Mejores prácticas y recomendaciones

Trident

NetApp
January 15, 2026

Tabla de contenidos

Mejores prácticas y recomendaciones . . . 1
- Despliegue . . . 1
  - Implementar en un espacio de nombres dedicado . . . 1
  - Utilice cuotas y límites de rango para controlar el consumo de almacenamiento. . . . 1
- Configuración de almacenamiento . . . 1
  - Descripción general de la plataforma . . . 1
  - Mejores prácticas de ONTAP y Cloud Volumes ONTAP . . . 1
  - Mejores prácticas de SolidFire . . . 6
  - ¿Dónde puedo encontrar más información? . . . 8
- Integrar Trident . . . 8
  - Selección y despliegue de controladores . . . 9
  - Diseño de clase de almacenamiento . . . 12
  - Diseño de piscina virtual . . . 13
  - Operaciones de volumen . . . 14
  - Servicio de métricas . . . 18
- Protección de datos y recuperación ante desastres . . . 19
  - replicación y recuperación de Trident . . . 19
  - replicación y recuperación de SVM . . . 20
  - replicación y recuperación de volumen . . . 21
  - Protección de datos de instantáneas . . . 21
- Seguridad . . . 21
  - Seguridad . . . 21
  - Configuración de clave unificada de Linux (LUKS) . . . 23
  - Cifrado en vuelo Kerberos . . . 29

Mejores prácticas y recomendaciones

Despliegue

Utilice las recomendaciones que se enumeran aquí al implementar Trident.

Implementar en un espacio de nombres dedicado

"Espacios de nombres"Proporcionan separación administrativa entre diferentes aplicaciones y constituyen una barrera para el intercambio de recursos. Por ejemplo, un PVC de un espacio de nombres no se puede consumir desde otro. Trident proporciona recursos PV a todos los espacios de nombres del clúster de Kubernetes y, en consecuencia, utiliza una cuenta de servicio con privilegios elevados.

Además, el acceso al pod Trident podría permitir a un usuario acceder a las credenciales del sistema de almacenamiento y otra información confidencial. Es importante garantizar que los usuarios de la aplicación y las aplicaciones de gestión no tengan la capacidad de acceder a las definiciones de objetos de Trident ni a los propios pods.

Utilice cuotas y límites de rango para controlar el consumo de almacenamiento.

Kubernetes cuenta con dos características que, combinadas, proporcionan un mecanismo potente para limitar el consumo de recursos por parte de las aplicaciones. El "mecanismo de cuota de almacenamiento" permite al administrador implementar límites de consumo de capacidad y recuento de objetos globales y específicos de la clase de almacenamiento por espacio de nombres. Además, utilizando un "límite de rango" Garantiza que las solicitudes de PVC se encuentren dentro de un valor mínimo y máximo antes de que la solicitud se envíe al proveedor.

Estos valores se definen para cada espacio de nombres, lo que significa que cada espacio de nombres debe tener valores definidos que se ajusten a sus requisitos de recursos. Consulte aquí para obtener información sobre "cómo aprovechar las cuotas" .

Configuración de almacenamiento

Cada plataforma de almacenamiento del portafolio de NetApp tiene capacidades únicas que benefician a las aplicaciones, ya sean contenerizadas o no.

Descripción general de la plataforma

Trident funciona con ONTAP y Element. No existe una plataforma que se adapte mejor a todas las aplicaciones y escenarios que otra; sin embargo, al elegir una plataforma se deben tener en cuenta las necesidades de la aplicación y del equipo que administra el dispositivo.

Debes seguir las mejores prácticas básicas para el sistema operativo anfitrión con el protocolo que estés utilizando. Opcionalmente, puede considerar incorporar las mejores prácticas de la aplicación, cuando estén disponibles, con la configuración de backend, clase de almacenamiento y PVC para optimizar el almacenamiento para aplicaciones específicas.

Mejores prácticas de ONTAP y Cloud Volumes ONTAP

Aprenda las mejores prácticas para configurar ONTAP y Cloud Volumes ONTAP para Trident.

Las siguientes recomendaciones son pautas para configurar ONTAP para cargas de trabajo en contenedores, que consumen volúmenes aprovisionados dinámicamente por Trident. Cada una debe ser considerada y evaluada para determinar su idoneidad en su entorno.

Utilice SVM dedicados a Trident.

Las máquinas virtuales de almacenamiento (SVM) proporcionan aislamiento y separación administrativa entre inquilinos en un sistema ONTAP . Dedicar una SVM a las aplicaciones permite la delegación de privilegios y la aplicación de las mejores prácticas para limitar el consumo de recursos.

Existen varias opciones disponibles para la gestión de la SVM:

- Proporcione la interfaz de administración del clúster en la configuración del backend, junto con las credenciales apropiadas, y especifique el nombre de la SVM.
- Cree una interfaz de administración dedicada para la SVM utilizando ONTAP System Manager o la CLI.
- Comparta el rol de gestión con una interfaz de datos NFS.

En cada caso, la interfaz debe estar en el DNS y el nombre DNS debe usarse al configurar Trident. Esto ayuda a facilitar algunos escenarios de recuperación ante desastres, por ejemplo, SVM-DR sin el uso de retención de identidad de red.

No hay preferencia entre tener una LIF de administración dedicada o compartida para la SVM; sin embargo, debe asegurarse de que sus políticas de seguridad de red se alineen con el enfoque que elija. En cualquier caso, la LIF de gestión debería ser accesible a través de DNS para facilitar la máxima flexibilidad. "SVM-DR" debe utilizarse conjuntamente con Trident.

Limitar el recuento de volumen máximo

Los sistemas de almacenamiento ONTAP tienen un número máximo de volúmenes, que varía según la versión del software y la plataforma de hardware. Referirse a "NetApp Hardware Universe" para su plataforma específica y versión de ONTAP para determinar los límites exactos. Cuando se agota el número de volúmenes, las operaciones de aprovisionamiento fallan no solo para Trident, sino para todas las solicitudes de almacenamiento.

Trident's `ontap-nas` y `ontap-san` Los controladores aprovisionan un FlexVolume para cada Volumen Persistente (PV) de Kubernetes que se crea. El `ontap-nas-economy` El controlador crea aproximadamente un FlexVolume por cada 200 PV (configurable entre 50 y 300). El `ontap-san-economy` El controlador crea aproximadamente un FlexVolume por cada 100 PV (configurable entre 50 y 200). Para evitar que Trident consuma todos los volúmenes disponibles en el sistema de almacenamiento, debe establecer un límite en la SVM. Puedes hacer esto desde la línea de comando:

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

El valor para `max-volumes` varía en función de varios criterios específicos de su entorno:

- Número de volúmenes existentes en el clúster ONTAP
- El número de volúmenes que prevé aprovisionar fuera de Trident para otras aplicaciones
- Número de volúmenes persistentes que se espera que consuman las aplicaciones de Kubernetes

El `max-volumes` El valor es el total de volúmenes aprovisionados en todos los nodos del clúster ONTAP , y no en un nodo ONTAP individual. Como resultado, es posible que encuentre algunas condiciones en las que

un nodo de clúster de ONTAP podría tener muchos más o menos volúmenes aprovisionados Trident que otro nodo.

Por ejemplo, un clúster ONTAP de dos nodos tiene la capacidad de alojar un máximo de 2000 volúmenes FlexVol . Establecer el recuento máximo de volumen en 1250 parece muy razonable. Sin embargo, si tan solo "agregados" Si los agregados asignados desde un nodo se asignan al SVM, o si los agregados asignados desde un nodo no se pueden aprovisionar (por ejemplo, debido a la capacidad), entonces el otro nodo se convierte en el destino de todos los volúmenes aprovisionados de Trident . Esto significa que el límite de volumen podría alcanzarse para ese nodo antes de que… `max-volumes` Se alcanza un valor determinado, lo que repercute tanto en Trident como en otras operaciones de volumen que utilizan ese nodo. **Puede evitar esta situación asegurándose de que los agregados de cada nodo del clúster se asignen a la SVM utilizada por Trident en igual número.**

Clonar un volumen

NetApp Trident admite la clonación de volúmenes al usar `ontap-nas` , `ontap-san` , `solidfire-san` , y `gcp-cvs` Controladores de almacenamiento. Al usar el `ontap-nas-flexgroup` o `ontap-nas-economy` controladores, la clonación no es compatible. La creación de un nuevo volumen a partir de un volumen existente dará como resultado la creación de una nueva instantánea.

> Evite clonar un PVC que esté asociado con una StorageClass diferente. Realice operaciones de clonación dentro de la misma StorageClass para garantizar la compatibilidad y evitar comportamientos inesperados.

Limitar el tamaño máximo de los volúmenes creados por Trident

Para configurar el tamaño máximo de los volúmenes que puede crear Trident, utilice el `limitVolumeSize` parámetro en su `backend.json` definición.

Además de controlar el tamaño del volumen en la matriz de almacenamiento, también debe aprovechar las capacidades de Kubernetes.

Limitar el tamaño máximo de los FlexVols creados por Trident

Para configurar el tamaño máximo de los FlexVols utilizados como pools para los controladores ontap-san-economy y ontap-nas-economy, utilice el siguiente comando: `limitVolumePoolSize` parámetro en su `backend.json` definición.

Configure Trident para usar CHAP bidireccional.

Puedes especificar el iniciador CHAP y los nombres de usuario y contraseñas de destino en la definición de tu backend y hacer que Trident habilite CHAP en la SVM. Utilizando el `useCHAP` En la configuración de su backend, Trident autentica las conexiones iSCSI para backends ONTAP con CHAP.

Cree y utilice una política de QoS para SVM.

