Cloud híbrido con componentes autogestionados (on-premises/AWS/GCP/Azure)

NetApp Solutions

NetApp
April 26, 2024

Tabla de contenidos

Soluciones de multicloud híbrido de NetApp para cargas de trabajo de contenedores de Red Hat OpenShift

Descripción general

NetApp está viendo un aumento significativo en los clientes que modernizan sus aplicaciones empresariales heredadas y crean nuevas aplicaciones con contenedores y plataformas de orquestación creadas en torno a Kubernetes. Red Hat OpenShift Container Platform es un ejemplo que consideramos adoptado por muchos de nuestros clientes.

A medida que más y más clientes empiezan a adoptar contenedores dentro de sus empresas, NetApp está perfectamente posicionada para poder dar respuesta a las necesidades de almacenamiento persistente de sus aplicaciones con estado y las necesidades de gestión de datos clásicas como la protección de datos, la seguridad de datos y la migración de datos. Sin embargo, estas necesidades se satisfacen utilizando diferentes estrategias, herramientas y métodos.

Las opciones de almacenamiento basado en ONTAP de NetApp que se enumeran a continuación, ofrecen seguridad, protección de datos, fiabilidad y flexibilidad para implementaciones de contenedores y Kubernetes.

- Almacenamiento autogestionado en las instalaciones:
  - Almacenamiento estructural (FAS) de NetApp, cabinas All Flash FAS (AFF), cabina All SAN (ASA) y ONTAP Select
- Almacenamiento gestionado por el proveedor en las instalaciones:
  - NetApp Keystone proporciona almacenamiento como servicio (STaaS)
- Almacenamiento autogestionado en el cloud:
  - Cloud Volumes ONTAP (CVO) de NetApp proporciona almacenamiento autogestionado en los proveedores a hiperescala
- Almacenamiento en el cloud gestionado por el proveedor:
  - Cloud Volumes Service para Google Cloud (CVS), Azure NetApp Files (ANF), Amazon FSx para ONTAP de NetApp ofrecen un almacenamiento totalmente gestionado en los proveedores a hiperescala

ONTAP feature highlights

Storage Administration

- Multi-tenancy
- FlexVol & FlexGroup
- LUN
- Quotas
- ONTAP CLI & API
- System Manager & BlueXP

Performance & Scalability

- FlexCache
- FlexClone
- nconnect, session trunking, multipathing
- Scale-out clusters

Availability & Resilience

- Multi-AZ HA deployment (MetroCluster)
- SnapShot & SnapRestore
- SnapMirror
- SnapMirror Business Continuity
- SnapMirror Cloud

Access Protocols

- NFS –v3, v4, v4.1, v4.2
- SMB – v2, v3
- iSCSI
- Multi-protocol access

Storage Efficiency

- Deduplication & Compression
- Compaction
- Thin provisioning
- Data Tiering (Fabric Pool)

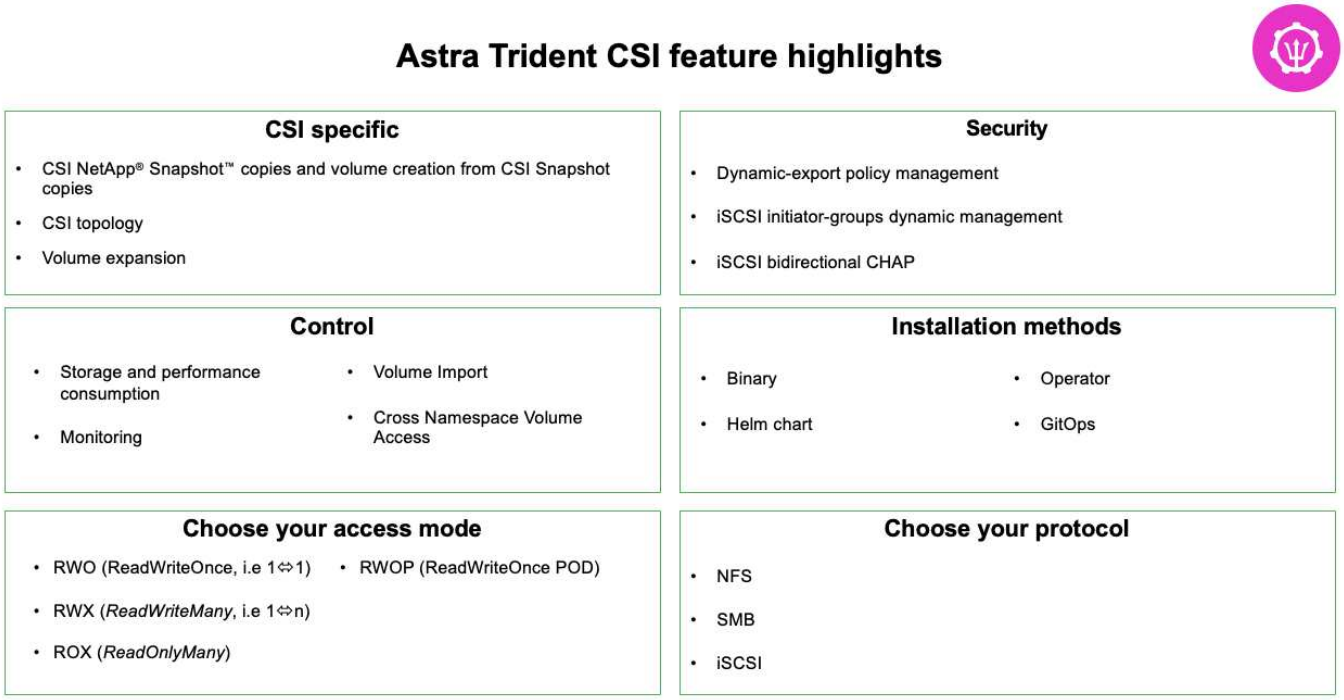
Security & Compliance

- Fpolicy & Vscan
- Active Directory integration
- LDAP & Kerberos
- Certificate based authentication

NetApp BlueXP le permite gestionar todos sus activos de almacenamiento y datos desde una única interfaz o plano de control.

Puedes usar BlueXP para crear y administrar almacenamiento en nube (por ejemplo, Cloud Volumes ONTAP y Azure NetApp Files), para mover, proteger y analizar datos, y para controlar muchos dispositivos de almacenamiento on-premises y en la periferia.

Astra Trident de NetApp es un orquestador de almacenamiento compatible con CSI que permite consumir almacenamiento persistente de forma rápida y sencilla, respaldado por diversas opciones de almacenamiento de NetApp mencionadas anteriormente. Es un software de código abierto que tiene soporte y mantenimiento de NetApp.



Las cargas de trabajo de contenedores vitales para el negocio necesitan más que volúmenes persistentes. Sus requisitos de gestión de datos requieren la protección y la migración de los objetos de aplicaciones kubernetes también.

