



## 시작하십시오 SnapCenter Service

NetApp  
May 18, 2022

# 목차

시작하십시오 .....	1
SnapCenter 서비스에 대해 자세히 알아보십시오 .....	1
시작하십시오 .....	3
커넥터를 생성하고 SnapCenter 서비스를 활성화하기 위한 필수 구성 요소입니다 .....	3
Azure for SnapCenter 서비스에서 커넥터를 생성합니다 .....	7
Azure NetApp Files용 SnapCenter 서비스를 활성화합니다 .....	8
HDBSQL 클라이언트를 설치합니다 .....	11

# 시작하십시오

## SnapCenter 서비스에 대해 자세히 알아보십시오

SnapCenter 서비스는 NetApp® 클라우드 스토리지에서 실행되는 애플리케이션을 위한 데이터 보호 기능을 제공합니다. NetApp Cloud Manager 내에서 지원되는 SnapCenter 서비스는 Azure NetApp Files에 상주하는 SAP HANA® 시스템을 효율적이고 애플리케이션 정합성이 보장된 정책 기반 백업 및 복원할 수 있도록 제공합니다.

있습니다

SnapCenter 서비스의 아키텍처에는 다음과 같은 구성 요소가 포함되어 있습니다.

- SnapCenter 서비스 UI는 Cloud Manager UI와 통합됩니다.

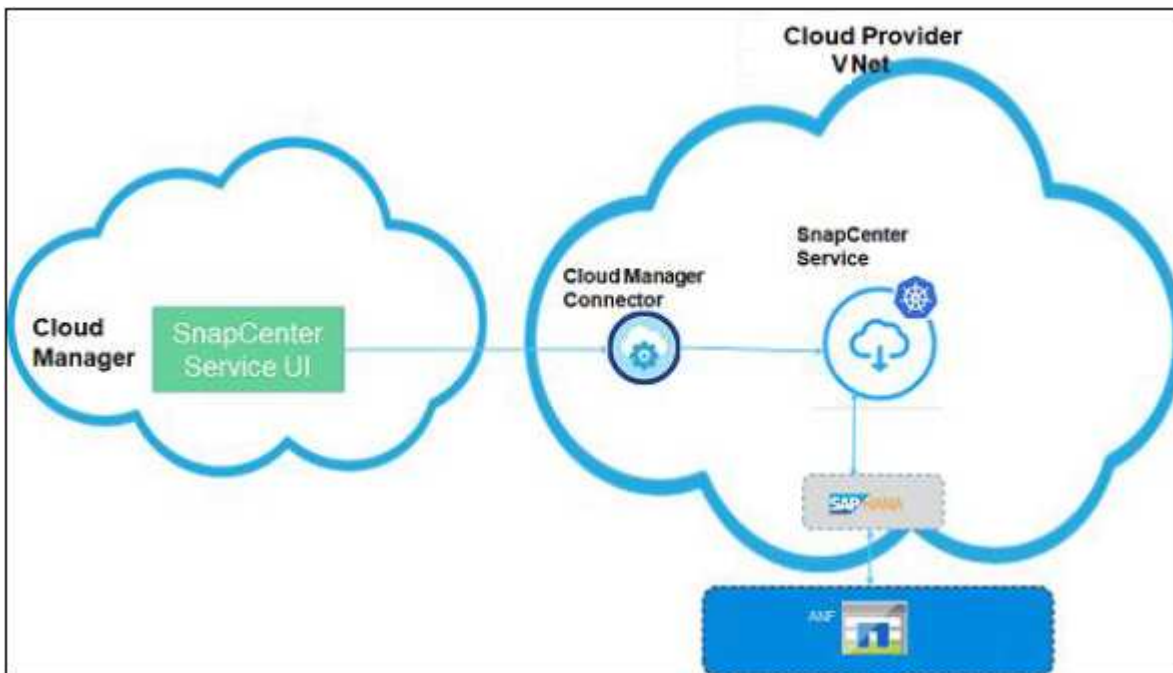
SnapCenter 서비스 UI는 NetApp에서 관리하는 Cloud Manager SaaS 프레임워크에서 제공되며, 다양한 스토리지 및 데이터 관리 기능을 제공합니다.

- Cloud Manager Connector는 Cloud Manager의 구성 요소로, SnapCenter 서비스와 기타 서비스의 라이프사이클 관리를 담당합니다.
- SnapCenter 서비스는 Azure Kubernetes Service(AKS)에서 호스팅되는 데이터 보호 서비스 세트로 데이터 보호 워크플로우를 조정합니다.



