



Kubernetes のドキュメント

Kubernetes clusters

NetApp
April 01, 2022

目次

Kubernetes のドキュメント	1
Cloud Manager の Kubernetes の新機能	2
2022 年 2 月 27 日	2
2022 年 1 月 11 日	2
2021 年 11 月 28 日	2
はじめに	3
Kubernetes の概要	3
要件	4
AWS での Kubernetes クラスタの要件	4
Azure での Kubernetes クラスタの要件	10
Google Cloud の Kubernetes クラスタの要件	15
Kubernetes クラスタを追加	21
Cloud Manager に Amazon Kubernetes クラスタを追加	21
Azure Kubernetes クラスタを Cloud Manager に追加	23
Cloud Manager に Google Cloud Kubernetes クラスタを追加	26
ネットアップのクラウドデータサービスを Kubernetes クラスタで使用できます	31
知識とサポート	32
サポートに登録します	32
ヘルプを表示します	32
法的通知	33

Kubernetes のドキュメント

Cloud Manager の Kubernetes の新機能

Cloud Manager の Kubernetes の新機能をご確認ください。

2022 年 2 月 27 日

Google Cloud で Kubernetes クラスタがサポートされます

Cloud Manager を使用して、Google Cloud 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るようになりました。

"[Google Cloud で Kubernetes クラスタを使用する方法をご確認ください](#)。"

2022 年 1 月 11 日

Azure で Kubernetes クラスタがサポートされます

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るようになりました。

"[Azure での Kubernetes クラスタの使用の開始](#)"

2021 年 11 月 28 日

AWS での Kubernetes クラスタのサポート

高度なデータ管理のために、管理対象 Kubernetes クラスタを Cloud Manager のキャンバスに追加できるようになりました。

- Amazon EKS クラスタを検出します
- Cloud Backup を使用して永続ボリュームをバックアップする

"[Kubernetes のサポートの詳細については、こちらをご覧ください](#)。"



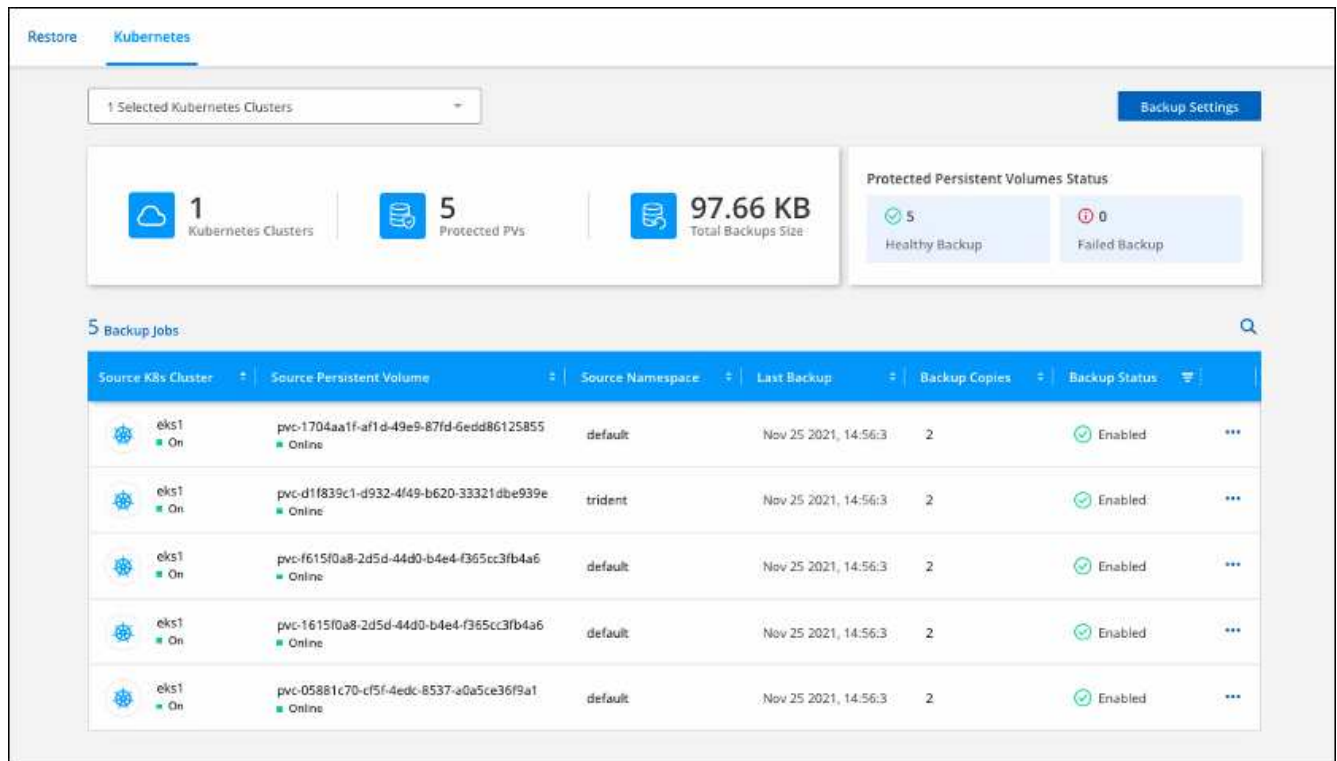
既存の Kubernetes サービス（* K8s * タブで利用可能）は廃止され、今後のリリースで削除される予定です。

