google Cloud 자격 증명이 필요한 동기화 관계를 생성하는 경우 Cloud Sync 사용자 인터페이스 또는 API를 통해 이러한 자격 증명을 지정해야 합니다. 또는 데이터 브로커 그룹을 설정하여 외부 HashCorp 볼트에서 직접 자격 증명(또는 비밀)에 액세스할 수도 있습니다.

이 기능은 Amazon S3, Azure 또는 Google Cloud 자격 증명이 필요한 동기화 관계가 있는 Cloud Sync API를 통해 지원됩니다.

URL을 설정하여 데이터 브로커 그룹에 자격 증명을 제공할 볼트를 준비합니다. 볼트의 비밀에 대한 URL은 `_creds_`로 끝나야 합니다.

그룹의 각 데이터 브로커에 대한 로컬 구성 파일을 수정하여 외부 볼트에서 자격 증명을 가져오도록 데이터 브로커 그룹을 준비합니다.

이제 모든 것이 설정되었으므로 API 호출을 전송하여 볼트를 사용하는 동기화 관계를 만들어 비밀을 가져올 수 있습니다.

볼트 준비 중

볼트의 비밀에 대한 URL을 Cloud Sync에 제공해야 합니다. 이러한 URL을 설정하여 볼트를 준비합니다. 만들려는 동기화 관계의 각 소스 및 타겟의 자격 증명에 대한 URL을 설정해야 합니다.

URL은 다음과 같이 설정해야 합니다.

`'/<path>/<requested>/<endpoint-protocol>creds'`

경로

비밀에 대한 접두사 경로입니다. 이는 귀하에게 고유한 모든 가치가 될 수 있습니다.

요청 ID입니다

생성해야 하는 요청 ID입니다. 동기화 관계를 생성할 때 API POST 요청의 헤더 중 하나에 ID를 제공해야 합니다.

엔드포인트 프로토콜

정의된 대로 다음 프로토콜 중 하나입니다 "[사후 관계 v2 문서에서](#)" S3, Azure 또는 GCP(각각 대문자여야 함).

크레드

URL은 `_creds_`로 끝나야 합니다.

예

다음 예제에서는 비밀에 대한 URL을 보여 줍니다.

소스 자격 증명의 전체 URL 및 경로 예

<http://example.vault.com:8200/my-path/all-secrets/hb312vdsr2/S3Creds> 으로 문의하십시오

예제에서 볼 수 있듯이 접두사 경로는 `_my-path/all-sids/_`이고 요청 ID는 `_hb312vdsr2_`이며 소스 끝점은 S3입니다.

대상 자격 증명의 전체 **URL** 및 경로 예

<http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds> 으로 문의하십시오

접두사 경로는 `_/my-path/all-sats/_`이고, 요청 ID는 `_n32hcbnejk2_`이며, 대상 끝점은 Azure입니다.

데이터 브로커 그룹을 준비하는 중입니다

그룹의 각 데이터 브로커에 대한 로컬 구성 파일을 수정하여 외부 볼트에서 자격 증명을 가져오도록 데이터 브로커 그룹을 준비합니다.

단계

1. 그룹의 데이터 브로커에 SSH를 연결합니다.
2. `/opt/netapp/databroker/config`에 있는 `local.json` 파일을 편집합니다.
3. `enable`을 `* true *`로 설정하고 다음과 같이 `_external-통합.hashicorp_`에서 `config` 매개 변수 필드를 설정합니다.

활성화됨

- 유효한 값: TRUE/FALSE
- Type:Boolean 을 입력합니다
- 기본값: false
- 참: 데이터 브로커는 외부의 HashashCorp Vault에서 비밀을 얻습니다
- 거짓: 데이터 브로커는 로컬 볼트에 자격 증명을 저장합니다

URL

- 유형: string
- 값: 외부 볼트의 URL

경로

- 유형: string
- 값: 자격 증명을 사용하여 비밀번호에 대한 접두사 경로입니다

거부 - 승인되지 않음

- 데이터 브로커가 승인되지 않은 외부 볼트를 거부하도록 할지 여부를 결정합니다
- Type:Boolean 을 입력합니다
- 기본값: false

인증 방법

- 데이터 브로커가 외부 볼트에서 자격 증명에 액세스하기 위해 사용해야 하는 인증 방법입니다
- 유형: string
- 유효한 값: "AWS-IAM"/"ROLE-APP"/"GCP-IAM"

역할 이름

- 유형: string
- 역할 이름(AWS-IAM 또는 GCP-IAM을 사용하는 경우)

정전동맥(&R)

- 유형: 문자열(APP-ROLE 사용 시)

네임스페이스

- 유형: string
- 네임스페이스(필요한 경우 X-Vault-Namespace 헤더)

4. 그룹의 다른 데이터 브로커에 대해 이 단계를 반복합니다.

AWS 역할 인증의 예

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "https://example.vault.com:8200",
      "path": "my-path/all-secrets",
      "reject-unauthorized": false,
      "auth-method": "aws-role",
      "aws-role": {
        "role-name": "my-role"
      }
    }
  }
}
```

GCP-IAM 인증의 예

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "http://ip-10-20-30-55.ec2.internal:8200",
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
      "gcp-iam": {
        "role-name": "my-iam-role"
      }
    }
  }
}
```

GCP-IAM 인증 사용 시 권한 설정

_GCP-IAM_인증 방법을 사용하는 경우 데이터 브로커에 다음과 같은 GCP 권한이 있어야 합니다.

```
- iam.serviceAccounts.signJwt
```

"데이터 브로커의 GCP 권한 요구 사항에 대해 자세히 알아보십시오".

볼트의 비밀을 사용하여 새 동기화 관계를 작성합니다

이제 모든 것이 설정되었으므로 API 호출을 전송하여 볼트를 사용하는 동기화 관계를 만들어 비밀을 가져올 수 있습니다.

Cloud Sync REST API를 사용하여 관계를 게시합니다.

Headers:

Authorization: Bearer <user-token>

Content-Type: application/json

x-account-id: <accountid>

x-netapp-external-request-id-src: request ID as part of path for source credentials

x-netapp-external-request-id-trg: request ID as part of path for target credentials

Body: post relationship v2 body

- 사용자 토큰 및 Cloud Central 계정 ID를 얻으려면 ["설명서의 이 페이지를 참조하십시오"](#).
- 사후 관계를 위한 본문을 구축하려면 ["관계 - v2 API 호출을 참조하십시오"](#).

