# 소스와 대상 간 데이터 동기화

## NetApp Copy and Sync

NetApp
December 16, 2025

# 목차

# 소스와 대상 간 데이터 동기화

## NetApp Copy and Sync 에서 개체 스토리지 간 데이터를 동기화하기 위한 데이터 브로커 준비

NetApp Copy and Sync 에서 개체 스토리지 간에 데이터를 동기화하려는 경우(예: Amazon S3에서 Azure Blob으로) 동기화 관계를 만들기 전에 데이터 브로커 그룹을 준비해야 합니다.

이 작업에 관하여

데이터 브로커 그룹을 준비하려면 스캐너 구성을 수정해야 합니다. 구성을 수정하지 않으면 이 동기화 관계에서 성능 문제가 발생할 수 있습니다.

시작하기 전에

개체 스토리지 간에 데이터를 동기화하는 데 사용하는 데이터 브로커 그룹은 이러한 유형의 동기화 관계만 관리해야 합니다. 데이터 브로커 그룹이 다른 유형의 동기화 관계(예: NFS 대 NFS 또는 개체 스토리지 대 SMB)를 관리하는 경우 해당 동기화 관계의 성능이 부정적인 영향을 받을 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. 복사 및 동기화에서 *데이터 브로커 관리*를 선택합니다.
3. 선택하다
4. 스캐너 구성을 업데이트하세요.
   a. *스캐너 동시성*을 *1*로 변경합니다.
   b. *스캐너 프로세스 제한*을 *1*로 변경합니다.
5. *구성 통합*을 선택합니다.

결과

복사 및 동기화는 데이터 브로커 그룹의 구성을 업데이트합니다.

다음은 무엇인가요?

방금 구성한 데이터 브로커 그룹을 사용하여 개체 스토리지 간의 동기화 관계를 만들 수 있습니다.

# NetApp Copy and Sync 에서 동기화 관계 만들기

동기화 관계를 생성하면 NetApp Copy and Sync 소스에서 대상으로 파일을 복사합니다. 최초 복사 후, 복사 및 동기화는 24시간마다 변경된 데이터를 동기화합니다.

일부 유형의 동기화 관계를 만들려면 먼저 NetApp Console 에서 시스템을 만들어야 합니다.

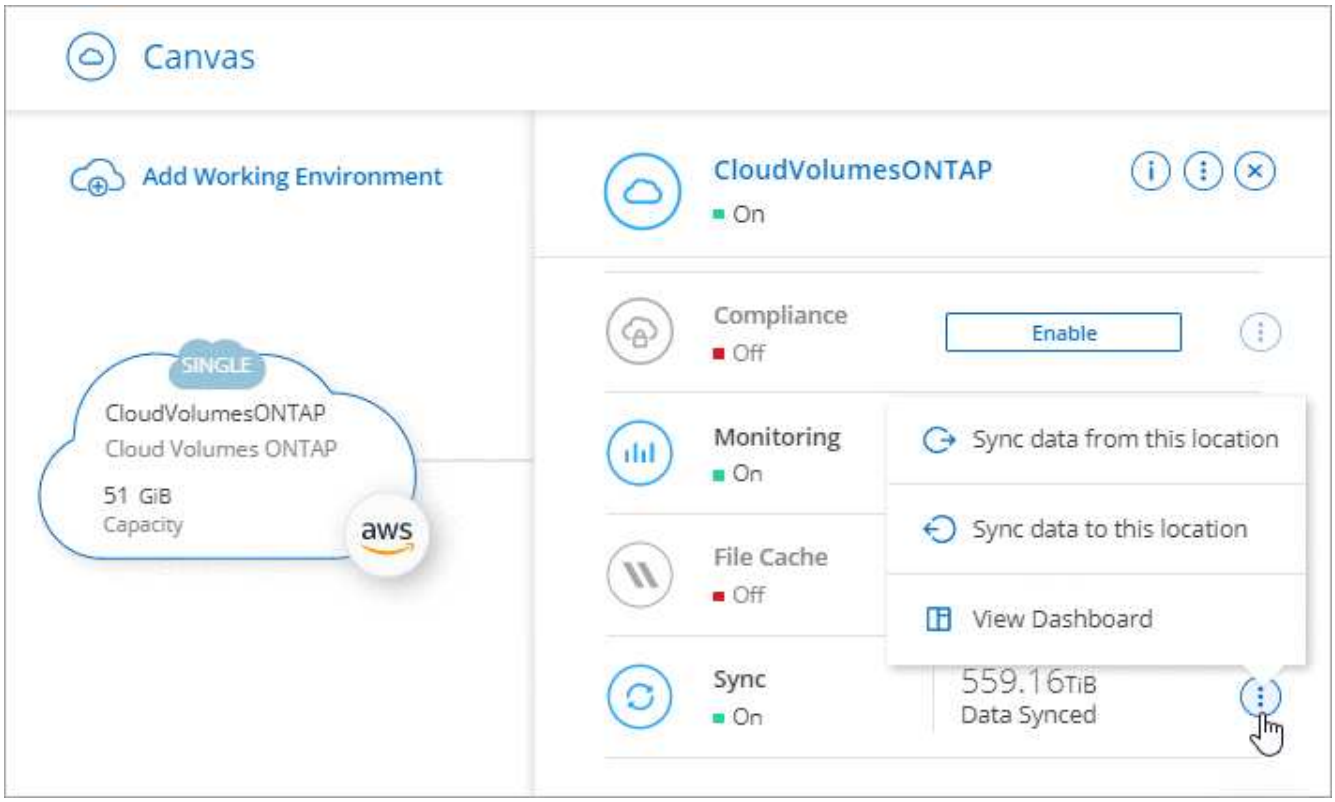
## 특정 유형의 시스템에 대한 동기화 관계 생성

다음 중 하나에 대한 동기화 관계를 만들려면 먼저 시스템을 만들거나 검색해야 합니다.

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

단계

1. "복사 및 동기화에 로그인하세요" .
2. 시스템을 생성하거나 발견합니다.
    - "Amazon FSx for ONTAP 시스템 생성"
    - "Azure NetApp Files 설정 및 검색"
    - "AWS에서 Cloud Volumes ONTAP 출시"
    - "Azure에서 Cloud Volumes ONTAP 시작"
    - "Google Cloud에서 Cloud Volumes ONTAP 출시"
    - "기존 Cloud Volumes ONTAP 시스템 추가"
    - "ONTAP 클러스터 검색"
3. *시스템 페이지*를 선택하세요.
4. 위에 나열된 유형 중 하나와 일치하는 시스템을 선택하세요.
5. 동기화 옆에 있는 작업 메뉴를 선택하세요.




6. 이 위치에서 데이터 동기화 또는 *이 위치에 데이터 동기화*를 선택하고 화면의 지시에 따라 동기화 관계를 설정합니다.

## 다른 유형의 동기화 관계 만들기

다음 단계를 사용하여 Amazon FSx for ONTAP, Azure NetApp Files, Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터가 아닌 지원되는 스토리지 유형과 데이터를 동기화합니다. 아래 단계에서는 NFS 서버에서 S3 버킷으로 동기화 관계를 설정하는 방법을 보여주는 예를 제공합니다.

1. NetApp Console 에서 *동기화*를 선택합니다.
2. 동기화 관계 정의 페이지에서 소스와 대상을 선택합니다.

   다음 단계에서는 NFS 서버에서 S3 버킷으로 동기화 관계를 만드는 방법의 예를 보여줍니다.