はじめに

Kubernetes の概要

高度なデータ管理のために、マネージド Kubernetes クラスタを Cloud Manager に追加の機能

- キャンバスにクラスタを追加して、ハイブリッドクラウドインフラストラクチャの一部として表示および管理します
- Cloud Backup Service を使用して永続ボリュームをバックアップする



サポートされる Kubernetes 環境

Cloud Manager は、Amazon Elastic Kubernetes Service（Amazon EKS）および Microsoft Azure Kubernetes Service（AKS）で実行されているマネージド Kubernetes クラスタをサポートします。

サポートされるバックエンドストレージ

ネットアップの Astra Trident は各 Kubernetes クラスタにインストールする必要があり、Cloud Volumes ONTAP はクラスタのバックエンドストレージとして設定する必要があります。

コスト

Cloud Manager で Kubernetes クラスタを検出する際に料金は発生しませんが、Cloud Backup Service を使用して永続ボリュームをバックアップした場合に料金が発生します。

要件

AWS での Kubernetes クラスタの要件

AWS 上の管理対象の Amazon Elastic Kubernetes Service (EKS) クラスタまたは自己管理型の Kubernetes クラスタを Cloud Manager に追加できます。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する必要があります。

このトピックでは、_Kubernetes cluster_where configuration is the same for EKS 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

Kubernetes クラスタには、NetApp Astra Trident がインストールされている必要があります。最新バージョンの 4 つの Astra Trident が必要です。"[インストール手順については、Astra Trident のドキュメントを参照](#)"。

Cloud Volumes ONTAP

Cloud Volumes ONTAP for AWS は、クラスタのバックエンドストレージとしてセットアップ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

必要な権限を持つコネクタが AWS 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 Connector ロールは、各 Kubernetes 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、AWS で Cloud Manager Connector を使用する必要があります。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。

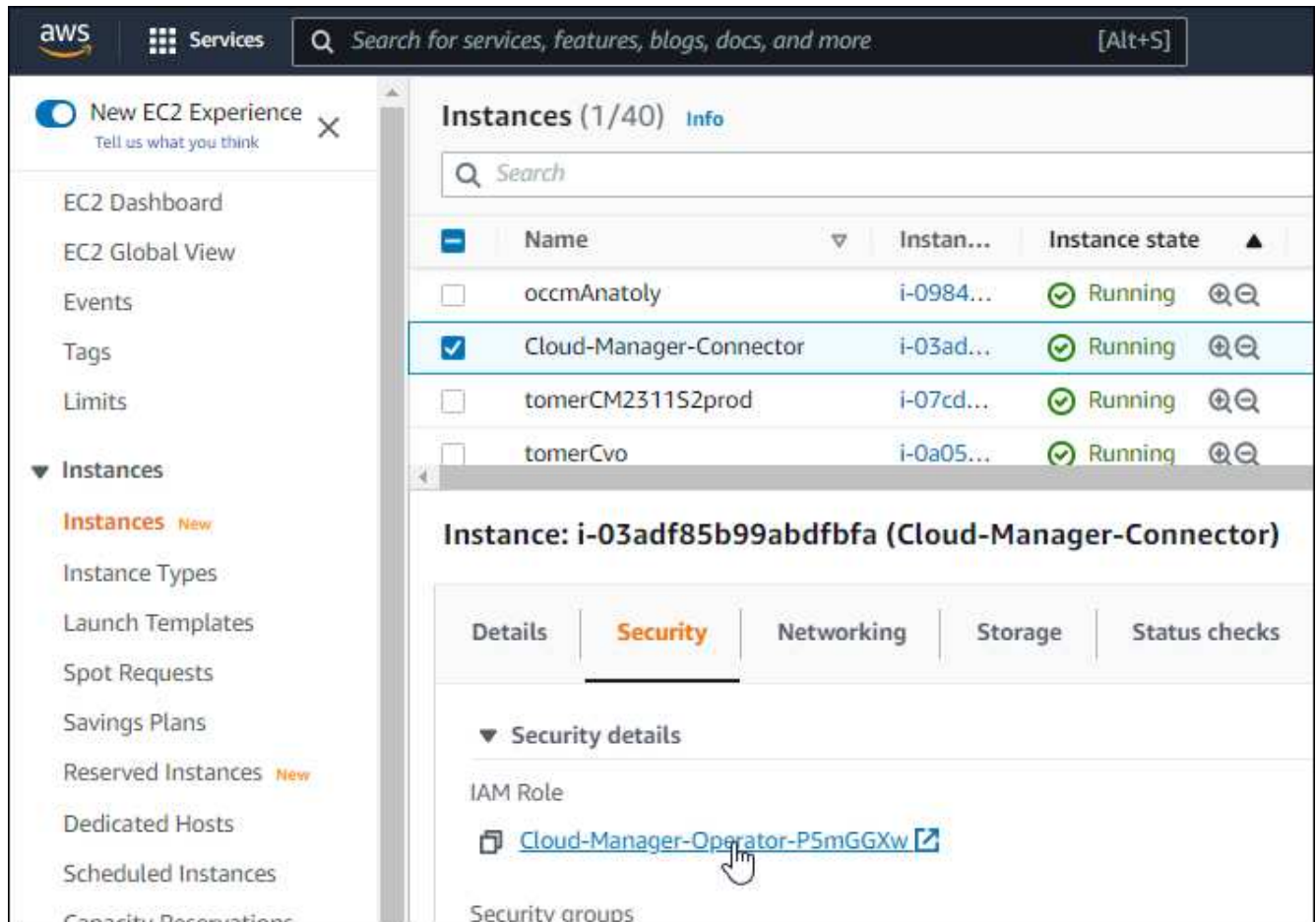
- "[Cloud Manager からコネクタを作成します](#)" (推奨)
- "[AWS Marketplace からコネクタを作成します](#)"
- "[AWS の既存の Linux ホストにコネクタをインストールします](#)"

