



Kubernetes クラスターのドキュメント

Kubernetes clusters

NetApp
April 16, 2024

目次

Kubernetes クラスタのドキュメント	1
BlueXPのKubernetesの新機能	2
2023年4月2日	2
2023年3月5日	2
2022年11月6日	2
2022年9月18日	2
2022年7月31日	2
2022年7月3日	3
2022年6月6日	3
2022年5月4日	3
2022 年 4 月 4 日	3
2022 年 2 月 27 日	3
2022 年 1 月 11 日	4
2021 年 11 月 28 日	4
はじめに	5
BlueXPでのKubernetesのデータ管理	5
Kubernetes クラスタの導入を開始する	6
要件	8
AWS での Kubernetes クラスタの要件	8
Azure での Kubernetes クラスタの要件	17
Google Cloud の Kubernetes クラスタの要件	25
OpenShiftでのKubernetesクラスタの要件	32
Kubernetes クラスタを追加	41
Amazon KubernetesクラスタをBlueXPに追加します	41
Azure KubernetesクラスタをBlueXPに追加します	43
Google Cloud KubernetesクラスタをBlueXPに追加します	46
OpenShiftクラスタをBlueXPにインポートします	50
Kubernetes クラスタを管理	52
Trident で Astra を管理	52
ストレージクラスを管理する	54
永続ボリュームを表示します	58
Kubernetes クラスタをワークスペースから削除	59
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	60
知識とサポート	61
サポートに登録します	61
ヘルプを表示します	65
法的通知	71
著作権	71
商標	71

特許	71
プライバシーポリシー	71
オープンソース	71

Kubernetes クラスタのドキュメント

BlueXPのKubernetesの新機能

BlueXPのKubernetesの最新情報をご紹介します。

2023年4月2日

- 次の操作を実行できます。 ["Astra Tridentをアンインストールします"](#) これは、TridentオペレータまたはBlueXPを使用してインストールしました。
- ユーザインターフェイスが改善され、ドキュメントのスクリーンショットが更新されました。

2023年3月5日

- BlueXPのKubernetesでAstra Trident 23.01がサポートされるようになりました。
- ユーザインターフェイスが改善され、ドキュメントのスクリーンショットが更新されました。

2022年11月6日

いつ ["ストレージクラスを定義する"](#)では、ブロックストレージやファイルシステムストレージに対して、ストレージクラスの経済性を実現できます。

2022年9月18日

自己管理OpenShiftクラスタをCloud Managerにインポートできるようになりました。

- ["OpenShiftでのKubernetesクラスタの要件"](#)
- ["OpenShiftクラスタをCloud Managerにインポートします"](#)

2022年7月31日

- ストレージクラスの新しい「-watch` verb」を使用して、YAMLの設定をバックアップおよびリストアできるようになりました。Cloud ManagerはKubernetesクラスタバックエンドに加えられた変更を監視し、クラスタで自動バックアップが設定されている場合は、新しい永続ボリュームのバックアップを自動的に有効にすることができます。

["AWS での Kubernetes クラスタの要件"](#)

["Azure での Kubernetes クラスタの要件"](#)

["Google Cloud の Kubernetes クラスタの要件"](#)

- いつ ["ストレージクラスを定義する"](#)をクリックし、ブロックストレージのファイルシステムタイプ (fstype) を指定できるようになりました。

2022年7月3日

- Tridentオペレータを使用してAstra Tridentを導入した場合、Cloud Managerで最新バージョンのAstra Tridentにアップグレードできるようになりました。

["Astra Tridentをインストールして管理"](#)

- KubernetesクラスタをドラッグしてAWS FSX for ONTAP 作業環境にドロップし、ストレージクラスをキャンバスから直接追加できるようになりました。

["ストレージクラスを追加します"](#)

2022年6月6日

Cloud Managerは、バックエンドストレージとしてAmazon FSx for ONTAP をサポートするようになりました。

2022年5月4日

ドラッグアンドドロップしてストレージクラスを追加します

KubernetesクラスタをドラッグしてCloud Volumes ONTAP 作業環境にドロップし、ストレージクラスをキャンバスから直接追加できるようになりました。

["ストレージクラスを追加します"](#)

2022 年 4 月 4 日

Cloud Manager のリソースページを使用して **Kubernetes** クラスタを管理

Kubernetes クラスタ管理の統合がクラスタ作業環境から直接強化されました。新しい["クイックスタート"](#) すぐに運用を開始できます。

クラスタリソースのページで次の操作を実行できるようになりました。

- ["Astra Trident をインストール"](#)
- ["ストレージクラスを追加する"](#)
- ["永続ボリュームを表示します"](#)
- ["クラスタを削除"](#)
- ["データサービスを有効化"](#)

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

BlueXPでのKubernetesのデータ管理

Astra Trident は、ネットアップが管理している、完全にサポートされているオープンソースプロジェクトです。Kubernetes と Persistent Volume フレームワークとネイティブに統合されている Astra Trident は、ネットアップストレージプラットフォームを任意に組み合わせて実行されているシステムから、ボリュームのプロビジョニングと管理をシームレスに行います。 ["Trident の詳細をご確認ください"](#)。

の機能

を使用します ["BlueXP"](#) Tridentオペレータを使用して互換性のあるバージョンのAstra Tridentを導入すると、次のことが可能になります。

- Kubernetesクラスタを追加および管理します
- ["Astra Tridentをインストール、アップグレード、アンインストール"](#)
- ["ストレージクラスを追加および削除します"](#)
- ["永続ボリュームを表示します"](#)
- ["Kubernetesクラスタを削除"](#) をクリックします
- ["BlueXPのバックアップとリカバリのアクティブ化と表示"](#)

サポートされる **Kubernetes** 環境

BlueXPは、次の環境で実行されるマネージドKubernetesクラスタをサポートしています。

- ["Amazon Elastic Kubernetes Service \(Amazon EKS \) "](#)
- ["Microsoft Azure Kubernetes Service \(AKS \) "](#)
- ["Google Kubernetes Engine \(GKE \) "](#)

サポートされている **Astra Trident** 環境

Astra Tridentの4つの最新バージョンのうちの1つ ["Tridentオペレータを使用して導入されています"](#) は必須です。



を使用してTridentを導入 `tridentctl` はサポートされていません。を使用してAstra Tridentを導入した場合 `tridentctl` では、BlueXPを使用してKubernetesクラスタを管理することはできません。実行する必要があります 再インストールしてください ["Trident演算子を使用する"](#) または ["BlueXPを使用している"](#)。

Astra Tridentは、BlueXPから直接インストールすることも、サポート対象バージョンにアップグレードすることもできます。

["Astra Tridentの前提条件を確認"](#)

サポートされるバックエンドストレージ

NetApp Astra Tridentは各Kubernetesクラスタにインストールする必要があります。また、Cloud Volumes ONTAP またはAmazon FSX for 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

BlueXPでは'_discover_'で使用しているKubernetesクラスタには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する場合には課金されます

Kubernetes クラスタの導入を開始する

を使用します **"BlueXP"** Kubernetesクラスタの管理は、いくつかの手順で開始できます。

1

前提条件を確認する

ご使用の環境がクラスタタイプ的前提条件を満たしていることを確認してください。

["AWS での Kubernetes クラスタの要件"](#)

["Azure での Kubernetes クラスタの要件"](#)

["Google Cloud の Kubernetes クラスタの要件"](#)

2

KubernetesクラスタをBlueXPに追加します

Kubernetesクラスタを追加し、BlueXPを使用して作業環境に接続できます。

["Amazon Kubernetes クラスタを追加"](#)

["Azure Kubernetes クラスタを追加"](#)

["Google Cloud Kubernetes クラスタを追加"](#)

3

永続ボリュームのプロビジョニングを開始します

Kubernetes の標準のインターフェイスと構成要素を使用して、永続ボリュームを要求および管理できます。BlueXPでは、NFSおよびiSCSIストレージクラスが作成されており、これを使用してPersistent Volumesをプロビジョニングできます。

["Trident を使用した最初のボリュームのプロビジョニングの詳細をご確認ください"](#)。

4

BlueXPを使用してクラスタを管理します

BlueXPにKubernetesクラスタを追加すると、BlueXPリソースページからクラスタを管理できます。

"Kubernetes クラスタを管理する方法について説明します。"

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BlueXPに追加できます。BlueXPにクラスタを追加する前に、次の要件が満たされ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

最新バージョンの 4 つの Astra Trident が必要です。Astra Tridentは、BlueXPから直接インストールまたはアップグレードできます。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、

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"](#)。

BlueXPコネクタ

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

BlueXP 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にBlueXPコネクタが必要です。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。

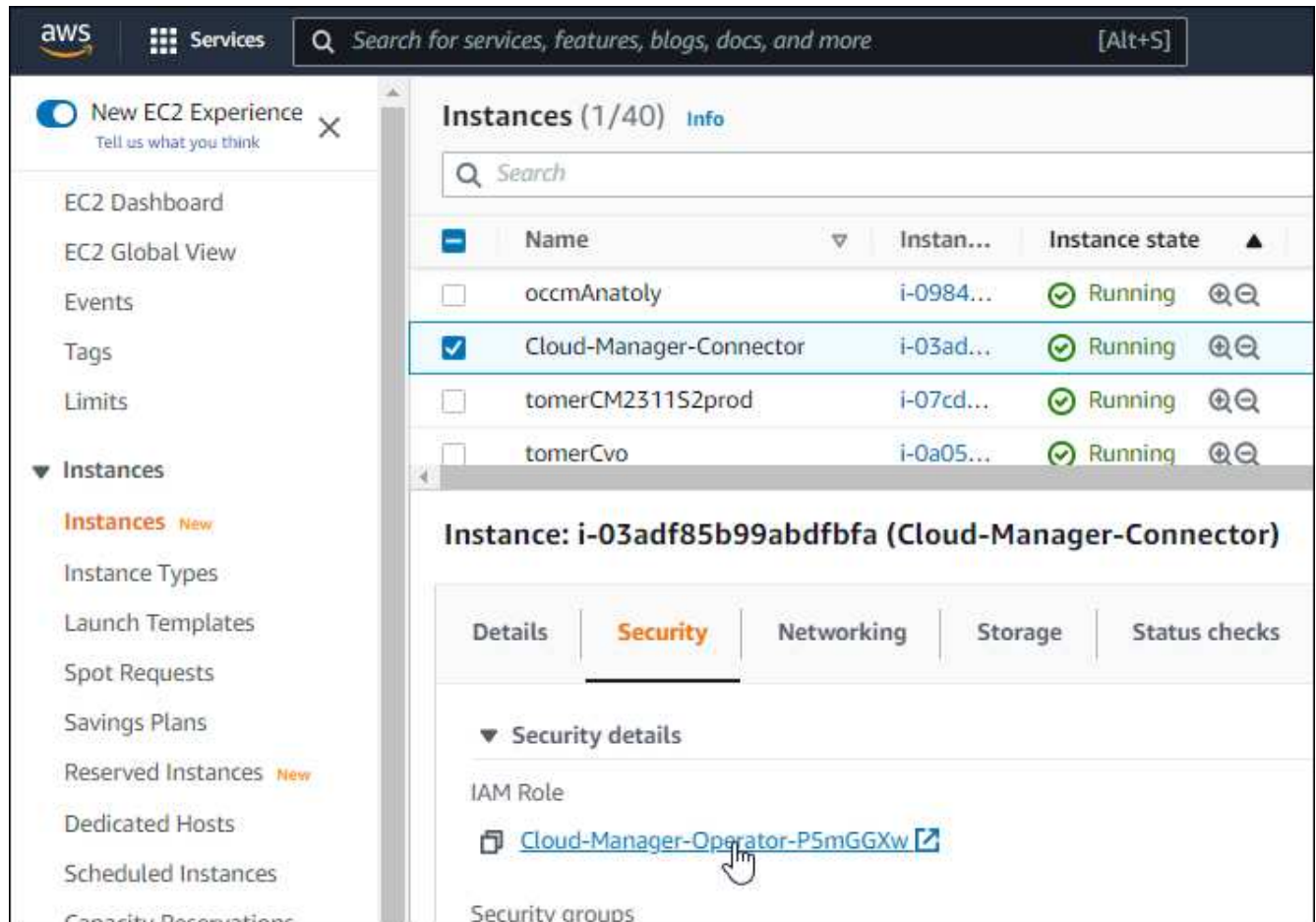
- ["BlueXPからコネクタを作成します"](#) (推奨)
- ["AWS Marketplace からコネクタを作成します"](#)
- ["AWS の既存の Linux ホストにコネクタをインストールします"](#)

