Prácticas recomendadas y recomendaciones

Trident

NetApp
September 26, 2025

Tabla de contenidos

Prácticas recomendadas y recomendaciones

Puesta en marcha

Utilice las recomendaciones que se enumeran aquí al implementar Trident.

Póngalo en marcha a un espacio de nombres dedicado

"Espacios de nombres" proporcionar separación administrativa entre diferentes aplicaciones y constituyen una barrera para el uso compartido de recursos. Por ejemplo, una RVP de un espacio de nombres no se puede consumir de otro. Trident proporciona recursos PV a todos los espacios de nombres del clúster de Kubernetes y, en consecuencia, aprovecha una cuenta de servicio que ha elevado el número de Privileges.

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

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

Kubernetes cuenta con dos funciones que, al combinarse, ofrecen un potente mecanismo que limita el consumo de recursos que consumen las aplicaciones. "mecanismo de cuotas de almacenamiento"Permite al administrador implementar límites de consumo globales y específicos de clase de almacenamiento, de capacidad y de recuento de objetos por espacio de nombres. Además, el uso de un "límite de rango" garantiza que las solicitudes RVP se encuentren dentro de un valor mínimo y máximo antes de que la solicitud se reenvíe al aprovisionador.

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

Configuración del almacenamiento

Cada plataforma de almacenamiento de la cartera de NetApp tiene unas funciones únicas que benefician a las aplicaciones, en contenedores 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, las necesidades de la aplicación y el equipo que administra el dispositivo deben tenerse en cuenta al elegir una plataforma.

Debe seguir las prácticas recomendadas de base para el sistema operativo del host con el protocolo que está aprovechando. Opcionalmente, es posible que desee considerar la incorporación de prácticas recomendadas para las aplicaciones, cuando esté disponible, con configuración de back-end, clase de almacenamiento y RVP para optimizar el almacenamiento para aplicaciones específicas.

Prácticas recomendadas para ONTAP y Cloud Volumes ONTAP

Conozca las prácticas recomendadas para configurar ONTAP y Cloud Volumes ONTAP para Trident.

Las siguientes recomendaciones son directrices para configurar ONTAP para cargas de trabajo en contenedores, que consumen volúmenes aprovisionados de forma dinámica por Trident. Cada uno de ellos debe considerarse y evaluarse según la idoneidad de su entorno.

Utilice SVM dedicadas a Trident

Las máquinas virtuales de almacenamiento (SVM) proporcionan separación de tareas administrativas y de aislamiento entre clientes en un sistema ONTAP. Dedicar una SVM a las aplicaciones permite delegar privilegios y aplicar prácticas recomendadas para limitar el consumo de recursos.

Existen varias opciones disponibles para la gestión de la SVM:

- Proporcione la interfaz de gestión del clúster en la configuración del back-end, junto con las credenciales adecuadas, y especifique el nombre de la SVM.
- Cree una interfaz de gestión dedicada para la SVM mediante ONTAP System Manager o la CLI.
- Comparta la función de gestión con una interfaz de datos NFS.

En cada caso, la interfaz debe estar en DNS, y se debe usar el nombre DNS al configurar Trident. Esto permite facilitar algunas situaciones de recuperación ante desastres, por ejemplo, SVM-DR sin retención de identidad de red.

No tiene ninguna preferencia entre tener una LIF de gestión dedicada o compartida para la SVM, sin embargo, debe asegurarse de que las políticas de seguridad de red se alineen con el enfoque que elija. Independientemente, el LIF de gestión debería ser accesible mediante DNS, lo que para facilitar la máxima flexibilidad debería "SVM-DR" ser usado en combinación con Trident.

Limite el número máximo de volúmenes

Los sistemas de almacenamiento de ONTAP tienen un número máximo de volúmenes, que varía en función de la versión del software y la plataforma de hardware. Consulte "NetApp Hardware Universe" para conocer su plataforma específica y la 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.

Los controladores y `ontap-san` Trident `ontap-nas` aprovisionan un FlexVolume para cada volumen persistente (VP) de Kubernetes que se crea. `ontap-nas-economy`El controlador crea aproximadamente un FlexVolume por cada 200 VP (configurable entre 50 y 300). `ontap-san-economy`El controlador crea aproximadamente un FlexVolume por cada 100 VP (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. Puede hacerlo desde la línea de comandos:

```
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:

- El número de volúmenes existentes en el clúster de ONTAP
- El número de volúmenes que espera aprovisionar fuera de Trident para otras aplicaciones
- El número de volúmenes persistentes que tienen previsto consumir las aplicaciones de Kubernetes

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

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

Por ejemplo, un clúster ONTAP de dos nodos tiene la capacidad de alojar un máximo de 2000 FlexVolumes. Tener el recuento de volumen máximo establecido en 1250 parece muy razonable. Sin embargo, si solo "agregados" de un nodo se asigna a la SVM o los agregados asignados desde un nodo no se pueden aprovisionar con respecto (por ejemplo, debido a la capacidad), el otro nodo se convierte en el destino para todos los volúmenes aprovisionados de Trident. Esto significa que se puede alcanzar el límite de volumen para ese nodo antes de `max-volumes` alcanzar el valor, lo que afecta tanto al Trident como a otras operaciones de volumen que usan ese nodo. **Puede evitar esta situación asegurándose de que los agregados de cada nodo del clúster están asignados a la SVM que utiliza Trident en los mismos números.**

Limite el tamaño máximo de los volúmenes que ha creado Trident

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

Además de controlar el tamaño del volumen en la cabina de almacenamiento, también se deben aprovechar las capacidades de Kubernetes.

Limite el tamaño máximo de FlexVols creados por Trident

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

Configure Trident para utilizar CHAP bidireccional

Puede especificar los nombres de iniciador CHAP y de usuario de destino y las contraseñas en la definición de back-end, y hacer que Trident habilite CHAP en la SVM. Cuando se usa `useCHAP` el parámetro en la configuración de back-end, Trident autentica las conexiones iSCSI para back-ends de ONTAP con CHAP.

Cree y utilice una política de calidad de servicio de SVM

Al aprovechar una política de calidad de servicio de ONTAP, aplicada a la SVM, se limita el número de IOPS consumibles por los volúmenes aprovisionados de Trident. Esto ayuda a "prevenir un matón" que el contenedor esté fuera de control o que pueda afectar a las cargas de trabajo fuera de la SVM de Trident.

Puede crear una política de calidad de servicio para la SVM en unos pasos. Consulte la documentación de su versión de ONTAP para obtener la información más precisa. El ejemplo siguiente crea una política de calidad de servicio 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 admite esta función, puede considerar el uso de una calidad de servicio

mínima para garantizar un volumen del rendimiento para cargas de trabajo en contenedores. La calidad de servicio adaptativa no es compatible con una política de nivel de SVM.

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

- Otras cargas de trabajo que utilizan la cabina de almacenamiento. Si hay otras cargas de trabajo, no relacionadas con la puesta en marcha de Kubernetes, y que utilizan los recursos de almacenamiento, se debe tener cuidado para garantizar que esas cargas de trabajo no se vean afectadas de forma accidental.
- Cargas de trabajo esperadas que se ejecutan en contenedores. Si las cargas de trabajo que tienen requisitos de IOPS elevados se ejecutan en contenedores, una política de calidad de servicio baja resulta en una mala experiencia.

Es importante recordar que una política de calidad de servicio asignada en el nivel de la SVM da como resultado que todos los volúmenes aprovisionados a la SVM compartan el mismo pool de IOPS. Si una, o una cifra pequeña, de las aplicaciones con contenedores tienen un requisito elevado de IOPS, podría convertirse en un problema para las otras cargas de trabajo con contenedores. Si este es el caso, puede que se desee considerar utilizar la automatización externa para asignar políticas de calidad de servicio por volumen.

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

Cree grupos de políticas de calidad de servicio para Trident

La calidad de servicio garantiza que el rendimiento de las cargas de trabajo críticas no se vea degradado por cargas de trabajo de la competencia. Los grupos de políticas de calidad de servicio de ONTAP proporcionan opciones de calidad de servicio para volúmenes y permiten a los usuarios definir el techo de rendimiento para una o más cargas de trabajo. Para obtener más información sobre QoS, consulte "Rendimiento garantizado con QoS" . Puede especificar grupos de políticas de calidad de servicio en el back-end o en un pool de almacenamiento y se aplican a cada volumen creado en ese pool o back-end.

ONTAP tiene dos tipos de grupos de políticas de calidad de servicio: Tradicionales y adaptativos. Los grupos de políticas tradicionales proporcionan un rendimiento máximo (o mínimo, en versiones posteriores) plano en IOPS. La calidad de servicio adaptativa escala automáticamente el rendimiento al tamaño de la carga de trabajo y mantiene la ratio de IOPS en TB|GB a medida que el tamaño de la carga de trabajo cambia. Esto supone una ventaja significativa cuando se gestionan cientos o miles de cargas de trabajo en una puesta en marcha de gran tamaño.

Tenga en cuenta lo siguiente al crear grupos de políticas de calidad de servicio:

- Debe definir la `qosPolicy` clave en el `defaults` bloque de la configuración de backend. Consulte el siguiente ejemplo de configuración del back-end:

```
  ---
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 entero según lo especifique el grupo de políticas. No se admiten los grupos de políticas compartidas.

Para obtener más información acerca de los grupos de políticas de QoS, consulte "Comandos de calidad de servicio de ONTAP 9.8" .

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

La limitación del acceso a los volúmenes NFS y a las LUN de iSCSI creadas por Trident es un componente crucial del sistema de seguridad para la puesta en marcha de Kubernetes. Si lo hace, se evita que los hosts que no forman parte del clúster de Kubernetes accedan a los volúmenes y que 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 supone que los recursos del mismo espacio de nombres se pueden compartir; sin embargo, es importante destacar que no existe ninguna funcionalidad entre espacios de nombres. Esto significa que aunque los VP sean objetos globales, cuando están enlazados a una RVP solo pueden acceder a ellos mediante POD que están en el mismo espacio de nombres. **Es fundamental asegurarse de que los espacios de nombres se utilizan para proporcionar la separación cuando sea apropiado.**

La preocupación principal de 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 puede acceder al almacenamiento montado en el host, pero que no está destinado al contenedor. "Espacios de nombres" están diseñados para evitar este tipo de compromiso. Sin embargo, hay una excepción: Contenedores privilegiados.

Un contenedor con privilegios es uno que se ejecuta con mucho más permisos de nivel de host de lo normal. Estos no se rechazan por defecto, así que asegúrese de desactivar la capacidad mediante el uso "directivas de seguridad de pod"de .

Para los volúmenes en los que se desea obtener acceso tanto a los hosts de Kubernetes como a los externos,

el almacenamiento se debe gestionar de forma tradicional, con el VP introducido por el administrador, y no gestionado por Trident. Esto garantiza que el volumen de almacenamiento se destruya solo cuando tanto los hosts de Kubernetes como los externos se desconectaron y ya no utilizan el volumen. Además, se puede aplicar una política de exportación personalizada, lo que permite el acceso desde los nodos del clúster de Kubernetes y los servidores objetivo fuera del clúster de Kubernetes.

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

Usar una política de exportación dedicada

Debe asegurarse de que existe una política de exportación para cada back-end 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 forma, Trident limita el acceso a los volúmenes que aprovisiona a los nodos en el clúster de Kubernetes y simplifica la adición o la eliminación de nodos.

También puede crear una política de exportación manualmente y rellenarla con una o varias reglas de exportación que procesarán cada solicitud de acceso a nodo:

- Utilice `vserver export-policy create` el comando CLI de ONTAP para crear la política de exportación.
- Añada reglas a la política de exportación mediante `vserver export-policy rule create` el comando de la CLI de ONTAP.

Si ejecuta estos comandos, puede restringir el acceso de los nodos de Kubernetes a los datos.

Deshabilite `showmount` para la SVM de aplicaciones

```
`showmount`La función permite que un cliente NFS consulte a la SVM para obtener una lista de exportaciones NFS disponibles. Un pod puesto en marcha en el clúster de Kubernetes puede emitir `showmount -e` el comando contra la LIF de datos y recibir una lista de montajes disponibles, incluidos los a los que no tiene acceso. Aunque esto, por sí solo, no supone un compromiso con la seguridad, proporciona información innecesaria, potencialmente que ayuda a un usuario no autorizado a conectarse con una exportación NFS.
```

Debe deshabilitarlo mediante `showmount` el comando CLI de ONTAP a nivel de SVM:

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

Mejores prácticas para SolidFire

Conozca las prácticas recomendadas para configurar el almacenamiento de SolidFire para Trident.

Crear cuenta de SolidFire

Cada cuenta SolidFire representa un propietario de volumen único y recibe su propio conjunto de credenciales de protocolo de autenticación por desafío mutuo (CHAP). Es posible acceder a los volúmenes asignados a una cuenta mediante el nombre de cuenta y las credenciales CHAP relativas o un grupo de acceso de volúmenes. Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.

Cree una política de calidad de servicio

Utilice las políticas de calidad de servicio de SolidFire si desea crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes.

Puede establecer parámetros de calidad de servicio por cada volumen. El rendimiento de cada volumen se puede garantizar mediante el establecimiento de tres parámetros configurables que definen la calidad de servicio: Min IOPS, Max IOPS y Burst IOPS.

Aquí pueden ver los valores mínimos, máximos y de ráfaga de IOPS en relación con el tamaño de bloque de 4 KB.