예

POST 요청의 예:

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik..."
Body:
{
  "dataBrokerId": "5e6e111d578dtyuu1555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    }
  },
  "target": {
    "protocol": "s3",
    "s3": {
      "bucket": "my-target-bucket"
    }
  }
}
```

무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불합니다

14일 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불할 수 있는 두 가지 방법이 있습니다. 첫 번째 옵션은 AWS 또는 Azure에서 용량제 또는 연간 결제를 구독하는 것입니다. 두 번째 옵션은 NetApp에서 직접 라이선스를 구매하는 것입니다.

AWS Marketplace 또는 Azure Marketplace에서 구독할 수 있습니다. 두 경우 모두 구독할 수 없습니다.

Marketplace 구독에서 NetApp의 라이선스를 사용할 수 있습니다. 예를 들어, 동기화 관계가 25개 있는 경우 라이선스를 사용하여 처음 20개 동기화 관계에 대한 비용을 지불하고 나머지 5개 동기화 관계를 사용하여 AWS 또는 Azure에서 사용한 만큼만 비용을 지불할 수 있습니다.

["라이선스 작동 방식에 대해 자세히 알아보십시오."](#)

무료 평가판이 끝난 후 즉시 결제하지 않으면 어떻게 합니까?

추가 관계를 만들 수 없습니다. 기존 관계는 삭제되지 않지만 라이선스를 구독하거나 입력할 때까지 관계를 변경할 수 없습니다.

AWS 구독

AWS를 사용하면 사용한 만큼만 지불하거나 연간 단위로 비용을 지불할 수 있습니다.

선불 종량제 단계

1. 동기화 > 라이선스 * 를 클릭합니다.
2. AWS * 를 선택합니다
3. 구독 * 을 클릭한 다음 * 계속 * 을 클릭합니다.
4. AWS Marketplace에서 구독한 다음 Cloud Sync 서비스에 다시 로그인하여 등록을 완료합니다.

다음 비디오는 프로세스를 보여 줍니다.

▶ https://docs.netapp.com/ko-kr/cloud-manager-sync//media/video_cloud_sync_registering.mp4 (video)

연간 지불 절차

1. ["AWS 마켓플레이스 페이지로 이동합니다"](#).
2. 구독 * 으로 계속 * 을 클릭합니다.
3. 계약 옵션을 선택하고 * 계약 작성 * 을 클릭합니다.

Azure에서 구독

Azure를 사용하면 사용한 만큼만 지불하거나 연간 단위로 비용을 지불할 수 있습니다.

관련 구독에 참가자 또는 소유자 권한이 있는 Azure 사용자 계정입니다.

단계

1. 동기화 > 라이선스 * 를 클릭합니다.

2. Azure * 를 선택합니다.
3. 구독 * 을 클릭한 다음 * 계속 * 을 클릭합니다.
4. Azure 포털에서 * 생성 * 을 클릭하고 옵션을 선택한 다음 * 구독 * 을 클릭합니다.

월간 * 을 선택하여 시간당 결제하거나, * Yearly * 를 선택하여 1년 단위로 선불로 결제합니다.

5. 배포가 완료되면 알림 팝업에서 SaaS 리소스의 이름을 클릭합니다.
6. Cloud Sync로 돌아가려면 * 계정 구성 * 을 클릭합니다.

다음 비디오는 프로세스를 보여 줍니다.

▶ https://docs.netapp.com/ko-kr/cloud-manager-sync//media/video_cloud_sync_registering_azure.mp4

(video)

NetApp에서 라이선스를 구매하여 Cloud Sync에 추가

동기화 관계를 사전에 결제하려면 하나 이상의 라이선스를 구입하여 Cloud Sync 서비스에 추가해야 합니다.

라이선스에 대한 일련 번호 및 라이선스가 연결된 NetApp Support 사이트 계정의 사용자 이름과 암호가 필요합니다.

단계

1. 라이선스를 [NetApp 문의](#)까지 구입하십시오.
2. Cloud Manager에서 * 동기화 > 라이선스 * 를 클릭합니다.
3. 라이선스 추가 * 를 클릭하고 필요한 정보를 추가합니다.
 - a. 일련 번호를 입력합니다.
 - b. 추가하는 라이선스와 연관된 NetApp Support 사이트 계정을 선택합니다.
 - 계정이 이미 Cloud Manager에 추가된 경우 드롭다운 목록에서 해당 계정을 선택합니다.
 - 계정이 아직 추가되지 않은 경우 * NSS 자격 증명 추가 * 를 클릭하고 사용자 이름 및 암호를 입력한 다음 * 등록 * 을 클릭하고 드롭다운 목록에서 선택합니다.
 - c. 추가 * 를 클릭합니다.

라이선스를 업데이트하는 중입니다

NetApp에서 구매한 Cloud Sync 라이선스를 연장한 경우, 새 만료 날짜는 Cloud Sync에서 자동으로 업데이트되지 않습니다. 만료 날짜를 새로 고치려면 라이선스를 다시 추가해야 합니다.

단계

1. Cloud Manager에서 * 동기화 > 라이선스 * 를 클릭합니다.
2. 라이선스 추가 * 를 클릭하고 필요한 정보를 추가합니다.
 - a. 일련 번호를 입력합니다.
 - b. 추가하고 있는 라이선스와 관련된 NetApp Support 사이트 계정을 선택합니다.
 - c. 추가 * 를 클릭합니다.

Cloud Sync는 기존 라이선스를 새 만료일로 업데이트합니다.


동기화 관계 관리

데이터를 즉시 동기화하고 일정을 변경하는 등 동기화 관계를 언제든지 관리할 수 있습니다.

즉각적인 데이터 동기화 수행

예약된 다음 동기화를 기다리지 않고 버튼을 눌러 소스와 타겟 간에 데이터를 즉시 동기화할 수 있습니다.

단계

1. Dashboard * 에서 동기화 관계로 이동하고  를 클릭합니다

2. 지금 동기화 * 를 클릭한 다음 * 동기화 * 를 클릭하여 확인합니다.

Cloud Sync는 관계에 대한 데이터 동기화 프로세스를 시작합니다.

동기화 성능을 가속화합니다

