



# **NetApp Copy and Sync 사용**

## NetApp Copy and Sync

NetApp  
December 16, 2025

# 목차

NetApp Copy and Sync 사용	1
소스와 대상 간 데이터 동기화	1
NetApp Copy and Sync에서 개체 스토리지 간 데이터를 동기화하기 위한 데이터 브로커 준비	1
NetApp Copy and Sync에서 동기화 관계 만들기	1
NetApp Copy and Sync에서 SMB 공유의 ACL 복사	9
NetApp Copy and Sync에서 전송 중 데이터 암호화를 사용하여 NFS 데이터 동기화	12
NetApp Copy and Sync에서 외부 HashiCorp Vault를 사용하도록 데이터 브로커 그룹 설정	15
NetApp Copy and Sync 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불하세요.	21
AWS 구독	21
Azure에서 구독	21
NetApp에서 라이센스를 구매하고 Copy and Sync에 추가합니다.	22
라이센스 업데이트	22
NetApp Copy and Sync에서 동기화 관계 관리	23
즉각적인 데이터 동기화를 수행합니다.	23
동기화 성능 가속화	23
자격 증명 업데이트	24
알림 설정	25
동기화 관계에 대한 설정 변경	26
관계 삭제	29
NetApp Copy and Sync에서 데이터 브로커 그룹 관리	30
데이터 브로커 그룹의 작동 방식	30
보안 권장 사항	31
그룹에 새로운 데이터 브로커 추가	31
그룹 이름 편집	32
통합 구성 설정	33
그룹 간 데이터 브로커 이동	33
프록시 구성 업데이트	34
데이터 브로커 구성 보기	34
데이터 브로커와 문제 해결	35
그룹에서 데이터 브로커 제거	36
데이터 브로커 그룹 삭제	37
NetApp Copy and Sync에서 구성은 조정하기 위한 보고서를 만들고 봅니다.	38
보고서 만들기	38
보고서 다운로드	40
보고서 오류 보기	41
보고서 삭제	41
NetApp Copy and Sync 용 데이터 브로커 제거	41

# NetApp Copy and Sync 사용

## 소스와 대상 간 데이터 동기화

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

NetApp Copy and Sync에서 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 구성의 설정을 수정해야 합니다. 설정을 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 구성의 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 구성의 업데이트입니다.

다음은 무엇인가요?

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

## NetApp Copy and Sync에서 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 Console에서 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.

The screenshot shows the Canvas interface with a Cloud Volumes ONTAP system configuration. The system is labeled "CloudVolumesONTAP" with "On" status. It has four settings: Compliance (Off), Monitoring (On), File Cache (Off), and Sync (On). The Sync section shows 559.16TiB Data Synced. A hand cursor is hovering over the Sync button.

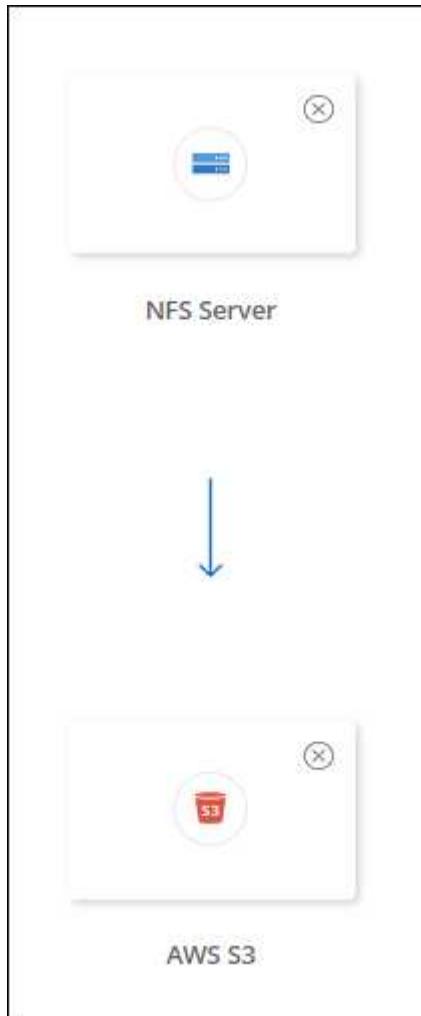
6. 이 위치에서 데이터 동기화 또는 \*이 위치에 데이터 동기화\*를 선택하고 화면의 지시에 따라 동기화 관계를 설정합니다.

## 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 Console에서 \*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.

1 Data Broker Group			
	Data Broker Group 1		
2 Data Brokers	1.81 KB/s Transfer Rate	1 Relationships	2 Active Data Brokers Status

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.



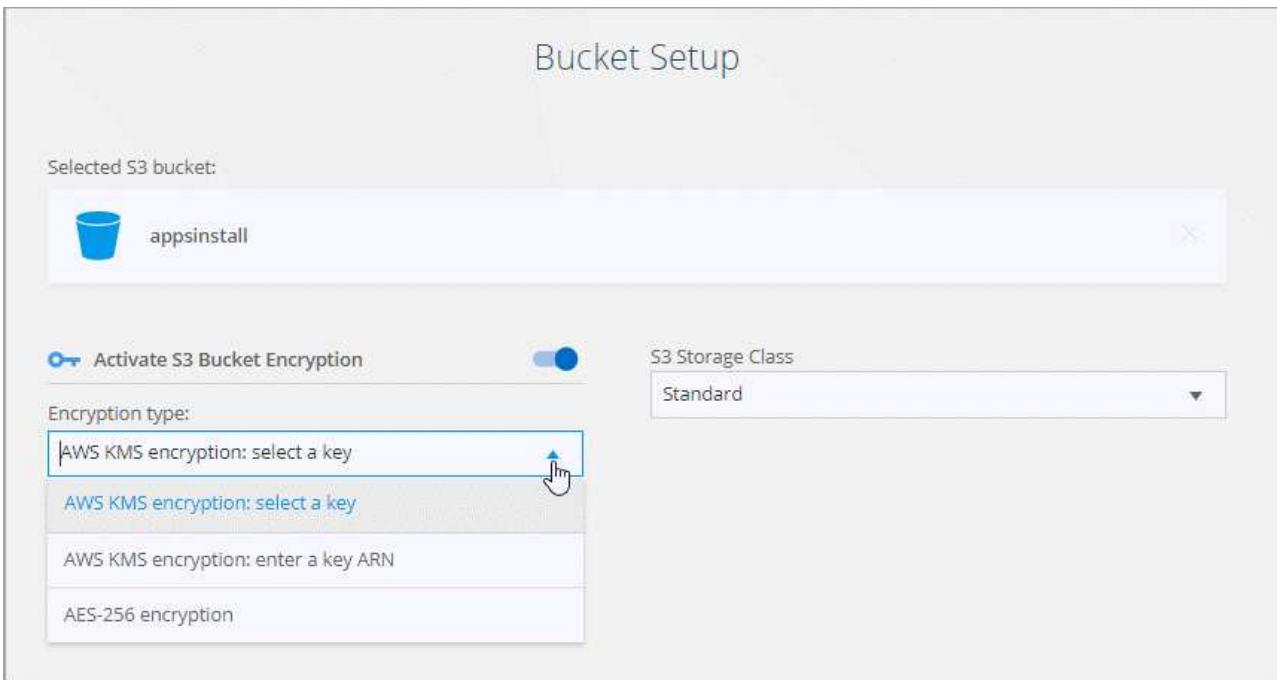
NFS 서버에서 두 개 이상의 디렉토리를 동기화하려면 작업을 마친 후 추가 동기화 관계를 만들어야 합니다.

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 StorageGRID로 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.

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

The screenshot shows the 'Relationship Tags' configuration page for an AWS S3 Bucket. At the top, there are tabs: 'AWS S3 Bucket' (selected), 'Settings' (with a checkmark), 'Tags/Metadata' (with a blue circle containing the number 6), and 'Review' (with a blue circle containing the number 7). Below the tabs, the section title 'Relationship Tags' is displayed. A descriptive text states: '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.' There are two radio button options: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below these options are input fields for 'Tag Key' and 'Tag Value', both with character limits of up to 128 and 256 respectively. At the bottom left is a button '+ Add Relationship Tag' and at the bottom right is a note 'Optional Field | [Up to 5]'. The entire interface has a clean, modern design with blue and white colors.



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.