必要な権限を既存のコネクタに追加します

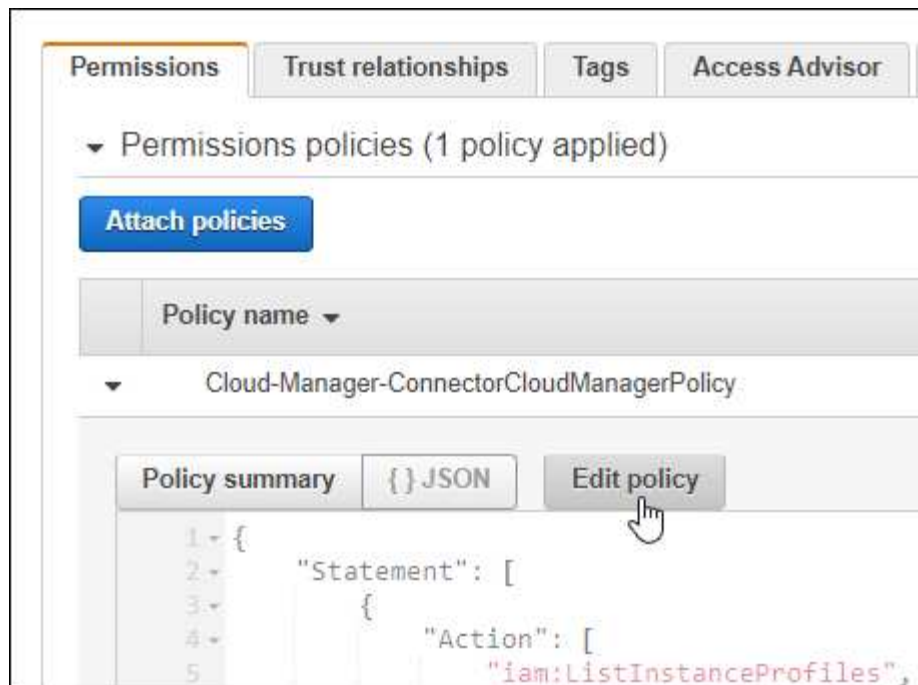
3.9.13 リリース以降、new_newly で作成されたコネクタには、Kubernetes クラスタの検出と管理を可能にする新しい AWS 権限が 3 つ含まれています。このリリースよりも前のリリースでコネクタを作成していた場合は、権限を付与するために、コネクタの IAM ロールの既存のポリシーを変更する必要があります。

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。

- EC2: DescribeRegions (説明領域)
- EKS : リストクラスタ
- 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。

異なる機能を有効にするには、異なる許可が必要です。

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

BlueXPを使用してストレージクラスを追加し、バックエンドへの変更がないかクラスタを監視するには、拡張された許可が必要です。

Astra Trident をインストールします

BlueXPがAstra Tridentをインストールするためには、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、BlueXPはAstra Tridentバックエンドと、Astra Tridentの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て、ストレージクラスと通信する必要があります。

手順

1. クラスタロールとロールバインドを作成します。
 - a. 要件に基づいて承認をカスタマイズできます。

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
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumes
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumeclaims
    verbs:
      - list
      - create
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - list
```



```

- apiGroups:
  - trident.netapp.io
  resources:
  - tridentbackends
  verbs:
  - list
  - watch
- apiGroups:
  - trident.netapp.io
  resources:
  - tridentorchestrators
  verbs:
  - get
  - watch

---
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

```

ストレージクラス

BlueXPを使用してストレージクラスを追加するには'拡張された認証を追加します

```

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
      - watch
      - create
      - delete
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - create
      - list
      - watch
      - delete
      - patch
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
      - tridentbackendconfigs
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch

---
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

```

コマンドラインを使用して完全な認証を行い、BlueXPでAstra Tridentをインストールできるようにします。

```
eksctl create iamidentitymapping --cluster < > --region < > --arn  
< > --group "system:masters" --username  
system:node:{{EC2PrivateDNSName}}
```

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BlueXPコネクタ用のIAMロールとの間に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、BlueXPコネクタのIAMロールへの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

Azureでは、BlueXPを使用して、マネージドAzure Kubernetesクラスタ（AKS）と自己管理Kubernetesクラスタを追加および管理できます。BlueXPにクラスタを追加する前に、次の要件が満たされていることを確認します



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。Astra Tridentは、BlueXPから直接インストールまたはアップグレードできます。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、

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"](#)。

BlueXPコネクタ

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

BlueXP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ています。BlueXP 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のBlueXPコネクタが必要です。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。

- ["BlueXP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。

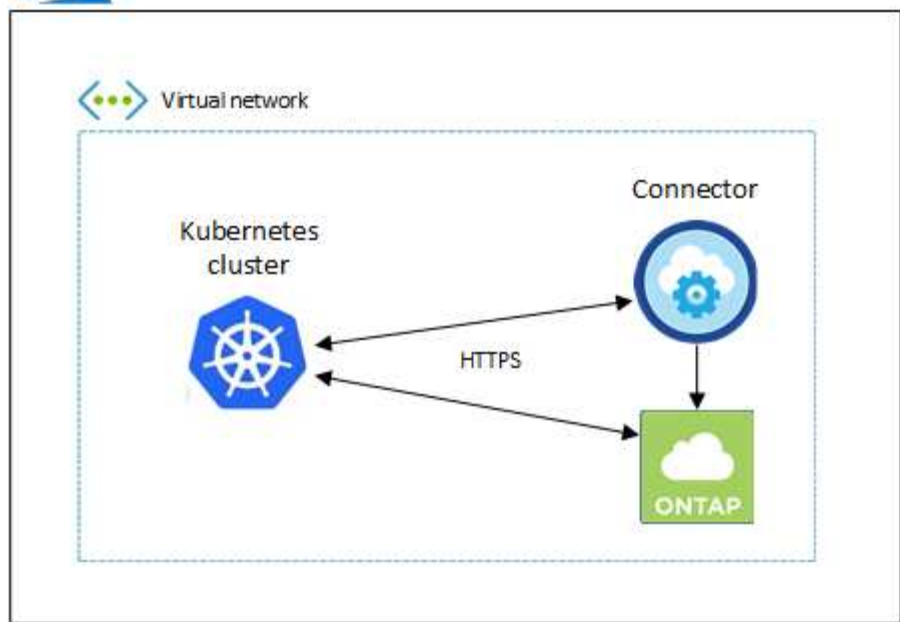
ネットワーク要件を確認します

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。

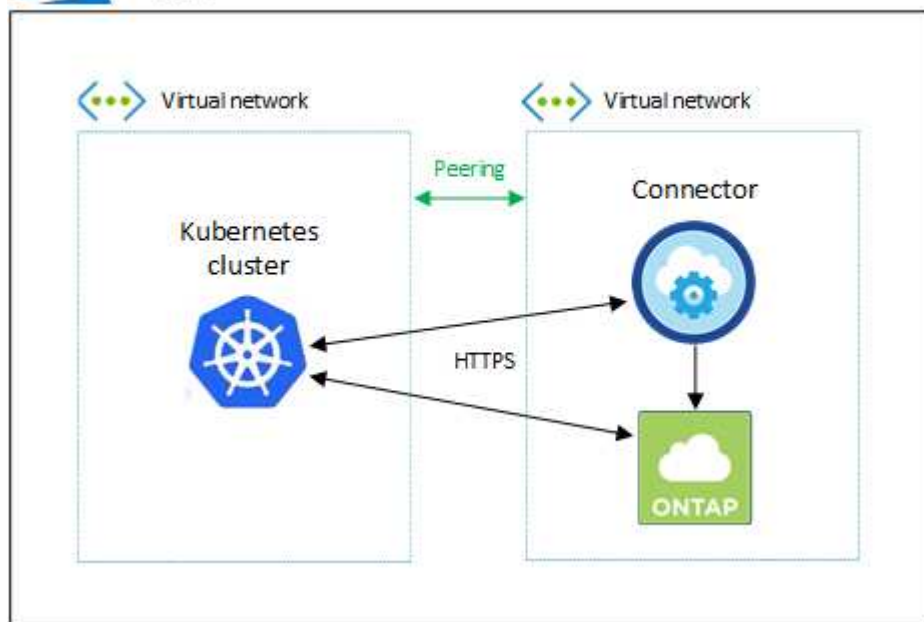
- 各 Kubernetes クラスタがコネクタからインバウンド接続を確立している必要があります
- コネクタには、ポート 443 経由で各 Kubernetes クラスタへのアウトバウンド接続が必要です

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

BlueXPを使用してストレージクラスを追加し、バックエンドへの変更がないかクラスタを監視するには、拡張された許可が必要です。

Astra Trident をインストールします

BlueXPがAstra Tridentをインストールするためには、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、BlueXPはAstra Tridentバックエンドと、Astra Tridentの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て、ストレージクラスと通信する必要があります。

作業を開始する前に

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。

The screenshot shows the 'System assigned' tab of an Azure managed identity. The 'Object (principal) ID' field is highlighted with a red box and contains the value '0c288856-adea-485b-a4dc-c15b5ce2c401'. The 'Status' is set to 'On'. The 'Permissions' section shows '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。

手順

クラスタロールとロールバインドを作成します。

1. 要件に基づいて承認をカスタマイズできます。

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。

を交換します subjects: kind: 変数にユーザ名とを入力します subjects: name: システムが割り当てた管理IDのオブジェクトID、または上記のように許可されたユーザーのユーザー名のいずれかを使用します。

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

```

resources:
  - storageclasses
verbs:
  - list
- apiGroups:
  - trident.netapp.io
resources:
  - tridentbackends
verbs:
  - list
  - watch
- apiGroups:
  - trident.netapp.io
resources:
  - tridentorchestrators
verbs:
  - get
  - watch
---
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

BlueXPを使用してストレージクラスを追加するには'拡張された認証を追加します

を交換します subjects: kind: 変数にユーザ名とを入力します subjects: user: システムが割り当てた管理IDのオブジェクトID、または上記のように許可されたユーザーのユーザー名のいずれかを使用します。

```

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
  - watch
  - create
  - delete
  - watch
- apiGroups:
  - storage.k8s.io
  resources:
  - storageclasses
  verbs:
  - get
  - create
  - list
  - watch
  - delete
  - patch
- apiGroups:
  - trident.netapp.io
  resources:
  - tridentbackends
  - tridentorchestrators
  - tridentbackendconfigs
  verbs:
  - get
  - list
  - watch
  - create
  - delete
  - watch
---
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のインストール

コマンドラインを使用して完全な認証を行い、BlueXPでAstra Tridentをインストールできるようにします。

```
eksctl create iamidentitymapping --cluster < > --region < > --arn <
> --group "system:masters" --username
system:node:{{EC2PrivateDNSName}}
```

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

管理対象のGoogle Kubernetes Engine (GKE) クラスタと、BlueXPを使用してGoogleで自己管理型Kubernetesクラスタを追加および管理できます。BlueXPにクラスタを追加する前に、次の要件が満たされていることを確認します



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。Astra Tridentは、BlueXPから直接インストールまたはアップグレードできます。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

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、コネクタを使用してBlueXP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](#)"。

BlueXPコネクタ

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

BlueXP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ています。BlueXPコネクタの役割は、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BlueXPコネクタが必要です。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。

- ["BlueXP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。

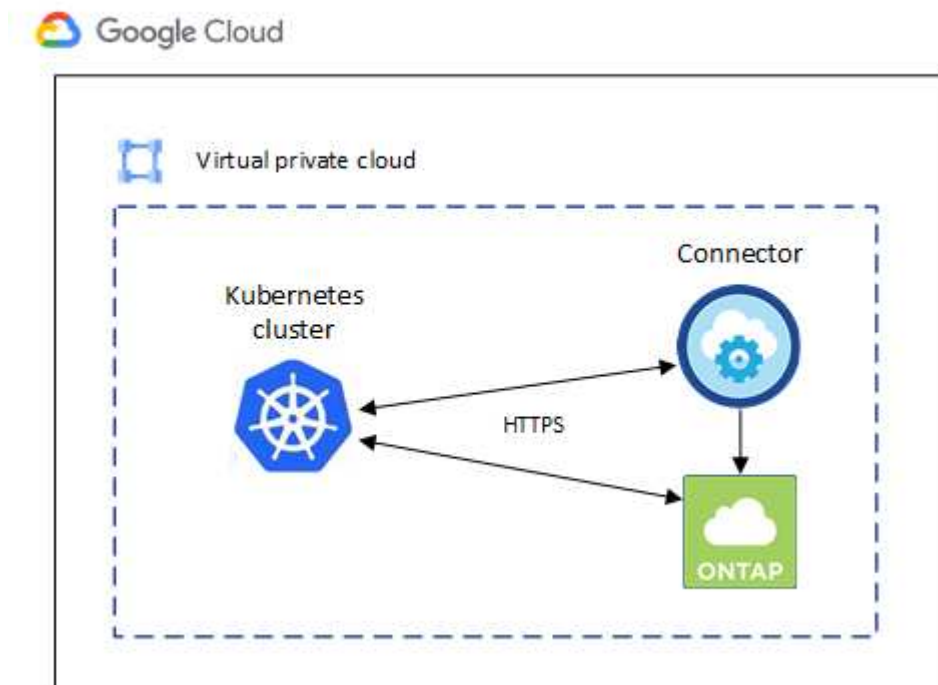
ネットワーク要件を確認します

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。

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

BlueXPを使用してストレージクラスを追加し、バックエンドへの変更がないかクラスタを監視するには、拡張された許可が必要です。

Astra Trident をインストールします

BlueXPがAstra Tridentをインストールするためには、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、BlueXPはAstra Tridentバックエンドと、Astra Tridentの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て、ストレージクラスと通信する必要があります。

作業を開始する前に

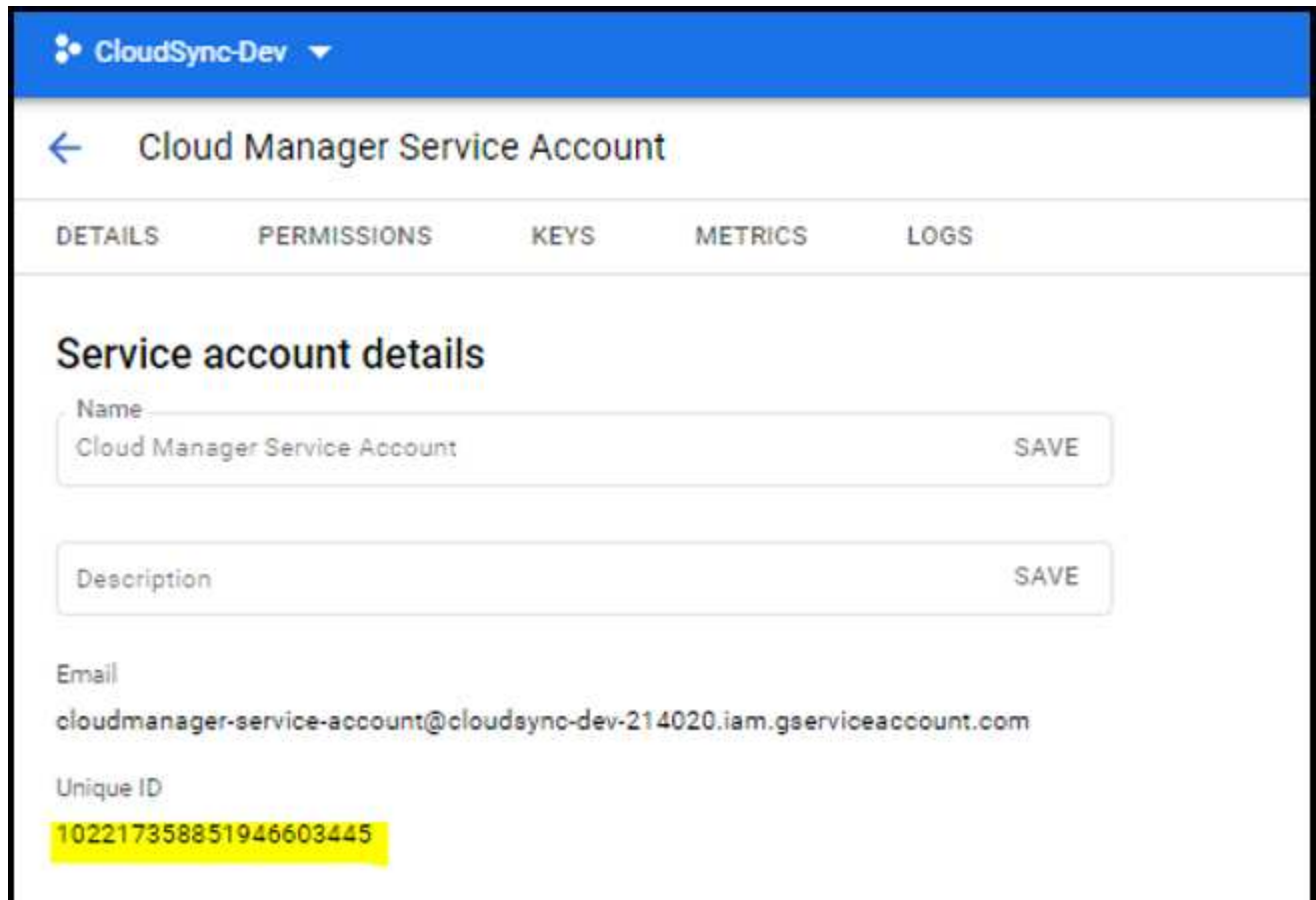
を設定します `subjects: name: YAMLファイルで、BlueXPの一意のIDを知っている必要があります。`

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](#)"。



手順

クラスターロールとロールバインドを作成します。

1. 要件に基づいて承認をカスタマイズできます。

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。

を交換します subjects: kind: 変数にユーザ名とを入力します subjects: name: 承認されたサービスアカウントの一意的IDを使用します。

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