必要な権限を既存のコネクタに追加します

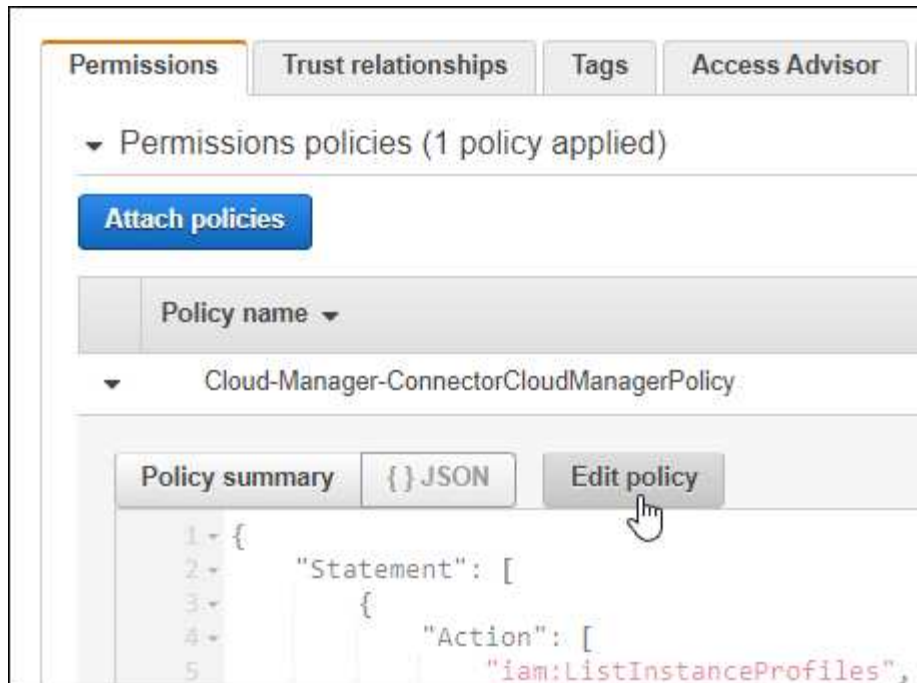
3.9.13 リリース以降、new_newly で作成されたコネクタには、Kubernetes クラスタの検出と管理を可能にする新しい AWS 権限が 3 つ含まれています。このリリースよりも前のリリースでコネクタを作成していた場合は、権限を付与するために、コネクタの IAM ロールの既存のポリシーを変更する必要があります。

手順

1. AWS コンソールにアクセスして EC2 サービスを開きます。
2. コネクタインスタンスを選択し、* セキュリティ * をクリックして、IAM ロールの名前をクリックし、IAM サービスでロールを表示します。



3. [* アクセス許可 *] タブで、ポリシーを展開し、[* ポリシーの編集 *] をクリックします。



4. JSON * をクリックして、最初のアクションセットに次の権限を追加します。

```
"eks:ListClusters",  
"eks:DescribeCluster",  
"iam:GetInstanceProfile"
```

