Openshift para instalaciones locales

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Tabla de contenidos

Openshift para instalaciones locales

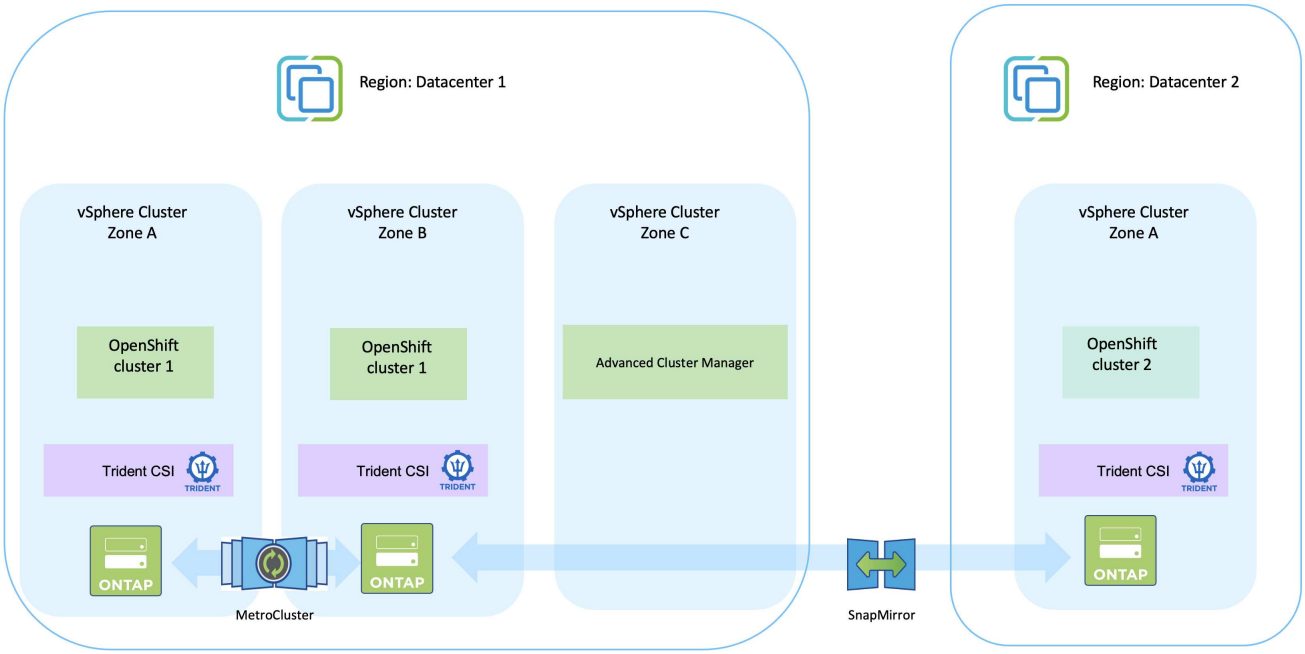
Solución NetApp con cargas de trabajo de la plataforma Red Hat OpenShift Container en VMware

Si los clientes necesitan ejecutar sus modernas aplicaciones en contenedores en la infraestructura de sus centros de datos privados, pueden hacerlo. Deben planificar e implementar la plataforma de contenedores Red Hat OpenShift (OCP) para lograr un entorno exitoso y listo para producción para implementar sus cargas de trabajo de contenedores. Sus clústeres OCP se pueden implementar en VMware o en hardware real.

El almacenamiento NetApp ONTAP ofrece protección de datos, confiabilidad y flexibilidad para implementaciones de contenedores. Trident actúa como proveedor de almacenamiento dinámico para consumir almacenamiento ONTAP persistente para las aplicaciones con estado de los clientes. NetApp Trident Protect se puede utilizar para los numerosos requisitos de gestión de datos de aplicaciones con estado, como protección de datos, migración y continuidad empresarial.

Con VMware vSphere, las herramientas de NetApp ONTAP proporcionan un complemento vCenter que se puede utilizar para aprovisionar almacenes de datos. Aplique etiquetas y úselas con OpenShift para almacenar la configuración y los datos del nodo. El almacenamiento basado en NVMe proporciona menor latencia y alto rendimiento.

