# 要件
## Kubernetes clusters

NetApp
July 19, 2022

# 目次

# 要件

## Azure での Kubernetes クラスタの要件

Cloud Manager を使用して、 Azure で管理対象 Azure Kubernetes クラスタ（ AKS ）と自己管理型 Kubernetes クラスタを追加および管理できます。Cloud Manager にクラスタを追加する前に、次の要件を満たしていることを確認してください。

このトピックでは、 _Kubernetes cluster_where configuration is the same for AKS and selfmanaged Kubernetes clusters を使用します。クラスタタイプは設定が異なる場所で指定します。

### 要件

**Astra Trident**

最新バージョンの 4 つの Astra Trident が必要です。Trident は Cloud Manager から直接インストールできます。お勧めします "前提条件を確認します" Astra Trident をインストールする前に、

Astra Trident をアップグレードするには、 "オペレータにアップグレードしてください"。

**Cloud Volumes ONTAP**

クラスタのバックエンドストレージとして Cloud Volumes ONTAP が設定されている必要があります。 "設定手順については、 Astra Trident のドキュメントを参照してください"。

**Cloud Manager Connector** の略

必要な権限を持つコネクタが Azure で実行されている必要があります。 詳細は以下をご覧ください。

ネットワーク接続

Kubernetes クラスタとコネクタの間、および Kubernetes クラスタと Cloud Volumes ONTAP の間にはネットワーク接続が必要です。 詳細は以下をご覧ください。

**RBAC** 許可

Cloud Manager は、 Active Directory を使用するかどうかに関係なく、 RBAC 対応のクラスタをサポートします。Cloud Manager Connector ロールは、各 Azure クラスタで許可されている必要があります。 詳細は以下をご覧ください。

### コネクタを準備します

Kubernetes クラスタを検出および管理するには、 Azure で Cloud Manager Connector を使用する必要があります。新しいコネクターを作成するか、必要な権限を持つ既存のコネクターを使用する必要があります。

新しいコネクターを作成します

次のリンクのいずれかの手順に従います。

- "Cloud Manager からコネクタを作成します" （推奨）
- "Azure Marketplace からコネクタを作成します"

- "既存の Linux ホストにコネクタをインストールします"

既存のコネクタに必要な権限を追加する（管理対象の **AKS** クラスタを検出する）

管理対象の AKS クラスタを検出するには、コネクタのカスタムロールを変更して権限を提供しなければならない場合があります。

手順

1. Connector 仮想マシンに割り当てられているロールを特定します。
   a. Azure ポータルで、仮想マシンサービスを開きます。
   b. Connector 仮想マシンを選択します。
   c. [ 設定 ] で、 [**Identity**] を選択します。
   d. Azure の役割の割り当て * をクリックします。
   e. Connector 仮想マシンに割り当てられているカスタムロールをメモしておきます。
2. カスタムロールを更新します。
   a. Azure ポータルで、 Azure サブスクリプションを開きます。
   b. [* アクセス制御（ IAM ） ]>[ 役割 * ] をクリックします。
   c. カスタムロールの省略記号 (...) をクリックし、 * 編集 * をクリックします。
   d. JSON をクリックして、次の権限を追加します。

```
"Microsoft.ContainerService/managedClusters/listClusterUserCredential
/action"
"Microsoft.ContainerService/managedClusters/read"
```

