



Documentación de los clústeres de Kubernetes

Kubernetes clusters

NetApp
April 16, 2024

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

Tabla de contenidos

Documentación de los clústeres de Kubernetes	1
Novedades de Kubernetes en BlueXP	2
02 de abril de 2023	2
05 de marzo de 2023	2
06 de noviembre de 2022	2
18 de septiembre de 2022	2
31 de julio de 2022	2
3 de julio de 2022	2
6 de junio de 2022	3
4 de mayo de 2022	3
4 de abril de 2022	3
27 de febrero de 2022	3
11 de enero de 2022	3
28 de noviembre de 2021	4
Manos a la obra	5
Gestión de datos de Kubernetes en BlueXP	5
Comience a usar los clústeres de Kubernetes	6
Requisitos	7
Requisitos para clústeres de Kubernetes en AWS	7
Requisitos para clústeres de Kubernetes en Azure	16
Requisitos para los clústeres de Kubernetes en Google Cloud	24
Requisitos para clústeres de Kubernetes en OpenShift	31
Añada clústeres de Kubernetes	40
Añada un clúster de Amazon Kubernetes a BlueXP	40
Añada un clúster de Azure Kubernetes a BlueXP	42
Añada un clúster de Google Cloud Kubernetes a BlueXP	45
Importe un clúster OpenShift a BlueXP	49
Gestione clústeres de Kubernetes	51
Gestione Astra Trident	51
Gestione las clases de almacenamiento	53
Vea los volúmenes persistentes	57
Quite los clústeres de Kubernetes del espacio de trabajo	57
Use los servicios de datos en el cloud de NetApp con clústeres de Kubernetes	58
Conocimiento y apoyo	60
Regístrese para recibir soporte	60
Obtenga ayuda	64
Avisos legales	70
Derechos de autor	70
Marcas comerciales	70
Estadounidenses	70
Política de privacidad	70
Código abierto	70

Documentación de los clústeres de Kubernetes

Novedades de Kubernetes en BlueXP

Descubre las novedades de Kubernetes en BlueXP.

02 de abril de 2023

- Ahora puede hacerlo ["Desinstale Astra Trident"](#) Que se instaló con el operador Trident o BlueXP.
- Se han realizado mejoras en la interfaz de usuario y se han actualizado las capturas de pantalla en la documentación.

05 de marzo de 2023

- Kubernetes en BlueXP ahora es compatible con Astra Trident 23.01.
- Se han realizado mejoras en la interfaz de usuario y se han actualizado las capturas de pantalla en la documentación.

06 de noviembre de 2022

Cuando ["definición de clases de almacenamiento"](#), ahora puede habilitar la economía de clase de almacenamiento para el almacenamiento de bloques o sistemas de ficheros.

18 de septiembre de 2022

Ahora puede importar clústeres de OpenShift autogestionados a Cloud Manager.

- ["Requisitos para clústeres de Kubernetes en OpenShift"](#)
- ["Importe un clúster de OpenShift a Cloud Manager"](#)

31 de julio de 2022

- Usando el nuevo `watch` verbo en la clase de almacenamiento, backup y restauración de configuraciones YAML, Cloud Manager ahora puede supervisar los clústeres de Kubernetes en busca de cambios realizados en el back-end del clúster y habilitar automáticamente el backup para nuevos volúmenes persistentes si se configuró el backup automático en el clúster.

["Requisitos para clústeres de Kubernetes en AWS"](#)

["Requisitos para clústeres de Kubernetes en Azure"](#)

["Requisitos para los clústeres de Kubernetes en Google Cloud"](#)

- Cuando ["definición de clases de almacenamiento"](#), ahora puede especificar un tipo de sistema de archivos (fstype) para el almacenamiento de bloques.

3 de julio de 2022

- Si se puso en marcha Astra Trident con el operador Trident, ahora puede actualizar a la última versión de Astra Trident mediante Cloud Manager.

["Instalar y gestionar Astra Trident"](#)

- Ahora puede arrastrar su clúster de Kubernetes y colocarlo en el entorno de trabajo AWS FSX para ONTAP y añadir una clase de almacenamiento directamente desde el lienzo.

["Añada la clase de almacenamiento"](#)

6 de junio de 2022

Cloud Manager ahora admite Amazon FSX para ONTAP como almacenamiento back-end.

4 de mayo de 2022

Arrastre y suelte para añadir clase de almacenamiento

Ahora puede arrastrar su clúster de Kubernetes y soltarlo al entorno de trabajo de Cloud Volumes ONTAP para añadir una clase de almacenamiento directamente desde el lienzo.

["Añada la clase de almacenamiento"](#)

4 de abril de 2022

Gestione clústeres de Kubernetes usando la página de recursos Cloud Manager

La gestión del clúster de Kubernetes ahora ha mejorado la integración directamente desde el entorno de trabajo de clústeres. Un nuevo ["Inicio rápido"](#) le pone en marcha rápidamente.

Ahora puede realizar las siguientes acciones desde la página de recursos del clúster.

- ["Instale Astra Trident"](#)
- ["Añada clases de almacenamiento"](#)
- ["Vea los volúmenes persistentes"](#)
- ["Quite los clústeres"](#)
- ["Habilitar los servicios de datos"](#)

27 de febrero de 2022

Compatibilidad con clústeres de Kubernetes en Google Cloud

Ahora puede añadir y gestionar clústeres gestionados de Google Kubernetes Engine (GKE) y clústeres de Kubernetes autogestionados en Google Cloud mediante Cloud Manager.

["Descubra cómo empezar a utilizar los clústeres de Kubernetes en Google Cloud"](#).

11 de enero de 2022

Compatibilidad con clústeres de Kubernetes en Azure

Ahora puede añadir y gestionar clústeres gestionados de Azure Kubernetes (AKS) y clústeres de Kubernetes autogestionados en Azure usando Cloud Manager.

["Introducción a los clústeres de Kubernetes en Azure"](#)

28 de noviembre de 2021

Compatibilidad con clústeres de Kubernetes en AWS

Ahora puede añadir sus clústeres de Kubernetes gestionados a Canvas de Cloud Manager para una gestión de datos avanzada.

- Descubra los clústeres de Amazon EKS
- Realice backups de volúmenes persistentes mediante Cloud Backup

["Obtenga más información sobre la compatibilidad con Kubernetes"](#).



El servicio Kubernetes existente (disponible a través de la pestaña **K8s**) ha sido obsoleto y se eliminará en una versión futura.

Manos a la obra

Gestión de datos de Kubernetes en BlueXP

Astra Trident es un proyecto de código abierto totalmente compatible y mantenido por NetApp. Astra Trident se integra de forma nativa con Kubernetes y su marco de trabajo de volumen persistente para aprovisionar y gestionar volúmenes sin problemas desde sistemas que ejecutan cualquier combinación de plataformas de almacenamiento de NetApp. ["Más información sobre Trident"](#).

Funciones

Uso ["BlueXP"](#) Además, una versión compatible de Astra Trident puesta en marcha con el operador Trident, podrá:

- Añada y gestione clústeres de Kubernetes
- ["Instalar, actualizar o desinstalar Astra Trident"](#)
- ["Añada y elimine clases de almacenamiento"](#)
- ["Vea los volúmenes persistentes"](#)
- ["Quite los clústeres de Kubernetes"](#) desde el espacio de trabajo
- ["Activa o visualiza el backup y la recuperación de BlueXP"](#)

Puestas en marcha de Kubernetes compatibles

BlueXP admite clústeres de Kubernetes gestionados que se ejecutan en:

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

Compatible con las puestas en marcha de Astra Trident

Una de las cuatro versiones más recientes de Astra Trident ["Se implementa mediante el operador Trident"](#) es obligatorio.



Astra Trident puso en marcha con `tridentctl` no es compatible. Si puso en marcha Astra Trident con `tridentctl`, No puede utilizar BlueXP para administrar los clústeres de Kubernetes. Debe y volver a instalar ["Utilice el operador Trident"](#) o. ["Uso de BlueXP"](#).

Puede instalar Astra Trident o actualizar a una versión compatible directamente desde BlueXP.

["Revise los requisitos previos de Astra Trident"](#)

Almacenamiento back-end compatible

NetApp Astra Trident debe instalarse en cada clúster de Kubernetes y Cloud Volumes ONTAP o Amazon FSX para ONTAP deben configurarse como almacenamiento de back-end para los clústeres.

Coste

Discover sus clústeres de Kubernetes en BlueXP, pero se le cobrará al realizar backup de los volúmenes persistentes mediante Cloud Backup Service.

Comience a usar los clústeres de Kubernetes

Uso **"BlueXP"** Puede empezar a gestionar los clústeres de Kubernetes en solo unos pasos.

1

Revise los requisitos previos

Compruebe que el entorno cumpla los requisitos previos del tipo de clúster.

["Requisitos para clústeres de Kubernetes en AWS"](#)

["Requisitos para clústeres de Kubernetes en Azure"](#)

["Requisitos para los clústeres de Kubernetes en Google Cloud"](#)

2

Añada sus clústeres de Kubernetes a BlueXP

Puede añadir clústeres de Kubernetes y conectarlos a un entorno de trabajo mediante BlueXP.

["Añada un clúster de Amazon Kubernetes"](#)

["Añada un clúster de Azure Kubernetes"](#)

["Añada un clúster de Google Cloud Kubernetes"](#)

3

Inicie el aprovisionamiento de volúmenes persistentes

Solicite y gestione volúmenes persistentes mediante construcciones e interfaces de Kubernetes nativas. BlueXP crea clases de almacenamiento NFS e iSCSI que puede utilizar al aprovisionar volúmenes persistentes.

["Más información sobre el aprovisionamiento de su primer volumen con Astra Trident"](#).

4

Gestione sus clústeres mediante BlueXP

Después de añadir clústeres de Kubernetes a BlueXP, puede gestionar los clústeres desde la página de recursos BlueXP.

["Descubra cómo gestionar los clústeres de Kubernetes."](#)

Requisitos

Requisitos para clústeres de Kubernetes en AWS

Puede añadir clústeres gestionados de Amazon Elastic Kubernetes Service (EKS) o clústeres de Kubernetes autogestionados en AWS a BlueXP. Antes de poder añadir los clústeres a BlueXP, debe asegurarse de que se cumplen los siguientes requisitos.



En este tema se utiliza *Kubernetes cluster*, donde la configuración es la misma para EKS y clústeres de Kubernetes autogestionados. El tipo de clúster se especifica dónde difiere la configuración.

Requisitos

Astra Trident

Se requiere una de las cuatro versiones más recientes de Astra Trident. Puede instalar o actualizar Astra Trident directamente desde BlueXP. Usted debe ["revise los requisitos previos"](#) Antes de instalar Astra Trident.

Cloud Volumes ONTAP

Cloud Volumes ONTAP para AWS debe configurarse como almacenamiento back-end para el clúster. ["Vaya a los documentos de Astra Trident para ver los pasos de configuración"](#).

Conector BlueXP

Debe ejecutarse un conector en AWS con los permisos necesarios. [Más información a continuación](#).

Conectividad de la red

Se requiere conectividad de red entre el clúster de Kubernetes y el conector y entre el clúster de Kubernetes y Cloud Volumes ONTAP. [Más información a continuación](#).

Autorización de RBAC

Debe autorizarse el rol BlueXP Connector en cada clúster de Kubernetes. [Más información a continuación](#).

Prepare un conector

Se requiere un conector BlueXP en AWS para detectar y gestionar clústeres de Kubernetes. Tendrá que crear un conector nuevo o utilizar un conector existente que tenga los permisos necesarios.

Cree un conector nuevo

Siga los pasos de uno de los siguientes enlaces.

- ["Cree un conector desde BlueXP"](#) (recomendado)
- ["Cree un conector desde AWS Marketplace"](#)
- ["Instale el conector en un host Linux existente en AWS"](#)

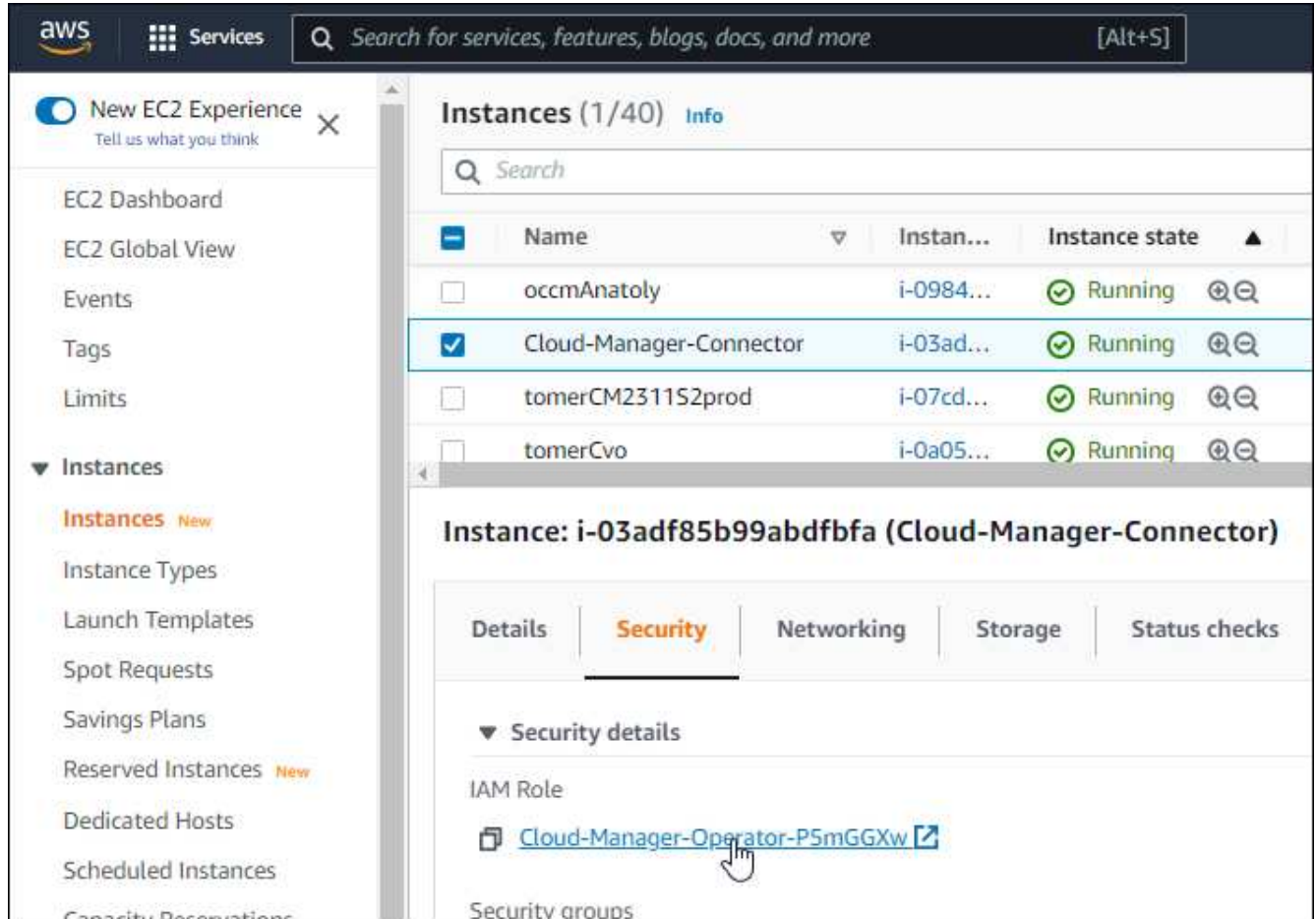
Agregue los permisos necesarios a un conector existente