Cloud Manager Connector와 SnapCenter 서비스는 클라우드 네트워크에 구축됩니다.

다음 다이어그램은 SnapCenter 서비스의 각 구성 요소 간의 관계를 보여 줍니다.



사용자가 시작한 요청의 경우 SnapCenter 서비스 UI는 클라우드 관리자 SaaS와 통신하며, 요청에 대한 유효성 검사가 완료되면 Cloud Manager Connector로 통화를 전달합니다. 그런 다음 커넥터는 SnapCenter 서비스와 통신하고

SnapCenter 서비스는 Azure NetApp Files 관리 API 및 HANA 시스템 명령을 호출하여 데이터 보호 작업을 수행합니다.

SnapCenter 서비스는 HANA 시스템과 동일한 VNET에 구축하거나 다른 서비스로 구축할 수 있습니다. SnapCenter 서비스와 HANA 시스템이 서로 다른 네트워크에 있는 경우 네트워크 연결을 설정해야 합니다.

## 지원되는 기능

SnapCenter 서비스는 다음 기능을 지원합니다.

- SAP HANA 시스템 추가
- SAP HANA 시스템 백업
  - 스냅샷 기반 백업과 파일 기반 백업을 모두 지원합니다
  - SAP HANA 시스템의 주문형 백업을 지원합니다
  - 시스템 정의 정책 또는 사용자 지정 정책을 사용하여 SAP HANA 시스템의 예약된 백업을 지원합니다

정책에서 시간별, 일별, 주별 및 월별 등 다양한 예약 빈도를 지정할 수 있습니다.

  - 비 데이터 볼륨 및 글로벌 비 데이터 볼륨 백업을 지원합니다
- 정책을 기반으로 백업을 유지합니다
- 사용자 지정 백업에서 SAP HANA 시스템 복원
- 백업 및 기타 작업 모니터링
- HANA 시스템에 데이터 및 로그 백업 카탈로그 관리
- 보호 요약, 구성 세부 정보 및 작업 상태를 대시보드에 표시합니다
- 이메일을 통해 알림 전송

## 제한 사항

SnapCenter 서비스 1.0에는 다음과 같은 제한 사항이 있습니다.

- 국제화는 지원되지 않으므로 영어 브라우저를 사용해야 합니다.
- "계정 관리자" 역할을 가진 클라우드 관리자 사용자만 SnapCenter 서비스를 활성화할 수 있습니다.
- AKS(Azure Kubernetes Service) 클러스터 노드 장애와 관련된 제한 사항
  - AKS 클러스터에서 노드 중 하나가 오프라인이 되면 기내 작업이 실패할 수 있지만 후속 작업은 실행됩니다.
  - AKS 클러스터에서 노드 중 하나가 중지되면 SAP HANA 시스템을 추가할 수 없지만 다른 작업은 문제 없이 실행됩니다.

HANA 시스템을 추가하려면 노드를 가져와야 합니다.

- 스케줄러는 고가용성 구성을 지원하지 않습니다.

스케줄러에서 사용하는 MySQL 노드가 다운되면 예약된 작업을 계속하려면 노드를 가져와야 합니다.

# 시작하십시오

SnapCenter 서비스를 시작하여 몇 가지 단계를 통해 데이터를 보호하십시오.

당신은 해야 한다 ["NetApp Cloud Central에 가입하십시오"](#), ["Cloud Manager에 로그인합니다"](#)를 선택한 다음 설정합니다 ["NetApp 계정"](#).

계정 관리자만 SnapCenter 서비스를 배포할 수 있습니다. 그러나 계정 관리자와 SnapCenter 관리자는 서로 다른 작업을 수행할 수 있습니다. ["자세한 정보"](#)

이 모든 것을 확인해야 합니다 ["필수 구성 요소"](#) 커넥터를 생성하고 SnapCenter 서비스를 활성화하는 것이 충족됩니다.

당신은 해야 한다 ["Azure for SnapCenter 서비스에서 커넥터를 생성합니다"](#).

모든 필수 구성 요소를 충족하는 커넥터가 있는 경우 이를 사용할 수 있습니다.

Cloud Manager에서 Azure NetApp Files 작업 환경을 생성하여 NetApp 계정, 용량 풀, 볼륨 및 스냅샷을 생성하고 관리합니다. ["자세한 정보"](#)

당신은 해야 한다 ["SnapCenter 서비스를 활성화합니다"](#) Cloud Manager UI 사용 SnapCenter 서비스가 활성화되면 SnapCenter 서비스를 호스팅하는 Azure Kubernetes Service(AKS) 클러스터가 생성됩니다.