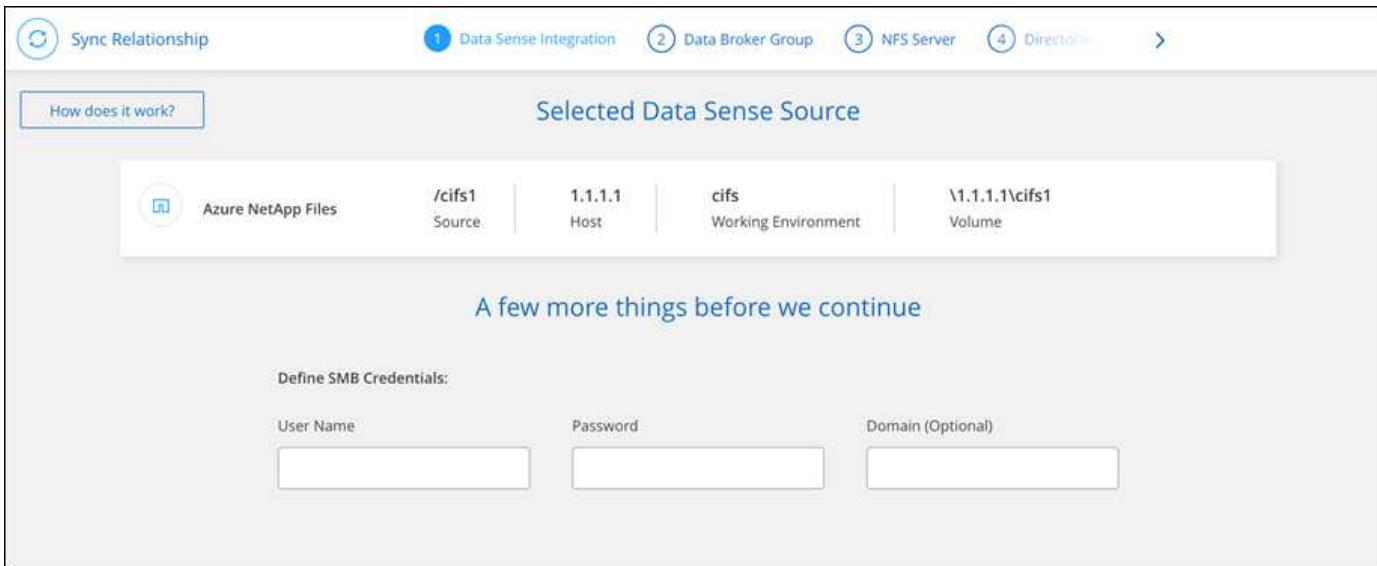
#### 결과

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 Classification에서 동기화 관계 만들기

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

NetApp Data Classification에서 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 Classification에서 동기화 관계를 시작하는 방법을 알아보세요." .

#### NetApp Copy and Sync에서 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

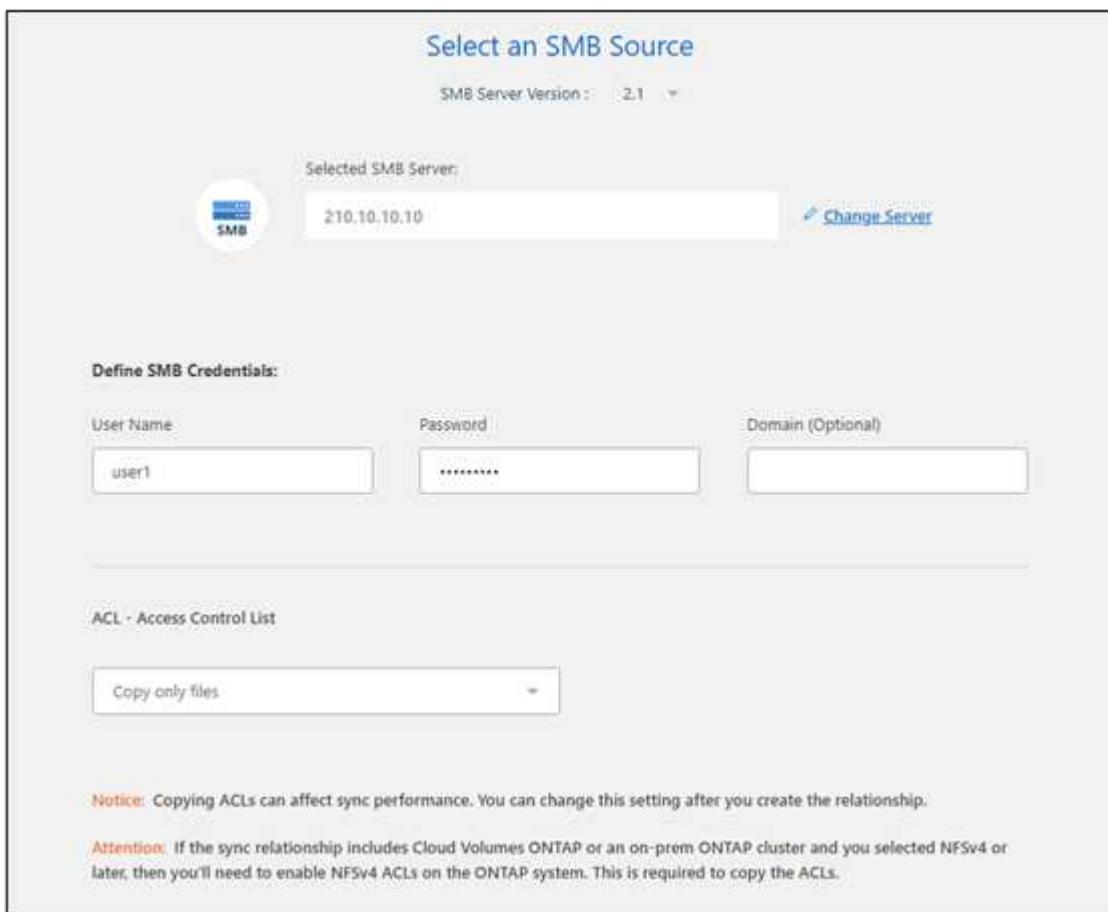
관계를 생성할 때 또는 관계를 생성한 후에 설정을 활성화하여 SMB 공유 간, 그리고 SMB 공유와 개체 스토리지 간에 ACL을 복사합니다.