> Los datos de la aplicación incluyen objetos de kubernetes además de los datos del usuario: Algunos ejemplos son los siguientes: - Objetos de kubernetes como especificaciones de pods, PVCs, despliegues, servicios - objetos de configuración personalizados como mapas de configuración y secretos - datos persistentes como copias Snapshot, copias de seguridad, clones - recursos personalizados como CRS y CRD

Astra Control de NetApp, disponible como software totalmente gestionado y autogestionado, proporciona orquestación para una gestión de datos de aplicaciones sólida. Consulte la "Documentación de Astra" Para obtener más información sobre la familia de productos Astra.

Esta documentación de referencia proporciona la validación de la migración y la protección de aplicaciones basadas en contenedores, puestas en marcha en la plataforma de contenedores RedHat OpenShift, mediante Astra Control Center de NetApp. Además, la solución proporciona detalles de alto nivel para la implementación y el uso de Red Hat Advanced Cluster Management (ACM) para la gestión de las plataformas de contenedores. En el documento también se destacan los detalles de la integración del almacenamiento de NetApp con las plataformas de contenedor Red Hat OpenShift mediante el aprovisionador CSI de Astra Trident. Astra Control Center se pone en marcha en el clúster de concentradores y se utiliza para gestionar las aplicaciones de contenedores y su ciclo de vida de almacenamiento persistente. Por último, proporciona una solución de replicación y conmutación al nodo de respaldo y conmutación de retorno tras recuperación para cargas de trabajo de contenedores en clústeres de Red Hat OpenShift gestionados en AWS (ROSA) utilizando Amazon FSx para NetApp ONTAP (FSxN) como almacenamiento persistente.

Solución de NetApp con cargas de trabajo de la plataforma de contenedores Red Hat OpenShift en un cloud híbrido

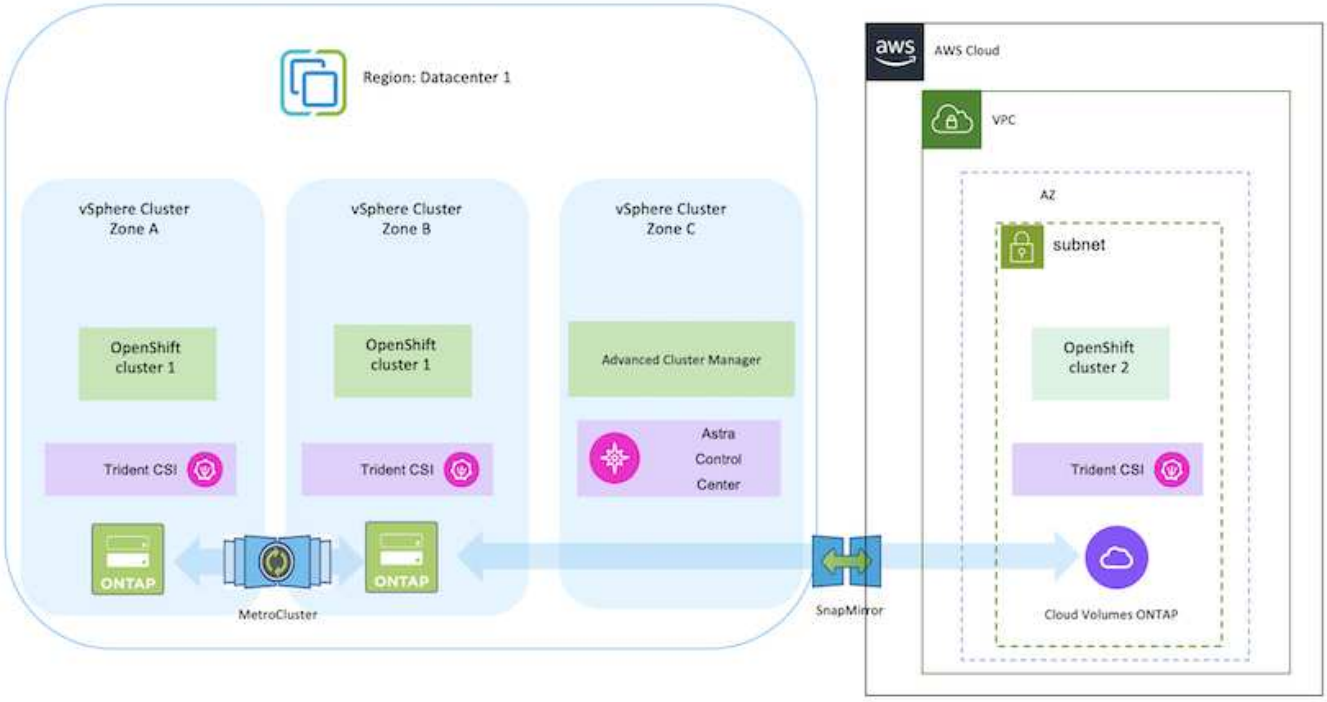
Los clientes pueden estar en un momento de su proceso de modernización cuando estén

listos para mover algunas cargas de trabajo seleccionadas o todas las cargas de trabajo de sus centros de datos al cloud. Pueden optar por usar contenedores OpenShift autogestionados y almacenamiento autogestionado de NetApp en la nube por diversos motivos. Deben planificar e implementar la plataforma de contenedores Red Hat OpenShift (OCP) en la nube para un entorno preparado para la producción con éxito para migrar las cargas de trabajo de contenedores desde sus centros de datos. Sus clústeres de OCP se pueden implementar en VMware o Bare Metal en sus centros de datos y en AWS, Azure o Google Cloud en el entorno de la nube.