당신은 해야 한다 ["HDBSQL 클라이언트를 설치합니다"](#) SAP HANA 데이터베이스에서 데이터 보호 작업을 수행합니다. HDBSQL 클라이언트는 SAP HANA 시스템과 통신하는 데 사용됩니다.

수동으로 해야 합니다 ["SAP HANA 시스템을 추가합니다"](#).

그러면 됩니다 ["SAP HANA 시스템을 백업합니다"](#) 시스템 정의 또는 사용자 정의 정책 사용 데이터 손실 발생 시 다음을 수행할 수 있습니다 ["SAP HANA 시스템을 복원합니다"](#) 해당 시스템의 백업을 사용합니다.

## 커넥터를 생성하고 SnapCenter 서비스를 활성화하기 위한 필수 구성 요소입니다

Azure에서 커넥터를 생성하고 SnapCenter 서비스를 활성화하기 전에 특정 사항을 확인해야 합니다.

- Connector에 대해 선택한 서브넷이 Azure Kubernetes Service(AKS)에 예약된 다음 IP 주소 범위와 겹치지 않아야 합니다. 169.254.0.0/16, 172.30.0.0/16, 172.31.0.0/16 및 192.0.2.0/24.
- 선택한 서브넷에서 실행 중인 AKS가 없는지 확인합니다.
- 선택한 서브넷이 해당 포트의 SAP HANA 시스템에 액세스할 수 있는지 확인합니다.
- 선택한 서브넷의 VNET가 SAP HANA 시스템의 VNET와 다른 경우 VNETs가 VPN 게이트웨이, 피어링 또는 기타 수단을 통해 서로 통신할 수 있는지 확인합니다.
- 방화벽 뒤에서 SnapCenter 서비스를 활성화하려면 에 설명된 작업을 수행해야 합니다 [\[Network requirements\]](#).

SnapCenter 서비스를 방화벽 뒤에서 활성화할지 여부를 먼저 결정해야 합니다. SnapCenter 서비스를 활성화한 후에는 방화벽 뒤에서 실행되도록 구성할 수 없습니다. 이는 AKS의 제한 사항입니다.

## 네트워크 요구 사항

Connector가 클라우드 환경 내의 리소스 및 프로세스를 관리할 수 있도록 네트워크를 설정합니다.

### 방화벽 구성

방화벽 뒤에서 SnapCenter 서비스를 활성화하려면 다음 작업을 수행해야 합니다.



Azure 방화벽을 사용하는 경우 스크립트를 사용하여 다음 단계를 수행할 수 있습니다. 자세한 내용은 을 참조하십시오 [\[Azure Firewall configuration\]](#).

#### • 단계 \*

1. 아래 네트워크 규칙을 방화벽에 추가합니다.

대상 끝점	프로토콜	포트	설명
"서비스 태그" -AzureCloud.<Region>: 1194	UDP입니다	1194	전용 커넥터 및 전용 SnapCenter 서비스 클러스터를 사용하려는 경우에는 필요하지 않습니다.
"서비스 태그" -AzureCloud.<Region>: 9000	TCP	9000입니다	전용 커넥터 및 전용 SnapCenter 서비스 클러스터를 사용하려는 경우에는 필요하지 않습니다.
FQDN- ntp.ubuntu.com:123 을 참조하십시오	UDP입니다	123을 선택합니다	Azure 가상 머신의 시간 동기화에 필요합니다.
"서비스 태그" -AzureCloud.<Region>: 443	TCP	443	전용 커넥터 및 전용 SnapCenter 서비스 클러스터를 사용하려는 경우에는 필요하지 않습니다.

2. 다음 FQDN 태그 및 포트 세부 정보를 사용하여 방화벽에 응용 프로그램 규칙을 추가합니다.

- FQDN 태그 - AzureKubernetesService
- HTTPS:443

3. 프로토콜 및 포트를 HTTPS:443으로 사용하여 아래 끝점과 함께 대상 FQDN으로 응용 프로그램 규칙을 추가합니다.

엔드포인트	목적
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> 으로 문의하십시오	Cloud Manager를 사용하면 대부분의 Azure 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a> 으로 문의하십시오	Cloud Manager를 사용하여 Azure 독일 지역에서 Cloud Volumes ONTAP를 구축 및 관리할 수 있습니다.

