



# **Documentazione sui cluster Kubernetes**

## Kubernetes clusters

NetApp  
April 16, 2024

This PDF was generated from <https://docs.netapp.com/it-it/bluexp-kubernetes/index.html> on April 16, 2024. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Sommario

Documentazione sui cluster Kubernetes	1
Novità di Kubernetes in BlueXP	2
02 aprile 2023	2
05 marzo 2023	2
06 novembre 2022	2
18 settembre 2022	2
31 luglio 2022	2
3 luglio 2022	2
6 giugno 2022	3
4 maggio 2022	3
4 aprile 2022	3
27 febbraio 2022	3
11 gennaio 2022	3
28 novembre 2021	4
Inizia subito	5
La gestione dei dati di Kubernetes in BlueXP	5
Inizia a utilizzare i cluster Kubernetes	6
Requisiti	7
Requisiti per i cluster Kubernetes in AWS	7
Requisiti per i cluster Kubernetes in Azure	16
Requisiti per i cluster Kubernetes in Google Cloud	24
Requisiti per i cluster Kubernetes in OpenShift	31
Aggiungere cluster Kubernetes	40
Aggiungere un cluster Amazon Kubernetes a BlueXP	40
Aggiungere un cluster Azure Kubernetes a BlueXP	42
Aggiungere un cluster Google Cloud Kubernetes a BlueXP	45
Importare un cluster OpenShift in BlueXP	49
Gestire i cluster Kubernetes	51
Gestire Astra Trident	51
Gestire le classi di storage	53
Visualizzare volumi persistenti	56
Rimuovere i cluster Kubernetes dallo spazio di lavoro	57
Utilizza i servizi dati cloud di NetApp con i cluster Kubernetes	58
Conoscenza e supporto	60
Registrati per ricevere assistenza	60
Richiedi assistenza	64
Note legali	70
Copyright	70
Marchi	70
Brevetti	70
Direttiva sulla privacy	70
Open source	70

# Documentazione sui cluster Kubernetes

# Novità di Kubernetes in BlueXP

Scopri le novità di Kubernetes in BlueXP.

## 02 aprile 2023

- Ora puoi farlo ["Disinstallare Astra Trident"](#) Che è stato installato utilizzando l'operatore Trident o BlueXP.
- Sono stati apportati miglioramenti all'interfaccia utente e sono state aggiornate le schermate nella documentazione.

## 05 marzo 2023

- Kubernetes in BlueXP supporta ora Astra Trident 23.01.
- Sono stati apportati miglioramenti all'interfaccia utente e sono state aggiornate le schermate nella documentazione.

## 06 novembre 2022

Quando ["definizione delle classi di storage"](#), è ora possibile abilitare lo storage economy di classe storage per lo storage a blocchi o su file system.

## 18 settembre 2022

Ora puoi importare cluster OpenShift autogestiti in Cloud Manager.

- ["Requisiti per i cluster Kubernetes in OpenShift"](#)
- ["Importare un cluster OpenShift in Cloud Manager"](#)

## 31 luglio 2022

- Utilizzando il nuovo `watch` Nella classe di storage e nelle configurazioni YAML di backup e ripristino, Cloud Manager può ora monitorare i cluster Kubernetes per le modifiche apportate al backend del cluster e abilitare automaticamente il backup per nuovi volumi persistenti se è stato configurato il backup automatico sul cluster.

["Requisiti per i cluster Kubernetes in AWS"](#)

["Requisiti per i cluster Kubernetes in Azure"](#)

["Requisiti per i cluster Kubernetes in Google Cloud"](#)

- Quando ["definizione delle classi di storage"](#), è ora possibile specificare un tipo di file system (fstype) per lo storage a blocchi.

## 3 luglio 2022

- Se Astra Trident è stato implementato utilizzando l'operatore Trident, è ora possibile eseguire l'aggiornamento alla versione più recente di Astra Trident utilizzando Cloud Manager.

["Installare e gestire Astra Trident"](#)

- È ora possibile trascinare il cluster Kubernetes e rilasciarlo nell'ambiente di lavoro AWS FSX per ONTAP per aggiungere una classe di storage direttamente da Canvas.

["Aggiungere classe di storage"](#)

## 6 giugno 2022

Cloud Manager ora supporta Amazon FSX per ONTAP come storage back-end.

## 4 maggio 2022

### Trascinare e rilasciare per aggiungere la classe di storage

È ora possibile trascinare il cluster Kubernetes e rilasciarlo nell'ambiente di lavoro Cloud Volumes ONTAP per aggiungere una classe di storage direttamente da Canvas.

["Aggiungere classe di storage"](#)

## 4 aprile 2022

### Gestire i cluster Kubernetes utilizzando la pagina delle risorse di Cloud Manager

Kubernetes Cluster Management ha ora migliorato l'integrazione direttamente dall'ambiente di lavoro del cluster. Un nuovo ["Avvio rapido"](#) ti consente di iniziare a lavorare rapidamente.

È ora possibile eseguire le seguenti operazioni dalla pagina delle risorse del cluster.

- ["Installare Astra Trident"](#)
- ["Aggiungere classi di storage"](#)
- ["Visualizzare volumi persistenti"](#)
- ["Rimuovere i cluster"](#)
- ["Abilitare i servizi dati"](#)

## 27 febbraio 2022

### Supporto per i cluster Kubernetes in Google Cloud

Ora puoi aggiungere e gestire cluster gestiti di Google Kubernetes Engine (GKE) e cluster di Kubernetes autogestiti in Google Cloud utilizzando Cloud Manager.

["Scopri come iniziare a utilizzare i cluster Kubernetes in Google Cloud"](#).

## 11 gennaio 2022

## Supporto per i cluster Kubernetes in Azure

Ora puoi aggiungere e gestire cluster di Azure Kubernetes gestiti (AKS) e cluster di Kubernetes autogestiti in Azure utilizzando Cloud Manager.

["Introduzione ai cluster Kubernetes in Azure"](#)

## 28 novembre 2021

## Supporto per i cluster Kubernetes in AWS

Ora puoi aggiungere i cluster Kubernetes gestiti a Canvas di Cloud Manager per una gestione avanzata dei dati.

- Scopri i cluster Amazon EKS
- Eseguire il backup dei volumi persistenti utilizzando Cloud Backup

["Scopri di più sul supporto di Kubernetes"](#).



Il servizio Kubernetes esistente (disponibile tramite la scheda **K8s**) è stato obsoleto e verrà rimosso in una release futura.

# Inizia subito

## La gestione dei dati di Kubernetes in BlueXP

Astra Trident è un progetto open source completamente supportato gestito da NetApp. Astra Trident si integra in modo nativo con Kubernetes e il suo framework per volumi persistenti per eseguire il provisioning e la gestione dei volumi da sistemi che eseguono qualsiasi combinazione di piattaforme storage NetApp. ["Scopri di più su Trident"](#).

### Caratteristiche

Utilizzo di ["BlueXP"](#) Inoltre, una versione compatibile di Astra Trident implementata utilizzando l'operatore Trident, è possibile:

- Aggiungere e gestire i cluster Kubernetes
- ["Installare, aggiornare o disinstallare Astra Trident"](#)
- ["Aggiungere e rimuovere classi di storage"](#)
- ["Visualizzare volumi persistenti"](#)
- ["Rimuovere i cluster Kubernetes"](#) dallo spazio di lavoro
- ["Attivare o visualizzare il backup e ripristino BlueXP"](#)

### Implementazioni Kubernetes supportate

BlueXP supporta cluster Kubernetes gestiti in esecuzione in:

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

### Implementazioni di Astra Trident supportate

Una delle quattro versioni più recenti di Astra Trident ["Implementato utilizzando l'operatore Trident"](#) è obbligatorio.



Astra Trident implementato con `tridentctl` non è supportato. Se hai implementato Astra Trident con `tridentctl`, Non è possibile utilizzare BlueXP per gestire i cluster Kubernetes. È necessario e reinstallarla ["Utilizzando l'operatore Trident"](#) oppure ["Utilizzando BlueXP"](#).

Puoi installare Astra Trident o effettuare l'aggiornamento a una versione supportata direttamente da BlueXP.

["Esaminare i prerequisiti di Astra Trident"](#)

### Storage back-end supportato

NetApp Astra Trident deve essere installato su ogni cluster Kubernetes e Cloud Volumes ONTAP o Amazon FSX per ONTAP deve essere configurato come storage back-end per i cluster.

## Costo

Non sono previsti costi per *scoprire* i cluster Kubernetes in BlueXP, ma verrà addebitato il costo del backup dei volumi persistenti utilizzando Cloud Backup Service.

## Inizia a utilizzare i cluster Kubernetes

Utilizzo di **"BlueXP"** Puoi iniziare a gestire i cluster Kubernetes in pochi passaggi.

1

### Esaminare i prerequisiti

Assicurarsi che l'ambiente soddisfi i prerequisiti per il tipo di cluster in uso.

["Requisiti per i cluster Kubernetes in AWS"](#)

["Requisiti per i cluster Kubernetes in Azure"](#)

["Requisiti per i cluster Kubernetes in Google Cloud"](#)

2

### Aggiungi i tuoi cluster Kubernetes a BlueXP

È possibile aggiungere cluster Kubernetes e connetterli a un ambiente di lavoro utilizzando BlueXP.

["Aggiungi un cluster Amazon Kubernetes"](#)

["Aggiungere un cluster Azure Kubernetes"](#)

["Aggiungi un cluster Google Cloud Kubernetes"](#)

3

### Avviare il provisioning dei volumi persistenti

Richiedere e gestire volumi persistenti utilizzando interfacce e costrutti Kubernetes nativi. BlueXP crea classi di storage NFS e iSCSI che è possibile utilizzare per il provisioning di volumi persistenti.

["Scopri di più sul provisioning del tuo primo volume con Astra Trident"](#).

4

### Gestisci i cluster con BlueXP

Dopo aver aggiunto i cluster Kubernetes a BlueXP, è possibile gestire i cluster dalla pagina delle risorse di BlueXP.

["Scopri come gestire i cluster Kubernetes."](#)



# Requisiti

## Requisiti per i cluster Kubernetes in AWS

Puoi aggiungere cluster Amazon Elastic Kubernetes Service (EKS) gestiti o cluster Kubernetes autogestiti su AWS a BlueXP. Prima di aggiungere i cluster a BlueXP, è necessario assicurarsi che siano soddisfatti i seguenti requisiti.



Questo argomento utilizza *Kubernetes cluster* dove la configurazione è la stessa per i cluster EKS e Kubernetes autogestiti. Viene specificato il tipo di cluster in cui la configurazione differisce.

### Requisiti

#### Astra Trident

È necessaria una delle quattro versioni più recenti di Astra Trident. Puoi installare o aggiornare Astra Trident direttamente da BlueXP. Dovresti ["esaminare i prerequisiti"](#) Prima di installare Astra Trident.

#### Cloud Volumes ONTAP

Cloud Volumes ONTAP per AWS deve essere configurato come storage back-end per il cluster. ["Consultare i documenti di Astra Trident per la procedura di configurazione"](#).

#### Connettore BlueXP

Un connettore deve essere in esecuzione in AWS con le autorizzazioni richieste. [Scopri di più di seguito](#).

#### Connettività di rete

È necessaria la connettività di rete tra il cluster Kubernetes e il connettore e tra il cluster Kubernetes e Cloud Volumes ONTAP. [Scopri di più di seguito](#).

#### Autorizzazione RBAC

Il ruolo BlueXP Connector deve essere autorizzato su ciascun cluster Kubernetes. [Scopri di più di seguito](#).

## Preparare un connettore

In AWS è necessario un connettore BlueXP per rilevare e gestire i cluster Kubernetes. Sarà necessario creare un nuovo connettore o utilizzare un connettore esistente con le autorizzazioni richieste.

### Creare un nuovo connettore

Seguire la procedura descritta in uno dei collegamenti riportati di seguito.

- ["Creare un connettore da BlueXP"](#) (consigliato)
- ["Creare un connettore da AWS Marketplace"](#)
- ["Installare il connettore su un host Linux esistente in AWS"](#)

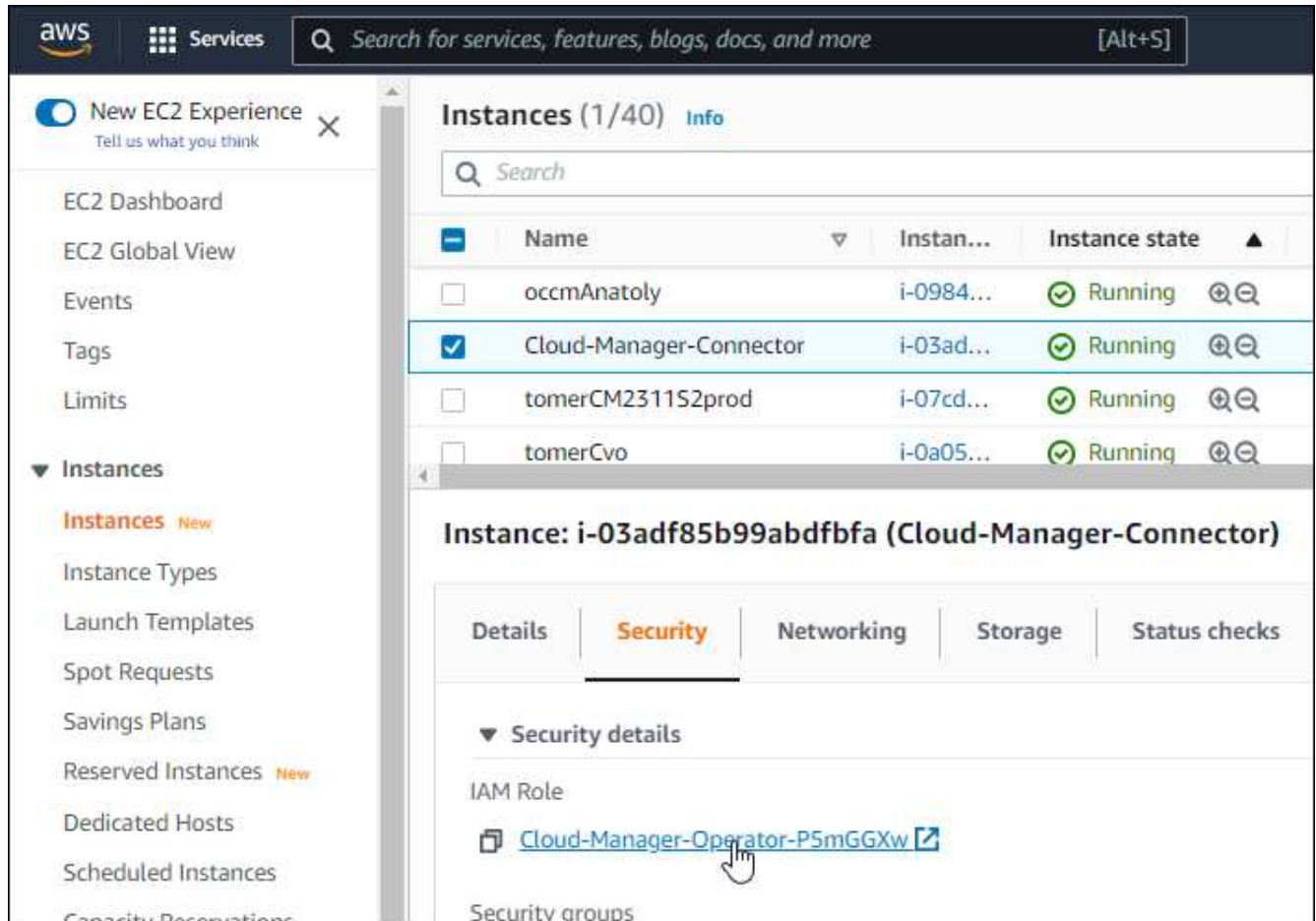
### Aggiungere le autorizzazioni richieste a un connettore esistente

