Dokumentation für Kubernetes-Cluster

Kubernetes clusters

NetApp
December 02, 2022

This PDF was generated from https://docs.netapp.com/de-de/cloud-manager-kubernetes/index.html on December 02, 2022. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

Dokumentation für Kubernetes-Cluster

Was ist neu bei Kubernetes in BlueXP

Die Neuerungen in Kubernetes finden Sie in BlueXP (früher Cloud Manager).

06. November 2022

Wenn "Definieren von Speicherklassen", Sie können jetzt Storage-Klasse Economy für Block- oder Dateisystem-Speicher aktivieren.

18. September 2022

Selbst gemanagte OpenShift-Cluster können jetzt in Cloud Manager importiert werden.

- "Anforderungen für Kubernetes-Cluster in OpenShift"
- "Fügen Sie einem OpenShift-Cluster zu Cloud Manager hinzu"

31 Juli 2022

- Verwenden der neuen `watch` Verb in der Storage-Klasse sowie Backup- und Restore-Konfigurationen von YAML kann Cloud Manager jetzt Kubernetes-Cluster auf Änderungen am Cluster-Backend überwachen und das Backup für neue persistente Volumes automatisch aktivieren, wenn auf dem Cluster ein automatisches Backup konfiguriert wurde.

  "Anforderungen an Kubernetes-Cluster in AWS"

  "Anforderungen an Kubernetes Cluster in Azure"

  "Anforderungen für Kubernetes-Cluster in Google Cloud"

- Wenn "Definieren von Speicherklassen", Sie können jetzt einen Dateisystemtyp (fstype) für Block Storage angeben.

3 Juli 2022

- Wenn Astra Trident über den Trident Operator implementiert wurde, können Sie jetzt mithilfe von Cloud Manager auf die neueste Version von Astra Trident upgraden.

  "Installation und Management von Astra Trident"

- Sie können jetzt Ihren Kubernetes-Cluster per Drag & Drop in die Arbeitsumgebung AWS FSX for ONTAP verschieben, um eine Storage-Klasse direkt aus dem Canvas hinzuzufügen.

  "Fügen Sie eine Storage-Klasse hinzu"

6. Juni 2022

Cloud Manager verbietet jetzt Amazon FSX für ONTAP als Backend-Storage.

4 Mai 2022

Ziehen Sie die Maus per Drag-and-Drop, um eine Speicherklasse hinzuzufügen

Sie können jetzt Ihren Kubernetes-Cluster ziehen und in die Cloud Volumes ONTAP-Arbeitsumgebung ablegen, um eine Storage-Klasse direkt aus dem Canvas hinzuzufügen.

"Fügen Sie eine Storage-Klasse hinzu"

4. April 2022

Managen Sie Kubernetes-Cluster über die Seite der Cloud Manager Ressourcen

Das Kubernetes-Cluster-Management bietet jetzt eine direkte Integration in die Cluster-Arbeitsumgebung. Eine neue "Schnellstart" Starten Sie schnell.

Sie können jetzt auf der Seite „Cluster-Ressource“ die folgenden Aktionen ausführen.

- "Installation Von Astra Trident"
- "Fügen Sie Speicherklassen hinzu"
- "Anzeige persistenter Volumes"
- "Cluster entfernen"
- "Unterstützung von Datenservices"

27 Februar 2022

Unterstützung von Kubernetes-Clustern in Google Cloud

Verwaltete Google Kubernetes Engine (GKE)-Cluster und automatisierte Kubernetes-Cluster in Google Cloud können jetzt über Cloud Manager hinzugefügt und gemanagt werden.

"Erste Schritte mit Kubernetes-Clustern in der Google Cloud".

11 Januar 2022

Unterstützung für Kubernetes-Cluster in Azure

Verwaltete Azure Kubernetes-Cluster (AKS) und automatisierte Kubernetes-Cluster in Azure können jetzt mithilfe von Cloud Manager hinzugefügt und gemanagt werden.

"Erste Schritte mit Kubernetes Clustern in Azure"

28. November 2021

Unterstützung von Kubernetes-Clustern in AWS

Managed-Kubernetes-Cluster können jetzt in Canvas von Cloud Manager hinzugefügt werden, um erweitertes Datenmanagement zu ermöglichen.

- Amazon EKS Cluster entdecken
- Erstellen Sie Backups persistenter Volumes mit Cloud Backup

"Erfahren Sie mehr über die Unterstützung von Kubernetes".

Der vorhandene Kubernetes-Service (verfügbar über die Registerkarte **K8s**) ist veraltet und wird in einer zukünftigen Version entfernt.

Los geht’s

Kubernetes-Datenmanagement in BlueXP

Astra Trident ist ein vollständig von NetApp unterstütztes Open-Source-Projekt. Astra Trident lässt sich nativ mit Kubernetes und dessen Persistent Volume Framework integrieren und ermöglicht das nahtlose Bereitstellen und Managen von Volumes auf Systemen, auf denen beliebige Kombinationen von NetApp Storage-Plattformen ausgeführt werden. "Weitere Informationen zu Trident".

Funktionen

Mit einer kompatiblen Version von Astra Trident, die über den Trident Operator implementiert wurde, können Sie Ihre Kubernetes-Cluster direkt über managen "BlueXP" (Ehemals Cloud Manager)

- Installation oder Upgrade von Astra Trident:
- Hinzufügen und Managen von Clustern in Ihrer Hybrid-Cloud-Infrastruktur
- Hinzufügen und Verwalten von Speicherklassen und Verbinden dieser mit Arbeitsumgebungen.
- Backup persistenter Volumes mit Cloud Backup Service –

Unterstützte Kubernetes-Implementierungen

BlueXP unterstützt Managed-Kubernetes-Cluster in folgenden Bereichen:

- "Amazon Elastic Kubernetes Service (Amazon EKS)"
- "Microsoft Azure Kubernetes Service (AKS)"
- "Google Kubernetes Engine (GKE)"

Unterstützte Astra Trident Implementierungen

Eine der vier aktuellsten Versionen von Astra Trident "Implementierung über den Trident-Operator" Ist erforderlich.

Sie können die aktuelle Version von Astra Trident direkt von BlueXP installieren oder upgraden.

"Voraussetzungen für Astra Trident prüfen"

Unterstützter Back-End Storage

NetApp Astra Trident muss auf jedem Kubernetes Cluster installiert sein, und Cloud Volumes ONTAP oder Amazon FSX für ONTAP muss als Back-End Storage für die Cluster konfiguriert werden.

Kosten

Es fallen keine Kosten an, Ihre Kubernetes Cluster in BlueXP zu entdecken_. Beim Backup persistenter Volumes mit Cloud Backup Service fallen Ihnen die Gebühren an.

Erste Schritte mit Kubernetes Clustern

Fügen Sie in nur wenigen Schritten Kubernetes-Cluster zu BlueXP hinzu, um erweitertes Datenmanagement zu ermöglichen.

Schnellstart

Wird Verwendet "BlueXP" Sie können Kubernetes-Cluster in nur wenigen Schritten managen.

Stellen Sie sicher, dass Ihre Umgebung die Voraussetzungen für Ihren Cluster-Typ erfüllt.

"Anforderungen an Kubernetes-Cluster in AWS"

"Anforderungen an Kubernetes Cluster in Azure"

"Anforderungen für Kubernetes-Cluster in Google Cloud"

Sie können Kubernetes-Cluster hinzufügen und sie mit BlueXP mit einer Arbeitsumgebung verbinden.

"Fügen Sie einen Amazon Kubernetes-Cluster hinzu"

"Fügen Sie einen Azure Kubernetes-Cluster hinzu"

"Fügen Sie einen Google Cloud Kubernetes Cluster hinzu"

Persistente Volumes können über native Kubernetes-Schnittstellen und -Konstrukte angefordert und gemanagt werden. BlueXP erstellt NFS- und iSCSI-Speicherklassen, die Sie bei der Bereitstellung persistenter Volumes verwenden können.

"Erfahren Sie mehr über die Bereitstellung Ihres ersten Volumens mit Astra Trident".

Nachdem Sie BlueXP Kubernetes-Cluster hinzugefügt haben, können Sie die Cluster auf der BlueXP-Ressourcenseite verwalten.

"Managen Sie Kubernetes-Cluster wie."

Anforderungen

Anforderungen an Kubernetes-Cluster in AWS

Sie können verwaltete Amazon Elastic Kubernetes Service (EKS) Cluster oder automatisierte Kubernetes-Cluster auf AWS zu BlueXP hinzufügen. Bevor Sie die Cluster zu BlueXP hinzufügen können, müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind.

In diesem Thema wird *Kubernetes Cluster* verwendet, wobei die Konfiguration für EKS und selbst gemanagte Kubernetes Cluster identisch ist. Der Cluster-Typ wird bei unterschiedlich der Konfiguration angegeben.

Anforderungen

Astra Trident

Eine der vier aktuellsten Versionen von Astra Trident ist erforderlich. Sie können Astra Trident direkt von BlueXP installieren oder aktualisieren. Sollten Sie "Prüfen Sie die Voraussetzungen" Vor der Installation von Astra Trident:

Cloud Volumes ONTAP

Cloud Volumes ONTAP für AWS muss als Back-End Storage für den Cluster eingerichtet werden. "In der Astra Trident Dokumentation finden Sie die Konfigurationsschritte".

BlueXP Connector

Ein Connector muss in AWS mit den erforderlichen Berechtigungen ausgeführt werden. a Connector,Weitere Informationen finden Sie unten.

Netzwerk-Konnektivität

Zwischen dem Kubernetes-Cluster und dem Connector sowie zwischen dem Kubernetes-Cluster und Cloud Volumes ONTAP ist eine Netzwerkverbindung erforderlich. networking requirements,Weitere Informationen finden Sie unten.

RBAC-Autorisierung

Die BlueXP Connector-Rolle muss für jeden Kubernetes-Cluster autorisiert sein. up RBAC authorization,Weitere Informationen finden Sie unten.

Bereiten Sie einen Konnektor vor

Für die Erkennung und das Management von Kubernetes-Clustern ist in AWS ein BlueXP Connector erforderlich. Sie müssen einen neuen Konnektor erstellen oder einen vorhandenen Konnektor verwenden, der über die erforderlichen Berechtigungen verfügt.

Erstellen Sie einen neuen Konnektor

Folgen Sie den Schritten in einem der nachfolgenden Links.

- "Erstellen Sie einen Connector von BlueXP" (Empfohlen)
- "Erstellen Sie einen Connector aus dem AWS Marketplace"

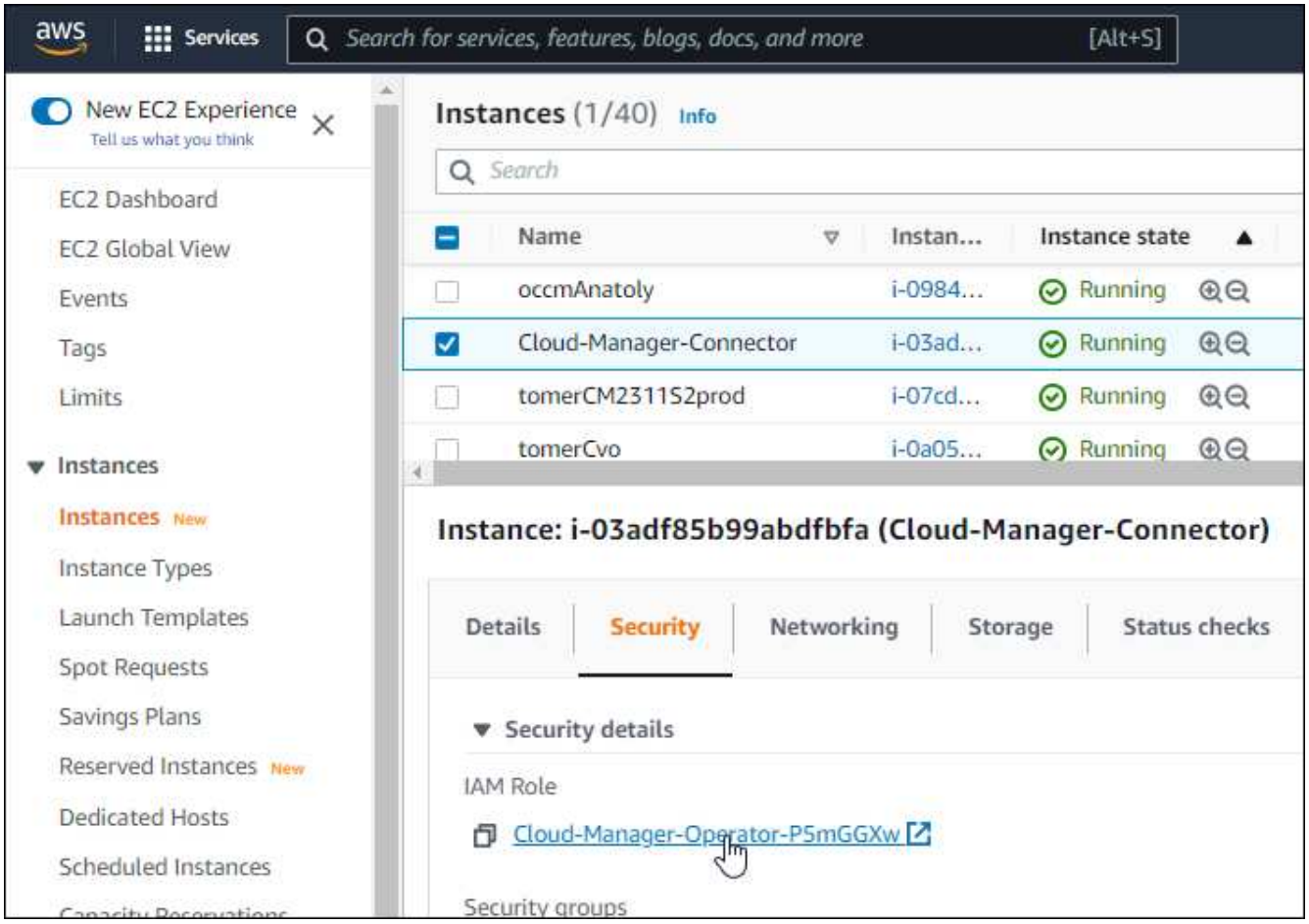
- "Installieren Sie den Connector auf einem vorhandenen Linux-Host in AWS"

Fügen Sie die erforderlichen Berechtigungen einem vorhandenen Konnektor hinzu

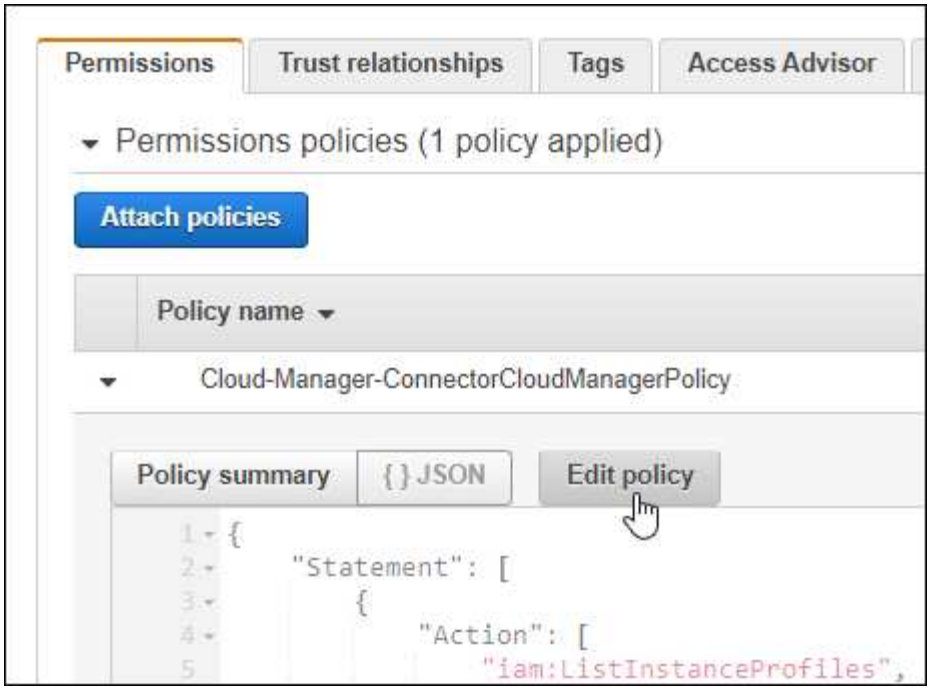
Ab Version 3.9.13 enthalten alle neu erstellten _Connectors drei neue AWS Berechtigungen, die das Erkennen und Managen von Kubernetes-Clustern ermöglichen. Wenn Sie vor dieser Version einen Connector erstellt haben, müssen Sie die vorhandene Richtlinie für die IAM-Rolle des Connectors ändern, um die Berechtigungen bereitzustellen.

Schritte

1. Gehen Sie zur AWS Konsole und öffnen Sie den EC2 Service.
2. Wählen Sie die Connector-Instanz aus, klicken Sie auf **Sicherheit** und klicken Sie auf den Namen der IAM-Rolle, um die Rolle im IAM-Service anzuzeigen.



3. Erweitern Sie auf der Registerkarte **Berechtigungen** die Richtlinie und klicken Sie auf **Richtlinie bearbeiten**.



4. Klicken Sie auf **JSON** und fügen Sie unter dem ersten Satz von Aktionen die folgenden Berechtigungen hinzu:

   - ec2:DescribeRegionen
   - eks:ListClusters
   - eks:DescribeCluster
   - iam:GetInstanceProfile

   "Zeigen Sie das vollständige JSON-Format für die Richtlinie an"

5. Klicken Sie auf **Richtlinie überprüfen** und dann auf **Änderungen speichern**.

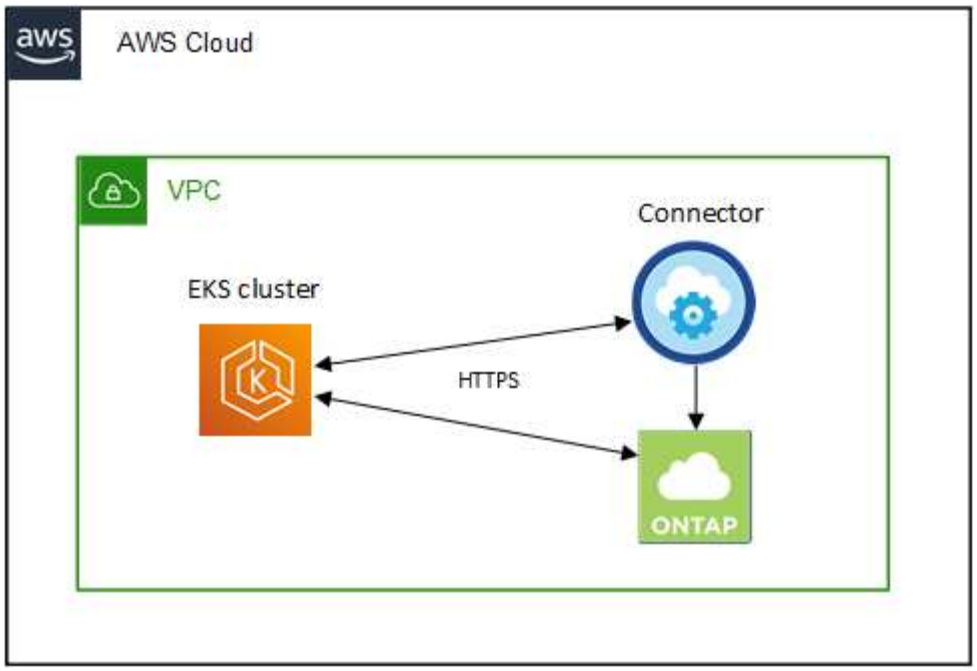
Netzwerkanforderungen prüfen

Sie müssen für die Netzwerkverbindung zwischen dem Kubernetes-Cluster und dem Connector sowie zwischen dem Kubernetes-Cluster und dem Cloud Volumes ONTAP-System sorgen, das dem Cluster Back-End-Storage bereitstellt.

