# Dokumentation für Kubernetes-Cluster

## Kubernetes clusters

NetApp
April 16, 2024

# Inhalt

# Dokumentation für Kubernetes-Cluster

# Was ist neu bei Kubernetes in BlueXP

Erfahren Sie mehr über Kubernetes in BlueXP.

## Bis 02. April 2023

- Das ist jetzt möglich "Deinstallieren Sie Astra Trident" Sie wurde über den Trident Operator oder BlueXP installiert.
- Die Benutzeroberfläche wurde verbessert und Screenshots wurden in der Dokumentation aktualisiert.

## 05 März 2023

- Kubernetes in BlueXP unterstützt jetzt Astra Trident 23.01.
- Die Benutzeroberfläche wurde verbessert und Screenshots wurden in der Dokumentation aktualisiert.

## 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"
- "Importieren Sie ein OpenShift-Cluster in Cloud Manager"

## 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 unterstützt jetzt Amazon FSX for ONTAP als Back-End 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

Wird Verwendet "BlueXP" Eine kompatible Version von Astra Trident, die über den Trident Operator bereitgestellt wird, bietet folgende Vorteile:

- Kubernetes-Cluster hinzufügen und managen
- "Installation, Upgrade oder Deinstallation von Astra Trident"
- "Speicherklassen hinzufügen und entfernen"
- "Anzeige persistenter Volumes"
- "Kubernetes-Cluster entfernen" Aus dem Arbeitsbereich
- "BlueXP Backup und Recovery aktivieren oder anzeigen"

### 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.

> 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".

Sie können Astra Trident direkt aus BlueXP installieren oder ein Upgrade auf eine unterstützte Version durchführen.

"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

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

**1 Voraussetzungen prüfen**

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"

**2 Fügen Sie Ihre Kubernetes Cluster zu BlueXP hinzu**

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"

**3 Starten Sie die Bereitstellung persistenter Volumes**

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".

**4 Verwalten Sie Ihre Cluster mit BlueXP**

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. 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. Weitere Informationen finden Sie unten.

**RBAC-Autorisierung**

Die BlueXP Connector-Rolle muss für jeden Kubernetes-Cluster autorisiert sein. 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.

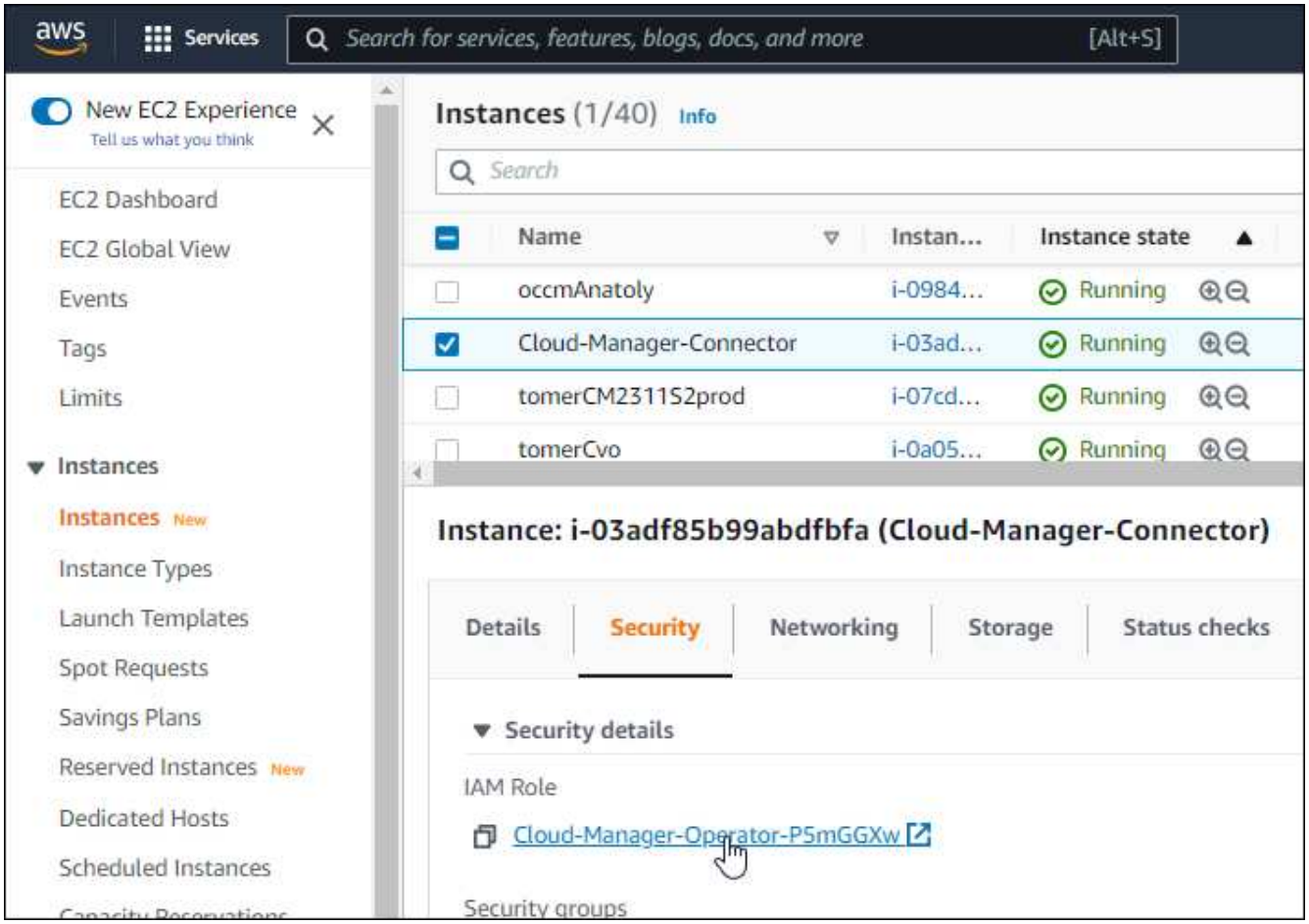
- "Erstellen Sie einen Connector von BlueXP" (Empfohlen)
- "Erstellen Sie einen Connector aus dem AWS Marketplace"
- "Installieren Sie den Connector auf einem vorhandenen Linux-Host in AWS"

### Fügen Sie die erforderlichen Berechtigungen einem vorhandenen Konnektor hinzu

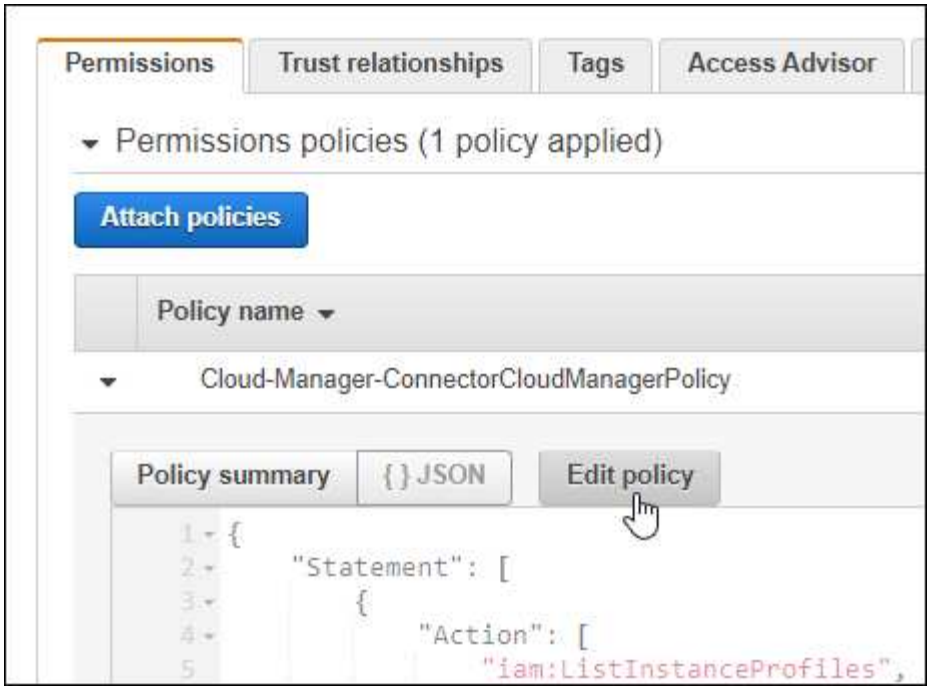
Ab Version 3.9.13 enthalten alle neu erstellten _Connectors drei neue AWS Berechtigungen, die das Erkennen und Managen von Kubernetes-Clustern ermöglichen. Wenn Sie vor dieser Version einen Connector erstellt haben, müssen Sie die vorhandene Richtlinie für die IAM-Rolle des Connectors ändern, um die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

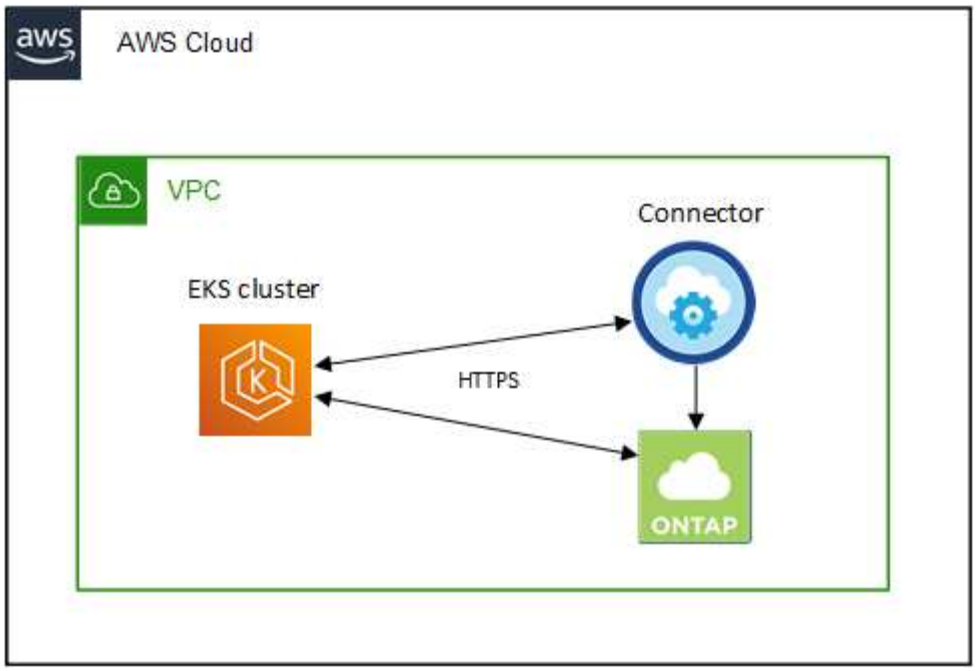
## Netzwerkanforderungen prüfen

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.

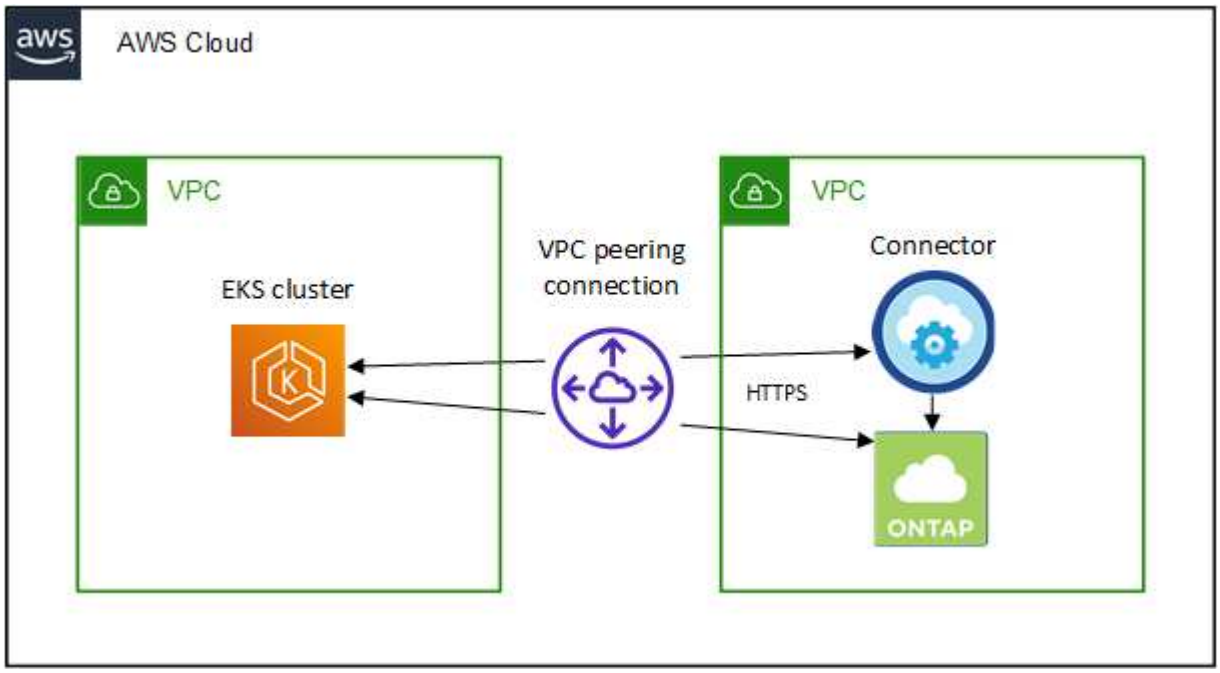
- Jeder Kubernetes-Cluster muss über eine eingehende Verbindung vom Connector verfügen
- Der Connector muss über Port 443 eine ausgehende Verbindung zu jedem Kubernetes-Cluster haben

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. Sie können die Autorisierung an Ihre Anforderungen anpassen.

**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
```

```yaml
            - 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. 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. 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. 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**.

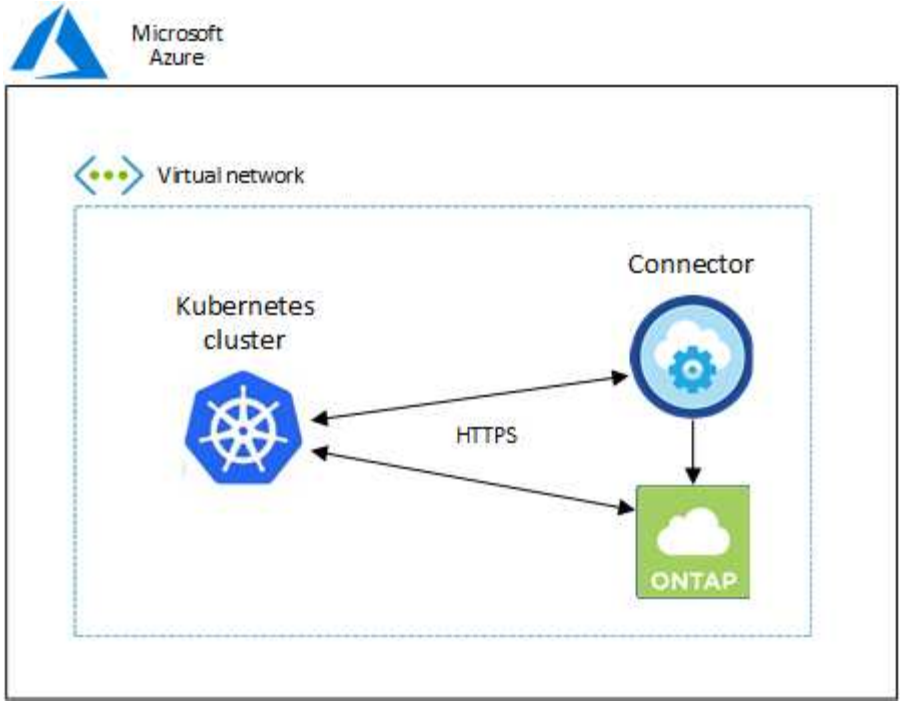
## Netzwerkanforderungen prüfen

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.