"ポリシーの完全な JSON 形式を表示します"。

5. [ポリシーの確認] をクリックし、[変更の保存] をクリックします。

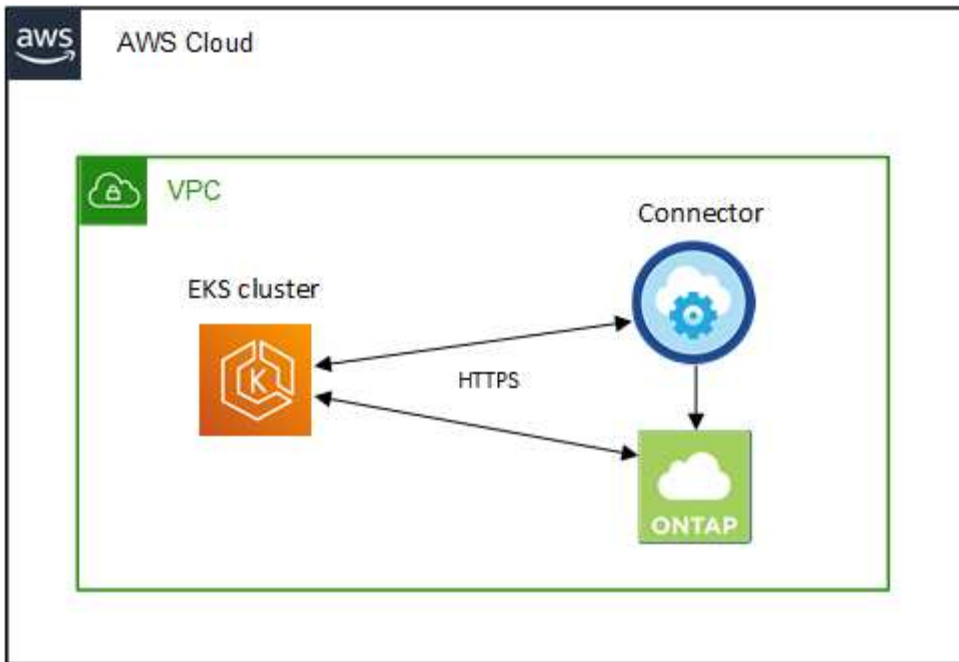
ネットワーク要件を確認します

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。

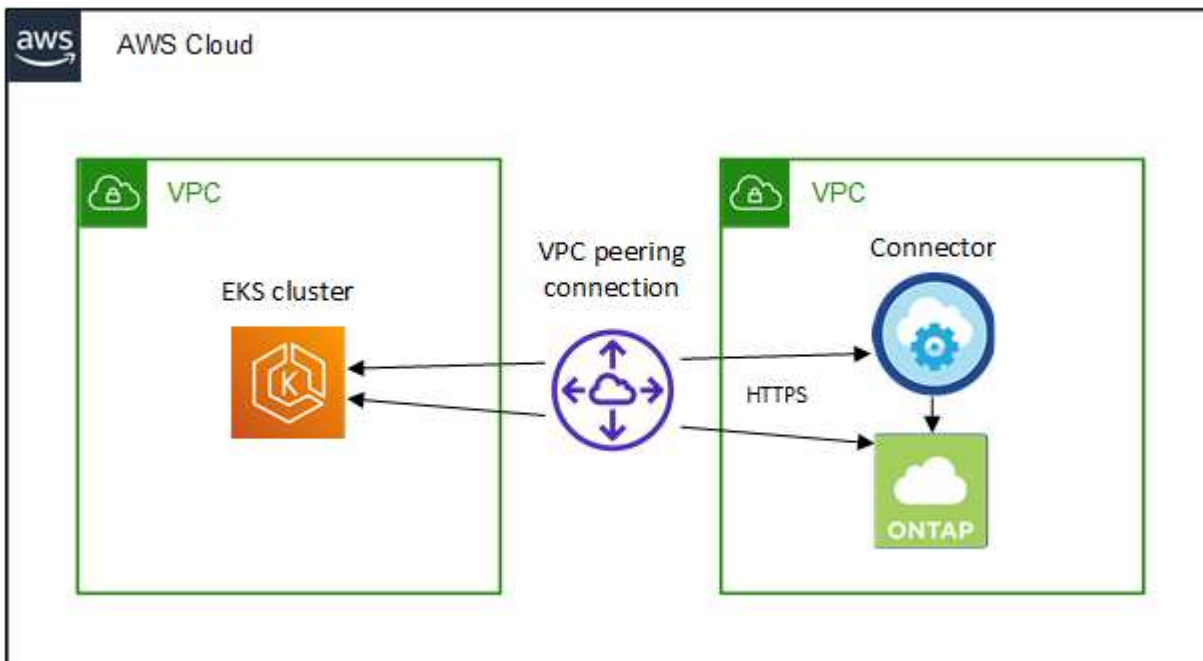
- 各 Kubernetes クラスタがコネクタからインバウンド接続を確立している必要があります
- コネクタには、ポート 443 経由で各 Kubernetes クラスタへのアウトバウンド接続が必要です

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 VPC にコネクタと Cloud Volumes ONTAP を導入することです。VPC が確立されていない場合は、VPC 間に VPC ピアリング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。



別の VPC で実行されている EKS クラスターを次に示します。この例では、VPC ピアリングによって、EKS クラスターの VPC とコネクタおよび Cloud Volumes ONTAP の VPC 間の接続が確立されます。



RBAC 許可をセットアップします

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

手順

1. クラスターロールとロールバインドを作成します。
 - a. 次のテキストを含む YAML ファイルを作成します。

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - secrets
      - namespaces
      - persistentvolumeclaims
      - persistentvolumes
    verbs:
      - get
      - list
      - create
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - list
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
    verbs:
      - get
      - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: Group
    name: cloudmanager-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```

- b. クラスタに構成を適用します。

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

2. 権限グループへの ID マッピングを作成します。

eksctl を使用します

eksctl を使用して、クラスタと Cloud Manager Connector 用の IAM ロールの間に IAM ID マッピングを作成します。

"[eksctl のマニュアルを参照してください](#)".

以下に例を示します。

```
eksctl create iamidentitymapping --cluster <eksCluster> --region  
<us-east-2> --arn <ARN of the Connector IAM role> --group  
cloudmanager-access-group --username  
system:node:{{EC2PrivateDNSName}}
```

aws -auth を編集します

AWS- auth ConfigMap を直接編集して、Cloud Manager Connector の IAM ロールに RBAC アクセスを追加します。

"[詳細な手順については、AWS EKS のドキュメントを参照してください](#)".

以下に例を示します。

```
apiVersion: v1  
data:  
  mapRoles: |  
    - groups:  
      - cloudmanager-access-group  
      rolearn: <ARN of the Connector IAM role>  
      username: system:node:{{EC2PrivateDNSName}}  
kind: ConfigMap  
metadata:  
  creationTimestamp: "2021-09-30T21:09:18Z"  
  name: aws-auth  
  namespace: kube-system  
  resourceVersion: "1021"  
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth  
  uid: dcc31de5-3838-11e8-af26-02e00430057c
```

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

Kubernetes クラスタには、NetApp Astra Trident が導入されている必要があります。Helm を使用して、最新バージョンの Astra Trident のいずれかをインストールします。"[Helm を使用してインストール手順については、Astra Trident のドキュメントを参照してください](#)"。

Cloud 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）
- "[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。

