



# Cloud Sync 설명서

## Cloud Sync

NetApp  
June 07, 2022

# 목차

Cloud Sync 설명서	1
릴리스 정보	2
Cloud Sync의 새로운 기능	2
제한 사항	13
시작하십시오	14
Cloud Sync 개요	14
Cloud Sync를 빠르게 시작합니다	16
지원되는 동기화 관계	17
소스와 타겟을 준비합니다	24
Cloud Sync의 네트워킹 개요	30
데이터 브로커를 설치합니다	34
Cloud Sync를 사용합니다	50
소스와 타겟 간에 데이터를 동기화합니다	50
무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불합니다	68
동기화 관계 관리	70
데이터 브로커 그룹을 관리합니다	75
구성을 조정하기 위해 보고서 작성 및 보기	82
데이터 브로커를 제거하는 중입니다	85
Cloud Sync API	87
시작하기	87
API 참조입니다	88
목록 API 사용	88
개념	91
라이선스 개요	91
데이터 개인 정보 보호	92
Cloud Sync 기술 FAQ	92
지식 및 지원	100
지원을 위해 등록하십시오	100
도움을 받으십시오	101
법적 고지	103
저작권	103
상표	103
특허	103
개인 정보 보호 정책	103
오픈 소스	103

# Cloud Sync 설명서

# 릴리스 정보

## Cloud Sync의 새로운 기능

Cloud Sync의 새로운 기능에 대해 알아보십시오.

**2022년 6월 6일**

### 연속 동기화

새로운 설정을 사용하면 소스 S3 버킷에서 타겟으로 변경 사항을 지속적으로 동기화할 수 있습니다.

초기 데이터 동기화 후 Cloud Sync는 소스 S3 버킷의 변경 사항을 수신 대기하고 변경 사항이 발생할 때마다 타겟에 계속 동기화합니다. 예약된 간격으로 소스를 다시 검색할 필요가 없습니다. 이 설정은 S3 버킷에서 S3, Google Cloud Storage, Azure Blob Storage, StorageGRID 또는 IBM Storage로 동기화할 때만 사용할 수 있습니다.

이 설정을 사용하려면 데이터 브로커와 연결된 IAM 역할에 다음 권한이 필요합니다.

```
"s3:GetBucketNotification",  
"s3:PutBucketNotification"
```

이러한 사용 권한은 사용자가 만든 새 데이터 브로커에 자동으로 추가됩니다.

["연속 동기화 설정에 대해 자세히 알아보십시오."](#)

### 모든 ONTAP 볼륨을 표시합니다

동기화 관계를 생성하면 Cloud Sync는 이제 소스 Cloud Volumes ONTAP 시스템, 온-프레미스 ONTAP 클러스터 또는 ONTAP 파일 시스템용 FSx의 모든 볼륨을 표시합니다.

이전 버전에서는 Cloud Sync가 선택한 프로토콜과 일치하는 볼륨만 표시합니다. 이제 모든 볼륨이 표시되지만 선택한 프로토콜과 일치하지 않거나 공유 또는 내보내기가 없는 볼륨은 회색으로 표시되고 선택할 수 없습니다.

### Azure Blob에 태그 복사 중

Azure Blob이 타겟인 동기화 관계를 만들면 Cloud Sync에서 이제 Azure Blob 컨테이너에 태그를 복사할 수 있습니다.

- Settings \* 페이지에서 \* Copy for Objects \* 설정을 사용하여 소스에서 Azure Blob 컨테이너로 태그를 복사할 수 있습니다. 이는 메타데이터 복사에 추가됩니다.
- 태그/메타데이터 \* 페이지에서 Azure Blob 컨테이너에 복사되는 개체에 설정할 Blob 인덱스 태그를 지정할 수 있습니다. 이전에는 관계 메타데이터만 지정할 수 있었습니다.

이러한 옵션은 Azure Blob이 타겟이고 소스가 Azure Blob 또는 S3 호환 엔드포인트(S3, StorageGRID 또는 IBM 클라우드 오브젝트 스토리지)인 경우에 지원됩니다.

## 2022년 5월 1일

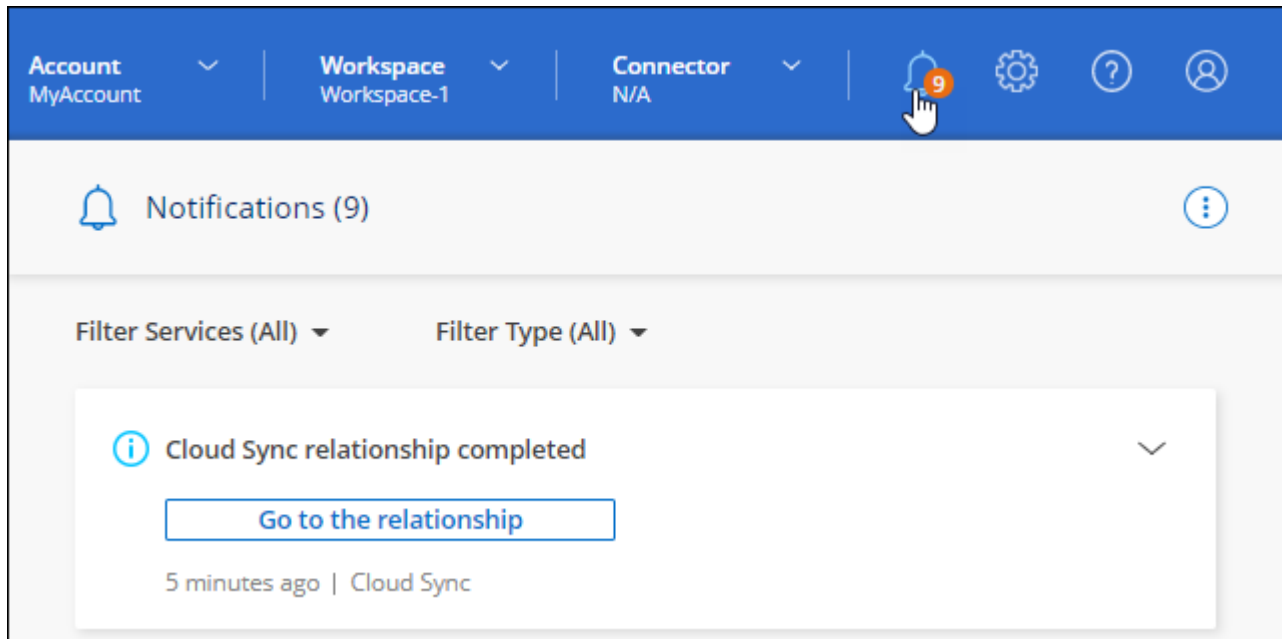
동기화 시간이 초과되었습니다

이제 동기화 관계에 새로운 \* 동기화 시간 초과 \* 설정을 사용할 수 있습니다. 이 설정을 사용하면 지정된 시간 또는 일 수 동안 동기화가 완료되지 않은 경우 Cloud Sync에서 데이터 동기화를 취소할지 여부를 정의할 수 있습니다.

["동기화 관계의 설정 변경에 대해 자세히 알아보십시오"](#).

알림

이제 새 \* 알림 \* 설정을 동기화 관계에 사용할 수 있습니다. 이 설정을 사용하면 Cloud Manager의 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.



["동기화 관계의 설정 변경에 대해 자세히 알아보십시오"](#).

## 2022년 4월 3일

데이터 브로커 그룹의 기능이 향상되었습니다

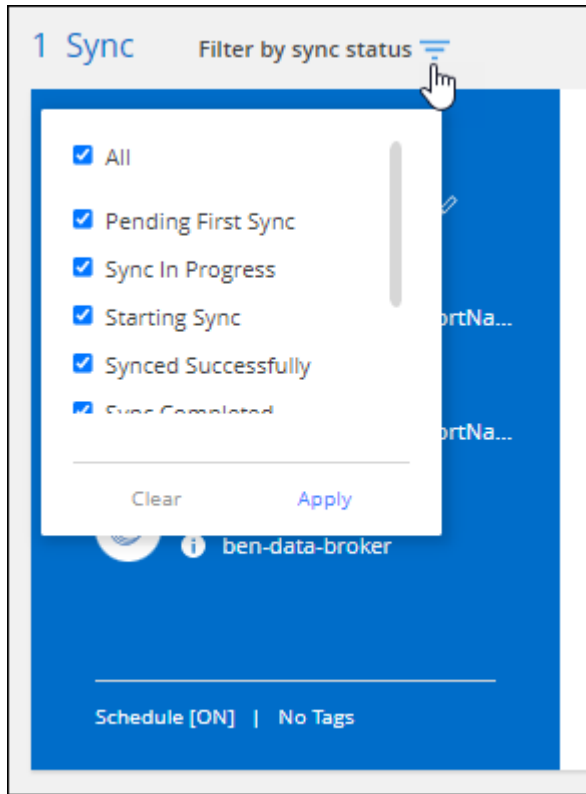
데이터 브로커 그룹을 개선한 사항은 다음과 같습니다.

- 이제 데이터 브로커를 신규 또는 기존 그룹으로 이동할 수 있습니다.
- 이제 데이터 브로커에 대한 프록시 구성을 업데이트할 수 있습니다.
- 마지막으로 데이터 브로커 그룹을 삭제할 수도 있습니다.

["데이터 브로커 그룹을 관리하는 방법에 대해 알아보십시오"](#).

## 대시보드 필터

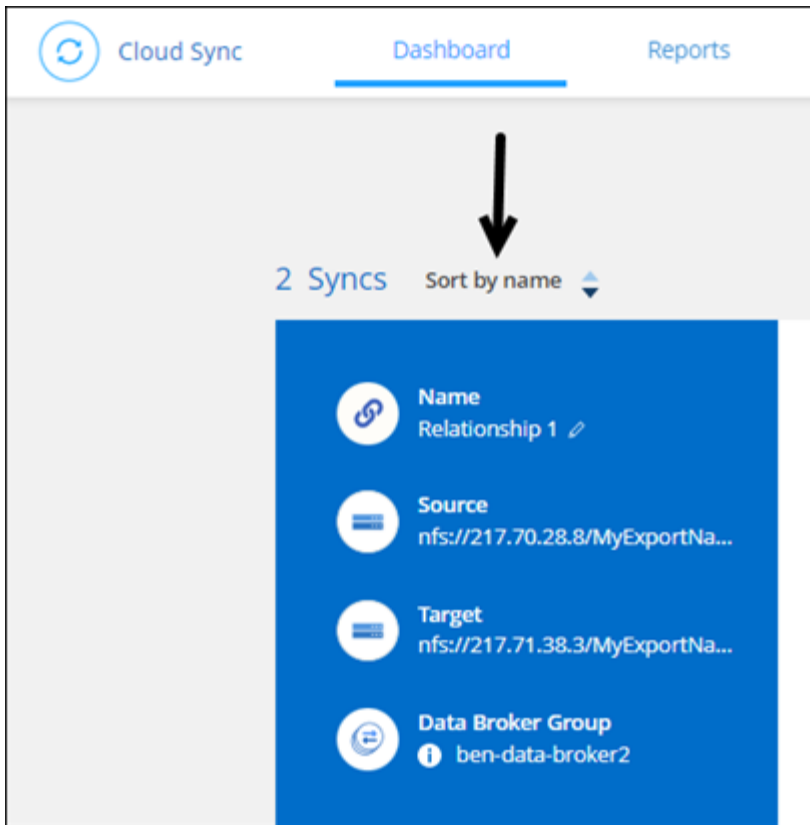
이제 동기화 대시보드의 내용을 필터링하여 특정 상태와 일치하는 동기화 관계를 보다 쉽게 찾을 수 있습니다. 예를 들어 실패 상태인 동기화 관계를 필터링할 수 있습니다



## 2022년 3월 3일

### 대시보드에서 정렬

이제 동기화 관계 이름을 기준으로 대시보드를 정렬합니다.



## 데이터 센스 통합 기능 향상

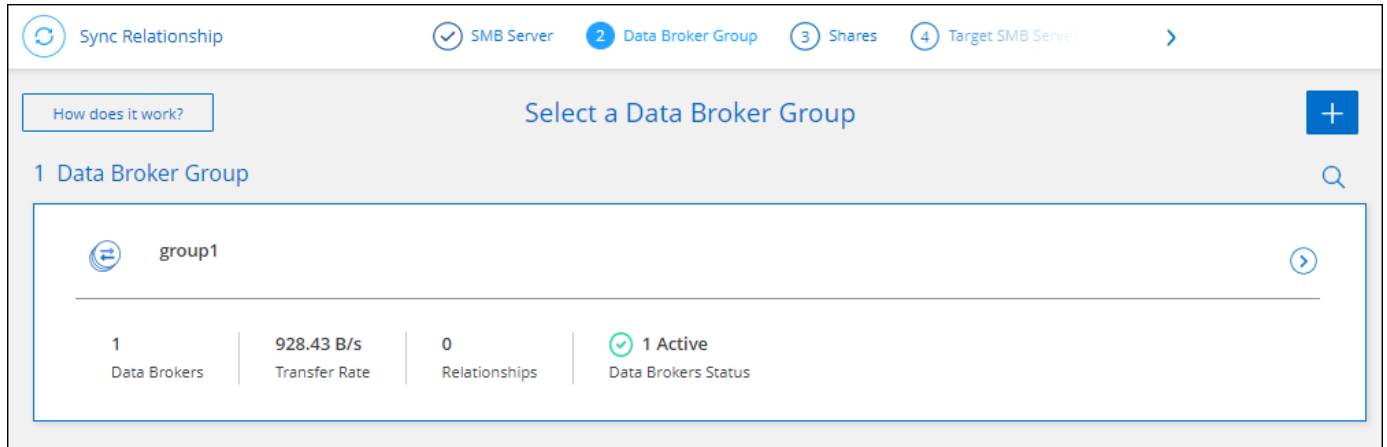
이전 릴리즈에서는 클라우드 데이터 센스와 Cloud Sync의 통합을 소개했습니다. 이 업데이트를 통해 동기화 관계를 보다 쉽게 만들 수 있도록 통합을 개선했습니다. Cloud Data Sense에서 데이터 동기화를 시작한 후에는 모든 소스 정보가 한 번에 포함되고 몇 가지 키 세부 정보만 입력하면 됩니다.

## 2022년 2월 6일

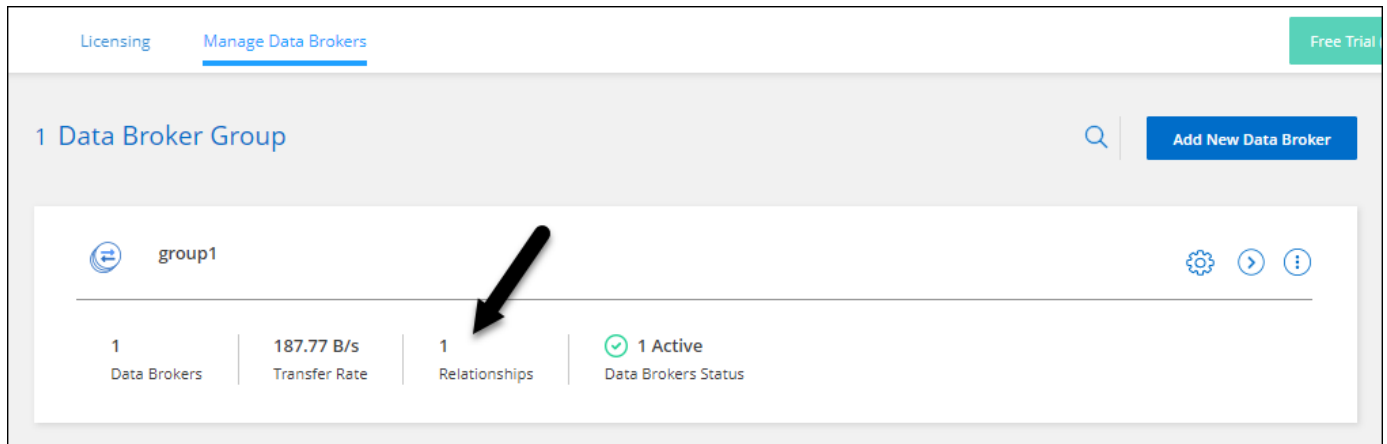
### 데이터 브로커 그룹의 개선 사항

데이터 브로커\_groups\_를 강조하여 데이터 브로커와 상호 작용하는 방법을 변경했습니다.

예를 들어, 새 동기화 관계를 생성할 때 특정 데이터 브로커가 아닌 관계에 사용할 데이터 브로커\_group\_을 선택합니다.



데이터 브로커 \* 관리 탭에는 데이터 브로커 그룹이 관리하는 동기화 관계의 수도 표시됩니다.



**PDF** 보고서를 다운로드합니다

이제 보고서의 PDF를 다운로드할 수 있습니다.

"보고서에 대해 자세히 알아보십시오".

**2022년 1월 2일**

새 **Box** 동기화 관계

두 가지 새로운 동기화 관계가 지원됩니다.

- Box를 Azure NetApp Files로 설정합니다
- ONTAP용 아마존 FSx로 상자를 이동합니다

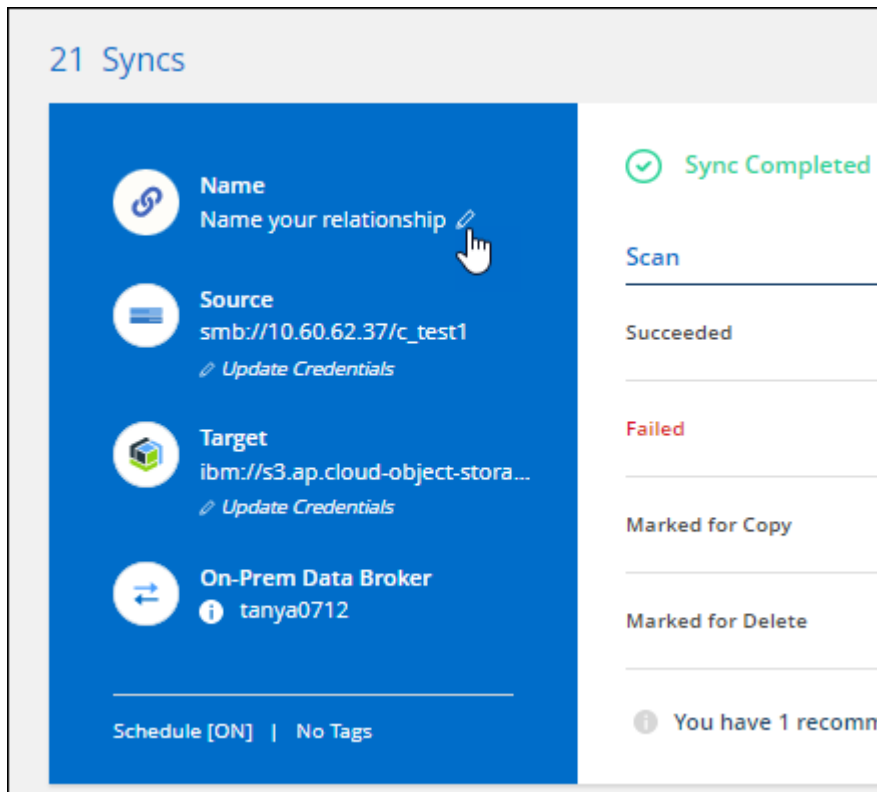
"지원되는 동기화 관계 목록을 봅니다".

관계 이름

이제 각 동기화 관계에 의미 있는 이름을 제공하여 각 관계의 목적을 보다 쉽게 파악할 수 있습니다. 관계를 만들 때



그리고 그 이후에 언제든지 이름을 추가할 수 있습니다.



### S3 개인 링크

Amazon S3와 데이터를 동기화할 때 S3 개인 링크를 사용할지 여부를 선택할 수 있습니다. 데이터 브로커가 소스에서 타겟으로 데이터를 복제하면 프라이빗 링크를 통해 전송됩니다.

이 기능을 사용하려면 데이터 브로커와 연결된 IAM 역할에 다음 권한이 필요합니다.

```
"ec2:DescribeVpcEndpoints"
```

이 권한은 사용자가 만든 새 데이터 브로커에 자동으로 추가됩니다.

### Glacier 빠른 검색

이제 Amazon S3가 동기화 관계의 타겟일 때 \_Glacier Instant Retrieval\_storage 클래스를 선택할 수 있습니다.

### 오브젝트 스토리지에서 SMB 공유까지 ACL

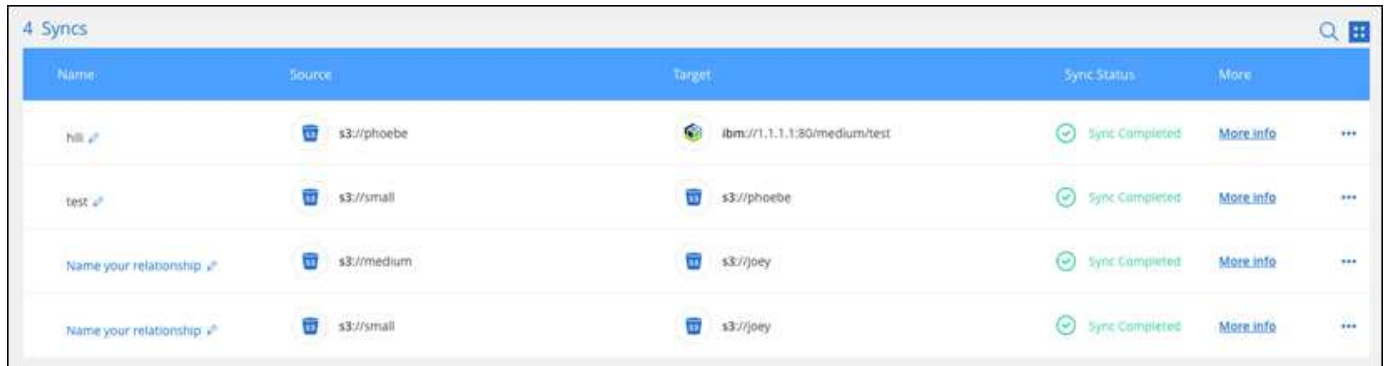
이제 Cloud Sync는 오브젝트 스토리지에서 SMB 공유로 ACL을 복사할 수 있도록 지원합니다. 이전에는 SMB 공유에서 오브젝트 스토리지로의 ACL 복사만 지원했습니다.

### SFTP에서 S3로

이제 사용자 인터페이스에서 SFTP에서 Amazon S3로 동기화 관계를 생성할 수 있습니다. 이 동기화 관계는 이전에 API에서만 지원되었습니다.

