



# はじめに SnapCenter Service

NetApp  
April 07, 2022

This PDF was generated from <https://docs.netapp.com/ja-jp/cloud-manager-snapcenter/concept-overview-architecture-limitation-functionalities-snapcenter-service.html> on April 07, 2022. Always check docs.netapp.com for the latest.

# 目次

はじめに .....	1
SnapCenter サービスについて .....	1
はじめに .....	3
Connector を作成して SnapCenter サービスを有効にするための前提条件 .....	3
Azure for SnapCenter サービスでコネクタを作成します .....	7
Azure NetApp Files の SnapCenter サービスを有効にします .....	8
HDBSQL クライアントをインストールします .....	12

# はじめに

## SnapCenter サービスについて

SnapCenter サービスは、ネットアップクラウドストレージで実行されているアプリケーションにデータ保護機能を提供します。NetApp Cloud Manager で SnapCenter サービスを有効にすると、Azure NetApp Files 上にある SAP HANA® システムを、アプリケーションと整合性のある方法で効率的にバックアップおよびリストアできます。

### アーキテクチャ

SnapCenter サービスのアーキテクチャには、次のコンポーネントが含まれています。

- SnapCenter サービス UI は、Cloud Manager UI に統合されています。

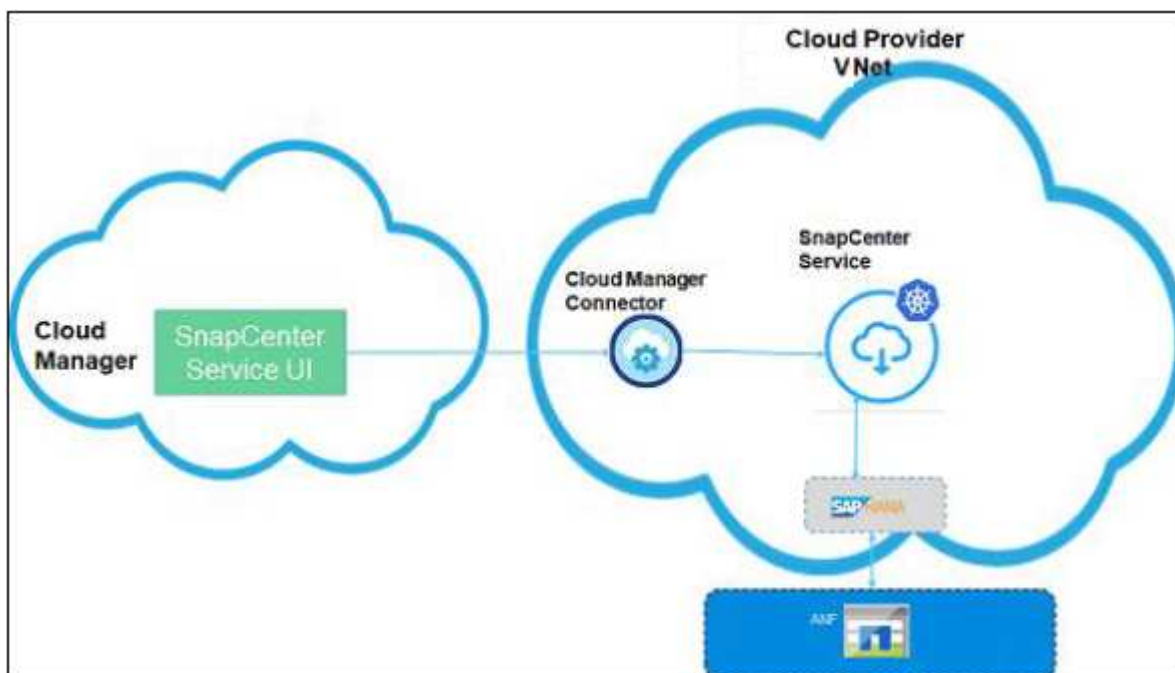
SnapCenter サービス UI は、ネットアップが管理する Cloud Manager SaaS フレームワークから提供されます。このフレームワークでは、複数のストレージ機能とデータ管理機能を利用できます。

