시작하기
NetApp Copy and Sync

NetApp
December 16, 2025

목차

시작하기

NetApp Copy and Sync 에 대해 알아보세요

NetApp Copy and Sync 클라우드나 사내에 있는 모든 대상으로 데이터를 마이그레이션하는 간단하고 안전하며 자동화된 방법을 제공합니다. 파일 기반 NAS 데이터 세트(NFS 또는 SMB), Amazon Simple Storage Service(S3) 객체 형식, NetApp StorageGRID 어플라이언스 또는 기타 클라우드 공급자 객체 저장소 등 어떤 것이든 Copy and Sync가 이를 변환하고 이동할 수 있습니다.

NetApp Console

NetApp Copy and Sync NetApp Console 통해 액세스할 수 있습니다.

NetApp Console 엔터프라이즈급 온프레미스 및 클라우드 환경 전반에서 NetApp 스토리지 및 데이터 서비스를 중앙에서 관리할 수 있는 기능을 제공합니다. NetApp 데이터 서비스에 액세스하고 사용하려면 콘솔이 필요합니다. 관리 인터페이스로서, 하나의 인터페이스에서 여러 스토리지 리소스를 관리할 수 있습니다. 콘솔 관리자는 기업 내 모든 시스템의 저장소와 서비스에 대한 액세스를 제어할 수 있습니다.

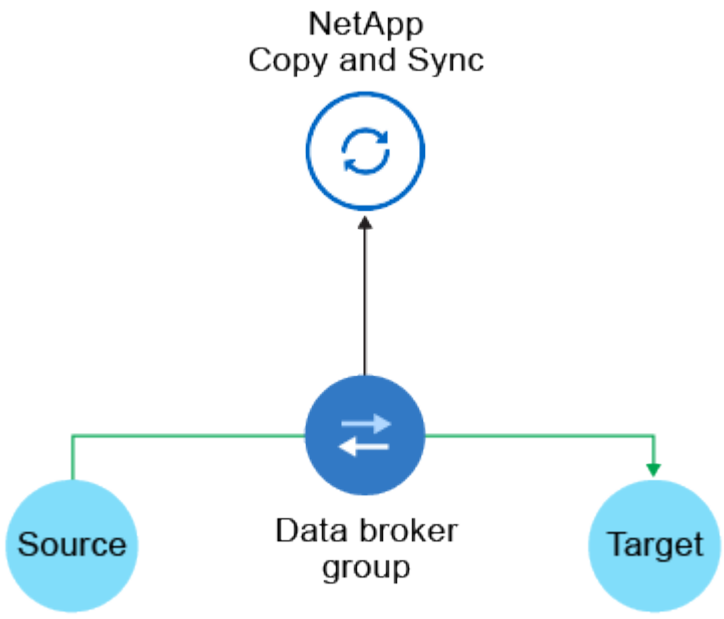
NetApp Console 사용하려면 라이선스나 구독이 필요하지 않으며, 스토리지 시스템이나 NetApp 데이터 서비스에 대한 연결을 보장하기 위해 클라우드에 Console 에이전트를 배포해야 할 때만 요금이 부과됩니다. 그러나 콘솔에서 액세스할 수 있는 일부 NetApp 데이터 서비스는 라이선스 기반이거나 구독 기반입니다.

자세히 알아보세요 "NetApp Console" .

NetApp Copy and Sync 작동 방식

NetApp Copy and Sync 데이터 브로커 그룹, NetApp Console 통해 사용 가능한 클라우드 기반 인터페이스, 소스 및 대상으로 구성된 SaaS(Software-as-a-Service) 플랫폼입니다.

다음 이미지는 복사 및 동기화 구성 요소 간의 관계를 보여줍니다.



NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(이를 _동기화 관계_라고 합니다). AWS, Azure, Google Cloud Platform 또는 사내에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 Copy and Sync와 통신하고 몇몇 다른 서비스와 저장소에 접속할 수 있도록 포트 443을 통한 아웃바운드 인터넷 연결이 필요합니다. "엔드포인트 목록 보기" .

최초 복사 후, 복사 및 동기화는 사용자가 설정한 일정에 따라 변경된 데이터를 동기화합니다.

지원되는 저장 유형

복사 및 동기화는 다음과 같은 저장 유형을 지원합니다.

- 모든 NFS 서버
- 모든 SMB 서버
- 아마존 EFS
- ONTAP 용 Amazon FSx
- 아마존 S3
- Azure Blob
- Azure 데이터 레이크 스토리지 Gen2
- Azure NetApp Files
- 상자(미리보기로 제공)
- Cloud Volumes ONTAP
- 구글 클라우드 스토리지
- 구글 드라이브
- IBM 클라우드 객체 스토리지
- 온프레미스 ONTAP 클러스터
- ONTAP S3 스토리지
- SFTP(API만 사용)
- StorageGRID

"지원되는 동기화 관계 보기" .

소송 비용

Copy and Sync를 사용하는 데에는 리소스 요금과 서비스 요금이라는 두 가지 유형의 비용이 있습니다.

자원 요금

리소스 요금은 클라우드에서 하나 이상의 데이터 브로커를 실행하는 데 드는 컴퓨팅 및 저장 비용과 관련됩니다.

서비스 요금

14일 무료 체험 기간이 종료된 후에는 동기화 관계에 대한 비용을 지불하는 두 가지 방법이 있습니다. 첫 번째 옵션은 AWS나 Azure에서 구독하는 것입니다. 이 경우 시간당 또는 연간 요금을 지불할 수 있습니다. 두 번째 옵션은 NetApp 에서 직접 라이선스를 구매하는 것입니다.

"라이선싱이 어떻게 작동하는지 알아보세요" .

NetApp Copy and Sync 위한 빠른 시작

NetApp Copy and Sync 시작하려면 몇 가지 단계가 필요합니다.

1 로그인하고 NetApp Console 설정하세요

NetApp Console 시작했어야 합니다. 여기에는 로그인, 계정 설정, 콘솔 에이전트 배포 및 시스템 생성이 포함됩니다.

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

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

Cloud Volumes ONTAP, 온프레미스 ONTAP 클러스터 및 Amazon FSx for ONTAP 에는 콘솔 에이전트가 필요합니다.

- "NetApp Console 을 시작하는 방법을 알아보세요"
- "콘솔 에이전트에 대해 자세히 알아보세요"

2 소스와 타겟을 준비하세요

소스와 타겟이 지원되고 설정되어 있는지 확인하세요. 가장 중요한 요구 사항은 데이터 브로커 그룹과 소스 및 타겟 위치 간의 연결을 확인하는 것입니다.

- "지원되는 관계 보기"
- "소스와 타겟을 준비하세요"

3 NetApp 데이터 브로커를 위한 위치 준비

NetApp 데이터 브로커 소프트웨어는 소스에서 타겟으로 데이터를 동기화합니다(이를 _동기화 관계_라고 합니다). AWS, Azure, Google Cloud Platform 또는 사내에서 데이터 브로커를 실행할 수 있습니다. 하나 이상의 데이터 브로커로 구성된 데이터 브로커 그룹은 NetApp Copy and Sync 와 통신하고 몇몇 다른 서비스와 저장소에 접속할 수 있도록 포트 443을 통한 아웃바운드 인터넷 연결이 필요합니다. "엔드포인트 목록 보기" .

NetApp Copy and Sync 동기화 관계를 생성할 때 설치 과정을 안내하며, 이때 클라우드에 데이터 브로커를 배포하거나 자체 Linux 호스트에 대한 설치 스크립트를 다운로드할 수 있습니다.

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

4 첫 번째 동기화 관계를 만드세요

로그인하세요 "NetApp Console" , *동기화*를 선택한 다음 소스와 대상에 대한 선택 항목을 끌어서 놓습니다. 화면의 지시에 따라 설정을 완료하세요. "자세히 알아보기" .

5 무료 평가판이 종료된 후 동기화 관계에 대한 비용을 지불하세요.

AWS 또는 Azure에 가입하여 사용량에 따라 요금을 지불하거나 연간 요금을 지불하세요. 또는 NetApp 에서 직접 라이선스를 구매하세요. NetApp Copy and Sync 의 라이선스 설정 페이지로 가서 설정하기만 하면 됩니다. "자세히 알아보기" .

NetApp Copy and Sync 에서 지원되는 동기화 관계

NetApp Copy and Sync 사용하면 소스에서 대상으로 데이터를 동기화할 수 있습니다. 이것을 동기화 관계라고 합니다. 시작하기 전에 지원되는 관계를 이해해야 합니다.

소스 위치	지원되는 대상 위치
아마존 EFS	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
ONTAP 용 Amazon FSx	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
아마존 S3	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
Azure Blob	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
Azure 데이터 레이크 스토리지 Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • ONTAP 용 FSx • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
Azure NetApp Files	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
상자 [1]	• ONTAP 용 Amazon FSx • 아마존 S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM 클라우드 객체 스토리지 • NFS 서버 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
Cloud Volumes ONTAP	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
구글 클라우드 스토리지	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID
구글 드라이브	• NFS 서버 • SMB 서버

소스 위치	지원되는 대상 위치
IBM 클라우드 객체 스토리지	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
NFS 서버	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • 구글 드라이브 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

소스 위치	지원되는 대상 위치
온프레미스 ONTAP 클러스터(NFS 또는 SMB)	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • SMB 서버 • StorageGRID
ONTAP S3 스토리지	• 아마존 S3 • Azure 데이터 레이크 스토리지 Gen2 • 구글 클라우드 스토리지 • NFS 서버 • SMB 서버 • StorageGRID • ONTAP S3 스토리지
SFTP [2]	S3

소스 위치	지원되는 대상 위치
SMB 서버	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • 구글 드라이브 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID
StorageGRID	• 아마존 EFS • ONTAP 용 Amazon FSx • 아마존 S3 • Azure Blob • Azure 데이터 레이크 스토리지 Gen2 • Azure NetApp Files • 상자 [1] • Cloud Volumes ONTAP • 구글 클라우드 스토리지 • IBM 클라우드 객체 스토리지 • NFS 서버 • 온프레미스 ONTAP 클러스터(NFS 또는 SMB) • ONTAP S3 스토리지 • SMB 서버 • StorageGRID

참고사항:

1. Box 지원은 미리보기로 제공됩니다.

2. 이 소스/대상과의 동기화 관계는 Copy 및 Sync API를 사용해서만 지원됩니다.
3. Blob 컨테이너가 대상인 경우 특정 Azure Blob 저장소 계층을 선택할 수 있습니다.
    - 뜨거운 보관
    - 시원한 보관
4. Amazon S3가 대상인 경우 특정 S3 스토리지 클래스를 선택할 수 있습니다.
    - 표준(기본 클래스)
    - 지능형 계층화
    - 표준-빈번하지 않은 액세스
    - 1존-접근 빈도 낮음
    - 빙하 심층 기록 보관소
    - Glacier Flexible Retrieval
    - 빙하 즉시 검색
5. Google Cloud Storage 버킷이 대상인 경우 특정 스토리지 클래스를 선택할 수 있습니다.
    - 기준
    - 니어라인
    - 콜드라인
    - 보관소

NetApp Copy and Sync 에서 소스와 대상을 준비합니다.