## 테이블 뷰 개선

쉽게 사용할 수 있도록 대시보드의 테이블 보기를 다시 설계했습니다. 추가 정보 \* 를 클릭하면 Cloud Sync가 대시보드를 필터링하여 해당 특정 관계에 대한 자세한 정보를 표시합니다.



Name	Source	Target	Sync Status	More
hll	s3://phoebe	ibmc/71.1.1.1:80/medium/test	Sync Completed	More info
test	s3://small	s3://phoebe	Sync Completed	More info
Name your relationship	s3://medium	s3://joey	Sync Completed	More info
Name your relationship	s3://small	s3://joey	Sync Completed	More info

## Jarkarta 지역 지원

Cloud Sync은 현재 AWS 아시아 태평양(자카르타) 지역에 데이터 브로커 구축을 지원하고 있습니다.

## 2021년 11월 28일

### SMB에서 오브젝트 스토리지까지의 ACL

소스 SMB 공유에서 오브젝트 스토리지(ONTAP S3 제외)로의 동기화 관계를 설정할 때 Cloud Sync에서 이제 ACL(액세스 제어 목록)을 복사할 수 있습니다.

Cloud Sync는 오브젝트 스토리지에서 SMB 공유로의 ACL 복제를 지원하지 않습니다.

"SMB 공유에서 ACL을 복사하는 방법에 대해 알아보십시오".

라이센스를 업데이트합니다

이제 확장된 Cloud Sync 라이선스를 업데이트할 수 있습니다.

NetApp에서 구매한 Cloud Sync 라이선스를 연장한 경우 라이선스를 다시 추가하여 만료일을 업데이트할 수 있습니다.

"라이선스를 업데이트하는 방법을 알아보십시오".

Box 자격 증명을 업데이트합니다

이제 기존 동기화 관계에 대한 Box 자격 증명을 업데이트할 수 있습니다.

"자격 증명을 업데이트하는 방법을 알아보십시오".

## 2021년 10월 31일

박스 지지대

Box 지원은 이제 Cloud Sync 사용자 인터페이스에서 미리 보기로 제공됩니다.

Box는 여러 유형의 동기화 관계의 소스 또는 타겟이 될 수 있습니다. ["지원되는 동기화 관계 목록을 봅니다"](#).

## 만든 날짜 설정

SMB 서버가 소스인 경우 `_Date Created` 라는 새로운 동기화 관계 설정을 사용하면 특정 날짜 이후, 특정 날짜 이전 또는 특정 시간 범위 간에 생성된 파일을 동기화할 수 있습니다.

["Cloud Sync 설정에 대해 자세히 알아보십시오"](#).

## 2021년 10월 4일

### 추가 박스 지원

Cloud Sync는 이제 에 대한 추가 동기화 관계를 지원합니다 ["상자에 입력합니다"](#) Cloud Sync API를 사용하는 경우:

- Amazon S3를 상자로 이동합니다
- IBM Cloud Object Storage to Box를 참조하십시오
- StorageGRID에서 Box로
- Box를 NFS 서버에 전송합니다
- Box를 SMB 서버로 전송합니다

["API를 사용하여 동기화 관계를 설정하는 방법에 대해 알아보십시오"](#).

### SFTP 경로 보고서

이제 가능합니다 ["보고서를 만듭니다"](#) SFTP 경로.

## 2021년 9월 2일

### ONTAP용 FSx 지원

이제 Amazon FSx for ONTAP 파일 시스템과 데이터를 동기화할 수 있습니다.

- ["ONTAP용 Amazon FSx에 대해 자세히 알아보십시오"](#)
- ["지원되는 동기화 관계를 봅니다"](#)
- ["ONTAP용 Amazon FSx에 대한 동기화 관계를 생성하는 방법을 알아보십시오"](#)

## 2021년 8월 1일

### 자격 증명을 업데이트합니다

이제 Cloud Sync를 사용하여 기존 동기화 관계에서 소스 또는 타겟의 최신 자격 증명으로 데이터 브로커를 업데이트할 수 있습니다.

이 향상된 기능은 보안 정책에 따라 자격 증명을 정기적으로 업데이트해야 하는 경우에 도움이 될 수 있습니다. ["자격 증명을 업데이트하는 방법을 알아보십시오"](#).



오브젝트 스토리지 타겟의 태그입니다

동기화 관계를 생성할 때 이제 동기화 관계에서 개체 스토리지 대상에 태그를 추가할 수 있습니다.

태그 추가는 Amazon S3, Azure Blob, Google Cloud Storage, IBM Cloud Object Storage 및 StorageGRID에서 지원됩니다.

박스 지원

이제 Cloud Sync가 지원됩니다 "상자에 입력합니다" Cloud Sync API를 사용할 경우 Amazon S3, StorageGRID 및 IBM 클라우드 오브젝트 스토리지와 동기화 관계의 소스로 사용됩니다.

["API를 사용하여 동기화 관계를 설정하는 방법에 대해 알아봅니다."](#)

## Google Cloud의 데이터 브로커를 위한 공용 IP

Google Cloud에서 데이터 브로커를 구축할 때 가상 머신 인스턴스에 대해 공용 IP 주소를 사용할지 여부를 선택할 수 있습니다.

["Google Cloud에서 데이터 브로커를 구축하는 방법을 알아보십시오."](#)

## Azure NetApp Files용 이중 프로토콜 볼륨

Azure NetApp Files에 대해 소스 또는 타겟 볼륨을 선택하면 동기화 관계에 대해 선택한 프로토콜에 관계 없이 Cloud Sync에 이중 프로토콜 볼륨이 표시됩니다.

## 2021년 7월 7일

### ONTAP S3 스토리지 및 Google Cloud Storage

Cloud Sync은 이제 사용자 인터페이스에서 ONTAP S3 스토리지와 Google 클라우드 스토리지 버킷 간의 동기화 관계를 지원합니다.

["지원되는 동기화 관계 목록을 봅니다."](#)

#### 개체 메타데이터 태그

이제 Cloud Sync는 동기화 관계를 생성하고 설정을 활성화하면 개체 기반 스토리지 간에 개체 메타데이터와 태그를 복사할 수 있습니다.

["개체에 대한 복사 설정에 대해 자세히 알아보세요."](#)

#### 하시코프 볼트 지원

이제 Google Cloud 서비스 계정으로 인증하여 외부 HashiCorp Vault에서 자격 증명에 액세스하도록 데이터 브로커를 설정할 수 있습니다.

["데이터 브로커가 있는 HashiCorp Vault를 사용하는 방법에 대해 자세히 알아보십시오."](#)

## S3 버킷의 태그 또는 메타데이터를 정의합니다

Amazon S3 버킷과의 동기화 관계를 설정할 때 이제 동기화 관계 마법사를 통해 타겟 S3 버킷의 오브젝트에 저장할 태그 또는 메타데이터를 정의할 수 있습니다.

태그 지정 옵션은 이전에 동기화 관계의 설정에 포함되어 있었습니다.

## 2021년 6월 7일

### Google Cloud의 스토리지 클래스

Google Cloud Storage 버킷이 동기화 관계의 타겟인 경우 이제 사용할 스토리지 클래스를 선택할 수 있습니다. Cloud Sync는 다음 스토리지 클래스를 지원합니다.

- 표준
- 니어라인
- 콜드라인
- 아카이브

## 2021년 5월 2일

보고서에 오류가 있습니다

이제 보고서에 있는 오류를 볼 수 있으며 마지막 보고서나 모든 보고서를 삭제할 수 있습니다.

["구성을 조정할 보고서를 만들고 보는 방법에 대해 자세히 알아보십시오"](#).

특성을 비교합니다

이제 각 동기화 관계에 대해 새 \* Compare by \* 설정을 사용할 수 있습니다.

이 고급 설정을 사용하면 Cloud Sync에서 파일 또는 디렉터리가 변경되었으며 다시 동기화되어야 하는지 여부를 결정할 때 특정 특성을 비교할지 여부를 선택할 수 있습니다.

["동기화 관계의 설정 변경에 대해 자세히 알아보십시오"](#).

## 2021년 4월 11일

독립 실행형 **Cloud Sync** 서비스가 폐기됩니다

독립 실행형 Cloud Sync 서비스가 폐기되었습니다. 이제 동일한 모든 기능을 사용할 수 있는 Cloud Manager에서 Cloud Sync에 직접 액세스할 수 있습니다.

Cloud Manager에 로그인한 후 맨 위에 있는 동기화 탭으로 전환하고 이전과 마찬가지로 관계를 볼 수 있습니다.

### Google Cloud 버킷 - 다양한 프로젝트

동기화 관계를 설정할 때 데이터 브로커의 서비스 계정에 필요한 권한을 제공하는 경우 다양한 프로젝트의 Google Cloud 버킷 중에서 선택할 수 있습니다.

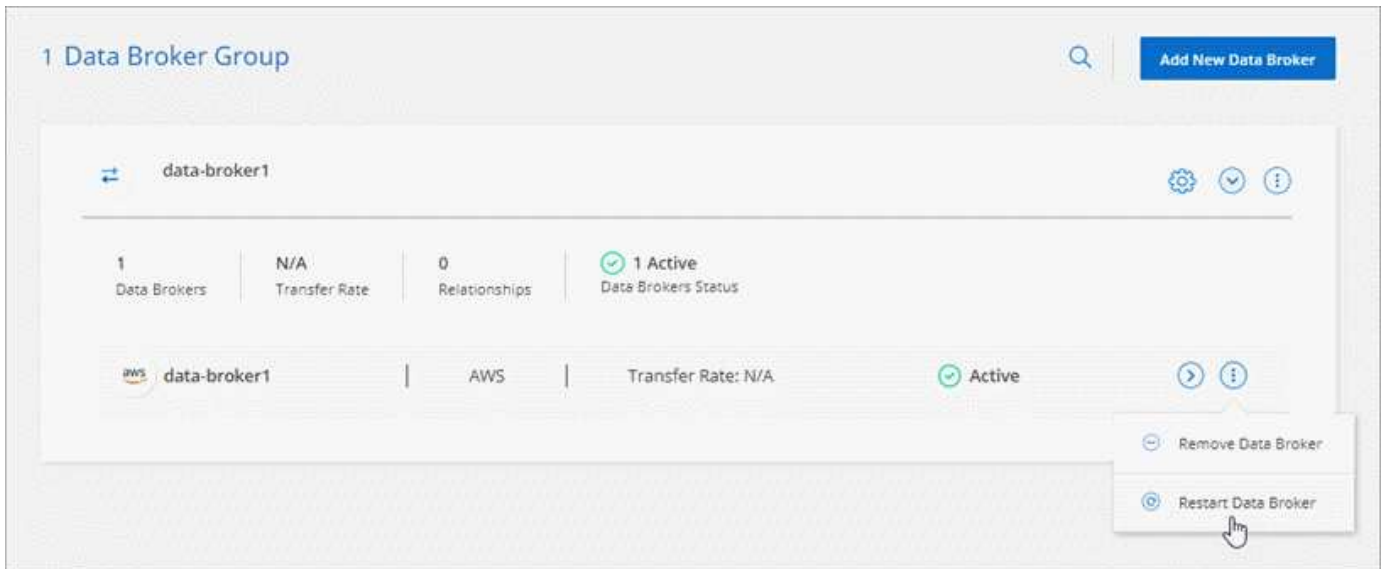
["서비스 계정 설정 방법에 대해 알아보십시오"](#).

### Google Cloud Storage와 S3 간 메타데이터

이제 Cloud Sync는 Google Cloud Storage와 S3 공급자(AWS S3, StorageGRID, IBM Cloud Object Storage) 간에 메타데이터를 복사합니다.

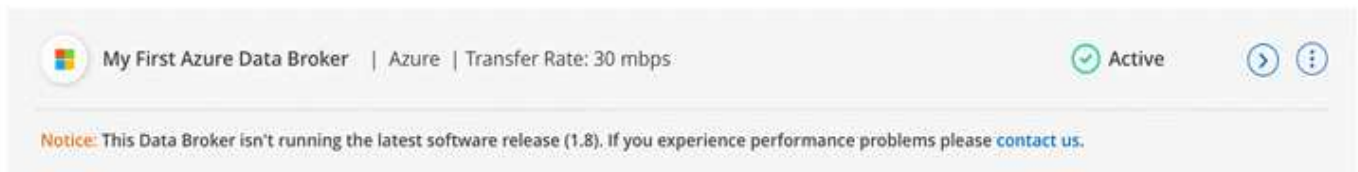
데이터 브로커를 다시 시작합니다

이제 Cloud Sync에서 데이터 브로커를 다시 시작할 수 있습니다.



최신 릴리스를 실행하지 않을 때 나타나는 메시지입니다

이제 Cloud Sync에서 데이터 브로커가 최신 소프트웨어 릴리스를 실행하고 있지 않은 경우를 식별합니다. 이 메시지를 통해 최신 기능을 사용할 수 있습니다.



## 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼, 장치 또는 기능을 식별합니다. 이러한 제한 사항을 주의 깊게 검토하십시오.

- Cloud Sync는 중국에서 지원되지 않습니다.
- 중국 외에 다음 지역에서는 Cloud Sync 데이터 브로커가 지원되지 않습니다.
  - Azure 미국 정부
  - Azure US DoD를 참조하십시오

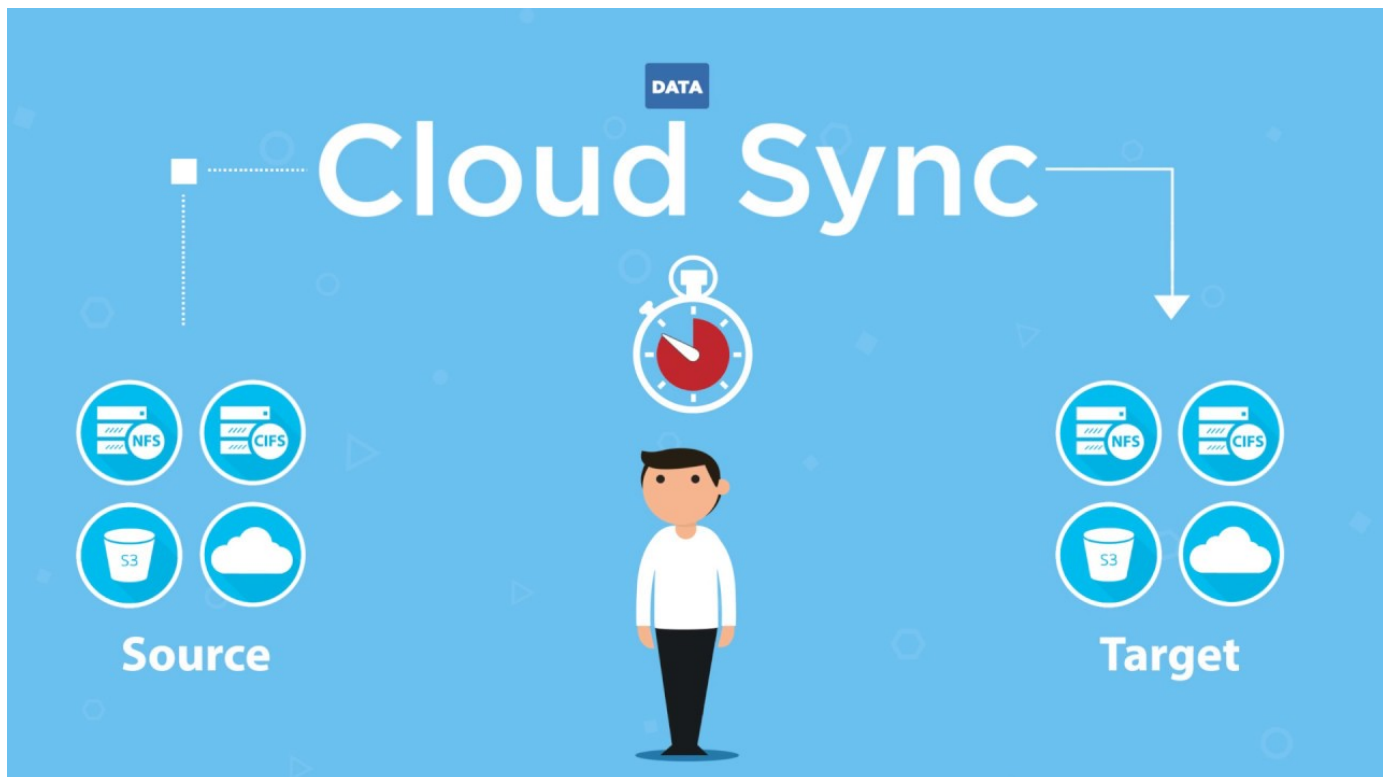
# 시작하십시오

## Cloud Sync 개요

NetApp Cloud Sync 서비스는 데이터를 클라우드 또는 온프레미스의 모든 타겟으로 간단하고 안전하게 자동화된 방법으로 마이그레이션합니다. StorageGRID는 파일 기반 NAS 데이터 세트(NFS 또는 SMB), Amazon S3(Simple Storage Service) 오브젝트 형식, NetApp Cloud Sync® 어플라이언스 또는 기타 클라우드 공급자 오브젝트 저장소 등 그 어떤 형태이든 변환 및 이동할 수 있습니다.

### 피쳐

Cloud Sync에 대한 개요는 다음 비디오에서 확인할 수 있습니다.

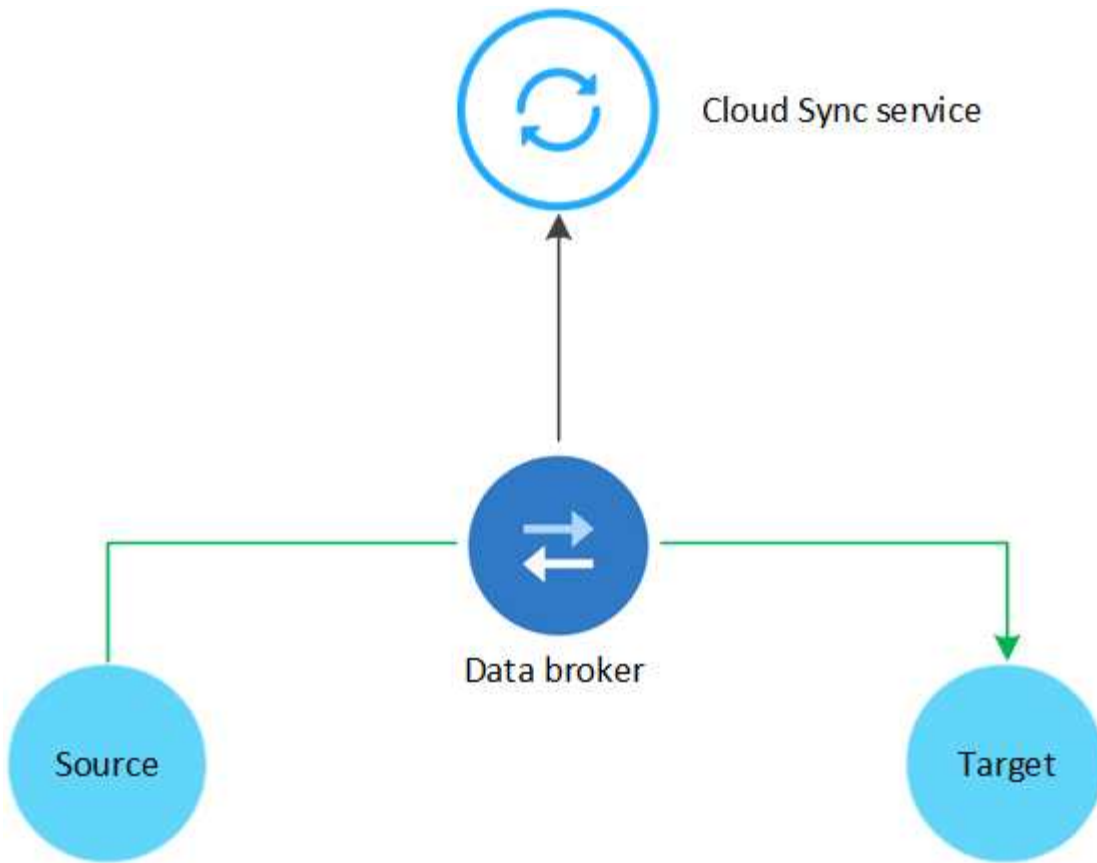


### Cloud Sync의 작동 방식

Cloud Sync는 데이터 브로커 그룹, Cloud Manager를 통해 사용 가능한 클라우드 기반 인터페이스, 소스 및 타겟으로 구성된 서비스형 소프트웨어(SaaS) 플랫폼입니다.

다음 이미지는 Cloud Sync 구성 요소 간의 관계를 보여줍니다.





NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(일명 A\_SYNC Relationship \_). AWS, Azure, Google Cloud Platform 또는 온프레미스에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 포트 443을 통한 아웃바운드 인터넷 연결이 있어야 Cloud Sync 서비스와 통신하고 몇 가지 다른 서비스 및 리포지토리에 연결할 수 있습니다. ["끝점 목록을 봅니다"](#).

초기 복사 후 서비스는 사용자가 설정한 일정에 따라 변경된 데이터를 동기화합니다.

## 지원되는 스토리지 유형입니다

Cloud Sync는 다음과 같은 스토리지 유형을 지원합니다.

- 모든 NFS 서버
- 모든 SMB 서버
- Amazon EFS
- ONTAP용 Amazon FSx
- Amazon S3
- Azure Blob
- Azure NetApp Files
- 상자(미리 보기로 사용 가능)
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google 클라우드 스토리지

- IBM 클라우드 오브젝트 스토리지
- 사내 ONTAP 클러스터
- ONTAP S3 스토리지
- SFTP(API만 사용)
- StorageGRID

"지원되는 동기화 관계를 봅니다".

## 비용

Cloud Sync 사용과 관련된 비용에는 리소스 비용 및 서비스 비용이라는 두 가지 유형이 있습니다.

### 리소스 비용

리소스 요금은 클라우드에서 하나 이상의 데이터 브로커를 실행하는 데 필요한 컴퓨팅 및 스토리지 비용과 관련이 있습니다.

### 서비스 요금

14일 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불할 수 있는 두 가지 방법이 있습니다. 첫 번째 옵션은 AWS 또는 Azure에서 가입하는 것입니다. 가입 서비스를 이용하면 시간 또는 연간 요금을 지불할 수 있습니다. 두 번째 옵션은 NetApp에서 직접 라이선스를 구매하는 것입니다.

"라이선스 작동 방식에 대해 알아보십시오".