- Cloud Manager Connector は、SnapCenter サービスやその他のサービスのライフサイクルを管理する、Cloud Manager のコンポーネントです。
- SnapCenter サービスは、Azure Kubernetes Service (AKS) 上にホストされる一連のデータ保護サービスであり、データ保護ワークフローをオーケストレーションします。



Cloud Manager Connector と SnapCenter サービスは、クラウドネットワークに導入されます。

次の図に、SnapCenter サービスの各コンポーネントの関係を示します。



ユーザが開始した要求については、SnapCenter サービス UI が Cloud Manager SaaS と通信し、要求を検証

すると Cloud Manager Connector にコールが転送されます。その後、Connector は SnapCenter サービスと通信し、SnapCenter サービスは Azure NetApp Files 管理 API と HANA システムコマンドを呼び出してデータ保護処理を実行します。

SnapCenter サービスは、HANA システムと同じ VNet に導入することも、別の VNet に導入することもできます。SnapCenter サービスシステムと HANA システムが異なるネットワークにある場合は、それらのシステム間にネットワーク接続を確立する必要があります。

## サポートされる機能

SnapCenter サービスは次の機能をサポートします。

- SAP HANA システムを追加しています
- SAP HANA システムのバックアップ
  - Snapshot ベースとファイルベースの両方のバックアップをサポートします
  - SAP HANA システムのオンデマンドバックアップをサポートします
  - システム定義のポリシーまたはカスタムポリシーを使用して、SAP HANA システムのスケジュールされたバックアップをサポートします

ポリシーでは、毎時、毎日、毎週、毎月などの異なるスケジュール頻度を指定できます。

- では、非データボリュームとグローバル非データボリュームの両方のバックアップがサポートされます
- ポリシーに基づいてバックアップを保持する
- ユーザ指定のバックアップからの SAP HANA システムのリストア
- バックアップおよびその他のジョブを監視しています
- 不要な HANA システム上のデータやログバックアップのカタログの削除
- 保護の概要、設定の詳細、およびジョブステータスをダッシュボードに表示する
- E メールでアラートを送信する

## 制限

SnapCenter サービス 1.0 には、次の制限事項があります。

- 国際化はサポートされていません。英語のブラウザを使用する必要があります。
- SnapCenter サービスを有効にできるのは、「Account Admin」ロールの Cloud Manager ユーザのみです。
- Azure Kubernetes Service (AKS) クラスタノード障害に関連する制限事項があります
  - AKS クラスタでノードの 1 つがオフラインになると、実行中のジョブは失敗する可能性があります。後続のジョブは実行されます。
  - AKS クラスタでは、ノードの 1 つがダウンした場合に SAP HANA システムを追加できませんが、他の処理は問題なしで実行されます。

HANA システムを追加するには、ノードを起動する必要があります。

- 。スケジューラはハイアベイラビリティ構成をサポートしていません。

スケジューラが使用する MySQL ノードが停止した場合、スケジュールされた処理を続行するにはノードを起動する必要があります。

## はじめに

SnapCenter サービスを利用して、データを保護する手順をいくつか紹介します。

お勧めします ["NetApp Cloud Central に登録"](#)、["Cloud Manager にログインします"](#)をクリックし、を設定します ["ネットアップアカウント"](#)。

SnapCenter サービスを導入できるのは、アカウント管理者だけです。ただし、アカウント管理者と SnapCenter 管理者は、どちらもさまざまな操作を実行できます。 ["詳細はこちら。"](#)

すべてのを確認してください ["前提条件"](#) コネクタを作成して SnapCenter サービスを有効にするには、次の手順を実行します。

お勧めします ["Azure for SnapCenter サービスでコネクタを作成します"](#)。

前提条件をすべて満たすコネクタがある場合は、そのコネクタを使用できます。

Cloud Manager で Azure NetApp Files 作業環境を作成し、ネットアップアカウント、容量プール、ボリューム、Snapshot を作成および管理します。 ["詳細はこちら。"](#)

お勧めします ["SnapCenter サービスを有効にします"](#) Cloud Manager UI を使用 SnapCenter サービスが有効になると、SnapCenter サービスをホストする Azure Kubernetes Service （AKS）クラスタが作成されます。

お勧めします ["HDBSQL クライアントをインストールします"](#) をクリックして、SAP HANA データベースに対してデータ保護処理を実行します。HDBSQL クライアントは、SAP HANA システムとの通信に使用されます。