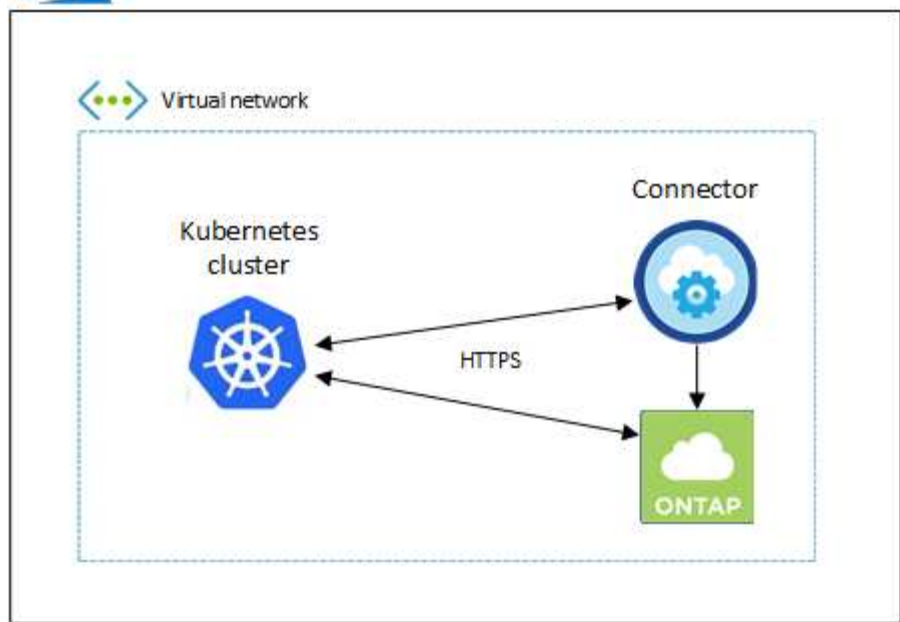
ネットワーク要件を確認します

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。

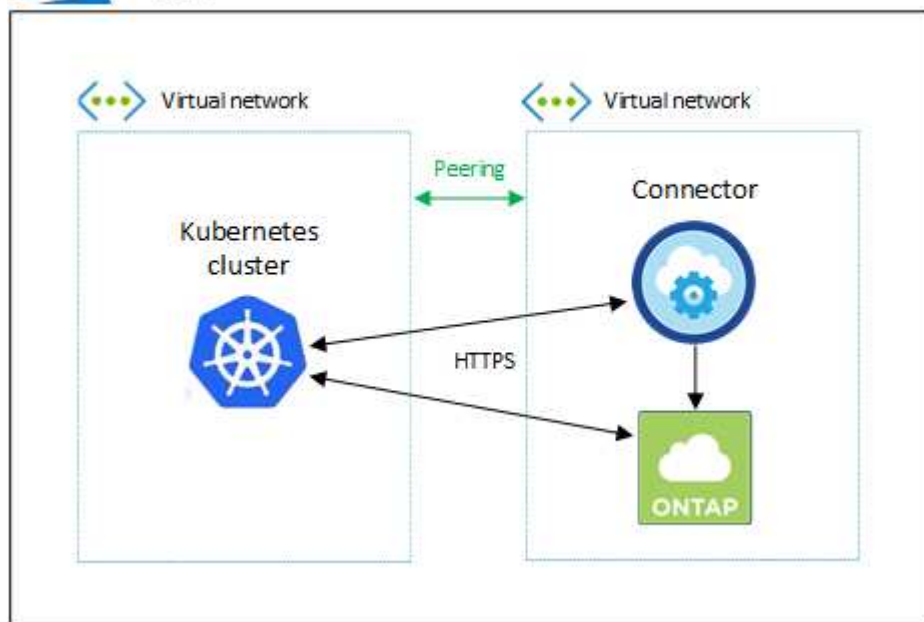
- 各 Kubernetes クラスタがコネクタからインバウンド接続を確立している必要があります
- コネクタには、ポート 443 経由で各 Kubernetes クラスタへのアウトバウンド接続が必要です

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。

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。

The screenshot shows the 'System assigned' tab in the Azure portal. At the top, there are tabs for 'System assigned' and 'User assigned'. Below them is a note: 'A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. \ in code. [Learn more about Managed identities.](#)'. There are buttons for 'Save', 'Discard', 'Refresh', and 'Got feedback?'. Below this is a 'Status' section with 'Off' and 'On' buttons, where 'On' is selected. The 'Object (principal) ID' field is highlighted with a red box and contains the value '0c288856-adea-485b-a4dc-c15b5ce2c401'. Below this is a 'Permissions' section with a button for 'Azure role assignments'.

- 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. 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。

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - secrets
      - namespaces
      - persistentvolumeclaims
      - persistentvolumes
    verbs:
      - get
      - list
      - create
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - list
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
    verbs:
      - get
      - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name: Object (principal) ID (for AKS) or username (for self-
managed)
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```


2. クラスタに構成を適用します。

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

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

Kubernetes クラスタには、NetApp Astra Trident が導入されている必要があります。Helm を使用して、最新バージョンの Astra Trident のいずれかをインストールします。"[Helm を使用してインストール手順については、Astra Trident のドキュメントを参照してください](#)"。