## Cloud Sync를 빠르게 시작합니다

Cloud Sync 서비스를 시작하는 데 몇 가지 단계가 포함되어 있습니다.

소스와 타겟이 지원되는지 확인하고 설정합니다. 가장 중요한 요구사항은 데이터 브로커 그룹과 소스 및 타겟 위치 간의 접속을 확인하는 것입니다.

- "지원되는 관계를 봅니다"
- "소스와 타겟을 준비합니다"

NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(일명 A\_SYNC Relationship \_). AWS, Azure, Google Cloud Platform 또는 온프레미스에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 포트 443을 통한 아웃바운드 인터넷 연결이 있어야 Cloud Sync 서비스와 통신하고 몇 가지 다른 서비스 및 리포지토리에 연결할 수 있습니다. "끝점 목록을 봅니다".

Cloud Sync는 동기화 관계를 생성할 때 설치 프로세스를 안내하며, 이 때 클라우드에 데이터 브로커를 구축하거나 자체 Linux 호스트에 대한 설치 스크립트를 다운로드할 수 있습니다.

- "AWS 설치를 검토합니다"
- "Azure 설치를 검토합니다"
- "Google Cloud 설치를 검토합니다"
- "Linux 호스트 설치를 검토합니다"

에 로그인합니다 "클라우드 관리자"를 클릭하고 \* 동기화 \* 를 클릭한 다음 선택한 소스 및 대상을 끌어서 놓습니다.

화면의 지시에 따라 설치를 완료합니다. ["자세한 정보"](#).

AWS 또는 Azure에서 가입하여 용량제 또는 연간 지불 가능합니다. 또는 NetApp에서 직접 라이선스를 구입합니다. Cloud Sync의 라이선스 설정 페이지로 이동하여 설정하기만 하면 됩니다. ["자세한 정보"](#).

## 지원되는 동기화 관계

Cloud Sync를 사용하면 소스에서 타겟으로 데이터를 동기화할 수 있습니다. 이를 동기화 관계라고 합니다. 시작하기 전에 지원되는 관계를 이해해야 합니다.

소스 위치	지원되는 타겟 위치
Amazon EFS	<ul style="list-style-type: none"><li>• Amazon EFS</li><li>• ONTAP용 Amazon FSx</li><li>• Amazon S3</li><li>• Azure Blob</li><li>• Azure NetApp Files</li><li>• Cloud Volumes ONTAP</li><li>• Cloud Volumes Service</li><li>• Google 클라우드 스토리지</li><li>• IBM 클라우드 오브젝트 스토리지</li><li>• NFS 서버</li><li>• 사내 ONTAP 클러스터</li><li>• SMB 서버</li><li>• StorageGRID</li></ul>
ONTAP용 Amazon FSx	<ul style="list-style-type: none"><li>• Amazon EFS</li><li>• ONTAP용 Amazon FSx</li><li>• Amazon S3</li><li>• Azure Blob</li><li>• Azure NetApp Files</li><li>• Cloud Volumes ONTAP</li><li>• Cloud Volumes Service</li><li>• Google 클라우드 스토리지</li><li>• IBM 클라우드 오브젝트 스토리지</li><li>• NFS 서버</li><li>• 사내 ONTAP 클러스터</li><li>• SMB 서버</li><li>• StorageGRID</li></ul>

소스 위치	지원되는 타겟 위치
Amazon S3	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• 상자 <sup>1</sup></li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>
Azure Blob	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>

소스 위치	지원되는 타겟 위치
Azure NetApp Files	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>
상자 <sup>1</sup>	<ul style="list-style-type: none"> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>

소스 위치	지원되는 타겟 위치
Cloud Volumes ONTAP	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>
Cloud Volumes Service	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>

소스 위치	지원되는 타겟 위치
Google 클라우드 스토리지	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• ONTAP S3 스토리지</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>
IBM 클라우드 오브젝트 스토리지	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• 상자 <sup>1</sup></li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>

소스 위치	지원되는 타겟 위치
NFS 서버	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>
온프레미스 ONTAP 클러스터	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>
ONTAP S3 스토리지	<ul style="list-style-type: none"> <li>• Google 클라우드 스토리지</li> <li>• SMB 서버</li> <li>• StorageGRID</li> <li>• ONTAP S3 스토리지</li> </ul>
SFTP <sup>2</sup>	S3



소스 위치	지원되는 타겟 위치
SMB 서버	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• ONTAP S3 스토리지</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>
StorageGRID	<ul style="list-style-type: none"> <li>• Amazon EFS</li> <li>• ONTAP용 Amazon FSx</li> <li>• Amazon S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• 상자 <sup>1</sup></li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Google 클라우드 스토리지</li> <li>• IBM 클라우드 오브젝트 스토리지</li> <li>• NFS 서버</li> <li>• 사내 ONTAP 클러스터</li> <li>• ONTAP S3 스토리지</li> <li>• SMB 서버</li> <li>• StorageGRID</li> </ul>

참고:

1. Box 지원은 미리 보기로 제공됩니다.
2. 이 소스/타겟과의 관계 동기화는 Cloud Sync API만 사용하여 지원됩니다.

3. Blob 컨테이너가 타겟인 경우 특정 Azure Blob 저장소 계층을 선택할 수 있습니다.
  - 핫 스토리지
  - 멋진 보관
4. Amazon S3가 타겟일 때 특정 S3 스토리지 클래스를 선택할 수 있습니다.
  - 표준(기본 클래스)
  - 지능형 계층화
  - 표준 - 낮은 액세스 빈도
  - 단일 영역 - 낮은 액세스 빈도
  - 빙하
  - Glacier 딥 아카이브
5. Google Cloud Storage 버킷이 타겟인 경우 특정 스토리지 클래스를 선택할 수 있습니다.
  - 표준
  - 니어라인
  - 콜드라인
  - 아카이브

## 소스와 타겟을 준비합니다

소스와 타겟이 다음 요구 사항을 충족하는지 확인합니다.

### 네트워킹

- 소스와 타겟이 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

예를 들어, NFS 서버가 데이터 센터에 있고 데이터 브로커가 AWS에 있는 경우 네트워크에서 VPC로 네트워크 연결(VPN 또는 Direct Connect)이 필요합니다.

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

### 대상 디렉토리

동기화 관계를 생성할 때 Cloud Sync를 사용하면 기존 타겟 디렉토리를 선택한 다음 필요에 따라 해당 디렉토리 내에 새 폴더를 생성할 수 있습니다. 따라서 선호하는 타겟 디렉토리가 이미 있는지 확인하십시오.

### 디렉토리를 읽을 수 있는 권한

소스 또는 타겟의 모든 디렉토리 또는 폴더를 표시하려면 Cloud Sync에서 디렉토리 또는 폴더에 대한 읽기 권한이 필요합니다.

### NFS 를 참조하십시오

파일 및 디렉토리에 uid/gid가 있는 소스/대상에서 사용 권한을 정의해야 합니다.

## 오브젝트 스토리지

- AWS 및 Google Cloud의 경우 데이터 브로커에 목록 개체 권한이 있어야 합니다. 이러한 권한은 데이터 브로커 설치 단계를 수행하는 경우 기본적으로 제공됩니다.
- Azure, StorageGRID 및 IBM의 경우 동기화 관계를 설정할 때 입력하는 자격 증명에는 목록 개체 권한이 있어야 합니다.

## 중소기업

동기화 관계를 설정할 때 입력하는 SMB 자격 증명에는 목록 폴더 권한이 있어야 합니다.



데이터 브로커에서는 기본적으로 .snapshot, ~snapshot, .copy-offload 디렉토리를 무시합니다

## Amazon S3 버킷 요구 사항

Amazon S3 버킷이 다음 요구사항을 충족하는지 확인하십시오.

### Amazon S3에 대해 지원되는 데이터 브로커 위치

S3 스토리지를 포함하는 동기화 관계는 AWS 또는 사내에 데이터 브로커가 배포되어야 합니다. 두 경우 모두 설치하는 동안 Cloud Sync에서 데이터 브로커를 AWS 계정에 연결하라는 메시지를 표시합니다.

- ["AWS 데이터 브로커를 구축하는 방법을 알아보십시오"](#)
- ["Linux 호스트에 데이터 브로커를 설치하는 방법에 대해 알아보십시오"](#)

### 지원되는 AWS 영역

중국 지역을 제외한 모든 지역이 지원됩니다.

### 다른 AWS 계정의 S3 버킷에 필요한 권한

동기화 관계를 설정할 때 데이터 브로커와 연결되지 않은 AWS 계정에 상주하는 S3 버킷을 지정할 수 있습니다.

["이 JSON 파일에 포함된 권한"](#) 데이터 브로커가 액세스할 수 있도록 이 S3 버킷에 적용해야 합니다. 이러한 사용 권한을 통해 데이터 브로커가 데이터를 버킷과 복사하거나 버킷의 오브젝트를 나열할 수 있습니다.


JSON 파일에 포함된 권한에 대해서는 다음을 참조하십시오.

1. `<BucketName>`은(는) 데이터 브로커와 연결되지 않은 AWS 계정에 상주하는 버킷의 이름입니다.
2. `<RoleARN>`은(는) 다음 중 하나로 교체해야 합니다.
  - 데이터 브로커가 Linux 호스트에 수동으로 설치된 경우, `<RoleARN>`은 데이터 브로커를 배포할 때 AWS 자격 증명을 제공한 AWS 사용자의 ARN 이어야 합니다.
  - CloudFormation 템플릿을 사용하여 AWS에 데이터 브로커가 배포된 경우, `<RoleARN>`은 템플릿에 의해 생성된 IAM 역할의 ARN 이어야 합니다.

EC2 콘솔로 이동하여 데이터 브로커 인스턴스를 선택하고 설명 탭에서 IAM 역할을 클릭하여 역할 ARN을 찾을 수 있습니다. 그런 다음 IAM 콘솔에서 역할 ARN이 포함된 요약 페이지를 볼 수 있습니다.

## Summary

[Delete role](#)

**Role ARN** `arn:aws:iam::642991748989:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

**Role description** [Edit](#)

### Azure Blob 스토리지 요구 사항

Azure Blob 저장소가 다음 요구사항을 충족하는지 확인합니다.

#### Azure Blob에 지원되는 데이터 브로커 위치

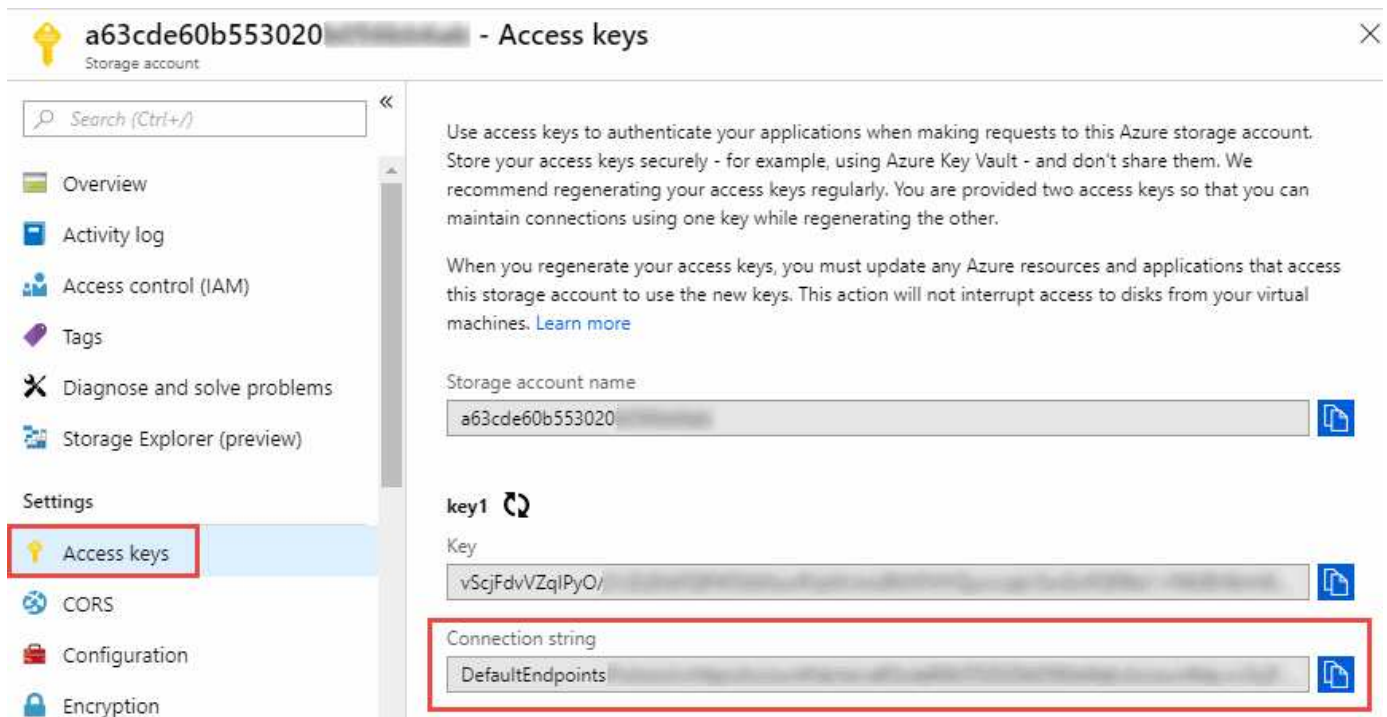
동기화 관계에 Azure Blob 스토리지가 포함된 경우 데이터 브로커가 모든 위치에 상주할 수 있습니다.

#### 지원되는 Azure 지역

중국, 미국 정부 및 미국 국방부 지역을 제외한 모든 지역이 지원됩니다.

#### Azure Blob 및 NFS/SMB를 포함하는 관계의 연결 문자열

Azure Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화 관계를 생성할 때 Cloud Sync에 스토리지 계정 연결 문자열을 제공해야 합니다.



The screenshot shows the 'Access keys' page for an Azure storage account. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Storage Explorer (preview), Settings, Access keys (highlighted), CORS, Configuration, and Encryption. The main content area includes instructions on using access keys and a section for 'key1' with fields for 'Key' and 'Connection string'. The 'Connection string' field is highlighted with a red box.

두 Azure Blob 컨테이너 간에 데이터를 동기화하려면 연결 문자열에 ["공유 액세스 서명입니다"](#) (SAS) Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화할 때 SAS를 사용할 수도 있습니다.

SAS는 Blob 서비스 및 모든 리소스 유형(서비스, 컨테이너 및 개체)에 대한 액세스를 허용해야 합니다. 또한 SAS에는 다음과 같은 사용 권한이 포함되어야 합니다.

- 소스 Blob 컨테이너의 경우 Read 및 List 입니다

- 대상 Blob 컨테이너의 경우 읽기, 쓰기, 목록, 추가 및 만들기 가 있습니다

**Shared access signature**

Allowed services *i*

☒ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types *i*

☒ Service ☒ Container ☒ Object

Allowed permissions *i*

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☐ Update ☐ Process

Start and expiry date/time *i*

Start

2018-10-23 10:07:32 AM

End

2019-10-23 6:07:32 PM

(UTC-04:00) --- Current Time Zone ---

Allowed IP addresses *i*

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols *i*

☒ HTTPS only ☐ HTTPS and HTTP

Signing key *i*

key1

**Generate SAS and connection string**

## Azure NetApp Files 요구 사항

Azure NetApp Files와 데이터를 동기화하거나에서 데이터를 동기화할 때 프리미엄 또는 울트라 서비스 수준을 사용합니다. 디스크 서비스 수준이 Standard인 경우 장애 및 성능 문제가 발생할 수 있습니다.



적합한 서비스 수준을 결정하는 데 도움이 필요한 경우 솔루션 설계자와 상의하십시오. 볼륨 크기와 볼륨 계층에 따라 처리량을 결정합니다.

"Azure NetApp Files 서비스 수준 및 처리량에 대해 자세히 알아보십시오".

## 박스 요건

- Box를 포함하는 동기화 관계를 생성하려면 다음 자격 증명을 제공해야 합니다.
  - 클라이언트 ID입니다
  - 클라이언트 암호
  - 개인 키

- 공개 키 ID입니다
- 암호 구문
- 엔터프라이즈 ID입니다
- Amazon S3에서 Box로 동기화 관계를 생성하는 경우 다음 설정이 1로 설정된 통합 구성이 있는 데이터 브로커 그룹을 사용해야 합니다.
  - 스캐너 동시 사용
  - 스캐너 프로세스 제한
  - 운송 업체 위탁 통화
  - 수송 프로세스 제한

"데이터 브로커 그룹에 대한 통합 구성을 정의하는 방법에 대해 알아보십시오".

## Google Cloud Storage 버킷 요구 사항

Google Cloud Storage 버킷이 다음 요구사항을 충족하는지 확인하십시오.

### Google Cloud Storage에 대한 지원 데이터 브로커 위치

Google Cloud Storage를 포함한 동기화 관계에는 Google Cloud 또는 사내에 구축된 데이터 브로커가 필요합니다. Cloud Sync는 동기화 관계를 생성할 때 데이터 브로커 설치 프로세스를 안내합니다.

- ["Google Cloud 데이터 브로커를 구축하는 방법을 알아보십시오"](#)
- ["Linux 호스트에 데이터 브로커를 설치하는 방법에 대해 알아보십시오"](#)

### 지원되는 Google Cloud 지역

모든 지역이 지원됩니다.

### 다른 Google Cloud 프로젝트의 버킷에 대한 권한

동기화 관계를 설정할 때 데이터 브로커의 서비스 계정에 필요한 권한을 제공하는 경우 다양한 프로젝트의 Google Cloud 버킷 중에서 선택할 수 있습니다. ["서비스 계정 설정 방법에 대해 알아보십시오"](#).

### SnapMirror 대상에 대한 권한입니다

동기화 관계의 소스가 SnapMirror 대상(읽기 전용)인 경우 "읽기/목록" 사용 권한으로 소스의 데이터를 타겟으로 동기화할 수 있습니다.

## NFS 서버 요구 사항

- NFS 서버는 NetApp 시스템이거나 NetApp이 아닌 시스템이 될 수 있습니다.
- 파일 서버는 데이터 브로커 호스트가 필요한 포트를 통해 내보내기에 액세스할 수 있도록 허용해야 합니다.
  - 111 TCP/UDP
  - 2049 TCP/UDP
  - 5555 TCP/UDP

- NFS 버전 3, 4.0, 4.1 및 4.2가 지원됩니다.

서버에서 원하는 버전을 활성화해야 합니다.

- ONTAP 시스템에서 NFS 데이터를 동기화하려면 SVM을 위한 NFS 내보내기 목록에 대한 액세스가 활성화되어 있는지 확인하십시오(vserver NFS modify -vserver\_svm\_name\_-showmount 설정).



showmount의 기본 설정은 ONTAP 9.2부터 \_enabled\_입니다.

## ONTAP 요구 사항

동기화 관계에 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 클러스터가 포함되어 있고 NFSv4 이상을 선택한 경우 ONTAP 시스템에서 NFSv4 ACL을 설정해야 합니다. ACL을 복제하려면 이 작업이 필요합니다.

## ONTAP S3 스토리지 요구 사항

을 포함하는 동기화 관계를 설정할 때 "ONTAP S3 스토리지"다음을 제공해야 합니다.

- ONTAP S3에 연결된 LIF의 IP 주소입니다
- ONTAP에서 사용하도록 구성된 액세스 키 및 암호 키입니다

## SMB 서버 요구 사항

- SMB 서버는 NetApp 시스템 또는 NetApp이 아닌 시스템일 수 있습니다.
- SMB 서버에 대한 권한이 있는 자격 증명을 Cloud Sync에 제공해야 합니다.
  - 소스 SMB 서버의 경우 목록 및 읽기 권한이 필요합니다.

Backup Operators 그룹의 구성원은 소스 SMB 서버에서 지원됩니다.

- 대상 SMB 서버의 경우 목록, 읽기 및 쓰기의 권한이 필요합니다.
- 파일 서버는 데이터 브로커 호스트가 필요한 포트를 통해 내보내기에 액세스할 수 있도록 허용해야 합니다.
  - 139 TCP 를 참조하십시오
  - 445 TCP
  - 137-138 UDP
- SMB 버전 1.0, 2.0, 2.1, 3.0 및 3.11이 지원됩니다.
- "Administrators" 그룹에 소스 및 대상 폴더에 "모든 권한" 권한을 부여합니다.

이 권한을 부여하지 않으면 데이터 브로커에 파일 또는 디렉터리에 대한 ACL을 가져올 수 있는 권한이 충분하지 않을 수 있습니다. 이 경우 "getxattr error 95" 오류가 발생합니다.

## 숨겨진 디렉토리 및 파일에 대한 SMB 제한

SMB 제한은 SMB 서버 간에 데이터를 동기화할 때 숨겨진 디렉터리 및 파일에 영향을 줍니다. 소스 SMB 서버의 디렉터리 또는 파일이 Windows를 통해 숨겨진 경우 숨겨진 속성은 타겟 SMB 서버로 복제되지 않습니다.

대소문자 구분 제한 때문에 **SMB** 동기화 동작이 발생합니다

SMB 프로토콜은 대/소문자를 구분하지 않으므로 대문자와 소문자가 동일하게 처리됩니다. 이 동작은 동기화 관계에 SMB 서버가 포함되어 있고 데이터가 이미 타겟에 존재하는 경우 덮어쓰 파일 및 디렉토리 복사 오류를 발생시킬 수 있습니다.

예를 들어, 소스에 "A"라는 파일이 있고 대상에 "A"라는 이름의 파일이 있다고 가정해 보겠습니다. Cloud Sync가 "A"라는 파일을 대상에 복사하면 파일 "A"가 소스의 파일 "A"에 의해 덮어쓰여집니다.

디렉토리의 경우 소스에 "b"라는 디렉토리가 있고 타겟에 "B"라는 디렉토리가 있다고 가정해 보겠습니다. Cloud Sync가 "b"라는 디렉토리를 타겟으로 복제하려고 하면 Cloud Sync에서 디렉토리가 이미 존재함을 나타냅니다. 따라서 Cloud Sync는 항상 "b"라는 이름의 디렉토리를 복사하지 못합니다.

이 제한을 피하는 가장 좋은 방법은 데이터를 빈 디렉토리에 동기화하는 것입니다.

## Cloud Sync의 네트워킹 개요

Cloud Sync용 네트워킹에는 데이터 브로커 그룹과 소스 및 대상 위치 간의 연결과 포트 443을 통한 데이터 브로커로부터의 아웃바운드 인터넷 연결이 포함됩니다.