```

      - storageclasses
    verbs:
      - list
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
    verbs:
      - list
      - watch
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentorchestrators
    verbs:
      - get
      - watch
---
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

BlueXPを使用してストレージクラスを追加するには'拡張された認証を追加します

を交換します subjects: kind: 変数にユーザ名とを入力します subjects: user: 承認されたサービスアカウントの一意のIDを使用します。

```

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
      - watch
      - create
      - delete
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - get
      - create
      - list
      - watch
      - delete
      - patch
  - apiGroups:
      - trident.netapp.io
    resources:
      - tridentbackends
      - tridentorchestrators
      - tridentbackendconfigs
    verbs:
      - get
      - list
      - watch
      - create
      - delete
      - watch

---
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のインストール

コマンドラインを使用して完全な認証を行い、BlueXPで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>
```

OpenShiftでのKubernetesクラスタの要件

BlueXPを使用して、自己管理型OpenShift Kubernetesクラスタを追加および管理できます。BlueXPにクラスタを追加する前に、次の要件が満たされていることを確認します

要件

Astra Trident

最新バージョンの 4 つの Astra Trident が必要です。Astra Tridentは、BlueXPから直接インストールまたはアップグレードできます。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、

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"](#)。

BlueXPコネクタ

Kubernetesクラスタをインポートおよび管理するには、BlueXPコネクタが必要です。クラウドプロバイダに必要な権限を持つ新しいコネクタを作成するか、既存のコネクタを使用する必要があります。

- ["AWSコネクタ"](#)
- ["Azure Connectorの場合"](#)
- ["Google Cloud Connectorの場合"](#)

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。

RBAC許可を使用したKubernetes構成ファイル (kubeconfig)

OpenShiftクラスタをインポートするには、さまざまな機能を有効にするために必要なRBAC許可を含むkubeconfigファイルが必要です。 [\[kubeconfigファイルを作成します\]](#)。

- 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のみです。
- ストレージクラスの追加：BlueXPを使用してストレージクラスを追加し、バックエンドへの変更がないかクラスタを監視するには、拡張された許可が必要です。
- Install Astra Trident：BlueXP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、BlueXPはAstra Trident/バックエンドと、Astra Tridentの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て、ストレージクラスタと通信する必要があります。

kubeconfigファイルを作成します

OpenShift CLIを使用して、BlueXPにインポートするkubeconfigファイルを作成します。

手順

1. パブリックURLにある「OC login」を使用して、管理ユーザとともにOpenShift CLIにログインします。
2. 次の手順でサービスアカウントを作成します。

- a. 「OC-service-account.yaml」という名前のサービスアカウントファイルを作成します。

名前と名前空間を必要に応じて調整します。ここで変更を行った場合は、以降の手順でも同じ変更を適用する必要があります。

```
oc-service-account.yaml
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: oc-service-account
  namespace: default
```

- a. サービスアカウントを適用します。

```
kubectl apply -f oc-service-account.yaml
```

3. 許可要件に基づいて、カスタムロールバインディングを作成します。

- a. 「OC-clusterrolebinding.yaml」という名前の「ClusterRoleBinding」ファイルを作成します。

```
oc-clusterrolebinding.yaml
```

- b. クラスタに必要な応じてRBAC許可を設定します。

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
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumes
    verbs:
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - pods
      - pods/exec
    verbs:
      - get
      - list
      - watch
  - apiGroups:
      - ''
    resources:
      - persistentvolumeclaims
    verbs:
      - list
      - create
      - watch
  - apiGroups:
      - storage.k8s.io
    resources:
      - storageclasses
    verbs:
      - list
```

```

- apiGroups:
  - trident.netapp.io
  resources:
  - tridentbackends
  verbs:
  - list
  - watch
- apiGroups:
  - trident.netapp.io
  resources:
  - tridentorchestrators
  verbs:
  - get
  - watch
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: k8s-access-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cloudmanager-access-clusterrole
subjects:
- kind: ServiceAccount
  name: oc-service-account
  namespace: default

```

ストレージクラス

BlueXPを使用してストレージクラスを追加するには'拡張された認証を追加します

```

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

```


フル管理者権限を付与し、BlueXPでAstra Tridentをインストールできるようにします。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cloudmanager-access-clusterrole
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: oc-service-account
  namespace: default
```

c. クラスタロールバインドを適用します。

```
kubectl apply -f oc-clusterrolebinding.yaml
```

4. 「<context>」をインストールの正しいコンテキストに置き換えて、サービスアカウントのシークレットをリストします。

```
kubectl get serviceaccount oc-service-account --context <context>
--namespace default -o json
```

出力の末尾は次のようになります。

```
"secrets": [
  { "name": "oc-service-account-dockercfg-vhz87"},
  { "name": "oc-service-account-token-r59kr"}
]
```

'ecsレット' 配列内の各要素のインデックスは 0 から始まります上の例では、「OC-service-account-dockercfg-vhz87」のインデックスは0になり、「OC-service-account-token-r59kr」のインデックスは1になります。出力で、「token」という単語が含まれるサービスアカウント名のインデックスをメモしてください。

5. 次のように kubeconfig を生成します。

a. 「create-kubeconfig.sh」ファイルを作成します。次のスクリプトの先頭にある「token_index」を正しい値に置き換えます。

create-kubeconfig.sh

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=oc-service-account
NAMESPACE=default
NEW_CONTEXT=oc
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
```

```
set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
--token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

- b. コマンドをソースにし、Kubernetes クラスタに適用します。

```
source create-kubeconfig.sh
```

結果

結果を使用します kubeconfig-sa ファイルを使用して、OpenShiftクラスタをBlueXPに追加します。

Kubernetes クラスタを追加

Amazon KubernetesクラスタをBlueXPに追加します

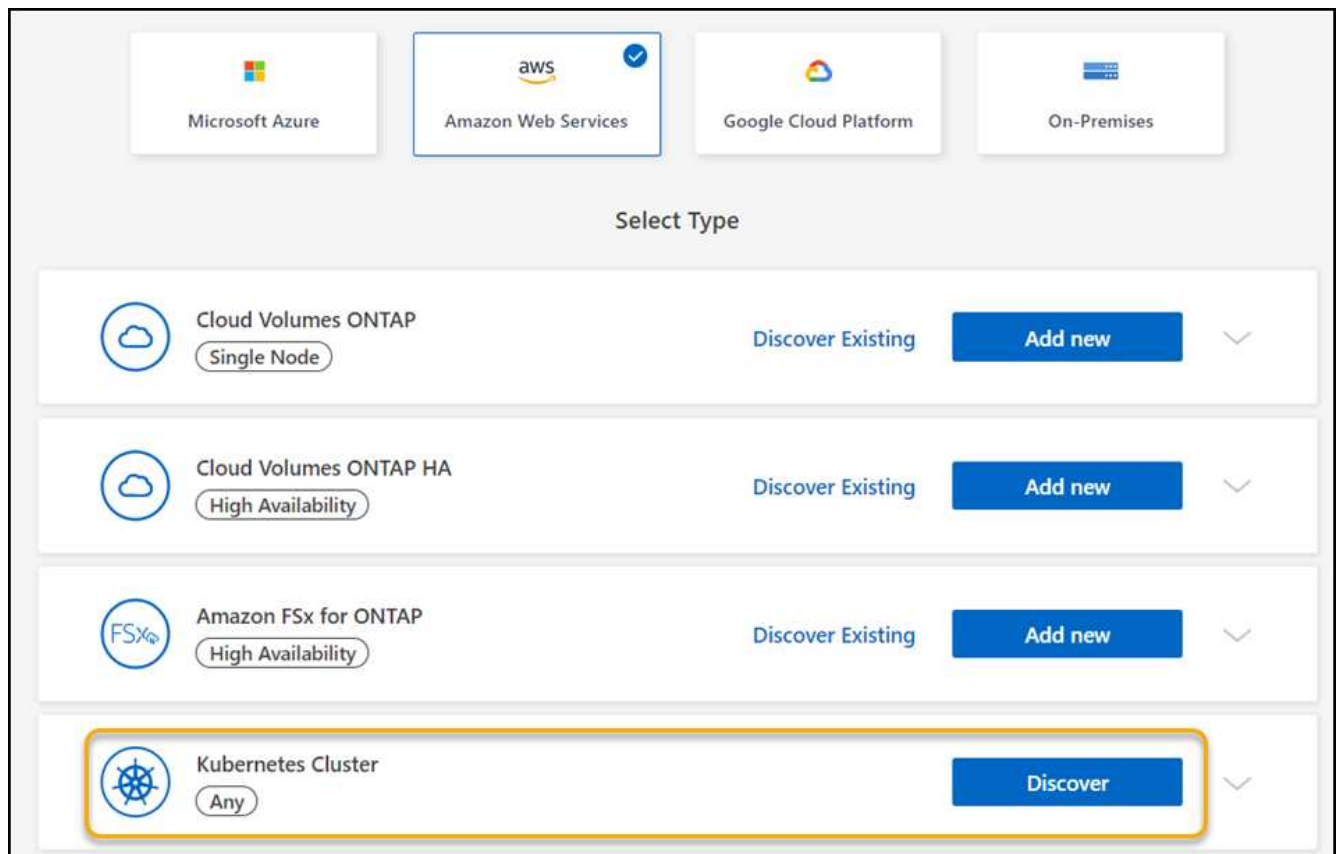
Kubernetesクラスタを検出またはBlueXPにインポートすることで、永続ボリュームをAmazon S3にバックアップできます。