NetApp Copy and Sync 에서 소스와 대상이 다음 요구 사항을 충족하는지 확인하세요.

네트워킹

- 소스와 대상은 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

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

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

대상 디렉토리

동기화 관계를 만들면 복사 및 동기화를 통해 기존 대상 디렉토리를 선택한 다음, 선택적으로 해당 디렉토리 내에 새 폴더를 만들 수 있습니다. 따라서 원하는 대상 디렉토리가 이미 존재하는지 확인하세요.

디렉토리 읽기 권한

소스 또는 대상의 모든 디렉토리나 폴더를 표시하려면 복사 및 동기화에 디렉토리나 폴더에 대한 읽기 권한이 필요합니다.

NFS

파일과 디렉토리의 uid/gid를 사용하여 소스/대상에 대한 권한을 정의해야 합니다.

객체 스토리지

- AWS 및 Google Cloud의 경우 데이터 브로커에는 목록 개체 권한이 있어야 합니다(이러한 권한은 데이터 브로커 설치 단계를 따르면 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 브로커는 기본적으로 다음 디렉토리를 무시합니다: .snapshot, ~snapshot, .copy-offload

Copy and Sync 기능을 사용하여 SMB 데이터를 Cloud Volumes ONTAP 으로 복사할 때 소스 시스템의 파일 및 폴더 소유권이 유지되지 않습니다. 이러한 동작은 복사 및 동기화 기능이 Linux SMB 클라이언트를 사용하기 때문에 발생하는데, 이 클라이언트는 전송 인증에 사용된 사용자 또는 서비스 계정에 소유권을 할당합니다. 접근 제어 목록은 유지될 수 있지만, 소유권 및 감사 정보는 원본 시스템과 다를 수 있습니다. 이는 예상되는 동작입니다.

Amazon S3 버킷 요구 사항

Amazon S3 버킷이 다음 요구 사항을 충족하는지 확인하세요.

Amazon S3에 지원되는 데이터 브로커 위치

S3 스토리지를 포함하는 동기화 관계에는 AWS 또는 사내에 배포된 데이터 브로커가 필요합니다. 어느 경우든, 복사 및 동기화는 설치 중에 데이터 브로커를 AWS 계정과 연결하라는 메시지를 표시합니다.

- "AWS 데이터 브로커를 배포하는 방법을 알아보세요"
- "Linux 호스트에 데이터 브로커를 설치하는 방법을 알아보세요"

지원되는 **AWS** 지역

중국 지역을 제외한 모든 지역이 지원됩니다.

다른 **AWS** 계정의 **S3** 버킷에 필요한 권한

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

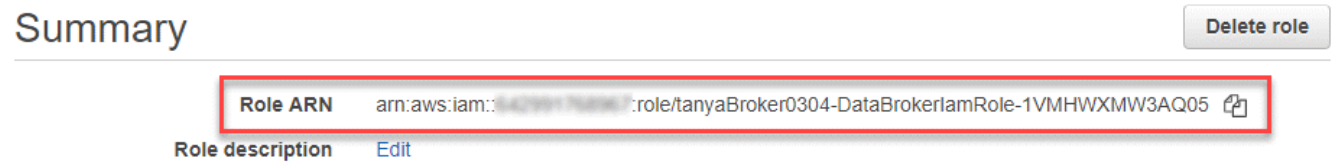
"이 JSON 파일에 포함된 권한"데이터 브로커가 액세스할 수 있도록 해당 S3 버킷에 적용해야 합니다. 이러한 권한을 통해 데이터 브로커는 버킷에서 데이터를 복사하거나 버킷에 있는 객체를 나열할 수 있습니다.

JSON 파일에 포함된 권한에 대해 다음 사항을 참고하세요.

1. _<BucketName>_은 데이터 브로커와 연결되지 않은 AWS 계정에 있는 버킷의 이름입니다.
2. _<RoleARN>_은 다음 중 하나로 대체되어야 합니다.

- Linux 호스트에 데이터 브로커를 수동으로 설치한 경우 _RoleARN_은 데이터 브로커를 배포할 때 AWS 자격 증명을 제공한 AWS 사용자의 ARN이어야 합니다.
- CloudFormation 템플릿을 사용하여 AWS에 데이터 브로커가 배포된 경우 _RoleARN_은 템플릿에서 생성된 IAM 역할의 ARN이어야 합니다.

  EC2 콘솔로 이동하여 데이터 브로커 인스턴스를 선택한 다음 설명 탭에서 IAM 역할을 선택하면 역할 ARN을 찾을 수 있습니다. 그러면 IAM 콘솔에서 역할 ARN이 포함된 요약 페이지가 표시됩니다.



Azure Blob 저장소 요구 사항

Azure Blob 저장소가 다음 요구 사항을 충족하는지 확인하세요.

Azure Blob에 지원되는 데이터 브로커 위치

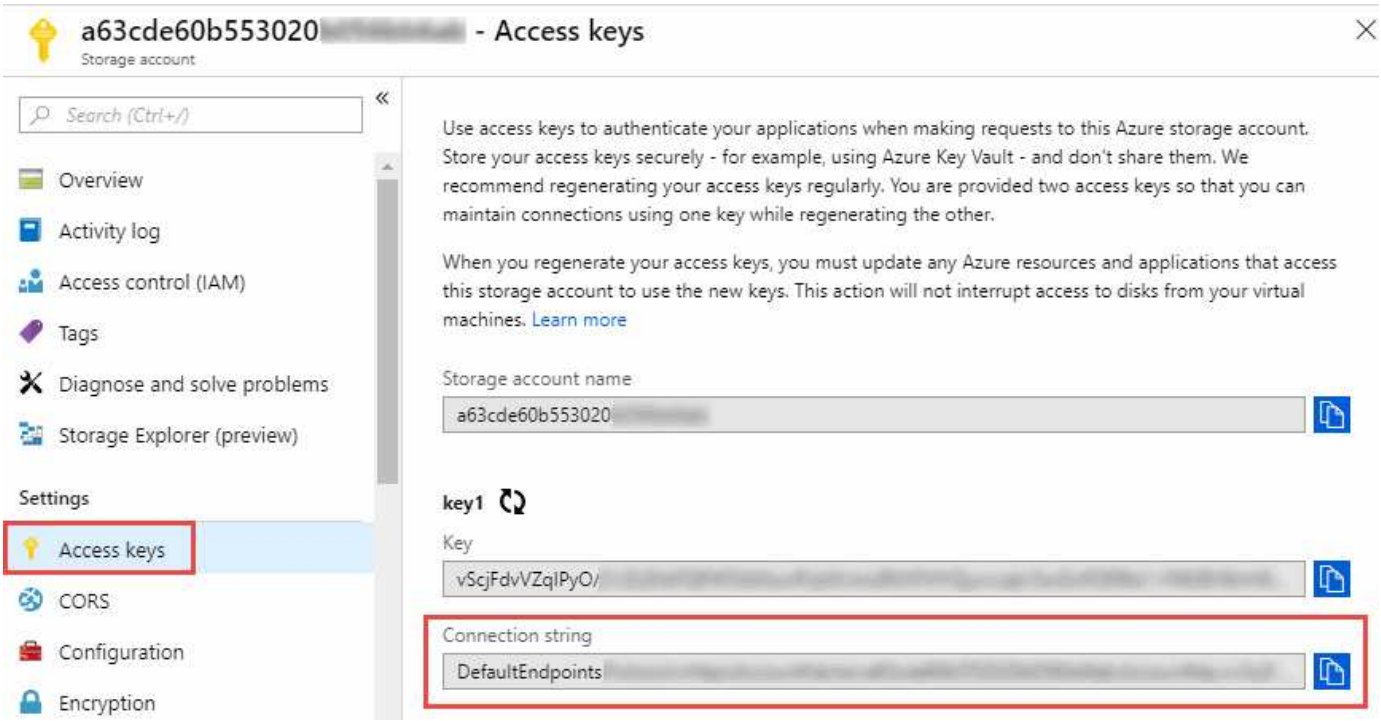
동기화 관계에 Azure Blob 저장소가 포함된 경우 데이터 브로커는 어느 위치에나 상주할 수 있습니다.

지원되는 Azure 지역

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

Azure Blob 및 NFS/SMB를 포함하는 관계에 대한 연결 문자열

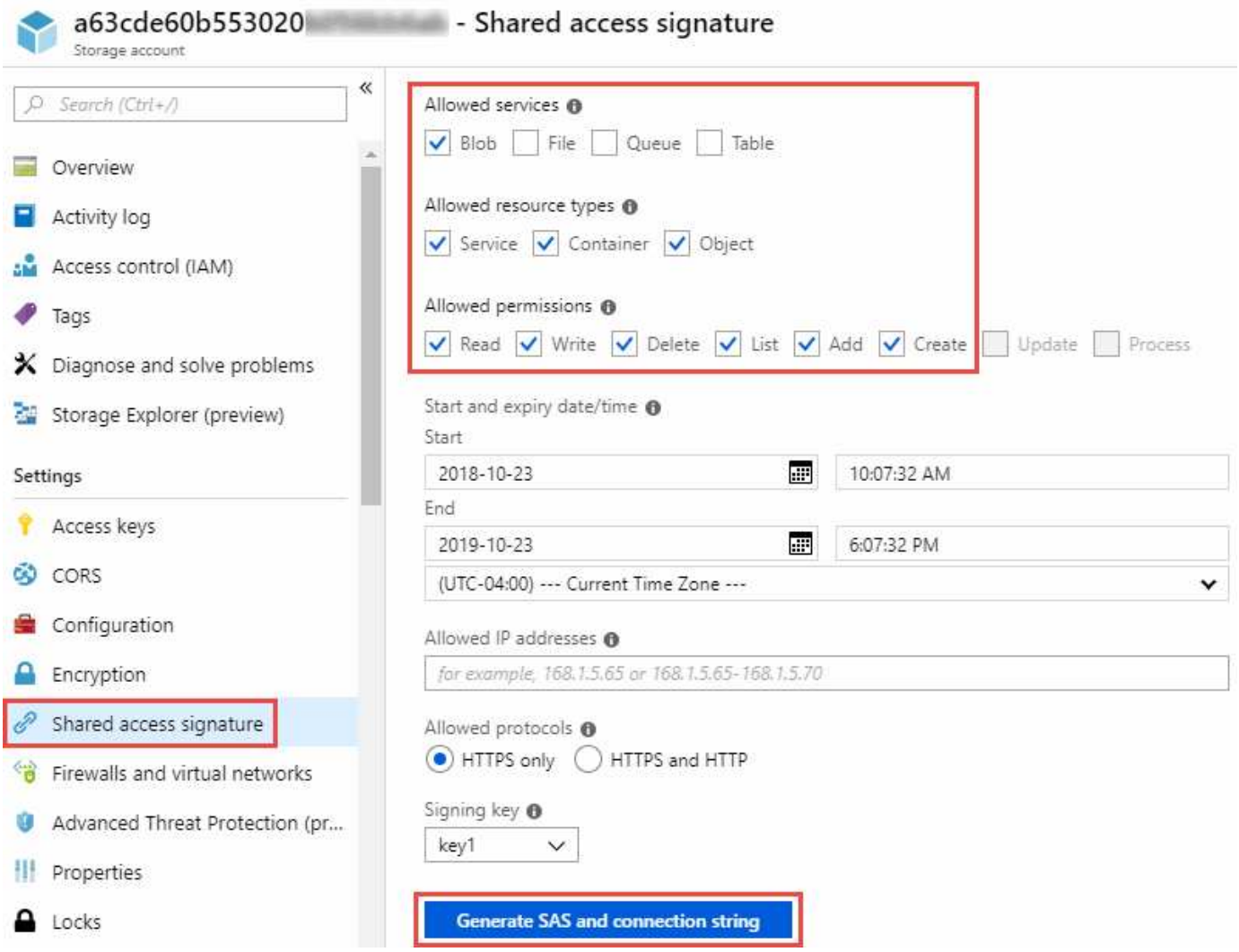
Azure Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화 관계를 만들 때는 저장소 계정 연결 문자열을 사용하여 Copy 및 Sync를 제공해야 합니다.