엔드포인트	목적
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> 으로 문의하십시오	Cloud Manager를 사용하여 Azure US Gov 지역에 Cloud Volumes ONTAP를 배포하고 관리할 수 있습니다.
<a href="https://api.services.cloud.netpp.com">https://api.services.cloud.netpp.com</a> 으로 문의하십시오	NetApp Cloud Central에 API 요청을 허용합니다.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a> 으로 문의하십시오	소프트웨어 이미지, 매니페스트 및 템플릿에 대한 액세스를 제공합니다.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Connector가 매니페스트, 템플릿 및 Cloud Volumes ONTAP 업그레이드 이미지에 액세스하고 다운로드할 수 있도록 합니다.
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a> 으로 문의하십시오	Docker를 실행하는 인프라에 대한 컨테이너 구성 요소의 소프트웨어 이미지에 액세스하고 Cloud Manager와의 서비스 통합을 위한 솔루션을 제공합니다.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a> 으로 문의하십시오	NetApp에서 감사 레코드의 데이터를 스트리밍할 수 있습니다.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a> 으로 문의하십시오	NetApp 계정을 포함한 Cloud Manager 서비스와 통신합니다.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> 으로 문의하십시오	NetApp Cloud Central과 통신하여 중앙 집중식 사용자 인증 제공
<a href="https://support.netapp.com">https://support.netapp.com</a> 으로 문의하십시오	NetApp AutoSupport과 커뮤니케이션:
<a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a> 으로 문의하십시오	시스템 라이선스 및 지원 등록을 위해 NetApp과 커뮤니케이션
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> 으로 문의하십시오	NetApp에서 지원 문제를 해결하는 데 필요한 정보를 수집할 수 있도록 지원합니다.
<a href="https://blob.core.windows.net">.blob.core.windows.net</a> 으로 문의하십시오	프록시를 사용할 때 HA 쌍에 필요합니다.
<a href="https://auth0.com">https://auth0.com</a> 으로 문의하십시오	Auth0 인증에 필요합니다.
<a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://production.cloudflare.docker.com">https://production.cloudflare.docker.com</a> 를 참조하십시오	이 명령어는 SnapCenter 서비스 워크플로우 엔진의 종속성을 검색합니다.
<a href="https://exeranl-log.cloudmanager.netapp.com">https://exeranl-log.cloudmanager.netapp.com</a> 으로 문의하십시오	통신을 통해 로그를 Cloud Manager 로그 저장소로 전송할 수 있습니다.

4. SnapCenter 서비스를 설치할 서버넷을 선택합니다.

5. 루트가 있는 라우팅 테이블 만들기:

- 서버넷에서 방화벽 내부 IP 주소로 트래픽을 전달합니다
- 방화벽 공용 IP 주소에서 인터넷으로 트래픽을 전달합니다.

6. 서브넷에 라우팅 테이블을 첨부합니다.

Cloud Manager Connector의 네트워킹 요구사항에 대한 자세한 내용은 [클라우드 매니저 커넥터에 대한 네트워킹 요구 사항](#)을 참조하십시오.

## Azure 방화벽 구성

Azure 방화벽 뒤에서 SnapCenter 서비스를 활성화하려면 다음 작업을 수행해야 합니다.

- 필요한 것 \*
- 방화벽을 만들어야 합니다(클래식 모드).
- SnapCenter 서비스에 대한 VNET 및 서브넷을 생성해야 합니다.
- 방화벽 리소스와 SnapCenter 서비스의 VNET가 서로 다른 테넌트에 있는 경우 Azure 셸의 두 테넌트에 모두 로그인해야 합니다.
- 방화벽 VNET와 SnapCenter VNET가 다른 경우 VNETs 간에 피어링을 설정해야 합니다.
- 단계 \*

1. [클라우드 매니저 커넥터](#)를 다운로드합니다 "scs\_azure\_firewall\_config.sh" 로컬 시스템에 대한 스크립트입니다.

2. [Azure CLI](#)에 로그인합니다 "Microsoft Azure 포털입니다".

3. [Azure CLI](#)를 클릭합니다 를 눌러 클라우드 셸을 열고 Bash 콘솔을 선택합니다.

a. Azure 클라우드 셸에 스크립트를 업로드합니다.

b. 스크립트를 실행할 권한을 할당합니다.