#### 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. 스스로 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.

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 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 **ACL**을 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:"[filepath]"
```

\_source\_와 \_target\_은 모두 UNC 형식을 사용하여 지정해야 합니다. 예: \\<서버>\<공유>\<경로>

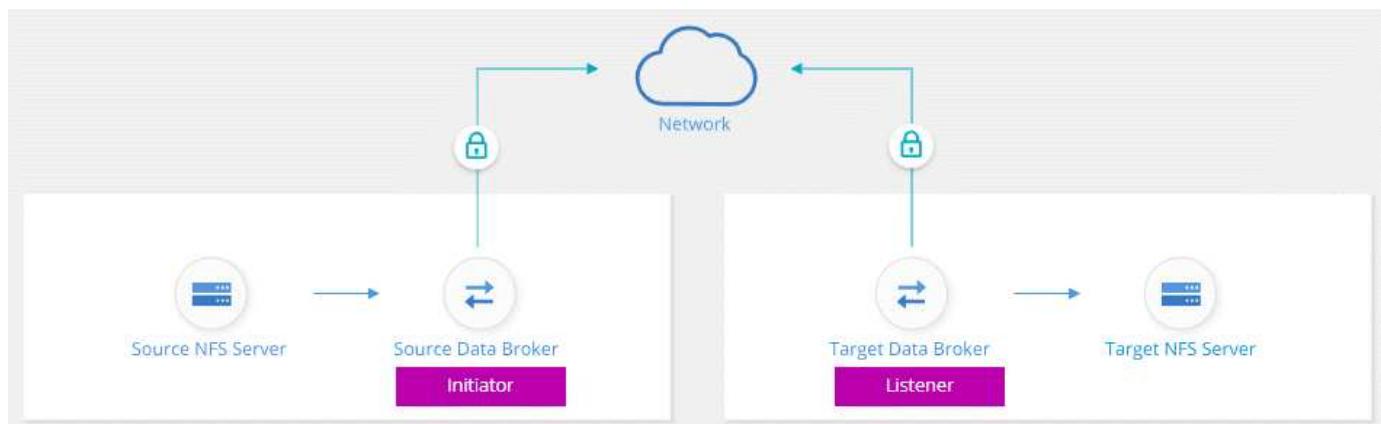
## NetApp Copy and Sync에서 전송 중 데이터 암호화를 사용하여 NFS 데이터 동기화

회사에 엄격한 보안 정책이 있는 경우 NetApp Copy and Sync의 전송 중 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 개의 NFS 서버 간에 데이터를 동기화하고 싶을 수 있습니다. 또는 Azure NetApp Files에서 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

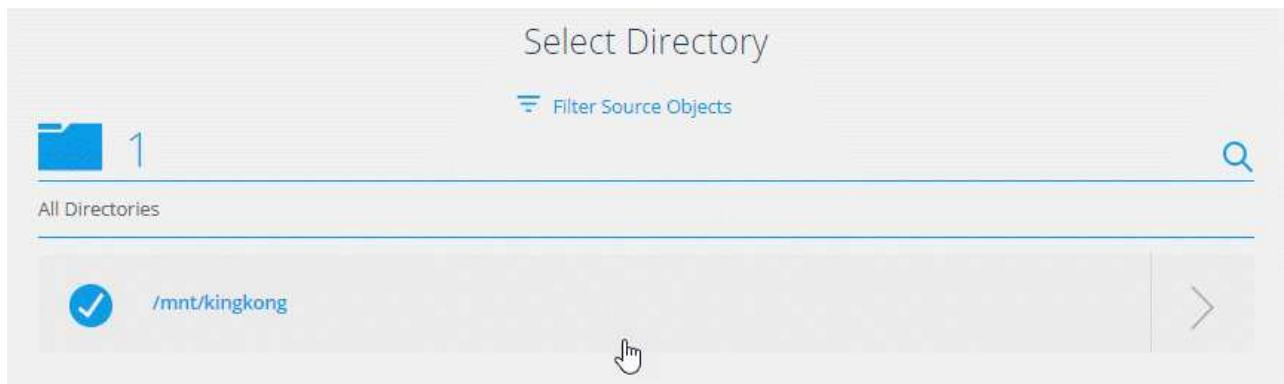
1. "[복사 및 동기화에 로그인하세요](#)" .
2. \*새 동기화 만들기\*를 선택합니다.
3. \*NFS 서버\*를 소스 및 대상 위치로 끌어다 놓거나 \* Azure NetApp Files\*를 소스 및 대상 위치로 끌어다 놓고 \*예 \*를 선택하여 전송 중인 데이터 암호화를 활성화합니다.
4. 다음 지시에 따라 관계를 생성하세요.

- 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.

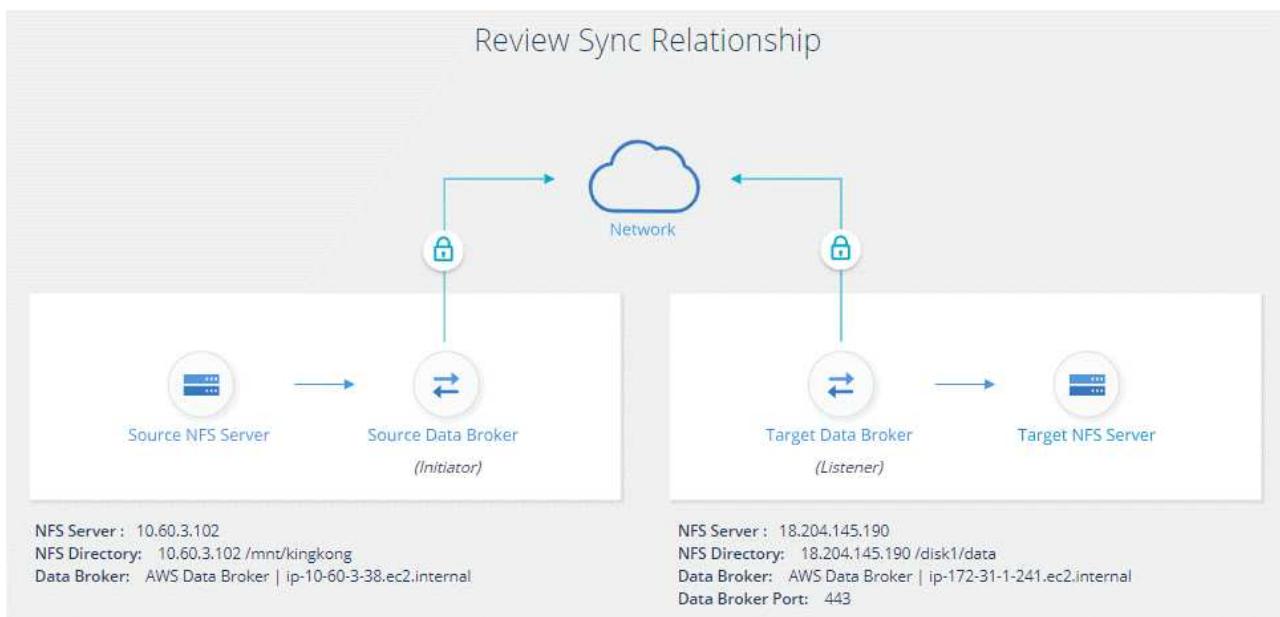
Select a Provider

Microsoft Azure	Amazon Web Services	Google Cloud Platform	On-Prem Data Broker

Data Broker Name: listener-data-broker

Port: 443

- 대상 디렉토리: 최상위 디렉토리를 선택하거나, 드릴다운하여 기존 하위 디렉토리를 선택하거나, 내보내기 내에 새 폴더를 만듭니다.
- 설정: 소스 파일과 폴더가 대상 위치에서 동기화되고 유지되는 방식을 정의합니다.
- 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

API를 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"
      }
    }
  }
}

```

# **NetApp Copy and Sync 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불하세요.**

NetApp Copy and Sync 14일 무료 평가판이 종료된 후에는 동기화 관계에 대한 비용을 두 가지 방법으로 지불할 수 있습니다. 첫 번째 옵션은 AWS 또는 Azure에 가입하여 사용량에 따라 요금을 지불하거나 연간 요금을 지불하는 것입니다. 두 번째 옵션은 NetApp에서 직접 라이선스를 구매하는 것입니다.

AWS Marketplace나 Azure Marketplace에서 구독할 수 있습니다. 두 곳 모두에서 구독할 수는 없습니다.

마켓플레이스 구독을 통해 NetApp 라이선스를 사용할 수 있습니다. 예를 들어, 동기화 관계가 25개라면 라이선스를 사용하여 처음 20개 동기화 관계에 대한 요금을 지불한 다음, 나머지 5개 동기화 관계에 대해서는 AWS 또는 Azure에서 사용량에 따라 요금을 지불할 수 있습니다.

["라이센스 작동 방식에 대해 자세히 알아보세요".](#)

무료 체험 기간이 종료된 후 즉시 결제하지 않으면 추가 관계를 생성할 수 없습니다. 기존 관계는 삭제되지 않지만, 구독하거나 라이선스를 입력하기 전까지는 관계를 변경할 수 없습니다.

라이선스는 NetApp Copy and Sync 또는 해당 웹사이트를 통해 관리해야 하며 NetApp Console 구독을 통해서는 관리하지 않습니다.

## **AWS 구독**

AWS를 사용하면 사용량에 따라 비용을 지불하거나 연간으로 지불할 수 있습니다.

사용량에 따른 결제 단계

1. NetApp Console 탐색 메뉴에서 \*모빌리티 > 복사 및 동기화\*를 선택합니다.
2. \*라이선스\*를 선택하세요.
3. \*AWS\*을 선택하세요.
4. \*구독\*을 선택한 다음 \*계속\*을 선택하세요.
5. AWS Marketplace에서 구독한 다음 Copy and Sync에 다시 로그인하여 등록을 완료하세요.

다음 영상은 그 과정을 보여줍니다.

[AWS Marketplace에서 복사 및 동기화 구독](#)

연간 지불 단계

1. ["AWS Marketplace 페이지로 이동"](#).
2. \*구독 계속하기\*를 선택하세요.
3. 계약 옵션을 선택한 다음 \*계약 생성\*을 선택하세요.

## **Azure에서 구독**

Azure를 사용하면 사용량에 따라 요금을 지불하거나 연간 요금을 지불할 수 있습니다.

## 필요한 것

해당 구독에 대한 기여자 또는 소유자 권한이 있는 Azure 사용자 계정입니다.

## 단계

1. NetApp Console 탐색 메뉴에서 \*모빌리티 > 복사 및 동기화\*를 선택합니다.
2. \*라이선스\*를 선택하세요.
3. \*Azure\*를 선택하세요.
4. \*구독\*을 선택한 다음 \*계속\*을 선택하세요.
5. Azure Portal에서 \*만들기\*를 선택하고 옵션을 선택한 다음 \*구독\*을 선택합니다.

시간당으로 결제하려면 \*월별\*을 선택하고, 1년치를 선불하려면 \*연별\*을 선택하세요.

6. 배포가 완료되면 알림 팝업에서 SaaS 리소스 이름을 선택합니다.
7. 복사 및 동기화로 돌아가려면 \*계정 구성\*을 선택하세요.

다음 영상은 그 과정을 보여줍니다.

## Azure Marketplace에서 복사 및 동기화 구독

### NetApp에서 라이센스를 구매하고 Copy and Sync에 추가합니다.

동기화 관계에 대한 비용을 선불로 지불하려면 하나 이상의 라이선스를 구매하여 Copy and Sync에 추가해야 합니다.