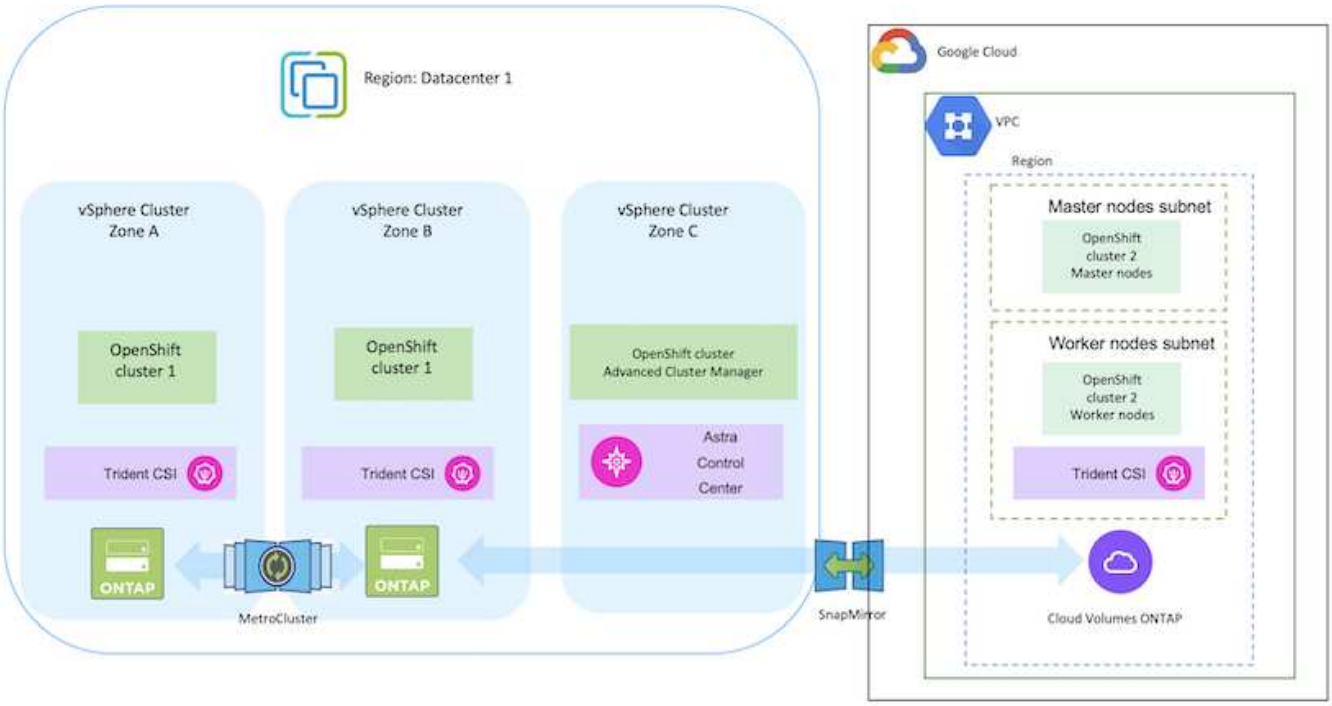
El almacenamiento de NetApp Cloud Volumes ONTAP ofrece protección de datos, fiabilidad y flexibilidad para puestas en marcha de contenedores en AWS, Azure y en Google Cloud. Astra Trident sirve como aprovisionador de almacenamiento dinámico para consumir almacenamiento persistente de Cloud Volumes ONTAP para las aplicaciones con estado de los clientes. Se puede usar Astra Control Center para orquestar los muchos requisitos de gestión de datos de aplicaciones con estado, como la protección de datos, la migración y la continuidad del negocio.

Solución de protección y migración de datos para cargas de trabajo de contenedores de OpenShift en un cloud híbrido mediante Astra Control Center

On-premises y AWS

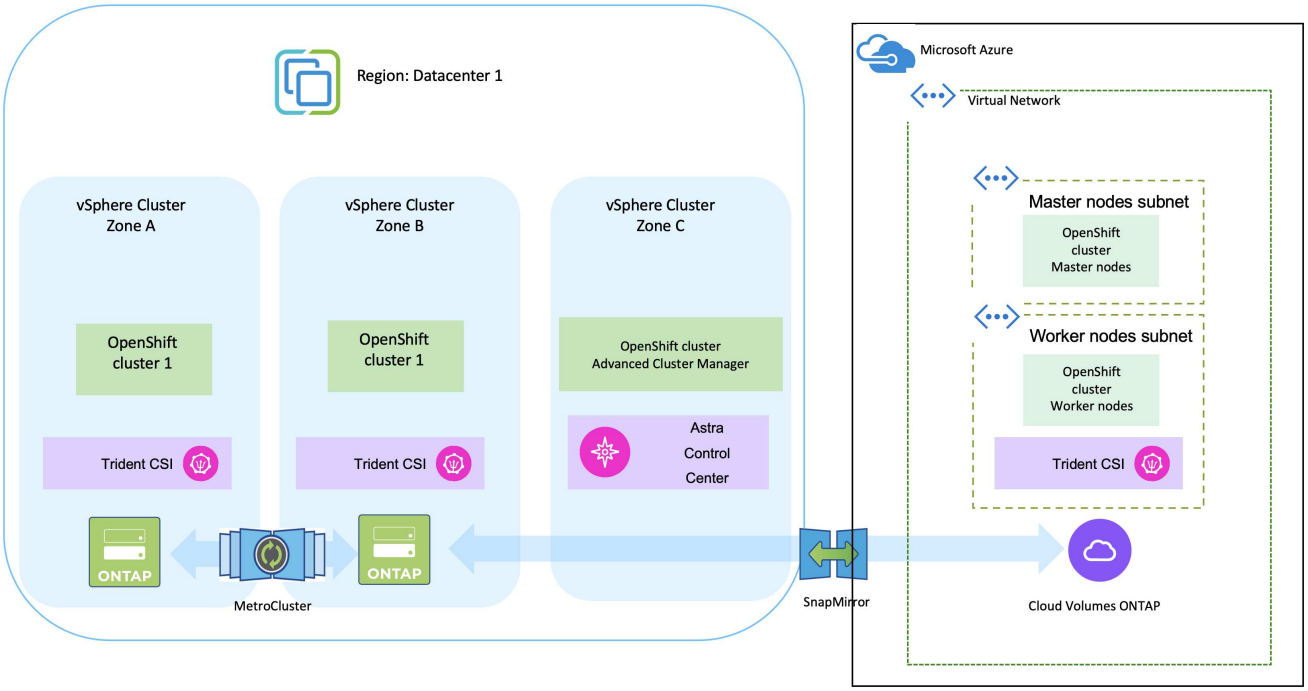


En las instalaciones y Google Cloud



En las instalaciones y Azure Cloud

[redacted]



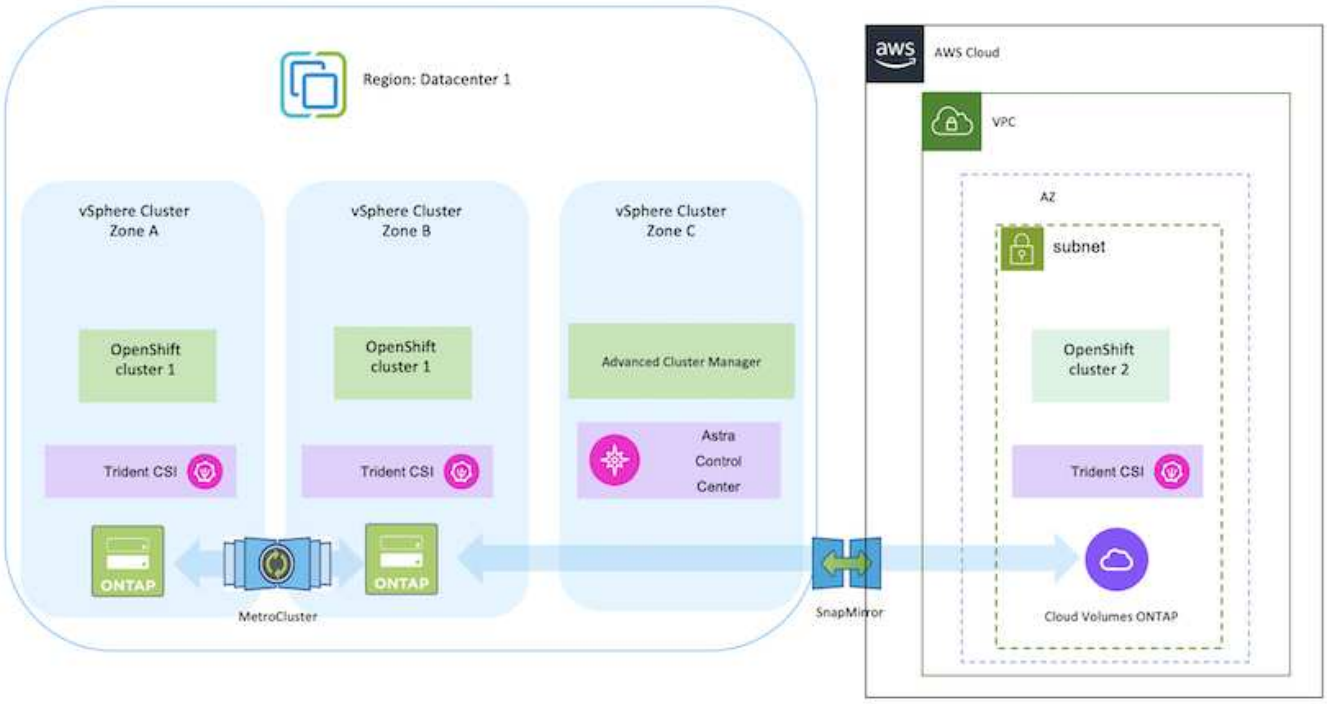
[redacted]