クラスタを検出

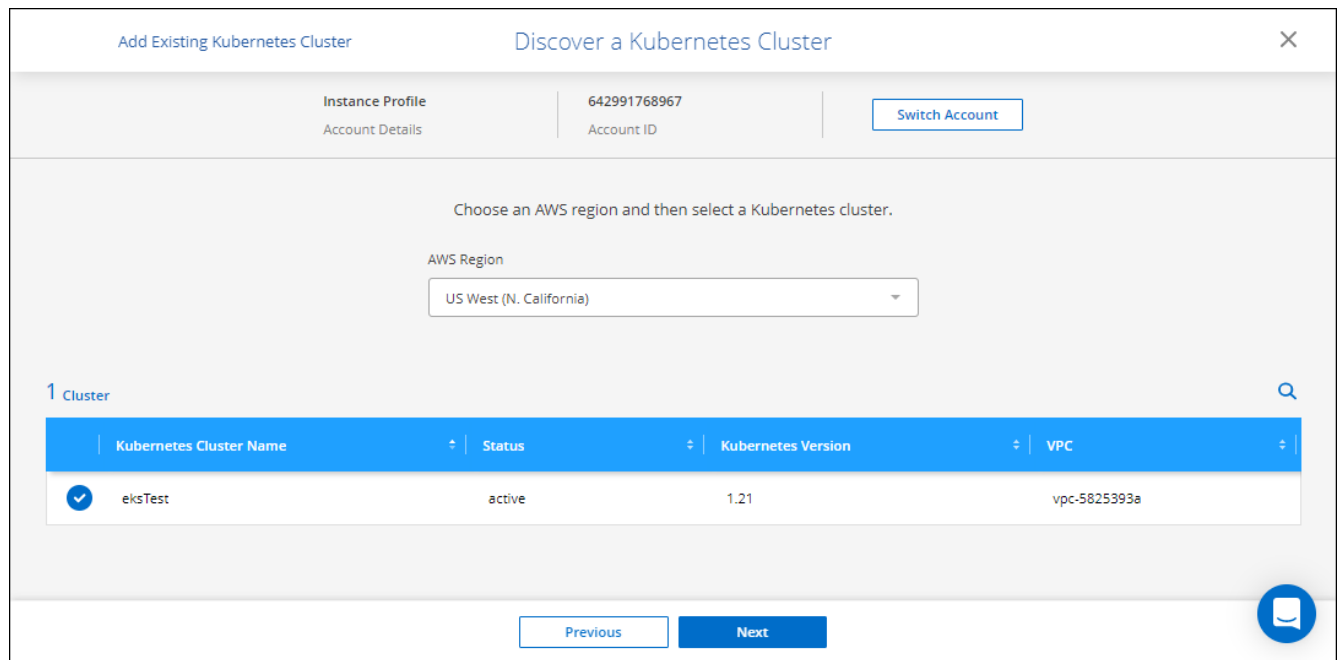
フルマネージドまたは自己管理型の Kubernetes クラスタを検出できます。管理対象クラスタが検出されている必要があります。インポートすることはできません。

手順

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



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*[次へ]*をクリックします。



結果

BlueXPはKubernetesクラスタをCanvasに追加します。

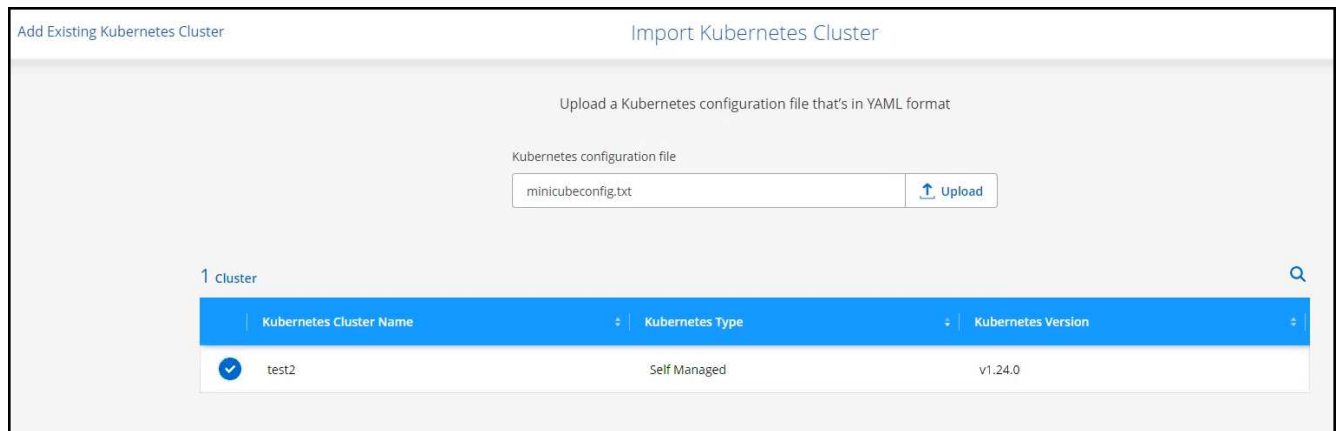


クラスタをインポートします

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 > Discover *を選択します。
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。



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

結果

BlueXPはKubernetesクラスタをCanvasに追加します。

Azure KubernetesクラスタをBlueXPに追加します

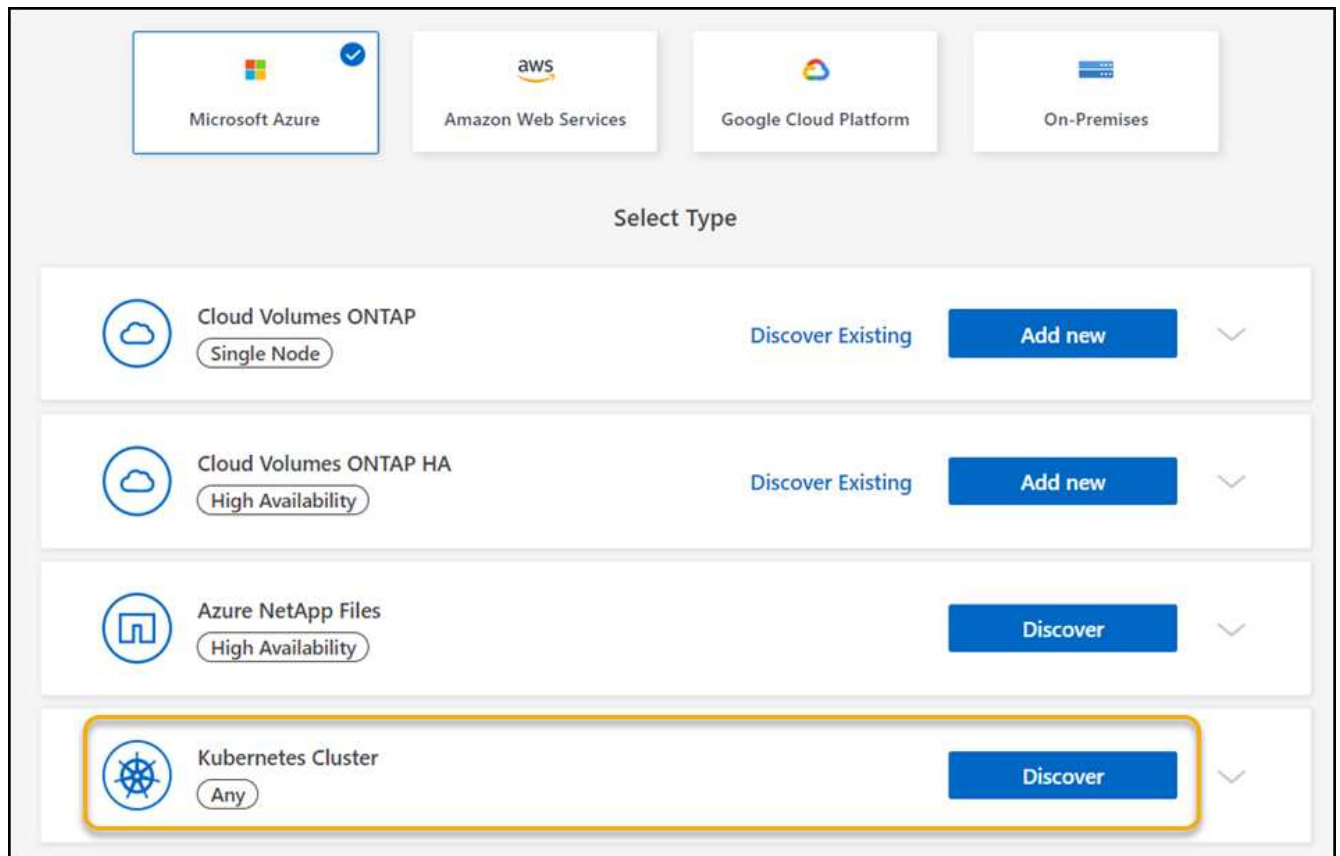
Kubernetesクラスタを検出またはBlueXPにインポートして、永続ボリュームをAzureにバックアップできるようにすることができます。

クラスタを検出

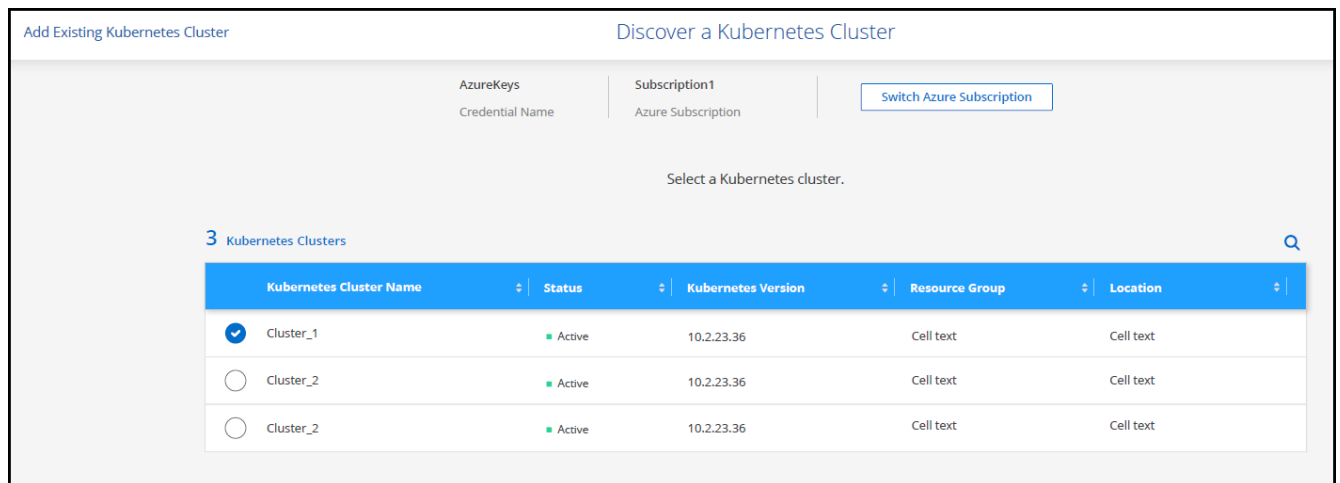
フルマネージドまたは自己管理型の Kubernetes クラスタを検出できます。管理対象クラスタが検出されている必要があります。インポートすることはできません。

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 > Discover *を選択します。

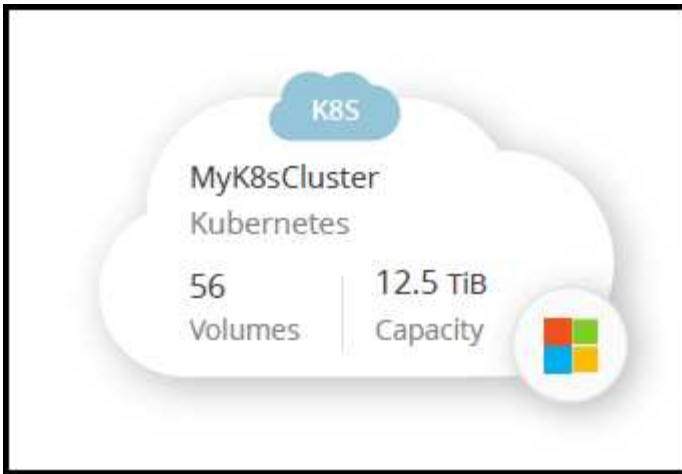


3. [Discover Cluster] を選択し、[Next] をクリックします。
4. Kubernetes クラスタを選択し、* Next * をクリックします。



結果

BlueXPはKubernetesクラスタをCanvasに追加します。



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 > Discover *を選択します。
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

⬆

結果

BlueXPはKubernetesクラスタをCanvasに追加します。

Google Cloud KubernetesクラスタをBlueXPに追加します

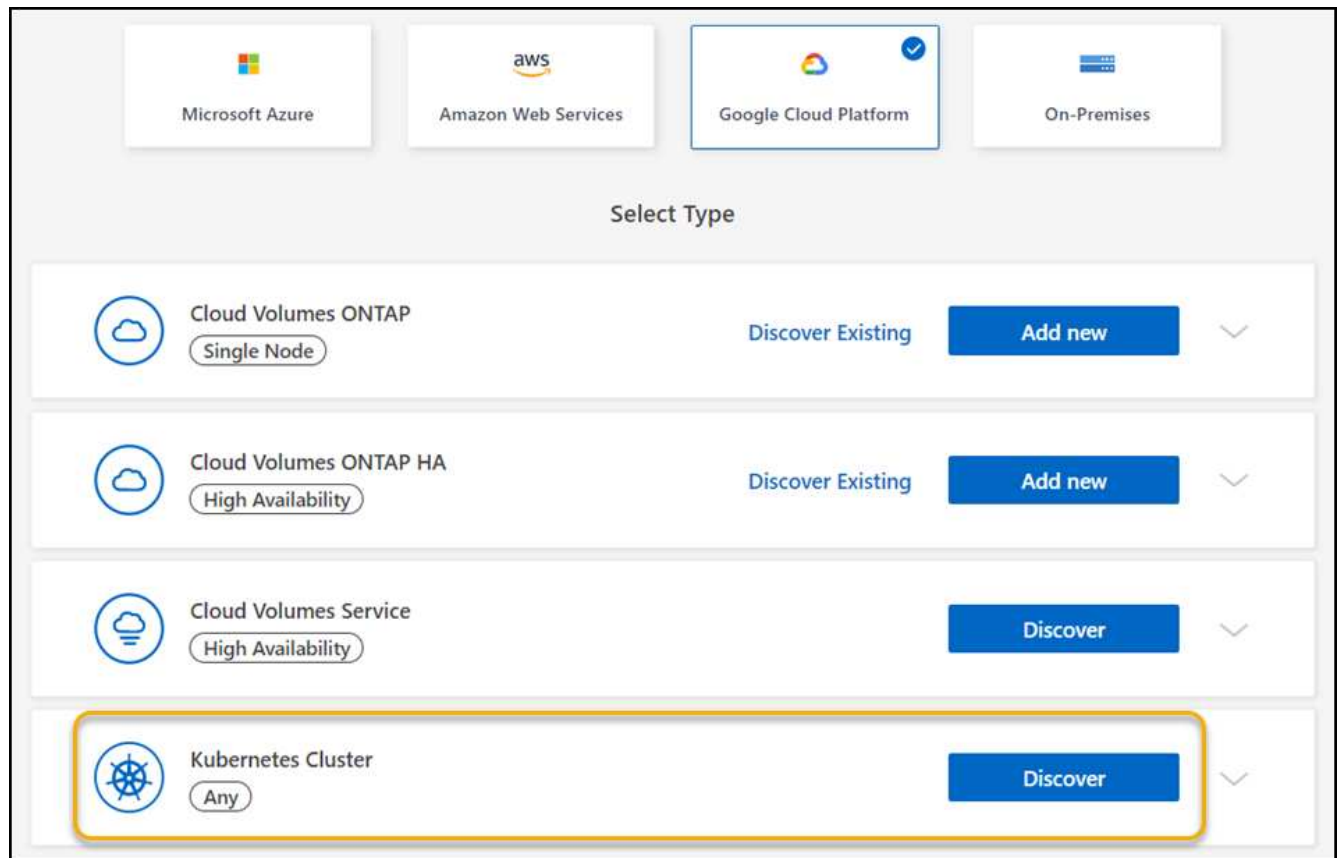
Kubernetesクラスタを検出またはBlueXPにインポートすると、永続ボリュームをGoogle Cloudにバックアップできます。