Cloud 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。

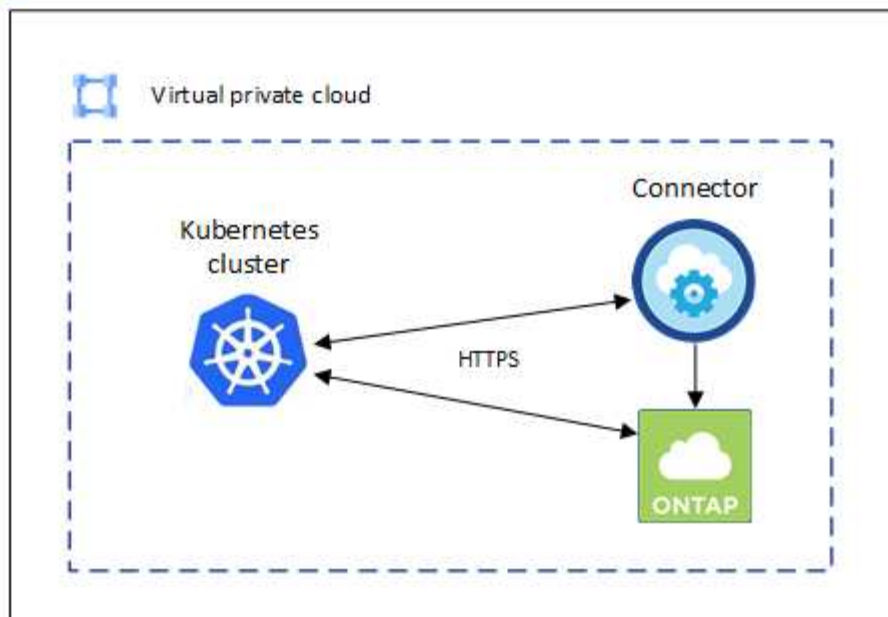
ネットワーク要件を確認します

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 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。