두 Azure Blob 컨테이너 간에 데이터를 동기화하려면 연결 문자열에 다음을 포함해야 합니다. "공유 액세스 서명" (SAS). Blob 컨테이너와 NFS 또는 SMB 서버 간에 동기화할 때 SAS를 사용하는 옵션도 있습니다.

SAS는 Blob 서비스와 모든 리소스 유형(서비스, 컨테이너, 개체)에 대한 액세스를 허용해야 합니다. SAS에는 다음 권한도 포함되어야 합니다.

- 소스 Blob 컨테이너의 경우: 읽기 및 나열
- 대상 Blob 컨테이너의 경우: 읽기, 쓰기, 나열, 추가 및 생성



Azure Blob 컨테이너를 포함하는 Continuous Sync 관계를 구현하도록 선택하는 경우 일반 연결 문자열이나 SAS 연결 문자열을 사용할 수 있습니다. SAS 연결 문자열을 사용하는 경우 가까운 미래에 만료되도록 설정해서는 안 됩니다.

Azure 데이터 레이크 스토리지 Gen2

Azure Data Lake를 포함하는 동기화 관계를 만들 때는 저장소 계정 연결 문자열을 사용하여 Copy and Sync를 제공해야 합니다. SAS(공유 액세스 서명)가 아닌 일반 연결 문자열이어야 합니다.

Azure NetApp Files 요구 사항

Azure NetApp Files 에서 데이터를 동기화할 때는 Premium 또는 Ultra 서비스 수준을 사용합니다. 디스크 서비스 수준이 표준인 경우 오류 및 성능 문제가 발생할 수 있습니다.

적절한 서비스 수준을 결정하는 데 도움이 필요하면 솔루션 아키텍트에게 문의하세요. 볼륨 크기와 볼륨 계층은 얻을 수 있는 처리량을 결정합니다.

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

상자 요구 사항

- Box를 포함하는 동기화 관계를 만들려면 다음 자격 증명을 제공해야 합니다.
  - 클라이언트 ID
  - 클라이언트 비밀번호
  - 개인 키
  - 공개 키 ID
  - 암호문구
  - 엔터프라이즈 ID
- Amazon S3에서 Box로 동기화 관계를 생성하는 경우 다음 설정이 1로 설정된 통합 구성을 갖는 데이터 브로커 그룹을 사용해야 합니다.
  - 스캐너 동시성
  - 스캐너 프로세스 제한
  - 전송자 동시성
  - 전송자 프로세스 제한

  "데이터 브로커 그룹에 대한 통합 구성을 정의하는 방법을 알아보세요." .

Google Cloud Storage 버킷 요구 사항

Google Cloud Storage 버킷이 다음 요구 사항을 충족하는지 확인하세요.

Google Cloud Storage에 지원되는 데이터 브로커 위치

Google Cloud Storage를 포함하는 동기화 관계에는 Google Cloud 또는 사내에 배포된 데이터 브로커가 필요합니다. 복사 및 동기화는 동기화 관계를 생성할 때 데이터 브로커 설치 프로세스를 안내합니다.

- "Google Cloud 데이터 브로커를 배포하는 방법을 알아보세요"
- "Linux 호스트에 데이터 브로커를 설치하는 방법을 알아보세요"

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 버킷에서 선택할 수 있습니다. "서비스 계정을 설정하는 방법을 알아보세요" .

SnapMirror 대상에 대한 권한

동기화 관계의 소스가 SnapMirror 대상(읽기 전용)인 경우 "읽기/나열" 권한만으로도 소스에서 대상으로 데이터를 동기화할 수 있습니다.

Google Cloud 버킷 암호화

고객 관리 KMS 키 또는 기본 Google 관리 키를 사용하여 대상 Google Cloud 버킷을 암호화할 수 있습니다. 버킷에 이미 KMS 암호화가 추가된 경우 기본 Google 관리 암호화가 재정의됩니다.

고객 관리 KMS 키를 추가하려면 데이터 브로커를 사용해야 합니다. "올바른 권한" , 키는 버킷과 같은 지역에 있어야 합니다.

구글 드라이브

Google Drive를 포함하는 동기화 관계를 설정하는 경우 다음을 제공해야 합니다.

- 데이터를 동기화하려는 Google Drive 위치에 액세스할 수 있는 사용자의 이메일 주소
- Google Drive에 액세스할 수 있는 권한이 있는 Google Cloud 서비스 계정의 이메일 주소
- 서비스 계정의 개인 키

서비스 계정을 설정하려면 Google 문서의 지침을 따르세요.

- "서비스 계정 및 자격 증명을 만듭니다."
- "도메인 전체 권한을 서비스 계정에 위임합니다."

OAuth 범위 필드를 편집할 때 다음 범위를 입력하세요.

- \ https://www.googleapis.com/auth/drive
- \ https://www.googleapis.com/auth/drive.file

NFS 서버 요구 사항

- NFS 서버는 NetApp 시스템이거나 NetApp 아닌 시스템일 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, 4.2가 지원됩니다.

  원하는 버전을 서버에서 활성화해야 합니다.

- ONTAP 시스템에서 NFS 데이터를 동기화하려면 SVM에 대한 NFS 내보내기 목록에 대한 액세스가 활성화되어

있는지 확인하세요(vserver nfs modify -vserver *svm_name* -showmount enabled).

ONTAP 9.2부터 showmount의 기본 설정은 _enabled_입니다.

ONTAP 요구 사항

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

ONTAP S3 스토리지 요구 사항

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

- ONTAP S3에 연결된 LIF의 IP 주소
- ONTAP 이 사용하도록 구성된 액세스 키와 비밀 키

SMB 서버 요구 사항

- SMB 서버는 NetApp 시스템이거나 NetApp 아닌 시스템일 수 있습니다.
- SMB 서버에 대한 권한이 있는 자격 증명을 복사 및 동기화에 제공해야 합니다.
  - 소스 SMB 서버의 경우 다음 권한이 필요합니다: 나열 및 읽기.

    백업 운영자 그룹의 구성원은 소스 SMB 서버를 통해 지원을 받습니다.

  - 대상 SMB 서버에는 다음 권한이 필요합니다: 나열, 읽기, 쓰기.
- 파일 서버는 데이터 브로커 호스트가 필요한 포트를 통해 내보내기에 액세스할 수 있도록 허용해야 합니다.
  - 139 TCP
  - 445 TCP
  - 137-138 UDP
- SMB 버전 1.0, 2.0, 2.1, 3.0 및 3.11이 지원됩니다.
- "관리자" 그룹에 소스 및 대상 폴더에 대한 "전체 제어" 권한을 부여합니다.

  이 권한을 부여하지 않으면 데이터 브로커가 파일이나 디렉토리에 대한 ACL을 가져올 수 있는 충분한 권한이 없을 수 있습니다. 이런 경우 다음 오류가 발생합니다. "getxattr error 95"

숨겨진 디렉토리 및 파일에 대한 **SMB** 제한

SMB 제한은 SMB 서버 간에 데이터를 동기화할 때 숨겨진 디렉터리와 파일에 영향을 미칩니다. 원본 SMB 서버에 있는 디렉토리나 파일 중 하나가 Windows를 통해 숨겨진 경우, 숨김 속성은 대상 SMB 서버로 복사되지 않습니다.

대소문자 구분 제한으로 인한 **SMB** 동기화 동작

SMB 프로토콜은 대소문자를 구분하지 않으므로 대문자와 소문자가 동일하게 처리됩니다. 동기화 관계에 SMB 서버가 포함되어 있고 데이터가 이미 대상에 있는 경우, 이러한 동작으로 인해 파일 덮어쓰기 및 디렉터리 복사 오류가 발생할 수 있습니다.

예를 들어, 소스에 "a"라는 파일이 있고, 대상에 "A"라는 파일이 있다고 가정해 보겠습니다. 복사 및 동기화를 통해 "a"라는 파일을 대상에 복사하면, 파일 "A"는 소스의 파일 "a"로 덮어쓰여집니다.

디렉토리의 경우 소스에 "b"라는 디렉토리가 있고, 타겟에 "B"라는 디렉토리가 있다고 가정해 보겠습니다. Copy and Sync가 "b"라는 디렉토리를 대상에 복사하려고 하면, Copy and Sync는 해당 디렉토리가 이미 존재한다는 오류를 수신합니다. 결과적으로 Copy and Sync는 항상 "b"라는 디렉토리를 복사하는 데 실패합니다.

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

NetApp Copy and Sync 대한 네트워킹 개요

NetApp Copy and Sync 위한 네트워킹에는 데이터 브로커 그룹과 소스 및 대상 위치 간의 연결, 그리고 포트 443을 통한 데이터 브로커의 아웃바운드 인터넷 연결이 포함됩니다.