Implemente y configure la plataforma Red Hat OpenShift Container en AWS

En esta sección se describe un flujo de trabajo de alto nivel sobre cómo configurar y gestionar clústeres de OpenShift en AWS e implementar aplicaciones con estado en ellos. Muestra el uso del almacenamiento Cloud Volumes ONTAP de NetApp con la ayuda de Astra Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Astra Control Center para realizar actividades de protección de datos y migración para las aplicaciones con estado.

> Existen varias formas de implementar los clústeres de plataformas de contenedores de Red Hat OpenShift en AWS. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

A continuación se muestra un diagrama que muestra los clústeres implementados en AWS y conectados al centro de datos mediante una VPN.



El proceso de configuración puede dividirse en los siguientes pasos:

Instale un clúster de OCP en AWS desde Advanced Cluster Management.

- Cree una VPC con una conexión VPN de sitio a sitio (mediante pfsense) para conectarse a la red local.
- La red local tiene conectividad a Internet.
- Cree 3 subredes privadas en 3 AZs diferentes.
- Cree una zona alojada privada de Route 53 y una resolución de DNS para la VPC.

Cree un clúster de OpenShift en AWS desde el Asistente de administración avanzada de clústeres (ACM). Consulte las instrucciones "aquí".

> También puede crear el clúster en AWS desde la consola de OpenShift Hybrid Cloud. Consulte "aquí" si desea obtener instrucciones.

> Al crear el clúster con ACM, tiene la capacidad de personalizar la instalación editando el archivo yaml después de completar los detalles en la vista de formulario. Después de crear el clúster, puede iniciar sesión ssh en los nodos del clúster para solucionar problemas o utilizar otra configuración manual. Utilice la clave ssh que proporcionó durante la instalación y el núcleo de nombre de usuario para iniciar sesión.

Pon en marcha Cloud Volumes ONTAP en AWS mediante BlueXP.

- Instale el conector en un entorno VMware en las instalaciones. Consulte las instrucciones "aquí".
- Pon en marcha una instancia de CVO en AWS usando el conector. Consulte las instrucciones "aquí".

> El conector también se puede instalar en el entorno de nube. Consulte "aquí" para obtener más información.

Instale Astra Trident en el clúster de OCP

- Ponga en marcha el operador Trident mediante Helm. Consulte las instrucciones "aquí"
- Cree un back-end y una clase de almacenamiento. Consulte las instrucciones "aquí".

Añada el clúster OCP en AWS al Astra Control Center.

Añada el clúster OCP en AWS a Astra Control Center.

Uso de la función de topología CSI de Trident para arquitecturas de varias zonas

Los proveedores de cloud, hoy en día, permiten que los administradores de clústeres de Kubernetes/OpenShift generen nodos de los clústeres basados en zonas. Los nodos se pueden ubicar en diferentes zonas de disponibilidad dentro de una región o en varias regiones. Para facilitar el aprovisionamiento de volúmenes para cargas de trabajo en una arquitectura de varias zonas, Astra Trident utiliza la topología CSI. Con la función de topología CSI, el acceso a los volúmenes puede limitarse a un subconjunto de nodos, en función de regiones y zonas de disponibilidad. Consulte "aquí" para obtener más detalles.

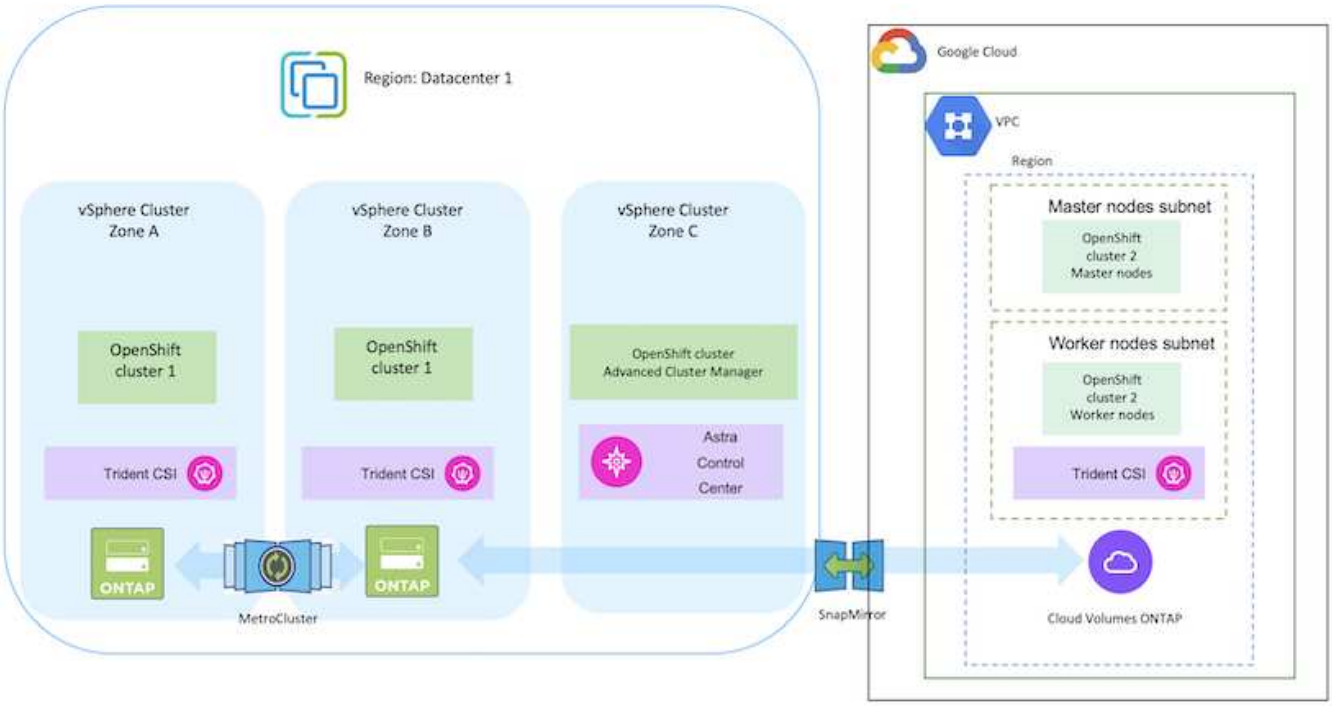
Kubernetes admite dos modos de vinculación de volúmenes: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Astra Trident crea el volumen sin reconocimiento de topología. Los volúmenes persistentes se crean sin dependencia alguna de los requisitos de programación del POD solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y vinculación de un Volumen persistente para una RVP se retrasa hasta que se programe y cree un pod que utilice la RVP. De esta forma, se crean volúmenes con el fin de cumplir las restricciones de programación que se aplican en los requisitos de topología. Los back-ends de almacenamiento de Astra Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (back-end compatible con topología). En el caso de StorageClasses que utilizan dicho back-end, solo se creará un volumen si lo solicita una aplicación programada en una región/zona admitida. (Clase StorageClass compatible con topología) "aquí" para obtener más detalles.