A partir de la versión 3.9.13, todos los conectores _recién creados incluyen tres nuevos permisos de AWS que

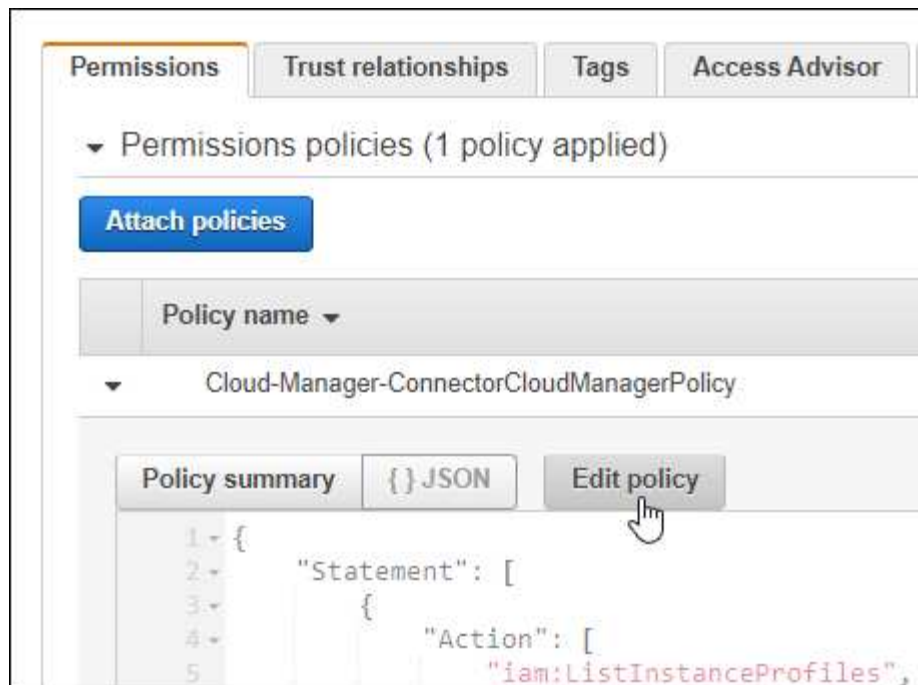
permiten la detección y la gestión de los clústeres de Kubernetes. Si ha creado un conector antes de esta versión, deberá modificar la directiva existente para el rol IAM del conector para proporcionar los permisos.

Pasos

1. Acceda a la consola de AWS y abra el servicio EC2.
2. Seleccione la instancia de conector, haga clic en **Seguridad** y haga clic en el nombre de la función IAM para ver el rol en el servicio IAM.



3. En la ficha **permisos**, expanda la directiva y haga clic en **Editar directiva**.



4. Haga clic en **JSON** y agregue los siguientes permisos en el primer conjunto de acciones:

- ec2:regiones descritas
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

["Vea el formato JSON completo para la política"](#)

5. Haga clic en **revisar directiva** y luego en **Guardar cambios**.

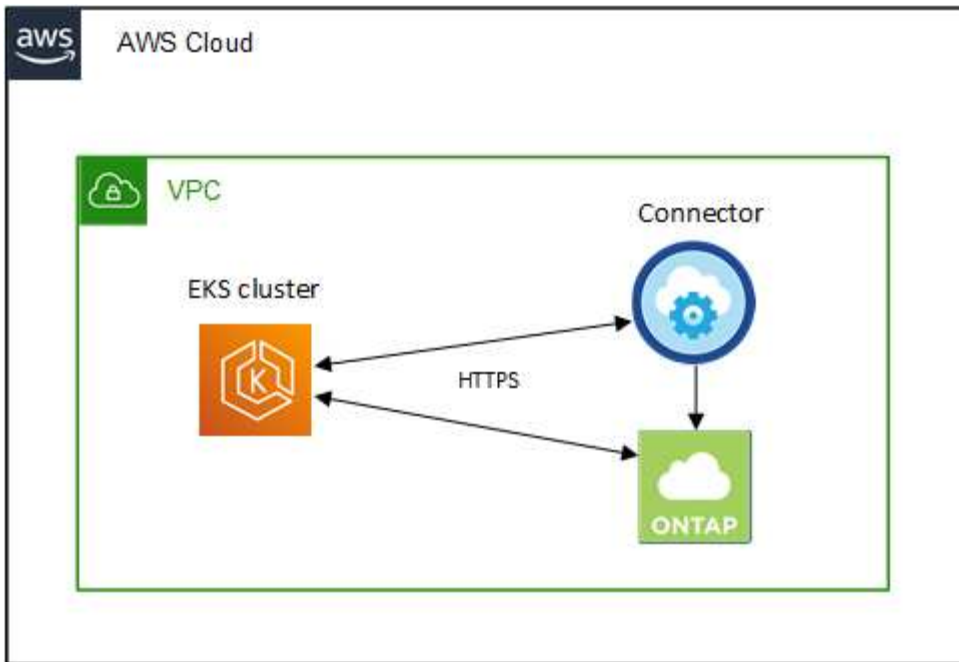
Revise los requisitos de red

Debe proporcionar conectividad de red entre el clúster de Kubernetes y el conector, y entre el clúster de Kubernetes y el sistema Cloud Volumes ONTAP que proporciona almacenamiento de back-end al clúster.

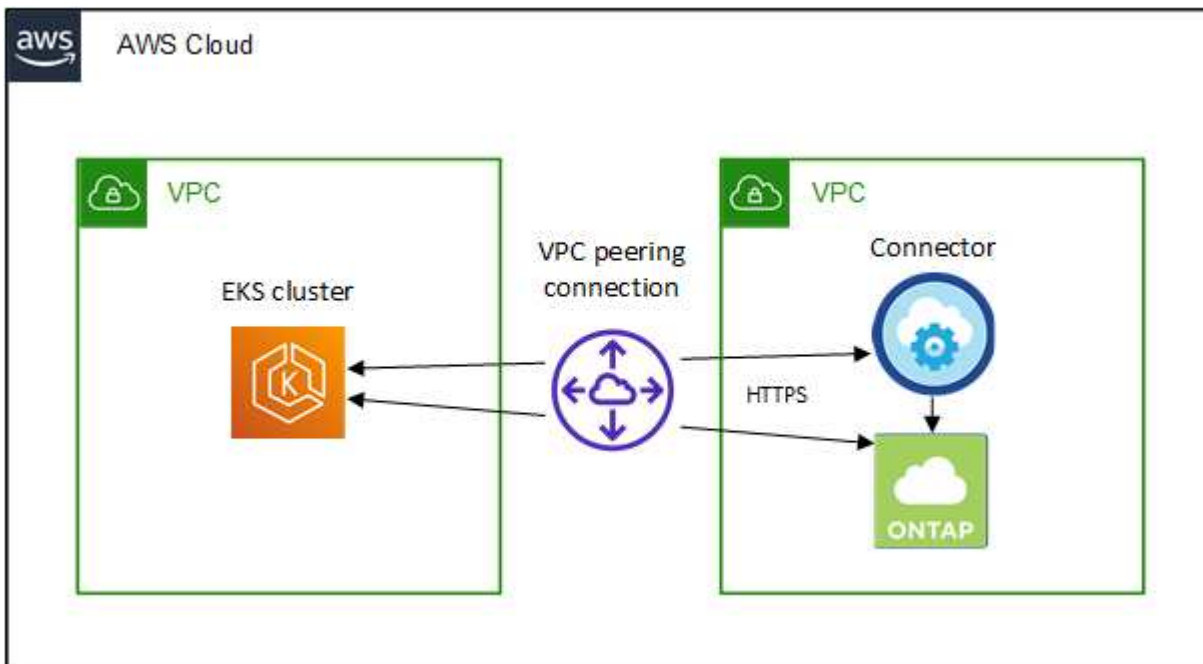
- Cada clúster de Kubernetes debe tener una conexión entrante desde el conector
- El conector debe tener una conexión de salida a cada clúster de Kubernetes a través del puerto 443

La forma más sencilla de proporcionar esta conectividad es poner en marcha el conector y Cloud Volumes ONTAP en el mismo VPC que el clúster de Kubernetes. De lo contrario, deberá configurar una conexión VPC peering entre los distintos VPC.

Aquí hay un ejemplo que muestra cada componente en el mismo VPC.



En este otro ejemplo se muestra un clúster de EKS que se ejecuta en un VPC diferente. En este ejemplo, VPC peering proporciona una conexión entre el VPC del clúster de EKS y el VPC del conector y Cloud Volumes ONTAP.



Configure la autorización de RBAC

Debe autorizar el rol de conector en cada clúster de Kubernetes para que el conector pueda detectar y gestionar un clúster.

Se requiere una autorización diferente para habilitar diferentes funciones.

Backup y restauración

El backup y la restauración solo necesitan una autorización básica.

Añada clases de almacenamiento

Se requiere una autorización ampliada para añadir clases de almacenamiento mediante BlueXP y supervisar el clúster en busca de cambios en el back-end.

Instale la trident

Debe proporcionar una autorización completa para que BlueXP instale Astra Trident.



Cuando se instala Astra Trident, BlueXP instala el secreto de Kubernetes y back-end de Astra Trident que contiene las credenciales que Astra Trident necesita para comunicarse con el clúster de almacenamiento.

Pasos

1. Cree una función y un enlace de roles del clúster.
 - a. Puede personalizar la autorización en función de sus requisitos.

Backup/restauración

Añada una autorización básica para habilitar el backup y la restauración para los clústeres de 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

```

Clases de almacenamiento

Agregue autorización expandida para agregar clases de almacenamiento con 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

```


Instalación de Trident

Utilice la línea de comandos para proporcionar autorización completa y habilitar BlueXP para instalar Astra Trident.

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

b. Aplique la configuración a un clúster.

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

2. Cree una asignación de identidad al grupo de permisos.

Utilice eksctl

Utilice eksctl para crear una asignación de identidad IAM entre un clúster y la función IAM del conector BlueXP.

["Vaya a la documentación de eksctl para obtener instrucciones completas".](#)

A continuación se muestra un ejemplo.

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

Editar autenticación de aws

Edite directamente ConfigMap de AWS-auth para agregar acceso de RBAC a la función IAM para el conector BlueXP.

["Vaya a la documentación de AWS EKS para obtener instrucciones completas".](#)

A continuación se muestra un ejemplo.

```
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
```

Requisitos para clústeres de Kubernetes en Azure

Puede añadir y gestionar clústeres de Kubernetes de Azure (AKS) gestionados y clústeres de Kubernetes autogestionados en Azure usando BlueXP. Antes de poder añadir los clústeres a BlueXP, asegúrese de que se cumplan los siguientes requisitos.



En este tema se utiliza *Kubernetes cluster*, donde la configuración es la misma para AKS y clústeres de Kubernetes autogestionados. El tipo de clúster se especifica dónde difiere la configuración.

Requisitos

Astra Trident

Se requiere una de las cuatro versiones más recientes de Astra Trident. Puede instalar o actualizar Astra Trident directamente desde BlueXP. Usted debe ["revise los requisitos previos"](#) Antes de instalar Astra Trident.

Cloud Volumes ONTAP

Cloud Volumes ONTAP debe configurarse como almacenamiento back-end para el clúster. ["Vaya a los documentos de Astra Trident para ver los pasos de configuración"](#).

Conector BlueXP

Un conector debe ejecutarse en Azure con los permisos necesarios. [Más información a continuación.](#)

Conectividad de la red

Se requiere conectividad de red entre el clúster de Kubernetes y el conector y entre el clúster de Kubernetes y Cloud Volumes ONTAP. [Más información a continuación.](#)

Autorización de RBAC

BlueXP admite clústeres habilitados para RBAC con y sin Active Directory. Debe autorizarse el rol BlueXP Connector en cada clúster de Azure. [Más información a continuación.](#)

Prepare un conector

Se necesita un conector BlueXP en Azure para detectar y gestionar clústeres de Kubernetes. Tendrá que crear un conector nuevo o utilizar un conector existente que tenga los permisos necesarios.