### 데이터 브로커 위치

데이터 브로커 그룹은 클라우드 또는 사내에 설치되는 하나 이상의 데이터 브로커로 구성됩니다.

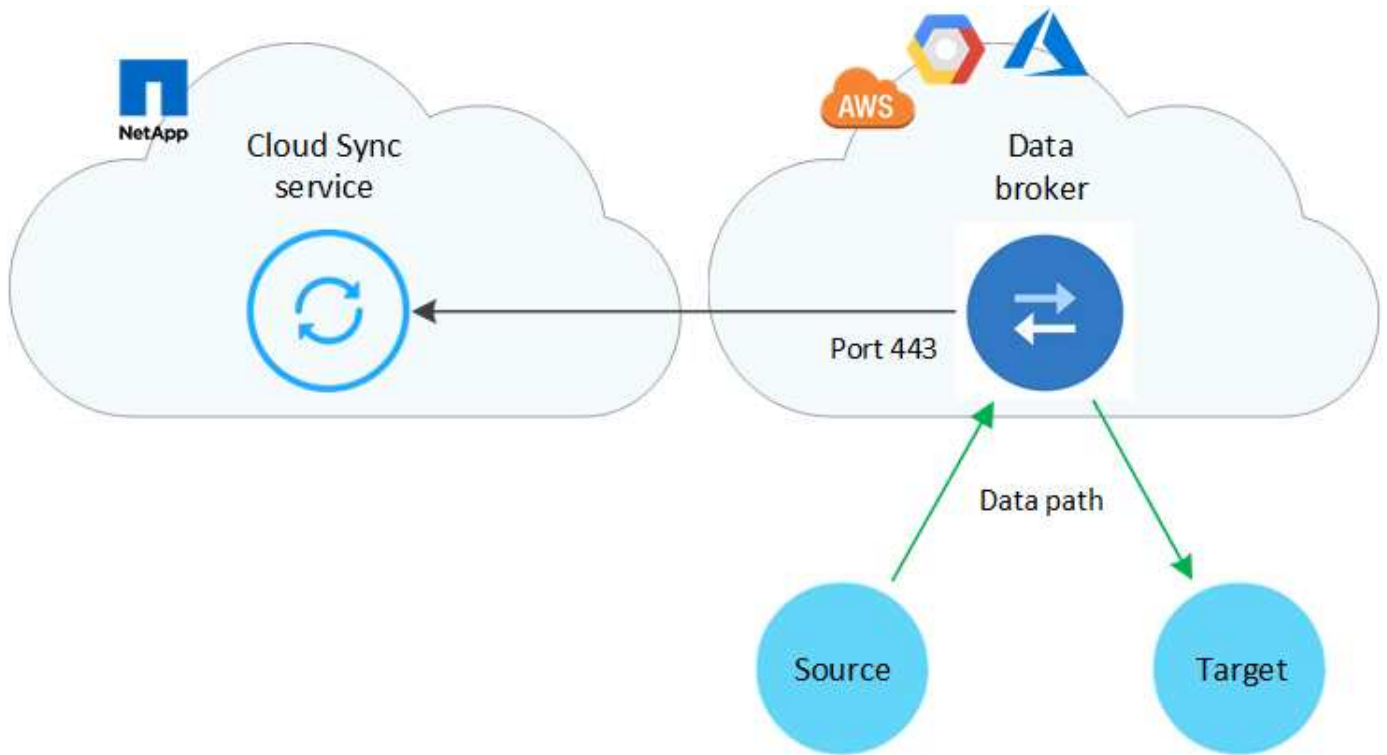
### 클라우드 내 데이터 브로커

다음 이미지는 AWS, Google Cloud 또는 Azure에서 클라우드에서 실행 중인 데이터 브로커를 보여줍니다. 데이터 브로커에 대한 연결이 있는 한 소스와 타겟이 모든 위치에 있을 수 있습니다. 예를 들어, 데이터 센터와 클라우드 공급자에 VPN 연결을 설정할 수 있습니다.



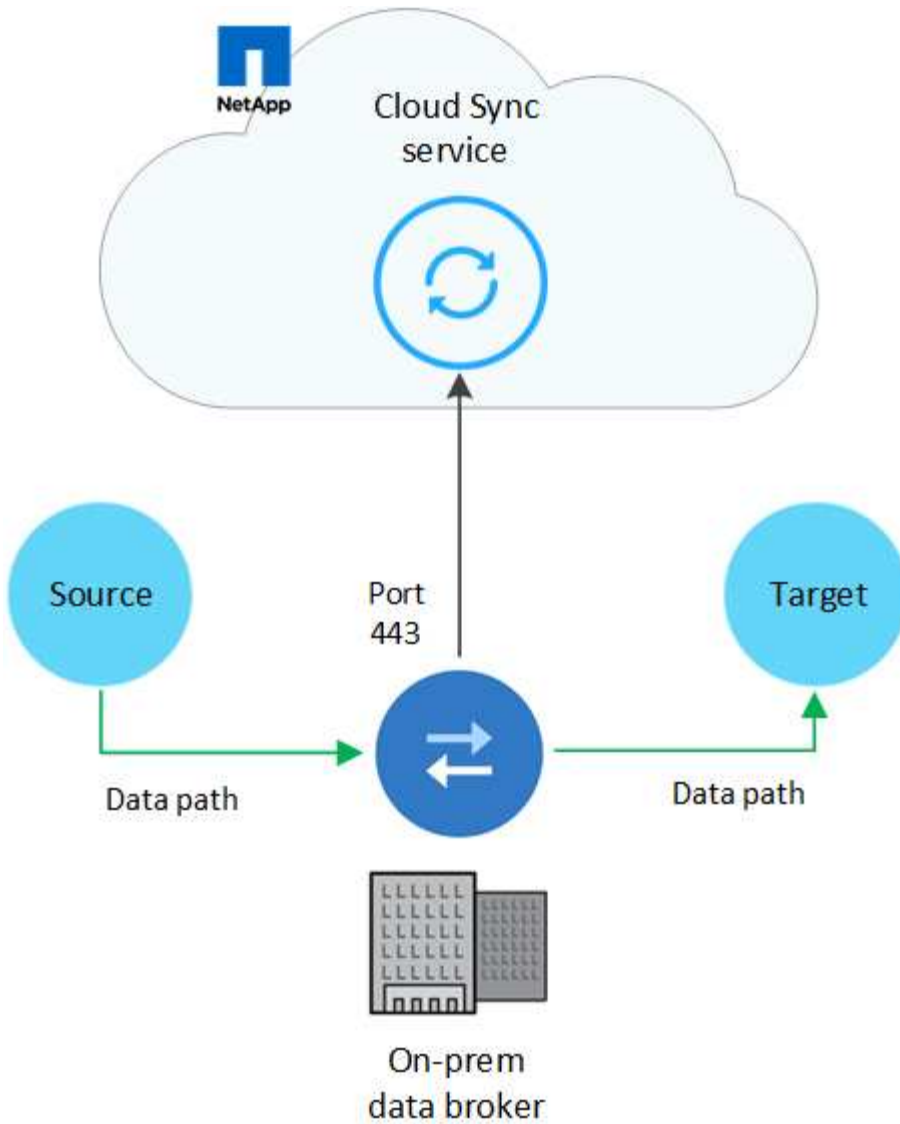
Cloud Sync은 AWS, Azure 또는 Google Cloud에 데이터 브로커를 구축할 경우 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.





#### 사내 데이터 브로커

다음 이미지는 사내 데이터 센터에서 실행되는 데이터 브로커를 보여줍니다. 다시 한 번 말씀드리지만, 데이터 브로커에 대한 연결이 있는 한 소스 및 타겟이 모든 위치에 있을 수 있습니다.



## 네트워킹 요구 사항

- 소스와 타겟이 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

예를 들어, NFS 서버가 데이터 센터에 있고 데이터 브로커가 AWS에 있는 경우 네트워크에서 VPC로 네트워크 연결(VPN 또는 Direct Connect)이 필요합니다.

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.
- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

## 네트워킹 엔드포인트

NetApp 데이터 브로커는 포트 443을 통한 아웃바운드 인터넷 액세스를 통해 Cloud Sync 서비스와 통신하고 몇 가지 다른 서비스 및 리포지토리에 연락해야 합니다. 로컬 웹 브라우저에서도 특정 작업을 수행하려면 끝점에 액세스해야 합니다. 아웃바운드 연결을 제한해야 하는 경우 아웃바운드 트래픽에 대해 방화벽을 구성할 때 다음 엔드포인트 목록을 참조하십시오.

## 데이터 브로커 엔드포인트

데이터 브로커가 다음 엔드포인트에 연결합니다.

엔드포인트	목적
<a href="https://olcentgbl.trafficmanager.net">https://olcentgbl.trafficmanager.net</a> 으로 문의하십시오	데이터 브로커 호스트의 CentOS 패키지를 업데이트하기 위해 리포지토리에 접속하려면 이 엔드포인트는 CentOS 호스트에 데이터 브로커를 수동으로 설치하는 경우에만 연결됩니다.
<a href="https://rpm.nodesource.com">https://rpm.nodesource.com</a> <a href="https://registry.npmjs.org">https://registry.npmjs.org</a> <a href="https://nodejs.org">https://nodejs.org</a> : 를 참조하십시오	개발에 사용되는 Node.js, NPM 및 기타 타사 패키지를 업데이트하기 위한 리포지토리에 접속합니다.
<a href="https://tgz.pm2.io">https://tgz.pm2.io</a> 으로 문의하십시오	Cloud Sync를 모니터링하는 데 사용되는 타사 패키지인 PM2를 업데이트하기 위한 리포지토리에 액세스합니다.
<a href="https://sqs.us-east-1.amazonaws.com">https://sqs.us-east-1.amazonaws.com</a> <a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a> 으로 문의하십시오	Cloud Sync에서 운영에 사용하는 AWS 서비스(파일 대기열 처리, 작업 등록, 데이터 브로커에 업데이트 제공)에 연락하려면
<a href="https://s3.region.amazonaws.com">https://s3.region.amazonaws.com</a> 예: s3.us-east-2.amazonaws.com:443 <a href="https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region">https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region</a> ["S3 엔드포인트 목록은 AWS 설명서를 참조하십시오"]	동기화 관계에 S3 버킷이 포함된 경우 Amazon S3에 연락하려면
<a href="https://s3.us-east-1.amazonaws.com">https://s3.us-east-1.amazonaws.com</a> 으로 문의하십시오	Cloud Sync에서 데이터 브로커 로그를 다운로드하면 데이터 브로커가 로그 디렉토리를 지퍼하고 로그를 us-east-1 지역의 미리 정의된 S3 버킷으로 업로드합니다.
<a href="https://cf.cloudsync.netapp.com">https://cf.cloudsync.netapp.com</a> <a href="https://repo.cloudsync.netapp.com">https://repo.cloudsync.netapp.com</a> 으로 문의하십시오	Cloud Sync 서비스에 문의하십시오.
<a href="https://support.netapp.com">https://support.netapp.com</a> 으로 문의하십시오	BYOL 라이선스를 사용하여 동기화 관계에 대한 NetApp 지원 팀에 문의
<a href="https://fedoraproject.org">https://fedoraproject.org</a> 으로 문의하십시오	설치 및 업데이트 중에 데이터 브로커 가상 머신에 7z를 설치하려면 다음을 수행합니다. 7z는 NetApp 기술 지원 팀에 AutoSupport 메시지 전송 기능이 필요합니다.
<a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> 으로 문의하십시오	데이터 브로커가 AWS에 구축되거나 사내 구축 시에 AWS 자격 증명이 제공되고 AWS 자격 증명이 제공됩니다. 데이터 브로커가 배포, 업데이트 및 재시작 중에 이 엔드포인트에 연결합니다.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> 으로 문의하십시오	데이터 센스를 사용하여 새 동기화 관계를 위한 소스 파일을 선택할 때 클라우드 데이터 센스에 문의하려면

## 웹 브라우저 끝점

문제 해결을 위해 로그를 다운로드하려면 웹 브라우저에서 다음 끝점에 액세스해야 합니다.

logs.cloudsync.netapp.com:443

# 데이터 브로커를 설치합니다

## AWS에서 새 데이터 브로커 생성

새 데이터 브로커 그룹을 생성하는 경우 Amazon Web Services 를 선택하여 VPC의 새 EC2 인스턴스에 데이터 브로커 소프트웨어를 배포합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

클라우드 또는 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치할 수도 있습니다. ["자세한 정보"](#).

지원되는 **AWS** 영역

중국 지역을 제외한 모든 지역이 지원됩니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

Cloud Sync는 AWS에 데이터 브로커를 구축할 때 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다. 설치 프로세스 중에 프록시 서버를 사용하도록 데이터 브로커를 구성할 수 있습니다.

아웃바운드 연결을 제한해야 하는 경우 를 참조하십시오 ["데이터 브로커가 연락하는 끝점 목록입니다"](#).

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

**AWS**에서 데이터 브로커를 구축하는 데 필요한 권한입니다

데이터 브로커를 구축하는 데 사용하는 AWS 사용자 계정에 에 포함된 권한이 있어야 합니다 ["NetApp에서 제공하는 정책입니다"](#).

**AWS** 데이터 브로커와 함께 **IAM** 역할을 사용해야 합니다

Cloud Sync는 데이터 브로커를 배포할 때 데이터 브로커 인스턴스에 대해 IAM 역할을 생성합니다. 원할 경우 자체 IAM 역할을 사용하여 데이터 브로커를 배포할 수 있습니다. 조직에 엄격한 보안 정책이 있는 경우 이 옵션을 사용할 수 있습니다.

IAM 역할은 다음 요구 사항을 충족해야 합니다.

- IAM 역할을 신뢰할 수 있는 엔터티로 사용하려면 EC2 서비스가 허용되어야 합니다.
- ["이 JSON 파일에 정의된 권한"](#) 데이터 브로커가 올바르게 작동할 수 있도록 IAM 역할에 연결해야 합니다.

데이터 브로커를 배포할 때 IAM 역할을 지정하려면 아래 단계를 따르십시오.

데이터 브로커 생성

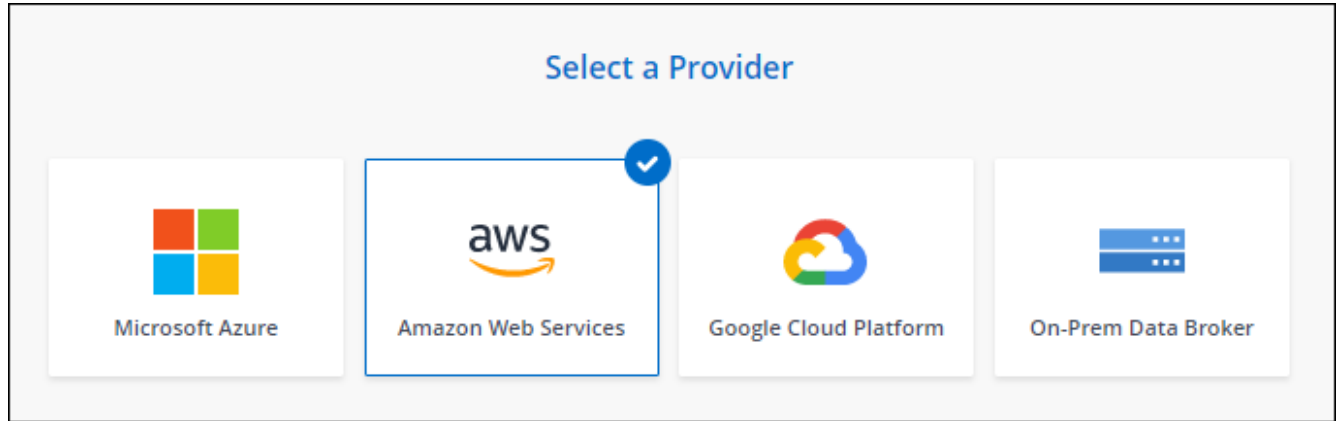
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 생성할 때 AWS에서 데이터 브로커를 설치하는 방법을 설명합니다.

단계

1. 새 동기화 만들기 \* 를 클릭합니다.
2. 동기화 관계 정의 \* 페이지에서 소스 및 대상을 선택하고 \* 계속 \* 을 클릭합니다.

데이터 브로커 그룹 \* 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 \* 페이지에서 \* 데이터 브로커 \* 생성 을 클릭한 다음 \* Amazon Web Services \* 를 선택합니다.



4. 데이터 브로커의 이름을 입력하고 \* 계속 \* 을 클릭합니다.
5. AWS 액세스 키를 입력하여 Cloud Sync에서 대신 AWS에서 데이터 브로커를 생성할 수 있습니다.

키는 다른 용도로 저장되거나 사용되지 않습니다.

액세스 키를 제공하지 않고 싶은 경우 페이지 하단에 있는 링크를 클릭하여 CloudFormation 템플릿을 대신 사용하십시오. 이 옵션을 사용할 경우 AWS에 직접 로그인하므로 자격 증명을 제공할 필요가 없습니다.

다음 비디오에서는 CloudFormation 템플릿을 사용하여 데이터 브로커 인스턴스를 시작하는 방법을 설명합니다.

▶ [https://docs.netapp.com/ko-kr/cloud-manager-sync//media/video\\_cloud\\_sync.mp4](https://docs.netapp.com/ko-kr/cloud-manager-sync//media/video_cloud_sync.mp4) (video)

6. AWS 액세스 키를 입력한 경우, 인스턴스에 대한 위치를 선택하고 키 쌍을 선택한 다음 공용 IP 주소 활성화 여부를 선택한 다음 기존 IAM 역할을 선택하거나 필드를 비워 Cloud Sync에서 역할을 생성합니다.

IAM 역할을 직접 선택할 경우 **필요한 권한을 제공해야 합니다.**

### Basic Settings

**Location**

Region  

US West | Oregon
▼

VPC  

vpc-3c46c059 - 10.60.21.0/25
▼

Subnet  

10.60.21.0/25
▼

**Connectivity**

Key Pair  

newKey
▼

**Enable Public IP?**

☒ Enable ☐ Disable

**IAM Role (optional)** ⓘ

7. VPC의 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.
  8. 데이터 브로커를 사용할 수 있게 되면 Cloud Sync에서 \* 계속 \* 을 클릭합니다.
- 다음 이미지는 AWS에 성공적으로 구축된 인스턴스를 보여줍니다.

✓ NFS Server
2 Data Broker Group
 3 Directories
 4 Target NFS Server
 >

### Select a Data Broker Group

1 Data Broker Group Q

⊞
ben-data-broker
➤

1	N/A	0	<span style="color: green;">✓</span> 1 Active
Data Brokers	Transfer Rate	Relationships	Data Brokers Status

9. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

AWS에 데이터 브로커를 구축하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브roker 그룹을 추가 동기화 관계에 사용할 수 있습니다.

데이터 브roker 인스턴스에 대한 세부 정보

Cloud Sync은 다음 구성을 사용하여 AWS에서 데이터 브roker를 생성합니다.

인스턴스 유형

m5n.xlarge(m5n.xlarge)(해당 지역에서 사용할 수 있는 경우), 그렇지 않은 경우 m5.xlarge

## vCPU

4

## RAM

16GB

## 운영 체제

Amazon Linux 2

## 디스크 크기 및 유형입니다

10GB GP2 SSD

## Azure에서 새 데이터 브로커 생성

새 데이터 브로커 그룹을 생성할 때 Microsoft Azure를 선택하여 VNET의 새 가상 머신에 데이터 브로커 소프트웨어를 배포합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

클라우드 또는 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치할 수도 있습니다. ["자세한 정보"](#).

## 지원되는 Azure 지역

중국, 미국 정부 및 미국 국방부 지역을 제외한 모든 지역이 지원됩니다.

## 네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

Cloud Sync는 Azure에 데이터 브로커를 배포할 때 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.

아웃바운드 연결을 제한해야 하는 경우 를 참조하십시오 ["데이터 브로커가 연락하는 끝점 목록입니다"](#).

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

## Azure에서 데이터 브로커를 배포하는 데 필요한 권한입니다

데이터 브로커를 배포하는 데 사용하는 Azure 사용자 계정에 다음과 같은 권한이 있는지 확인합니다.

```
{
  "Name": "Azure Data Broker",
  "Actions": [
    "Microsoft.Resources/subscriptions/read",
    "Microsoft.Resources/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
```

```

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/publicIPAddresses/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",

"Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Compute/disks/write",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/publicIPAddresses/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/publicIPAddresses/join/action",
    "Microsoft.Network/networkInterfaces/join/action"
],
"NotActions": [],
"AssignableScopes": [],
"Description": "Azure Data Broker",
"IsCustom": "true"
}

```

## 인증 방법

데이터 브로커를 구축할 때는 가상 머신의 인증 방법, 즉 암호 또는 SSH 공개-개인 키 쌍을 선택해야 합니다.

키 쌍 생성에 대한 도움말은 을 참조하십시오 ["Azure 설명서: Azure에서 Linux VM용 SSH 공개-개인 키 쌍을 생성하고 사용합니다"](#).



## 데이터 브로커 생성

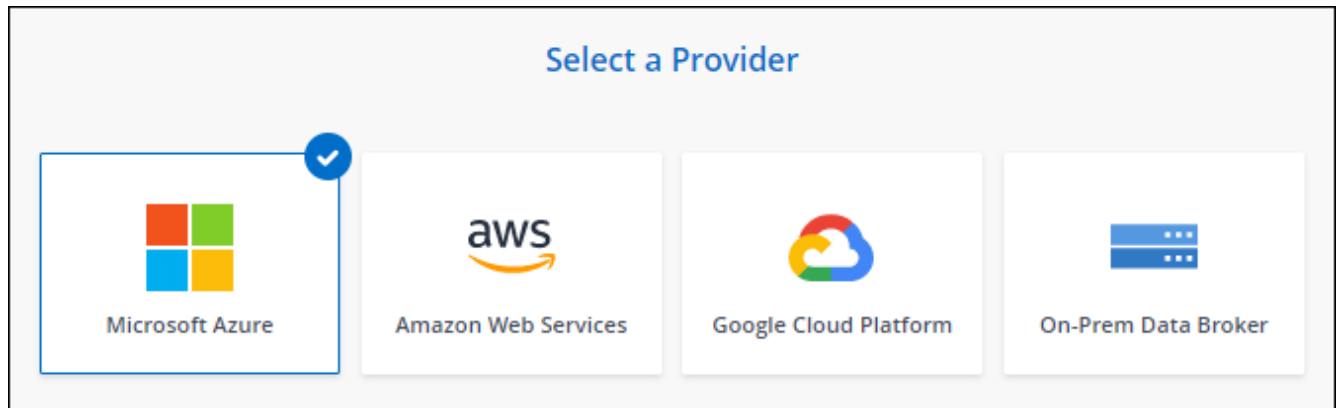
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 만들 때 Azure에서 데이터 브로커를 설치하는 방법을 설명합니다.