手動で行う必要があります ["SAP HANA システムを追加します"](#)。

そのあとで、を実行できます ["SAP HANA システムをバックアップ"](#) システム定義またはカスタムのポリシーを使用する。データ損失が発生した場合は、を実行できます ["SAP HANA システムをリストア"](#) そのシステムのバックアップを使用する。

## Connector を作成して SnapCenter サービスを有効にするための前提条件

Azure でコネクタを作成して SnapCenter サービスを有効にする前に、特定のことを確認する必要があります。

- コネクタ用に選択したサブネットが、Azure Kubernetes Service （AKS）用に予約されている 169.254.0/16、172.17.0.0/16、172.17.0.0/16、172.31.0.0/16、および 192.0.2.0/24 の IP アドレス範囲と重複しないようにします。
- 選択したサブネットで AKS が実行されていないことを確認します。
- 選択したサブネットが、それぞれのポート上の SAP HANA システムにアクセスできることを確認しま

す。

- 選択したサブネットの VNet が SAP HANA システムの VNet と異なる場合は、VPN ゲートウェイ、ピアリング、またはその他の手段を使用して VNet が相互に通信できることを確認してください。
- ファイアウォールの背後で SnapCenter サービスを有効にする場合は、に記載されている操作を実行する必要があります [\[Network requirements\]](#)。

ファイアウォールの内側で SnapCenter サービスを有効にするかどうかを事前に決定する必要があります。SnapCenter サービスを有効にすると、ファイアウォールの内側で実行するように設定できなくなります。これは AKS の制限です。

## ネットワーク要件

クラウド環境内のリソースやプロセスをコネクタで管理できるように、ネットワークをセットアップします。

### ファイアウォールの設定

ファイアウォールの背後で SnapCenter サービスを有効にする場合は、次の操作を実行する必要があります。



Azure ファイアウォールを使用している場合は、スクリプトを使用して以下の手順を実行できます。詳細については、を参照してください [\[Azure Firewall configuration\]](#)。

#### • 手順 \*

1. 以下のネットワークルールをファイアウォールに追加します。

デスティネーションエンドポイント	プロトコル	ポート	コメント
"サービスタグ" -AzureCloud.< 地域 >:1194.	UDP	1194	プライベートコネクタとプライベート SnapCenter サービス クラスタを使用する場合は不要です。
"サービスタグ" -AzureCloud .< リージョン >:9000	TCP	9、000	プライベートコネクタとプライベート SnapCenter サービス クラスタを使用する場合は不要です。
FQDN - ntp.ubuntu.com:123	UDP	123	Azure 仮想マシンでの時刻同期に必要です。
"サービスタグ" -AzureCloud.<Region>:443	TCP	443	プライベートコネクタとプライベート SnapCenter サービス クラスタを使用する場合は不要です。

2. 次の FQDN タグとポートの詳細を指定して、ファイアウォールにアプリケーションルールを追加します。

- FQDN タグ - AzureNusesService

▪ HTTPS : 443

3. プロトコルとポートが HTTPS のターゲット FQDN として、以下のエンドポイントを含むアプリケーションルールを追加します。 443

エンドポイント	目的
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Cloud Manager では、ほとんどの Azure リージョンに Cloud Volumes ONTAP を導入して管理できます。
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	Cloud Manager は、Azure Germany リージョンに Cloud Volumes ONTAP を導入して管理できます。
<a href="https://management.usgovcloudapi.net/">https://management.usgovcloudapi.net/</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Cloud Manager は、Azure US GOV リージョンに Cloud Volumes ONTAP を導入して管理できます。
\ <a href="https://api.services.cloud.netpp.com">https://api.services.cloud.netpp.com</a>	NetApp Cloud Central への API 要求を許可します。
\ <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>	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
¥ <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>	コネクタがマニフェスト、テンプレート、および Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできるようにします。
\ <a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a>	Docker を実行しているインフラのコンテナコンポーネントのソフトウェアイメージにアクセスでき、Cloud Manager とのサービス統合のためのソリューションを提供します。
\ <a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	ネットアップが監査レコードからデータをストリーミングできるようにします。
\ <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	ネットアップアカウントを含む Cloud Manager サービスとの通信
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
\ <a href="https://support.netapp.com">https://support.netapp.com</a>	ネットアップ AutoSupport との通信：
\ <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>	システムライセンスとサポート登録を行うためのネットアップとの通信
¥ <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>	ネットアップがサポートの問題のトラブルシューティングに必要な情報を収集できるようにします。
* .blob.core.windows.net	プロキシを使用する場合は HA ペアに必要です。
\ <a href="https://auth0.com">https://auth0.com</a>	Auth0 認証の場合は必須です。
¥ <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>	SnapCenter サービスワークフローエンジンの依存関係を取得します。