A partire dalla release 3.9.13, tutti i \_connettori appena creati includono tre nuove autorizzazioni AWS che consentono il rilevamento e la gestione dei cluster Kubernetes. Se è stato creato un connettore prima di

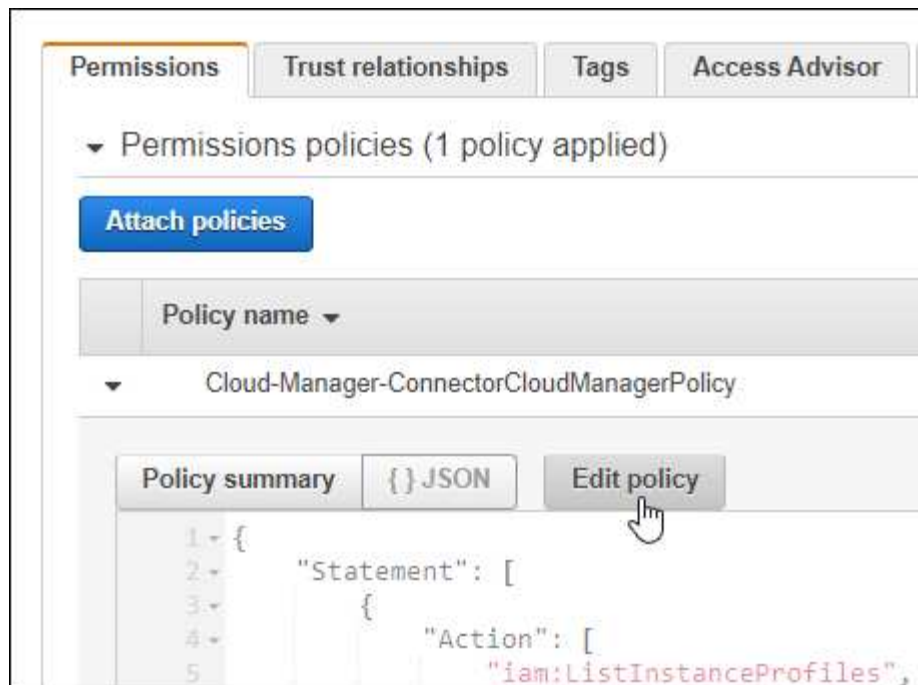
questa release, sarà necessario modificare il criterio esistente per il ruolo IAM del connettore per fornire le autorizzazioni.

## Fasi

1. Accedere alla console AWS e aprire il servizio EC2.
2. Selezionare l'istanza del connettore, fare clic su **Security** e fare clic sul nome del ruolo IAM per visualizzare il ruolo nel servizio IAM.



3. Nella scheda **Permissions**, espandere il criterio e fare clic su **Edit policy**.



4. Fare clic su **JSON** e aggiungere le seguenti autorizzazioni nella prima serie di azioni:

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

["Visualizza il formato JSON completo per la policy"](#)

5. Fare clic su **Review policy** (esamina policy), quindi su **Save changes** (Salva modifiche).

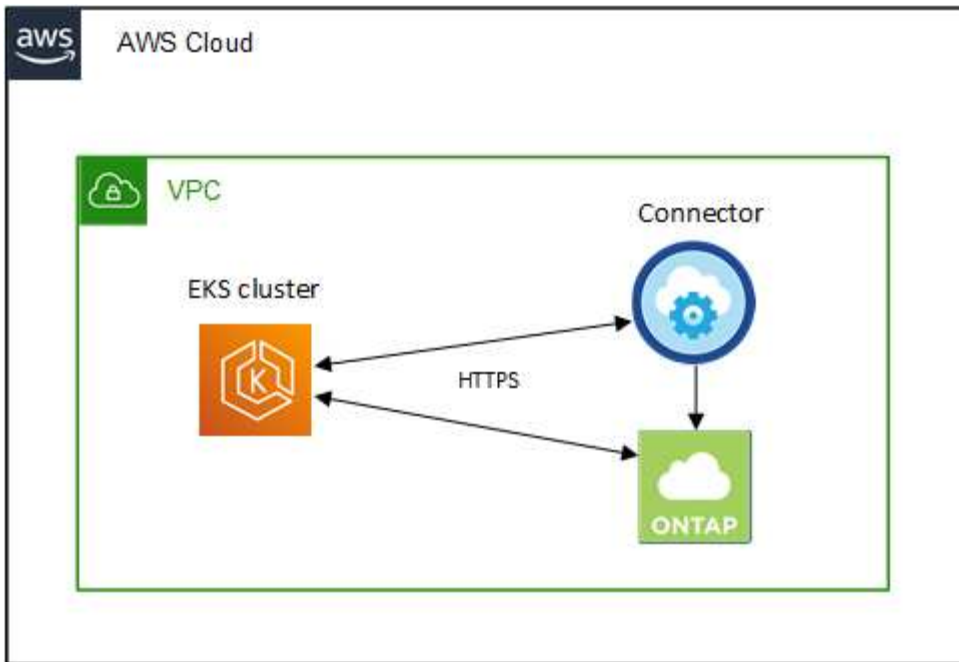
## Esaminare i requisiti di rete

È necessario fornire la connettività di rete tra il cluster Kubernetes e il connettore e tra il cluster Kubernetes e il sistema Cloud Volumes ONTAP che fornisce lo storage back-end al cluster.

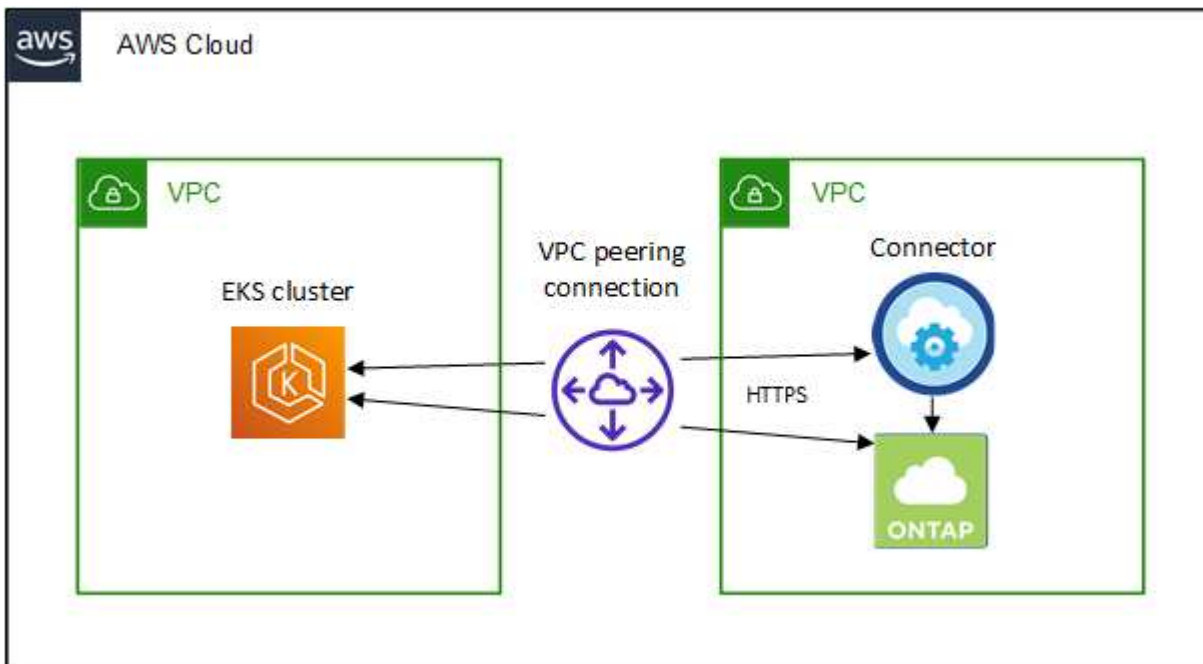
- Ogni cluster Kubernetes deve disporre di una connessione in entrata dal connettore
- Il connettore deve disporre di una connessione in uscita a ciascun cluster Kubernetes sulla porta 443

Il modo più semplice per fornire questa connettività consiste nell'implementare il connettore e Cloud Volumes ONTAP nello stesso VPC del cluster Kubernetes. In caso contrario, è necessario impostare una connessione di peering VPC tra i diversi VPC.

Ecco un esempio che mostra ogni componente dello stesso VPC.



Ecco un altro esempio che mostra un cluster EKS in esecuzione in un VPC diverso. In questo esempio, il peering VPC fornisce una connessione tra il VPC per il cluster EKS e il VPC per il connettore e Cloud Volumes ONTAP.



## Impostare l'autorizzazione RBAC

È necessario autorizzare il ruolo del connettore su ciascun cluster Kubernetes in modo che il connettore possa rilevare e gestire un cluster.

Per abilitare funzionalità diverse è necessaria un'autorizzazione diversa.

### Backup e ripristino

Il backup e il ripristino richiedono solo un'autorizzazione di base.

## Aggiungere classi di storage

È necessaria un'autorizzazione estesa per aggiungere classi di storage utilizzando BlueXP e monitorare il cluster per rilevare eventuali modifiche al backend.

## Installare Astra Trident

Devi fornire l'autorizzazione completa per BlueXP per installare Astra Trident.



Durante l'installazione di Astra Trident, BlueXP installa il backend Astra Trident e il segreto Kubernetes che contiene le credenziali che Astra Trident deve comunicare con il cluster di storage.

## Fasi

1. Creare un ruolo del cluster e un'associazione di ruoli.
  - a. Puoi personalizzare l'autorizzazione in base ai tuoi requisiti.

## Backup/ripristino

Aggiungere l'autorizzazione di base per abilitare il backup e il ripristino per i cluster Kubernetes.

```
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

```

### Classi di storage

Aggiunta di autorizzazioni estese per aggiungere classi di storage utilizzando BlueXP.

```

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

```

## Installazione di Trident



Utilizzare la riga di comando per fornire l'autorizzazione completa e abilitare BlueXP per installare Astra Trident.

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

b. Applicare la configurazione a un cluster.

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

2. Creare un mapping di identità per il gruppo di autorizzazioni.

### Utilizzare eksctl

Utilizzare eksctl per creare una mappatura delle identità IAM tra un cluster e il ruolo IAM per BlueXP Connector.

["Per istruzioni complete, consultare la documentazione eksctl"](#).

Di seguito viene fornito un esempio.

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

### Modifica aws-auth

Modificare direttamente aws-auth ConfigMap per aggiungere l'accesso RBAC al ruolo IAM per BlueXP Connector.

["Per istruzioni complete, consultare la documentazione di AWS EKS"](#).

Di seguito viene fornito un esempio.

```
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
```

## Requisiti per i cluster Kubernetes in Azure

È possibile aggiungere e gestire cluster Azure Kubernetes gestiti (AKS) e cluster Kubernetes autogestiti in Azure utilizzando BlueXP. Prima di aggiungere i cluster a BlueXP, assicurarsi che siano soddisfatti i seguenti requisiti.



Questo argomento utilizza *Kubernetes cluster* dove la configurazione è la stessa per i cluster AKS e Kubernetes autogestiti. Viene specificato il tipo di cluster in cui la configurazione differisce.

## Requisiti

### Astra Trident

È necessaria una delle quattro versioni più recenti di Astra Trident. Puoi installare o aggiornare Astra Trident direttamente da BlueXP. Dovresti ["esaminare i prerequisiti"](#) Prima di installare Astra Trident.

### Cloud Volumes ONTAP

Cloud Volumes ONTAP deve essere configurato come storage back-end per il cluster. ["Consultare i documenti di Astra Trident per la procedura di configurazione"](#).

### Connettore BlueXP

Un connettore deve essere in esecuzione in Azure con le autorizzazioni richieste. [Scopri di più di seguito](#).

### Connettività di rete

È necessaria la connettività di rete tra il cluster Kubernetes e il connettore e tra il cluster Kubernetes e Cloud Volumes ONTAP. [Scopri di più di seguito](#).

### Autorizzazione RBAC

BlueXP supporta cluster abilitati per RBAC con e senza Active Directory. Il ruolo BlueXP Connector deve essere autorizzato su ciascun cluster Azure. [Scopri di più di seguito](#).

## Preparare un connettore

Per rilevare e gestire i cluster Kubernetes, è necessario un connettore BlueXP in Azure. Sarà necessario creare un nuovo connettore o utilizzare un connettore esistente con le autorizzazioni richieste.

### Creare un nuovo connettore

Seguire la procedura descritta in uno dei collegamenti riportati di seguito.