Implemente y configure la plataforma Red Hat OpenShift Container en GCP

Implemente y configure la plataforma Red Hat OpenShift Container en GCP

En esta sección se describe un flujo de trabajo de alto nivel sobre cómo configurar y gestionar clústeres de OpenShift en GCP e implementar aplicaciones con estado en ellos. Muestra el uso del almacenamiento Cloud Volumes ONTAP de NetApp con la ayuda de Astra Trident para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Astra Control Center para realizar actividades de protección de datos y migración para las aplicaciones con estado.

Aquí hay un diagrama que muestra los clústeres implementados en GCP y conectados al centro de datos mediante una VPN.



Hay varias formas de implementar clústeres de plataformas de contenedores Red Hat OpenShift en GCP. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

El proceso de configuración puede dividirse en los siguientes pasos:

Instale un clúster OCP en GCP desde la CLI.

- Asegúrese de haber cumplido todos los requisitos previos indicados "aquí".
- Para la conectividad VPN entre on-premises y GCP, se creó y configuró una VM pfsense. Para ver instrucciones, consulte "aquí".
  - La dirección de la puerta de enlace remota en pfsense solo se puede configurar después de haber creado una puerta de enlace VPN en Google Cloud Platform.
  - Las direcciones IP de red remota para la fase 2 solo se pueden configurar después de que el programa de instalación del clúster de OpenShift ejecute y cree los componentes de infraestructura para el clúster.
  - La VPN en Google Cloud solo se puede configurar después de que el programa de instalación cree los componentes de infraestructura para el clúster.
- Ahora instale el clúster OpenShift en GCP.
  - Obtenga el programa de instalación y el secreto de extracción e implemente el clúster siguiendo los pasos que se proporcionan en la documentación "aquí".
  - La instalación crea una red VPC en Google Cloud Platform. También crea una zona privada en Cloud DNS y añade Un registro.
    - Utilice la dirección de bloque CIDR de la red VPC para configurar pfsense y establecer la conexión VPN. Asegúrese de que los firewalls están configurados correctamente.
    - Agregue registros en el DNS del entorno local utilizando la dirección IP en los registros A del DNS de Google Cloud.
  - La instalación del clúster se completa y proporcionará un archivo kubeconfig y un nombre de usuario y contraseña para iniciar sesión en la consola del clúster.

Pon en marcha Cloud Volumes ONTAP en GCP mediante BlueXP.

- Instala un conector en Google Cloud. Consulte las instrucciones "aquí".
- Pon en marcha una instancia de CVO en Google Cloud mediante el conector. Consulte las instrucciones aquí. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Instale Astra Trident en el clúster OCP de GCP

- Como se muestra, hay muchos métodos para poner en marcha Astra Trident "aquí".
- Para este proyecto, se instaló Astra Trident poniendo en marcha el operador Astra Trident de forma manual mediante las instrucciones "aquí".
- Crear backend y clases de almacenamiento. Consulte las instrucciones "aquí".

Añade el clúster OCP en GCP a Astra Control Center.

- Crea un archivo KubeConfig independiente con un rol de clúster que contenga los permisos mínimos necesarios para que Astra Control gestione un clúster. Se pueden encontrar las instrucciones "aquí".
- Añada el clúster a Astra Control Center siguiendo las instrucciones "aquí"

Uso de la función de topología CSI de Trident para arquitecturas de varias zonas

Los proveedores de cloud, hoy en día, permiten que los administradores de clústeres de Kubernetes/OpenShift generen nodos de los clústeres basados en zonas. Los nodos se pueden ubicar en diferentes zonas de disponibilidad dentro de una región o en varias regiones. Para facilitar el aprovisionamiento de volúmenes para cargas de trabajo en una arquitectura de varias zonas, Astra Trident utiliza la topología CSI. Con la función de topología CSI, el acceso a los volúmenes puede limitarse a un subconjunto de nodos, en función de regiones y zonas de disponibilidad. Consulte "aquí" para obtener más detalles.

> Kubernetes admite dos modos de vinculación de volúmenes: - Cuando ***VolumeBindingMode*** **se establece en** ***Immediate*** (predeterminado), Astra Trident crea el volumen sin reconocimiento de topología. Los volúmenes persistentes se crean sin dependencia alguna de los requisitos de programación del POD solicitante. - Cuando ***VolumeBindingMode*** **se establece en** ***WaitForFirstConsumer***, la creación y vinculación de un Volumen persistente para una RVP se retrasa hasta que se programe y cree un pod que utilice la RVP. De esta forma, se crean volúmenes con el fin de cumplir las restricciones de programación que se aplican en los requisitos de topología. Los back-ends de almacenamiento de Astra Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (back-end compatible con topología). En el caso de StorageClasses que utilizan dicho back-end, solo se creará un volumen si lo solicita una aplicación programada en una región/zona admitida. (Clase StorageClass compatible con topología) "aquí" para obtener más detalles.