エンドポイント	目的
\ <a href="https://exteranl-log.cloudmanager.netapp.com">https://exteranl-log.cloudmanager.netapp.com</a>	通信で Cloud Manager のログリポジトリにログを転送できます。

4. SnapCenter サービスをインストールするサブネットを選択してください。
5. ルートを含むルートテーブルを作成します。
  - サブネットからファイアウォールの内部 IP アドレスにトラフィックを転送します
  - ファイアウォールのパブリック IP アドレスからインターネットにトラフィックを転送します。
6. ルートテーブルをサブネットに接続します。

Cloud Manager Connector のネットワーク要件の詳細については、を参照してください "[コネクタのネットワーク要件](#)"。

## Azure ファイアウォールの設定

Azure ファイアウォールの背後で SnapCenter サービスを有効にする場合は、次の操作を実行する必要があります。

- 必要なもの \*
- ファイアウォールを作成しておく必要があります（クラシックモード）。
- SnapCenter サービス用の VNet とサブネットを作成しておく必要があります。
- ファイアウォールリソースと SnapCenter サービスの VNet が異なるテナントにある場合は、Azure シェルの両方のテナントにログインする必要があります。
- ファイアウォール VNet と SnapCenter VNet が異なる場合は、VNet 間のピアリングを確立する必要があります。
- 手順 \*

1. をダウンロードします "[scs\\_azure\\_firewall\\_config.sh](#)" ローカルシステムにスクリプトをインストールします。
2. にログインします "[Microsoft Azure ポータル](#)"。

3.  をクリックしてクラウドシェルを開き、Bash コンソールを選択します。

- a. スクリプトを Azure クラウドシェルにアップロードします。
- b. スクリプトを実行する権限を割り当てます。

```
chmod +x ./scs_aze_firewall_config.sh
```

- c. スクリプトを実行します。

```
scs_azure_firewall_config.sh -fwsubid <Firewall_SubscriptionID>-fwname <Firewall_name> -fwrg
<Firewall_Resource_group> -scssubid <SnapCenter_Service_SubscriptionID>-scsvnet
<SnapCenter Service_vnet_name> -scssubnet <SnapCenter Service_Subnet_name>
-svnet_sv_group> SnapCenter <sr_net_group>
```





リソースグループを作成していない場合は、リソースグループが作成されます。コネクタの作成時に同じリソースグループを使用すると、SnapCenter サービス関連のリソースをすべて同じリソースグループに含めることができます。

- 結果 \*
- ファイアウォールルールが設定されている。
- SnapCenter サービス用のリソースグループが作成されます。
- SnapCenter サービスリソースグループにルートテーブルが作成されます。
- ルートテーブルルールが設定されます。
- ルートテーブルがサブネットに接続されます。

## HANA システムへの接続

SnapCenter サービスクラスタは、HDBSQL コマンドを使用して、ユーザのネットワーク内の HANA システムと通信する必要があります。SnapCenter クラスタと HANA システム間の通信チャンネルは、次のようなさまざまなネットワークアーキテクチャを使用して許可する必要があります。

- Connector および SnapCenter サービスクラスタは、HANA システムと同じ VNet に導入されます
- Connector および SnapCenter サービスクラスタは、HANA システムのように別の VNet に導入され、2 つの VNet 間の VNet ピアリングを使用して通信が確立されます。
- Connector および SnapCenter サービスクラスタは、HANA システムとして別の VNet に導入され、2 つの VNet 間の VPN ゲートウェイを使用して通信が確立されます。