Al aprovechar una política QoS de ONTAP , aplicada a la SVM, se limita el número de IOPS que pueden consumir los volúmenes aprovisionados de Trident . Esto ayuda a "prevenir el acoso" o un contenedor fuera de control que afecte a cargas de trabajo externas a la SVM de Trident .

Puedes crear una política QoS para la SVM en pocos pasos. Consulte la documentación de su versión de ONTAP para obtener la información más precisa. El ejemplo a continuación crea una política de QoS que limita el total de IOPS disponibles para la SVM a 5000.

```
# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>
```

Además, si su versión de ONTAP lo admite, puede considerar el uso de un mínimo de QoS para garantizar una cantidad de rendimiento para las cargas de trabajo en contenedores. La QoS adaptativa no es compatible con una política a nivel de SVM.

El número de IOPS dedicadas a las cargas de trabajo en contenedores depende de muchos aspectos. Entre otras cosas, estas incluyen:

- Otras cargas de trabajo que utilizan la matriz de almacenamiento. Si existen otras cargas de trabajo, no relacionadas con la implementación de Kubernetes, que utilizan los recursos de almacenamiento, se debe tener cuidado para garantizar que dichas cargas de trabajo no se vean afectadas negativamente de forma accidental.
- Cargas de trabajo previstas que se ejecutan en contenedores. Si las cargas de trabajo con altos requisitos de IOPS se ejecutan en contenedores, una política de QoS baja resulta en una mala experiencia.

Es importante recordar que una política de QoS asignada a nivel de SVM da como resultado que todos los volúmenes aprovisionados al SVM compartan el mismo grupo de IOPS. Si una, o un pequeño número, de las aplicaciones en contenedores tienen un alto requerimiento de IOPS, podrían convertirse en un problema para las demás cargas de trabajo en contenedores. Si este es el caso, quizás le convenga considerar el uso de automatización externa para asignar políticas de QoS por volumen.

> Debe asignar el grupo de políticas QoS al SVM **únicamente** si su versión de ONTAP es anterior a la 9.8.

Cree grupos de políticas de QoS para Trident.

La calidad de servicio (QoS) garantiza que el rendimiento de las cargas de trabajo críticas no se vea degradado por cargas de trabajo competidoras. Los grupos de políticas QoS de ONTAP proporcionan opciones de QoS para volúmenes y permiten a los usuarios definir el límite máximo de rendimiento para una o más cargas de trabajo. Para obtener más información sobre QoS, consulte "Garantizar el rendimiento con QoS" . Puede especificar grupos de políticas QoS en el backend o en un grupo de almacenamiento, y estos se aplicarán a cada volumen creado en ese grupo o backend.

ONTAP cuenta con dos tipos de grupos de políticas QoS: tradicionales y adaptativas. Los grupos de políticas tradicionales proporcionan un rendimiento máximo (o mínimo, en versiones posteriores) fijo en IOPS. La QoS adaptativa ajusta automáticamente el rendimiento al tamaño de la carga de trabajo, manteniendo la relación de IOPS a TB/GB a medida que cambia el tamaño de la carga de trabajo. Esto proporciona una ventaja significativa cuando se gestionan cientos o miles de cargas de trabajo en una implementación de gran tamaño.

Tenga en cuenta lo siguiente al crear grupos de políticas de QoS:

- Debes configurar el `qosPolicy` clave en el `defaults` bloque de la configuración del backend. Vea el siguiente ejemplo de configuración de backend:

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
storage:
  - labels:
      performance: extreme
    defaults:
      adaptiveQosPolicy: extremely-adaptive-pg
  - labels:
      performance: premium
    defaults:
      qosPolicy: premium-pg
```

- Debe aplicar los grupos de políticas por volumen, de modo que cada volumen obtenga el rendimiento total especificado por el grupo de políticas. No se admiten grupos de políticas compartidas.

Para obtener más información sobre los grupos de políticas de QoS, consulte "Referencia de comandos de ONTAP" .

Limitar el acceso a los recursos de almacenamiento a los miembros del clúster de Kubernetes

Limitar el acceso a los volúmenes NFS, LUN iSCSI y LUN FC creados por Trident es un componente crítico de la postura de seguridad para su implementación de Kubernetes. Al hacerlo, se evita que los hosts que no forman parte del clúster de Kubernetes accedan a los volúmenes y potencialmente modifiquen los datos de forma inesperada.

Es importante comprender que los espacios de nombres son el límite lógico de los recursos en Kubernetes. Se asume que los recursos en el mismo espacio de nombres se pueden compartir; sin embargo, es importante destacar que no existe capacidad para compartir entre espacios de nombres. Esto significa que, aunque los PV son objetos globales, cuando están vinculados a un PVC solo son accesibles para los pods que se encuentran en el mismo espacio de nombres. **Es fundamental garantizar que se utilicen espacios de nombres para proporcionar separación cuando sea apropiado.**

La principal preocupación para la mayoría de las organizaciones con respecto a la seguridad de los datos en un contexto de Kubernetes es que un proceso en un contenedor pueda acceder al almacenamiento montado en el host, pero que no está destinado al contenedor. "Espacios de nombres" están diseñados para prevenir este tipo de vulneración. Sin embargo, existe una excepción: los contenedores privilegiados.

Un contenedor privilegiado es aquel que se ejecuta con muchos más permisos a nivel de host de lo normal. Estas opciones no están denegadas de forma predeterminada, así que asegúrese de deshabilitar la funcionalidad mediante el uso de "políticas de seguridad de pods" .

Para los volúmenes en los que se desea acceso tanto desde Kubernetes como desde hosts externos, el

almacenamiento debe gestionarse de forma tradicional, con el PV introducido por el administrador y no gestionado por Trident. Esto garantiza que el volumen de almacenamiento se destruya solo cuando tanto Kubernetes como los hosts externos se hayan desconectado y ya no estén utilizando el volumen. Además, se puede aplicar una política de exportación personalizada, que permite el acceso desde los nodos del clúster de Kubernetes y servidores específicos fuera del clúster de Kubernetes.

Para implementaciones que tienen nodos de infraestructura dedicados (por ejemplo, OpenShift) u otros nodos que no pueden programar aplicaciones de usuario, se deben utilizar políticas de exportación separadas para limitar aún más el acceso a los recursos de almacenamiento. Esto incluye la creación de una política de exportación para los servicios que se implementan en esos nodos de infraestructura (por ejemplo, los servicios de métricas y registro de OpenShift) y las aplicaciones estándar que se implementan en nodos que no son de infraestructura.

Utilice una política de exportación específica

Debe asegurarse de que exista una política de exportación para cada backend que solo permita el acceso a los nodos presentes en el clúster de Kubernetes. Trident puede crear y gestionar automáticamente políticas de exportación. De esta manera, Trident limita el acceso a los volúmenes que aprovisiona a los nodos del clúster de Kubernetes y simplifica la adición o eliminación de nodos.

Como alternativa, también puede crear una política de exportación manualmente y completarla con una o más reglas de exportación que procesen cada solicitud de acceso a un nodo:

- Utilice el `vserver export-policy create` Comando CLI de ONTAP para crear la política de exportación.
- Agregue reglas a la política de exportación utilizando el `vserver export-policy rule create` Comando CLI de ONTAP .

Al ejecutar estos comandos, podrá restringir qué nodos de Kubernetes tienen acceso a los datos.

Desactivar `showmount` para la aplicación SVM

El `showmount` Esta función permite que un cliente NFS consulte al SVM para obtener una lista de las exportaciones NFS disponibles. Un pod desplegado en el clúster de Kubernetes puede emitir el `showmount -e` Ejecuta el comando contra el servidor y recibe una lista de los puntos de montaje disponibles, incluidos aquellos a los que no tiene acceso. Si bien esto, por sí solo, no constituye una vulneración de la seguridad, sí proporciona información innecesaria que podría ayudar a un usuario no autorizado a conectarse a una exportación NFS.

Debes desactivar `showmount` utilizando el comando CLI de ONTAP a nivel de SVM:

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

Mejores prácticas de SolidFire

Aprenda las mejores prácticas para configurar el almacenamiento SolidFire para Trident.

Crear cuenta de Solidfire

Cada cuenta de SolidFire representa un propietario de volumen único y recibe su propio conjunto de credenciales del Protocolo de Autenticación por Desafío-Respuesta (CHAP). Puede acceder a los volúmenes asignados a una cuenta utilizando el nombre de la cuenta y las credenciales CHAP correspondientes o a

través de un grupo de acceso a volúmenes. Una cuenta puede tener asignados hasta dos mil volúmenes, pero un volumen solo puede pertenecer a una cuenta.

Crea una política de QoS

Utilice las políticas de Calidad de Servicio (QoS) de SolidFire si desea crear y guardar una configuración de calidad de servicio estandarizada que se pueda aplicar a muchos volúmenes.

Puede configurar los parámetros de QoS para cada volumen. El rendimiento de cada volumen se puede garantizar configurando tres parámetros configurables que definen la QoS: IOPS mínimas, IOPS máximas e IOPS de ráfaga.

Aquí están los posibles valores mínimos, máximos y de ráfaga de IOPS para el tamaño de bloque de 4Kb.

Parámetro IOPS	Definición	Valor mínimo	Valor predeterminado	Valor máximo (4 KB)
IOPS mínimas	El nivel de rendimiento garantizado para un volumen.	50	50	15000
IOPS máximas	El rendimiento no excederá este límite.	50	15000	200.000
Burst IOPS	IOPS máximo permitido en un escenario de ráfaga corta.	50	15000	200.000

Aunque el IOPS máximo y el IOPS de ráfaga se pueden configurar hasta en 200.000, el rendimiento máximo real de un volumen está limitado por el uso del clúster y el rendimiento por nodo.

El tamaño del bloque y el ancho de banda influyen directamente en el número de IOPS. A medida que aumenta el tamaño de los bloques, el sistema incrementa el ancho de banda hasta el nivel necesario para procesar los bloques de mayor tamaño. A medida que aumenta el ancho de banda, disminuye el número de IOPS que el sistema puede alcanzar. Referirse a "Calidad de servicio de SolidFire" Para obtener más información sobre QoS y rendimiento.

Autenticación de SolidFire

Element admite dos métodos de autenticación: CHAP y Grupos de Acceso por Volumen (VAG). CHAP utiliza el protocolo CHAP para autenticar el host ante el servidor backend. Los grupos de acceso a volúmenes controlan el acceso a los volúmenes que aprovisionan. NetApp recomienda utilizar CHAP para la autenticación, ya que es más sencillo y no tiene límites de escalabilidad.

Trident con el aprovisionador CSI mejorado admite el uso de la autenticación CHAP. Los VAG solo deben utilizarse en el modo de funcionamiento tradicional no CSI.

La autenticación CHAP (verificación de que el iniciador es el usuario de volumen previsto) solo es compatible con el control de acceso basado en cuentas. Si utiliza CHAP para la autenticación, dispone de dos opciones:

CHAP unidireccional y CHAP bidireccional. El protocolo CHAP unidireccional autentica el acceso al volumen utilizando el nombre de cuenta de SolidFire y el secreto del iniciador. La opción CHAP bidireccional proporciona la forma más segura de autenticar el volumen porque el volumen autentica al host a través del nombre de cuenta y el secreto del iniciador, y luego el host autentica al volumen a través del nombre de cuenta y el secreto del destino.

Sin embargo, si no se puede habilitar CHAP y se requieren VAG, cree el grupo de acceso y agregue los iniciadores de host y los volúmenes al grupo de acceso. Cada IQN que agregue a un grupo de acceso puede acceder a cada volumen del grupo con o sin autenticación CHAP. Si el iniciador iSCSI está configurado para usar la autenticación CHAP, se utiliza el control de acceso basado en cuentas. Si el iniciador iSCSI no está configurado para usar la autenticación CHAP, entonces se utiliza el control de acceso de Grupo de Acceso a Volumen.

¿Dónde puedo encontrar más información?

A continuación se enumeran algunos de los documentos sobre mejores prácticas. Buscar en el "Biblioteca NetApp" para las versiones más recientes.

- ONTAP*
- "Guía de buenas prácticas e implementación de NFS"
- "Administración SAN"(para iSCSI)
- "Configuración de iSCSI Express para RHEL"

Software Element

- "Configuración de SolidFire para Linux"
- NetApp HCI*
- "Requisitos previos para la implementación de NetApp HCI"
- "Acceda al motor de implementación de NetApp"

Información sobre las mejores prácticas de la aplicación

- "Mejores prácticas para MySQL en ONTAP"
- "Mejores prácticas para MySQL en SolidFire"
- "NetApp SolidFire y Cassandra"
- "Mejores prácticas de Oracle en SolidFire"
- "Mejores prácticas de PostgreSQL en SolidFire"

No todas las aplicaciones tienen directrices específicas; es importante trabajar con su equipo de NetApp y utilizar las "Biblioteca NetApp" para encontrar la documentación más actualizada.

Integrar Trident

Para integrar Trident, se requiere la integración de los siguientes elementos de diseño y arquitectura: selección e implementación de controladores, diseño de clases de almacenamiento, diseño de grupos virtuales, impactos de Persistent Volume Claim (PVC) en el aprovisionamiento de almacenamiento, operaciones de volumen e implementación de servicios de OpenShift utilizando Trident.

Selección y despliegue de controladores

Seleccione e implemente un controlador de backend para su sistema de almacenamiento.

Controladores de backend de ONTAP

Los controladores backend de ONTAP se diferencian por el protocolo utilizado y la forma en que se aprovisionan los volúmenes en el sistema de almacenamiento. Por lo tanto, considere cuidadosamente qué controlador implementar.

En un nivel superior, si su aplicación tiene componentes que necesitan almacenamiento compartido (varios pods que acceden al mismo PVC), los controladores basados en NAS serían la opción predeterminada, mientras que los controladores iSCSI basados en bloques satisfacen las necesidades de almacenamiento no compartido. Elija el protocolo en función de los requisitos de la aplicación y el nivel de familiaridad de los equipos de almacenamiento e infraestructura. En términos generales, hay poca diferencia entre ellos para la mayoría de las aplicaciones, por lo que a menudo la decisión se basa en si se necesita o no almacenamiento compartido (donde más de un pod necesitará acceso simultáneo).

Los controladores de backend de ONTAP disponibles son:

- `ontap-nas`Cada PV aprovisionado es un ONTAP FlexVolume completo.
- `ontap-nas-economy`Cada PV aprovisionado es un qtree, con un número configurable de qtrees por FlexVolume (el valor predeterminado es 200).
- `ontap-nas-flexgroup`Cada PV se aprovisiona como un ONTAP FlexGroup completo y se utilizan todos los agregados asignados a una SVM.
- `ontap-san`Cada PV aprovisionado es un LUN dentro de su propio FlexVolume.
- `ontap-san-economy`Cada PV aprovisionado es un LUN, con un número configurable de LUN por FlexVolume (el valor predeterminado es 100).

Elegir entre los tres controladores NAS tiene algunas repercusiones en las funciones que se ponen a disposición de la aplicación.

Tenga en cuenta que, en las tablas siguientes, no todas las capacidades están expuestas a través de Trident. Algunas de estas funcionalidades deben ser aplicadas por el administrador de almacenamiento después del aprovisionamiento si se desea dicha funcionalidad. Las notas a pie de página en superíndice distinguen la funcionalidad de cada característica y controlador.

Controladores NAS ONTAP	Instantáneas	Clones	Políticas de exportación dinámicas	Multi-attach	Calidad de servicio	Cambiar tamaño	Replicación
`ontap-nas`	Sí	Sí	Sí, nota al pie:5[]	Sí	Sí, nota al pie:1[]	Sí	Sí, nota al pie:1[]
`ontap-nas-economy`	Sin nota al pie:3[]	Sin nota al pie:3[]	Sí, nota al pie:5[]	Sí	Sin nota al pie:3[]	Sí	Sin nota al pie:3[]
`ontap-nas-flexgroup`	Sí, nota al pie:1[]	NO	Sí, nota al pie:5[]	Sí	Sí, nota al pie:1[]	Sí	Sí, nota al pie:1[]

Trident ofrece 2 controladores SAN para ONTAP, cuyas capacidades se muestran a continuación.

Controladores SAN de ONTAP	Instantáneas	Clones	Multi-attach	CHAP bidireccional	Calidad de servicio	Cambiar tamaño	Replicación
`ontap-san`	Sí	Sí	Sí, nota al pie:4[]	Sí	Sí, nota al pie:1[]	Sí	Sí, nota al pie:1[]
`ontap-san-economy`	Sí	Sí	Sí, nota al pie:4[]	Sí	Sin nota al pie:3[]	Sí	Sin nota al pie:3[]

> Nota al pie de las tablas anteriores: Sí (nota al pie 1): No gestionado por Trident. Sí (nota al pie 2): Gestionado por Trident, pero sin granularidad PV. No (nota al pie 3): No gestionado por Trident ni con granularidad PV. Sí (nota al pie 4): Compatible con volúmenes de bloques sin formato. Sí (nota al pie 5): Compatible con Trident.

Las características que no son granulares a nivel de PV se aplican a todo el FlexVolume y todos los PV (es decir, qtrees o LUN en FlexVols compartidos) compartirán una programación común.

Como podemos ver en las tablas anteriores, gran parte de la funcionalidad entre los `ontap-nas` y `ontap-nas-economy` es lo mismo. Sin embargo, debido a que `ontap-nas-economy` El controlador limita la capacidad de controlar la programación a nivel de cada PV, lo que puede afectar especialmente a la planificación de la recuperación ante desastres y las copias de seguridad. Para los equipos de desarrollo que deseen aprovechar la funcionalidad de clonación de PVC en el almacenamiento ONTAP , esto solo es posible al usar el `ontap-nas` , `ontap-san` o `ontap-san-economy` conductores.

> El `solidfire-san` El controlador también es capaz de clonar PVC.

Controladores de backend de Cloud Volumes ONTAP

Cloud Volumes ONTAP proporciona control de datos junto con funciones de almacenamiento de clase empresarial para diversos casos de uso, incluyendo recursos compartidos de archivos y almacenamiento a nivel de bloque que admiten protocolos NAS y SAN (NFS, SMB/CIFS e iSCSI). Los controladores compatibles para Cloud Volume ONTAP son `ontap-nas` , `ontap-nas-economy` , `ontap-san` y `ontap-san-economy` . Estas son aplicables a Cloud Volume ONTAP para Azure y Cloud Volume ONTAP para GCP.

Controladores de backend de Amazon FSx para ONTAP

Amazon FSx for NetApp ONTAP le permite aprovechar las características, el rendimiento y las capacidades administrativas de NetApp con las que ya está familiarizado, al tiempo que se beneficia de la simplicidad, la agilidad, la seguridad y la escalabilidad del almacenamiento de datos en AWS. FSx para ONTAP admite muchas funciones del sistema de archivos ONTAP y API de administración. Los controladores compatibles para Cloud Volume ONTAP son `ontap-nas` , `ontap-nas-economy` , `ontap-nas-flexgroup` , `ontap-san` y `ontap-san-economy` .

Controladores de backend NetApp HCI/ SolidFire

El `solidfire-san` El controlador utilizado con las plataformas NetApp HCI/ SolidFire ayuda al administrador a configurar un backend de Element para Trident en función de los límites de QoS. Si desea diseñar su backend para establecer límites de QoS específicos en los volúmenes aprovisionados por Trident, utilice `type` parámetro en el archivo backend. El administrador también puede restringir el tamaño del volumen que se puede crear en el almacenamiento mediante la `limitVolumeSize` parámetro. Actualmente, las funciones de almacenamiento de Element, como el cambio de tamaño y la replicación de volúmenes, no son compatibles

con la versión anterior. `solidfire-san` conductor. Estas operaciones deben realizarse manualmente a través de la interfaz web de Element Software.

Controlador SolidFire	Instantáneas	Clones	Multi-attach	CHAP	Calidad de servicio	Cambiar tamaño	Replicación
`solidfire-san`	Sí	Sí	Sí, nota al pie:2[]	Sí	Sí	Sí	Sí, nota al pie:1[]

> Nota al pie: Sí (nota al pie 1): No gestionado por Trident. Sí (nota al pie 2): Compatible con volúmenes de bloques sin formato.

Controladores de backend de Azure NetApp Files

Trident utiliza el `azure-netapp-files` conductor para gestionar el"Azure NetApp Files" servicio.