관계를 관리하는 그룹에 추가 데이터 브로커를 추가하여 동기화 관계의 성능을 가속화합니다. 추가 데이터 브로커는 _new_data 브로커여야 합니다.


데이터 브로커 그룹이 다른 동기화 관계를 관리하는 경우 그룹에 추가한 새 데이터 브로커가 동기화 관계의 성능을 가속화합니다.

예를 들어, 다음과 같은 세 가지 관계가 있다고 가정해 보겠습니다.

- 관계 1은 데이터 브로커 그룹 A에서 관리합니다
- 관계 2는 데이터 브로커 그룹 B에 의해 관리됩니다
- 관계 3은 데이터 브로커 그룹 A에서 관리합니다

관계 1의 성능을 가속화하여 데이터 브로커 그룹 A에 새로운 데이터 브로커를 추가하고 싶을 것입니다 그룹 A도 동기화 관계 3을 관리하므로 관계의 동기화 성능도 자동으로 빨라집니다.

단계

1. 관계에 있는 기존 데이터 브로커 중 하나 이상이 온라인 상태인지 확인합니다.
2. Dashboard * 에서 동기화 관계로 이동하고 를 클릭합니다 
3. Accelerate * 를 클릭합니다.
4. 프롬프트에 따라 새 데이터 브로커를 생성합니다.

Cloud Sync는 새 데이터 브로커를 그룹에 추가합니다. 다음 데이터 동기화의 성능을 가속해야 합니다.

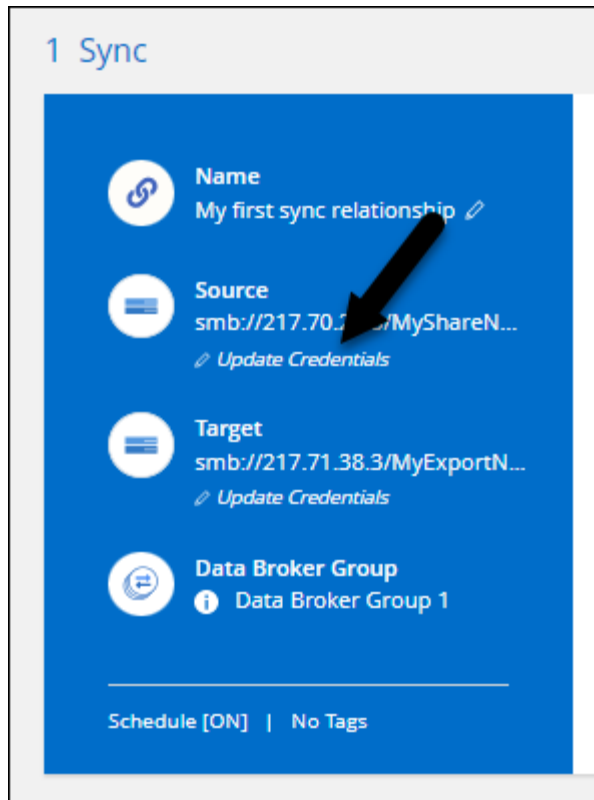
자격 증명을 업데이트하는 중입니다

기존 동기화 관계에서 소스 또는 타겟의 최신 자격 증명으로 데이터 브로커를 업데이트할 수 있습니다. 보안 정책에 따라 자격 증명을 정기적으로 업데이트해야 하는 경우 자격 증명을 업데이트하는 것이 도움이 될 수 있습니다.

Cloud Sync에서 Azure Blob, Box, IBM Cloud Object Storage, StorageGRID, ONTAP S3 Storage, SFTP 및 SMB 서버에 대한 자격 증명에 필요한 소스 또는 대상에서 자격 증명 업데이트가 지원됩니다.

단계

1. 동기화 대시보드 * 에서 자격 증명에 필요한 동기화 관계로 이동한 다음 * 자격 증명 업데이트 * 를 클릭합니다.



2. 자격 증명을 입력하고 * 업데이트 * 를 클릭합니다.

SMB 서버에 대한 참고 사항: 도메인이 새로운 경우 자격 증명을 업데이트할 때 지정해야 합니다. 도메인이 변경되지 않은 경우 다시 입력할 필요가 없습니다.

동기화 관계를 만들 때 도메인을 입력했지만 자격 증명을 업데이트할 때 새 도메인을 입력하지 않은 경우 Cloud Sync는 사용자가 제공한 원래 도메인을 계속 사용합니다.

Cloud Sync는 데이터 브로커에서 자격 증명을 업데이트합니다. 데이터 브로커가 데이터 동기화를 위해 업데이트된 자격 증명을 사용하기 전까지 10분 정도 걸릴 수 있습니다.

동기화 관계에 대한 설정을 변경합니다

원본 파일 및 폴더가 대상 위치에서 동기화 및 유지되는 방식을 정의하는 설정을 수정합니다.

1. Dashboard * 에서 동기화 관계로 이동하고 를 클릭합니다
2. 설정 * 을 클릭합니다.
3. 설정을 수정합니다.

General

Schedule

ON | Every 1 Day

Retries

Retry 3 times before skipping file

Files and Directories

Compare By

The following attributes (and size): uid, gid, mode, mtime

Recently Modified Files

Exclude files that are modified up to 30 Seconds before a scheduled sync

Delete Files On Source

Never delete files from the source location

Delete Files On Target

Never delete files from the target location

File Types

Include All: Files, Directories, Symbolic Links

Exclude File Extensions

None

File Size

All

Date Modified

All

Date Created

All

ACL - Access Control List

Inactive

Reset to defaults

다음은 각 설정에 대한 간단한 설명입니다.

스케줄

향후 동기화를 위한 반복 일정을 선택하거나 동기화 일정을 해제합니다. 1분마다 데이터를 동기화하도록 관계를 예약할 수 있습니다.

동기화 시간 초과

동기화가 지정된 시간 또는 일 수에 완료되지 않은 경우 Cloud Sync에서 데이터 동기화를 취소할지 여부를 정의합니다.

알림

클라우드 관리자의 알림 센터에서 Cloud Sync 알림을 수신할지 여부를 선택할 수 있습니다. 성공적인 데이터

동기화, 실패한 데이터 동기화 및 취소된 데이터 동기화를 위한 알림을 활성화할 수 있습니다.

다시 시도

Cloud Sync에서 파일을 건너뛰기 전에 동기화를 재시도할 횟수를 정의합니다.

비교 기준

파일 또는 디렉토리가 변경되었으며 다시 동기화되어야 하는지 여부를 결정할 때 Cloud Sync에서 특정 속성을 비교해야 하는지 여부를 선택합니다.

이 속성을 선택 취소하더라도 Cloud Sync에서는 경로, 파일 크기 및 파일 이름을 확인하여 소스를 타겟과 비교합니다. 변경 사항이 있으면 해당 파일과 디렉토리를 동기화합니다.

Cloud Sync에서 다음 특성을 비교하도록 선택하거나 사용하지 않도록 설정할 수 있습니다.

- * mtime *: 파일의 마지막 수정 시간입니다. 이 속성은 디렉토리에 대해 유효하지 않습니다.
- * uid *, * gid * 및 * 모드 *: Linux용 권한 플래그

개체 복사

관계를 만든 후에는 이 옵션을 편집할 수 없습니다.

최근에 수정된 파일

예약된 동기화 전에 최근에 수정된 파일을 제외하도록 선택합니다.

소스에서 파일 삭제

Cloud Sync가 파일을 타겟 위치에 복사한 후 소스 위치에서 파일을 삭제하도록 선택합니다. 이 옵션에는 원본 파일이 복사된 후 삭제되므로 데이터가 손실될 위험이 포함됩니다.

이 옵션을 활성화하면 데이터 브로커에서 local.json 파일의 매개 변수도 변경해야 합니다. 파일을 열고 다음과 같이 업데이트합니다.