- ["Creare un connettore da BlueXP"](#) (consigliato)
- ["Creare un connettore da Azure Marketplace"](#)
- ["Installare il connettore su un host Linux esistente"](#)

### Aggiungere le autorizzazioni richieste a un connettore esistente (per rilevare un cluster AKS gestito)

Se si desidera rilevare un cluster AKS gestito, potrebbe essere necessario modificare il ruolo personalizzato del connettore per fornire le autorizzazioni.

### Fasi

1. Identificare il ruolo assegnato alla macchina virtuale Connector:
  - a. Nel portale Azure, aprire il servizio macchine virtuali.
  - b. Selezionare la macchina virtuale Connector.
  - c. In Impostazioni, selezionare **identità**.
  - d. Fare clic su **assegnazioni dei ruoli Azure**.

- e. Prendere nota del ruolo personalizzato assegnato alla macchina virtuale del connettore.
2. Aggiornare il ruolo personalizzato:
- Nel portale Azure, apri il tuo abbonamento ad Azure.
  - Fare clic su **controllo di accesso (IAM) > ruoli**.
  - Fare clic sui puntini di sospensione (...) Per il ruolo personalizzato, quindi fare clic su **Modifica**.
  - Fare clic su JSON e aggiungere le seguenti autorizzazioni:

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

- e. Fare clic su **Review + update**, quindi su **Update**.

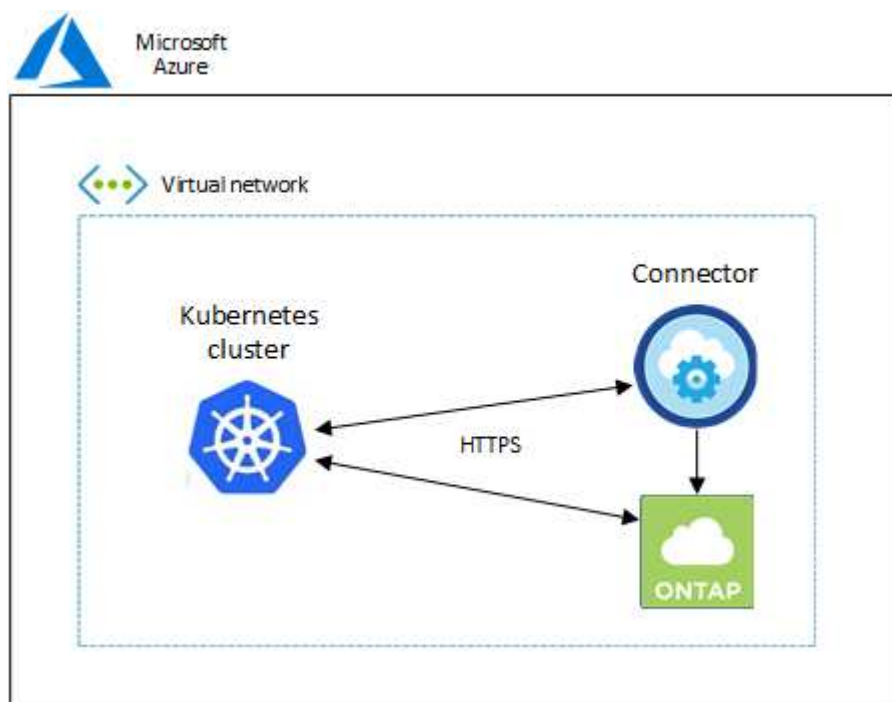
## Esaminare i requisiti di rete

È necessario fornire la connettività di rete tra il cluster Kubernetes e il connettore e tra il cluster Kubernetes e il sistema Cloud Volumes ONTAP che fornisce lo storage back-end al cluster.

- Ogni cluster Kubernetes deve disporre di una connessione in entrata dal connettore
- Il connettore deve disporre di una connessione in uscita a ciascun cluster Kubernetes sulla porta 443

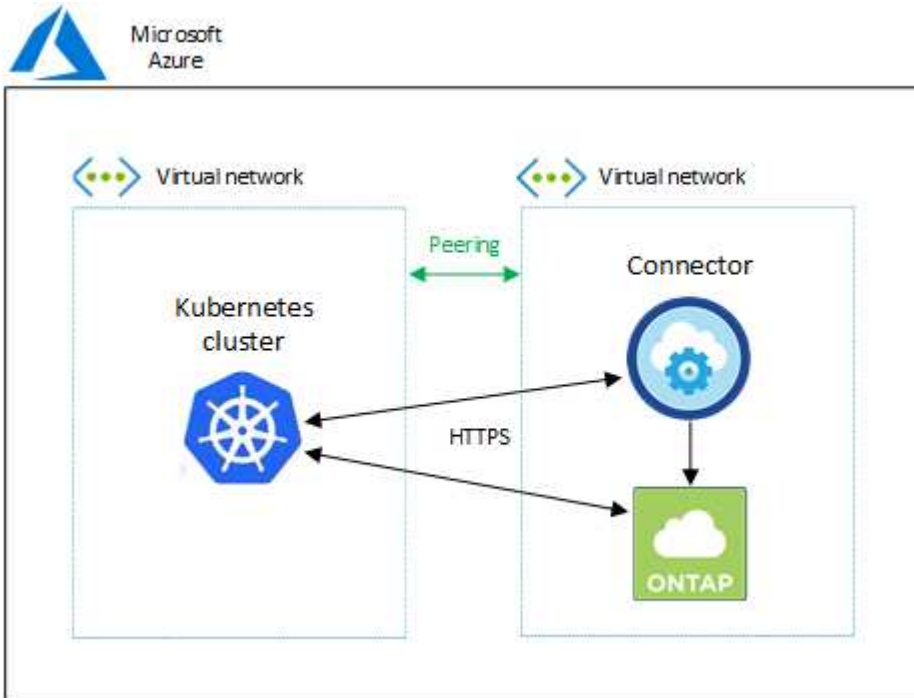
Il modo più semplice per fornire questa connettività consiste nell'implementare il connettore e Cloud Volumes ONTAP nello stesso VNET del cluster Kubernetes. In caso contrario, è necessario impostare una connessione peering tra i diversi VNet.

Di seguito viene riportato un esempio che mostra ciascun componente dello stesso VNET.



Ecco un altro esempio che mostra un cluster Kubernetes in esecuzione in un VNET diverso. In questo

esempio, il peering fornisce una connessione tra VNET per il cluster Kubernetes e VNET per il connettore e Cloud Volumes ONTAP.



## Impostare l'autorizzazione RBAC

La convalida RBAC viene eseguita solo sui cluster Kubernetes con Active Directory (ad) attivato. I cluster Kubernetes senza ad passeranno automaticamente la convalida.

È necessario autorizzare il ruolo del connettore su ciascun cluster Kubernetes in modo che il connettore possa rilevare e gestire un cluster.

### Backup e ripristino

Il backup e il ripristino richiedono solo un'autorizzazione di base.

### Aggiungere classi di storage

È necessaria un'autorizzazione estesa per aggiungere classi di storage utilizzando BlueXP e monitorare il cluster per rilevare eventuali modifiche al backend.

### Installare Astra Trident

Devi fornire l'autorizzazione completa per BlueXP per installare Astra Trident.



Durante l'installazione di Astra Trident, BlueXP installa il backend Astra Trident e il segreto Kubernetes che contiene le credenziali che Astra Trident deve comunicare con il cluster di storage.

### Prima di iniziare

RBAC subjects: name: La configurazione varia leggermente in base al tipo di cluster Kubernetes.

- Se si sta implementando un cluster \* AKS gestito, è necessario l'ID dell'oggetto per l'identità gestita assegnata dal sistema per il connettore. Questo ID è disponibile nel portale di gestione di Azure.

**System assigned**    User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. \n in code. [Learn more about Managed identities.](#)

Save   Discard   Refresh   |   Got feedback?

Status ⓘ

Off   **On**

Object (principal) ID ⓘ

0c288856-adea-485b-a4dc-c15b5ce2c401

Permissions ⓘ

Azure role assignments

- Se si sta implementando un cluster Kubernetes\* a gestione automatica, è necessario il nome utente di qualsiasi utente autorizzato.

## Fasi

Creare un ruolo del cluster e un'associazione di ruoli.

1. Puoi personalizzare l'autorizzazione in base ai tuoi requisiti.

## Backup/ripristino

Aggiungere l'autorizzazione di base per abilitare il backup e il ripristino per i cluster Kubernetes.

Sostituire `subjects: kind: variable` con il nome utente e `subjects: name:` Con l'ID oggetto per l'identità gestita assegnata dal sistema o il nome utente di qualsiasi utente autorizzato, come descritto in precedenza.

```
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

```

### Classi di storage

Aggiunta di autorizzazioni estese per aggiungere classi di storage utilizzando BlueXP.

Sostituire `subjects: kind: variabile` con il nome utente e `subjects: user:` Con l'ID oggetto per l'identità gestita assegnata dal sistema o il nome utente di qualsiasi utente autorizzato, come descritto in precedenza.

```

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
```

### Installazione di Trident

Utilizzare la riga di comando per fornire l'autorizzazione completa e abilitare BlueXP per installare Astra Trident.

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

2. Applicare la configurazione a un cluster.

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

## Requisiti per i cluster Kubernetes in Google Cloud

È possibile aggiungere e gestire cluster gestiti di Google Kubernetes Engine (GKE) e cluster di Kubernetes autogestiti in Google utilizzando BlueXP. Prima di aggiungere i cluster a BlueXP, assicurarsi che siano soddisfatti i seguenti requisiti.



In questo argomento viene utilizzato *Kubernetes cluster*, dove la configurazione è la stessa per i cluster GKE e Kubernetes autogestiti. Viene specificato il tipo di cluster in cui la configurazione differisce.

### Requisiti

#### Astra Trident

È necessaria una delle quattro versioni più recenti di Astra Trident. Puoi installare o aggiornare Astra Trident direttamente da BlueXP. Dovresti ["esaminare i prerequisiti"](#) Prima di installare Astra Trident

#### Cloud Volumes ONTAP

Cloud Volumes ONTAP deve essere in BlueXP con lo stesso account di tenancy, spazio di lavoro e connettore del cluster Kubernetes. ["Consultare i documenti di Astra Trident per la procedura di configurazione"](#).

#### Connettore BlueXP

Un connettore deve essere in esecuzione in Google con le autorizzazioni richieste. [Scopri di più di seguito](#).

#### Connettività di rete

È necessaria la connettività di rete tra il cluster Kubernetes e il connettore e tra il cluster Kubernetes e

Cloud Volumes ONTAP. [Scopri di più di seguito.](#)

## Autorizzazione RBAC

BlueXP supporta cluster abilitati per RBAC con e senza Active Directory. Il ruolo BlueXP Connector deve essere autorizzato su ciascun cluster GKE. [Scopri di più di seguito.](#)

## Preparare un connettore

Per rilevare e gestire i cluster Kubernetes, è necessario un connettore BlueXP in Google. Sarà necessario creare un nuovo connettore o utilizzare un connettore esistente con le autorizzazioni richieste.

### Creare un nuovo connettore

Seguire la procedura descritta in uno dei collegamenti riportati di seguito.

- ["Creare un connettore da BlueXP"](#) (consigliato)
- ["Installare il connettore su un host Linux esistente"](#)

### Aggiungere le autorizzazioni richieste a un connettore esistente (per rilevare un cluster GKE gestito)

Se si desidera rilevare un cluster GKE gestito, potrebbe essere necessario modificare il ruolo personalizzato del connettore per fornire le autorizzazioni.

#### Fasi

1. Poni "Console cloud", Accedere alla pagina **ruoli**.
2. Utilizzando l'elenco a discesa nella parte superiore della pagina, selezionare il progetto o l'organizzazione che contiene il ruolo che si desidera modificare.
3. Fare clic su un ruolo personalizzato.
4. Fare clic su **Edit role** (Modifica ruolo) per aggiornare le autorizzazioni del ruolo.
5. Fare clic su **Add Permissions** (Aggiungi autorizzazioni) per aggiungere le seguenti nuove autorizzazioni al ruolo.

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

6. Fare clic su **Update** (Aggiorna) per salvare il ruolo modificato.

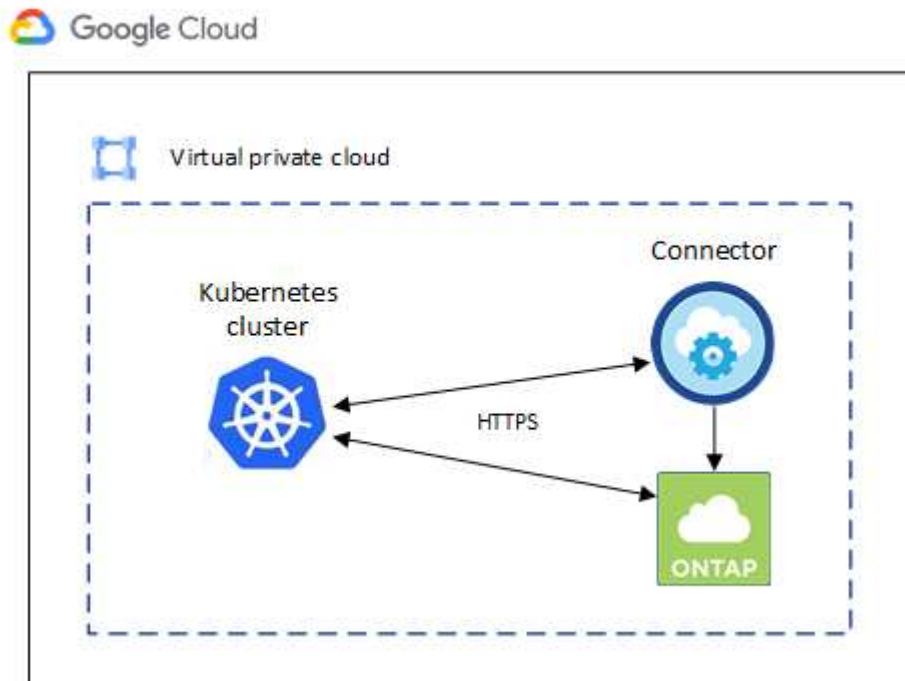
## Esaminare i requisiti di rete

È necessario fornire la connettività di rete tra il cluster Kubernetes e il connettore e tra il cluster Kubernetes e il sistema Cloud Volumes ONTAP che fornisce lo storage back-end al cluster.