"chmod + x./scs\_Azure\_firewall\_config.sh"를 선택합니다

c. 스크립트를 실행합니다.

```
./scs_azure_firewall_config.sh -fwsubid <Firewall_SubscriptionID> -fwname <Firewall_name>  
-fwrg <Firewall_Resource_group> -scssubid <SnapCenter_Service_SubscriptionID> -scsvnet  
<SnapCenter_Service_VNET_name> -scsssubnet <SnapCenter_Service_Subnet_name>  
-scnetservice_vnet_vnssrSnapCenter_service.vnet_cnet_svnet_svnet_cssid<cnet_ssid>
```



자원 그룹을 만들지 않은 경우 스크립트는 자원 그룹을 만듭니다. 커넥터를 생성하는 동안 동일한 리소스 그룹을 사용하여 모든 SnapCenter 서비스 관련 리소스가 동일한 리소스 그룹에 있도록 할 수 있습니다.

- 결과 \*
- 방화벽 규칙이 구성되었습니다.
- SnapCenter 서비스에 대한 리소스 그룹이 생성됩니다.
- 라우트 테이블은 SnapCenter 서비스 리소스 그룹에 생성됩니다.
- 라우팅 테이블 규칙이 구성됩니다.
- 라우팅 테이블이 서브넷에 연결되어 있습니다.



## HANA 시스템에 연결

SnapCenter 서비스 클러스터는 HDBSQL 명령을 사용하여 사용자 네트워크의 HANA 시스템과 통신해야 합니다. SnapCenter 클러스터와 HANA 시스템 간의 통신 채널은 다음과 같은 다양한 네트워크 아키텍처를 사용하여 허용되어야 합니다.

- 커넥터 및 SnapCenter 서비스 클러스터는 HANA 시스템과 동일한 VNET에 구축됩니다
- 커넥터 및 SnapCenter 서비스 클러스터는 HANA 시스템과 마찬가지로 다른 VNET에 구축되며, 통신은 두 VNETs 간의 VNET 피어링을 사용하여 설정됩니다.
- 커넥터와 SnapCenter 서비스 클러스터는 HANA 시스템과 다른 VNET에 구축되며, 통신은 두 VNETs 사이의 VPN 게이트웨이를 사용하여 설정됩니다.

## 보안 그룹 구성

HANA 시스템에 네트워크 보안 그룹(NSG)이 구성되어 있는 경우, 사용자 저장소 키에 지정된 대로 SnapCenter 서비스 포트에서 HANA 시스템 포트로의 인바운드 통신을 허용해야 합니다.

- 프로토콜: 모든 TCP
- 서브넷: SnapCenter AKS 클러스터 서브넷
- 용도: HDBSQL 명령을 실행합니다

SnapCenter AKS 클러스터에서 실행되는 HANA 서비스는 SSL이 활성화된 HANA 시스템과의 SSL 통신을 지원합니다.

## Azure for SnapCenter 서비스에서 커넥터를 생성합니다

Cloud Manager 기능을 사용하려면 먼저 계정 관리자가 Connector를 배포해야 합니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다.

기본적으로 Azure Marketplace에서 Connector를 만들 수 있습니다. 이 단계를 수행하는 동안 ["Azure Marketplace에서 커넥터를 만듭니다"](#) 다음 사항을 기억해야 합니다.

- Cloud Manager for Cloud Volumes ONTAP가 지정된 모든 곳에서 SnapCenter 서비스에도 활용할 수 있습니다.
- Cloud Manager Name의 경우 더 나은 식별을 위해 Connector VM 이름을 지정합니다. Cloud Manager UI에서 커넥터 이름으로 표시됩니다.
- 공용 IP를 사용하지 않고 커넥터를 구성했거나 방화벽을 구성한 경우 커넥터 시스템에 연결할 점프 호스트가 있어야 합니다.

있는 경우 ["사용자 동의"](#) Azure Active Directory에서 활성화되었거나 테넌트 관리자가 동의를 제공할 수 있는 경우 Cloud Manager UI에서 Connector를 생성할 수 있습니다.

## 사용자 동의를 활성화되었습니다

Azure Active Directory에서 사용자 동의를 활성화된 경우 ["Cloud Manager에서 커넥터를 생성합니다"](#).

## 사용자 동의를 비활성화되었습니다

1. 다음 중 하나를 수행합니다.

- Active Directory에서 관리자 동의 워크플로가 구성된 경우 다음을 수행해야 합니다 **"관리자 동의 요청"**.
- 관리자 동의 워크플로가 구성되어 있지 않은 경우 다음을 수행해야 합니다.
  - i. **"테넌트 전체 관리자 동의를 부여하기 위한 URL을 구성합니다"**.