Encontrará más información sobre este controlador y cómo configurarlo en"Configuración de backend de Trident para Azure NetApp Files" .

Controlador de Azure NetApp Files	Instantáneas	Clones	Multi-attach	Calidad de servicio	Expandir	Replicación
`azure-netapp-files`	Sí	Sí	Sí	Sí	Sí	Sí, nota al pie:1[]

> Nota al pie: Sí. Nota al pie 1: No gestionado por Trident.

Cloud Volumes Service en el controlador backend de Google Cloud

Trident utiliza el `gcp-cvs` Controlador para conectarse con el Cloud Volumes Service en Google Cloud.

El `gcp-cvs` El controlador utiliza grupos virtuales para abstraer el backend y permitir que Trident determine la ubicación del volumen. El administrador define los grupos virtuales en el `backend.json` archivos. Las clases de almacenamiento utilizan selectores para identificar los grupos virtuales por etiqueta.

- Si se definen grupos virtuales en el backend, Trident intentará crear un volumen en los grupos de almacenamiento de Google Cloud a los que están limitados esos grupos virtuales.
- Si no se definen grupos virtuales en el backend, Trident seleccionará un grupo de almacenamiento de Google Cloud de entre los grupos de almacenamiento disponibles en la región.

Para configurar el backend de Google Cloud en Trident, debe especificar `projectNumber` , `apiRegion` , y `apiKey` en el archivo de backend. Puedes encontrar el número de proyecto en la consola de Google Cloud. La clave API se toma del archivo de clave privada de la cuenta de servicio que creó al configurar el acceso a la API para Cloud Volumes Service en Google Cloud.

Para obtener detalles sobre los tipos y niveles de servicio de Cloud Volumes Service en Google Cloud, consulte:"Obtenga más información sobre la compatibilidad de Trident con CVS para GCP" .

Controlador del Cloud Volumes Service para Google Cloud	Instantáneas	Clones	Multi-attach	Calidad de servicio	Expandir	Replicación
`gcp-cvs`	Sí	Sí	Sí	Sí	Sí	Disponible únicamente en el tipo de servicio CVS-Performance.

Notas de replicación

- La replicación no la gestiona Trident.
- El clon se creará en el mismo grupo de almacenamiento que el volumen de origen.

Diseño de clase de almacenamiento

Es necesario configurar y aplicar clases de almacenamiento individuales para crear un objeto de clase de almacenamiento de Kubernetes. En esta sección se explica cómo diseñar una clase de almacenamiento para su aplicación.

Utilización específica del backend

El filtrado se puede utilizar dentro de un objeto de clase de almacenamiento específico para determinar qué grupo o conjunto de grupos de almacenamiento se utilizará con esa clase de almacenamiento específica. Se pueden configurar tres conjuntos de filtros en la clase de almacenamiento: `storagePools` , `additionalStoragePools` , y/o `excludeStoragePools` .

El `storagePools` Este parámetro ayuda a restringir el almacenamiento al conjunto de pools que coincidan con los atributos especificados. El `additionalStoragePools` El parámetro se utiliza para ampliar el conjunto de pools que Trident utiliza para el aprovisionamiento, junto con el conjunto de pools seleccionados por los atributos y `storagePools` parámetros. Puede utilizar cualquiera de los parámetros por separado o ambos juntos para asegurarse de que se selecciona el conjunto adecuado de grupos de almacenamiento.

El `excludeStoragePools` El parámetro se utiliza para excluir específicamente el conjunto de pools enumerados que coinciden con los atributos.

Emular políticas de QoS

Si desea diseñar clases de almacenamiento para emular políticas de calidad de servicio, cree una clase de almacenamiento con la siguiente estructura: `media` atributo como `hdd` o `ssd` . Basado en el `media` Trident seleccionará el backend apropiado que corresponda al atributo mencionado en la clase de almacenamiento. `hdd` o `ssd` agrega para que coincida con el atributo de medios y luego dirige el aprovisionamiento de los volúmenes al agregado específico. Por lo tanto, podemos crear una clase de almacenamiento PREMIUM que tendría `media` atributo establecido como `ssd` lo cual podría clasificarse como la política QoS PREMIUM. Podemos crear otra clase de almacenamiento STANDARD que tendría el atributo de medios establecido como `hdd`, que podría clasificarse como la política QoS STANDARD. También podríamos usar el atributo "IOPS" en la clase de almacenamiento para redirigir el aprovisionamiento a un dispositivo Element que se puede definir como una política de QoS.

Utilizar el backend en función de características específicas

Las clases de almacenamiento se pueden diseñar para dirigir el aprovisionamiento de volúmenes en un backend específico donde se habilitan funciones como el aprovisionamiento ligero y grueso, instantáneas, clones y cifrado. Para especificar qué almacenamiento utilizar, cree clases de almacenamiento que especifiquen el backend apropiado con la función requerida habilitada.

piscinas virtuales

Los pools virtuales están disponibles para todos los backends de Trident . Puedes definir grupos virtuales para cualquier backend, utilizando cualquier controlador que proporcione Trident .

Los grupos virtuales permiten a un administrador crear un nivel de abstracción sobre los backends a los que se puede hacer referencia a través de clases de almacenamiento, para una mayor flexibilidad y una ubicación eficiente de los volúmenes en los backends. Se pueden definir diferentes backends con la misma clase de servicio. Además, se pueden crear múltiples grupos de almacenamiento en el mismo backend, pero con características diferentes. Cuando una clase de almacenamiento se configura con un selector con etiquetas específicas, Trident elige un backend que coincida con todas las etiquetas del selector para ubicar el volumen. Si las etiquetas del selector de clase de almacenamiento coinciden con varios grupos de almacenamiento, Trident elegirá uno de ellos para aprovisionar el volumen.

Diseño de piscina virtual

Al crear un backend, generalmente se puede especificar un conjunto de parámetros. Antes, el administrador no podía crear otro backend con las mismas credenciales de almacenamiento y un conjunto de parámetros diferente. Con la introducción de los grupos virtuales, este problema se ha solucionado. Un grupo virtual es una abstracción de nivel entre el backend y la clase de almacenamiento de Kubernetes, que permite al administrador definir parámetros y etiquetas, a los que se puede hacer referencia mediante clases de almacenamiento de Kubernetes como selector, de forma independiente del backend. Se pueden definir grupos virtuales para todos los backends de NetApp compatibles con Trident. Esta lista incluye SolidFire/ NetApp HCI, ONTAP, Cloud Volumes Service en GCP y Azure NetApp Files.

> Al definir grupos virtuales, se recomienda no intentar reorganizar el orden de los grupos virtuales existentes en una definición de backend. También es recomendable no editar/modificar los atributos de un grupo virtual existente y, en su lugar, definir un nuevo grupo virtual.

Emulación de diferentes niveles de servicio/QoS

Es posible diseñar pools virtuales para emular clases de servicio. Utilizando la implementación de grupo virtual para Cloud Volume Service para Azure NetApp Files, examinemos cómo podemos configurar diferentes clases de servicio. Configure el backend de Azure NetApp Files con varias etiquetas que representen diferentes niveles de rendimiento. Colocar `servicelevel` ajuste cada aspecto al nivel de rendimiento adecuado y añada los demás aspectos necesarios bajo cada etiqueta. Ahora crea diferentes clases de almacenamiento de Kubernetes que se correspondan con diferentes grupos virtuales. Utilizando el `parameters.selector` En cada campo, cada StorageClass especifica qué grupos virtuales se pueden usar para alojar un volumen.

Asignación de un conjunto específico de aspectos

Se pueden diseñar múltiples pools virtuales con un conjunto específico de aspectos a partir de un único backend de almacenamiento. Para ello, configure el backend con múltiples etiquetas y establezca los aspectos necesarios bajo cada etiqueta. Ahora crea diferentes clases de almacenamiento de Kubernetes usando `parameters.selector` campo que se asignaría a diferentes grupos virtuales. Los volúmenes que se aprovisionan en el backend tendrán los aspectos definidos en el grupo virtual elegido.

Características del PVC que afectan al aprovisionamiento de almacenamiento

Algunos parámetros que van más allá de la clase de almacenamiento solicitada pueden afectar el proceso de decisión de aprovisionamiento de Trident al crear un PVC.

Modo de acceso

Al solicitar almacenamiento a través de un PVC, uno de los campos obligatorios es el modo de acceso. El modo deseado puede afectar al backend seleccionado para alojar la solicitud de almacenamiento.

Trident intentará hacer coincidir el protocolo de almacenamiento utilizado con el método de acceso especificado según la siguiente matriz. Esto es independiente de la plataforma de almacenamiento subyacente.

	Leer y escribir una vez	Solo lecturaMuchos	LeerEscribirMuchos
iSCSI	Sí	Sí	Sí (Bloque sin procesar)
Sistema Nacional de Archivos	Sí	Sí	Sí

Una solicitud de PVC ReadWriteMany enviada a una implementación de Trident sin un backend NFS configurado dará como resultado que no se aprovisione ningún volumen. Por este motivo, el solicitante deberá utilizar el modo de acceso adecuado para su aplicación.

Operaciones de volumen

Modificar volúmenes persistentes

Los volúmenes persistentes son, con dos excepciones, objetos inmutables en Kubernetes. Una vez creada, la política de reclamaciones y su tamaño pueden modificarse. Sin embargo, esto no impide que algunos aspectos del volumen se modifiquen fuera de Kubernetes. Esto puede ser conveniente para personalizar el volumen para aplicaciones específicas, para garantizar que la capacidad no se consuma accidentalmente o simplemente para mover el volumen a un controlador de almacenamiento diferente por cualquier motivo.

> Actualmente, los provisionadores integrados de Kubernetes no admiten operaciones de cambio de tamaño de volumen para PV NFS, iSCSI o FC. Trident admite la expansión de volúmenes NFS, iSCSI y FC.

Los detalles de conexión del PV no se pueden modificar después de su creación.

Crear instantáneas de volumen bajo demanda

Trident admite la creación de instantáneas de volumen bajo demanda y la creación de PVC a partir de instantáneas utilizando el marco CSI. Las instantáneas proporcionan un método conveniente para mantener copias puntuales de los datos y tienen un ciclo de vida independiente del PV de origen en Kubernetes. Estas instantáneas se pueden utilizar para clonar PVC.

Crear volúmenes a partir de instantáneas

Trident también admite la creación de PersistentVolumes a partir de instantáneas de volumen. Para lograr esto, simplemente cree un PersistentVolumeClaim y mencione el `datasource` como la instantánea requerida a partir de la cual se debe crear el volumen. Trident gestionará este PVC creando un volumen con los datos presentes en la instantánea. Con esta función, es posible duplicar datos entre regiones, crear entornos de

prueba, reemplazar un volumen de producción dañado o corrupto en su totalidad, o recuperar archivos y directorios específicos y transferirlos a otro volumen conectado.

Mover volúmenes en el clúster

Los administradores de almacenamiento tienen la capacidad de mover volúmenes entre agregados y controladores en el clúster ONTAP sin interrumpir el funcionamiento del consumidor de almacenamiento. Esta operación no afecta a Trident ni al clúster de Kubernetes, siempre y cuando el agregado de destino sea uno al que tenga acceso la SVM que utiliza Trident . Es importante destacar que, si el agregado se ha añadido recientemente al SVM, será necesario actualizar el backend volviéndolo a añadir a Trident. Esto hará que Trident reinvente la SVM para que se reconozca el nuevo agregado.

Sin embargo, Trident no admite automáticamente el traslado de volúmenes entre backends. Esto incluye transferencias entre SVM en el mismo clúster, entre clústeres o a una plataforma de almacenamiento diferente (incluso si ese sistema de almacenamiento está conectado a Trident).

Si se copia un volumen a otra ubicación, se puede utilizar la función de importación de volúmenes para importar los volúmenes actuales a Trident.

Ampliar volúmenes

Trident admite el cambio de tamaño de los volúmenes persistentes (PV) NFS, iSCSI y FC. Esto permite a los usuarios cambiar el tamaño de sus volúmenes directamente a través de la capa de Kubernetes. La expansión de volumen es posible para todas las principales plataformas de almacenamiento de NetApp , incluidos los backends de ONTAP, SolidFire/ NetApp HCI y Cloud Volumes Service . Para permitir una posible expansión posterior, establezca `allowVolumeExpansion` a `true` en su StorageClass asociada con el volumen. Siempre que sea necesario cambiar el tamaño del volumen persistente, edite el `spec.resources.requests.storage` anotación en la reclamación de volumen persistente al tamaño de volumen requerido. Trident se encargará automáticamente de redimensionar el volumen en el clúster de almacenamiento.

Importar un volumen existente a Kubernetes

La importación de volúmenes ofrece la posibilidad de importar un volumen de almacenamiento existente a un entorno Kubernetes. Actualmente, esto cuenta con el apoyo de `ontap-nas` , `ontap-nas-flexgroup` , `solidfire-san` , `azure-netapp-files` , y `gcp-cvs` conductores. Esta función resulta útil al migrar una aplicación existente a Kubernetes o durante escenarios de recuperación ante desastres.

Al utilizar ONTAP y `solidfire-san` Conductores, utilicen el comando `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` Importar un volumen existente a Kubernetes para que sea administrado por Trident. El archivo PVC YAML o JSON utilizado en el comando de importación de volumen apunta a una clase de almacenamiento que identifica a Trident como el proveedor. Cuando utilice un backend NetApp HCI/ SolidFire , asegúrese de que los nombres de los volúmenes sean únicos. Si los nombres de los volúmenes están duplicados, clone el volumen con un nombre único para que la función de importación de volúmenes pueda distinguirlos.

Si el `azure-netapp-files` o `gcp-cvs` Se utiliza el controlador, utilice el comando `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` para importar el volumen a Kubernetes para que sea administrado por Trident. Esto garantiza una referencia de volumen única.

Cuando se ejecute el comando anterior, Trident encontrará el volumen en el servidor y leerá su tamaño. Añadirá automáticamente (y sobrescribirá si es necesario) el tamaño de volumen configurado del PVC. Luego, Trident crea el nuevo PV y Kubernetes vincula el PVC al PV.

Si un contenedor se desplegara de forma que requiriera el PVC importado específico, permanecería en estado

pendiente hasta que el par PVC/PV se vinculara mediante el proceso de importación de volumen. Una vez unidos los pares PVC/PV, el contenedor debería subir, siempre que no haya otros problemas.

Servicio de registro

La implementación y la gestión del almacenamiento para el registro se han documentado en"netapp.io" en el"blog" .

Servicio de registro

Al igual que otros servicios de OpenShift, el servicio de registro se implementa utilizando Ansible con parámetros de configuración proporcionados por el archivo de inventario, también conocido como hosts, que se proporciona al playbook. Se abordarán dos métodos de instalación: la implementación del registro durante la instalación inicial de OpenShift y la implementación del registro después de que se haya instalado OpenShift.

A partir de la versión 3.9 de Red Hat OpenShift, la documentación oficial desaconseja el uso de NFS para el servicio de registro debido a la preocupación por la corrupción de datos. Esto se basa en las pruebas realizadas por Red Hat a sus productos. El servidor NFS de ONTAP no presenta estos problemas y puede respaldar fácilmente una implementación de registro. En última instancia, la elección del protocolo para el servicio de registro depende de usted; tenga en cuenta que ambos funcionarán perfectamente al usar plataformas NetApp y no hay razón para evitar NFS si esa es su preferencia.

Si elige usar NFS con el servicio de registro, deberá configurar la variable de Ansible. `openshift_enable_unsupported_configurations` a `true` para evitar que falle el instalador.

Empezar

El servicio de registro puede, opcionalmente, implementarse tanto para las aplicaciones como para las operaciones centrales del propio clúster de OpenShift. Si elige implementar el registro de operaciones, especifique la variable `openshift_logging_use_ops` como `true` Se crearán dos instancias del servicio. Las variables que controlan la instancia de registro para operaciones contienen "ops" en ellas, mientras que la instancia para aplicaciones no.