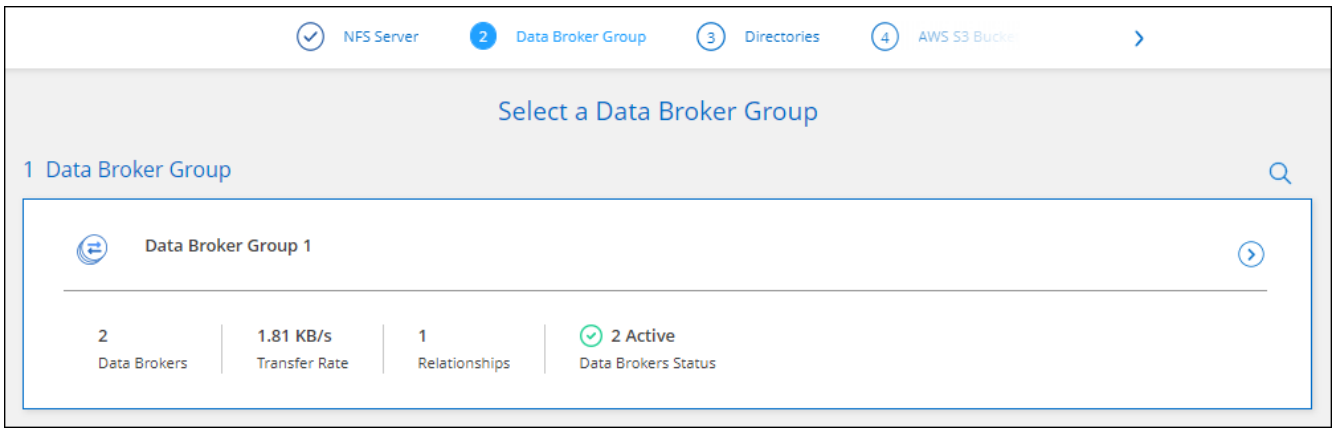

3. **NFS** 서버 페이지에서 AWS와 동기화하려는 NFS 서버의 IP 주소나 정규화된 도메인 이름을 입력합니다.
4. 데이터 브로커 그룹 페이지에서 프롬프트에 따라 AWS, Azure 또는 Google Cloud Platform에서 데이터 브로커 가상 머신을 만들거나 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치합니다.

   자세한 내용은 다음 페이지를 참조하세요.

   - "AWS에서 데이터 브로커 만들기"
   - "Azure에서 데이터 브로커 만들기"
   - "Google Cloud에서 데이터 브로커 만들기"

- "Linux 호스트에 데이터 브로커 설치"

5. 데이터 브로커를 설치한 후 *계속*을 선택하세요.



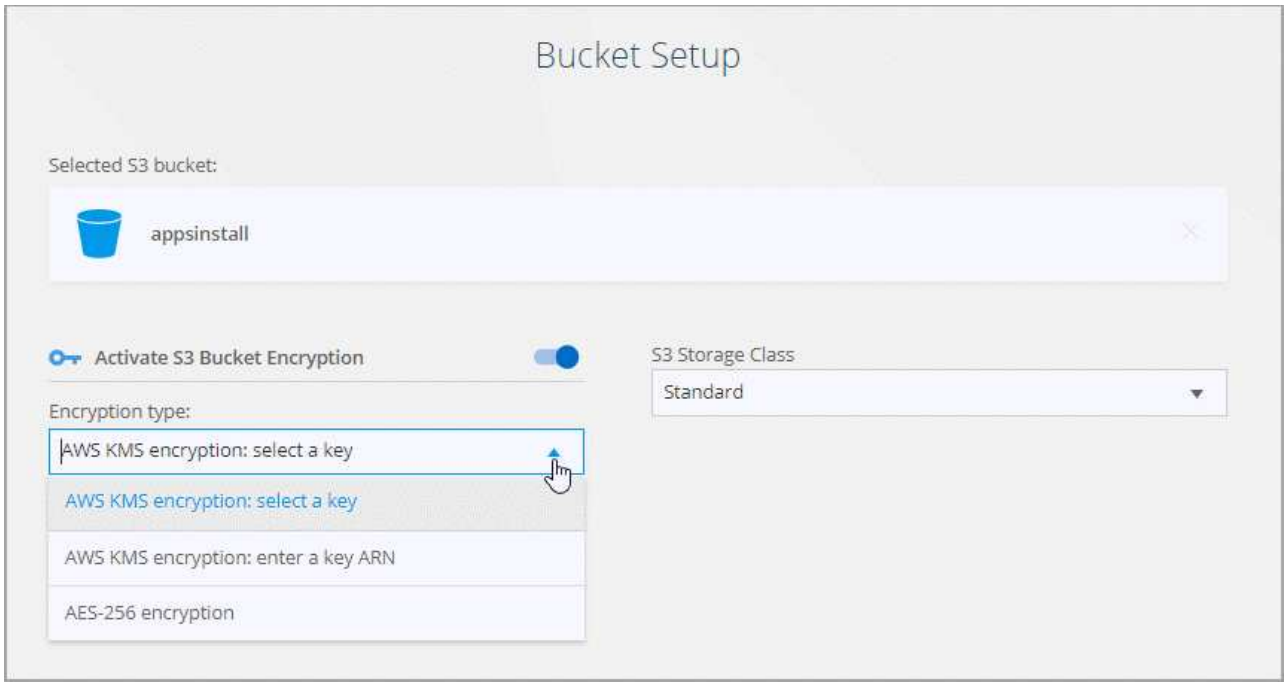

6. 디렉토리 페이지에서 최상위 디렉토리나 하위 디렉토리를 선택하세요.

   복사 및 동기화에서 내보내기를 검색할 수 없는 경우 *수동으로 내보내기 추가*를 선택하고 NFS 내보내기의 이름을 입력합니다.

   NFS 서버에서 두 개 이상의 디렉토리를 동기화하려면 작업을 마친 후 추가 동기화 관계를 만들어야 합니다.

7. **AWS S3** 버킷 페이지에서 버킷을 선택하세요.
   - 버킷 내의 기존 폴더를 선택하거나 버킷 내에 만든 새 폴더를 선택하려면 드릴다운합니다.
   - AWS 계정과 연결되지 않은 S3 버킷을 선택하려면 *목록에 추가*를 선택하세요. "S3 버킷에 특정 권한을 적용해야 합니다." .

8. 버킷 설정 페이지에서 버킷을 설정합니다.
   - S3 버킷 암호화를 활성화할지 선택한 다음 AWS KMS 키를 선택하거나 KMS 키의 ARN을 입력하거나 AES-256 암호화를 선택합니다.
   - S3 스토리지 클래스를 선택하세요. "지원되는 스토리지 클래스 보기" .




9. 설정 페이지에서 소스 파일과 폴더가 대상 위치에서 동기화되고 유지되는 방식을 정의합니다.

일정

향후 동기화를 위해 반복 일정을 선택하거나 동기화 일정을 끕니다. 최대 1분마다 데이터를 동기화하도록 관계를 예약할 수 있습니다.

동기화 시간 초과

동기화가 지정된 분, 시간 또는 일 수 내에 완료되지 않을 경우 복사 및 동기화가 데이터 동기화를 취소해야 하는지 여부를 정의합니다.

알림

NetApp 콘솔의 알림 센터에서 복사 및 동기화 알림을 받을지 여부를 선택할 수 있습니다. 성공적인 데이터 동기화, 실패한 데이터 동기화, 취소된 데이터 동기화에 대한 알림을 활성화할 수 있습니다.

재시도

복사 및 동기화가 파일을 건너뛰기 전에 동기화를 다시 시도해야 하는 횟수를 정의합니다.