## 필요한 것

라이선스의 일련 번호와 라이선스가 연결된 NetApp 지원 사이트 계정의 사용자 이름과 비밀번호가 필요합니다.

## 단계

1. [NetApp에 문의](#)로 라이선스를 구매하세요.
2. ["복사 및 동기화에 로그인하세요"](#).
3. \*라이선스\*를 선택하세요.
4. \*라이선스 추가\*를 선택하고 필요한 정보를 추가하세요.
  - a. 일련번호를 입력하세요.
  - b. 추가하려는 라이선스와 연결된 NetApp 지원 사이트 계정을 선택하세요.
    - 계정이 이미 NetApp Console에 추가된 경우 드롭다운 목록에서 해당 계정을 선택하세요.
    - 아직 계정이 추가되지 않은 경우 \*NSS 자격 증명 추가\*를 선택하고 사용자 이름과 비밀번호를 입력한 다음 \*등록\*을 선택하고 드롭다운 목록에서 해당 계정을 선택하세요.
  - c. \*추가\*를 선택하세요.

## 라이센스 업데이트

NetApp에서 구매한 복사 및 동기화 라이선스를 연장한 경우, 새로운 만료 날짜가 복사 및 동기화에서 자동으로 업데이트되지 않습니다. 만료 날짜를 새로 고치려면 라이선스를 다시 추가해야 합니다. 라이선스는 NetApp Console 구독이 아닌 Copy and Sync 또는 해당 웹사이트를 통해 관리해야 합니다.

#### 단계

1. NetApp Console 탐색 메뉴에서 \*모빌리티 > 복사 및 동기화\*를 선택합니다.
2. \*라이선스\*를 선택하세요.
3. \*라이선스 추가\*를 선택하고 필요한 정보를 추가하세요.
  - a. 일련번호를 입력하세요.
  - b. 추가하려는 라이선스와 연결된 NetApp 지원 사이트 계정을 선택하세요.
  - c. \*추가\*를 선택하세요.

#### 결과

복사 및 동기화는 기존 라이센스를 새로운 만료 날짜로 업데이트합니다.

## NetApp Copy and Sync 에서 동기화 관계 관리

NetApp Copy and Sync에서 데이터를 즉시 동기화하고, 일정을 변경하는 등 언제든지 동기화 관계를 관리할 수 있습니다.

즉각적인 데이터 동기화를 수행합니다.

다음에 예약된 동기화를 기다리지 않고도 소스와 대상 간에 데이터를 즉시 동기화할 수 있습니다.

#### 단계

1. ["복사 및 동기화에 로그인하세요"](#).
2. \*대시보드\*에서 동기화 관계로 이동하여 다음을 선택합니다. 
3. \*지금 동기화\*를 선택한 다음 \*동기화\*를 선택하여 확인합니다.

#### 결과

복사 및 동기화는 관계에 대한 데이터 동기화 프로세스를 시작합니다.

## 동기화 성능 가속화

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

#### 작동 원리

데이터 브로커 그룹이 다른 동기화 관계를 관리하는 경우 그룹에 추가하는 새 데이터 브로커도 해당 동기화 관계의 성능을 가속화합니다.

예를 들어, 세 가지 관계가 있다고 가정해 보겠습니다.

- 관계 1은 데이터 브로커 그룹 A에 의해 관리됩니다.
- 관계 2는 데이터 브로커 그룹 B에서 관리합니다.
- 관계 3은 데이터 브로커 그룹 A에서 관리합니다.

관계 1의 성능을 가속화하기 위해 데이터 브로커 그룹 A에 새로운 데이터 브로커를 추가합니다. 그룹 A는 동기화 관계 3도 관리하므로 관계에 대한 동기화 성능도 자동으로 가속화됩니다.

#### 단계

1. 관계에 있는 기존 데이터 브로커 중 하나 이상이 온라인 상태인지 확인하세요.
2. \*대시보드\*에서 동기화 관계로 이동하여 다음을 선택합니다. 
3. \*가속\*을 선택하세요.
4. 화면의 지시에 따라 새로운 데이터 브로커를 생성하세요.

#### 결과

복사 및 동기화는 그룹에 새로운 데이터 브로커를 추가합니다. 다음 데이터 동기화의 성능이 가속화되어야 합니다.

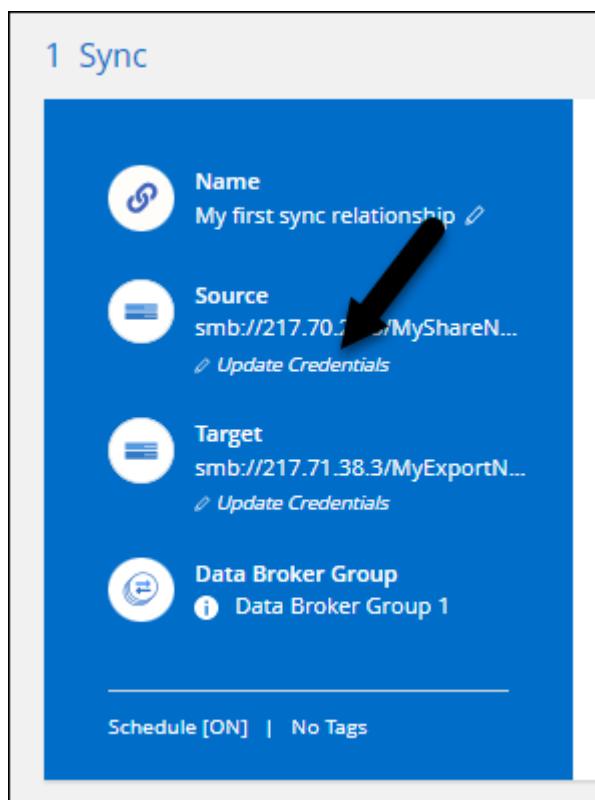
### 자격 증명 업데이트

기존 동기화 관계에서 소스 또는 대상의 최신 자격 증명으로 데이터 브로커를 업데이트할 수 있습니다. 보안 정책에 따라 주기적으로 자격 증명을 업데이트해야 하는 경우 자격 증명을 업데이트하면 도움이 될 수 있습니다.

자격 증명 업데이트는 Copy and Sync에 자격 증명이 필요한 모든 소스 또는 대상(Azure Blob, Box, IBM Cloud Object Storage, StorageGRID, ONTAP S3 Storage, SFTP 및 SMB 서버)에서 지원됩니다.

#### 단계

1. \*동기화 대시보드\*에서 자격 증명이 필요한 동기화 관계로 이동한 다음 \*자격 증명 업데이트\*를 선택합니다.



2. 자격 증명을 입력하고 \*업데이트\*를 선택하세요.

SMB 서버에 대한 참고 사항: 도메인이 새 것이라면 자격 증명을 업데이트할 때 해당 도메인을 지정해야 합니다.

도메인이 변경되지 않았다면 다시 입력할 필요가 없습니다.

동기화 관계를 생성할 때 도메인을 입력했지만 자격 증명을 업데이트할 때 새 도메인을 입력하지 않으면 복사 및 동기화는 사용자가 제공한 원래 도메인을 계속 사용합니다.

## 결과

복사 및 동기화는 데이터 브로커의 자격 증명을 업데이트합니다. 데이터 브로커가 업데이트된 자격 증명을 사용하여 데이터 동기화를 시작할 때까지 최대 10분이 걸릴 수 있습니다.

## 알림 설정

각 동기화 관계에 대한 알림 설정을 사용하면 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.

The screenshot shows the NetApp Cloud Sync Notifications page. At the top, there are account, workspace, and connector dropdowns, followed by a notifications icon with a red badge indicating 9 notifications. Below the header, there are filters for services and types. A single notification is listed: "Cloud Sync relationship completed" (with an info icon), which was received "5 minutes ago | Cloud Sync". There is a "Go to the relationship" button and a more options menu (three dots) next to the notification.

또한, 이메일로 알림을 받으실 수도 있습니다.

## 단계

1. 동기화 관계에 대한 설정을 수정합니다.
  - a. \*대시보드\*에서 동기화 관계로 이동하여 다음을 선택합니다. 
  - b. \*설정\*을 선택하세요.
  - c. \*알림\*을 활성화하세요.
  - d. \*설정 저장\*을 선택하세요.
2. 이메일로 알림을 받으려면 알림 및 알림 설정을 구성하세요.
  - a. \*설정 > 알림 및 알림 설정\*을 선택하세요.
  - b. 사용자 한 명 또는 여러 사용자를 선택하고 정보 알림 유형을 선택하세요.
  - c. \*적용\*을 선택하세요.

## 결과

이제 NetApp 콘솔의 알림 센터에서 복사 및 동기화 알림을 받게 되며, 해당 옵션을 구성한 경우 일부 알림은 이메일로 도착합니다.