Vídeo de demostración

Instalación de OpenShift Cluster en Google Cloud Platform

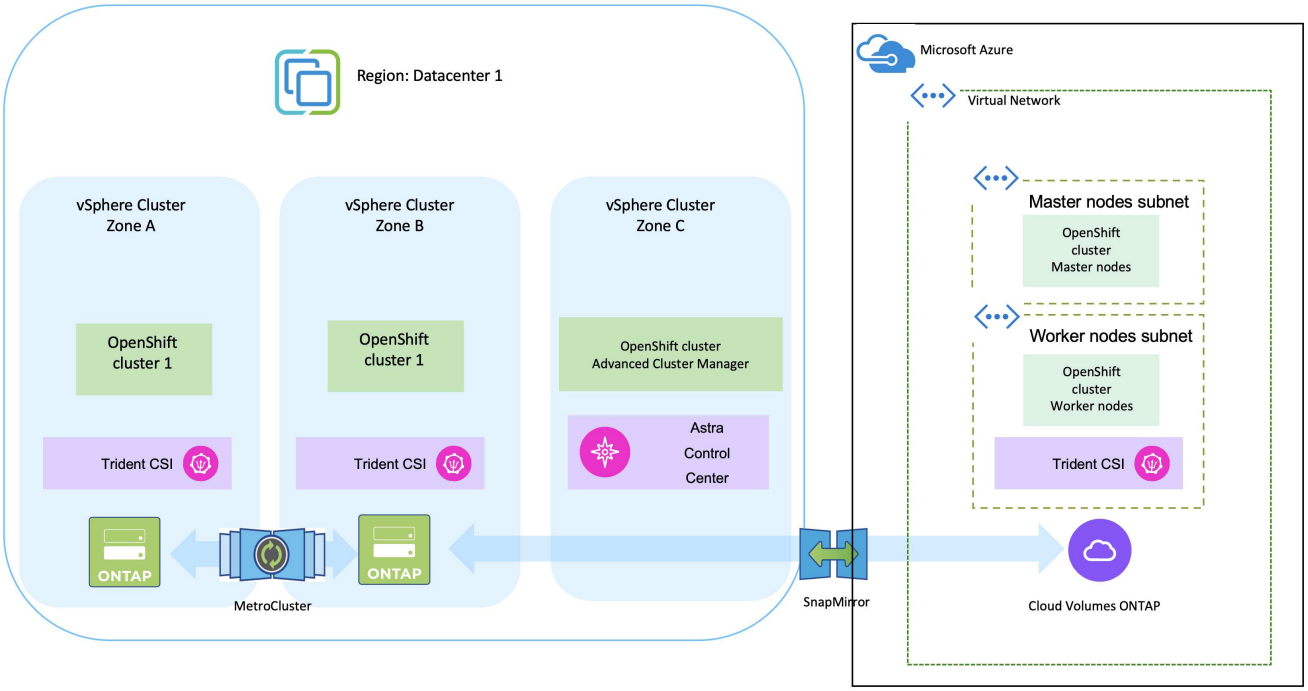
Importar clústeres de OpenShift a Astra Control Center

Implemente y configure la plataforma Red Hat OpenShift Container en Azure

Implemente y configure la plataforma Red Hat OpenShift Container en Azure

En esta sección se describe un flujo de trabajo de alto nivel sobre cómo configurar y gestionar clústeres OpenShift en Azure e implementar aplicaciones con estado en ellos. Muestra el uso del almacenamiento de NetApp Cloud Volumes ONTAP con la ayuda del aprovisionador de Astra Trident/Astra Control para proporcionar volúmenes persistentes. Se proporcionan detalles sobre el uso de Astra Control Center para realizar actividades de protección de datos y migración para las aplicaciones con estado.

Aquí hay un diagrama que muestra los clústeres implementados en Azure y conectados al centro de datos mediante una VPN.



Hay varias formas de implementar los clústeres de plataformas de contenedores de Red Hat OpenShift en Azure. Esta descripción de alto nivel de la configuración proporciona enlaces de documentación para el método específico utilizado. Puede consultar los otros métodos en los enlaces correspondientes que se proporcionan en la "sección recursos".

El proceso de configuración puede dividirse en los siguientes pasos:

Instale un clúster OCP en Azure desde la CLI.

- Asegúrese de haber cumplido todos los requisitos previos indicados "aquí".
- Cree una VPN, subredes y grupos de seguridad de red y una zona DNS privada. Cree una puerta de enlace VPN y una conexión VPN de sitio a sitio.
- Para la conectividad VPN entre las instalaciones y Azure, se creó y configuró una máquina virtual pfsense. Para ver instrucciones, consulte "aquí".
- Obtenga el programa de instalación y el secreto de extracción e implemente el clúster siguiendo los pasos que se proporcionan en la documentación "aquí".
- La instalación del clúster se completa y proporcionará un archivo kubeconfig y un nombre de usuario y contraseña para iniciar sesión en la consola del clúster.

A continuación se proporciona un archivo install-config.yaml de ejemplo.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
```

```
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

Pon en marcha Cloud Volumes ONTAP en Azure mediante BlueXP.

- Instale un conector en Azure. Consulte las instrucciones "aquí".
- Pon en marcha una instancia de CVO en Azure usando el conector. Consulte el enlace de instrucciones:https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [aquí.]

Instale Astra Control Provisioner en el clúster OCP en Azure

- Para este proyecto, Astra Control Provisioner (ACP) se instaló en todos los clústeres (clúster en las instalaciones, clúster en las instalaciones donde se puso en marcha Astra Control Center y el clúster en Azure). Obtenga más información sobre el aprovisionador de Astra Control "aquí".
- Crear backend y clases de almacenamiento. Consulte las instrucciones "aquí".

Añada el clúster OCP en Azure al Astra Control Center.

- Crea un archivo KubeConfig independiente con un rol de clúster que contenga los permisos mínimos necesarios para que Astra Control gestione un clúster. Se pueden encontrar las instrucciones "aquí".
- Añada el clúster a Astra Control Center siguiendo las instrucciones "aquí"

Uso de la función de topología CSI de Trident para arquitecturas de varias zonas

Los proveedores de cloud, hoy en día, permiten que los administradores de clústeres de Kubernetes/OpenShift generen nodos de los clústeres basados en zonas. Los nodos se pueden ubicar en diferentes zonas de disponibilidad dentro de una región o en varias regiones. Para facilitar el aprovisionamiento de volúmenes para cargas de trabajo en una arquitectura de varias zonas, Astra Trident utiliza la topología CSI. Con la función de topología CSI, el acceso a los volúmenes puede limitarse a un subconjunto de nodos, en función de regiones y zonas de disponibilidad. Consulte "aquí" para obtener más detalles.

> Kubernetes admite dos modos de vinculación de volúmenes: - Cuando ***VolumeBindingMode* se establece en *Immediate*** (predeterminado), Astra Trident crea el volumen sin reconocimiento de topología. Los volúmenes persistentes se crean sin dependencia alguna de los requisitos de programación del POD solicitante. - Cuando ***VolumeBindingMode* se establece en *WaitForFirstConsumer***, la creación y vinculación de un Volumen persistente para una RVP se retrasa hasta que se programe y cree un pod que utilice la RVP. De esta forma, se crean volúmenes con el fin de cumplir las restricciones de programación que se aplican en los requisitos de topología. Los back-ends de almacenamiento de Astra Trident se pueden diseñar para aprovisionar volúmenes de forma selectiva según las zonas de disponibilidad (back-end compatible con topología). En el caso de StorageClasses que utilizan dicho back-end, solo se creará un volumen si lo solicita una aplicación programada en una región/zona admitida. (Clase StorageClass compatible con topología) "aquí" para obtener más detalles.

Vídeo de demostración

Utilizar Astra Control para la conmutación al nodo de respaldo y la conmutación de retorno tras recuperación de aplicaciones

Protección de datos mediante Astra Control Center

Esta página muestra las opciones de protección de datos para aplicaciones basadas en contenedores Red Hat OpenShift que se ejecutan en VMware vSphere o en la nube mediante Astra Control Center (ACC).