연속 동기화

초기 데이터 동기화 후, 복사 및 동기화는 소스 S3 버킷이나 Google Cloud Storage 버킷의 변경 사항을 수신하고 발생하는 모든 변경 사항을 대상에 지속적으로 동기화합니다. 예약된 간격으로 소스를 다시 스캔할 필요가 없습니다.

이 설정은 동기화 관계를 생성할 때와 S3 버킷 또는 Google Cloud Storage에서 Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3 및 StorageGRID 또는 Azure Blob Storage에서 Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS 및 StorageGRID 로 데이터를 동기화할 때만 사용할 수 있습니다.

이 설정을 활성화하면 다음과 같이 다른 기능에 영향을 미칩니다.

- 동기화 일정이 비활성화되었습니다.
- 다음 설정은 기본값으로 돌아갑니다: 동기화 시간 초과, 최근 수정된 파일, 수정 날짜.

- S3가 소스인 경우 크기별 필터는 복사 이벤트에서만 활성화됩니다(삭제 이벤트에서는 활성화되지 않음).
- 관계가 생성된 후에는 관계를 가속화하거나 삭제할 수만 있습니다. 동기화를 중단하거나, 설정을 수정하거나, 보고서를 볼 수 없습니다.

외부 버킷과 지속적인 동기화 관계를 만드는 것이 가능합니다. 그렇게 하려면 다음 단계를 따르세요.

i. 외부 버킷 프로젝트에 대한 Google Cloud 콘솔로 이동합니다.

ii. *클라우드 스토리지 > 설정 > 클라우드 스토리지 서비스 계정*으로 이동합니다.

iii. local.json 파일을 업데이트합니다.

```
{
"protocols": {
    "gcp": {
        "storage-account-email": <storage account email>
}
}
}
```

iv. 데이터 브로커를 다시 시작합니다.

A. sudo pm2 모두 중지

B. sudo pm2 모두 시작

v. 해당 외부 버킷과 지속적인 동기화 관계를 만듭니다.

> 외부 버킷과 지속적인 동기화 관계를 생성하는 데 사용되는 데이터 브로커는 해당 프로젝트의 버킷과 다른 지속적인 동기화 관계를 생성할 수 없습니다.

비교 기준

복사 및 동기화에서 파일이나 디렉토리가 변경되어 다시 동기화해야 하는지 여부를 결정할 때 특정 속성을 비교해야 하는지 여부를 선택합니다.

이러한 속성의 선택을 해제하더라도 복사 및 동기화는 경로, 파일 크기, 파일 이름을 확인하여 소스와 대상을 비교합니다. 변경 사항이 있으면 해당 파일과 디렉토리를 동기화합니다.

다음 속성을 비교하여 복사 및 동기화를 활성화하거나 비활성화할 수 있습니다.

- **mtime**: 파일의 마지막 수정 시간. 이 속성은 디렉토리에 유효하지 않습니다.
- **uid**, **gid**, 및 **mode**: Linux의 권한 플래그입니다.

개체에 대한 복사

이 옵션을 활성화하면 개체 저장소 메타데이터와 태그를 복사할 수 있습니다. 사용자가 소스의 메타데이터를 변경하면 복사 및 동기화는 다음 동기화에서 이 개체를 복사하지만, 사용자가 소스의 태그를 변경하고 데이터 자체는 변경하지 않으면 복사 및 동기화는 다음 동기화에서 개체를 복사하지 않습니다.

관계를 만든 후에는 이 옵션을 편집할 수 없습니다.

태그 복사는 Azure Blob 또는 S3 호환 엔드포인트(S3, StorageGRID 또는 IBM Cloud Object Storage)를 대상으로 포함하는 동기화 관계에서 지원됩니다.

다음 엔드포인트 간의 "클라우드 간" 관계를 통해 메타데이터 복사가 지원됩니다.

- AWS S3
- Azure Blob
- 구글 클라우드 스토리지
- IBM 클라우드 객체 스토리지
- StorageGRID

최근 수정된 파일

예약된 동기화 전에 최근 수정된 파일을 제외하도록 선택합니다.

소스에서 파일 삭제

복사 및 동기화를 통해 파일을 대상 위치로 복사한 후 소스 위치에서 파일을 삭제하도록 선택합니다. 이 옵션을 사용하면 원본 파일이 복사된 후 삭제되므로 데이터 손실 위험이 있습니다.

이 옵션을 활성화하면 데이터 브로커의 local.json 파일에서 매개변수도 변경해야 합니다. 파일을 열고 다음과 같이 업데이트하세요.

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

local.json 파일을 업데이트한 후에는 다시 시작해야 합니다. `pm2 restart all` .

대상의 파일 삭제

소스에서 파일이 삭제된 경우 대상 위치에서도 파일을 삭제하도록 선택합니다. 기본적으로 대상 위치에서 파일을 삭제하지 않습니다.

파일 유형

각 동기화에 포함할 파일 유형을 정의합니다. 파일, 디렉토리, 심볼릭 링크, 하드 링크입니다.

하드 링크는 보안되지 않은 NFS 간 관계에만 사용할 수 있습니다. 사용자는 하나의 스캐너 프로세스와 하나의 스캐너 동시성으로 제한되며, 스캔은 루트 디렉토리에서 실행해야 합니다.

파일 확장자 제외

동기화에서 제외할 정규식이나 파일 확장자를 지정하려면 파일 확장자를 입력하고 *Enter*를 누릅니다. 예를 들어, *.log 파일을 제외하려면 *log* 또는 _.log_를 입력합니다. 여러 개의 확장자를 사용하는 경우 구분 기호는 필요하지 않습니다. 다음 영상은 짧은 데모를 제공합니다.

동기화 관계에 대한 파일 확장자 제외

정규 표현식은 와일드카드나 글로브 표현식과 다릅니다. 이 기능은 정규 표현식에서만 작동합니다.

디렉토리 제외

이름이나 디렉토리 전체 경로를 입력하고 *Enter*를 눌러 동기화에서 제외할 정규식이나 디렉토리를 최대 15개까지 지정합니다. .copy-offload, .snapshot, ~snapshot 디렉토리는 기본적으로 제외됩니다.

정규 표현식은 와일드카드나 글로브 표현식과 다릅니다. 이 기능은 정규 표현식에서만 작동합니다.

파일 크기

크기에 관계없이 모든 파일을 동기화하거나 특정 크기 범위에 속하는 파일만 동기화하도록 선택합니다.

수정 날짜

마지막 수정 날짜와 관계없이 모든 파일을 선택합니다. 특정 날짜 이후, 특정 날짜 이전 또는 기간 사이에 수정된 파일을 선택합니다.