```
{
  "workers":{
    "transferrer":{
      "delete-on-source": true
    }
  }
}
```

대상에서 파일 삭제

파일이 소스에서 삭제된 경우 대상 위치에서 파일을 삭제하도록 선택합니다. 기본값은 대상 위치에서 파일을 삭제하지 않는 것입니다.

파일 형식

파일, 디렉토리 및 심볼 링크 등 각 동기화에 포함할 파일 유형을 정의합니다.

파일 확장명 제외

파일 확장명을 입력하고 * Enter * 를 눌러 동기화에서 제외할 파일 확장명을 지정합니다. 예를 들어, *.log

파일을 제외하려면 `_log_` 또는 `_.log_`를 입력합니다. 여러 확장자에 대해 구분 기호가 필요하지 않습니다. 다음 비디오는 짧은 데모를 제공합니다.

▶ https://docs.netapp.com/ko-kr/cloud-manager-sync//media/video_file_extensions.mp4 (video)

파일 크기

파일 크기나 특정 크기 범위에 있는 파일에 관계없이 모든 파일을 동기화하도록 선택합니다.

수정한 날짜

마지막으로 수정한 날짜, 특정 날짜 이후 수정된 파일, 특정 날짜 이전 또는 시간 범위 사이에 관계없이 모든 파일을 선택합니다.

만든 날짜

SMB 서버가 소스인 경우 이 설정을 사용하면 특정 날짜 이후, 특정 날짜 이전 또는 특정 시간 범위 간에 생성된 파일을 동기화할 수 있습니다.

ACL - 액세스 제어 목록

SMB 서버에서 ACL 복사 - 관계를 생성할 때 또는 관계를 생성한 후에 설정을 사용합니다.


4. 설정 저장 * 을 클릭합니다.

Cloud Sync는 새 설정과 동기화 관계를 수정합니다.

관계를 삭제하는 중입니다

소스와 타겟 간에 데이터를 더 이상 동기화할 필요가 없는 경우 동기화 관계를 삭제할 수 있습니다. 이 작업으로 데이터 브로커 그룹(또는 개별 데이터 브로커 인스턴스)은 삭제되지 않으며, 대상에서 데이터가 삭제되지 않습니다.

단계

1. Dashboard * 에서 동기화 관계로 이동하고  를 클릭합니다
2. 삭제 * 를 클릭한 다음 * 삭제 * 를 다시 클릭하여 확인합니다.

Cloud Sync 동기화 관계를 삭제합니다.

데이터 브로커 그룹을 관리합니다

데이터 브로커 그룹은 소스 위치의 데이터를 타겟 위치로 동기화합니다. 생성하는 각 동기화 관계에 대해 그룹에 하나 이상의 데이터 브로커가 필요합니다. 그룹에 새 데이터 브로커를 추가하거나, 그룹에 대한 정보를 보는 등 데이터 브로커 그룹을 관리할 수 있습니다.

데이터 브로커 그룹의 작동 방식

데이터 브로커 그룹에는 하나 이상의 데이터 브로커가 포함될 수 있습니다. 데이터 브로커를 함께 그룹화하면 동기화 관계의 성능을 향상시킬 수 있습니다.

그룹은 여러 관계를 관리할 수 있습니다

데이터 브로커 그룹은 한 번에 하나 이상의 동기화 관계를 관리할 수 있습니다.

예를 들어, 다음과 같은 세 가지 관계가 있다고 가정해 보겠습니다.

- 관계 1은 데이터 브로커 그룹 A에서 관리합니다
- 관계 2는 데이터 브로커 그룹 B에 의해 관리됩니다
- 관계 3은 데이터 브로커 그룹 A에서 관리합니다

관계 1의 성능을 가속화하여 데이터 브로커 그룹 A에 새로운 데이터 브로커를 추가하고 싶을 것입니다 그룹 A도 동기화 관계 3 을 관리하므로 관계의 동기화 성능도 자동으로 빨라집니다.

그룹의 데이터 브로커 수입니다

대부분의 경우 단일 데이터 브로커가 동기화 관계에 대한 성능 요구사항을 충족할 수 있습니다. 그렇지 않으면 그룹에 추가 데이터 브로커를 추가하여 동기화 성능을 가속화할 수 있습니다. 하지만 먼저 동기화 성능에 영향을 줄 수 있는 다른 요소를 확인해야 합니다. ["여러 데이터 브로커가 필요한 시기를 결정하는 방법에 대해 자세히 알아보십시오"](#).

보안 권장 사항

데이터 브로커 시스템의 보안을 유지하려면 다음 사항을 따르는 것이 좋습니다.

