데이터 브로커를 설치합니다

BlueXP copy and sync

NetApp
April 08, 2024

목차

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. BlueXP 복사 및 동기화는 설치 과정을 안내합니다. 하지만 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.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동으로 실행됩니다. 루트 권한으로 실행하는 것은 데이터 브로커 작업에 대한 요구 사항입니다. 예를 들어 공유를 마운트하는 것입니다.

네트워킹 요구 사항

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

  BlueXP 복사 및 동기화가 AWS에 데이터 브로커를 배포할 때 필요한 아웃바운드 통신을 가능하게 하는 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.

AWS에서 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 하는 요구 사항

BlueXP 복사 및 동기화가 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

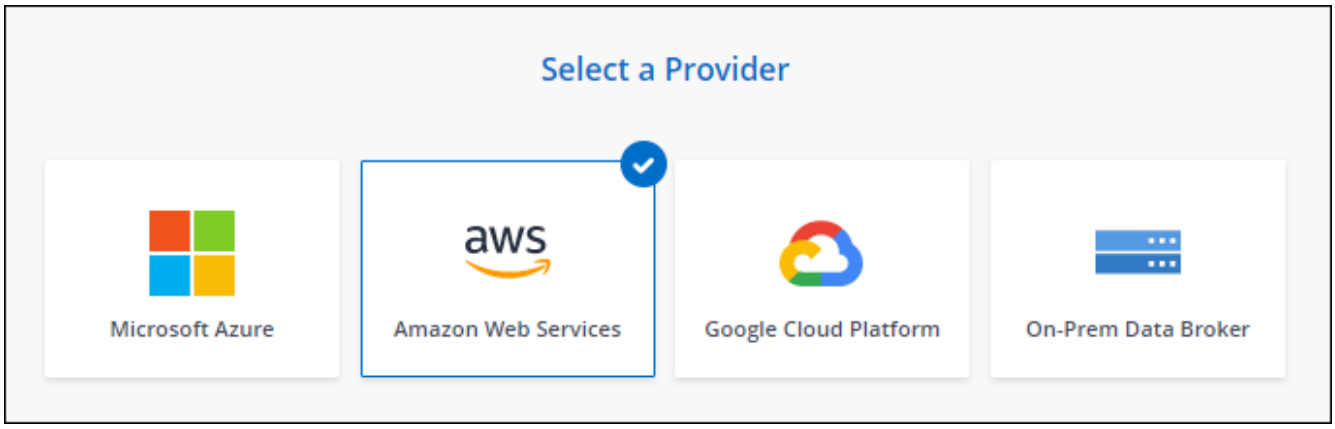
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 생성할 때 AWS에서 데이터 브로커를 설치하는 방법을 설명합니다.

단계

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

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

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



4. 데이터 브로커의 이름을 입력하고 * Continue * 를 선택합니다.
5. AWS 액세스 키를 입력하여 BlueXP 복사 및 동기화를 통해 AWS에서 데이터 브로커를 생성할 수 있습니다.

   키는 다른 용도로 저장되거나 사용되지 않습니다.