A medida que los usuarios realizan el proceso de modernización de sus aplicaciones con Red Hat OpenShift, debe implementarse una estrategia de protección de datos para protegerlos de la eliminación accidental o de cualquier otro error humano. A menudo, también es necesaria una estrategia de protección para los fines normativos o de cumplimiento de normativas con el fin de proteger sus datos contra un diaster.

Los requisitos de protección de datos varían desde volver a una copia puntual hasta conmutar automáticamente por error a un dominio de fallo diferente sin intervención humana alguna. Muchos clientes eligen ONTAP como su plataforma de almacenamiento preferida para las aplicaciones de Kubernetes por sus completas funciones, como multi-tenancy, multiprotocolo, ofertas de alto rendimiento y capacidad, replicación

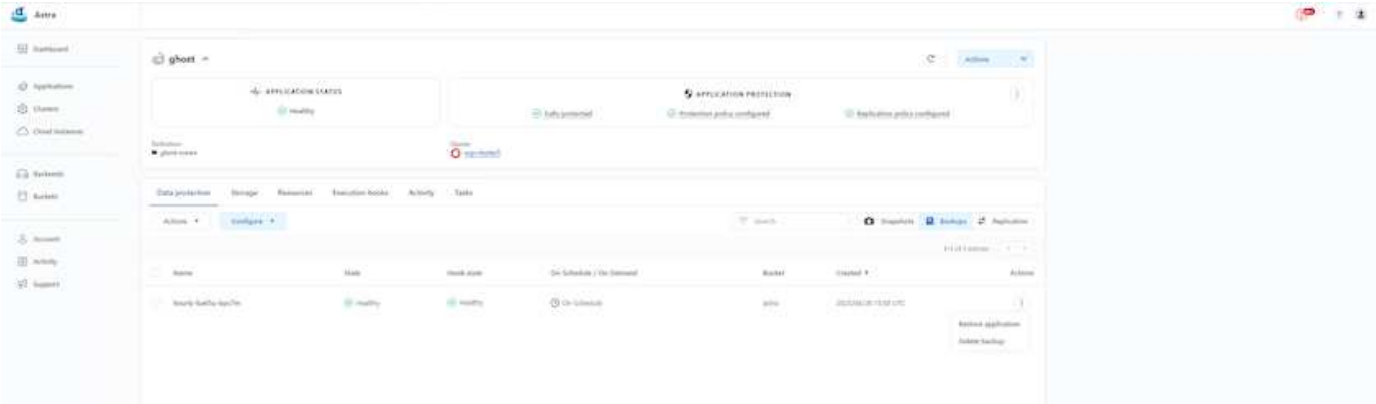
y almacenamiento en caché para ubicaciones multisitio, seguridad y flexibilidad.

Es posible que los clientes tengan configurado un entorno cloud como extensión de su centro de datos, para que puedan aprovechar las ventajas del cloud y estar bien posicionados para mover sus cargas de trabajo en el futuro. Para estos clientes, realizar backup de sus aplicaciones OpenShift y sus datos en el entorno de cloud se convierte en una opción inevitable. Luego, pueden restaurar las aplicaciones y los datos asociados en un clúster de OpenShift en la nube o en el centro de datos.

Copia de seguridad y restauración con ACC

Los propietarios de aplicaciones pueden revisar y actualizar las aplicaciones descubiertas por ACC. ACC puede realizar copias Snapshot mediante CSI y realizar backups utilizando la copia snapshot puntual. El destino de backup puede ser un almacén de objetos en el entorno de cloud. La política de protección puede configurarse para los backups programados y la cantidad de versiones de backup que deben conservarse. El objetivo de punto de recuperación mínimo es de una hora.