## 동기화 관계에 대한 설정 변경

대상 위치에서 소스 파일과 폴더가 동기화되고 유지되는 방식을 정의하는 설정을 수정합니다.

1. \*대시보드\*에서 동기화 관계로 이동하여 다음을 선택합니다. 
2. \*설정\*을 선택하세요.
3. 설정을 수정합니다.

**General**

Schedule	ON   Every 1 Day	▼
Retries	Retry 3 times before skipping file	▼
<b>Files and Directories</b>		
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	▼
<a href="#"> Reset to defaults</a>		▼

각 설정에 대한 간략한 설명은 다음과 같습니다.

#### 일정

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

#### 동기화 시간 초과

동기화가 지정된 시간(분, 시간 또는 일) 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.

알림을 받으려면

재시도

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

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

관계를 만든 후에는 이 옵션을 편집할 수 없습니다.

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. 기본값은 대상 위치에서 파일을 삭제하지 않는 것입니다.

## 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.

## 4. \*설정 저장\*을 선택하세요.

## 결과

복사 및 동기화는 새로운 설정으로 동기화 관계를 수정합니다.

## 관계 삭제

더 이상 소스와 대상 간에 데이터를 동기화할 필요가 없으면 동기화 관계를 삭제할 수 있습니다. 이 작업은 데이터 브로커 그룹(또는 개별 데이터 브로커 인스턴스)을 삭제하지 않으며 대상에서 데이터를 삭제하지 않습니다.

## 옵션 1: 단일 동기화 관계 삭제

단계

1. \*대시보드\*에서 동기화 관계로 이동하여 다음을 선택합니다. 
2. \*삭제\*를 선택한 다음 다시 \*삭제\*를 선택하여 확인합니다.

결과

복사 및 동기화는 동기화 관계를 삭제합니다.

## 옵션 2: 여러 동기화 관계 삭제

단계

1. \*대시보드\*에서 "새 동기화 만들기" 버튼으로 이동하여 선택하세요. 
2. 삭제하려는 동기화 관계를 선택하고, \*삭제\*를 선택한 다음, 다시 \*삭제\*를 선택하여 확인합니다.

결과

복사 및 동기화는 동기화 관계를 삭제합니다.

## NetApp Copy and Sync 에서 데이터 브로커 그룹 관리

NetApp Copy and Sync 의 데이터 브로커 그룹은 소스 위치에서 대상 위치로 데이터를 동기화합니다. 생성하는 각 동기화 관계에는 그룹에 하나 이상의 데이터 브로커가 필요합니다. 그룹에 새로운 데이터 브로커를 추가하고, 그룹에 대한 정보를 보는 등 데이터 브로커 그룹을 관리합니다.

### 데이터 브로커 그룹의 작동 방식

데이터 브로커 그룹에는 하나 이상의 데이터 브로커가 포함될 수 있습니다. 데이터 브로커를 그룹화하면 동기화 관계의 성능을 개선하는 데 도움이 될 수 있습니다.

그룹은 여러 관계를 관리할 수 있습니다.

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

예를 들어, 세 가지 관계가 있다고 가정해 보겠습니다.

- 관계 1은 데이터 브로커 그룹 A에 의해 관리됩니다.
- 관계 2는 데이터 브로커 그룹 B에서 관리합니다.
- 관계 3은 데이터 브로커 그룹 A에서 관리합니다.

관계 1의 성능을 가속화하기 위해 데이터 브로커 그룹 A에 새로운 데이터 브로커를 추가합니다. 그룹 A는 동기화 관계 3도 관리하므로 관계에 대한 동기화 성능도 자동으로 가속화됩니다.

## 그룹 내 데이터 브로커 수

많은 경우, 단일 데이터 브로커가 동기화 관계에 대한 성능 요구 사항을 충족할 수 있습니다. 그렇지 않은 경우 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 경우를 결정하는 방법에 대해 자세히 알아보세요."](#).

## 보안 권장 사항

데이터 브로커 머신의 보안을 보장하기 위해 NetApp 다음을 권장합니다.

- SSH는 X11 전달을 허용해서는 안 됩니다.
- SSH는 TCP 연결 전달을 허용해서는 안 됩니다.
- SSH는 터널을 허용해서는 안 됩니다.
- SSH는 클라이언트 환경 변수를 허용해서는 안 됩니다.

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

## 그룹에 새로운 데이터 브로커 추가

새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다.

- 새로운 동기화 관계를 생성할 때

["동기화 관계를 생성할 때 새 데이터 브로커를 만드는 방법을 알아보세요."](#).

- 데이터 브로커 관리 페이지에서 \*새 데이터 브로커 추가\*를 선택하면 새 그룹에 데이터 브로커가 생성됩니다.
- 기존 그룹에서 새 데이터 브로커를 만들어 데이터 브로커 관리 페이지에서

## 시작하기 전에

- 암호화된 동기화 관계를 관리하는 그룹에 데이터 브로커를 추가할 수 없습니다.
- 기존 그룹에서 데이터 브로커를 만들려면 해당 데이터 브로커가 온프레미스 데이터 브로커이거나 동일한 유형의 데이터 브로커여야 합니다.

예를 들어, 그룹에 AWS 데이터 브로커가 포함되어 있는 경우 해당 그룹에서 AWS 데이터 브로커나 온프레미스 데이터 브로커를 만들 수 있습니다. Azure 데이터 브로커나 Google Cloud 데이터 브로커는 동일한 데이터 브로커 유형이 아니므로 만들 수 없습니다.

## 새 그룹에서 데이터 브로커를 만드는 단계

1. ["복사 및 동기화에 로그인하세요"](#).
2. \*동기화 > 데이터 브로커 관리\*를 선택합니다.
3. \*새로운 데이터 브로커 추가\*를 선택하세요.
4. 화면의 지시에 따라 데이터 브로커를 생성하세요.

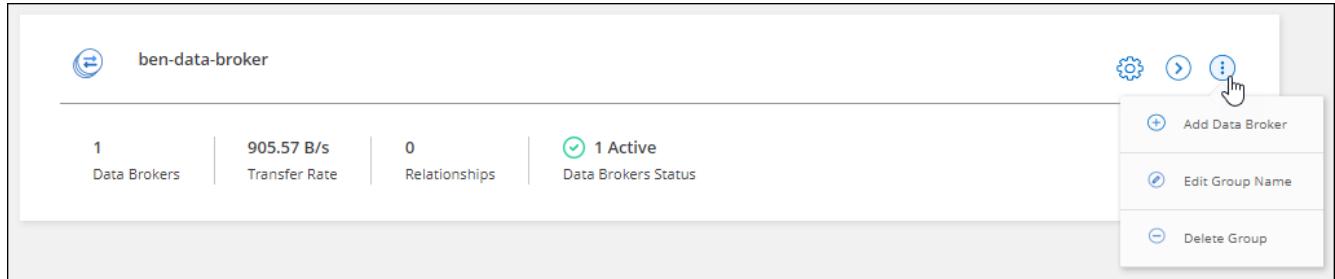
도움이 필요하면 다음 페이지를 참조하세요.

- ["AWS에서 데이터 브로커 만들기"](#)

- "Azure에서 데이터 브로커 만들기"
- "Google Cloud에서 데이터 브로커 만들기"
- "Linux 호스트에 데이터 브로커 설치"

기존 그룹에서 데이터 브로커를 만드는 단계

1. ["복사 및 동기화에 로그인하세요"](#).
2. \*동기화 > 데이터 브로커 관리\*를 선택합니다.
3. 작업 메뉴를 선택하고 \*데이터 브로커 추가\*를 선택합니다.



4. 메시지에 따라 그룹에서 데이터 브로커를 만듭니다.

도움이 필요하면 다음 페이지를 참조하세요.

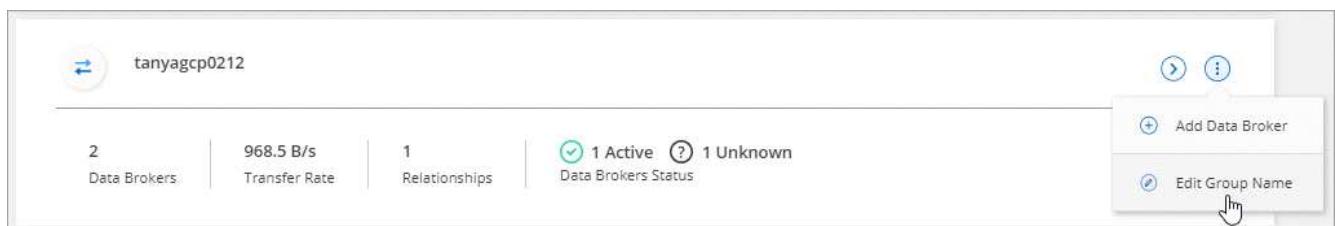
- ["AWS에서 데이터 브로커 만들기"](#)
- ["Azure에서 데이터 브로커 만들기"](#)
- ["Google Cloud에서 데이터 브로커 만들기"](#)
- ["Linux 호스트에 데이터 브로커 설치"](#)

## 그룹 이름 편집

언제든지 데이터 브로커 그룹의 이름을 변경할 수 있습니다.

