소스와 타겟 간에 데이터를 동기화합니다

BlueXP copy and sync

NetApp
April 08, 2024

목차

소스와 타겟 간에 데이터를 동기화합니다

동기화 관계를 생성합니다

동기화 관계를 생성하면 BlueXP 복사 및 동기화 서비스가 소스에서 타겟으로 파일을 복사합니다. 초기 복사 후, 서비스는 24시간마다 변경된 데이터를 동기화합니다.

동기화 관계의 일부 유형을 생성하려면 먼저 BlueXP에서 작업 환경을 만들어야 합니다.

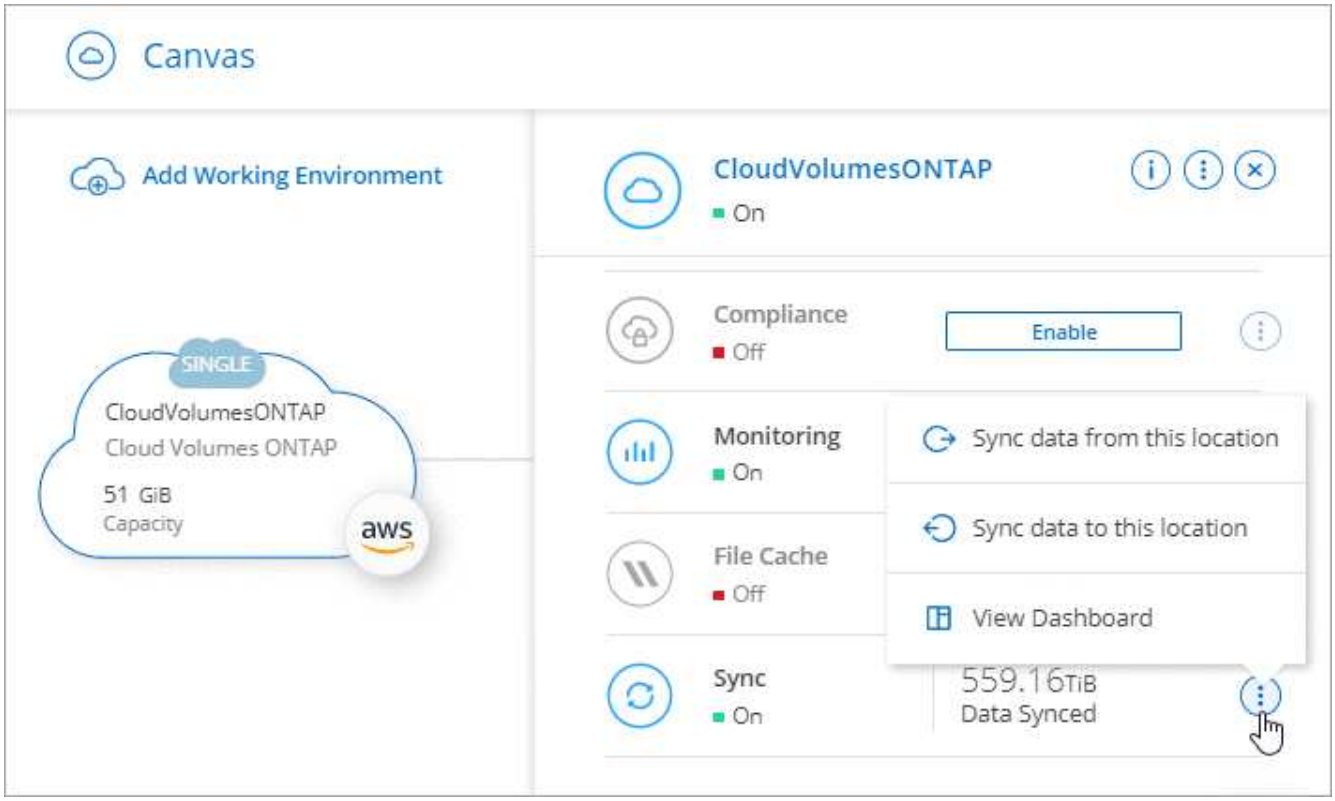
특정 유형의 작업 환경에 대한 동기화 관계를 생성합니다

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 선택합니다.
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.