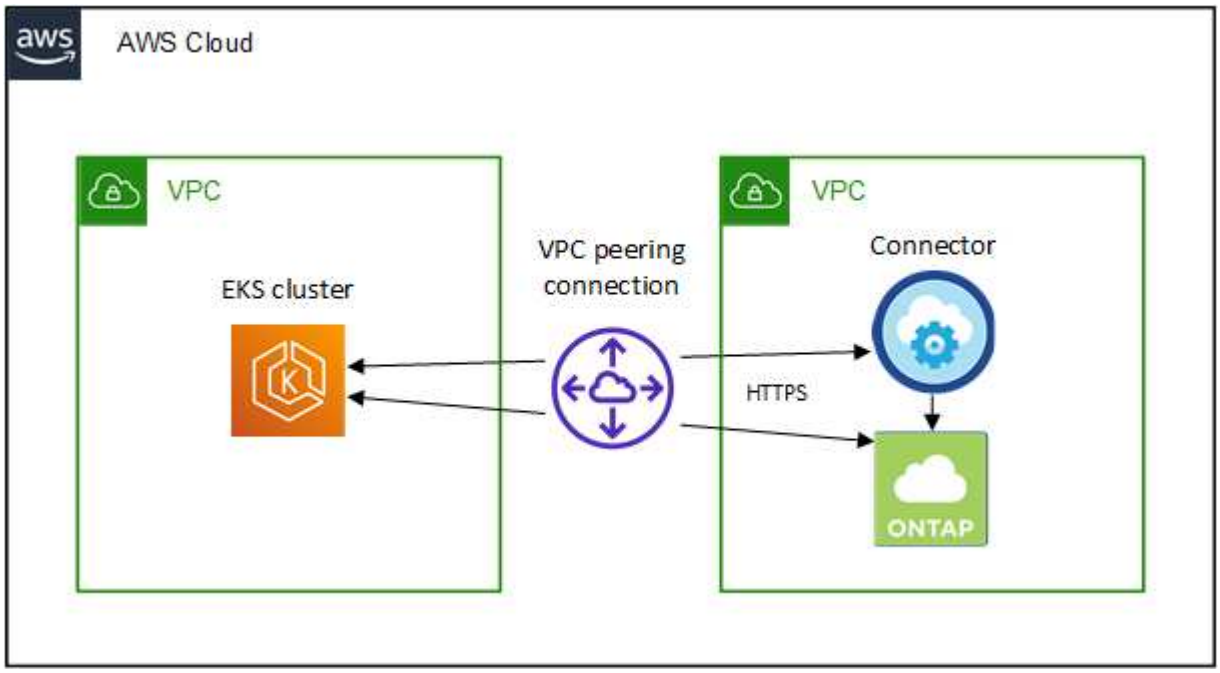
- Jeder Kubernetes-Cluster muss über eine eingehende Verbindung vom Connector verfügen
- Der Connector muss über Port 443 eine ausgehende Verbindung zu jedem Kubernetes-Cluster haben

Die einfachste Möglichkeit für diese Konnektivität ist die Implementierung von Connector und Cloud Volumes ONTAP in derselben VPC wie der Kubernetes-Cluster. Andernfalls müssen Sie eine VPC-Peering-Verbindung zwischen den verschiedenen VPCs einrichten.

In diesem Beispiel wird jede Komponente in derselben VPC angezeigt.



Ein weiteres Beispiel zeigt einen EKS-Cluster, der in einem anderen VPC ausgeführt wird. In diesem Beispiel stellt VPC Peering eine Verbindung zwischen der VPC für das EKS-Cluster und der VPC für den Connector und Cloud Volumes ONTAP her.



Einrichtung der RBAC-Autorisierung

Sie müssen die Connector-Rolle auf jedem Kubernetes-Cluster autorisieren, damit der Connector einen Cluster ermitteln und verwalten kann.

Es ist eine andere Autorisierung erforderlich, um andere Funktionen zu aktivieren.

Backup und Restore

Für Backup und Restore ist nur eine Grundautorisierung erforderlich.

Fügen Sie Speicherklassen hinzu

Erweiterte Autorisierung ist erforderlich, um Speicherklassen mithilfe von BlueXP hinzuzufügen und den Cluster auf Änderungen am Backend zu überwachen.

Installieren Sie Astra Trident

Zur Installation von Astra Trident müssen Sie für BlueXP die vollständige Autorisierung bereitstellen.

Bei der Installation von Astra Trident installiert BlueXP das Astra Trident Back-End und das Kubernetes Secret, das die Zugangsdaten enthält, die Astra Trident zur Kommunikation mit dem Storage-Cluster benötigt.

Schritte

1. Erstellen Sie eine Cluster-Rolle und Rollenbindung.
   a. Erstellen Sie eine YAML-Datei, die den folgenden Text enthält, der auf Ihren Autorisierungsanforderungen basiert.

Backup/Restore

Fügen Sie eine grundlegende Autorisierung hinzu, um Backup und Restore für Kubernetes-Cluster zu ermöglichen.

```
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
```

Speicherklassen

Fügen Sie erweiterte Berechtigungen hinzu, um Speicherklassen mithilfe von BlueXP hinzuzufügen.

```
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
```

Installation Von Trident

Über die Befehlszeile erhalten Sie die vollständige Autorisierung, und BlueXP kann Astra Trident installieren.

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

b. Wenden Sie die Konfiguration auf ein Cluster an.

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

2. Erstellen Sie eine Identitätszuordnung zur Berechtigungsgruppe.

Verwenden Sie eksctl

Verwenden Sie eksctl, um eine IAM-Identitätszuordnung zwischen einem Cluster und der IAM-Rolle für den BlueXP Connector zu erstellen.

"Die vollständige Anleitung finden Sie in der eksctl-Dokumentation".

Im Folgenden finden Sie ein Beispiel.

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

Bearbeiten von aws-auth

Bearbeiten Sie die aws-auth ConfigMap direkt, um dem BlueXP Connector den RBAC-Zugriff auf die IAM-Rolle hinzuzufügen.

"Vollständige Anweisungen finden Sie in der AWS EKS-Dokumentation".

Im Folgenden finden Sie ein Beispiel.

```
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
```

Anforderungen an Kubernetes Cluster in Azure

Verwaltete Azure Kubernetes-Cluster (AKS) und automatisierte Kubernetes-Cluster in Azure können mithilfe von BlueXP hinzugefügt und gemanagt werden. Bevor Sie die Cluster zu BlueXP hinzufügen können, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind.

In diesem Thema wird *Kubernetes Cluster* verwendet, wobei die Konfiguration für AKS und selbst gemanagte Kubernetes Cluster identisch ist. Der Cluster-Typ wird bei unterschiedlich der Konfiguration angegeben.

Anforderungen

Astra Trident

Eine der vier aktuellsten Versionen von Astra Trident ist erforderlich. Sie können Astra Trident direkt von BlueXP installieren oder aktualisieren. Sollten Sie "Prüfen Sie die Voraussetzungen" Vor der Installation von Astra Trident:

Cloud Volumes ONTAP

Cloud Volumes ONTAP muss als Back-End Storage für den Cluster eingerichtet werden. "In der Astra Trident Dokumentation finden Sie die Konfigurationsschritte".

BlueXP Connector

In Azure muss ein Connector mit den erforderlichen Berechtigungen ausgeführt werden. a Connector,Weitere Informationen finden Sie unten.

Netzwerk-Konnektivität

Zwischen dem Kubernetes-Cluster und dem Connector sowie zwischen dem Kubernetes-Cluster und Cloud Volumes ONTAP ist eine Netzwerkverbindung erforderlich. networking requirements,Weitere Informationen finden Sie unten.

RBAC-Autorisierung

BlueXP unterstützt RBAC-fähige Cluster mit und ohne Active Directory. Die BlueXP Connector-Rolle muss für jeden Azure-Cluster autorisiert sein. up RBAC authorization,Weitere Informationen finden Sie unten.

Bereiten Sie einen Konnektor vor

Für das Erkennen und Managen von Kubernetes-Clustern ist ein BlueXP Connector in Azure erforderlich. Sie müssen einen neuen Konnektor erstellen oder einen vorhandenen Konnektor verwenden, der über die erforderlichen Berechtigungen verfügt.

Erstellen Sie einen neuen Konnektor

Folgen Sie den Schritten in einem der nachfolgenden Links.

- "Erstellen Sie einen Connector von BlueXP" (Empfohlen)
- "Erstellen Sie einen Connector aus dem Azure Marketplace"
- "Installieren Sie den Connector auf einem vorhandenen Linux-Host"

Fügen Sie die erforderlichen Berechtigungen einem bestehenden Connector hinzu (um ein verwaltetes AKS-Cluster zu ermitteln)

Wenn Sie einen verwalteten AKS-Cluster ermitteln möchten, müssen Sie möglicherweise die benutzerdefinierte Rolle ändern, damit der Connector die Berechtigungen bereitstellen kann.

Schritte

1. Identifizieren Sie die Rolle, die der virtuellen Konnektor-Maschine zugewiesen ist:
   a. Öffnen Sie im Azure-Portal den Virtual Machines-Service.

b. Wählen Sie die virtuelle Verbindungsmaschine aus.
c. Wählen Sie unter Einstellungen **Identität** aus.
d. Klicken Sie auf **Azure Rollenzuweisungen**.
e. Notieren Sie sich die benutzerdefinierte Rolle, die der virtuellen Connector-Maschine zugewiesen ist.

2. Aktualisieren der benutzerdefinierten Rolle:
   a. Öffnen Sie im Azure-Portal Ihr Azure-Abonnement.
   b. Klicken Sie auf **Zugriffskontrolle (IAM) > Rollen**.
   c. Klicken Sie auf die Ellipsen (…) für die benutzerdefinierte Rolle und dann auf **Bearbeiten**.
   d. Klicken Sie auf JSON und fügen Sie die folgenden Berechtigungen hinzu:

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

   e. Klicken Sie auf **Review + Update** und dann auf **Update**.

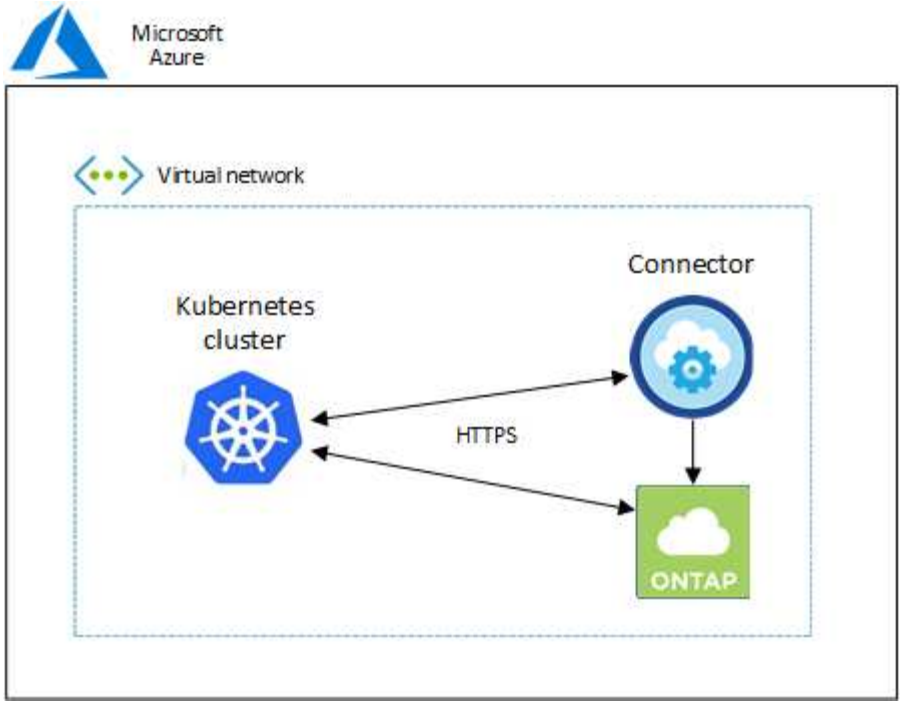
Netzwerkanforderungen prüfen

Sie müssen für die Netzwerkverbindung zwischen dem Kubernetes-Cluster und dem Connector sowie zwischen dem Kubernetes-Cluster und dem Cloud Volumes ONTAP-System sorgen, das dem Cluster Back-End-Storage bereitstellt.

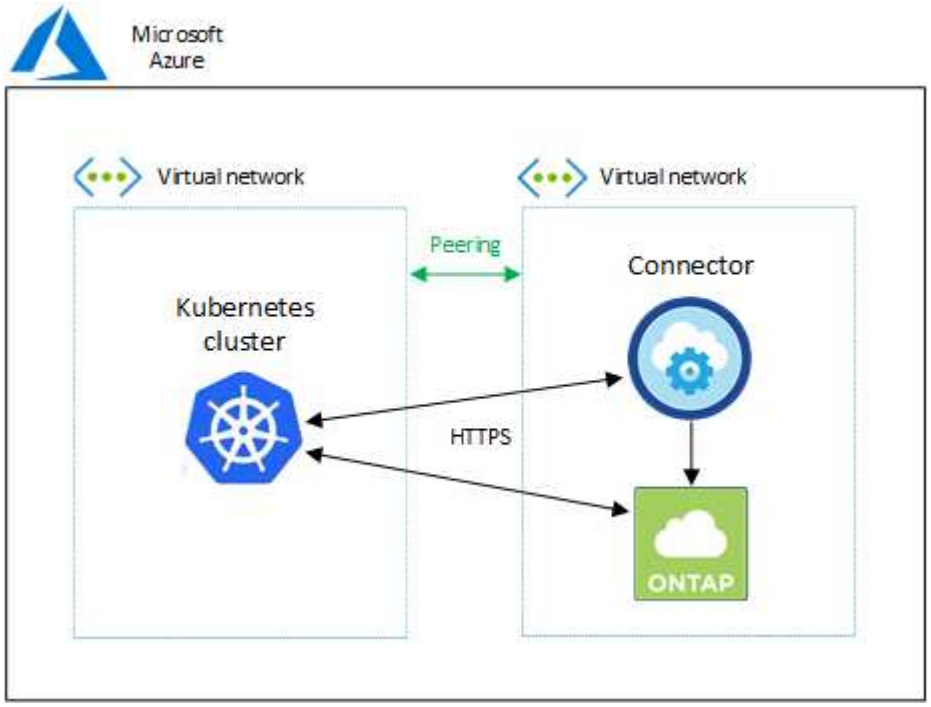
- Jeder Kubernetes-Cluster muss über eine eingehende Verbindung vom Connector verfügen
- Der Connector muss über Port 443 eine ausgehende Verbindung zu jedem Kubernetes-Cluster haben

Die einfachste Möglichkeit, diese Konnektivität bereitzustellen, ist die Implementierung von Connector und Cloud Volumes ONTAP im selben vnet wie der Kubernetes-Cluster. Andernfalls müssen Sie eine Peering-Verbindung zwischen den verschiedenen VNets einrichten.

Hier ein Beispiel, das jede Komponente im selben vnet zeigt.



Ein weiteres Beispiel zeigt einen Kubernetes Cluster, der in einem anderen vnet ausgeführt wird. In diesem Beispiel stellt Peering eine Verbindung zwischen dem vnet für den Kubernetes-Cluster und dem vnet für den Connector und Cloud Volumes ONTAP bereit.



Einrichtung der RBAC-Autorisierung

Die RBAC-Validierung erfolgt nur auf Kubernetes Clustern mit aktiviertem Active Directory (AD). Kubernetes-Cluster ohne AD bestehen die Validierung automatisch.

Sie benötigen für jeden Kubernetes Cluster eine Autorisierung der Connector-Rolle, damit der Connector einen Cluster ermitteln und verwalten kann.

Backup und Restore

Für Backup und Restore ist nur eine Grundautorisierung erforderlich.

Fügen Sie Speicherklassen hinzu

Erweiterte Autorisierung ist erforderlich, um Speicherklassen mithilfe von BlueXP hinzuzufügen und den Cluster auf Änderungen am Backend zu überwachen.

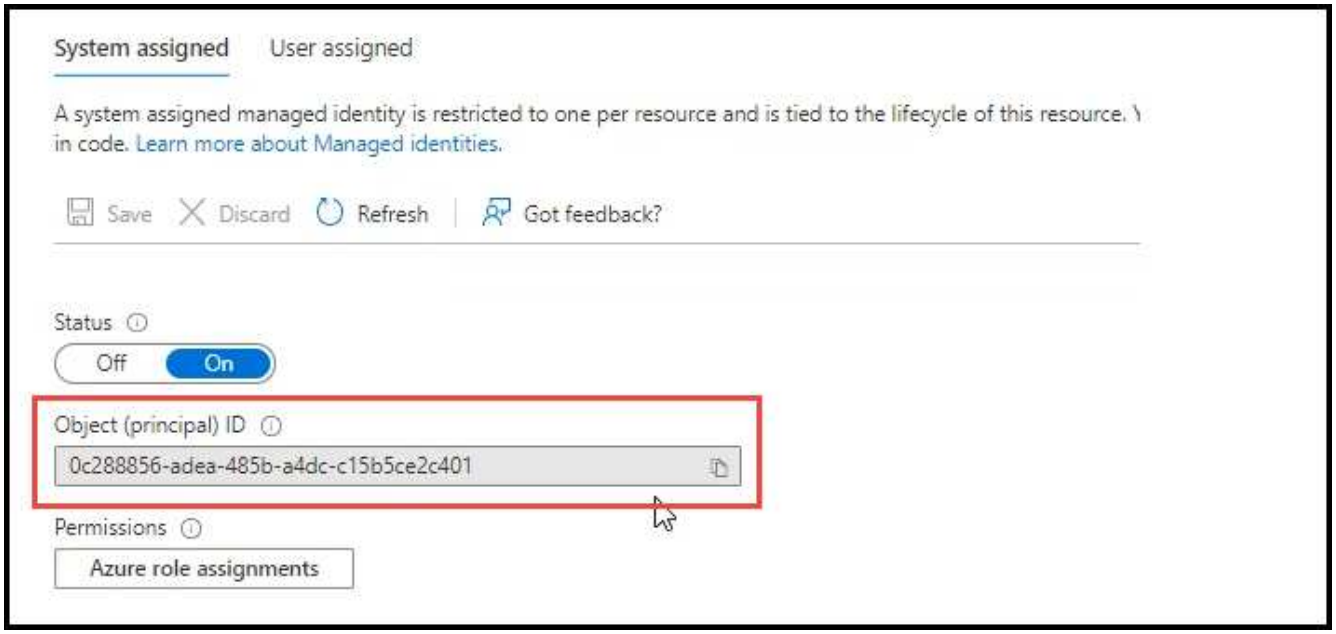
Installieren Sie Astra Trident

Zur Installation von Astra Trident müssen Sie für BlueXP die vollständige Autorisierung bereitstellen.