단계

1. ["복사 및 동기화에 로그인하세요"](#).
2. \*동기화 > 데이터 브로커 관리\*를 선택합니다.
3. 작업 메뉴를 선택하고 \*그룹 이름 편집\*을 선택하세요.



4. 새 이름을 입력하고 \*저장\*을 선택하세요.

결과

복사 및 동기화는 데이터 브로커 그룹의 이름을 업데이트합니다.

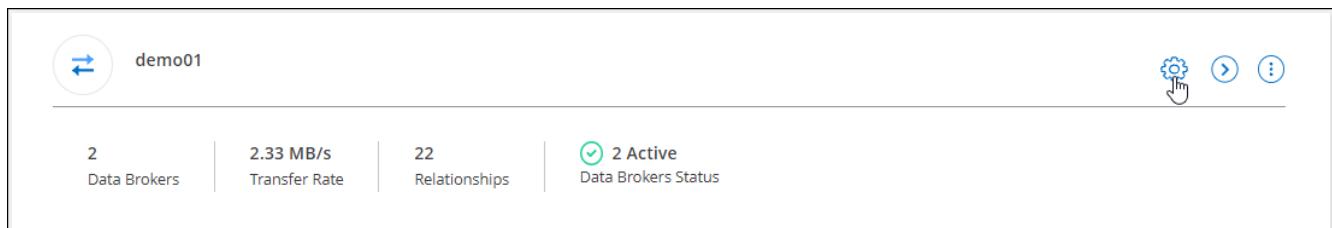
## 통합 구성 설정

동기화 프로세스 중에 동기화 관계에 오류가 발생하는 경우, 데이터 브로커 그룹의 동시성을 통합하면 동기화 오류 수를 줄이는 데 도움이 될 수 있습니다. 그룹 구성을 변경하면 전송 속도가 느려져 성능에 영향을 미칠 수 있습니다.

구성을 직접 변경하는 것은 권장하지 않습니다. 구성을 언제 변경해야 하는지, 어떻게 변경해야 하는지 알아보려면 NetApp에 문의하세요.

단계

1. "복사 및 동기화에 로그인하세요".
2. \*데이터 브로커 관리\*를 선택하세요.
3. 데이터 브로커 그룹에 대한 설정 아이콘을 선택합니다.



4. 필요에 따라 설정을 변경한 다음 \*구성 통합\*을 선택합니다.

다음 사항에 유의하세요.

- 어떤 설정을 변경할지 선택할 수 있습니다. 네 가지 설정을 모두 한꺼번에 변경할 필요는 없습니다.
- 새로운 구성이 데이터 브로커로 전송되면 데이터 브로커가 자동으로 다시 시작되어 새로운 구성 사용합니다.
- 이 변경 사항이 적용되어 복사 및 동기화 인터페이스에 표시될 때까지 최대 1분이 걸릴 수 있습니다.
- 데이터 브로커가 실행 중이 아니면 Copy and Sync가 통신할 수 없기 때문에 구성이 변경되지 않습니다. 데이터 브로커가 다시 시작되면 구성이 변경됩니다.
- 통합 구성 설정하면 모든 새로운 데이터 브로커가 자동으로 새 구성 사용합니다.

## 그룹 간 데이터 브로커 이동

대상 데이터 브로커 그룹의 성능을 가속화해야 하는 경우 데이터 브로커를 한 그룹에서 다른 그룹으로 이동합니다.

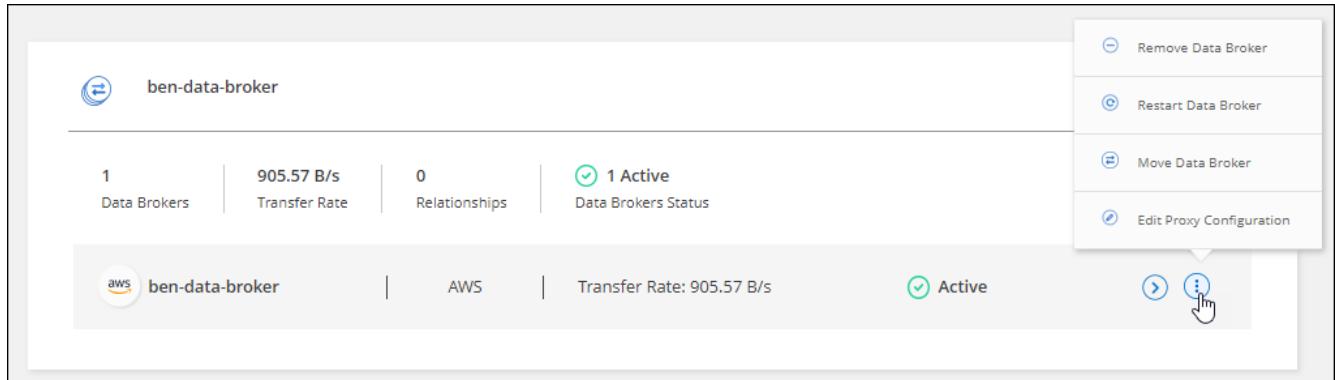
예를 들어, 데이터 브로커가 더 이상 동기화 관계를 관리하지 않는 경우 동기화 관계를 관리하는 다른 그룹으로 쉽게 이동할 수 있습니다.

제한 사항

- 데이터 브로커 그룹이 동기화 관계를 관리하고 그룹에 데이터 브로커가 하나뿐인 경우 해당 데이터 브로커를 다른 그룹으로 이동할 수 없습니다.
- 암호화된 동기화 관계를 관리하는 그룹으로 데이터 브로커를 이동할 수 없습니다.
- 현재 배포 중인 데이터 브로커는 이동할 수 없습니다.

단계

1. "복사 및 동기화에 로그인하세요".
2. \*동기화 > 데이터 브로커 관리\*를 선택합니다.
3. 선택하다 그룹 내 데이터 브로커 목록을 확장합니다.
4. 데이터 브로커의 작업 메뉴를 선택하고 \*데이터 브로커 이동\*을 선택합니다.



5. 새로운 데이터 브로커 그룹을 만들거나 기존 데이터 브로커 그룹을 선택하세요.
6. \*이동\*을 선택하세요.

#### 결과

복사 및 동기화는 데이터 브로커를 새 데이터 브로커 그룹이나 기존 데이터 브로커 그룹으로 이동합니다. 이전 그룹에 다른 데이터 브로커가 없는 경우 복사 및 동기화는 해당 그룹을 삭제합니다.

## 프록시 구성 업데이트

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

#### 단계

1. "복사 및 동기화에 로그인하세요".
2. \*동기화 > 데이터 브로커 관리\*를 선택합니다.
3. 선택하다 그룹 내 데이터 브로커 목록을 확장합니다.
4. 데이터 브로커의 작업 메뉴를 선택하고 \*프록시 구성 편집\*을 선택합니다.
5. 프록시에 대한 세부 정보를 지정합니다: 호스트 이름, 포트 번호, 사용자 이름, 비밀번호.
6. \*업데이트\*를 선택하세요.

#### 결과

복사 및 동기화는 인터넷 액세스를 위해 프록시 구성을 사용하도록 데이터 브로커를 업데이트합니다.

## 데이터 브로커 구성 보기

데이터 브로커의 호스트 이름, IP 주소, 사용 가능한 CPU 및 RAM 등을 파악하기 위해 해당 브로커에 대한 세부 정보를 보고 싶을 수 있습니다.

Copy and Sync는 데이터 브로커에 대한 다음과 같은 세부 정보를 제공합니다.

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



스캐너는 소스와 타겟을 스캔하여 무엇을 복사해야 할지 결정합니다. 전송자는 실제로 복사를 수행합니다. NetApp 담당자는 이러한 구성 세부 정보를 사용하여 성능을 최적화할 수 있는 작업을 제안할 수 있습니다.

## 단계

1. ["복사 및 동기화에 로그인하세요"](#).
2. \*동기화 > 데이터 브로커 관리\*를 선택합니다.
3. 선택하다 그룹 내 데이터 브로커 목록을 확장합니다.
4. 선택하다 데이터 브로커에 대한 세부 정보를 보려면.

