Configure su proveedor de cloud

Astra Control Service

NetApp
June 04, 2024

Tabla de contenidos

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".

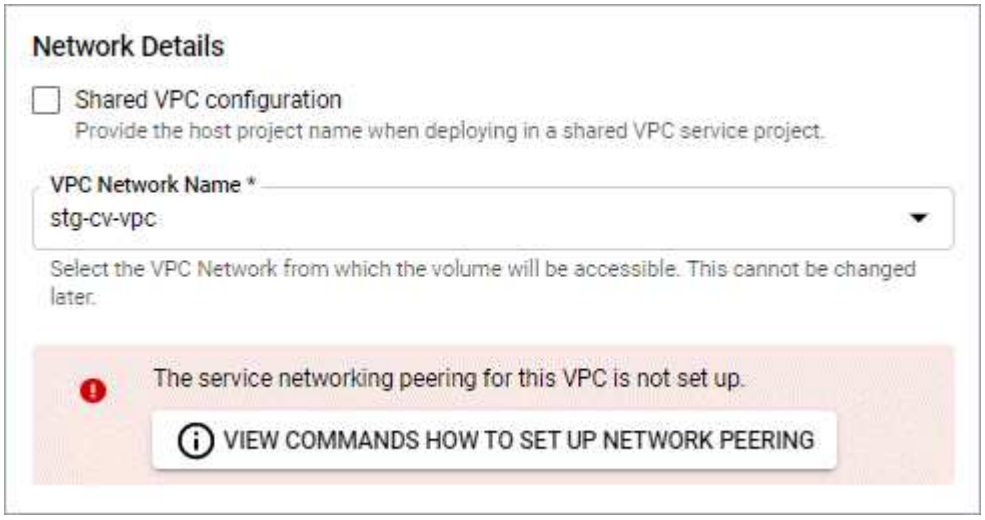
2. "Vaya a Cloud Volumes en Google Cloud Platform".
3. En la página **Volumes**, seleccione **Crear**.
4. En **Tipo de servicio**, seleccione **CVS** o **CVS-Performance**.

   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".