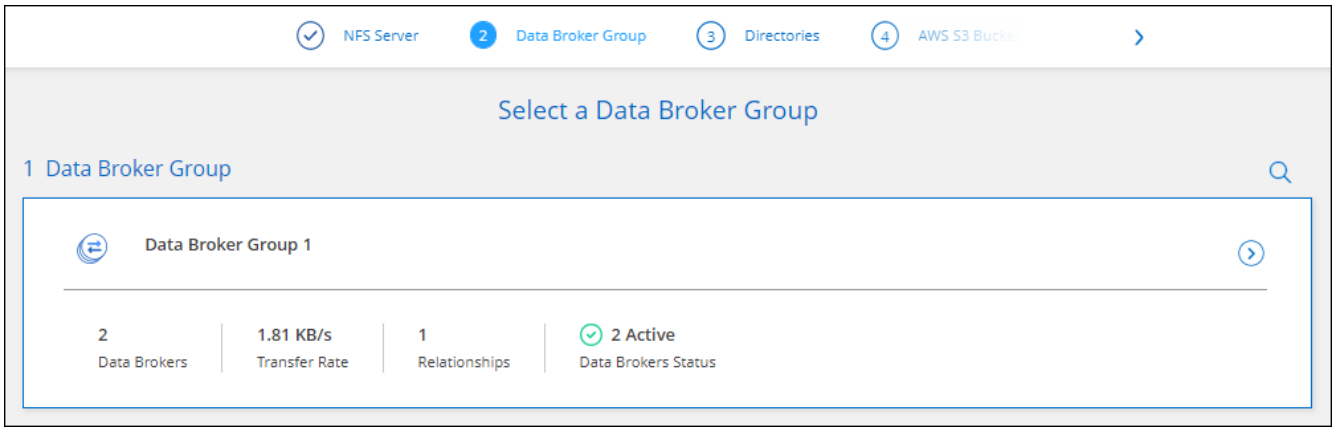
1. BlueXP에서 * 동기화 * 를 선택합니다.
2. 동기화 관계 정의 * 페이지에서 소스 및 대상을 선택합니다.

   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 선택합니다.

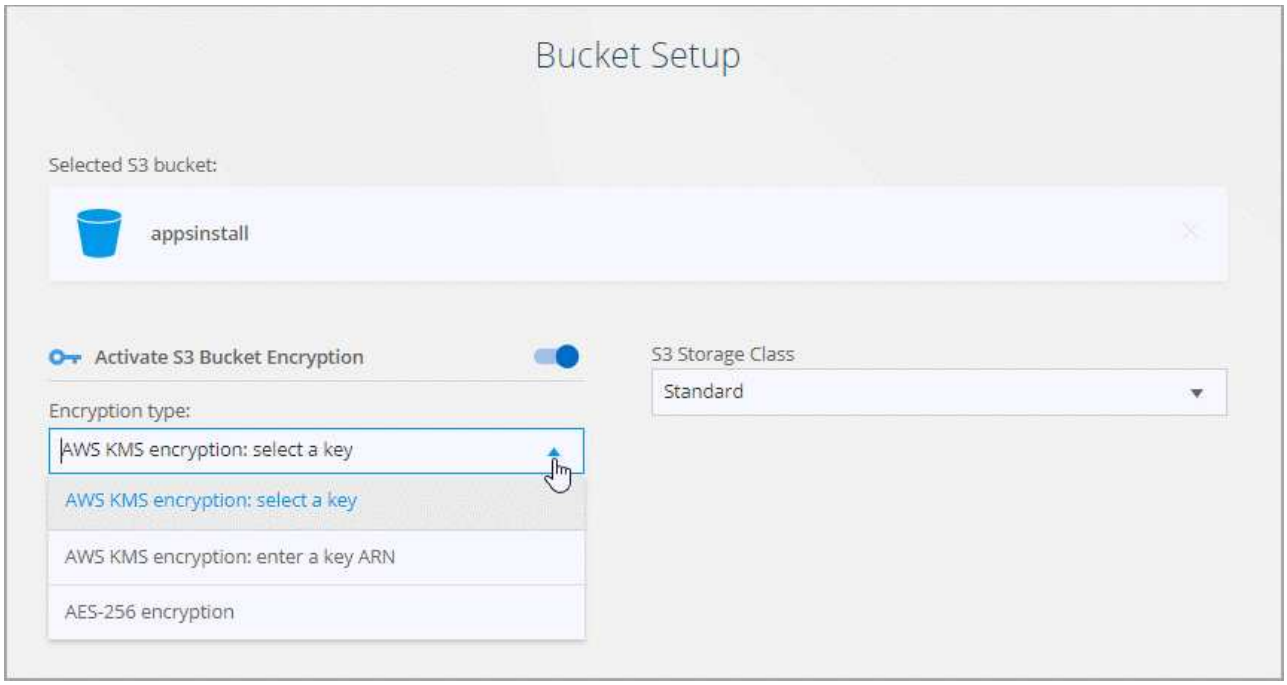


6. [[FILTER](* 디렉터리*) 페이지에서 최상위 디렉터리나 하위 디렉터리를 선택합니다.

   BlueXP 복사 및 동기화가 내보내기를 검색할 수 없는 경우 * 내보내기 수동 추가 * 를 선택하고 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 선택하여 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

지정된 분, 시간 또는 일 수 동안 동기화가 완료되지 않은 경우 BlueXP 복사 및 동기화가 데이터 동기화를 취소할지 여부를 정의합니다.