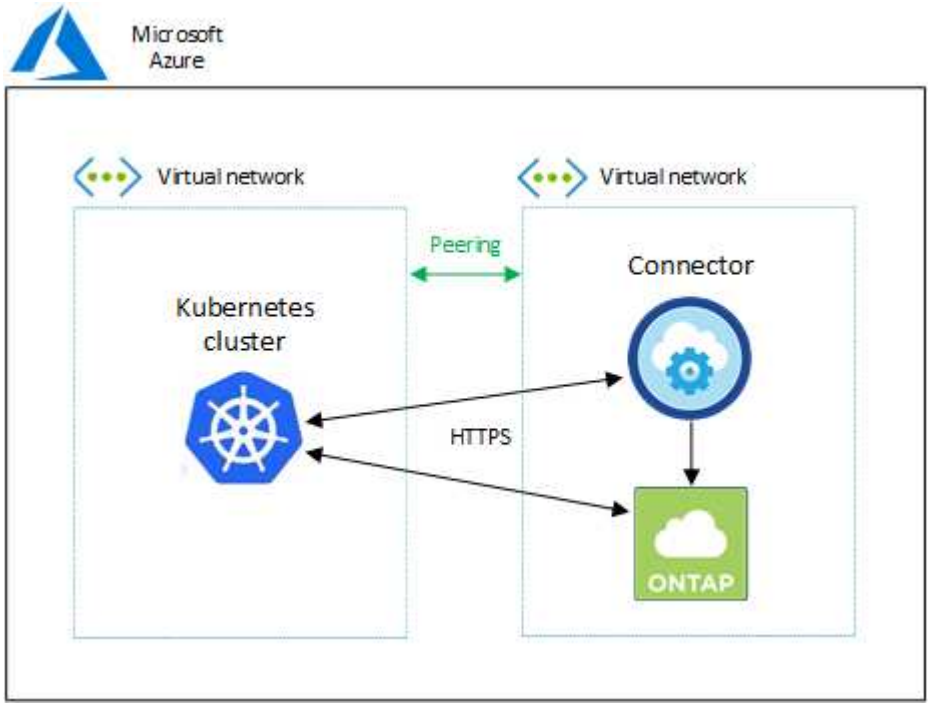
- Jeder Kubernetes-Cluster muss über eine eingehende Verbindung vom Connector verfügen
- Der Connector muss über Port 443 eine ausgehende Verbindung zu jedem Kubernetes-Cluster haben

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**

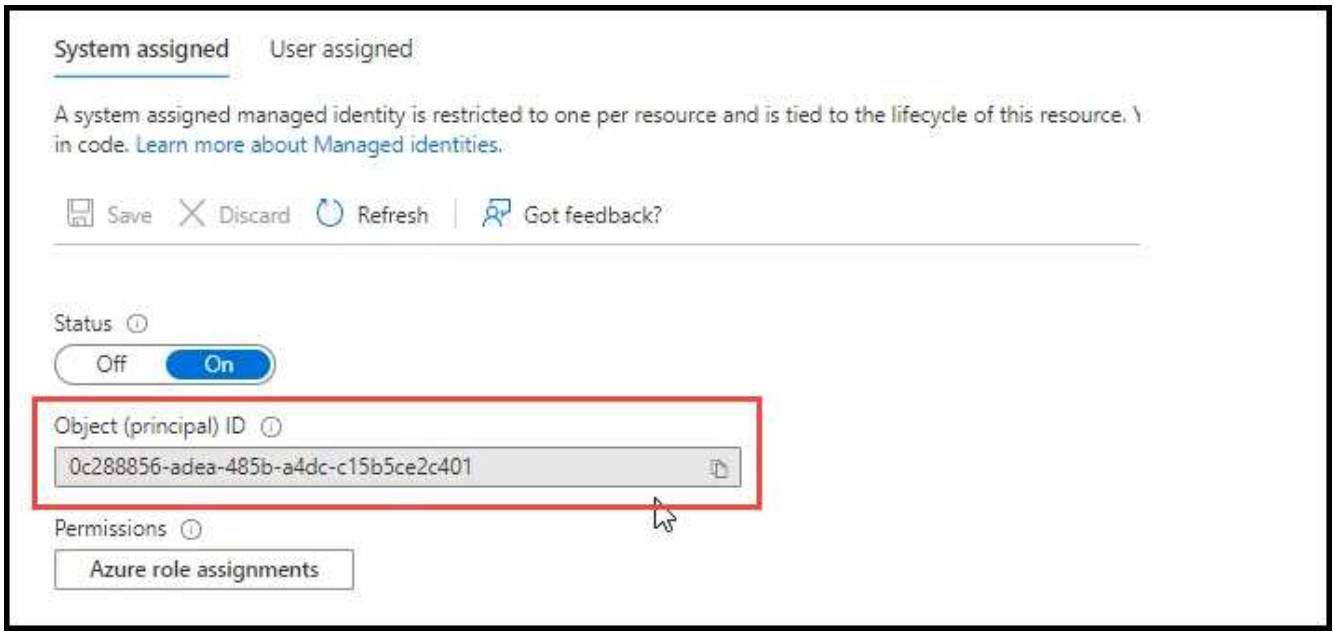
Zur Installation von Astra Trident müssen Sie für BlueXP die vollständige Autorisierung bereitstellen.

> 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.

**Bevor Sie beginnen**

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.

**Schritte**

Erstellen Sie eine Cluster-Rolle und Rollenbindung.

1. Sie können die Autorisierung an Ihre Anforderungen anpassen.

**Backup/Restore**

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

Ersetzen Sie den `subjects: kind:` Variable mit Ihrem Benutzernamen und `subjects: name:` Entweder mit der Objekt-ID für die vom System zugewiesene verwaltete Identität oder mit dem Benutzernamen eines autorisierten Benutzers, wie oben beschrieben.

```
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.

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.

```
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.

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

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. 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. 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. 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.

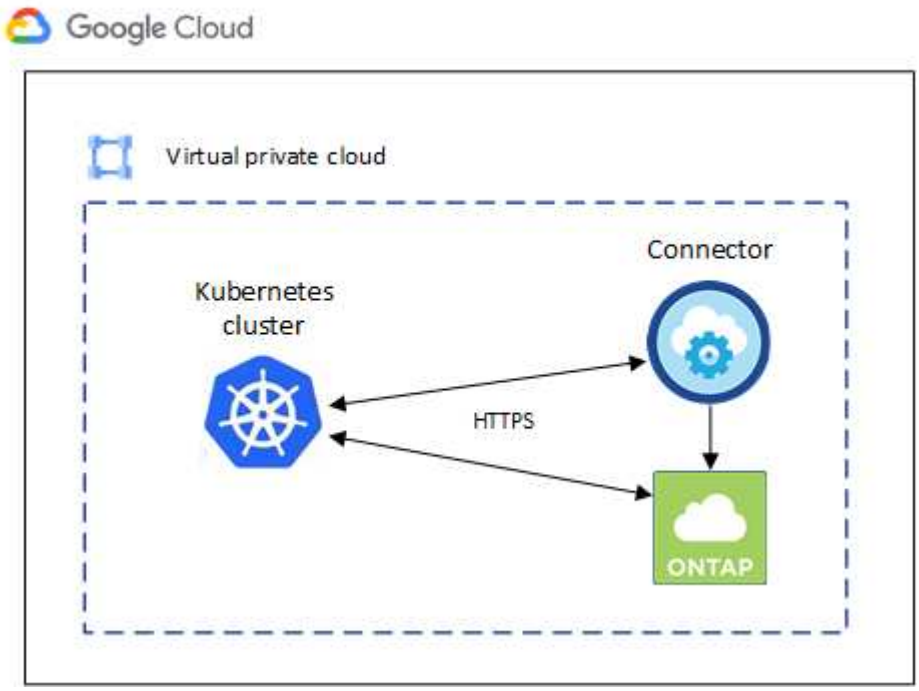
## Netzwerkanforderungen prüfen

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.

#### Bevor Sie beginnen

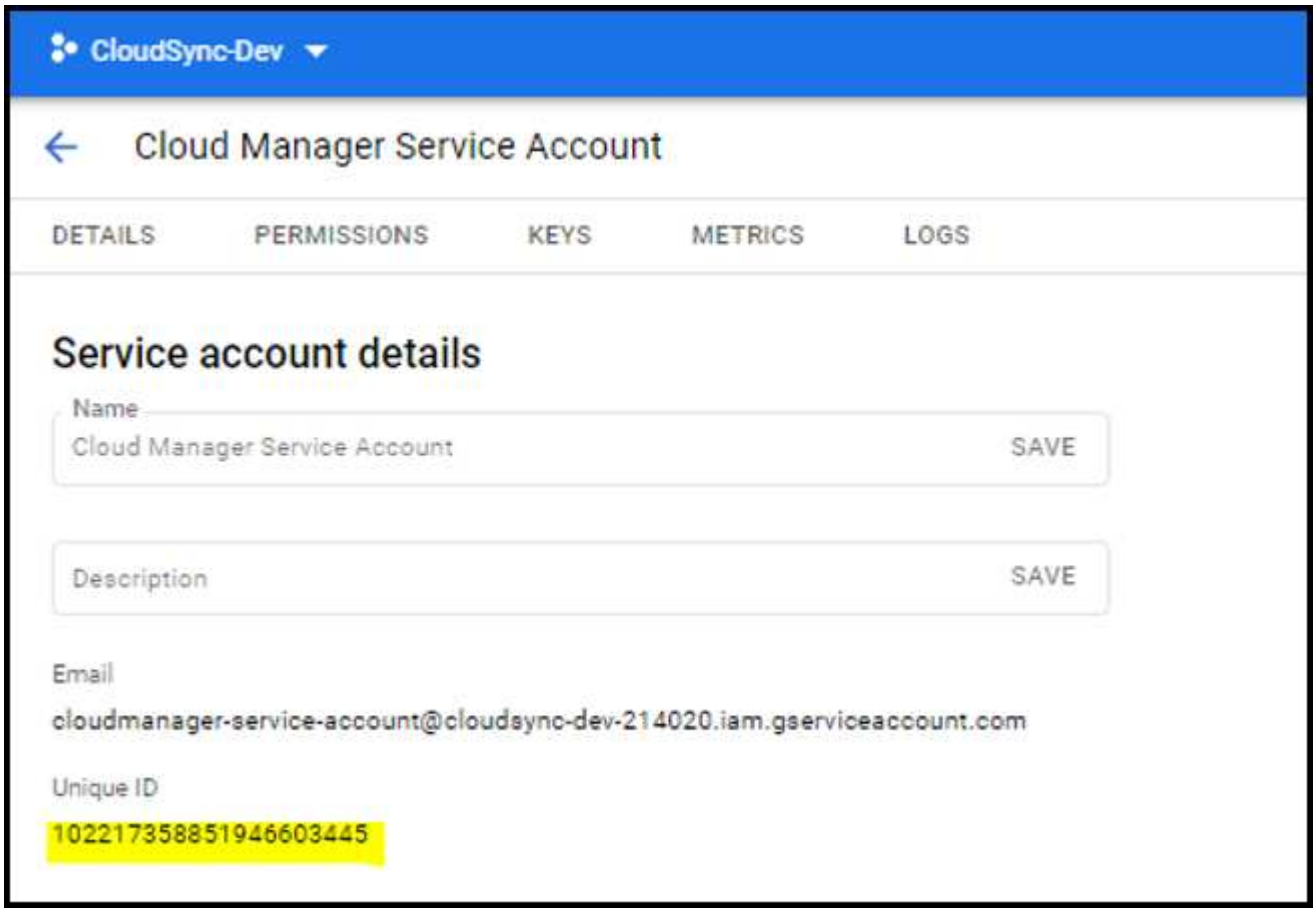
Zu konfigurieren `subjects: name:` In der YAML-Datei müssen Sie die eindeutige BlueXP-ID kennen.

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".




**Schritte**

Erstellen Sie eine Cluster-Rolle und Rollenbindung.

1. Sie können die Autorisierung an Ihre Anforderungen anpassen.

**Backup/Restore**

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

Ersetzen Sie den `subjects: kind:` Variable mit Ihrem Benutzernamen und `subjects: name:` Mit der eindeutigen ID für das autorisierte Servicekonto.

```
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.

Ersetzen Sie den `subjects: kind:` Variable mit Ihrem Benutzernamen und `subjects: user:` Mit der eindeutigen ID für das autorisierte Servicekonto.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
          - ''
      resources:
```

```yaml
            - 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. Erstellen Sie eine kubeconfig-Datei.

- 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
```

**Ergebnis**

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

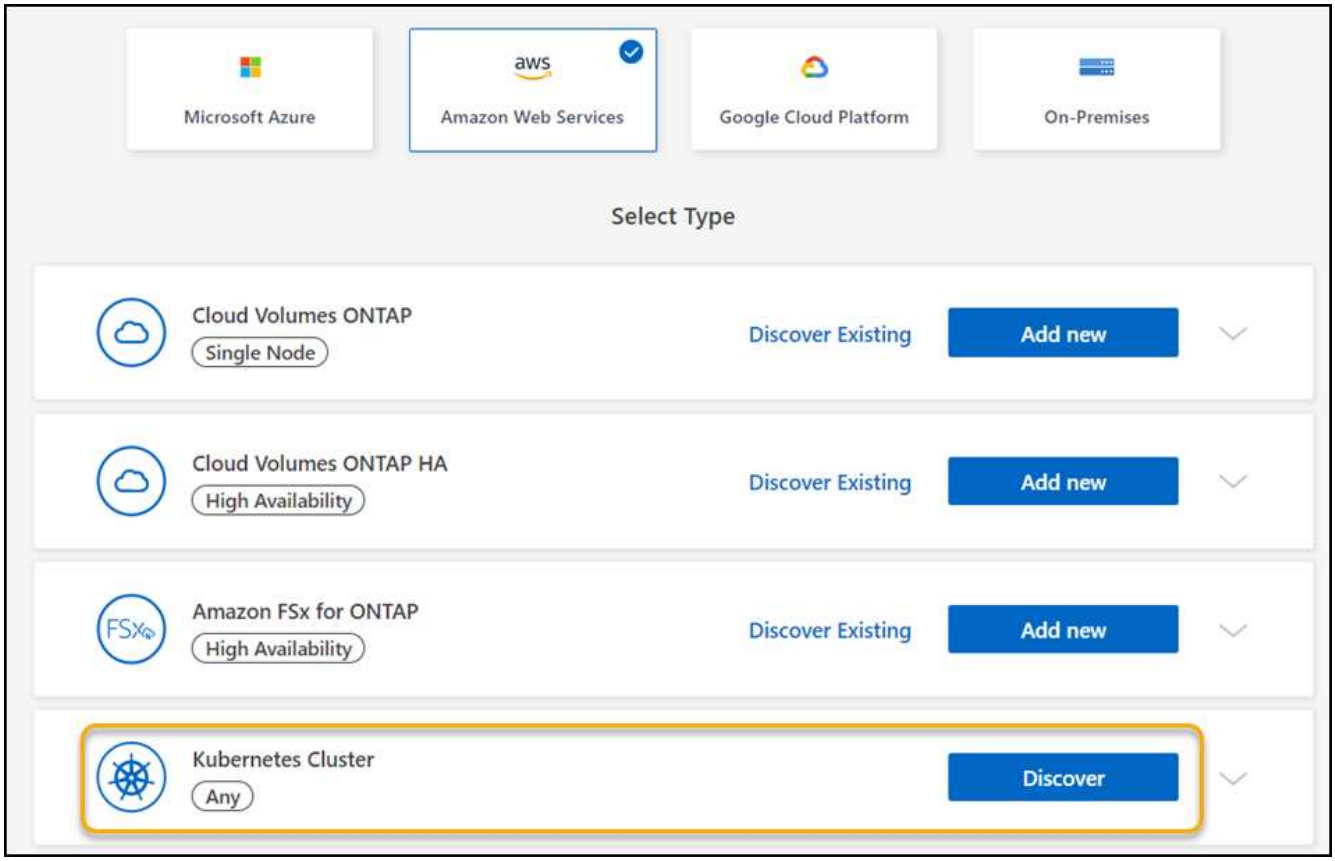
Kubernetes-Cluster können ermittelt oder in BlueXP importiert werden, sodass Sie persistente Volumes in Amazon S3 sichern können.