- SSH는 X11 전달을 허용하지 않아야 합니다
- SSH는 TCP 연결 전달을 허용하지 않아야 합니다
- SSH는 터널을 허용하지 않아야 합니다
- SSH는 클라이언트 환경 변수를 수용해서는 안 됩니다

이러한 보안 권장 사항은 데이터 브로커 시스템에 대한 무단 연결을 방지하는 데 도움이 될 수 있습니다.

그룹에 새 데이터 브로커를 추가합니다

다음과 같은 여러 가지 방법으로 새 데이터 브로커를 생성할 수 있습니다.

- 새 동기화 관계를 생성할 때

["동기화 관계를 생성할 때 새 데이터 브로커를 생성하는 방법에 대해 알아보십시오"](#).

- 새 그룹에서 데이터 브로커를 만드는 * 새 데이터 브로커 추가 * 를 클릭하여 * 데이터 브로커 관리 * 페이지에서
- 기존 그룹에 새 데이터 브로커를 생성하여 * 데이터 브로커 관리 * 페이지에서

시작하기 전에

- 암호화된 동기화 관계를 관리하는 그룹에 데이터 브로커를 추가할 수 없습니다.
- 기존 그룹에서 데이터 브로커를 생성하려면 데이터 브로커가 사내 데이터 브로커이거나 동일한 유형의 데이터 브로커가 되어야 합니다.

예를 들어, 그룹에 AWS 데이터 브로커가 포함된 경우 해당 그룹에 AWS 데이터 브로커나 온프레미스 데이터 브로커를 생성할 수 있습니다. 동일한 데이터 브로커 유형이 아니므로 Azure 데이터 브로커 또는 Google Cloud 데이터 브로커를 생성할 수 없습니다.

새 그룹에서 데이터 브로커를 생성하는 단계입니다

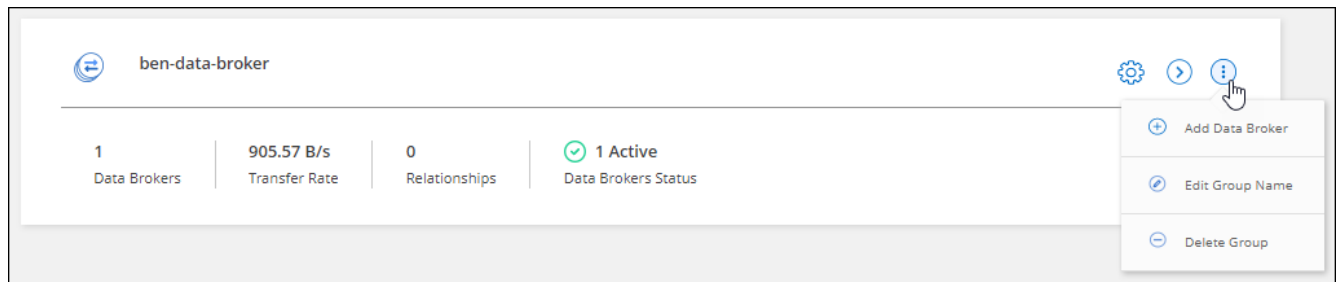
1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 새 데이터 브로커 추가 * 를 클릭합니다.
3. 프롬프트에 따라 데이터 브로커를 생성합니다.

자세한 내용은 다음 페이지를 참조하십시오.

- ["AWS에서 데이터 브로커를 생성합니다"](#)
- ["Azure에서 데이터 브로커를 생성합니다"](#)
- ["Google Cloud에서 데이터 브로커를 생성합니다"](#)
- ["Linux 호스트에 데이터 브로커 설치"](#)

기존 그룹에서 데이터 브로커를 생성하는 단계

1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 작업 메뉴를 클릭하고 * 데이터 브로커 추가 * 를 선택합니다.



3. 프롬프트에 따라 그룹에 데이터 브로커를 생성합니다.

자세한 내용은 다음 페이지를 참조하십시오.

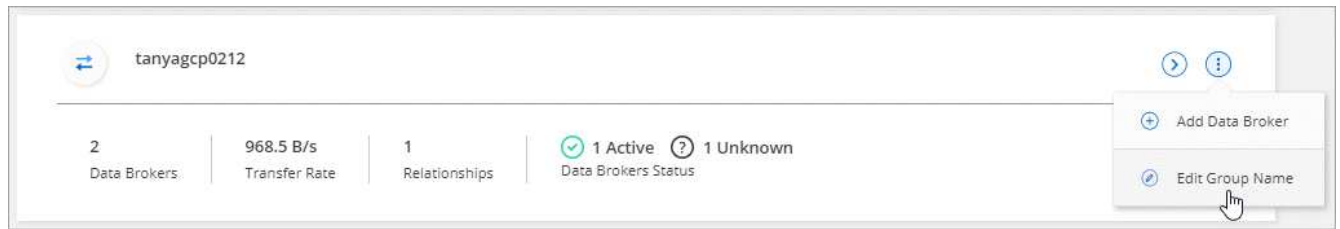
- ["AWS에서 데이터 브로커를 생성합니다"](#)
- ["Azure에서 데이터 브로커를 생성합니다"](#)
- ["Google Cloud에서 데이터 브로커를 생성합니다"](#)
- ["Linux 호스트에 데이터 브로커 설치"](#)

그룹 이름을 편집합니다

언제든지 데이터 브로커 그룹의 이름을 변경합니다.

단계

1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 작업 메뉴를 클릭하고 * 그룹 이름 편집 * 을 선택합니다.



3. 새 이름을 입력하고 * 저장 * 을 클릭합니다.

Cloud Sync가 데이터 브로커 그룹의 이름을 업데이트합니다.

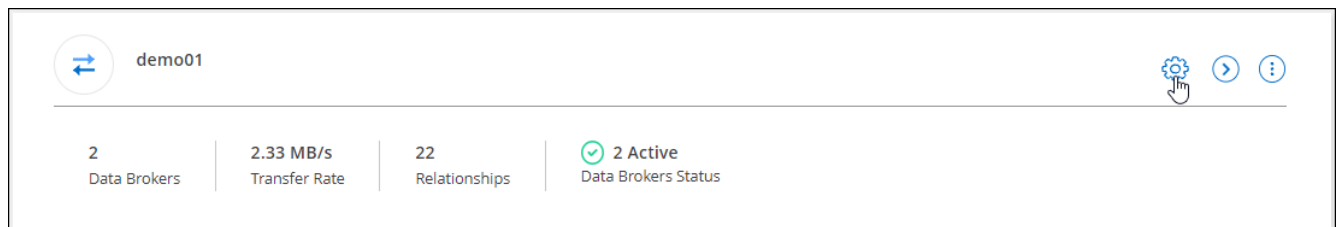
통합 구성을 설정합니다

동기화 프로세스 중에 동기화 관계에 오류가 발생하면 데이터 브로커 그룹의 동시성을 통합하면 동기화 오류 수를 줄일 수 있습니다. 그룹 구성을 변경하면 전송 속도가 느려져 성능에 영향을 줄 수 있습니다.

직접 구성을 변경하지 않는 것이 좋습니다. 구성을 변경할 시기와 변경 방법을 알아보려면 NetApp에 문의해야 합니다.

단계

1. 데이터 브로커 관리 * 를 클릭합니다.
2. 데이터 브로커 그룹의 설정 아이콘을 클릭합니다.



3. 필요에 따라 설정을 변경한 다음 * 구성 취소 * 를 클릭합니다.

다음 사항에 유의하십시오.