알림

BlueXP의 알림 센터에서 BlueXP 복사 및 동기화 알림 수신 여부를 선택할 수 있습니다. 성공적인 데이터 동기화, 실패한 데이터 동기화 및 취소된 데이터 동기화를 위한 알림을 활성화할 수 있습니다.

다시 시도

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

연속 동기화

초기 데이터 동기화 후 BlueXP 복사 및 동기화는 소스 S3 버킷 또는 Google Cloud Storage 버킷의 변경 사항을 수신 대기시키고 변경 사항이 발생할 때마다 타겟에 대한 변경 사항을 지속적으로 동기화합니다. 예약된 간격으로 소스를 다시 검색할 필요가 없습니다.

이 설정은 동기화 관계를 생성하고 S3 버킷 또는 Google Cloud Storage의 데이터를 Azure Blob 스토리지, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3, Azure StorageGRID Blob 스토리지에서 Azure Blob 스토리지, CIFS, Google 클라우드 스토리지, IBM 클라우드 오브젝트 스토리지, NFS 및 StorageGRID * 까지 지원합니다.

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.
- S3이 소스인 경우 크기별로 필터링은 삭제 이벤트가 아닌 복사 이벤트에서만 활성화됩니다.
- 관계가 생성된 후에는 관계를 가속화하거나 삭제할 수만 있습니다. 동기화를 중단하거나, 설정을 수정하거나, 보고서를 볼 수 없습니다.

  외부 버킷과 연속 동기화 관계를 생성할 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

  i. 외부 버킷의 프로젝트를 보려면 Google Cloud 콘솔로 이동하십시오.
  ii. 클라우드 스토리지 > 설정 > 클라우드 스토리지 서비스 계정 * 으로 이동합니다.
  iii. 로컬 .json 파일 업데이트:

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

iv. 데이터 브로커 재시작:

   A. sudo pm2 모두 중지합니다

   B. sudo pm2 모두 시작

v. 관련 외부 버킷과 연속 동기화 관계를 생성합니다.

> 외부 버킷과의 연속 동기화 관계를 생성하는 데 사용되는 데이터 브로커는 프로젝트의 버킷과 또 다른 연속 동기화 관계를 생성할 수 없습니다.

비교 기준

파일 또는 디렉토리가 변경되었으며 다시 동기화되어야 하는지 여부를 결정할 때 BlueXP 복사 및 동기화가 특정 속성을 비교해야 하는지 여부를 선택합니다.

이러한 속성을 선택 취소하더라도 경로, 파일 크기 및 파일 이름을 확인하여 BlueXP 복사 및 동기화는 여전히 소스를 대상과 비교합니다. 변경 사항이 있으면 해당 파일과 디렉토리를 동기화합니다.

다음 속성을 비교할 때 BlueXP 복사 및 동기화를 활성화 또는 비활성화할 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 BlueXP는 다음 동기화 시 이 개체를 복사하고 동기화하지만 사용자가 소스(데이터 자체는 아님)의 태그를 변경하면 BlueXP 복사 및 동기화는 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