Solución de protección y migración de datos para cargas de trabajo de contenedores OpenShift mediante Trident Protect

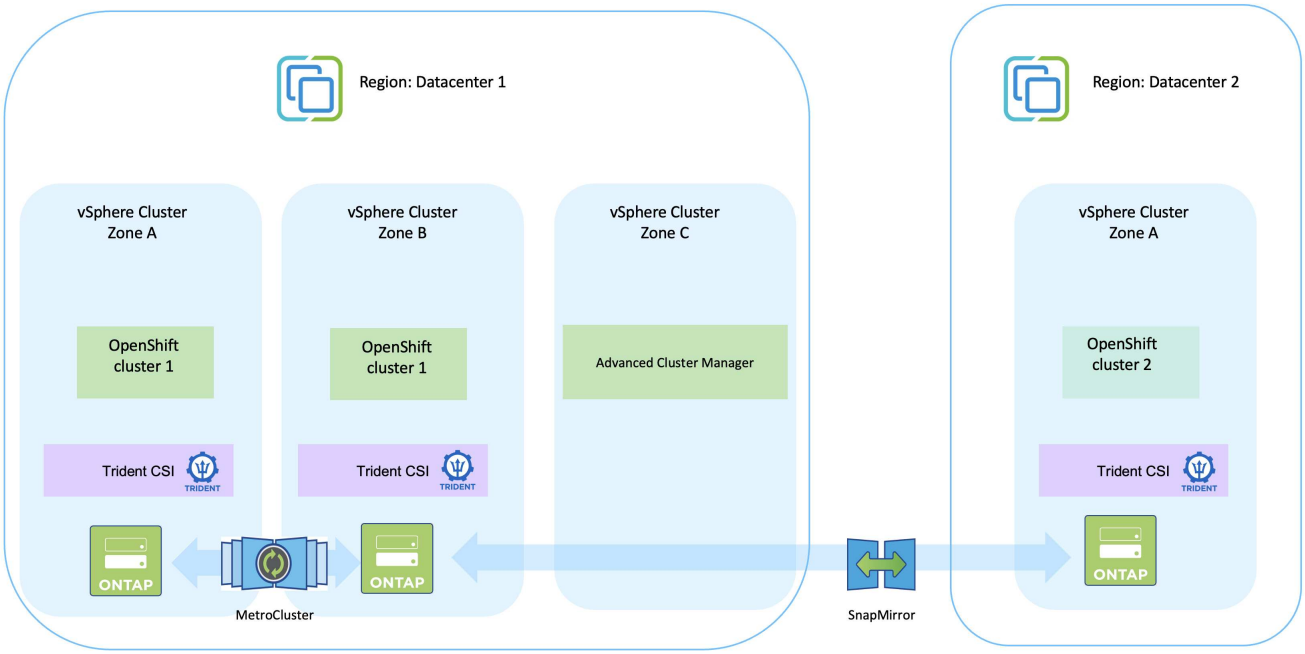


Implementar y configurar la plataforma Red Hat OpenShift Container en VMware

Esta sección describe un flujo de trabajo de alto nivel sobre cómo configurar y administrar clústeres de OpenShift y administrar aplicaciones con estado en ellos. Se muestra el uso de matrices de almacenamiento NetApp ONTAP con la ayuda de Trident para proporcionar volúmenes persistentes.

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

Aquí se muestra un diagrama que representa los clústeres implementados en VMware en un centro de datos.



El proceso de configuración se puede dividir en los siguientes pasos:

Implementar y configurar una máquina virtual CentOS

- Se implementa en el entorno VMware vSphere.
- Esta máquina virtual se utiliza para implementar algunos componentes como NetApp Trident y NetApp Trident Protect para la solución.
- Se configura un usuario root en esta máquina virtual durante la instalación.

Implementar y configurar un clúster de OpenShift Container Platform en VMware vSphere (Hub Cluster)

Consulte las instrucciones para el"Despliegue asistido" Método para implementar un clúster OCP.