Bei der Installation von Astra Trident installiert BlueXP das Astra Trident Back-End und das Kubernetes Secret, das die Zugangsdaten enthält, die Astra Trident zur Kommunikation mit dem Storage-Cluster benötigt.

Ihre RBAC `subjects: name:` Die Konfiguration variiert basierend auf Ihrem Kubernetes-Cluster-Typ leicht.

- Wenn Sie einen **verwalteten AKS-Cluster** bereitstellen, benötigen Sie die Objekt-ID für die vom System zugewiesene verwaltete Identität für den Connector. Diese ID steht im Azure-Managementportal zur Verfügung.



- Wenn Sie ein **selbst verwaltetes Kubernetes Cluster** bereitstellen, benötigen Sie den Benutzernamen eines autorisierten Benutzers.

Erstellen Sie eine Cluster-Rolle und Rollenbindung.

1. Erstellen Sie eine YAML-Datei, die den folgenden Text enthält, der auf Ihren Autorisierungsanforderungen basiert. Ersetzen Sie den `subjects: kind:` Variable mit Ihrem Benutzernamen und `subjects: user:` Entweder mit der Objekt-ID für die vom System zugewiesene verwaltete Identität oder mit dem Benutzernamen eines autorisierten Benutzers, wie oben beschrieben.

Backup/Restore

Fügen Sie eine grundlegende Autorisierung hinzu, um Backup und Restore für Kubernetes-Cluster zu ermöglichen.

```
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
```

Speicherklassen

Fügen Sie erweiterte Berechtigungen hinzu, um Speicherklassen mithilfe von BlueXP hinzuzufügen.

```
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
```

Installation Von Trident

Über die Befehlszeile erhalten Sie die vollständige Autorisierung, und BlueXP kann Astra Trident installieren.

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

2. Wenden Sie die Konfiguration auf ein Cluster an.

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

Anforderungen für Kubernetes-Cluster in Google Cloud

Verwaltete Google Kubernetes Engine (GKE)-Cluster und automatisierte Kubernetes-Cluster können in Google mithilfe von BlueXP hinzugefügt und gemanagt werden. Bevor Sie die Cluster zu BlueXP hinzufügen können, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind.

In diesem Thema wird *Kubernetes Cluster* verwendet, wobei die Konfiguration für GKE und selbst gemanagte Kubernetes Cluster die gleiche ist. Der Cluster-Typ wird bei unterschiedlich der Konfiguration angegeben.

Anforderungen

Astra Trident

Eine der vier aktuellsten Versionen von Astra Trident ist erforderlich. Sie können Astra Trident direkt von BlueXP installieren oder aktualisieren. Sollten Sie "Prüfen Sie die Voraussetzungen" Vor der Installation von Astra Trident

Cloud Volumes ONTAP

Cloud Volumes ONTAP muss sich unter BlueXP im Rahmen desselben Mandanten-Kontos, Arbeitsumgebung und Konnektors befinden wie der Kubernetes-Cluster. "In der Astra Trident Dokumentation finden Sie die Konfigurationsschritte".

BlueXP Connector

Ein Connector muss in Google mit den erforderlichen Berechtigungen ausgeführt werden. a Connector,Weitere Informationen finden Sie unten.

Netzwerk-Konnektivität

Zwischen dem Kubernetes-Cluster und dem Connector sowie zwischen dem Kubernetes-Cluster und Cloud Volumes ONTAP ist eine Netzwerkverbindung erforderlich. networking requirements,Weitere Informationen finden Sie unten.

RBAC-Autorisierung

BlueXP unterstützt RBAC-fähige Cluster mit und ohne Active Directory. Die BlueXP Connector-Rolle muss für jedes GKE-Cluster autorisiert sein. up RBAC authorization,Weitere Informationen finden Sie unten.

Bereiten Sie einen Konnektor vor

Für das Erkennen und Managen von Kubernetes-Clustern ist ein BlueXP Connector in Google erforderlich. Sie müssen einen neuen Konnektor erstellen oder einen vorhandenen Konnektor verwenden, der über die erforderlichen Berechtigungen verfügt.

Erstellen Sie einen neuen Konnektor

Folgen Sie den Schritten in einem der nachfolgenden Links.

- "Erstellen Sie einen Connector von BlueXP" (Empfohlen)
- "Installieren Sie den Connector auf einem vorhandenen Linux-Host"

Fügen Sie die erforderlichen Berechtigungen einem vorhandenen Konnektor hinzu (um ein verwaltetes GKE-Cluster zu ermitteln).

Wenn Sie ein verwaltetes GKE-Cluster ermitteln möchten, müssen Sie möglicherweise die benutzerdefinierte Rolle ändern, damit der Connector die Berechtigungen bereitstellen kann.

Schritte

1. In "Cloud Console", Gehen Sie zur Seite **Rollen**.
2. Wählen Sie in der Dropdown-Liste oben auf der Seite das Projekt oder die Organisation aus, das die Rolle enthält, die Sie bearbeiten möchten.
3. Klicken Sie auf eine benutzerdefinierte Rolle.
4. Klicken Sie auf **Rolle bearbeiten**, um die Berechtigungen der Rolle zu aktualisieren.
5. Klicken Sie auf **Berechtigungen hinzufügen**, um der Rolle folgende neue Berechtigungen hinzuzufügen.

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

6. Klicken Sie auf **Aktualisieren**, um die bearbeitete Rolle zu speichern.

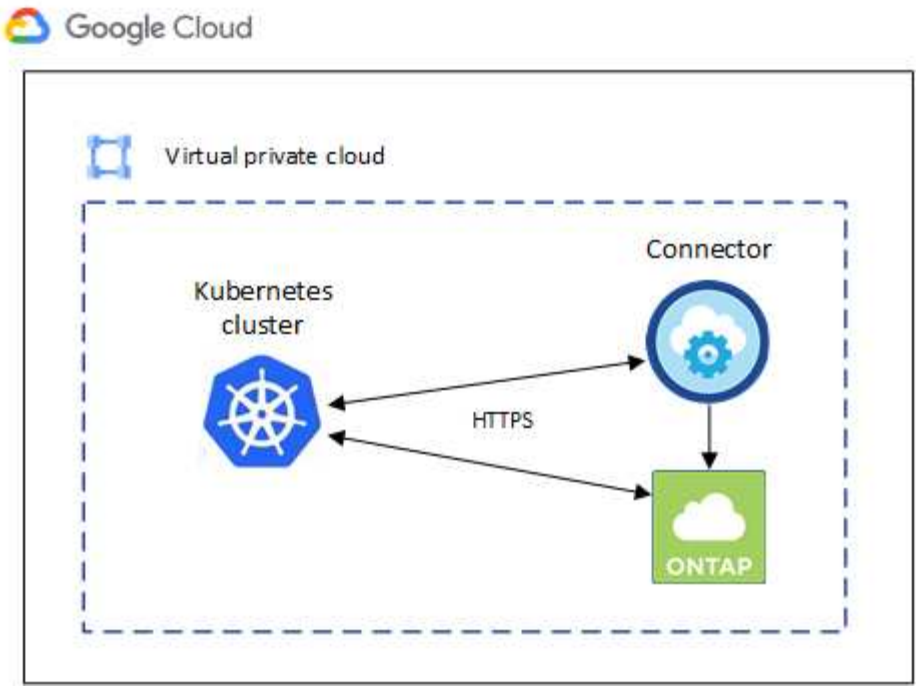
Netzwerkanforderungen prüfen

Sie müssen für die Netzwerkverbindung zwischen dem Kubernetes-Cluster und dem Connector sowie zwischen dem Kubernetes-Cluster und dem Cloud Volumes ONTAP-System sorgen, das dem Cluster Back-End-Storage bereitstellt.

- Jeder Kubernetes-Cluster muss über eine eingehende Verbindung vom Connector verfügen
- Der Connector muss über Port 443 eine ausgehende Verbindung zu jedem Kubernetes-Cluster haben

Die einfachste Möglichkeit für diese Konnektivität ist die Implementierung von Connector und Cloud Volumes ONTAP in derselben VPC wie der Kubernetes-Cluster. Andernfalls müssen Sie eine Peering-Verbindung zwischen den verschiedenen VPC einrichten.

In diesem Beispiel wird jede Komponente in derselben VPC angezeigt.



Einrichtung der RBAC-Autorisierung

Die RBAC-Validierung erfolgt nur auf Kubernetes Clustern mit aktiviertem Active Directory (AD). Kubernetes-Cluster ohne AD bestehen die Validierung automatisch.

Sie benötigen für jeden Kubernetes Cluster eine Autorisierung der Connector-Rolle, damit der Connector einen Cluster ermitteln und verwalten kann.

Backup und Restore

Für Backup und Restore ist nur eine Grundautorisierung erforderlich.

Fügen Sie Speicherklassen hinzu

Erweiterte Autorisierung ist erforderlich, um Speicherklassen mithilfe von BlueXP hinzuzufügen und den Cluster auf Änderungen am Backend zu überwachen.

Installieren Sie Astra Trident

Zur Installation von Astra Trident müssen Sie für BlueXP die vollständige Autorisierung bereitstellen.

> Bei der Installation von Astra Trident installiert BlueXP das Astra Trident Back-End und das Kubernetes Secret, das die Zugangsdaten enthält, die Astra Trident zur Kommunikation mit dem Storage-Cluster benötigt.

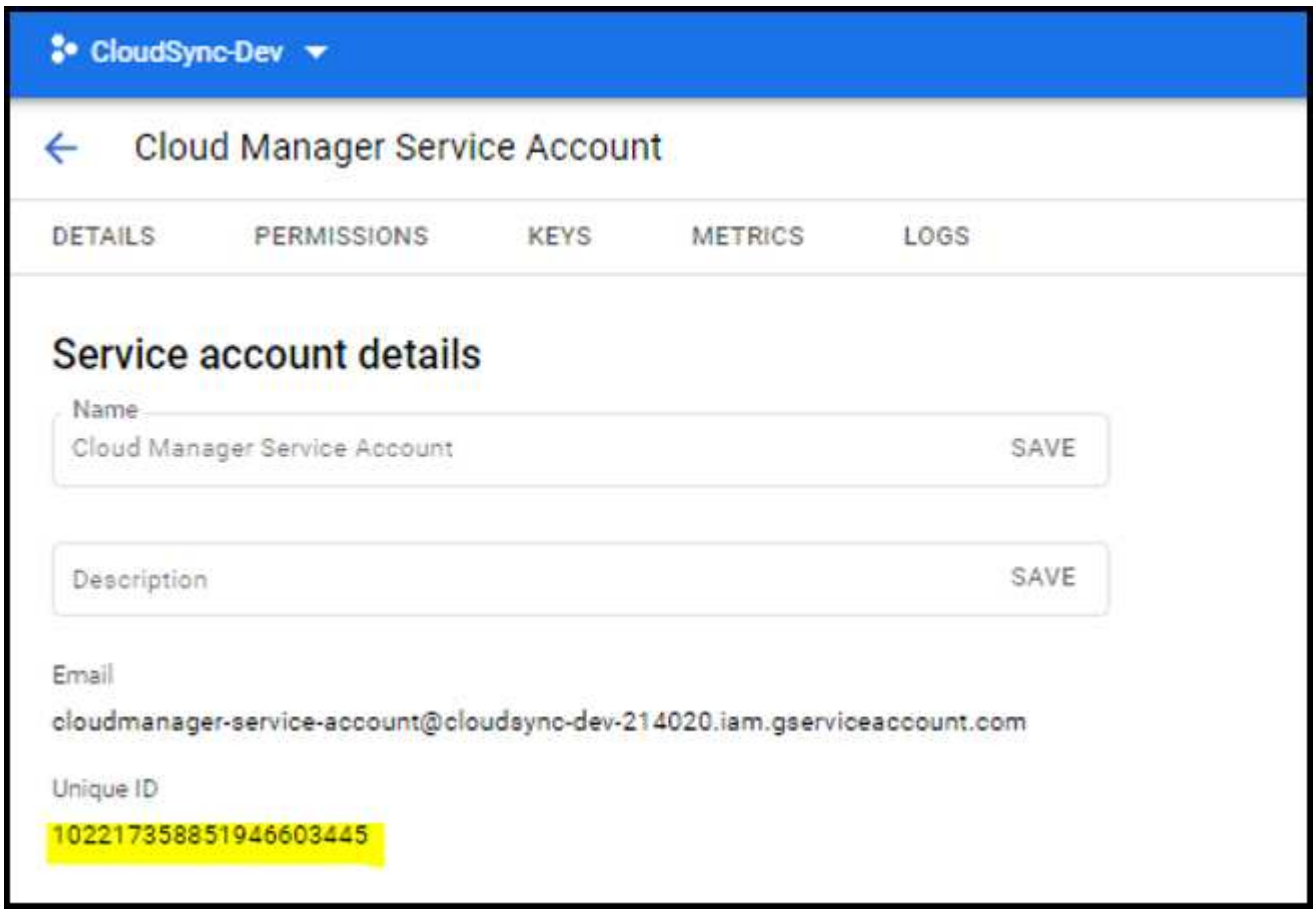
Zu konfigurieren `subjects: name:` In der YAML-Datei müssen Sie die eindeutige BlueXP-ID kennen.

Sie können die eindeutige ID auf zwei Arten finden:

- Verwenden des Befehls:

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

- In den Service-Konto-Details auf dem "Cloud Console".



Erstellen Sie eine Cluster-Rolle und Rollenbindung.

1. Erstellen Sie eine YAML-Datei, die den folgenden Text enthält, der auf Ihren Autorisierungsanforderungen basiert. Ersetzen Sie den `subjects: kind:` Variable mit Ihrem Benutzernamen und `subjects: user:` Mit der eindeutigen ID für das autorisierte Servicekonto.

Backup/Restore

Fügen Sie eine grundlegende Autorisierung hinzu, um Backup und Restore für Kubernetes-Cluster zu ermöglichen.

```
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
```

Speicherklassen

Fügen Sie erweiterte Berechtigungen hinzu, um Speicherklassen mithilfe von BlueXP hinzuzufügen.

```
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
```

Installation Von Trident

Über die Befehlszeile erhalten Sie die vollständige Autorisierung, und BlueXP kann Astra Trident installieren.

```
kubectl create clusterrolebinding test --clusterrole cluster-admin
--user <Unique ID>
```

2. Wenden Sie die Konfiguration auf ein Cluster an.

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

Anforderungen für Kubernetes-Cluster in OpenShift

Selbst gemanagte OpenShift Kubernetes-Cluster können mithilfe von BlueXP hinzugefügt und gemanagt werden. Bevor Sie die Cluster zu BlueXP hinzufügen können, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind.

Anforderungen

Astra Trident

Eine der vier aktuellsten Versionen von Astra Trident ist erforderlich. Sie können Astra Trident direkt von BlueXP installieren oder aktualisieren. Sollten Sie "Prüfen Sie die Voraussetzungen" Vor der Installation von Astra Trident:

Cloud Volumes ONTAP

Cloud Volumes ONTAP muss als Back-End Storage für den Cluster eingerichtet werden. "In der Astra Trident Dokumentation finden Sie die Konfigurationsschritte".

BlueXP Connector

Für den Import und das Management von Kubernetes-Clustern ist ein BlueXP Connector erforderlich. Sie müssen einen neuen Konnektor erstellen oder einen vorhandenen Konnektor verwenden, der die erforderlichen Berechtigungen für Ihren Cloud-Provider besitzt:

- "AWS Connector"
- "Azure Connector"
- "Google Cloud Connector"

Netzwerk-Konnektivität

Zwischen dem Kubernetes-Cluster und dem Connector sowie zwischen dem Kubernetes-Cluster und Cloud Volumes ONTAP ist eine Netzwerkverbindung erforderlich.

Kubernetes-Konfigurationsdatei (kubeconfig) mit RBAC-Autorisierung

Zum Importieren von OpenShift-Clustern benötigen Sie eine kubeconfig-Datei mit der RBAC-Berechtigung, die erforderlich ist, um verschiedene Funktionen zu ermöglichen. a kubeconfig file.

- Backup und Restore: Backup und Restore erfordern nur grundlegende Autorisierung.

- Hinzufügen von Speicherklassen: Erweiterte Autorisierung ist erforderlich, um Speicherklassen über BlueXP hinzuzufügen und den Cluster auf Änderungen am Backend zu überwachen.
- Installation Astra Trident: Sie müssen über die vollständige Autorisierung für BlueXP verfügen, um Astra Trident zu installieren.

Bei der Installation von Astra Trident installiert BlueXP das Astra Trident Back-End und das Kubernetes Secret, das die Zugangsdaten enthält, die Astra Trident zur Kommunikation mit dem Storage-Cluster benötigt.

Erstellen Sie eine kubeconfig-Datei

Erstellen Sie mit der OpenShift-CLI eine kubeconfig-Datei für den Import in BlueXP.

Schritte

1. Melden Sie sich über an der OpenShift-CLI an `oc login` Auf eine öffentliche URL mit einem administrativen Benutzer.
2. Erstellen Sie ein Service-Konto wie folgt:

   a. Erstellen Sie eine Dienstkontendatei mit dem Namen `oc-service-account.yaml`.

   Passen Sie Namen und Namespace nach Bedarf an. Wenn hier Änderungen vorgenommen werden, sollten Sie die gleichen Änderungen in den folgenden Schritten anwenden.

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

+

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

   a. Wenden Sie das Servicekonto an:

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

3. Erstellen Sie basierend auf Ihren Autorisierungsanforderungen eine benutzerdefinierte Rollenbindung.

   a. Erstellen Sie ein `ClusterRoleBinding` Datei aufgerufen `oc-clusterrolebinding.yaml`.

```
oc-clusterrolebinding.yaml
```

   b. Konfigurieren Sie die RBAC-Autorisierung nach Bedarf für Ihr Cluster.