Cree un conector nuevo

Siga los pasos de uno de los siguientes enlaces.

- ["Cree un conector desde BlueXP"](#) (recomendado)
- ["Cree un conector desde Azure Marketplace"](#)
- ["Instale el conector en un host Linux existente"](#)

Agregar los permisos necesarios a un conector existente (para detectar un clúster AKS gestionado)

Si desea detectar un clúster AKS gestionado, puede que necesite modificar la función personalizada para que Connector proporcione los permisos.

Pasos

1. Identifique la función asignada a la máquina virtual conector:
 - a. En el portal de Azure, abra el servicio Virtual Machines.
 - b. Seleccione la máquina virtual conector.
 - c. En Configuración, seleccione **identidad**.

- d. Haga clic en **asignaciones de roles de Azure**.
 - e. Anote la función personalizada asignada a la máquina virtual conector.
2. Actualice el rol personalizado:
- a. En el portal de Azure, abra su suscripción a Azure.
 - b. Haga clic en **Control de acceso (IAM) > roles**.
 - c. Haga clic en los puntos suspensivos (...). Para la función personalizada y, a continuación, haga clic en **Editar**.
 - d. Haga clic en JSON y añada los siguientes permisos:

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

- e. Haga clic en **revisar + actualizar** y, a continuación, haga clic en **Actualizar**.

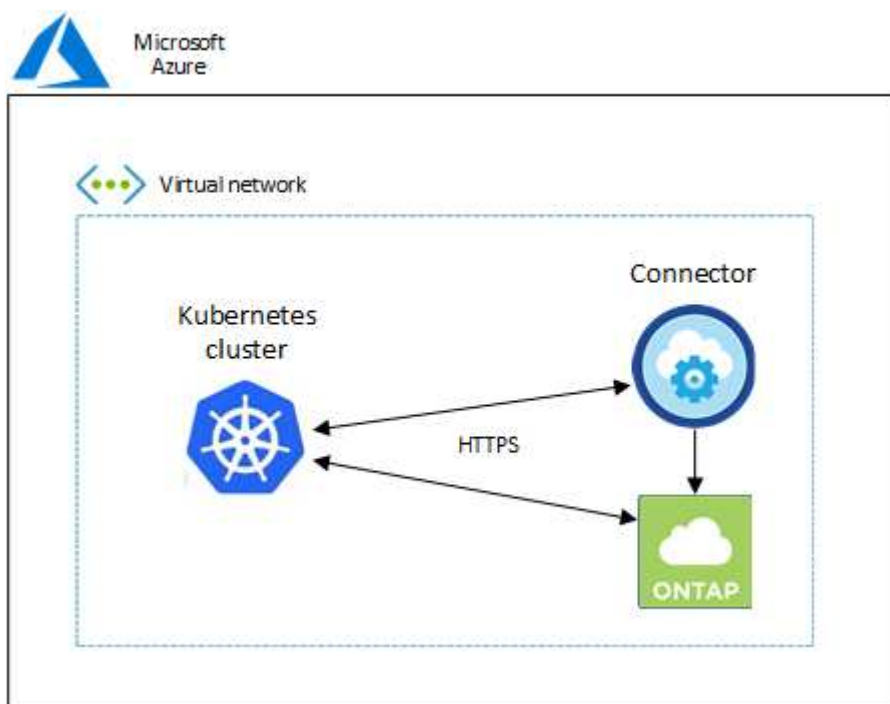
Revise los requisitos de red

Debe proporcionar conectividad de red entre el clúster de Kubernetes y el conector, y entre el clúster de Kubernetes y el sistema Cloud Volumes ONTAP que proporciona almacenamiento de back-end al clúster.

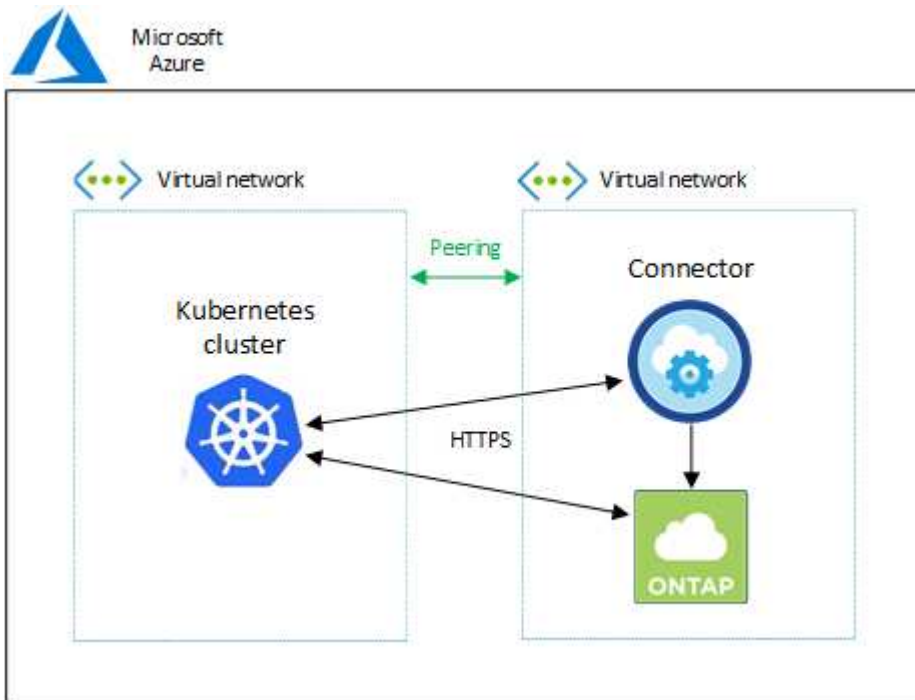
- Cada clúster de Kubernetes debe tener una conexión entrante desde el conector
- El conector debe tener una conexión de salida a cada clúster de Kubernetes a través del puerto 443

La forma más sencilla de proporcionar esta conectividad es poner en marcha el conector y Cloud Volumes ONTAP en la misma red que el clúster de Kubernetes. De lo contrario, debe configurar una conexión de interconexión entre los distintos VNets.

A continuación se muestra un ejemplo que muestra cada componente en el mismo vnet.



Y este es otro ejemplo que muestra un clúster Kubernetes que se ejecuta en un vnet diferente. En este ejemplo, peering proporciona una conexión entre el vnet del clúster de Kubernetes y el vnet del conector y Cloud Volumes ONTAP.



Configure la autorización de RBAC

La validación de RBAC solo se produce en clústeres de Kubernetes con Active Directory (AD) habilitado. Los clústeres de Kubernetes sin AD pasarán la validación automáticamente.

Es necesario autorizar el rol de conector en cada clúster de Kubernetes para que el conector pueda detectar y gestionar un clúster.

Backup y restauración

El backup y la restauración solo necesitan una autorización básica.

Añada clases de almacenamiento

Se requiere una autorización ampliada para añadir clases de almacenamiento mediante BlueXP y supervisar el clúster en busca de cambios en el back-end.

Instale la trident

Debe proporcionar una autorización completa para que BlueXP instale Astra Trident.



Cuando se instala Astra Trident, BlueXP instala el secreto de Kubernetes y back-end de Astra Trident que contiene las credenciales que Astra Trident necesita para comunicarse con el clúster de almacenamiento.

Antes de empezar

Su RBAC subjects: name: La configuración varía ligeramente según el tipo de clúster de Kubernetes.

- Si va a implementar un clúster **AKS gestionado**, necesita el identificador de objeto para la identidad administrada asignada por el sistema para el conector. Este ID está disponible en el portal de gestión de

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

- Si va a implementar un **clúster Kubernetes autogestionado**, necesita el nombre de usuario de cualquier usuario autorizado.

Pasos

Cree una función y un enlace de roles del clúster.

1. Puede personalizar la autorización en función de sus requisitos.

Backup/restauración

Añada una autorización básica para habilitar el backup y la restauración para los clústeres de Kubernetes.

Sustituya el `subjects: kind: variable` con su nombre de usuario y. `subjects: name:` Con el ID de objeto para la identidad administrada asignada por el sistema o el nombre de usuario de cualquier usuario autorizado como se ha descrito anteriormente.

```
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

```

Clases de almacenamiento

Agregue autorización expandida para agregar clases de almacenamiento con BlueXP.

Sustituya el `subjects: kind: variable` con su nombre de usuario y `subjects: user:` Con el ID de objeto para la identidad administrada asignada por el sistema o el nombre de usuario de cualquier usuario autorizado como se ha descrito anteriormente.

```

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
```

Instalación de Trident

Utilice la línea de comandos para proporcionar autorización completa y habilitar BlueXP para instalar Astra Trident.

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

2. Aplique la configuración a un clúster.

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

Requisitos para los clústeres de Kubernetes en Google Cloud

Puede añadir y gestionar clústeres gestionados de Google Kubernetes Engine (GKE) y clústeres de Kubernetes autogestionados en Google mediante BlueXP. Antes de poder añadir los clústeres a BlueXP, asegúrese de que se cumplan los siguientes requisitos.



En este tema se utiliza *Kubernetes cluster*, donde la configuración es la misma para los clústeres GKE y Kubernetes autogestionados. El tipo de clúster se especifica dónde difiere la configuración.

Requisitos

Astra Trident

Se requiere una de las cuatro versiones más recientes de Astra Trident. Puede instalar o actualizar Astra Trident directamente desde BlueXP. Usted debe ["revise los requisitos previos"](#) Antes de instalar Astra Trident

Cloud Volumes ONTAP

Cloud Volumes ONTAP debe estar en BlueXP con la misma cuenta de seguridad, espacio de trabajo y conector que el clúster de Kubernetes. ["Vaya a los documentos de Astra Trident para ver los pasos de configuración"](#).

Conector BlueXP

Un conector debe estar en ejecución en Google con los permisos necesarios. [Más información a continuación](#).

Conectividad de la red

Se requiere conectividad de red entre el clúster de Kubernetes y el conector y entre el clúster de Kubernetes y Cloud Volumes ONTAP. [Más información a continuación.](#)

Autorización de RBAC

BlueXP admite clústeres habilitados para RBAC con y sin Active Directory. La función conector BlueXP debe estar autorizada en cada clúster GKE. [Más información a continuación.](#)

Prepare un conector

Se necesita un conector BlueXP en Google para detectar y gestionar clústeres de Kubernetes. Tendrá que crear un conector nuevo o utilizar un conector existente que tenga los permisos necesarios.

Cree un conector nuevo

Siga los pasos de uno de los siguientes enlaces.

- ["Cree un conector desde BlueXP"](#) (recomendado)
- ["Instale el conector en un host Linux existente"](#)

Agregar los permisos necesarios a un conector existente (para detectar un clúster GKE administrado)

Si desea detectar un clúster GKE administrado, es posible que deba modificar la función personalizada para que Connector proporcione los permisos.

Pasos

1. Pulg ["Consola de cloud"](#), Vaya a la página **roles**.
2. Mediante la lista desplegable situada en la parte superior de la página, seleccione el proyecto o la organización que contiene la función que desea editar.
3. Haga clic en una función personalizada.
4. Haga clic en **Editar rol** para actualizar los permisos del rol.
5. Haga clic en **Agregar permisos** para agregar los siguientes permisos nuevos a la función.

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

6. Haga clic en **Actualizar** para guardar la función editada.

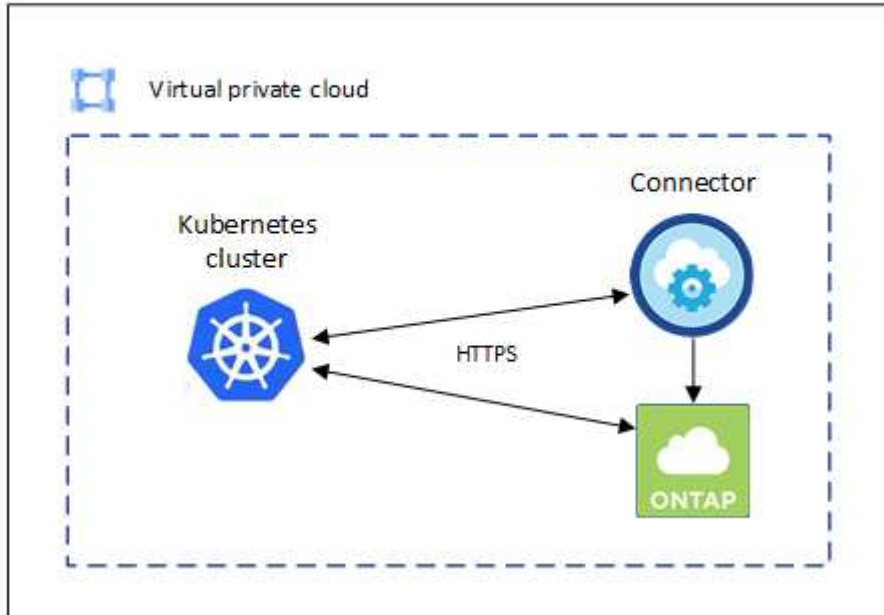
Revise los requisitos de red

Debe proporcionar conectividad de red entre el clúster de Kubernetes y el conector, y entre el clúster de Kubernetes y el sistema Cloud Volumes ONTAP que proporciona almacenamiento de back-end al clúster.

- Cada clúster de Kubernetes debe tener una conexión entrante desde el conector
- El conector debe tener una conexión de salida a cada clúster de Kubernetes a través del puerto 443

La forma más sencilla de proporcionar esta conectividad es poner en marcha el conector y Cloud Volumes ONTAP en el mismo VPC que el clúster de Kubernetes. De lo contrario, deberá configurar una conexión entre iguales entre el VPC diferente.

Aquí hay un ejemplo que muestra cada componente en el mismo VPC.



Configure la autorización de RBAC

La validación de RBAC solo se produce en clústeres de Kubernetes con Active Directory (AD) habilitado. Los clústeres de Kubernetes sin AD pasarán la validación automáticamente.