- 변경할 설정을 선택하고 선택할 수 있습니다. 한 번에 네 가지 설정을 모두 변경할 필요는 없습니다.
- 새 구성을 데이터 브로커로 보낸 후 데이터 브로커가 자동으로 다시 시작하고 새 구성을 사용합니다.
- 이 변경 사항이 발생할 때까지 1분 정도 걸릴 수 있으며 Cloud Sync 인터페이스에 표시될 수 있습니다.
- 데이터 브로커가 실행되고 있지 않으면 Cloud Sync에서 데이터 브로커와 통신할 수 없기 때문에 구성이 변경되지 않습니다. 데이터 브로커가 다시 시작되면 구성이 변경됩니다.
- 통합 구성을 설정하면 새 데이터 브로커가 자동으로 새 구성을 사용합니다.

그룹 간에 데이터 브로커 이동

대상 데이터 브로커 그룹의 성능을 높여야 하는 경우 그룹 간에 데이터 브로커를 이동할 수 있습니다.

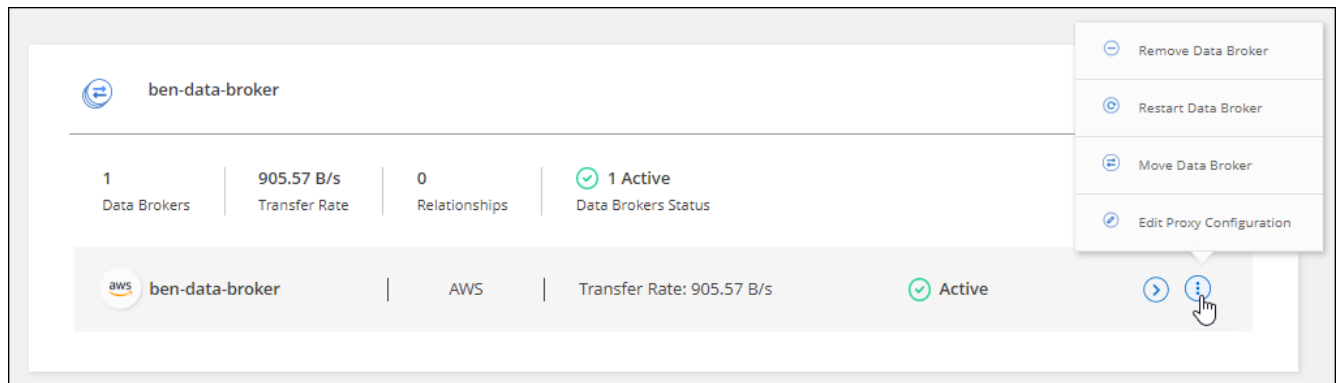
예를 들어, 데이터 브로커에서 동기화 관계를 더 이상 관리하지 않는 경우 동기화 관계를 관리하는 다른 그룹으로 쉽게 이동할 수 있습니다.

제한 사항

- 데이터 브로커 그룹이 동기화 관계를 관리하고 있고 그룹에 데이터 브로커가 하나만 있는 경우에는 해당 데이터 브로커를 다른 그룹으로 이동할 수 없습니다.
- 암호화된 동기화 관계를 관리하는 그룹으로 데이터 브로커를 이동하거나 그룹에서 데이터 브로커를 이동할 수 없습니다.
- 현재 구축 중인 데이터 브로커는 이동할 수 없습니다.

단계

1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 을 클릭합니다 > 그룹의 데이터 브로커 목록을 확장합니다.
3. 데이터 브로커에 대한 작업 메뉴를 클릭하고 * 데이터 브로커 이동 * 을 선택합니다.



4. 새 데이터 브로커 그룹을 만들거나 기존 데이터 브로커 그룹을 선택합니다.
5. 이동 * 을 클릭합니다.

Cloud Sync는 데이터 브로커를 신규 또는 기존 데이터 브로커 그룹으로 옮깁니다. 이전 그룹에 다른 데이터 브로커가 없으면 Cloud Sync에서 삭제합니다.

프록시 구성을 업데이트합니다

새 프록시 구성에 대한 세부 정보를 추가하거나 기존 프록시 구성을 편집하여 데이터 브로커의 프록시 구성을 업데이트합니다.

단계

1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 을 클릭합니다 > 그룹의 데이터 브로커 목록을 확장합니다.
3. 데이터 브로커에 대한 작업 메뉴를 클릭하고 * 프록시 구성 편집 * 을 선택합니다.
4. 프록시에 대한 세부 정보(호스트 이름, 포트 번호, 사용자 이름 및 암호)를 지정합니다.
5. Update * 를 클릭합니다.

Cloud Sync는 데이터 브로커를 업데이트하여 인터넷 액세스에 프록시 구성을 사용합니다.

데이터 브로커의 구성을 봅니다

데이터 브로커에 대한 세부 정보를 보고 호스트 이름, IP 주소, 사용 가능한 CPU 및 RAM 등을 식별할 수 있습니다.

Cloud Sync에서는 데이터 브로커에 대해 다음과 같은 세부 정보를 제공합니다.

- 기본 정보: 인스턴스 ID, 호스트 이름 등
- 네트워크: 지역, 네트워크, 서브넷, 사설 IP 등
- 소프트웨어: Linux 배포, 데이터 브로커 버전 등
- 하드웨어: CPU 및 RAM
- 구성: 데이터 브로커의 두 가지 주요 프로세스(스캐너 및 전송기)에 대한 세부 정보입니다



스캐너가 소스와 대상을 스캔하고 복사할 대상을 결정합니다. 전송자는 실제 복사를 수행합니다. NetApp 직원은 이러한 구성 세부 정보를 사용하여 성능을 최적화할 수 있는 조치를 제안할 수 있습니다.

단계

1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 을 클릭합니다 > 그룹의 데이터 브로커 목록을 확장합니다.
3. 을 클릭합니다 > 데이터 브로커에 대한 세부 정보를 봅니다.

tanyagcp0212