Configurar las variables de Ansible según el método de despliegue es importante para garantizar que los servicios subyacentes utilicen el almacenamiento correcto. Analicemos las opciones para cada uno de los métodos de implementación.

Las tablas que aparecen a continuación contienen únicamente las variables relevantes para la configuración del almacenamiento en lo que respecta al servicio de registro. Puedes encontrar otras opciones en"Documentación de registro de Red Hat OpenShift" que deberá revisarse, configurarse y utilizarse de acuerdo con su implementación.

Las variables de la tabla siguiente harán que el playbook de Ansible cree un PV y un PVC para el servicio de registro utilizando los detalles proporcionados. Este método es significativamente menos flexible que usar el playbook de instalación de componentes después de la instalación de OpenShift; sin embargo, si dispone de volúmenes existentes, es una opción.

Variable	Detalles
`openshift_logging_storage_kind`	Empezar a `nfs` para que el instalador cree un PV NFS para el servicio de registro.

Variable	Detalles
`openshift_logging_storage_host`	El nombre de host o la dirección IP del host NFS. Esto debe configurarse con el dataLIF de su máquina virtual.
`openshift_logging_storage_nfs_directory`	La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen está unido como `/openshift_logging` , usarías esa ruta para esta variable.
`openshift_logging_storage_volume_name`	El nombre, por ejemplo `pv_ose_logs` , del PV para crear.
`openshift_logging_storage_volume_size`	El tamaño de la exportación NFS, por ejemplo `100Gi` .

Si su clúster de OpenShift ya está en funcionamiento y, por lo tanto, Trident se ha implementado y configurado, el instalador puede utilizar el aprovisionamiento dinámico para crear los volúmenes. Será necesario configurar las siguientes variables.

Variable	Detalles
`openshift_logging_es_pvc_dynamic`	Establézcalo en verdadero para usar volúmenes aprovisionados dinámicamente.
`openshift_logging_es_pvc_storage_class_name`	El nombre de la clase de almacenamiento que se utilizará en el PVC.
`openshift_logging_es_pvc_size`	El tamaño del volumen solicitado en el PVC.
`openshift_logging_es_pvc_prefix`	Un prefijo para los PVC utilizados por el servicio de registro.
`openshift_logging_es_ops_pvc_dynamic`	Empezar a `true` utilizar volúmenes aprovisionados dinámicamente para la instancia de registro de operaciones.
`openshift_logging_es_ops_pvc_storage_class_name`	El nombre de la clase de almacenamiento para la instancia de registro de operaciones.
`openshift_logging_es_ops_pvc_size`	El tamaño de la solicitud de volumen para la instancia de operaciones.
`openshift_logging_es_ops_pvc_prefix`	Un prefijo para los PVC de la instancia ops.

Implementar la pila de registro

Si va a implementar el registro como parte del proceso de instalación inicial de OpenShift, solo necesita seguir el proceso de implementación estándar. Ansible configurará e implementará los servicios y objetos de OpenShift necesarios para que el servicio esté disponible tan pronto como Ansible finalice.

Sin embargo, si realiza la implementación después de la instalación inicial, Ansible deberá utilizar el playbook del componente. Este proceso puede variar ligeramente con diferentes versiones de OpenShift, así que asegúrese de leer y seguir las instrucciones."Documentación de Red Hat OpenShift Container Platform 3.11" para tu versión.

Servicio de métricas

El servicio de métricas proporciona información valiosa al administrador sobre el estado, la utilización de recursos y la disponibilidad del clúster de OpenShift. También es necesario para la funcionalidad de escalado automático de pods y muchas organizaciones utilizan datos del servicio de métricas para sus aplicaciones de facturación interna y/o de visualización de datos.

Al igual que con el servicio de registro y con OpenShift en su conjunto, Ansible se utiliza para implementar el servicio de métricas. Asimismo, al igual que el servicio de registro, el servicio de métricas se puede implementar durante la configuración inicial del clúster o después de que esté operativo utilizando el método de instalación de componentes. Las siguientes tablas contienen las variables importantes a la hora de configurar el almacenamiento persistente para el servicio de métricas.

Las tablas que aparecen a continuación solo contienen las variables relevantes para la configuración del almacenamiento en lo que respecta al servicio de métricas. En la documentación se incluyen muchas otras opciones que deben revisarse, configurarse y utilizarse de acuerdo con su implementación.

Variable	Detalles
`openshift_metrics_storage_kind`	Empezar a `nfs` para que el instalador cree un PV NFS para el servicio de registro.
`openshift_metrics_storage_host`	El nombre de host o la dirección IP del host NFS. Esto debe configurarse con el dataLIF de su SVM.
`openshift_metrics_storage_nfs_directory`	La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen está unido como `/openshift_metrics` , usarías esa ruta para esta variable.
`openshift_metrics_storage_volume_name`	El nombre, por ejemplo `pv_ose_metrics` , del PV para crear.
`openshift_metrics_storage_volume_size`	El tamaño de la exportación NFS, por ejemplo `100Gi` .

Si su clúster de OpenShift ya está en funcionamiento y, por lo tanto, Trident se ha implementado y configurado, el instalador puede utilizar el aprovisionamiento dinámico para crear los volúmenes. Será necesario configurar las siguientes variables.

Variable	Detalles
`openshift_metrics_cassandra_pvc_prefix`	Un prefijo para usar en los PVC métricos.
`openshift_metrics_cassandra_pvc_size`	El tamaño de los volúmenes a solicitar.
`openshift_metrics_cassandra_storage_type`	El tipo de almacenamiento que se utilizará para las métricas debe configurarse como dinámico para que Ansible cree PVC con la clase de almacenamiento adecuada.
`openshift_metrics_cassanda_pvc_storage_class_name`	El nombre de la clase de almacenamiento que se va a utilizar.

Implementar el servicio de métricas

Con las variables de Ansible apropiadas definidas en su archivo hosts/inventory, implemente el servicio utilizando Ansible. Si realiza la implementación durante la instalación de OpenShift, el PV se creará y utilizará automáticamente. Si realiza la implementación utilizando los playbooks de componentes, después de la instalación de OpenShift, Ansible crea los PVC necesarios y, después de que Trident haya aprovisionado el almacenamiento para ellos, implementa el servicio.

Las variables anteriores, así como el proceso de implementación, pueden cambiar con cada versión de OpenShift. Asegúrese de revisar y seguir"Guía de implementación de OpenShift de Red Hat" para su versión, de modo que esté configurada para su entorno.

Protección de datos y recuperación ante desastres

Obtenga información sobre las opciones de protección y recuperación para Trident y los volúmenes creados con Trident. Debe contar con una estrategia de protección y recuperación de datos para cada aplicación con requisitos de persistencia.

replicación y recuperación de Trident

Puedes crear una copia de seguridad para restaurar Trident en caso de desastre.

replicación de Trident

Trident utiliza CRD de Kubernetes para almacenar y gestionar su propio estado y el etcd del clúster de Kubernetes para almacenar sus metadatos.

Pasos

1. Realice una copia de seguridad del clúster de Kubernetes etcd utilizando"Kubernetes: Copia de seguridad de un clúster etcd" .
2. Coloque los artefactos de copia de seguridad en un FlexVol volume.

> NetApp recomienda proteger la SVM donde reside el FlexVol con una relación SnapMirror a otra SVM.

Recuperación de Trident

Utilizando CRD de Kubernetes y la instantánea etcd del clúster de Kubernetes, puede recuperar Trident.

Pasos

1. Desde la SVM de destino, monte el volumen que contiene los archivos de datos y certificados etcd de Kubernetes en el host que se configurará como nodo maestro.
2. Copie todos los certificados necesarios relacionados con el clúster de Kubernetes en `/etc/kubernetes/pki` y los archivos miembros de etcd bajo `/var/lib/etcd` .
3. Restaure el clúster de Kubernetes desde la copia de seguridad de etcd usando"Kubernetes: Restauración de un clúster etcd" .
4. Correr `kubectl get crd` para verificar que todos los recursos personalizados de Trident se hayan cargado y recuperar los objetos de Trident para verificar que todos los datos estén disponibles.

replicación y recuperación de SVM

Trident no puede configurar relaciones de replicación; sin embargo, el administrador de almacenamiento puede usar "ONTAP SnapMirror" para replicar una SVM.

En caso de desastre, puede activar el SVM de destino SnapMirror para comenzar a servir datos. Podrás volver a la configuración principal cuando se restablezcan los sistemas.

Acerca de esta tarea

Tenga en cuenta lo siguiente al utilizar la función de replicación SVM de SnapMirror :

- Debes crear un backend distinto para cada SVM con SVM-DR habilitado.
- Configure las clases de almacenamiento para seleccionar los backends replicados solo cuando sea necesario para evitar que se aprovisionen volúmenes que no necesitan replicación en los backends que admiten SVM-DR.
- Los administradores de aplicaciones deben comprender el coste y la complejidad adicionales asociados a la replicación y considerar cuidadosamente su plan de recuperación antes de iniciar este proceso.

replicación de SVM

Puedes utilizar"ONTAP: Replicación SVM de SnapMirror" para crear la relación de replicación SVM.

SnapMirror te permite configurar opciones para controlar qué replicar. Necesitarás saber qué opciones seleccionaste al realizar la operación.Recuperación de SVM usando Trident .

- "-identity-preserve true"Replica toda la configuración SVM.
- "-descartar-configuraciones de red"Excluye las LIF y la configuración de red relacionada.
- "-identity-preserve falso"Solo replica los volúmenes y la configuración de seguridad.

Recuperación de SVM usando Trident

Trident no detecta automáticamente los fallos de SVM. En caso de desastre, el administrador puede iniciar manualmente la conmutación por error de Trident al nuevo SVM.

Pasos

1. Cancele las transferencias SnapMirror programadas y en curso, rompa la relación de replicación, detenga la SVM de origen y, a continuación, active la SVM de destino SnapMirror .
2. Si usted especificó `-identity-preserve false` o `-discard-config network` Al configurar la replicación de SVM, actualice `managementLIF` y `dataLIF` en el archivo de definición del backend de Trident .
3. Confirmar `storagePrefix` está presente en el archivo de definición del backend de Trident . Este parámetro no se puede cambiar. Omitiendo `storagePrefix` provocará un fallo en la actualización del backend.
4. Actualice todos los backends necesarios para reflejar el nuevo nombre de SVM de destino utilizando:

   ```
   ./tridentctl update backend <backend-name> -f <backend-json-file> -n
   <namespace>
   ```

5. Si usted especificó `-identity-preserve false` o `discard-config network` , debes reiniciar todos

los pods de la aplicación.

> Si usted especificó `-identity-preserve true` Todos los volúmenes aprovisionados por Trident comienzan a proporcionar datos cuando se activa la SVM de destino.

replicación y recuperación de volumen

Trident no puede configurar las relaciones de replicación de SnapMirror ; sin embargo, el administrador de almacenamiento puede usar"replicación y recuperación de ONTAP SnapMirror" para replicar volúmenes creados por Trident.

Luego puede importar los volúmenes recuperados a Trident mediante"importación de volumen de tridentctl" .

> La importación no es compatible con `ontap-nas-economy` , `ontap-san-economy` , o `ontap-flexgroup-economy` conductores.

Protección de datos de instantáneas

Puedes proteger y restaurar datos usando:

- Un controlador de instantáneas externo y CRD para crear instantáneas de volúmenes de Kubernetes de volúmenes persistentes (PV).

  "Instantáneas de volumen"

- Instantáneas de ONTAP para restaurar todo el contenido de un volumen o para recuperar archivos o LUN individuales.

  "Instantáneas de ONTAP"

Seguridad

Seguridad

Siga las recomendaciones que se enumeran aquí para garantizar la seguridad de su instalación de Trident .

Ejecutar Trident en su propio espacio de nombres.

Es importante impedir que las aplicaciones, los administradores de aplicaciones, los usuarios y las aplicaciones de gestión accedan a las definiciones de objetos de Trident o a los pods para garantizar un almacenamiento fiable y bloquear posibles actividades maliciosas.

Para separar las demás aplicaciones y usuarios de Trident, instale siempre Trident en su propio espacio de nombres de Kubernetes.(`trident`). Al colocar Trident en su propio espacio de nombres, se garantiza que solo el personal administrativo de Kubernetes tenga acceso al pod de Trident y a los artefactos (como los secretos de backend y CHAP, si corresponde) almacenados en los objetos CRD con espacio de nombres. Debe asegurarse de permitir únicamente a los administradores el acceso al espacio de nombres de Trident y, por lo tanto, el acceso a `tridentctl` solicitud.

Utilice la autenticación CHAP con los backends SAN de ONTAP.

Trident admite la autenticación basada en CHAP para cargas de trabajo SAN de ONTAP (utilizando el `ontap-san` y `ontap-san-economy` conductores). NetApp recomienda utilizar CHAP bidireccional con Trident para la autenticación entre un host y el backend de almacenamiento.

Para los backends ONTAP que utilizan los controladores de almacenamiento SAN, Trident puede configurar CHAP bidireccional y administrar los nombres de usuario y secretos de CHAP a través de `tridentctl` . Referirse a"Prepárese para configurar el backend con los controladores SAN de ONTAP." Para comprender cómo Trident configura CHAP en los sistemas backend de ONTAP .

Utilice la autenticación CHAP con los sistemas backend NetApp HCI y SolidFire.

NetApp recomienda implementar CHAP bidireccional para garantizar la autenticación entre un host y los backends de NetApp HCI y SolidFire . Trident utiliza un objeto secreto que incluye dos contraseñas CHAP por inquilino. Cuando se instala Trident , gestiona los secretos CHAP y los almacena en un `tridentvolume` Objeto CR para el PV correspondiente. Cuando se crea un PV, Trident utiliza los secretos CHAP para iniciar una sesión iSCSI y comunicarse con el sistema NetApp HCI y SolidFire a través de CHAP.

Los volúmenes creados por Trident no están asociados a ningún grupo de acceso a volúmenes.

Utilice Trident con NVE y NAE

NetApp ONTAP proporciona cifrado de datos en reposo para proteger los datos confidenciales en caso de que un disco sea robado, devuelto o reutilizado. Para más detalles, consulte"Descripción general de la configuración de NetApp Volume Encryption" .

- Si NAE está habilitado en el backend, cualquier volumen aprovisionado en Trident estará habilitado para NAE.
  - Puedes configurar la bandera de cifrado NVE a `""` para crear volúmenes compatibles con NAE.
- Si NAE no está habilitado en el backend, cualquier volumen aprovisionado en Trident tendrá NVE habilitado a menos que la bandera de cifrado NVE esté configurada en `false` (el valor predeterminado) en la configuración del backend.

Los volúmenes creados en Trident en un backend habilitado para NAE deben estar cifrados con NVE o NAE.

- Puedes configurar la bandera de cifrado NVE a `true` en la configuración del backend de Trident para anular el cifrado NAE y usar una clave de cifrado específica por volumen.
- Configurar la bandera de cifrado NVE a `false` En un backend habilitado para NAE se crea un volumen habilitado para NAE. No se puede deshabilitar el cifrado NAE configurando la bandera de cifrado NVE en `false` .

- Puede crear manualmente un volumen NVE en Trident configurando explícitamente la bandera de cifrado NVE a `true` .

Para obtener más información sobre las opciones de configuración del backend, consulte:

- "Opciones de configuración SAN de ONTAP"
- "Opciones de configuración de ONTAP NAS"

Configuración de clave unificada de Linux (LUKS)

Puede habilitar Linux Unified Key Setup (LUKS) para cifrar los volúmenes ONTAP SAN y ONTAP SAN ECONOMY en Trident. Trident admite la rotación de contraseñas y la expansión de volumen para volúmenes cifrados con LUKS.

En Trident, los volúmenes cifrados con LUKS utilizan el cifrado y el modo aes-xts-plain64, tal como recomienda"NIST" .

> El cifrado LUKS no es compatible con los sistemas ASA r2. Para obtener información sobre los sistemas ASA r2, consulte"Conozca los sistemas de almacenamiento ASA r2" .

Antes de empezar

- Los nodos de trabajo deben tener instalado cryptsetup 2.1 o superior (pero inferior a 3.0). Para obtener más información, visite"Gitlab: configuración de criptografía" .
- Por motivos de rendimiento, NetApp recomienda que los nodos de trabajo sean compatibles con las nuevas instrucciones del estándar de cifrado avanzado (AES-NI). Para verificar la compatibilidad con AES-NI, ejecute el siguiente comando:

  ```
  grep "aes" /proc/cpuinfo
  ```

  Si no se devuelve nada, su procesador no admite AES-NI. Para obtener más información sobre AES-NI, visite:"Intel: Instrucciones del estándar de cifrado avanzado (AES-NI)" .

Habilitar el cifrado LUKS

Puede habilitar el cifrado por volumen en el host mediante Linux Unified Key Setup (LUKS) para volúmenes ONTAP SAN y ONTAP SAN ECONOMY.

Pasos

1. Define los atributos de cifrado LUKS en la configuración del backend. Para obtener más información sobre las opciones de configuración de backend para ONTAP SAN, consulte"Opciones de configuración SAN de ONTAP" .

```
{
  "storage": [
    {
      "labels": {
        "luks": "true"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "true"
      }
    },
    {
      "labels": {
        "luks": "false"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "false"
      }
    }
  ]
}
```

2. Usar `parameters.selector` para definir los grupos de almacenamiento utilizando el cifrado LUKS. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. Crea un secreto que contenga la contraseña LUKS. Por ejemplo:

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

Limitaciones

Los volúmenes cifrados con LUKS no pueden aprovechar la deduplicación y compresión de ONTAP .

Configuración del backend para importar volúmenes LUKS

Para importar un volumen LUKS, debe configurar `luksEncryption` a(`true` en el backend. El `luksEncryption` Esta opción le indica a Trident si el volumen es compatible con LUKS.(`true`) o no cumple con LUKS(`false`) como se muestra en el siguiente ejemplo.