クラスタを検出

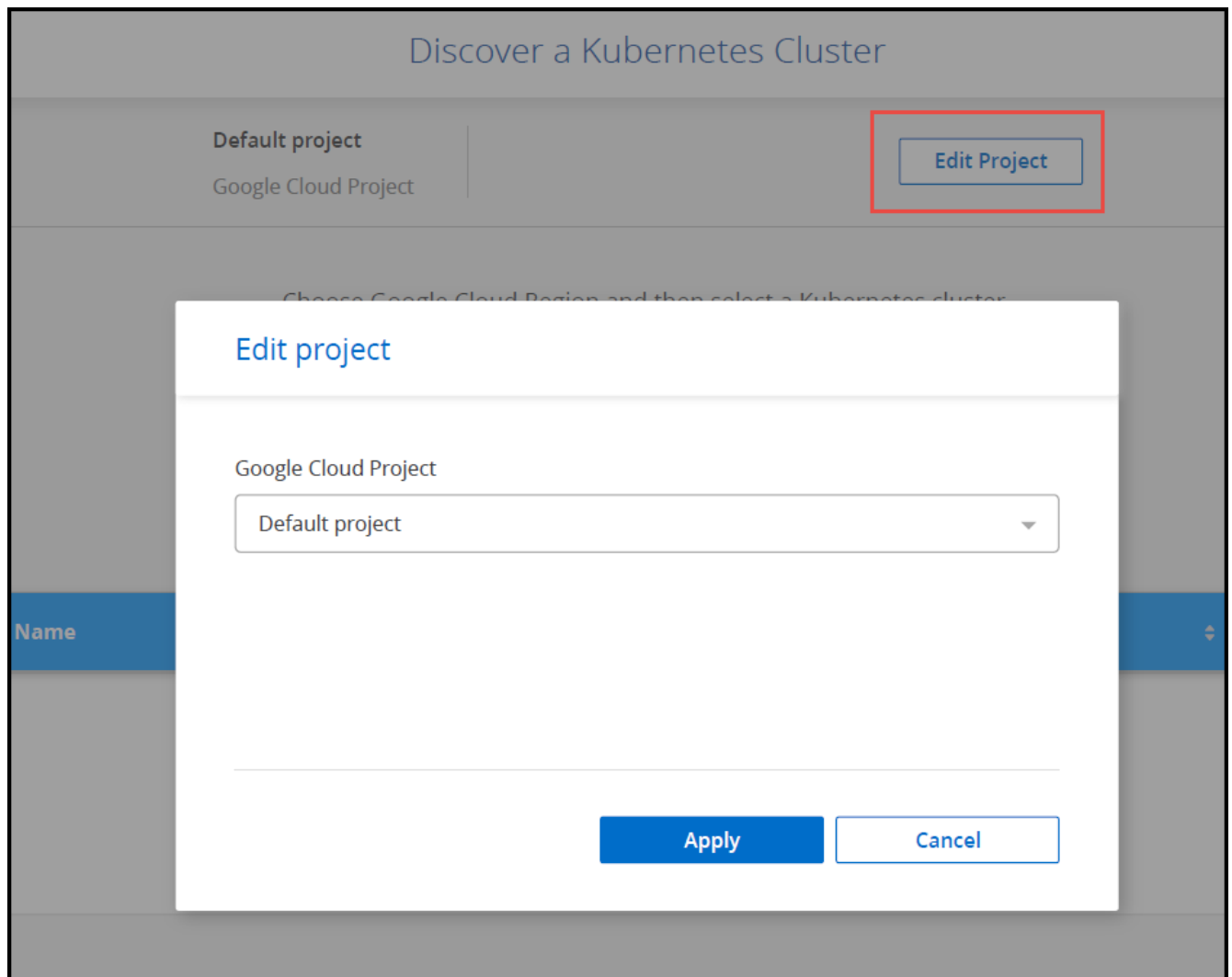
フルマネージドまたは自己管理型の Kubernetes クラスタを検出できます。管理対象クラスタが検出されている必要があります。インポートすることはできません。

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 > Discover *を選択します。

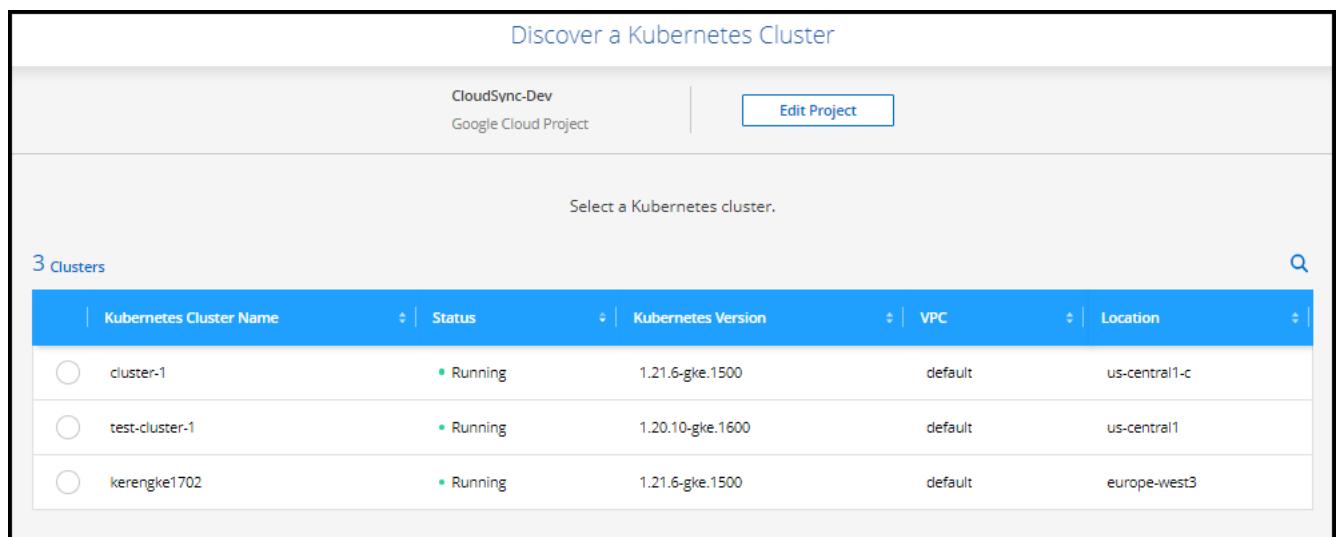


3. [Discover Cluster] を選択し、[Next] をクリックします。
4. 別の Google Cloud プロジェクトの Kubernetes クラスタを選択するには、* プロジェクトの編集 * をクリックし、使用可能なプロジェクトを選択します。



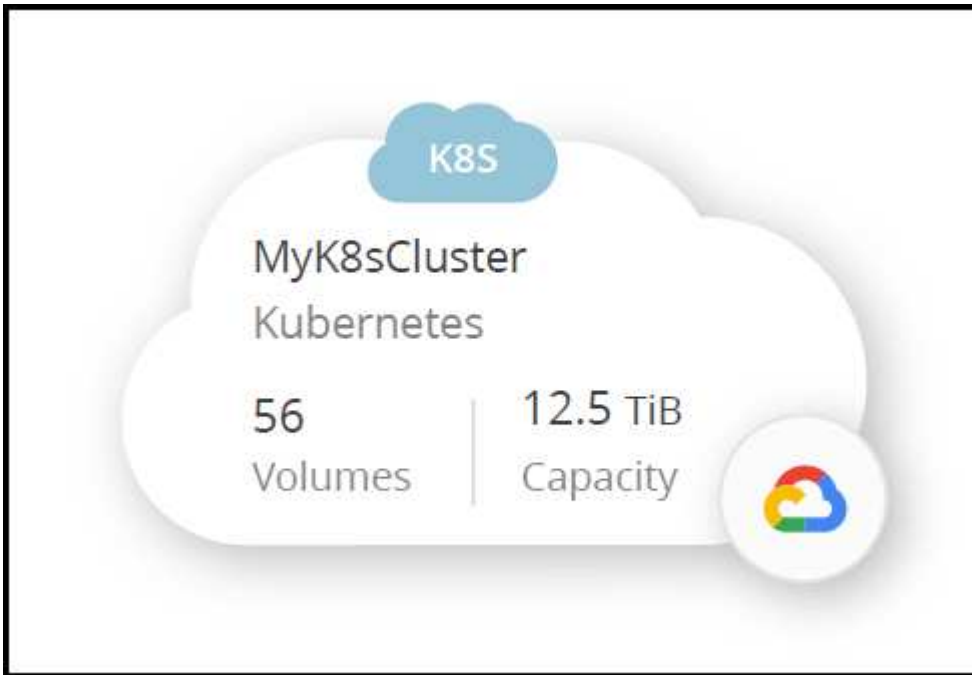
ページのスクリーンショット。"]

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



結果

BlueXPはKubernetesクラスタをCanvasに追加します。



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 > Discover *を選択します。
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

結果

BlueXPはKubernetesクラスタをCanvasに追加します。

OpenShiftクラスタをBlueXPにインポートします

自己管理OpenShiftクラスタをBlueXPにインポートして、クラウドプロバイダへの永続ボリュームのバックアップを開始できるようにします。

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。

作業を開始する前に

OpenShiftクラスタをインポートする前に、次の作業が必要です。

- で作成した「kubeconfig -sa」ファイル ["kubeconfigファイルを作成します"](#)。
- クラスタの公開認証局（ca.crtなど）、クライアントキー（tls.keyなど）、およびクライアント証明書（tls.crtなど）のファイル。

手順

1. Canvas *で、*作業環境の追加*を選択します。
2. クラウドプロバイダを選択し、* Kubernetes Cluster > Discover *を選択します。
3. [クラスタのインポート]、[次へ]の順に選択します。
4. をアップロードします kubeconfig-sa で作成したファイル ["kubeconfigファイルを作成します"](#)。Kubernetesクラスタを選択し、* Next *を選択します。

The screenshot shows the 'Import Kubernetes Cluster' window. At the top, it says 'Add Existing Kubernetes Cluster' and 'Import Kubernetes Cluster'. Below this, it instructs to 'Upload a Kubernetes configuration file that's in YAML format'. There is a text input field for the 'Kubernetes configuration file' with the value 'minicubeconfig.txt' and an 'Upload' button. Below the upload section, there is a table with the heading '1 Cluster'. The table has three columns: 'Kubernetes Cluster Name', 'Kubernetes Type', and 'Kubernetes Version'. The table contains one row with the values 'test2', 'Self Managed', and 'v1.24.0'.