### 단계

1. 새 동기화 만들기 \* 를 클릭합니다.
2. 동기화 관계 정의 \* 페이지에서 소스 및 대상을 선택하고 \* 계속 \* 을 클릭합니다.

데이터 브로커 그룹 \* 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 \* 페이지에서 \* 데이터 브로커 \* 만들기 를 클릭한 다음 \* Microsoft Azure \* 를 선택합니다.



4. 데이터 브로커의 이름을 입력하고 \* 계속 \* 을 클릭합니다.
5. 메시지가 표시되면 Microsoft 계정에 로그인합니다. 메시지가 표시되지 않으면 \* Azure에 로그인 \* 을 클릭합니다.

이 양식은 Microsoft에서 소유하고 호스팅됩니다. 자격 증명이 NetApp에 제공되지 않습니다.

6. 데이터 브로커의 위치를 선택하고 가상 시스템에 대한 기본 세부 정보를 입력합니다.

Location	Virtual Machine
Subscription <div>OCCM Dev ▼</div>	VM Name <div>netappdatabroker</div>
Azure Region <div>West US 2 ▼</div>	User Name <div>databroker</div>
VNet <div>Vnet1 ▼</div>	<b>Authentication Method:</b> <input checked="" type="radio"/> Password <input type="radio"/> Public Key
Subnet <div>Subnet1 ▼</div>	Enter Password <div>.....</div>
	<b>Resource Group:</b> <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group

7. VNET에서 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.

8. 계속 \* 을 클릭하고 배포가 완료될 때까지 페이지를 열어 둡니다.

이 프로세스는 최대 7분 정도 소요될 수 있습니다.

9. Cloud Sync에서 데이터 브로커를 사용할 수 있게 되면 \* 계속 \* 을 클릭합니다.

10. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

Azure에서 데이터 브로커를 구축하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브로커를 추가 동기화 관계에 사용할 수 있습니다.

## 관리자 동의를 필요하다는 메시지를 받았습니까?

Cloud Sync에서 사용자 대신 조직의 리소스에 액세스할 수 있는 권한이 필요하므로 관리자 승인이 필요하다는 메시지가 나타나면 다음 두 가지 옵션을 사용할 수 있습니다.

1. AD 관리자에게 다음 권한을 제공하도록 요청하십시오.

Azure에서 \* 관리 센터 > Azure AD > 사용자 및 그룹 > 사용자 설정 \* 으로 이동하여 \* 사용자가 회사 데이터에 액세스하는 앱에 대신 \* 사용자 동의를 할 수 있습니다 \*.

2. AD 관리자에게 다음 URL(관리자 동의 엔드포인트)을 사용하여 \* CloudSync-AzureDataBrokerCreator \* 에 대해 사용자 대신 동의하도록 요청하십시오.

`https://login.microsoftonline.com/{FILL 여기서 귀하의 테넌트 ID}  
/v2.0/adminConsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85 &  
redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read`

URL에 표시된 것처럼 앱 URL은 `https://cloudsync.netapp.com` 이고 응용 프로그램 클라이언트 ID는 `8ee4ca3a-bafa-4831-97cc-5a38923cab85`입니다.

데이터 브로커 **VM**에 대한 세부 정보

Cloud Sync는 다음 구성을 사용하여 Azure에서 데이터 브로커를 생성합니다.

**VM** 유형입니다

표준 DS4 v2

**vCPU**

8

**RAM**

28GB

운영 체제

CentOS 7.7

디스크 크기 및 유형입니다

64GB 프리미엄 SSD

## Google Cloud에서 새로운 데이터 브로커 생성

새 데이터 브로커 그룹을 생성하는 경우 Google Cloud Platform 을 선택하여 Google Cloud VPC의 새 가상 머신 인스턴스에 데이터 브로커 소프트웨어를 배포합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

클라우드 또는 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치할 수도 있습니다. ["자세한 정보"](#).

## 지원되는 Google Cloud 지역

모든 지역이 지원됩니다.

## 네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Cloud Sync 서비스를 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

Cloud Sync가 Google Cloud에 데이터 브로커를 배포할 때 필요한 아웃바운드 통신을 지원하는 보안 그룹을 만듭니다.

아웃바운드 연결을 제한해야 하는 경우 를 참조하십시오 ["데이터 브로커가 연락하는 끝점 목록입니다"](#).

- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

## Google Cloud에서 데이터 브로커를 배포하는 데 필요한 권한입니다

데이터 브로커를 배포하는 Google Cloud 사용자에게 다음과 같은 권한이 있는지 확인합니다.

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

## 서비스 계정에 필요한 권한입니다

데이터 브로커를 배포할 때 다음과 같은 권한이 있는 서비스 계정을 선택해야 합니다.