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"](#)。

CloudSync-Dev

←

Cloud Manager Service Account

DETAILSPERMISSIONSKEYSMETRICSLOGS

Service account details

Name

Cloud Manager Service Account

SAVE

Description

SAVE

Email

cloudmanager-service-account@cloudsync-dev-214020.iam.gserviceaccount.com

Unique ID

102217358851946603445

クラスタロールとロールバインドを作成します。

1. 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。

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cloudmanager-access-clusterrole
rules:
  - apiGroups:
      - ''
    resources:
      - secrets
      - namespaces
      - persistentvolumeclaims
      - persistentvolumes
    verbs:
      - get
      - list
      - create
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - list
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
    verbs:
      - get
      - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
subjects:
  - kind: User
    name: "uniqueID"
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
  apiGroup: rbac.authorization.k8s.io

```

2. クラスタに構成を適用します。

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

Kubernetes クラスタを追加

Cloud Manager に Amazon Kubernetes クラスタを追加

Kubernetes clusters を Cloud Manager で検出またはインポートして、永続ボリュームを Amazon S3 にバックアップできるようにすることができます。

クラスタを検出

フルマネージドまたは自己管理型の Kubernetes クラスタを検出できます。管理対象クラスタが検出されている必要があります。インポートすることはできません。

手順

1. Canvas * で、* 作業環境の追加 * をクリックします。
2. Amazon Web Services * > * Kubernetes Cluster * を選択し、* Next * をクリックします。

The screenshot shows a 'Add Working Environment' dialog box. It has two main sections: 'Choose a Location' and 'Choose Type'. In the 'Choose a Location' section, there are four options: 'Microsoft Azure' (selected with a blue checkmark), 'Amazon Web Services', 'Google Cloud Platform', and 'On-Premises'. In the 'Choose Type' section, there are four options: 'Cloud Volumes ONTAP Single Node', 'Cloud Volumes ONTAP HA High Availability', 'Azure NetApp Files High Availability', and 'Kubernetes Cluster Any' (selected with a blue checkmark). A blue 'Next' button is located at the bottom center of the dialog.

3. [Discover Cluster] を選択し、[Next] をクリックします。
4. AWS リージョンを選択し、Kubernetes クラスタを選択して、* Next * をクリックします。



Cloud Manager によって Kubernetes クラスタがキャンバスに追加されます。



クラスタをインポートします

Kubernetes 構成ファイルを使用して、自己管理型の Kubernetes クラスタをインポートできます。

手順

1. Canvas * で、* 作業環境の追加 * をクリックします。
2. Amazon Web Services * > * Kubernetes Cluster * を選択し、* Next * をクリックします。
3. [クラスタのインポート] を選択し、[次へ] をクリックします。
4. Kubernetes 構成ファイルを YAML 形式でアップロードします。

Add Existing Kubernetes Cluster

Import Kubernetes Cluster

Upload a Kubernetes configuration file that's in YAML format

Kubernetes configuration file

minicubeconfig.txt Upload

1 Cluster

Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
test2	Self Managed	v1.24.0

5. Kubernetes クラスタを選択し、* Next * をクリックします。

Cloud Manager によって Kubernetes クラスタがキャンバスに追加されます。

Azure Kubernetes クラスタを Cloud Manager に追加

Kubernetes クラスタを検出または Cloud Manager にインポートして、永続ボリュームを Azure にバックアップできるようにすることができます。

クラスタを検出

フルマネージドまたは自己管理型の Kubernetes クラスタを検出できます。管理対象クラスタが検出されている必要があります。インポートすることはできません。

手順

1. Canvas * で、* 作業環境の追加 * をクリックします。
2. Microsoft Azure * > * Kubernetes Cluster * を選択し、* Next * をクリックします。

Add Working Environment

Choose a Location

Microsoft Azure

Amazon Web Services

Google Cloud Platform

On-Premises

Choose Type

Cloud Volumes ONTAP
Single Node

Cloud Volumes ONTAP HA
High Availability

Azure NetApp Files
High Availability

Kubernetes Cluster
Any

Next

3. [Discover Cluster] を選択し、[Next] をクリックします。
4. Kubernetes クラスタを選択し、* Next * をクリックします。

Add Existing Kubernetes Cluster

Discover a Kubernetes Cluster

AzureKeys

Credential Name

Subscription1

Azure Subscription

Switch Azure Subscription

Select a Kubernetes cluster.

3 Kubernetes Clusters

Kubernetes Cluster Name	Status	Kubernetes Version	Resource Group	Location
<input checked="" type="radio"/> Cluster_1	Active	10.2.23.36	Cell text	Cell text
<input type="radio"/> Cluster_2	Active	10.2.23.36	Cell text	Cell text
<input type="radio"/> Cluster_2	Active	10.2.23.36	Cell text	Cell text

Cloud Manager によって Kubernetes クラスタがキャンバスに追加されます。



クラスタをインポートします

Kubernetes 構成ファイルを使用して、自己管理型の Kubernetes クラスタをインポートできます。

始める前に

Kubernetes クラスタをインポートするには、クラスタロール YAML ファイルで指定したユーザの認証局、クライアントキー、およびクライアント証明書が必要です。Kubernetes クラスタ管理者は、Kubernetes クラスタでユーザを作成する際にこれらの認定資格を取得します。