Parámetro de IOPS	Definición	Valor mínimo	Valor predeterminado	Valor máx. (4KB)
IOPS mín	El nivel garantizado de rendimiento de un volumen.	50	50	15000
Tasa máx. De IOPS	El rendimiento no superará este límite.	50	15000	200.000
IOPS de ráfaga	IOPS máximo permitido en un escenario de ráfaga breve.	50	15000	200.000

Aunque Max IOPS y Burst IOPS se pueden establecer con un valor máximo de 200,000 000, el rendimiento máximo en el mundo real de un volumen se ve limitado por el uso del clúster y el rendimiento por cada nodo.

El tamaño de bloque y el ancho de banda influyen directamente en el número de IOPS. A medida que estos aumenten, el sistema aumentará el ancho de banda hasta el nivel que necesite para procesar los tamaños de bloque más grandes. A medida que aumenta el ancho de banda, se reduce el número de IOPS que el sistema es capaz de conseguir. Consulte "Calidad de servicio de SolidFire" para obtener más información sobre calidad de servicio y rendimiento.

Autenticación SolidFire

Element admite dos métodos para la autenticación: CHAP y grupos de acceso de volumen (VAG). CHAP utiliza el protocolo CHAP para autenticar el host al back-end. Los grupos de acceso de volúmenes controlan el acceso a los volúmenes que aprovisiona. NetApp recomienda utilizar CHAP para la autenticación, ya que es más sencillo y sin límites de escalado.

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

La autenticación CHAP (verificación de que el iniciador es el usuario de volumen objetivo) solo se admite con control de acceso basado en la cuenta. Si se utiliza CHAP para la autenticación, hay dos opciones disponibles: CHAP unidireccional y CHAP bidireccional. CHAP unidireccional autentica el acceso al volumen mediante el nombre de cuenta de SolidFire y el secreto de iniciador. La opción CHAP bidireccional proporciona la manera más segura de autenticar el volumen, ya que el volumen autentica el host a través del nombre de cuenta y el secreto de iniciador, y luego el host autentica el volumen por medio del nombre de cuenta y el secreto de destino.

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

¿Dónde encontrar más información?

A continuación se enumeran algunas de las prácticas recomendadas. Busque las versiones más recientes en la "Biblioteca de NetApp".

ONTAP

- "Prácticas recomendadas y guía de implementación de NFS"
- "Guía de administración de los sistemas SAN" (Para iSCSI)
- "Configuración exprés de iSCSI para RHEL"

Software Element

- "Configuración de SolidFire para Linux"

NetApp HCI

- "Requisitos previos de la implementación de NetApp HCI"
- "Acceda al motor de implementación de NetApp"

Información sobre las prácticas recomendadas de la aplicación

- "Prácticas recomendadas para MySQL en ONTAP"
- "Prácticas recomendadas para MySQL en SolidFire"
- "NetApp SolidFire y Cassandra"
- "Prácticas recomendadas de Oracle en SolidFire"
- "Prácticas recomendadas de PostgreSQL en SolidFire"

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

Integre Trident

Para integrar Trident, los siguientes elementos de diseño y arquitectura requieren integración: Selección y puesta en marcha de controladores, diseño de la clase de almacenamiento, diseño de pools virtuales, reclamación de volumen persistente (RVP) impactos en el aprovisionamiento de almacenamiento, operaciones de volúmenes y puesta en marcha de servicios OpenShift mediante Trident.

Selección y despliegue del conductor

Seleccione e implemente un controlador de back-end para el sistema de almacenamiento.

Controladores de entorno de administración ONTAP

Los controladores de entorno de administración de ONTAP se diferencian por el protocolo utilizado y cómo se aprovisionan los volúmenes en el sistema de almacenamiento. Por lo tanto, tenga cuidado al decidir qué controlador implementar.

En un nivel superior, si la aplicación cuenta con componentes que necesitan almacenamiento compartido (varios POD que acceden al mismo PVC), los controladores basados en NAS serán la opción predeterminada, mientras que los controladores iSCSI basados en bloques satisfacen las necesidades de almacenamiento no compartido. Elija el protocolo según los requisitos de la aplicación y el nivel de comodidad de los equipos de almacenamiento e infraestructura. Por lo general, existe poca diferencia entre ellas para la mayoría de las aplicaciones, con tanta frecuencia la decisión se basa en si se necesita o no almacenamiento compartido (donde más de un pod necesitará acceso simultáneo).

Los controladores de entorno de administración de ONTAP disponibles son:

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

La elección entre los tres controladores NAS tiene algunas ramificaciones a las funciones, que están disponibles para la aplicación.

Tenga en cuenta que, en las siguientes tablas, no todas las capacidades se exponen a través de Trident. El administrador de almacenamiento debe aplicar algunas después del aprovisionamiento si se desea disponer de esta funcionalidad. Las notas al pie de la superíndice distinguen la funcionalidad por característica y controlador.

Controladores para NAS de ONTAP	Snapshot	Clones	Políticas de exportación dinámicas	Conexión múltiple	Calidad de servicio	Cambie el tamaño	Replicación
`ontap-nas`	Sí	Sí	Nota de pie de página:5[]	Sí	Nota de pie de página:1[]	Sí	Nota de pie de página:1[]
`ontap-nas-economy`	Nota de la oferta:3[]	Nota de la oferta:3[]	Nota de pie de página:5[]	Sí	Nota de la oferta:3[]	Sí	Nota de la oferta:3[]
`ontap-nas-flexgroup`	Nota de pie de página:1[]	NO	Nota de pie de página:5[]	Sí	Nota de pie de página:1[]	Sí	Nota de pie de página:1[]

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

Controladores para SAN de ONTAP	Snapshot	Clones	Conexión múltiple	CHAP bidireccional	Calidad de servicio	Cambie el tamaño	Replicación
`ontap-san`	Sí	Sí	Nota de pie de página:4[]	Sí	Nota de pie de página:1[]	Sí	Nota de pie de página:1[]
`ontap-san-economy`	Sí	Sí	Nota de pie de página:4[]	Sí	Nota de la oferta:3[]	Sí	Nota de la oferta:3[]

> Nota al pie de las tablas anteriores: Yes [1]: No administrado por Trident Yes [2]: Administrado por Trident, pero no por PV granular Yes [3]: No gestionado por Trident y no por PV granular Yes [4]: Soportado para volúmenes de bloque sin procesar Yes [5]: Soportado por Trident

Las funciones que no son granulares en los VP se aplican a todo el FlexVolume y todos los VP (es decir, qtrees o LUN de FlexVols compartidos) compartirán un programa común.

Como podemos ver en las tablas anteriores, gran parte de la funcionalidad entre `ontap-nas` y `ontap-nas-economy` es la misma. Sin embargo, dado que `ontap-nas-economy` la controladora limita la capacidad para controlar la programación con una granularidad por VP, esto puede afectar a la recuperación ante desastres y a la planificación de backup en particular. Para los equipos de desarrollo que desean aprovechar la funcionalidad de clon de RVP en el almacenamiento de ONTAP, esto solo es posible cuando se utilizan los `ontap-nas` `ontap-san` controladores o. `ontap-san-economy`

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

Controladores de entorno de administración Cloud Volumes ONTAP

Cloud Volumes ONTAP proporciona control de datos junto con funciones de almacenamiento empresarial para diversos casos de uso, como recursos compartidos de archivos y almacenamiento a nivel de bloque que presta servicio a 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`. Estos son aplicables a Cloud Volume ONTAP para Azure, Cloud Volume ONTAP para GCP.