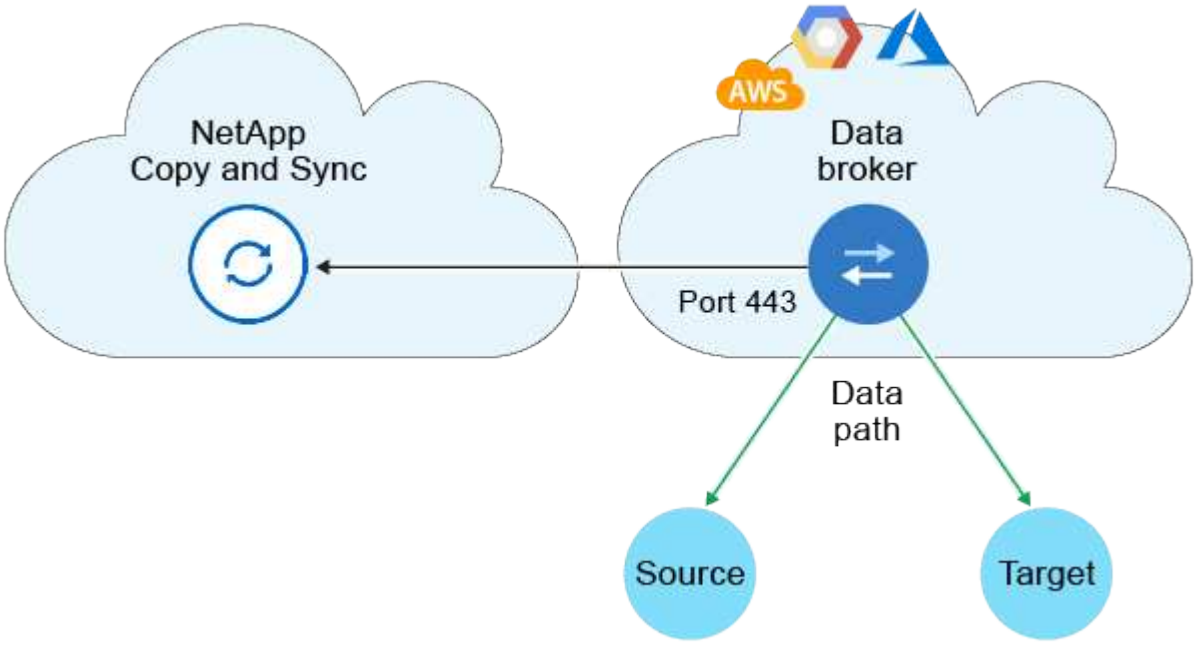
데이터 브로커 위치

데이터 브로커 그룹은 클라우드나 회사 내부에 설치된 하나 이상의 데이터 브로커로 구성됩니다.

클라우드의 데이터 브로커

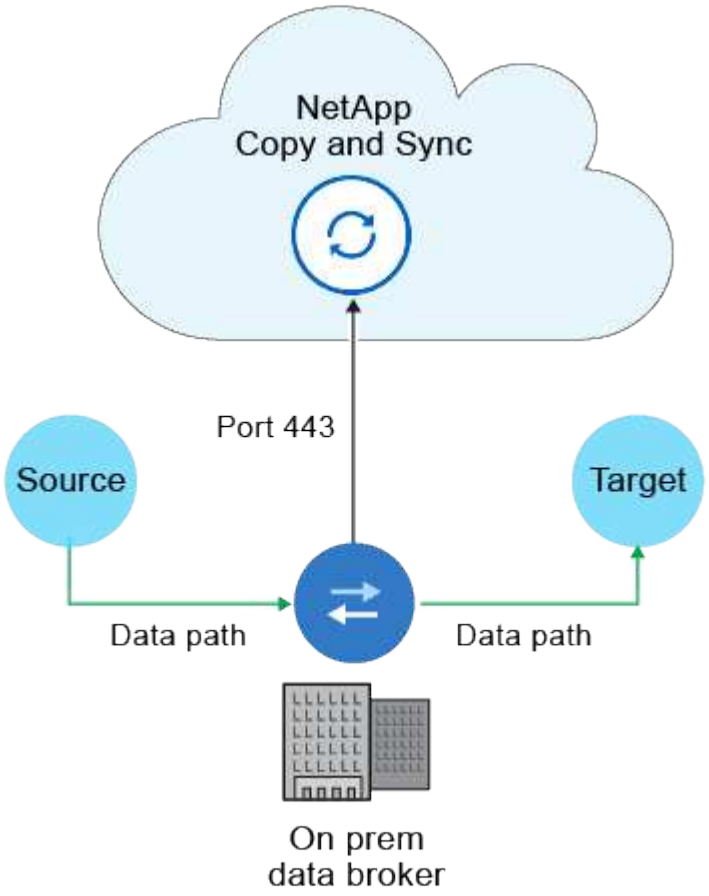
다음 이미지는 AWS, Google Cloud 또는 Azure의 클라우드에서 실행되는 데이터 브로커를 보여줍니다. 데이터 브로커에 연결되어 있는 한 소스와 타겟은 어느 위치에나 있을 수 있습니다. 예를 들어, 데이터 센터에서 클라우드 제공업체로 VPN 연결이 있을 수 있습니다.

Copy and Sync가 AWS, Azure 또는 Google Cloud에 데이터 브로커를 배포하는 경우, 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.



귀사 구내의 데이터 브로커

다음 이미지는 데이터 센터에서 온프레미스로 실행되는 데이터 브로커를 보여줍니다. 다시 말해, 소스와 타겟은 데이터 브로커에 연결되어 있는 한 어느 위치에나 있을 수 있습니다.



네트워킹 요구 사항

- 소스와 대상은 데이터 브로커 그룹에 네트워크로 연결되어 있어야 합니다.

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

- 데이터 브로커는 포트 443을 통해 복사 및 동기화 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.
- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

네트워킹 엔드포인트

NetApp 데이터 브로커는 Copy and Sync와 통신하고 몇몇 다른 서비스와 저장소에 접속하기 위해 포트 443을 통한 아웃바운드 인터넷 액세스가 필요합니다. 특정 작업을 수행하려면 로컬 웹 브라우저에서도 엔드포인트에 액세스해야 합니다. 아웃바운드 연결을 제한해야 하는 경우 아웃바운드 트래픽에 대한 방화벽을 구성할 때 다음 엔드포인트 목록을 참조하세요.

데이터 브로커 엔드포인트

데이터 브로커는 다음 엔드포인트에 접속합니다.

엔드포인트	목적
\ https://olcentgbl.trafficmanager.net	데이터 브로커 호스트에 대한 CentOS 패키지를 업데이트하기 위해 저장소에 문의합니다. 이 엔드포인트는 CentOS 호스트에 데이터 브로커를 수동으로 설치하는 경우에만 접속됩니다.
\ https://rpm.nodesource.com \ https://registry.npmjs.org \ https://nodejs.org:	개발에 사용되는 Node.js, npm 및 기타 타사 패키지를 업데이트하기 위해 저장소에 문의합니다.
\ https://tgz.pm2.io	복사 및 동기화를 모니터링하는 데 사용되는 타사 패키지인 PM2를 업데이트하기 위한 저장소에 액세스합니다.
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	Copy and Sync가 작업(파일 대기, 작업 등록, 데이터 브로커에 업데이트 전달)에 사용하는 AWS 서비스에 문의합니다.
\ https://s3.*region*.amazonaws.com 예: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["S3 엔드포인트 목록은 AWS 설명서를 참조하세요."^]	동기화 관계에 S3 버킷이 포함된 경우 Amazon S3에 연락합니다.
\ https://s3.amazonaws.com/	Copy and Sync에서 데이터 브로커 로그를 다운로드하면 데이터 브로커가 로그 디렉토리를 압축하고 해당 로그를 us-east-1 지역의 미리 정의된 S3 버킷에 업로드합니다.
\ https://storage.googleapis.com/	동기화 관계에서 GCP 버킷을 사용하는 경우 Google Cloud에 문의합니다.
https://storage-account.blob.core.windows.netAzure Data Lake Gen2를 사용하는 경우:https://storage-account.dfs.core.windows.net[] 여기서 _storage-account_는 사용자의 소스 저장소 계정입니다.	사용자의 Azure 스토리지 계정 주소에 대한 프록시를 엽니다.
\ https://cf.cloudsync.netapp.com \ https://repo.cloudsync.netapp.com	Copy and Sync에 문의하세요.
\ https://support.netapp.com	동기화 관계에 BYOL 라이선스를 사용하는 경우 NetApp 지원팀에 문의하세요.
\ https://fedoraproject.org	설치 및 업데이트 중에 데이터 브로커 가상 머신에 7z를 설치합니다. NetApp 기술 지원팀에 AutoSupport 메시지를 보내려면 7z가 필요합니다.
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	데이터 브로커가 AWS에 배포되거나 사내에 배포되고 AWS 자격 증명이 제공되는 경우 AWS 자격 증명을 확인합니다. 데이터 브로커는 배포 중, 업데이트 시, 재시작 시 이 엔드포인트에 접속합니다.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com	새로운 동기화 관계에 대한 소스 파일을 선택하기 위해 분류를 사용하는 경우 NetApp Data Classification 문의하세요.
\ https://pubsub.googleapis.com	Google 스토리지 계정에서 지속적인 동기화 관계를 만드는 경우.

엔드포인트	목적
https://storage-account.queue.core.windows.net\ https://management.azure.com/subscriptions/ ${subscriptionId} /resourceGroups/${resourceGroup}/providers/Microsoft.EventGrid/* 여기서 _storage-account_는 사용자의 원본 저장소 계정이고, _subscriptionid_는 원본 구독 ID이고, _resourceGroup_은 원본 리소스 그룹입니다.	Azure Storage 계정에서 지속적인 동기화 관계를 만드는 경우.

웹 브라우저 엔드포인트

문제 해결을 위해 로그를 다운로드하려면 웹 브라우저가 다음 엔드포인트에 액세스해야 합니다.

logs.cloudsync.netapp.com:443

NetApp Copy and Sync 에 로그인하세요

NetApp Console 사용하여 NetApp Copy and Sync 에 로그인합니다.

콘솔에 로그인하려면 NetApp 지원 사이트 자격 증명을 사용하거나 이메일과 비밀번호를 사용하여 NetApp 클라우드 로그인에 가입할 수 있습니다. "로그인에 대해 자세히 알아보세요" .

NetApp Copy and Sync ID 액세스 관리를 사용하여 각 사용자가 특정 작업에 대해 갖는 액세스 권한을 관리합니다.

필수 **NetApp Console** 역할 조직 관리자 역할. "NetApp Console 액세스 역할에 대해 알아보세요" .

단계

1. 웹 브라우저를 열고 이동하세요 "NetApp Console" .

   NetApp Console 로그인 페이지가 나타납니다.

2. 콘솔에 로그인합니다.
3. 콘솔 왼쪽 탐색에서 모바일 > *복사 및 동기화*를 선택합니다.