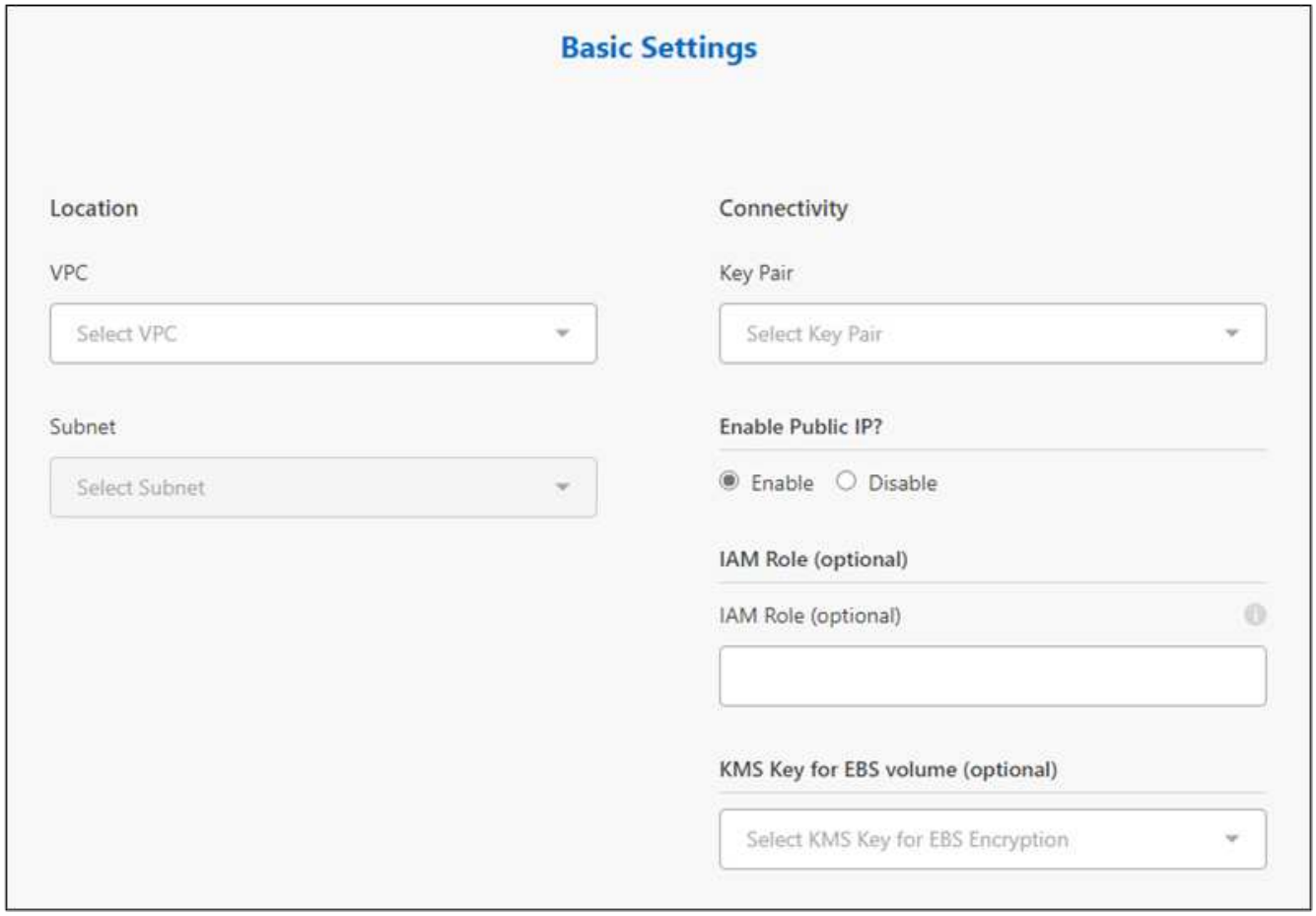
   액세스 키를 제공하지 않으려면 페이지 하단의 링크를 선택하여 CloudFormation 템플릿을 대신 사용합니다. 이 옵션을 사용할 경우 AWS에 직접 로그인하므로 자격 증명을 제공할 필요가 없습니다.

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

   ▶ https://docs.netapp.com/ko-kr/bluexp-copy-sync//media/video_cloud_sync.mp4 *(video)*