- Ogni cluster Kubernetes deve disporre di una connessione in entrata dal connettore
- Il connettore deve disporre di una connessione in uscita a ciascun cluster Kubernetes sulla porta 443

Il modo più semplice per fornire questa connettività consiste nell'implementare il connettore e Cloud Volumes ONTAP nello stesso VPC del cluster Kubernetes. In caso contrario, è necessario impostare una connessione peering tra i diversi VPC.

Ecco un esempio che mostra ogni componente dello stesso VPC.



## Impostare l'autorizzazione RBAC

La convalida RBAC viene eseguita solo sui cluster Kubernetes con Active Directory (ad) attivato. I cluster Kubernetes senza ad passeranno automaticamente la convalida.

È necessario autorizzare il ruolo del connettore su ciascun cluster Kubernetes in modo che il connettore possa rilevare e gestire un cluster.

## Backup e ripristino

Il backup e il ripristino richiedono solo un'autorizzazione di base.

## Aggiungere classi di storage

È necessaria un'autorizzazione estesa per aggiungere classi di storage utilizzando BlueXP e monitorare il cluster per rilevare eventuali modifiche al backend.

## Installare Astra Trident

Devi fornire l'autorizzazione completa per BlueXP per installare Astra Trident.



Durante l'installazione di Astra Trident, BlueXP installa il backend Astra Trident e il segreto Kubernetes che contiene le credenziali che Astra Trident deve comunicare con il cluster di storage.

## Prima di iniziare

Da configurare `subjects: name:` Nel file YAML, è necessario conoscere l'ID univoco di BlueXP.

Puoi trovare l'ID univoco in due modi:

- Utilizzando il comando:

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

- Nel campo Service account Details (Dettagli account servizio) del "Console cloud".

CloudSync-Dev ▼

← Cloud Manager Service Account

DETAILS PERMISSIONS KEYS METRICS LOGS

### Service account details

Name  
Cloud Manager Service Account SAVE

Description SAVE

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

Unique ID  
102217358851946603445

## Fasi

Creare un ruolo del cluster e un'associazione di ruoli.

1. Puoi personalizzare l'autorizzazione in base ai tuoi requisiti.

## Backup/ripristino

Aggiungere l'autorizzazione di base per abilitare il backup e il ripristino per i cluster Kubernetes.

Sostituire `subjects: kind: variable` con il nome utente e `subjects: name:` Con l'ID univoco dell'account di servizio autorizzato.

```
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

```

### Classi di storage

Aggiunta di autorizzazioni estese per aggiungere classi di storage utilizzando BlueXP.

Sostituire subjects: kind: variabile con il nome utente e. subjects: user: Con l'ID univoco dell'account di servizio autorizzato.

```

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
```

### Installazione di Trident

Utilizzare la riga di comando per fornire l'autorizzazione completa e abilitare BlueXP per installare Astra Trident.

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

2. Applicare la configurazione a un cluster.

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

## Requisiti per i cluster Kubernetes in OpenShift

È possibile aggiungere e gestire cluster OpenShift Kubernetes autogestiti utilizzando BlueXP. Prima di aggiungere i cluster a BlueXP, assicurarsi che siano soddisfatti i seguenti requisiti.

### Requisiti

#### Astra Trident

È necessaria una delle quattro versioni più recenti di Astra Trident. Puoi installare o aggiornare Astra Trident direttamente da BlueXP. Dovresti ["esaminare i prerequisiti"](#) Prima di installare Astra Trident.

#### Cloud Volumes ONTAP

Cloud Volumes ONTAP deve essere configurato come storage back-end per il cluster. ["Consultare i documenti di Astra Trident per la procedura di configurazione"](#).

#### Connettore BlueXP

Per importare e gestire i cluster Kubernetes è necessario un connettore BlueXP. È necessario creare un nuovo connettore o utilizzare un connettore esistente che disponga delle autorizzazioni necessarie per il provider cloud:

- ["Connettore AWS"](#)
- ["Connettore Azure"](#)
- ["Google Cloud Connector"](#)

#### Connettività di rete

È necessaria la connettività di rete tra il cluster Kubernetes e il connettore e tra il cluster Kubernetes e Cloud Volumes ONTAP.

## File di configurazione di Kubernetes (kubeconfig) con autorizzazione RBAC

Per importare i cluster OpenShift, è necessario un file kubeconfig con l'autorizzazione RBAC richiesta per abilitare funzionalità diverse. [Creare un file kubeconfig](#).

- Backup e ripristino: Il backup e il ripristino richiedono solo un'autorizzazione di base.
- Aggiunta di classi di storage: È richiesta un'autorizzazione estesa per aggiungere classi di storage utilizzando BlueXP e monitorare il cluster per rilevare eventuali modifiche al backend.
- Installare Astra Trident: Devi fornire l'autorizzazione completa per BlueXP per installare Astra Trident.



Durante l'installazione di Astra Trident, BlueXP installa il backend Astra Trident e il segreto Kubernetes che contiene le credenziali che Astra Trident deve comunicare con il cluster di storage.

## Creare un file kubeconfig

Utilizzando la CLI di OpenShift, creare un file kubeconfig da importare in BlueXP.

### Fasi

1. Accedere alla CLI di OpenShift utilizzando `oc login` Su un URL pubblico con un utente amministrativo.
2. Creare un account di servizio come segue:
  - a. Creare un file di account del servizio denominato `oc-service-account.yaml`.

Regolare il nome e lo spazio dei nomi in base alle esigenze. Se le modifiche vengono apportate qui, è necessario applicare le stesse modifiche nei passaggi seguenti.

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

+

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

- a. Applicare l'account del servizio:

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

3. Creare un'associazione di ruoli personalizzata in base ai requisiti di autorizzazione.
  - a. Creare un `ClusterRoleBinding` file chiamato `oc-clusterrolebinding.yaml`.

```
oc-clusterrolebinding.yaml
```

- b. Configurare l'autorizzazione RBAC in base alle esigenze del cluster.

## Backup/ripristino

Aggiungere l'autorizzazione di base per abilitare il backup e il ripristino per i cluster Kubernetes.

```
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

```

### Classi di storage

Aggiunta di autorizzazioni estese per aggiungere classi di storage utilizzando BlueXP.

```

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

```

## Installazione di Trident

Concedere l'autorizzazione amministrativa completa e abilitare BlueXP per l'installazione di 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. Applicare l'associazione del ruolo del cluster:

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

4. Elencare i segreti dell'account di servizio, sostituendo <context> con il contesto corretto per l'installazione:

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

La fine dell'output dovrebbe essere simile a quanto segue:

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

Gli indici di ciascun elemento in `secrets` l'array inizia con 0. Nell'esempio precedente, l'indice per `oc-service-account-dockercfg-vhz87` sarebbe 0 e l'indice per `oc-service-account-token-r59kr` sarebbe 1. Nell'output, annotare l'indice del nome dell'account del servizio che contiene la parola "token".

5. Generare il kubeconfig come segue:

- Creare un `create-kubeconfig.sh` file. Sostituire `TOKEN_INDEX` all'inizio del seguente script con il valore corretto.

## 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. Eseguire la sorgente dei comandi per applicarli al cluster Kubernetes.

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

## Risultato

Verrà utilizzato il risultato kubeconfig-sa File per aggiungere un cluster OpenShift a BlueXP.

# Aggiungere cluster Kubernetes

## Aggiungere un cluster Amazon Kubernetes a BlueXP

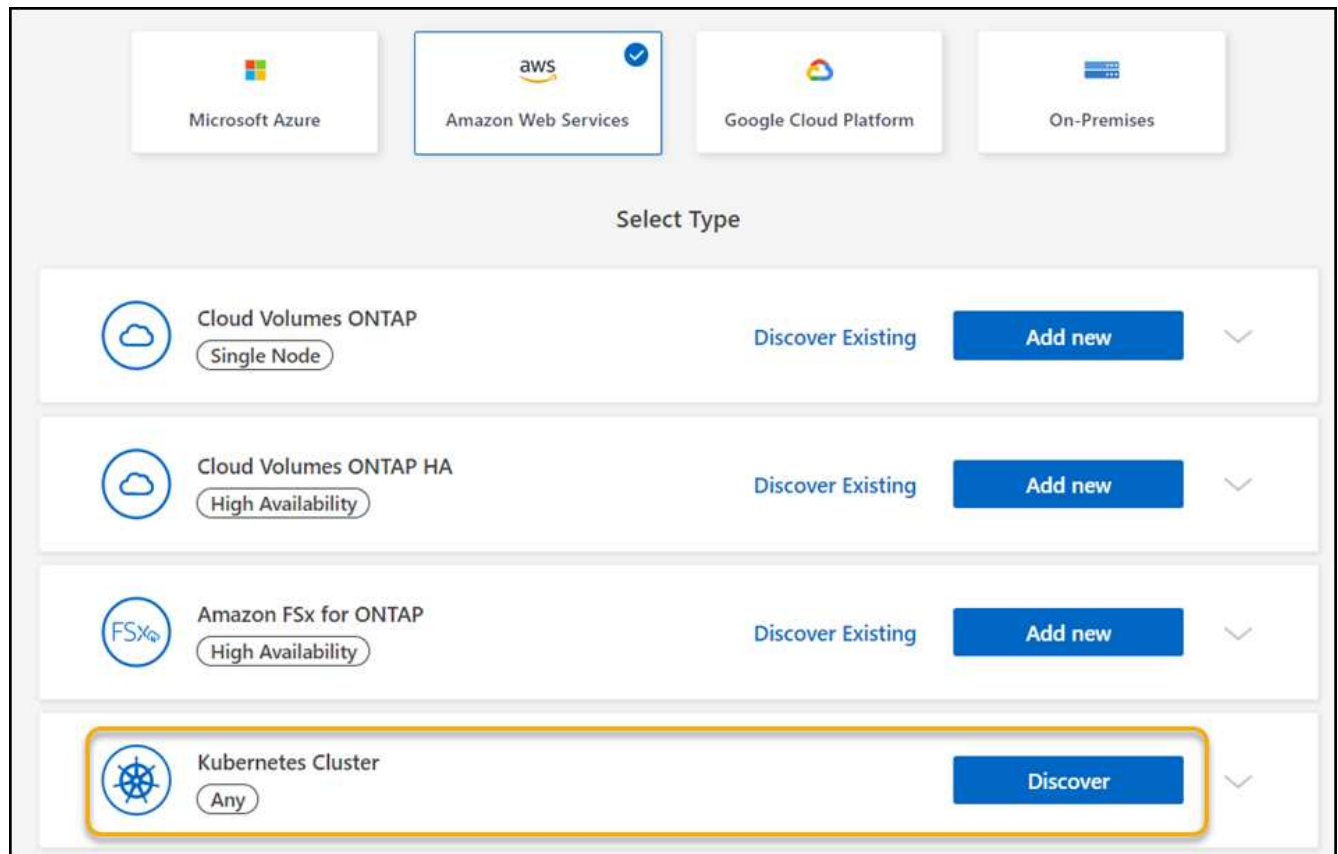
Puoi scoprire o importare i cluster Kubernetes in BlueXP in modo da poter eseguire il backup dei volumi persistenti in Amazon S3.

### Individuare un cluster

È possibile scoprire un cluster Kubernetes completamente gestito o autogestito. I cluster gestiti devono essere rilevati e non possono essere importati.

#### Fasi

1. In **Canvas**, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
2. Selezionare **Amazon Web Services > Kubernetes Cluster > Discover**.



3. Selezionare **Discover Cluster** (Discover Cluster) e fare clic su **Next** (Avanti).
4. Scegliere una regione AWS, selezionare un cluster Kubernetes e fare clic su **Avanti**.



## Risultato

BlueXP aggiunge il cluster Kubernetes a Canvas.

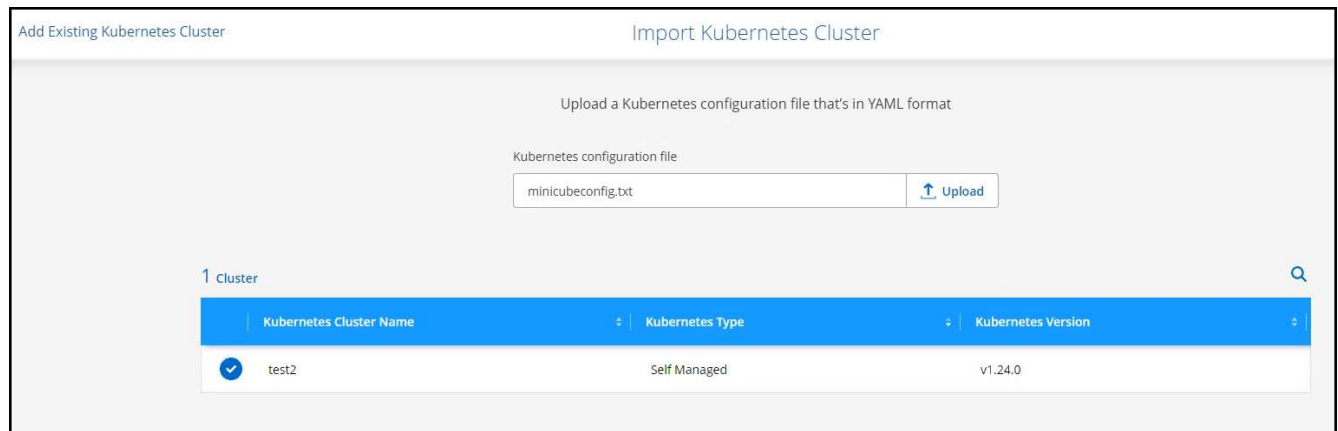


## Importare un cluster

È possibile importare un cluster Kubernetes autogestito utilizzando un file di configurazione Kubernetes.

### Fasi

1. In **Canvas**, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
2. Selezionare **Amazon Web Services > Kubernetes Cluster > Discover**.
3. Selezionare **Importa cluster** e fare clic su **Avanti**.
4. Caricare un file di configurazione Kubernetes in formato YAML.



5. Selezionare il cluster Kubernetes e fare clic su **Avanti**.

### Risultato

BlueXP aggiunge il cluster Kubernetes a Canvas.