데이터 브로커 설치

NetApp Copy and Sync 위해 **AWS**에서 새로운 데이터 브로커 만들기

NetApp Copy and Sync 대한 새로운 데이터 브로커 그룹을 생성할 때 VPC의 새 EC2 인스턴스에 데이터 브로커 소프트웨어를 배포하려면 Amazon Web Services를 선택하세요.

NetApp Copy and Sync 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

클라우드나 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치하는 옵션도 있습니다. "자세히 알아보기" .

지원되는 **AWS** 지역

중국 지역을 제외한 모든 지역이 지원됩니다.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 복사 및 동기화 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Copy and Sync가 AWS에 데이터 브로커를 배포하면 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다. 설치 과정에서 프록시 서버를 사용하도록 데이터 브로커를 구성할 수 있습니다.

  아웃바운드 연결을 제한해야 하는 경우 다음을 참조하세요."데이터 브로커가 연락하는 엔드포인트 목록" .

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

AWS에 데이터 브로커를 배포하는 데 필요한 권한

데이터 브로커를 배포하는 데 사용하는 AWS 사용자 계정에는 다음에 포함된 권한이 있어야 합니다. "이 NetApp 제공 정책" .

AWS 데이터 브로커에서 자체 **IAM** 역할을 사용하기 위한 요구 사항

Copy and Sync가 데이터 브로커를 배포하면 데이터 브로커 인스턴스에 대한 IAM 역할이 생성됩니다. 원하는 경우 사용자 고유의 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.

- EC2 서비스는 신뢰할 수 있는 엔터티로서 IAM 역할을 맡을 수 있어야 합니다.
- "이 JSON 파일에 정의된 권한"데이터 브로커가 제대로 작동하려면 IAM 역할에 연결되어야 합니다.

데이터 브로커를 배포할 때 IAM 역할을 지정하려면 아래 단계를 따르세요.

데이터 브로커 생성

새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 생성할 때 AWS에 데이터 브로커를 설치하는 방법을 설명합니다.

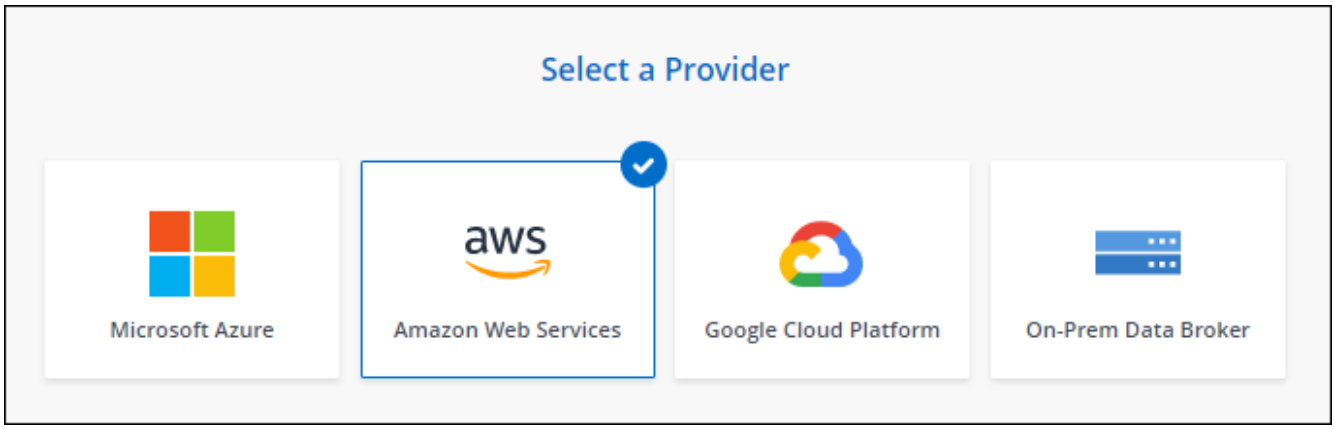
단계

1. "복사 및 동기화에 로그인하세요" .

2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *Amazon Web Services*를 선택합니다.



5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.
6. AWS 액세스 키를 입력하면 Copy and Sync가 사용자를 대신하여 AWS에서 데이터 브로커를 생성할 수 있습니다.

   키는 저장되지 않으며 다른 목적으로 사용되지 않습니다.

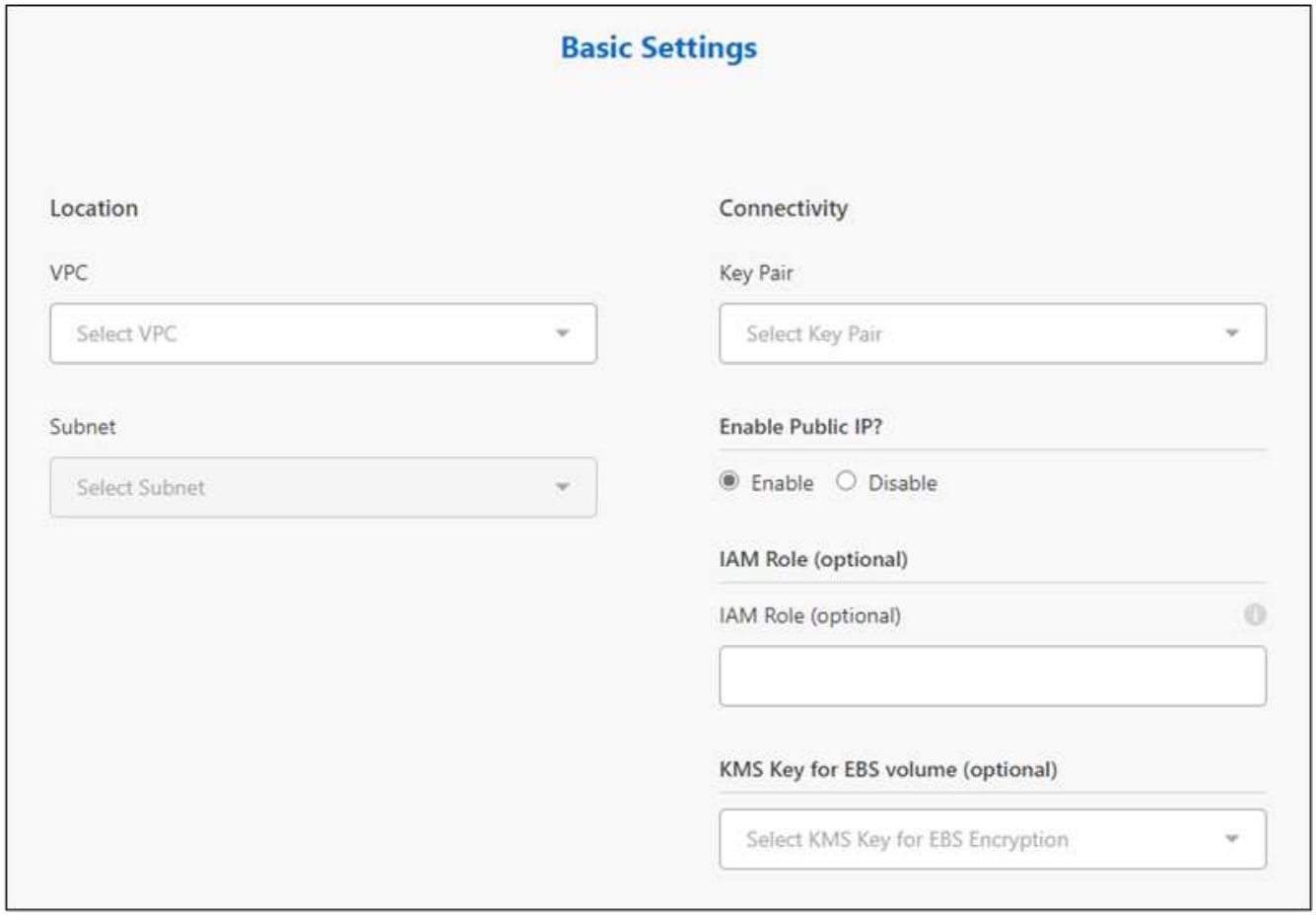
   액세스 키를 제공하지 않으려면 페이지 하단의 링크를 선택하여 대신 CloudFormation 템플릿을 사용하세요. 이 옵션을 사용하면 AWS에 직접 로그인하므로 자격 증명을 제공할 필요가 없습니다.

   다음 비디오는 CloudFormation 템플릿을 사용하여 데이터 브로커 인스턴스를 시작하는 방법을 보여줍니다.

   AWS CloudFormation 템플릿에서 데이터 브로커 시작

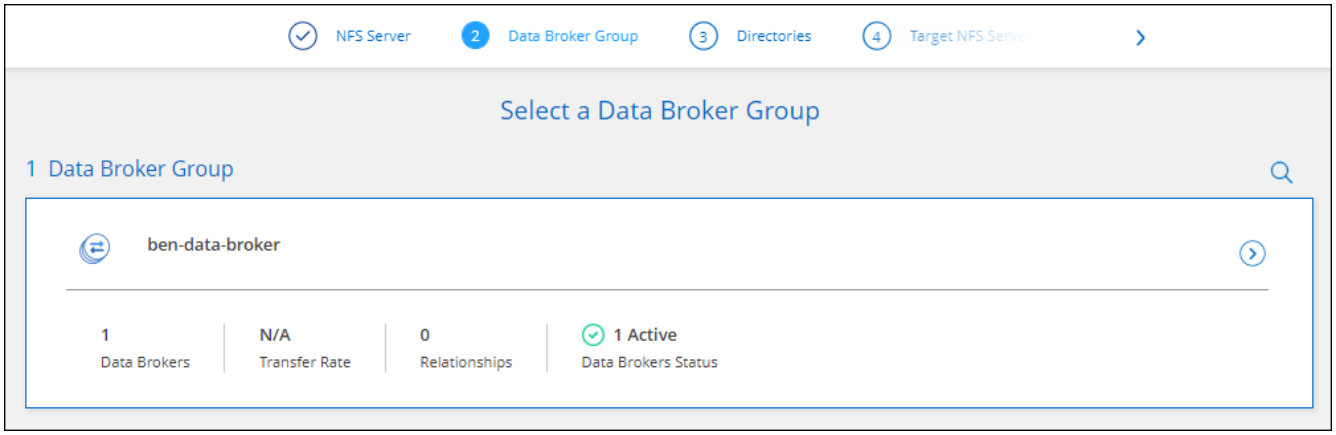
7. AWS 액세스 키를 입력한 경우 인스턴스의 위치를 선택하고, 키 쌍을 선택하고, 공용 IP 주소를 활성화할지 여부를 선택하고, 기존 IAM 역할을 선택하거나, 필드를 비워 두면 복사 및 동기화가 해당 역할을 자동으로 생성합니다. KMS 키를 사용하여 데이터 브로커를 암호화하는 옵션도 있습니다.

