Manos a la obra

Astra Control Service

NetApp
October 21, 2024

Tabla de contenidos

Manos a la obra . . . 1
- Más información sobre Astra Control . . . 1
- Puestas en marcha de Kubernetes compatibles . . . 5
- Inicio rápido del servicio Astra Control . . . 5
- Configure su proveedor de cloud . . . 7
- Regístrese para obtener una cuenta de Astra Control Service . . . 28
- Añada un clúster a Astra Control Service . . . 29
- El futuro . . . 72
- Vídeos de Astra Control Service . . . 72

Manos a la obra

Más información sobre Astra Control

Astra Control es una solución de gestión del ciclo de vida de los datos de las aplicaciones de Kubernetes que simplifica las operaciones para aplicaciones con estado. Proteja, realice backups y migre cargas de trabajo de Kubernetes con facilidad, y cree instantáneamente clones de aplicaciones que funcionen.

Funciones

Astra Control ofrece funcionalidades cruciales para la gestión del ciclo de vida de los datos de las aplicaciones Kubernetes:

- Gestione automáticamente el almacenamiento persistente
- Crear copias Snapshot y backups bajo demanda que se tienen en cuenta las aplicaciones
- Automatice las operaciones de backup y Snapshot condicionadas por políticas
- Migre aplicaciones y datos de un clúster de Kubernetes a otro
- Replicar aplicaciones en un sistema remoto mediante la tecnología SnapMirror de NetApp (Astra Control Center)
- Clone aplicaciones de almacenamiento provisional a producción
- Visualizar el estado de la protección y el estado de la aplicación
- Trabaje con una interfaz de usuario web o una API para implementar sus flujos de trabajo de backup y migración

Modelos de puesta en marcha

Astra Control está disponible en dos modelos de implementación:

- **Astra Control Service**: Un servicio gestionado por NetApp que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes en varios entornos de proveedores de cloud, así como clústeres de Kubernetes autogestionados.
- **Astra Control Center**: Software autogestionado que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes que se ejecutan en su entorno local. Astra Control Center también se puede instalar en entornos de varios proveedores de cloud con un entorno de administración del almacenamiento Cloud Volumes ONTAP de NetApp.

	Servicio de control Astra	**Astra Control Center**
¿Cómo se ofrece?	Como un servicio cloud totalmente gestionado de NetApp	Como software que se puede descargar, instalar y gestionar
¿Dónde está alojado?	En un cloud público que elija NetApp	En su propio clúster de Kubernetes
¿Cómo se actualiza?	Gestionado por NetApp	Usted administra cualquier actualización

	Servicio de control Astra	Astra Control Center

¿Cuáles son las distribuciones de Kubernetes compatibles?	• * Proveedores en la nube*
	  ◦ Amazon Web Services
	  ▪ Amazon Elastic Kubernetes Service (EKS)
	  ◦ Google Cloud
	  ▪ Google Kubernetes Engine (GKE)
	  ◦ Microsoft Azure
	  ▪ Azure Kubernetes Service (AKS)
	• **Clusters autogestionados**
	  ◦ Kubernetes (ascendente)
	  ◦ Motor Kubernetes de rancher (RKE)
	  ◦ OpenShift Container Platform de Red Hat
	• * Clústeres locales*
	  ◦ Red Hat OpenShift Container Platform en las instalaciones
		• Azure Kubernetes Service en HCI de pila de Azure
		• Anthos de Google
		• Kubernetes (ascendente)
		• Motor Kubernetes de rancher (RKE)
		• OpenShift Container Platform de Red Hat

	Servicio de control Astra	Astra Control Center
¿Cuáles son los back-ends de almacenamiento compatibles?	• * Proveedores en la nube* ◦ Amazon Web Services ▪ Amazon EBS ▪ Amazon FSX para ONTAP de NetApp ▪ "Cloud Volumes ONTAP" ◦ Google Cloud ▪ Disco persistente de Google ▪ Cloud Volumes Service de NetApp ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure ▪ Discos gestionados de Azure ▪ Azure NetApp Files ▪ "Cloud Volumes ONTAP" • **Clusters autogestionados** ◦ Amazon EBS ◦ Discos gestionados de Azure ◦ Disco persistente de Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "El Longhorn" • * Clústeres locales* ◦ NetApp MetroCluster ◦ Sistemas ONTAP AFF y FAS de NetApp ◦ ONTAP Select de NetApp ◦ "Cloud Volumes ONTAP" ◦ "El Longhorn"	• Sistemas ONTAP AFF y FAS de NetApp • ONTAP Select de NetApp • "Cloud Volumes ONTAP" • "El Longhorn"

Funcionamiento del servicio Astra Control

Astra Control Service es un servicio cloud gestionado por NetApp que siempre está activo y actualizado con las últimas funcionalidades. Utiliza varios componentes para habilitar la gestión del ciclo de vida de los datos de aplicaciones.

En un nivel superior, Astra Control Service funciona de esta manera:

- Para comenzar a trabajar con Astra Control Service, configure su proveedor de cloud y inscríbase para obtener una cuenta Astra.

+ ** para los clusters GKE, el servicio Astra Control utiliza "Cloud Volumes Service de NetApp para Google Cloud" O discos persistentes de Google como back-end de almacenamiento para sus volúmenes persistentes.

+ ** para clusters de AKS, el servicio de control de Astra utiliza "Azure NetApp Files" O Azure gestionó discos como back-end de almacenamiento para sus volúmenes persistentes.

+ ** para clústeres de Amazon EKS, el servicio Astra Control utiliza "Amazon Elastic Block Store" o. "Amazon FSX para ONTAP de NetApp" como back-end de almacenamiento para sus volúmenes persistentes.

- Agregue su primera tecnología Kubernetes al servicio Astra Control. A continuación, el servicio de control de Astra realiza lo siguiente:
  - Crea un almacén de objetos en su cuenta de proveedor de cloud, que es donde se almacenan las copias de backup.

+ en Azure, Astra Control Service también crea un grupo de recursos, una cuenta de almacenamiento y claves para el contenedor Blob.

- Crea un nuevo rol de administrador y una cuenta de servicio de Kubernetes en el clúster.
- Utiliza el nuevo rol de administrador para instalar el enlace../concepts/architecture#astra-control-components[Astra Control Provisioner] en el clúster y crear una o varias clases de almacenamiento.
- Si utilizas una oferta de almacenamiento de servicios en la nube de NetApp como back-end de almacenamiento, el servicio Astra Control utiliza el aprovisionador de control de Astra para aprovisionar volúmenes persistentes para tus aplicaciones. Si utiliza discos administrados de Amazon EBS o Azure como back-end de almacenamiento, deberá instalar un controlador CSI específico del proveedor. Se proporcionan instrucciones de instalación en "Configure Amazon Web Services" y.. "Configure Microsoft Azure con discos gestionados de Azure".
  - En este momento, puede definir aplicaciones del clúster. Se aprovisionan volúmenes persistentes en el back-end de almacenamiento mediante la nueva clase de almacenamiento predeterminada.
  - A continuación, utilice Astra Control Service para gestionar estas aplicaciones y empiece a crear copias Snapshot, copias de seguridad y clones.

El plan gratuito de Astra Control le permite gestionar hasta 10 espacios de nombres en su cuenta. Si desea gestionar más de 10 espacios de nombres, deberá configurar la facturación mediante la actualización del plan gratuito al plan Premium.

Cómo funciona Astra Control Center

Astra Control Center se ejecuta en forma local en su propia nube privada.

Astra Control Center admite los clústeres de Kubernetes con un tipo de almacenamiento configurado por el aprovisionador de Astra Control con un back-end de almacenamiento de ONTAP.

Astra Control Center está totalmente integrado en el ecosistema del asesor digital de AutoSupport y Active IQ (también conocido como asesor digital) para proporcionar a los usuarios y al servicio de soporte de NetApp información sobre solución de problemas e uso.

Puede probar Astra Control Center con una licencia de evaluación de 90 días. La versión de evaluación es compatible con las opciones de correo electrónico y comunidad. Además, tendrá acceso a los artículos de la base de conocimientos y a la documentación desde la consola de soporte del producto.

Para instalar y utilizar Astra Control Center, tendrá que estar seguro "requisitos".

En un nivel superior, Astra Control Center funciona de esta manera:

- Instala Astra Control Center en su entorno local. Obtenga más información sobre cómo "Instalar Astra Control Center".
- Puede realizar algunas tareas de configuración como las siguientes:
  - Configurar la licencia.
  - Añada el primer clúster.
  - Añada el back-end de almacenamiento que se detecta al añadir el clúster.
  - Agregue un bloque de almacenamiento de objetos que almacenará las copias de seguridad de la aplicación.

Obtenga más información sobre cómo "Configure Astra Control Center".

Puede añadir aplicaciones al clúster. O bien, si ya tiene algunas aplicaciones en el clúster que se están gestionando, puede utilizar Astra Control Center para gestionarlas. A continuación, utilice Astra Control Center para crear copias Snapshot, backups, clones y relaciones de replicación.

Si quiere más información

- "Documentación de la familia de productos Astra de NetApp"
- "Documentación de Astra Control Center"
- "Documentación de la API de Astra Control"
- "Documentación de Astra Trident"
- "Documentación de ONTAP"

Puestas en marcha de Kubernetes compatibles

Astra Control Service puede gestionar las aplicaciones que se ejecutan en un clúster de Kubernetes gestionado en Amazon Elastic Kubernetes Service (EKS) y los clústeres que gestiona por su cuenta.

Astra Control Service puede gestionar las aplicaciones que se ejecutan en un clúster de Kubernetes gestionado en Google Kubernetes Engine (GKE) y los clústeres que gestiona por su cuenta.

Astra Control Service puede gestionar las aplicaciones que se ejecutan en un clúster de Kubernetes gestionado en Azure Kubernetes Service (AKS) y clústeres que gestiona por su cuenta.

- "Descubra cómo configurar Amazon Web Services para Astra Control Service".
- "Descubra cómo configurar Google Cloud para Astra Control Service".
- "Descubra cómo configurar Microsoft Azure con Azure NetApp Files para el servicio Astra Control".
- "Descubra cómo configurar Microsoft Azure con los discos gestionados de Azure para el servicio Astra Control".
- "Descubra cómo preparar los clústeres autogestionados antes de agregarlos al servicio de control de Astra".

Inicio rápido del servicio Astra Control

Esta página ofrece una descripción general de alto nivel de los pasos que necesita

completar para empezar con Astra Control Service. Los vínculos de cada paso le llevan a una página que proporciona más detalles.

[Uno] Configure su proveedor de cloud

1. Google Cloud:
    - Revise los requisitos del clúster de Google Kubernetes Engine.
    - Compre Cloud Volumes Service para Google Cloud a través de Google Cloud Marketplace.
    - Habilite las API necesarias.
    - Cree una cuenta de servicio y una clave de cuenta de servicio.
    - Configure la agrupación de redes desde su VPC a Cloud Volumes Service para Google Cloud.

      "Más información acerca de los requisitos de Google Cloud".

2. Servicios web de Amazon:
    - Revise los requisitos del clúster de Amazon Web Services.
    - Cree una cuenta de Amazon.
    - Instale la CLI de Amazon Web Services.
    - Cree un usuario de IAM.
    - Cree y adjunte una directiva de permisos.
    - Guarde las credenciales del usuario de IAM.

      "Obtenga más información acerca de los requisitos de Amazon Web Services".

3. Azure de Microsoft:

    - Revise los requisitos del clúster de Azure Kubernetes Service para el back-end de almacenamiento que ha decidido usar.

      "Obtenga más información acerca de los requisitos de Microsoft Azure y Azure NetApp Files".

   "Obtenga más información acerca de los requisitos de disco gestionado de Microsoft Azure y Azure".

Si va a gestionar su propio clúster y no está alojado en un proveedor de cloud, revise los requisitos de los clústeres autogestionados.
"Obtenga más información sobre los requisitos de clúster autogestionados".

[Dos] Complete el registro de Astra Control

1. Cree un "BlueXP de NetApp" cuenta.
2. Especifica tu ID de correo electrónico de BlueXP de NetApp al crear tu cuenta de Astra Control "Desde la página de producto de Astra Control".

"Obtenga más información sobre el proceso de registro".

[Tres] Agregue clústeres a Astra Control

Después de iniciar sesión, seleccione **Agregar clúster** para comenzar a gestionar el clúster con Astra Control.

"Obtenga más información acerca de cómo añadir clústeres".

Configure su proveedor de cloud

Configure Amazon Web Services

Hay que realizar algunos pasos para preparar su proyecto de Amazon Web Services antes de poder gestionar los clústeres de Amazon Elastic Kubernetes Service (EKS) con Astra Control Service.

Inicio rápido para configurar Amazon Web Services

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Amazon Web Services

Compruebe que los clústeres estén en buen estado y que ejecuten una versión de Kubernetes compatible, que los nodos de trabajo estén en línea y que ejecuten Linux o Windows, etc. Obtenga más información sobre este paso.