## Aggiungere un cluster Azure Kubernetes a BlueXP

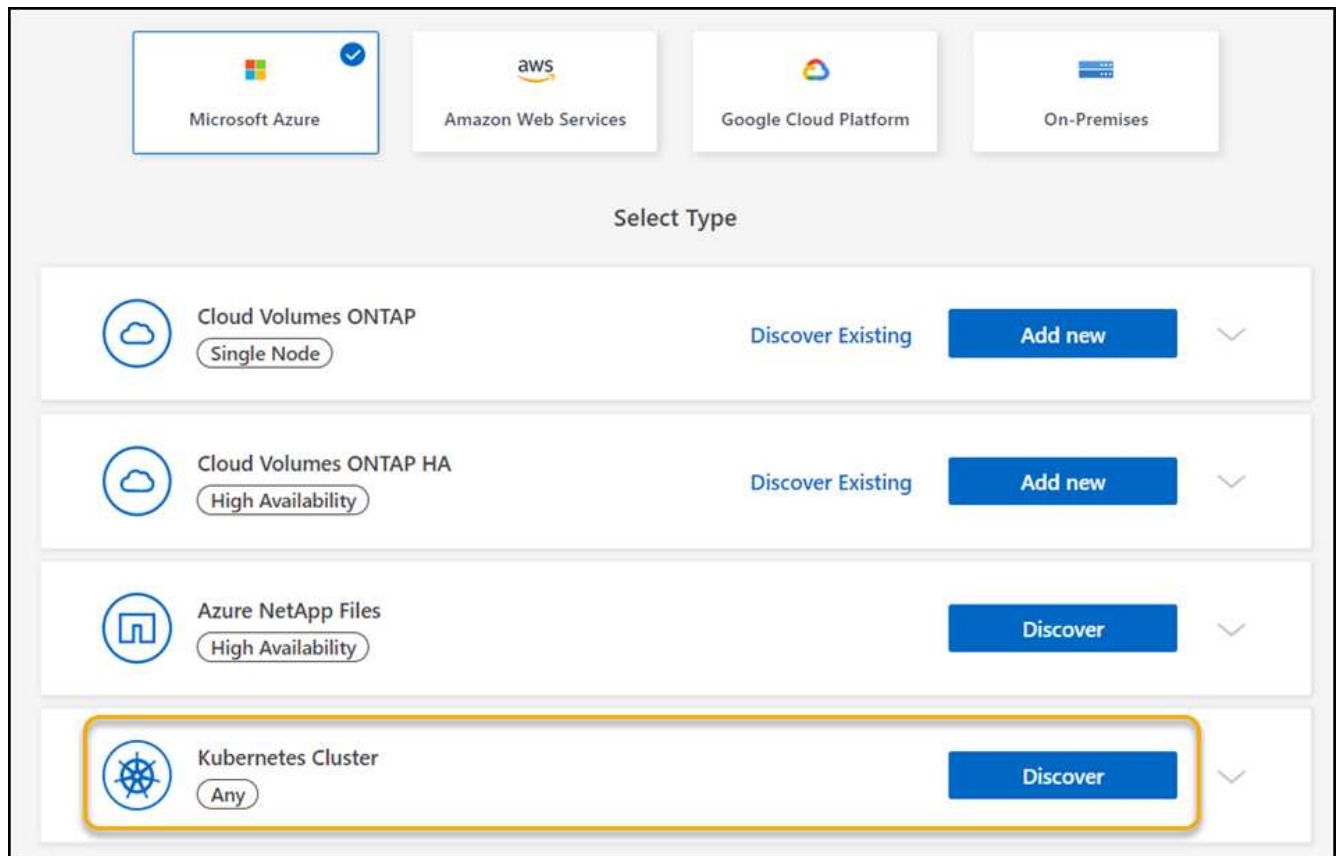
È possibile rilevare o importare cluster Kubernetes in BlueXP in modo da poter eseguire il backup di volumi persistenti in Azure.

### Individuare un cluster

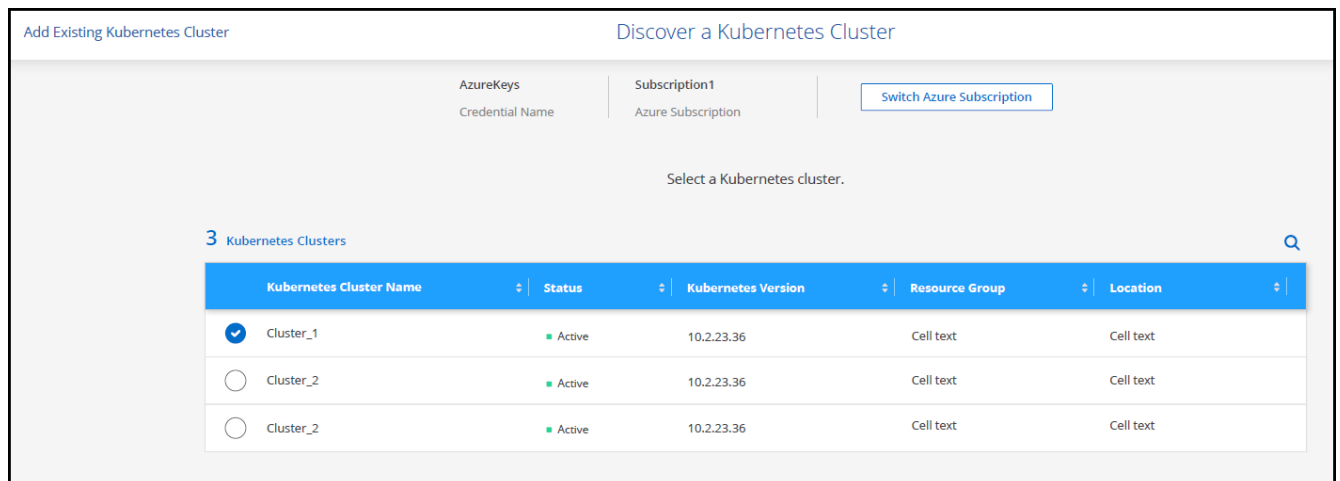
È possibile scoprire un cluster Kubernetes completamente gestito o autogestito. I cluster gestiti devono essere rilevati e non possono essere importati.

### Fasi

1. In **Canvas**, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
2. Selezionare **Microsoft Azure > Kubernetes Cluster > Discover**.

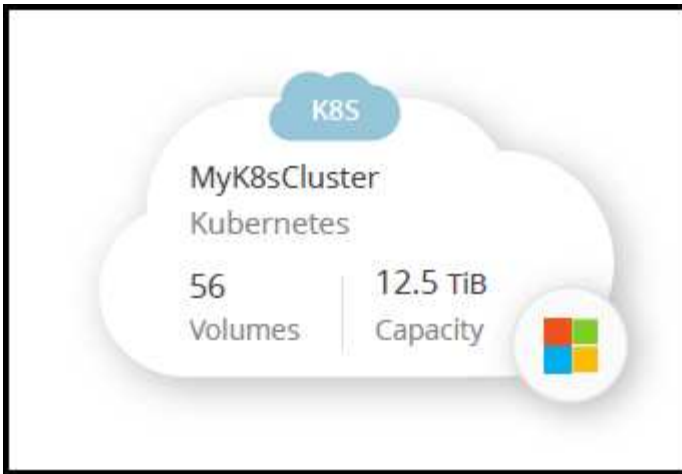


3. Selezionare **Discover Cluster** (Discover Cluster) e fare clic su **Next** (Avanti).
4. Selezionare un cluster Kubernetes e fare clic su **Avanti**.



## Risultato

BlueXP aggiunge il cluster Kubernetes a Canvas.



## Importare un cluster

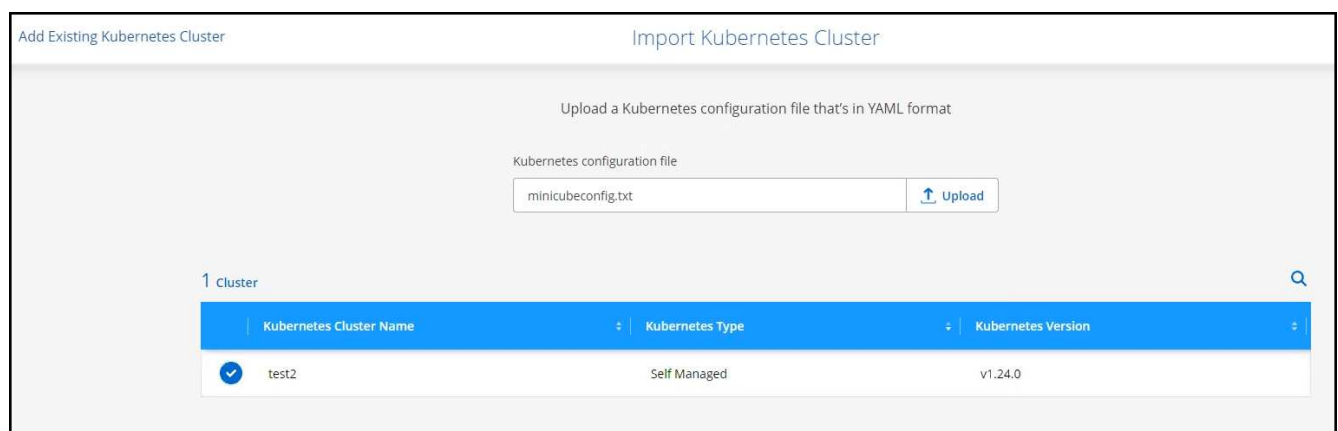
È possibile importare un cluster Kubernetes autogestito utilizzando un file di configurazione Kubernetes.

### Prima di iniziare

Per importare i cluster Kubernetes, sono necessari i certificati autorità di certificazione, chiave client e certificato client per l'utente specificato nel file YAML del ruolo del cluster. L'amministratore del cluster Kubernetes riceve queste certificazioni quando crea utenti sul cluster Kubernetes.

#### Fasi

1. In **Canvas**, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
2. Selezionare **Microsoft Azure > Kubernetes Cluster > Discover**.
3. Selezionare **Importa cluster** e fare clic su **Avanti**.
4. Caricare un file di configurazione Kubernetes in formato YAML.




5. Caricare i certificati del cluster forniti dall'amministratore del cluster Kubernetes.


## Upload Cluster Certificates

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


Certificate Authority

No file selected 

Client Key

No file selected 

Client Certificate

No file selected 

### Risultato

BlueXP aggiunge il cluster Kubernetes a Canvas.

## Aggiungere un cluster Google Cloud Kubernetes a BlueXP

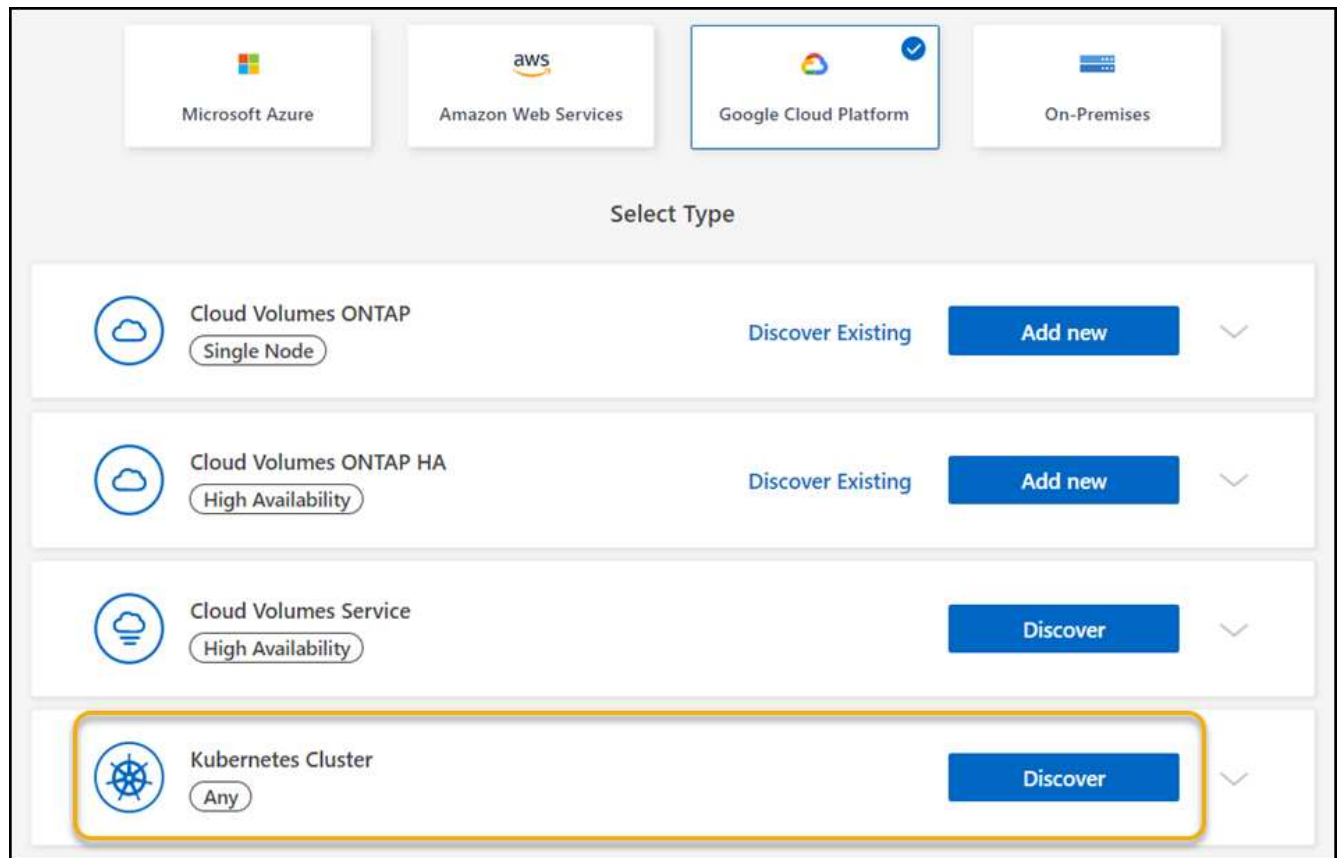
Puoi scoprire o importare i cluster Kubernetes in BlueXP in modo da poter eseguire il backup dei volumi persistenti in Google Cloud.

### Individuare un cluster

È possibile scoprire un cluster Kubernetes completamente gestito o autogestito. I cluster gestiti devono essere rilevati e non possono essere importati.