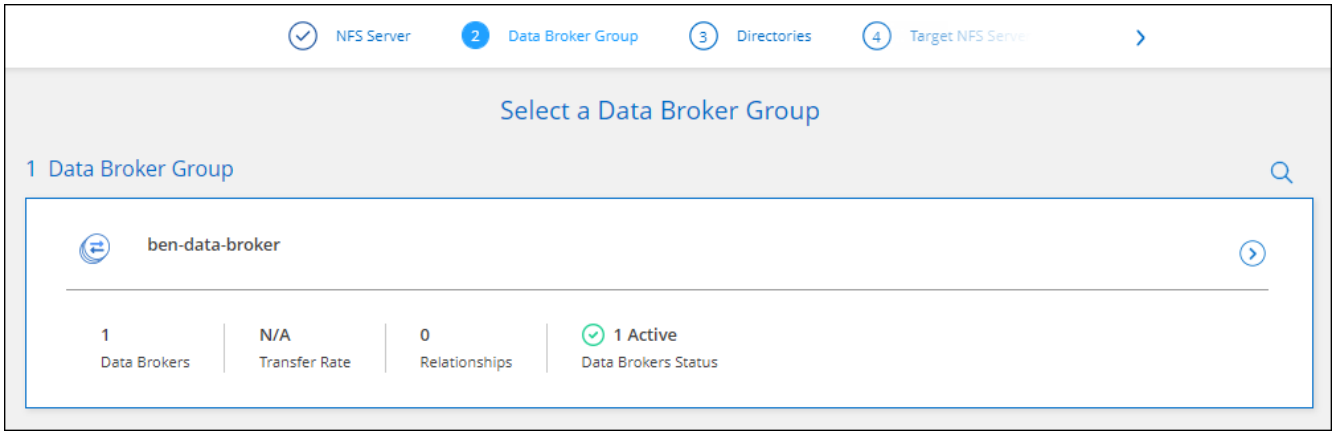
6. AWS 액세스 키를 입력한 경우, 인스턴스에 대한 위치를 선택하고 키 쌍을 선택하고, 공용 IP 주소를 활성화할지 여부를 선택하고, 기존 IAM 역할을 선택하거나, 필드를 비워 두면 BlueXP 복사 및 동기화에서 역할을 생성할 수 있습니다. KMS 키를 사용하여 데이터 브로커를 암호화할 수도 있습니다.

   IAM 역할을 직접 선택할 경우 필요한 권한을 제공해야 합니다.



7. VPC의 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.
8. 데이터 브로커를 사용할 수 있게 되면 BlueXP 복사 및 동기화에서 * 계속 * 을 선택합니다.

   다음 이미지는 AWS에 성공적으로 구축된 인스턴스를 보여줍니다.



9. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

결과

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

데이터 브로커 인스턴스에 대한 세부 정보

BlueXP 복사 및 동기화는 다음 구성을 사용하여 AWS에서 데이터 브로커를 생성합니다.

Node.js 호환성
: v21.2.0

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 2023

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. BlueXP 복사 및 동기화는 설치 과정을 안내합니다. 하지만 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.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동으로 실행됩니다. 루트 권한으로 실행하는 것은 데이터 브로커 작업에 대한 요구 사항입니다. 예를 들어 공유를 마운트하는 것입니다.