### Erkennen eines Clusters

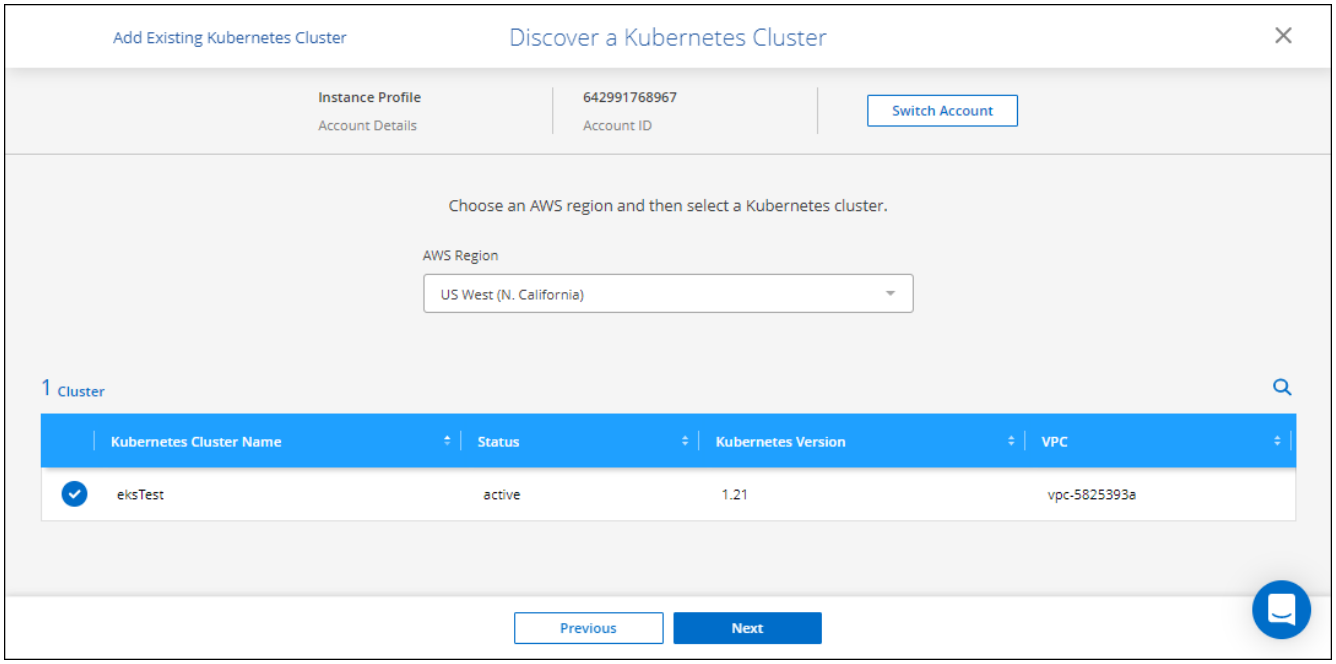
Es wird ein vollständig gemanagter oder selbst gemanagter Kubernetes Cluster ermittelt. Verwaltete Cluster müssen erkannt werden; sie können nicht importiert werden.

#### Schritte

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

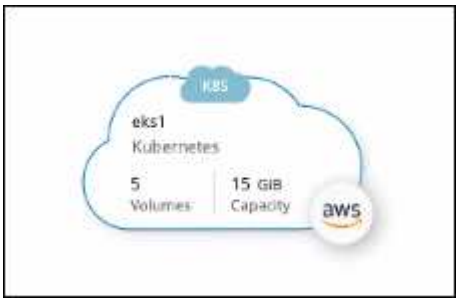



3. Wählen Sie **Discover Cluster** und klicken Sie auf **Next**.
4. Wählen Sie eine AWS-Region aus, wählen Sie einen Kubernetes-Cluster aus und klicken Sie auf **Weiter**.




**Ergebnis**

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

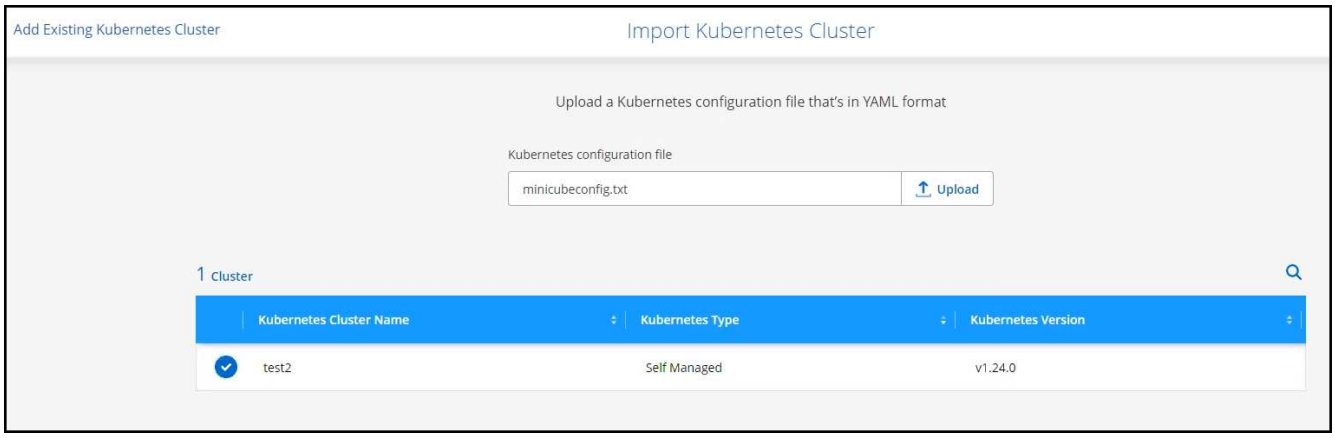



## Importieren Sie einen Cluster

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** > **Discover**.
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**.

**Ergebnis**

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

# Fügen Sie einen Azure Kubernetes Cluster zu BlueXP hinzu

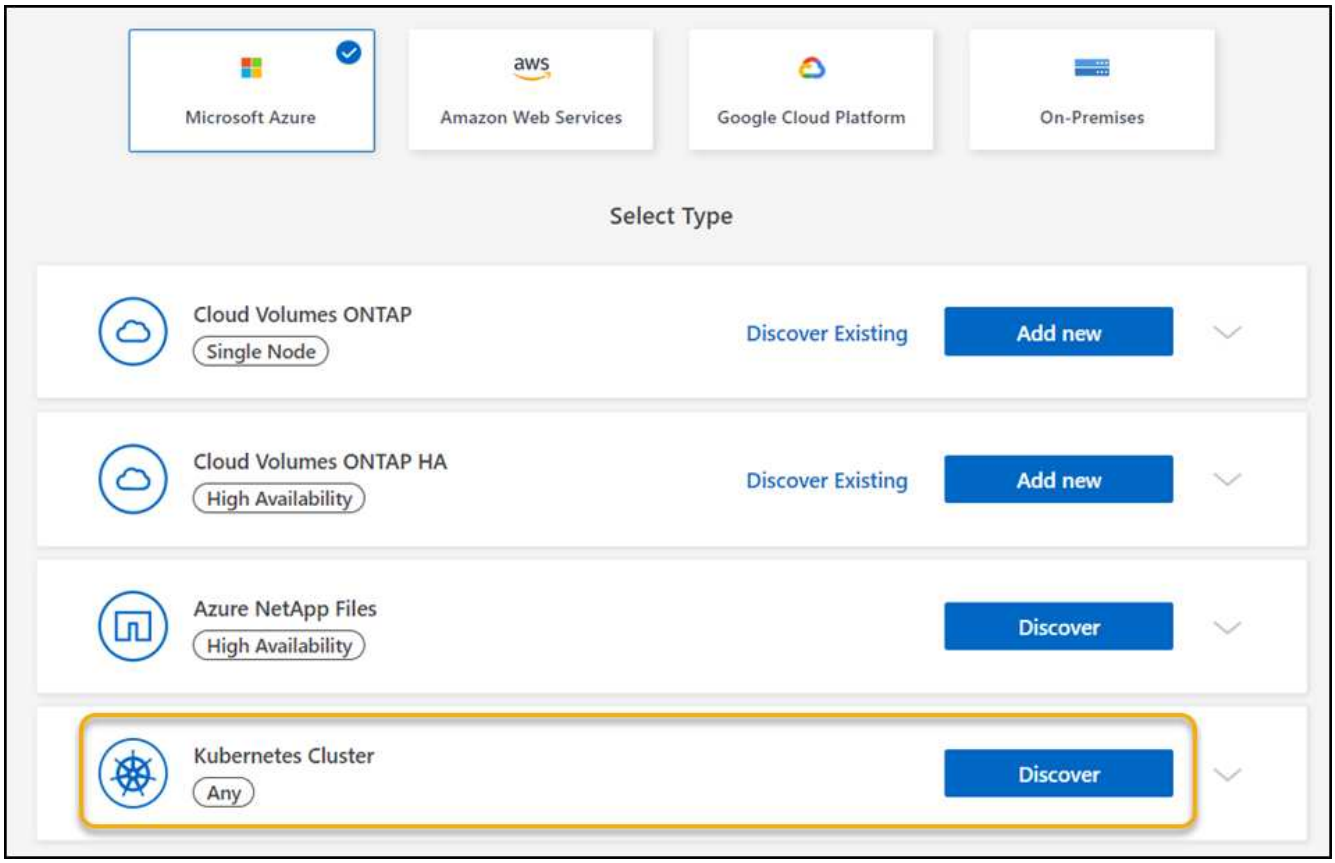
Sie können Kubernetes-Cluster ermitteln oder in BlueXP importieren, damit Sie persistente Volumes in Azure sichern können.

## Erkennen eines Clusters

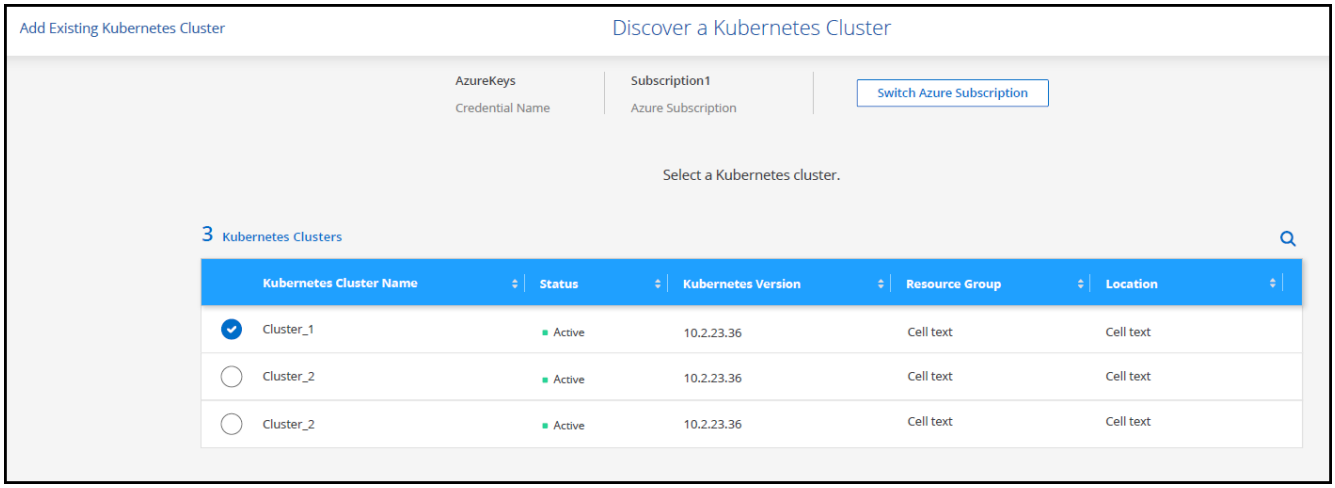
Es wird ein vollständig gemanagter oder selbst gemanagter Kubernetes Cluster ermittelt. Verwaltete Cluster müssen erkannt werden; sie können nicht importiert werden.

**Schritte**

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

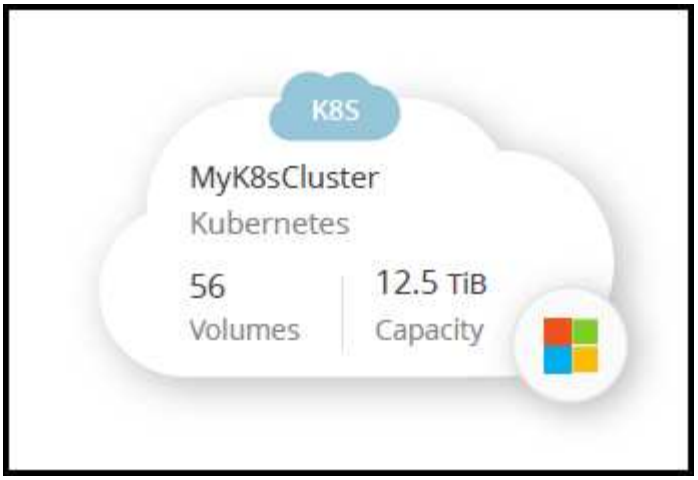



3. Wählen Sie **Discover Cluster** und klicken Sie auf **Next**.
4. Wählen Sie einen Kubernetes Cluster aus und klicken Sie auf **Next**.