   자신의 IAM 역할을 선택하는 경우필요한 권한을 제공해야 합니다. .



8. VPC에서 인터넷 접속에 프록시가 필요한 경우 프록시 구성을 지정합니다.
9. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.

   다음 이미지는 AWS에 성공적으로 배포된 인스턴스를 보여줍니다.



10. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.

결과

AWS에 데이터 브로커를 배포하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브로커 그룹을 추가 동기화 관계와 함께 사용할 수 있습니다.

데이터 브로커 인스턴스에 대한 세부 정보

Copy and Sync는 다음 구성을 사용하여 AWS에서 데이터 브로커를 생성합니다.

Node.js 호환성
: v21.2.0

인스턴스 유형
: 해당 지역에서 사용 가능한 경우 m5n.xlarge, 그렇지 않은 경우 m5.xlarge

vCPU
: 4

숫양
: 16GB

운영 체제
: 아마존 리눅스 2023

디스크 크기 및 유형
: 10GB GP2 SSD

NetApp Copy and Sync 위해 Azure에서 새 데이터 브로커 만들기

NetApp Copy and Sync 대한 새 데이터 브로커 그룹을 만들 때 VNet의 새 가상 머신에 데이터 브로커 소프트웨어를 배포하려면 Microsoft Azure를 선택하세요. NetApp Copy and Sync 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

클라우드나 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치하는 옵션도 있습니다. "자세히 알아보기" .

지원되는 **Azure** 지역

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

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 Copy and Sync 서비스에 대한 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Copy and Sync가 Azure에 데이터 브로커를 배포하면 필요한 아웃바운드 통신을 활성화하는 보안 그룹을 만듭니다.

  아웃바운드 연결을 제한해야 하는 경우 다음을 참조하세요."데이터 브로커가 연락하는 엔드포인트 목록" .

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

Azure에서 데이터 브로커를 배포하는 데 필요한 권한

데이터 브로커를 배포하는 데 사용하는 Azure 사용자 계정에 다음 권한이 있는지 확인하세요.

```
{
    "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",
                    "Microsoft.Storage/storageAccounts/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/write",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/delete",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action",
                    "Microsoft.EventGrid/systemTopics/read",
                    "Microsoft.EventGrid/systemTopics/write",
                    "Microsoft.EventGrid/systemTopics/delete",
                    "Microsoft.EventGrid/eventSubscriptions/write",
                    "Microsoft.Storage/storageAccounts/write"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write"

"Microsoft.Network/networkSecurityGroups/securityRules/read",
                    "Microsoft.Network/networkSecurityGroups/read",
```

```
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}
```

메모:

1. 다음 권한은 다음을 활성화하려는 경우에만 필요합니다. "연속 동기화 설정" Azure에서 다른 클라우드 저장소 위치로의 동기화 관계에 대해:
    - 'Microsoft.Storage/storageAccounts/read',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',

- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/삭제',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action',
- 'Microsoft.EventGrid/systemTopics/read',
- 'Microsoft.EventGrid/systemTopics/write',
- 'Microsoft.EventGrid/systemTopics/삭제',
- 'Microsoft.EventGrid/eventSubscriptions/write',
- 'Microsoft.Storage/storageAccounts/write'

또한 Azure에서 Continuous Sync를 구현하려는 경우 할당 가능한 범위를 리소스 그룹 범위가 아닌 구독 범위로 설정해야 합니다.

2. 다음 권한은 데이터 브로커 생성에 대한 보안을 직접 선택하려는 경우에만 필요합니다.
   - "Microsoft.Network/networkSecurityGroups/securityRules/read"
   - "Microsoft.Network/networkSecurityGroups/read"

인증 방법

데이터 브로커를 배포할 때 가상 머신에 대한 인증 방법(암호 또는 SSH 공개-개인 키 쌍)을 선택해야 합니다.

키 쌍 생성에 대한 도움말은 다음을 참조하세요. "Azure 설명서: Azure에서 Linux VM에 대한 SSH 공개-개인 키 쌍 만들기 및 사용" .

데이터 브로커 생성

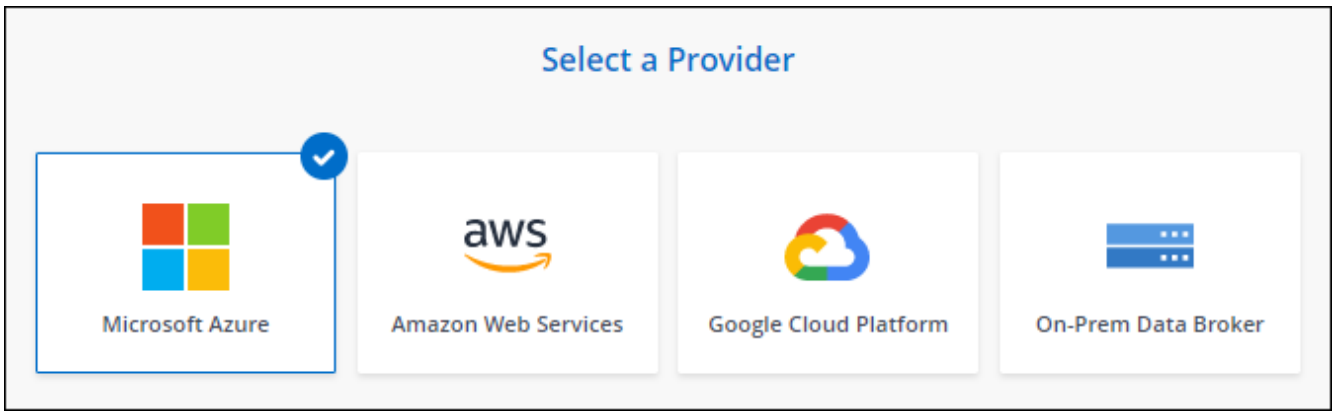
새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 만들 때 Azure에 데이터 브로커를 설치하는 방법을 설명합니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

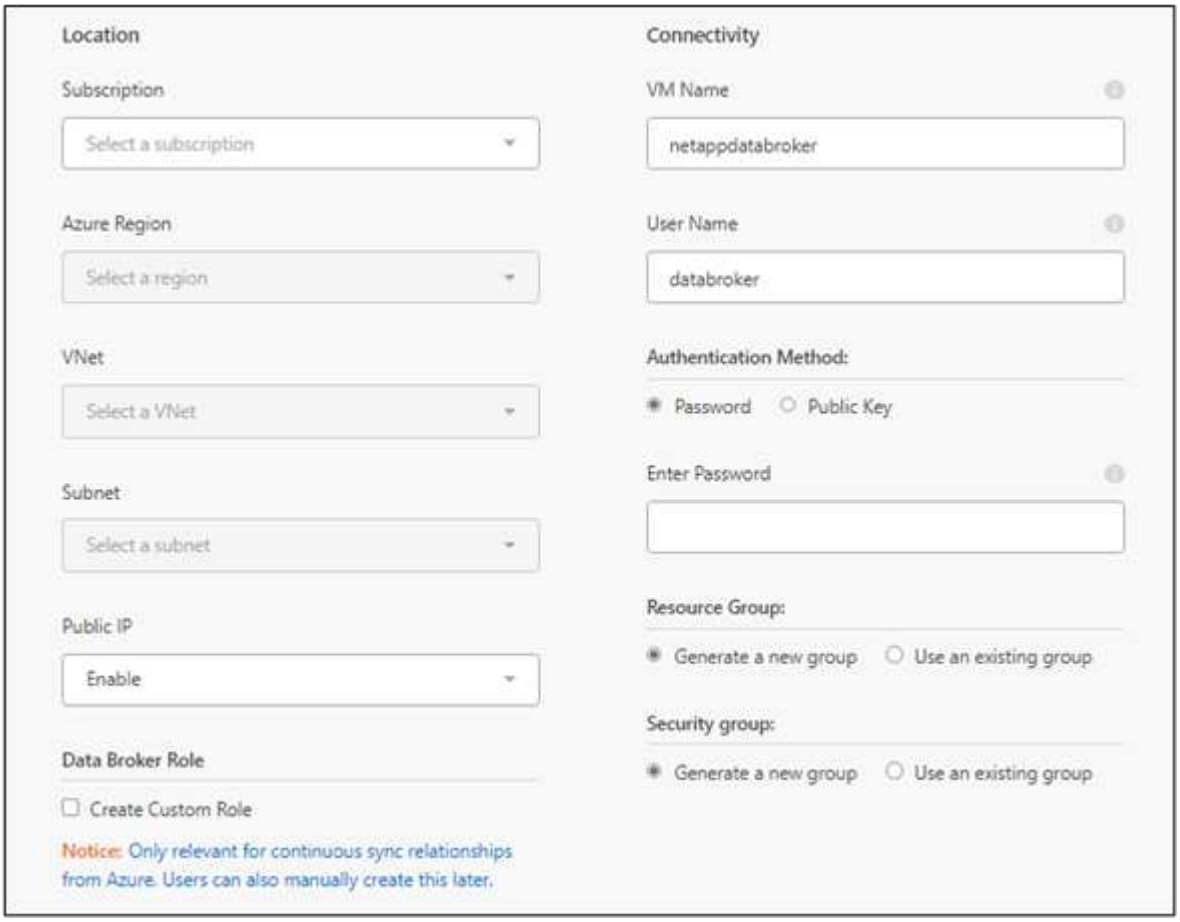
4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *Microsoft Azure*를 선택합니다.



5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.
6. 메시지가 표시되면 Microsoft 계정에 로그인하세요. 메시지가 표시되지 않으면 *Azure에 로그인*을 선택하세요.

   이 양식은 Microsoft에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

7. 데이터 브로커의 위치를 선택하고 가상 머신에 대한 기본 세부 정보를 입력합니다.



지속적인 동기화 관계를 구현하려면 데이터 브로커에 사용자 지정 역할을 할당해야 합니다. 이 작업은 브로커가 생성된 후 수동으로 수행할 수도 있습니다.

8. VNet에서 인터넷 접속에 프록시가 필요한 경우 프록시 구성을 지정합니다.
9. *계속*을 선택하세요. 데이터 브로커에 S3 권한을 추가하려면 AWS 액세스 키와 비밀 키를 입력하세요.

10. *계속*을 선택하고 배포가 완료될 때까지 페이지를 열어 두세요.

    이 과정은 최대 7분이 걸릴 수 있습니다.

11. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.
12. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.

결과

Azure에 데이터 브로커를 배포하고 새로운 동기화 관계를 만들었습니다. 이 데이터 브로커를 추가 동기화 관계와 함께 사용할 수 있습니다.

관리자 동의가 필요하다는 메시지를 받으셨나요?