[Dos] Cree una cuenta de Amazon

Si aún no tiene una cuenta de Amazon, debe crear una para poder utilizar EKS. Obtenga más información sobre este paso.

[Tres] Instale la CLI de Amazon Web Services

Instale la CLI de AWS para que pueda gestionar AWS desde la línea de comandos. Siga las instrucciones paso a paso.

[Cuatro] Opcional: Cree un usuario de IAM

Cree un usuario de Amazon Identity and Access Management (IAM). También puede omitir este paso y utilizar un usuario de IAM existente con el servicio Astra Control Service.

Lea las instrucciones paso a paso.

[Cinco] Cree y adjunte una directiva de permisos

Cree una directiva con los permisos necesarios para que Astra Control Service interactúe con su cuenta de AWS.

Lea las instrucciones paso a paso.

[Seis] Guarde las credenciales del usuario de IAM

Guarde las credenciales del usuario de IAM para poder importar las credenciales en Astra Control Service.

Lea las instrucciones paso a paso.

Requisitos del clúster de EKS

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service.

La versión de Kubernetes

Un clúster de debe ejecutar una versión de Kubernetes en el rango de 1,25 a 1,28.

Tipo de imagen

El tipo de imagen para cada nodo de trabajo debe ser Linux.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Aprovisionador de Astra Control

Se necesitan un aprovisionador de Astra Control y una controladora Snapshot externa para las operaciones con back-ends de almacenamiento. Para habilitar estas operaciones, haga lo siguiente:

1. "Instale los CRD de instantánea y el controlador de instantánea".
2. "Habilita el aprovisionador de Astra Control".
3. "Cree una instancia de VolumeSnapshotClass".

Controladores CSI para Amazon Elastic Block Store (EBS)

Si utiliza el back-end de almacenamiento de Amazon EBS, debe instalar el controlador Container Storage Interface (CSI) para EBS (no se instala automáticamente).

Consulte los pasos para obtener instrucciones sobre la instalación del controlador CSI.

Instale una instantánea externa

Si aún no lo ha hecho, "Instale los CRD de instantánea y el controlador de instantánea".

Instale el controlador CSI como complemento Amazon EKS

1. Cree el rol IAM del controlador Amazon EBS CSI para las cuentas de servicio. Siga las instrucciones "En la documentación de Amazon", Mediante los comandos de la CLI de AWS de las instrucciones.
2. Añada el complemento Amazon EBS CSI con el siguiente comando de la CLI de AWS, reemplazando la información entre paréntesis <> por valores específicos de su entorno. Sustituya <DRIVER_ROLE> por el nombre de la función de controlador EBS CSI que creó en el paso anterior:

```
aws eks create-addon \
  --cluster-name <CLUSTER_NAME> \
  --addon-name aws-ebs-csi-driver \
  --service-account-role-arn
arn:aws:iam::<ACCOUNT_ID>:role/<DRIVER_ROLE>
```

Configure la clase de almacenamiento EBS

1. Clonar el repositorio del controlador Amazon EBS CSI GitHub en su sistema.

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-
driver.git
```

2. Desplácese al directorio de ejemplo de aprovisionamiento dinámico.

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. Implemente la clase de almacenamiento ebs-sc y la reclamación de volumen persistente ebs-Claim desde el directorio manifest.

```
kubectl apply -f manifests/storageclass.yaml
kubectl apply -f manifests/claim.yaml
```

4. Describa la clase de almacenamiento ebs-sc.

```
kubectl describe storageclass ebs-sc
```

Debe ver el resultado que describe los atributos de la clase de almacenamiento.

Cree una cuenta de Amazon

Si aún no dispone de una cuenta de Amazon, debe crear una para activar la facturación para Amazon EKS.

Pasos

1. Vaya a la "Página de inicio de Amazon" , Seleccione **Iniciar sesión** en la parte superior derecha y seleccione **Iniciar aquí**.
2. Siga las indicaciones para crear una cuenta.

Instale la CLI de Amazon Web Services

Instale la CLI de AWS para que pueda gestionar recursos de AWS desde la línea de comandos.

Paso

1. Vaya a. "Introducción a la CLI de AWS" Y siga las instrucciones para instalar la CLI.

Opcional: Cree un usuario de IAM

Cree un usuario de IAM para que pueda utilizar y gestionar los recursos y servicios de AWS con mayor seguridad. También puede omitir este paso y utilizar un usuario de IAM existente con el servicio Astra Control Service.

Paso

1. Vaya a. "Creación de usuarios de IAM" Y siga las instrucciones para crear un usuario de IAM.

Cree y adjunte una directiva de permisos

Cree una directiva con los permisos necesarios para que Astra Control Service interactúe con su cuenta de AWS.

Pasos

1. Cree un nuevo archivo llamado `policy.json`.
2. Copie el siguiente contenido JSON en el archivo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "fsx:DescribeVolumes",
                "ec2:DescribeRegions",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "iam:SimulatePrincipalPolicy",
                "s3:ListAllMyBuckets",
                "eks:DescribeCluster",
                "eks:ListNodegroups",
                "eks:DescribeNodegroup",
                "eks:ListClusters",
                "iam:GetUser",
                "s3:DeleteObject",
                "s3:DeleteBucket",
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Cree la política:

```
POLICY_ARN=$(aws iam create-policy  --policy-name <policy-name> --policy
-document file://policy.json  --query='Policy.Arn' --output=text)
```

4. Adjunte la política al usuario del IAM. Sustituya `<IAM-USER-NAME>` Con el nombre de usuario del usuario de IAM que ha creado o un usuario de IAM existente:

```
aws iam attach-user-policy --user-name <IAM-USER-NAME> --policy-arn
=$POLICY_ARN
```

Guarde las credenciales del usuario de IAM

Guarde las credenciales del usuario de IAM para que pueda conocer al usuario el Servicio de control de Astra.

Pasos

1. Descargue las credenciales. Sustituya `<IAM-USER-NAME>` Con el nombre de usuario del usuario de IAM que se desea utilizar:

```
aws iam create-access-key --user-name <IAM-USER-NAME> --output json >
credential.json
```

Resultado

La `credential.json` Se crea el archivo y puede importar las credenciales en Astra Control Service.

Configure Google Cloud

Hay que realizar algunos pasos para preparar su proyecto de Google Cloud antes de poder gestionar los clústeres de Google Kubernetes Engine con Astra Control Service.

> Si no empieza a utilizar Google Cloud Volumes Service para Google Cloud como back-end de almacenamiento pero tiene previsto utilizarlo más adelante, debería completar los pasos necesarios para configurar Google Cloud Volumes Service para Google Cloud ahora. La creación de una cuenta de servicio más adelante significa que puede perder el acceso a los bloques de almacenamiento existentes.

Inicio rápido para configurar Google Cloud

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Google Kubernetes Engine

Compruebe que el estado de los clústeres sea bueno y ejecute una versión de Kubernetes compatible, que los nodos de trabajador estén en línea y que ejecuten un tipo de imagen compatible, etc. Obtenga más información sobre este paso.

[Dos] (Opcional): Adquiera Cloud Volumes Service para Google Cloud

Si planea utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, vaya a la página Cloud Volumes Service de NetApp en Google Cloud Marketplace y seleccione Purchase. Obtenga más información sobre este paso.

[Tres] Habilite API en su proyecto de Google Cloud

Habilite las siguientes API de Google Cloud:

- Google Kubernetes Engine
- Almacenamiento en cloud
- API JSON para el almacenamiento en cloud

- Uso de servicios
- API de Cloud Resource Manager
- Cloud Volumes Service de NetApp
  - Necesario para Cloud Volumes Service para Google Cloud
  - Opcional (pero recomendado) para Google Persistent Disk
- API de gestión de consumidores de servicios
- API de redes de servicio
- API de gestión de servicios

Siga las instrucciones paso a paso.

[Cuatro] Cree una cuenta de servicio que tenga los permisos necesarios

Cree una cuenta de servicio de Google Cloud que tenga los siguientes permisos:

- Administrador de Kubernetes Engine
- Administrador de Cloud Volumes de NetApp
  - Necesario para Cloud Volumes Service para Google Cloud
  - Opcional (pero recomendado) para Google Persistent Disk
- Administrador de almacenamiento
- Visor del uso del servicio
- Visor de red de computación

Lea las instrucciones paso a paso.

[Cinco] Cree una clave de cuenta de servicio

Cree una clave para la cuenta de servicio y guarde el archivo de claves en una ubicación segura. Siga las instrucciones paso a paso.

[Seis] (Opcional): Configure la agrupación de redes para el VPC

Si tiene pensado utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, configure interconexión de redes entre su VPC y Cloud Volumes Service para Google Cloud. Siga las instrucciones paso a paso.

Requisitos del clúster GKE

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service. Tenga en cuenta que algunos de estos requisitos solo son aplicables si planea utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento.

La versión de Kubernetes

Un clúster de debe ejecutar una versión de Kubernetes en el rango de 1,26 a 1,28.

Tipo de imagen

El tipo de imagen para cada nodo de trabajo debe ser `COS_CONTAINERD`.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Región de Google Cloud

Si piensa utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, los clústeres se deben ejecutar en un "Región de Google Cloud en la que es compatible Cloud Volumes Service para Google Cloud." Tenga en cuenta que Astra Control Service admite ambos tipos de servicios: CVS y CVS-Performance. Como práctica recomendada, debe elegir una región que sea compatible con Cloud Volumes Service para Google Cloud, incluso si no la utiliza como back-end de almacenamiento. Esto facilita el uso de Cloud Volumes Service para Google Cloud como back-end de almacenamiento futuro si cambian sus requisitos de rendimiento.

Redes

Si planea usar Cloud Volumes Service para Google Cloud como back-end de almacenamiento, el clúster debe residir en un VPC que tenga una relación entre iguales con Cloud Volumes Service para Google Cloud. Este paso se describe a continuación.

Clústeres privados

Si el clúster es privado, el "redes autorizadas" Debe permitir la dirección IP del servicio Astra Control:

52.188.218.166/32

Modo de funcionamiento para un clúster GKE

Debe usar el modo de funcionamiento estándar. El modo de piloto automático no se ha probado en este momento. "Obtenga más información sobre los modos de funcionamiento".

Pools de almacenamiento

Si usa NetApp Cloud Volumes Service como back-end de almacenamiento con el tipo de servicio CVS, debe configurar los pools de almacenamiento antes de poder aprovisionar volúmenes. Consulte "Tipo de servicio, clases de almacenamiento y tamaño VP para clústeres GKE" si quiere más información.

Opcional: Adquiera Cloud Volumes Service para Google Cloud

Astra Control Service puede utilizar Cloud Volumes Service para Google Cloud como back-end de almacenamiento para sus volúmenes persistentes. Si planea utilizar este servicio, debe adquirir Cloud Volumes Service para Google Cloud en Google Cloud Marketplace para permitir la facturación de volúmenes persistentes.

Paso

1. Vaya a la "Página de Cloud Volumes Service de NetApp" En Google Cloud Marketplace, seleccione **Compra** y siga las indicaciones.

   "Siga las instrucciones paso a paso de la documentación de Google Cloud para adquirir y activar el servicio".

Habilite API en su proyecto

Su proyecto necesita permisos para acceder a API específicas de Google Cloud. Las API se utilizan para interactuar con recursos de Google Cloud, como los clústeres de Google Kubernetes Engine (GKE) y el almacenamiento de Cloud Volumes Service de NetApp.

Paso

1. "Utilice la consola de Google Cloud o la interfaz de línea de comandos gcloud para habilitar las siguientes API":
    - Google Kubernetes Engine
    - Almacenamiento en cloud
    - API JSON para el almacenamiento en cloud
    - Uso de servicios
    - API de Cloud Resource Manager
    - NetApp Cloud Volumes Service (necesario para Cloud Volumes Service para Google Cloud)
    - API de gestión de consumidores de servicios
    - API de redes de servicio
    - API de gestión de servicios

En el siguiente vídeo se muestra cómo habilitar las API desde la consola de Google Cloud.

► https://docs.netapp.com/es-es/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

Cree una cuenta de servicio

Astra Control Service utiliza una cuenta de servicio de Google Cloud para facilitar la gestión de datos de aplicaciones de Kubernetes en su nombre.

Pasos

1. Vaya a Google Cloud y. "cree una cuenta de servicio mediante la consola, el comando gcloud u otro método preferido".
2. Otorgue a la cuenta de servicio las siguientes funciones:
    - **Kubernetes Engine Admin**: Se utiliza para enumerar clústeres y crear acceso de administrador para administrar aplicaciones.
    - **NetApp Cloud Volumes Admin**: Se utiliza para gestionar el almacenamiento persistente para aplicaciones.
    - **Administrador de almacenamiento**: Se utiliza para gestionar bloques y objetos para copias de seguridad de aplicaciones.
    - **Visor de uso del servicio**: Se utiliza para comprobar si están habilitadas las API necesarias de Cloud Volumes Service para Google Cloud.
    - **Visor de red de computación**: Se utiliza para comprobar si el VPC de Kubernetes está permitido para llegar a Cloud Volumes Service para Google Cloud.

Si desea usar gcloud, puede seguir los pasos de la interfaz Astra Control. Seleccione **cuenta > credenciales > Agregar credenciales** y, a continuación, seleccione **instrucciones**.

Si desea utilizar la consola de Google Cloud, en el siguiente vídeo se muestra cómo crear la cuenta de servicio desde la consola.

► https://docs.netapp.com/es-es/astra-control-service/media/get-started/video-create-gcp-service-

account.mp4 *(video)*

Configure la cuenta de servicio para un VPC compartido

Para administrar clústeres GKE que residen en un proyecto, pero que usan un VPC de otro proyecto (un VPC compartido), entonces debe especificar la cuenta de servicio Astra como miembro del proyecto host con la función **Visor de red informática**.

Pasos

1. Desde la consola de Google Cloud, vaya a **IAM & Admin** y seleccione **Cuentas de servicio**.
2. Busque la cuenta de servicio de Astra que tiene "los permisos necesarios" y, a continuación, copie la dirección de correo electrónico.
3. Vaya al proyecto anfitrión y seleccione **IAM y Admin** > **IAM**.
4. Seleccione **Agregar** y agregue una entrada para la cuenta de servicio.
   a. **Nuevos miembros**: Introduzca la dirección de correo electrónico de la cuenta de servicio.
   b. **Rol**: Seleccione **Visor de redes de computación**.
   c. Seleccione **Guardar**.

Resultado

La adición de un clúster GKE mediante un VPC compartido funcionará por completo con Astra.

Cree una clave de cuenta de servicio

En lugar de proporcionar un nombre de usuario y una contraseña al Servicio de control de Astra, proporcionará una clave de cuenta de servicio al agregar su primer clúster. Astra Control Service utiliza la clave de cuenta de servicio para establecer la identidad de la cuenta de servicio que acaba de configurar.

La clave de cuenta de servicio es texto sin formato almacenado en el formato JavaScript Object Notation (JSON). Contiene información sobre los recursos de GCP a los que tiene permiso para acceder.

Solo puede ver o descargar el archivo JSON cuando crea la clave. Sin embargo, puede crear una nueva clave en cualquier momento.

Pasos

1. Vaya a Google Cloud y. "cree una clave de cuenta de servicio mediante la consola, el comando gcloud u otro método preferido".
2. Cuando se le solicite, guarde el archivo de claves de la cuenta de servicio en una ubicación segura.

En el siguiente vídeo se muestra cómo crear la clave de cuenta de servicio desde la consola de Google Cloud.

► https://docs.netapp.com/es-es/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

Opcional: Configure la agrupación de redes para el VPC

Si piensa utilizar Cloud Volumes Service para Google Cloud como servicio de back-end de almacenamiento, el paso final es configurar una agrupación de redes entre su VPC y Cloud Volumes Service para Google Cloud.

La forma más sencilla de configurar Network peering es obtener los comandos gcloud directamente de Cloud Volumes Service. Los comandos se encuentran disponibles en Cloud Volumes Service al crear un nuevo sistema de archivos.

Pasos

1. "Ve a los mapas de regiones globales de NetApp BlueXP" E identifique el tipo de servicio que usará en la región de Google Cloud en la que resida su clúster.

   Cloud Volumes Service ofrece dos tipos de servicios: CVS y CVS-Performance. "Obtenga más información sobre estos tipos de servicio".

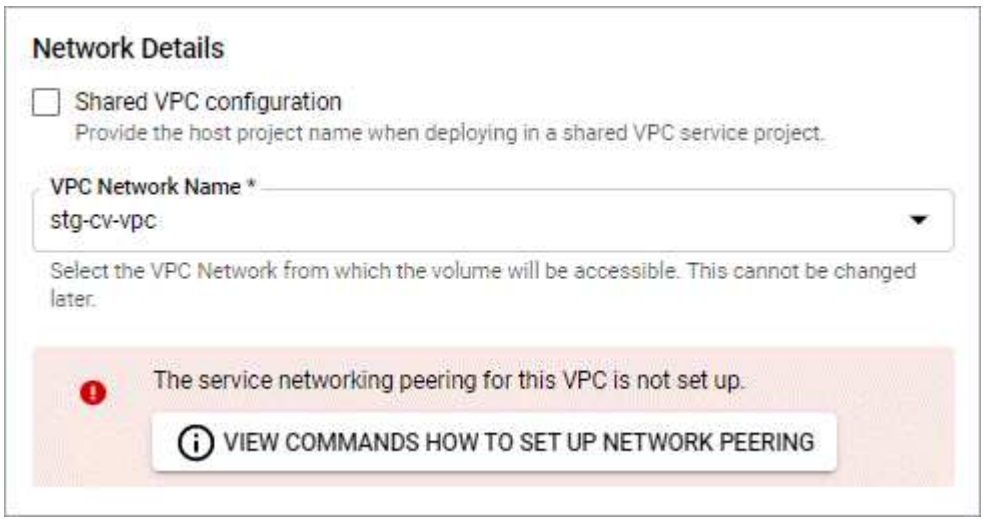
2. "Vaya a Cloud Volumes en Google Cloud Platform".
3. En la página **Volumes**, seleccione **Crear**.
4. En **Tipo de servicio**, seleccione **CVS** o **CVS-Performance**.

   Debe elegir el tipo de servicio correcto para su región de Google Cloud. Este es el tipo de servicio que ha identificado en el paso 1. Después de seleccionar un tipo de servicio, la lista de regiones de la página se actualiza con las regiones en las que se admite ese tipo de servicio.

   Después de este paso, solo tendrá que introducir la información de red para obtener los comandos.

5. En **Región**, seleccione su región y zona.
6. En **Detalles de red**, seleccione su VPC.

   Si no ha configurado la conexión de red, verá la siguiente notificación:



7. Seleccione el botón para ver los comandos de configuración de conexión de red.
8. Copie los comandos y ejecútelos en Cloud Shell.

   Para obtener más detalles sobre el uso de estos comandos, consulte "Inicio rápido de Cloud Volumes

Service para GCP".

"Obtenga más información sobre cómo configurar el acceso a los servicios privados y la configuración de la conexión a redes".

9. Una vez que haya terminado, puede seleccionar cancelar en la página **Crear sistema de archivos**.

   Comenzamos a crear este volumen sólo para obtener los comandos de conexión en red.

Configure Microsoft Azure con Azure NetApp Files

Es necesario realizar algunos pasos para preparar su suscripción a Microsoft Azure antes de poder gestionar los clústeres de Azure Kubernetes Service con Astra Control Service. Siga estas instrucciones si tiene pensado utilizar Azure NetApp Files como back-end de almacenamiento.

Inicio rápido para configurar Azure

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Azure Kubernetes Service

Compruebe que el estado de los clústeres sea bueno y ejecute una versión compatible de Kubernetes, que los pools de nodos estén en línea y que ejecuten Linux, etc. Obtenga más información sobre este paso.

[Dos] Regístrese para Microsoft Azure

Cree una cuenta de Microsoft Azure. Obtenga más información sobre este paso.

[Tres] Regístrese para Azure NetApp Files

Registre el proveedor de recursos de NetApp. Obtenga más información sobre este paso.

[Cuatro] Cree una cuenta de NetApp

Vaya a Azure NetApp Files en el portal de Azure y cree una cuenta de NetApp. Obtenga más información sobre este paso.

[Cinco] Configure pools de capacidad

Configure uno o varios pools de capacidad para los volúmenes persistentes. Obtenga más información sobre este paso.

[Seis] Delegar una subred en Azure NetApp Files

Delegue una subred en Azure NetApp Files para que el servicio de control de Astra pueda crear volúmenes persistentes en esa subred. Obtenga más información sobre este paso.

[Siete] Cree un principal de servicio de Azure

Cree una entidad de servicio de Azure con la función Colaborador. Obtenga más información sobre este paso.

[Ocho] Opcional: Configurar la redundancia para bloques de backup de Azure

De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Como paso opcional, puede configurar un nivel de redundancia más duradero para bloques de Azure. Obtenga más información sobre este paso.

Requisitos del clúster de Azure Kubernetes Service

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service.

La versión de Kubernetes

Los clústeres deben ejecutar Kubernetes, de la versión 1,26 a la 1,28.

Tipo de imagen

El tipo de imagen para todos los pools de nodos debe ser Linux.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Región de Azure

Los clústeres deben residir en una región donde Azure NetApp Files esté disponible. "Consulte los productos de Azure por región".

