데이터 브로커 설치

NetApp Copy and Sync

NetApp
November 06, 2025

목차

데이터 브로커 설치

NetApp Copy and Sync 위해 AWS에서 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

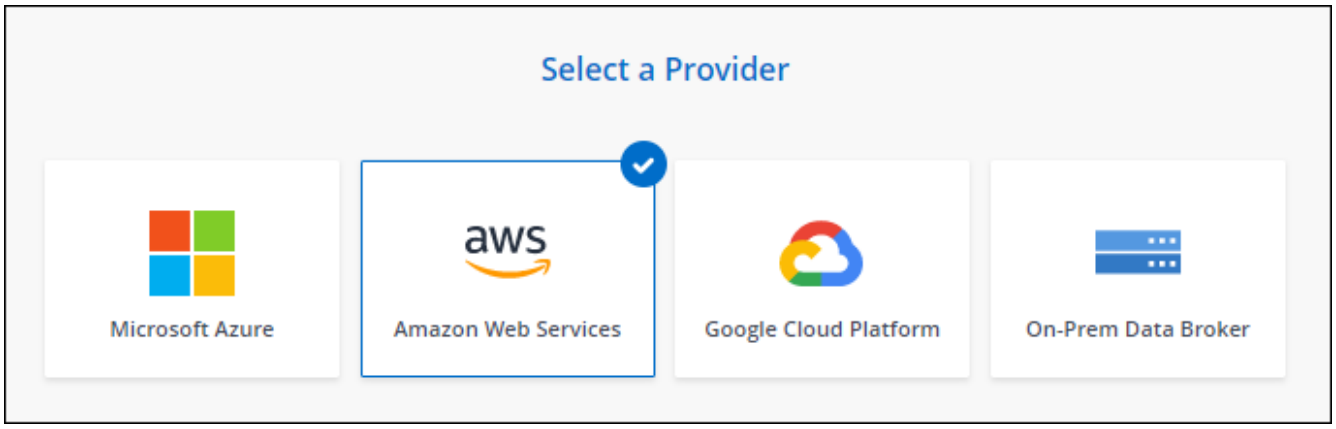
새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 생성할 때 AWS에 데이터 브로커를 설치하는 방법을 설명합니다.

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.

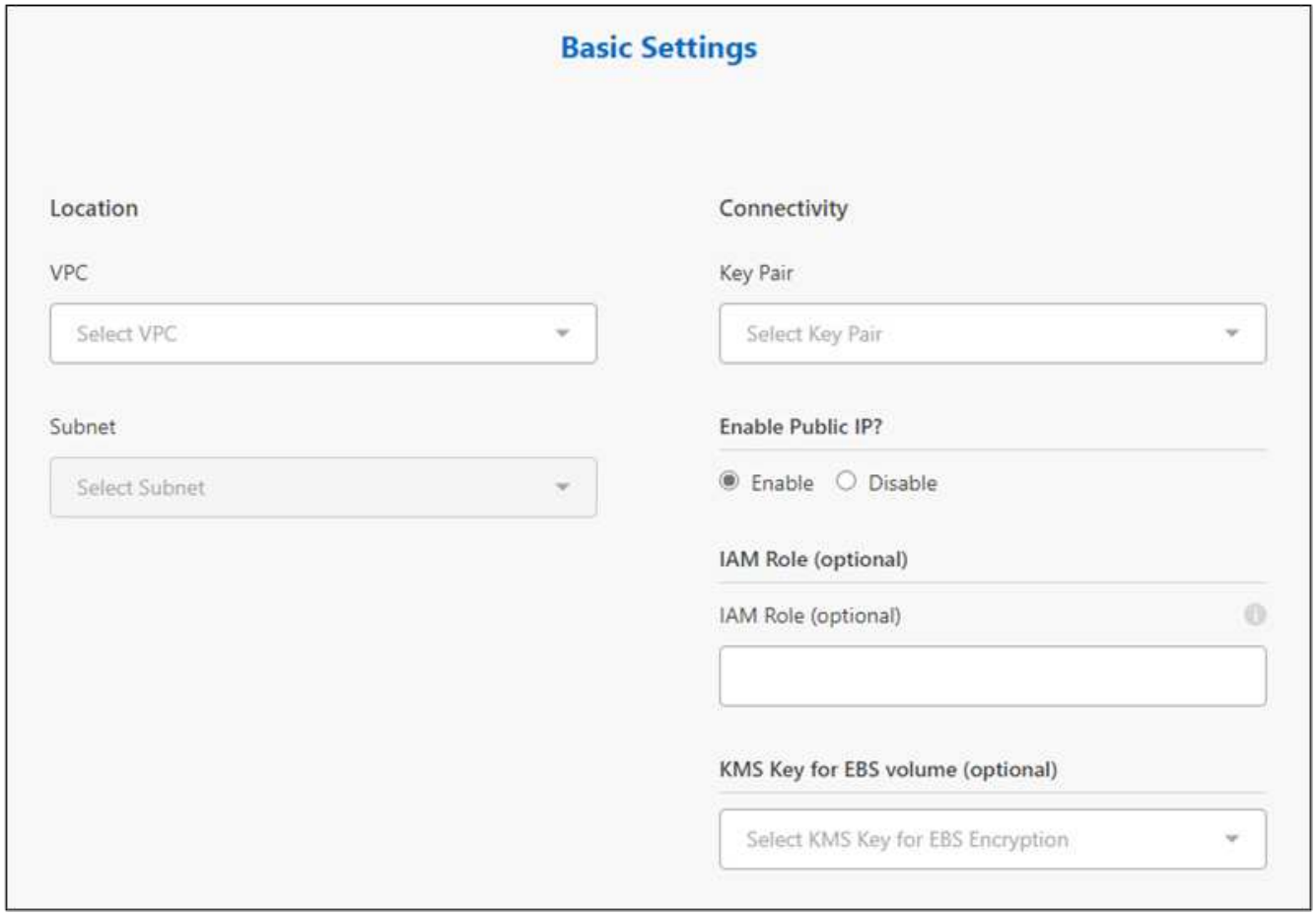
   액세스 키를 제공하지 않으려면 페이지 하단의 링크를 선택하여 대신 CloudFormation 템플릿을 사용하세요. 이 옵션을 사용하면 AWS에 직접 로그인하므로 자격 증명을 제공할 필요가 없습니다.