**Ergebnis**

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.




## Importieren Sie einen Cluster

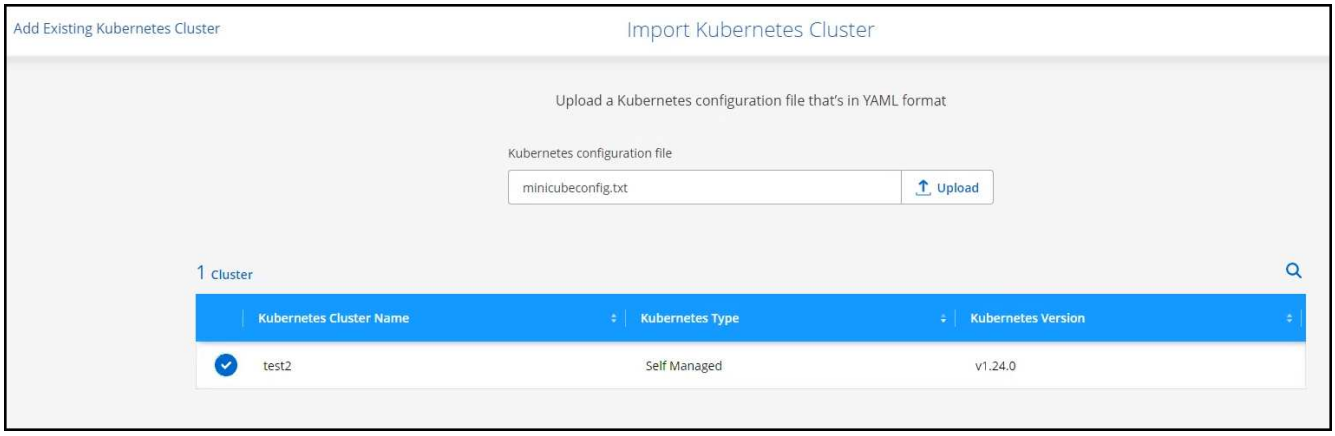
Es ist möglich, ein selbst verwaltetes Kubernetes-Cluster mithilfe einer Kubernetes-Konfigurationsdatei zu importieren.

## Bevor Sie beginnen

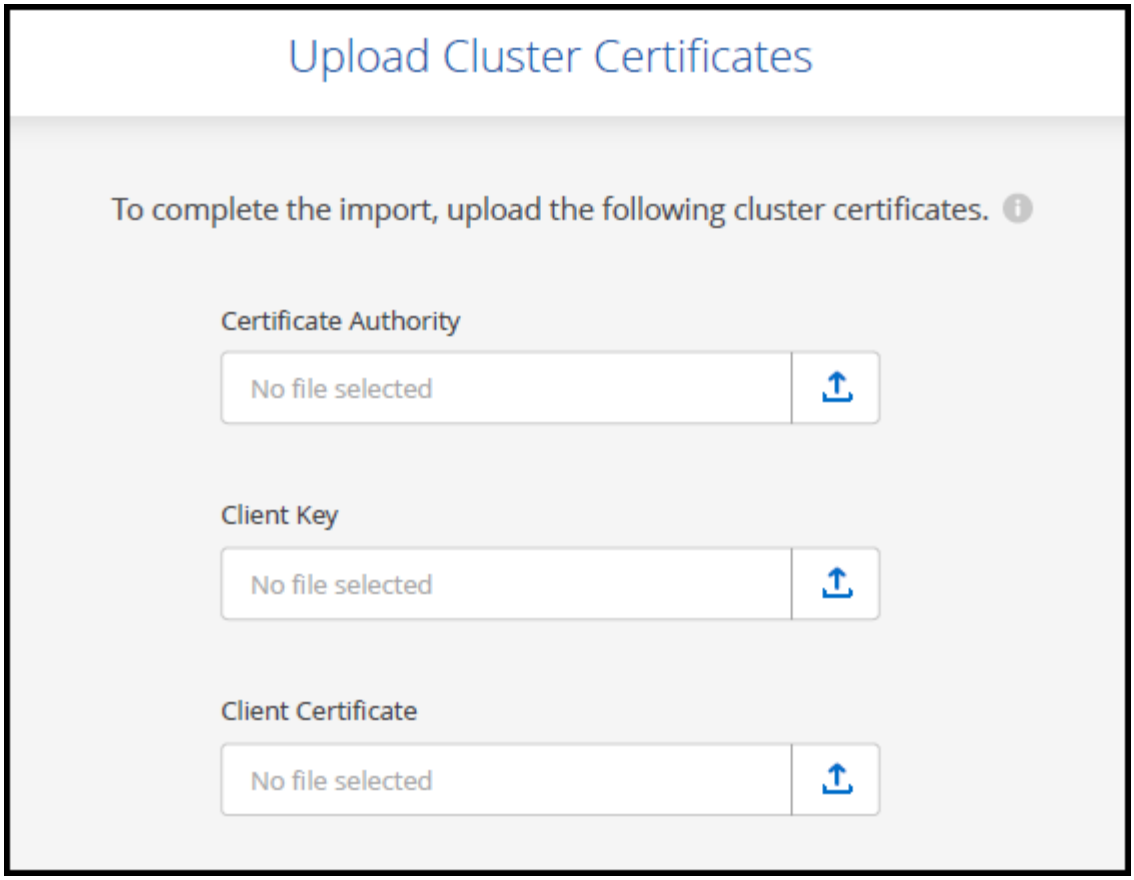
Für den in der Clusterrolle YAML-Datei angegebenen Benutzer benötigen Sie Zertifikate für Zertifizierungsstelle, Clientschlüssel und Clientzertifikat, um Kubernetes-Cluster zu importieren. Der Kubernetes-Cluster-Administrator erhält diese Zertifizierungen, wenn er Benutzer auf dem Kubernetes-Cluster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

### Schritte

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




**Ergebnis**

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

# Fügen Sie ein Google Cloud Kubernetes Cluster zu BlueXP hinzu

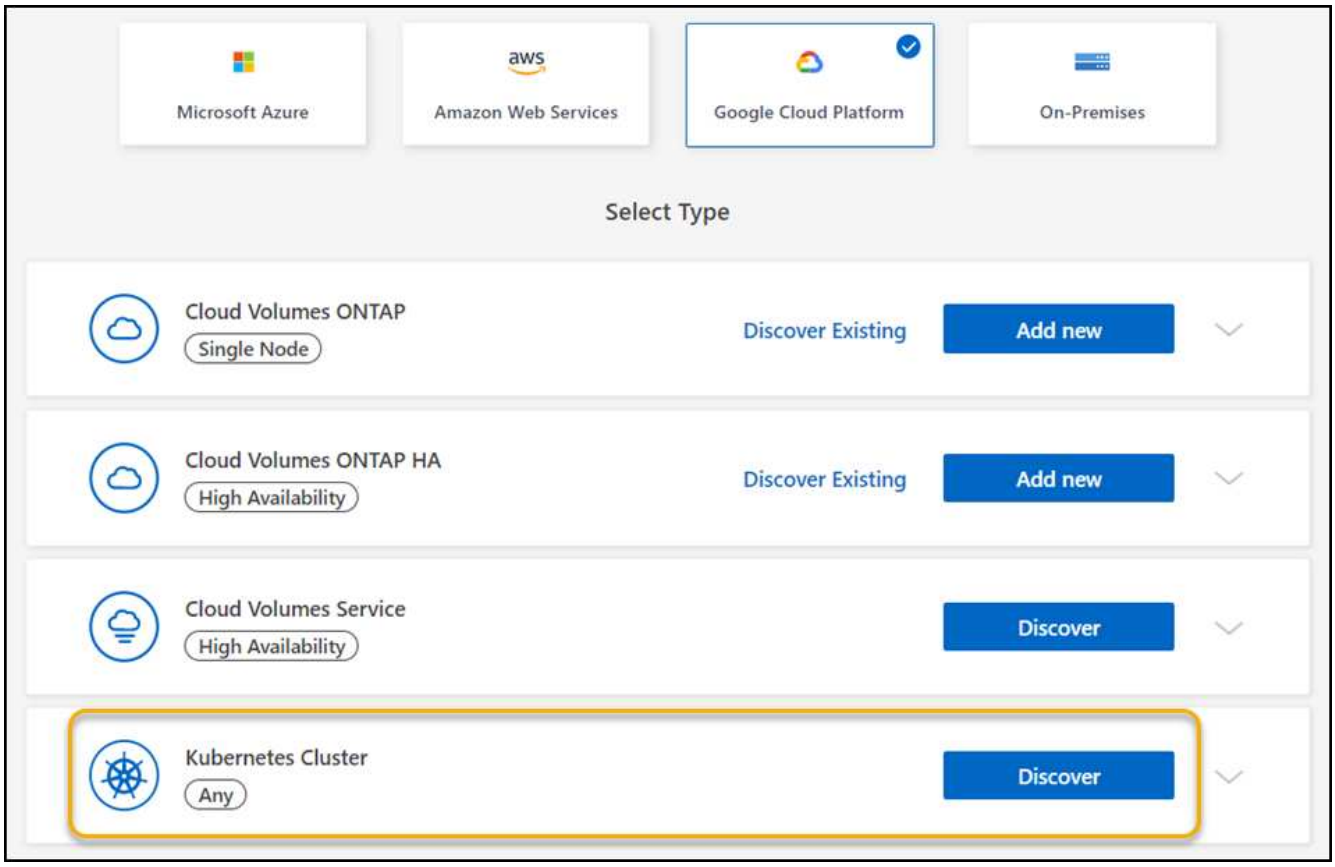
Kubernetes-Cluster können ermittelt oder in BlueXP importiert werden, sodass Sie persistente Volumes in Google Cloud sichern können.

## Erkennen eines Clusters

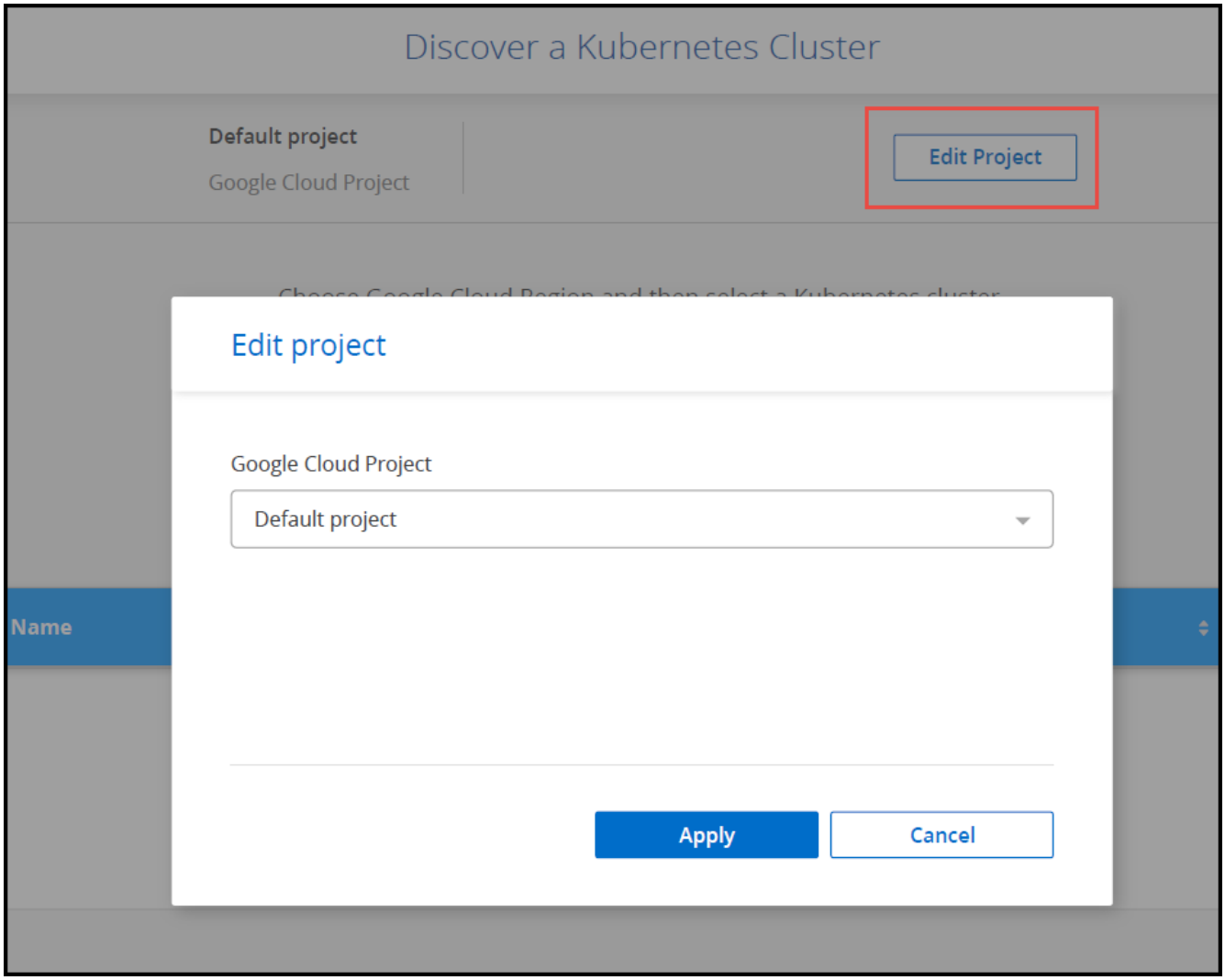
Es wird ein vollständig gemanagter oder selbst gemanagter Kubernetes Cluster ermittelt. Verwaltete Cluster müssen erkannt werden; sie können nicht importiert werden.

**Schritte**

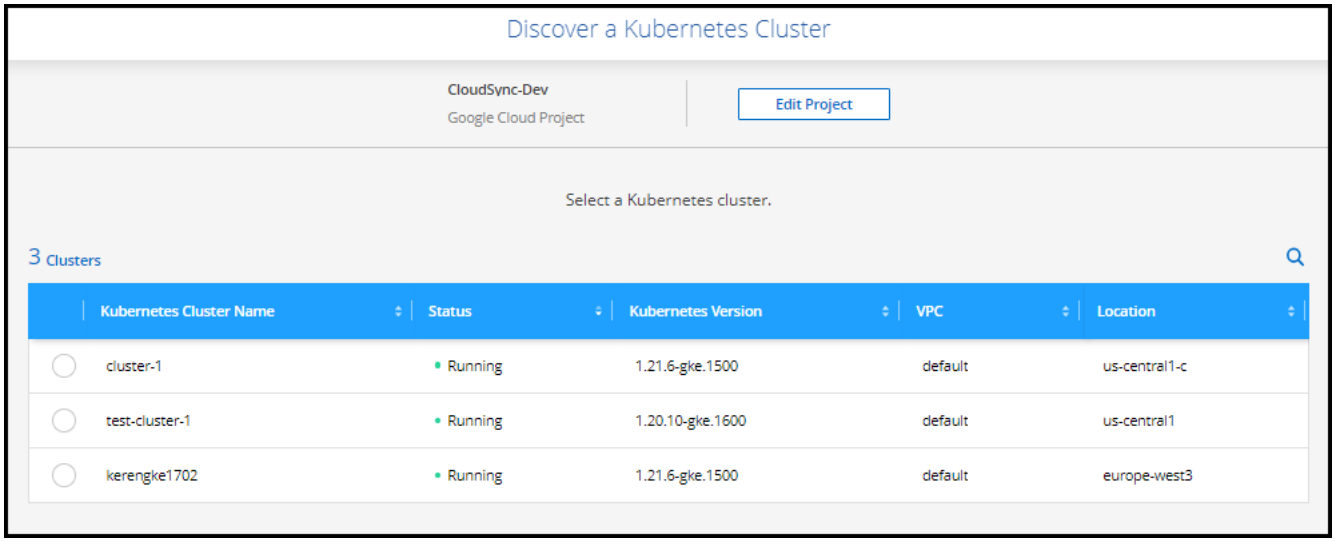
1. Klicken Sie auf der **Arbeitsfläche** auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie **Google Cloud Platform** > **Kubernetes Cluster** > **Discover**.