Es necesario autorizar el rol de conector en cada clúster de Kubernetes para que el conector pueda detectar y gestionar un clúster.

Backup y restauración

El backup y la restauración solo necesitan una autorización básica.

Añada clases de almacenamiento

Se requiere una autorización ampliada para añadir clases de almacenamiento mediante BlueXP y supervisar el clúster en busca de cambios en el back-end.

Instale la trident

Debe proporcionar una autorización completa para que BlueXP instale Astra Trident.



Cuando se instala Astra Trident, BlueXP instala el secreto de Kubernetes y back-end de Astra Trident que contiene las credenciales que Astra Trident necesita para comunicarse con el clúster de almacenamiento.

Antes de empezar

Para configurar `subjects: name:` En el archivo YAML, debe conocer el ID único de BlueXP.

Puede encontrar el ID único de dos maneras:

- Con el comando:

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

- En Detalles de la cuenta de servicio en la "[Consola de 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

Pasos

Cree una función y un enlace de roles del clúster.

1. Puede personalizar la autorización en función de sus requisitos.

Backup/restauración

Añada una autorización básica para habilitar el backup y la restauración para los clústeres de Kubernetes.

Sustituya el `subjects: kind: variable` con su nombre de usuario y `subjects: name:` Con el ID exclusivo para la cuenta de servicio autorizada.

```
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

```

Clases de almacenamiento

Agregue autorización expandida para agregar clases de almacenamiento con BlueXP.

Sustituya el `subjects: kind: variable` con su nombre de usuario y `subjects: user:` Con el ID exclusivo para la cuenta de servicio autorizada.

```

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
```

Instalación de Trident

Utilice la línea de comandos para proporcionar autorización completa y habilitar BlueXP para instalar Astra Trident.

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

2. Aplique la configuración a un clúster.

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

Requisitos para clústeres de Kubernetes en OpenShift

Puede añadir y gestionar clústeres de Kubernetes de OpenShift autogestionados mediante BlueXP. Antes de poder añadir los clústeres a BlueXP, asegúrese de que se cumplan los siguientes requisitos.

Requisitos

Astra Trident

Se requiere una de las cuatro versiones más recientes de Astra Trident. Puede instalar o actualizar Astra Trident directamente desde BlueXP. Usted debe ["revise los requisitos previos"](#) Antes de instalar Astra Trident.

Cloud Volumes ONTAP

Cloud Volumes ONTAP debe configurarse como almacenamiento back-end para el clúster. ["Vaya a los documentos de Astra Trident para ver los pasos de configuración"](#).

Conector BlueXP

Se necesita un conector BlueXP para importar y gestionar clústeres de Kubernetes. Tendrá que crear un nuevo conector o utilizar un conector existente que tenga los permisos necesarios para su proveedor de cloud:

- ["Conector AWS"](#)
- ["Conector de Azure"](#)
- ["Conector de Google Cloud"](#)

Conectividad de la red

Se requiere conectividad de red entre el clúster de Kubernetes y el conector y entre el clúster de

Archivo de configuración de Kubernetes (kubeconfig) con autorización de RBAC

Para importar clústeres OpenShift, necesita un archivo kubeconfig con la autorización RBAC necesaria para habilitar diferentes funcionalidades. [Cree un archivo kubeconfig](#).

- Backup y restauración: El backup y la restauración solo requieren una autorización básica.
- Añadir clases de almacenamiento: Se requiere una autorización ampliada para agregar clases de almacenamiento con BlueXP y supervisar el clúster para realizar cambios en el back-end.
- Instalar Astra Trident: Necesita proporcionar una autorización completa para que BlueXP instale Astra Trident.



Cuando se instala Astra Trident, BlueXP instala el secreto de Kubernetes y back-end de Astra Trident que contiene las credenciales que Astra Trident necesita para comunicarse con el clúster de almacenamiento.

Cree un archivo kubeconfig

Con la CLI de OpenShift, cree un archivo kubeconfig para importarlo a BlueXP.

Pasos

1. Inicie sesión en la CLI de OpenShift mediante `oc login` En una URL pública con un usuario administrativo.
2. Cree una cuenta de servicio del siguiente modo:

- a. Cree un archivo de cuenta de servicio llamado `oc-service-account.yaml`.

Ajuste el nombre y el espacio de nombres según sea necesario. Si se realizan cambios aquí, debe aplicar los mismos cambios en los pasos siguientes.

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

+

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

- a. Aplicar la cuenta de servicio:

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

3. Cree un enlace de funciones personalizado en función de sus requisitos de autorización.

- a. Cree un ClusterRoleBinding archivo llamado `oc-clusterrolebinding.yaml`.

```
oc-clusterrolebinding.yaml
```

- b. Configure la autorización de RBAC según sea necesario para el clúster.

Backup/restauración

Añada una autorización básica para habilitar el backup y la restauración para los clústeres de 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

```

Clases de almacenamiento

Agregue autorización expandida para agregar clases de almacenamiento con 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

```

Instalación de Trident

Conceda la autorización completa de administración y habilite BlueXP para instalar 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. Aplique el enlace de roles del clúster:

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

4. Enumere los secretos de la cuenta de servicio, reemplazando <context> con el contexto correcto para su instalación:

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

El final de la salida debe ser similar a lo siguiente:

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

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `oc-service-account-dockercfg-vhz87` sería 0 y el índice para `oc-service-account-token-r59kr` sería 1. En la salida, anote el índice del nombre de la cuenta de servicio que contiene la palabra "token".

5. Genere la kubeconfig de la siguiente manera:

- Cree un `create-kubeconfig.sh` archivo. Sustituya `TOKEN_INDEX` al principio de la secuencia de comandos siguiente con el valor correcto.

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. Origen de los comandos para aplicarlos al clúster de Kubernetes.

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

Resultado

Utilizará el resultado kubeconfig-sa Archivo para agregar un clúster OpenShift a BlueXP.

Añada clústeres de Kubernetes

Añada un clúster de Amazon Kubernetes a BlueXP

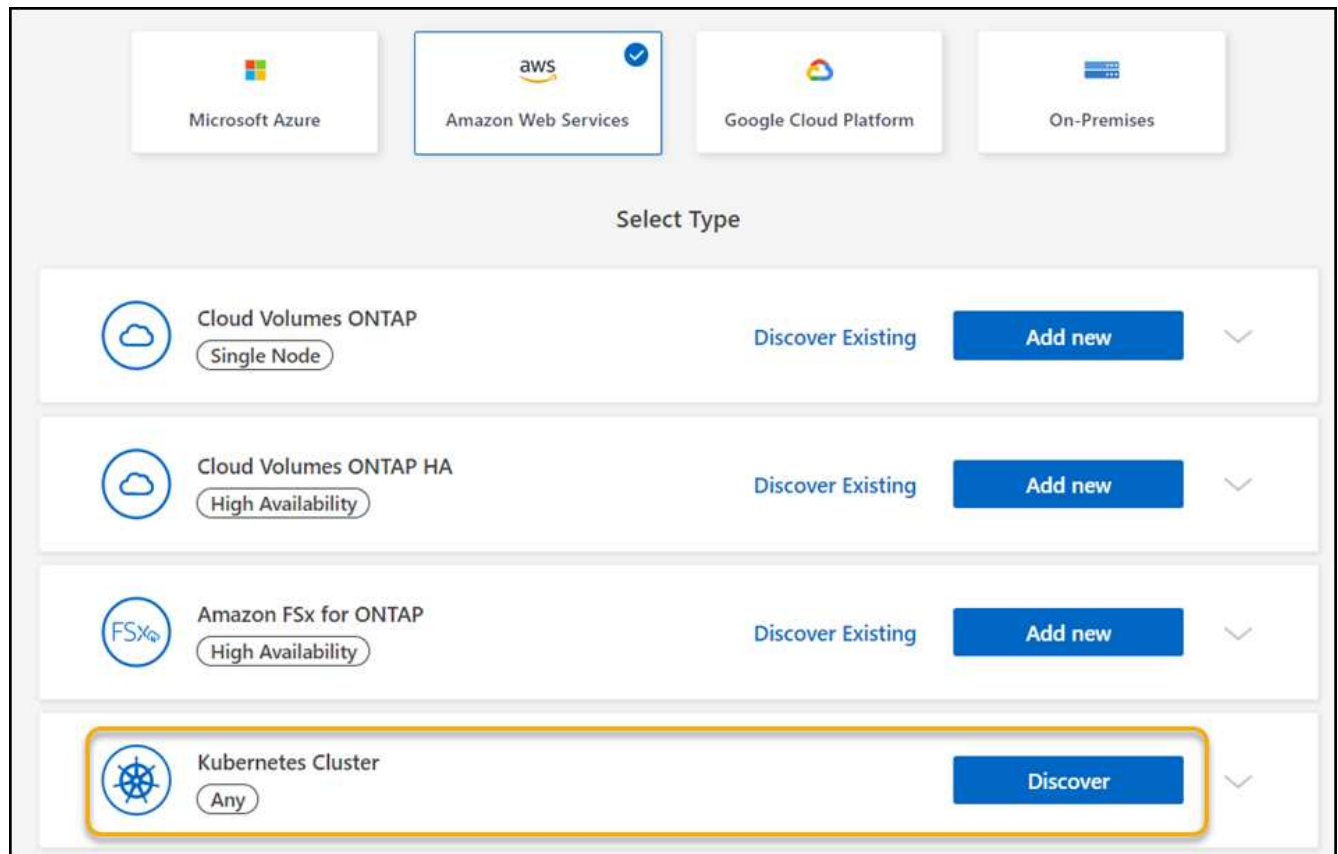
Puede detectar o importar clústeres de Kubernetes en BlueXP para realizar backups de volúmenes persistentes en Amazon S3.

Detectar un clúster

Puede detectar un clúster de Kubernetes totalmente gestionado o autogestionado. Se deben detectar los clústeres gestionados, pero no se pueden importar.

Pasos

1. En **Canvas**, haga clic en **Agregar entorno de trabajo**.
2. Seleccione **Amazon Web Services > clúster Kubernetes > Discover**.



3. Seleccione **Discover Cluster** y haga clic en **Siguiente**.
4. Elija una región de AWS, seleccione un clúster de Kubernetes y haga clic en **Siguiente**.



Resultado

BlueXP añade el clúster Kubernetes al lienzo.

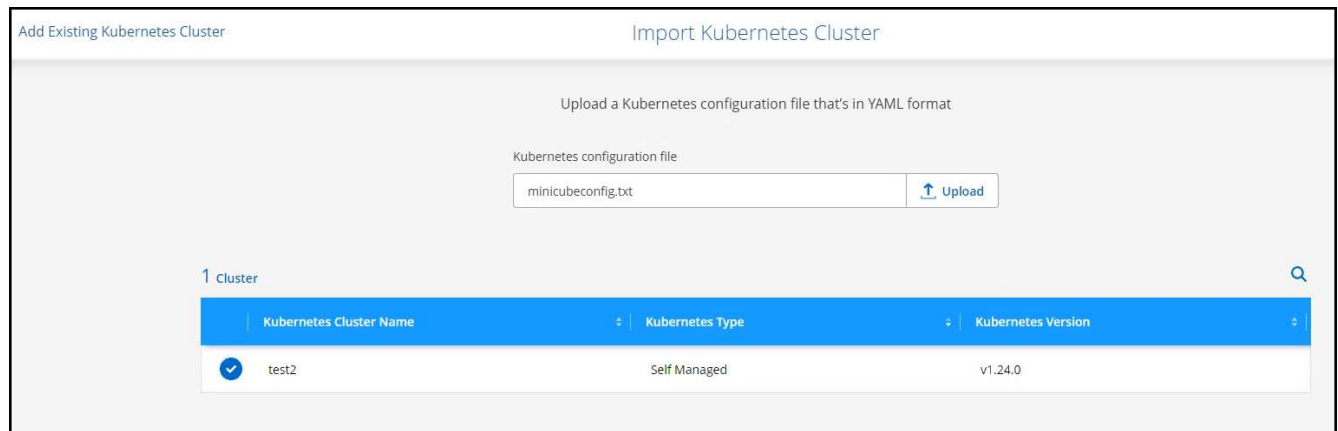


Importe un clúster

Es posible importar un clúster de Kubernetes autogestionado mediante un archivo de configuración de Kubernetes.

Pasos

1. En **Canvas**, haga clic en **Agregar entorno de trabajo**.
2. Seleccione **Amazon Web Services > clúster Kubernetes > Discover**.
3. Seleccione **clúster de importación** y haga clic en **Siguiente**.
4. Cargue un archivo de configuración de Kubernetes en formato YAML.



5. Seleccione el clúster de Kubernetes y haga clic en **Siguiente**.

Resultado

BlueXP añade el clúster Kubernetes al lienzo.