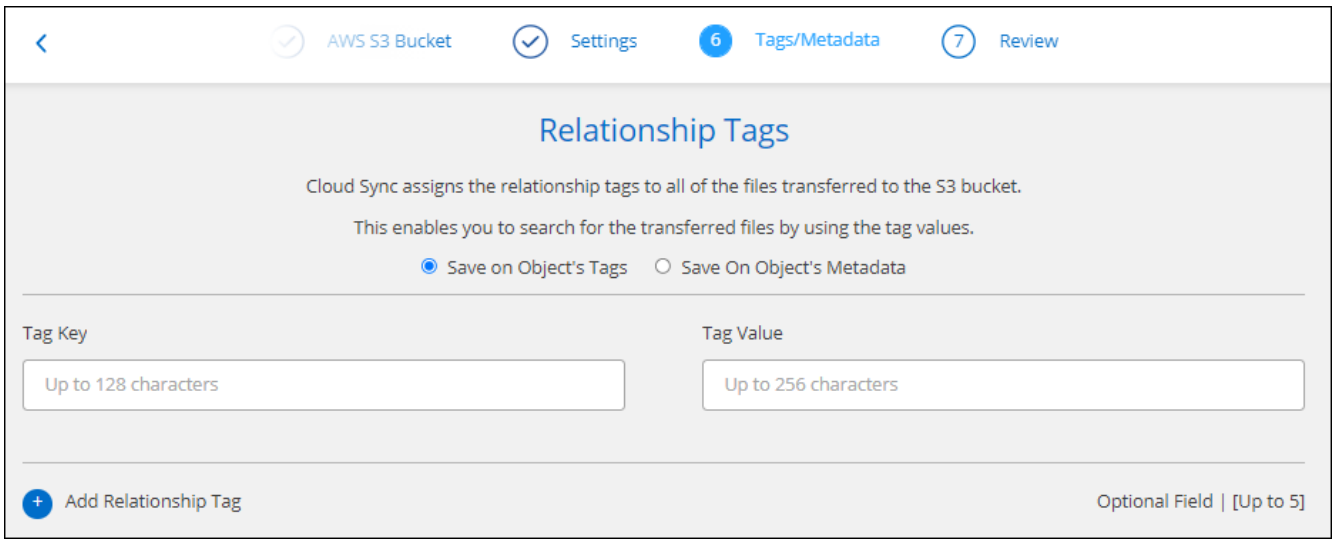
생성 날짜

SMB 서버가 소스인 경우, 이 설정을 사용하면 특정 날짜 이후, 특정 날짜 이전 또는 특정 기간 사이에 생성된 파일을 동기화할 수 있습니다.

**ACL -** 액세스 제어 목록

관계를 생성할 때 또는 관계를 생성한 후에 설정을 활성화하여 SMB 서버에서 ACL만 복사하거나, 파일만 복사하거나, ACL과 파일을 모두 복사합니다.

10. 태그/메타데이터 페이지에서 S3 버킷으로 전송되는 모든 파일에 태그로 키-값 쌍을 저장할지, 아니면 모든 파일에 메타데이터 키-값 쌍을 할당할지 선택합니다.




StorageGRID 및 IBM Cloud Object Storage에 데이터를 동기화할 때도 동일한 기능을 사용할 수 있습니다. Azure 및 Google Cloud Storage의 경우 메타데이터 옵션만 사용할 수 있습니다.

11. 동기화 관계의 세부 정보를 검토한 다음 *관계 만들기*를 선택합니다.

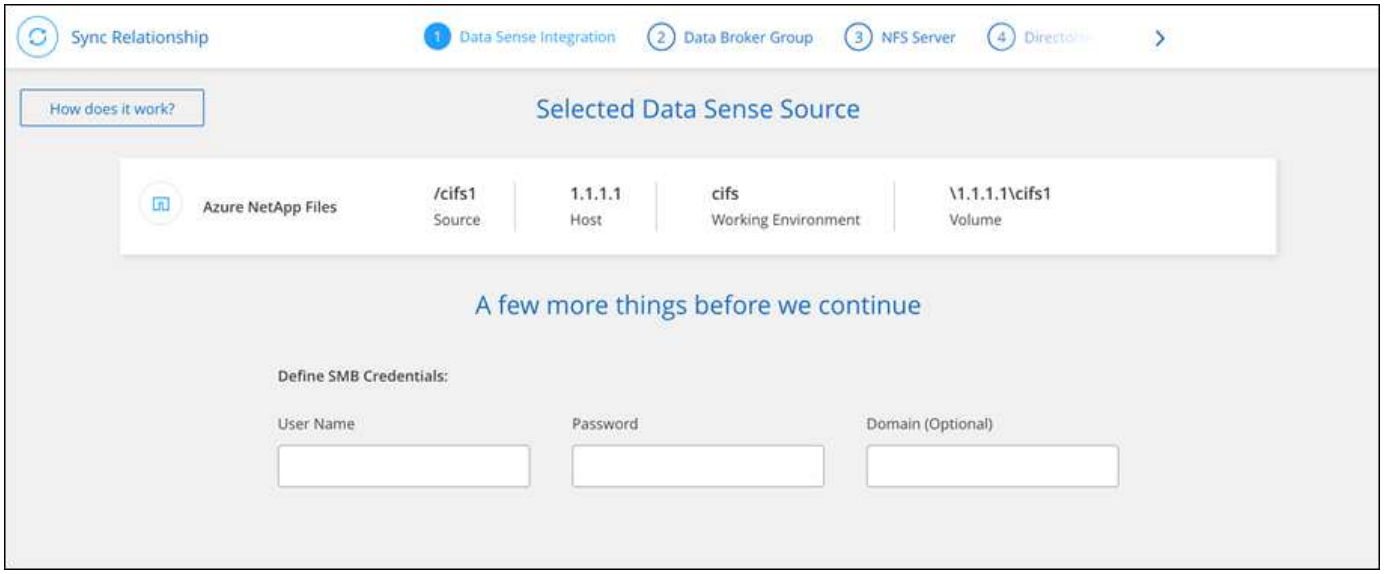
결과

복사 및 동기화는 소스와 대상 간의 데이터 동기화를 시작합니다. 동기화에 걸린 시간, 동기화가 중단되었는지 여부, 복사, 스캔 또는 삭제된 파일 수에 대한 동기화 통계를 사용할 수 있습니다. 그런 다음 다음을 관리할 수 있습니다. "동기화 관계" , "데이터 브로커를 관리하세요" , 또는 "성능과 구성을 최적화하기 위한 보고서 생성" .

### NetApp Data Classification 에서 동기화 관계 만들기

Copy and Sync는 NetApp Data Classification 과 통합되어 있습니다. NetApp Data Classification 내에서 복사 및 동기화를 사용하여 대상 위치로 동기화하려는 소스 파일을 선택할 수 있습니다.

NetApp Data Classification 에서 데이터 동기화를 시작하면 모든 소스 정보가 단일 단계에 포함되며 몇 가지 주요 세부 정보만 입력하면 됩니다. 그런 다음 새로운 동기화 관계에 대한 대상 위치를 선택합니다.




"NetApp Data Classification 에서 동기화 관계를 시작하는 방법을 알아보세요." .

# NetApp Copy and Sync 에서 SMB 공유의 ACL 복사

NetApp Copy and Sync SMB 공유 간, 그리고 SMB 공유와 개체 스토리지( ONTAP S3 제외) 간에 액세스 제어 목록(ACL)을 복사할 수 있습니다. 필요한 경우 robocopy를 사용하여 SMB 공유 간 ACL을 수동으로 보존할 수도 있습니다.

선택

- ACL을 자동으로 복사하도록 복사 및 동기화 설정
- SMB 공유 간 ACL을 수동으로 복사합니다.