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

5. 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



Client Key



Client Certificate



結果

BlueXPはKubernetesクラスタをCanvasに追加します。

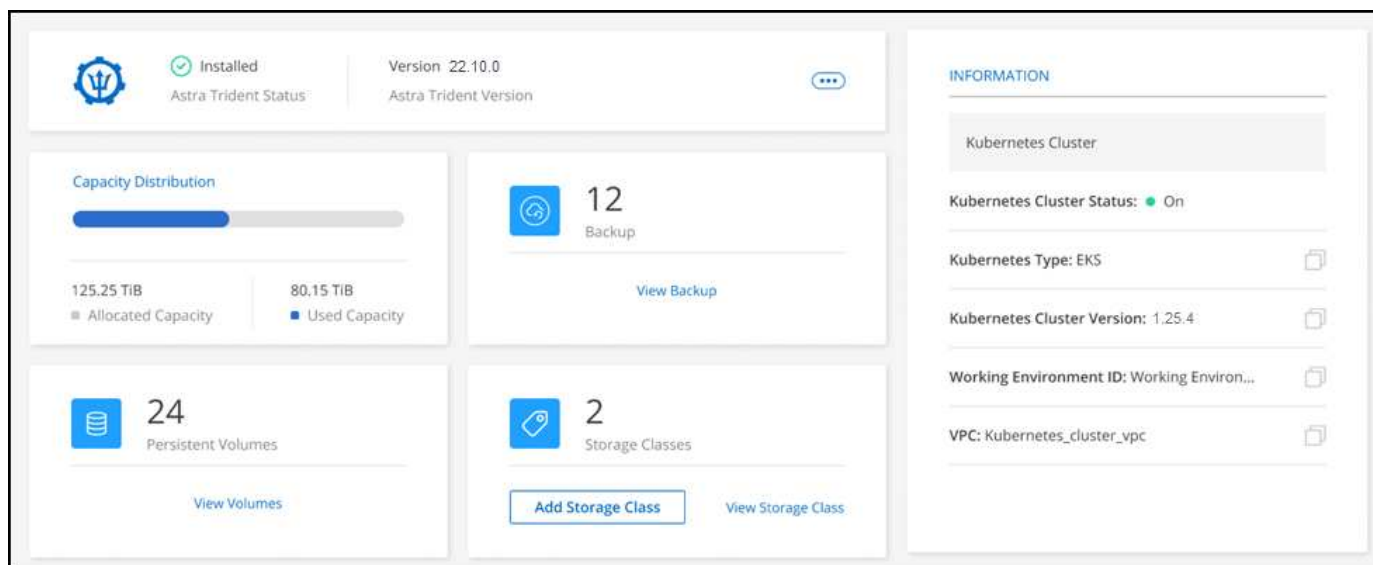
Kubernetes クラスタを管理

Trident で Astra を管理

管理対象のKubernetesクラスタをCanvasに追加したら、BlueXPを使用して、互換性のあるAstra Tridentのインストールの確認、Astra Tridentのインストールまたは最新バージョンへのアップグレード、Astra Tridentのアンインストールを行うことができます。

BlueXPのAstra Trident

BlueXPにKubernetesクラスタを追加すると、Astra TridentとKubernetesクラスタを概要ページで管理できるようになります。概要ページを開くには、CanvasでKubernetes作業環境をダブルクリックします。



サポートされるAstra Tridentバージョン

Tridentオペレータを使用して導入された、最新の4つのバージョンのAstra Tridentのうちの1つ（手動またはHelmチャートを使用）が必要です。Astra Trident がインストールされていない場合や、互換性のないバージョンのAstra Trident がインストールされている場合は、クラスタに必要な処理があることが表示されます。



を使用してTridentを導入 `tridentctl` はサポートされていません。を使用してAstra Tridentを導入した場合 ``tridentctl`` の場合、BlueXPを使用してKubernetesクラスタを管理したり、Astra Tridentをアンインストールしたりすることはできません。実行する必要があります。を使用して手動でAstra Tridentを再インストールします **"Tridentオペレータ"** またはを使用してBlueXPで使用できます **Astra Tridentのインストールまたはアップグレード**。

Astra Trident の詳細については、を参照してください **"Astra Trident のドキュメント"**。

Astra Tridentのインストールまたはアップグレード

Astra Tridentのインストールステータスとバージョンは概要ページで確認できます。Astra Tridentがまだインストールされていない場合や互換性のないバージョンがインストールされている場合は、BlueXPを使用して

管理できます。

手順

1. キャンバスで Kubernetes 作業環境をダブルクリックするか、* 作業環境の入力 * をクリックします。
 - a. Astra Trident がインストールされていない場合は、* Trident のインストール * をクリックします。

1 | Install Astra Trident

Astra Trident enables management of storage resources across all popular NetApp storage platforms.

Install Trident

- b. サポートされていないバージョンのAstra Tridentがインストールされている場合は、* Tridentのアップグレード*をクリックします。

Upgrade Astra Trident

Astra Trident enables management of storage resources across all popular NetApp storage platforms.

Upgrade Trident



BlueXPを使用して、21.01より前のバージョンのAstra Tridentからアップグレードすることはできません。以前のバージョンからアップグレードするには、を参照してください ["オペレータにアップグレードしてください"](#)。

結果

最新バージョンの Astra Trident がインストールされている。ストレージクラスを追加できるようになりました。

Astra Trident をアンインストール

BlueXPまたはTridentオペレータ（Helmまたは手動）を使用してAstra Tridentをインストールした場合は、BlueXPを使用してアンインストールできます。



- Astra Tridentをアンインストールしたあとに新しい永続ボリュームを作成することはできませんが、既存のボリュームは引き続き使用できます。
- Astra Tridentのアンインストール中はバックアップを使用できません。
- Astra Tridentを作業環境にいつでも再インストールして、クラスタの管理を継続できます。

BlueXPを使用してAstra Tridentをアンインストールしても、インストール時に適用されたAstra Tridentサービスがすべて削除されるわけではありません。Astra Tridentで作成されるすべてのカスタムリソース定義（CRD）を含め、Astra Tridentを完全に削除する方法については、を参照してください ["Tridentオペレータを使用してアンインストールします"](#)

手順

1. 概要ページで、省略記号と* Uninstall Astra Trident *を選択します。



2. [Uninstall]*を選択して、Astra Tridentを確認してアンインストールします。

結果

作業環境からAstra Tridentがアンインストールされました。Astra Tridentはいつでも再インストールできます。

ストレージクラスを管理する

キャンバスに管理対象のKubernetesクラスタを追加したら、BlueXPを使用してストレージクラスを管理できます。



ストレージクラスが定義されていない場合は、「必須」の操作がクラスタに表示されます。Canvas上のクラスタをダブルクリックすると、アクションページが開き、ストレージクラスが追加されます。

ストレージクラスを追加します

手順

1. キャンバスから、Kubernetes作業環境をCloud Volumes ONTAP またはAmazon FSX for ONTAP 作業環境にドラッグアンドドロップして、ストレージクラスウィザードを開きます。
2. ストレージクラスの名前を指定します。
3. 「* Filesystem 」または「 Block * storage」を選択します。
 - a. **Block** storageの場合は、File System Type (fstype) を選択します。

Storage Class Name

-cm

Storage Class

☐ Filesystem ☒ Block

Select File System Type

ext4

ext4

ext3

xfs

Storage Class Economy ⓘ

Support Volume Expansion ☒ Yes ☐ No

Volume Binding Mode ☒ Immediate ☐ WaitForFirstConsumer

Set as Default Storage Class ☒ Yes ☐ No

- b. * Block または Filesystem *ストレージの場合、ストレージクラスの経済性を有効にすることができます。

Storage Class ☒ Filesystem ☐ Block

Storage Class Economy ⓘ ☒ Enable Economy for Storage Class

Support Volume Expansion ☒ Yes ☐ No

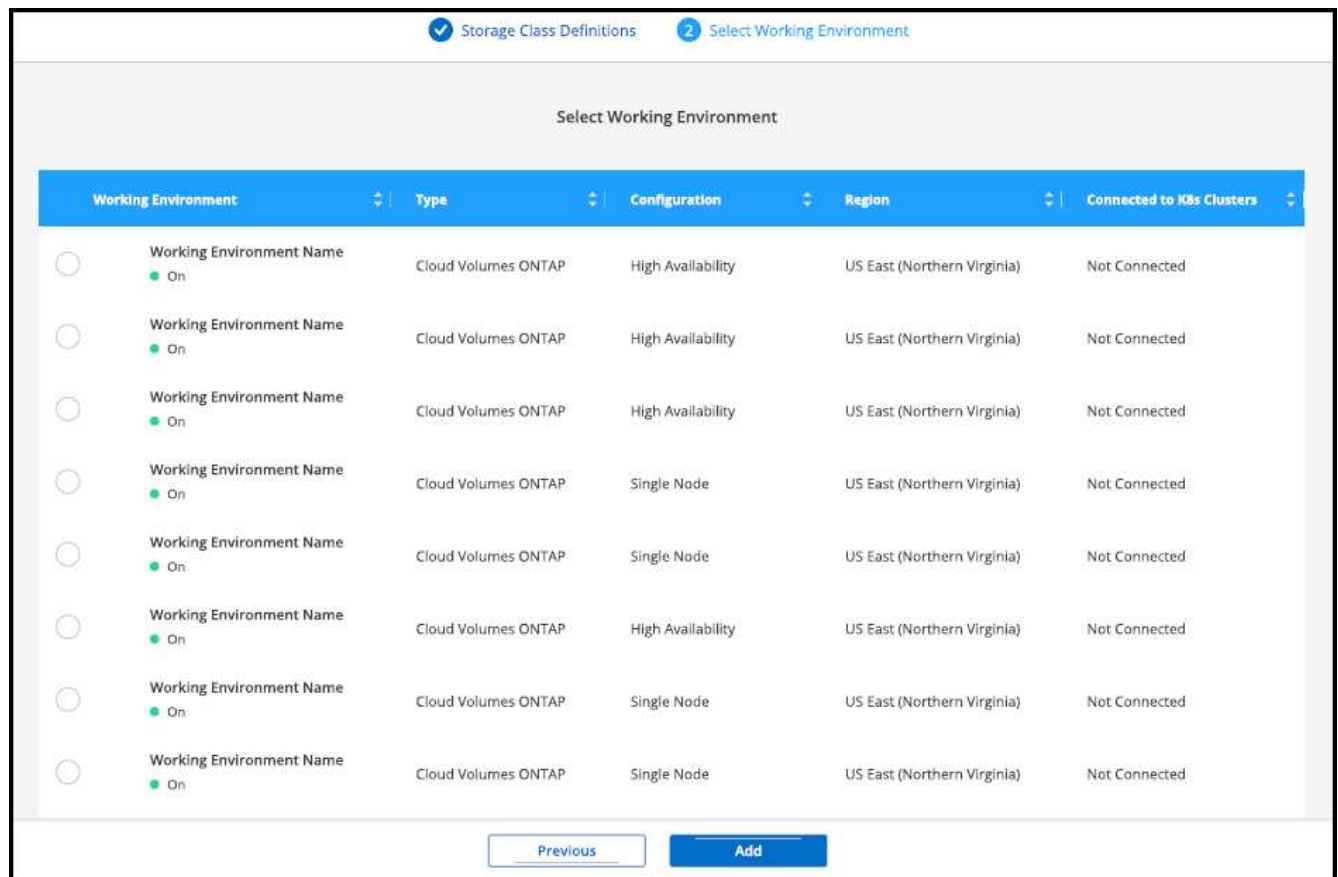
Volume Binding Mode ☒ Immediate ☐ WaitForFirstConsumer

Set as Default Storage Class ☒ Yes ☐ No



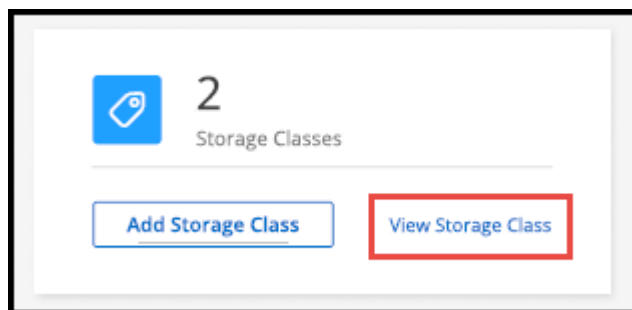
ストレージクラスエコノミーを使用している場合、バックアップとリストアはサポートされません。

- ボリュームの拡張、ボリュームバインド、およびデフォルトのストレージクラスに関するオプションを選択します。「* 次へ *」をクリックします。
- クラスタに接続する作業環境を選択します。[追加 (Add)] をクリックします。



結果

をクリックすると、Kubernetes クラスタのリソースページでストレージクラスを表示できます。



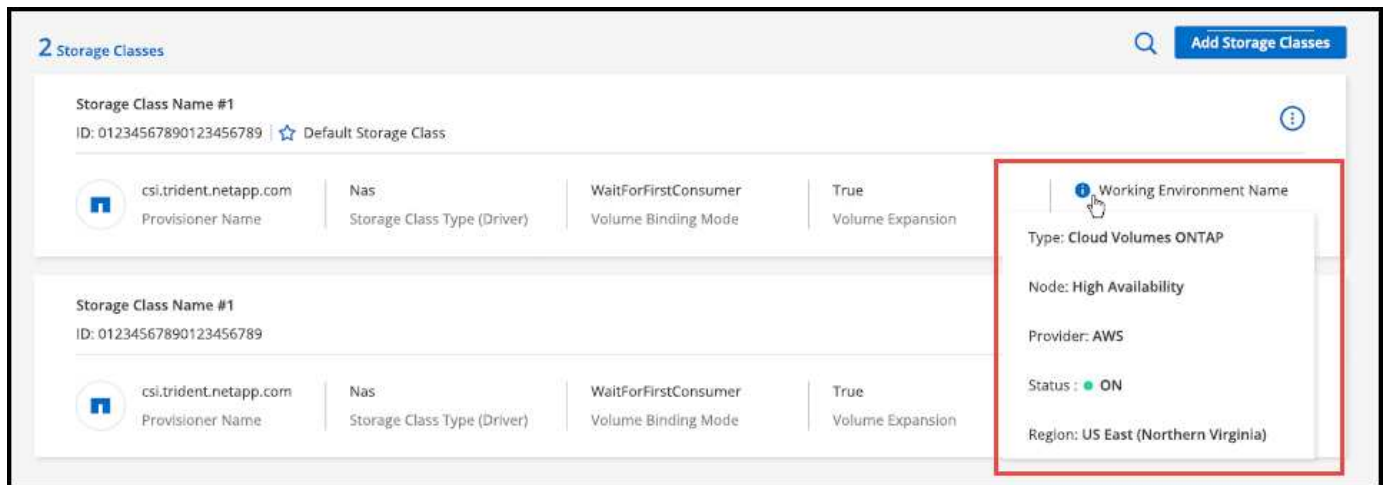
作業環境の詳細を表示

手順

1. キャンバスで Kubernetes 作業環境をダブルクリックするか、* 作業環境の入力 * をクリックします。
2. [* ストレージクラス *] タブをクリックします。
3. 情報アイコンをクリックして、作業環境の詳細を確認します。