2 Data Brokers | 968.5 B/s Transfer Rate | 1 Relationships | 1 Active 1 Unknown Data Brokers Status

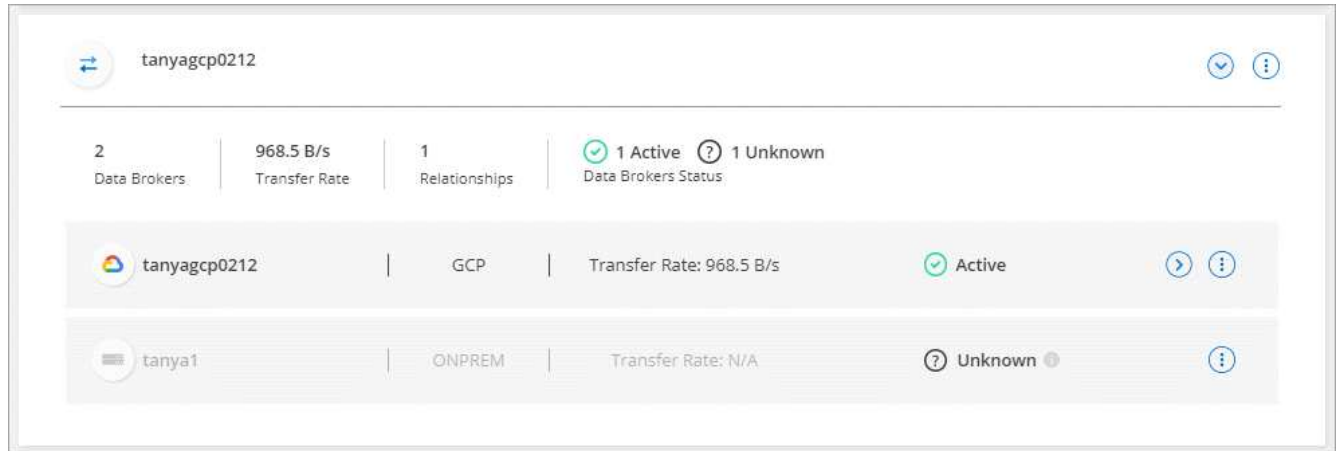
tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active	
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project ID
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version
Hardware	4 Available CPUs	62.22 MB Available RAM		
Configuration	50 Scanner Concurrency	4 Scanner CPUs	50 Transferer Concurrency	4 Transferer CPUs

데이터 브로커로 문제를 해결합니다

Cloud Sync에서는 문제를 해결하는 데 도움이 되는 각 데이터 브로커의 상태를 표시합니다.

단계

1. "알 수 없음" 또는 "실패" 상태의 데이터 브로커를 식별합니다.



2. 에 마우스를 올려 놓습니다 ⓘ 아이콘을 클릭하여 실패 원인을 확인합니다.
3. 문제를 해결하십시오.

예를 들어, 데이터 브로커가 오프라인인 경우 다시 시작하기만 하면 되고, 초기 구축에 실패한 경우 데이터 브로커를 제거해야 할 수 있습니다.

그룹에서 데이터 브로커를 제거합니다

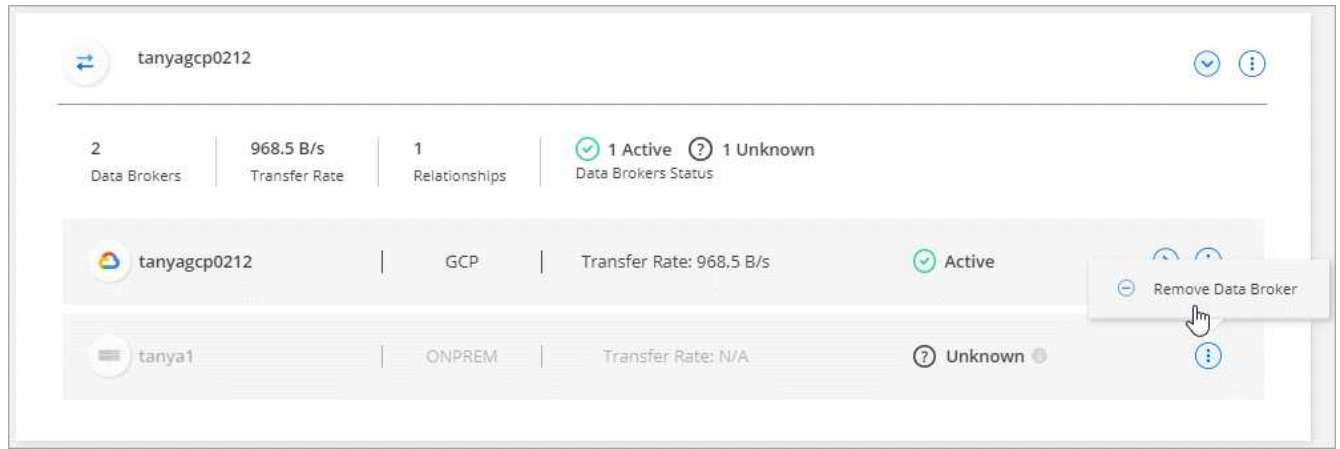
더 이상 필요하지 않거나 초기 구축에 실패한 경우 그룹에서 데이터 브로커를 제거할 수 있습니다. 이 작업을 수행하면 Cloud Sync의 레코드에서 데이터 브로커만 삭제됩니다. 데이터 브로커와 추가 클라우드 리소스를 수동으로 삭제해야 합니다.

알아야 할 사항

- Cloud Sync 그룹에서 마지막 데이터 브로커를 제거하면 그룹이 삭제됩니다.
- 해당 그룹을 사용하는 관계가 있는 경우 그룹에서 마지막 데이터 브로커를 제거할 수 없습니다.

단계

1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 을 클릭합니다 ➡ 그룹의 데이터 브로커 목록을 확장합니다.
3. 데이터 브로커에 대한 작업 메뉴를 클릭하고 * 데이터 브로커 * 를 선택합니다.



4. 데이터 브로커 * 제거 를 클릭합니다.

Cloud Sync는 그룹에서 데이터 브로커를 제거합니다.

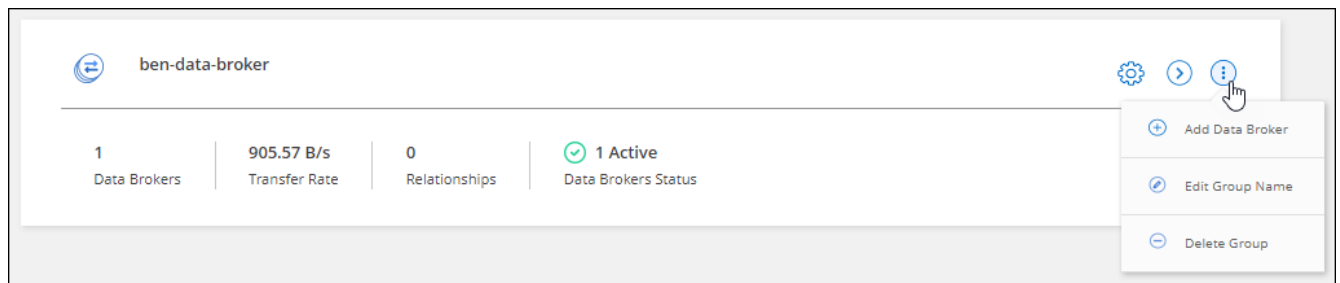
데이터 브로커 그룹을 삭제합니다

데이터 브로커 그룹이 더 이상 동기화 관계를 관리하지 않으면 그룹을 삭제할 수 있습니다. 그러면 Cloud Sync에서 모든 데이터 브로커가 제거됩니다.

Cloud Sync에서 제거하는 데이터 브로커는 Cloud Sync의 레코드에서만 삭제됩니다. 클라우드 공급자 및 추가 클라우드 리소스를 수동으로 데이터 브로커 인스턴스를 삭제해야 합니다.

단계

1. 동기화 > 데이터 브로커 관리 * 를 클릭합니다.
2. 작업 메뉴를 클릭하고 * 그룹 삭제 * 를 선택합니다.



3. 확인하려면 그룹 이름을 입력하고 * 그룹 삭제 * 를 클릭합니다.

Cloud Sync는 데이터 브로커를 제거하고 그룹을 삭제합니다.

구성을 조정하기 위해 보고서 작성 및 보기

NetApp 직원의 도움을 받아 데이터 브로커 구성을 조정하고 성능을 개선하는 데 사용할 수 있는 정보를 보고서를 생성하고 확인합니다.

각 보고서는 동기화 관계의 경로에 대한 세부 정보를 제공합니다. 예를 들어, 파일 시스템에 대한 보고서는 디렉토리 및 파일 수, 파일 크기 분포, 디렉토리의 전체 및 깊이 등을 보여 줍니다.

보고서 작성

보고서를 만들 때마다 Cloud Sync는 경로를 검색한 다음 세부 정보를 보고서로 컴파일합니다.

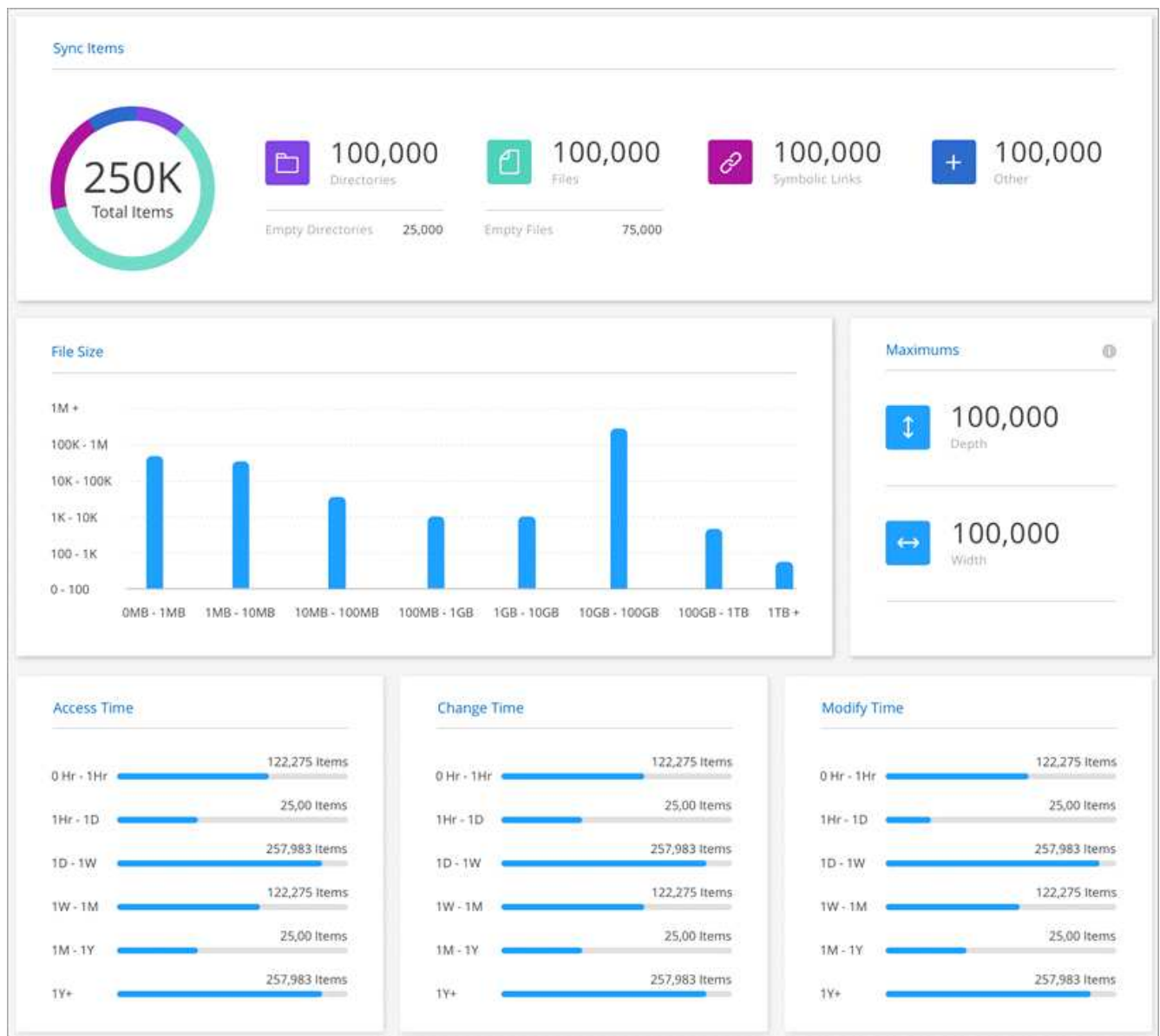