Restauración de una aplicación a partir de una copia de seguridad mediante ACC

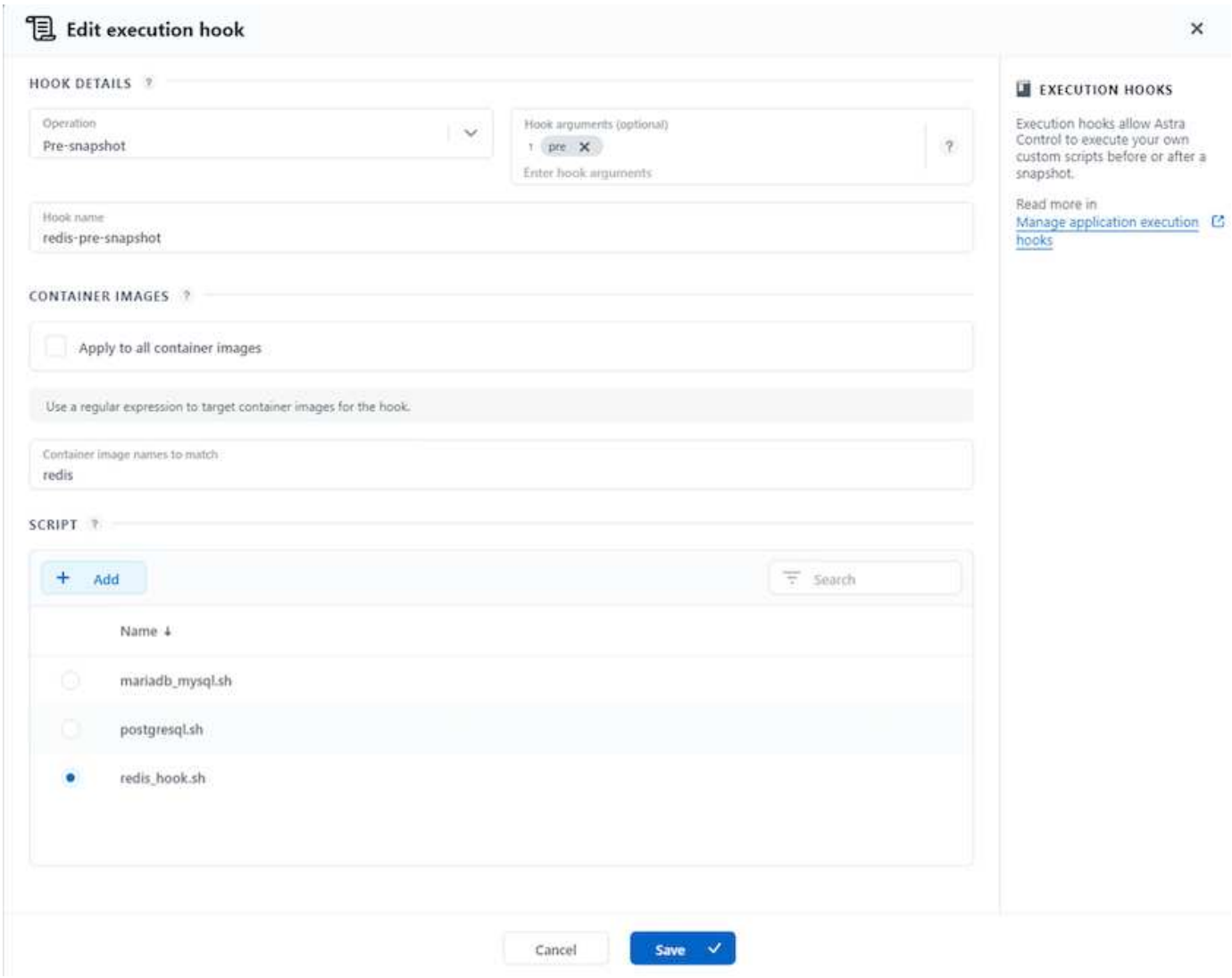


Enlaces de ejecución específicos de la aplicación

Aunque las funciones de protección de datos en el arreglo de almacenamiento están disponibles, a menudo se necesitan pasos adicionales para realizar backups y restaurar la consistencia de la aplicación. Los pasos adicionales específicos de la aplicación pueden ser: - Antes o después de crear una copia snapshot. - antes o después de crear una copia de seguridad. - Después de restaurar a partir de una copia Snapshot o copia de seguridad. Astra Control puede ejecutar estos pasos específicos de la aplicación codificados como scripts personalizados denominados «enlaces de ejecución».

La de NetApp "Proyecto de código abierto Verda" proporciona ganchos de ejecución para aplicaciones nativas de la nube populares para que la protección de aplicaciones sea sencilla, robusta y fácil de orquestar. Siéntase libre de contribuir a ese proyecto si tiene suficiente información para una aplicación que no está en el repositorio.

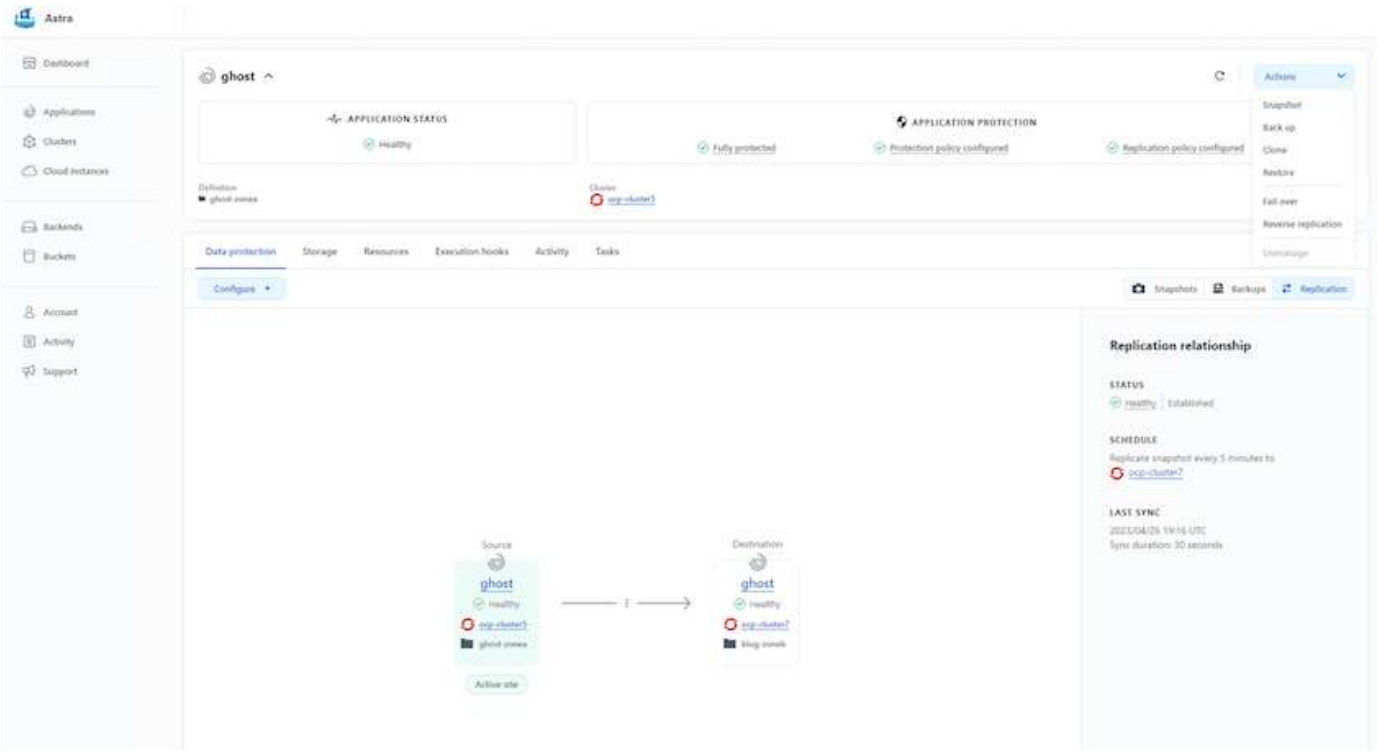
Enlace de ejecución de ejemplo para la instantánea previa de una aplicación de redis.



Replicación con ACC

Para la protección regional o para una solución de objetivo de punto de recuperación y objetivo de tiempo de recuperación bajos, una aplicación se puede replicar en otra instancia de Kubernetes que se ejecute en otro sitio, preferiblemente en otra región. ACC utiliza SnapMirror asíncrono de ONTAP con un objetivo de punto de recuperación mínimo de 5 minutos. Consulte "aquí" Para obtener instrucciones de configuración de SnapMirror.

SnapMirror con ACC



los controladores de almacenamiento san y nas económicos no admiten la función de replicación. Consulte "aquí" para obtener más detalles.

Vídeo de demostración:

"Vídeo de demostración de la recuperación de desastres con Astra Control Center"

Protección de datos con Astra Control Center

Hay disponible más información sobre las funciones de protección de datos de Astra Control Center "aquí"

Recuperación ante desastres (conmutación por error y conmutación tras recuperación con replicación) con ACC

Utilizar Astra Control para la conmutación al nodo de respaldo y la conmutación de retorno tras recuperación de aplicaciones

Migración de datos mediante Astra Control Center

Esta página muestra las opciones de migración de datos para las cargas de trabajo de contenedor en clústeres de Red Hat OpenShift con Astra Control Center (ACC). Concretamente, los clientes pueden utilizar ACC para mover algunas cargas de trabajo seleccionadas o todas las cargas de trabajo de sus centros de datos en las instalaciones al cloud; clonar sus aplicaciones al cloud para fines de pruebas o trasladarlas del centro de datos al cloud

Migración de datos

Para migrar una aplicación de un entorno a otro, puede utilizar una de las siguientes funciones de ACC:

- **replicación**
- **copia de seguridad y restauración**
- **clone**

Consulte la "sección de protección de datos" para las opciones **replicación y copia de seguridad y restauración**. Consulte "aquí" para más detalles acerca de **clonación**.

> La función de replicación de Astra solo se admite con Trident Container Storage Interface (CSI). Sin embargo, la replicación no es compatible con los controladores de economía nas y san.

Realización de la replicación de datos mediante ACC