Añada un clúster de Azure Kubernetes a BlueXP

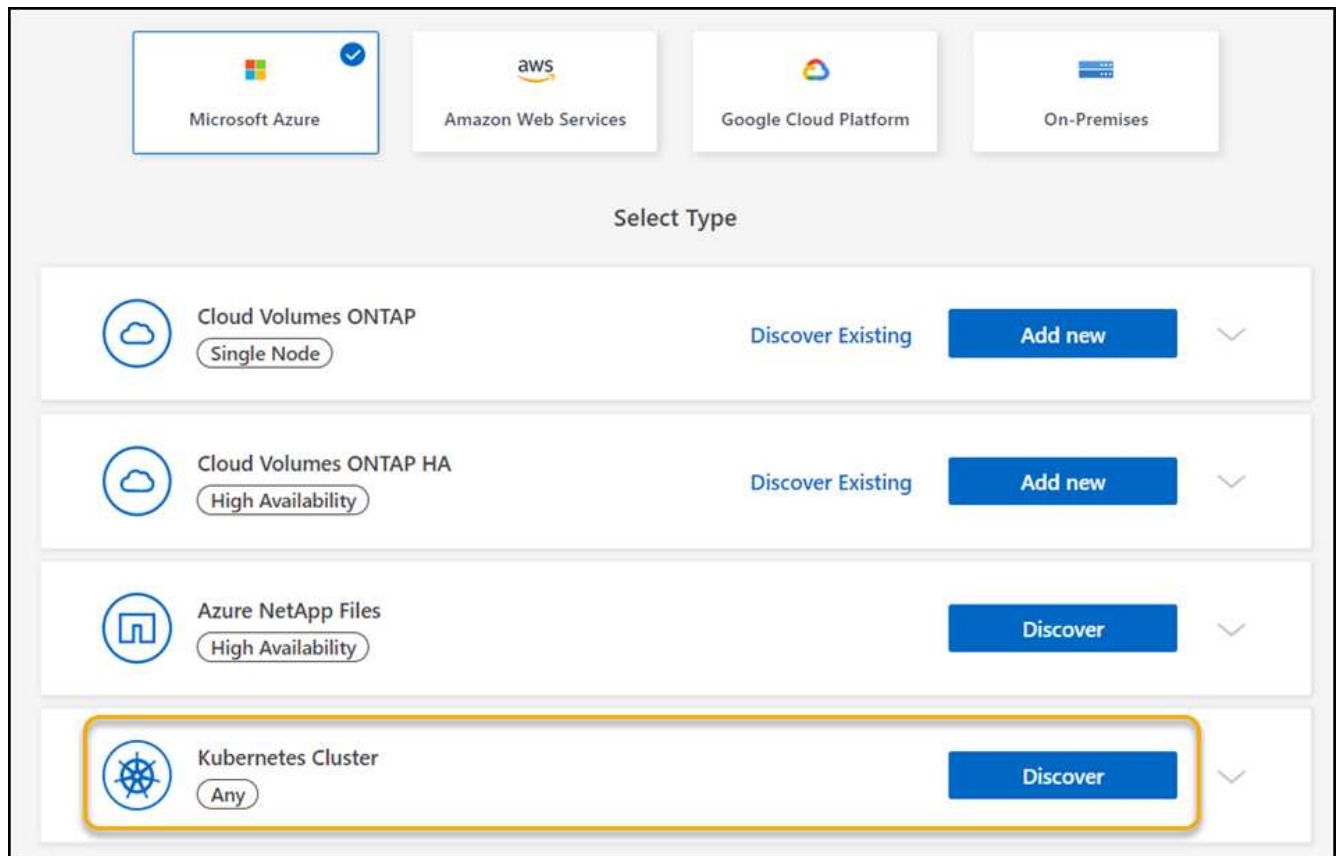
Puede detectar o importar clústeres de Kubernetes en BlueXP para que pueda realizar backups de volúmenes persistentes en Azure.

Detectar un clúster

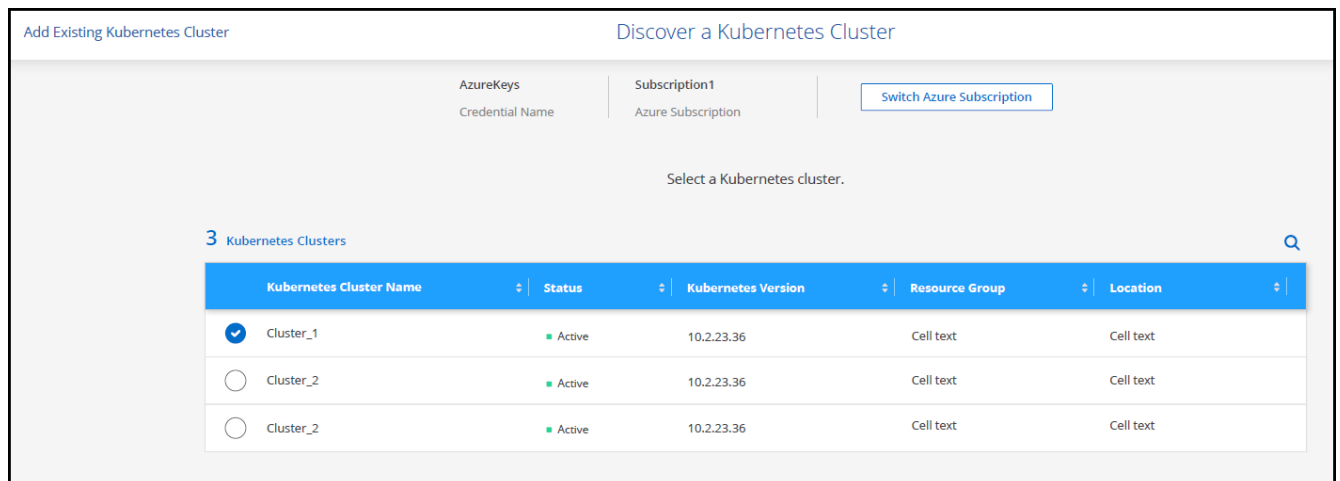
Puede detectar un clúster de Kubernetes totalmente gestionado o autogestionado. Se deben detectar los clústeres gestionados, pero no se pueden importar.

Pasos

1. En **Canvas**, haga clic en **Agregar entorno de trabajo**.
2. Seleccione **Microsoft Azure > clúster Kubernetes > Discover**.

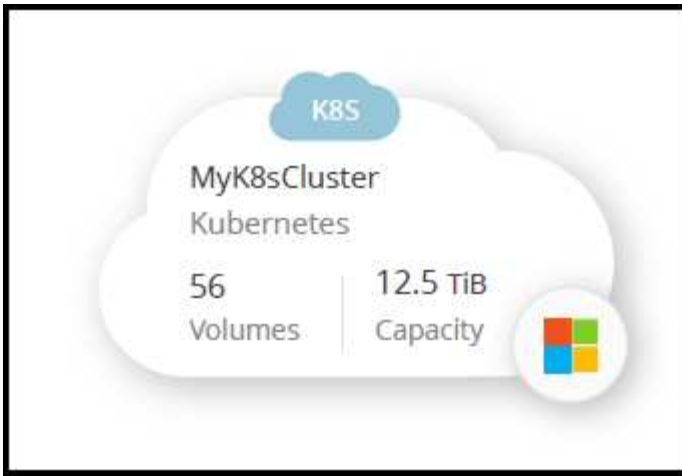


3. Seleccione **Discover Cluster** y haga clic en **Siguiente**.
4. Seleccione un clúster de Kubernetes y haga clic en **Siguiente**.



Resultado

BlueXP añade el clúster Kubernetes al lienzo.



Importe un clúster

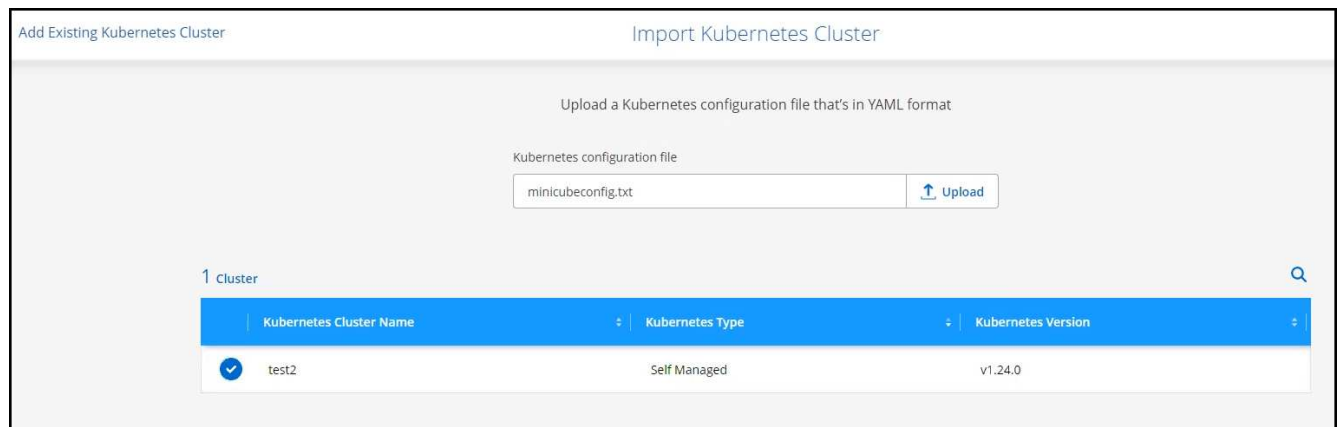
Es posible importar un clúster de Kubernetes autogestionado mediante un archivo de configuración de Kubernetes.

Antes de empezar

Necesitará certificados de entidad de certificación, clave de cliente y certificado de cliente para el usuario especificado en el archivo YAML de rol de clúster para importar clústeres de Kubernetes. El administrador del clúster de Kubernetes recibe estas certificaciones cuando se crean usuarios en el clúster de Kubernetes.

Pasos

1. En **Canvas**, haga clic en **Agregar entorno de trabajo**.
2. Seleccione **Microsoft Azure > clúster Kubernetes > Discover**.
3. Seleccione **clúster de importación** y haga clic en **Siguiente**.
4. Cargue un archivo de configuración de Kubernetes en formato YAML.



5. Cargue los certificados de clúster proporcionados por el administrador del clúster de 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

Resultado

BlueXP añade el clúster Kubernetes al lienzo.

Añada un clúster de Google Cloud Kubernetes a BlueXP

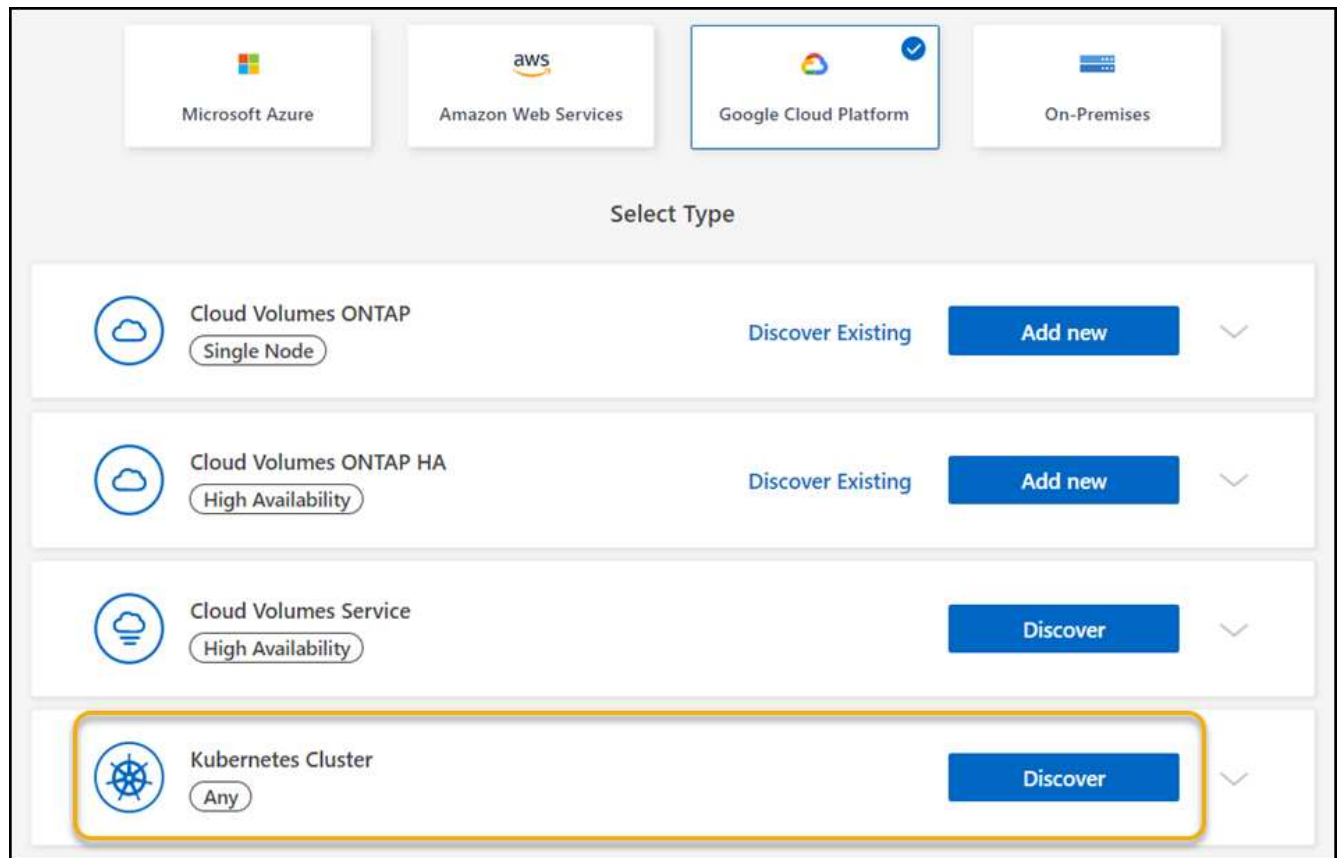
Puede detectar o importar clústeres de Kubernetes en BlueXP para que pueda realizar backups de volúmenes persistentes en Google Cloud.

Detectar un clúster

Puede detectar un clúster de Kubernetes totalmente gestionado o autogestionado. Se deben detectar los clústeres gestionados, pero no se pueden importar.

Pasos

1. En **Canvas**, haga clic en **Agregar entorno de trabajo**.
2. Seleccione **Google Cloud Platform > Kubernetes Cluster > Discover**.



3. Seleccione **Discover Cluster** y haga clic en **Siguiente**.
4. Para seleccionar un clúster de Kubernetes en otro Google Cloud Project, haga clic en **Editar proyecto** y elija un proyecto disponible.



5. Seleccione un clúster de Kubernetes y haga clic en **Siguiente**.



Resultado

BlueXP añade el clúster Kubernetes al lienzo.