The screenshot shows the 'Data Brokers' section of the NetApp Copy and Sync interface. At the top, it displays summary statistics: 2 Data Brokers, a Transfer Rate of 968.5 B/s, and 1 Relationship. Below this, the 'Data Brokers Status' section shows 1 Active broker and 1 Unknown broker. The main table provides detailed information for the active broker, tanyagcp0212:

Information	Value	Value	Value	Value
Broker ID	5fc766b3d3e3664b9e116...	Instance ID	tanyagcp0212-mnx-data-...	Host Name
Region	us-east1-b	Network	255.255.240.0	Project Id
Linux Distribution & Version	linux	Vault Version	14.15.1	Data Broker Version
Available CPUs	4	Available RAM	62.22 MB	
Scanner Concurrency	50	Scanner CPUs	4	Transferrer Concurrency
				Transferrer CPUs

## 데이터 브로커와 문제 해결

복사 및 동기화는 문제 해결에 도움이 되는 각 데이터 브로커의 상태를 표시합니다.

## 단계

1. ["복사 및 동기화에 로그인하세요"](#).

2. "알 수 없음" 또는 "실패" 상태인 데이터 브로커를 식별합니다.

The screenshot shows a summary of data brokers. At the top, it displays 'tanyagcp0212' with a refresh icon. Below that, there are four metrics: '2 Data Brokers', '968.5 B/s Transfer Rate', '1 Relationships', and '1 Active 1 Unknown Data Brokers Status'. The main list contains two entries:

Broker	Type	Status	Transfer Rate
tanyagcp0212	GCP	Active	Transfer Rate: 968.5 B/s
tanya1	ONPREM	Unknown	Transfer Rate: N/A

3. 위에 마우스를 올려 놓으세요 ⓘ 실패 이유를 보려면 아이콘을 클릭하세요.

4. 문제를 해결하세요.

예를 들어, 데이터 브로커가 오프라인인 경우 간단히 다시 시작해야 할 수도 있고, 초기 배포에 실패한 경우 데이터 브로커를 제거해야 할 수도 있습니다.

## 그룹에서 데이터 브로커 제거

더 이상 필요하지 않거나 초기 배포에 실패한 경우 그룹에서 데이터 브로커를 제거할 수 있습니다. 이 작업을 수행하면 Copy and Sync 레코드에서 데이터 브로커만 삭제됩니다. 데이터 브로커와 추가 클라우드 리소스를 직접 수동으로 삭제해야 합니다.

당신이 알아야 할 것들

- 복사 및 동기화는 그룹에서 마지막 데이터 브로커를 제거하면 그룹을 삭제합니다.
- 해당 그룹을 사용하는 관계가 있는 경우, 해당 그룹에서 마지막 데이터 브로커를 제거할 수 없습니다.

단계

- "복사 및 동기화에 로그인하세요".
- \*동기화 > 데이터 브로커 관리\*를 선택합니다.
- 선택하다 ➤ 그룹 내 데이터 브로커 목록을 확장합니다.
- 데이터 브로커에 대한 작업 메뉴를 선택하고 \*데이터 브로커 제거\*를 선택합니다.

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

tanya1 | ONPREM | Transfer Rate: N/A | Unknown

Remove Data Broker

5. \*데이터 브로커 제거\*를 선택하세요.

#### 결과

복사 및 동기화를 통해 그룹에서 데이터 브로커가 제거됩니다.

#### 데이터 브로커 그룹 삭제

데이터 브로커 그룹이 더 이상 동기화 관계를 관리하지 않는 경우 그룹을 삭제하면 모든 데이터 브로커가 복사 및 동기화에서 제거됩니다.

Copy and Sync에서 제거한 데이터 브로커는 Copy and Sync의 레코드에서만 삭제됩니다. 클라우드 공급자와 추가 클라우드 리소스에서 데이터 브로커 인스턴스를 수동으로 삭제해야 합니다.

#### 단계

1. "복사 및 동기화에 로그인하세요".
2. \*동기화 > 데이터 브로커 관리\*를 선택합니다.
3. 작업 메뉴를 선택하고 \*그룹 삭제\*를 선택하세요.

ben-data-broker

1 Data Brokers | 905.57 B/s Transfer Rate | 0 Relationships | 1 Active Data Brokers Status

Add Data Broker

Edit Group Name

Delete Group

4. 확인하려면 그룹 이름을 입력하고 \*그룹 삭제\*를 선택하세요.

#### 결과

복사 및 동기화는 데이터 브로커를 제거하고 그룹을 삭제합니다.

# NetApp Copy and Sync 에서 구성을 조정하기 위한 보고서를 만들고 봅니다.

NetApp Copy and Sync에서 보고서를 만들고 확인하여 NetApp 직원의 도움을 받아 데이터 브로커의 구성을 조정하고 성능을 개선하는 데 사용할 수 있는 정보를 얻으세요.

각 보고서는 동기화 관계의 경로에 대한 심층적인 세부 정보를 제공합니다. 여기에는 디렉토리, 파일, 심볼릭 링크의 수, 파일 크기의 분포, 디렉토리의 깊이와 너비, 수정 시간, 액세스 시간이 포함됩니다. 이는 대시보드에서 사용할 수 있는 동기화 통계와 다릅니다. ["동기화를 성공적으로 생성하고 완료"](#).

## 보고서 만들기

보고서를 생성할 때마다 복사 및 동기화가 경로를 스캔한 다음 세부 정보를 보고서로 컴파일합니다.

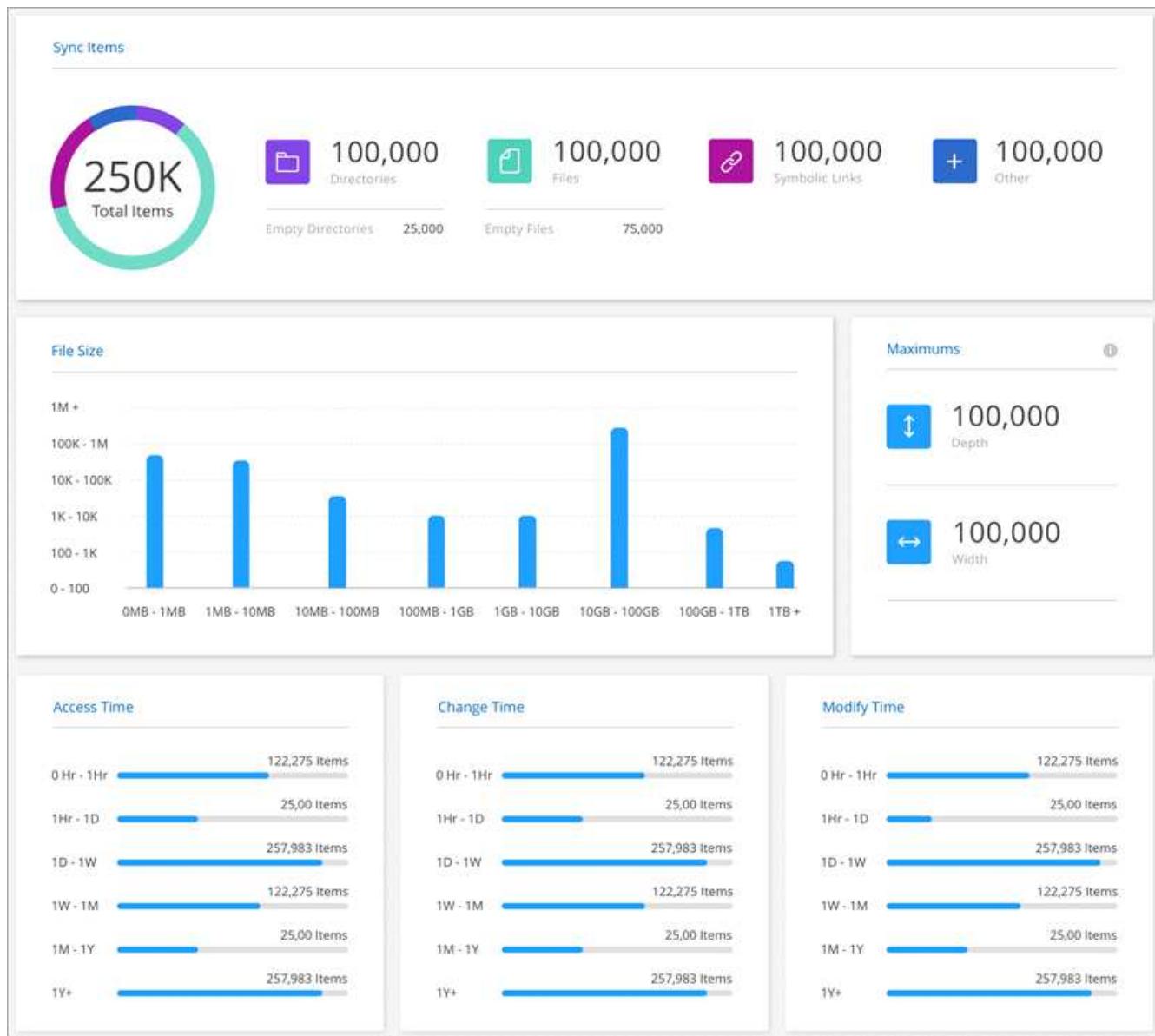
### 단계

1. ["복사 및 동기화에 로그인하세요"](#).
2. \*동기화 > 보고서\*를 선택합니다.