Backup/Restore

Fügen Sie eine grundlegende Autorisierung hinzu, um Backup und Restore für Kubernetes-Cluster zu ermöglichen.

```
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
```

Speicherklassen

Fügen Sie erweiterte Berechtigungen hinzu, um Speicherklassen mithilfe von BlueXP hinzuzufügen.

```
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
```

Installation Von Trident

Gewähren Sie eine vollständige Administratorautorisierung und aktivieren Sie BlueXP die Installation von Astra Trident.

```
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. Wenden Sie die Bindung der Cluster-Rolle an:

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

4. Listen Sie die Geheimnisse des Dienstkontos auf, ersetzen Sie `<context>` Mit dem richtigen Kontext für Ihre Installation:

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

Das Ende der Ausgabe sollte wie folgt aussehen:

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

Die Indizes für jedes Element im `secrets` Array beginnt mit 0. Im obigen Beispiel der Index für `oc-service-account-dockercfg-vhz87` Wäre 0 und der Index für `oc-service-account-token-r59kr` Sind es 1. Notieren Sie in Ihrer Ausgabe den Index für den Namen des Dienstkontos, der das Wort „Token“ darin enthält.

5. Erzeugen Sie den kubeconfig wie folgt:

a. Erstellen Sie ein `create-kubeconfig.sh` Datei: Austausch `TOKEN_INDEX` Am Anfang des folgenden Skripts mit dem korrekten Wert.

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. Geben Sie die Befehle an, um sie auf Ihren Kubernetes-Cluster anzuwenden.

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

Sie werden das resultierende verwenden `kubeconfig-sa` Datei zum Hinzufügen eines OpenShift-Clusters zu BlueXP.

Fügen Sie Kubernetes Cluster hinzu

Fügen Sie einen Amazon Kubernetes Cluster zu BlueXP hinzu

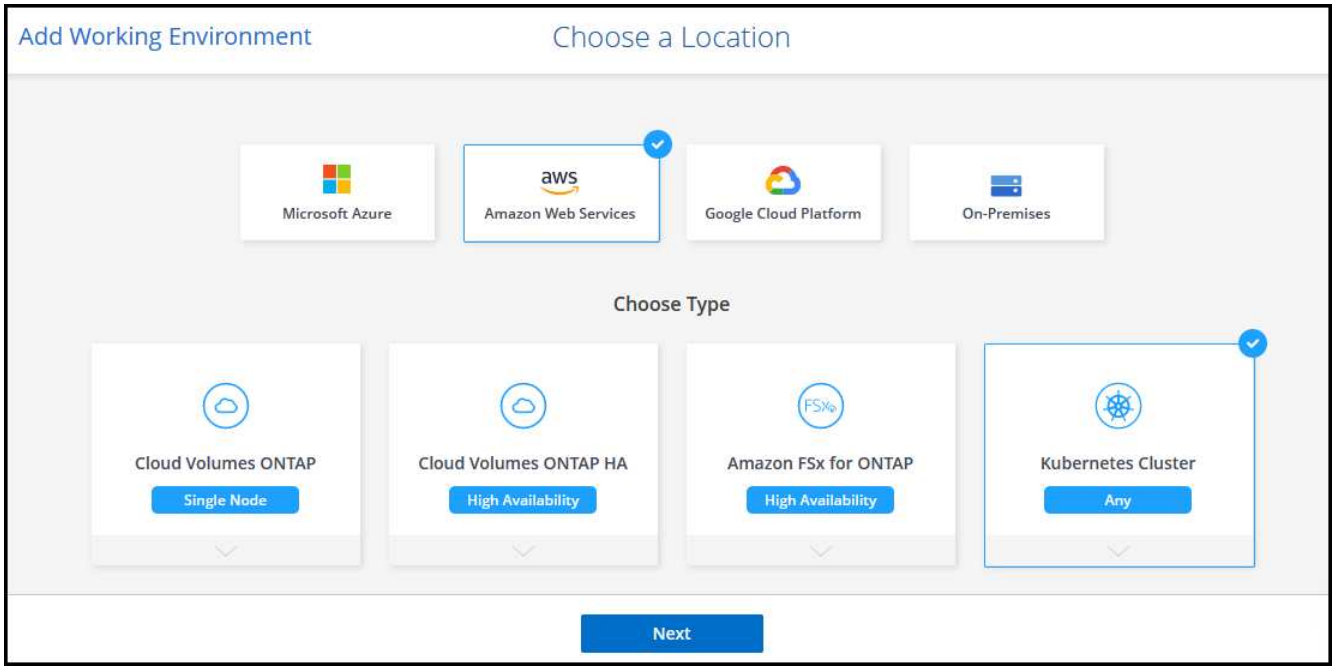
Kubernetes-Cluster können ermittelt oder in BlueXP importiert werden, sodass Sie persistente Volumes in Amazon S3 sichern können.

Erkennen eines Clusters

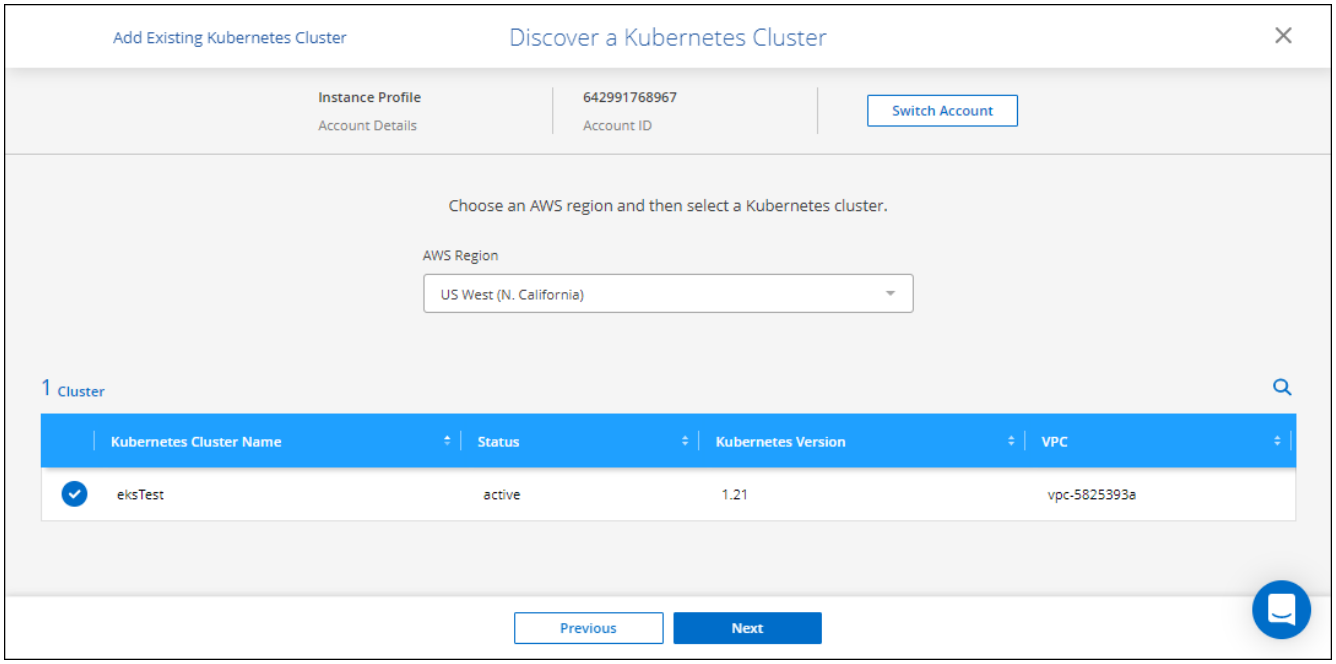
Es wird ein vollständig gemanagter oder selbst gemanagter Kubernetes Cluster ermittelt. Verwaltete Cluster müssen erkannt werden; sie können nicht importiert werden.

Schritte

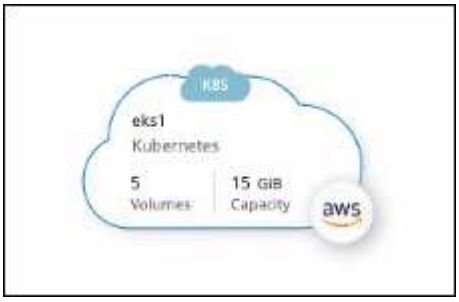
1. Klicken Sie auf der **Arbeitsfläche** auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Amazon Web Services** > **Kubernetes Cluster** und klicken Sie auf **Weiter**.



3. Wählen Sie **Discover Cluster** und klicken Sie auf **Next**.
4. Wählen Sie eine AWS-Region aus, wählen Sie einen Kubernetes-Cluster aus und klicken Sie dann auf **Weiter**.



BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

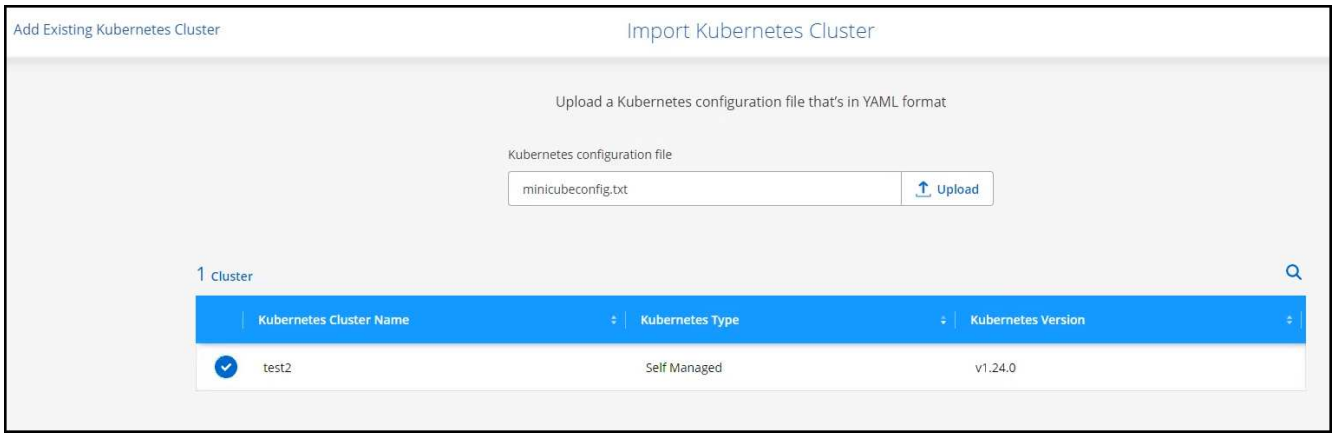


Importieren Sie einen Cluster

Es ist möglich, ein selbst verwaltetes Kubernetes-Cluster mithilfe einer Kubernetes-Konfigurationsdatei zu importieren.

Schritte

1. Klicken Sie auf der **Arbeitsfläche** auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Amazon Web Services** > **Kubernetes Cluster** und klicken Sie auf **Weiter**.
3. Wählen Sie **Cluster importieren** und klicken Sie auf **Weiter**.
4. Laden Sie eine Kubernetes-Konfigurationsdatei im YAML-Format hoch.



5. Wählen Sie den Kubernetes Cluster aus und klicken Sie auf **Next**.

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

Fügen Sie einen Azure Kubernetes Cluster zu BlueXP hinzu

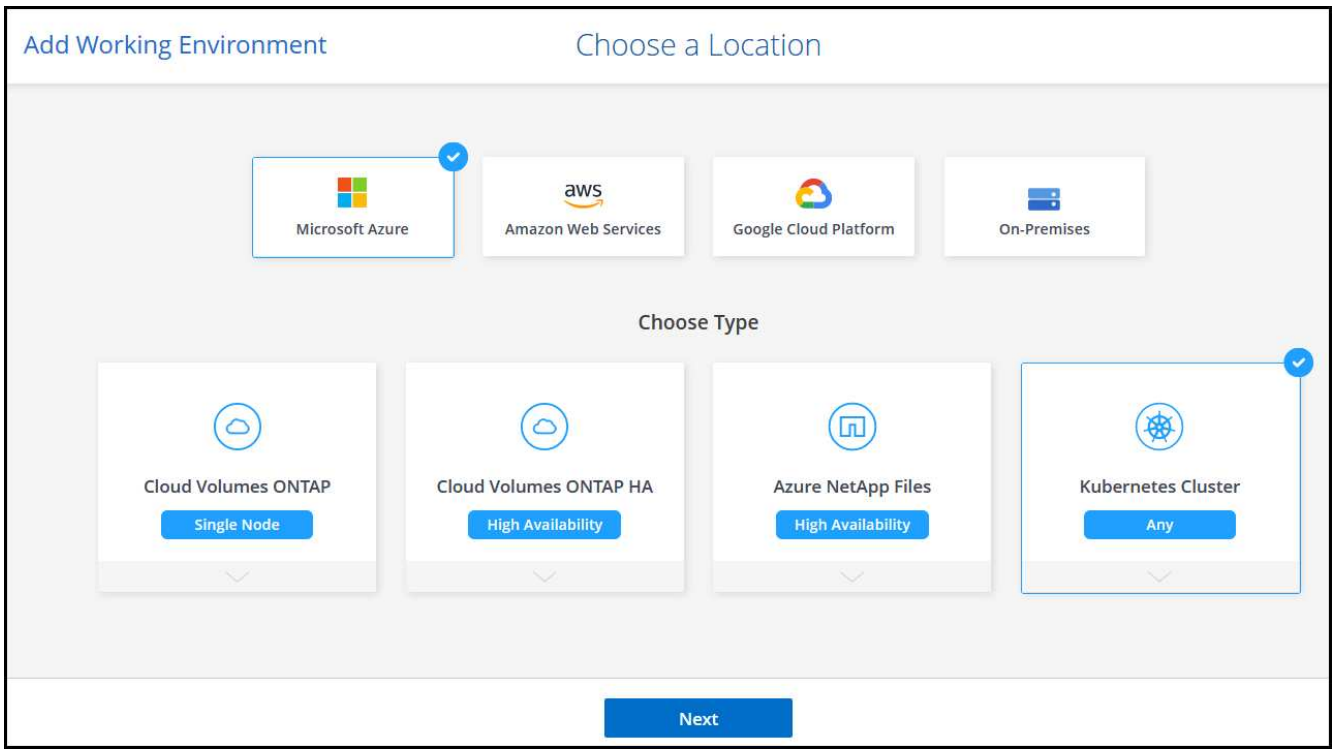
Sie können Kubernetes-Cluster ermitteln oder in BlueXP importieren, damit Sie persistente Volumes in Azure sichern können.

Erkennen eines Clusters

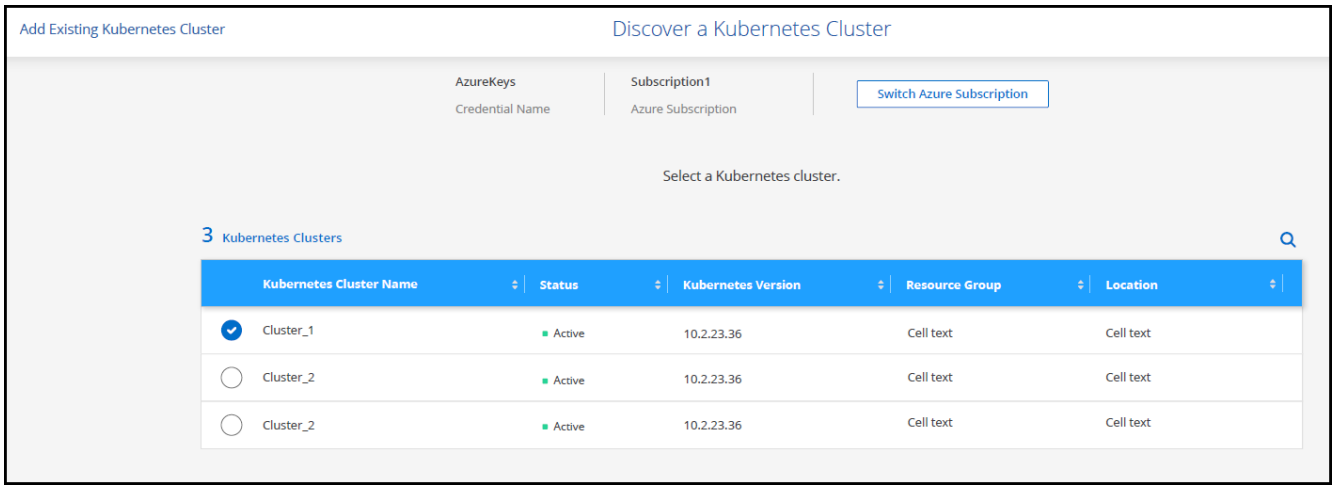
Es wird ein vollständig gemanagter oder selbst gemanagter Kubernetes Cluster ermittelt. Verwaltete Cluster müssen erkannt werden; sie können nicht importiert werden.

Schritte

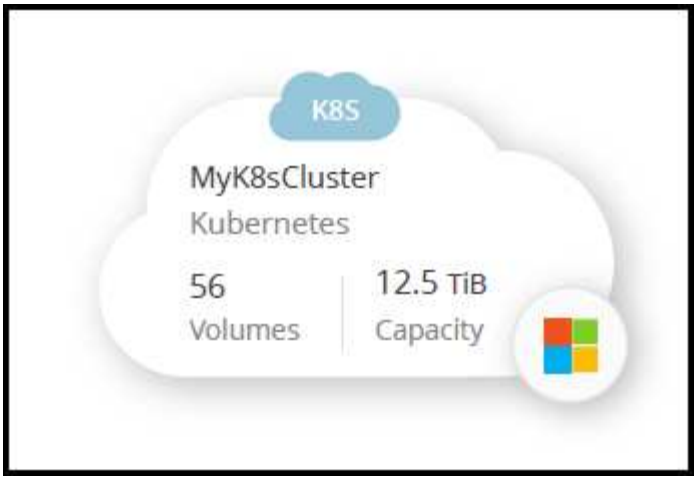
1. Klicken Sie auf der **Arbeitsfläche** auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Microsoft Azure** > **Kubernetes Cluster** und klicken Sie auf **Weiter**.



3. Wählen Sie **Discover Cluster** und klicken Sie auf **Next**.
4. Wählen Sie einen Kubernetes Cluster aus und klicken Sie auf **Next**.



BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.



Importieren Sie einen Cluster

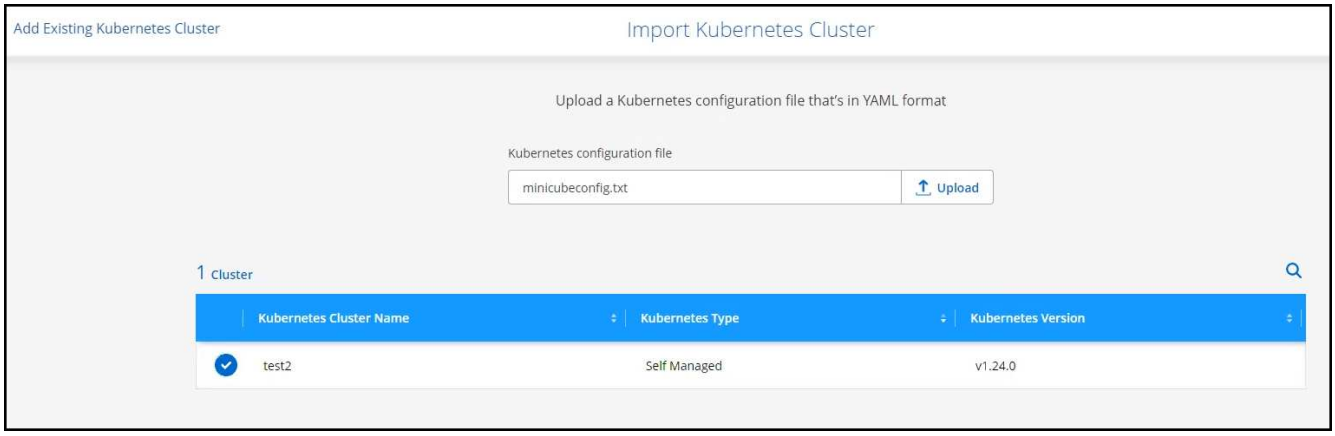
Es ist möglich, ein selbst verwaltetes Kubernetes-Cluster mithilfe einer Kubernetes-Konfigurationsdatei zu importieren.

Bevor Sie beginnen