Importe un clúster

Es posible importar un clúster de Kubernetes autogestionado mediante un archivo de configuración de Kubernetes.

Antes de empezar

Necesitará certificados de entidad de certificación, clave de cliente y certificado de cliente para el usuario especificado en el archivo YAML de rol de clúster para importar clústeres de Kubernetes. El administrador del clúster de Kubernetes recibe estas certificaciones cuando se crean usuarios en el clúster de Kubernetes.

Pasos

1. En **Canvas**, haga clic en **Agregar entorno de trabajo**.
2. Seleccione **Google Cloud Platform > Kubernetes Cluster > Discover**.
3. Seleccione **clúster de importación** y haga clic en **Siguiente**.
4. Cargue un archivo de configuración de Kubernetes en 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

Resultado

BlueXP añade el clúster Kubernetes al lienzo.

Importe un clúster OpenShift a BlueXP

Importe un clúster OpenShift autogestionado a BlueXP para que pueda empezar a realizar backups de volúmenes persistentes a su proveedor de cloud.

Importe un clúster

Es posible importar un clúster de Kubernetes autogestionado mediante un archivo de configuración de Kubernetes.

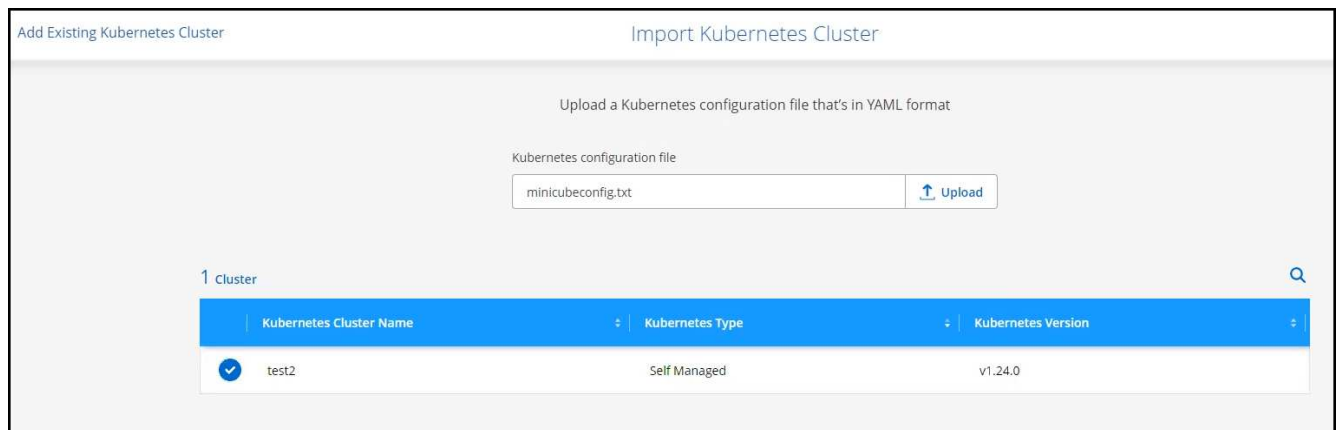
Antes de empezar

Antes de importar un clúster de OpenShift, necesita:

- El archivo 'kubeconfig-sa' creado en ["cree un archivo kubeconfig"](#).
- Los archivos public Certificate Authority (por ejemplo, ca.crt), Client Key (por ejemplo, tls.key) y Client Certification (por ejemplo, tls.crt) para el clúster.

Pasos

1. En **Canvas**, seleccione **Agregar entorno de trabajo**.
2. Seleccione su proveedor de cloud y seleccione **clúster de Kubernetes > Discover**.
3. Seleccione **clúster de importación** y **Siguiente**.
4. Cargue el kubeconfig-sa archivo en el que ha creado ["cree un archivo kubeconfig"](#). Seleccione el clúster de Kubernetes y seleccione **Siguiente**.



Add Existing Kubernetes Cluster

Import Kubernetes Cluster

Upload a Kubernetes configuration file that's in YAML format

Kubernetes configuration file

minikubeconfig.txt [Upload](#)

1 Cluster


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

5. Cargue los certificados del clúster.


Upload Cluster Certificates

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


Certificate Authority



Client Key



Client Certificate



Resultado

BlueXP añade el clúster Kubernetes al lienzo.

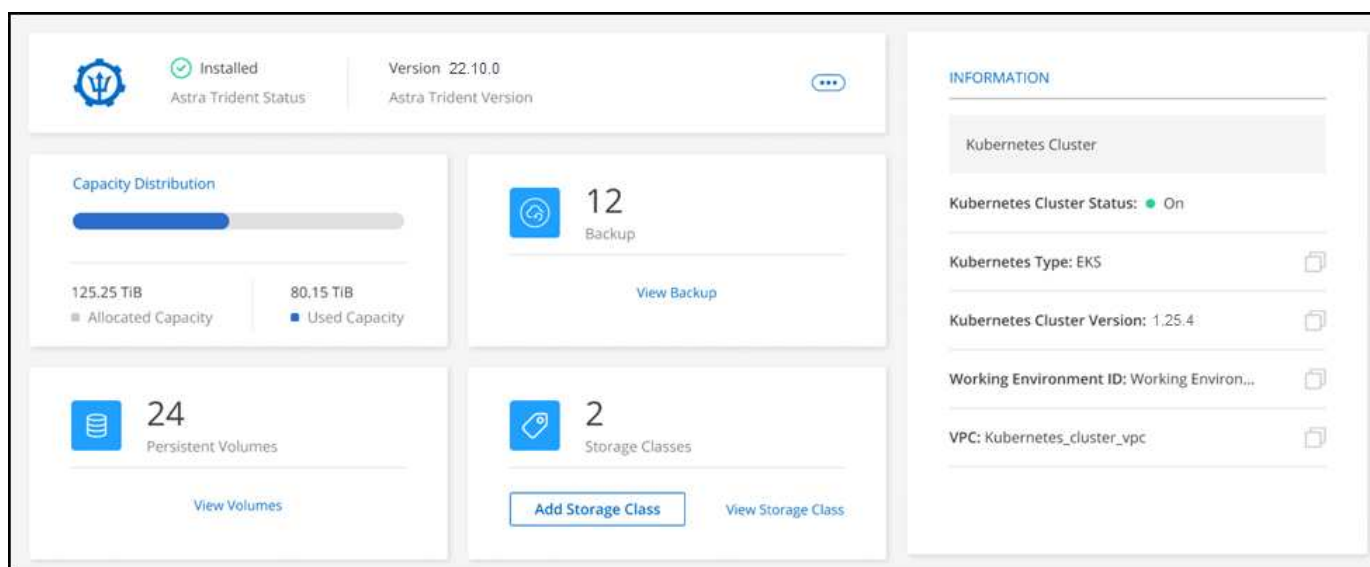
Gestione clústeres de Kubernetes

Gestione Astra Trident

Después de añadir un clúster de Kubernetes gestionado al lienzo, puede utilizar BlueXP para confirmar una instalación compatible de Astra Trident, instalar o actualizar Astra Trident a la versión más reciente o desinstalar Astra Trident.

Astra Trident en BlueXP

Después de añadir clústeres de Kubernetes a BlueXP, puede gestionar Astra Trident y sus clústeres de Kubernetes desde la página de descripción general. Para abrir la página de resumen, haga doble clic en el entorno de trabajo de Kubernetes en el lienzo.



Versiones compatibles de Astra Trident

Es necesaria una de las cuatro versiones más recientes de Astra Trident implementadas mediante el operador Trident, ya sea manualmente o mediante el gráfico Helm. Si Astra Trident no está instalado o se ha instalado una versión incompatible de Astra Trident, el clúster mostrará que hay una acción necesaria.



Astra Trident puso en marcha con `tridentctl` no es compatible. Si puso en marcha Astra Trident con `tridentctl`, No puede utilizar BlueXP para gestionar sus clústeres de Kubernetes ni desinstalar Astra Trident. Debe Y vuelva a instalar Astra Trident manualmente mediante "[El operador de Trident](#)" O en BlueXP usando [Instalar o actualizar Astra Trident](#).

Para obtener más información sobre Astra Trident, consulte "[Documentación de Astra Trident](#)".

Instalar o actualizar Astra Trident

En la página de descripción general, puede revisar el estado y la versión de la instalación de Astra Trident. Si Astra Trident aún no está instalado o hay una versión incompatible instalada, puede gestionarla con BlueXP.

Pasos

1. Haga doble clic en el entorno de trabajo de Kubernetes en el lienzo o haga clic en **Entrar en entorno de trabajo**.

a. Si Astra Trident no está instalado, haga clic en **instalar Trident**.

1 | Install Astra Trident

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

Install Trident

b. Si hay instalada una versión no compatible de Astra Trident, haga clic en **Actualizar Trident**.

Upgrade Astra Trident

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

Upgrade Trident



No puede utilizar BlueXP para actualizar desde las versiones de Astra Trident anteriores a 21.01. Para actualizar desde una versión anterior, consulte ["Actualizar con el operador"](#).

Resultados

Se ha instalado la última versión de Astra Trident. Ahora puede agregar clases de almacenamiento.

Desinstale Astra Trident

Si instaló Astra Trident con BlueXP o con el operador Trident (ya sea Helm o manualmente), puede desinstalarla mediante BlueXP.



- Después de desinstalar Astra Trident no puede crear volúmenes persistentes nuevos, pero los volúmenes existentes aún están disponibles.
- Mientras se desinstala Astra Trident, la copia de seguridad no está disponible.
- Puede volver a instalar Astra Trident en el entorno de trabajo en cualquier momento para continuar gestionando los clústeres.

La desinstalación de Astra Trident con BlueXP no elimina todos los servicios de Astra Trident aplicados durante la instalación. Para eliminar por completo Astra Trident, incluidas todas las definiciones de recursos personalizados (CRD) que crea, consulte ["Desinstale mediante el operador Trident"](#)

Pasos

1. En la página de descripción general, seleccione las elipses y **Desinstalar Astra Trident**.



2. Seleccione **Desinstalar** para confirmar y desinstalar Astra Trident.

Resultados

Astra Trident ahora se desinstala del entorno de trabajo. Puede volver a instalar Astra Trident en cualquier momento.

Gestione las clases de almacenamiento

Después de añadir un clúster de Kubernetes gestionado al lienzo, puede utilizar BlueXP para gestionar las clases de almacenamiento.



Si no se define ninguna clase de almacenamiento, el clúster mostrará que es necesaria una acción. Al hacer doble clic en el clúster del lienzo se abre la página de acciones para añadir una clase de almacenamiento.

Añada la clase de almacenamiento

Pasos

1. Desde el lienzo, arrastre y suelte el entorno de trabajo de Kubernetes en el entorno de trabajo Cloud Volumes ONTAP o Amazon FSX para ONTAP para abrir el asistente de clase de almacenamiento.
2. Escriba un nombre para la clase de almacenamiento.
3. Seleccione almacenamiento **sistema de archivos** o **bloque**.
 - a. Para almacenamiento **Block**, seleccione un tipo de sistema de archivos (fstype)

- b. Para almacenamiento **Block** o **Filesystem**, puede seleccionar activar la economía de clase de almacenamiento.

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



No se admiten los backups y las restauraciones al utilizar la economía de clase de almacenamiento.

- Seleccione opciones para la expansión de volumen, el enlace de volumen y la clase de almacenamiento predeterminada. Haga clic en **Siguiente**.
- Seleccione un entorno de trabajo para conectarse al clúster. Haga clic en **Agregar**.

☒ Storage Class Definitions
 ☒ Select Working Environment

Select Working Environment

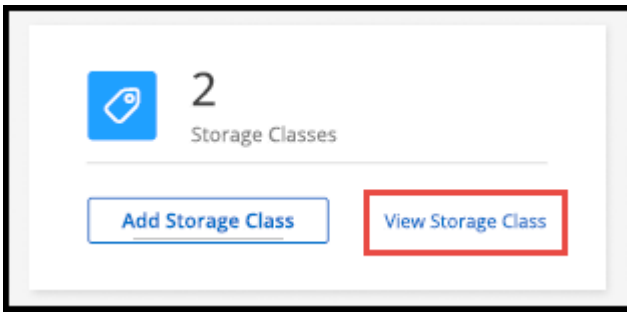
Working Environment	Type	Configuration	Region	Connected to K8s Clusters
<input type="radio"/> Working Environment Name On	Cloud Volumes ONTAP	High Availability	US East (Northern Virginia)	Not Connected
<input type="radio"/> Working Environment Name On	Cloud Volumes ONTAP	High Availability	US East (Northern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

Previous

Add

Resultados

Puede hacer clic en para ver la clase de almacenamiento en la página de recursos del clúster de Kubernetes.