네트워킹 요구 사항

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

  BlueXP 복사 및 동기화가 Azure에 데이터 브로커를 배포할 때 필요한 아웃바운드 통신을 가능하게 하는 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",
                    "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"
}
```

참고:

1. 다음 권한은 를 사용하도록 설정할 경우에만 필요합니다 "연속 동기화 설정" Azure에서 다른 클라우드 저장소 위치로의 동기화 관계:
    - '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/스토리지/스토리지 계정/쓰기)

또한 Azure에서 Continuous Sync를 구현하려는 경우 할당 가능한 범위를 구독 범위 및 * NOT * 리소스 그룹 범위로 설정해야 합니다.

2. 다음 권한은 데이터 브로커 생성을 위해 자체 보안을 선택할 경우에만 필요합니다.
   - "Microsoft.Network/networkSecurityGroups/securityRules/read" 참조하십시오
   - "Microsoft.Network/networkSecurityGroups/read" 참조하십시오

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

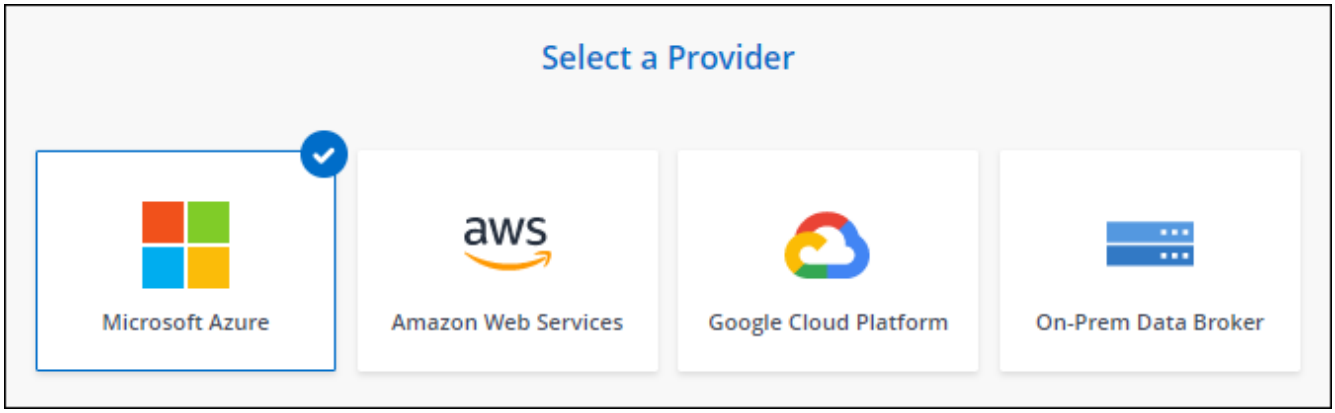
새로운 데이터 브로커를 생성하는 방법은 몇 가지가 있습니다. 다음 단계에서는 동기화 관계를 만들 때 Azure에서 데이터 브로커를 설치하는 방법을 설명합니다.

단계

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

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

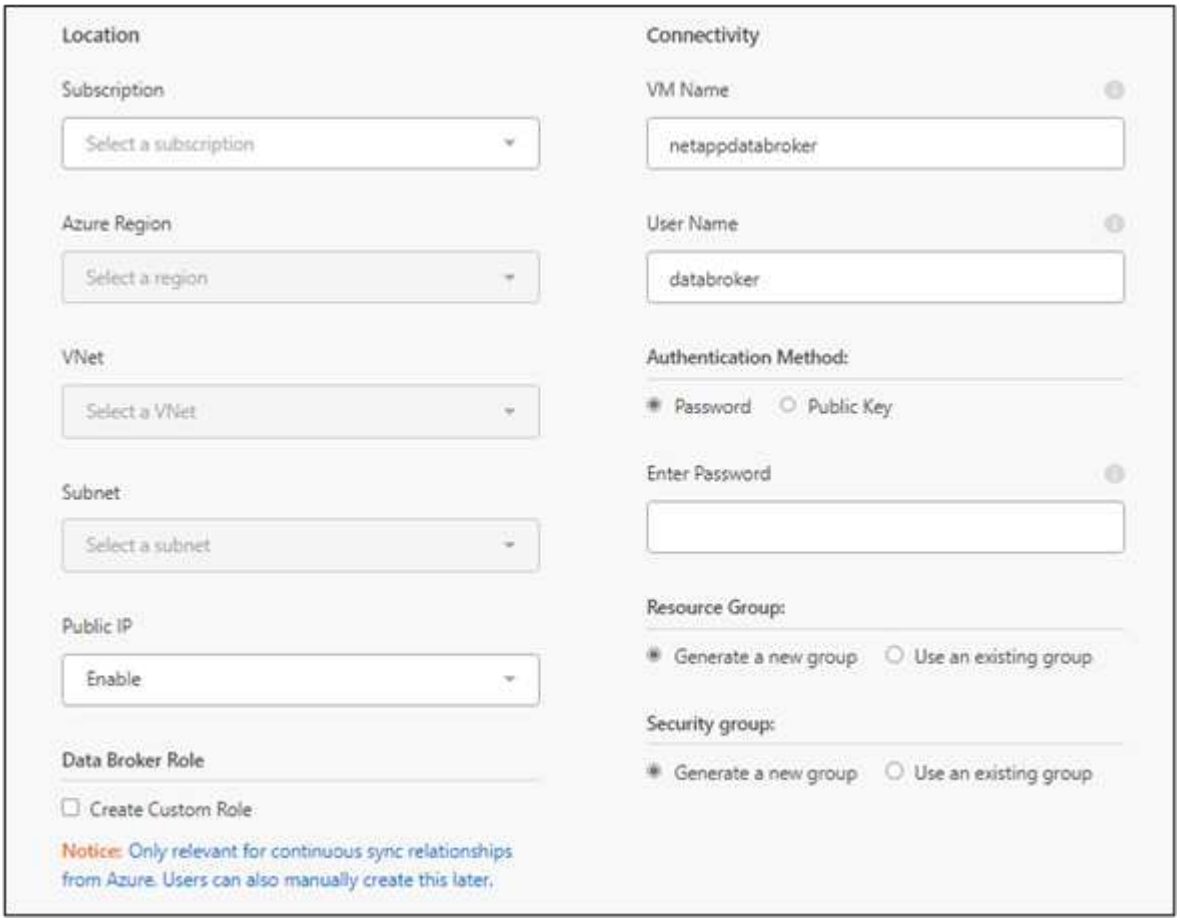
3. 데이터 브로커 그룹 * 페이지에서 * 데이터 브로커 * 를 선택한 다음 * Microsoft Azure * 를 선택합니다.



4. 데이터 브로커의 이름을 입력하고 * Continue * 를 선택합니다.
5. 메시지가 표시되면 Microsoft 계정에 로그인합니다. 메시지가 표시되지 않으면 * Azure에 로그인 * 을 선택합니다.

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

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