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
- iam.serviceAccounts.signJwt
```



"iam.serviceAccounts.signJwt" 권한은 외부 HashashCorp 볼트를 사용하도록 데이터 브로커를 설정할 계획에만 필요합니다.

## 데이터 브로커 생성

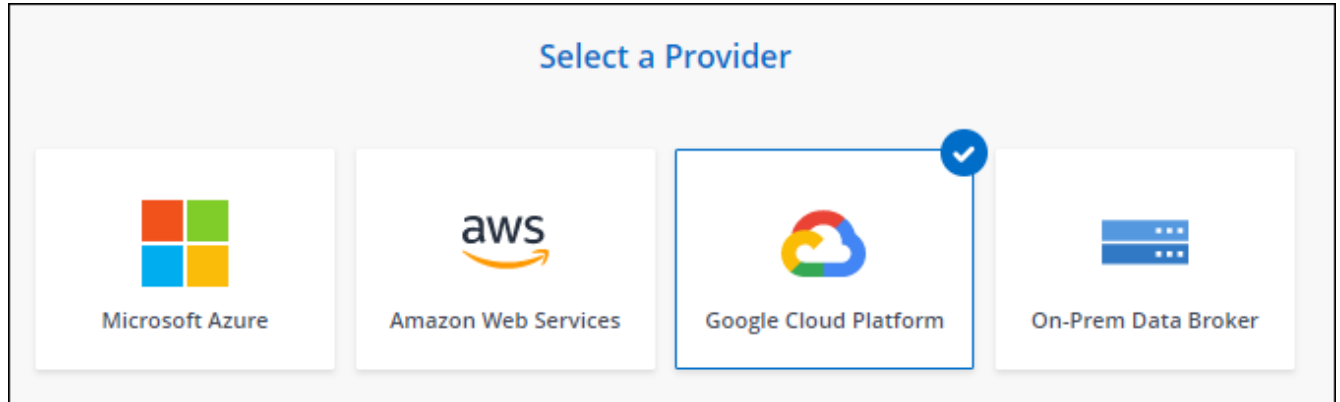
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 생성할 때 Google Cloud에 데이터 브로커를 설치하는 방법을 설명합니다.

## 단계

1. 새 동기화 만들기 \* 를 클릭합니다.
2. 동기화 관계 정의 \* 페이지에서 소스 및 대상을 선택하고 \* 계속 \* 을 클릭합니다.

데이터 브로커 그룹 \* 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 \* 페이지에서 \* 데이터 브로커 \* 만들기 를 클릭한 다음 \* Microsoft Azure \* 를 선택합니다.



4. 데이터 브로커의 이름을 입력하고 \* 계속 \* 을 클릭합니다.
5. 메시지가 표시되면 Google 계정으로 로그인합니다.

이 양식은 Google에서 소유하고 호스팅됩니다. 자격 증명이 NetApp에 제공되지 않습니다.

6. 프로젝트 및 서비스 계정을 선택한 다음 공용 IP 주소 활성화 또는 비활성화 여부를 포함하여 데이터 브로커의 위치를 선택합니다.

공용 IP 주소를 사용하지 않는 경우 다음 단계에서 프록시 서버를 정의해야 합니다.

Basic Settings

<b>Project</b> Project <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">OCCM-Dev ▼</div> Service Account <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">test ▼</div> Select a Service Account that includes <a href="#">these permissions</a>	<b>Location</b> Region <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">us-west1 ▼</div> Zone <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">us-west1-a ▼</div> VPC <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">default ▼</div> Subnet <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">default ▼</div> Public IP <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">Enable ▼</div>
--	---

7. VPC의 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.

인터넷 액세스에 프록시가 필요한 경우 프록시는 Google Cloud에 있어야 하며 데이터 브로커와 동일한 서비스 계정을 사용해야 합니다.

8. 데이터 브로커를 사용할 수 있게 되면 Cloud Sync에서 \* 계속 \* 을 클릭합니다.

인스턴스를 구축하는 데 약 5~10분이 소요됩니다. Cloud Sync 서비스에서 진행 상황을 모니터링할 수 있으며, 이 경우 인스턴스를 사용할 수 있을 때 자동으로 새로 고쳐집니다.

9. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

Google Cloud에 데이터 브로커를 구축하고 새로운 동기화 관계를 구축했습니다. 이 데이터 브로커를 추가 동기화 관계에 사용할 수 있습니다.

다른 **Google Cloud** 프로젝트에 버킷을 사용할 수 있는 권한 제공

동기화 관계를 생성하고 Google 클라우드 스토리지를 소스 또는 타겟으로 선택할 때, Cloud Sync을 사용하면 데이터 브로커의 서비스 계정에 사용할 수 있는 버킷 중에서 선택할 수 있습니다. 기본적으로 여기에는 데이터 브로커 서비스 계정과 `_Same_PROJECT`에 있는 버킷이 포함됩니다. 그러나 필요한 권한을 제공하는 경우 `_other_projects`에서 버킷을 선택할 수 있습니다.

단계

1. Google Cloud Platform 콘솔을 열고 클라우드 스토리지 서비스를 로드합니다.

2. 동기화 관계에서 소스 또는 타겟으로 사용할 버킷의 이름을 클릭합니다.
3. 사용 권한 \* 을 클릭합니다.
4. 추가 \* 를 클릭합니다.
5. 데이터 브로커의 서비스 계정 이름을 입력합니다.
6. 에서 제공하는 역할을 선택합니다 [위와 동일한 권한](#).
7. 저장 \* 을 클릭합니다.

동기화 관계를 설정하면 이제 해당 버킷을 동기화 관계의 소스 또는 타겟으로 선택할 수 있습니다.

데이터 브로커 **VM** 인스턴스에 대한 세부 정보

Cloud Sync은 다음 구성을 사용하여 Google Cloud에서 데이터 브로커를 생성합니다.

기계 유형

N1-표준-4

**vCPU**

4

**RAM**

15GB

운영 체제

Red Hat Enterprise Linux 7.7

디스크 크기 및 유형입니다

20GB HDD PD 표준

## Linux 호스트에 데이터 브로커 설치

새 데이터 브로커 그룹을 생성할 때 사내 Linux 호스트 또는 클라우드의 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치하려면 온프레미스 데이터 브로커 옵션을 선택합니다. Cloud Sync는 설치 프로세스를 안내하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

**Linux** 호스트 요구 사항

- \* 운영 체제 \*:
  - CentOS 7.0, 7.7 및 8.0
  - CentOS 스트림은 지원되지 않습니다.
  - Red Hat Enterprise Linux 7.7 및 8.0
  - Ubuntu 서버 20.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

데이터 브로커를 설치하기 전에 호스트에서 'yum update all' 명령을 실행해야 합니다.

Red Hat Enterprise Linux 시스템은 Red Hat 서브스크립션 관리 에 등록되어 있어야 합니다. 등록되지 않은 경우, 시스템은 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 리포지토리에 액세스할 수 없습니다.

- RAM \*: 16GB
- \* CPU \*: 4코어
- \* 여유 디스크 공간 \*: 10GB
- \* SELinux \*: 을 사용하지 않는 것이 좋습니다 "SELinux" 호스트.

SELinux는 데이터 브로커 소프트웨어 업데이트를 차단하는 정책을 적용하고 데이터 브로커가 정상 작동에 필요한 엔드포인트에 접속하는 것을 차단할 수 있습니다.

#### 네트워킹 요구 사항

- Linux 호스트에 소스와 타겟에 대한 접속이 있어야 합니다.
- 파일 서버는 Linux 호스트가 내보내기에 액세스할 수 있도록 허용해야 합니다.
- AWS로 나가는 트래픽을 위해 Linux 호스트에서 포트 443이 열려 있어야 합니다(데이터 브로커가 Amazon SQS 서비스와 지속적으로 통신).
- 소스, 타겟 및 데이터 브로커가 NTP(Network Time Protocol) 서비스를 사용하도록 구성하는 것이 좋습니다. 세 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

#### AWS에 대한 액세스 설정

S3 버킷을 포함하는 동기화 관계에 데이터 브로커를 사용할 계획이라면, AWS 액세스를 위한 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때는 프로그래밍 방식의 액세스와 특정 권한이 있는 AWS 사용자에게 AWS 키를 제공해야 합니다.

##### 단계

1. 을 사용하여 IAM 정책을 생성합니다 "NetApp에서 제공하는 정책입니다"

"AWS 지침을 확인하십시오"

2. 프로그래밍 방식으로 액세스할 수 있는 IAM 사용자를 생성합니다.

"AWS 지침을 확인하십시오"

데이터 브로커 소프트웨어를 설치할 때는 AWS 키를 지정해야 하므로 AWS 키를 반드시 복사해야 합니다.

#### Google Cloud에 대한 액세스를 활성화합니다

Google Cloud Storage 버킷을 포함하여 동기화 관계에 데이터 브로커를 사용할 계획이라면, Google Cloud 액세스를 위한 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 특정 권한이 있는 서비스 계정에 대한 키를 제공해야 합니다.

##### 단계

1. 스토리지 관리자 권한이 없는 경우 Google Cloud 서비스 계정을 생성합니다.



2. JSON 형식으로 저장된 서비스 계정 키를 생성합니다.

"Google Cloud 지침을 봅니다"

파일에는 최소한 "project\_id", "private\_key" 및 "client\_email" 속성이 포함되어야 합니다.



키를 만들면 파일이 생성되어 컴퓨터에 다운로드됩니다.

3. JSON 파일을 Linux 호스트에 저장합니다.

### Microsoft Azure에 대한 액세스 설정

Azure에 대한 액세스는 관계 동기화 마법사에서 스토리지 계정 및 연결 문자열을 제공하여 관계에 따라 정의됩니다.

### 데이터 브로커 설치

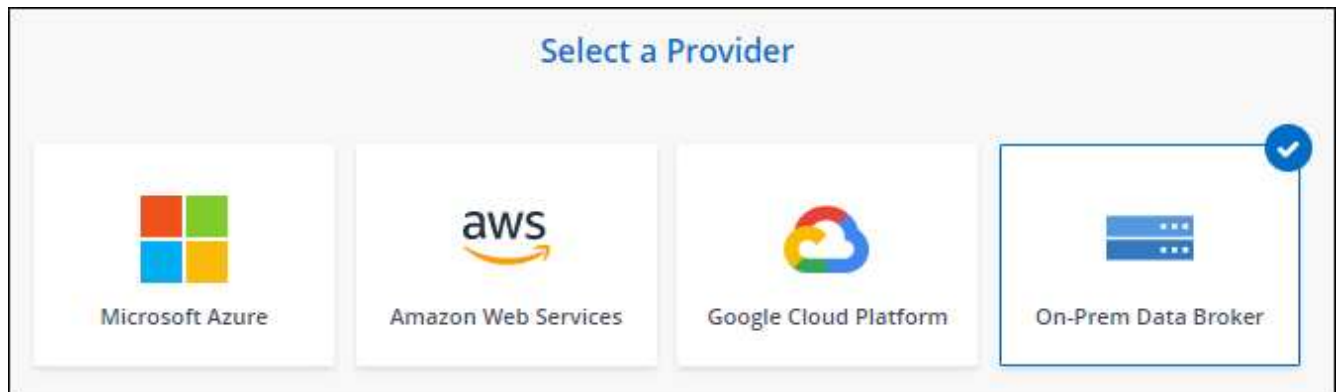
동기화 관계를 생성할 때 Linux 호스트에 데이터 브로커를 설치할 수 있습니다.

### 단계

1. 새 동기화 만들기 \* 를 클릭합니다.
2. 동기화 관계 정의 \* 페이지에서 소스 및 대상을 선택하고 \* 계속 \* 을 클릭합니다.

데이터 브로커 그룹 \* 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 \* 페이지에서 \* 데이터 브로커 생성 \* 을 클릭한 다음 \* 온프레미스 데이터 브로커 \* 를 선택합니다.



옵션에 \* \_On-Premise\_Data Broker \* 라는 레이블이 표시되어 있지만 이 옵션은 온프레미스 또는 클라우드의 Linux 호스트에 적용됩니다.

4. 데이터 브로커의 이름을 입력하고 \* 계속 \* 을 클릭합니다.

지침 페이지가 곧 로드됩니다. 설치 프로그램을 다운로드할 수 있는 고유 링크가 포함된 다음 지침을 따라야 합니다.

5. 지침 페이지에서 다음을 수행합니다.

- a. AWS \*, \* Google Cloud \* 또는 둘 모두에 대한 액세스를 활성화할지 여부를 선택합니다.
- b. 설치 옵션 \* 프록시 없음 \*, \* 프록시 서버 사용 \* 또는 \* 인증 프록시 서버 사용 \* 을 선택합니다.

c. 명령을 사용하여 데이터 브로커를 다운로드하고 설치하십시오.

다음 단계에서는 가능한 각 설치 옵션에 대한 세부 정보를 제공합니다. 지침 페이지에 따라 설치 옵션에 따라 정확한 명령을 가져옵니다.

d. 설치 프로그램 다운로드:

- 프록시 없음:

'<URI>-o data\_broker\_installer.sh'라는 문구입니다

- 프록시 서버 사용:

'<URI>-o data\_broker\_installer.sh -x <proxy\_host>:<proxy\_port>'

- 인증 시 프록시 서버 사용:

'<URI>-o data\_broker\_installer.sh -x  
<proxy\_username>:<proxy\_password>@<proxy\_host>:<proxy\_port>'

**URI**입니다

Cloud Sync 설치 파일의 URI가 지침 페이지에 표시됩니다. 이 내용은 화면의 지시에 따라 온-프레임 데이터 브로커를 배포할 때 로드됩니다. 이 URI는 링크가 동적으로 생성되고 한 번만 사용할 수 있으므로 여기서 반복되지 않습니다. [다음 단계에 따라 Cloud Sync에서 URI를 가져옵니다.](#)

e. 슈퍼유저로 전환하고 설치 프로그램을 실행 가능하게 만든 후 소프트웨어를 설치합니다.



아래 나열된 각 명령에는 AWS 액세스 및 Google Cloud 액세스에 대한 매개 변수가 포함되어 있습니다. 지침 페이지에 따라 설치 옵션에 따라 정확한 명령을 가져옵니다.

- 프록시 구성 없음:

'sudo -s chmod + x data\_broker\_installer.sh./data\_broker\_installer.sh -a <AWS\_access\_key> -s  
<AWS\_secret\_key> -g <absolute\_path\_to\_the\_json\_file>'

- 프록시 구성:

sudo -s chmod + x data\_broker\_installer.sh. /data\_broker\_installer.sh -a <AWS\_access\_key> -s  
<AWS\_secret\_key> -g <absolute\_path\_to\_the\_json\_file> -h <proxy\_host> -p <proxy\_port>

- 인증이 있는 프록시 구성:

sudo -s chmod + x data\_broker\_installer.sh. /data\_broker\_installer.sh -a <AWS\_access\_key> -s  
<AWS\_secret\_key> -g <absolute\_path\_to\_the\_json\_file> -h <proxy\_host> -p <proxy\_username>  
-w <proxy\_password>

**AWS 키**

사용자가 준비해야 하는 키입니다 [다음 단계를 따릅니다](#). AWS 키는 데이터 브로커에 저장되며 사내 또는 클라우드 네트워크에서 실행됩니다. NetApp은 데이터 브로커 외에 다른 키는 사용하지 않습니다.

**JSON 파일**

미리 준비해야 하는 서비스 계정 키가 포함된 JSON 파일입니다 [다음 단계를 따릅니다](#).

6. 데이터 브로커를 사용할 수 있게 되면 Cloud Sync에서 \* 계속 \* 을 클릭합니다.
7. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

# 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.

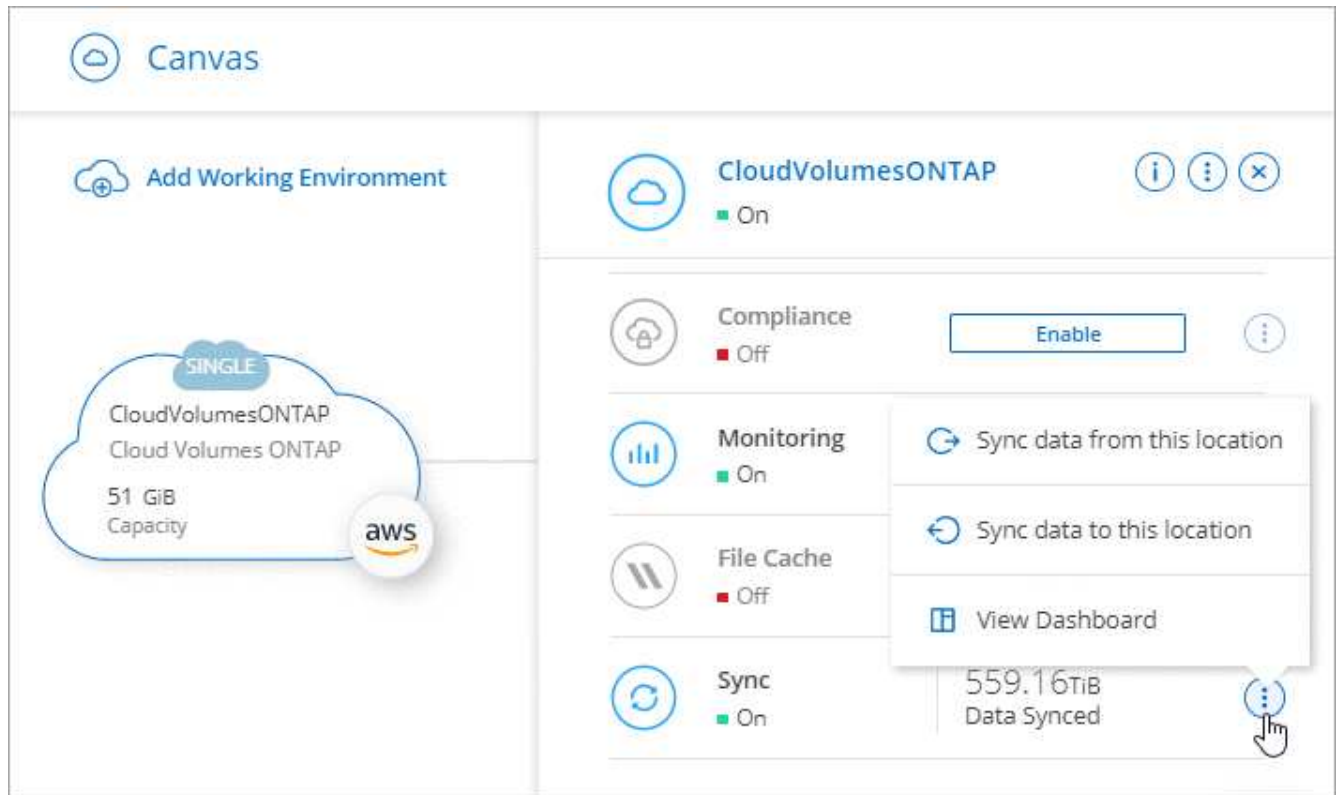
특정 유형의 작업 환경에 대한 동기화 관계를 생성합니다

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.

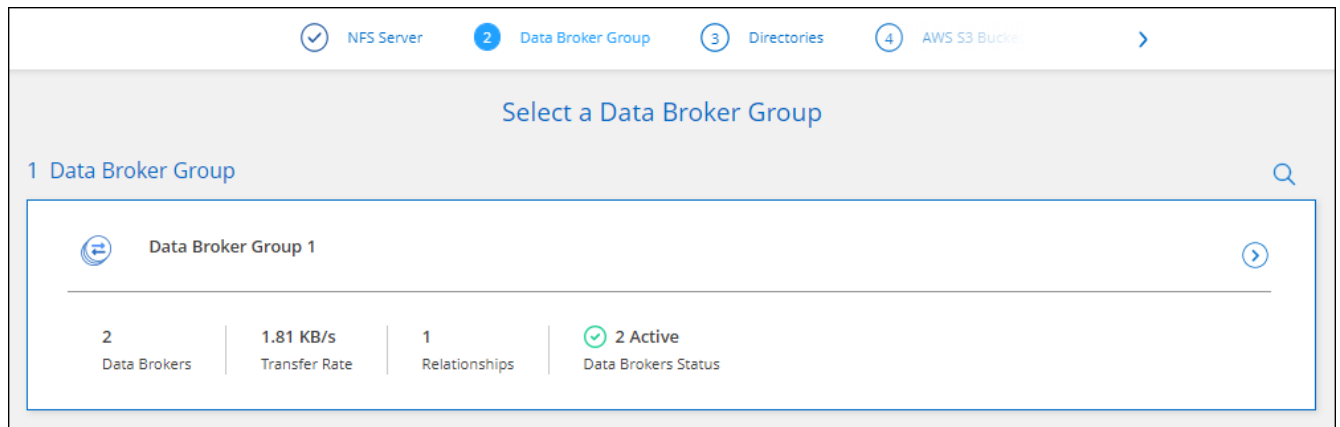


3. NFS 서버 \* 페이지에서 AWS에 동기화할 NFS 서버의 IP 주소 또는 정규화된 도메인 이름을 입력합니다.
4. Data Broker Group \* 페이지에서 프롬프트에 따라 AWS, Azure 또는 Google Cloud Platform에서 데이터 브로커 가상 컴퓨터를 만들거나 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치합니다.

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.



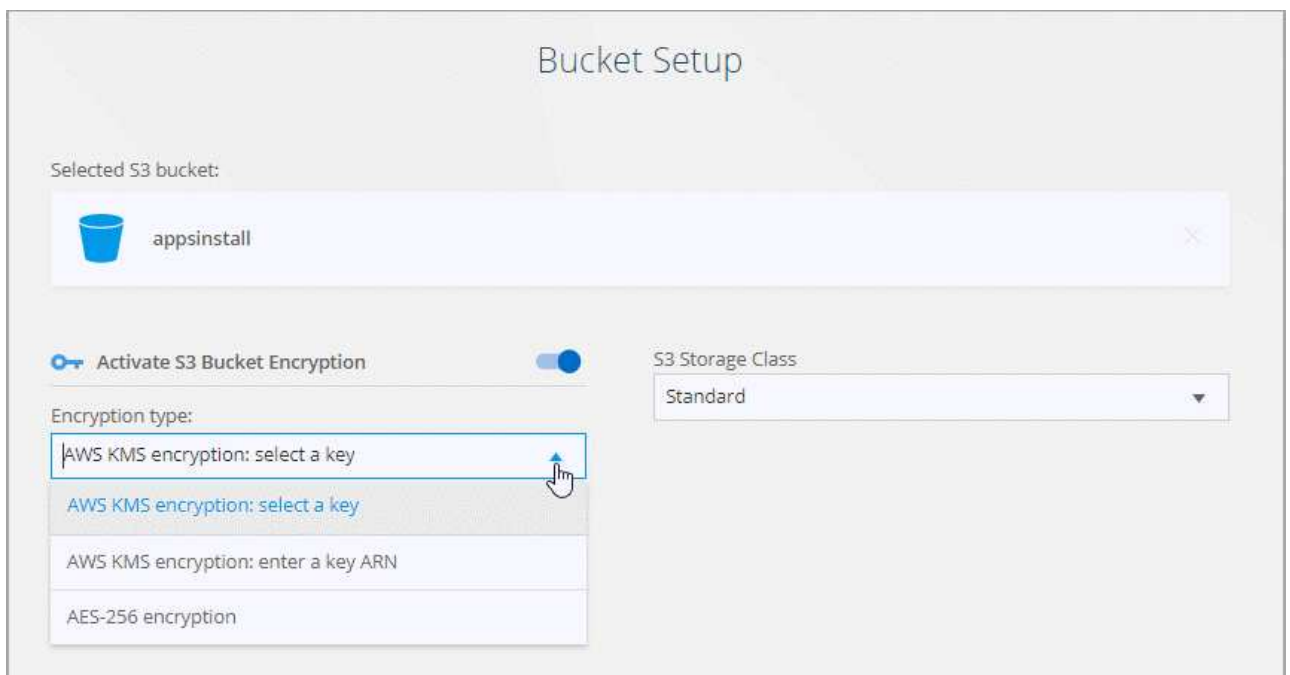
NFS 서버에 둘 이상의 디렉토리를 동기화하려는 경우 작업을 완료한 후 동기화 관계를 추가로 생성해야 합니다.

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.

연속 동기화

초기 데이터 동기화 후 Cloud Sync는 소스 S3 버킷의 변경 사항을 수신 대기하고 변경 사항이 발생할 때마다 타겟에 계속 동기화합니다. 예약된 간격으로 소스를 다시 검색할 필요가 없습니다.

이 설정은 동기화 관계를 생성하고 S3 버킷에서 S3, Google Cloud Storage, Azure Blob Storage, StorageGRID 또는 IBM Storage로 동기화할 때만 사용할 수 있습니다.

이 설정을 사용하면 다음과 같은 다른 기능에 영향을 줍니다.

- 동기화 스케줄이 비활성화되었습니다.
- 동기화 시간 초과, 최근에 수정한 파일 및 수정한 날짜 등의 설정이 기본값으로 되돌아갑니다.
- 크기별 필터링은 삭제 이벤트가 아닌 복사 이벤트에서만 활성화됩니다.
- 관계가 생성된 후에는 관계를 가속화하거나 삭제할 수만 있습니다. 동기화를 중단하거나, 설정을 수정하거나, 보고서를 볼 수 없습니다.

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 Azure Blob 또는 S3 호환 엔드포인트(S3, StorageGRID 또는 IBM 클라우드 오브젝트 스토리지)가 타겟으로 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](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.

The screenshot shows the 'Relationship Tags' configuration page. At the top, there are navigation tabs: '<', 'AWS S3 Bucket', 'Settings', '6 Tags/Metadata', and '7 Review'. The main heading is 'Relationship Tags'. Below it, a message 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 buttons: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below these are two input fields: 'Tag Key' with a placeholder 'Up to 128 characters' and 'Tag Value' with a placeholder 'Up to 256 characters'. At the bottom left is a button '+ Add Relationship Tag'. At the bottom right is the text '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.

"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>

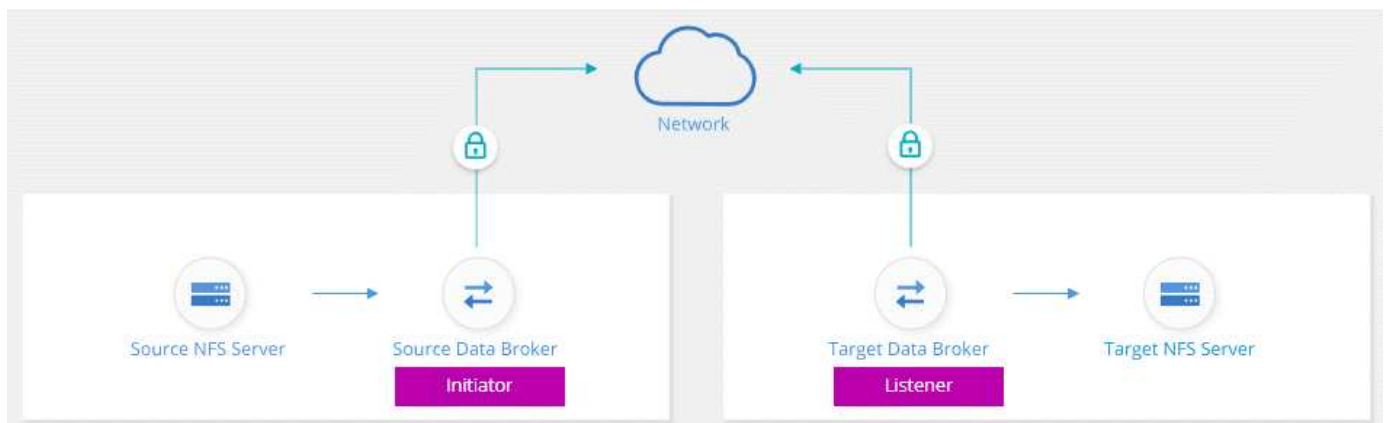
### 전송 중 데이터 암호화를 사용하여 NFS 데이터 동기화

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.

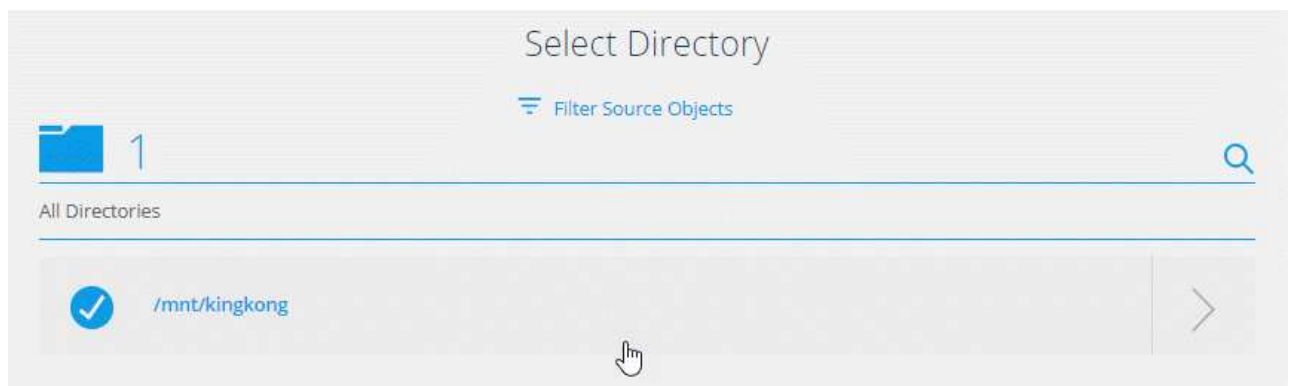
단계

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.

**Select a Provider**

Microsoft Azure

Amazon Web Services

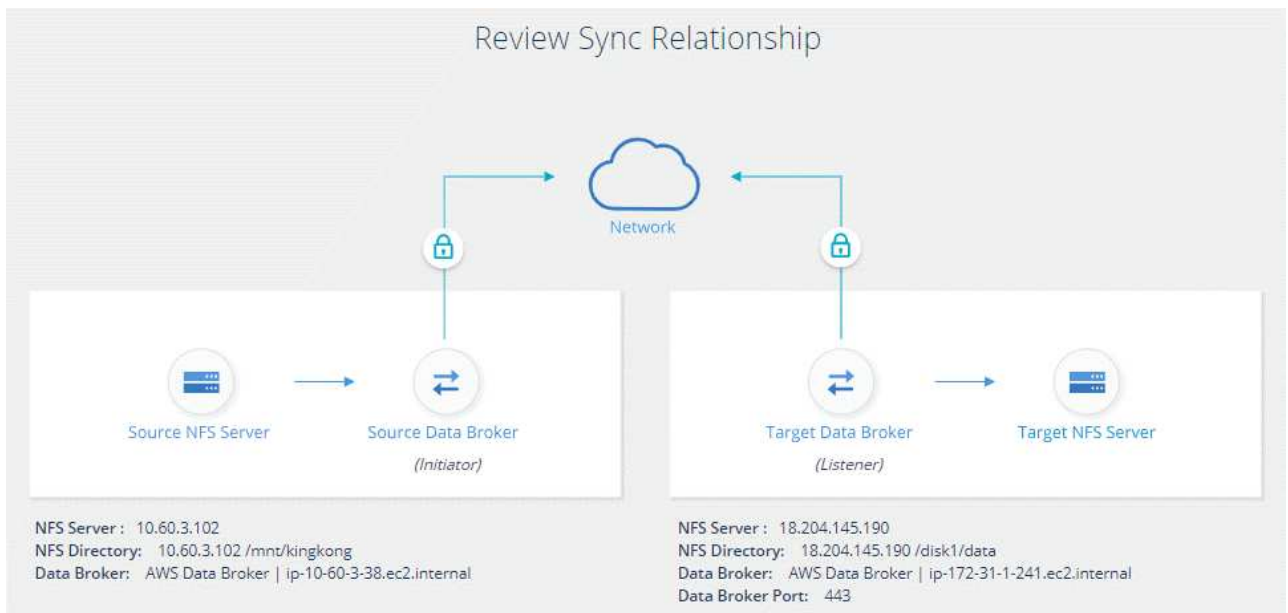
Google Cloud Platform

On-Prem Data Broker

Data Broker Name

Port

- 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/hb312vdasr2/S3Creds> 으로 문의하십시오

예제에서 볼 수 있듯이 접두사 경로는 `_my-path/all-sids/_`이고 요청 ID는 `_hb312vdasr2_`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](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](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 3 을 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](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

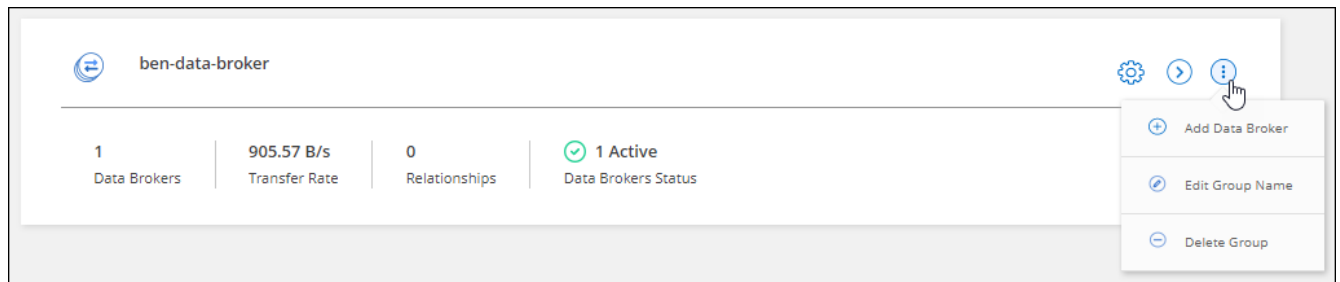
1. 동기화 > 데이터 브로커 관리 \* 를 클릭합니다.
2. 새 데이터 브로커 추가 \* 를 클릭합니다.
3. 프롬프트에 따라 데이터 브로커를 생성합니다.

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.

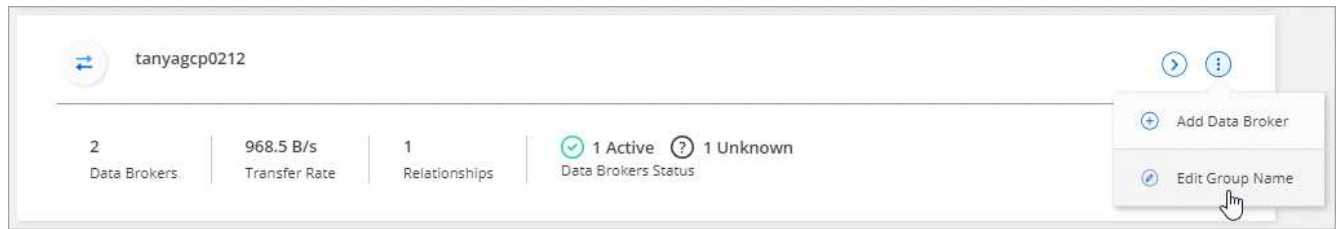
- ["AWS에서 데이터 브로커를 생성합니다"](#)
- ["Azure에서 데이터 브로커를 생성합니다"](#)
- ["Google Cloud에서 데이터 브로커를 생성합니다"](#)
- ["Linux 호스트에 데이터 브로커 설치"](#)

## 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.

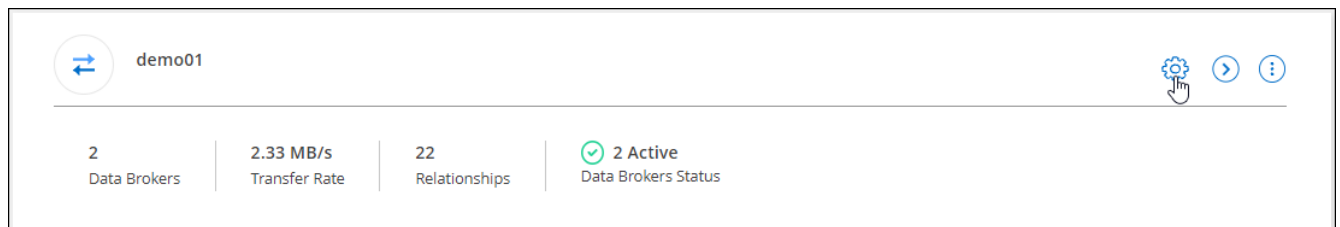
## 통합 구성을 설정합니다

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.

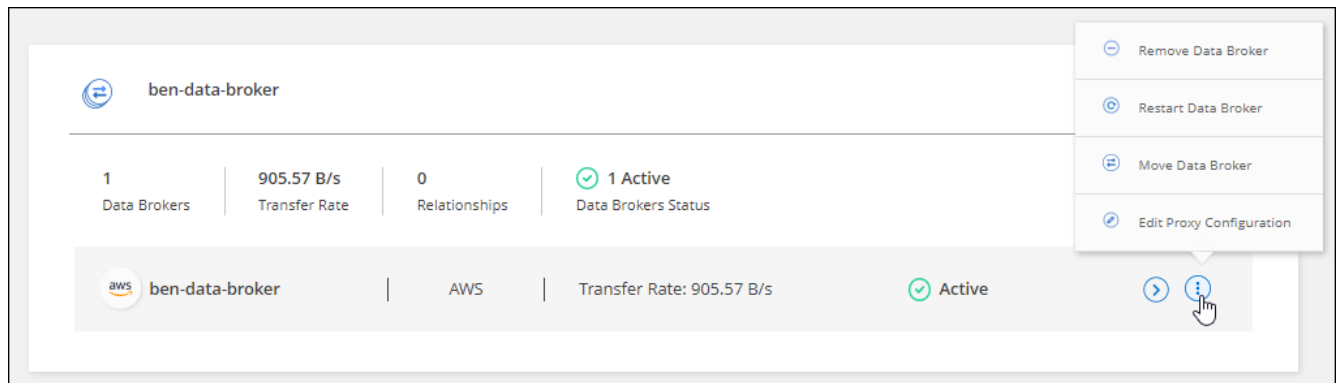
제한 사항



- 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

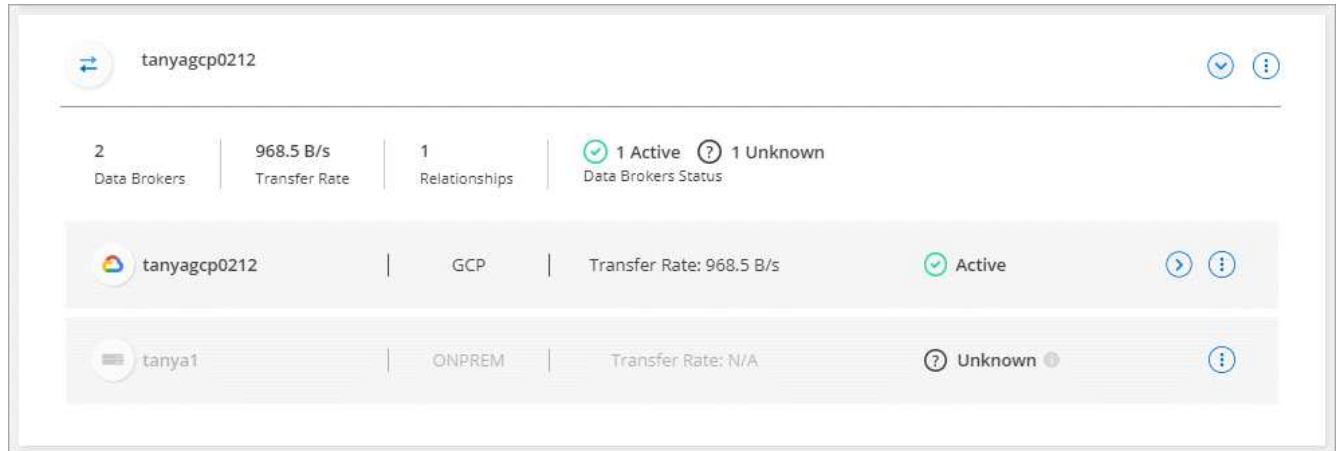
tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active	
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project ID
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux 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

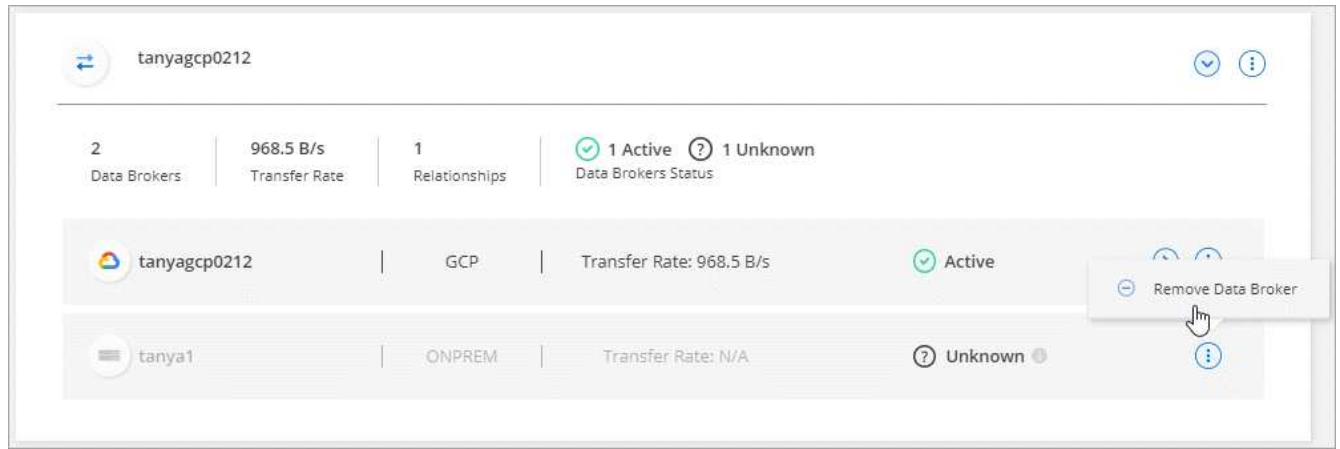
더 이상 필요하지 않거나 초기 구축에 실패한 경우 그룹에서 데이터 브로커를 제거할 수 있습니다. 이 작업을 수행하면 Cloud Sync의 레코드에서 데이터 브로커만 삭제됩니다. 데이터 브로커와 추가 클라우드 리소스를 수동으로 삭제해야 합니다.

### 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.

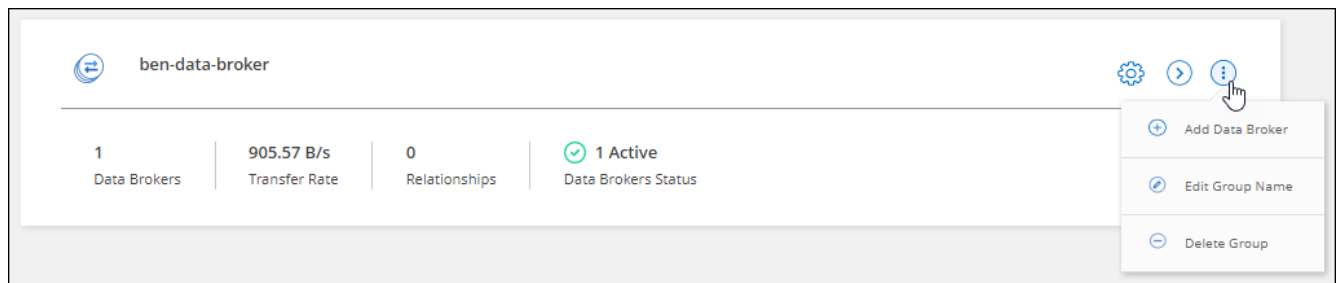
## 데이터 브로커 그룹을 삭제합니다

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.

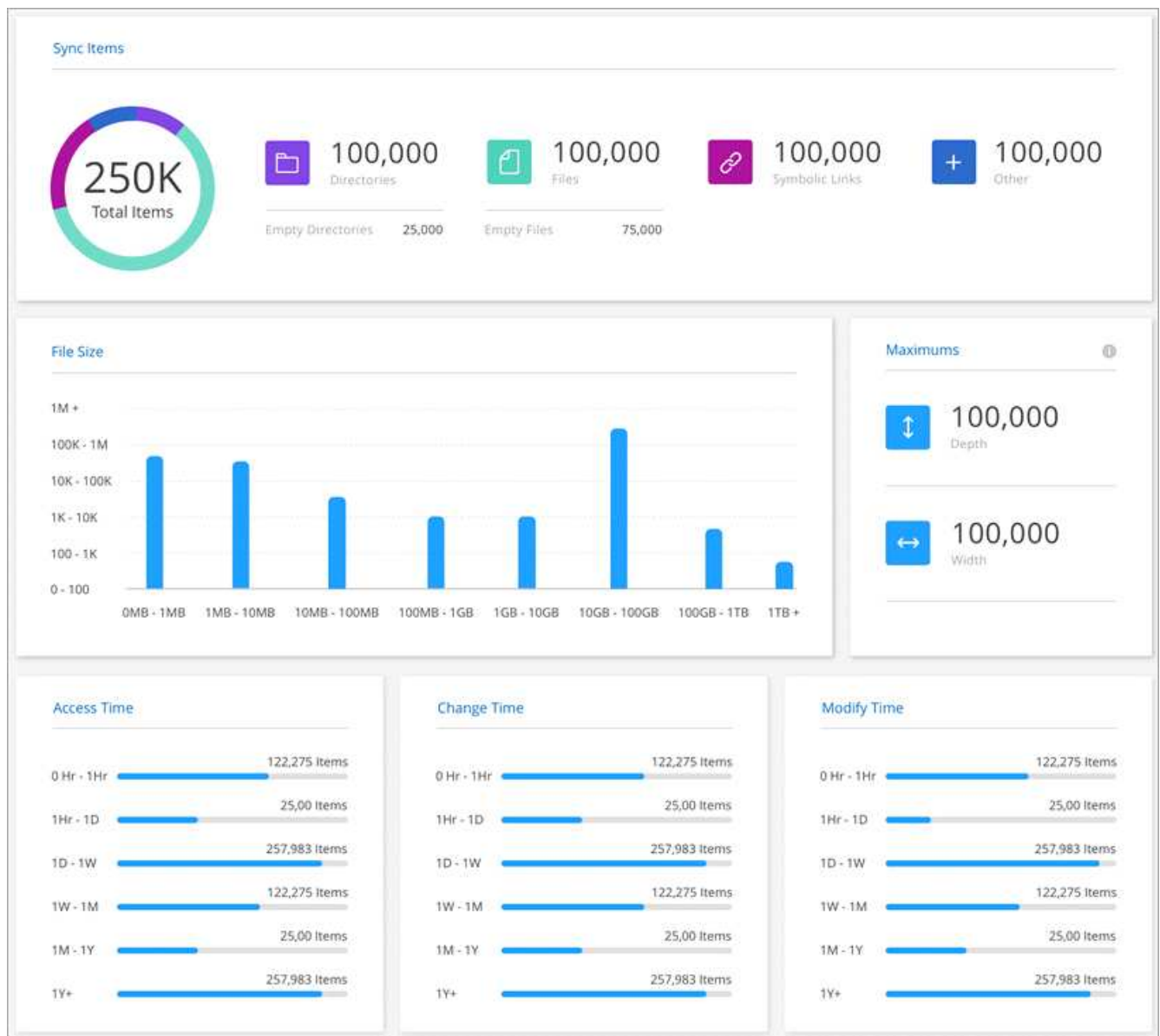
단계

1. 동기화 > 보고서 \* 를 클릭합니다.

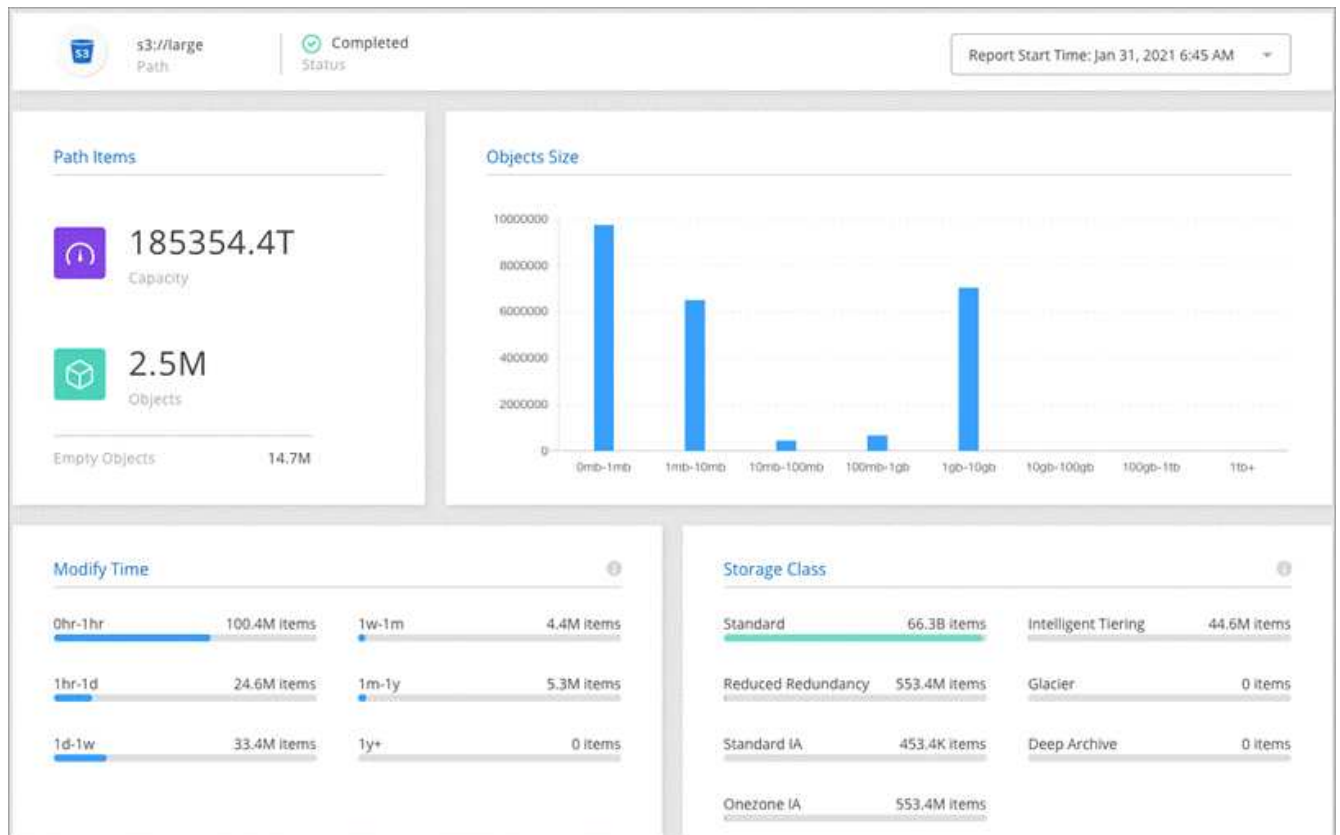
각 동기화 관계의 경로(원본 또는 대상)가 테이블에 표시됩니다.

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.

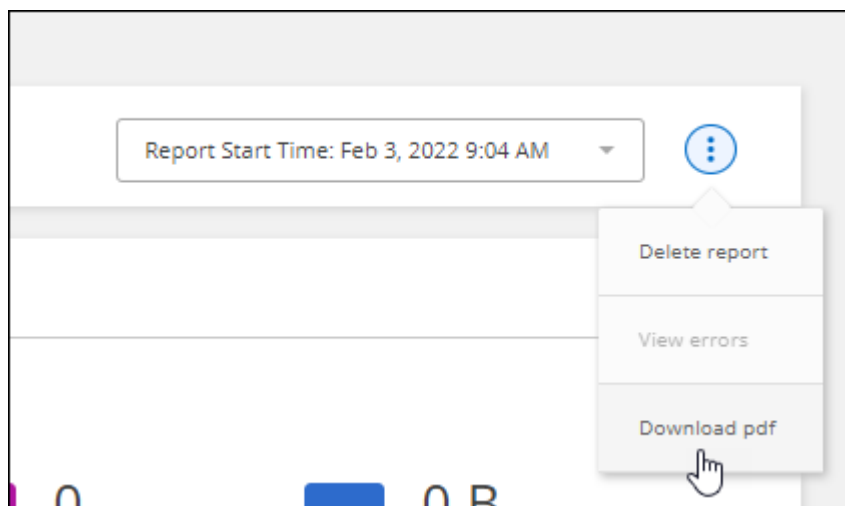


보고서를 다운로드하는 중입니다

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.



# Cloud Sync API

웹 UI를 통해 사용할 수 있는 Cloud Sync 기능은 RESTful API를 통해서도 사용할 수 있습니다.

## 시작하기

Cloud Sync API를 시작하려면 사용자 토큰과 Cloud Central 계정 ID를 얻어야 합니다. API 호출을 할 때 인증 헤더에 토큰과 계정 ID를 추가해야 합니다.

단계

1. NetApp Cloud Central에서 사용자 토큰을 얻습니다.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
  "username": "<user_email>",
  "scope": "profile",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
  "grant_type": "password",
  "password": "<user_password>"
}
```