단계

1. 동기화 > 보고서 * 를 클릭합니다.

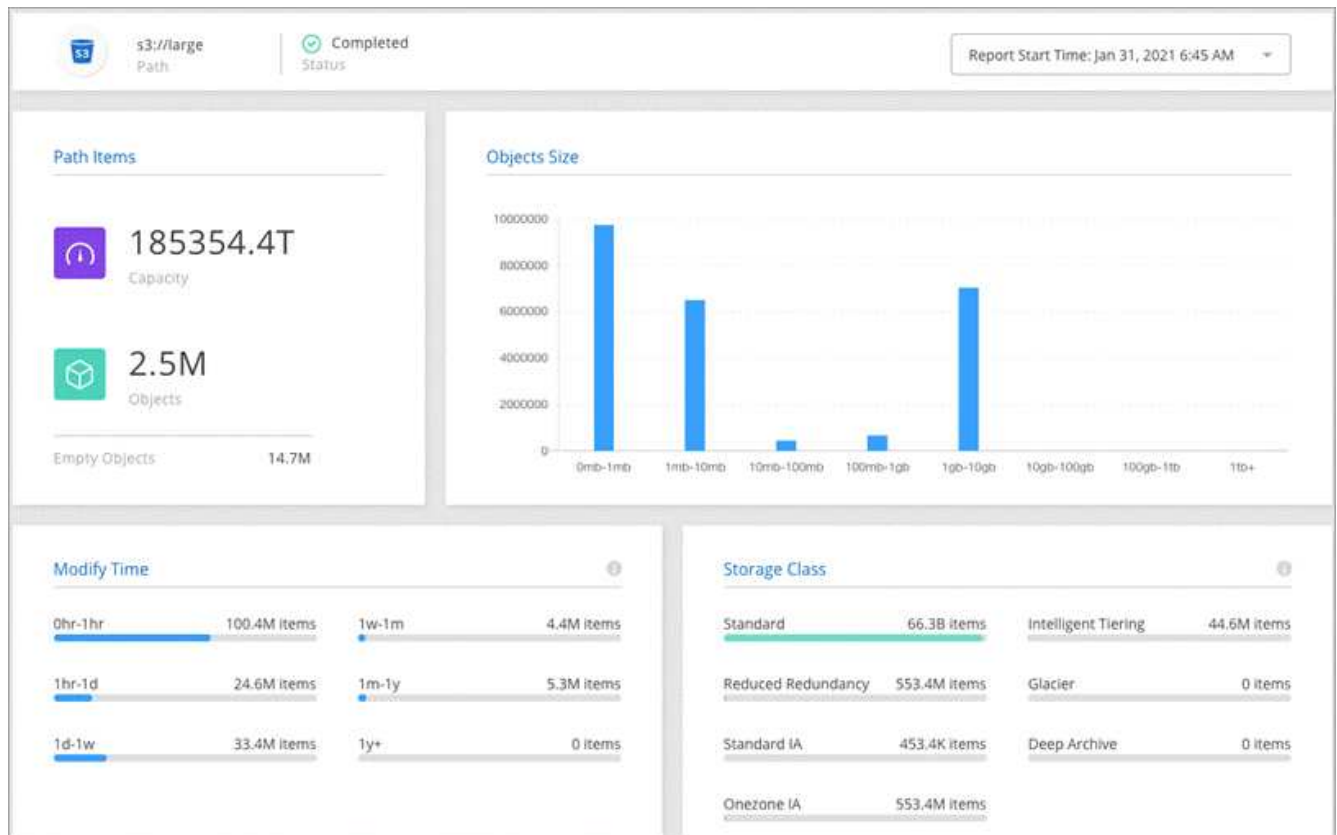
각 동기화 관계의 경로(원본 또는 대상)가 테이블에 표시됩니다.

2. 보고서 작업 * 열에서 특정 경로로 이동하여 * 생성 * 을 클릭하거나 작업 메뉴를 클릭하고 * 새로 만들기 * 를 선택합니다.
3. 보고서가 준비되면 작업 메뉴를 클릭하고 * 보기 * 를 선택합니다.

다음은 파일 시스템 경로에 대한 샘플 보고서입니다.



다음은 오브젝트 스토리지에 대한 샘플 보고서입니다.

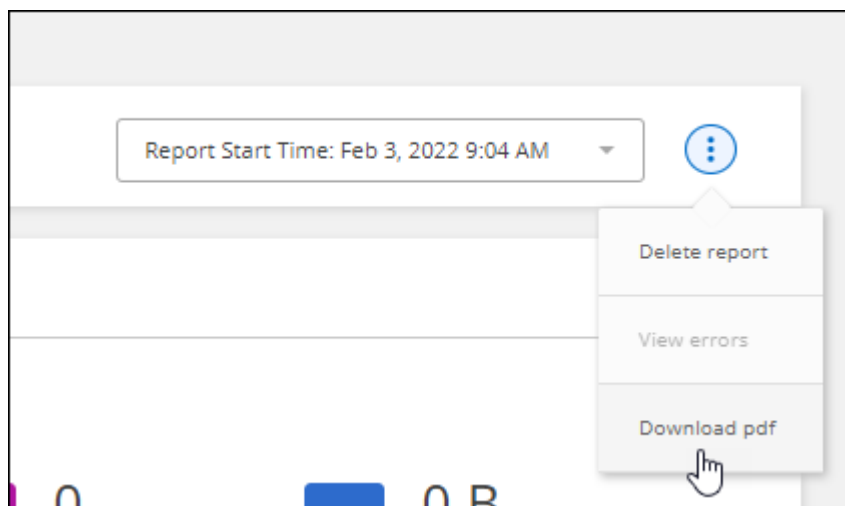


보고서를 다운로드하는 중입니다

보고서를 오프라인으로 보거나 공유할 수 있도록 PDF로 보고서를 다운로드할 수 있습니다.

단계

1. 동기화 > 보고서 * 를 클릭합니다.
2. 보고서 작업 * 열에서 작업 메뉴를 클릭하고 * 보기 * 를 선택합니다.
3. 보고서 오른쪽 상단에서 작업 메뉴를 클릭하고 * PDF 다운로드 * 를 선택합니다.



보고서 오류를 보는 중입니다

경로 테이블은 가장 최근 보고서에 오류가 있는지 여부를 식별합니다. 오류는 Cloud Sync가 경로를 스캔할 때 발생한 문제를 나타냅니다.

예를 들어 보고서에 권한 거부 오류가 있을 수 있습니다. 이 유형의 오류는 Cloud Sync가 전체 파일 및 디렉토리 세트를 스캔하는 기능에 영향을 미칠 수 있습니다.

오류 목록을 확인한 후 문제를 해결하고 보고서를 다시 실행할 수 있습니다.

단계

1. 동기화 > 보고서 * 를 클릭합니다.
2. Errors * 열에서 보고서에 오류가 있는지 여부를 확인합니다.
3. 오류가 있는 경우 오류 수 옆에 있는 화살표를 클릭합니다.

20 Paths

Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

4. 오류 정보를 사용하여 문제를 해결하십시오.

문제를 해결한 후에는 다음에 보고서를 실행할 때 오류가 나타나지 않습니다.

보고서를 삭제하는 중입니다

수정한 오류가 포함되어 있거나 보고서가 제거된 동기화 관계에 연결되어 있는 경우 해당 보고서를 삭제할 수 있습니다.

단계

1. 동기화 > 보고서 * 를 클릭합니다.
2. 보고서 작업 * 열에서 경로에 대한 작업 메뉴를 클릭하고 * 마지막 보고서 삭제 * 또는 * 모든 보고서 삭제 * 를 선택합니다.
3. 보고서 또는 보고서를 삭제할 것인지 확인합니다.

데이터 브로커를 제거하는 중입니다

필요한 경우 제거 스크립트를 실행하여 데이터 브로커가 설치되었을 때 생성된 데이터 브로커와 패키지 및 디렉토리를 제거합니다.

단계

1. 데이터 브로커 호스트에 로그인합니다.
2. 데이터 브로커 디렉터리 '/opt/netapp/databroker'로 변경합니다
3. 다음 명령을 실행합니다.

```
chmod+x uninstaller-DataBroker.sh../uninstaller-DataBroker.sh
```

4. 'y'를 눌러 제거를 확인합니다.

Copyright Information

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

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

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

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

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

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

Trademark Information

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