Controladores de entorno de administración de Amazon FSX para ONTAP

Amazon FSx para NetApp ONTAP te permite aprovechar las funciones, el rendimiento y las funcionalidades administrativas de NetApp que ya conoces, a la vez que aprovechas la simplicidad, la agilidad, la seguridad y la escalabilidad de almacenar datos en AWS. FSX para ONTAP es compatible con 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 back-end de HCI/SolidFire de NetApp

```
`solidfire-san`El controlador que se utiliza con las plataformas NetApp
HCI/SolidFire ayuda al administrador a configurar un back-end de Element
para Trident basándose en los límites de calidad de servicio. Si desea
diseñar su backend de modo que establezca los límites específicos de QoS
en los volúmenes aprovisionados por Trident, utilice el `type` parámetro
en el archivo backend. El administrador también puede restringir el tamaño
del volumen que se puede crear en el almacenamiento con `limitVolumeSize`
el parámetro. Actualmente, las funciones de almacenamiento de Element como
el cambio de tamaño de volúmenes y la replicación de volúmenes no se
admiten mediante `solidfire-san` el controlador. Estas operaciones se
deben realizar manualmente mediante la interfaz de usuario web del
software Element.
```

Controlador SolidFire	Snapshot	Clones	Conexión múltiple	CHAP	Calidad de servicio	Cambie el tamaño	Replicación
`solidfire-san`	Sí	Sí	Nota de pie de página:2[]	Sí	Sí	Sí	Nota de pie de página:1[]

> Nota al pie de página: Yes [1]: No gestionado por Trident Yes [2]: Compatible con volúmenes de bloque sin procesar

Controladores de entorno de administración Azure NetApp Files

Trident utiliza `azure-netapp-files` el controlador para administrar "Azure NetApp Files"el servicio.

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

Controlador Azure NetApp Files	Snapshot	Clones	Conexión múltiple	Calidad de servicio	Expanda	Replicación
`azure-netapp-files`	Sí	Sí	Sí	Sí	Sí	Nota de pie de página:1[]

> Nota al pie de página: YesFootnote:1[]: No administrado por Trident

Cloud Volumes Service en el controlador back-end de Google Cloud

Trident usa `gcp-cvs` el controlador para asociarse con el Cloud Volumes Service en Google Cloud.

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

- Si los pools virtuales están definidos en el backend, Trident intentará crear un volumen en los pools de almacenamiento de Google Cloud a los que esos pools virtuales están limitados.
- Si los pools virtuales no están definidos en el backend, Trident seleccionará un pool de almacenamiento de Google Cloud de los pools de almacenamiento disponibles en la región.

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

Para obtener más información sobre los tipos de servicio y los niveles de servicio de Cloud Volumes Service en Google Cloud, consulte "Obtén más información sobre el soporte de Trident para CVS para GCP".

Controlador de Cloud Volumes Service para Google Cloud	Snapshot	Clones	Conexión múltiple	Calidad de servicio	Expanda	Replicación
`gcp-cvs`	Sí	Sí	Sí	Sí	Sí	Disponible solo en el tipo de servicio CVS-Performance.

Notas de replicación

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

Diseño de clase de almacenamiento

Las clases de almacenamiento individuales deben configurarse y aplicarse para crear un objeto de clase de almacenamiento Kubernetes. En esta sección se analiza cómo diseñar una clase de almacenamiento para su aplicación.

Utilización de back-end específica

El filtrado se puede usar en un objeto de clase de almacenamiento específico para determinar el pool o conjunto de pools de almacenamiento que se utilizarán con esa clase de almacenamiento específica. Se pueden definir tres conjuntos de filtros en la clase de almacenamiento `storagePools:`, `additionalStoragePools` Y/o `excludeStoragePools`.

```
`storagePools`El parámetro ayuda a restringir el almacenamiento al
conjunto de pools que coinciden con los atributos especificados.
`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. Es posible usar un parámetro de forma independiente o ambos
juntos para garantizar que se seleccione el conjunto adecuado de pools de
almacenamiento.
```

El `excludeStoragePools` parámetro se utiliza para excluir específicamente el juego de pools mostrado que coincide con los atributos.

Emular las políticas de calidad de servicio

Si desea diseñar clases de almacenamiento para emular políticas de calidad de servicio, cree una clase de almacenamiento con el `media` atributo `hdd` como o. `ssd` En función del `media` atributo mencionado en la clase de almacenamiento, Trident seleccionará el back-end adecuado que sirve `hdd` o `ssd` agrega para que coincida con el atributo de medio y, a continuación, dirigirá el aprovisionamiento de los volúmenes al agregado concreto. Por lo tanto, podemos crear una clase PREMIUM de almacenamiento que tendría `media` un conjunto de atributos que `ssd` podría clasificarse como la política de calidad de servicio DE PREMIUM. Podemos crear otro ESTÁNDAR de clase de almacenamiento que tenga el conjunto de atributos de medios como "hdd", que podría clasificarse como política DE calidad DE servicio ESTÁNDAR. 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 calidad de servicio.

Utilizar back-end basado en funciones específicas

Las clases de almacenamiento se pueden diseñar para dirigir el aprovisionamiento de volúmenes en un entorno de administración específico, donde se habilitan funciones como thin provisioning y thick, copias Snapshot, clones y cifrado. Para especificar qué almacenamiento se debe utilizar, cree clases de almacenamiento que especifiquen el back-end adecuado con la función necesaria habilitada.

Pools virtuales

Los pools virtuales están disponibles para todos los back-ends de Trident. Puede definir pools virtuales para cualquier backend, utilizando cualquier controlador que proporcione Trident.

Los pools virtuales permiten a un administrador crear un nivel de abstracción sobre los back-ends que se

puede hacer referencia a través de las clases de almacenamiento, para obtener mayor flexibilidad y colocación eficiente de los volúmenes en back-ends. Pueden definirse distintos back-ends con la misma clase de servicio. Es más, es posible crear varios pools de almacenamiento en el mismo back-end, pero con características diferentes. Cuando se configura una clase de almacenamiento con un selector con etiquetas específicas, Trident elige un back-end que coincide con todas las etiquetas de selector para colocar el volumen. Si las etiquetas de selector de clase de almacenamiento coinciden con varios pools de almacenamiento, Trident elegirá uno de ellos de los que aprovisionar el volumen.