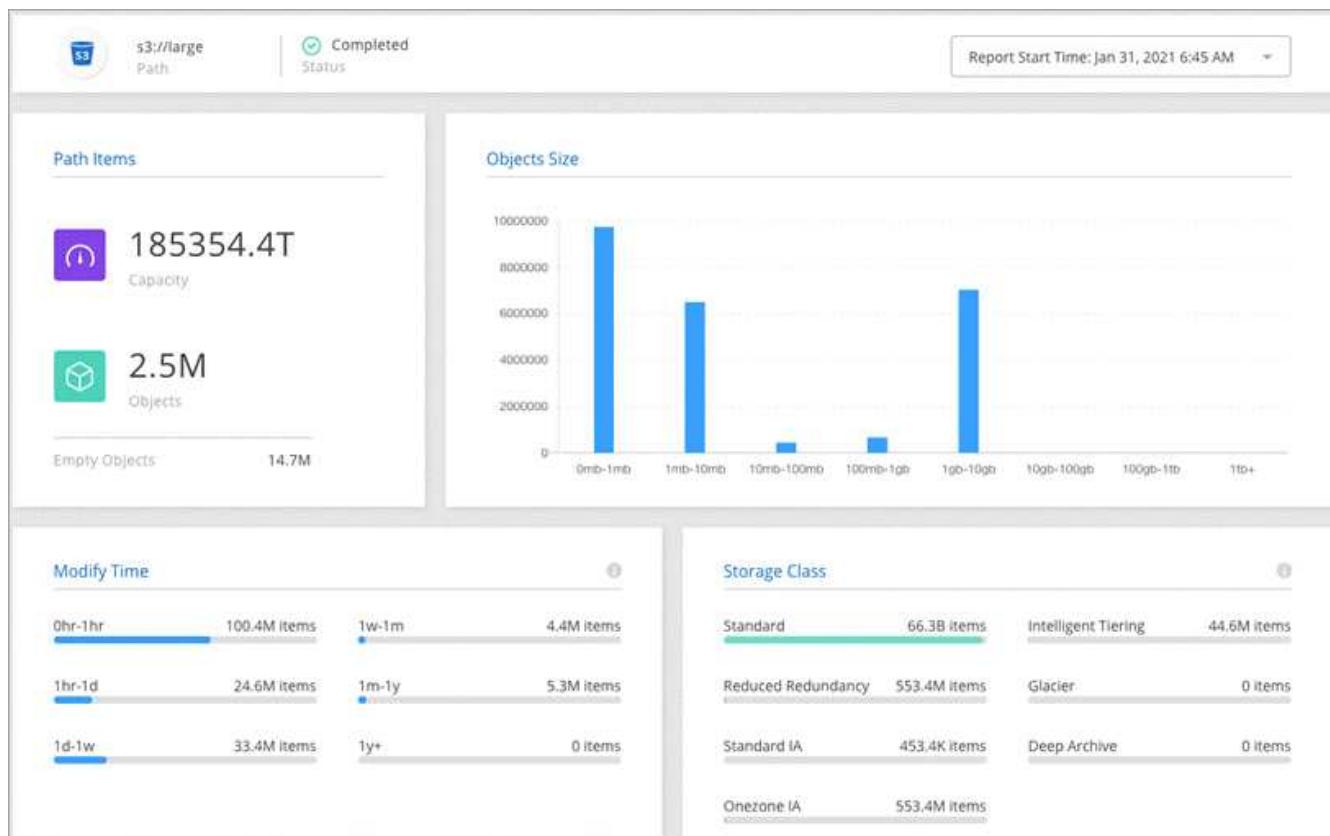
각 동기화 관계의 경로(소스 또는 대상)가 표에 표시됩니다.

3. 보고서 작업 열에서 특정 경로로 이동하여 \*만들기\*를 선택하거나 작업 메뉴를 선택하고 \*새로 만들기\*를 선택합니다.
4. 보고서가 준비되면 작업 메뉴를 선택하고 \*보기\*를 선택하세요.

다음은 파일 시스템 경로에 대한 샘플 보고서입니다.



다음은 개체 저장소에 대한 샘플 보고서입니다.

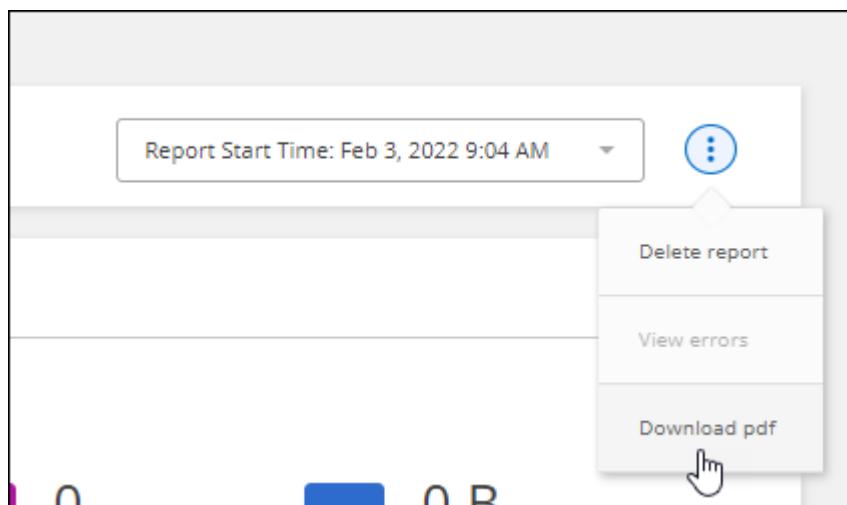


## 보고서 다운로드

오프라인에서 보거나 공유할 수 있도록 보고서를 PDF로 다운로드할 수 있습니다.

### 단계

- "[복사 및 동기화에 로그인하세요](#)".
- \*동기화 > 보고서\*를 선택합니다.
- 보고서 작업 열에서 작업 메뉴를 선택하고 \*보기\*를 선택합니다.
- 보고서 오른쪽 상단에서 작업 메뉴를 선택하고 \*pdf 다운로드\*를 선택하세요.



## 보고서 오류 보기

경로 테이블은 최신 보고서에 오류가 있는지 여부를 식별합니다. 오류는 Copy and Sync가 경로를 스캔할 때 발생한 문제를 나타냅니다.

예를 들어, 보고서에 권한 거부 오류가 포함될 수 있습니다. 이러한 유형의 오류는 Copy and Sync가 전체 파일과 디렉터리를 검색하는 기능에 영향을 미칠 수 있습니다.

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

### 단계

1. ["복사 및 동기화에 로그인하세요"](#).
2. \*동기화 > 보고서\*를 선택합니다.
3. 오류 열에서 보고서에 오류가 있는지 확인합니다.
4. 오류가 있는 경우 오류 개수 옆에 있는 화살표를 선택하세요.

20 Paths								Reports Actions
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 ↗	...		

5. 오류에 있는 정보를 사용하여 문제를 해결하세요.

문제를 해결한 후에는 다음에 보고서를 실행할 때 오류가 나타나지 않아야 합니다.

## 보고서 삭제

보고서에 수정한 오류가 포함되어 있거나, 보고서가 제거한 동기화 관계와 관련된 경우 해당 보고서를 삭제할 수 있습니다.

### 단계

1. \*동기화 > 보고서\*를 선택합니다.
2. 보고서 작업 열에서 경로에 대한 작업 메뉴를 선택하고 마지막 보고서 삭제 또는 \*모든 보고서 삭제\*를 선택합니다.
3. 보고서를 삭제할지 확인하세요.

## NetApp Copy and Sync 용 데이터 브로커 제거

필요한 경우 제거 스크립트를 실행하여 데이터 브로커와 NetApp Copy and Sync에 대해 데이터 브로커가 설치될 때 생성된 패키지 및 디렉터리를 제거합니다.

## 단계

1. 데이터 브로커 호스트에 로그인합니다.
2. 데이터 브로커 디렉토리로 변경: /opt/netapp/databroker
3. 다음 명령을 실행하세요.

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

4. 'y'를 눌러 제거를 확인하세요.

## 저작권 정보

Copyright © 2025 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 그레픽, 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 있으며 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/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.