### ACL을 복사하기 위한 복사 및 동기화 설정

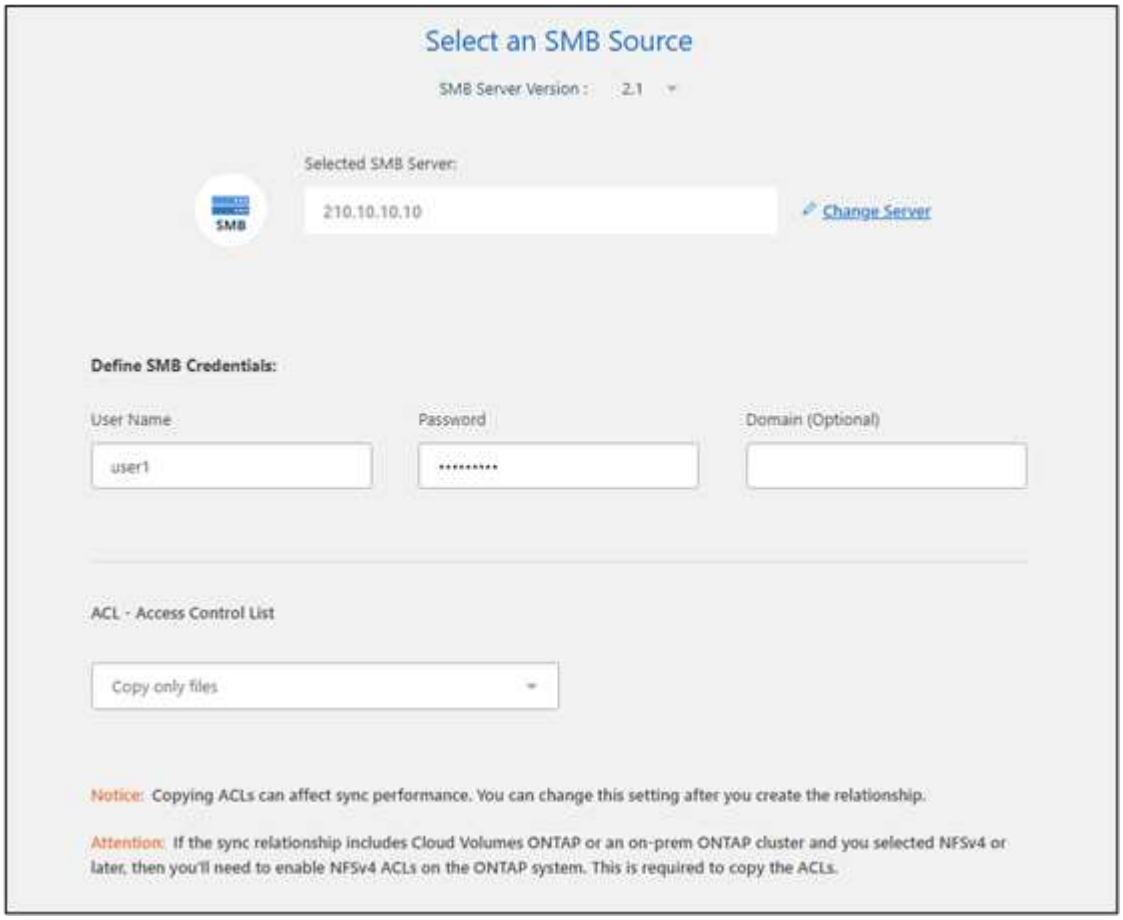
관계를 생성할 때 또는 관계를 생성한 후에 설정을 활성화하여 SMB 공유 간, 그리고 SMB 공유와 개체 스토리지 간에 ACL을 복사합니다.

시작하기 전에

이 기능은 AWS, Azure, Google Cloud Platform 또는 온프레미스 데이터 브로커 등 모든 유형의 데이터 브로커에서 작동합니다. 온프레미스 데이터 브로커는 다음을 실행할 수 있습니다."지원되는 모든 운영 체제" .

새로운 관계를 위한 단계

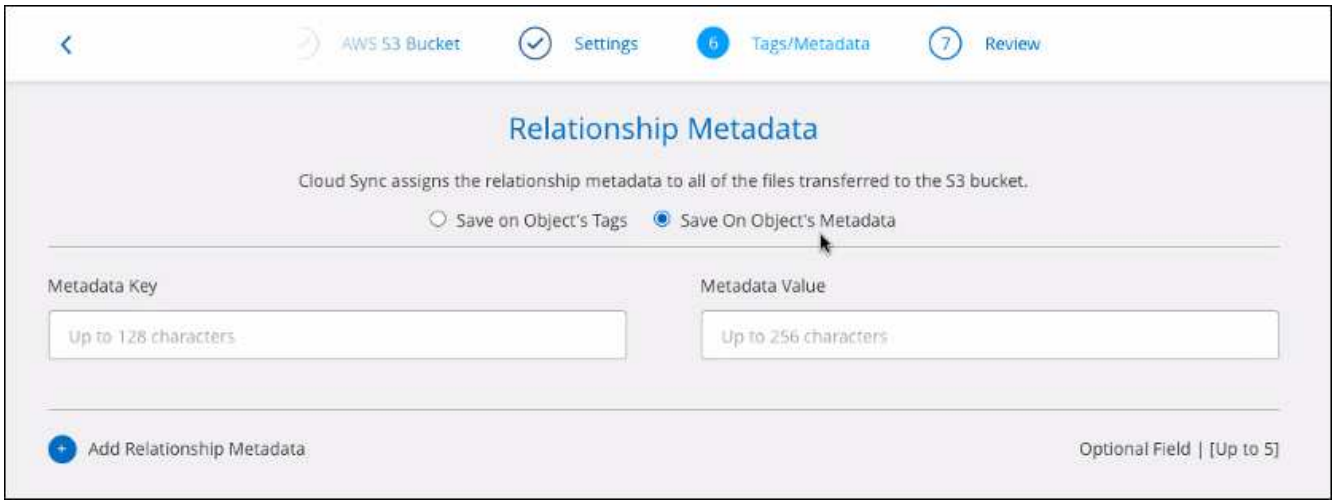
1. "복사 및 동기화에 로그인하세요" .
2. 복사 및 동기화에서 *새 동기화 만들기*를 선택합니다.
3. 소스로 SMB 서버 또는 개체 스토리지를 끌어다 놓고, 대상으로 SMB 서버 또는 개체 스토리지를 끌어다 놓은 다음 *계속*을 선택합니다.
4. **SMB** 서버 페이지에서:
   a. 새로운 SMB 서버를 입력하거나 기존 서버를 선택하고 *계속*을 선택하세요.
   b. SMB 서버에 대한 자격 증명을 입력하세요.
   c. 파일만 복사, **ACL**만 복사, 파일 및 **ACL** 복사 중 하나를 선택하고 *계속*을 선택합니다.




5. 나머지 메시지에 따라 동기화 관계를 만듭니다.

   SMB에서 개체 스토리지로 ACL을 복사할 때 대상에 따라 ACL을 개체의 태그나 개체의 메타데이터에 복사할 수 있습니다. Azure 및 Google Cloud Storage의 경우 메타데이터 옵션만 사용할 수 있습니다.

   다음 스크린샷은 이러한 선택을 할 수 있는 단계의 예를 보여줍니다.




기존 관계에 대한 단계

1. 동기화 관계 위에 마우스를 올려놓고 작업 메뉴를 선택하세요.
2. *설정*을 선택하세요.
3. 파일만 복사, **ACL**만 복사, 파일 및 **ACL** 복사 중 하나를 선택하고 *계속*을 선택합니다.
4. *설정 저장*을 선택하세요.

복사 및 동기화 기능은 SMB ACL(권한)을 유지하지만 파일 또는 폴더의 소유권은 복사하지 않습니다. SMB ACL 이전 작업에는 소유권 정보가 포함되지 않습니다.

결과

데이터를 동기화할 때, 복사 및 동기화는 소스와 대상 간의 ACL을 보존합니다.

## SMB 공유 간 ACL을 수동으로 복사합니다.

Windows robocopy 명령을 사용하면 SMB 공유 간의 ACL을 수동으로 보존할 수 있습니다.

ACL 외에도 소유권(소유자 및 그룹)을 유지해야 하는 경우 다음을 사용할 수 있습니다. `robocopy` 명령. 사용 `/copyall` 플래그는 ACL, 소유권 및 감사 정보를 복사합니다.