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.

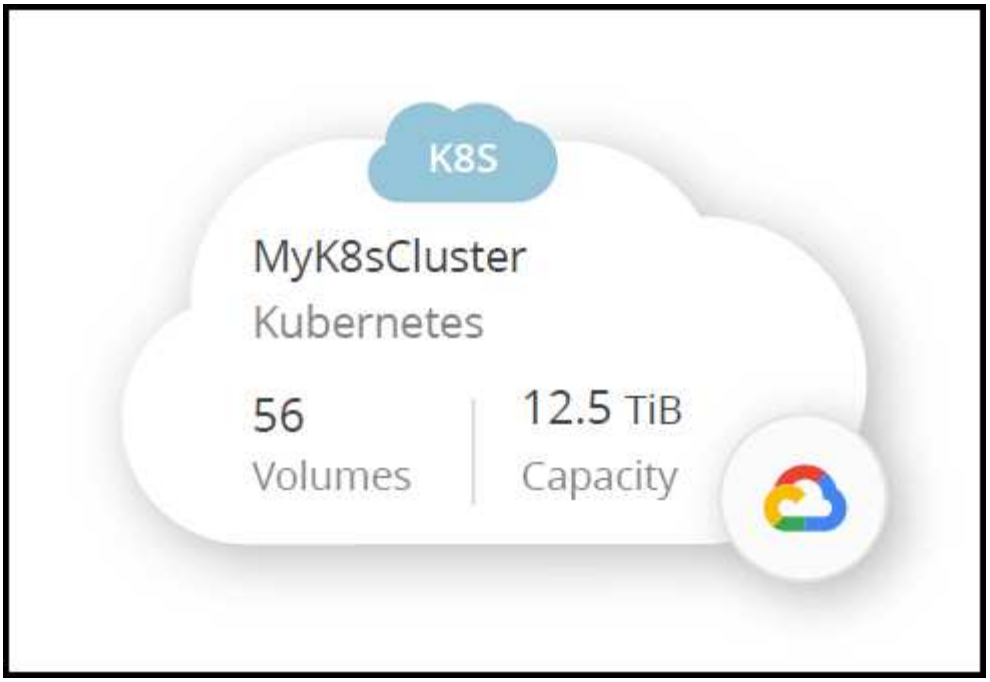



5. Wählen Sie einen Kubernetes Cluster aus und klicken Sie auf **Next**.




**Ergebnis**

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.




## Importieren Sie einen Cluster

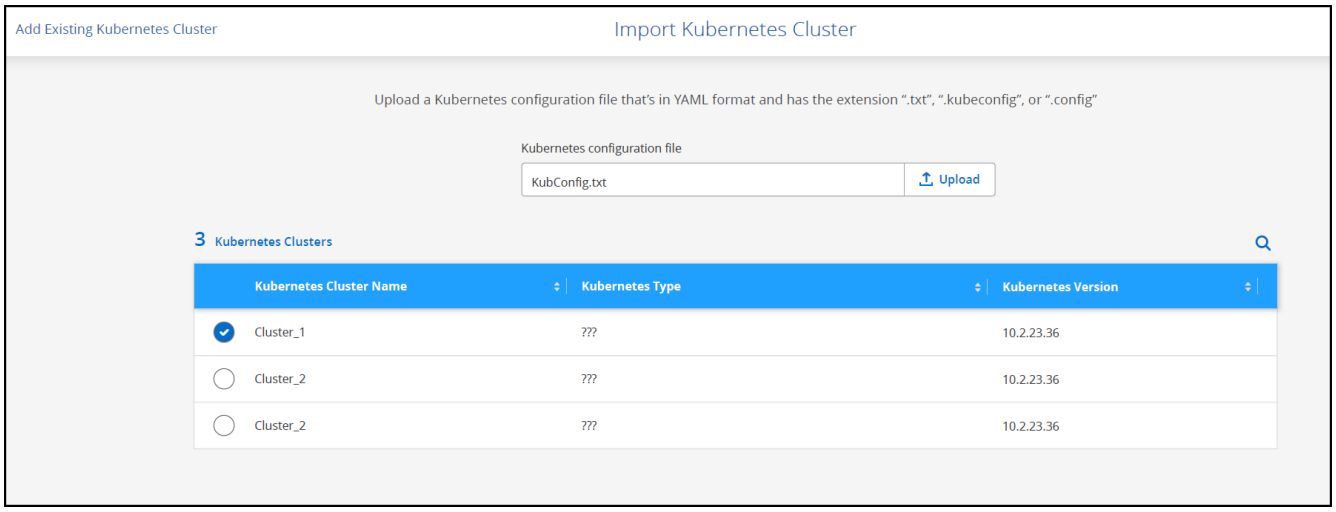
Es ist möglich, ein selbst verwaltetes Kubernetes-Cluster mithilfe einer Kubernetes-Konfigurationsdatei zu importieren.

## 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** > **Discover**.
3. Wählen Sie **Cluster importieren** und klicken Sie auf **Weiter**.
4. Laden Sie eine Kubernetes-Konfigurationsdatei im YAML-Format hoch.




### Ergebnis

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

# Importieren Sie ein OpenShift-Cluster in BlueXP

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.

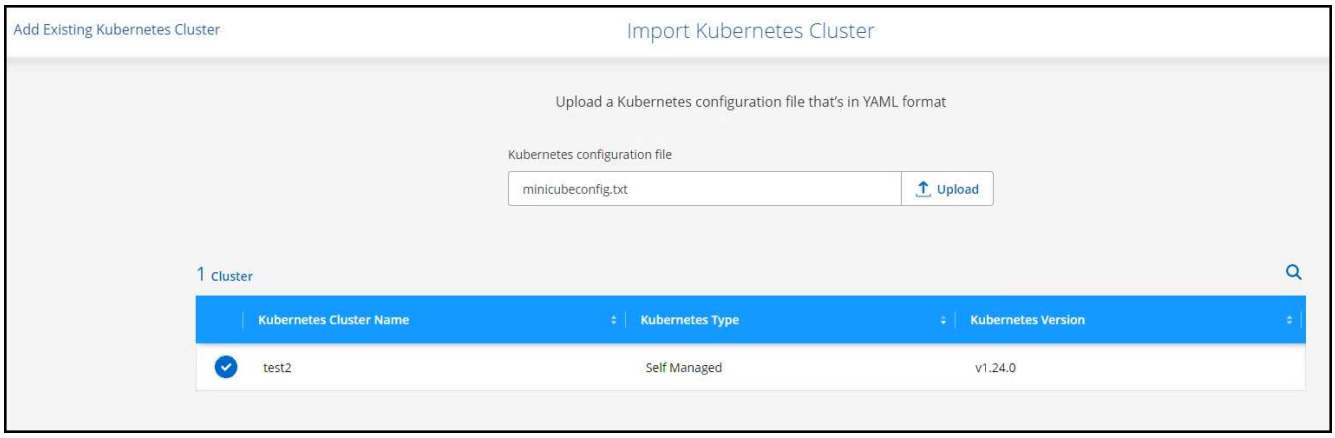
### Bevor Sie beginnen

Vor dem Importieren eines OpenShift-Clusters müssen Sie:

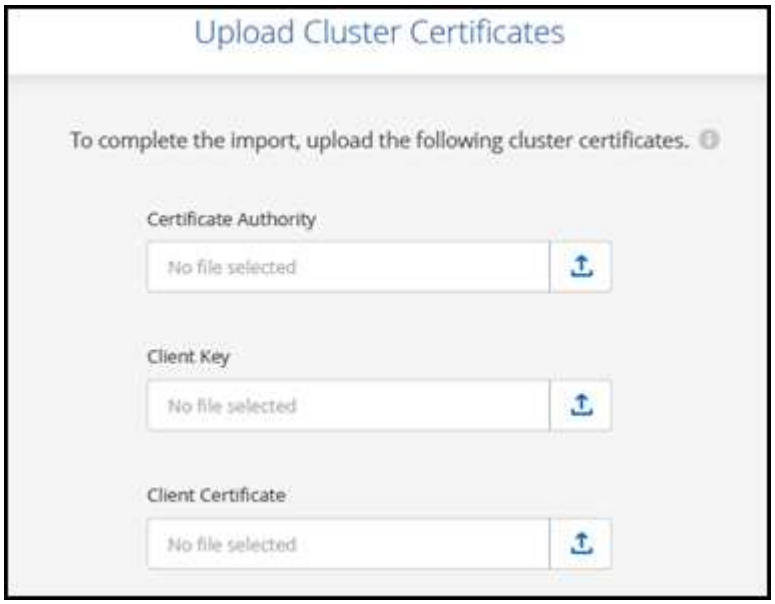
- Die Datei `kubeconfig-sa`, die Sie in erstellt haben "Erstellen Sie eine kubeconfig-Datei".
- Die öffentlichen Zertifikatsinstanz (z. B. Ca.crt), der Clientschlüssel (z. B. tls.Key) und die Clientzertifizierungs- (z. B. tls.crt)-Dateien für den Cluster.

### Schritte

1. Wählen Sie auf der **Arbeitsfläche** die Option * Arbeitsumgebung hinzufügen*.
2. Wählen Sie Ihren Cloud-Provider aus und wählen Sie **Kubernetes Cluster** > **Discover**.
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.




**Ergebnis**

BlueXP fügt dem Canvas den Kubernetes-Cluster hinzu.

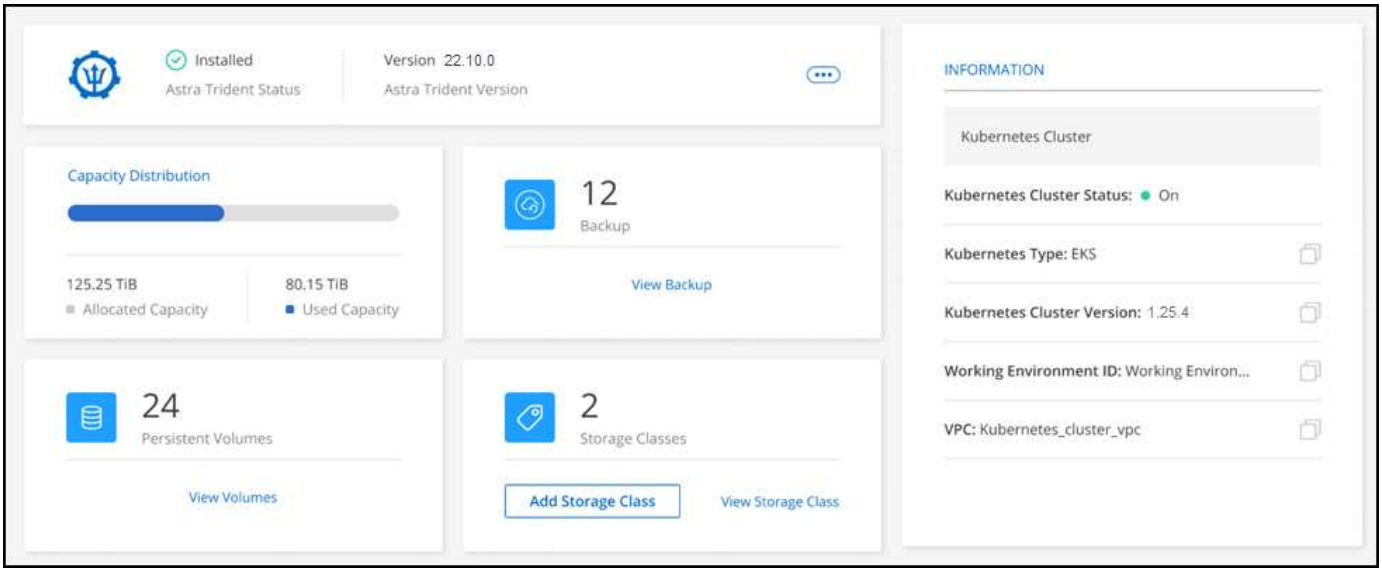
# Managen Sie Kubernetes-Cluster

## Managen Sie Astra Trident

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

### Astra Trident in BlueXP

Nachdem Sie Kubernetes-Cluster zu BlueXP hinzugefügt haben, können Sie Astra Trident und Ihre Kubernetes-Cluster über die Übersichtsseite managen. Doppelklicken Sie zum Öffnen der Übersichtsseite auf die Kubernetes-Arbeitsumgebung auf dem Bildschirm.




#### Unterstützte Astra Trident Versionen

Eine der vier aktuellsten Versionen von Astra Trident ist mit dem Trident-Operator implementiert – entweder manuell oder mit Helm-Chart. Wenn Astra Trident nicht installiert ist oder eine inkompatible Version von Astra Trident installiert ist, wird im Cluster angezeigt, dass eine Aktion erforderlich ist.

> Astra Trident ist implementiert mit `tridentctl` Wird nicht unterstützt. Bei der Implementierung von Astra Trident mit `tridentctl`, Sie können BlueXP nicht verwenden, um Ihre Kubernetes-Cluster zu verwalten oder Astra Trident zu deinstallieren. Unbedingt Und installieren Sie Astra Trident entweder manuell mit "Trident Betreiber" Oder in BlueXP basierend auf NetApp Installation oder Upgrade von Astra Trident.

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

### Installation oder Upgrade von Astra Trident

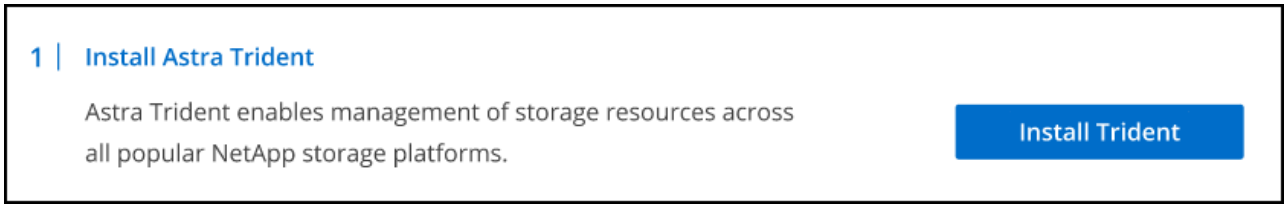
Ihren Astra Trident Installationsstatus und Ihre Version können Sie auf der Übersichtsseite einsehen. Wenn Astra Trident noch nicht installiert ist oder eine inkompatible Version installiert ist, können Sie das mit BlueXP

verwalten.