## セキュリティグループの設定

HANA システムにネットワークセキュリティグループ（NSG）が設定されている場合は、ユーザストアキーで指定されたとおりに、SnapCenter サービスのポートから HANA システムのポートへのインバウンド通信を許可する必要があります。

- Protocol : すべての TCP
- サブネット : SnapCenter AKS クラスタサブネット
- 目的 : HDBSQL コマンドを実行する場合

SnapCenter AKS クラスタで実行されている HANA サービスは、SSL が有効になっている HANA システムとの SSL 通信をサポートします。

## Azure for SnapCenter サービスでコネクタを作成します

Cloud Manager の機能を使用するには、アカウント管理者がコネクタを導入する必要があります。Connector を使用すると、Cloud Manager でパブリッククラウド環境内のリソースとプロセスを管理できます。

デフォルトでは、Azure Marketplace から Connector を作成できます。の手順を実行しているとき ["Azure Marketplace からコネクタを作成します"](#)では、次の点に注意してください。

- Cloud Manager for Cloud Volumes ONTAP が指定されている場合は、SnapCenter サービスにも同じ機能

を利用できます。

- Cloud Manager Name に、よりわかりやすいようにコネクタ VM の名前を指定します。これは、Cloud Manager UI にコネクタ名として表示されます。
- パブリック IP なしでコネクタを設定した場合、またはファイアウォールを設定した場合は、コネクタマシンに接続するジャンプホストが必要です。

ある場合 ["ユーザーの同意"](#) Azure Active Directory で有効にするか、テナント管理者から同意を得られる場合は、Cloud Manager UI からコネクタを作成できます。

## ユーザー同意が有効になっています

Azure Active Directory でユーザの同意が有効になっている場合は、["Cloud Manager からコネクタを作成します"](#)。

## ユーザーの同意が無効になっています

1. 次のいずれかを実行します。

- 管理者の同意ワークフローが Active Directory で設定されている場合は、次の手順を実行します ["管理者の同意を要求します"](#)。
- 管理者の同意ワークフローが設定されていない場合は、次の操作を実行します。
  - i. ["テナント全体の管理者の同意を得るための URL を作成します"](#)。



clientID に `989efff4-9a9e-46fa-9f17-de39e15714f9` を指定します。これは、Cloud Manager ウィザードで指定された Cloud Manager Azure アプリケーション ID です。

- ii. ブラウザで URL を実行し、同意を得るようにテナント管理者に依頼します。

表示されたエラーは管理者が無視できます

2. ["Cloud Manager からコネクタを作成します"](#)。



コンピュータに接続するには、コネクタの作成時に入力したユーザ名とパスワード、またはキーが必要です

## Azure NetApp Files の SnapCenter サービスを有効にします

SnapCenter サービスは、Cloud Manager の UI を使用して有効にできます。SnapCenter サービスが有効になると、SnapCenter サービスをホストする Azure Kubernetes Service (AKS) クラスタが作成されます。

- 必要なもの \*
- 「microsoft.ContainerService」リソースプロバイダを Azure サブスクリプションに登録する必要があります。詳細については、[を参照してください](#) ["リソースプロバイダの登録方法"](#)。
- すべてのを確認してください ["前提条件"](#) 達成された。

- このタスクについて \*

AKS クラスタは、コネクタの作成時に選択した同じリソースグループと同じサブネット内に作成されます。パブリック IP アドレスを指定せずにコネクタを作成すると、プライベートモードで AKS クラスタが作成されます。

AKS クラスタを作成および管理するには、必要な権限を持つユーザが割り当てられた管理対象 ID が必要です。ユーザーが割り当てた管理対象 ID が作成され、Connector VM に割り当てられます。

- 手順 \*

1. Cloud Manager にログインします
2. Cloud Manager で作成したコネクタを選択します。

保護する SAP HANA システムへのネットワーク接続がコネクタにあることを確認します。

3. [すべてのサービス > \*SnapCenter \* > \*Enable] をクリックします。
4. 次のいずれかを実行します。

- Cloud Manager UI からコネクタを作成しており、ロールの作成と割り当てを行う権限がある場合は、ユーザに割り当てられた管理対象 ID が SnapCenter サービスのインストール時に自動的に作成されます。