結果

作業環境の詳細パネルが開きます。



デフォルトのストレージクラスを設定

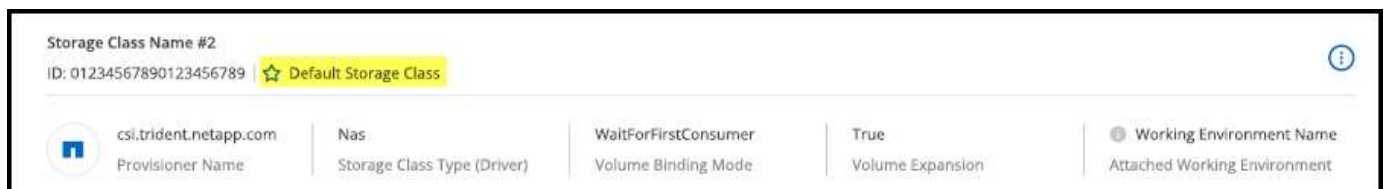
手順

1. キャンバスで Kubernetes 作業環境をダブルクリックするか、* 作業環境の入力 * をクリックします。
2. [* ストレージクラス *] タブをクリックします。
3. ストレージクラスのアクションメニューをクリックし、* デフォルトに設定 * をクリックします。



結果

選択したストレージクラスがデフォルトとして設定されます。



ストレージクラスを削除する

手順

1. キャンバスで Kubernetes 作業環境をダブルクリックするか、* 作業環境の入力 * をクリックします。
2. [* ストレージクラス *] タブをクリックします。
3. ストレージクラスのアクションメニューをクリックし、* デフォルトに設定 * をクリックします。



4. [削除] をクリックして、ストレージクラスの削除を確認します。



結果

選択したストレージクラスが削除されます。

永続ボリュームを表示します

キャンバスに管理対象のKubernetesクラスタを追加すると、BlueXPを使用して永続ボリュームを表示できるようになります。



BlueXPは、Kubernetesクラスタでバックエンドの変更を監視し、新しいボリュームが追加されると永続ボリュームテーブルを更新します。クラスタで自動バックアップが設定されている場合、新しい永続ボリュームでは自動的にバックアップが有効になります。

手順

1. キャンバスで Kubernetes 作業環境をダブルクリックするか、* 作業環境の入力 * をクリックします。
2. 概要 * タブで * ボリュームの表示 * をクリックするか、* 永続ボリューム * タブをクリックします。永続ボリュームが設定されていない場合は、を参照してください ["プロビジョニング"](#) Astra Trident でのボリュームのプロビジョニングの詳細については、

結果

設定されている永続ボリュームの表が表示されます。

Volumes Summary

8

Total Volumes

400

GiB

Total Allocated Capacity

201.2

GiB

Total Used Capacity

8 Volumes

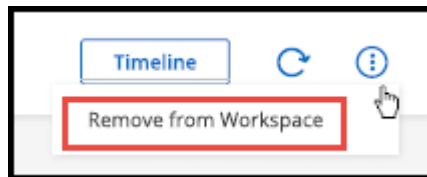
Volume Name	Name Space	Storage Class	Access Mode	Allocated Capacity	Used Capacity
Volumes Very Long Name <div>● On</div>	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB
Volumes Very Long Name <div>● On</div>	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB

Kubernetes クラスタをワークスペースから削除

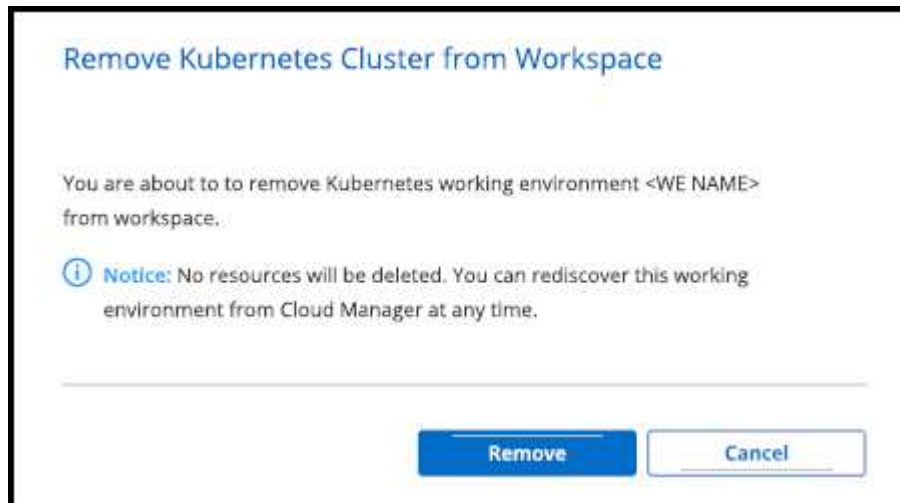
管理対象KubernetesクラスタをCanvasに追加すると、BlueXPを使用してワークスペースからクラスタを削除できます。

手順

1. キャンバスで Kubernetes 作業環境をダブルクリックするか、* 作業環境の入力 * をクリックします。
2. ページの右上にあるアクションメニューを選択し、* ワークスペースから削除 * をクリックします。



3. ワークスペースからのクラスタの削除を確認するには、* Remove * をクリックします。このクラスタはいつでも再検出できます。



結果

Kubernetes クラスタがワークスペースから削除され、キャンバスに表示されなくなります。

ネットアップのクラウドデータサービスを **Kubernetes** クラスターで使用

管理対象のKubernetesクラスターを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。

BlueXPのバックアップとリカバリを使用して、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。


"BlueXPのバックアップとリカバリを使用してKubernetesクラスターのデータを保護する方法をご紹介します"


Restore


Kubernetes

1 Selected Kubernetes Clusters


Backup Settings


 1
Kubernetes Clusters

 5
Protected PVs











 97.66 KB
Total Backups Size

Protected Persistent Volumes Status

 5
Healthy Backup

 0
Failed Backup

5 Backup Jobs

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

BlueXPとそのストレージソリューションおよびサービスに固有のテクニカルサポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウドプロバイダのファイルサービスでNetAppのサポートは有効になりません。クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- ["ONTAP 対応の Amazon FSX"](#)
- ["Azure NetApp Files の特長"](#)
- ["Cloud Volumes Service for Google Cloud"](#)

サポート登録の概要

サポート資格を有効にする登録には、次の2つの形式があります。

- BlueXPアカウントIDサポートサブスクリプションの登録(BlueXPの[サポートリソース]ページにある20桁の960xxxxxxxxxシリアル番号)。

これは、BlueXP内のすべてのサービスのシングルサポートサブスクリプションIDとして機能します。各BlueXPアカウントレベルのサポート契約が登録されている必要があります。

- クラウドプロバイダのマーケットプレイスでのサブスクリプションに関連付けられているCloud Volumes ONTAP のシリアル番号を登録している (909201xxxxxxxxのシリアル番号) 。

これらのシリアル番号は、通常PAY_GOシリアル番号と呼ばれ、Cloud Volumes ONTAP の導入時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録することで、サポートチケットのオープンやケースの自動生成などの機能を利用できます。登録を完了するには、以下の手順でNetApp Support Site (NSS) アカウントをBlueXPに追加してください。

NetAppサポートにBlueXPアカウントに登録します

サポートに登録してサポート利用資格をアクティブ化するには、BlueXPアカウントの1人のユーザがNetApp Support SiteアカウントをBlueXPログインに関連付ける必要があります。ネットアップサポートへの登録方法は、NetApp Support Site (NSS) アカウントがあるかどうかによって異なります。

NSSアカウントをお持ちの既存のお客様

NSSアカウントをお持ちのネットアップのお客様は、BlueXPからサポートに登録するだけで済みます。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[クレデンシャル]*を選択します。

2. [ユーザクレデンシャル]*を選択します。
3. [NSSクレデンシャルの追加]*を選択し、NetApp Support Site (NSS) 認証プロンプトに従います。
4. 登録プロセスが正常に完了したことを確認するには、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。

[リソース]ページに、アカウントがサポートに登録されていることが表示されます。



他のBlueXPユーザにNetApp Support Siteアカウントが関連付けられていない場合、このサポート登録ステータスは表示されません。ただし、BlueXPアカウントがサポートに登録されていないわけではありません。アカウント内の1人のユーザがこれらの手順を実行している限り、アカウントは登録されています。

NSSアカウントを持たない既存のお客様

NetAppの既存のお客様で、ライセンスとシリアル番号は_NO_NSSアカウントしかお持ちでない場合は、NSSアカウントを作成してBlueXPログインに関連付ける必要があります。

手順

1. を実行してNetApp Support Site アカウントを作成します ["NetApp Support Site ユーザー登録フォーム"](#)
 - a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
 - b. 必ず、上記のシリアル番号フィールドに使用されているBlueXPアカウントのシリアル番号(960xxxx)をコピーしてください。これにより、アカウント処理が高速化されます。
2. の手順を実行して、新しいNSSアカウントをBlueXPログインに関連付けます [NSSアカウントをお持ちの既存のお客様](#)。

ネットアップのソリューションを初めて導入する場合は

ネットアップ製品を初めてご利用になり、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

手順

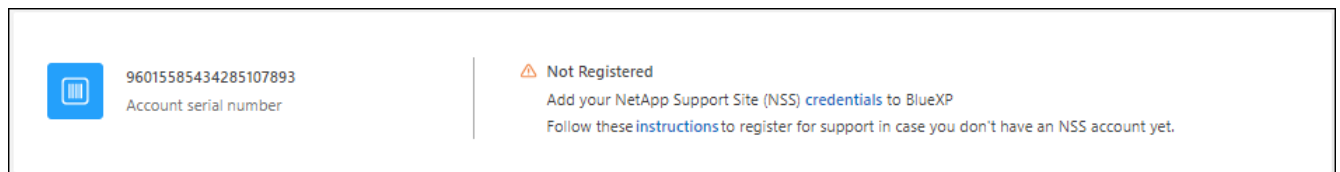
1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット

ト。サポートは最初に表示されるオプションです"]

2. サポート登録ページでアカウントIDのシリアル番号を確認します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. に移動します **"ネットアップサポート登録サイト"** 「ネットアップ登録のお客様ではありません」を選択します。
4. 必須フィールドに入力します（赤いアスタリスクのフィールド）。
5. [製品ライン（Product Line）]フィールドで、[Cloud Manager *]を選択し、該当する課金プロバイダーを選択します。
6. 上記の手順2からアカウントのシリアル番号をコピーし、セキュリティチェックを完了して、ネットアップのグローバルデータプライバシーポリシーを確認します。

この安全なトランザクションを完了するために、メールボックスに電子メールがすぐに送信されます。確認メールが数分で届かない場合は、必ずスパムフォルダを確認してください。

7. Eメールからアクションを確認します。

確認ではネットアップにリクエストが送信され、NetApp Support Site アカウントを作成することを推奨します。

8. を実行してNetApp Support Site アカウントを作成します **"NetApp Support Site ユーザー登録フォーム"**
 - a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
 - b. シリアル番号フィールドには、上記のアカウントのシリアル番号（960xxxx）を必ずコピーしてください。これにより、アカウント処理が高速化されます。

完了後

このプロセスについては、ネットアップからご連絡ください。これは、新規ユーザ向けの1回限りのオンボーディング演習です。

NetApp Support Siteアカウントを作成したら、の順序を実行してアカウントをBlueXPログインに関連付けます [NSSアカウントをお持ちの既存のお客様](#)。

Cloud Volumes ONTAPサポートのためにNSSクレデンシャルを関連付けます

NetApp Support Siteで次の主要なワークフローを有効にするには、BlueXPアカウントにクレデンシャルを関連付ける必要がCloud Volumes ONTAPあります。

- 従量課金制のCloud Volumes ONTAPシステムのサポートを登録しています

お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、NSS アカウントを用意する必要があります。

- お客様所有のライセンスを使用（BYOL）する場合のCloud Volumes ONTAP の導入

ライセンスキーをBlueXPでアップロードし、購入した契約期間のサブスクリプションを有効にするには、NSSアカウントを提供する必要があります。これには、期間の更新の自動更新も含まれます。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードしています

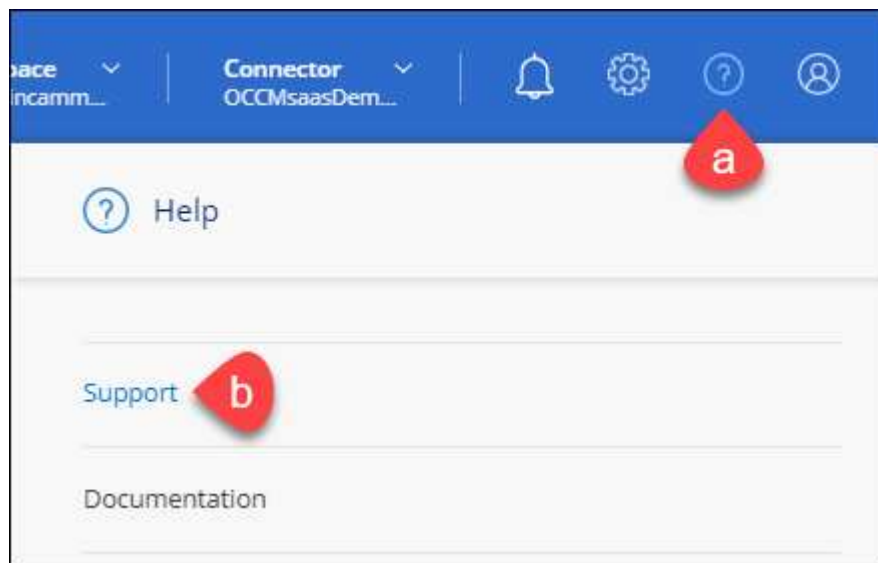
NSSクレデンシャルをBlueXPアカウントに関連付ける方法は、BlueXPユーザログインに関連付けられたNSSアカウントとは異なります。