> Recuerde lo siguiente: - Crear una clave pública y privada ssh para proporcionarla al instalador. Estas claves se utilizarán para iniciar sesión en los nodos maestro y de trabajo si es necesario. - Descargue el programa instalador desde el instalador asistido. Este programa se utiliza para iniciar las máquinas virtuales que crea en el entorno VMware vSphere para los nodos maestro y de trabajo. - Las máquinas virtuales deben tener los requisitos mínimos de CPU, memoria y disco duro. (Consulte los comandos de creación de vm en"este" página para los nodos maestro y de trabajo que proporcionan esta información) - El diskUUID debe estar habilitado en todas las máquinas virtuales. - Cree un mínimo de 3 nodos para el maestro y 3 nodos para el trabajador. - Una vez que el instalador los descubra, active el botón de alternancia de integración de VMware vSphere.

Instalar la gestión avanzada de clústeres en el clúster del concentrador

Esto se instala utilizando el Operador de administración de clúster avanzado en el clúster central. Consulte las instrucciones"aquí" .

Instalar dos clústeres OCP adicionales (origen y destino)

- Los clústeres adicionales se pueden implementar mediante el ACM en el clúster central.
- Consulte las instrucciones"aquí" .

Configurar el almacenamiento de NetApp ONTAP

- Instalar un clúster ONTAP con conectividad a las máquinas virtuales OCP en el entorno VMWare.
- Crear un SVM.
- Configurar el almacenamiento de datos NAS para acceder al almacenamiento en SVM.

Instalar NetApp Trident en los clústeres OCP

- Instalar NetApp Trident en los tres clústeres: concentrador, de origen y de destino
- Consulte las instrucciones"aquí" .
- Cree un backend de almacenamiento para ontap-nas.
- Cree una clase de almacenamiento para ontap-nas.
- Consulte las instrucciones"aquí" .

Implementar una aplicación en el clúster de origen

Utilice OpenShift GitOps para implementar una aplicación. (por ejemplo, Postgres, Ghost)

El siguiente paso es utilizar Trident Protect para la protección de datos y la migración de datos desde el clúster

de origen al de destino. Referirse"aquí" para obtener instrucciones.

Protección de datos mediante Astra

Esta página muestra las opciones de protección de datos para las aplicaciones basadas en Red Hat OpenShift Container que se ejecutan en VMware vSphere utilizando Trident Protect (ACC).

A medida que los usuarios emprenden el proceso de modernización de sus aplicaciones con Red Hat OpenShift, se debe implementar una estrategia de protección de datos para protegerlos contra la eliminación accidental o cualquier otro error humano. A menudo también se requiere una estrategia de protección por motivos regulatorios o de cumplimiento para proteger sus datos ante un desastre.

Los requisitos de protección de datos varían desde volver a una copia de un punto en el tiempo hasta conmutar automáticamente a un dominio de falla diferente sin ninguna intervención humana. Muchos clientes eligen ONTAP como su plataforma de almacenamiento preferida para sus aplicaciones Kubernetes debido a sus ricas características como multitenencia, multiprotocolo, alto rendimiento y ofertas de capacidad, replicación y almacenamiento en caché para ubicaciones de múltiples sitios, seguridad y flexibilidad.