**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**.

   Ein Upgrade von Astra Trident Versionen vor 21.01 kann nicht mit BlueXP durchgeführt werden. Informationen zum Upgrade von einer früheren Version finden Sie unter "Upgrade mit dem Bediener".

**Ergebnisse**

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

## Deinstallieren Sie Astra Trident

Wenn Sie Astra Trident mit BlueXP installiert haben oder den Trident Operator verwenden (entweder Helm oder manuell), können Sie ihn mit BlueXP deinstallieren.

- Nach der Deinstallation von Astra Trident können Sie keine neuen persistenten Volumes erstellen, es sind aber noch vorhandene Volumes verfügbar.
- Astra Trident wird deinstalliert, aber das Backup ist nicht verfügbar.
- Sie können Astra Trident jederzeit in der Arbeitsumgebung neu installieren, um mit dem Management von Clustern fortzufahren.

Durch die Deinstallation von Astra Trident mit BlueXP werden nicht alle Astra Trident Services entfernt, die während der Installation angewendet werden. Informationen zum vollständigen Entfernen von Astra Trident, einschließlich aller von ihm erstellten benutzerdefinierten Ressourcendefinitionen (CRDs) finden Sie unter "Deinstallieren mit dem Trident-Operator"

**Schritte**

1. Wählen Sie auf der Übersichtsseite die Ellipsen aus und **Astra Trident deinstallieren**.


2. Wählen Sie **Uninstall**, um Astra Trident zu bestätigen und zu deinstallieren.

**Ergebnisse**

Astra Trident wird jetzt aus der Arbeitsumgebung deinstalliert. Sie können Astra Trident jederzeit neu installieren.

# Management von Storage-Klassen

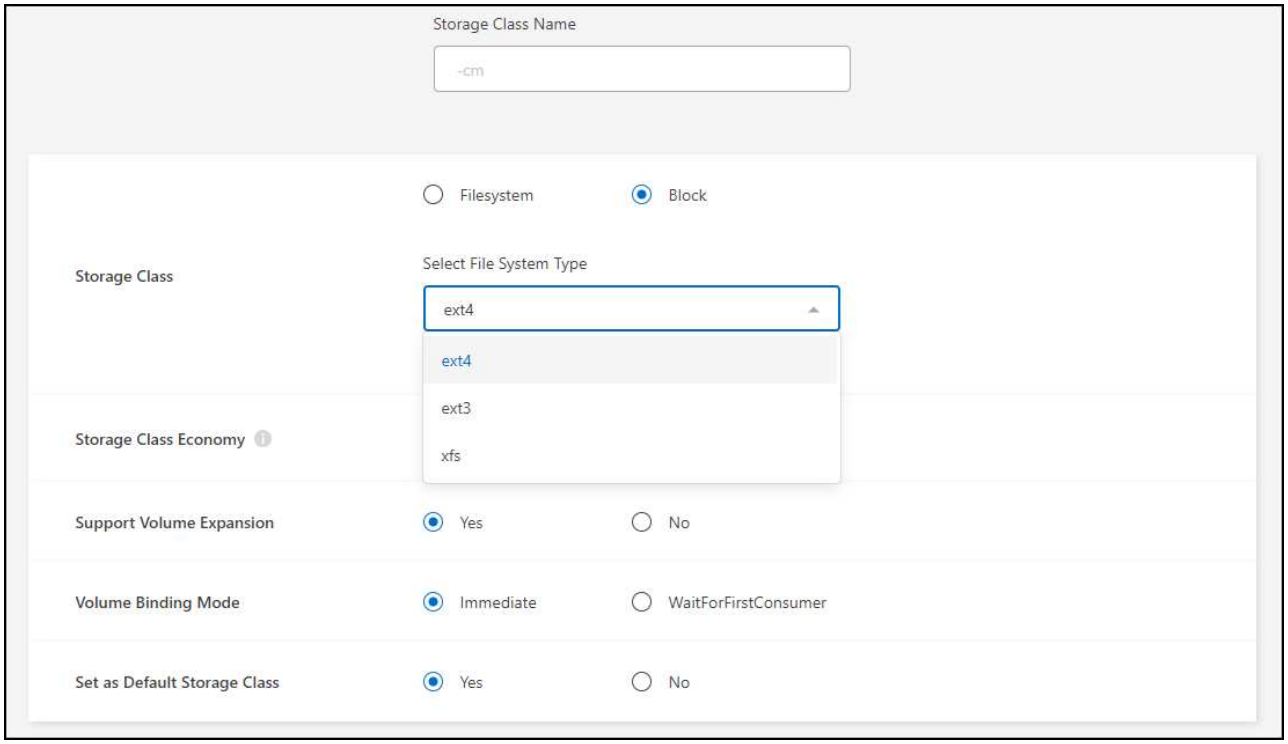
Nachdem Sie einen verwalteten Kubernetes-Cluster zu Canvas hinzugefügt haben, können Sie BlueXP zum Verwalten von Speicherklassen verwenden.

> 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.

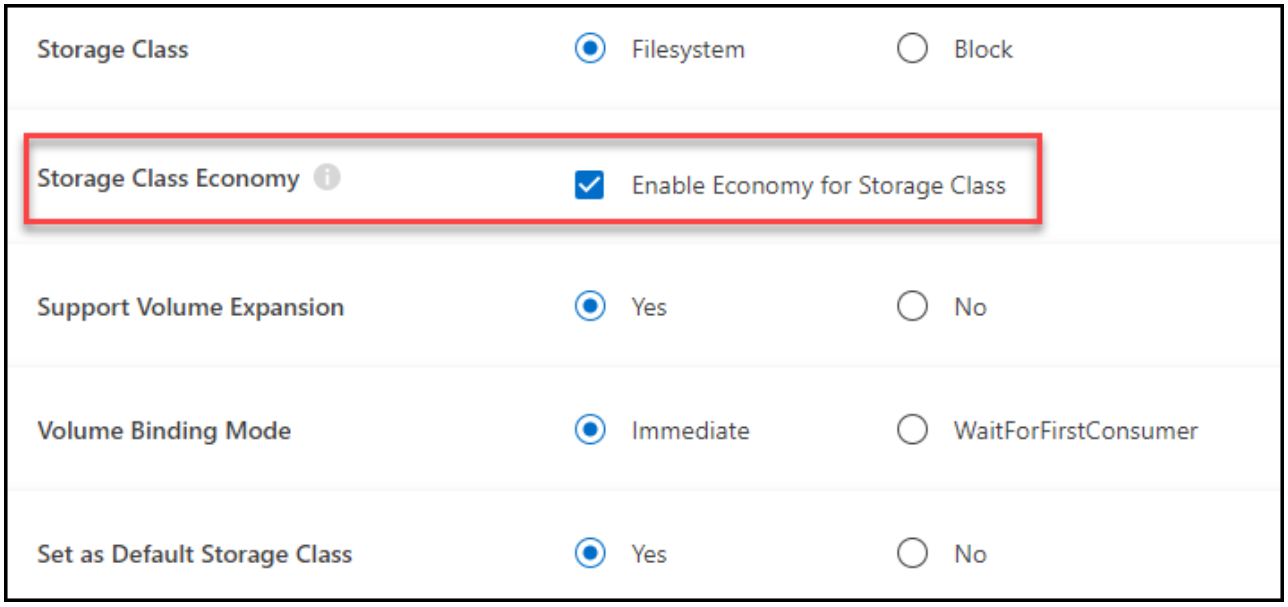
## Fügen Sie eine Storage-Klasse hinzu

**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.

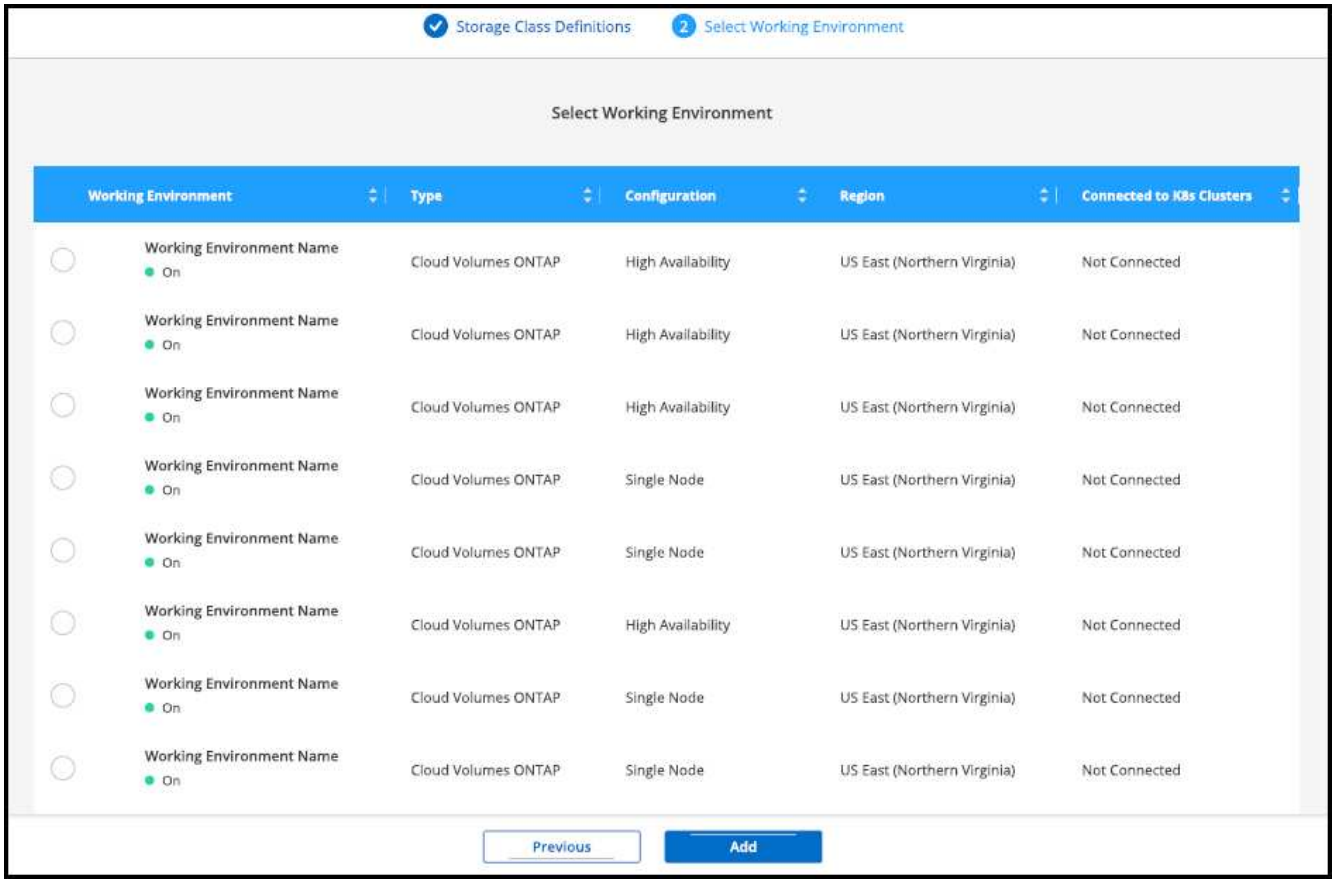



b. Für **Block** oder **Filesystem**-Speicher können Sie wählen, um die Wirtschaftlichkeit der Storage-Klasse zu ermöglichen.



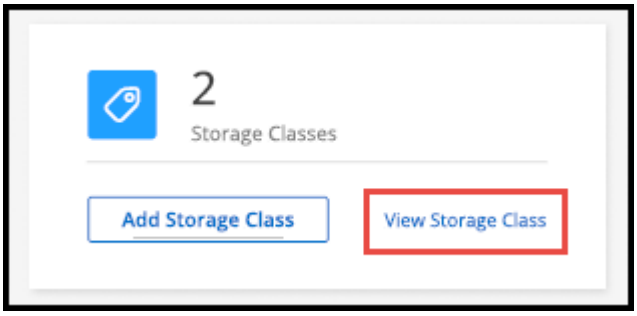

Backup und Restore werden in wirtschaftlicher Nutzung von Storage-Klasse nicht unterstützt.

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**.




**Ergebnisse**

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



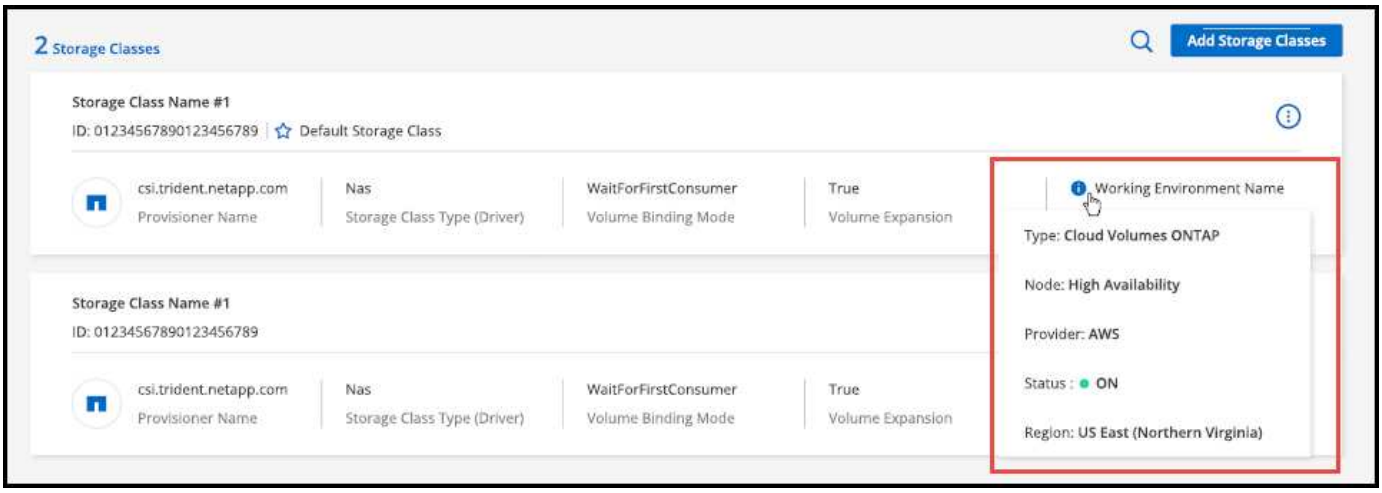

## Details zur Arbeitsumgebung anzeigen

**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.

**Ergebnisse**

Das Fenster Details zur Arbeitsumgebung wird geöffnet.