- i. 「\* Azure ログインを使用 \*」を選択します。
- ii. [準備完了] ページで、[\* 続行] をクリックします。
- iii. Azure クレデンシャルを指定します。





Azure のログインアカウントに十分な権限があることを確認してください。権限および権限の割り当て方法については、を参照してください [\[Permissions required for Azure login account\]](#)。

- Azure Marketplace で作成したコネクタ、またはロールを作成して割り当てる権限がない場合は、次の手順に従って、ユーザが割り当てた管理対象 ID を作成します。

- i. 「\* Azure CLI スクリプトを使用 \*」を選択します。
- ii. Azure アカウントに対する十分な権限がない場合は、管理者にお問い合わせください。

権限および権限の割り当て方法については、を参照してください [\[Permissions required for Azure login account\]](#)。

- iii. をダウンロードします ["prerequisite\\_azure.sh"](#) ローカルシステムにスクリプトをインストールします。
- iv. にログインします ["Microsoft Azure ポータル"](#)。
- v.  をクリックします  をクリックしてクラウドシェルを開き、Bash コンソールを選択します。
- vi. スクリプトを Azure クラウドシェルにアップロードします。
- vii. スクリプトを実行する権限を割り当てます。

```
chmod +x./利用 前提条件 _azure.sh
```

viii. スクリプトを実行します。

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

5. クラスタ構成ページで、次の手順を実行します。

a. クラスタ構成を選択

- High Availability \* を選択すると、3 つのワーカーノードを含む Azure Kubernetes Service (AKS) クラスタが使用可能なゾーン全体に作成されます。
- Single Node \* を選択すると、シングルノードの AKS クラスタが作成されます。

b. Kubernetes ポッドのアドレス範囲を指定します。

Kubernetes ポッドのアドレス範囲が、仮想ネットワーク、ピア関係にある仮想ネットワーク、接続されているオンプレミスネットワークの IP 範囲と重複しないようにします。また、範囲はサービスアドレス範囲および Docker ブリッジアドレスと重複しないようにしてください。

c. Kubernetes Service のアドレスを指定します。

Kubernetes サービスのアドレス範囲が、仮想ネットワーク、ピア関係にある仮想ネットワーク、および接続されているオンプレミスネットワークの IP 範囲と重複しないようにします。また、範囲はポッドのアドレス範囲および Docker ブリッジアドレスと重複しないようにします。

d. Docker ブリッジネットワークを指定します。

Docker Bridge アドレスが、仮想ネットワーク、ピア関係にある仮想ネットワーク、および接続されているオンプレミスネットワークの IP 範囲と重複しないようにします。また、範囲が Pod のアドレス範囲およびサービスアドレス範囲と重複しないようにしてください。

e. パブリック IP を使用せずにコネクタを作成し、VNet でカスタム DNS サーバを使用している場合は、「\* カスタム DNS サーバのサポート \*」を選択します。




カスタム DNS サーバがホストされている VNet のプライベート DNS ゾーンに仮想ネットワークリンクを作成する必要があります。プライベート DNS ゾーン名とリソースグループ名が UI に表示されます。

6. [ レビュー ] ページで詳細を確認し、[ 有効にする ] をクリックします。

7. SnapCenter サービスを正常に有効にしたら、[\* 終了 \*] をクリックします。

• 結果 \*

• SnapCenter サービスを有効にすると、AKS クラスタが作成されます。をクリックすると、AKS クラスタの詳細を表示できます 。



SnapCenter サービスを有効にできなかった場合は、問題を修正して [\* 再試行 \*] をクリックします。

• ユーザーに割り当てられた管理対象 ID を作成すると、カスタムロールに割り当てられます。

- ユーザーに割り当てられた管理対象 ID は 'コネクタリソースグループの範囲' で以下の権限を持つカスタムロールに割り当てられます

```
"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"
```

- ユーザーが割り当てた管理対象 ID は、コネクタの VNet の範囲で以下の権限を持つカスタムロールに割り当てられます。

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

- ファイアウォールにルーティングするためにサブネット上にルートテーブルが設定されている場合、ユーザーに割り当てられた管理対象 ID は、ルートテーブルの範囲で次の権限を持つカスタムロールに割り当てられます。