ClientID를 \_989efff4-9a9e-46fa-9f17-de39e15714f9\_ 로 지정합니다. Cloud Manager 마법사에서 이름이 지정된 Cloud Manager Azure 애플리케이션 ID입니다.

- ii. 테넌트 관리자에게 브라우저에서 URL을 실행하고 동의하도록 요청합니다.

관리자가 표시된 오류를 무시할 수 있습니다

2. **"Cloud Manager에서 커넥터를 생성합니다"**.



커넥터를 생성하는 동안 제공된 사용자 이름 및 암호 또는 키는 컴퓨터에 연결해야 합니다

## Azure NetApp Files용 SnapCenter 서비스를 활성화합니다

Cloud Manager UI를 사용하여 SnapCenter 서비스를 사용하도록 설정할 수 있습니다. SnapCenter 서비스가 활성화되면 SnapCenter 서비스를 호스팅하는 Azure Kubernetes Service(AKS) 클러스터가 생성됩니다.

- 필요한 것 \*
- Azure 구독에 "Microsoft.ContainerService" 리소스 공급자를 등록해야 합니다. 자세한 내용은 [을 참조하십시오 "리소스 공급자 등록 방법"](#).
- 이 모든 것을 확인해야 합니다 **"필수 구성 요소"** 충족됩니다.
- 이 작업에 대한 정보 \*

AKS 클러스터는 Connector를 생성하는 동안 선택한 동일한 리소스 그룹과 동일한 서브넷에 생성됩니다. 커넥터가 공용 IP 주소 없이 생성된 경우 AKS 클러스터는 비공개 모드로 생성됩니다.

AKS 클러스터를 생성 및 관리하려면 필요한 권한이 있는 사용자가 할당한 관리 ID가 필요합니다. 사용자가 할당한 관리 ID가 생성되어 Connector VM에 할당되어야 합니다.

- 단계 \*
- 1. Cloud Manager에 로그인합니다.
- 2. Cloud Manager에서 생성한 Connector를 선택합니다.

Connector가 보호할 SAP HANA 시스템에 대한 네트워크 연결을 가지고 있는지 확인합니다.

- 3. 모든 서비스 \* > \* SnapCenter \* > \* 활성화 \* 를 클릭합니다.
- 4. 다음 중 하나를 수행합니다.

- Cloud Manager UI에서 커넥터를 만든 경우 역할을 만들고 할당할 수 있는 권한이 있으면 SnapCenter

서비스 설치 시 사용자가 할당한 관리 ID가 자동으로 생성됩니다.

- i. Azure 로그인 사용 \* 을 선택합니다.
- ii. 준비 완료 페이지에서 \* 계속 \* 을 클릭합니다.
- iii. Azure 자격 증명을 지정합니다.



Azure 로그인 계정에 충분한 권한이 있는지 확인해야 합니다. 사용 권한 및 사용 권한 할당 방법에 대한 자세한 내용은 을 참조하십시오 [\[Permissions required for Azure login account\]](#).

- Azure Marketplace에서 Connector를 만들었거나 역할을 생성 및 할당할 권한이 없는 경우 아래 단계에 따라 사용자에게 할당된 관리 ID를 생성합니다.

- i. Use Azure CLI script \* 를 선택합니다.
- ii. Azure 계정에 대한 충분한 권한이 없는 경우 관리자에게 문의하십시오.

사용 권한 및 사용 권한 할당 방법에 대한 자세한 내용은 을 참조하십시오 [\[Permissions required for Azure login account\]](#).

- iii. 를 다운로드합니다 "prerequisite\_azure.sh" 로컬 시스템에 대한 스크립트입니다.
- iv. 에 로그인합니다 "Microsoft Azure 포털입니다".

v.

을 클릭합니다  를 눌러 클라우드 셸을 열고 Bash 콘솔을 선택합니다.

- vi. Azure 클라우드 셸에 스크립트를 업로드합니다.
- vii. 스크립트를 실행할 권한을 할당합니다.

"chmod + x./선수 조건\_sAzure.sh"

- viii. 스크립트를 실행합니다.

```
./prerequisite_azure.sh -s <subscription_ID> -g <connector_resourcegroup_name> -c  
<connector_vm_name>
```

## 5. 클러스터 구성 페이지에서 다음을 수행합니다.

- a. 클러스터 구성을 선택합니다.