```
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

Configuración de PVC para importar volúmenes LUKS

Para importar volúmenes LUKS de forma dinámica, configure la anotación `trident.netapp.io/luksEncryption` a `true` e incluir una clase de almacenamiento habilitada para LUKS en el PVC como se muestra en este ejemplo.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: luks-sc
```

Rotar una frase de contraseña LUKS

Puedes cambiar la contraseña LUKS y confirmar el cambio.

> No olvide una frase de contraseña hasta que haya verificado que ya no está siendo referenciada por ningún volumen, instantánea o secreto. Si se pierde la contraseña a la que se hace referencia, es posible que no pueda montar el volumen y los datos permanecerán cifrados e inaccesibles.

Acerca de esta tarea

La rotación de la contraseña LUKS se produce cuando se crea un pod que monta el volumen después de que se haya especificado una nueva contraseña LUKS. Cuando se crea un nuevo pod, Trident compara la contraseña LUKS del volumen con la contraseña activa del secreto.

- Si la contraseña del volumen no coincide con la contraseña activa del secreto, se produce una rotación.
- Si la contraseña del volumen coincide con la contraseña activa del secreto, `previous-luks-passphrase` El parámetro se ignora.

Pasos

1. Añade el `node-publish-secret-name` y `node-publish-secret-namespace` Parámetros de StorageClass. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identificar las contraseñas existentes en el volumen o instantánea.

Volumen

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["A"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["A"]
```

3. Actualice la clave secreta LUKS del volumen para especificar las contraseñas nueva y anterior. Asegurar `previous-luke-passphrase-name` y `previous-luks-passphrase` Coincide con la contraseña anterior.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Crea un nuevo pod para montar el volumen. Esto es necesario para iniciar la rotación.
5. Verifique que la contraseña se haya rotado.