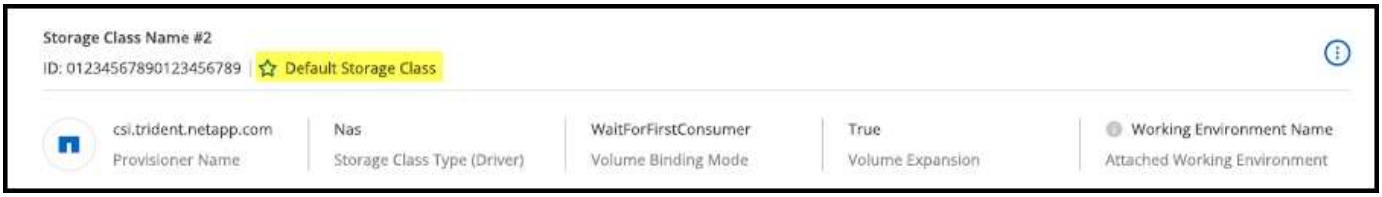

## Legen Sie die Standard-Storage-Klasse fest

### 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**.


### Ergebnisse

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.


**Ergebnisse**

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.

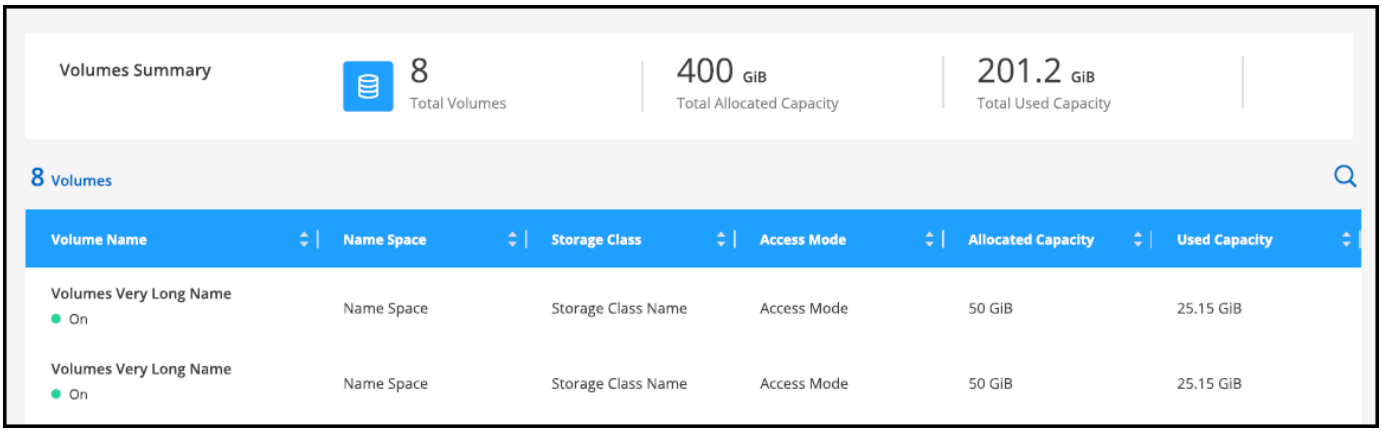
> BlueXP überwacht den Kubernetes-Cluster auf Änderungen am Backend und aktualisiert die persistente Volume-Tabelle, wenn neue Volumes hinzugefügt werden. Wenn auf dem Cluster ein automatisches Backup konfiguriert wurde, wird das Backup auf den neuen persistenten Volumes automatisch aktiviert.

**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.

**Ergebnisse**

Eine Tabelle der konfigurierten persistenten Volumes wird angezeigt.

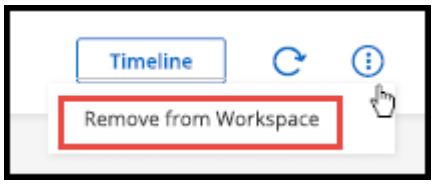



# Entfernen Sie Kubernetes Cluster aus dem Workspace

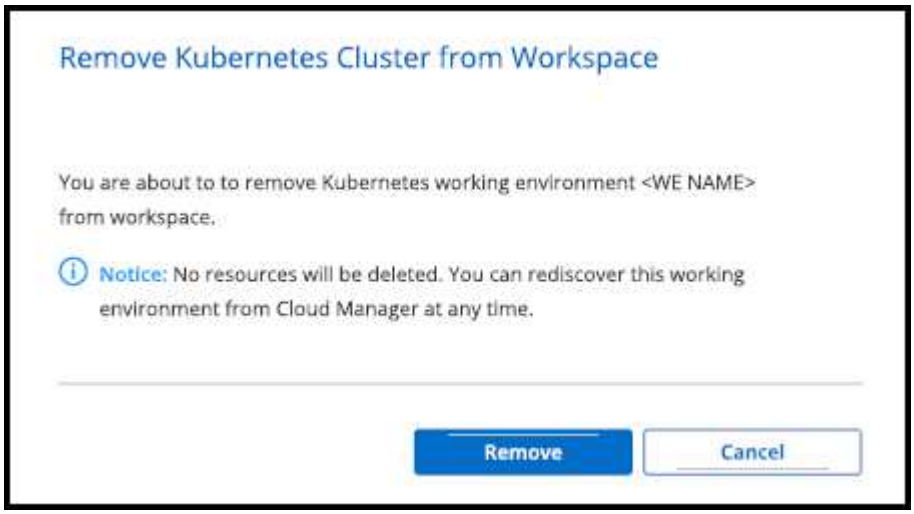
Nachdem Sie einen verwalteten Kubernetes-Cluster zum Canvas hinzugefügt haben, können Sie mit BlueXP Cluster aus dem Arbeitsbereich entfernen.

### 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.




### Ergebnisse

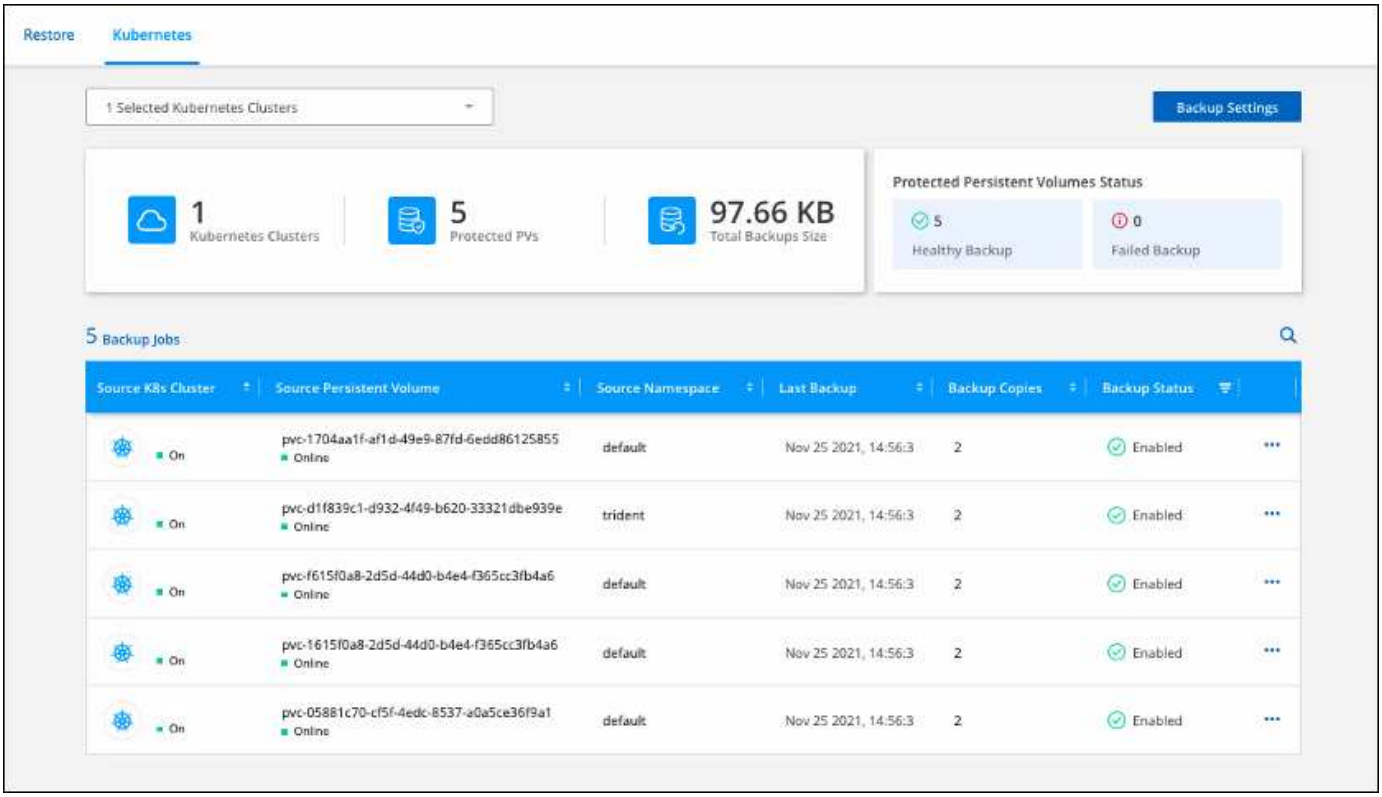
Der Kubernetes-Cluster wird aus dem Workspace entfernt und ist nicht mehr auf dem Canvas sichtbar.

# 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.

Mit BlueXP Backup und Recovery können Sie persistente Volumes in Objektspeicher sichern.

"Erfahren Sie, wie Sie Ihre Kubernetes-Cluster-Daten mit BlueXP Backup und Recovery schützen".



# Wissen und Support

## Für den Support anmelden

Für den Support von BlueXP und seinen Storage-Lösungen und Services ist eine Support-Registrierung erforderlich. Um wichtige Workflows für Cloud Volumes ONTAP Systeme zu ermöglichen, ist außerdem eine Support-Registrierung erforderlich.

Durch die Registrierung für den Support wird die NetApp-Unterstützung für einen Fileservice eines Cloud-Providers nicht aktiviert. Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

### 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. Die Registrierung ist abgeschlossen, indem wie unten beschrieben Konten der NetApp Support Website (NSS) zu BlueXP hinzugefügt werden.

### Registrieren Sie Ihr BlueXP Konto für NetApp Support

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer in Ihrem BlueXP Konto ein NetApp Support Site Konto mit seinen BlueXP Anmeldedaten verknüpfen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

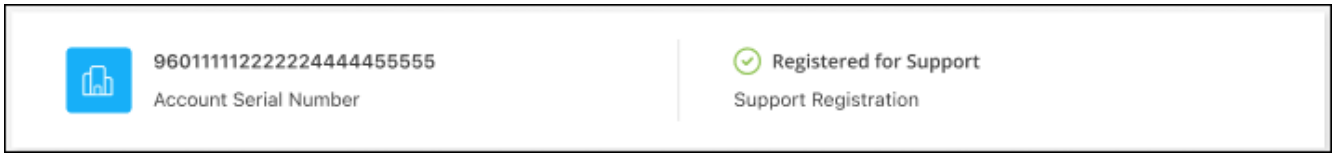
#### Bestandskunde mit NSS-Konto

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 auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Eingabeaufforderung für die NetApp-Support-Website (NSS)-Authentifizierung.
4. Um zu bestätigen, dass die Registrierung erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konto für Support registriert ist.

   Beachten Sie, dass andere BlueXP Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie ihrem BlueXP Login kein NetApp Support Site Konto zugeordnet haben. Das bedeutet jedoch nicht, dass Ihr BlueXP Konto nicht für den Support registriert ist. Solange ein Benutzer im Konto diese Schritte befolgt hat, wurde Ihr Konto registriert.

### Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über vorhandene Lizenzen und Seriennummern sowie *No* NSS Konto verfügen, müssen Sie ein NSS Konto erstellen und es Ihren BlueXP Anmeldedaten zuordnen.

#### Schritte

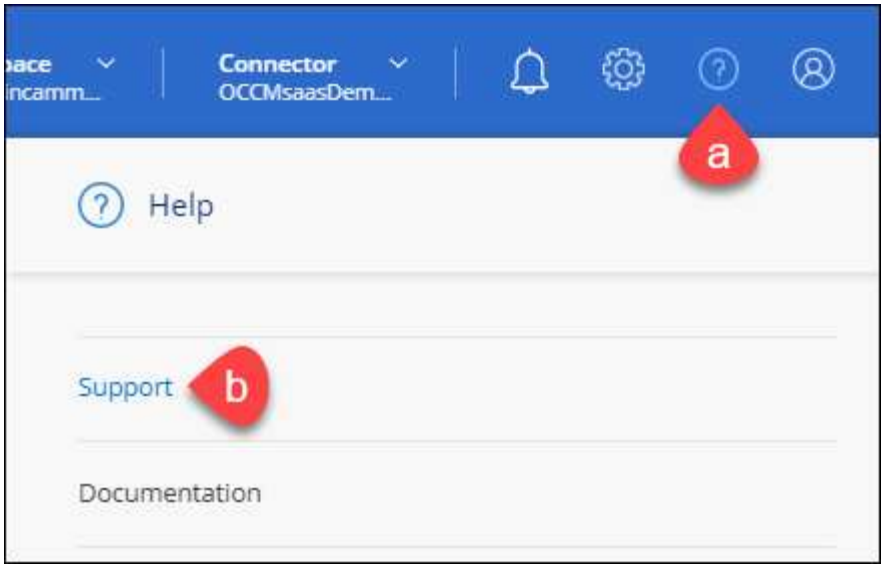
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.
2. Ordnen Sie Ihr neues NSS-Konto Ihrer BlueXP Anmeldung zu, indem Sie die unter aufgeführten Schritte durchführen Bestandskunde mit NSS-Konto.

### Neu bei NetApp

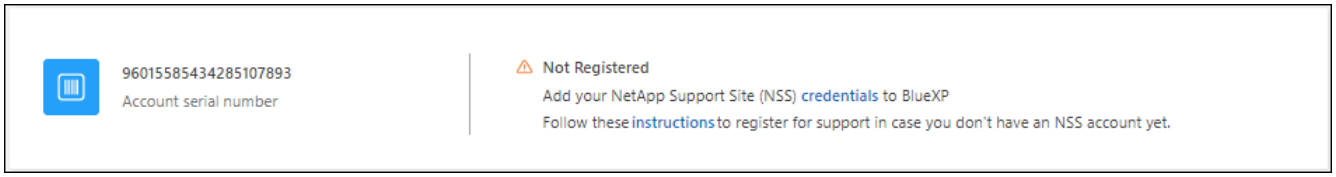
Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

#### Schritte

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




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.

**Nachdem Sie fertig sind**

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

Wenn Sie über Ihren NetApp Support Site Account verfügen, ordnen Sie das Konto Ihrer BlueXP Anmeldung zu, indem Sie die Schritte unter ausführen Bestandskunde mit NSS-Konto.

## Verknüpfen von NSS-Anmeldeinformationen für den Cloud Volumes ONTAP-Support

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu ermöglichen, müssen die Zugangsdaten für die NetApp Support Website mit Ihrem BlueXP Konto verknüpft werden:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für Support

  Die Bereitstellung Ihres NSS Kontos ist erforderlich, um Support für Ihr System zu aktivieren und Zugang zu den technischen Support-Ressourcen von NetApp zu erhalten.

- Implementierung von Cloud Volumes ONTAP unter Verwendung von BYOL (Bring-Your-Own-License)

  Die Bereitstellung Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für den von Ihnen erworbenen Zeitraum aktivieren kann. Dies schließt automatische Updates für Vertragsverlängerungen ein.