   e. [ * Review + update * ] をクリックし、 [ * Update * ] をクリックします。

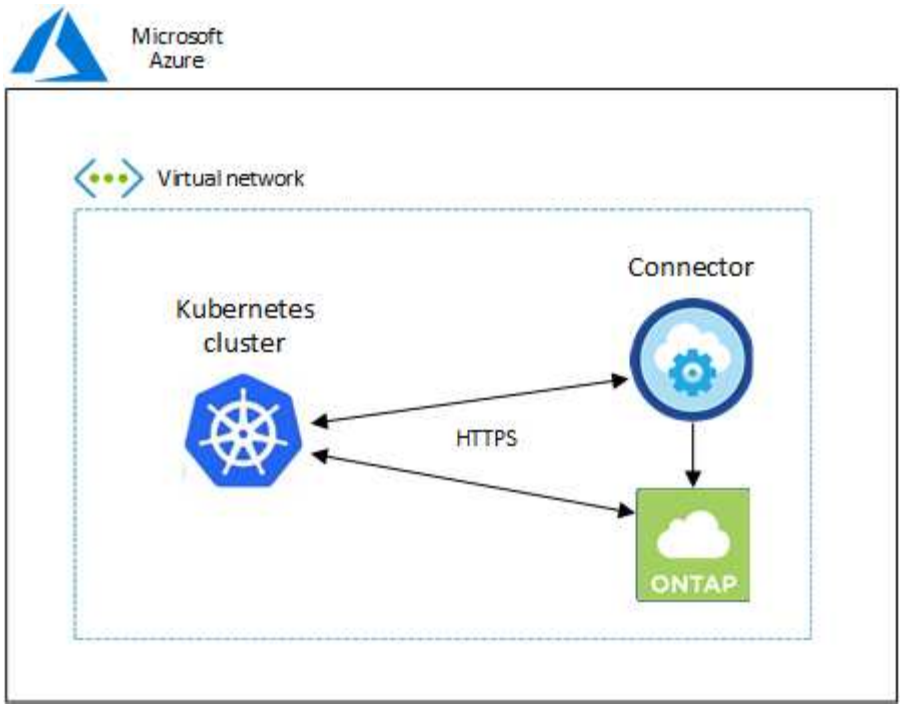
## ネットワーク要件を確認します

Kubernetes クラスタとコネクタの間、および Kubernetes クラスタとクラスタにバックエンドストレージを提供する Cloud Volumes ONTAP システムとの間にネットワーク接続を提供する必要があります。

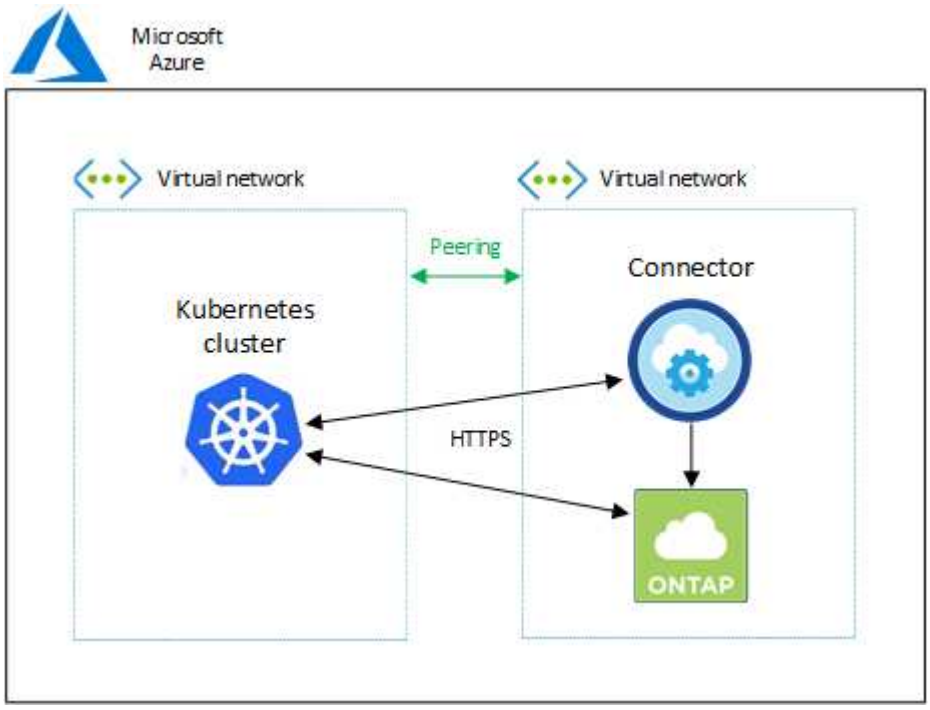
- 各 Kubernetes クラスタがコネクタからインバウンド接続を確立している必要があります
- コネクタには、ポート 443 経由で各 Kubernetes クラスタへのアウトバウンド接続が必要です

この接続を確立する最も簡単な方法は、 Kubernetes クラスタと同じ VNet にコネクタと Cloud Volumes ONTAP を導入することです。それ以外の場合は、異なる VNet 間のピアリング接続を設定する必要があります。

以下は、同じ VNet 内の各コンポーネントの例です。




別の VNet で実行される Kubernetes クラスタの例を次に示します。この例では、ピアリングによって Kubernetes クラスタの VNet とコネクタおよび Cloud Volumes ONTAP の VNet 間の接続が確立されます。




## RBAC 許可をセットアップします

RBAC の検証は、 Active Directory （ AD ）が有効になっている Kubernetes クラスタでのみ実行されます。AD を使用しない Kubernetes クラスタは、検証に自動的に合格します。