Microsoft에서 Copy and Sync가 사용자를 대신하여 조직의 리소스에 액세스하려면 권한이 필요하므로 관리자 승인이 필요하다고 알리는 경우 두 가지 옵션이 있습니다.

1. AD 관리자에게 다음 권한을 부여해 달라고 요청하세요.

   Azure에서 *관리 센터 > Azure AD > 사용자 및 그룹 > 사용자 설정*으로 이동하여 *사용자는 앱이 자신을 대신하여 회사 데이터에 액세스하는 데 동의할 수 있음*을 활성화합니다.

2. 다음 URL을 사용하여 AD 관리자에게 *CloudSync-AzureDataBrokerCreator*에 대한 동의를 요청하세요(이것이 관리자 동의 엔드포인트입니다).

   \ https://login.microsoftonline.com/ {여기에 테넌트 ID를 입력하세요}/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 대로, 앱 URL은 https://cloudsync.netapp.com 이고 애플리케이션 클라이언트 ID는 8ee4ca3a-bafa-4831-97cc-5a38923cab85입니다.

데이터 브로커 **VM**에 대한 세부 정보

복사 및 동기화는 다음 구성을 사용하여 Azure에 데이터 브로커를 만듭니다.

Node.js 호환성
: v21.2.0

VM 유형
: 표준 DS4 v2

vCPU
: 8

숫양
: 28GB

운영 체제

로키 리눅스 9.0

디스크 크기 및 유형

64GB 프리미엄 SSD

Google Cloud에서 NetApp Copy and Sync 위한 새로운 데이터 브로커 만들기

NetApp Copy and Sync 대한 새 데이터 브로커 그룹을 만들 때 Google Cloud Platform을 선택하여 Google Cloud VPC의 새 가상 머신 인스턴스에 데이터 브로커 소프트웨어를 배포합니다. NetApp Copy and Sync 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

클라우드나 사내에 있는 기존 Linux 호스트에 데이터 브로커를 설치하는 옵션도 있습니다. "자세히 알아보기" .

지원되는 **Google Cloud** 지역

모든 지역이 지원됩니다.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- 데이터 브로커는 포트 443을 통해 복사 및 동기화 작업을 폴링할 수 있도록 아웃바운드 인터넷 연결이 필요합니다.

  Copy and Sync가 Google Cloud에 데이터 브로커를 배포하면 필요한 아웃바운드 통신을 지원하는 보안 그룹을 생성합니다.

  아웃바운드 연결을 제한해야 하는 경우 다음을 참조하세요."데이터 브로커가 연락하는 엔드포인트 목록" .

- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

Google Cloud에 데이터 브로커를 배포하는 데 필요한 권한

데이터 브로커를 배포하는 Google Cloud 사용자에게 다음 권한이 있는지 확인하세요.

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

서비스 계정에 필요한 권한

데이터 브로커를 배포할 때 다음 권한이 있는 서비스 계정을 선택해야 합니다.

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update
- iam.serviceAccounts.signJwt
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

참고사항:

1. "iam.serviceAccounts.signJwt" 권한은 외부 HashiCorp 볼트를 사용하도록 데이터 브로커를 설정하려는 경우에만 필요합니다.
2. "pubsub.*" 및 "storage.buckets.update" 권한은 Google Cloud Storage에서 다른 클라우드 스토리지 위치로의 동기화 관계에 대해 지속적인 동기화 설정을 활성화하려는 경우에만 필요합니다. "연속 동기화 옵션에 대해 자세히 알아보세요" .
3. "cloudkms.cryptoKeys.list" 및 "cloudkms.keyRings.list" 권한은 대상 Google Cloud Storage 버킷에서 고객 관리 KMS 키를 사용하려는 경우에만 필요합니다.

데이터 브로커 생성

새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 생성할 때 Google Cloud에 데이터 브로커를 설치하는 방법을 설명합니다.

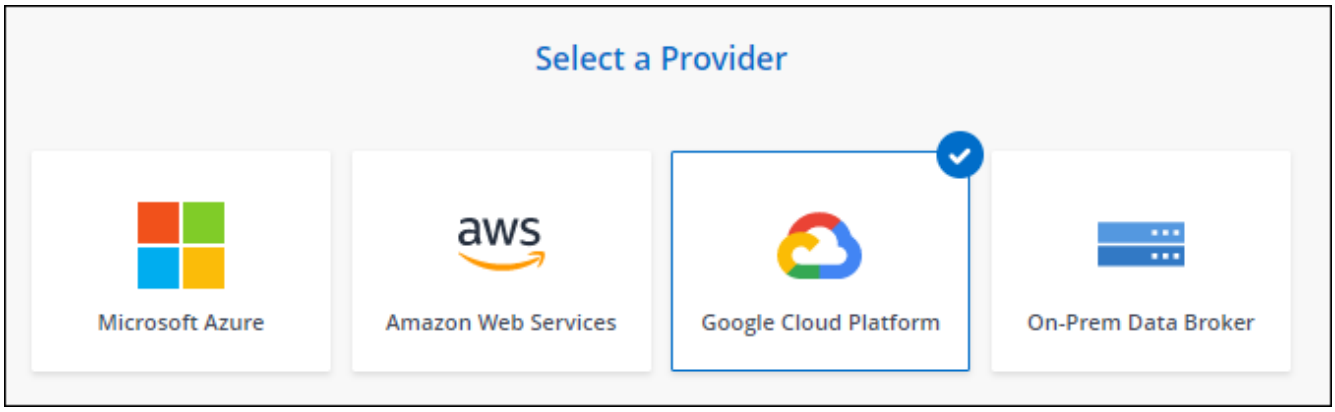
단계

1. "복사 및 동기화에 로그인하세요" .

2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *Google Cloud Platform*을 선택합니다.

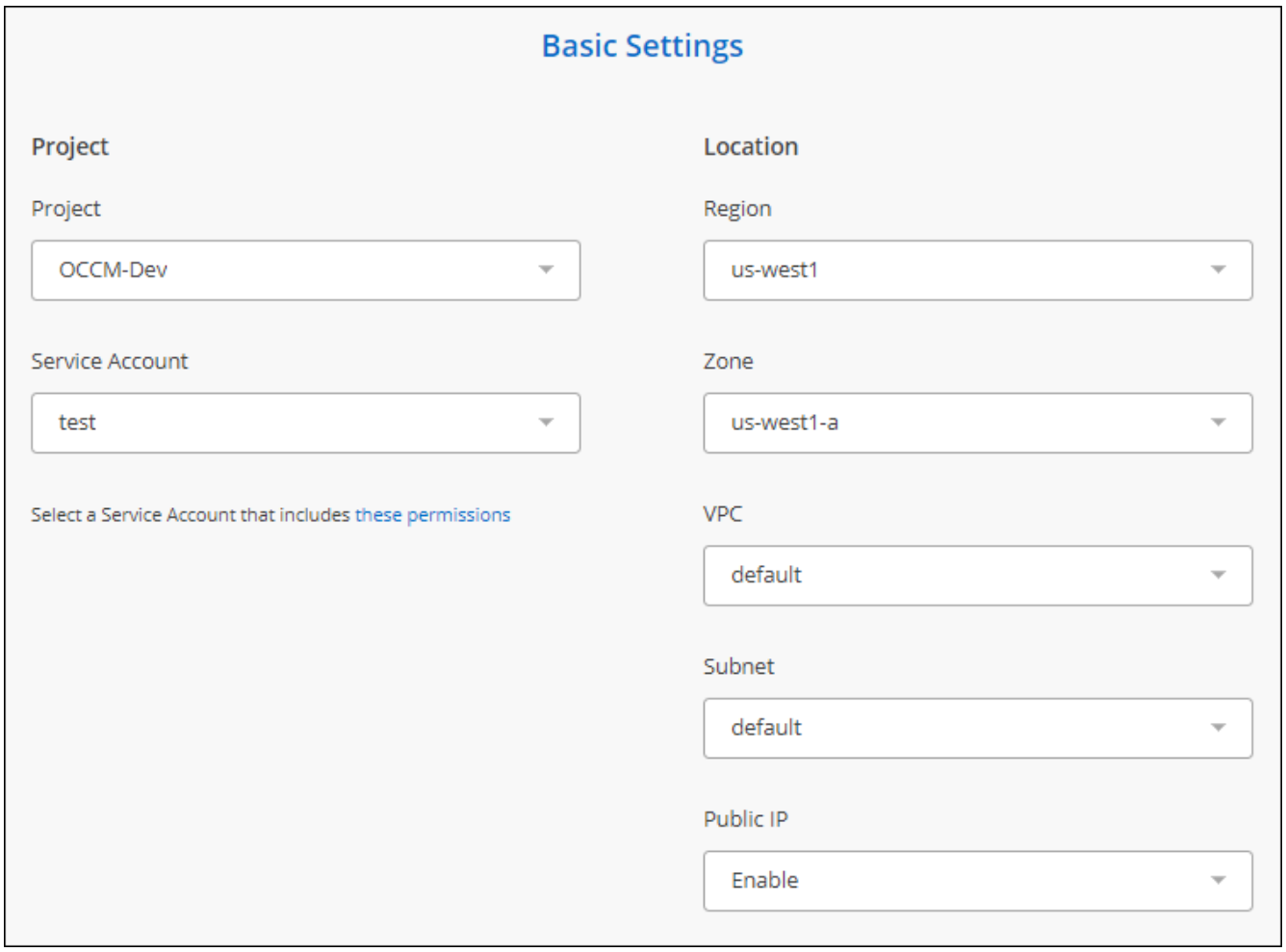


5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.
6. 메시지가 표시되면 Google 계정으로 로그인하세요.

   이 양식은 Google에서 소유하고 호스팅합니다. 귀하의 자격 증명은 NetApp 에 제공되지 않습니다.

7. 프로젝트와 서비스 계정을 선택한 다음, 데이터 브로커의 위치를 선택합니다. 여기에는 공용 IP 주소를 활성화할지 비활성화할지 여부도 포함됩니다.

   공용 IP 주소를 활성화하지 않으면 다음 단계에서 프록시 서버를 정의해야 합니다.



8. VPC에서 인터넷 접속에 프록시가 필요한 경우 프록시 구성을 지정합니다.

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

9. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.

   인스턴스를 배포하는 데 약 5~10분이 걸립니다. 인스턴스를 사용할 수 있게 되면 자동으로 새로 고쳐지는 복사 및 동기화에서 진행 상황을 모니터링할 수 있습니다.

10. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.

결과

Google Cloud에 데이터 브로커를 배포하고 새로운 동기화 관계를 생성했습니다. 이 데이터 브로커를 추가 동기화 관계와 함께 사용할 수 있습니다.