Suscripción

Los clústeres deben residir en una suscripción en la que Azure NetApp Files esté habilitado. Podrá elegir una suscripción cuando lo desee Regístrese para Azure NetApp Files.

Neta virtual

Considere los siguientes requisitos de vnet:

- Los clústeres deben residir en una red virtual que tenga acceso directo a una subred delegada de Azure NetApp Files. Aprenda a configurar una subred delegada.
- Si sus clústeres de Kubernetes están en una vnet con una relación entre iguales a la subred delegada de Azure NetApp Files que se encuentra en otra vnet, ambos lados de la conexión de paridad deben estar en línea.
- Tenga en cuenta que el límite predeterminado para el número de IP utilizadas en un vnet (incluidos los VNets de conexión inmediata) con Azure NetApp Files es 1,000. "Ver los límites de recursos de Azure NetApp Files".

  Si está cerca del límite, tiene dos opciones:

  - Puede hacerlo "enviar una solicitud de aumento de límite". Si necesita ayuda, póngase en contacto con su representante de NetApp.
  - Al crear un nuevo clúster de Amazon Kubernetes Service (AKS), especifique una nueva red para el clúster. Una vez creada la nueva red, aprovisione una nueva subred y delegue la subred a Azure NetApp Files.

Regístrese para Microsoft Azure

Si no tiene una cuenta de Microsoft Azure, comience registrándose en Microsoft Azure.

Pasos

1. Vaya a la "Página de suscripción a Azure" Para suscribirse al servicio de Azure.
2. Seleccione un plan y siga las instrucciones para completar la suscripción.

Regístrese para Azure NetApp Files

Obtenga acceso a Azure NetApp Files registrando el proveedor de recursos de NetApp.

Pasos

1. Inicie sesión en el portal de Azure.
2. "Siga la documentación de Azure NetApp Files para registrar el proveedor de recursos de NetApp".

Cree una cuenta de NetApp

Cree una cuenta de NetApp en Azure NetApp Files.

Paso

1. "Siga la documentación de Azure NetApp Files para crear una cuenta de NetApp desde el portal de Azure".

Configure un pool de capacidad

Se requieren uno o más pools de capacidad para que Astra Control Service pueda aprovisionar volúmenes persistentes en un pool de capacidad. Astra Control Service no crea pools de capacidad para usted.

Tenga en cuenta lo siguiente al configurar pools de capacidad para sus aplicaciones de Kubernetes:

- Los pools de capacidad deben crearse en la misma región de Azure en la que los clústeres de AKS se gestionarán con Astra Control Service.
- Un pool de capacidad puede tener un nivel de servicio Ultra, Premium o estándar. Cada uno de estos niveles de servicio está diseñado para satisfacer distintas necesidades de rendimiento. El servicio Astra Control es compatible con las tres.

  Es necesario configurar un pool de capacidad para cada nivel de servicio que se desea usar con los clústeres de Kubernetes.

  "Obtenga más información acerca de los niveles de servicio de Azure NetApp Files".

- Antes de crear un pool de capacidad para las aplicaciones que pretenda proteger con Astra Control Service, elija el rendimiento y la capacidad necesarios para esas aplicaciones.

  El aprovisionamiento de la cantidad adecuada de capacidad garantiza que los usuarios puedan crear volúmenes persistentes a medida que sean necesarios. Si la capacidad no está disponible, no se pueden aprovisionar los volúmenes persistentes.

- Un pool de capacidad de Azure NetApp Files puede usar el tipo de calidad de servicio manual o automática. Astra Control Service admite pools de capacidad de QoS automática. No se admiten pools de capacidad de calidad de servicio manual.

Paso

1. "Siga la documentación de Azure NetApp Files para configurar un pool de capacidad de calidad de servicio automática".

Delegar una subred en Azure NetApp Files

Debe delegar una subred en Azure NetApp Files para que el Servicio de control Astra pueda crear volúmenes persistentes en esa subred. Tenga en cuenta que Azure NetApp Files permite tener sólo una subred delegada en un vnet.

Si utiliza VNets con una relación entre iguales, ambos lados de la conexión entre iguales deben estar en línea: El vnet donde residen sus clústeres de Kubernetes y el vnet que tiene la subred delegada de Azure NetApp Files.

Paso

1. "Siga la documentación de Azure NetApp Files para delegar una subred en Azure NetApp Files".

Después de terminar

Espere unos 10 minutos antes de detectar el clúster que se ejecuta en la subred delegada.

Cree un principal de servicio de Azure

Astra Control Service requiere una entidad de servicio de Azure que tenga asignada la función Contributor. Astra Control Service utiliza este servicio principal para facilitar la gestión de los datos de aplicaciones de Kubernetes en su nombre.

Un principal de servicio es una identidad creada específicamente para su uso con aplicaciones, servicios y herramientas. La asignación de un rol al director de servicio restringe el acceso a recursos específicos de Azure.

Siga los pasos que se indican a continuación para crear un principal de servicio con la CLI de Azure. Deberá guardar el resultado en un archivo JSON y proporcionarlo al servicio de control de Astra más adelante. "Consulte la documentación de Azure para obtener más detalles sobre el uso de la CLI".

En los pasos siguientes se asume que tiene permiso para crear un principal de servicio y que tiene instalado el SDK de Microsoft Azure (comando az) en su equipo.

Requisitos

- El principal de servicio debe utilizar autenticación regular. No se admiten certificados.
- El director de servicio debe tener acceso a su suscripción de Azure a Contributor o propietario.
- La suscripción o el grupo de recursos que elija para Scope debe contener los clústeres de AKS y su cuenta de Azure NetApp Files.

Pasos

1. Identifique la suscripción y el ID de inquilino en los que residen los clústeres de AKS (estos son los clústeres que desea gestionar en Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Realice una de las siguientes acciones, en función de si utiliza una suscripción completa o un grupo de

recursos:

- Cree el principal de servicio, asigne la función Colaborador y especifique el ámbito de toda la suscripción donde residen los clústeres.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

- Cree el principal de servicio, asigne la función Colaborador y especifique el grupo de recursos donde residen los clústeres.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. Almacene la salida de la CLI de Azure resultante como archivo JSON.

   Tendrá que proporcionar este archivo para que Astra Control Service pueda descubrir sus clústeres de AKS y gestionar las operaciones de gestión de datos de Kubernetes. "Obtenga más información sobre la gestión de credenciales en Astra Control Service".

4. Opcional: Agregue el ID de suscripción al archivo JSON para que Astra Control Service rellene automáticamente el ID cuando seleccione el archivo.

   De lo contrario, deberá introducir el identificador de suscripción en Astra Control Service cuando se le solicite.

   ejemplo

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Opcional: Pruebe el director de servicio. Elija entre los siguientes comandos de ejemplo según el ámbito que utilice su principal de servicio.

Alcance de la suscripción

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Ámbito del grupo de recursos

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Opcional: Configurar la redundancia para bloques de backup de Azure

Puede configurar un nivel de redundancia más duradero para bloques de backup de Azure. De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Para utilizar una opción de redundancia más duradera para bloques de Azure, debe hacer lo siguiente:

Pasos

1. Cree una cuenta de almacenamiento de Azure que utilice el nivel de redundancia necesario "estas instrucciones".
2. Cree un contenedor de Azure en la nueva cuenta de almacenamiento con "estas instrucciones".
3. Agregue el contenedor como cucharón al servicio de control Astra. Consulte "Añadir un bloque más".
4. (Opcional) para utilizar el bloque recién creado como bloque predeterminado para los backups de Azure, establezca esta opción como el bloque predeterminado para Azure. Consulte "Cambiar el bloque predeterminado".

Configure Microsoft Azure con discos gestionados de Azure

Es necesario realizar algunos pasos para preparar su suscripción a Microsoft Azure antes de poder gestionar los clústeres de Azure Kubernetes Service con Astra Control Service. Siga estas instrucciones si tiene pensado utilizar discos gestionados de Azure como back-end de almacenamiento.

Inicio rápido para configurar Azure

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

[Uno] Revise los requisitos del servicio Astra Control para Azure Kubernetes Service

Compruebe que el estado de los clústeres sea bueno y ejecute una versión compatible de Kubernetes, que los pools de nodos estén en línea y que ejecuten Linux, etc. Obtenga más información sobre este paso.

[Dos] Regístrese para Microsoft Azure

Cree una cuenta de Microsoft Azure. Obtenga más información sobre este paso.

[Tres] Cree un principal de servicio de Azure

Cree una entidad de servicio de Azure con la función Colaborador. Obtenga más información sobre este paso.

[Cuatro] Configure los detalles del controlador de la interfaz de almacenamiento del contenedor (CSI)

Necesita configurar su suscripción a Azure y el clúster para que funcionen con los controladores CSI. Obtenga más información sobre este paso.

[Cinco] Opcional: Configurar la redundancia para bloques de backup de Azure

De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Como paso opcional, puede configurar un nivel de redundancia más duradero para bloques de Azure. Obtenga más información sobre este paso.

Requisitos del clúster de Azure Kubernetes Service

Un clúster de Kubernetes debe cumplir los siguientes requisitos para que pueda detectar y gestionar estos sistemas desde el servicio Astra Control Service.

La versión de Kubernetes

Los clústeres deben ejecutar Kubernetes, de la versión 1,26 a la 1,28.

Tipo de imagen

El tipo de imagen para todos los pools de nodos debe ser Linux.

Estado del clúster

Los clústeres deben ejecutarse en buen estado y tener al menos un nodo de trabajo en línea sin nodos de trabajo en estado con errores.

Región de Azure

Como práctica recomendada, debe elegir una región que sea compatible con Azure NetApp Files, incluso si no la utiliza como back-end de almacenamiento. Esto facilita el uso de Azure NetApp Files como back-end de almacenamiento en el futuro si sus requisitos de rendimiento cambian. "Consulte los productos de Azure por región".

Controladores CSI

Los clústeres deben tener instalados los controladores CSI adecuados.

Regístrese para Microsoft Azure

Si no tiene una cuenta de Microsoft Azure, comience registrándose en Microsoft Azure.

Pasos

1. Vaya a la "Página de suscripción a Azure" Para suscribirse al servicio de Azure.
2. Seleccione un plan y siga las instrucciones para completar la suscripción.

Cree un principal de servicio de Azure

Astra Control Service requiere una entidad de servicio de Azure que tenga asignada la función Contributor. Astra Control Service utiliza este servicio principal para facilitar la gestión de los datos de aplicaciones de Kubernetes en su nombre.

Un principal de servicio es una identidad creada específicamente para su uso con aplicaciones, servicios y herramientas. La asignación de un rol al director de servicio restringe el acceso a recursos específicos de Azure.

Siga los pasos que se indican a continuación para crear un principal de servicio con la CLI de Azure. Deberá guardar el resultado en un archivo JSON y proporcionarlo al servicio de control de Astra más adelante. "Consulte la documentación de Azure para obtener más detalles sobre el uso de la CLI".

En los pasos siguientes se asume que tiene permiso para crear un principal de servicio y que tiene instalado el SDK de Microsoft Azure (comando az) en su equipo.

Requisitos

- El principal de servicio debe utilizar autenticación regular. No se admiten certificados.
- El director de servicio debe tener acceso a su suscripción de Azure a Contributor o propietario.
- La suscripción o el grupo de recursos que elija para Scope debe contener los clústeres de AKS y su cuenta de Azure NetApp Files.

Pasos

1. Identifique la suscripción y el ID de inquilino en los que residen los clústeres de AKS (estos son los clústeres que desea gestionar en Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Realice una de las siguientes acciones, en función de si utiliza una suscripción completa o un grupo de recursos:
   - Cree el principal de servicio, asigne la función Colaborador y especifique el ámbito de toda la suscripción donde residen los clústeres.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-ID
     ```

   - Cree el principal de servicio, asigne la función Colaborador y especifique el grupo de recursos donde residen los clústeres.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-
     ID/resourceGroups/RESOURCE-GROUP-ID
     ```

3. Almacene la salida de la CLI de Azure resultante como archivo JSON.

Tendrá que proporcionar este archivo para que Astra Control Service pueda descubrir sus clústeres de AKS y gestionar las operaciones de gestión de datos de Kubernetes. "Obtenga más información sobre la gestión de credenciales en Astra Control Service".

4. Opcional: Agregue el ID de suscripción al archivo JSON para que Astra Control Service rellene automáticamente el ID cuando seleccione el archivo.

   De lo contrario, deberá introducir el identificador de suscripción en Astra Control Service cuando se le solicite.

   ejemplo

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Opcional: Pruebe el director de servicio. Elija entre los siguientes comandos de ejemplo según el ámbito que utilice su principal de servicio.

   Alcance de la suscripción

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

   Ámbito del grupo de recursos

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Configure los detalles del controlador de la interfaz de almacenamiento del contenedor (CSI)

Para utilizar discos administrados de Azure con Astra Control Service, tendrá que instalar los controladores CSI necesarios.

Active la función de controlador CSI en su suscripción a Azure

Antes de instalar los controladores CSI, debe activar la función de controlador CSI en su suscripción a Azure.

Pasos

1. Abra la interfaz de línea de comandos de Azure.
2. Ejecute el siguiente comando para registrar el controlador:

```
az feature register --namespace "Microsoft.ContainerService" --name
"EnableAzureDiskFileCSIDriver"
```

3. Ejecute el siguiente comando para garantizar que el cambio se propaga:

```
az provider register -n Microsoft.ContainerService
```

Debería ver una salida similar a la siguiente:

```
{
"id": "/subscriptions/b200155f-001a-43be-87be-
3edde83acef4/providers/Microsoft.Features/providers/Microsoft.ContainerSer
vice/features/EnableAzureDiskFileCSIDriver",
"name": "Microsoft.ContainerService/EnableAzureDiskFileCSIDriver",
"properties": {
   "state": "Registering"
},
"type": "Microsoft.Features/providers/features"
}
```

Instale los controladores CSI de disco gestionado de Azure en su clúster de Azure Kubernetes Service

Puede instalar los controladores de Azure CSI para completar la preparación.

Paso

1. Vaya a. "La documentación del controlador Microsoft CSI".
2. Siga las instrucciones para instalar los controladores CSI necesarios.

Opcional: Configurar la redundancia para bloques de backup de Azure

Puede configurar un nivel de redundancia más duradero para bloques de backup de Azure. De forma predeterminada, los bloques Astra Control Service utilizan para almacenar las copias de seguridad de Azure Kubernetes Service utilizan la opción de redundancia almacenamiento redundante local (LRS). Para utilizar una opción de redundancia más duradera para bloques de Azure, debe hacer lo siguiente:

Pasos

1. Cree una cuenta de almacenamiento de Azure que utilice el nivel de redundancia necesario "estas instrucciones".
2. Cree un contenedor de Azure en la nueva cuenta de almacenamiento con "estas instrucciones".
3. Agregue el contenedor como cucharón al servicio de control Astra. Consulte "Añadir un bloque más".

4. (Opcional) para utilizar el bloque recién creado como bloque predeterminado para los backups de Azure, establezca esta opción como el bloque predeterminado para Azure. Consulte "Cambiar el bloque predeterminado".

Regístrese para obtener una cuenta de Astra Control Service

Para utilizar el servicio de control de Astra, necesitas una cuenta del servicio de control de Astra que esté asociada con tu cuenta de BlueXP de NetApp. Completa el proceso de registro del servicio Astra Control y, si aún no tienes una cuenta de BlueXP, regístrate en BlueXP para acceder a Astra Control Service.

Regístrese para obtener una cuenta de Astra Control

Antes de iniciar sesión en Astra Control Service, necesita completar un proceso de registro para obtener una cuenta de Astra Control Service.

Cuando utilice Astra Control Service, gestionará sus aplicaciones desde una cuenta. Una cuenta incluye usuarios que pueden ver y gestionar las aplicaciones de la cuenta, así como los detalles de facturación.

Pasos

1. "Ve a la página de Astra Control en BlueXP".
2. Selecciona **Regístrate para el plan gratuito**.
3. Proporcione la información necesaria en el formulario.

   Algunas cosas importantes que debe tener en cuenta al rellenar el formulario:

   - El nombre y la dirección de su empresa deben ser precisos porque los verificamos para cumplir los requisitos de Global Trade Compliance.
   - * Nombre de cuenta Astra* es el nombre de la cuenta de Servicio Astra de su empresa. Verá este nombre en la interfaz de usuario de Astra Control Service. Tenga en cuenta que puede crear cuentas adicionales (hasta 5), si es necesario.
   - En el campo **Dirección de correo electrónico empresarial**, si tienes una cuenta de NetApp BlueXP, ingresa el correo electrónico que usas para esa cuenta aquí. Si aún no tienes una cuenta de NetApp BlueXP, utiliza la dirección de correo electrónico que introdujiste aquí cuando te registres en BlueXP.
4. Seleccione **Crear cuenta**.

Regístrese en BlueXP

El servicio Astra Control está integrado con el servicio de autenticación de NetApp BlueXP. Puedes iniciar sesión en NetApp BlueXP con tus credenciales del sitio de soporte de BlueXP o de NetApp. Si aún no tienes una cuenta del sitio de soporte de NetApp o BlueXP de NetApp, regístrate en BlueXP para poder acceder a Astra Control Service y a otros servicios cloud de NetApp. Si ya tienes una cuenta del sitio de soporte de BlueXP o NetApp y has completado el registro, podrás acceder a ella "Servicio de control Astra" Usando directamente tus credenciales del sitio de soporte de BlueXP o de NetApp.

También puedes utilizar el inicio de sesión único para iniciar sesión en BlueXP mediante las credenciales de tu directorio corporativo (identidad federada). Para obtener más información, visite la "Centro de ayuda" Y, a continuación, seleccione **Opciones de inicio de sesión de Cloud Central**.

Pasos

1. Vaya a. "BlueXP de NetApp".
2. En la parte superior derecha, selecciona **Comenzar**.
3. Seleccione **Registrarse**.
4. Rellene el formulario.

   Asegúrese de que el número de teléfono y la dirección de correo electrónico que introduce aquí son los mismos que utilizó en el formulario de registro de Astra Control anterior.

5. Seleccione **Registrarse**.

   La dirección de correo electrónico que introduzcas en estos formularios corresponde a tu ID de usuario de NetApp BlueXP. Usa este ID de usuario de BlueXP cuando te registres para obtener una nueva cuenta de Astra Control o cuando un administrador de Astra Control te invite a una cuenta existente de Astra Control.

6. Espera un correo electrónico de BlueXP de NetApp. El correo electrónico viene de la dirección saas.support@netapp.com, y puede tardar varios minutos en llegar. Asegúrese de comprobar su carpeta de spam.
7. Cuando llegue el correo electrónico, seleccione el vínculo del correo electrónico para comprobar su dirección de correo electrónico.

Resultado

Ahora tienes un inicio de sesión activo de usuario de BlueXP.

Ahora que estás registrado, puedes acceder a Astra Control directamente con tus credenciales de BlueXP desde https://astra.netapp.io.

Añada un clúster a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control. Esto te permite utilizar el servicio Astra Control para proteger tus aplicaciones en el clúster.

Según el tipo de clúster que deba añadir a Astra Control Service, deberá realizar distintos pasos para añadir el clúster.

- "Añade un clúster público gestionado por proveedores a Astra Control Service": Utilice estos pasos para agregar un clúster que tenga una dirección IP pública y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.
- "Añada un clúster privado gestionado por un proveedor a Astra Control Service": Utilice estos pasos para agregar un clúster que tenga una dirección IP privada y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.

- "Añade un clúster público autogestionado a Astra Control Service": Utilice estos pasos para agregar un cluster que tenga una dirección IP pública y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.
- "Añade un clúster privado autogestionado a Astra Control Service": Utilice estos pasos para agregar un cluster que tenga una dirección IP privada y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.

Instala Astra Connector para gestionar los clústeres

Astra Connector es el software que reside en sus clústeres gestionados y facilita la comunicación entre el clúster gestionado y Astra Control. En el caso de los clústeres que se gestionen mediante Astra Control Service, hay dos versiones disponibles de Astra Connector:

- **Versión anterior de Astra Connector**: "Instala la versión anterior de Astra Connector" En el clúster, si tiene pensado gestionar el clúster con flujos de trabajo no nativos de Kubernetes.
- [Vista previa técnica] **Conector Astra de Kubernetes declarativo**: "Instala Astra Connector para clústeres gestionados con flujos de trabajo de Kubernetes declarativos" En el clúster si tiene pensado gestionar el clúster mediante flujos de trabajo de Kubernetes declarativos. Después de instalar Astra Connector en tu clúster, el clúster se añade automáticamente a Astra Control.

> El Astra Connector declarativo de Kubernetes solo está disponible como parte del programa para la primera adopción de Astra Control (EAP). Póngase en contacto con su representante de ventas de NetApp para obtener información sobre cómo unirse al EAP.

Instala la versión anterior de Astra Connector

Astra Control Service utiliza la versión anterior de Astra Connector para permitir la comunicación entre Astra Control Service y clústeres privados que no son nativos de Kubernetes. Tienes que instalar Astra Connector en clústeres privados que quieras gestionar con flujos de trabajo que no sean nativos de Kubernetes.

La versión anterior de Astra Connector admite los siguientes tipos de clústeres privados gestionados con flujos de trabajo no nativos de Kubernetes:

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service en AWS (ROSA)
- ROSA con AWS PrivateLink
- Red Hat OpenShift Container Platform en las instalaciones

Acerca de esta tarea

- Cuando realice estos pasos, ejecute estos comandos en el clúster privado que desee administrar con Astra Control Service.
- Si utiliza un host de Bastion, emita estos comandos desde la línea de comandos del host de Bastion.

Antes de empezar

- Necesita acceso al clúster privado que desea gestionar con Astra Control Service.
- Necesitas permisos de administrador de Kubernetes para instalar el operador Astra Connector en el clúster.

Pasos

1. Instale el operador Astra Connector anterior en el clúster privado que desea gestionar con flujos de trabajo que no sean nativos de Kubernetes. Cuando se ejecuta este comando, el espacio de nombres `astra-connector-operator` se crea y la configuración se aplica al espacio de nombres:

```
kubectl apply -f https://github.com/NetApp/astra-connector-operator/releases/download/23.07.0-202310251519/astraconnector_operator.yaml
```

2. Compruebe que el operador está instalado y listo:

```
kubectl get all -n astra-connector-operator
```

3. Obtén un token de API de Astra Control. Consulte la "Documentación de Astra Automation" si desea obtener instrucciones.
4. Cree el espacio de nombres de Astra-Connector:

```
kubectl create ns astra-connector
```

5. Cree el archivo Astra Connector CR y asígnele el nombre `astra-connector-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - **<ASTRA_CONTROL_SERVICE_URL>**: La URL de la interfaz de usuario web del servicio de control de Astra. Por ejemplo:

     ```
     https://astra.netapp.io
     ```

   - **<ASTRA_CONTROL_SERVICE_API_TOKEN>**: El token de la API Astra Control que obtuviste en el paso anterior.
   - **<PRIVATE_AKS_CLUSTER_NAME>**: (Solo clústeres de AKS): El nombre del clúster privado del servicio de Azure Kubernetes. Elimine el comentario y rellene esta línea sólo si está agregando un cluster AKS privado.
   - **<ASTRA_CONTROL_ACCOUNT_ID>**: Obtenido de la interfaz de usuario web de Astra Control. Selecciona el icono de la figura en la parte superior derecha de la página y selecciona **Acceso API**.

```yaml
apiVersion: netapp.astraconnector.com/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  natssync-client:
    cloud-bridge-url: <ASTRA_CONTROL_SERVICE_URL>
  imageRegistry:
    name: theotw
    secret: ""
  astra:
    token: <ASTRA_CONTROL_SERVICE_API_TOKEN>
    #clusterName: <PRIVATE_AKS_CLUSTER_NAME>
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    acceptEULA: yes
```

6. Después de rellenar el `astra-connector-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-connector-cr.yaml
```

7. Compruebe que Astra Connector está completamente implementado:

```
kubectl get all -n astra-connector
```

8. Compruebe que el clúster esté registrado en Astra Control:

```
kubectl get astraconnector -n astra-connector
```

Debería ver una salida similar a la siguiente:

```
NAME               REGISTERED   ASTRACONNECTORID
STATUS
astra-connector    true         be475ae5-1511-4eaa-9b9e-712f09b0d065
Registered with Astra
```

Toma nota del ASTRACONNECTORID, lo necesitarás cuando añadas el clúster a Astra Control.

El futuro

Ahora que ha instalado Astra Connector, está listo para añadir su clúster privado a Astra Control Service.

- "Añada un clúster privado gestionado por un proveedor a Astra Control Service": Utilice estos pasos para agregar un clúster que tenga una dirección IP privada y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.
- "Añade un clúster privado autogestionado a Astra Control Service": Utilice estos pasos para agregar un cluster que tenga una dirección IP privada y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.

Si quiere más información

- "Añadir un clúster"

(Vista previa técnica) Instale el Astra Connector declarativo de Kubernetes

Los clústeres gestionados mediante flujos de trabajo de Kubernetes declarativos utilizan Astra Connector para permitir la comunicación entre el clúster gestionado y Astra Control. Tienes que instalar Astra Connector en todos los clústeres que gestionarás con flujos de trabajo de Kubernetes declarativos.

Instalas el conector Astra de Kubernetes declarativo mediante comandos de Kubernetes y archivos de recursos personalizados (CR).

Acerca de esta tarea

- Cuando realice estos pasos, ejecute estos comandos en el clúster que desee gestionar con Astra Control.
- Si utiliza un host de Bastion, emita estos comandos desde la línea de comandos del host de Bastion.

Antes de empezar

- Necesitas acceder al clúster que quieras gestionar con Astra Control.
- Necesitas permisos de administrador de Kubernetes para instalar el operador Astra Connector en el clúster.

> Si el clúster está configurado con la aplicación de admisión de seguridad de POD, que es el valor predeterminado para los clústeres de Kubernetes 1,25 y posteriores, tiene que habilitar las restricciones PSA en los espacios de nombres correspondientes. Consulte "Prepare su entorno para la gestión de clústeres con Astra Control" si desea obtener instrucciones.

Pasos

1. Instale el operador Astra Connector en el clúster que desee gestionar con flujos de trabajo de Kubernetes declarativos. Cuando se ejecuta este comando, el espacio de nombres `astra-connector-operator` se crea y la configuración se aplica al espacio de nombres:

```
kubectl apply -f https://github.com/NetApp/astra-connector-
operator/releases/download/24.02.0-
202403151353/astraconnector_operator.yaml
```

2. Compruebe que el operador está instalado y listo:

```
kubectl get all -n astra-connector-operator
```

3. Obtén un token de API de Astra Control. Consulte la "Documentación de Astra Automation" si desea obtener instrucciones.
4. Cree un secreto con el token. Reemplaza <API_TOKEN> por el token que has recibido de Astra Control:

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Crea un secreto de Docker para extraer la imagen de Astra Connector. Sustituya los valores entre paréntesis <> por información de su entorno:

> Puedes encontrar la instancia de <ASTRA_CONTROL_ACCOUNT_ID> en la interfaz de usuario web de Astra Control. En la interfaz de usuario web, seleccione el icono de figura en la parte superior derecha de la página y seleccione **Acceso API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Cree el archivo Astra Connector CR y asígnele el nombre `astra-connector-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <ASTRA_CONTROL_ACCOUNT_ID>: Obtenida de la interfaz de usuario web de Astra Control durante el paso anterior.
   - <CLUSTER_NAME>: El nombre que se debe asignar este clúster en Astra Control.
   - <ASTRA_CONTROL_URL>: La URL de interfaz de usuario web de Astra Control. Por ejemplo:

     ```
     https://astra.control.url
     ```

```yaml
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

7. Después de rellenar el `astra-connector-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -n astra-connector -f astra-connector-cr.yaml
```

8. Compruebe que Astra Connector está completamente implementado:

```
kubectl get all -n astra-connector
```

9. Compruebe que el clúster esté registrado en Astra Control:

```
kubectl get astraconnectors.astra.netapp.io -A
```

Debería ver una salida similar a la siguiente:

```
NAMESPACE          NAME               REGISTERED   ASTRACONNECTORID
STATUS
astra-connector    astra-connector    true         00ac8-2cef-41ac-8777-
ed0583e   Registered with Astra
```

10. Compruebe que el clúster aparezca en la lista de clústeres gestionados de la página **Clusters** de la interfaz de usuario web de Astra Control.

Agregue un clúster gestionado por el proveedor

Añade un clúster público gestionado por proveedores a Astra Control Service

Después de configurar tu entorno de cloud, estarás listo para crear un clúster de Kubernetes y luego añadirlo a Astra Control Service.

- Cree un clúster de Kubernetes
- Añada el clúster a Astra Control Service
- Cambie la clase de almacenamiento predeterminada

Cree un clúster de Kubernetes

Si todavía no tiene un clúster, puede crear uno que cumpla "Requisitos del servicio Astra Control para Amazon Elastic Kubernetes Service (EKS)". Si todavía no tiene un clúster, puede crear uno que cumpla "Requisitos del servicio Astra Control para Google Kubernetes Engine (GKE)". Si todavía no tiene un clúster, puede crear uno que cumpla "Requisitos del servicio Astra Control para Azure Kubernetes Service (AKS) con Azure NetApp Files" o. "Requisitos del servicio Astra Control Service para Azure Kubernetes Service (AKS) con discos gestionados de Azure".

> Astra Control Service es compatible con clústeres AKS que utilizan Azure Active Directory (Azure AD) para la autenticación y la gestión de identidades. Cuando cree el clúster, siga las instrucciones que se indican en "documentación oficial" Para configurar el clúster de modo que use Azure AD. Debe asegurarse de que sus clústeres cumplen los requisitos de la integración de Azure AD gestionada por AKS.

Añada el clúster a Astra Control Service

Después de iniciar sesión en Astra Control Service, el primer paso es empezar a gestionar los clústeres. Antes de añadir un clúster al servicio Astra Control Service, tendrá que realizar tareas específicas y asegurarse de que el clúster cumple determinados requisitos.