これらのNSSクレデンシャルは、特定のBlueXPアカウントIDに関連付けられています。BlueXPアカウントに属するユーザは、*[サポート]>[NSS管理]*からこれらのクレデンシャルにアクセスできます。

- お客様レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することもできます。
- パートナーアカウントまたはリセラーアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することはできますが、お客様レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [NSS Management]>[Add NSS Account]*を選択します。
3. プロンプトが表示されたら、*続行*を選択してMicrosoftログインページにリダイレクトします。

NetAppでは、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

4. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

これらのアクションにより、BlueXPはライセンスのダウンロード、ソフトウェアのアップグレード検証、および将来のサポート登録などの目的でNSSアカウントを使用できます。

次の点に注意してください。

- NSSアカウントは、お客様レベルのアカウントである必要があります（ゲストアカウントや一時アカウントではありません）。複数のお客様レベルのNSSアカウントを設定できます。
- NSSアカウントがパートナーレベルのアカウントの場合、作成できるNSSアカウントは1つだけです。お客様レベルのNSSアカウントを追加しようとすると、パートナーレベルのアカウントが存在する場合は、次のエラーメッセージが表示されます。

「別のタイプのNSSユーザーがすでに存在するため、このアカウントではNSS顧客タイプは許可されていません。」

既存のお客様レベルのNSSアカウントがあり、パートナーレベルのアカウントを追加しようとする場合も同様です。

- ログインに成功すると、ネットアップはNSSのユーザ名を保存します。

これはシステムによって生成されたIDで、電子メールにマッピングされます。[NSS Management]ページで、から電子メールを表示できます [...](#) メニュー。

- ログイン認証情報トークンを更新する必要がある場合は、の[認証情報の更新*]オプションも使用できます [...](#) メニュー。

このオプションを使用すると、再度ログインするように求められます。これらのアカウントのトークンは90日後に期限切れになります。このことを通知する通知が投稿されます。

ヘルプを表示します

ネットアップでは、BlueXPとそのクラウドサービスをさまざまな方法でサポートしています。ナレッジベース（KB）記事やコミュニティフォーラムなど、24時間365日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

クラウドプロバイダのファイルサービスのサポート

クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- ["ONTAP 対応の Amazon FSX"](#)
- ["Azure NetApp Files の特長"](#)
- ["Cloud Volumes Service for Google Cloud"](#)

BlueXPおよびそのストレージソリューションとサービスに固有のテクニカルサポートを受けるには、以下に記載されているサポートオプションを使用してください。

セルフサポートオプションを使用します

次のオプションは、1日24時間、週7日間無料でご利用いただけます。

- ドキュメント

現在表示しているBlueXPのマニュアル。

- ["ナレッジベース"](#)

BlueXPナレッジベースで問題のトラブルシューティングに役立つ記事を検索します。

- ["コミュニティ"](#)

BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりできます。

ネットアップサポートと一緒にケースを作成します

上記のセルフサポートオプションに加え、サポートを有効にしたあとで問題が発生した場合は、ネットアップサポートの担当者と相談して解決できます。

始める前に

- [ケースの作成]*機能を使用するには、最初にNetApp Support SiteクレデンシャルをBlueXPログインに関連付ける必要があります。 ["BlueXPログインに関連付けられているクレデンシャルの管理方法について説明します"](#)。
- シリアル番号のあるONTAPシステムのケースをオープンする場合は、そのシステムのシリアル番号にNSSアカウントを関連付ける必要があります。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. **[Resources]**ページで、**[Technical Support]**で次のいずれかのオプションを選択します。
 - a. 電話で誰かと話をしたい場合は、*[電話]*を選択します。netapp.comのページに移動し、電話番号が表示されます。
 - b. [ケースの作成]*を選択して、NetAppサポートスペシャリストとのチケットをオープンします。
 - **Service:**問題 が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能を備えたテクニカルサポート問題 に固有のBlueXPなどです。
 - **作業環境:**ストレージに該当する場合は、* Cloud Volumes ONTAP *または*オンプレミス*を選択し、関連する作業環境を選択します。


作業環境のリストは、サービスの上部バナーで選択したBlueXPアカウント、ワークスペース、コネクタの範囲内にあります。

- ケース優先度：ケースの優先度を選択します。優先度は、[低]、[中]、[高]、[クリティカル]のいずれかになります。

これらの優先度の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスポインタを合わせます。

- *事象の説明*：実行したエラーメッセージやトラブルシューティング手順など、問題の詳細な概要を入力します。
- その他のメールアドレス：この問題を他のユーザーに知らせる場合は、追加のメールアドレスを入力します。
- 添付ファイル（オプション）：一度に1つずつ、最大5つの添付ファイルをアップロードできます。

添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、およびcsv。

ntapitdemo 


NetApp Support Site Account

Service

Select ▼

Working Enviroment


Select ▼

Case Priority 

Low - General guidance ▼

Issue Description



Provide detailed description of problem, applicable error messages and troubleshooting steps taken.



Additional Email Addresses (Optional) 

Type here

Attachment (Optional)

No files selected

 Upload 

完了後

ポップアップにサポートケース番号が表示されます。ネットアップのサポート担当者がケースを確認し、すぐに対応させていただきます。

サポートケースの履歴を確認するには、*[設定]>[タイムライン]*を選択し、「サポートケースの作成」というアクションを検索します。右端のボタンをクリックすると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラーメッセージが表示される場合があります。

"選択したサービスに対してケースを作成する権限がありません"

このエラーは、NSSアカウントとそれに関連付けられているレコードの会社が、BlueXPアカウントのシリアル番号(例960xxxx) または動作環境のシリアル番号。次のいずれかのオプションを使用して、サポートを受けることができます。

- 製品内のチャットを使用します
- テクニカル以外のケースをに送信します <https://mysupport.netapp.com/site/help>

サポートケースの管理（プレビュー）

アクティブなサポートケースと解決済みのサポートケースは、BlueXPから直接表示および管理できます。NSSアカウントと会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の2つのビューがあります。
 - 左側のビューには、指定したユーザNSSアカウントによって過去3カ月間にオープンされたケースの総数が表示されます。
 - 右側のビューには、ユーザのNSSアカウントに基づいて、過去3カ月間にオープンしたケースの総数が会社レベルで表示されます。

テーブルの結果には、選択したビューに関連するケースが反映されます。

- 目的の列を追加または削除したり、[優先度]や[ステータス]などの列の内容をフィルタリングしたりできます。他の列には、並べ替え機能だけがあります。

詳細については、以下の手順を参照してください。

- ケースごとに、ケースノートを更新したり、ステータスが「Closed」または「Pending Closed」でないケースをクローズしたりすることができます。

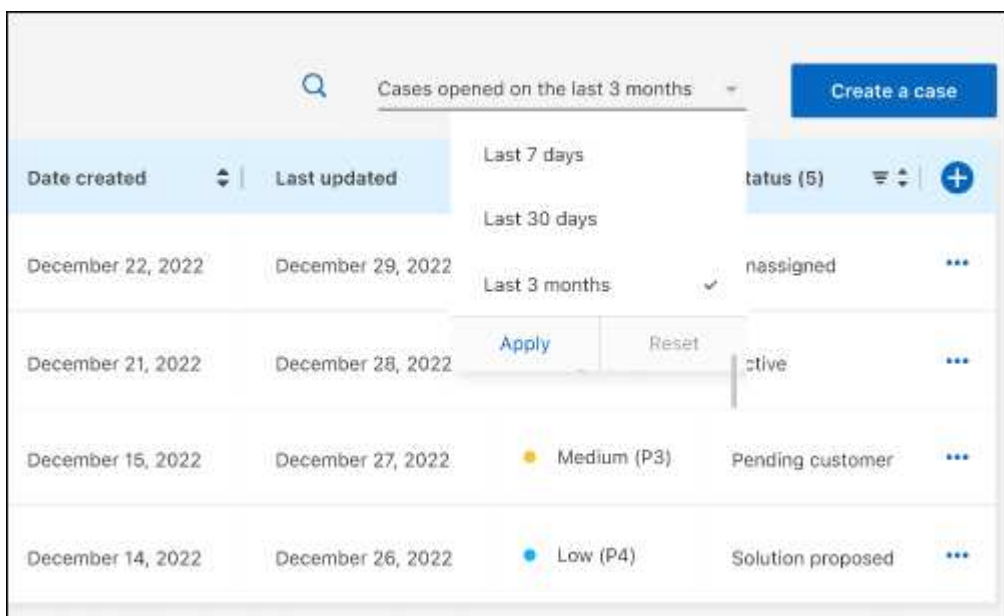
手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [ケース管理]*を選択し、プロンプトが表示されたらNSSアカウントをBlueXPに追加します。

ケース管理*ページには、BlueXPユーザアカウントに関連付けられたNSSアカウントに関連するオープンケースが表示されます。これは、*NSS管理*ページの上部に表示されるNSSアカウントと同じです。

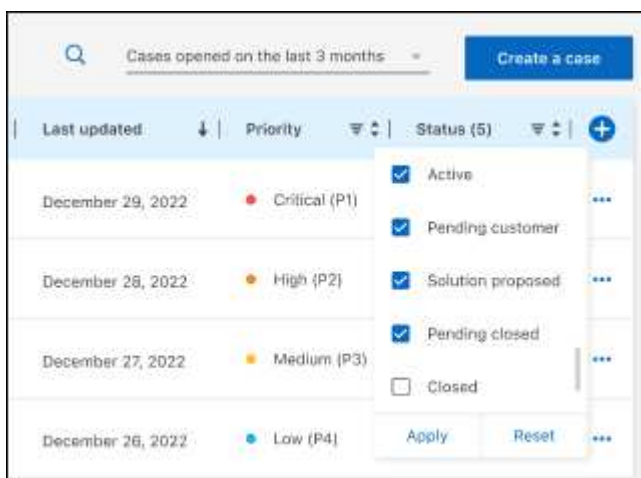
3. 必要に応じて、テーブルに表示される情報を変更します。

- [Organization's Cases]*で[View]*を選択すると、会社に関連付けられているすべてのケースが表示されます。
- 正確な日付範囲を選択するか、別の期間を選択して、日付範囲を変更します。




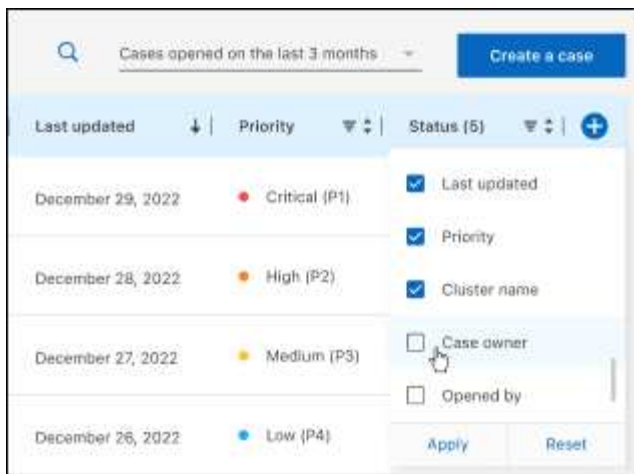
ページのテーブルの上にあるオプションのスクリーンショット。正確な日付範囲、または過去7日、30日、または3カ月を選択できます。"]

- 列の内容をフィルタリングします。



列のフィルタオプションのスクリーンショット。[Active]や[Closed]など、特定のステータスに一致するケースを除外できます。"]

- テーブルに表示される列を変更するには、 次に、表示する列を選択します。

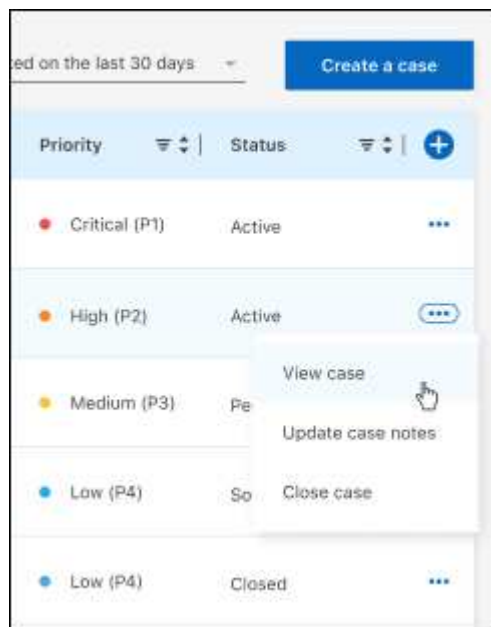


4. 既存のケースを管理するには、... 使用可能なオプションのいずれかを選択します。

- ケースの表示: 特定のケースの詳細を表示します。
- ケースノートの更新: 問題の詳細を入力するか、*ファイルのアップロード*を選択して最大5つのファイルを添付します。

添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、およびcsv。

- ケースをクローズ: ケースをクローズする理由の詳細を入力し、*ケースをクローズ*を選択します。



法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

プライバシーポリシー

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

["BlueXPに関する注意事項"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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な保証、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、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

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って保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、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。