コネクタがクラスタを検出して管理できるように、各 Kubernetes クラスタで Connector ロールを承認する必要があります。

バックアップとリストア

バックアップとリストアに必要なのは、基本的な許可だけです。

ストレージクラスを追加する

Cloud Manager を使用してストレージクラスを追加するには、拡張された許可が必要です。

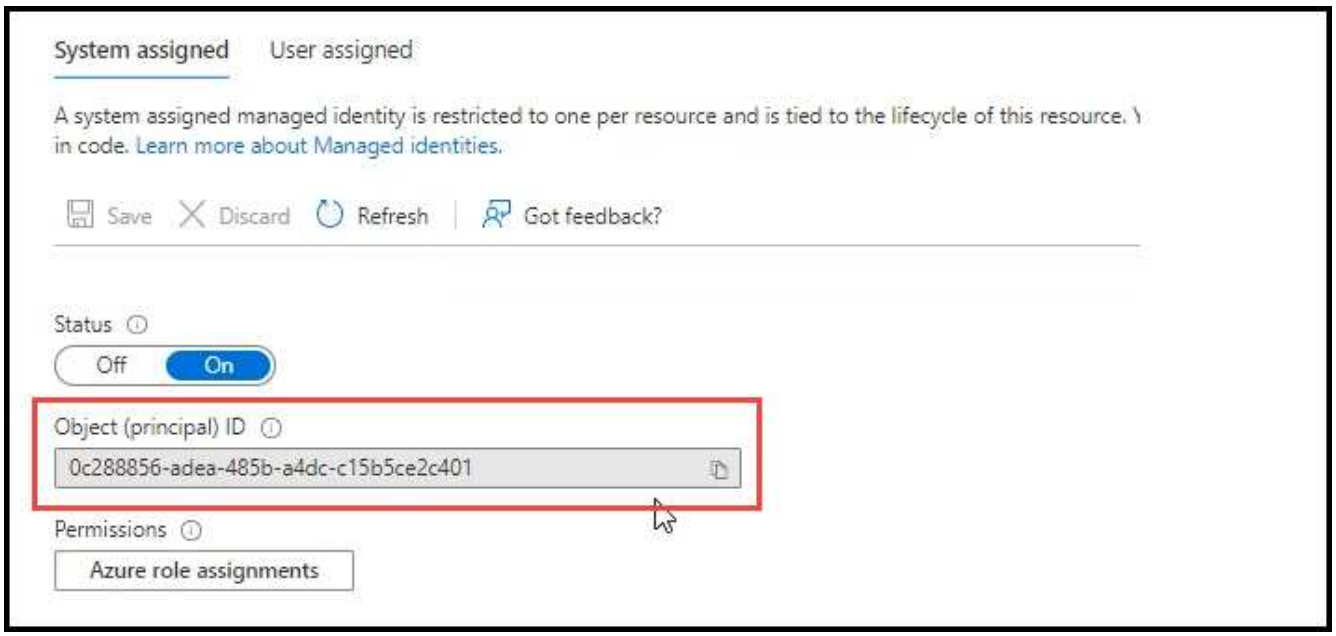
**Astra Trident** をインストールします

Cloud Manager が Astra Trident をインストールするための完全な権限を付与する必要があります。

Astra Trident をインストールすると、 Cloud Manager は Astra Trident バックエンドと、 Astra Trident がストレージクラスタと通信するために必要なクレデンシャルを含む Kubernetes シークレットをインストールします。

RBAC のサブジェクト名 : name:` の構成は、 Kubernetes クラスタのタイプによって若干異なります。

- 管理対象 AKS クラスタ * を導入する場合、コネクターにシステムが割り当てた管理 ID のオブジェクト ID が必要です。この ID は Azure 管理ポータルで入手できます。




- 自己管理型の Kubernetes クラスタ * を導入する場合は、許可されたユーザのユーザ名が必要です。

クラスタロールとロールバインドを作成します。

1. 許可要件に基づいて次のテキストを含む YAML ファイルを作成します。「 Subjects:kind 」変数をユーザ名に置き換え、「 Subjects:user:` 」をシステムに割り当てられた管理対象 ID のオブジェクト ID または上記の権限を持つユーザのユーザ名に置き換えます。

バックアップ / リストア

Kubernetes クラスタのバックアップとリストアを有効にするための基本的な許可を追加する。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
        - ''
      resources:
        - namespaces
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumes
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - pods
        - pods/exec
      verbs:
        - get
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumeclaims
      verbs:
        - list
        - create
    - apiGroups:
        - storage.k8s.io
      resources:
        - storageclasses
      verbs:
        - list
    - apiGroups:
        - trident.netapp.io
      resources:
        - tridentbackends
```

```
      verbs:
          - list
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentorchestrators
      verbs:
          - get
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

ストレージクラス

拡張された権限を追加し、 Cloud Manager を使用してストレージクラスを追加します。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
          - ''
      resources:
          - secrets
          - namespaces
          - persistentvolumeclaims
          - persistentvolumes
          - pods
          - pods/exec
      verbs:
          - get
          - list
          - create
          - delete
    - apiGroups:
```

```
            - storage.k8s.io
        resources:
            - storageclasses
        verbs:
            - get
            - create
            - list
            - delete
            - patch
    - apiGroups:
            - trident.netapp.io
        resources:
            - tridentbackends
            - tridentorchestrators
            - tridentbackendconfigs
        verbs:
            - get
            - list
            - create
            - delete
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

**Trident** をインストール

コマンドラインを使用して完全な権限を付与し、 Cloud Manager が Astra Trident をインストールできるようにします。

```
kubectl create clusterrolebinding test --clusterrole cluster-admin
--user <Object (principal) ID>
```

2. クラスタに構成を適用します。

```
kubectl apply -f <file-name>
```

## 著作権情報



## 商標情報