- Aktualisieren der Cloud Volumes ONTAP Software auf die neueste Version

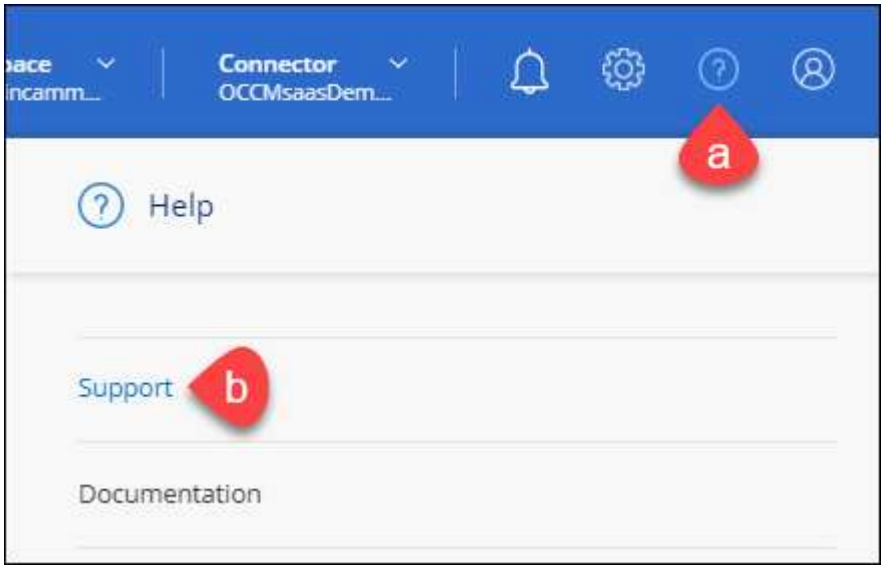
Das Zuordnen der NSS-Anmeldedaten zu Ihrem BlueXP Konto unterscheidet sich von dem NSS-Konto, das mit einer BlueXP Benutzeranmeldung verknüpft ist.

Diese NSS-Zugangsdaten sind mit Ihrer spezifischen BlueXP Konto-ID verknüpft. Benutzer, die zum BlueXP Konto gehören, können über **Support > NSS Management** auf diese Anmeldedaten zugreifen.

- 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 auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite umgeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices, die speziell auf Support und Lizenzierung zugeschnitten sind.

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 NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder Temporärkonto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto vorhanden sein, wenn es sich bei diesem Konto um ein Partner-Level-Konto handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da es bereits NSS-Benutzer unterschiedlichen Typs gibt.“

   Dasselbe gilt, wenn Sie bereits NSS-Konten auf Kundenebene haben und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet ist. 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. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird gesendet, um Sie darüber zu informieren.

# 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.

## Unterstützung für Fileservices von Cloud-Providern

Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

Wenn Sie technischen Support für BlueXP und seine Storage-Lösungen und -Services erhalten möchten, nutzen Sie die unten beschriebenen Support-Optionen.

## Nutzen Sie Self-Support-Optionen

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

- Dokumentation

  Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- "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.

## Erstellen Sie einen Fall mit dem 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.

#### Bevor Sie beginnen

- Um die Funktion **Fall erstellen** nutzen zu können, müssen Sie zunächst Ihre Anmeldedaten für die NetApp Support-Website mit Ihren BlueXP Anmeldedaten verknüpfen. "Managen Sie Zugangsdaten für Ihre BlueXP Anmeldung".
- Wenn Sie einen Fall für ein ONTAP System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer des Systems verknüpft sein.

#### Schritte

1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie auf der Seite **Ressourcen** eine der verfügbaren Optionen unter Technischer Support:

   a. Wählen Sie **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. Wählen Sie **Fall erstellen**, um ein Ticket mit einem NetApp-Supportspezialisten zu öffnen:

      - **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.

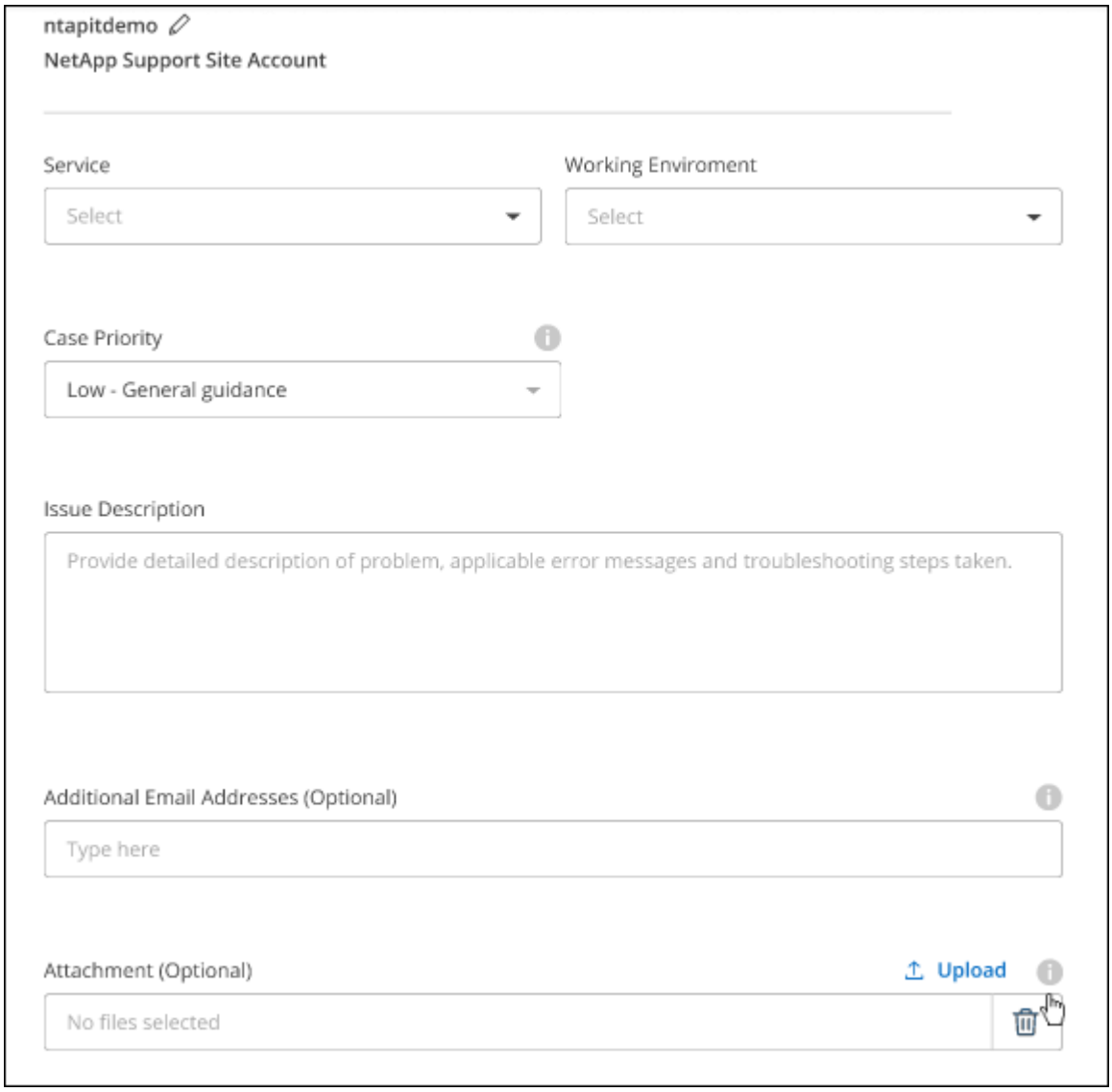
        Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **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.
- **Anhang (optional)**: Laden Sie bis zu fünf Anhänge nacheinander hoch.

  Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.




**Nachdem Sie fertig sind**

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

Um eine Historie deiner Support-Fälle anzuzeigen, kannst du **Einstellungen > Chronik** auswählen 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 Hilfe mit einer der folgenden Optionen anfordern:

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

## Managen Ihrer Support-Cases (Vorschau)

Sie können aktive und gelöste Support-Cases direkt über BlueXP anzeigen und managen. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Fälle verwalten.

Case Management ist als Vorschau verfügbar. Wir planen, diese Erfahrungen weiter zu verbessern und in zukünftigen Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Ihr Feedback über den Product-Chat.

Beachten Sie Folgendes:

- Das Case-Management-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der Fälle, die in den letzten 3 Monaten durch das von Ihnen angegebene NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto an.

  Die Ergebnisse in der Tabelle geben die Fälle in Bezug auf die ausgewählte Ansicht wieder.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten nur Sortierfunktionen.

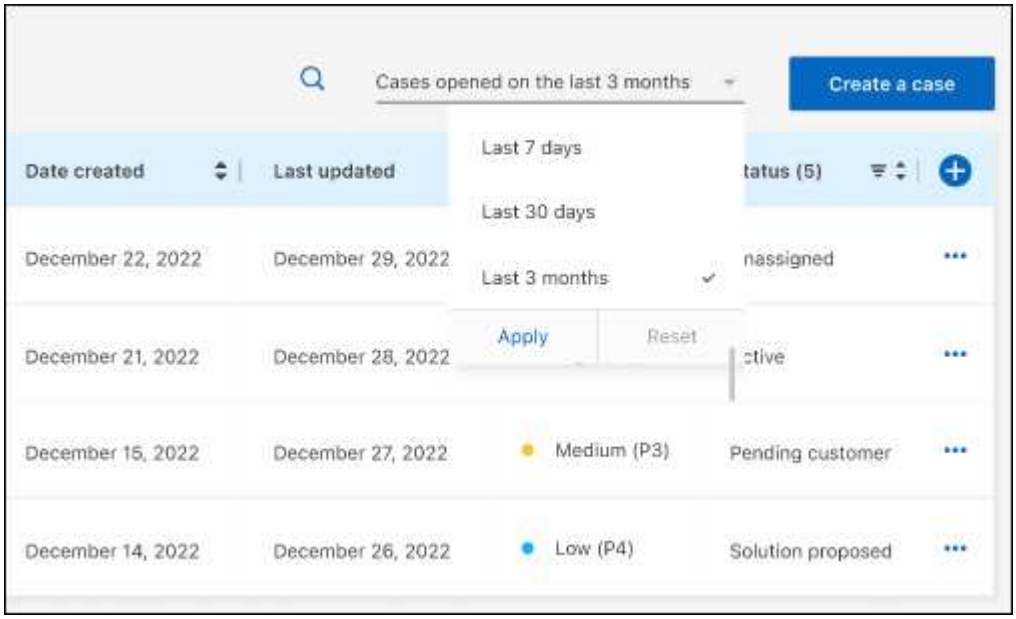
  Weitere Informationen erhalten Sie in den Schritten unten.
- Auf Fallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Geschlossen“ oder „Geschlossen“ befindet.

**Schritte**

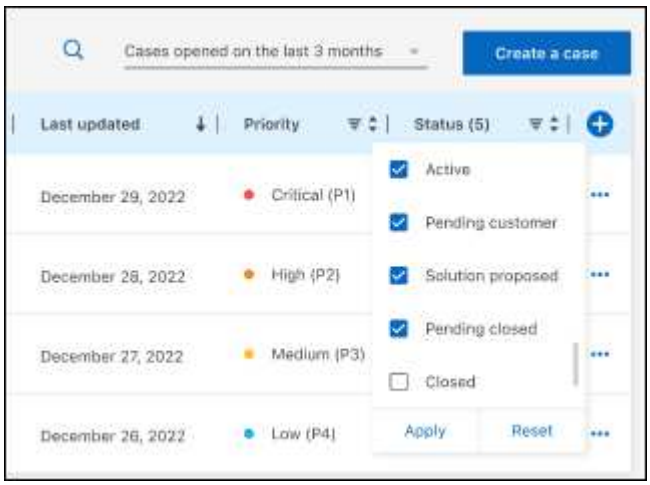
1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie **Case Management** aus und fügen Sie bei Aufforderung Ihr NSS-Konto zu BlueXP hinzu.

   Auf der Seite **Case Management** werden offene Fälle im Zusammenhang mit dem NSS-Konto angezeigt, das mit Ihrem BlueXP Benutzerkonto verknüpft ist. Dies ist das gleiche NSS-Konto, das oben auf der Seite **NSS Management** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:

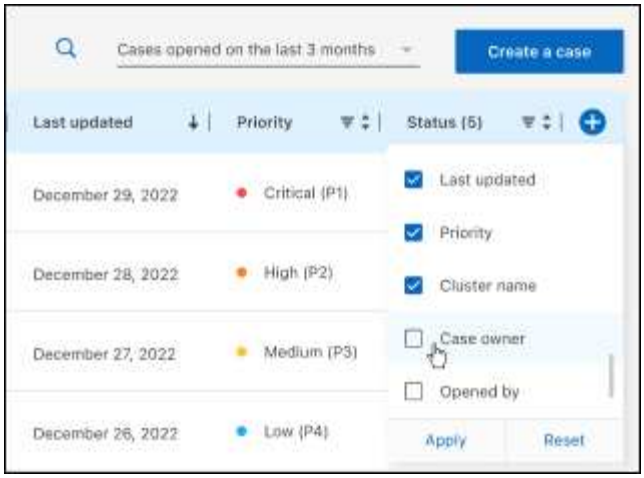
- Wählen Sie unter **Vorgänge der Organisation Ansicht** aus, um alle mit Ihrem Unternehmen verbundenen Fälle anzuzeigen.
- Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.




- Filtern Sie den Inhalt der Spalten.




- Ändern Sie die Spalten, die in der Tabelle angezeigt werden, indem Sie auswählen Und wählen Sie dann die Spalten, die Sie anzeigen möchten.

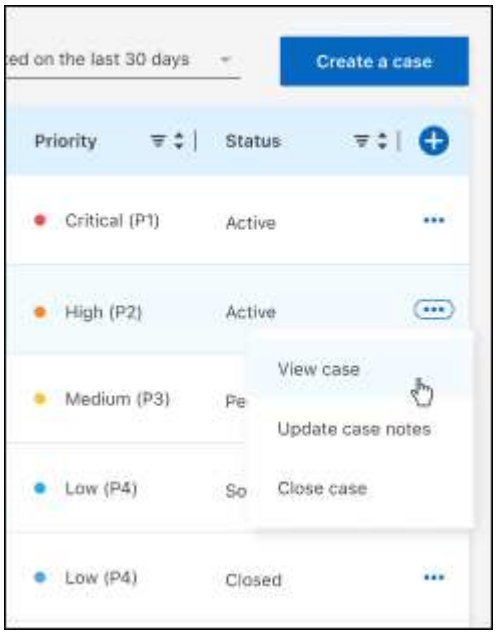



4. Managen Sie einen bestehenden Fall, indem Sie auswählen ••• Und eine der verfügbaren Optionen auswählen:

   - **Fall anzeigen**: Vollständige Details zu einem bestimmten Fall anzeigen.
   - **Aktennotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um maximal fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

   - **Fall schließen**: Geben Sie Einzelheiten darüber an, warum Sie den Fall schließen und wählen Sie **Fall schließen**.



# Rechtliche Hinweise

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

## Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

## 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.

"https://www.netapp.com/company/legal/trademarks/"

## Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

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

## Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

## Open Source

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

"Hinweis für BlueXP"