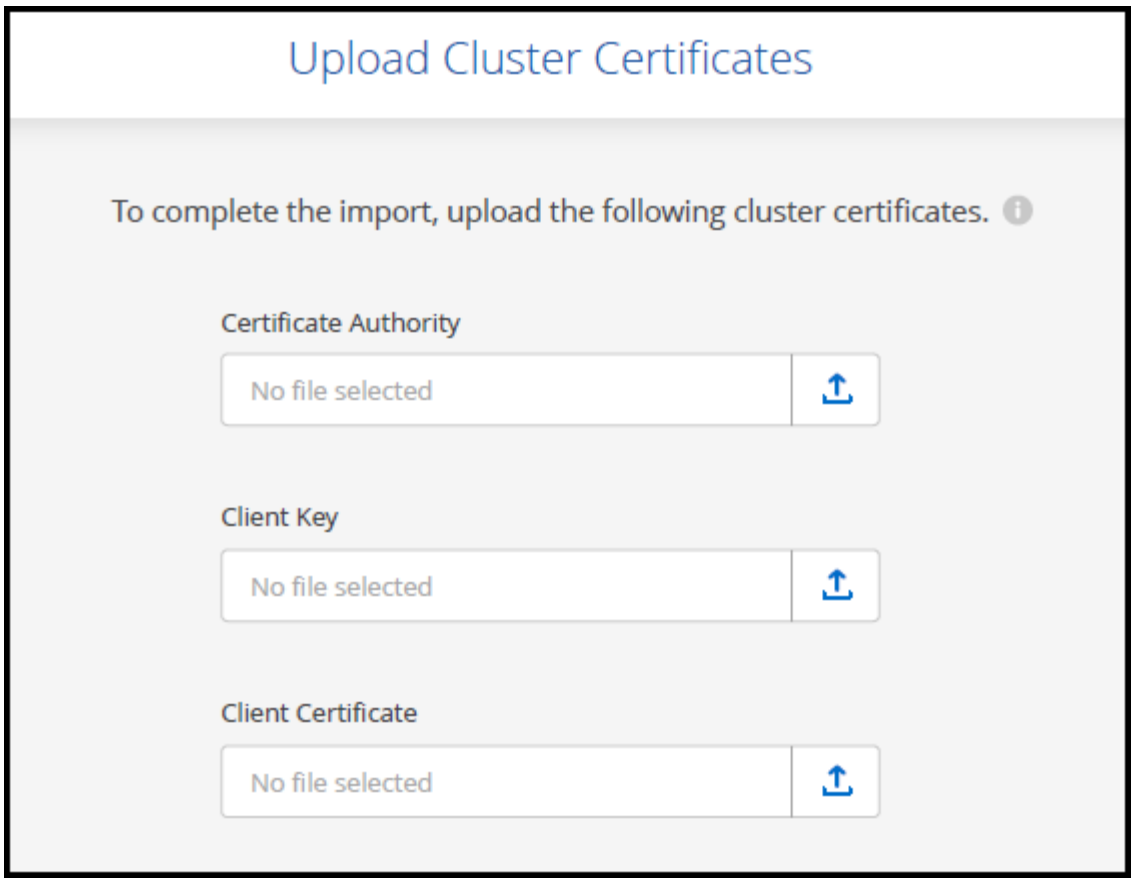
Für den in der Clusterrolle YAML-Datei angegebenen Benutzer benötigen Sie Zertifikate für Zertifizierungsstelle, Clientschlüssel und Clientzertifikat, um Kubernetes-Cluster zu importieren. Der Kubernetes-Cluster-Administrator erhält diese Zertifizierungen, wenn er Benutzer auf dem Kubernetes-Cluster erstellt.

Schritte

1. Klicken Sie auf der **Arbeitsfläche** auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Microsoft Azure** > **Kubernetes Cluster** und klicken Sie auf **Weiter**.
3. Wählen Sie **Cluster importieren** und klicken Sie auf **Weiter**.
4. Laden Sie eine Kubernetes-Konfigurationsdatei im YAML-Format hoch.



5. Laden Sie die vom Kubernetes-Clusteradministrator bereitgestellten Clusterzertifikate hoch.



BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

Fügen Sie ein Google Cloud Kubernetes Cluster zu BlueXP hinzu

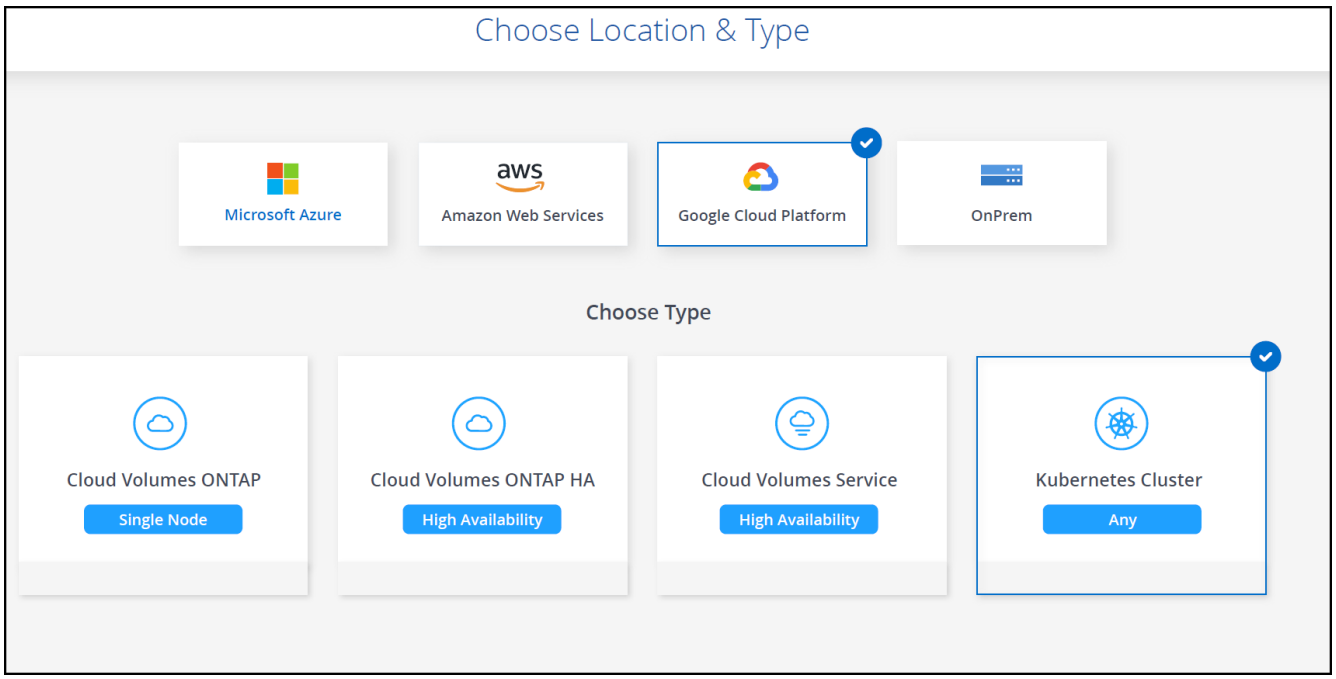
Kubernetes-Cluster können ermittelt oder in BlueXP importiert werden, sodass Sie persistente Volumes in Google Cloud sichern können.

Erkennen eines Clusters

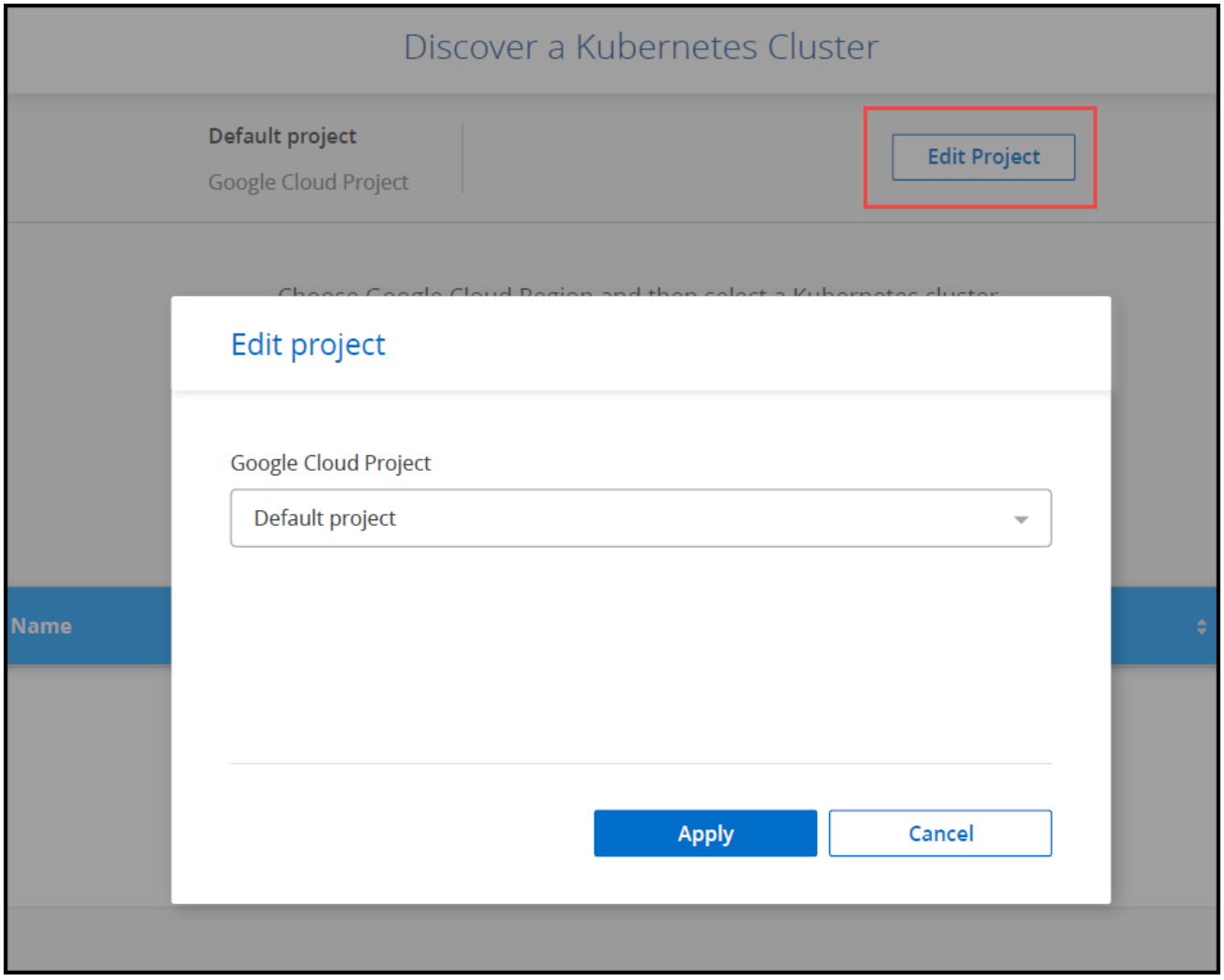
Es wird ein vollständig gemanagter oder selbst gemanagter Kubernetes Cluster ermittelt. Verwaltete Cluster müssen erkannt werden; sie können nicht importiert werden.

Schritte

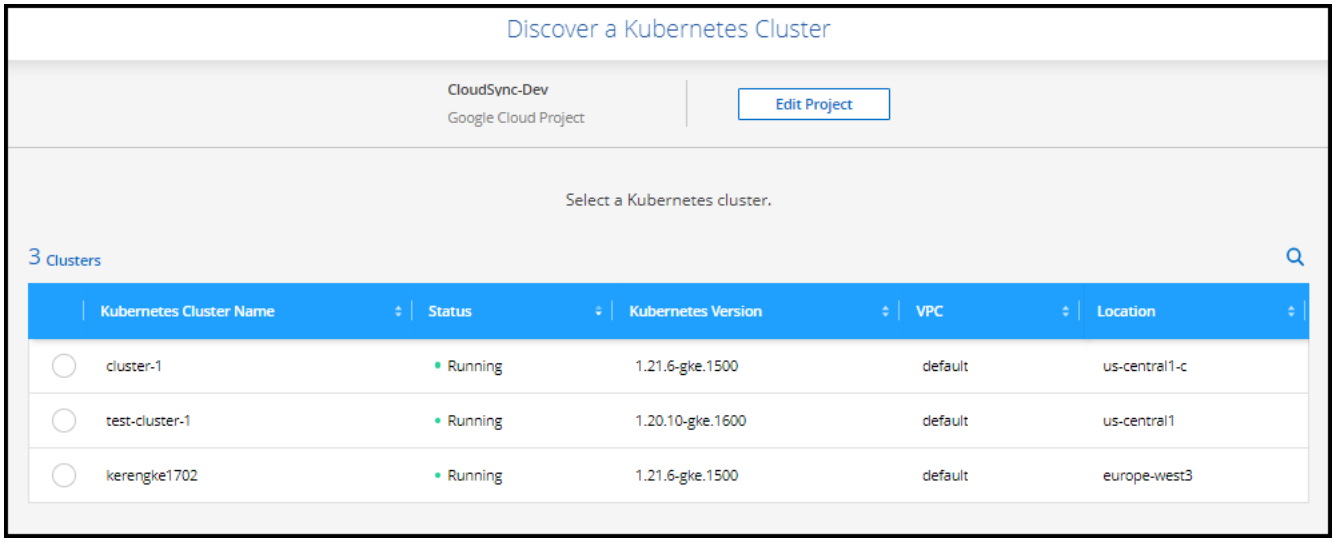
1. Klicken Sie auf der **Arbeitsfläche** auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Google Cloud Platform** > **Kubernetes Cluster** und klicken Sie auf **Weiter**.



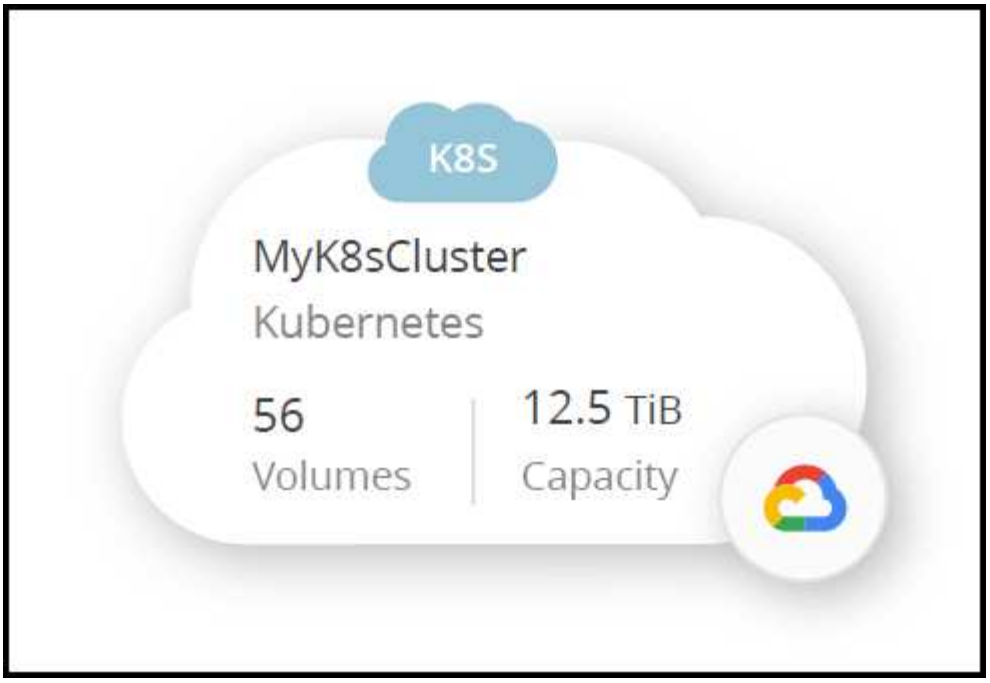
3. Wählen Sie **Discover Cluster** und klicken Sie auf **Next**.
4. Um einen Kubernetes-Cluster in einem anderen Google Cloud-Projekt auszuwählen, klicken Sie auf **Projekt bearbeiten** und wählen ein verfügbares Projekt aus.



5. Wählen Sie einen Kubernetes Cluster aus und klicken Sie auf **Next**.



BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.



Importieren Sie einen Cluster

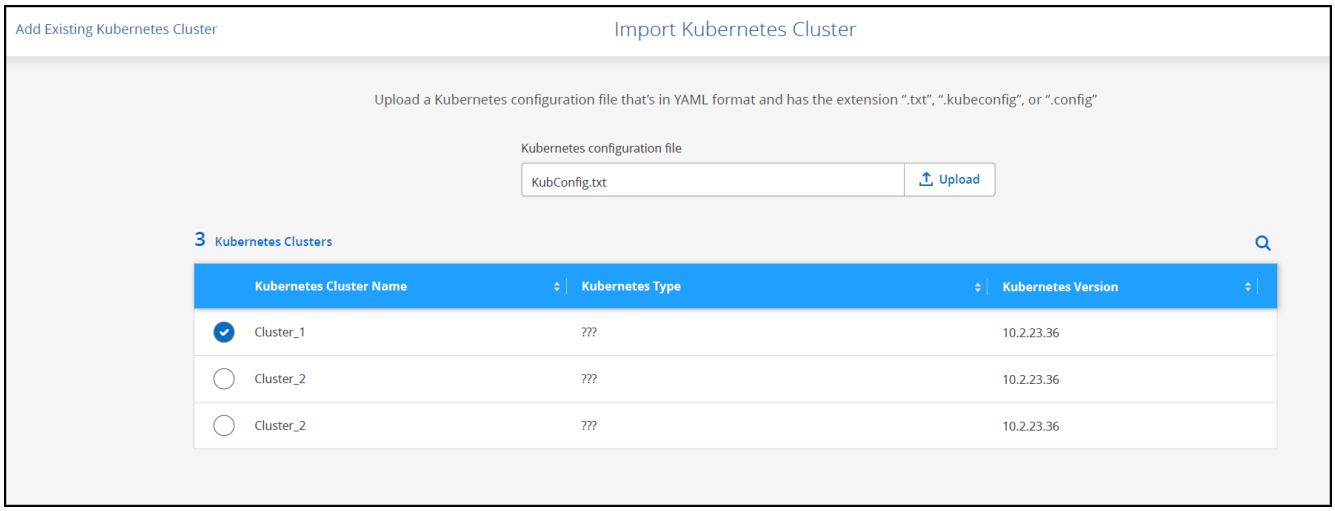
Es ist möglich, ein selbst verwaltetes Kubernetes-Cluster mithilfe einer Kubernetes-Konfigurationsdatei zu importieren.

Bevor Sie beginnen

Für den in der Clusterrolle YAML-Datei angegebenen Benutzer benötigen Sie Zertifikate für Zertifizierungsstelle, Clientschlüssel und Clientzertifikat, um Kubernetes-Cluster zu importieren. Der Kubernetes-Cluster-Administrator erhält diese Zertifizierungen, wenn er Benutzer auf dem Kubernetes-Cluster erstellt.

Schritte

1. Klicken Sie auf der **Arbeitsfläche** auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Google Cloud Platform** > **Kubernetes Cluster** und klicken Sie auf **Weiter**.
3. Wählen Sie **Cluster importieren** und klicken Sie auf **Weiter**.
4. Laden Sie eine Kubernetes-Konfigurationsdatei im YAML-Format hoch.



BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

Fügen Sie BlueXP ein OpenShift-Cluster hinzu

Importieren Sie einen selbst gemanagten OpenShift-Cluster in BlueXP, damit Sie das Backup persistenter Volumes bei Ihrem Cloud-Provider starten können.

Importieren Sie einen Cluster

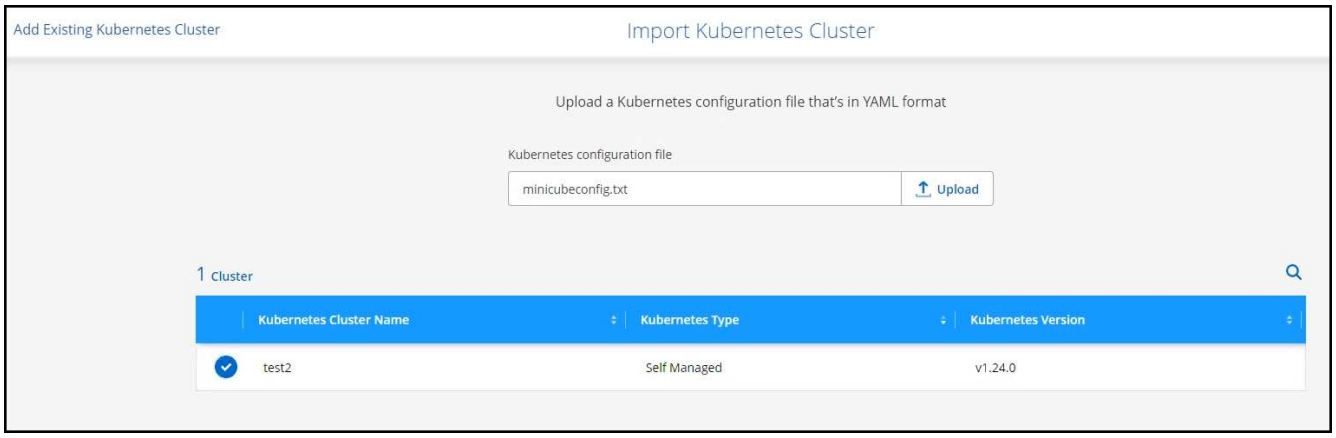
Es ist möglich, ein selbst verwaltetes Kubernetes-Cluster mithilfe einer Kubernetes-Konfigurationsdatei zu importieren.

Vor dem Hinzufügen eines OpenShift-Clusters müssen folgende Anforderungen berücksichtigt werden:

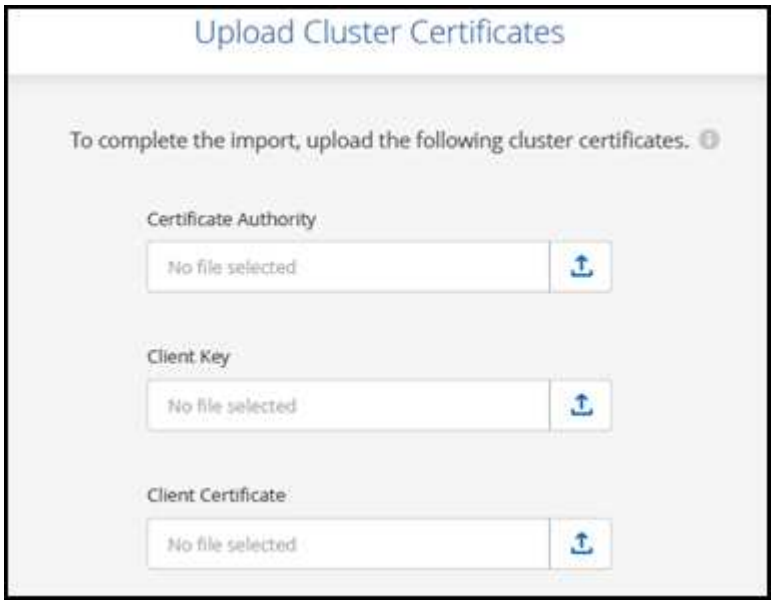
- Die Datei `kubeconfig-sa`, die Sie in erstellt haben "Erstellen Sie eine kubeconfig-Datei".
- Die öffentlichen Zertifikatsinstanz (z. B. Ca.crt), der Clientschlüssel (z. B. tls.Key) und die Clientzertifizierungs- (z. B. tls.crt)-Dateien für den Cluster.

Schritte

1. Wählen Sie auf der **Arbeitsfläche** die Option * Arbeitsumgebung hinzufügen*.
2. Wählen Sie Ihren Cloud-Provider aus und wählen Sie **Kubernetes Cluster** und dann **Next**.
3. Wählen Sie **Cluster importieren** und dann **Weiter**.
4. Laden Sie die hoch `kubeconfig-sa` Datei, in der Sie erstellt haben "Erstellen Sie eine kubeconfig-Datei". Wählen Sie den Kubernetes Cluster aus und wählen Sie **Next** aus.



5. Laden Sie die Cluster-Zertifikate hoch.



BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

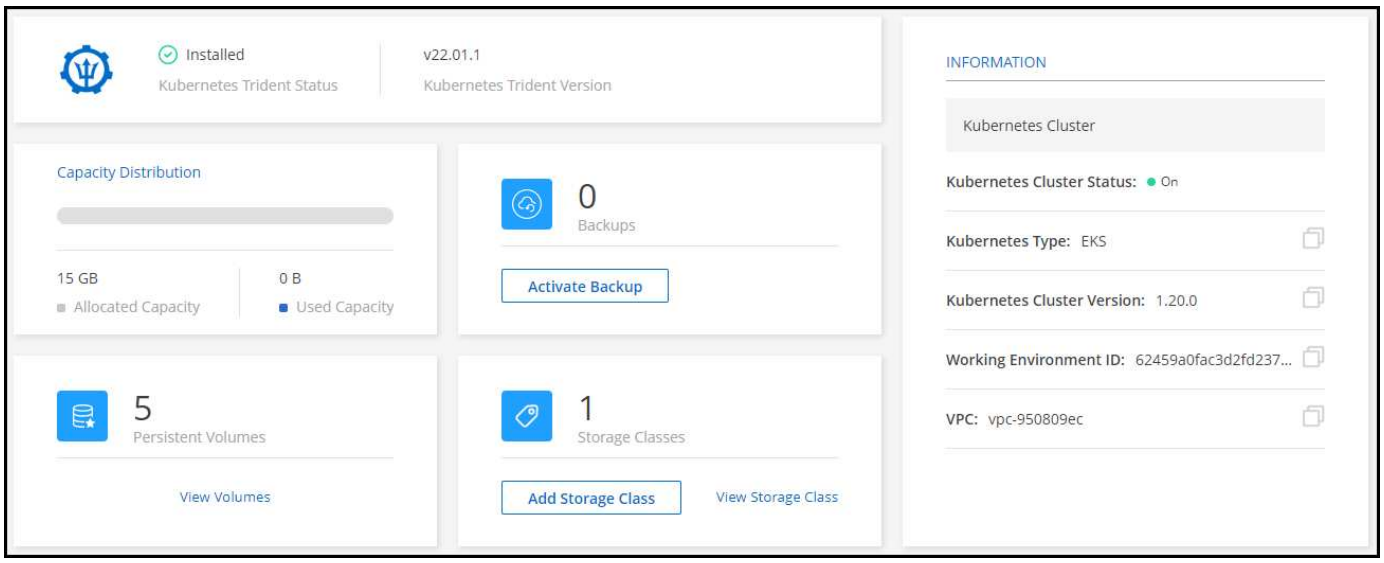
Managen Sie Kubernetes-Cluster

Mit BlueXP können Sie Astra Trident installieren oder aktualisieren, Storage-Klassen konfigurieren, Cluster entfernen und Datenservices aktivieren.