Al gestionar clústeres de Azure Kubernetes Service y Google Kubernetes Engine, tenga en cuenta que tiene dos opciones para la instalación del aprovisionador de Astra Control y la gestión del ciclo de vida:

- Puedes utilizar el servicio Astra Control para gestionar automáticamente el ciclo de vida del aprovisionador Astra Control. Para hacerlo, asegúrese de que Astra Trident no esté instalado y que Astra Control Provisioner no esté habilitado en el clúster que desee gestionar con Astra Control Service. En este caso, Astra Control Service habilita automáticamente Astra Control Provisioning cuando se comienza a gestionar el clúster, y las actualizaciones del aprovisionador de Astra Control se realizan automáticamente.
- Puede gestionar el ciclo de vida de Astra Control Provisionador tú mismo. Para ello, habilite el aprovisionador de Astra Control en el clúster antes de gestionar el clúster con Astra Control Service. En este caso, Astra Control Service detecta que Astra Control Provisioning ya está habilitado y no lo reinstala ni gestiona las actualizaciones del aprovisionador de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para seguir los pasos, habilita el aprovisionador de Astra Control.

Al gestionar clústeres de Amazon Web Services con Astra Control Service, si necesita back-ends de almacenamiento que solo puede utilizarse con el aprovisionador de Astra Control, tendrá que habilitar el aprovisionador de Astra Control manualmente en el clúster antes de gestionarlo con el servicio de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para conocer los pasos que hay que seguir para habilitar el aprovisionador de Astra Control.

Antes de empezar

Amazon Web Services

- Debe tener el archivo JSON que contenga las credenciales del usuario de IAM que creó el clúster. "Aprenda a crear un usuario de IAM".
- Se requiere el aprovisionador de Astra Control para Amazon FSx para NetApp ONTAP. Si tienes pensado usar Amazon FSx para NetApp ONTAP como back-end de almacenamiento para tu clúster de EKS, consulte la información del aprovisionador de control de Astra en la "Requisitos del clúster de EKS".
- (Opcional) Si necesita proporcionarlo `kubectl` Consulte las instrucciones de la sección para obtener acceso al comando de un clúster a otros usuarios de IAM que no son el creador del clúster "¿Cómo puedo proporcionar acceso a otros usuarios de IAM y a otras funciones tras la creación del clúster en Amazon EKS?".
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Amazon Web Services. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Microsoft Azure

- Debe tener el archivo JSON que contenga el resultado de la CLI de Azure cuando cree el principal del servicio. "Aprenda a configurar un director de servicios".

  También necesitará su ID de suscripción de Azure si no lo ha añadido al archivo JSON.

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Microsoft Azure. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Google Cloud

- Debe tener el archivo de clave de cuenta de servicio para una cuenta de servicio que tenga los permisos necesarios. "Aprenda a configurar una cuenta de servicio".
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Google Cloud. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Pasos

1. (Opcional) Si añade un clúster de Amazon EKS o desea gestionar la instalación y actualizaciones de Astra Control Provisionador, habilite Astra Control Provisionador en el clúster. Consulte "Habilita el aprovisionador de Astra Control" para pasos de habilitación.
2. Abra la interfaz de usuario web de Astra Control Service en un navegador.
3. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

4. **Proveedor**: Seleccione su proveedor de cloud y, a continuación, proporcione las credenciales necesarias para crear una nueva instancia de cloud, o seleccione una instancia de cloud existente para utilizar.
5. **Amazon Web Services**: Proporcione detalles sobre su cuenta de usuario de Amazon Web Services IAM cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener las credenciales del usuario IAM que creó el clúster.

6. **Microsoft Azure**: Proporcione detalles sobre el principal de servicio de Azure cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener el resultado de la CLI de Azure al crear el principal del servicio. También puede incluir su ID de suscripción para que se agregue automáticamente a Astra. De lo contrario, deberá introducir manualmente el ID después de proporcionar JSON.

7. **Google Cloud Platform**: Proporcione el archivo de clave de cuenta de servicio cargando el archivo o pegando el contenido del portapapeles.

   Astra Control Service utiliza la cuenta de servicio para descubrir los clústeres que se ejecutan en Google Kubernetes Engine.

8. **Otros**: Esta pestaña es para uso solo con clusters autogestionados.
   a. **Nombre de la instancia de nube**: Proporcione un nombre para la nueva instancia de nube que se creará al agregar este clúster. Más información acerca de "instancias de cloud".
   b. Seleccione **Siguiente**.

      Astra Control Service muestra una lista de clústeres entre los que puede elegir.

   c. **Clúster**: Selecciona un clúster de la lista para añadirlo a Astra Control Service.

      > Al seleccionar de la lista de clusters, preste atención a la columna **Eligiblity**. Si un clúster es «no elegible» o «parcialmente elegible», pase el cursor por encima del estado para determinar si hay un problema con el clúster. Por ejemplo, podría identificar que el clúster no tiene un nodo de trabajo.

   d. Seleccione **Siguiente**.
   e. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
9. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
10. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:

- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
  - "Azure NetApp Files"
  - "Discos gestionados de Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX para ONTAP de NetApp"
  - "Cloud Volumes ONTAP de NetApp"

  Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

  a. Seleccione **Siguiente**.
  b. **Revisar y aprobar**: Revise los detalles de la configuración.
  c. Selecciona **Add** para agregar el clúster a Astra Control Service.

Resultado

Si este es el primer clúster que se ha añadido para este proveedor de cloud, Astra Control Service crea un almacén de objetos para el proveedor de cloud para realizar backups de las aplicaciones que se ejecutan en clústeres aptos. (Cuando añada clústeres posteriores para este proveedor de cloud, no se crearán más almacenes de objetos). Si ha especificado una clase de almacenamiento predeterminada, Astra Control Service establece la clase de almacenamiento predeterminada que ha especificado. En el caso de clústeres gestionados en Amazon Web Services o Google Cloud Platform, Astra Control Service también crea una cuenta de administrador en el clúster. Estas acciones pueden tardar varios minutos.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Añada un clúster privado gestionado por un proveedor a Astra Control Service

Puede utilizar Astra Control Service para gestionar clústeres privados de Google Kubernetes Engine (GKE). En estas instrucciones se asume que ya ha creado un clúster privado de AKS o OpenShift y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres privados de AKS o OpenShift, consulte la siguiente documentación:

- "Documentación de Azure para clústeres AKS privados"
- "Documentación de Azure para clústeres de OpenShift privados"

Puede utilizar Astra Control Service para gestionar clústeres privados de Azure Kubernetes Service (AKS) y clústeres privados de Red Hat OpenShift en AKS. En estas instrucciones se asume que ya ha creado un clúster privado de AKS o OpenShift y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres privados de AKS o OpenShift, consulte la siguiente documentación:

- "Documentación de Azure para clústeres AKS privados"
- "Documentación de Azure para clústeres de OpenShift privados"

Puede utilizar Astra Control Service para gestionar clústeres privados de Amazon Elastic Kubernetes Service (EKS). En estas instrucciones se asume que ya ha creado un clúster EKS privado y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres EKS privados, consulte la "Documentación de Amazon EKS".

Tienes que realizar las siguientes tareas para añadir tu clúster privado a Astra Control Service:

1. Instala Astra Connector
2. Configure el almacenamiento persistente
3. Añada el clúster gestionado por proveedores privados a Astra Control Service

Instala Astra Connector

Antes de agregar un clúster privado, tiene que instalar Astra Connector en el clúster para que Astra Control se pueda comunicar con él. Consulte "Instala la versión anterior de Astra Connector para clústeres privados gestionados con flujos de trabajo que no sean nativos de Kubernetes" si desea obtener instrucciones.

Configure el almacenamiento persistente

Configure el almacenamiento persistente para el clúster. Consulte la documentación para empezar para obtener más información sobre la configuración del almacenamiento persistente:

- "Configure Microsoft Azure con Azure NetApp Files"
- "Configure Microsoft Azure con discos gestionados de Azure"
- "Configure Amazon Web Services"
- "Configure Google Cloud"

Añada el clúster gestionado por proveedores privados a Astra Control Service

Ahora puede añadir el clúster privado a Astra Control Service.

Al gestionar clústeres de Azure Kubernetes Service y Google Kubernetes Engine, tenga en cuenta que tiene dos opciones para la instalación del aprovisionador de Astra Control y la gestión del ciclo de vida:

- Puedes utilizar el servicio Astra Control para gestionar automáticamente el ciclo de vida del aprovisionador Astra Control. Para hacerlo, asegúrese de que Astra Trident no esté instalado y que Astra Control Provisioner no esté habilitado en el clúster que desee gestionar con Astra Control Service. En este caso, Astra Control Service habilita automáticamente Astra Control Provisioning cuando se comienza a gestionar el clúster, y las actualizaciones del aprovisionador de Astra Control se realizan automáticamente.
- Puede gestionar el ciclo de vida de Astra Control Provisionador tú mismo. Para ello, habilite el aprovisionador de Astra Control en el clúster antes de gestionar el clúster con Astra Control Service. En este caso, Astra Control Service detecta que Astra Control Provisioning ya está habilitado y no lo reinstala ni gestiona las actualizaciones del aprovisionador de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para seguir los pasos, habilita el aprovisionador de Astra Control.

Al gestionar clústeres de Amazon Web Services con Astra Control Service, si necesita back-ends de almacenamiento que solo puede utilizarse con el aprovisionador de Astra Control, tendrá que habilitar el aprovisionador de Astra Control manualmente en el clúster antes de gestionarlo con el servicio de Astra Control. Consulte "Habilita el aprovisionador de Astra Control" Para conocer los pasos que hay que seguir para habilitar el aprovisionador de Astra Control.

Antes de empezar

Amazon Web Services

- Debe tener el archivo JSON que contenga las credenciales del usuario de IAM que creó el clúster. "Aprenda a crear un usuario de IAM".
- Se requiere el aprovisionador de Astra Control para Amazon FSx para NetApp ONTAP. Si tienes pensado usar Amazon FSx para NetApp ONTAP como back-end de almacenamiento para tu clúster de EKS, consulte la información del aprovisionador de control de Astra en la "Requisitos del clúster de EKS".
- (Opcional) Si necesita proporcionarlo `kubectl` Consulte las instrucciones de la sección para obtener acceso al comando de un clúster a otros usuarios de IAM que no son el creador del clúster "¿Cómo puedo proporcionar acceso a otros usuarios de IAM y a otras funciones tras la creación del clúster en Amazon EKS?".
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Amazon Web Services. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Microsoft Azure

- Debe tener el archivo JSON que contenga el resultado de la CLI de Azure cuando cree el principal del servicio. "Aprenda a configurar un director de servicios".

  También necesitará su ID de suscripción de Azure si no lo ha añadido al archivo JSON.

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Microsoft Azure. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Google Cloud

- Debe tener el archivo de clave de cuenta de servicio para una cuenta de servicio que tenga los permisos necesarios. "Aprenda a configurar una cuenta de servicio".
- Si el clúster es privado, el "redes autorizadas" Debe permitir la dirección IP del servicio Astra Control:

  52.188.218.166/32

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Google Cloud. Consulte el Cloud Volumes ONTAP "documentación de configuración".

Pasos

1. (Opcional) Si añade un clúster de Amazon EKS o desea gestionar la instalación y actualizaciones de Astra Control Provisionador, habilite Astra Control Provisionador en el clúster. Consulte "Habilita el aprovisionador de Astra Control" para pasos de habilitación.
2. Abra la interfaz de usuario web de Astra Control Service en un navegador.
3. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

4. **Proveedor**: Seleccione su proveedor de cloud y, a continuación, proporcione las credenciales necesarias para crear una nueva instancia de cloud, o seleccione una instancia de cloud existente para utilizar.

5. **Amazon Web Services**: Proporcione detalles sobre su cuenta de usuario de Amazon Web Services IAM cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener las credenciales del usuario IAM que creó el clúster.

6. **Microsoft Azure**: Proporcione detalles sobre el principal de servicio de Azure cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

   El archivo JSON debe contener el resultado de la CLI de Azure al crear el principal del servicio. También puede incluir su ID de suscripción para que se agregue automáticamente a Astra. De lo contrario, deberá introducir manualmente el ID después de proporcionar JSON.

7. **Google Cloud Platform**: Proporcione el archivo de clave de cuenta de servicio cargando el archivo o pegando el contenido del portapapeles.

   Astra Control Service utiliza la cuenta de servicio para descubrir los clústeres que se ejecutan en Google Kubernetes Engine.

8. **Otros**: Esta pestaña es para uso solo con clusters autogestionados.
   a. **Nombre de la instancia de nube**: Proporcione un nombre para la nueva instancia de nube que se creará al agregar este clúster. Más información acerca de "instancias de cloud".
   b. Seleccione **Siguiente**.