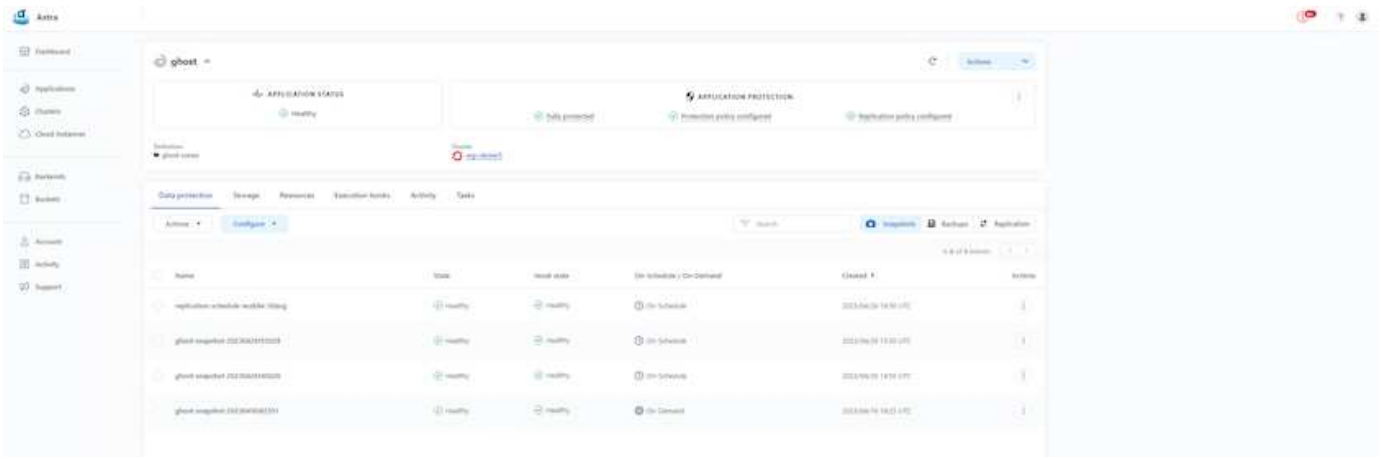
La protección de datos en ONTAP se puede lograr mediante **instantáneas**, **copias de seguridad y restauración** ad hoc o controladas por políticas.

Tanto las copias de seguridad como las instantáneas protegen los siguientes tipos de datos: - **Los metadatos de la aplicación que representan el estado de la aplicación** - **Todos los volúmenes de datos persistentes asociados con la aplicación** - **Todos los artefactos de recursos que pertenecen a la aplicación**

Instantánea con ACC

Se puede capturar una copia de los datos en un punto en el tiempo utilizando Snapshot con ACC. La política de protección define la cantidad de copias de instantáneas que se deben conservar. La opción de horario mínimo disponible es por hora. Se pueden tomar copias instantáneas manuales a pedido en cualquier momento y en intervalos más cortos que las copias instantáneas programadas. Las copias instantáneas se almacenan en el mismo volumen aprovisionado que la aplicación.

Configuración de instantáneas con ACC

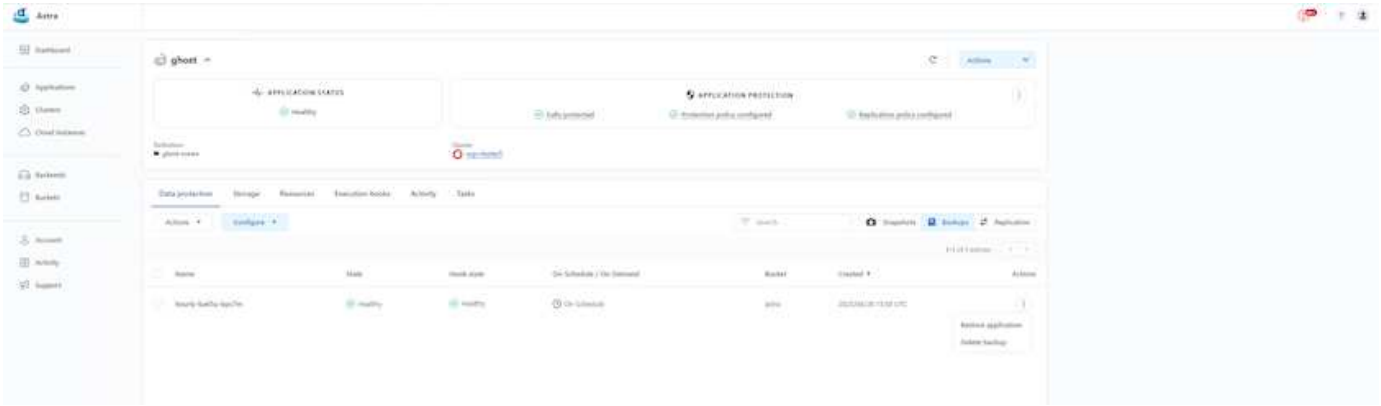


Copia de seguridad y restauración con ACC

Una copia de seguridad se basa en una instantánea. Trident Protect puede tomar copias instantáneas usando CSI y realizar copias de seguridad usando la copia instantánea de un punto en el tiempo. La copia de seguridad se almacena en un almacén de objetos externo (cualquier compatible con S3, incluido ONTAP S3 en una ubicación diferente). Se puede configurar la política de protección para las copias de seguridad programadas y la cantidad de versiones de copia de seguridad a conservar. El RPO mínimo es de una hora.