### Fasi

1. In **Canvas**, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
2. Selezionare **Google Cloud Platform > Kubernetes Cluster > Discover**.



3. Selezionare **Discover Cluster** (Discover Cluster) e fare clic su **Next** (Avanti).
4. Per selezionare un cluster Kubernetes in un altro progetto Google Cloud, fai clic su **Modifica progetto** e scegli un progetto disponibile.



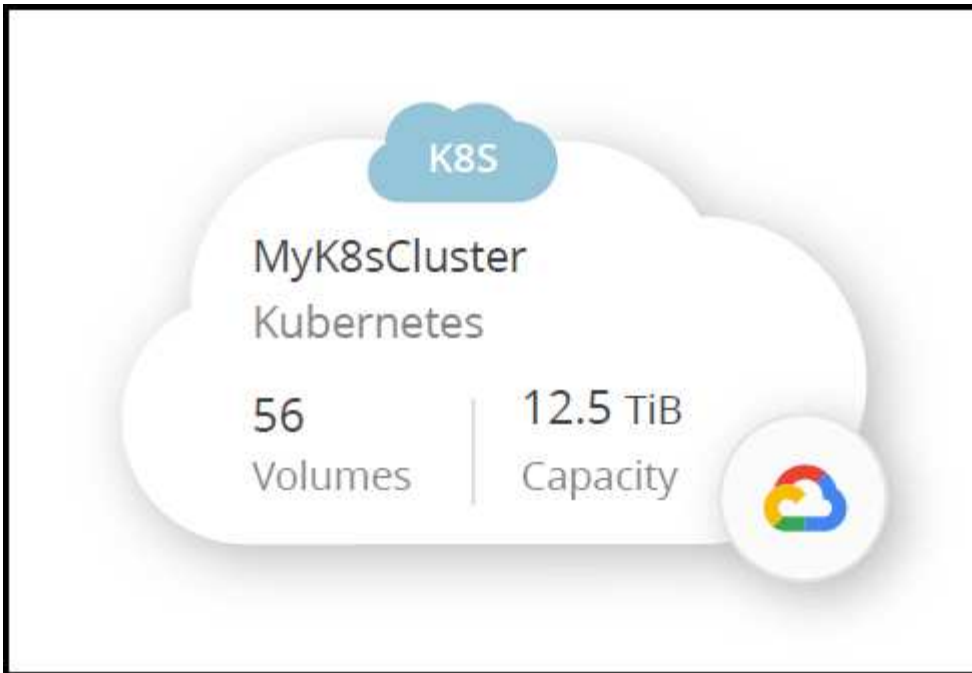


5. Selezionare un cluster Kubernetes e fare clic su **Avanti**.



## Risultato

BlueXP aggiunge il cluster Kubernetes a Canvas.



## Importare un cluster

È possibile importare un cluster Kubernetes autogestito utilizzando un file di configurazione Kubernetes.

## Prima di iniziare

Per importare i cluster Kubernetes, sono necessari i certificati autorità di certificazione, chiave client e certificato client per l'utente specificato nel file YAML del ruolo del cluster. L'amministratore del cluster Kubernetes riceve queste certificazioni quando crea utenti sul cluster Kubernetes.

### Fasi

1. In **Canvas**, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro).
2. Selezionare **Google Cloud Platform > Kubernetes Cluster > Discover**.
3. Selezionare **Importa cluster** e fare clic su **Avanti**.
4. Caricare un file di configurazione Kubernetes in formato YAML.

Add Existing Kubernetes Cluster

Import Kubernetes Cluster

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

Kubernetes configuration file

KubConfig.txt

Upload

3 Kubernetes Clusters

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

## Risultato

BlueXP aggiunge il cluster Kubernetes a Canvas.

# Importare un cluster OpenShift in BlueXP

Importa un cluster OpenShift autogestiti in BlueXP per iniziare a eseguire il backup dei volumi persistenti nel tuo provider cloud.

## Importare un cluster

È possibile importare un cluster Kubernetes autogestito utilizzando un file di configurazione Kubernetes.

### Prima di iniziare

Prima di importare un cluster OpenShift, è necessario:

- Il file `kubeconfig-sa` creato in ["creare un file kubeconfig"](#).
- I file Public Certificate Authority (ad esempio, ca.crt), Client Key (ad esempio tls.key) e Client Certification (ad esempio, tls.crt) per il cluster.

### Fasi

1. In **Canvas**, selezionare **Add Working Environment** (Aggiungi ambiente di lavoro).
2. Seleziona il tuo provider cloud e seleziona **Kubernetes Cluster > Discover**.
3. Selezionare **Importa cluster**, quindi **Avanti**.
4. Caricare kubeconfig-sa file creato in ["creare un file kubeconfig"](#). Selezionare il cluster Kubernetes e selezionare **Avanti**.

Add Existing Kubernetes Cluster

Import Kubernetes Cluster

Upload a Kubernetes configuration file that's in YAML format

Kubernetes configuration file

minikubeconfig.txt

1 Cluster

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

5. Caricare i certificati del cluster.

### Upload Cluster Certificates

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

Certificate Authority

No file selected

⬆️⬆️

Client Key

No file selected

⬆️⬆️

Client Certificate

No file selected

⬆️⬆️

## Risultato

BlueXP aggiunge il cluster Kubernetes a Canvas.

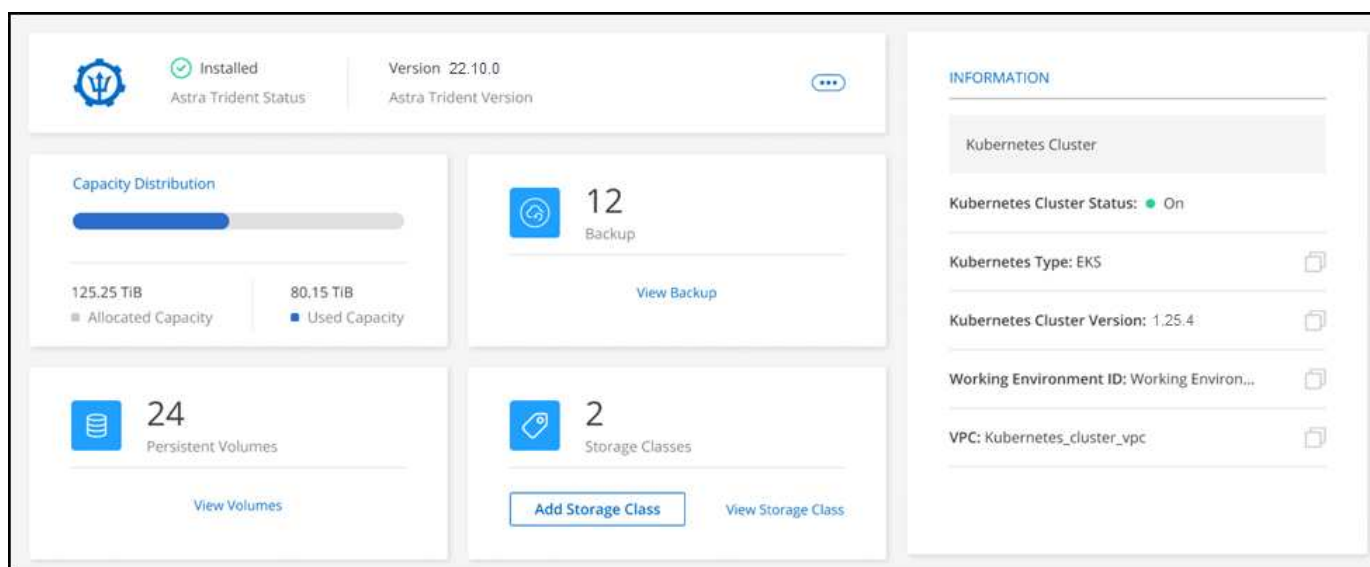
# Gestire i cluster Kubernetes

## Gestire Astra Trident

Dopo aver aggiunto un cluster Kubernetes gestito a Canvas, è possibile utilizzare BlueXP per confermare un'installazione di Astra Trident compatibile, installare o aggiornare Astra Trident alla versione più recente o disinstallare Astra Trident.

### Astra Trident in BlueXP

Dopo aver aggiunto i cluster Kubernetes a BlueXP, puoi gestire Astra Trident e i cluster Kubernetes dalla pagina panoramica. Per aprire la pagina panoramica, fare doppio clic sull'ambiente di lavoro Kubernetes in Canvas.



### Versioni supportate di Astra Trident

È necessaria una delle quattro versioni più recenti di Astra Trident implementate utilizzando l'operatore Trident, manualmente o utilizzando la mappa Helm. Se Astra Trident non è installato o è installata una versione incompatibile di Astra Trident, il cluster mostrerà che è necessario eseguire un'azione.



Astra Trident implementato con `tridentctl` non è supportato. Se hai implementato Astra Trident con `tridentctl`, Non è possibile utilizzare BlueXP per gestire i cluster Kubernetes o disinstallare Astra Trident. È necessario E reinstallare Astra Trident manualmente utilizzando "L'operatore Trident" O in BlueXP con [Installare o aggiornare Astra Trident](#).

Per ulteriori informazioni su Astra Trident, vedere ["Documentazione di Astra Trident"](#).

### Installare o aggiornare Astra Trident

Puoi rivedere lo stato e la versione dell'installazione di Astra Trident nella pagina panoramica. Se Astra Trident non è già installato o se è installata una versione incompatibile, è possibile gestirla utilizzando BlueXP.

#### Fasi

1. Fare doppio clic sull'ambiente di lavoro Kubernetes in Canvas o fare clic su **Enter Working Environment**.

a. Se Astra Trident non è installato, fare clic su **Installa Trident**.

**1 | Install Astra Trident**

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

Install Trident

b. Se è installata una versione non supportata di Astra Trident, fare clic su **Upgrade Trident** (Aggiorna Trident).

**Upgrade Astra Trident**

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

Upgrade Trident



Non è possibile utilizzare BlueXP per eseguire l'aggiornamento da Astra Trident versioni precedenti alla 21.01. Per eseguire l'aggiornamento da una versione precedente, fare riferimento a. ["Eseguire l'upgrade con l'operatore"](#).

## Risultati

È installata l'ultima versione di Astra Trident. È ora possibile aggiungere classi di storage.

## Disinstallare Astra Trident

Se Astra Trident è stato installato utilizzando BlueXP o l'operatore Trident (Helm o manualmente), è possibile disinstallarlo utilizzando BlueXP.

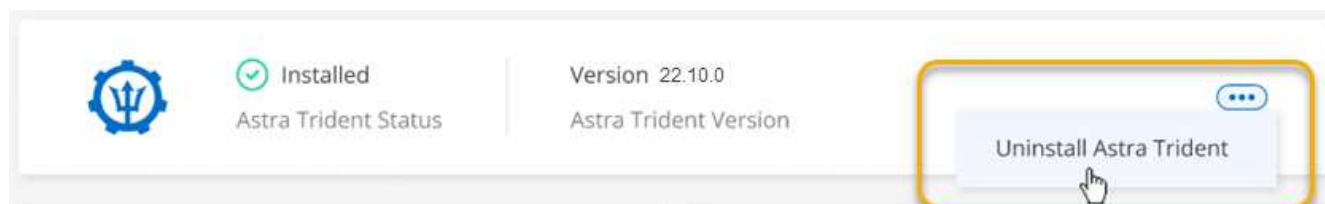


- Dopo aver disinstallato Astra Trident non è possibile creare nuovi volumi persistenti, ma i volumi esistenti sono ancora disponibili.
- Mentre Astra Trident è disinstallato, il backup non è disponibile.
- Puoi reinstallare Astra Trident nell'ambiente di lavoro in qualsiasi momento per continuare a gestire i cluster.

La disinstallazione di Astra Trident con BlueXP non rimuove tutti i servizi Astra Trident applicati durante l'installazione. Per rimuovere completamente Astra Trident, incluse tutte le definizioni di risorse personalizzate (CRD) create, fare riferimento a. ["Eseguire la disinstallazione utilizzando l'operatore Trident"](#)

## Fasi

1. Dalla pagina panoramica, selezionare i puntini di sospensione e **Disinstalla Astra Trident**.



2. Selezionare **Disinstalla** per confermare e disinstallare Astra Trident.

## Risultati

Astra Trident viene disinstallato dall'ambiente di lavoro. Puoi reinstallare Astra Trident in qualsiasi momento.

# Gestire le classi di storage

Dopo aver aggiunto un cluster Kubernetes gestito a Canvas, è possibile utilizzare BlueXP per gestire le classi di storage.



Se non viene definita alcuna classe di storage, il cluster mostra che è necessaria un'azione. Facendo doppio clic sul cluster in Canvas si apre la pagina delle azioni per aggiungere una classe di storage.

## Aggiungere classe di storage

### Fasi

1. Da Canvas, trascinare l'ambiente di lavoro Kubernetes sull'ambiente di lavoro Cloud Volumes ONTAP o Amazon FSX per ONTAP per aprire la procedura guidata della classe di storage.
2. Specificare un nome per la classe di storage.
3. Selezionare lo storage **filesystem** o **block**.
  - a. Per lo storage **block**, selezionare un tipo di file system (fstype)

- b. Per lo storage **block** o **filesystem**, è possibile scegliere di abilitare l'economia della classe di storage.

Storage Class

☒ Filesystem
 ☐ Block

Storage Class Economy ⓘ

☒ Enable Economy for Storage Class

Support Volume Expansion

☒ Yes
 ☐ No

Volume Binding Mode

☒ Immediate
 ☐ WaitForFirstConsumer

Set as Default Storage Class

☒ Yes
 ☐ No



Backup e ripristino non sono supportati quando si utilizza storage class economy.

- Selezionare le opzioni per l'espansione del volume, il binding del volume e la classe di storage predefinita. Fare clic su **Avanti**.
- Selezionare un ambiente di lavoro per la connessione al cluster. Fare clic su **Aggiungi**.