2. Cloud Central 계정 ID를 받습니다.

```
GET https://api.cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

이 API는 다음과 같은 응답을 반환합니다.

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. 각 API 호출의 Authorization 헤더에 사용자 토큰 및 계정 ID를 추가합니다.

◦ 예 \*

다음 예제는 Microsoft Azure에서 데이터 브로커를 생성하기 위한 API 호출을 보여줍니다. user\_token> 및 <accountId>를 이전 단계에서 얻은 토큰 및 ID 로 바꾸기만 하면 됩니다.

```
POST https://api.cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

### 토큰이 만료되면 어떻게 해야 합니까?

NetApp Cloud Central의 사용자 토큰에 만료일이 있습니다. 토큰을 새로 고치려면 1단계에서 API를 다시 호출해야 합니다.

API 응답에는 토큰이 만료되는 시점을 나타내는 "expires\_in" 필드가 포함됩니다.

## API 참조입니다

각 Cloud Sync API에 대한 설명서는 에서 확인할 수 있습니다 <https://api.cloudsync.netapp.com/docs>.

## 목록 API 사용

목록 API는 비동기 API로, 결과가 즉시 반환되지 않습니다(예: ``get/data-브로커/{id}/list-nfs-export-folders' 및 'get/data-d브로커/{id}/list-s3-vket'). 서버의 유일한 응답은 HTTP 상태 202입니다. 실제 결과를 얻으려면 Get/Messages/client API를 사용해야 한다.

단계

1. 사용할 목록 API를 호출합니다.
2. Get/Messages/client API를 이용하여 작업 결과를 조회한다.
3. 방금 받은 ID에 동일한 API를 추가하여  
'get/http://api.cloudsync.netapp.com/api/messages/client?last=<id\_from\_step\_2>' 사용합니다

ID는 'get/messages/client' API를 호출할 때마다 변경됩니다.

◦ 예 \*

list-s3-Bucket API를 호출하면 결과가 즉시 반환되지 않습니다.

```
GET http://api.cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

결과는 HTTP 상태 코드 202입니다. 이는 메시지가 수락되었지만 아직 처리되지 않았음을 의미합니다.

작업 결과를 얻으려면 다음 API를 사용해야 합니다.

```
GET http://api.cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

결과는 ID 필드가 포함된 객체 하나가 포함된 배열입니다. ID 필드는 서버가 보낸 마지막 메시지를 나타냅니다. 예를 들면 다음과 같습니다.

```
[
  {
    "header": {
      "requestId": "init",
      "clientId": "init",
      "agentId": "init"
    },
    "payload": {
      "init": {}
    },
    "id": "5801"
  }
]
```

이제 방금 수신한 ID를 사용하여 다음 API 호출을 수행합니다.

```
GET
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

그 결과 일련의 메시지가 나타납니다. 각 메시지 안에는 작업 이름(키)과 그 결과(값)로 구성된 페이로드 객체가 있습니다. 예를 들면 다음과 같습니다.