Volumen

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["B"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["B"]
```

Resultados

La contraseña se rotó cuando solo se devolvió la nueva contraseña en el volumen y la instantánea.

> Si se devuelven dos frases de contraseña, por ejemplo `luksPassphraseNames: ["B", "A"]` , la rotación está incompleta. Puedes activar una nueva cápsula para intentar completar la rotación.

Habilitar la expansión de volumen

Puede habilitar la expansión de volumen en un volumen cifrado con LUKS.

Pasos

1. Habilitar el `CSINodeExpandSecret` Puerta de características (beta 1.25+). Referirse a "Kubernetes 1.25: Uso de secretos para la expansión de volúmenes CSI basada en nodos" Para más detalles.
2. Añade el `node-expand-secret-name` y `node-expand-secret-namespace` Parámetros de StorageClass. Por ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

Resultados

Cuando se inicia la expansión del almacenamiento en línea, el kubelet pasa las credenciales apropiadas al controlador.

Cifrado en vuelo Kerberos

Mediante el cifrado en tránsito de Kerberos, puede mejorar la seguridad del acceso a los datos habilitando el cifrado para el tráfico entre su clúster administrado y el backend de almacenamiento.

Trident admite el cifrado Kerberos para ONTAP como backend de almacenamiento:

- * ONTAP local* - Trident admite el cifrado Kerberos a través de conexiones NFSv3 y NFSv4 desde Red Hat OpenShift y clústeres Kubernetes ascendentes a volúmenes ONTAP locales.

Puede crear, eliminar, cambiar el tamaño, crear instantáneas, clonar, clonar en modo de solo lectura e importar volúmenes que utilicen cifrado NFS.

Configurar el cifrado Kerberos en vuelo con volúmenes ONTAP locales

Puede habilitar el cifrado Kerberos en el tráfico de almacenamiento entre su clúster administrado y un backend de almacenamiento ONTAP local.

> El cifrado Kerberos para el tráfico NFS con backends de almacenamiento ONTAP locales solo es compatible mediante el uso de `ontap-nas` Controlador de almacenamiento.

Antes de empezar

- Asegúrese de tener acceso a `tridentctl` utilidad.
- Asegúrese de tener acceso de administrador al backend de almacenamiento de ONTAP .
- Asegúrese de conocer el nombre del volumen o volúmenes que compartirá desde el backend de almacenamiento de ONTAP .
- Asegúrese de haber preparado la máquina virtual de almacenamiento ONTAP para que admita el cifrado Kerberos para volúmenes NFS. Referirse a "Habilitar Kerberos en un dataLIF" para obtener instrucciones.
- Asegúrese de que todos los volúmenes NFSv4 que utilice con cifrado Kerberos estén configurados correctamente. Consulte la sección Configuración del dominio NFSv4 de NetApp (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4" .

Agregar o modificar las políticas de exportación de ONTAP

Debe agregar reglas a las políticas de exportación de ONTAP existentes o crear nuevas políticas de exportación que admitan el cifrado Kerberos para el volumen raíz de la máquina virtual de almacenamiento de ONTAP , así como para cualquier volumen de ONTAP compartido con el clúster de Kubernetes ascendente. Las reglas de política de exportación que agregue, o las nuevas políticas de exportación que cree, deben admitir los siguientes protocolos de acceso y permisos de acceso:

Protocolos de acceso

Configure la política de exportación con los protocolos de acceso NFS, NFSv3 y NFSv4.

Detalles de acceso

Puede configurar una de las tres versiones diferentes de cifrado Kerberos, según sus necesidades de volumen:

- **Kerberos 5** - (autenticación y cifrado)
- **Kerberos 5i** - (autenticación y cifrado con protección de identidad)
- **Kerberos 5p** - (autenticación y cifrado con protección de identidad y privacidad)

Configure la regla de política de exportación de ONTAP con los permisos de acceso adecuados. Por ejemplo, si los clústeres van a montar los volúmenes NFS con una combinación de cifrado Kerberos 5i y Kerberos 5p, utilice la siguiente configuración de acceso:

Tipo	Acceso de solo lectura	Acceso de lectura/escritura	acceso de superusuario
UNIX	Habilitado	Habilitado	Habilitado
Kerberos 5i	Habilitado	Habilitado	Habilitado
Kerberos 5p	Habilitado	Habilitado	Habilitado

Consulte la siguiente documentación para obtener información sobre cómo crear políticas de exportación de ONTAP y reglas de políticas de exportación:

- "Crear una política de exportación"
- "Agregar una regla a una política de exportación"

Crea un backend de almacenamiento

Puede crear una configuración de backend de almacenamiento Trident que incluya capacidad de cifrado Kerberos.

Acerca de esta tarea

Cuando crea un archivo de configuración de backend de almacenamiento que configura el cifrado Kerberos, puede especificar una de las tres versiones diferentes de cifrado Kerberos mediante el `spec.nfsMountOptions` parámetro:

- `spec.nfsMountOptions: sec=krb5`(autenticación y cifrado)
- `spec.nfsMountOptions: sec=krb5i`(autenticación y cifrado con protección de identidad)
- `spec.nfsMountOptions: sec=krb5p`(autenticación y cifrado con protección de identidad y privacidad)

Especifique solo un nivel de Kerberos. Si se especifica más de un nivel de cifrado Kerberos en la lista de parámetros, solo se utilizará la primera opción.

Pasos

1. En el clúster administrado, cree un archivo de configuración de backend de almacenamiento utilizando el siguiente ejemplo. Reemplace los valores entre corchetes <> con información de su entorno:

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilice el archivo de configuración que creó en el paso anterior para crear el backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Si falla la creación del backend, algo falla en la configuración del backend. Puedes consultar los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede volver a ejecutar el comando de creación.

Crear una clase de almacenamiento

Puede crear una clase de almacenamiento para aprovisionar volúmenes con cifrado Kerberos.

Acerca de esta tarea

Al crear un objeto de clase de almacenamiento, puede especificar una de las tres versiones diferentes de cifrado Kerberos mediante el `mountOptions` parámetro:

- `mountOptions: sec=krb5`(autenticación y cifrado)
- `mountOptions: sec=krb5i`(autenticación y cifrado con protección de identidad)
- `mountOptions: sec=krb5p`(autenticación y cifrado con protección de identidad y privacidad)

Especifique solo un nivel de Kerberos. Si se especifica más de un nivel de cifrado Kerberos en la lista de parámetros, solo se utilizará la primera opción. Si el nivel de cifrado que especificó en la configuración del backend de almacenamiento es diferente del nivel que especificó en el objeto de clase de almacenamiento, el objeto de clase de almacenamiento tiene prioridad.

Pasos

1. Crea un objeto StorageClass de Kubernetes, utilizando el siguiente ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions:
  - sec=krb5i #can be krb5, krb5i, or krb5p
parameters:
  backendType: ontap-nas
  storagePools: ontapnas_pool
  trident.netapp.io/nasType: nfs
allowVolumeExpansion: true
```

2. Crea la clase de almacenamiento:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Asegúrese de que se haya creado la clase de almacenamiento:

```
kubectl get sc ontap-nas-sc
```

   Debería ver un resultado similar al siguiente:

```
NAME          PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

volúmenes de provisiones

Después de crear un backend de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar un volumen. Para obtener instrucciones, consulte "Provisión de un volumen" .

Configurar el cifrado Kerberos en vuelo con volúmenes de Azure NetApp Files

Puede habilitar el cifrado Kerberos en el tráfico de almacenamiento entre su clúster administrado y un único backend de almacenamiento de Azure NetApp Files o un grupo virtual de backends de almacenamiento de Azure NetApp Files .

Antes de empezar

- Asegúrese de haber habilitado Trident en el clúster Red Hat OpenShift administrado.
- Asegúrese de tener acceso a `tridentctl` utilidad.
- Asegúrese de haber preparado el backend de almacenamiento de Azure NetApp Files para el cifrado Kerberos teniendo en cuenta los requisitos y siguiendo las instrucciones en "Documentación de Azure NetApp Files" .
- Asegúrese de que todos los volúmenes NFSv4 que utilice con cifrado Kerberos estén configurados correctamente. Consulte la sección Configuración del dominio NFSv4 de NetApp (página 13) del "Guía de mejoras y prácticas recomendadas de NetApp NFSv4" .

Crea un backend de almacenamiento

Puede crear una configuración de backend de almacenamiento de Azure NetApp Files que incluya la capacidad de cifrado Kerberos.

Acerca de esta tarea

Cuando crea un archivo de configuración de backend de almacenamiento que configura el cifrado Kerberos, puede definirlo para que se aplique en uno de dos niveles posibles:

- El **nivel de backend de almacenamiento** que utiliza el `spec.kerberos` campo
- El **nivel de piscina virtual** que utiliza el `spec.storage.kerberos` campo

Cuando se define la configuración a nivel de grupo virtual, el grupo se selecciona utilizando la etiqueta en la clase de almacenamiento.

En cualquiera de los dos niveles, puede especificar una de las tres versiones diferentes de cifrado Kerberos:

- `kerberos: sec=krb5`(autenticación y cifrado)
- `kerberos: sec=krb5i`(autenticación y cifrado con protección de identidad)
- `kerberos: sec=krb5p`(autenticación y cifrado con protección de identidad y privacidad)

Pasos

1. En el clúster administrado, cree un archivo de configuración de backend de almacenamiento utilizando uno de los siguientes ejemplos, según dónde necesite definir el backend de almacenamiento (nivel de backend de almacenamiento o nivel de grupo virtual). Reemplace los valores entre corchetes <> con información de su entorno:

Ejemplo de nivel de backend de almacenamiento

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

Ejemplo de nivel de piscina virtual

```
---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

2. Utilice el archivo de configuración que creó en el paso anterior para crear el backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Si falla la creación del backend, algo falla en la configuración del backend. Puedes consultar los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede volver a ejecutar el comando de creación.

Crear una clase de almacenamiento

Puede crear una clase de almacenamiento para aprovisionar volúmenes con cifrado Kerberos.

Pasos

1. Crea un objeto StorageClass de Kubernetes, utilizando el siguiente ejemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: azure-netapp-files
  trident.netapp.io/nasType: nfs
  selector: type=encryption
```

2. Crea la clase de almacenamiento:

```
kubectl create -f sample-input/storage-class-sc-nfs.yaml
```

3. Asegúrese de que se haya creado la clase de almacenamiento:

```
kubectl get sc -sc-nfs
```

Debería ver un resultado similar al siguiente:

```
NAME          PROVISIONER             AGE
sc-nfs        csi.trident.netapp.io   15h
```

volúmenes de provisiones

Después de crear un backend de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar un volumen. Para obtener instrucciones, consulte "Provisión de un volumen" .