> 연속 동기화 관계를 구현하려는 경우 데이터 브로커에 사용자 지정 역할을 할당해야 합니다. 브로커가 생성된 후 수동으로 이 작업을 수행할 수도 있습니다.

7. VNET에서 인터넷 액세스에 프록시가 필요한 경우 프록시 구성을 지정합니다.
8. Continue * 를 선택합니다. 데이터 브로커에 S3 권한을 추가하려면 AWS 액세스 및 비밀 키를 입력합니다.

9. Continue * 를 선택하고 배포가 완료될 때까지 페이지를 열어 둡니다.

   이 프로세스는 최대 7분 정도 소요될 수 있습니다.

10. BlueXP 복사 및 동기화에서 데이터 브로커가 사용 가능해지면 * 계속 * 을 선택합니다.
11. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

결과

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

관리자 동의가 필요하다는 메시지를 받았습니까?

BlueXP 복사 및 동기화에 사용자 대신 조직의 리소스에 액세스할 수 있는 권한이 필요하므로 Microsoft에서 관리자 승인이 필요하다고 알리는 경우 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-5a38923cab85입니다.

데이터 브로커 **VM**에 대한 세부 정보

BlueXP 복사 및 동기화는 다음 구성을 사용하여 Azure에서 데이터 브로커를 생성합니다.

Node.js 호환성
: v21.2.0

VM 유형입니다
: 표준 DS4 v2

vCPU
: 8

RAM
: 28GB

운영 체제

Rocky Linux 9.0

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. BlueXP 복사 및 동기화는 설치 과정을 안내합니다. 하지만 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.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동으로 실행됩니다. 루트 권한으로 실행하는 것은 데이터 브로커 작업에 대한 요구 사항입니다. 예를 들어 공유를 마운트하는 것입니다.

네트워킹 요구 사항

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

  BlueXP 복사 및 동기화가 Google Cloud에 데이터 브로커를 배포할 때 필요한 아웃바운드 통신을 가능하게 하는 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.

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.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
```