Astra Trident ist implementiert mit `tridentctl` Wird nicht unterstützt. Bei der Implementierung von Astra Trident mit `tridentctl`, Sie können BlueXP nicht für das Management Ihrer Kubernetes-Cluster verwenden. Unbedingt Und Neuinstallation "Verwenden des Betreibers von Trident" Oder "Verwendung von BlueXP".

Funktionen

Nachdem Sie BlueXP Kubernetes-Cluster hinzugefügt haben, können Sie die Cluster über die Ressourcenseite verwalten. Doppelklicken Sie auf die Kubernetes-Arbeitsumgebung auf dem Canvas, um die Ressourcenseite zu öffnen.



Auf der Ressourcen-Seite können Sie:

- Anzeigen des Kubernetes Cluster-Status
- Überprüfen Sie, ob die kompatible Version von Astra Trident installiert ist oder ob Sie ein Upgrade auf die neueste Version von Astra Trident durchführen. Siehe "Installation Von Astra Trident".
- Speicherklassen hinzufügen und entfernen. Siehe "Management von Storage-Klassen".
- Anzeige persistenter Volumes Siehe "Anzeige persistenter Volumes".
- Entfernen Sie Kubernetes Cluster aus dem Workspace. Siehe "Cluster entfernen".
- Cloud Backup aktivieren oder anzeigen Siehe "Nutzen Sie NetApp Cloud-Datenservices".

Installation oder Upgrade von Astra Trident

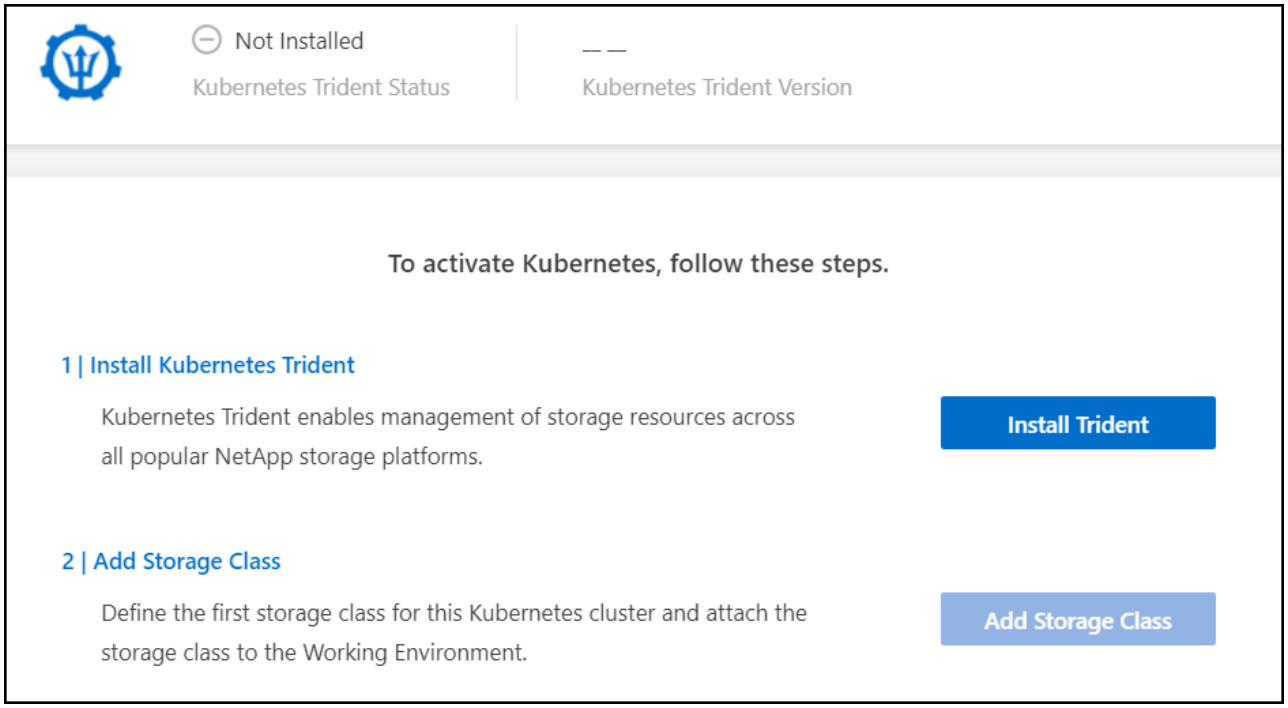
Nachdem Sie einen gemanagten Kubernetes Cluster zum Canvas hinzugefügt haben, können Sie mit BlueXP eine kompatible Astra Trident Installation bestätigen oder Astra Trident auf die neueste Version installieren oder aktualisieren.

- Wenn Astra Trident nicht installiert ist oder eine inkompatible Version von Astra Trident installiert ist, wird im Cluster angezeigt, dass eine Aktion erforderlich ist.
- Eine der vier aktuellsten Versionen von Astra Trident ist mit dem Trident-Operator implementiert – entweder manuell oder mit Helm-Chart.
- Astra Trident ist implementiert mit `tridentctl` Wird nicht unterstützt. Bei der Implementierung von Astra Trident mit `tridentctl`, Sie können BlueXP nicht für das Management Ihrer Kubernetes-Cluster verwenden. Unbedingt Und Neuinstallation "Verwenden des Betreibers von Trident" Oder verwenden Sie die nachstehenden Schritte.

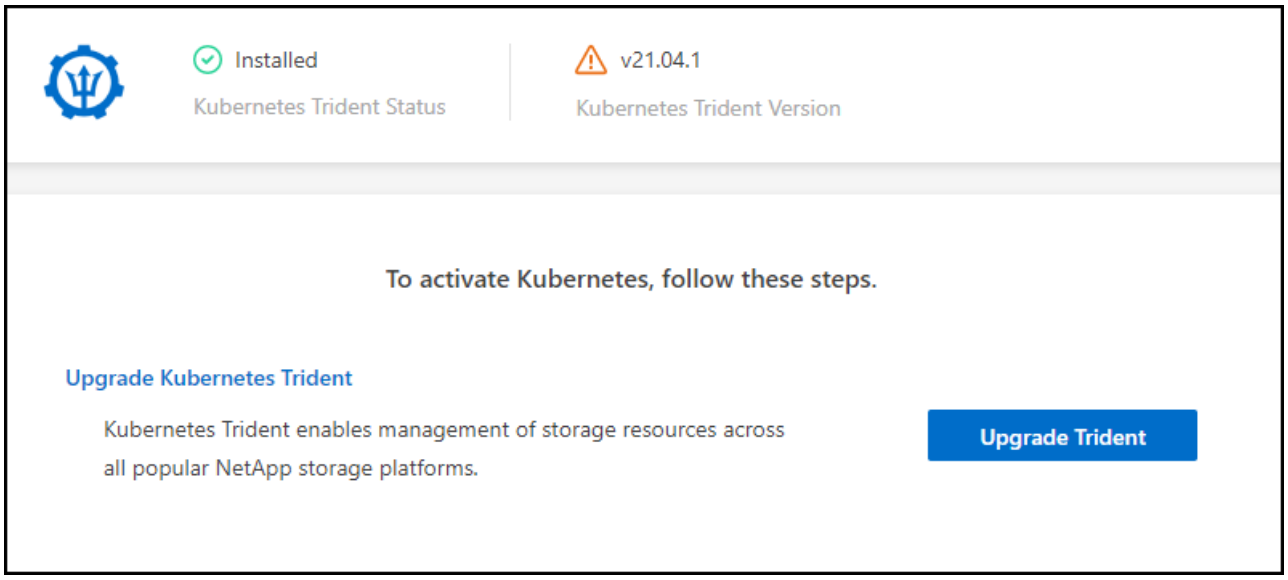
Weitere Informationen zu Astra Trident finden Sie unter "Astra Trident-Dokumentation".

Schritte

1. Doppelklicken Sie auf der Arbeitsfläche von Kubernetes auf die Arbeitsumgebung oder klicken Sie auf **Arbeitsumgebung eingeben**.
   a. Falls Astra Trident nicht installiert ist, klicken Sie auf **Trident installieren**.



   b. Wenn eine nicht unterstützte Version von Astra Trident installiert ist, klicken Sie auf **Upgrade Trident**.



Die neueste Version von Astra Trident ist installiert. Sie können nun Speicherklassen hinzufügen.

Management von Storage-Klassen

Nachdem Sie einen verwalteten Kubernetes-Cluster zu Canvas hinzugefügt haben, können Sie BlueXP zum Verwalten von Speicherklassen verwenden.

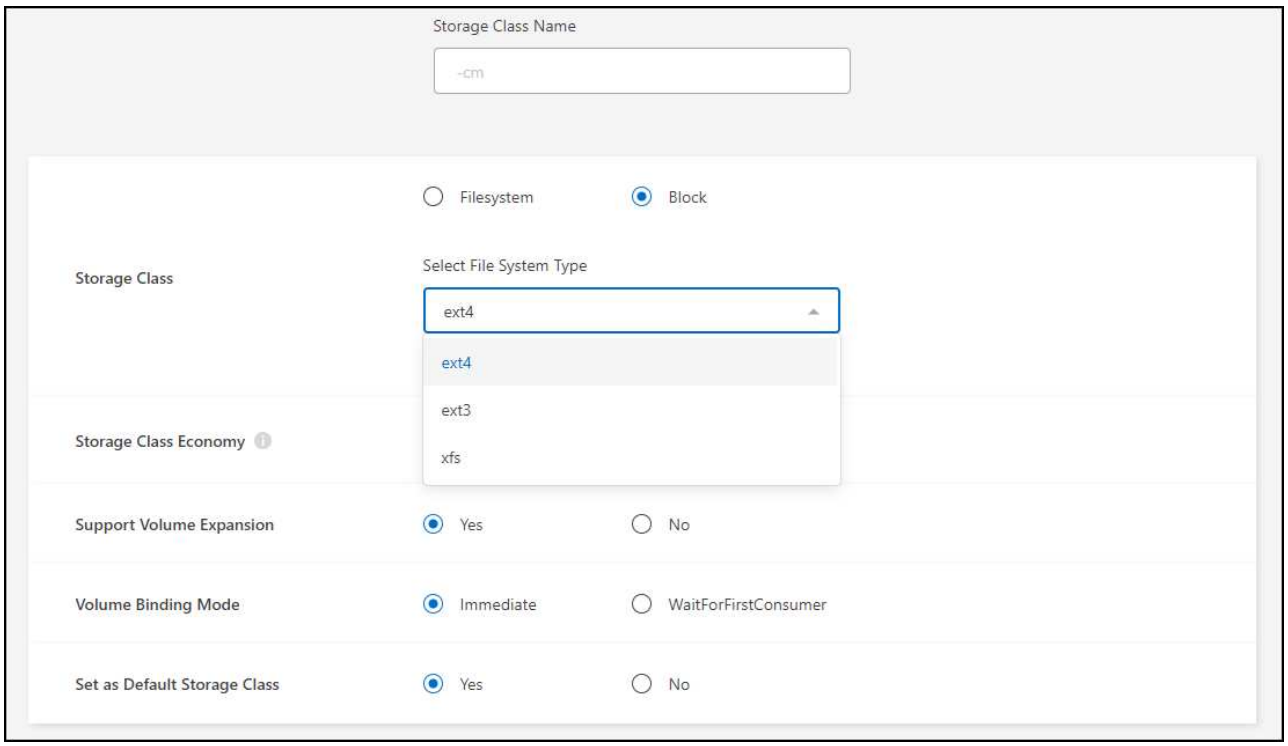
Wenn keine Storage-Klasse definiert ist, wird im Cluster eine Aktion angezeigt, die erforderlich ist. Durch Doppelklicken auf das Cluster auf der Arbeitsfläche wird die Aktionsseite geöffnet, um eine Speicherklasse hinzuzufügen.

Fügen Sie eine Storage-Klasse hinzu

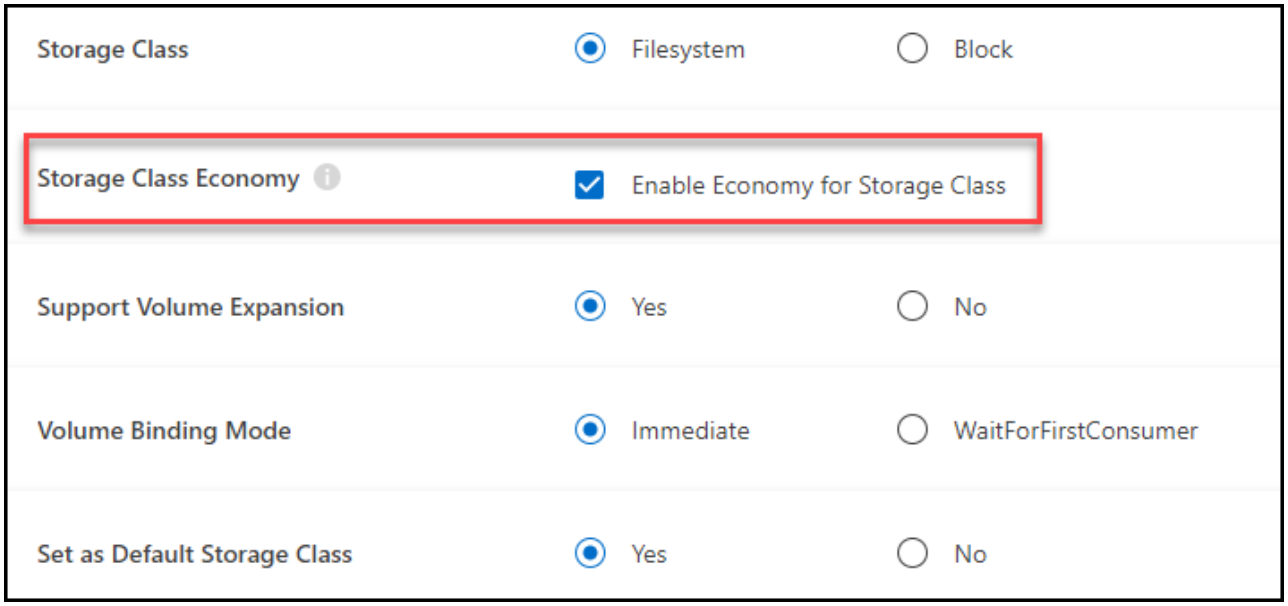
Schritte

1. Klicken Sie auf dem Bildschirm auf die Kubernetes-Arbeitsumgebung per Drag and Drop in die Arbeitsumgebung Cloud Volumes ONTAP oder Amazon FSX für ONTAP, um den Storage-Klassen-Assistenten zu öffnen.
2. Geben Sie einen Namen für die Speicherklasse ein.
3. Wählen Sie **Filesystem** oder **Block**-Speicher aus.

    a. Wählen Sie für **Block**-Speicher einen Dateisystemtyp (fstype) aus.

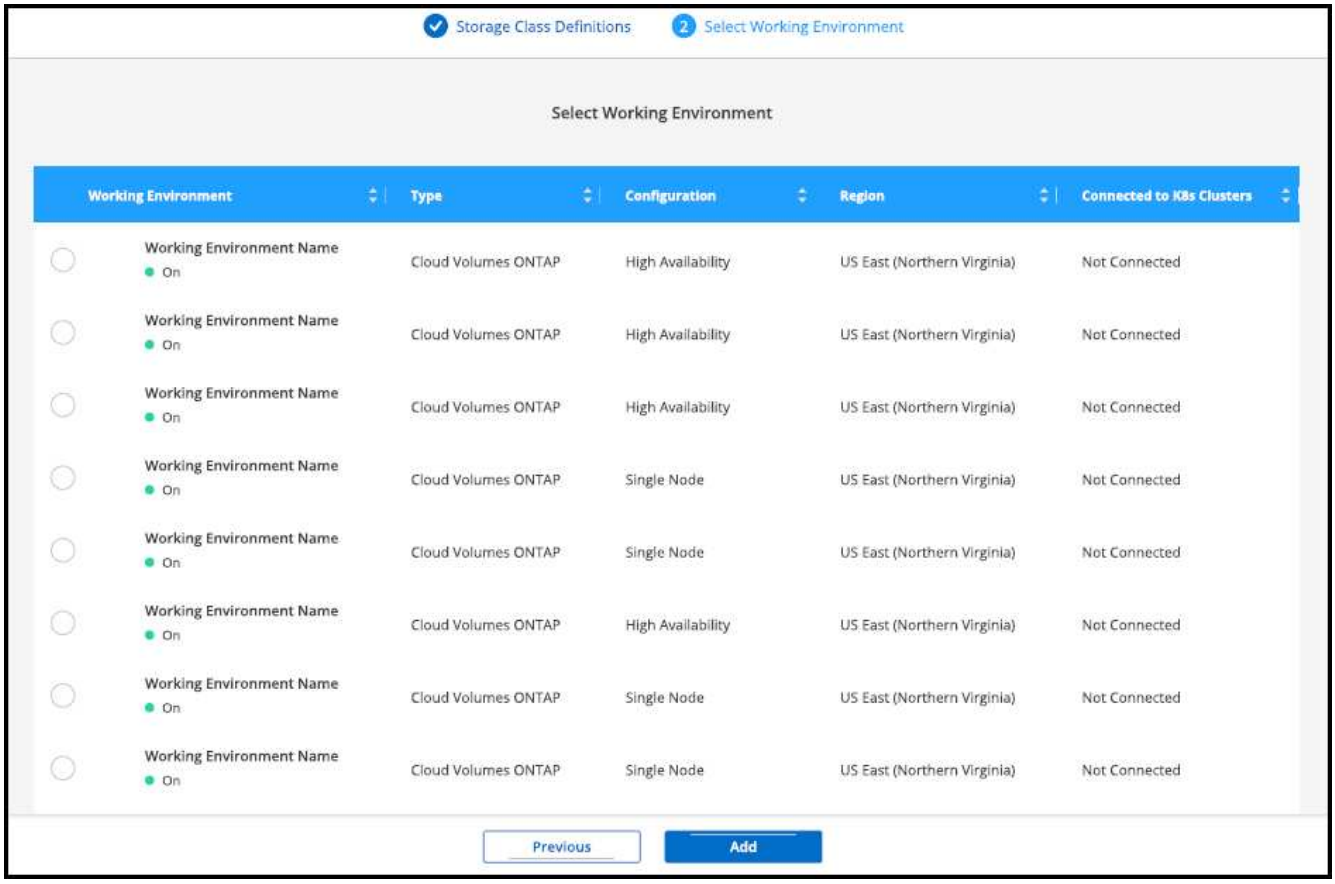


b. Für **Block** oder **Filesystem**-Speicher können Sie wählen, um die Wirtschaftlichkeit der Storage-Klasse zu ermöglichen.

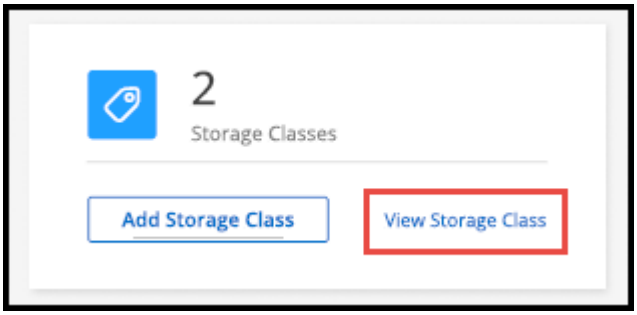


Backup und Restore werden in wirtschaftlicher Nutzung von Storage-Klasse nicht unterstützt.

4. Wählen Sie Optionen für Volume-Erweiterung, Volume-Bindung und Standard-Storage-Klasse aus. Klicken Sie Auf **Weiter**.
5. Wählen Sie eine Arbeitsumgebung aus, in der eine Verbindung zum Cluster hergestellt werden soll. Klicken Sie Auf **Hinzufügen**.



Sie können auf klicken, um die Storage-Klasse auf der Ressourcenseite für das Kubernetes-Cluster anzuzeigen.

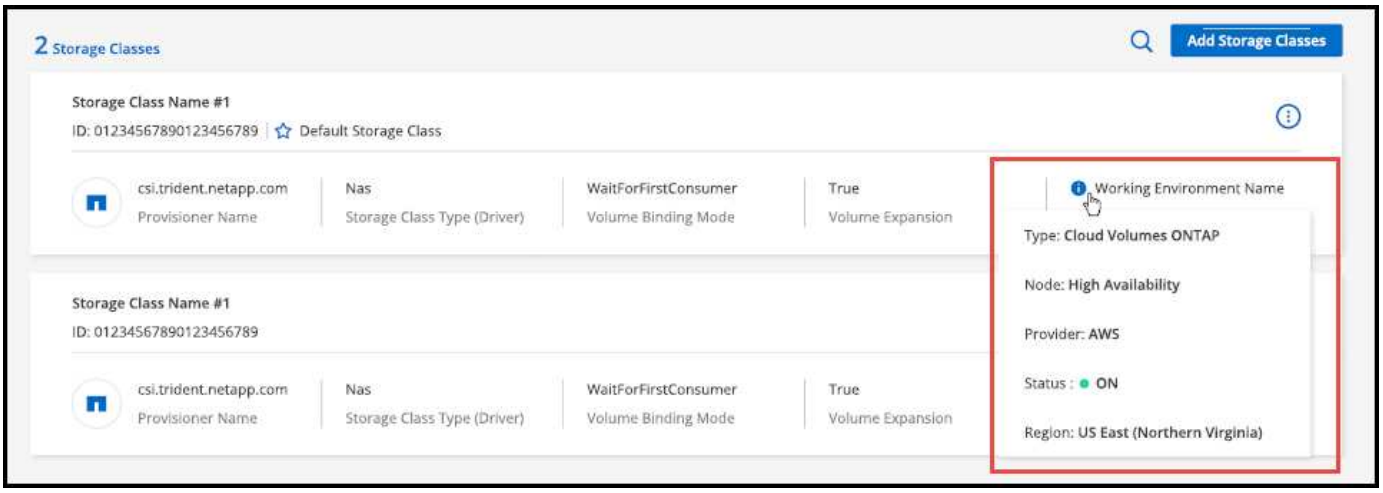


Details zur Arbeitsumgebung anzeigen

Schritte

1. Doppelklicken Sie auf der Arbeitsfläche von Kubernetes auf die Arbeitsumgebung oder klicken Sie auf **Arbeitsumgebung eingeben**.
2. Klicken Sie auf die Registerkarte **Speicherklassen**.