Diseño de pool virtual

Al crear un back-end, generalmente puede especificar un conjunto de parámetros. Era imposible que el administrador creara otro back-end con las mismas credenciales de almacenamiento y con un conjunto de parámetros diferente. Con la introducción de pools virtuales, este problema se ha aliviado. Los pools virtuales son una abstracción de niveles introducida entre el back-end y la clase de almacenamiento de Kubernetes de modo que el administrador puede definir parámetros junto con etiquetas a las que se puede hacer referencia a través de las clases de almacenamiento de Kubernetes como selector, de forma independiente del back-end. Se pueden definir pools virtuales para todos los back-ends de NetApp compatibles con Trident. Esta lista incluye HCI de SolidFire/NetApp, ONTAP, Cloud Volumes Service en GCP y Azure NetApp Files.

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

Emulación de distintos niveles de servicio/calidad de servicio

Se pueden diseñar pools virtuales para emular clases de servicio. Al utilizar la implementación de pools virtuales para el servicio Cloud Volume para Azure NetApp Files, examinemos cómo podemos configurar distintas clases de servicio. Configure el backend de Azure NetApp Files con varias etiquetas, que representan diferentes niveles de rendimiento. Establezca `servicelevel` Aspect en el nivel de rendimiento adecuado y agregue otros aspectos requeridos en cada etiqueta. Ahora cree diferentes clases de almacenamiento de Kubernetes que se asignarán a diferentes pools virtuales. En este `parameters.selector` campo, cada StorageClass llama la atención sobre los pools virtuales que se pueden usar para alojar un volumen.

Asignación de un conjunto específico de aspectos

Se pueden diseñar varios pools virtuales con un conjunto específico de aspectos a partir de un único back-end de almacenamiento. Para ello, configure el backend con varias etiquetas y defina los aspectos necesarios en cada etiqueta. Ahora cree diferentes clases de almacenamiento de Kubernetes utilizando `parameters.selector` el campo que se asignaría a diferentes pools virtuales. Los volúmenes que se aprovisionan en el back-end tendrán los aspectos definidos en el pool virtual elegido.

Las características de PVC que afectan al aprovisionamiento de almacenamiento

Algunos parámetros aparte de la clase de almacenamiento solicitada pueden afectar al proceso de decisiones de aprovisionamiento de Trident al crear una RVP.

Modo de acceso

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

Trident intentará hacer coincidir el protocolo de almacenamiento utilizado con el método de acceso especificado de acuerdo con la siguiente matriz. Es independiente de la plataforma de almacenamiento

subyacente.

	ReadWriteOnce	ReadOnlyMany	ReadWriteMany
ISCSI	Sí	Sí	Sí (bloque sin formato)
NFS	Sí	Sí	Sí

Si se solicita un PVC ReadWriteMany enviado a una implementación de Trident sin un back-end de NFS configurado, no se aprovisionará ningún volumen. Por este motivo, el solicitante debe usar el modo de acceso adecuado para su aplicación.

Operaciones de volumen

Modifique los volúmenes persistentes

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

Los aprovisionadores de árbol de Kubernetes no admiten las operaciones de cambio de tamaño de volumen para NFS o iSCSI VP en este momento. Trident admite la expansión de los volúmenes NFS e iSCSI.

Los detalles de conexión del VP no se pueden modificar una vez creado.

Cree snapshots de volumen bajo demanda

Trident admite la creación de instantáneas de volumen bajo demanda y la creación de RVP a partir de instantáneas mediante el marco CSI. Las copias Snapshot proporcionan un método cómodo de mantener copias de un momento específico de los datos y poseen un ciclo de vida independiente del VP de origen de Kubernetes. Estas instantáneas se pueden utilizar para clonar EVs.

Crear volúmenes a partir de snapshots

Trident también admite la creación de PersistentVolumes a partir de las snapshots de volúmenes. Para ello, solo tiene que crear una reclamación de volumen persistente y mencionar la `datasource` snapshot necesaria a partir de la que se debe crear el volumen. Trident gestionará la RVP creando un volumen con los datos presentes en la snapshot. Con esta función, es posible duplicar datos entre regiones, crear entornos de prueba, reemplazar un volumen de producción dañado o dañado en su totalidad, o recuperar archivos y directorios específicos y transferirlos a otro volumen adjunto.

Mueva volúmenes al clúster

Los administradores de almacenamiento pueden mover volúmenes entre agregados y controladoras en el clúster de ONTAP de forma no disruptiva al consumidor de almacenamiento. Esta operación no afecta a Trident ni al clúster de Kubernetes, siempre y cuando el agregado de destino sea una a la que tenga acceso la SVM a la que utiliza Trident. Lo que es más importante, si se acaba de añadir el agregado a la SVM, se deberá actualizar el back-end volviendo a añadirlo a Trident. Esto activará que Trident vuelva a inventariar la SVM con el fin de reconocer el nuevo agregado.

Sin embargo, Trident no admite automáticamente el movimiento de volúmenes entre back-ends. Esto incluye entre las SVM del mismo clúster, entre clústeres o en una plataforma de almacenamiento diferente (aunque dicho sistema de almacenamiento sea una que esté conectado a Trident).

Si se copia un volumen en otra ubicación, es posible que se use la función de importación de volúmenes para importar los volúmenes actuales a Trident.

Expanda los volúmenes

Trident admite el cambio de tamaño de VP de NFS e iSCSI. De este modo, los usuarios pueden cambiar el tamaño de sus volúmenes directamente desde la capa de Kubernetes. La expansión de volumen es posible para las principales plataformas de almacenamiento de NetApp, como ONTAP, HCI de SolidFire/NetApp y back-ends de Cloud Volumes Service. Para permitir una posible expansión más adelante, establezca `allowVolumeExpansion` en `true` en el StorageClass asociado con el volumen. Siempre que sea necesario cambiar el tamaño del volumen persistente, edite la `spec.resources.requests.storage` anotación en la reclamación Volumen persistente al tamaño de volumen deseado. Trident se ocupa automáticamente de ajustar el tamaño del volumen en el clúster de almacenamiento.

Importe un volumen existente en Kubernetes

La importación de volúmenes ofrece la posibilidad de importar un volumen de almacenamiento existente en un entorno de Kubernetes. Actualmente es compatible con `ontap-nas` `azure-netapp-files` los controladores , , `ontap-nas-flexgroup`, , `solidfire-san` y. `gcp-cvs` Esta función es útil cuando se pasa una aplicación existente a Kubernetes o durante escenarios de recuperación ante desastres.

Cuando use la ONTAP y `solidfire-san` los controladores, utilice el comando `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` para importar un volumen existente a Kubernetes que gestionará Trident. El archivo RVP YAML o JSON utilizado en el comando de importación del volumen señala a una clase de almacenamiento que identifica a Trident como el aprovisionador. Cuando se utiliza un back-end de HCI/SolidFire de NetApp, asegúrese de que los nombres de los volúmenes sean únicos. Si los nombres de los volúmenes se duplican, clone el volumen en un nombre único de modo que la función de importación de volumen pueda distinguir entre ellos.

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

Cuando se ejecuta el comando anterior, Trident encontrará el volumen en el backend y leerá su tamaño. Añadirá (y sobrescribirá automáticamente si es necesario) el tamaño de volumen de la RVP configurada. A continuación, Trident crea el nuevo VP y Kubernetes enlaza la RVP al VP.