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

   AWS CloudFormation 템플릿에서 데이터 브로커 시작

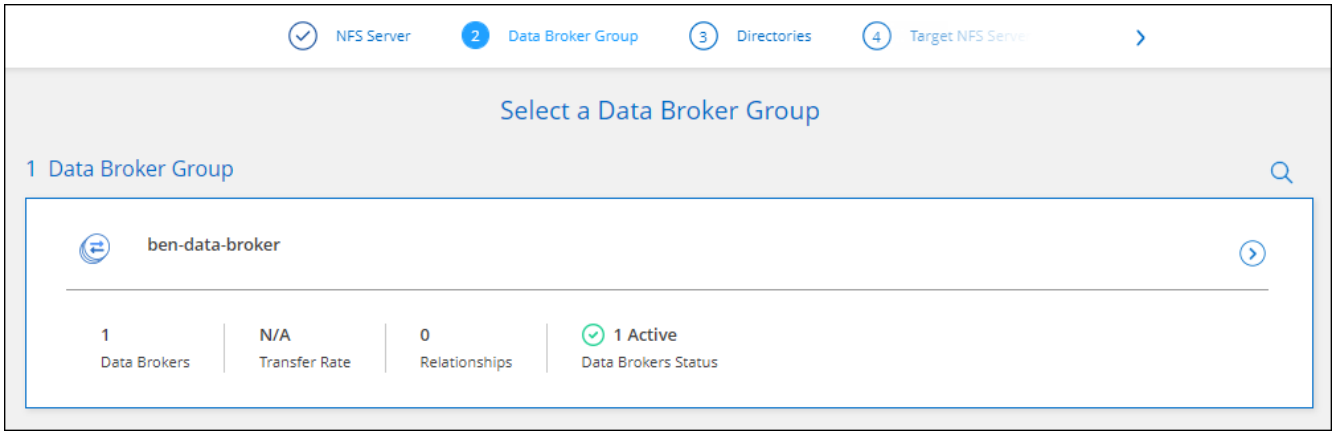
7. AWS 액세스 키를 입력한 경우 인스턴스의 위치를 선택하고, 키 쌍을 선택하고, 공용 IP 주소를 활성화할지 여부를 선택하고, 기존 IAM 역할을 선택하거나, 필드를 비워 두면 복사 및 동기화가 해당 역할을 자동으로 생성합니다. KMS 키를 사용하여 데이터 브로커를 암호화하는 옵션도 있습니다.