참고:

1. "iam.serviceAccounts.signJwt" 권한은 외부 HashashCorp 볼트를 사용하도록 데이터 브로커를 설정할 계획에만 필요합니다.
2. "pubsub. * " 및 "storage.pubket.update" 권한은 Google Cloud Storage에서 다른 클라우드 저장소 위치로 동기화 관계에 대해 연속 동기화 설정을 사용하려는 경우에만 필요합니다. "연속 동기화 옵션에 대해 자세히 알아보십시오".
3. "cloudkms.cryptoKeys.list" 및 "cloudkms.keyRings.list" 권한은 대상 Google Cloud Storage 버킷에서 고객 관리 KMS 키를 사용할 계획인 경우에만 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.

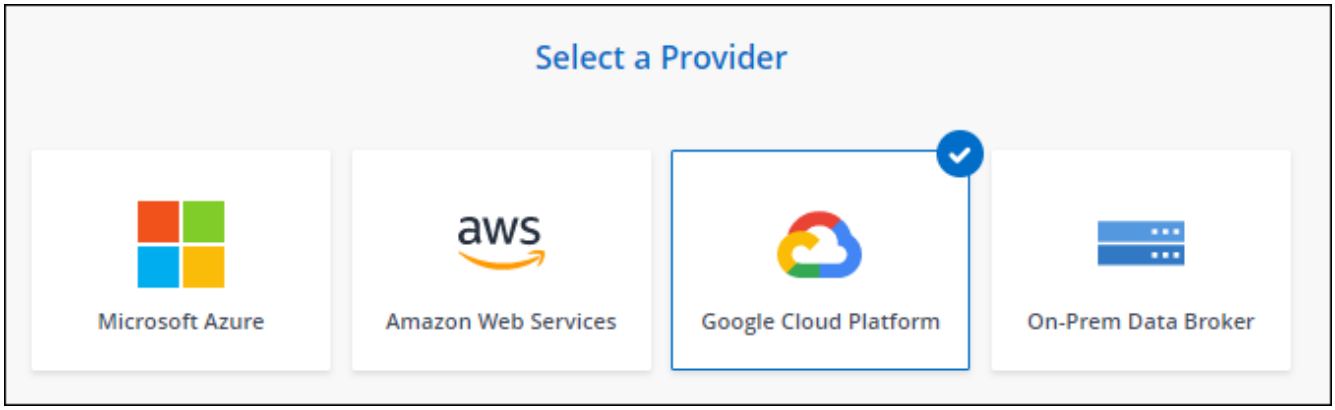
단계

1. 새 동기화 만들기 * 를 선택합니다.

2. 동기화 관계 정의 * 페이지에서 소스 및 대상을 선택하고 * 계속 * 을 선택합니다.