BlueXP 복사 후 소스 위치에서 파일을 삭제하고 파일을 타겟 위치에 동기화하도록 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
}
}
}
```

로컬 .json 파일을 업데이트한 후 다시 시작해야 합니다. `pm2 restart all`.

대상에서 파일 삭제

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

파일 형식

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

> 하드 링크는 보안되지 않은 NFS 대 NFS 관계에만 사용할 수 있습니다. 사용자는 하나의 스캐너 프로세스와 하나의 스캐너 동시 접속으로 제한되며 루트 디렉터리에서 스캔을 실행해야 합니다.

파일 확장명 제외

파일 확장자를 입력하고 * Enter * 를 눌러 동기화에서 제외할 regex 또는 파일 확장자를 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/bluexp-copy-sync//media/video_file_extensions.mp4 *(video)*

> 정규식 또는 정규식은 와일드카드나 glob 식과 다릅니다. 이 기능은 * 만 * regex와 함께 사용할 수 있습니다.

제외 디렉터리

이름 또는 디렉토리 전체 경로를 입력하고 * Enter * 를 눌러 동기화에서 제외할 최대 15개의 regex 또는 디렉토리를 지정합니다. copy-offload, .snapshot, ~snapshot 디렉토리는 기본적으로 제외됩니다.

정규식 또는 정규식은 와일드카드나 glob 식과 다릅니다. 이 기능은 * 만 * regex와 함께 사용할 수 있습니다.

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.

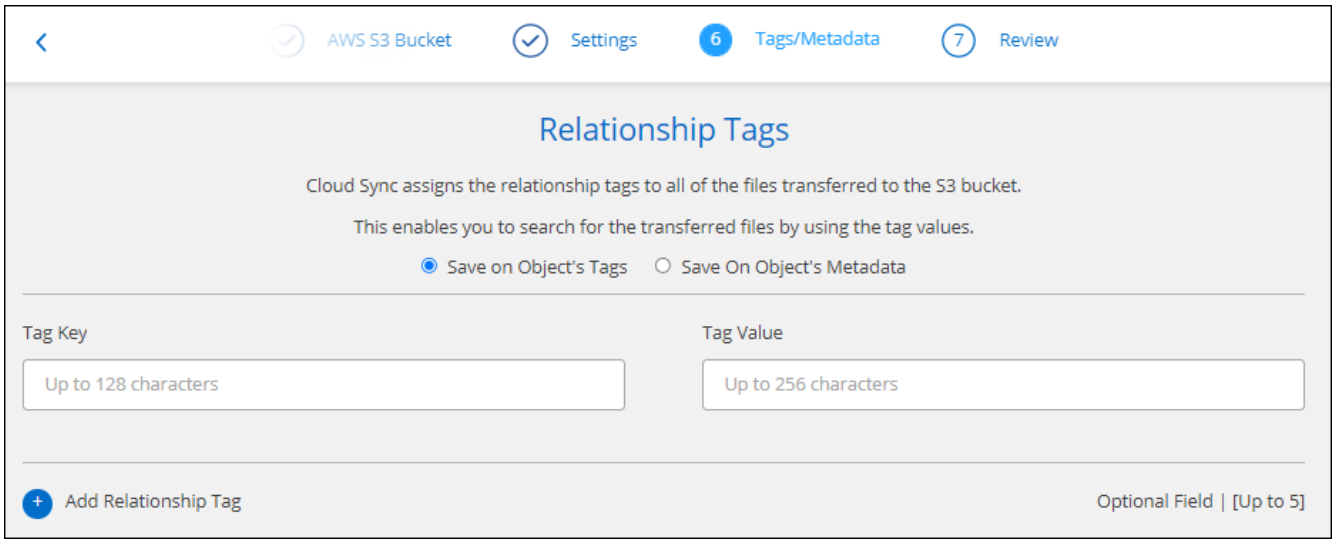