단계

1. 두 SMB 공유에 대한 전체 액세스 권한이 있는 Windows 호스트를 식별합니다.
2. 두 엔드포인트 중 하나에 인증이 필요한 경우 **net use** 명령을 사용하여 Windows 호스트에서 엔드포인트에 연결합니다.

   Robocopy를 사용하기 전에 이 단계를 수행해야 합니다.

3. 복사 및 동기화에서 소스 및 대상 SMB 공유 간에 새 관계를 만들거나 기존 관계를 동기화합니다.
4. 데이터 동기화가 완료되면 Windows 호스트에서 다음 명령을 실행하여 ACL과 소유권을 동기화합니다.

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

_source_와 _target_은 모두 UNC 형식을 사용하여 지정해야 합니다. 예: \\<서버>\<공유>\<경로>

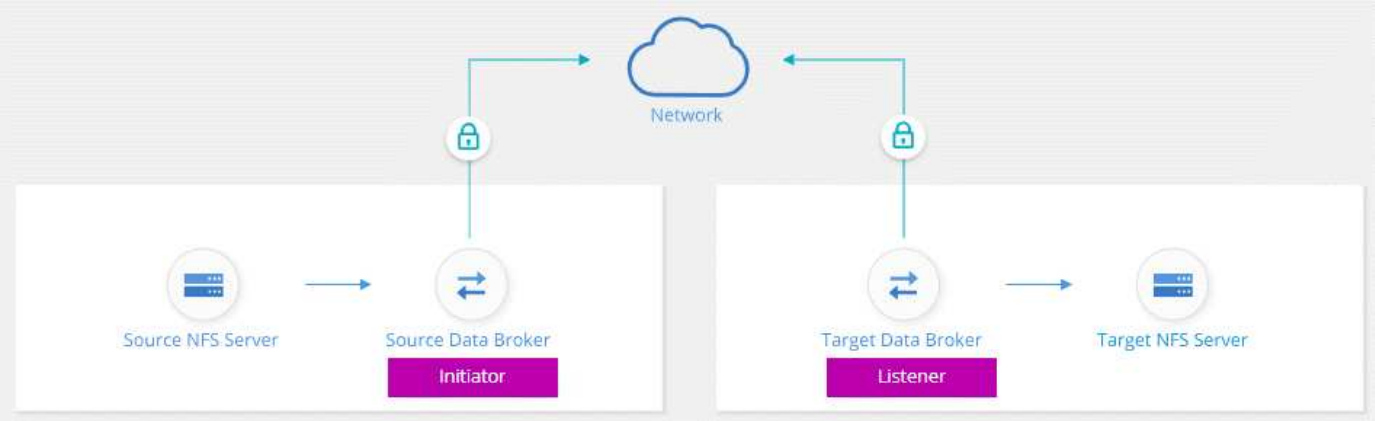
# NetApp Copy and Sync 에서 전송 중 데이터 암호화를 사용하여 NFS 데이터 동기화

회사에 엄격한 보안 정책이 있는 경우 NetApp Copy and Sync 의 전송 중 데이터 암호화를 사용하여 NFS 데이터를 동기화할 수 있습니다. 이 기능은 NFS 서버에서 다른 NFS 서버로, Azure NetApp Files 에서 Azure NetApp Files 로 지원됩니다.

예를 들어, 서로 다른 네트워크에 있는 두 개의 NFS 서버 간에 데이터를 동기화하고 싶을 수 있습니다. 또는 Azure NetApp Files 에서 서브넷이나 지역 간에 데이터를 안전하게 전송해야 할 수도 있습니다.

## 전송 중인 데이터 암호화 작동 방식

전송 중 데이터 암호화는 두 데이터 브로커 간 네트워크를 통해 전송되는 NFS 데이터를 암호화합니다. 다음 이미지는 두 개의 NFS 서버와 두 개의 데이터 브로커 간의 관계를 보여줍니다.




한 데이터 브로커는 개시자 역할을 합니다. 데이터를 동기화할 시간이 되면 다른 데이터 브로커, 즉 _리스너_에 연결 요청을 보냅니다. 해당 데이터 브로커는 포트 443에서 요청을 수신합니다. 필요한 경우 다른 포트를 사용할 수 있지만, 해당 포트가 다른 서비스에서 사용되고 있지 않은지 확인하세요.

예를 들어, 온프레미스 NFS 서버에서 클라우드 기반 NFS 서버로 데이터를 동기화하는 경우 연결 요청을 수신하는 데이터 브로커와 연결 요청을 보내는 데이터 브로커를 선택할 수 있습니다.

기내 암호화의 작동 방식은 다음과 같습니다.

1. 동기화 관계를 만든 후, 개시자는 다른 데이터 브로커와 암호화된 연결을 시작합니다.
2. 소스 데이터 브로커는 TLS 1.3을 사용하여 소스의 데이터를 암호화합니다.
3. 그런 다음 네트워크를 통해 대상 데이터 브로커로 데이터를 전송합니다.
4. 대상 데이터 브로커는 데이터를 대상에 전송하기 전에 암호를 해독합니다.

5. 최초 복사 후, 복사 및 동기화 기능은 변경된 데이터를 24시간마다 동기화합니다. 동기화할 데이터가 있는 경우, 시작자는 다른 데이터 브로커와 암호화된 연결을 열면서 프로세스가 시작됩니다.

   데이터를 더 자주 동기화하려는 경우"관계를 생성한 후 일정을 변경할 수 있습니다." .

## 지원되는 **NFS** 버전

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

## 프록시 서버 제한

암호화된 동기화 관계를 생성하면 암호화된 데이터는 HTTPS를 통해 전송되며 프록시 서버를 통해 라우팅될 수 없습니다.

## 시작하는 데 필요한 것

다음 사항을 꼭 확인하세요.

- 두 개의 NFS 서버가 충족합니다."소스 및 타겟 요구 사항" 또는 두 개의 서브넷이나 지역에 Azure NetApp Files .
- 서버의 IP 주소 또는 정규화된 도메인 이름입니다.
- 두 데이터 브로커의 네트워크 위치.

  기존 데이터 브로커를 선택할 수 있지만 해당 브로커가 개시자 역할을 해야 합니다. 리스너 데이터 브로커는 새로운 데이터 브로커여야 합니다.

  기존 데이터 브로커 그룹을 사용하려면 그룹에 데이터 브로커가 하나만 있어야 합니다. 그룹 내 여러 데이터 브로커는 암호화된 동기화 관계에서 지원되지 않습니다.

  아직 데이터 브로커를 배포하지 않았다면 데이터 브로커 요구 사항을 검토하세요. 엄격한 보안 정책이 있으므로 포트 443에서의 아웃바운드 트래픽을 포함한 네트워킹 요구 사항을 검토해야 합니다."인터넷 엔드포인트" 데이터 브로커가 연락하는 곳.

  - "AWS 설치 검토"
  - "Azure 설치 검토"
  - "Google Cloud 설치 검토"
  - "Linux 호스트 설치 검토"

## 데이터 전송 중 암호화를 사용하여 **NFS** 데이터 동기화

두 NFS 서버 간 또는 Azure NetApp Files 간에 새로운 동기화 관계를 만들고, 진행 중 암호화 옵션을 활성화한 다음, 화면의 지시를 따릅니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *새 동기화 만들기*를 선택합니다.