3. Klicken Sie auf das Informationssymbol, um Details zur Arbeitsumgebung anzuzeigen.

Das Fenster Details zur Arbeitsumgebung wird geöffnet.

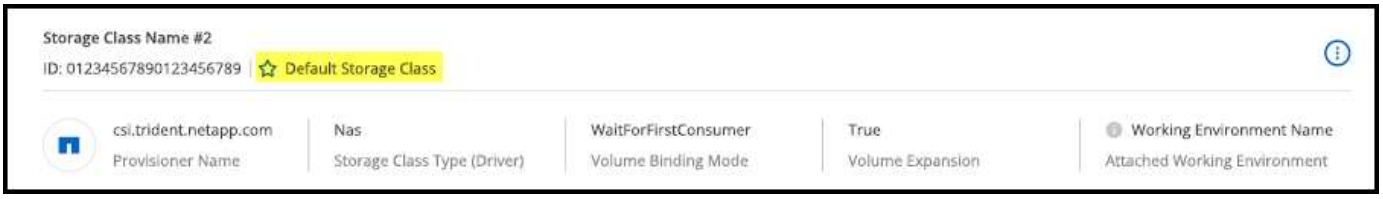


Legen Sie die Standard-Storage-Klasse fest

Schritte

1. Doppelklicken Sie auf der Arbeitsfläche von Kubernetes auf die Arbeitsumgebung oder klicken Sie auf **Arbeitsumgebung eingeben**.
2. Klicken Sie auf die Registerkarte **Speicherklassen**.
3. Klicken Sie auf das Aktionsmenü für die Speicherklasse und klicken Sie auf **als Standard**.

Die ausgewählte Speicherklasse wird als Standard festgelegt.



Speicherklasse entfernen

Schritte

1. Doppelklicken Sie auf der Arbeitsfläche von Kubernetes auf die Arbeitsumgebung oder klicken Sie auf **Arbeitsumgebung eingeben**.
2. Klicken Sie auf die Registerkarte **Speicherklassen**.
3. Klicken Sie auf das Aktionsmenü für die Speicherklasse und klicken Sie auf **als Standard**.

4. Klicken Sie auf **Entfernen**, um das Entfernen der Speicherklasse zu bestätigen.

Die ausgewählte Speicherklasse wird entfernt.

Anzeige persistenter Volumes

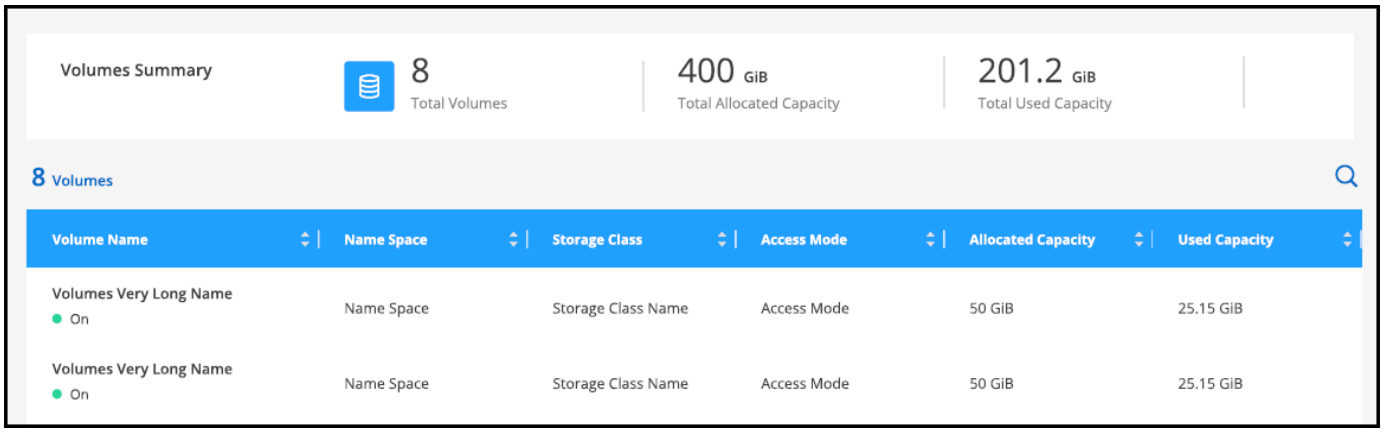
Nachdem Sie einen verwalteten Kubernetes-Cluster zu Canvas hinzugefügt haben, können Sie mit BlueXP persistente Volumes anzeigen.

BlueXP überwacht den Kubernetes-Cluster auf Änderungen am Backend und aktualisiert die persistente Volume-Tabelle, wenn neue Volumes hinzugefügt werden. Wenn auf dem Cluster ein automatisches Backup konfiguriert wurde, wird das Backup auf den neuen persistenten Volumes automatisch aktiviert.

Schritte

1. Doppelklicken Sie auf der Arbeitsfläche von Kubernetes auf die Arbeitsumgebung oder klicken Sie auf **Arbeitsumgebung eingeben**.
2. Klicken Sie auf der Registerkarte **Übersicht** auf **Volumes anzeigen** oder klicken Sie auf die Registerkarte **Persistente Volumes**. Wenn keine persistenten Volumes konfiguriert sind, lesen Sie "Bereitstellung" Weitere Informationen zur Bereitstellung von Volumes im Astra Trident erhalten Sie.

Eine Tabelle der konfigurierten persistenten Volumes wird angezeigt.

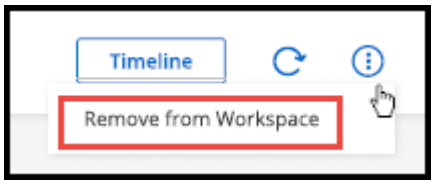


Entfernen Sie Kubernetes Cluster aus dem Workspace

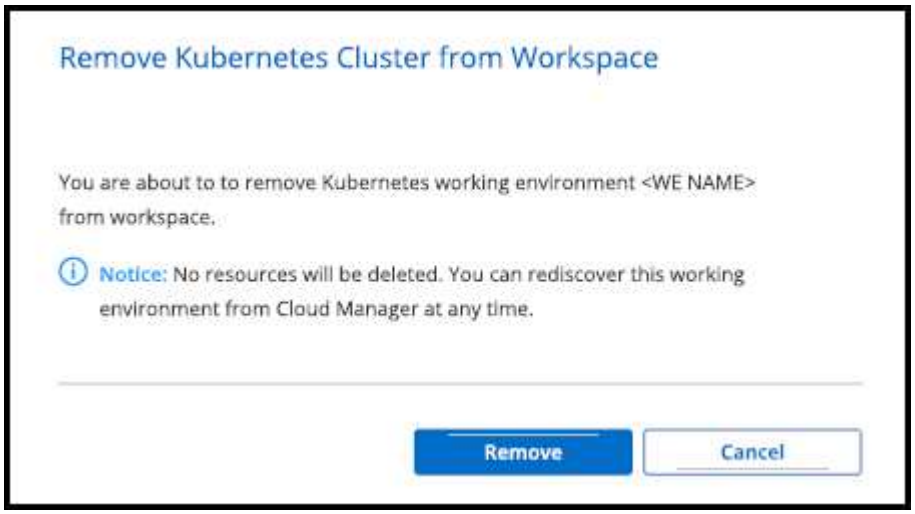
Nachdem Sie einen verwalteten Kubernetes-Cluster zum Canvas hinzugefügt haben, können Sie mit BlueXP Cluster aus dem Arbeitsbereich entfernen.

Schritte

1. Doppelklicken Sie auf der Arbeitsfläche von Kubernetes auf die Arbeitsumgebung oder klicken Sie auf **Arbeitsumgebung eingeben**.
2. Wählen Sie oben rechts auf der Seite das Menü Aktionen aus und klicken Sie auf **aus Arbeitsbereich entfernen**.



3. Klicken Sie auf **Entfernen**, um das Entfernen des Clusters aus dem Arbeitsbereich zu bestätigen. Sie können diesen Cluster jederzeit wiederentdecken.



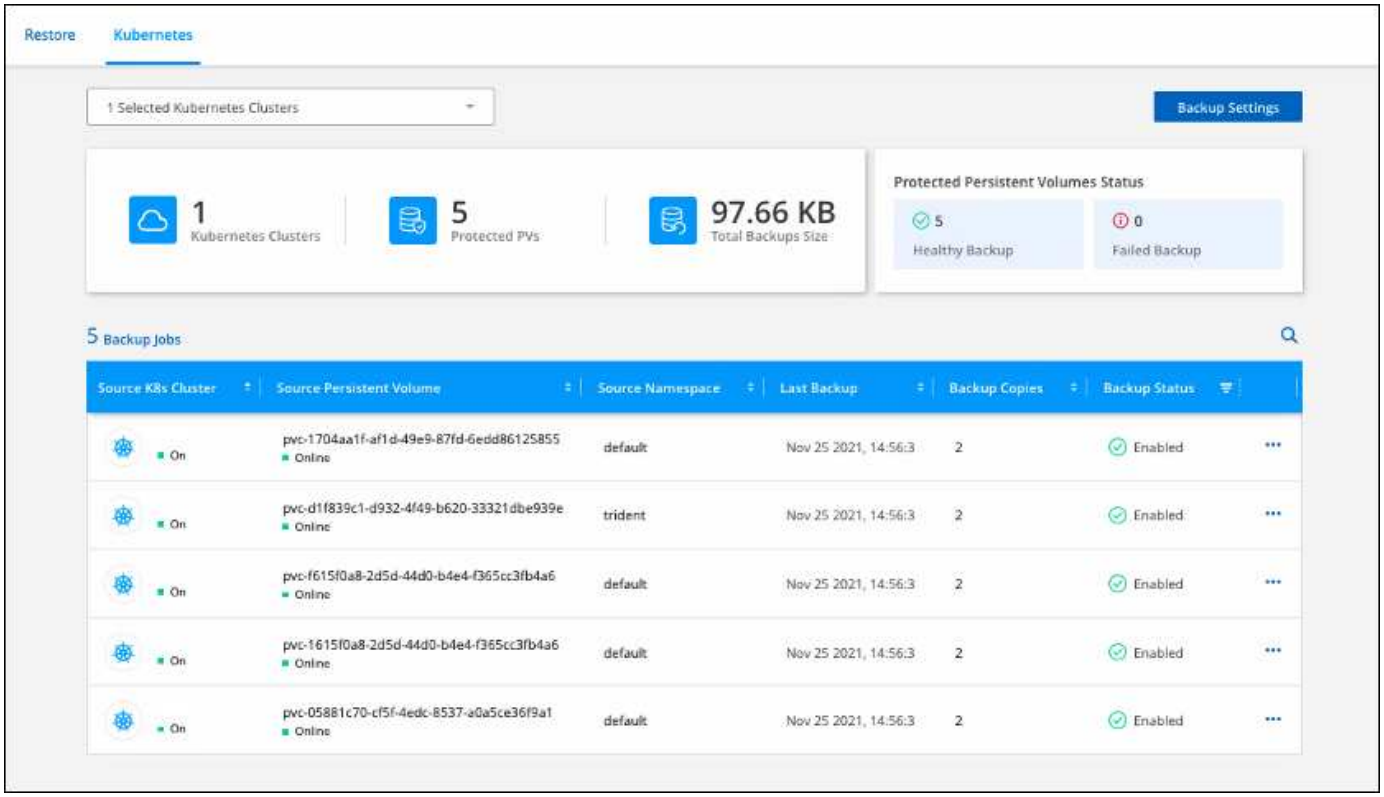
Der Kubernetes-Cluster wird aus dem Workspace entfernt und ist nicht mehr auf dem Canvas sichtbar.

Verwenden Sie NetApp Cloud-Datenservices mit Kubernetes Clustern

Nachdem Sie ein gemanagtes Kubernetes-Cluster zu Canvas hinzugefügt haben, können Sie NetApp Cloud-Datenservices für erweitertes Datenmanagement nutzen.

Cloud Backup ermöglicht das Backup persistenter Volumes auf Objekt-Storage.

"So schützen Sie Ihre Kubernetes-Cluster-Daten mit Cloud Backup".



Wissen und Support

Für den Support anmelden

Bevor Sie einen Support-Fall beim technischen Support von NetApp eröffnen können, müssen Sie BlueXP einen NetApp Support Site Account (NSS) hinzufügen und sich dann für den Support registrieren.

Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren Ihres BlueXP-Konto-ID-Support-Abonnements (Ihre 20-stellige Seriennummer 960xxxxxxxxx auf der Seite Support-Ressourcen in BlueXP).

  Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

  Diese Seriennummern werden als *PAYGO Seriennummern* bezeichnet und werden zum Zeitpunkt der Cloud Volumes ONTAP Implementierung von BlueXP generiert.

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen.

Ihre Anmeldung hängt davon ab, ob Sie ein neuer oder bereits bestehender Kunde oder Partner sind.

- Bestehender Kunde oder Partner

  Als bestehender NetApp Kunde oder Partner können Sie mit Ihrem NSS SSO-Konto (NetApp Support Site) die oben genannten Registrierungen durchführen. Im Support Dashboard stellt BlueXP eine **NSS Management**-Seite zur Verfügung, auf der Sie Ihr NSS-Konto hinzufügen können. Sobald Sie Ihr NSS-Konto hinzugefügt haben, registriert BlueXP diese Seriennummern automatisch für Sie.