☒ Storage Class Definitions
 ☒ Select Working Environment

Select Working Environment

Working Environment	Type	Configuration	Region	Connected to K8s Clusters
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name <input checked="" type="checkbox"/> On	Cloud Volumes ONTAP	Single Node	US East (Northern Virginia)	Not Connected

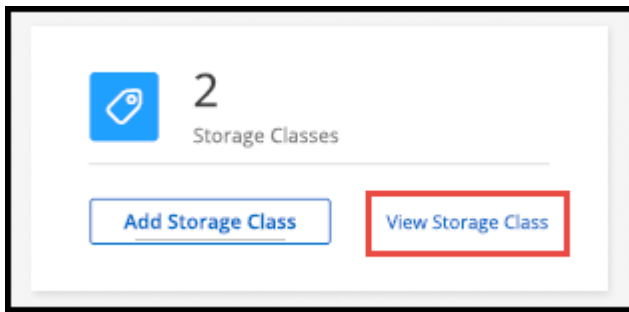
Previous

Add

## Risultati

È possibile fare clic per visualizzare la classe di storage dalla pagina delle risorse del cluster Kubernetes.





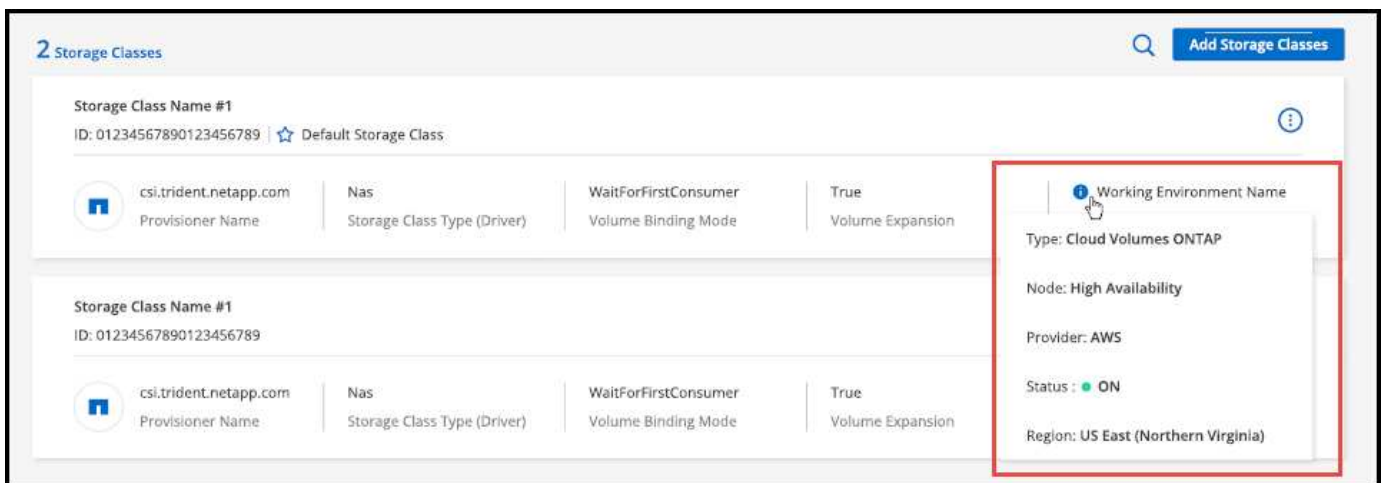
## Visualizza i dettagli dell'ambiente di lavoro

### Fasi

1. Fare doppio clic sull'ambiente di lavoro Kubernetes in Canvas o fare clic su **Enter Working Environment**.
2. Fare clic sulla scheda **Storage CLASSES**.
3. Fare clic sull'icona delle informazioni per visualizzare i dettagli dell'ambiente di lavoro.

### Risultati

Viene visualizzato il pannello dei dettagli dell'ambiente di lavoro.



## Impostare la classe di storage predefinita

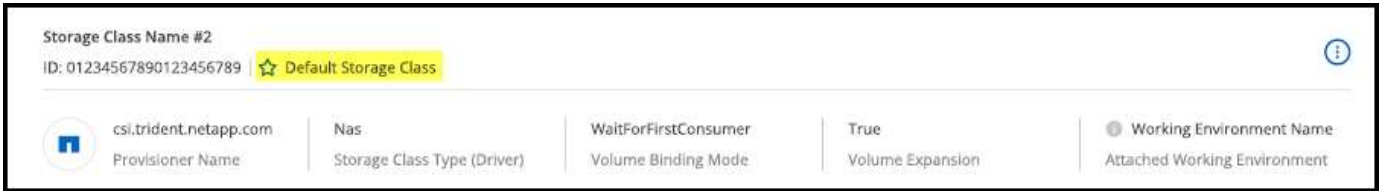
### Fasi

1. Fare doppio clic sull'ambiente di lavoro Kubernetes in Canvas o fare clic su **Enter Working Environment**.
2. Fare clic sulla scheda **Storage CLASSES**.
3. Fare clic sul menu delle azioni della classe di storage e fare clic su **Set as Default** (Imposta come predefinita).



## Risultati

La classe di storage selezionata viene impostata come predefinita.



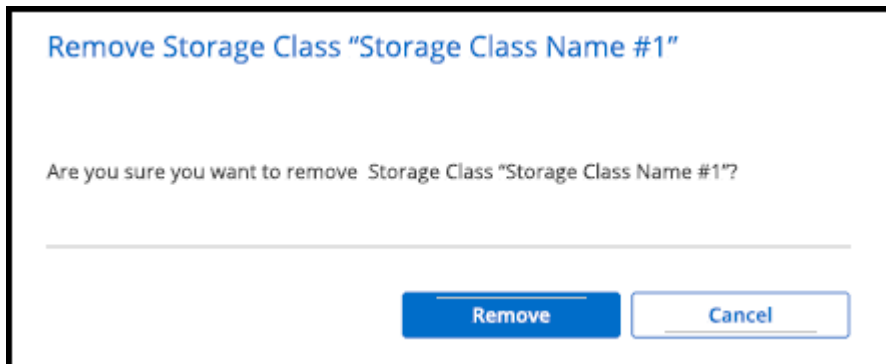
## Rimuovere la classe di storage

### Fasi

1. Fare doppio clic sull'ambiente di lavoro Kubernetes in Canvas o fare clic su **Enter Working Environment**.
2. Fare clic sulla scheda **Storage CLASSES**.
3. Fare clic sul menu delle azioni della classe di storage e fare clic su **Set as Default** (Imposta come predefinita).



4. Fare clic su **Remove** (Rimuovi) per confermare la rimozione della classe di storage.



## Risultati

La classe di storage selezionata viene rimossa.

## Visualizzare volumi persistenti

Dopo aver aggiunto un cluster Kubernetes gestito a Canvas, è possibile utilizzare BlueXP per visualizzare i volumi persistenti.



BlueXP monitora il cluster Kubernetes per rilevare eventuali modifiche al backend e aggiorna la tabella dei volumi persistenti quando vengono aggiunti nuovi volumi. Se è stato configurato il backup automatico sul cluster, il backup viene attivato automaticamente sui nuovi volumi persistenti.

## Fasi

1. Fare doppio clic sull'ambiente di lavoro Kubernetes in Canvas o fare clic su **Enter Working Environment**.
2. Fare clic su **View Volumes** (Visualizza volumi) dalla scheda **Overview** (Panoramica) oppure fare clic sulla scheda **Persistent Volumes** (volumi persistenti). Se non sono configurati volumi persistenti, vedere ["Provisioning"](#) Per informazioni dettagliate sul provisioning dei volumi in Astra Trident.

## Risultati

Viene visualizzata una tabella dei volumi persistenti configurati.

Volumes Summary

8

Total Volumes

400

GiB

Total Allocated Capacity

201.2

GiB

Total Used Capacity

8 Volumes

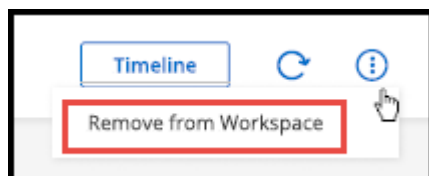
Volume Name	Name Space	Storage Class	Access Mode	Allocated Capacity	Used Capacity
<div>Volumes Very Long Name</div> <div><div></div> On</div>	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB
<div>Volumes Very Long Name</div> <div><div></div> On</div>	Name Space	Storage Class Name	Access Mode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

## Rimuovere i cluster Kubernetes dallo spazio di lavoro

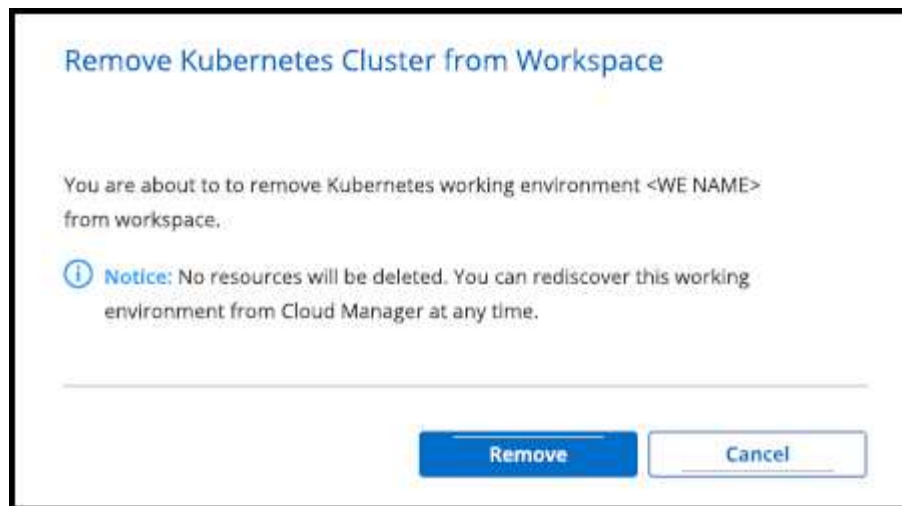
Dopo aver aggiunto un cluster Kubernetes gestito a Canvas, è possibile utilizzare BlueXP per rimuovere i cluster dall'area di lavoro.

## Fasi

1. Fare doppio clic sull'ambiente di lavoro Kubernetes in Canvas o fare clic su **Enter Working Environment**.
2. Nella parte superiore destra della pagina, selezionare il menu delle azioni e fare clic su **Rimuovi dall'area di lavoro**.



3. Fare clic su **Remove** (Rimuovi) per confermare la rimozione del cluster dall'area di lavoro. È possibile riscoprire questo cluster in qualsiasi momento.



### Risultati

Il cluster Kubernetes viene rimosso dall'area di lavoro e non è più visibile in Canvas.

## Utilizza i servizi dati cloud di NetApp con i cluster Kubernetes

Dopo aver aggiunto un cluster Kubernetes gestito a Canvas, puoi utilizzare i servizi dati cloud di NetApp per una gestione avanzata dei dati.

È possibile utilizzare il backup e il ripristino di BlueXP per eseguire il backup dei volumi persistenti nello storage a oggetti.

["Scopri come proteggere i dati del cluster Kubernetes utilizzando il backup e il ripristino BlueXP".](#)

1 Selected Kubernetes Clusters

Backup Settings



1

Kubernetes Clusters



5

Protected PVs



97.66 KB

Total Backups Size

## Protected Persistent Volumes Status

5

Healthy Backup

0

Failed Backup

## 5 Backup Jobs



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

# Conoscenza e supporto

## Registrati per ricevere assistenza

È necessaria la registrazione del supporto per ricevere supporto tecnico specifico per BlueXP e le relative soluzioni e servizi storage. È inoltre necessaria la registrazione del supporto per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP.

La registrazione per il supporto non attiva il supporto NetApp per un file service provider cloud. Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- ["Amazon FSX per ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service per Google Cloud"](#)

## Panoramica sulla registrazione del supporto

Esistono due forme di registrazione per attivare i diritti di supporto:

- Registrazione dell'abbonamento al supporto per l'ID account BlueXP (il numero di serie a 20 cifre 960xxxxxxxxx nella pagina Support Resources di BlueXP).

Questa funzione funge da unico ID di abbonamento al supporto per qualsiasi servizio all'interno di BlueXP. Ogni abbonamento al supporto a livello di account BlueXP deve essere registrato.

- Registrazione dei numeri di serie Cloud Volumes ONTAP associati a un abbonamento nel mercato del provider cloud (si tratta di numeri di serie 909201xxxxxxxx a 20 cifre).

Questi numeri seriali sono comunemente denominati *numeri seriali PAYGO* e vengono generati da BlueXP al momento dell'implementazione di Cloud Volumes ONTAP.

La registrazione di entrambi i tipi di numeri di serie offre funzionalità come l'apertura di ticket di supporto e la generazione automatica dei casi. La registrazione viene completata aggiungendo account del sito di supporto NetApp a BlueXP come descritto di seguito.

## Registrare l'account BlueXP per il supporto NetApp

Per registrarsi al supporto e attivare i diritti di supporto, un utente del proprio account BlueXP deve associare un account del sito di supporto NetApp al proprio account di accesso BlueXP. La modalità di registrazione al supporto NetApp dipende dal fatto che si disponga già di un account NetApp Support Site (NSS).

### Cliente esistente con un account NSS

Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

### Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **User Credentials** (credenziali utente).
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp.
4. Per confermare che la procedura di registrazione è stata eseguita correttamente, selezionare l'icona Guida e selezionare **supporto**.

La pagina **risorse** dovrebbe mostrare che il tuo account è registrato per il supporto.



Si noti che gli altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Tuttavia, ciò non significa che il tuo account BlueXP non sia registrato per il supporto. Se un utente dell'account ha seguito questa procedura, l'account è stato registrato.

### Cliente esistente ma nessun account NSS

Se sei un cliente NetApp con licenze e numeri di serie esistenti ma *no* account NSS, devi creare un account NSS e associarlo al tuo login BlueXP.

#### Fasi

1. Creare un account NetApp Support Site completando il "[Modulo di registrazione per l'utente del sito di supporto NetApp](#)"
  - a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
  - b. Assicurarsi di copiare il numero di serie dell'account BlueXP (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.
2. Associare il nuovo account NSS al login BlueXP completando la procedura riportata sotto [Cliente esistente con un account NSS](#).