만든 날짜

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

관계를 만들 때 또는 관계를 만든 후에 설정을 활성화하여 SMB 서버에서 ACL만, 파일 전용 또는 ACL 및 파일을 복사합니다.

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



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 선택합니다.

결과 *

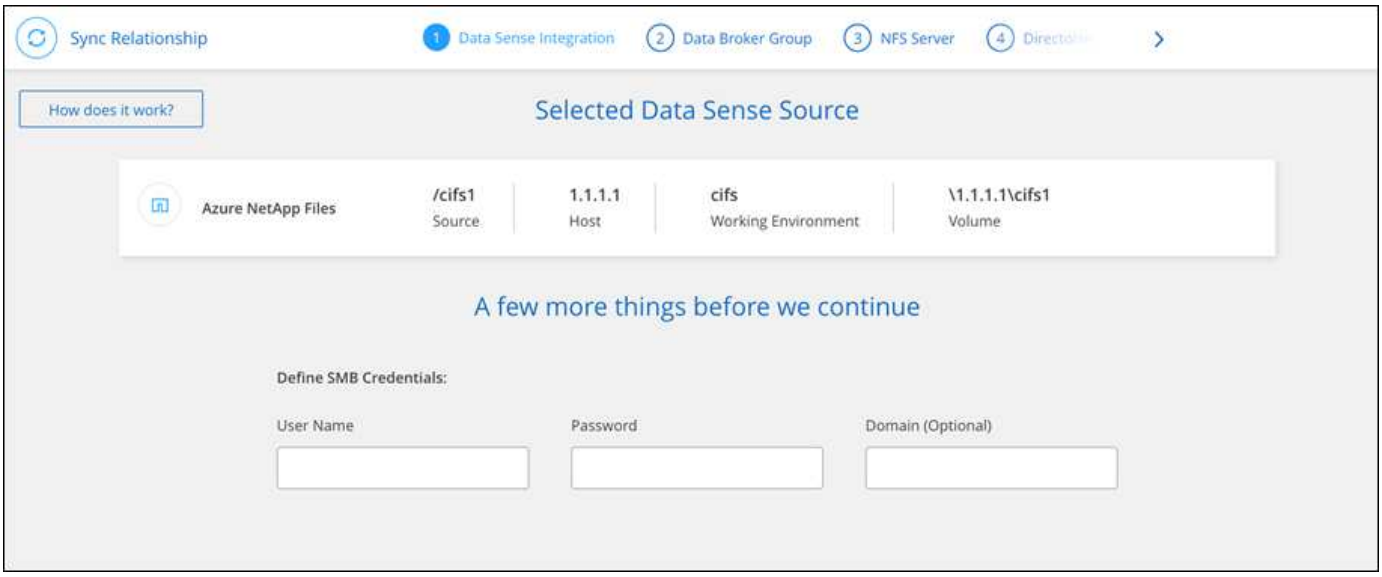
BlueXP 복사 및 동기화는 소스와 대상 간의 데이터 동기화를 시작합니다.

BlueXP 분류에서 동기화 관계를 생성합니다

BlueXP 복사 및 동기화는 BlueXP 분류와 통합되어 있습니다. BlueXP 분류 내에서 BlueXP 복사 및 동기화를 사용하여

대상 위치에 동기화할 소스 파일을 선택할 수 있습니다.

BlueXP 분류에서 데이터 동기화를 시작하면 모든 소스 정보가 한 번에 포함되고 몇 가지 키 세부 정보만 입력하면 됩니다. 그런 다음 새 동기화 관계의 타겟 위치를 선택합니다.



"BlueXP 분류에서 동기화 관계를 시작하는 방법에 대해 알아봅니다".

SMB 공유에서 ACL 복사

BlueXP 복사 및 동기화는 SMB 공유 간, SMB 공유와 오브젝트 스토리지 간(ONTAP S3 제외) ACL(액세스 제어 목록)을 복사할 수 있습니다. 필요한 경우 Robo-Copy를 사용하여 SMB 공유 간의 ACL을 수동으로 보존할 수도 있습니다.

선택

- BlueXP 복사 및 동기화를 설정하여 ACL을 자동으로 복사합니다
- SMB 공유 간에 ACL을 수동으로 복사합니다

BlueXP 복사 및 동기화를 설정하여 ACL을 복사합니다