Restaurar una aplicación desde una copia de seguridad mediante ACC

ACC restaura la aplicación desde el depósito S3 donde se almacenan las copias de seguridad.



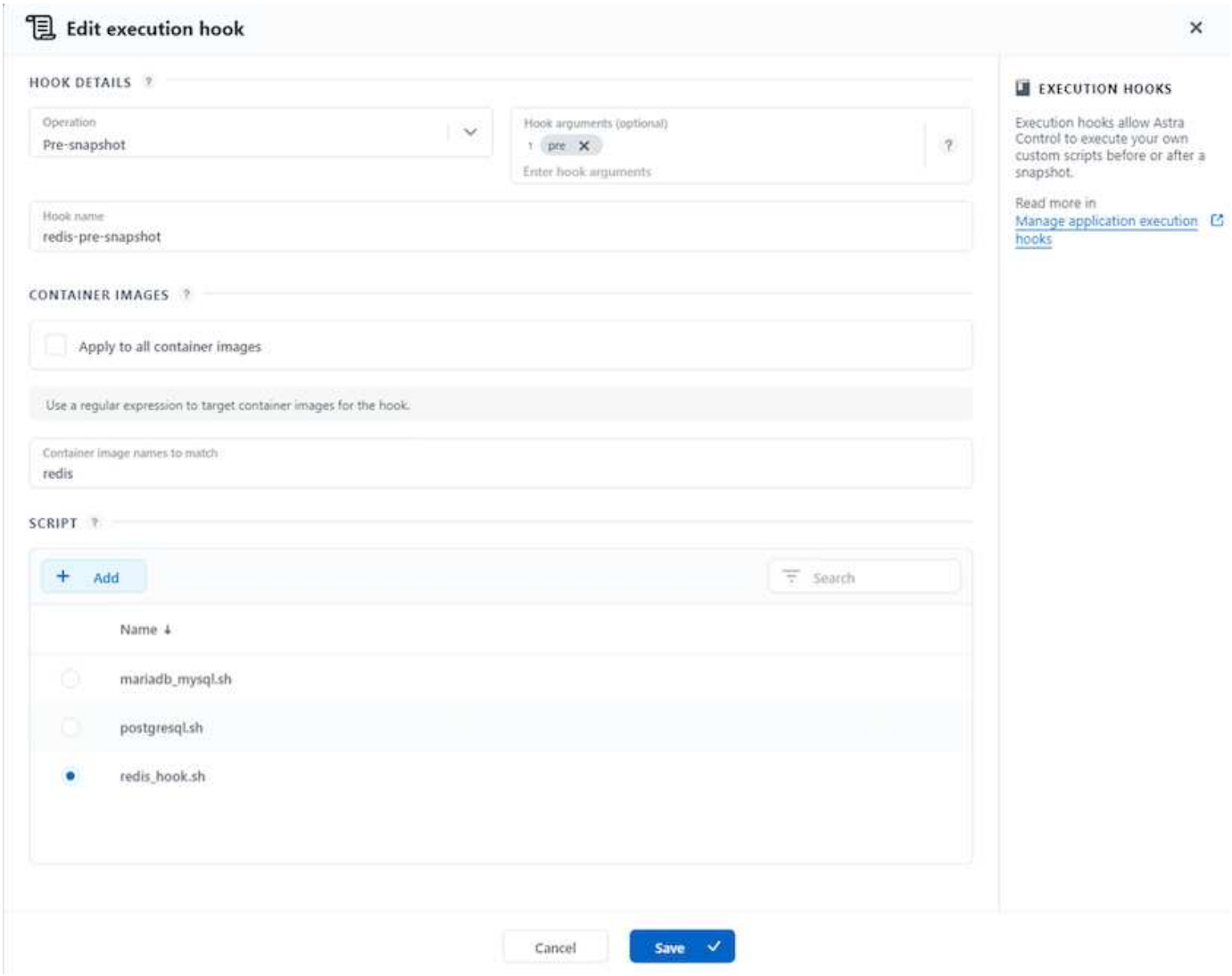
Ganchos de ejecución específicos de la aplicación