   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

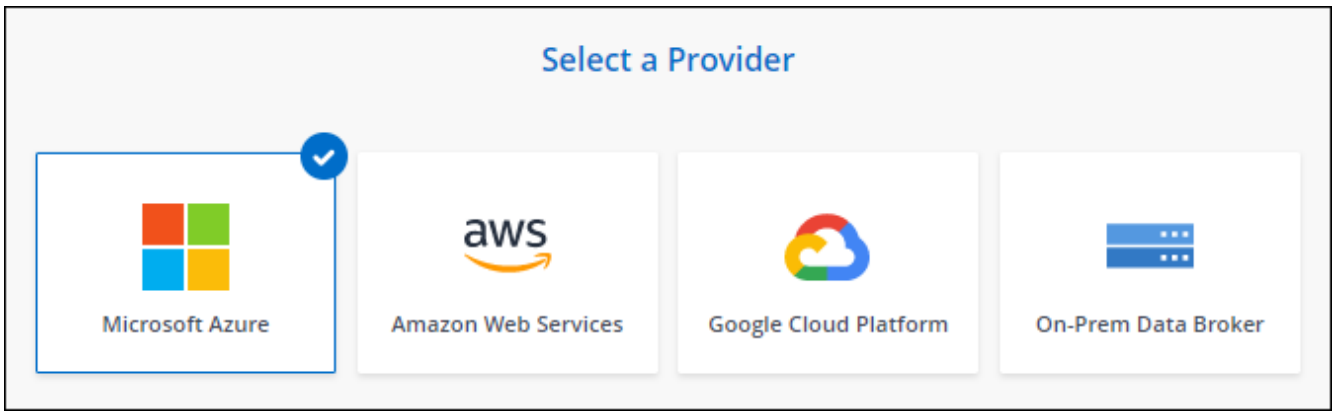
새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 만들 때 Azure에 데이터 브로커를 설치하는 방법을 설명합니다.

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.

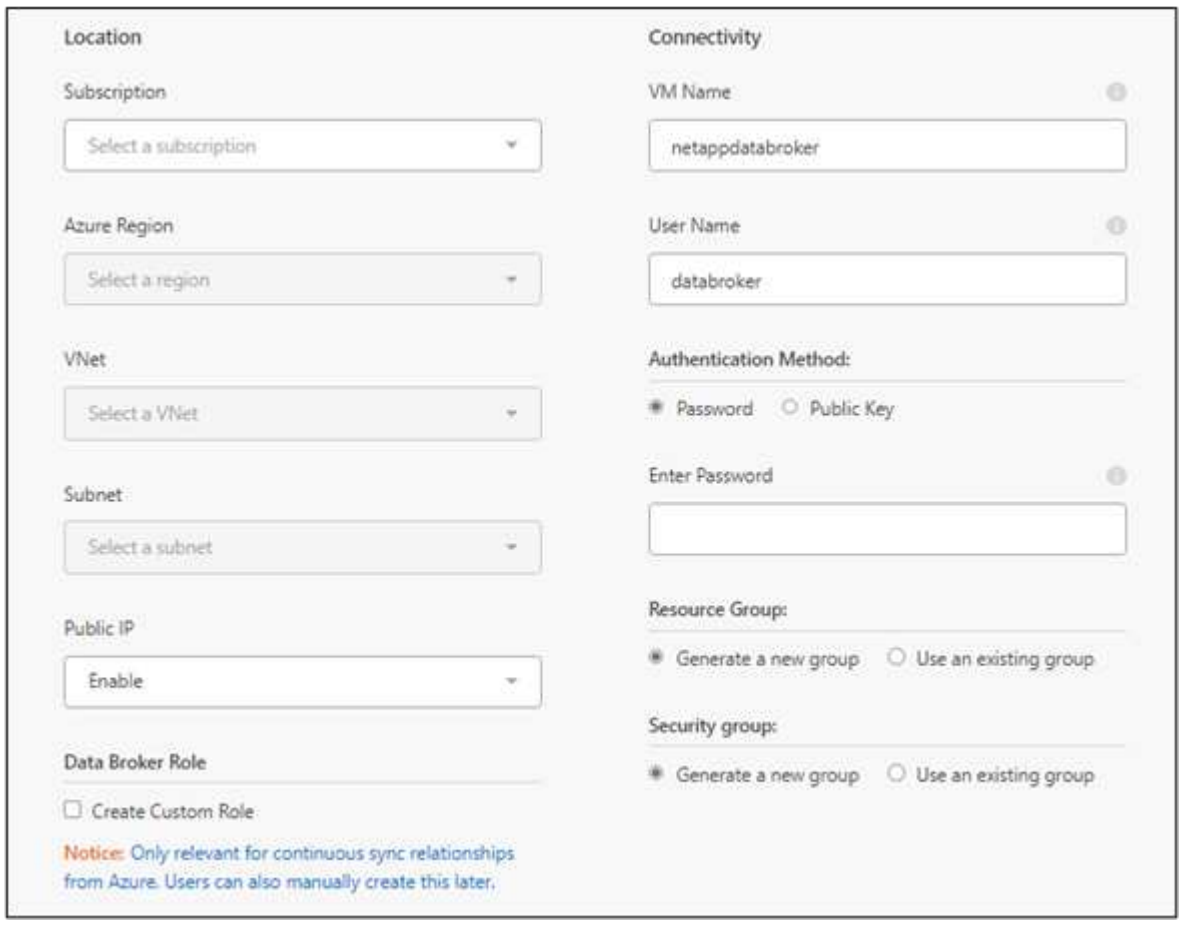
4. 데이터 브로커 그룹 페이지에서 *데이터 브로커 만들기*를 선택한 다음 *Microsoft Azure*를 선택합니다.