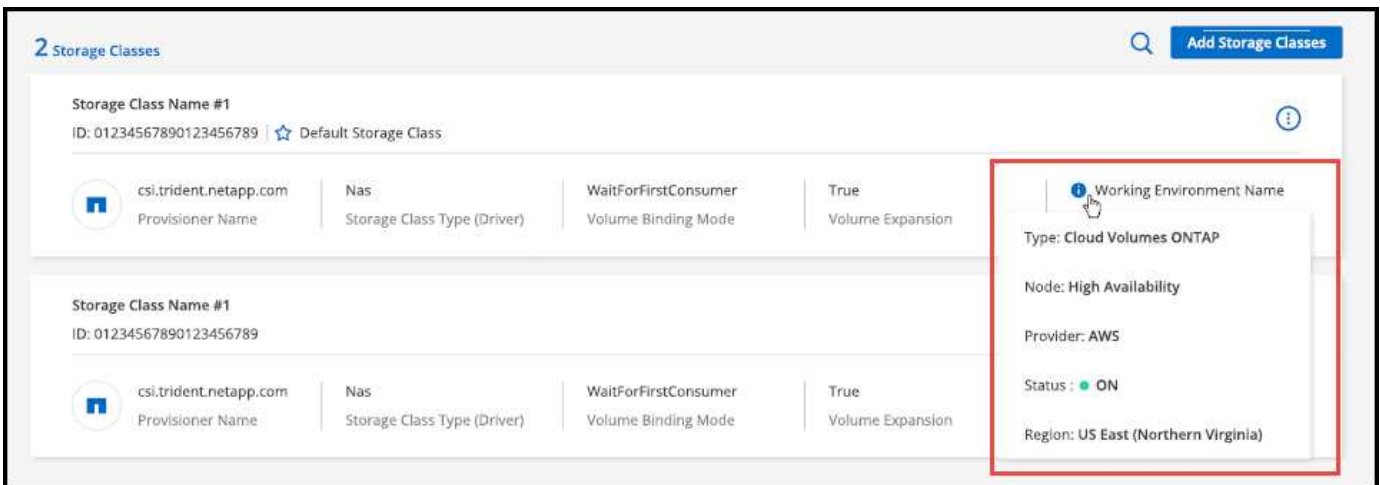
Ver detalles del entorno de trabajo

Pasos

1. Haga doble clic en el entorno de trabajo de Kubernetes en el lienzo o haga clic en **Entrar en entorno de trabajo**.
2. Haga clic en la ficha **clases de almacenamiento**.
3. Haga clic en el icono de información para ver los detalles del entorno de trabajo.

Resultados

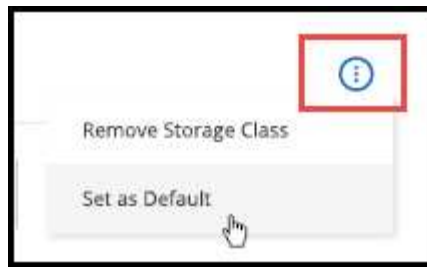
Se abrirá el panel de detalles del entorno de trabajo.



Establecer la clase de almacenamiento predeterminada

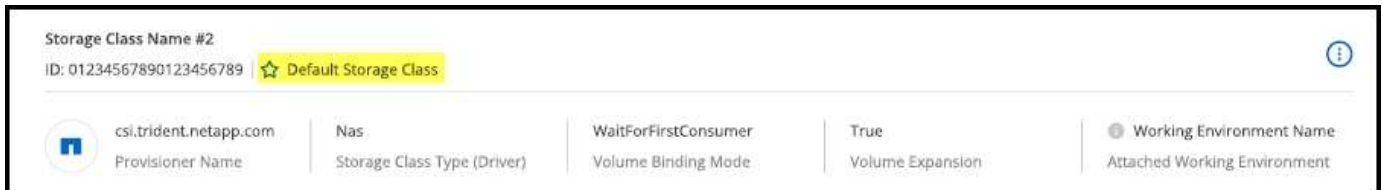
Pasos

1. Haga doble clic en el entorno de trabajo de Kubernetes en el lienzo o haga clic en **Entrar en entorno de trabajo**.
2. Haga clic en la ficha **clases de almacenamiento**.
3. Haga clic en el menú de acciones de la clase de almacenamiento y haga clic en **establecer como predeterminado**.



Resultados

La clase de almacenamiento seleccionada se establece como predeterminada.



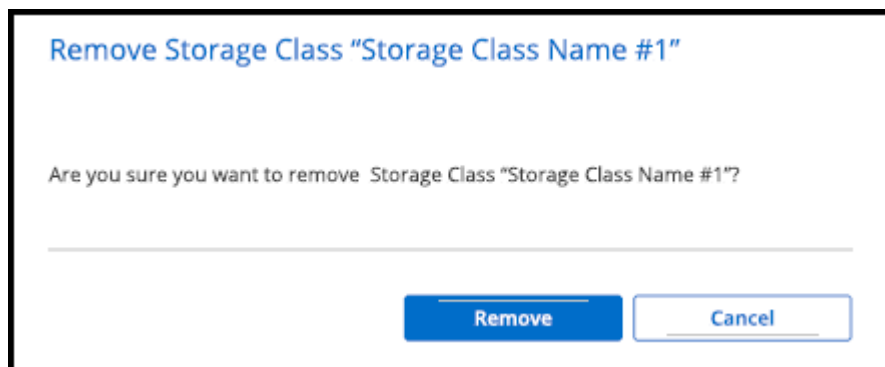
Quite la clase de almacenamiento

Pasos

1. Haga doble clic en el entorno de trabajo de Kubernetes en el lienzo o haga clic en **Entrar en entorno de trabajo**.
2. Haga clic en la ficha **clases de almacenamiento**.
3. Haga clic en el menú de acciones de la clase de almacenamiento y haga clic en **establecer como predeterminado**.



4. Haga clic en **Quitar** para confirmar la eliminación de la clase de almacenamiento.



Resultados

Se elimina la clase de almacenamiento seleccionada.

Vea los volúmenes persistentes

Después de añadir un clúster de Kubernetes gestionado al lienzo, puedes utilizar BlueXP para ver los volúmenes persistentes.



BlueXP supervisa el clúster de Kubernetes en busca de cambios en el back-end y actualiza la tabla de volúmenes persistentes cuando se añaden nuevos volúmenes. Si se configuró el backup automático en el clúster, el backup se habilita automáticamente en los nuevos volúmenes persistentes.


Pasos

1. Haga doble clic en el entorno de trabajo de Kubernetes en el lienzo o haga clic en **Entrar en entorno de trabajo**.
2. Haga clic en **Ver volúmenes** en la ficha **Descripción general** o haga clic en la ficha **volúmenes persistentes**. Si no se configuran volúmenes persistentes, consulte ["El provisionamiento"](#) Para obtener más información sobre el aprovisionamiento de volúmenes en Astra Trident.

Resultados

Se muestra una tabla de los volúmenes persistentes configurados.

Volumes Summary



8

Total Volumes


400 GiB

Total Allocated Capacity

201.2 GiB

Total Used Capacity

8 Volumes



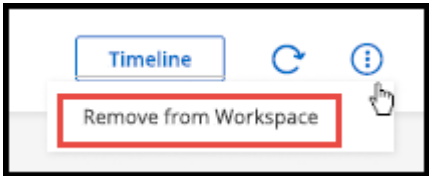
Volume Name	Name Space	Storage Class	Access Mode	Allocated Capacity	Used Capacity
Volumes Very Long Name <div><div></div>On</div>	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB
Volumes Very Long Name <div><div></div>On</div>	Name Space	Storage Class Name	Access Mode	50 GiB	25.15 GiB

Quite los clústeres de Kubernetes del espacio de trabajo

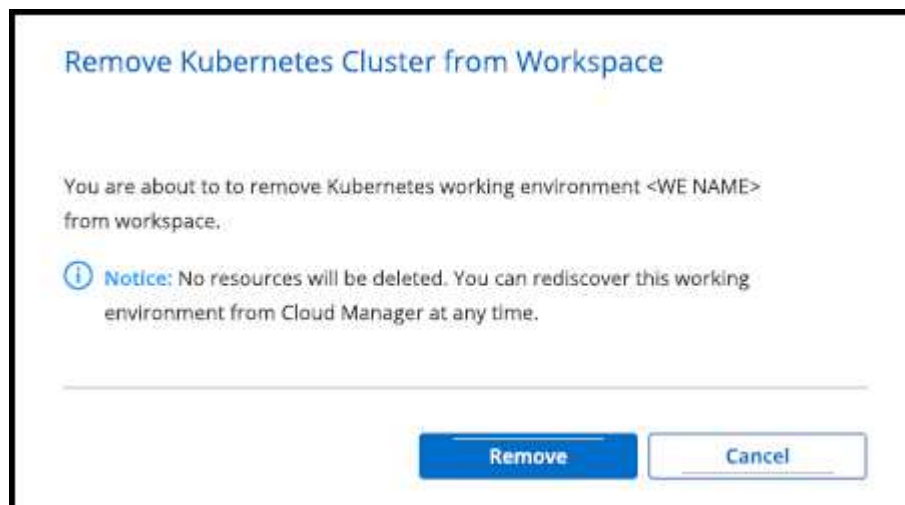
Después de agregar un clúster de Kubernetes gestionado al lienzo, puede utilizar BlueXP para eliminar clústeres del espacio de trabajo.

Pasos

1. Haga doble clic en el entorno de trabajo de Kubernetes en el lienzo o haga clic en **Entrar en entorno de trabajo**.
2. En la parte superior derecha de la página, seleccione el menú acciones y haga clic en **Quitar de Workspace**.



3. Haga clic en **Quitar** para confirmar la eliminación del clúster del área de trabajo. Es posible volver a detectar este clúster en cualquier momento.



Resultados

El clúster de Kubernetes se elimina del espacio de trabajo y ya no es visible en Canvas.

Use los servicios de datos en el cloud de NetApp con clústeres de Kubernetes

Después de añadir un clúster de Kubernetes gestionado al lienzo, podrá utilizar los servicios de datos en el cloud de NetApp para la gestión de datos avanzada.

Puedes utilizar el backup y la recuperación de datos de BlueXP para realizar backups de volúmenes persistentes en el almacenamiento de objetos.

["Descubre cómo proteger tus datos de clústeres de Kubernetes con el backup y la recuperación de 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	...

Conocimiento y apoyo

Regístrese para recibir soporte

Es necesario registrarse en soporte para recibir soporte técnico específico para BlueXP y sus servicios y soluciones de almacenamiento. También es necesario registrar soporte para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP.

Al registrarse para recibir soporte, no se habilita el soporte de NetApp para un servicio de archivos de proveedor de cloud. Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener ayuda» en la documentación de BlueXP para ese producto.

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

Información general del registro de soporte

Existen dos formas de registro para activar el derecho de asistencia:

- Registro de la suscripción al soporte de ID de cuenta de BlueXP (número de serie de 20 dígitos xxxx960xxxxx que se encuentra en la página Recursos de asistencia técnica de BlueXP).

Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de BlueXP. Debe registrarse cada suscripción de asistencia técnica a nivel de cuenta de BlueXP.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de cloud (estos son números de serie de 20 dígitos 909201xxxxxxxx).

Estos números de serie se denominan comúnmente *PAYGO serial Numbers* y son generados por BlueXP en el momento de la implementación de Cloud Volumes ONTAP.

El registro de ambos tipos de números de serie permite funcionalidades, como abrir tickets de soporte y la generación automática de casos. Para completar el registro, añada cuentas del sitio de soporte de NetApp (NSS) a BlueXP, como se describe a continuación.

Registra tu cuenta de BlueXP para recibir soporte de NetApp

Para registrarte para obtener soporte y activar el soporte, un usuario de tu cuenta de BlueXP debe asociar una cuenta en el sitio de soporte de NetApp a su inicio de sesión en BlueXP. La forma de registrarse para recibir soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta de NSS

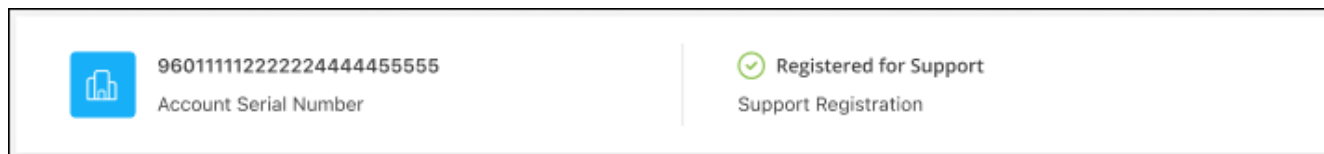
Si es cliente de NetApp con una cuenta de NSS, solo tiene que registrarse para recibir soporte a través de BlueXP.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.

2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga el aviso de autenticación del sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro se ha realizado correctamente, seleccione el icono Ayuda y seleccione **Soporte**.

La página **Recursos** debe mostrar que su cuenta está registrada para soporte.



Tenga en cuenta que los otros usuarios de BlueXP no verán este mismo estado de registro de soporte si no han asociado una cuenta del sitio de soporte de NetApp con su inicio de sesión de BlueXP. Sin embargo, eso no significa que tu cuenta de BlueXP no esté registrada para el soporte técnico. Siempre y cuando un usuario de la cuenta haya seguido estos pasos, su cuenta se ha registrado.

Cliente existente pero no cuenta NSS

Si eres un cliente existente de NetApp con licencias y números de serie existentes, pero *no* NSS, deberás crear una cuenta NSS y asociarla al inicio de sesión de BlueXP.

Pasos

1. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
 - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
 - b. Asegúrese de copiar el número de serie de la cuenta BlueXP (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.
2. Asocia tu nueva cuenta de NSS con tu inicio de sesión de BlueXP. Para ello, sigue los pasos que se muestran en [Cliente existente con una cuenta de NSS](#).

Totalmente nuevo en NetApp

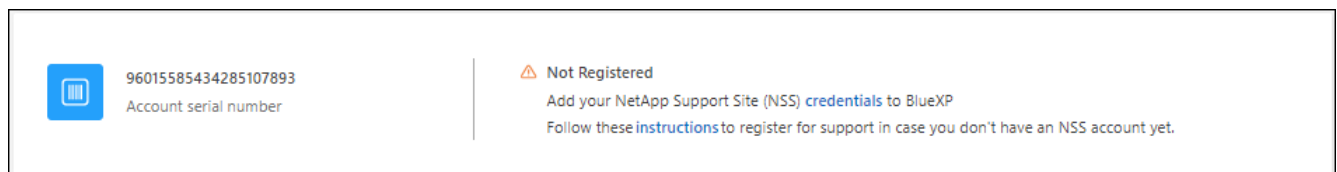
Si es totalmente nuevo en NetApp y no tiene una cuenta de NSS, siga cada paso que se indica a continuación.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Busque el número de serie de su ID de cuenta en la página Support Registration.