Si se puso en marcha un contenedor de modo que requería la RVP específica importada, este permanecería en estado pendiente hasta que el par PVC/VP se enlaza a través del proceso de importación del volumen. Una vez enlazados el par PVC/PV, el contenedor debería aparecer, siempre que no haya otros problemas.

Implementar servicios OpenShift

Los servicios de clúster de valor añadido de OpenShift proporcionan una funcionalidad importante a los administradores de clúster y a las aplicaciones que se alojan. Sin embargo, el almacenamiento que utilizan estos servicios puede aprovisionarse con los recursos locales de nodos, esto limita con frecuencia la capacidad, el rendimiento, la capacidad de recuperación y la sostenibilidad del servicio. Sin embargo, al aprovechar una cabina de almacenamiento empresarial para ofrecer la capacidad de estos servicios se puede mejorar considerablemente el servicio. Al igual que sucede con todas las aplicaciones, OpenShift y los administradores de almacenamiento deberían trabajar estrechamente para determinar cuáles son las mejores

opciones para cada uno de ellos. La documentación de Red Hat debe utilizarse en gran medida para determinar los requisitos y garantizar que se satisfagan las necesidades de tamaño y rendimiento.

Servicio de registro

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

Servicio de registro

Al igual que otros servicios de OpenShift, el servicio de registro se implementa mediante Ansible con los parámetros de configuración suministrados por el archivo de inventario, también conocido como hosts, que se proporcionan al libro de estrategia. Hay dos métodos de instalación que se tratarán: Implementar el registro durante la instalación inicial de OpenShift y desplegar el registro después de que OpenShift haya sido instalado.

A partir de Red Hat OpenShift versión 3.9, la documentación oficial recomienda contra NFS para el servicio de registro debido a problemas relacionados con la corrupción de datos. Esto se basa en las pruebas de Red Hat de sus productos. El servidor NFS de ONTAP no tiene estos problemas y puede realizar fácilmente una puesta en marcha de registro. Finalmente, la elección del protocolo para el servicio de registro depende de usted; simplemente sabe que ambos funcionarán bien cuando usen las plataformas de NetApp y no hay motivos para evitar NFS si eso es lo que prefiere.

Si decide utilizar NFS con el servicio de registro, deberá establecer la variable Ansible `openshift_enable_unsupported_configurations` para `true` evitar que el instalador falle.

Manos a la obra

Opcionalmente, el servicio de registro puede implementarse tanto para aplicaciones como para las operaciones principales del propio clúster OpenShift. Si decide desplegar el registro de operaciones, especificando la variable `openshift_logging_use_ops` como `true`, se crearán dos instancias del servicio. Las variables que controlan la instancia de registro de las operaciones contienen "OPS" en ellas, mientras que la instancia de las aplicaciones no.

Configurar las variables de Ansible de acuerdo con el método de puesta en marcha es importante para garantizar que los servicios subyacentes utilizan el almacenamiento correcto. Veamos las opciones para cada uno de los métodos de despliegue.

Las siguientes tablas solo incluyen las variables relevantes para la configuración del almacenamiento en relación con el servicio de registro. Puede encontrar otras opciones en "Documentación de registro de RedHat OpenShift" las que se deben revisar, configurar y utilizar según su implementación.

Las variables de la siguiente tabla harán que el libro de estrategia de Ansible cree un VP y una RVP para el servicio de registro con los detalles proporcionados. Este método es significativamente menos flexible que usar la tableta playbook de instalación de componentes después de la instalación de OpenShift; sin embargo, si tiene volúmenes existentes disponibles, es una opción.

Variable	Detalles
`openshift_logging_storage_kind`	Establezca en `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 en la LIF de datos de su máquina virtual.
`openshift_logging_storage_nfs_directory`	La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen se une como `/openshift_logging`, usaría esa ruta para esta variable.
`openshift_logging_storage_volume_name`	El nombre, por ejemplo `pv_ose_logs`, del VP que se va a crear.
`openshift_logging_storage_volume_size`	El tamaño de la exportación NFS, por ejemplo `100Gi`.

Si su clúster OpenShift ya se está ejecutando 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`	Establezca esta opción en true para usar volúmenes aprovisionados dinámicamente.
`openshift_logging_es_pvc_storage_class_name`	El nombre de la clase de almacenamiento que se utilizará en la RVP.
`openshift_logging_es_pvc_size`	El tamaño del volumen solicitado en la RVP.
`openshift_logging_es_pvc_prefix`	Prefijo para los EVs que utiliza el servicio de registro.
`openshift_logging_es_ops_pvc_dynamic`	Establezca esta opción `true` para utilizar volúmenes aprovisionados de forma dinámica para la instancia de registro de operaciones.
`openshift_logging_es_ops_pvc_storage_class_name`	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`	Prefijo para las RVP de instancia de OPS.

Despliegue la pila de registro

Si va a implementar el registro como parte del proceso de instalación inicial de OpenShift, sólo tendrá que seguir el proceso de implementación estándar. Ansible configurará y pondrá en marcha los servicios y los objetos de OpenShift necesarios para que el servicio esté disponible tan pronto como finalice Ansible.

No obstante, si se pone en marcha después de la instalación inicial, Ansible deberá usar el libro de estrategia de los componentes. Este proceso puede cambiar ligeramente con diferentes versiones de OpenShift, así que asegúrese de leer y seguir "Documentación de Red Hat OpenShift Container Platform 3.11" para su versión.

Servicio de métricas

El servicio de métricas proporciona al administrador información valiosa sobre el estado, la utilización de recursos y la disponibilidad del clúster OpenShift. También es necesaria para la funcionalidad de escala

automática en pod y muchas organizaciones usan datos del servicio de mediciones para su cargo y/o para mostrar aplicaciones.

Al igual que sucede con el servicio de registro y OpenShift en su conjunto, Ansible se utiliza para poner en marcha el servicio de métricas. Además, al igual que el servicio de registro, el servicio de métricas se puede implementar durante una configuración inicial del cluster o después de su funcionamiento 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 siguientes tablas solo contienen las variables relevantes para la configuración del almacenamiento en cuanto se relaciona con el servicio de mediciones. Hay muchas otras opciones en la documentación que se deben revisar, configurar y utilizar de acuerdo con su implementación.

Variable	Detalles
`openshift_metrics_storage_kind`	Establezca en `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 en el LIF de datos de su SVM.
`openshift_metrics_storage_nfs_directory`	La ruta de montaje para la exportación NFS. Por ejemplo, si el volumen se une como `/openshift_metrics`, usaría esa ruta para esta variable.
`openshift_metrics_storage_volume_name`	El nombre, por ejemplo `pv_ose_metrics`, del VP que se va a crear.
`openshift_metrics_storage_volume_size`	El tamaño de la exportación NFS, por ejemplo `100Gi`.