```
[
  {
    "payload": {
      "list-s3-buckets": [
        {
          "tags": [
            {
              "Value": "100$",
              "Key": "price"
            }
          ],
          "region": {
            "displayName": "US West (Oregon)",
            "name": "us-west-2"
          },
          "name": "small"
        }
      ]
    },
    "header": {
      "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
      "clientId": "5beb032f548e6e35f4ed1ba9",
      "agentId": "5bed61f4489fb04e34a9aac6"
    },
    "id": "5802"
  }
]
```

# 개념

## 라이선스 개요

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.

### 마켓플레이스 구독

AWS 또는 Azure에서 Cloud Sync 서비스를 구독하면 시간 단위로 지불하거나 연간 비용을 지불할 수 있습니다. "[AWS 또는 Azure를 통해 가입할 수 있습니다](#)"를 선택합니다.

### 시간별 구독

시간 단위 용량제 구독을 통해 생성하는 동기화 관계 수에 따라 시간 단위로 비용이 청구됩니다.

- "[Azure에서 가격을 확인할 수 있습니다](#)"
- "[AWS에서 용량제 가격 보기](#)"

### 연간 구독

연간 구독은 사전에 지불하는 20개의 동기화 관계에 대한 라이선스를 제공합니다. 동기화 관계가 20개를 초과하고 AWS를 통해 구독한 경우 추가 관계에 대한 비용은 시간당 지불합니다.

["AWS에서 연간 가격 보기"](#)

## NetApp이 라이선스를 구입해야 합니다

동기화 관계를 맺는 데 필요한 또 다른 방법은 NetApp에서 라이선스를 직접 구매하는 것입니다. 각 라이선스를 통해 최대 20개의 동기화 관계를 생성할 수 있습니다.

AWS 또는 Azure 구독에서 이러한 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.

["라이선스를 구매하여 Cloud Sync에 추가하는 방법에 대해 알아보십시오."](#)

### 사용권 조항

BYOL(Bring Your Own License)을 Cloud Sync 서비스로 구매하는 고객은 라이선스 소유 권한과 관련된 제한 사항을 숙지해야 합니다.

- 고객은 BYOL 라이선스를 제공 날짜로부터 1년을 초과하지 않는 기간 동안 활용할 수 있습니다.
- 고객은 BYOL 라이선스를 활용하여 소스와 타겟(각각 "동기화 관계") 간에 총 20개의 개별 연결을 설정할 수 있습니다.
- 고객의 사용 권한은 고객이 20개의 동기화 관계 제한에 도달했는지 여부에 관계없이 1년 라이선스 기간이 종료될 때 만료됩니다.

- 고객이 라이선스를 갱신하기로 선택한 경우 이전 라이선스 부여에서 연결된 사용되지 않은 동기화 관계가 라이선스 갱신으로 롤오버되지 않습니다.

## 데이터 개인 정보 보호

NetApp은 Cloud Sync 서비스를 사용하면서 제공한 자격 증명에 대한 액세스 권한을 가지고 있지 않습니다. 자격 증명은 네트워크에 상주하는 데이터 브로커 컴퓨터에 직접 저장됩니다.

선택한 구성에 따라 새 관계를 만들 때 Cloud Sync에서 자격 증명을 묻는 메시지가 나타날 수 있습니다. 예를 들어, SMB 서버를 포함하는 관계를 설정하거나 AWS에서 데이터 브로커를 구축할 때

이러한 자격 증명은 항상 데이터 브로커 자체에 직접 저장됩니다. 데이터 브로커는 온프레미스 또는 클라우드 계정 등 네트워크 내 시스템에 상주합니다. 자격 증명은 NetApp에서 사용할 수 없습니다.

자격 증명은 HashiCorp Vault를 사용하여 데이터 브로커 컴퓨터에서 로컬로 암호화됩니다.

## Cloud Sync 기술 FAQ

이 FAQ는 질문에 대한 간단한 답변을 찾는 경우에 도움이 될 수 있습니다.

### 시작하기

다음 질문은 Cloud Sync를 시작하는 것과 관련이 있습니다.

#### Cloud Sync의 작동 방식

Cloud Sync는 NetApp 데이터 브로커 소프트웨어를 사용하여 소스 데이터를 타겟(이것을 `_sync 관계 _` 라고 함)으로 동기화합니다.

데이터 브로커 그룹은 소스와 타겟 간의 동기화 관계를 제어합니다. 동기화 관계를 설정한 후 Cloud Sync는 소스 시스템을 분석하고 이를 여러 복제 스트림으로 분해하여 선택한 타겟 데이터를 푸시합니다.

초기 복사 후 서비스는 사용자가 설정한 일정에 따라 변경된 데이터를 동기화합니다.

#### 14일 무료 평가판은 어떻게 작동합니까?

14일 무료 평가판은 Cloud Sync 서비스에 등록할 때 시작됩니다. 14일 동안 생성한 Cloud Sync 관계에는 NetApp 비용이 적용되지 않습니다. 하지만 구축하는 데이터 브로커에 대한 모든 리소스 비용이 계속 적용됩니다.

#### Cloud Sync 비용은 얼마입니까?

Cloud Sync 사용과 관련된 비용에는 서비스 요금과 리소스 요금이라는 두 가지 유형이 있습니다.

- 서비스 요금 \*

용량제 가격으로, 생성한 동기화 관계 수를 기준으로 Cloud Sync 서비스 요금은 시간당 부과됩니다.

- ["AWS에서 용량제 가격 보기"](#)
- ["AWS에서 연간 가격 보기"](#)

- ["Azure에서 가격을 확인할 수 있습니다"](#)

Cloud Sync 라이선스는 NetApp 담당자를 통해서도 제공됩니다. 각 라이선스로 12개월간 20개의 동기화 관계를 사용할 수 있습니다.

["라이선스에 대해 자세히 알아보십시오"](#).



Cloud Sync 관계는 Cloud Volumes Service 및 Azure NetApp Files에서 무료로 제공됩니다.

- 리소스 비용 \*

리소스 요금은 클라우드에서 데이터 브로커를 실행하는 데 필요한 컴퓨팅 및 스토리지 비용과 관련이 있습니다.

### Cloud Sync는 어떻게 청구되니까?

14일 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불할 수 있는 두 가지 방법이 있습니다. 첫 번째 옵션은 AWS 또는 Azure에서 가입하는 것입니다. 가입 시 사용한 만큼만 지불하거나 연간 비용을 지불할 수 있습니다. 두 번째 옵션은 NetApp에서 직접 라이선스를 구매하는 것입니다.

### 클라우드 외부에서 Cloud Sync를 사용할 수 있습니까?

예, 비클라우드 아키텍처에서 Cloud Sync를 사용할 수 있습니다. 소스와 타겟이 사내에 있을 수 있으므로 데이터 브로커 소프트웨어도 사용할 수 있습니다.

클라우드 외부에서 Cloud Sync를 사용하는 방법은 다음과 같습니다.

- 사내 동기화의 경우 NetApp StorageGRID를 통해 프라이빗 Amazon S3 버킷을 사용할 수 있습니다.
- 데이터 브로커 그룹은 Cloud Sync 서비스와 통신하기 위해 인터넷 연결이 필요합니다.
- NetApp에서 직접 라이선스를 구입하지 않을 경우 PAYGO Cloud Sync 서비스 청구를 위해 AWS 또는 Azure 계정이 필요합니다.

### Cloud Sync에 어떻게 액세스하니까?

Cloud Sync는 Cloud Manager의 \* 동기화 \* 탭에서 사용할 수 있습니다.

### 데이터 브로커 그룹이란 무엇입니까?

각 데이터 브로커는 데이터 브로커 그룹에 속해 있습니다. 데이터 브로커를 함께 그룹화하면 동기화 관계의 성능을 향상시킬 수 있습니다.

### 지원되는 소스 및 타겟

동기화 관계에서 지원되는 소스 및 타겟과 관련된 다음 질문

### Cloud Sync가 지원하는 소스와 대상은 무엇입니까?

Cloud Sync는 다양한 유형의 동기화 관계를 지원합니다. ["전체 목록을 보십시오"](#).

**Cloud Sync**는 어떤 버전의 **NFS** 및 **SMB**를 지원합니까?

Cloud Sync는 NFS 버전 3 이상과 SMB 버전 1 이상을 지원합니다.

["동기화 요구 사항에 대해 자세히 알아보십시오"](#).

**Amazon S3**가 타겟일 때 데이터는 특정 **S3** 스토리지 클래스로 계층화할 수 있습니까?

예. AWS S3가 타겟인 경우 특정 S3 스토리지 클래스를 선택할 수 있습니다.

- 표준(기본 클래스)
- 지능형 계층화
- 표준 - 낮은 액세스 빈도
- 단일 영역 - 낮은 액세스 빈도
- 빙하
- Glacier 딥 아카이브

**Azure Blob** 스토리지의 스토리지 계층에는 어떻게 됩니까?

Blob 컨테이너가 타겟인 경우 특정 Azure Blob 저장소 계층을 선택할 수 있습니다.

- 핫 스토리지
- 멋진 보관

**Google Cloud** 스토리지 계층을 지원합니까?

예, Google Cloud Storage 버킷이 타겟인 경우 특정 스토리지 클래스를 선택할 수 있습니다.

- 표준
- 니어라인
- 콜드라인
- 아카이브

## 네트워킹

다음 질문은 Cloud Sync의 네트워킹 요구 사항과 관련이 있습니다.

**Cloud Sync**의 네트워킹 요구 사항은 무엇입니까?

Cloud Sync 환경에서는 데이터 브로커 그룹이 선택한 프로토콜 또는 오브젝트 스토리지 API(Amazon S3, Azure Blob, IBM 클라우드 오브젝트 스토리지)를 통해 소스 및 타겟에 연결되어 있어야 합니다.

또한 데이터 브로커 그룹은 포트 443을 통해 아웃바운드 인터넷 연결을 필요로 하므로 Cloud Sync 서비스와 통신하고 몇 가지 다른 서비스 및 리포지토리에 연결할 수 있습니다.

자세한 내용을 보려면 ["네트워킹 요구 사항을 검토합니다"](#).



데이터 브로커와 함께 프록시 서버를 사용할 수 있습니까?

예.

Cloud Sync는 기본 인증을 사용하거나 사용하지 않는 프록시 서버를 지원합니다. 데이터 브로커를 배포할 때 프록시 서버를 지정하면 데이터 브로커의 모든 HTTP 및 HTTPS 트래픽이 프록시를 통해 라우팅됩니다. NFS 또는 SMB와 같은 비 HTTP 트래픽은 프록시 서버를 통해 라우팅할 수 없습니다.

프록시 서버의 유일한 제한 사항은 NFS 또는 Azure NetApp Files 동기화 관계를 사용하여 전송 중 데이터 암호화를 사용하는 것입니다. 암호화된 데이터는 HTTPS를 통해 전송되며 프록시 서버를 통해 라우팅할 수 없습니다.

## 데이터 동기화

다음 질문은 데이터 동기화 작동 방식과 관련이 있습니다.

동기화가 얼마나 자주 발생합니까?

기본 스케줄은 일별 동기화에 대해 설정됩니다. 초기 동기화 후 다음을 수행할 수 있습니다.

- 원하는 일 수, 시간 또는 분으로 동기화 일정을 수정합니다
- 동기화 일정을 비활성화합니다
- 동기화 일정 삭제(데이터가 손실되지 않음. 동기화 관계만 제거됨)

최소 동기화 일정은 무엇입니까?

1분마다 데이터를 동기화하도록 관계를 예약할 수 있습니다.

데이터 브로커 그룹이 파일 동기화 실패 시 재시도합니까? 아니면 시간 초과입니까?

데이터 브로커 그룹은 단일 파일이 전송되지 않을 때 시간 초과되지 않습니다. 대신 데이터 브로커 그룹은 파일을 건너뛰기 전에 3번 재시도합니다. 재시도 값은 동기화 관계에 대한 설정에서 구성할 수 있습니다.

["동기화 관계의 설정을 변경하는 방법에 대해 알아봅니다".](#)

매우 큰 데이터 세트가 있는 경우 어떻게 해야 합니까?

단일 디렉토리에 600,000개 이상의 파일이 있는 경우 페이로드를 처리하도록 데이터 브로커 그룹을 구성할 수 있도록 <mailto:ng-cloudsync-support@netapp.com> [contact us] 를 사용합니다. 데이터 브로커 그룹에 메모리를 추가해야 할 수도 있습니다.

마운트 지점의 총 파일 수에는 제한이 없습니다. 계층 구조(최상위 디렉토리 또는 하위 디렉토리)의 레벨에 관계없이 60만 개 이상의 파일이 있는 대규모 디렉토리에 대해서는 추가 메모리가 필요합니다.

## 보안

보안과 관련된 다음 질문입니다.

**Cloud Sync는 안전합니까?**

예. 모든 Cloud Sync 서비스 네트워킹 연결은 을 사용하여 수행됩니다 ["아마존 단순 대기열 서비스\(SQS\)"](#).

데이터 브로커 그룹과 Amazon S3, Azure Blob, Google Cloud Storage 및 IBM Cloud Object Storage 간의 모든 통신은 HTTPS 프로토콜을 통해 수행됩니다.

사내(소스 또는 타겟) 시스템에서 Cloud Sync를 사용하는 경우 다음과 같은 몇 가지 권장 연결 옵션을 활용할 수 있습니다.

- 인터넷에 연결되지 않은 AWS Direct Connect, Azure ExpressRoute 또는 Google Cloud Interconnect 연결 (지정한 클라우드 네트워크와만 통신할 수 있음)
- 온-프레미스 게이트웨이 장치와 클라우드 네트워크 간의 VPN 연결
- S3 버킷, Azure Blob 스토리지 또는 Google Cloud Storage를 통한 추가 보안 데이터 전송을 위해 Amazon Private S3 Endpoint, Azure Virtual Network 서비스 끝점 또는 Private Google Access를 설정할 수 있습니다.

이러한 방법 중 하나라도 있으면 사내 NAS 서버와 Cloud Sync 데이터 브로커 그룹 간에 보안 연결이 설정됩니다.

### Cloud Sync에서 데이터를 암호화합니까?

- Cloud Sync는 소스 및 타겟 NFS 서버 간에 전송 중 데이터 암호화를 지원합니다. ["자세한 정보"](#).
- SMB의 경우 Cloud Sync는 서버 측에서 암호화한 SMB 3.0 및 3.11 데이터를 지원합니다. Cloud Sync는 암호화된 데이터를 소스에서 데이터가 암호화된 상태로 유지되는 타겟으로 복사합니다.

Cloud Sync는 SMB 데이터 자체를 암호화할 수 없습니다.

- Amazon S3 버킷이 동기화 관계의 타겟인 경우 AWS KMS 암호화 또는 AES-256 암호화를 사용하여 데이터 암호화를 사용할지 여부를 선택할 수 있습니다.

## 권한

다음 질문은 데이터 권한과 관련이 있습니다.

### SMB 데이터 권한이 타겟 위치에 동기화됩니까?

소스 SMB 공유와 타겟 SMB 공유 간, 소스 SMB 공유에서 오브젝트 스토리지(ONTAP S3 제외) 간에 액세스 제어 목록(ACL)을 보존하도록 Cloud Sync를 설정할 수 있습니다.



Cloud Sync는 오브젝트 스토리지에서 SMB 공유로의 ACL 복제를 지원하지 않습니다.

["SMB 공유 간에 ACL을 복사하는 방법에 대해 알아봅니다"](#).

### NFS 데이터 권한이 타겟 위치에 동기화됩니까?

Cloud Sync는 다음과 같이 NFS 서버 간에 NFS 권한을 자동으로 복제합니다.

- NFS 버전 3: Cloud Sync는 사용 권한과 사용자 그룹 소유자를 복사합니다.
- NFS 버전 4: Cloud Sync는 ACL을 복제합니다.

## 오브젝트 스토리지 메타데이터

Cloud Sync는 다음과 같은 유형의 동기화 관계를 위해 소스에서 타겟으로 오브젝트 스토리지 메타데이터를 복제합니다.

- Amazon S3 → Amazon S3 <sup>1</sup>
- Amazon S3 → StorageGRID 를 선택합니다
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID
- StorageGRID → Google 클라우드 스토리지
- Google 클라우드 스토리지 → StorageGRID<sup>1</sup>
- Google Cloud Storage → IBM Cloud Object Storage <sup>1</sup>
- Google Cloud Storage → Amazon S3 <sup>1</sup>
- Amazon S3 → Google Cloud Storage 를 클릭합니다
- IBM Cloud Object Storage → Google Cloud Storage
- StorageGRID → IBM 클라우드 오브젝트 스토리지
- IBM 클라우드 오브젝트 스토리지 → StorageGRID
- IBM 클라우드 오브젝트 스토리지 → IBM 클라우드 오브젝트 스토리지

<sup>1</sup> 이러한 동기화 관계의 경우 해야 합니다 ["동기화 관계를 만들 때 개체에 대한 복사 설정을 활성화합니다"](#).

## 성능

다음 질문은 Cloud Sync 성능과 관련이 있습니다.

동기화 관계의 진행률 표시기는 무엇을 나타냅니까?

동기화 관계는 데이터 브로커 그룹의 네트워크 어댑터의 처리량을 보여 줍니다. 여러 데이터 브로커를 사용하여 동기화 성능을 가속화하면 처리량은 모든 트래픽의 합계입니다. 이 처리량은 20초마다 새로 고쳐집니다.

성능 문제가 발생했습니다. 동시 전송 수를 제한할 수 있습니까?

용량이 매우 큰 파일(각 BB가 여러 개 있는 경우)이 있으면 전송 프로세스를 완료하는 데 시간이 오래 걸릴 수 있으며 성능에 영향을 줄 수 있습니다.

동시 전송 수를 제한하는 것은 도움이 될 수 있습니다. <mailto:ng-cloudsync-support@netapp.com> [문의처].

**Azure NetApp Files**에서 성능이 낮은 이유는 무엇입니까?

Azure NetApp Files 간에 데이터를 동기화할 때 디스크 서비스 수준이 Standard인 경우 장애 및 성능 문제가 발생할 수 있습니다.

동기화 성능을 향상시키려면 서비스 수준을 Premium 또는 Ultra로 변경합니다.

["Azure NetApp Files 서비스 수준 및 처리량에 대해 자세히 알아보십시오"](#).

**AWS용 Cloud Volumes Service**의 성능이 낮은 이유는 무엇입니까?

클라우드 볼륨과 데이터를 동기화할 때 클라우드 볼륨의 성능 수준이 Standard인 경우 장애 및 성능 문제가 발생할 수 있습니다.

동기화 성능을 향상시키려면 서비스 수준을 Premium 또는 Extreme으로 변경하십시오.

그룹에 필요한 데이터 브로커는 몇 개입니까?

새 관계를 만들 때는 가속화된 동기화 관계에 속하는 기존 데이터 브로커를 선택하지 않는 한 그룹의 단일 데이터 브로커로 시작합니다. 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 요소가 데이터 전송 성능에 영향을 줄 수 있습니다. 네트워크 대역폭, 지연 시간, 네트워크 토폴로지, 데이터 브로커 VM 사양 및 스토리지 시스템 성능 때문에 전반적인 동기화 성능이 영향을 받을 수 있습니다. 예를 들어, 그룹의 단일 데이터 브로커는 100MB/s에 도달할 수 있지만 타겟의 디스크 처리량은 64MB/s만 허용할 수 있습니다 따라서 데이터 브로커 그룹은 데이터를 복사하려고 계속 노력하고 있지만 타겟 고객은 데이터 브로커 그룹의 성능을 충족할 수 없습니다.

따라서 대상의 네트워킹 성능과 디스크 처리량을 확인해야 합니다.

그런 다음 그룹에 추가 데이터 브로커를 추가하여 해당 관계의 로드를 공유함으로써 동기화 성능을 높일 수 있습니다. ["동기화 성능을 가속화하는 방법에 대해 알아보십시오"](#).

## 항목을 삭제하는 중입니다

다음 질문은 원본 및 대상에서 동기화 관계 및 데이터를 삭제하는 것과 관련이 있습니다.

**Cloud Sync** 관계를 삭제하면 어떻게 됩니까?

관계를 삭제하면 이후의 모든 데이터 동기화가 중지되고 결제가 종료됩니다. 대상에 동기화된 데이터는 그대로 유지됩니다.

소스 서버에서 항목을 삭제하면 어떻게 됩니까? 대상에서도 제거됩니까?

기본적으로 활성 동기화 관계가 있는 경우 소스 서버에서 삭제된 항목은 다음 동기화 중에 대상에서 삭제되지 않습니다. 그러나 각 관계의 동기화 설정에는 Cloud Sync가 소스에서 삭제된 경우 대상 위치의 파일을 삭제하도록 정의할 수 있는 옵션이 있습니다.

["동기화 관계의 설정을 변경하는 방법에 대해 알아보십시오"](#).

대상에서 항목을 삭제하면 어떻게 됩니까? 소스에서도 제거됩니까?

대상에서 삭제된 항목은 원본에서 제거되지 않습니다. 관계는 소스에서 타겟으로 한 방향입니다. 다음 동기화 주기에서 Cloud Sync는 소스를 타겟과 비교하여 항목이 누락되었음을 확인하고 Cloud Sync 소스에서 타겟으로 다시 복사합니다.

## 문제 해결

["NetApp 기술 자료: Cloud Sync FAQ: 지원 및 문제 해결"](#)

## 데이터 브로커 딥 다이브

다음 질문은 데이터 브로커와 관련이 있습니다.

데이터 브로커의 아키텍처를 설명해 줄 수 있습니까?

물론입니다. 다음은 가장 중요한 사항입니다.

- 데이터 브로커는 Linux 호스트에서 실행되는 node.js 애플리케이션입니다.
- Cloud Sync는 다음과 같이 데이터 브로커를 배포합니다.
  - AWS: AWS CloudFormation 템플릿에서
  - Azure: Azure Resource Manager에서
  - Google: Google Cloud Deployment Manager에서
  - 고유한 Linux 호스트를 사용하는 경우 소프트웨어를 수동으로 설치해야 합니다
- 데이터 브로커 소프트웨어는 자동으로 최신 버전으로 업그레이드합니다.
- 데이터 브로커는 AWS SQS를 안정적이고 안전한 통신 채널과 제어 및 모니터링용으로 사용합니다. 또한 SQS는 지속성 계층을 제공합니다.
- 그룹에 추가 데이터 브로커를 추가하여 전송 속도를 높이고고가용성을 추가할 수 있습니다. 하나의 데이터 브로커가 실패하는 경우 서비스 복원력을 제공합니다.

# 지식 및 지원

## 지원을 위해 등록하십시오

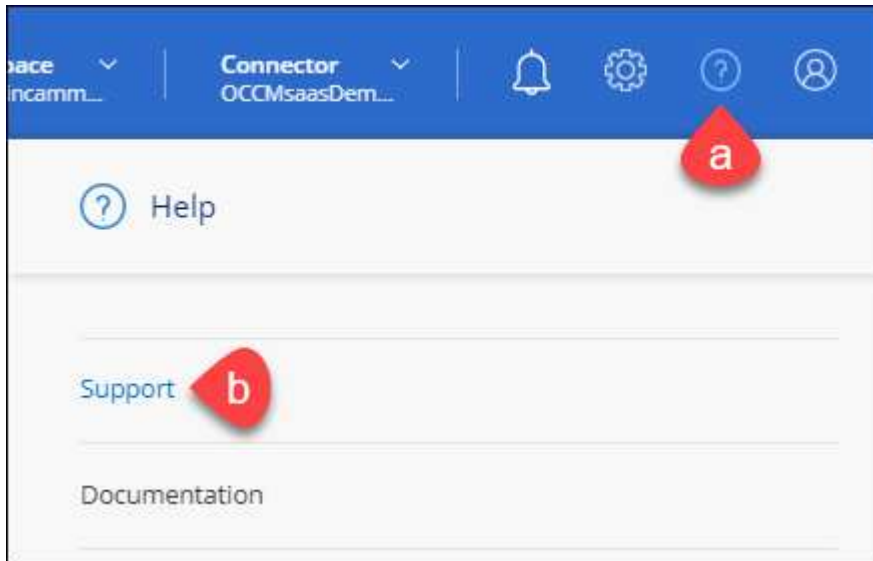
NetApp 기술 지원으로 지원 케이스를 생성하기 전에 NetApp Support 사이트 계정을 Cloud Manager에 추가한 다음 지원을 위해 등록해야 합니다.

### NSS 계정을 추가합니다

지원 대시보드를 이용하면 모든 NetApp Support 사이트 계정을 단일 위치에서 추가 및 관리할 수 있습니다.

단계

1. 아직 NetApp Support 사이트 계정이 없는 경우 **"1인 등록"**.
2. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.



3. NSS 관리 > NSS 계정 추가 \* 를 클릭합니다.
4. 메시지가 표시되면 \* 계속 \* 을 클릭하여 Microsoft 로그인 페이지로 리디렉션됩니다.

NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다.

5. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

이 작업을 수행하면 Cloud Manager에서 NSS 계정을 사용할 수 있습니다.

참고 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님).

### 계정을 등록하여 지원을 받을 수 있습니다

지원 등록은 지원 대시보드의 Cloud Manager에서 가능합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 \* 지원 \* 을 선택합니다.



2. Resources \* 탭에서 \* Register for Support \* 를 클릭합니다.
3. 등록할 NSS 자격 증명을 선택한 다음 \* 등록 \* 을 클릭합니다.

## 도움을 받으십시오

NetApp은 다양한 방법으로 Cloud Manager 및 클라우드 서비스를 지원합니다. 기술 자료(KB) 기사 및 커뮤니티 포럼과 같은 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. 지원 등록에는 웹 티켓팅을 통한 원격 기술 지원이 포함됩니다.

### 자체 지원

이 옵션은 하루 24시간, 주 7일 동안 무료로 사용할 수 있습니다.

- "기술 자료"

Cloud Manager 기술 자료를 검색하여 문제를 해결할 수 있는 유용한 문서를 찾습니다.

- "커뮤니티"

Cloud Manager 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새 토론을 만들어보십시오.

- 문서화

현재 보고 있는 Cloud Manager 문서입니다.

- <mailto:ng-cloudmanager-feedback@netapp.com> [피드백 이메일]

저희는 귀하의 의견을 소중하게 생각합니다. 클라우드 관리자 개선에 도움이 되는 피드백을 제출해 주십시오.

## NetApp 지원

위의 자체 지원 옵션 외에도 NetApp 지원 엔지니어와 협력하여 지원을 활성화한 이후의 모든 문제를 해결할 수 있습니다.

단계

1. Cloud Manager에서 \* 도움말 > 지원 \* 을 클릭합니다.
2. 기술 지원 아래에서 사용 가능한 옵션 중 하나를 선택합니다.
  - a. NetApp 기술 지원을 위한 전화 번호를 찾으려면 \* 문의하다
  - b. 문제 열기 \* 를 클릭하고 옵션 중 하나를 선택한 다음 \* 보내기 \* 를 클릭합니다.

NetApp 담당자가 귀하의 케이스를 검토하고 곧 다시 귀하에 연락을 드릴 것입니다.



# 법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

## 저작권

<http://www.netapp.com/us/legal/copyright.aspx>

## 상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/us/media/patents-page.pdf>

## 개인 정보 보호 정책

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## 오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이선스에 대한 정보를 제공합니다.

"Cloud Sync에 대한 고지 사항"

## 저작권 정보

Copyright © 2022 NetApp, Inc. All rights reserved. 미국에서 인쇄된 본 문서의 어떤 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 그래픽, 전자적 또는 기계적 수단(사진 복사, 레코딩 등)으로도 저작권 소유자의 사전 서면 승인 없이 전자 검색 시스템에 저장 또는 저장.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지 사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 "있는 그대로" 제공되며 상품성 및 특정 목적에 대한 적합성에 대한 명시적 또는 묵시적 보증을 포함하여 이에 제한되지 않고, 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 또는 파생적 손해(소계 물품 또는 서비스의 조달, 사용 손실, 데이터 또는 수익 손실, 계약, 엄격한 책임 또는 불법 행위(과실 또는 그렇지 않은 경우)에 관계없이 어떠한 책임도 지지 않으며, 이는 이러한 손해의 가능성을 사전에 알고 있던 경우에도 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 구입의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

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

권리 제한 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.277-7103(1988년 10월) 및 FAR 52-227-19(1987년 6월)의 기술 데이터 및 컴퓨터 소프트웨어의 권리(Rights in Technical Data and Computer Software) 조항의 하위 조항 (c)(1)(ii)에 설명된 제한사항이 적용됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 에 나열된 마크는 NetApp에 있습니다 <http://www.netapp.com/TM> 는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.