      Astra Control Service muestra una lista de clústeres entre los que puede elegir.

   c. **Clúster**: Selecciona un clúster de la lista para añadirlo a Astra Control Service.

      > Al seleccionar de la lista de clusters, preste atención a la columna **Eligiblity**. Si un clúster es «no elegible» o «parcialmente elegible», pase el cursor por encima del estado para determinar si hay un problema con el clúster. Por ejemplo, podría identificar que el clúster no tiene un nodo de trabajo.

9. Seleccione **Siguiente**.
10. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
    a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
    b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:

- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
- "Azure NetApp Files"
- "Discos gestionados de Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX para ONTAP de NetApp"
- "Cloud Volumes ONTAP de NetApp"

  Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

c. Seleccione **Siguiente**.

d. **Revisar y aprobar**: Revise los detalles de la configuración.

e. Selecciona **Add** para agregar el clúster a Astra Control Service.

Resultado

Si este es el primer clúster que se ha añadido para este proveedor de cloud, Astra Control Service crea un almacén de objetos para el proveedor de cloud para realizar backups de las aplicaciones que se ejecutan en clústeres aptos. (Cuando añada clústeres posteriores para este proveedor de cloud, no se crearán más almacenes de objetos). Si ha especificado una clase de almacenamiento predeterminada, Astra Control Service establece la clase de almacenamiento predeterminada que ha especificado. En el caso de clústeres gestionados en Amazon Web Services o Google Cloud Platform, Astra Control Service también crea una cuenta de administrador en el clúster. Estas acciones pueden tardar varios minutos.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Agregue un clúster autogestionado

Añade un clúster público autogestionado a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control.

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Puede agregar un clúster autogestionado a Astra Control Service cargando un `kubeconfig.yaml` archivo. Deberá asegurarse de que el clúster cumple los requisitos que se indican aquí.

Distribuciones de Kubernetes compatibles

Puede utilizar Astra Control Service para gestionar los siguientes tipos de clústeres públicos autogestionados:

Distribución de Kubernetes	Versiones compatibles
Kubernetes (ascendente)	1,27 a 1,29
Motor Kubernetes de rancher (RKE)	RKE 1: Versiones 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versiones 1.23.16 y 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versiones 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
OpenShift Container Platform de Red Hat	4,12 hasta 4,14

En estas instrucciones se asume que ya ha creado un clúster autogestionado.

- Añada el clúster a Astra Control Service
- Cambie la clase de almacenamiento predeterminada

Añada el clúster a Astra Control Service

Después de iniciar sesión en Astra Control Service, el primer paso es empezar a gestionar los clústeres. Antes de añadir un clúster al servicio Astra Control Service, tendrá que realizar tareas específicas y asegurarse de que el clúster cumple determinados requisitos.

Antes de empezar

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Los clústeres autogestionados pueden utilizar Astra Control Provisioner para interactuar con los servicios de almacenamiento de NetApp o pueden usar controladores de la interfaz de almacenamiento de contenedores (CSI) para interactuar con Amazon Elastic Block Store (EBS), los discos gestionados de Azure y el disco persistente de Google.

Astra Control Service es compatible con clústeres autogestionados que utilizan las siguientes distribuciones de Kubernetes:

- OpenShift Container Platform de Red Hat
- Motor Kubernetes del rancher
- Subida de Kubernetes

Su clúster autogestionado debe cumplir con los siguientes requisitos:

- El clúster debe estar accesible a través de Internet.
- Si está utilizando o planea utilizar almacenamiento habilitado con controladores CSI, se deben instalar los controladores CSI adecuados en el clúster. Para obtener más información sobre el uso de los controladores CSI para integrar el almacenamiento, consulte la documentación del servicio de almacenamiento.
- Tiene acceso al archivo kubeconfig de cluster que incluye solo un elemento de contexto. Siga "estas instrucciones" para generar un archivo kubeconfig.
- Si va a agregar el clúster mediante un archivo kubeconfig que hace referencia a una entidad de certificación (CA) privada, agregue la siguiente línea al `cluster` sección del archivo kubeconfig. Esto permite a Astra Control añadir el clúster:

  ```
  insecure-skip-tls-verify: true
  ```

- **Sólo rancher**: Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig proporcionado por Rancher para utilizar un contexto de plano de control en lugar del contexto del servidor API Rancher. Esto reduce la carga en el servidor API de Rancher y mejora el rendimiento.
- **Requisitos del aprovisionador de Astra Control**: Debes tener un aprovisionador de Astra Control configurado correctamente, incluidos sus componentes de Astra Trident, para gestionar clústeres.
  - **Revise los requisitos del entorno de Astra Trident**: Antes de instalar o actualizar el aprovisionador de Astra Control, revise el "compatibles con front-ends, back-ends y configuraciones de host".
  - **Habilitar la funcionalidad de aprovisionamiento de Astra Control**: Se recomienda instalar Astra Trident 23,10 o posterior y activar "Funcionalidad de almacenamiento avanzada de Astra Control Provisioning". En las siguientes versiones, Astra Control no será compatible con Astra Trident si el aprovisionador de Astra Control también no está habilitado.
  - **Configurar un backend de almacenamiento**: Al menos un backend de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster.
  - **Configure una clase de almacenamiento**: Al menos una clase de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster. Si se configura una clase de almacenamiento

predeterminada, asegúrese de que es la clase de almacenamiento **Only** que tiene la anotación predeterminada.

- **Configure un controlador de instantáneas de volumen e instale una clase de instantáneas de volumen**: "Instale una controladora Snapshot de volumen" Para poder crear instantáneas en Astra Control. "Cree" al menos uno `VolumeSnapshotClass` Mediante Astra Trident.

Pasos

1. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

2. **Proveedor**: Selecciona la pestaña **Otro** para agregar detalles sobre tu cluster autogestionado.
   a. **Otros**: Proporcione detalles sobre su cluster autogestionado cargando un `kubeconfig.yaml` o bien, pegue el contenido de `kubeconfig.yaml` desde el portapapeles.

   > Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "Documentación de Kubernetes" para obtener información acerca de cómo crear `kubeconfig` archivos.

3. **Nombre de credencial**: Proporciona un nombre para la credencial de clúster autogestionada que estás cargando en Astra Control. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
4. **Identificador de ruta privado**: Este campo es solo para uso con clusters privados.
5. Seleccione **Siguiente**.
6. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
   a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
   b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

   > Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:
   >
   > - Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
   > - Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
   > - Azure NetApp Files: Información sobre rendimiento y resiliencia
   > - Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
   > - Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
   > - Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
   > - Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
  - "Azure NetApp Files"
  - "Discos gestionados de Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX para ONTAP de NetApp"
  - "Cloud Volumes ONTAP de NetApp"

    Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

c. Seleccione **Siguiente**.

d. **Revisar y aprobar**: Revise los detalles de la configuración.

e. Selecciona **Add** para agregar el clúster a Astra Control Service.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Añade un clúster privado autogestionado a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control.

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Puede agregar un clúster autogestionado a Astra Control Service cargando un `kubeconfig.yaml` archivo. Deberá asegurarse de que el clúster cumple los requisitos que se indican aquí.

Distribuciones de Kubernetes compatibles

Puede utilizar Astra Control Service para gestionar los siguientes tipos de clústeres privados autogestionados:

Distribución de Kubernetes	Versiones compatibles
Kubernetes (ascendente)	1,27 a 1,29
Motor Kubernetes de rancher (RKE)	RKE 1: Versiones 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versiones 1.23.16 y 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versiones 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
OpenShift Container Platform de Red Hat	4,12 hasta 4,14

En estas instrucciones se asume que ya ha creado un clúster privado y ha preparado un método seguro para

acceder de forma remota a él.

Tienes que realizar las siguientes tareas para añadir tu clúster privado a Astra Control Service:

1. Instala Astra Connector
2. Configure el almacenamiento persistente
3. Añada el clúster autogestionado privado a Astra Control Service

Instala Astra Connector

Antes de agregar un clúster privado, tiene que instalar Astra Connector en el clúster para que Astra Control se pueda comunicar con él. Consulte "Instala la versión anterior de Astra Connector para clústeres privados gestionados con flujos de trabajo que no sean nativos de Kubernetes" si desea obtener instrucciones.

Configure el almacenamiento persistente

Configure el almacenamiento persistente para el clúster. Consulte la documentación para empezar para obtener más información sobre la configuración del almacenamiento persistente:

- "Configure Microsoft Azure con Azure NetApp Files"
- "Configure Microsoft Azure con discos gestionados de Azure"
- "Configure Amazon Web Services"
- "Configure Google Cloud"

Añada el clúster autogestionado privado a Astra Control Service

Ahora puede añadir el clúster privado a Astra Control Service.

Antes de empezar

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Los clústeres autogestionados pueden utilizar Astra Control Provisioner para interactuar con los servicios de almacenamiento de NetApp o pueden usar controladores de la interfaz de almacenamiento de contenedores (CSI) para interactuar con Amazon Elastic Block Store (EBS), los discos gestionados de Azure y el disco persistente de Google.

Astra Control Service es compatible con clústeres autogestionados que utilizan las siguientes distribuciones de Kubernetes:

- OpenShift Container Platform de Red Hat
- Motor Kubernetes del rancher
- Subida de Kubernetes

Su clúster autogestionado debe cumplir con los siguientes requisitos:

- El clúster debe estar accesible a través de Internet.
- Si está utilizando o planea utilizar almacenamiento habilitado con controladores CSI, se deben instalar los controladores CSI adecuados en el clúster. Para obtener más información sobre el uso de los controladores CSI para integrar el almacenamiento, consulte la documentación del servicio de almacenamiento.
- Tiene acceso al archivo kubeconfig de cluster que incluye solo un elemento de contexto. Siga "estas instrucciones" para generar un archivo kubeconfig.
- Si va a agregar el clúster mediante un archivo kubeconfig que hace referencia a una entidad de certificación (CA) privada, agregue la siguiente línea al `cluster` sección del archivo kubeconfig. Esto permite a Astra Control añadir el clúster:

  ```
  insecure-skip-tls-verify: true
  ```

- **Sólo rancher**: Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig proporcionado por Rancher para utilizar un contexto de plano de control en lugar del contexto del servidor API Rancher. Esto reduce la carga en el servidor API de Rancher y mejora el rendimiento.
- **Requisitos del aprovisionador de Astra Control**: Debes tener un aprovisionador de Astra Control configurado correctamente, incluidos sus componentes de Astra Trident, para gestionar clústeres.
  - **Revise los requisitos del entorno de Astra Trident**: Antes de instalar o actualizar el aprovisionador de Astra Control, revise el "compatibles con front-ends, back-ends y configuraciones de host".
  - **Habilitar la funcionalidad de aprovisionamiento de Astra Control**: Se recomienda instalar Astra Trident 23,10 o posterior y activar "Funcionalidad de almacenamiento avanzada de Astra Control Provisioning". En las siguientes versiones, Astra Control no será compatible con Astra Trident si el aprovisionador de Astra Control también no está habilitado.
  - **Configurar un backend de almacenamiento**: Al menos un backend de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster.
  - **Configure una clase de almacenamiento**: Al menos una clase de almacenamiento debe ser "Configuradas en Astra Trident" en el clúster. Si se configura una clase de almacenamiento

predeterminada, asegúrese de que es la clase de almacenamiento **Only** que tiene la anotación predeterminada.

- **Configure un controlador de instantáneas de volumen e instale una clase de instantáneas de volumen**: "Instale una controladora Snapshot de volumen" Para poder crear instantáneas en Astra Control. "Cree" al menos uno `VolumeSnapshotClass` Mediante Astra Trident.

Pasos

1. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

   Siga las instrucciones para añadir el clúster.

2. **Proveedor**: Selecciona la pestaña **Otro** para agregar detalles sobre tu cluster autogestionado.
3. **Otros**: Proporcione detalles sobre su cluster autogestionado cargando un `kubeconfig.yaml` o bien, pegue el contenido de `kubeconfig.yaml` desde el portapapeles.

   > Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "estas instrucciones" para obtener información acerca de cómo crear `kubeconfig` archivos.

4. **Nombre de credencial**: Proporciona un nombre para la credencial de clúster autogestionada que estás cargando en Astra Control. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
5. **Identificador de ruta privado**: Introduce el identificador de ruta privado, que puedes obtener del Astra Connector. Si consulta el Astra Connector a través del `kubectl get astraconnector -n astra-connector` comando, el identificador de ruta privada se denomina `ASTRACONNECTORID`.

   > El identificador de ruta privada es el nombre asociado con Astra Connector que permite gestionar un clúster de Kubernetes privado con Astra. En este contexto, un clúster privado es un clúster de Kubernetes que no expone su servidor API a Internet.