3. Vaya a. "[Sitio de registro de soporte de NetApp](#)" Y seleccione **no soy un cliente registrado de NetApp**.
4. Rellene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **línea de productos**, seleccione **Cloud Manager** y, a continuación, seleccione el proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta desde el paso 2 anterior, complete la comprobación de seguridad y confirme que ha leído la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón de correo para finalizar esta transacción segura. Asegúrese de comprobar sus carpetas de spam si el correo electrónico de validación no llega en pocos minutos.

7. Confirme la acción desde el correo electrónico.

Confirmar envía su solicitud a NetApp y recomienda que cree una cuenta en la página de soporte de NetApp.

8. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
 - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
 - b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.

Después de terminar

NetApp debería ponerse en contacto con usted durante este proceso. Este es un ejercicio de incorporación puntual para nuevos usuarios.

Cuando tengas tu cuenta en el sitio de soporte de NetApp, asocia la cuenta con el inicio de sesión de BlueXP siguiendo los pasos que se muestran a continuación [Cliente existente con una cuenta de NSS](#).

Asocie credenciales de NSS para soporte de Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su cuenta de BlueXP para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para recibir soporte

Se requiere que proporcione su cuenta de NSS para activar el soporte de su sistema y obtener acceso a los recursos de soporte técnico de NetApp.

- Puesta en marcha de Cloud Volumes ONTAP cuando usted traiga su propia licencia (BYOL)

Es necesario proporcionar su cuenta NSS para que BlueXP pueda cargar su clave de licencia y activar la suscripción para el plazo que adquirió. Esto incluye actualizaciones automáticas para renovaciones de términos.

- Actualizar el software Cloud Volumes ONTAP a la versión más reciente

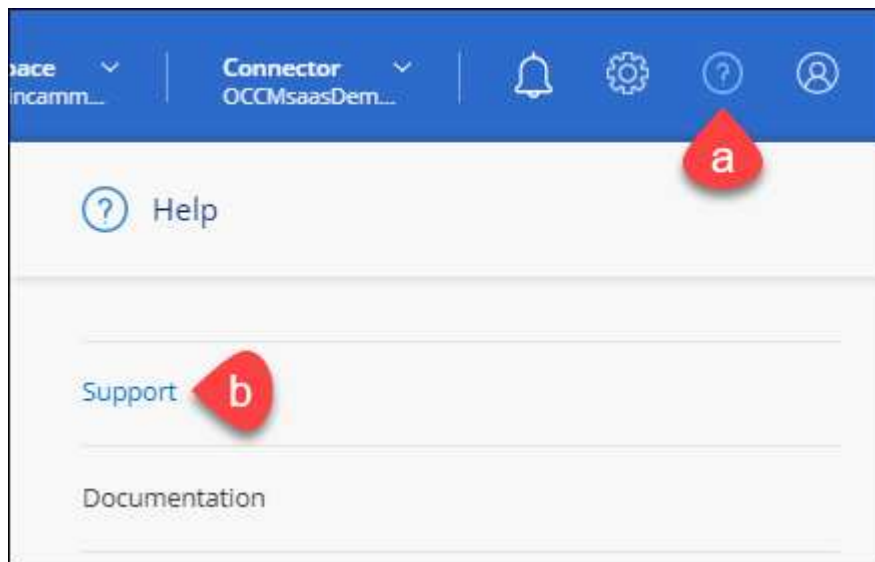
La asociación de credenciales de NSS con su cuenta de BlueXP es diferente de la cuenta de NSS asociada con un inicio de sesión de usuario de BlueXP.

Estas credenciales de NSS están asociadas con tu ID de cuenta de BlueXP específico. Los usuarios que pertenecen a la cuenta BlueXP pueden acceder a estas credenciales desde **Soporte > Gestión NSS**.

- Si tiene una cuenta de nivel de cliente, puede añadir una o varias cuentas de NSS.
- Si tiene una cuenta de partner o distribuidor, puede añadir una o varias cuentas de NSS, pero no se podrán añadir junto con las cuentas de nivel de cliente.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta de NSS**.
3. Cuando se le solicite, seleccione **continuar** para que se le redirija a una página de inicio de sesión de

Microsoft.

NetApp utiliza Microsoft Entra ID como proveedor de identidad para los servicios de autenticación específicos de soporte y licencias.

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico registrada en el sitio de soporte de NetApp y contraseña para realizar el proceso de autenticación.

Estas acciones permiten a BlueXP utilizar su cuenta NSS para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.


Tenga en cuenta lo siguiente:


- La cuenta NSS debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal). Puede tener varias cuentas de NSS en el nivel del cliente.
- Sólo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de partner. Si intenta agregar cuentas de NSS de nivel de cliente y existe una cuenta de nivel de partner, obtendrá el siguiente mensaje de error:

"El tipo de cliente NSS no está permitido para esta cuenta, ya que ya hay usuarios NSS de tipo diferente."

Lo mismo sucede si tiene cuentas de NSS de nivel de cliente preexistentes e intenta añadir una cuenta de nivel de partner.

- Después de iniciar sesión correctamente, NetApp almacenará el nombre de usuario de NSS.

Se trata de un ID generado por el sistema que se asigna a su correo electrónico. En la página **NSS Management**, puede mostrar su correo electrónico desde  de windows

- Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en la  de windows

Con esta opción se le solicita que vuelva a iniciar sesión. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se enviará una notificación para avisarle de ello.

Obtenga ayuda

NetApp ofrece soporte para BlueXP y sus servicios cloud de diversas maneras. Hay disponibles amplias opciones de auto soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un foro de la comunidad. Su registro de soporte incluye soporte técnico remoto a través de tickets web.

Obtenga soporte para un servicio de archivos de proveedores de cloud

Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener ayuda» en la documentación de BlueXP para ese producto.

- ["Amazon FSX para ONTAP"](#)
- ["Azure NetApp Files"](#)

- ["Cloud Volumes Service para Google Cloud"](#)

Para recibir soporte técnico específico sobre BlueXP y sus soluciones y servicios de almacenamiento, use las opciones de soporte descritas a continuación.

Utilice opciones de soporte automático

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- Documentación

La documentación de BlueXP que está viendo actualmente.

- ["Base de conocimientos"](#)

Busque en la base de conocimientos de BlueXP para encontrar artículos útiles para resolver problemas.

- ["Comunidades"](#)

Únase a la comunidad de BlueXP para seguir los debates en curso o crear otros nuevos.

Cree un caso con el soporte de NetApp

Además de las opciones de autosoporte anteriores, puede trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de activar el soporte de.

Antes de empezar

- Para utilizar la funcionalidad **Crear un caso**, primero debes asociar tus credenciales del sitio de soporte de NetApp con el inicio de sesión de BlueXP. ["Descubre cómo gestionar las credenciales asociadas con tu inicio de sesión de BlueXP"](#).
- Si abre un caso para un sistema ONTAP que tiene un número de serie, su cuenta de NSS deberá estar asociada con el número de serie de ese sistema.

Pasos

1. En BlueXP, selecciona **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:
 - a. Selecciona **Llámanos** si quieres hablar con alguien por teléfono. Se le dirigirá a una página de netapp.com que enumera los números de teléfono a los que puede llamar.
 - b. Selecciona **Crear un caso** para abrir un ticket con un especialista en Soporte NetApp:
 - **Servicio:** Seleccione el servicio con el que está asociado el problema. Por ejemplo, cuando BlueXP es específico de un problema de soporte técnico con flujos de trabajo o funcionalidades dentro del servicio.
 - **Entorno de trabajo:** Si se aplica al almacenamiento, seleccione **Cloud Volumes ONTAP** o **On-Prem** y, a continuación, el entorno de trabajo asociado.

La lista de entornos de trabajo se encuentra dentro del ámbito de la cuenta BlueXP, el área de trabajo y el conector que ha seleccionado en el banner superior del servicio.

- **Prioridad de caso:** Elija la prioridad para el caso, que puede ser Baja, Media, Alta o crítica.

Para obtener más información sobre estas prioridades, pase el ratón sobre el icono de información

situado junto al nombre del campo.

- **Descripción del problema:** Proporcione una descripción detallada del problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que haya realizado.
- **Direcciones de correo electrónico adicionales:** Introduzca direcciones de correo electrónico adicionales si desea que alguien más conozca este problema.
- **Accesorio (opcional):** Cargue hasta cinco archivos adjuntos, uno a la vez.

Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.

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

Después de terminar

Aparecerá una ventana emergente con el número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y le pondrá en contacto con usted próximamente.

Para obtener un historial de sus casos de soporte, puede seleccionar **Ajustes > Línea de tiempo** y buscar acciones denominadas "Crear caso de soporte". Un botón situado en el extremo derecho le permite ampliar la acción para ver los detalles.

Es posible que se encuentre el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso en el servicio seleccionado"

Este error podría significar que la cuenta NSS y la compañía de registro con la que está asociada no es la misma compañía de registro para el número de serie de la cuenta de BlueXP (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede solicitar ayuda utilizando una de las siguientes opciones:

- Usar el chat en el producto
- Envíe un caso no técnico en <https://mysupport.netapp.com/site/help>

Gestione sus casos de soporte (vista previa)

Puede ver y gestionar los casos de soporte activos y resueltos directamente desde BlueXP. Es posible gestionar los casos asociados con su cuenta de NSS y con su empresa.

La gestión de casos está disponible como vista previa. Tenemos pensado perfeccionar esta experiencia y añadir mejoras en próximos lanzamientos. Envíenos sus comentarios mediante el chat en el producto.

Tenga en cuenta lo siguiente:

- La consola de gestión de casos en la parte superior de la página ofrece dos vistas:
 - La vista de la izquierda muestra el total de casos abiertos en los últimos 3 meses por la cuenta de usuario NSS que ha proporcionado.
 - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su compañía en función de su cuenta NSS de usuario.

Los resultados de la tabla reflejan los casos relacionados con la vista seleccionada.

- Puede agregar o quitar columnas de interés y filtrar el contenido de columnas como prioridad y estado. Otras columnas proporcionan funciones de clasificación.

Consulte los pasos a continuación para obtener más información.

- En el nivel por caso, ofrecemos la posibilidad de actualizar las notas de un caso o cerrar un caso que no esté ya en estado cerrado o pendiente de cierre.

Pasos

1. En BlueXP, selecciona **Ayuda > Soporte**.
2. Selecciona **Gestión de casos** y, si se te solicita, agrega tu cuenta de NSS a BlueXP.

La página **Administración de casos** muestra casos abiertos relacionados con la cuenta NSS asociada con su cuenta de usuario de BlueXP. Esta es la misma cuenta NSS que aparece en la parte superior de la página **NSS Management**.

3. Si lo desea, puede modificar la información que se muestra en la tabla:
 - En **Casos de la organización**, selecciona **Ver** para ver todos los casos asociados a tu empresa.
 - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un marco de tiempo diferente.

Search icon Cases opened on the last 3 months Create a case

Date created	Last updated	Last 7 days	Last 30 days	Last 3 months	Status (5)	
December 22, 2022	December 29, 2022				Assigned	...
December 21, 2022	December 28, 2022	Apply	Reset		Active	...
December 15, 2022	December 27, 2022			Medium (P3)	Pending customer	...
December 14, 2022	December 26, 2022			Low (P4)	Solution proposed	...

- Filtre el contenido de las columnas.

Search icon Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	<input checked="" type="checkbox"/> Active <input checked="" type="checkbox"/> Pending customer	...
December 28, 2022	High (P2)	<input checked="" type="checkbox"/> Solution proposed <input checked="" type="checkbox"/> Pending closed	...
December 27, 2022	Medium (P3)	<input type="checkbox"/> Closed	...
December 26, 2022	Low (P4)	Apply Reset	...

- Seleccione para cambiar las columnas que aparecen en la tabla  y, a continuación, seleccione las columnas que desea mostrar.

Search icon Cases opened on the last 3 months Create a case

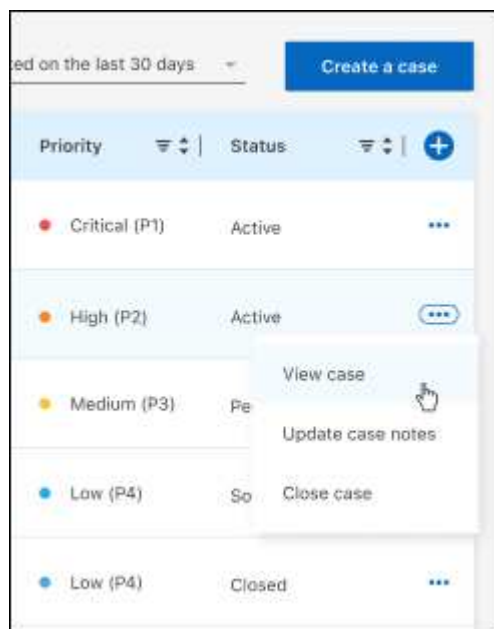
Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	<input checked="" type="checkbox"/> Last updated <input checked="" type="checkbox"/> Priority <input checked="" type="checkbox"/> Cluster name	...
December 28, 2022	High (P2)	<input type="checkbox"/> Case owner <input type="checkbox"/> Opened by	...
December 27, 2022	Medium (P3)	Apply Reset	...
December 26, 2022	Low (P4)		...

4. Seleccione para gestionar un caso existente ... y seleccione una de las opciones disponibles:

- **Ver caso:** Ver todos los detalles sobre un caso específico.
- **Actualizar notas de caso:** Proporcione detalles adicionales sobre su problema o seleccione **cargar archivos** para adjuntar hasta un máximo de cinco archivos.

Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.

- **Cerrar caso:** Proporciona detalles sobre por qué estás cerrando el caso y selecciona **Cerrar caso**.



Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

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

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

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

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

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

Política de privacidad

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

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

["Aviso para BlueXP"](#)

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.