3. *NFS 서버*를 소스 및 대상 위치로 끌어다 놓거나 * Azure NetApp Files*를 소스 및 대상 위치로 끌어다 놓고 *예*를 선택하여 전송 중인 데이터 암호화를 활성화합니다.
4. 다음 지시에 따라 관계를 생성하세요.

   a. **NFS** 서버/* Azure NetApp Files*: NFS 버전을 선택한 다음 새 NFS 소스를 지정하거나 기존 서버를 선택합니다.

   b. 데이터 브로커 기능 정의: 포트에서 연결 요청을 _수신_하는 데이터 브로커와 연결을 _시작_하는 데이터 브로커를 정의합니다. 귀하의 네트워킹 요구 사항에 따라 선택하세요.

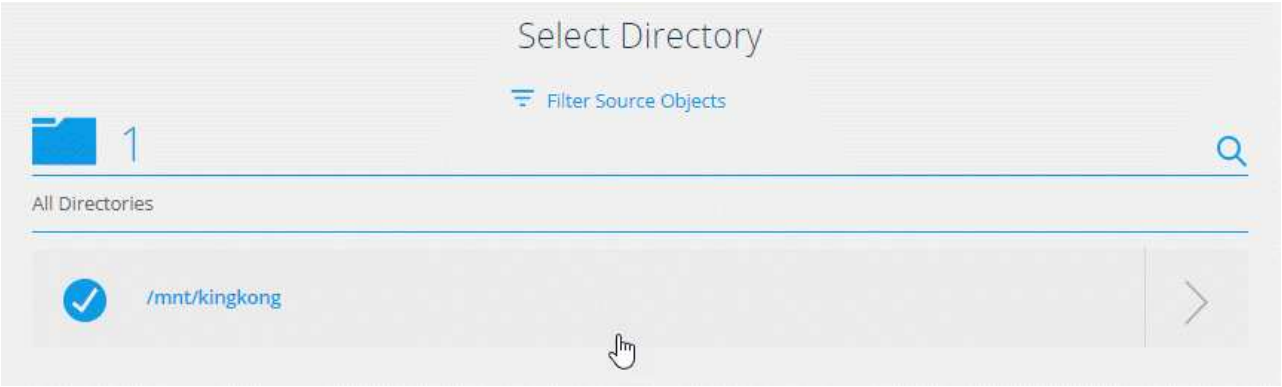
   c. 데이터 브로커: 메시지에 따라 새로운 소스 데이터 브로커를 추가하거나 기존 데이터 브로커를 선택합니다.

      다음 사항에 유의하세요.

      - 기존 데이터 브로커 그룹을 사용하려면 그룹에 데이터 브로커가 하나만 있어야 합니다. 그룹 내 여러 데이터 브로커는 암호화된 동기화 관계에서 지원되지 않습니다.
      - 소스 데이터 브로커가 리스너 역할을 하는 경우 새로운 데이터 브로커여야 합니다.
      - 새로운 데이터 브로커가 필요한 경우 Copy and Sync에서 설치 지침을 안내합니다. 클라우드에 데이터 브로커를 배포하거나 자체 Linux 호스트에 대한 설치 스크립트를 다운로드할 수 있습니다.

   d. 디렉토리: 모든 디렉토리를 선택하거나, 드릴다운하여 하위 디렉토리를 선택하여 동기화할 디렉토리를 선택합니다.

      *소스 개체 필터링*을 선택하여 소스 파일과 폴더가 대상 위치에서 동기화되고 유지되는 방식을 정의하는 설정을 수정합니다.

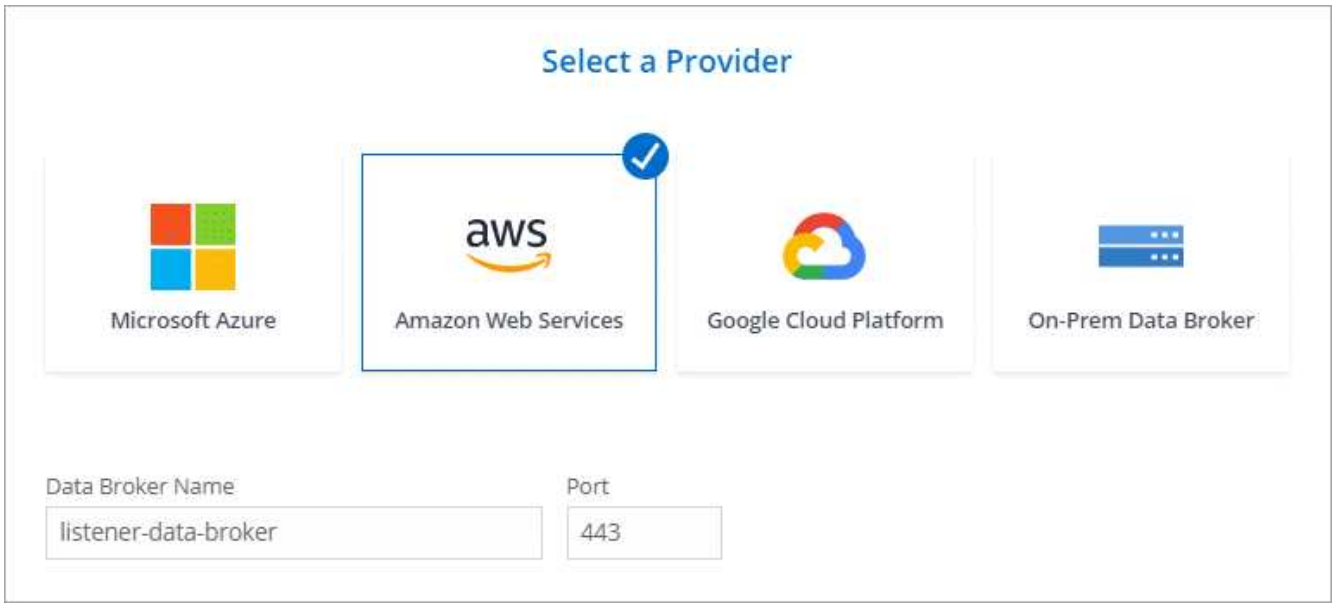



   e. 대상 **NFS** 서버/대상 **Azure NetApp Files**: NFS 버전을 선택한 다음 새 NFS 대상을 입력하거나 기존 서버를 선택합니다.

   f. 대상 데이터 브로커: 메시지에 따라 새로운 소스 데이터 브로커를 추가하거나 기존 데이터 브로커를 선택합니다.

      대상 데이터 브로커가 리스너 역할을 하는 경우 새로운 데이터 브로커여야 합니다.