### Novità di NetApp

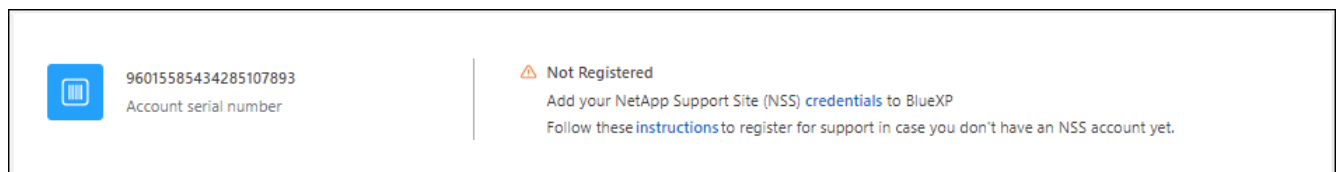
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

#### Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Individuare il numero di serie dell'ID account nella pagina Support Registration (registrazione supporto).



3. Selezionare ["Sito per la registrazione del supporto NetApp"](#) E selezionare **non sono un cliente NetApp registrato**.
4. Compilare i campi obbligatori (con asterischi rossi).
5. Nel campo **Product Line**, selezionare **Cloud Manager**, quindi selezionare il provider di fatturazione appropriato.
6. Copia il numero di serie del tuo account dal punto 2 precedente, completa il controllo di sicurezza, quindi conferma di aver letto la Global Data Privacy Policy di NetApp.

Viene immediatamente inviata un'e-mail alla casella di posta fornita per finalizzare questa transazione sicura. Controllare le cartelle di spam se l'e-mail di convalida non arriva in pochi minuti.

7. Confermare l'azione dall'interno dell'e-mail.

La conferma invia la tua richiesta a NetApp e ti consiglia di creare un account NetApp Support Site.

8. Creare un account NetApp Support Site completando il ["Modulo di registrazione per l'utente del sito di supporto NetApp"](#)
  - a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
  - b. Assicurarsi di copiare il numero di serie dell'account (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.

#### Al termine

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di assunzione per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp, associare l'account al login BlueXP completando la procedura indicata in [Cliente esistente con un account NSS](#).



## Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

Per attivare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP, è necessario associare le credenziali del sito di supporto NetApp all'account BlueXP:

- Registrazione dei sistemi Cloud Volumes ONTAP pay-as-you-go per il supporto

È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

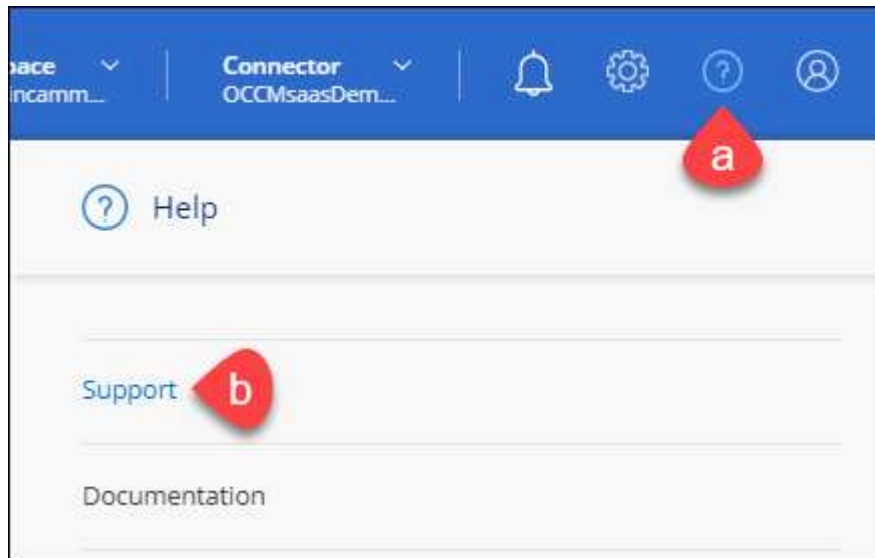
L'associazione delle credenziali NSS all'account BlueXP è diversa dall'account NSS associato a un account utente BlueXP.

Queste credenziali NSS sono associate all'ID account BlueXP specifico. Gli utenti che appartengono all'account BlueXP possono accedere a queste credenziali da **Support > NSS Management**.

- Se disponi di un account a livello di cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o reseller, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

### Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

Tenere presente quanto segue:


- L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
- Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

"Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

Lo stesso vale se si dispone di account NSS a livello di cliente preesistenti e si tenta di aggiungere un account a livello di partner.

- Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da  menu.

- Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in  menu.

Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

## Richiedi assistenza

NetApp fornisce supporto per BlueXP e i suoi servizi cloud in diversi modi. Sono disponibili opzioni complete di supporto autonomo gratuito 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include il supporto tecnico remoto via web ticketing.

### Ottieni supporto per un file service del cloud provider

Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- ["Amazon FSX per ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service per Google Cloud"](#)

Per ricevere supporto tecnico specifico di BlueXP e delle relative soluzioni e servizi storage, utilizza le opzioni di supporto descritte di seguito.

## Utilizzare le opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- Documentazione

La documentazione BlueXP attualmente visualizzata.

- ["Knowledge base"](#)

Cercare nella Knowledge base di BlueXP articoli utili per la risoluzione dei problemi.

- ["Community"](#)

Unisciti alla community BlueXP per seguire le discussioni in corso o crearne di nuove.

## Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo l'attivazione del supporto.

### Prima di iniziare

- Per utilizzare la funzione **creazione di un caso**, è necessario prima associare le credenziali del sito di supporto NetApp al login BlueXP. ["Scopri come gestire le credenziali associate all'accesso a BlueXP"](#).
- Se stai aprendo un caso per un sistema ONTAP con un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

### Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Nella pagina **risorse**, scegliere una delle opzioni disponibili in supporto tecnico:
  - a. Selezionare **Chiamateci** se si desidera parlare con qualcuno al telefono. Viene visualizzata una pagina su netapp.com che elenca i numeri di telefono che è possibile chiamare.
  - b. Selezionare **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp:
    - **Servizio:** Selezionare il servizio a cui è associato il problema. Ad esempio, BlueXP quando si tratta di un problema di supporto tecnico relativo a flussi di lavoro o funzionalità all'interno del servizio.
    - **Ambiente di lavoro:** Se applicabile allo storage, selezionare **Cloud Volumes ONTAP** o **on-premise** e quindi l'ambiente di lavoro associato.

L'elenco degli ambienti di lavoro rientra nell'ambito dell'account, dell'area di lavoro e del connettore BlueXP selezionato nel banner superiore del servizio.
    - **Priorità caso:** Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

Per ulteriori informazioni su queste priorità, passare il mouse sull'icona delle informazioni accanto al nome del campo.
    - **Descrizione del problema:** Fornire una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o procedure di risoluzione dei problemi che sono state eseguite.
    - **Indirizzi e-mail aggiuntivi:** Inserisci indirizzi e-mail aggiuntivi se desideri informare qualcun altro del problema.

- **Allegato (opzionale):** Carica fino a cinque allegati, uno alla volta.

Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

The screenshot shows a web form titled "ntapitdemo" with a sub-header "NetApp Support Site Account". The form contains several sections: "Service" and "Working Enviroment" (note the typo) each with a "Select" dropdown menu; "Case Priority" with a dropdown menu showing "Low - General guidance" and an information icon; "Issue Description" with a large text area containing the placeholder "Provide detailed description of problem, applicable error messages and troubleshooting steps taken."; "Additional Email Addresses (Optional)" with a text input field labeled "Type here" and an information icon; and "Attachment (Optional)" with a file selection area showing "No files selected", an "Upload" button with an upward arrow icon, an information icon, and a trash can icon.

### Al termine

Viene visualizzata una finestra a comparsa con il numero del caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei casi di supporto, selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "Crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzare i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso per il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società di registrazione a cui è associato non sono la stessa società di registrazione per il numero di serie dell'account BlueXP (ad es. 960xxxx) o il numero di serie dell'ambiente di lavoro. È possibile richiedere assistenza utilizzando una delle seguenti opzioni:

- Utilizza la chat integrata nel prodotto
- Inviare un caso non tecnico all'indirizzo <https://mysupport.netapp.com/site/help>

## Gestire i casi di supporto (anteprima)

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente da BlueXP. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

La gestione del caso è disponibile come anteprima. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

Tenere presente quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS dell'utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base all'account NSS dell'utente.

I risultati della tabella riflettono i casi correlati alla vista selezionata.

- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

Per ulteriori informazioni, consulta la procedura riportata di seguito.

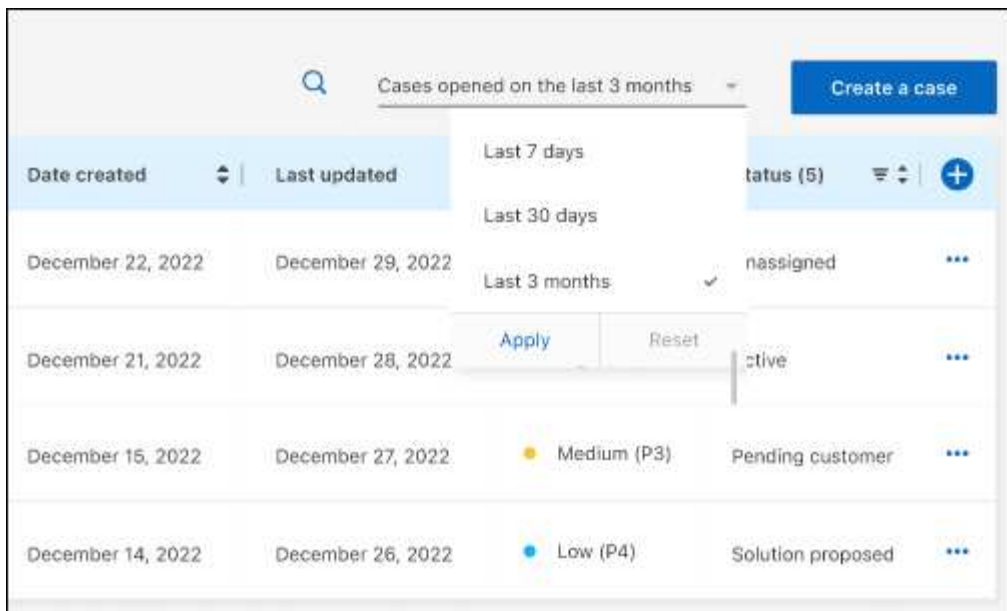
- A livello di caso, offriamo la possibilità di aggiornare le note del caso o chiudere un caso che non è già in stato chiuso o in attesa di chiusura.

### Fasi

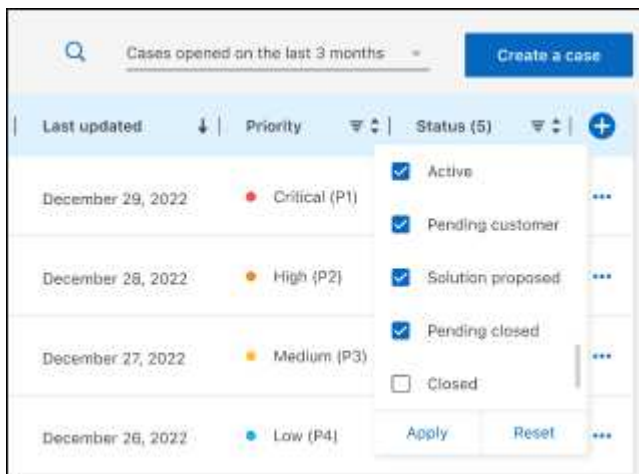
1. In BlueXP, selezionare **Guida > supporto**.
2. Selezionare **Gestione casi** e, se richiesto, aggiungere l'account NSS a BlueXP.


La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.

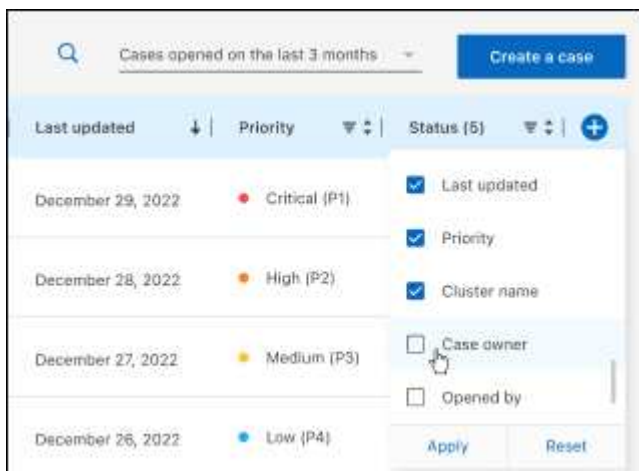
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
  - In **Organization's Cases** (casi dell'organizzazione), selezionare **View** (Visualizza) per visualizzare tutti i casi associati alla società.
  - Modificare l'intervallo di date scegliendo un intervallo di date esatto o scegliendo un intervallo di tempo diverso.



- Filtrare il contenuto delle colonne.



- Modificare le colonne visualizzate nella tabella selezionando  e quindi scegliere le colonne che si desidera visualizzare.

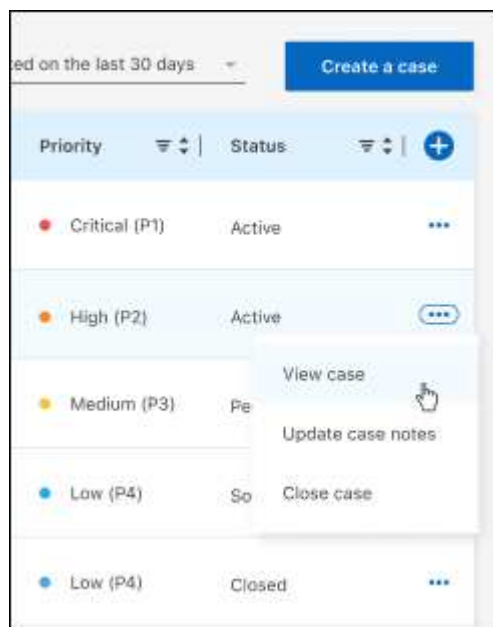


4. Gestire un caso esistente selezionando ... e selezionando una delle opzioni disponibili:

- **Visualizza caso:** Visualizza tutti i dettagli relativi a un caso specifico.
- **Aggiorna note sul caso:** Fornisci ulteriori dettagli sul problema oppure seleziona **carica file** per allegare fino a un massimo di cinque file.

Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

- **Chiudi caso:** Fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.



# Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

## Copyright

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

## Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

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

## Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

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

## Direttiva sulla privacy

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

## Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

["Avviso per BlueXP"](#)



## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.