SMB 공유를 생성하거나 관계를 생성한 후 설정을 사용하여 SMB 공유와 SMB 공유 및 오브젝트 스토리지 간에 ACL을 복사합니다.

시작하기 전에

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".

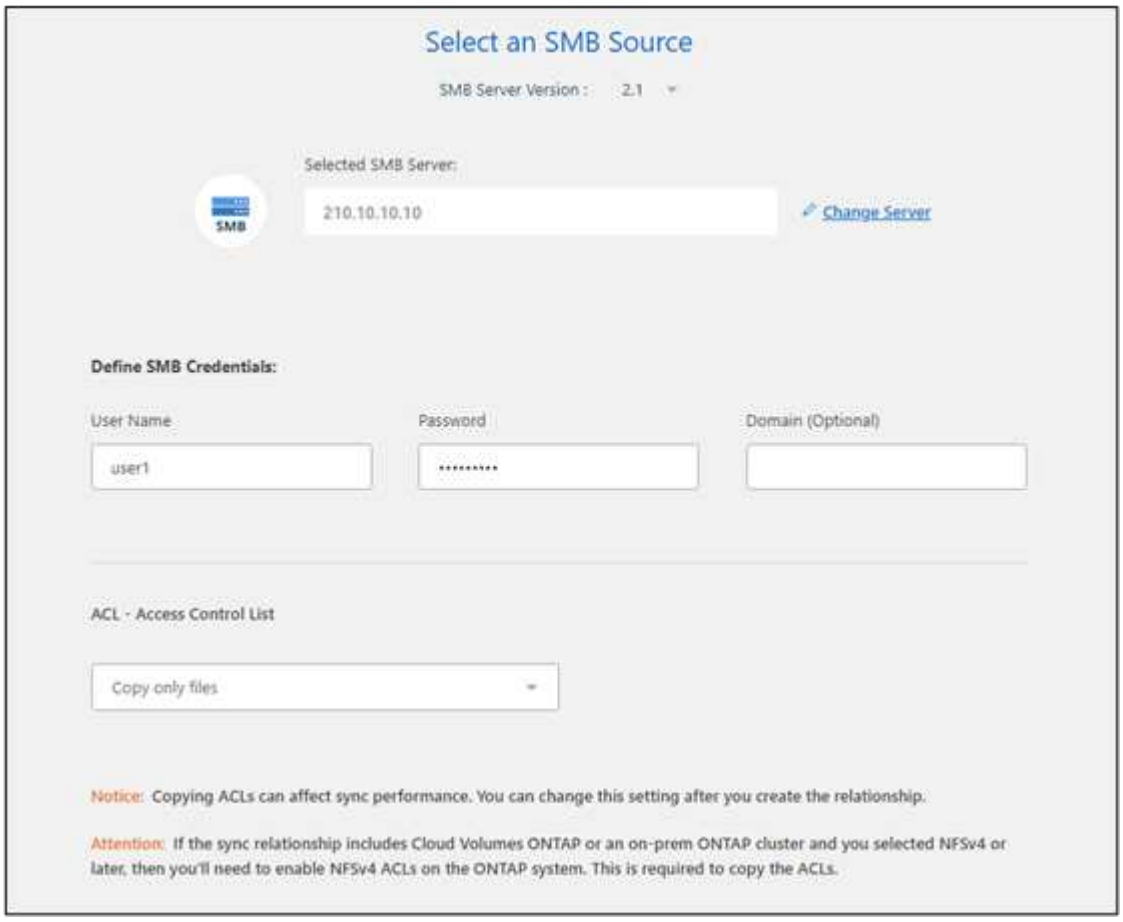
새로운 관계를 위한 단계

1. BlueXP 복사 및 동기화에서 * 새 동기화 생성 * 을 선택합니다.
2. SMB 서버 또는 오브젝트 스토리지를 소스로, SMB 서버 또는 오브젝트 스토리지로 끌어 놓고 * 계속 * 을 선택합니다.
3. SMB 서버 * 페이지에서 다음을 수행합니다.

a. 새 SMB 서버를 입력하거나 기존 서버를 선택하고 * 계속 * 을 선택합니다.

b. SMB 서버의 자격 증명을 입력합니다.

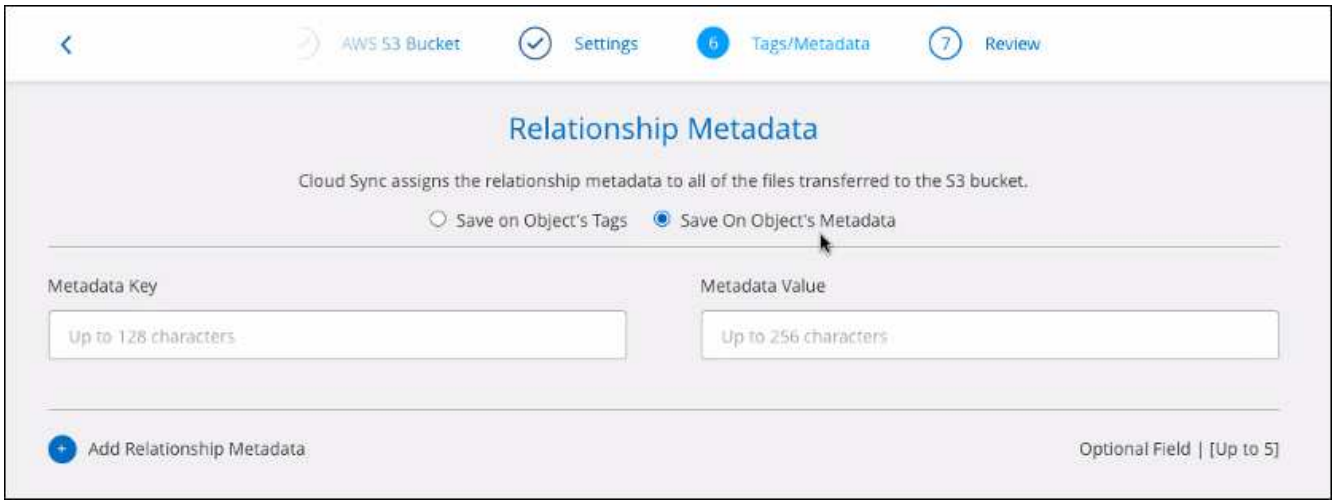
c. 파일 * 복사 전용 *, * ACL * 복사 또는 * 파일 및 ACL * 복사 중 하나를 선택하고 * 계속 * 을 선택합니다.



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.



기존 관계에 대한 단계

1. 동기화 관계 위로 마우스를 가져가서 작업 메뉴를 선택합니다.
2. 설정 * 을 선택합니다.
3. 파일 * 복사 전용 *, * ACL * 복사 또는 * 파일 및 ACL * 복사 중 하나를 선택하고 * 계속 * 을 선택합니다.
4. 설정 저장 * 을 선택합니다.

결과

데이터를 동기화할 때 BlueXP 복사 및 동기화는 소스와 타겟 간의 ACL을 보존합니다.

SMB 공유 간에 ACL을 수동으로 복사합니다

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. BlueXP 복사 및 동기화에서 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