手順

1. Canvas * で、* 作業環境の追加 * をクリックします。
2. Microsoft Azure * > * Kubernetes Cluster * を選択し、* Next * をクリックします。
3. [クラスタのインポート] を選択し、[次へ] をクリックします。
4. Kubernetes 構成ファイルを YAML 形式でアップロードします。

Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
test2	Self Managed	v1.24.0

5. Kubernetes クラスタ管理者から提供されたクラスタ証明書をアップロードします。

Upload Cluster Certificates

To complete the import, upload the following cluster certificates. ⓘ

Certificate Authority

No file selected

⬆

Client Key

No file selected

⬆

Client Certificate

No file selected

⬆

Cloud Manager によって Kubernetes クラスタがキャンバスに追加されます。

Cloud Manager に Google Cloud Kubernetes クラスタを追加

Kubernetes クラスタを検出または Cloud Manager にインポートすることで、永続ボリュームを Google Cloud にバックアップできます。


クラスタを検出


フルマネージドまたは自己管理型の Kubernetes クラスタを検出できます。管理対象クラスタが検出されている必要があります。インポートすることはできません。


手順


1. Canvas * で、* 作業環境の追加 * をクリックします。
2. Google Cloud Platform * > * Kubernetes Cluster * を選択し、* Next * をクリックします。

Choose Location & Type



Microsoft Azure



Amazon Web Services



Google Cloud Platform



OnPrem

Choose Type


Cloud Volumes ONTAP
Single Node


Cloud Volumes ONTAP HA
High Availability


Cloud Volumes Service
High Availability

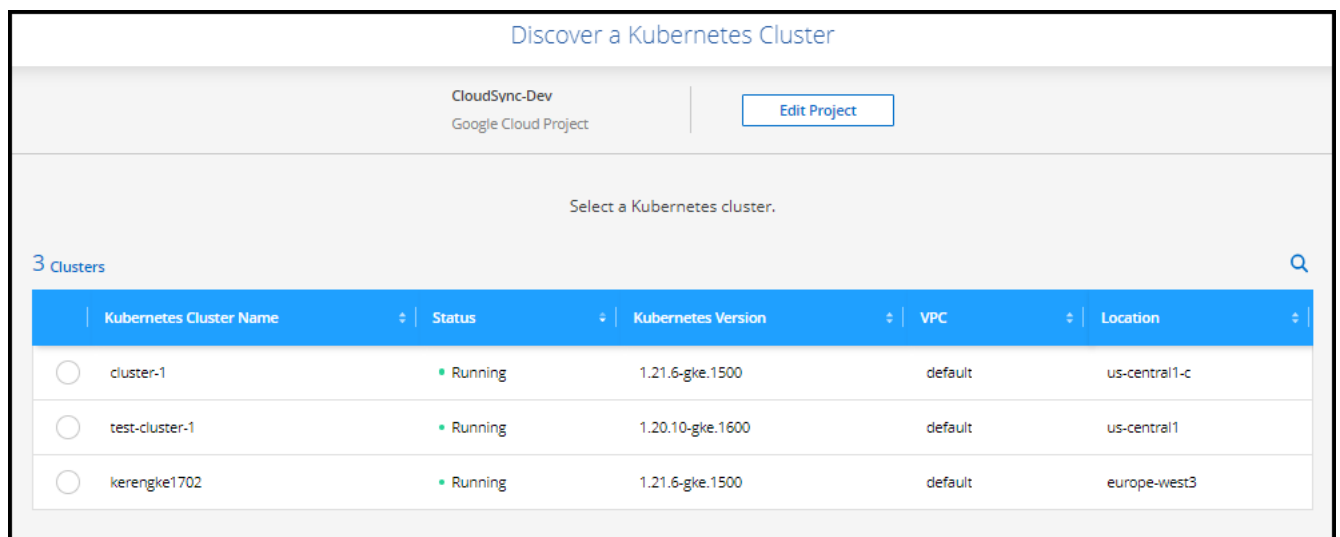

Kubernetes Cluster
Any

3. [Discover Cluster] を選択し、[Next] をクリックします。
4. 別の Google Cloud プロジェクトの Kubernetes クラスタを選択するには、* プロジェクトの編集 * をクリックし、使用可能なプロジェクトを選択します。

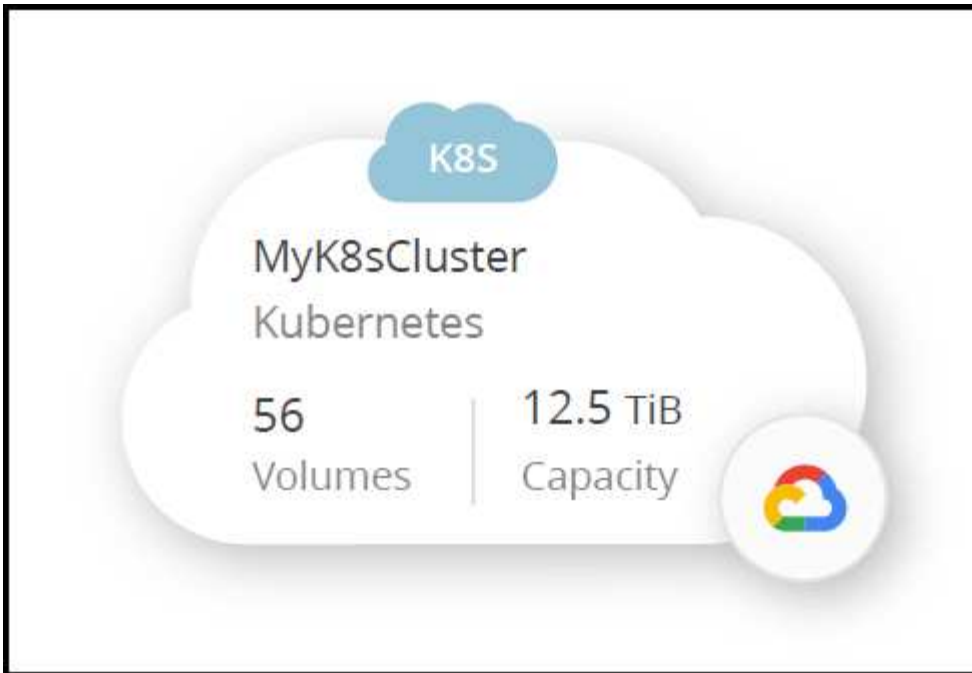


ページのスクリーンショット。"]

5. Kubernetes クラスタを選択し、 * Next * をクリックします。



Cloud Manager によって Kubernetes クラスタがキャンバスに追加されます。



クラスタをインポートします

Kubernetes 構成ファイルを使用して、自己管理型の Kubernetes クラスタをインポートできます。

始める前に

Kubernetes クラスタをインポートするには、クラスタロール YAML ファイルで指定したユーザの認証局、クライアントキー、およびクライアント証明書が必要です。Kubernetes クラスタ管理者は、Kubernetes クラスタでユーザを作成する際にこれらの認定資格を取得します。

手順

1. Canvas * で、* 作業環境の追加 * をクリックします。
2. Google Cloud Platform * > * Kubernetes Cluster * を選択し、* Next * をクリックします。
3. [クラスタのインポート] を選択し、[次へ] をクリックします。
4. Kubernetes 構成ファイルを YAML 形式でアップロードします。

Add Existing Kubernetes Cluster

Import Kubernetes Cluster

Upload a Kubernetes configuration file that's in YAML format and has the extension ".txt", ".kubeconfig", or ".config"

Kubernetes configuration file

KubConfig.txt

Upload

3 Kubernetes Clusters

Kubernetes Cluster Name	Kubernetes Type	Kubernetes Version
<input checked="" type="radio"/> Cluster_1	???	10.2.23.36
<input type="radio"/> Cluster_2	???	10.2.23.36
<input type="radio"/> Cluster_2	???	10.2.23.36

Cloud Manager によって Kubernetes クラスタがキャンバスに追加されます。

ネットアップのクラウドデータサービスを Kubernetes クラスタで使用できます

管理対象の Kubernetes クラスタを Canvas に追加すると、ネットアップのクラウドデータサービスを使用して高度なデータ管理を行うことができます。

現時点では、Kubernetes クラスタで Cloud Backup がサポートされます。Cloud Backup を使用して、永続ボリュームをオブジェクトストレージにバックアップできます。

"永続ボリュームのバックアップ方法については、[Cloud Backup のドキュメント](#)を参照してください。"

The screenshot displays the 'Restore' tab in the Canvas interface, specifically for 'Kubernetes'. At the top, a dropdown menu shows '1 Selected Kubernetes Clusters'. To the right is a 'Backup Settings' button. Below this, a summary section shows: 1 Kubernetes Clusters, 5 Protected PVs, and 97.66 KB Total Backups Size. To the right of this is a 'Protected Persistent Volumes Status' section showing 5 Healthy Backups and 0 Failed Backups. Below the summary is a '5 Backup Jobs' section with a search icon. A table lists the backup jobs with columns: Source K8s Cluster, Source Persistent Volume, Source Namespace, Last Backup, Backup Copies, Backup Status, and an action menu.

Source K8s Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backup Copies	Backup Status	
eks1 On	pvc-1704aa1f-af1d-49e9-87fd-6edd86125855 Online	default	Nov 25 2021, 14:56:3	2	Enabled	...
eks1 On	pvc-d1f839c1-d932-4f49-b620-33321dbe939e Online	trident	Nov 25 2021, 14:56:3	2	Enabled	...
eks1 On	pvc-f615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6 Online	default	Nov 25 2021, 14:56:3	2	Enabled	...
eks1 On	pvc-1615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6 Online	default	Nov 25 2021, 14:56:3	2	Enabled	...
eks1 On	pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1 Online	default	Nov 25 2021, 14:56:3	2	Enabled	...

知識とサポート

サポートに登録します

...

ヘルプを表示します

...

法的通知

""

""

- "Cloud Manager 3.9 に関する注意事項"
- "Cloud Backup に関する通知です"

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.