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

- コネクタがパブリック IP なしでインストールされている場合、ユーザーが割り当てた管理対象 ID は、プライベート DNS ゾーンの範囲で以下の権限を持つカスタムロールに割り当てられます。

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

## Azure のログインアカウントには権限が必要です

Azure ログインアカウントは、ユーザーが割り当てた管理対象 ID、必要なロールを作成し、その ID を Connector VM に割り当てるために使用されます。



ログインアカウントのクレデンシャルは SnapCenter サービス内のどこにも保存されず、API の呼び出しには使用されません。クレデンシャルは、UI でのみ使用されます。

• 手順 \*

1. を使用して、カスタムロールを作成します ["SnapCenter の導入 \\_ ロール 1.json"](#) ファイル。

SnapCenter\_Deployment\_Role1.json ファイルの <Subscription\_ID> を、Azure サブスクリプション ID に置き換える必要があります。

2. コネクタのリソースグループの範囲で、ロールをログインアカウントに割り当てます。
3. を使用して、カスタムロールを作成します ["SnapCenter の導入 \\_ ロール 2.json"](#) ファイル。

SnapCenter\_Deployment\_Role2.json ファイルの <Subscription\_ID> を、Azure サブスクリプション ID に置き換える必要があります。

4. コネクタの VNet 以降の範囲でログインアカウントにロールを割り当てます。
5. ある場合 ["ファイアウォールを設定しました"](#)を使用して、カスタムロールを作成します ["SnapCenter - 導入 - Role3.json"](#) ファイル。

SnapCenter\_Deployment\_Role3.json ファイルの <Subscription\_ID> を Azure サブスクリプション ID に置き換える必要があります。

6. SnapCenter サブネットに関連付けられているルートテーブルの範囲で、ロールをログインアカウントに割り当てます。

## HDBSQL クライアントをインストールします

SnapCenter サービスを有効にしたあと、SAP HANA データベースに対してデータ保護処理を実行する HDBSQL クライアントをインストールします。HDBSQL クライアントは、SAP HANA システムとの通信に使用されます。

• 手順 \*

1. SAP アカウントから HDB クライアントソフトウェアをダウンロードします。

拡張子（.sar）を持つアーカイブファイルです。例：IMDB\_CLIENT20\_008\_20-80002082.sar



HDB Client ソフトウェアのバージョンは 2.4.202.1590784230 以降である必要があります。

2. SAP アカウントから最新の SAPCAR ユーティリティをダウンロードします。例：SAPCAR\_1010-70006178.EXE
3. Cloud Manager UI で、\* Connector \* をクリックしてコネクタ名を取得します。
4. にログインします ["Microsoft Azure ポータル"](#)。
5. 仮想マシン \* をクリックします。
6. Cloud Manager Connector を検索し、コネクタに割り当てられているパブリック IP アドレスをコピーします。

コネクタでパブリック IP が有効になっていない場合は、ジャンプホストを使用する必要があります。

7. SAPCAR ユーティリティと HDB クライアントアーカイブ（.sar）ファイルをコネクタマシンにコピーします。

コネクタパスにファイルをコピーするには、クレデンシャル、またはコネクタの作成時に指定したキーが必要です。

- 'cp <SAPCAR\_utility><username>@<IP\_address> : /home/<username>`
- 'cp <HDB\_Client\_archive><username>@<IP\_address> : /home/<username>`

ファイルは /home/<username> にコピーされます。

8. SSH のクレデンシャルまたはキーを使用して Connector VM にログインします。
9. Connector VM で次のコマンドを実行して、HDBSQL クライアントを AKS にインストールします。
  - a. 'UDO cp /home/<username>/<SAPCAR\_utility>/var/lib/docker/volumes/cloudmanager\_snapcenter/volume/\_data/'
  - b. 'UDO cp  
/home/<username>/<HDB\_Client\_archive>/var/lib/docx/volumes/cloudmanager\_snapcenter/volume/\_data/'
  - c. 'sudo docker exec-it cloudmanager\_snapcenter /bash/opt/NetApp/hdbclient/hdbclient.sh  
--archivefile <HDB\_Client\_archive> --archiveTESAR\_utility>`

• 詳細はこちら \*

["SCP を使用してファイルを移動する方法"](#)



## 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.