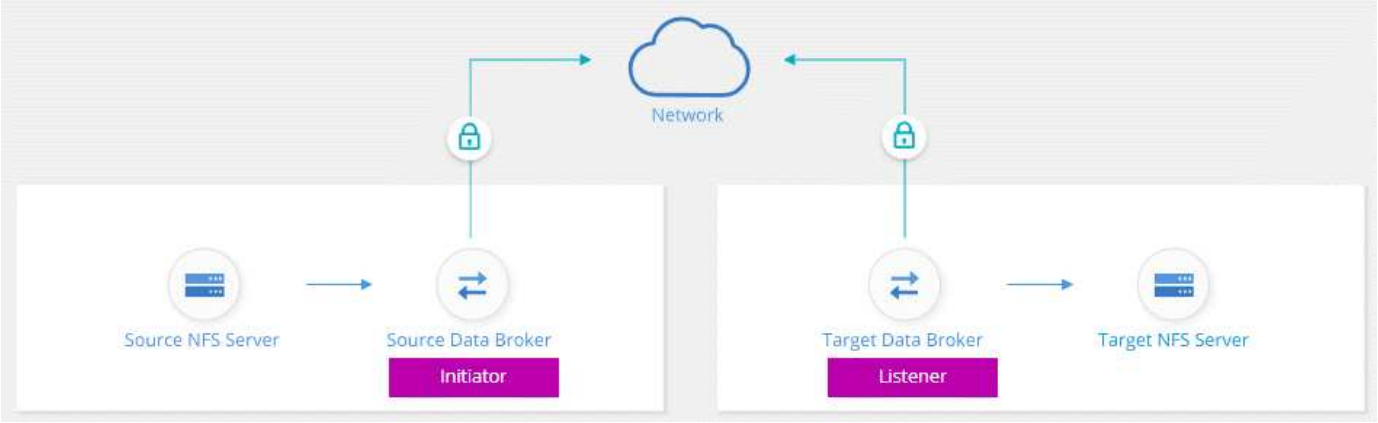
회사에 엄격한 보안 정책이 있는 경우 전송 중인 데이터 암호화를 사용하여 NFS 데이터를

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 선택합니다.
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.

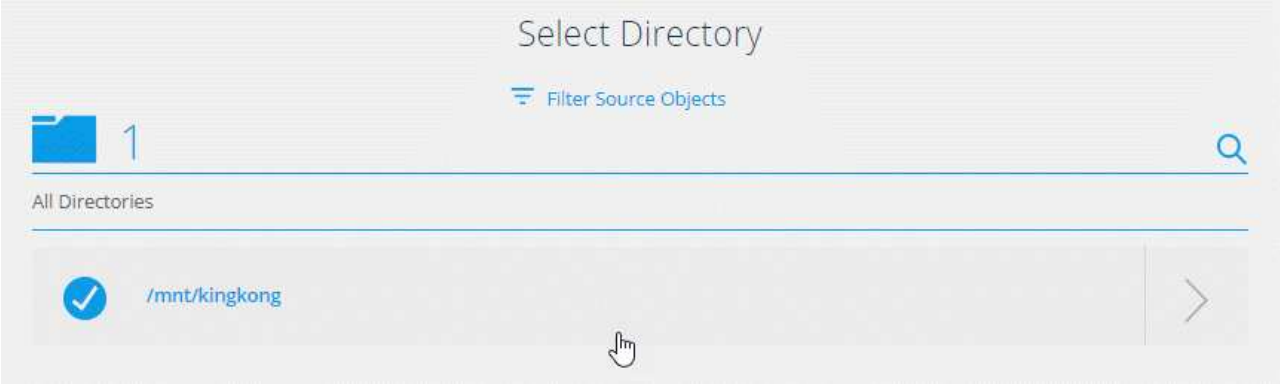
      - 기존 데이터 브로커 그룹을 사용하려면 그룹에 데이터 브로커가 하나만 있어야 합니다. 암호화된 동기화

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 BlueXP 복사 및 동기화에 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 선택합니다.

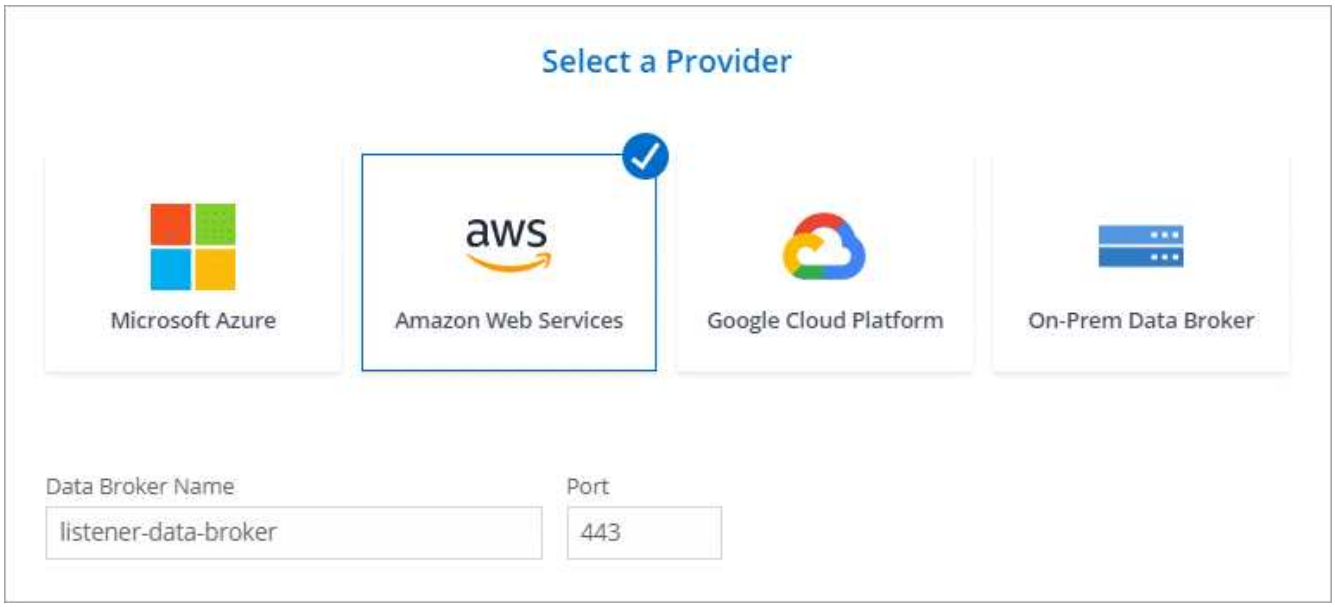


e. * 타겟 NFS 서버 * / * 타겟 Azure NetApp Files *: NFS 버전을 선택한 다음 새 NFS 타겟을 입력하거나 기존 서버를 선택합니다.

f. * 대상 데이터 브로커 *: 프롬프트에 따라 새 소스 데이터 브로커를 추가하거나 기존 데이터 브로커를 선택합니다.

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

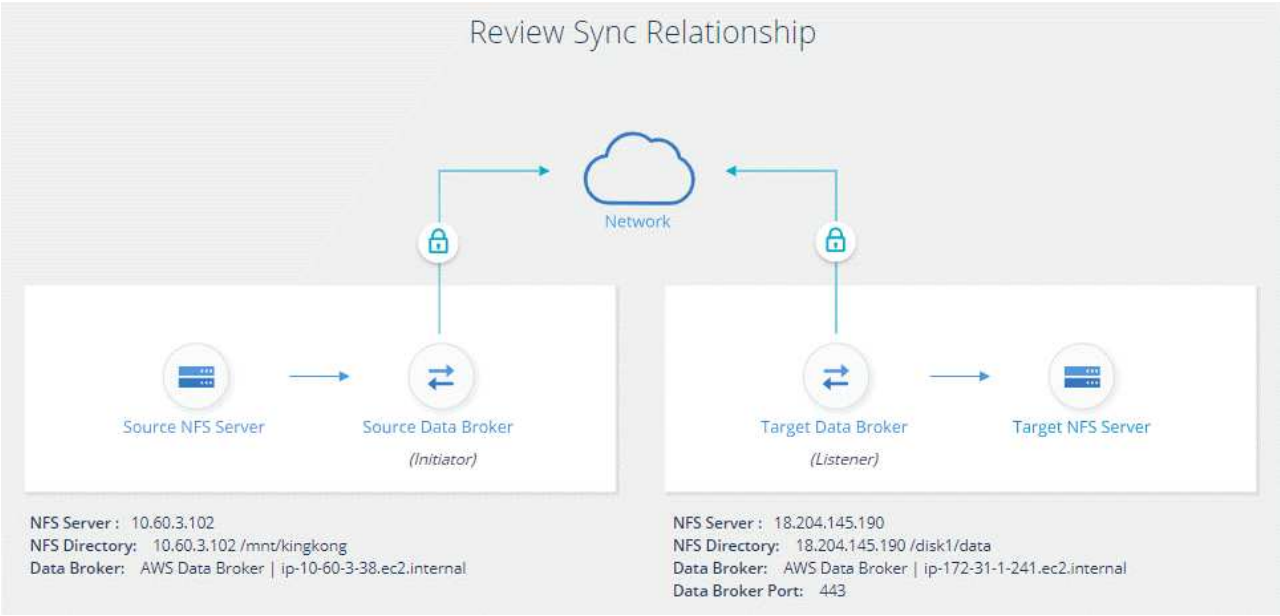
다음은 대상 데이터 브로커가 수신기로 작동할 때의 프롬프트의 예입니다. 포트를 지정하는 옵션을 확인합니다.



a. * 대상 디렉터리 *: 최상위 디렉터리를 선택하거나 드릴다운하여 기존 하위 디렉터리를 선택하거나 내보내기 내에 새 폴더를 만듭니다.

b. * 설정 *: 원본 파일과 폴더가 대상 위치에서 동기화 및 유지되는 방식을 정의합니다.

c. * 검토 *: 동기화 관계의 세부 정보를 검토한 다음 * 관계 생성 * 을 선택합니다.



결과

BlueXP 복사 및 동기화는 새 동기화 관계를 생성합니다. 완료되면 * Dashboard에서 보기 * 를 선택하여 새 관계에 대한 세부 정보를 봅니다.

외부 **HashCorp Vault**를 사용하도록 데이터 브로커 그룹을 설정합니다

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

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

1 볼트를 준비합니다

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

2 데이터 브로커 그룹을 준비합니다

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

3 API를 사용하여 동기화 관계를 생성합니다

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

볼트 준비 중

BlueXP 복사본을 제공하고 URL과 볼트 내 비밀에 동기화해야 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 **ID**입니다
: 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/config에 있는 local.json 파일을 편집합니다.

3. enable을 * 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.

BlueXP 복사 및 동기화 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 BlueXP 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"
        }
    }
}
```