Además, los ganchos de ejecución se pueden configurar para que se ejecuten junto con una operación de protección de datos de una aplicación administrada. Si bien están disponibles las funciones de protección de datos a nivel de matriz de almacenamiento, a menudo se necesitan pasos adicionales para realizar copias de seguridad y restauraciones consistentes con las aplicaciones. Los pasos adicionales específicos de la aplicación podrían ser: - antes o después de crear una copia instantánea. - antes o después de crear una copia de seguridad. - después de restaurar desde una copia instantánea o de respaldo.

Astra Control puede ejecutar estos pasos específicos de la aplicación codificados como scripts personalizados llamados ganchos de ejecución.

"Proyecto NetApp Verda en GitHub"Proporciona ganchos de ejecución para aplicaciones nativas de la nube populares para que la protección de aplicaciones sea sencilla, sólida y fácil de orquestar. Siéntete libre de contribuir a ese proyecto si tienes suficiente información para una aplicación que no está en el repositorio.

Ejemplo de gancho de ejecución para pre-instantánea de una aplicación redis.



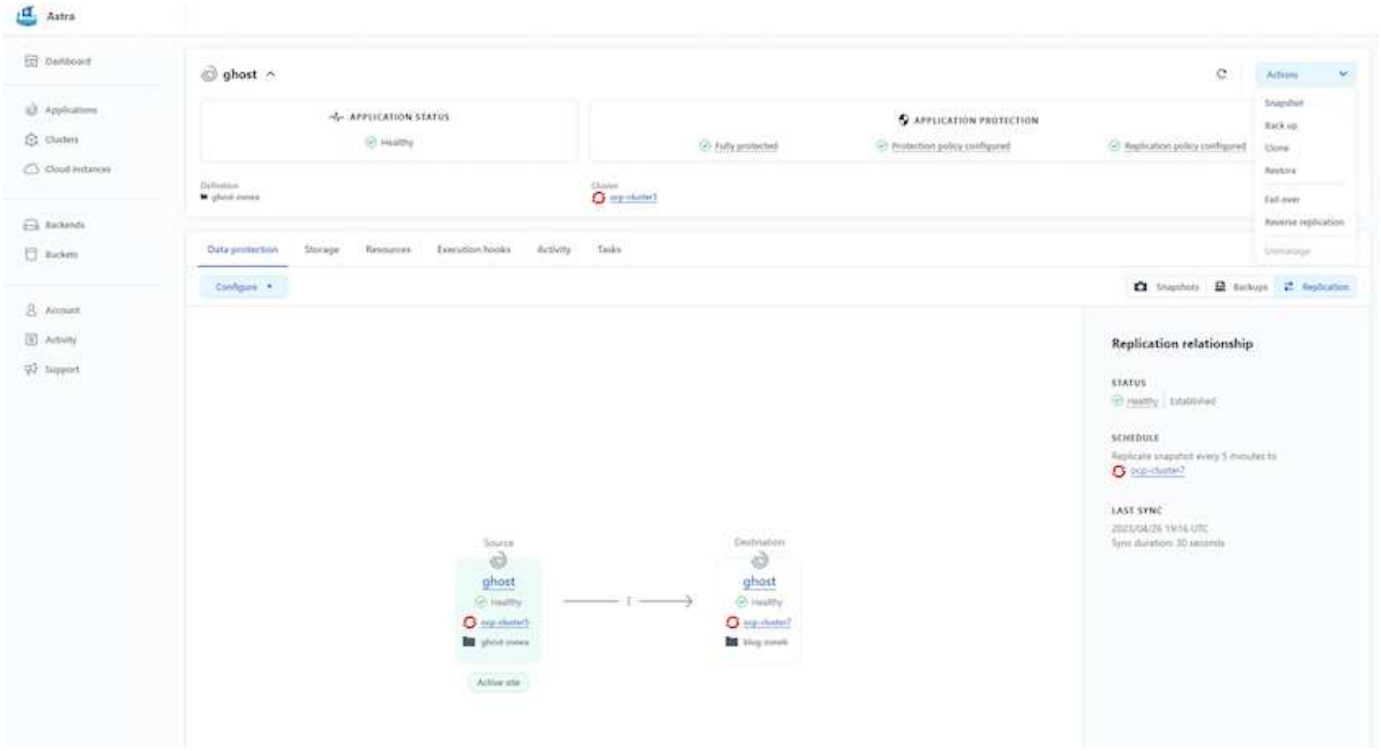
Replicación con ACC

Para obtener protección regional o una solución de RPO y RTO bajos, una aplicación se puede replicar en otra instancia de Kubernetes que se ejecute en un sitio diferente, preferiblemente en otra región. Trident Protect utiliza SnapMirror asíncrono de ONTAP con un RPO de tan solo 5 minutos. La replicación se realiza replicando a ONTAP y luego una conmutación por error crea los recursos de Kubernetes en el clúster de destino.

> Tenga en cuenta que la replicación es diferente de la copia de seguridad y la restauración, donde la copia de seguridad va a S3 y la restauración se realiza desde S3. Consulte el enlace: https://docs.netapp.com/us-en/astra-control-center/concepts/data-protection.html#replication-to-a-remote-cluster [aquí] para obtener detalles adicionales sobre las diferencias entre los dos tipos de protección de datos.

Referirse"aquí" para obtener instrucciones de configuración de SnapMirror .

SnapMirror con ACC



Los controladores de almacenamiento san-economy y nas-economy no admiten la función de replicación. Referirse"aquí" Para más detalles.

Vídeo de demostración:

"Vídeo de demostración de recuperación ante desastres con Trident Protect"

