



要件 Kubernetes clusters

NetApp
June 06, 2022

目次

要件	1
Google Cloud の Kubernetes クラスタの要件	1

要件

Google Cloud の Kubernetes クラスタの要件

Cloud Manager を使用して、Google で管理対象 Google Kubernetes Engine (GKE) クラスタと自己管理型 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 構成は、GKE クラスタと自己管理型 Kubernetes クラスタで同じです。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

Cloud Volumes ONTAP は、Kubernetes クラスタと同じテナンシーアカウント、ワークスペース、コネクタで Cloud Manager に配置する必要があります。["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 Connector が Google 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 GKE 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、Google の Cloud Manager Connector が必要です。新しいコネクタを作成するか、必要な権限を持つ既存のコネクタを使用する必要があります。

新しいコネクタを作成します

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)
- ["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 **GKE** クラスタを検出するため）

管理対象 GKE クラスタを検出する場合は、コネクタのカスタムロールを変更して権限を付与する必要があります。

手順

1. インチ "[Cloud Console の略](#)"をクリックし、* Roles * ページに移動します。
2. ページ上部のドロップダウンリストを使用して、編集するロールを含むプロジェクトまたは組織を選択します。
3. カスタムロールをクリックします。
4. 役割の権限を更新するには、* 役割の編集 * をクリックします。
5. [権限の追加 *] をクリックして、次の新しい権限を役割に追加します。

```
container.clusters.get  
container.clusters.list
```

6. [更新（Update）] をクリックして、編集したロールを保存する。

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する必要があります
- 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 VPC 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 VPC 間にピア接続を設定する必要があります。

以下は、同じ VPC 内の各コンポーネントの例です。



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。

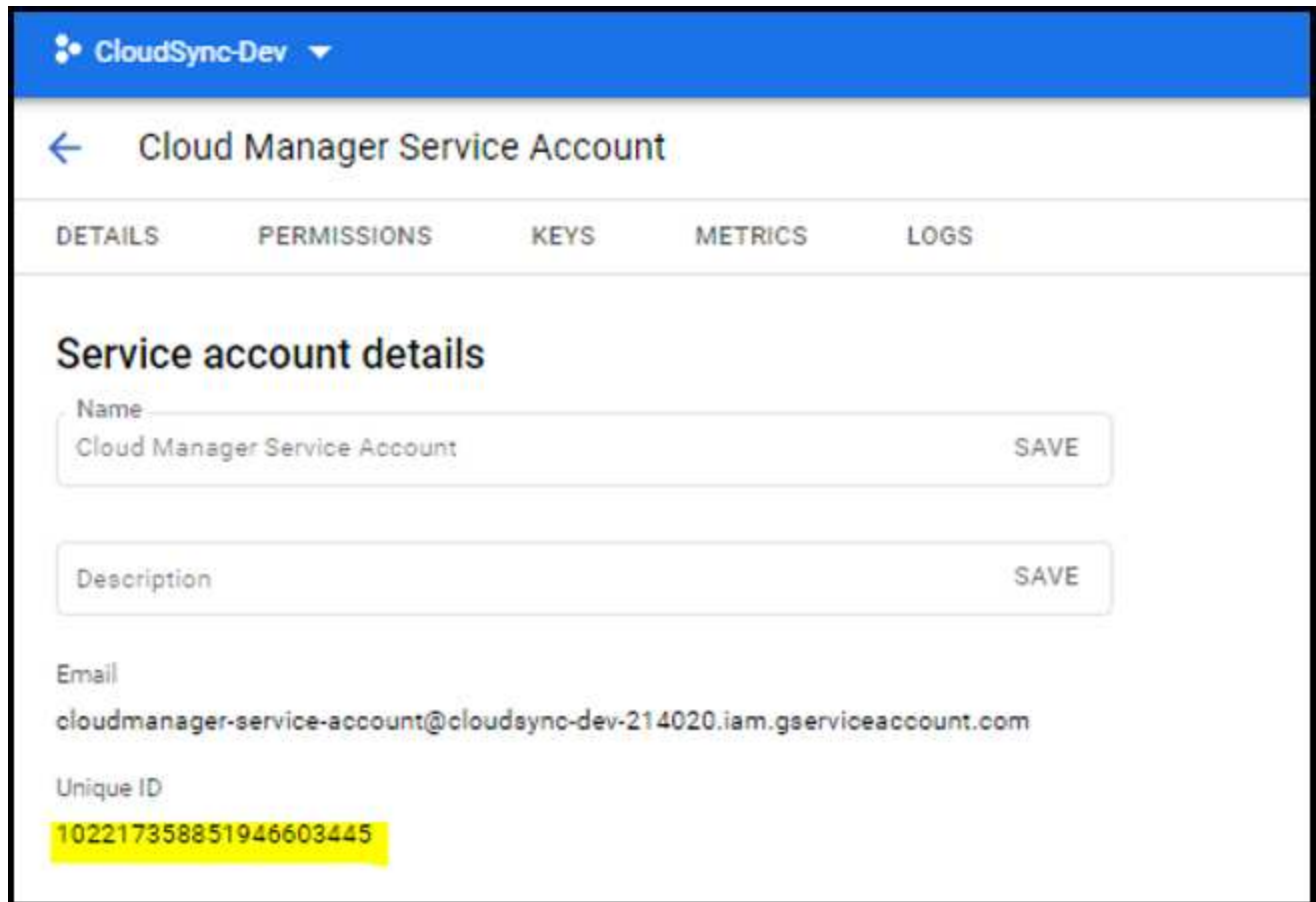
YAML ファイルで「Subjects:name:」を設定するには、Cloud Manager の一意の ID を知っている必要があります。

一意の ID は、次の 2 つの方法のいずれかで確認できます。

- コマンドを使用します。

```
gcloud iam service-accounts list
gcloud iam service-accounts describe <service-account-email>
```

- のサービスアカウントの詳細で確認します "[Cloud Console の略](#)".



クラスター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」変数をユーザー名に置き換え、「Subjects:user:」を認証されたサービスアカウントの一意の ID 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 <Unique 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

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、またはその他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1 つ以上の米国特許、その他の国の特許、および出願中の特許により特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> は、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。