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

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

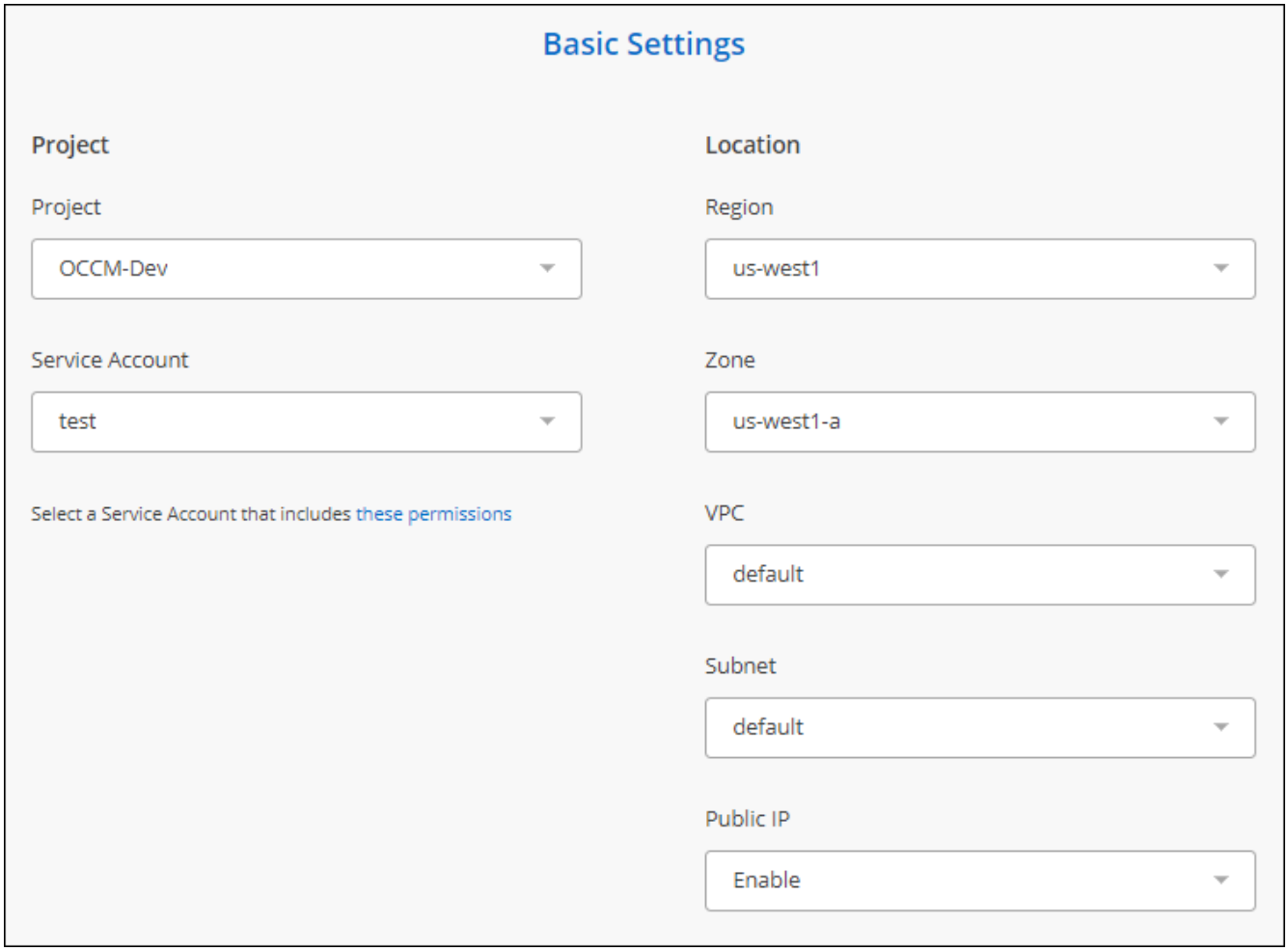


4. 데이터 브로커의 이름을 입력하고 * Continue * 를 선택합니다.
5. 메시지가 표시되면 Google 계정으로 로그인합니다.

   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.



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 BlueXP 복사 및 동기화에서 * 계속 * 을 선택합니다.

   인스턴스를 구축하는 데 약 5~10분이 소요됩니다. BlueXP 복사 및 동기화 서비스에서 진행 상황을 모니터링할 수 있으며, 인스턴스를 사용할 수 있을 때 자동으로 새로 고쳐집니다.

9. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.

결과

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 Cloud Storage를 소스 또는 타겟으로 선택할 때 BlueXP 복사 및 동기화를 통해 데이터 브로커의 서비스 계정에 사용할 수 있는 사용 권한이 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 선택합니다.
3. 사용 권한 * 을 선택합니다.
4. 추가 * 를 선택합니다.
5. 데이터 브로커의 서비스 계정 이름을 입력합니다.
6. 에서 제공하는 역할을 선택합니다 위와 동일한 권한.
7. 저장 * 을 선택합니다.

결과

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

데이터 브로커 VM 인스턴스에 대한 세부 정보

BlueXP 복사 및 동기화는 다음 구성을 사용하여 Google Cloud에서 데이터 브로커를 생성합니다.