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

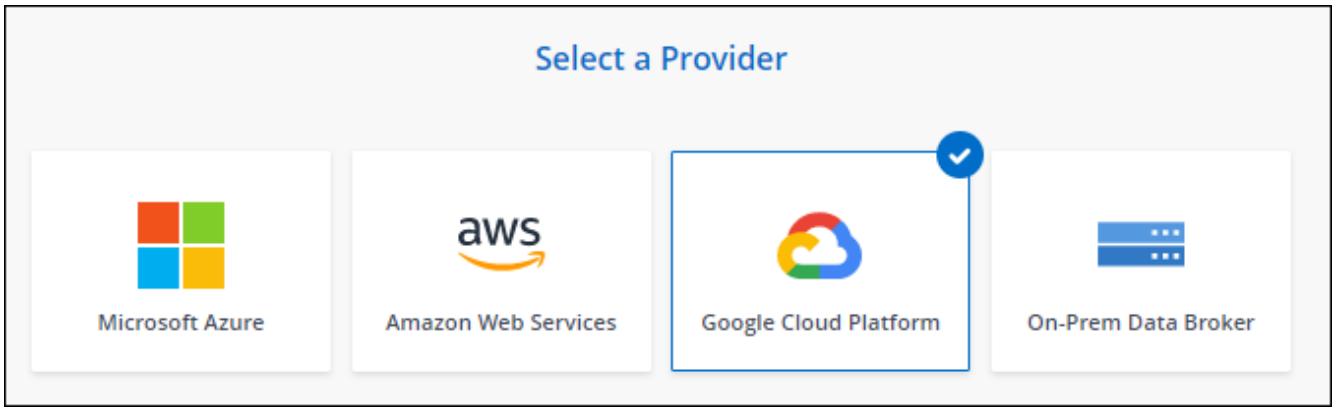
새로운 데이터 브로커를 만드는 방법에는 여러 가지가 있습니다. 이 단계에서는 동기화 관계를 생성할 때 Google Cloud에 데이터 브로커를 설치하는 방법을 설명합니다.

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.