6. Seleccione **Siguiente**.
7. (Opcional) **Almacenamiento**: Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
   a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
   b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:

- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- "Cloud Volumes Service para Google Cloud"
- "Disco persistente de Google"
- "Azure NetApp Files"
- "Discos gestionados de Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX para ONTAP de NetApp"
- "Cloud Volumes ONTAP de NetApp"

  Más información acerca de "Clases de almacenamiento para clústeres de Amazon Web Services". Más información acerca de "Clases de almacenamiento para clústeres de AKS". Más información acerca de "Clases de almacenamiento para clústeres GKE".

c. Seleccione **Siguiente**.

d. **Revisar y aprobar**: Revise los detalles de la configuración.

e. Selecciona **Add** para agregar el clúster a Astra Control Service.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede Cambie la clase de almacenamiento predeterminada con la línea de comandos.

Pasos

1. En la interfaz de usuario de Astra Control Service, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

Comprueba la versión de Astra Trident

Para añadir un clúster autogestionado que utilice el aprovisionador de Astra Control o Astra Trident para los servicios de almacenamiento, asegúrese de que la versión instalada de Astra Trident sea la versión 23,10 o la más reciente.

Pasos

1. Determine la versión de Astra Trident que ejecuta:

```
kubectl get tridentversions -n trident
```

Si Astra Trident está instalado, verá una salida similar a la siguiente:

```
NAME      VERSION
trident   24.02.0
```

Si Astra Trident no está instalado, verá una salida similar a la siguiente:

```
error: the server doesn't have a resource type "tridentversions"
```

2. Debe realizar una de las siguientes acciones:
   - Si utiliza Astra Trident 23,01 o una versión anterior, utilice estos "instrucciones" Para actualizar a una versión más reciente de Astra Trident antes de actualizar a Astra Control Provisioner. Puede hacerlo "realice una actualización directa" Para Astra Control Provisioner 24,02 si tu Astra Trident está en una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a Astra Control Provisioner 24,02.
   - Si utiliza Astra Trident 23,10 o una versión posterior, compruebe que el aprovisionador de Astra Control haya sido "activado". El aprovisionador de Astra Control no funcionará con versiones de Astra Control Center anteriores a la 23,10. "Actualiza tu aprovisionador de Astra Control" De modo que tiene la misma versión que Astra Control Center que vas a actualizar para acceder a la funcionalidad más reciente.
3. Asegúrese de que los pods estén ejecutando:

```
kubectl get pods -n trident
```

4. Compruebe si las clases de almacenamiento utilizan los controladores Astra Trident compatibles. El nombre del aprovisionador debe ser `csi.trident.netapp.io`. Consulte el siguiente ejemplo:

```
kubectl get sc
```

Respuesta de ejemplo:

```
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
```

Cree un archivo kubeconfig

Puede añadir un clúster a Astra Control Service mediante un archivo kubeconfig. En función del tipo de cluster que desee agregar, es posible que necesite crear manualmente un archivo kubeconfig para el cluster mediante pasos específicos.

- Cree un archivo kubeconfig para los clústeres de Amazon EKS
- Cree un archivo kubeconfig para los clústeres de Red Hat OpenShift Service en AWS (ROSA)
- Cree un archivo kubeconfig para otros tipos de clusters

Cree un archivo kubeconfig para los clústeres de Amazon EKS

Siga estas instrucciones para crear un archivo kubeconfig y un secreto de token permanente para los clústeres de Amazon EKS. Se necesita un secreto de token permanente para los clústeres alojados en EKS.

Pasos

1. Siga las instrucciones de la documentación de Amazon para generar un archivo kubeconfig:

   "Creación o actualización de un archivo kubeconfig para un clúster de Amazon EKS"

2. Cree una cuenta de servicio del siguiente modo:

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

      Ajuste el nombre de la cuenta de servicio según sea necesario. El espacio de nombres `kube-system` es necesario para estos pasos. Si cambia aquí el nombre de la cuenta de servicio, debe aplicar los mismos cambios en los siguientes pasos.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astra-admin-account
  namespace: kube-system
```

3. Aplicar la cuenta de servicio:

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

4. Cree un `ClusterRoleBinding` archivo llamado `astracontrol-clusterrolebinding.yaml`.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astra-admin-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astra-admin-account
  namespace: kube-system
```

5. Aplique el enlace de roles del clúster:

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

6. Se ha llamado a crear un archivo secreto de token de cuenta de servicio `astracontrol-secret.yaml`.

```
<strong>astracontrol-secret.yaml</strong>
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: astra-admin-account
  name: astra-admin-account
  namespace: kube-system
type: kubernetes.io/service-account-token
```

7. Aplique el secreto de token:

```
kubectl apply -f astracontrol-secret.yaml
```

8. Recupere el secreto de token:

```
kubectl get secret astra-admin-account -n kube-system -o
jsonpath='{.data.token}' | base64 -d
```

9. Sustituya el `user` Sección del archivo kubeconfig de AWS EKS con el token, como se muestra en el

siguiente ejemplo:

```
user:
    token: k8s-aws-
v1.aHR0cHM6Ly9zdHMudXMtd2VzdC0yLmFtYXpvbmF3cy5jb20vP0FjdGlvbj1HZXRDYWxsZ
XJJZGVudGl0eSZWZXJzaW9uPTIwMTEtMDYtMTUmWC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQ
y1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBM1JEWDdKU0haWU9LSEQ2SyUyRjIwMjMwN
DAzJTJGdXMtd2VzdC0yJTJGc3RzJTJGYXdzNF9yZXF1ZXN0JlgtQW16LURhdGU9MjAyMzA0M
DNUMjA0MzQwWiZYLUFtei1FeHBpcmVzPTYwJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCUzQ
ngtazhzLWF3cy1pZCZYLUFtei1TaWduYXR1cmU9YjU4ZWM0NzdiM2NkZGYxNGRhNzU4MGI2Z
WQ2zY2NzI2YWIwM2UyNThjMjRhNTJjNmVhNjc4MTRlNjJkOTg2Mg
```

Cree un archivo kubeconfig para los clústeres de Red Hat OpenShift Service en AWS (ROSA)

Siga estas instrucciones para crear un archivo kubeconfig para clústeres de Red Hat OpenShift Service en AWS (ROSA).

Pasos

1. Inicie sesión en el clúster ROSA.
2. Cree una cuenta de servicio:

```
oc create sa astracontrol-service-account
```

3. Añada un rol de clúster:

```
oc adm policy add-cluster-role-to-user cluster-admin -z astracontrol-
service-account
```

4. Con el siguiente ejemplo, cree un archivo de configuración secreto de cuenta de servicio:

```
<strong>secret-astra-sa.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-account"
type: kubernetes.io/service-account-token
```

5. Cree el secreto:

```
oc create -f secret-astra-sa.yaml
```

6. Edite la cuenta de servicio que ha creado y agregue el nombre secreto de la cuenta de servicio de Astra Control a `secrets` sección:

```
oc edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-dvfcd
kind: ServiceAccount
metadata:
  creationTimestamp: "2023-08-04T04:18:30Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "169770"
  uid: 965fa151-923f-4fbd-9289-30cad15998ac
secrets:
- name: astracontrol-service-account-dockercfg-dvfcd
- name: secret-astracontrol-service-account ####ADD THIS ONLY####
```

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

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

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

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-dvfcd"},
{ "name": "secret-astracontrol-service-account"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-dvfcd` sería 0 y el índice para `secret-astracontrol-service-account` sería 1. En la salida, anote el número de índice del secreto de la cuenta de servicio. Necesitará este número de índice en el siguiente paso.

8. Genere la kubeconfig de la siguiente manera:

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

```
<strong>create-kubeconfig.sh</strong>
```

```
# 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=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
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
```

9. (Opcional) cambie el nombre de la Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Cree un archivo kubeconfig para otros tipos de clusters

Siga estas instrucciones para crear un archivo kubeconfig de rol limitado o ampliado para Rancher, upstream Kubernetes y Red Hat OpenShift clusters.

Para los clústeres que se gestionan mediante kubeconfig, opcionalmente puede crear un rol de administrador de permisos limitado o de permisos ampliados para Astra Control Service.

Este procedimiento le ayuda a crear un kubeconfig independiente si cualquiera de los siguientes escenarios se aplica a su entorno:

- Deseas limitar los permisos de Astra Control a los clústeres que gestiona
- Usas varios contextos y no puedes usar el comando predeterminado de Astra Control configurado durante la instalación o un rol limitado con un solo contexto no funcionará en tu entorno

Antes de empezar

Asegúrese de que tiene lo siguiente para el clúster que tiene intención de administrar antes de completar los pasos del procedimiento:

- A. "versión compatible" de kubectl está instalado.
- Acceso kubectl al clúster que pretendes añadir y gestionar mediante Astra Control Service

> Para este procedimiento, no necesita acceso kubectl al clúster que ejecuta Astra Control Service.

- Una imagen de referencia activa para el clúster que pretende gestionar con derechos de administrador del clúster para el contexto activo

Pasos

1. Cree una cuenta de servicio:
   a. Cree un archivo de cuenta de servicio llamado `astracontrol-service-account.yaml`.

```
<strong>astracontrol-service-account.yaml</strong>
```

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

   b. Aplicar la cuenta de servicio:

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

2. Cree uno de los siguientes roles de clúster con permisos suficientes para que Astra Control gestione un clúster:

Rol de clúster limitado

Este rol contiene los permisos mínimos necesarios para que Astra Control gestione un clúster:

a. Cree un `ClusterRole` archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
  - deployments
```

```
    - horizontalpodautoscalers
    - ingresses
    - jobs
    - namespaces
    - networkpolicies
    - persistentvolumeclaims
    - poddisruptionbudgets
    - pods
    - podtemplates
    - replicasets
    - replicationcontrollers
    - replicationcontrollers/scale
    - rolebindings
    - roles
    - secrets
    - serviceaccounts
    - services
    - statefulsets
    - tridentmirrorrelationships
    - tridentsnapshotinfos
    - volumesnapshots
    - volumesnapshotcontents
    verbs:
    - delete

  # Watch resources
  # Necessary to monitor progress
  - apiGroups:
    - ""
    resources:
    - pods
    - replicationcontrollers
    - replicationcontrollers/scale
    verbs:
    - watch

  # Update resources
  - apiGroups:
    - ""
    - build.openshift.io
    - image.openshift.io
    resources:
    - builds/details
    - replicationcontrollers
    - replicationcontrollers/scale
    - imagestreams/layers
```

```
  - imagestreamtags
  - imagetags
  verbs:
  - update
```

b. (Solo para clústeres de OpenShift) Añada lo siguiente al final del `astra-admin-account.yaml` archivo:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
  - update
```

c. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

Rol del clúster ampliado

Este rol contiene permisos ampliados para que un clúster lo gestione Astra Control. Puedes usar este rol si utilizas varios contextos y no puedes utilizar el comando kubeconfig predeterminado de Astra Control configurado durante la instalación o un rol limitado con un único contexto no funcionará en tu entorno:

> Lo siguiente `ClusterRole` Los pasos son un ejemplo general de Kubernetes. Consulte la documentación de la distribución de Kubernetes para obtener instrucciones específicas de su entorno.

a. Cree un `ClusterRole` archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

b. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

3. Cree el enlace de rol de clúster para el rol del clúster a la cuenta de servicio:

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

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

b. Aplique el enlace de roles del clúster:

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

4. Crear y aplicar el secreto de token:
   a. Cree un archivo secreto de token llamado `secret-astracontrol-service-account.yaml`.

```
<strong>secret-astracontrol-service-account.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

   b. Aplique el secreto de token:

```
kubectl apply -f secret-astracontrol-service-account.yaml
```

5. Agregue el secreto de token a la cuenta de servicio agregando su nombre a la `secrets` array (la última línea del siguiente ejemplo):

```
kubectl edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},
"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>
```

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

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

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

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-48xhx` sería 0 y el índice para `secret-astracontrol-service-account` sería 1. En la salida, anote el número de índice del secreto de la cuenta de servicio. Necesitará este número de índice en el siguiente paso.

7. Genere la kubeconfig de la siguiente manera:
   a. Cree un `create-kubeconfig.sh` archivo.
   b. Sustituya `TOKEN_INDEX` al principio de la secuencia de comandos siguiente con el valor correcto.

```
<strong>create-kubeconfig.sh</strong>
```

```
# 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=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
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
```

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

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

8. (Opcional) cambie el nombre de la Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

El futuro

Ahora que ha iniciado sesión y añadido un clúster a Astra Control, está listo para empezar a utilizar las funciones de gestión de datos de aplicaciones de Astra Control.

- "Inicie la gestión de aplicaciones"
- "Proteja sus aplicaciones"
- "Clone aplicaciones"
- "Configurar facturación"
- "Invitar y administrar usuarios"
- "Gestione las credenciales del proveedor de cloud"
- "Gestionar notificaciones"
- "Pon en marcha una instancia autogestionada de Astra Control"

Vídeos de Astra Control Service

Echa un vistazo a NetApp TV para obtener el contenido más reciente en vídeo, sobre Astra Control Service. NetApp TV incluye vídeos que muestran determinadas funciones

de Astra Control Service o cómo completar ciertas tareas comunes.

"Vídeos de Astra Control Service"