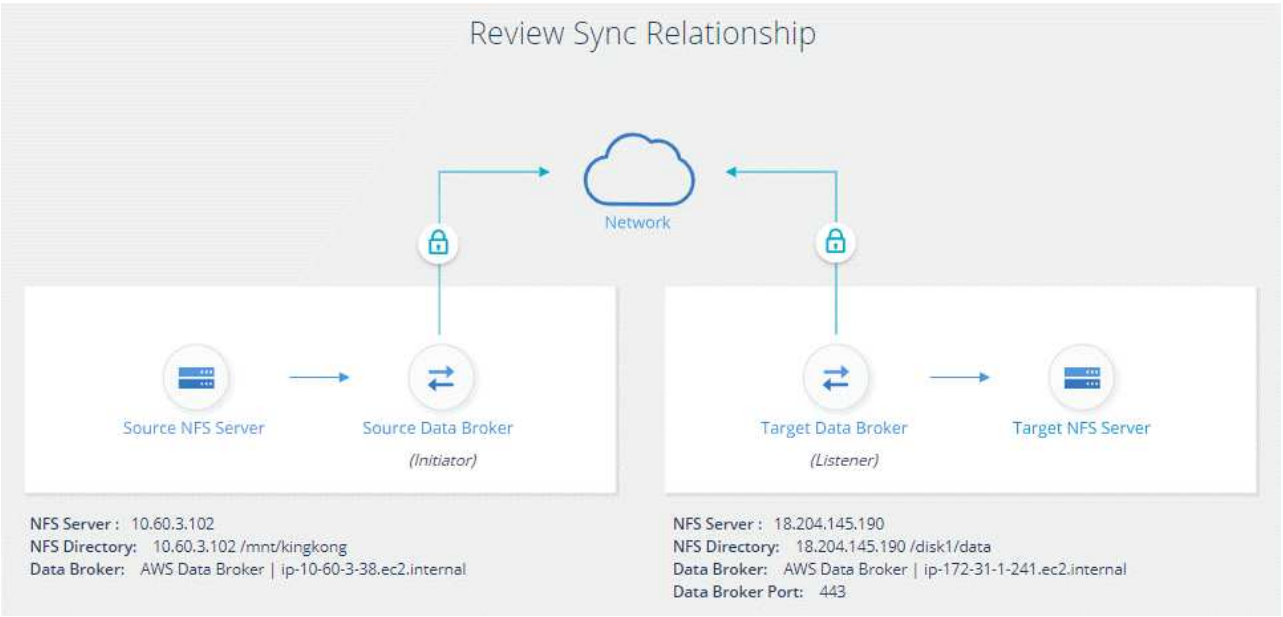
      대상 데이터 브로커가 리스너 역할을 할 때 나타나는 프롬프트의 예는 다음과 같습니다. 포트를 지정하는 옵션에 주목하세요.




a. 대상 디렉토리: 최상위 디렉토리를 선택하거나, 드릴다운하여 기존 하위 디렉토리를 선택하거나, 내보내기 내에 새 폴더를 만듭니다.

b. 설정: 소스 파일과 폴더가 대상 위치에서 동기화되고 유지되는 방식을 정의합니다.

c. 검토: 동기화 관계의 세부 정보를 검토한 다음 *관계 만들기*를 선택합니다.




결과

복사 및 동기화를 통해 새로운 동기화 관계가 생성됩니다. 완료되면 *대시보드에서 보기*를 선택하여 새 관계에 대한 세부 정보를 확인하세요.

# NetApp Copy and Sync 에서 외부 HashiCorp Vault를 사용하도록 데이터 브로커 그룹 설정

Amazon S3, Azure 또는 Google Cloud 자격 증명이 필요한 동기화 관계를 만드는 경우

NetApp Copy and Sync 사용자 인터페이스 또는 API를 통해 해당 자격 증명을 지정해야 합니다. 또 다른 방법은 데이터 브로커 그룹을 설정하여 외부 HashiCorp Vault에서 직접 자격 증명(또는 비밀)에 액세스하는 것입니다.

이 기능은 Amazon S3, Azure 또는 Google Cloud 자격 증명이 필요한 동기화 관계를 갖춘 Copy and Sync API를 통해 지원됩니다.

1 금고를 준비하세요

URL을 설정하여 데이터 브로커 그룹에 자격 증명을 제공하도록 볼트를 준비합니다. 보관소의 비밀에 대한 URL은 _Creds_로 끝나야 합니다.

2 데이터 브로커 그룹 준비

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

3 **API**를 사용하여 동기화 관계 만들기

이제 모든 것이 설정되었으므로 API 호출을 보내 볼트를 사용하여 비밀을 가져오는 동기화 관계를 만들 수 있습니다.

## 금고를 준비하세요

보관소에 있는 비밀의 URL을 복사하여 동기화해야 합니다. 해당 URL을 설정하여 볼트를 준비합니다. 만들려는 동기화 관계의 각 소스 및 대상에 대한 자격 증명에 대한 URL을 설정해야 합니다.

URL은 다음과 같이 설정해야 합니다.

```
/<path>/<requestid>/<endpoint-protocol>Creds
```

길
: 비밀에 대한 접두사 경로입니다. 이는 귀하에게만 고유한 값이 될 수 있습니다.

요청 **ID**
: 생성해야 하는 요청 ID입니다. 동기화 관계를 만들 때 API POST 요청의 헤더 중 하나에 ID를 제공해야 합니다.

엔드포인트 프로토콜
: 다음 프로토콜 중 하나, 정의된 대로 "관계 v2 문서 게시" : S3, AZURE 또는 GCP(각각 대문자여야 함).

신용
: URL은 _Creds_로 끝나야 합니다.

예시

다음 예에서는 비밀에 대한 URL을 보여줍니다.

소스 자격 증명에 대한 전체 **URL** 및 경로의 예

\ http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds 모든 비밀/hb312vdasr2/S3Creds

예시에서 볼 수 있듯이 접두사 경로는 _/my-path/all-secrets/_이고, 요청 ID는 _hb312vdasr2_이며, 소스 엔드포인트는 S3입니다.

대상 자격 증명에 대한 전체 **URL** 및 경로의 예

\ http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds 모든 비밀/n32hcbnejk2/AZURECreds

접두사 경로는 _/my-path/all-secrets/_이고, 요청 ID는 _n32hcbnejk2_이며, 대상 엔드포인트는 Azure입니다.

## 데이터 브로커 그룹 준비

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

단계

1. 그룹 내 데이터 브로커에 SSH를 실행합니다.
2. /opt/netapp/databroker/config에 있는 local.json 파일을 편집합니다.
3. enable을 *true*로 설정하고 *external-integrations.hashicorp* 아래의 구성 매개변수 필드를 다음과 같이 설정합니다.

   활성화됨
   - 유효한 값: true/false
   - 유형: 부울
   - 기본값: false
   - 사실: 데이터 브로커는 귀하의 외부 HashiCorp Vault에서 비밀을 얻습니다.
   - 거짓: 데이터 브로커는 로컬 볼트에 자격 증명을 저장합니다.

   **URL**
   - 유형: 문자열
   - 값: 외부 볼트에 대한 URL

   길
   - 유형: 문자열
   - 값: 자격 증명을 사용하여 비밀에 대한 접두사 경로

   거부-무단
   - 데이터 브로커가 승인되지 않은 외부 볼트를 거부할지 여부를 결정합니다.
   - 유형: 부울
   - 기본값: false

인증 방법
- 데이터 브로커가 외부 볼트에서 자격 증명에 액세스하는 데 사용해야 하는 인증 방법
- 유형: 문자열
- 유효한 값: "aws-iam" / "role-app" / "gcp-iam"

역할 이름
- 유형: 문자열
- 역할 이름(aws-iam 또는 gcp-iam을 사용하는 경우)

비밀 **ID** 및 루트 **ID**
- 유형: 문자열(app-role을 사용하는 경우)

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

4. 그룹 내의 다른 데이터 브로커에 대해서도 이 단계를 반복합니다.

**aws-role** 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** 인증을 사용할 때 권한 설정

*gcp-iam* 인증 방법을 사용하는 경우 데이터 브로커에 다음과 같은 GCP 권한이 있어야 합니다.

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

"데이터 브로커에 대한 GCP 권한 요구 사항에 대해 자세히 알아보세요." .

## 볼트의 비밀을 사용하여 새로운 동기화 관계 만들기

이제 모든 것이 설정되었으므로 API 호출을 보내 볼트를 사용하여 비밀을 가져오는 동기화 관계를 만들 수 있습니다.

Copy and 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 토큰과 NetApp Console 계정 ID를 얻으려면"설명서의 이 페이지를 참조하세요" .
- 게시물 관계에 대한 신체를 구축하려면 "관계-v2 API 호출을 참조하세요." .

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"
        }
    }
}
```