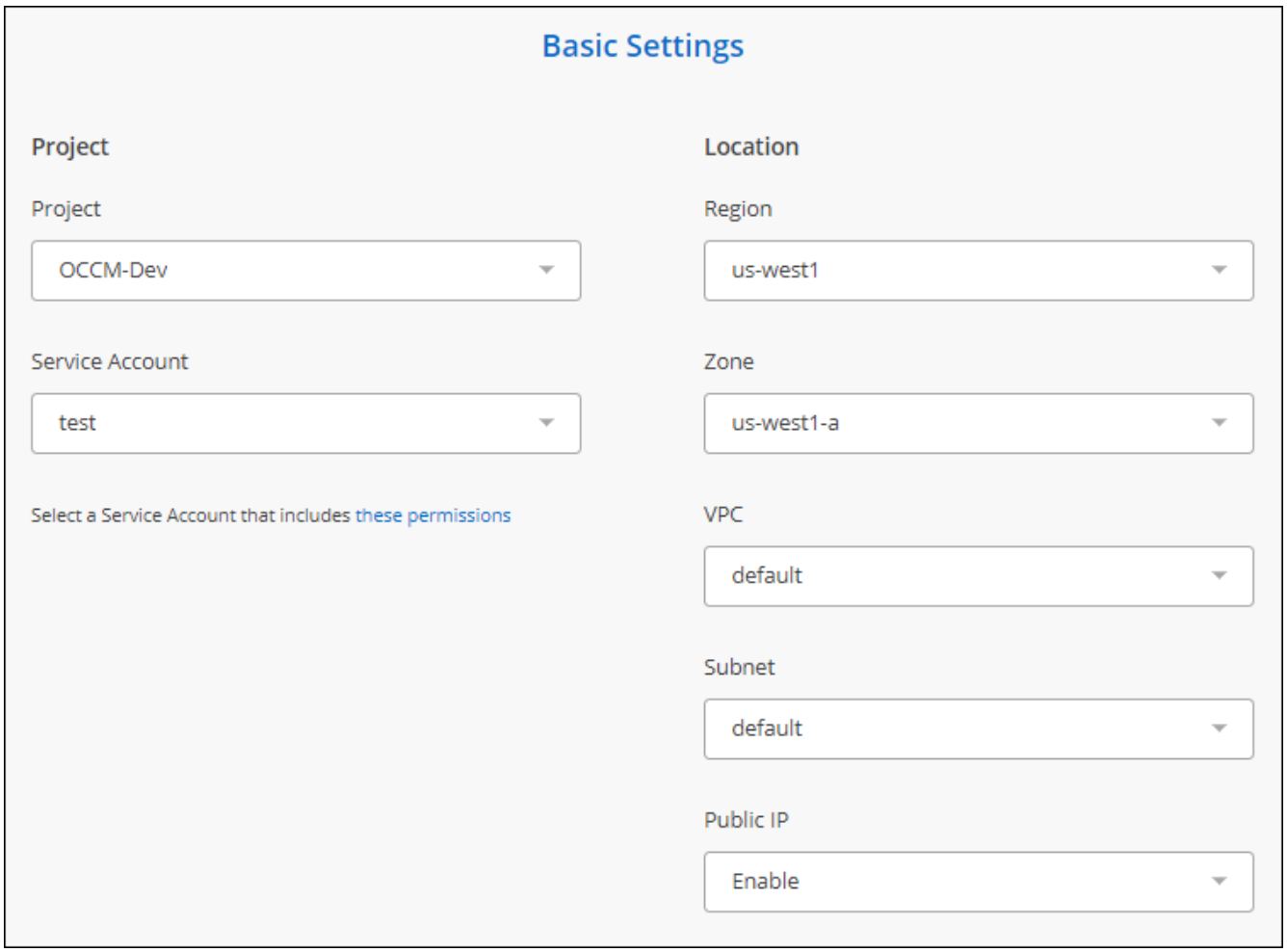


5. 데이터 브로커의 이름을 입력하고 *계속*을 선택합니다.
6. 메시지가 표시되면 Google 계정으로 로그인하세요.

   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

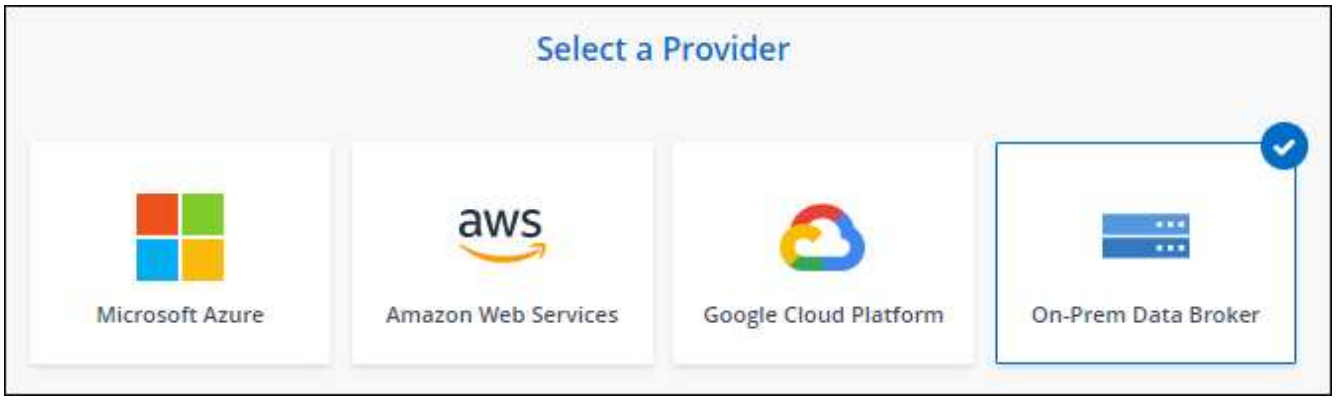
동기화 관계를 만들 때 Linux 호스트에 데이터 브로커를 설치할 수 있습니다.

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.