Node.js 호환성
: v21.2.0

기계 유형
: N2-표준-4

vCPU
: 4

RAM
: 15GB

운영 체제
: Rocky Linux 9.0

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. BlueXP 복사 및 동기화는 설치 과정을 안내합니다. 하지만 설치 준비에 도움이 되도록 이 페이지에서 요구 사항과 단계를 반복합니다.

Linux 호스트 요구 사항

- * Node.js 호환성 *: v21.2.0
- * 운영 체제 *:

- CentOS 8.0 및 8.5

  CentOS 스트림은 지원되지 않습니다.

- Red Hat Enterprise Linux 8.5, 8.8 및 8.9
- 록키 리눅스 9
- Ubuntu 서버 20.04 LTS
- SUSE Linux Enterprise Server 15 SP1

  데이터 브로커를 설치하기 전에 호스트에서 'yum update' 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.

루트 권한

데이터 브로커 소프트웨어는 Linux 호스트에서 루트로 자동으로 실행됩니다. 루트 권한으로 실행하는 것은 데이터 브로커 작업에 대한 요구 사항입니다. 예를 들어 공유를 마운트하는 것입니다.

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

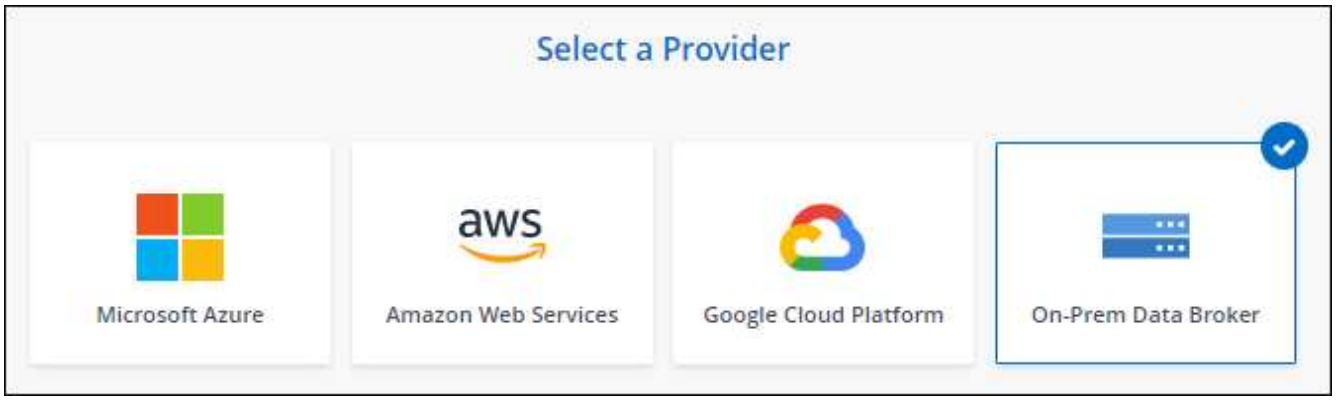
동기화 관계를 생성할 때 Linux 호스트에 데이터 브로커를 설치할 수 있습니다.

단계

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

   데이터 브로커 그룹 * 페이지가 나타날 때까지 단계를 완료합니다.

3. 데이터 브로커 그룹 * 페이지에서 * 데이터 브로커 생성 * 을 선택한 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 * Continue * 를 선택합니다.

   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.

      > 사용자는 로컬 사용자여야 합니다. 도메인 사용자는 지원되지 않습니다.

   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>'

        URI입니다

        BlueXP 복사 및 동기화는 지침 페이지에 설치 파일의 URI를 표시합니다. 이 내용은 프롬프트에 따라 사내 데이터 브로커를 배포할 때 로드됩니다. 이 URI는 링크가 동적으로 생성되고 한 번만 사용할 수 있으므로 여기서 반복되지 않습니다. 다음 단계에 따라 BlueXP 복사 및 동기화에서 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 BlueXP 복사 및 동기화에서 * 계속 * 을 선택합니다.
7. 마법사의 페이지를 완료하여 새 동기화 관계를 생성합니다.