- High Availability \* 를 선택하면 사용 가능한 영역에 작업자 노드 3개가 포함된 Azure Kubernetes Service(AKS) 클러스터가 생성됩니다.
- 단일 노드 \* 를 선택하면 단일 노드가 있는 AKS 클러스터가 생성됩니다.

- b. Kubernetes Pod 주소 범위를 지정하십시오.

Kubernetes Pod 주소 범위가 가상 네트워크, 피어링된 가상 네트워크 및 연결된 온프레미스 네트워크의 IP 범위와 중복되지 않도록 하십시오. 또한 서비스 주소 범위 및 Docker 브리지 주소와 범위가 겹치지 않아야 합니다.

- c. Kubernetes Service 주소를 지정하십시오.

Kubernetes 서비스 주소 범위가 가상 네트워크의 IP 범위, 피어링된 가상 네트워크 및 연결된 온프레미스 네트워크와 겹치지 않도록 하십시오. 또한 범위가 Pod 주소 범위 및 Docker 브리지 주소와 중복되어서는

안 됩니다.

- d. Docker 브리지 네트워크를 지정합니다.

Docker Bridge 주소가 가상 네트워크, 피어링된 가상 네트워크 및 연결된 사내 네트워크의 IP 범위와 중복되지 않는지 확인합니다. 또한 범위가 Pod 주소 범위 및 서비스 주소 범위와 겹치면 안 됩니다.

- e. Connector가 공용 IP 없이 생성되고 VNET에서 사용자 지정 DNS 서버를 사용하는 경우 \* 사용자 지정 DNS 서버 지원 \* 을 선택합니다.




사용자 지정 DNS 서버가 호스팅되는 VNETs의 전용 DNS 영역에 가상 네트워크 링크를 만들어야 합니다. 전용 DNS 영역 이름과 리소스 그룹 이름이 UI에 표시됩니다.

- 6. 검토 페이지에서 세부 정보를 검토하고 \* 활성화 \* 를 클릭합니다.

- 7. SnapCenter 서비스를 성공적으로 활성화한 후 \* 마침 \* 을 클릭합니다.

• 결과 \*

- SnapCenter 서비스를 성공적으로 활성화하면 AKS 클러스터가 생성됩니다. 을 클릭하여 AKS 클러스터 세부 정보를 볼 수 있습니다 .



SnapCenter 서비스를 활성화하지 못한 경우 문제를 해결하고 \* 재시도 \* 를 클릭할 수 있습니다.

- 사용자가 할당한 관리 ID를 만들면 사용자 지정 역할에 할당됩니다.

- 사용자가 할당한 관리 ID는 커넥터 리소스 그룹의 범위 아래 권한이 있는 사용자 지정 역할에 할당됩니다.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",  
"Microsoft.ContainerService/managedClusters/read",  
"Microsoft.ContainerService/managedClusters/write",  
"Microsoft.ContainerService/managedClusters/delete",  
"Microsoft.ContainerService/managedClusters/listClusterUserCredential/  
action",  
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",  
"Microsoft.ManagedIdentity/userAssignedIdentities/read",  
"Microsoft.Compute/virtualMachines/read",  
"Microsoft.Network/networkInterfaces/read"
```

- 사용자가 할당한 관리 ID는 Connector의 VNET 범위에서 아래 권한이 있는 사용자 지정 역할에 할당됩니다.

```
"Microsoft.Authorization/roleAssignments/read",  
"Microsoft.Network/virtualNetworks/subnets/join/action",  
"Microsoft.Network/virtualNetworks/subnets/read",  
"Microsoft.Network/virtualNetworks/read",  
"Microsoft.Network/virtualNetworks/join/action"
```

- 방화벽에 라우팅하기 위해 서브넷에 라우팅 테이블이 구성되어 있는 경우, 사용자가 할당한 관리 ID는 라우팅 테이블의 범위에서 아래 권한이 있는 사용자 지정 역할에 할당됩니다.

```
"Microsoft.Network/routeTables/*",
"Microsoft.Network/networkInterfaces/effectiveRouteTable/action",
"Microsoft.Network/networkWatchers/nextHop/action"
```

- Connector가 공용 IP 없이 설치된 경우, 사용자가 할당한 관리 ID는 개인 DNS 영역의 범위에서 아래 권한이 있는 사용자 지정 역할에 할당됩니다.