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

동기화 관계를 생성하고 Google Cloud Storage를 소스 또는 대상으로 선택하면 복사 및 동기화를 통해 데이터 브로커의 서비스 계정에서 사용할 수 있는 버킷을 선택할 수 있습니다. 기본적으로 여기에는 데이터 브로커 서비스 계정과 동일한 프로젝트에 있는 버킷이 포함됩니다. 하지만 필요한 권한을 제공하면 다른 프로젝트에서 버킷을 선택할 수 있습니다.

단계

1. Google Cloud Platform 콘솔을 열고 Cloud Storage 서비스를 로드합니다.
2. 동기화 관계에서 소스 또는 대상으로 사용할 버킷의 이름을 선택합니다.
3. *권한*을 선택하세요.
4. *추가*를 선택하세요.
5. 데이터 브로커 서비스 계정의 이름을 입력하세요.
6. 제공하는 역할을 선택하세요위에 표시된 것과 동일한 권한 .
7. *저장*을 선택하세요.

결과

동기화 관계를 설정하면 이제 동기화 관계에서 해당 버킷을 소스 또는 대상으로 선택할 수 있습니다.

데이터 브로커 **VM** 인스턴스에 대한 세부 정보

복사 및 동기화는 다음 구성을 사용하여 Google Cloud에 데이터 브로커를 생성합니다.

Node.js 호환성
: v21.2.0

기계 유형
: n2-표준-4

vCPU
: 4

숫양
: 15GB

운영 체제
: 로키 리눅스 9.0

디스크 크기 및 유형
: 20GB HDD pd-standard

NetApp Copy and Sync 위해 **Linux** 호스트에 데이터 브로커 설치

NetApp Copy and Sync 대한 새 데이터 브로커 그룹을 만들 때 온프레미스 데이터 브로커 옵션을 선택하여 온프레미스 Linux 호스트 또는 클라우드의 기존 Linux 호스트에 데이터 브로커 소프트웨어를 설치합니다. NetApp Copy and Sync 설치 과정을 안내하지만, 설치를 준비하는 데 도움이 되도록 이 페이지에서도 요구 사항과 단계를 반복해서 설명합니다.

Linux 호스트 요구 사항

- **Node.js** 호환성: v21.2.0
- 운영체제:
  - CentOS 8.0 및 8.5

CentOS Stream은 지원되지 않습니다.

- Red Hat Enterprise Linux 8.5, 8.8, 8.9 및 9.4
- 로키 리눅스 9
- Ubuntu Server 20.04 LTS, 23.04 LTS 및 24.04 LTS
- SUSE Linux Enterprise Server 15 SP1

명령 `yum update` 데이터 브로커를 설치하기 전에 호스트에서 실행해야 합니다.

Red Hat Enterprise Linux 시스템은 Red Hat Subscription Management에 등록해야 합니다. 등록되지 않은 경우, 시스템은 설치 중에 필요한 타사 소프트웨어를 업데이트하기 위해 저장소에 접근할 수 없습니다.

- 램: 16GB
- **CPU**: 4코어
- 사용 가능한 디스크 공간: 10GB
- **SELinux**: 호스트에서 SELinux를 비활성화하는 것이 좋습니다.

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

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동 실행됩니다. 데이터 브로커 작업을 위해서는 루트로 실행해야 합니다. 예를 들어, 주식을 마운트하는 것입니다.

네트워킹 요구 사항

- Linux 호스트는 소스와 대상에 연결되어 있어야 합니다.
- 파일 서버는 Linux 호스트가 내보내기에 액세스할 수 있도록 허용해야 합니다.
- AWS로의 아웃바운드 트래픽을 위해서는 Linux 호스트에서 포트 443이 열려 있어야 합니다(데이터 브로커는 Amazon SQS 서비스와 지속적으로 통신합니다).
- NetApp 소스, 대상 및 데이터 브로커를 구성하여 NTP(네트워크 시간 프로토콜) 서비스를 사용할 것을 권장합니다. 세 가지 구성 요소 간의 시간 차이는 5분을 초과해서는 안 됩니다.

AWS에 대한 액세스 활성화

S3 버킷을 포함하는 동기화 관계로 데이터 브로커를 사용하려는 경우 AWS 액세스를 위해 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 프로그래밍 방식 액세스와 특정 권한이 있는 AWS 사용자에 대한 AWS 키를 제공해야 합니다.

단계

1. 다음을 사용하여 IAM 정책을 만듭니다. "이 NetApp 제공 정책"

   "AWS 지침 보기"

2. 프로그래밍 방식 액세스 권한이 있는 IAM 사용자를 만듭니다.

"AWS 지침 보기"

데이터 브로커 소프트웨어를 설치할 때 AWS 키를 지정해야 하므로 반드시 복사하세요.

Google Cloud에 대한 액세스 활성화

Google Cloud Storage 버킷을 포함하는 동기화 관계로 데이터 브로커를 사용하려는 경우 Google Cloud 액세스를 위해 Linux 호스트를 준비해야 합니다. 데이터 브로커를 설치할 때 특정 권한이 있는 서비스 계정에 대한 키를 제공해야 합니다.

단계

1. 아직 스토리지 관리자 권한이 있는 Google Cloud 서비스 계정이 없다면 하나 만드세요.
2. JSON 형식으로 저장된 서비스 계정 키를 만듭니다.

   "Google Cloud 지침 보기"

   파일에는 최소한 "project_id", "private_key" 및 "client_email" 속성이 포함되어야 합니다.

   키를 생성하면 파일이 생성되어 컴퓨터에 다운로드됩니다.

3. JSON 파일을 Linux 호스트에 저장합니다.

Microsoft Azure에 대한 액세스 활성화

Azure에 대한 액세스는 동기화 관계 마법사에서 저장소 계정과 연결 문자열을 제공하여 관계별로 정의됩니다.

데이터 브로커 설치

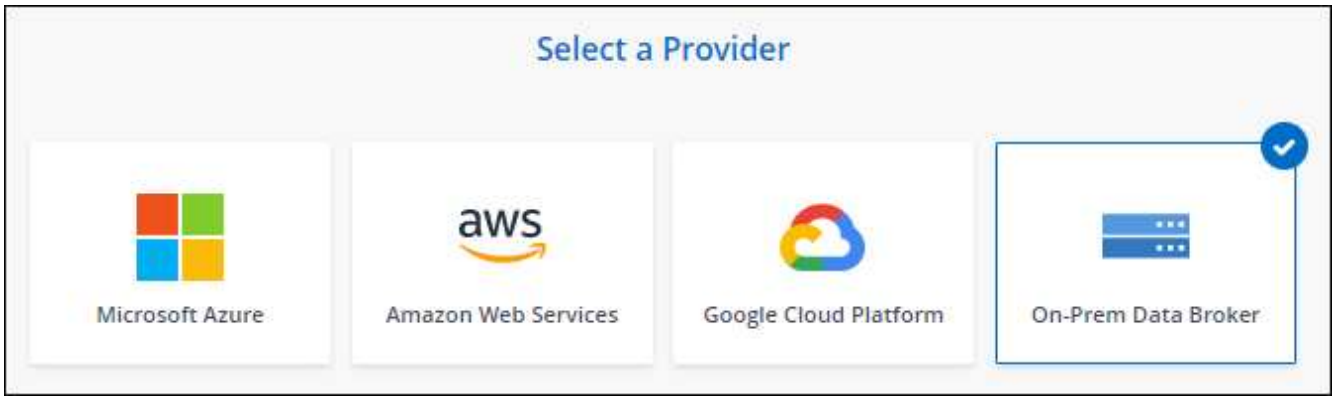
동기화 관계를 만들 때 Linux 호스트에 데이터 브로커를 설치할 수 있습니다.

단계

1. "복사 및 동기화에 로그인하세요" .
2. *새 동기화 만들기*를 선택합니다.
3. 동기화 관계 정의 페이지에서 소스와 대상을 선택하고 *계속*을 선택합니다.

   데이터 브로커 그룹 페이지에 도달할 때까지 단계를 완료하세요.

4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *온프레미스 데이터 브로커*를 선택합니다.



해당 옵션은 *온프레미스 데이터 브로커*로 표시되어 있지만, 이는 사내 또는 클라우드의 Linux 호스트에 적용됩니다.

5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.

   곧 지침 페이지가 로드됩니다. 다음 지침을 따라야 합니다. 이 지침에는 설치 프로그램을 다운로드할 수 있는 고유 링크가 포함되어 있습니다.

6. 지침 페이지에서:

   a. **AWS**, **Google Cloud** 또는 둘 다에 대한 액세스를 활성화할지 선택합니다.

   b. 설치 옵션을 선택하세요: 프록시 없음, 프록시 서버 사용, 인증과 함께 프록시 서버 사용.

      사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.

   c. 명령을 사용하여 데이터 브로커를 다운로드하고 설치합니다.

      다음 단계에서는 가능한 각 설치 옵션에 대한 자세한 내용을 제공합니다. 설치 옵션에 따라 정확한 명령을 얻으려면 지침 페이지를 따르세요.

   d. 설치 프로그램을 다운로드하세요:

      - 프록시 없음:

        ```
        curl <URI> -o data_broker_installer.sh
        ```

      - 프록시 서버 사용:

        ```
        curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
        ```

      - 인증과 함께 프록시 서버를 사용합니다.

        ```
        curl <URI> -o data_broker_installer.sh -x
        <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
        ```

        URI

        복사 및 동기화는 설치 파일의 URI를 지침 페이지에 표시합니다. 이 URI는 온프레미스 데이터 브로커를 배포하기 위한 프롬프트를 따르면 로드됩니다. 해당 URI는 여기서 반복되지 않습니다. 링크는 동적으로 생성되고 한 번만 사용할 수 있기 때문입니다. Copy and Sync에서 URI를 얻으려면 다음 단계를 따르세요. .

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

> 아래 나열된 각 명령에는 AWS 액세스 및 Google Cloud 액세스에 대한 매개변수가 포함되어 있습니다. 설치 옵션에 따라 정확한 명령을 얻으려면 지침 페이지를 따르세요.

- 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>
```

- 인증을 통한 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> -u
<proxy_username> -w <proxy_password>
```

AWS 키

이는 사용자가 준비해야 하는 키입니다.다음 단계를 따르세요 . AWS 키는 온프레미스 또는 클라우드 네트워크에서 실행되는 데이터 브로커에 저장됩니다. NetApp 데이터 브로커 외부의 키를 사용하지 않습니다.

JSON 파일

이것은 당신이 준비해야 할 서비스 계정 키가 포함된 JSON 파일입니다.다음 단계를 따르세요 .

7. 데이터 브로커를 사용할 수 있게 되면 복사 및 동기화에서 *계속*을 선택합니다.
8. 마법사의 페이지를 완료하여 새로운 동기화 관계를 만듭니다.