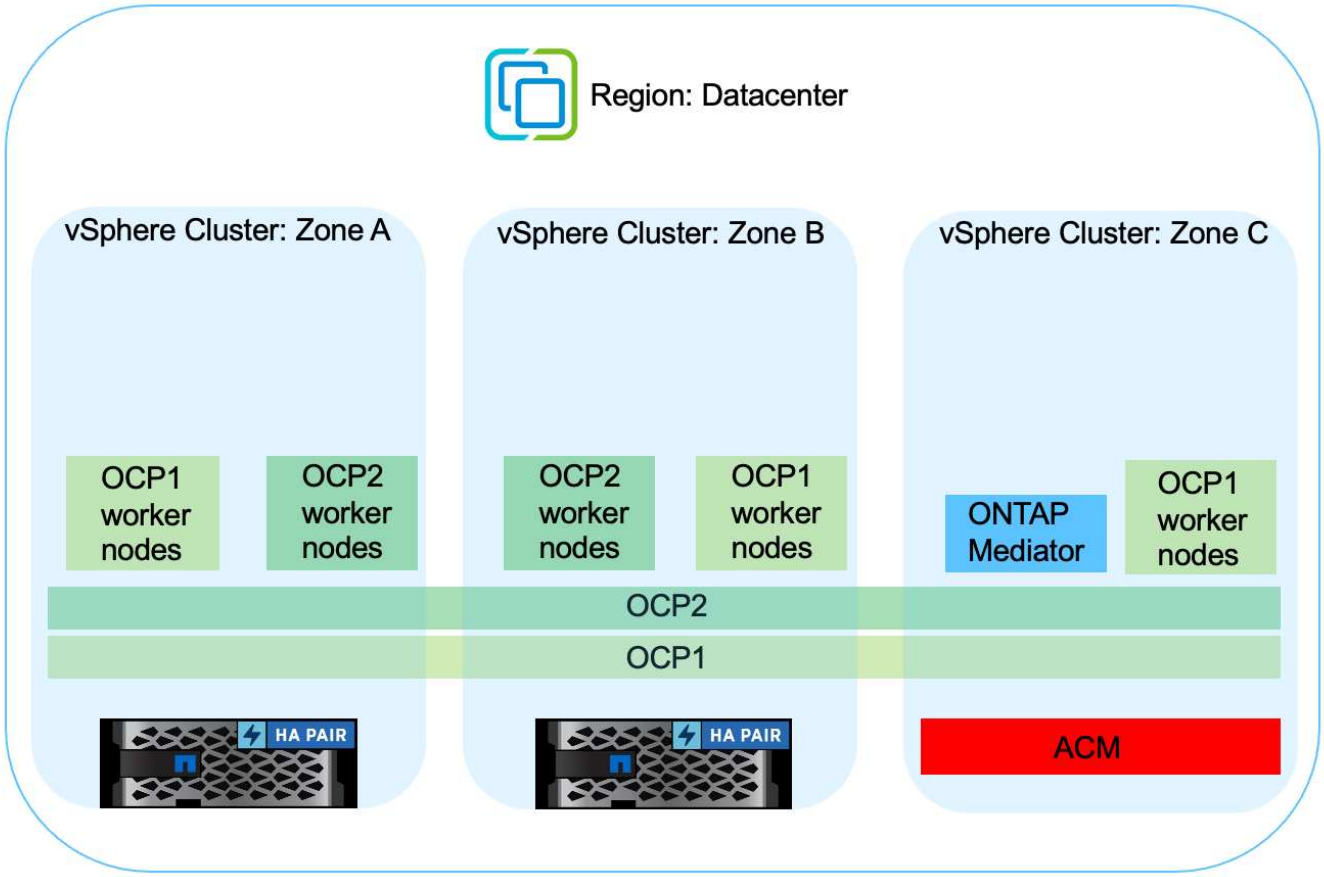
Protección de datos con Trident Protect

Continuidad de negocio con MetroCluster

La mayor parte de nuestra plataforma de hardware para ONTAP tiene características de alta disponibilidad para proteger contra fallas del dispositivo, evitando la necesidad de realizar recuperación ante desastres. Pero para protegerse de incendios o cualquier otro desastre y continuar el negocio con cero RPO y bajo RTO, a menudo se utiliza una solución MetroCluster .

Los clientes que actualmente cuentan con un sistema ONTAP pueden ampliarlo a MetroCluster agregando sistemas ONTAP compatibles dentro de las limitaciones de distancia para brindar recuperación ante desastres a nivel de zona. Trident, la CSI (interfaz de almacenamiento de contenedores) admite NetApp ONTAP, incluida la configuración de MetroCluster , así como otras opciones como Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP, etc. Trident ofrece cinco opciones de controlador de almacenamiento para ONTAP y todas son compatibles con la configuración de MetroCluster . Referirse"aquí" para obtener detalles adicionales sobre los controladores de almacenamiento ONTAP compatibles con Trident.

La solución MetroCluster requiere una extensión de red de capa 2 o la capacidad de acceder a la misma dirección de red desde ambos dominios de falla. Una vez que la configuración de MetroCluster está en su lugar, la solución es transparente para los propietarios de las aplicaciones, ya que todos los volúmenes en el svm de MetroCluster están protegidos y obtienen los beneficios de SyncMirror (RPO cero).



Para la configuración de backend de Trident (TBC), no especifique dataLIF ni SVM cuando utilice la configuración de MetroCluster . Especifique la IP de administración de SVM para managementLIF y use las credenciales del rol vsadmin.

Los detalles sobre las funciones de protección de datos de Trident Protect están disponibles"aquí"

Migración de datos mediante Trident Protect

Esta página muestra las opciones de migración de datos para cargas de trabajo de contenedores en clústeres de Red Hat OpenShift con Trident Protect.

A menudo es necesario trasladar las aplicaciones de Kubernetes de un entorno a otro. Para migrar una aplicación junto con sus datos persistentes, se puede utilizar NetApp Trident Protect.

Migración de datos entre diferentes entornos de Kubernetes

ACC admite varias versiones de Kubernetes, incluidas Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Upstream Kubernetes, etc. Para obtener más detalles, consulte"aquí" .

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

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

Consulte la"sección de protección de datos" para las opciones de **replicación y copia de seguridad y restauración**.

Referirse"aquí" para obtener detalles adicionales sobre la **clonación**.

Realizar la replicación de datos mediante ACC