```
"Microsoft.Network/privateDnsZones/*"
```

## Azure 로그인 계정에 필요한 권한입니다

Azure 로그인 계정은 사용자가 할당한 관리 ID, 필요한 역할을 만들고 ID를 커넥터 VM에 할당하는 데 사용됩니다.



로그인 계정의 자격 증명은 SnapCenter 서비스의 어느 곳에도 저장되지 않으며 API를 호출하는 데 사용되지 않습니다. 자격 증명은 UI에서만 사용됩니다.

### • 단계 \*

1. 를 사용하여 사용자 지정 역할을 만듭니다 "SnapCenter\_Deployment\_Role1.json입니다" 파일.

SnapCenter\_Deployment\_Role1.json 파일의 <Subscription\_ID>를 Azure 구독 ID로 바꿔야 합니다.

2. Connector의 리소스 그룹 범위에 있는 로그인 계정에 역할을 할당합니다.

3. 를 사용하여 사용자 지정 역할을 만듭니다 "SnapCenter\_Deployment\_Role2.json입니다" 파일.

SnapCenter\_Deployment\_Role2.json 파일의 <Subscription\_ID>를 Azure 구독 ID로 바꿔야 합니다.

4. Connector의 VNET 이상의 범위에서 로그인 계정에 역할을 할당합니다.

5. 있는 경우 "방화벽이 구성되었습니다"에서 를 사용하여 사용자 지정 역할을 만듭니다 "SnapCenter - 배포 - Role3.json" 파일.

SnapCenter\_Deployment\_Role3.json 파일의 <Subscription\_ID>를 Azure 구독 ID로 바꿔야 합니다.

6. SnapCenter 서브넷에 연결된 라우트 테이블의 범위에서 로그인 계정에 역할을 할당합니다.

## HDBSQL 클라이언트를 설치합니다

SnapCenter 서비스를 활성화한 후 HDBSQL 클라이언트를 설치하여 SAP HANA 데이터베이스에 대한 데이터 보호 작업을 수행합니다. HDBSQL 클라이언트는 SAP HANA 시스템과 통신하는 데 사용됩니다.

### • 단계 \*

1. SAP 계정에서 HDB 클라이언트 소프트웨어를 다운로드합니다.

확장자가 (.sar)인 아카이브 파일입니다. 예: IMDB\_CLIENT20\_008\_20-80002082.SAR



HDB 클라이언트 소프트웨어 버전은 2.4.202.1590784230 이상이어야 합니다.

2. SAP 계정에서 최신 SAPCAR 유틸리티를 다운로드합니다. 예: \_SAPCAR\_1010-70006178.EXE \_
3. Cloud Manager UI에서 \* Connector \* 를 클릭하여 커넥터 이름을 얻습니다.
4. 예 로그인합니다 "[Microsoft Azure 포털입니다](#)".
5. Virtual Machines \* 를 클릭합니다.
6. Cloud Manager Connector를 검색하고 Connector에 할당된 공용 IP 주소를 복사합니다.

커넥터에 공용 IP가 활성화되어 있지 않으면 점프 호스트를 사용해야 합니다.

7. SAPCAR 유틸리티 및 HDB 클라이언트 아카이브 파일(.sar)을 커넥터 시스템으로 복사합니다.

Connector 경로에 파일을 복사하려면 Connector를 만드는 동안 제공된 키 또는 자격 증명이 필요합니다.

- SCP<SAPCAR\_UTILITY><username>@<ip\_address>:/home/<username>'
- 'sp<hdb\_client\_archive><username>@<ip\_address>:/home/<username>'

파일이 /home/<username>(으)로 복사됩니다.

8. ssh 자격 증명 또는 키를 사용하여 Connector VM에 로그인합니다.
9. Connector VM에서 다음 명령을 실행하여 HDBSQL 클라이언트를 AKS에 설치합니다.
  - a. 'SUDO CP/HOME/<사용자 이름>/<SAPCAR\_UTILITY>/var/lib/docker/volumes/cloudmanager\_snapcenter\_volume/\_data/'
  - b. 'SUDO CP/HOME/<사용자 이름>/<HDB\_Client\_archive>/var/lib/docker/volumes/cloudmanager\_snapcenter\_volume/\_data/'
  - c. 'SUDO Docker Exec - it cloudmanager\_snapcenter/bin/bash/opt/netapp/hdbclient/hdbclient.sh - -archivefile <HDB\_Client\_archive> — archiveutil <SAPCAR\_utility>'

- 자세한 정보 찾기 \*

"SCP를 사용하여 파일을 이동하는 방법"

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.