  ```
  an NSS account to BlueXP,Erfahren Sie, wie Sie Ihr NSS-Konto hinzufügen.
  ```

- Neu bei NetApp

  Wenn Sie neu bei NetApp sind, müssen Sie eine einmalige Registrierung Ihrer BlueXP Account ID Seriennummer auf der Support-Registrierungsseite von NetApp abschließen. Sobald Sie diese Registrierung abgeschlossen und ein neues NSS-Konto erstellt haben, können Sie dieses Konto in BlueXP verwenden, um sich in Zukunft automatisch zu registrieren.

  ```
  with NetApp,Erfahren Sie, wie Sie sich mit NetApp anmelden können.
  ```

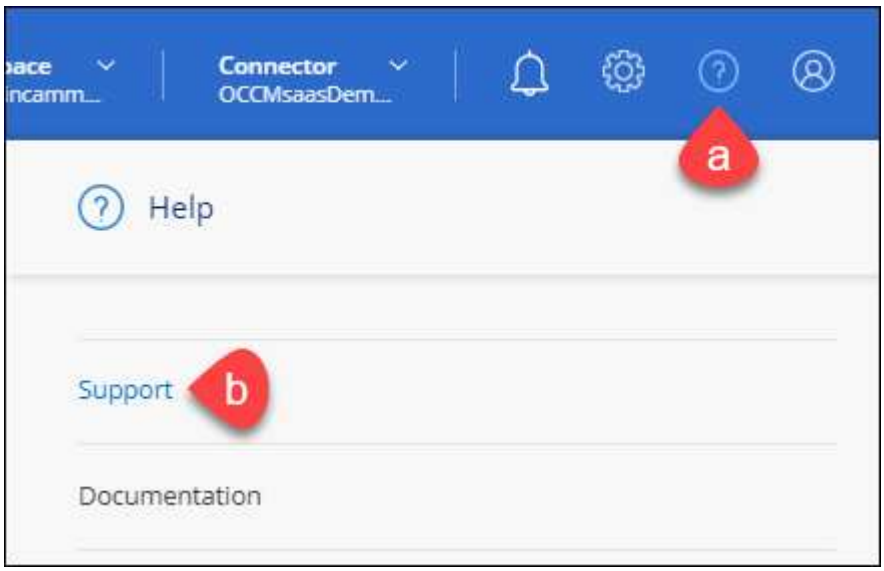
Fügen Sie ein NSS-Konto zu BlueXP hinzu

Über das Support Dashboard können Sie Ihre NetApp Support Site Konten zur Verwendung mit BlueXP hinzufügen und managen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie einen Partner- oder Reseller-Account haben, können Sie ein oder mehrere NSS-Konten hinzufügen, können aber nicht neben Kunden-Level Accounts hinzugefügt werden.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Klicken Sie auf **NSS Management > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

   NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

   Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

   Beachten Sie Folgendes:

   - Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
   - Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern. Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet wird. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ••• Menü.
   - Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ••• Menü. Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden.

Mit NetApp registrieren

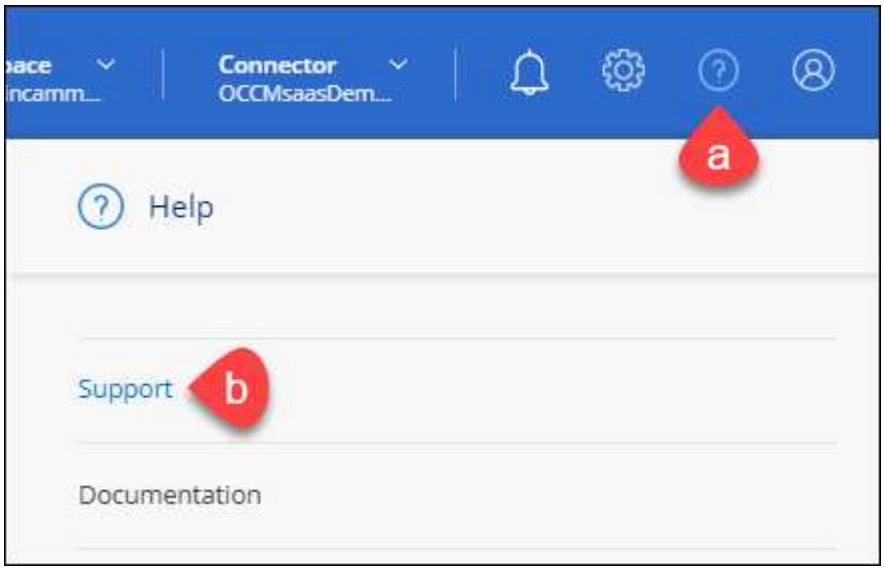
Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

Bestandskunde mit NSS-Konto

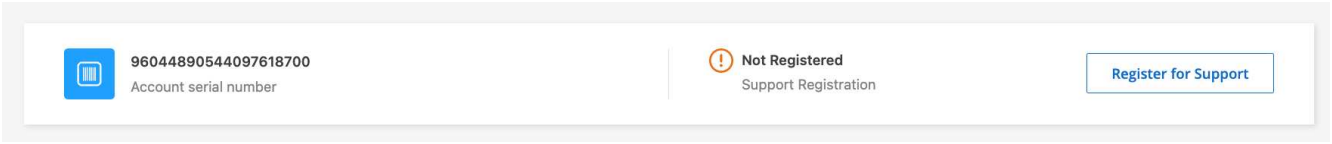
Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Wenn Sie dies noch nicht getan haben, fügen Sie Ihr NSS-Konto bei BlueXP hinzu.
3. Klicken Sie auf der Seite **Ressourcen** auf **für Support registrieren**.



Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits Kunde von NetApp mit vorhandenen Lizenzen und Seriennummern sind, aber *no* NSS Konto, müssen Sie nur ein NSS-Konto erstellen.

Schritte

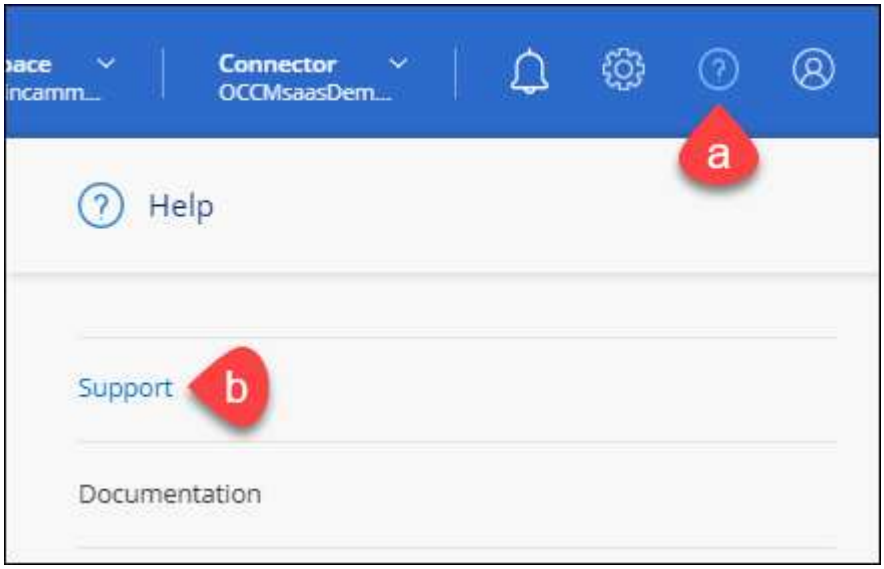
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.

Neu bei NetApp

Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.

3. Navigieren Sie zu "Die Support-Registrierungs-Website von NetApp" Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

   Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

7. Bestätigen Sie die Aktion in der E-Mail.

   Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch

wird die Kontobearbeitung beschleunigt.

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Sobald Sie Ihren NetApp Support Site Account besitzen, können Sie im Portal BlueXP diesen NSS-Account für zukünftige Registrierungen hinzufügen.

Holen Sie sich Hilfe

NetApp bietet Unterstützung für BlueXP und seine Cloud-Services auf unterschiedliche Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Self-Support

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- "Wissensdatenbank"

  Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- "Communitys"

  Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

- Dokumentation

  Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- Mailto:ng-cloudmanager-feedback@netapp.com[Feedback email]

  Wir wissen Ihre Vorschläge zu schätzen. Senden Sie uns Ihr Feedback, um BlueXP zu verbessern.

NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

Um die * Case erstellen*-Fähigkeit zu verwenden, müssen Sie zuerst eine einmalige Registrierung Ihrer BlueXP Account ID-Seriennummer (dh 960xxxx) mit NetApp "Erfahren Sie, wie Sie sich für Support registrieren".

Schritte

1. Klicken Sie in BlueXP auf **Hilfe > Support**.
2. Wählen Sie eine der verfügbaren Optionen unter Technical Support:
   a. Klicken Sie auf **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.
   b. Klicken Sie auf **Case erstellen**, um ein Ticket mit einem NetApp Support-Experten zu öffnen:

- **NetApp Support Site Account**: Wählen Sie das entsprechende NSS-Konto für die Person aus, die den Support-Case eröffnet. Diese Person ist der primäre Ansprechpartner bei NetApp, der Sie sich zusätzlich zu den unten aufgeführten zusätzlichen E-Mails mit anderen Kunden in Verbindung setzen kann.

  Wenn Ihr NSS-Konto nicht angezeigt wird, können Sie im Support-Bereich von BlueXP zur Registerkarte **NSS Management** navigieren, um es dort hinzuzufügen.

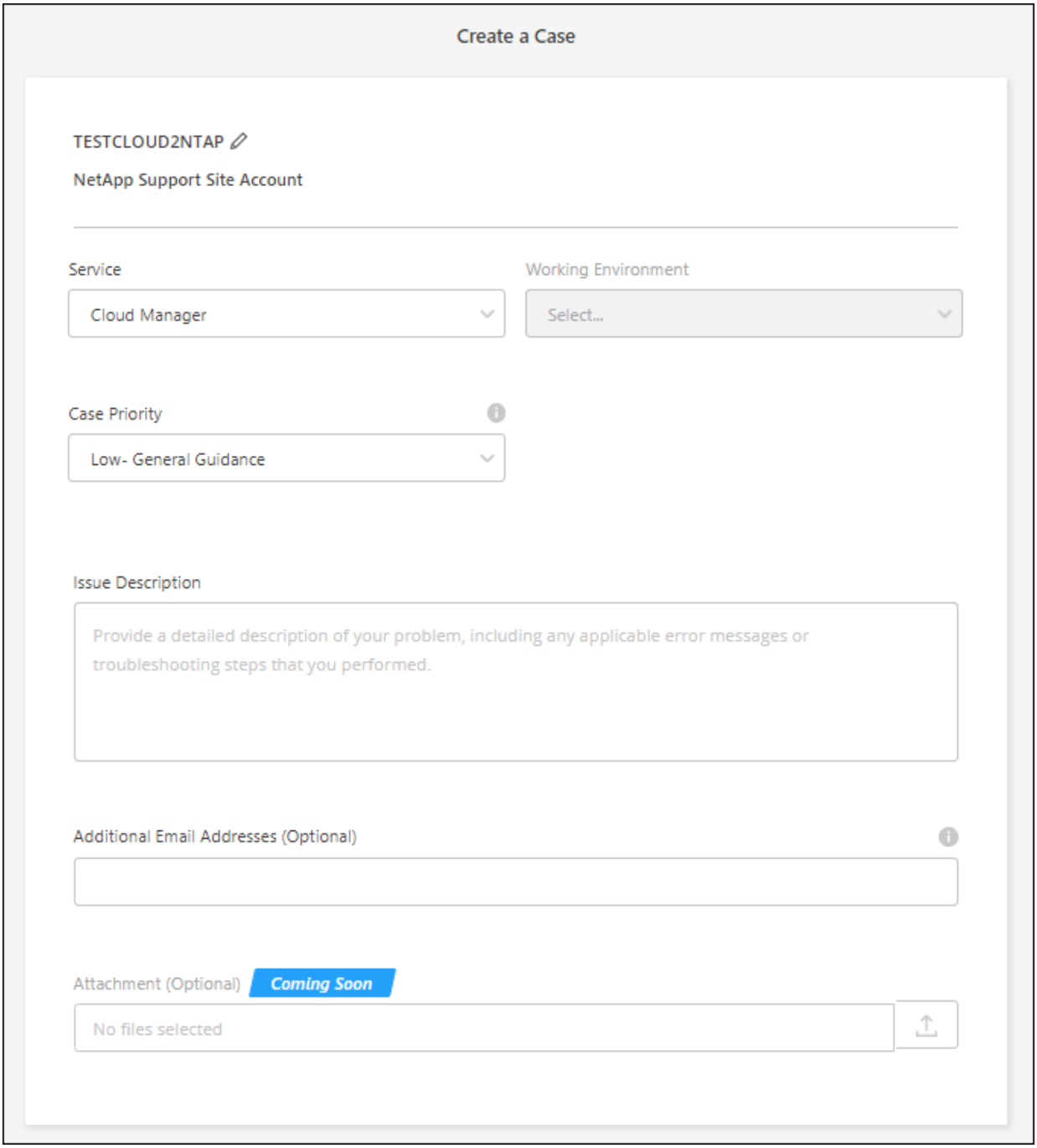
- **Service**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
- **Arbeitsumgebung**: Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

  Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Case Priority**: Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

  Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.



Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall und macht Sie umgehend mit.

Für eine Historie Ihrer Supportfälle können Sie auf **Einstellungen > Timeline** klicken und nach Aktionen mit dem Namen „Support Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Service zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh

960xxxx) oder Seriennummer der Arbeitsumgebung. Sie können Ihre Liste der NSS-Konten oben im **Case erstellen**-Formular überprüfen, um die richtige Übereinstimmung zu finden, oder Sie können Hilfe mit einer der folgenden Optionen suchen:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter https://mysupport.netapp.com/site/help

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

http://www.netapp.com/us/legal/copyright.aspx

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/us/media/patents-page.pdf

Datenschutzrichtlinie

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis für BlueXP"
- "Hinweis zum Cloud Backup"

Copyright-Informationen

Copyright © 2022 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.