Si su clúster OpenShift ya se está ejecutando 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`	Prefijo que se utiliza para las RVP de métricas.
`openshift_metrics_cassandra_pvc_size`	El tamaño de los volúmenes que se van a solicitar.
`openshift_metrics_cassandra_storage_type`	El tipo de almacenamiento que se utilizará para las métricas, debe establecerse una dinámica para que Ansible cree RVP 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 definidas en el archivo de hosts/inventario, ponga en marcha el servicio con Ansible. Si va a implementar en el momento de la instalación de OpenShift, el PV se creará y utilizará automáticamente. Si va a poner en marcha mediante los libros de estrategia de componentes, después de la instalación de OpenShift, Ansible crea las RVP necesarias y, después de que Trident haya aprovisionado

almacenamiento para ellos, pone en marcha el servicio.

Las variables anteriores y el proceso de implementación pueden cambiar con cada versión de OpenShift. Asegúrese de revisar y seguir "Guía de implementación de OpenShift de redhat"la versión de modo que esté configurada para el entorno.

Protección de datos y recuperación ante desastres

Conozca las opciones de protección y recuperación para Trident y volúmenes creados mediante Trident. Debería tener una estrategia de protección y recuperación de datos para cada aplicación con un requisito de persistencia.

Replicación y recuperación de Trident

Puede crear un backup para restaurar Trident en caso de desastre.

Replicación de Trident

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

Pasos

1. Haga una copia de seguridad del clúster etcd de Kubernetes con "Kubernetes: Realizar backups de un clúster etcd".
2. Coloque los artefactos de backup en un FlexVol.

> Le recomendamos que proteja la SVM en la que reside FlexVol con una relación de SnapMirror con otra SVM.

Recuperación de Trident

Con los 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 certificados y archivos de datos ETCD de Kubernetes en el host que se configurará como nodo maestro.
2. Copie todos los certificados necesarios correspondientes al clúster de Kubernetes en `/etc/kubernetes/pki` y los archivos de miembros etcd en `/var/lib/etcd`.
3. Restaure el clúster de Kubernetes desde el backup etcd con "Kubernetes: Restaurar un clúster ETCD".
4. Ejecutar `kubectl get crd` para verificar que todos los recursos personalizados de Trident han surgido y recuperado los objetos de Trident para verificar que todos los datos están disponibles.

Replicación y recuperación de SVM

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

En caso de desastre, puede activar la SVM de destino de SnapMirror para empezar a servir datos. Puede volver al primario cuando se restauran los sistemas.

Acerca de esta tarea

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

- Debe crear un back-end distinto para cada SVM con la función SVM-DR habilitada.
- Configure las clases de almacenamiento para seleccionar los back-ends replicados solo cuando sea necesario para evitar tener volúmenes que no necesitan replicación aprovisionados en los back-ends que admitan SVM-DR.
- Los administradores de aplicaciones deben comprender el coste y la complejidad adicionales asociados con la replicación y estudiar detenidamente su plan de recuperación antes de iniciar este proceso.

Replicación de SVM

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

SnapMirror le permite configurar opciones para controlar lo que se va a replicar. Necesitará saber qué opciones seleccionó al realizar la preformación Recuperación de SVM mediante Trident.

- "-identity-preserve true" Replica toda la configuración de la SVM.
- "-descarte-configs red" Excluye las LIF y la configuración de red relacionada.
- "-identity-preserve false" replica solo los volúmenes y la configuración de seguridad.

Recuperación de SVM mediante Trident

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

Pasos

1. Cancelar las transferencias programadas y continuas de SnapMirror, interrumpir la relación de replicación, detener la SVM de origen y, a continuación, activar la SVM de destino de SnapMirror.
2. Si especificó `-identity-preserve false` o `-discard-config network` al configurar la replicación de SVM, actualice el `managementLIF` y `dataLIF` en el archivo de definición de backend de Trident.
3. Confirme que `storagePrefix` está presente en el archivo de definición de backend de Trident. Este parámetro no puede cambiarse. Si se omite `storagePrefix`, se producirá un error en la actualización del backend.
4. Actualice todos los back-ends requeridos para reflejar el nuevo nombre de la SVM de destino mediante:

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

5. Si ha especificado `-identity-preserve false` o. `discard-config network`, debe devolver todos los pods de aplicación.

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

Replicación y recuperación de volúmenes

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

Luego, es posible importar los volúmenes recuperados a Trident con "importación de volumen tridentctl".

> La importación no está soportada en `ontap-nas-economy` los controladores , , `ontap-san-economy`o. `ontap-flexgroup-economy`

Protección de datos Snapshot

Puede proteger y restaurar datos con:

- Un controlador snapshot externo y CRD para crear snapshots de volúmenes de Kubernetes de volúmenes persistentes (VP).

  "Copias de Snapshot de volumen"

- Snapshots de ONTAP para restaurar el contenido completo de un volumen o para recuperar archivos o LUN individuales.

  "Snapshots de ONTAP"

Seguridad

Seguridad

Utilice las recomendaciones que se indican aquí para asegurarse de que la instalación de Trident es segura.

Ejecute Trident en su propio espacio de nombres

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

Para separar el resto de 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 el back-end y los secretos CHAP, si procede) almacenados en los objetos CRD con nombres. Debe asegurarse de permitir solo el acceso de los administradores al espacio de nombres Trident y, por lo tanto, el acceso a la `tridentctl` aplicación.

Utilice la autenticación CHAP con los back-ends DE SAN de ONTAP

Trident admite la autenticación basada en CHAP para cargas de trabajo SAN de ONTAP (mediante `ontap-san` y `ontap-san-economy` controladores). NetApp recomienda el uso de CHAP bidireccional con Trident para la autenticación entre un host y el back-end de almacenamiento.

Para los back-ends ONTAP que utilizan los controladores de almacenamiento SAN, Trident puede configurar

CHAP bidireccional y gestionar nombres de usuario y secretos CHAP a través de `tridentctl`. Consulte "Prepárese para configurar el back-end con los controladores SAN de ONTAP"para comprender cómo configura Trident CHAP en back-ends de ONTAP.

Utilice la autenticación CHAP con NetApp HCI y back-ends de SolidFire

NetApp recomienda poner en marcha CHAP bidireccional para garantizar la autenticación entre un host y los back-ends de NetApp HCI y SolidFire. Trident utiliza un objeto secreto que incluye dos contraseñas CHAP por inquilino. Cuando Trident está instalado, administra los secretos CHAP y los almacena en un `tridentvolume` objeto CR para el VP respectivo. Al crear un VP, 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 que crea Trident no se asocian con ningún grupo de acceso de volúmenes.

Utilice Trident con NVE y NAE

ONTAP de NetApp proporciona cifrado de datos en reposo para proteger los datos confidenciales en el caso de robo, devolución o reasignación de un disco. Para obtener más información, consulte "Configure la información general de cifrado de volúmenes de NetApp".

- Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Trident será habilitado para NAE.
- Si NAE no está habilitado en el back-end, cualquier volumen aprovisionado en Trident tendrá la función NVE habilitada, a menos que establezca la marca de cifrado de NVE en `false` la configuración de back-end.

Los volúmenes creados en Trident en un back-end habilitado para NAE deben estar cifrados NVE o NAE.

- Puede establecer el indicador de cifrado de NVE `true` en la configuración de back-end de Trident para anular el cifrado NAE y usar una clave de cifrado específica por volumen.
- Al configurar la marca de cifrado de NVE `false` en un back-end habilitado para NAE, se crea un volumen con la función NAE habilitada. No se puede deshabilitar el cifrado NAE mediante la marca de cifrado de NVE en `false`.

- Se puede crear manualmente un volumen de NVE en Trident mediante la configuración explícita de la marca de cifrado de NVE en `true`.

Para obtener más información sobre las opciones de configuración del back-end, consulte:

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

Configuración de clave unificada de Linux (LUKS)

Puede habilitar la configuración de clave unificada de Linux (LUKS) para cifrar los volúmenes de ECONOMÍA DE SAN de ONTAP y SAN de ONTAP en Trident. Trident admite la rotación de frase de acceso 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, como recomienda

"NIST".

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: Cryptsetup".
- Por motivos de rendimiento, recomendamos que los nodos de trabajo admitan las nuevas instrucciones estándar de cifrado avanzado (AES-ni). Para verificar el soporte de 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 estándar de cifrado avanzado (AES-ni)".

Active el cifrado LUKS

Puede habilitar el cifrado por volumen en el lado del host usando la configuración de clave unificada de Linux (LUKS) para SAN de ONTAP y volúmenes DE ECONOMÍA SAN de ONTAP.

Pasos

1. Defina los atributos de cifrado LUKS en la configuración de backend. Para obtener más información sobre las opciones de configuración de backend para SAN de ONTAP, consulte "Opciones de configuración de 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. Se utiliza `parameters.selector` para definir los pools de almacenamiento mediante 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. Cree un secreto que contenga la frase de paso 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 LUKS no pueden aprovechar la deduplicación y la compresión de ONTAP.

Configuración de backend para importar volúmenes LUKS

Para importar un volumen LUKS, debe establecer `luksEncryption` en(`true` en el backend. `luksEncryption`La opción indica a Trident si el volumen es compatible con LUKS (`true`) o no 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 dinámicamente, establezca la anotación `trident.netapp.io/luksEncryption` en `true` e incluya una clase de almacenamiento habilitada para LUKS en la RVP 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
```

Gire una frase de paso LUKS

Puede girar la frase de paso de LUKS y confirmar la rotación.

> No olvide una clave de acceso hasta que haya verificado que ya no hace referencia a ningún volumen, snapshot o secreto. Si se pierde una clave de acceso de referencia, es posible que no se pueda montar el volumen y los datos seguirán estando cifrados e inaccesibles.

Acerca de esta tarea

LA rotación DE la frase de paso LUKS se produce cuando se crea un pod que monta el volumen después de especificar una nueva frase de paso LUKS. Cuando se crea un nuevo pod, Trident compara la frase de acceso LUKS del volumen con la frase de acceso activa del secreto.

- Si la clave de acceso del volumen no coincide con la clave de acceso activa en el secreto, se produce la rotación.
- Si la clave de acceso del volumen coincide con la clave de acceso activa en el secreto, `previous-luks-passphrase` se omite el parámetro.

Pasos

1. Añada `node-publish-secret-name` los parámetros y `node-publish-secret-namespace` 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. Identifique las bases de datos passhrases existentes en el volumen o la snapshot.

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 el secreto LUKS del volumen para especificar las passphrases nuevas y anteriores. Asegúrese de que `previous-luke-passphrase-name` `previous-luks-passphrase`coincide con la frase de 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. Cree un nuevo pod montando el volumen. Esto es necesario para iniciar la rotación.
5. Compruebe que se ha girado la frase de paso.

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 frase de contraseña se giró cuando solo se devuelve la nueva frase de contraseña en el volumen y la instantánea.

Si se devuelven dos contraseñas, por ejemplo `luksPassphraseNames: ["B", "A"]`, la rotación está incompleta. Puede activar un nuevo pod para intentar completar la rotación.

Habilite la expansión de volumen

Es posible habilitar la ampliación de volumen en un volumen cifrado LUKS.

Pasos

1. Active la `CSINodeExpandSecret` puerta de función (beta 1,25+). Consulte "Kubernetes 1.25: Use Secrets for Node-Driven Expansion of CSI Volumes" para obtener más información.
2. Añada `node-expand-secret-name` los parámetros y `node-expand-secret-namespace` 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

Al iniciar la ampliación de almacenamiento en línea, el kubelet pasa las credenciales adecuadas al controlador.

Cifrado en tránsito de Kerberos

Con el cifrado en tiempo real de Kerberos, puede mejorar la seguridad de acceso a los datos al habilitar el cifrado del tráfico entre su clúster gestionado y el entorno de administración de almacenamiento.

Trident es compatible con el cifrado Kerberos para ONTAP como back-end de almacenamiento:

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

Puede crear, eliminar, cambiar el tamaño, copiar, clonar, Clone de solo lectura e importe volúmenes que usen cifrado NFS.

Configure el cifrado de Kerberos en tránsito con volúmenes de ONTAP locales

Es posible habilitar el cifrado de Kerberos en el tráfico de almacenamiento entre el clúster gestionado y un back-end de almacenamiento de ONTAP en las instalaciones.

> El cifrado de Kerberos para el tráfico NFS con back-ends de almacenamiento de ONTAP en las instalaciones solo se admite mediante `ontap-nas` el controlador de almacenamiento.

Antes de empezar

- Asegúrese de tener acceso a la `tridentctl` utilidad.
- Asegúrese de tener acceso de administrador al back-end de almacenamiento de ONTAP.
- Asegúrese de conocer el nombre del volumen o los volúmenes que compartirá desde el back-end de almacenamiento ONTAP.
- Asegúrese de haber preparado la máquina virtual de almacenamiento de ONTAP para admitir el cifrado de Kerberos para los volúmenes de NFS. Consulte "Habilite Kerberos en una LIF de datos" para obtener instrucciones.
- Asegúrese de que los volúmenes de NFSv4 GB que utilice con el cifrado de Kerberos se hayan configurado correctamente. Consulte la sección Configuración del dominio de NetApp NFSv4 (página 13) de "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Añada o modifique las políticas de exportación de ONTAP

Tiene que agregar reglas a políticas de exportación de ONTAP existentes o crear nuevas políticas de exportación que sean compatibles con el cifrado de 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 políticas de exportación que añada, o las nuevas políticas de exportación que cree, deben admitir los siguientes protocolos de acceso y permisos de acceso:

Protocolos de acceso

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

Detalles de acceso

Puede configurar una de tres versiones diferentes de cifrado de Kerberos, según las necesidades del

volumen:

- **Kerberos 5** - (autenticación y cifrado)
- **Kerberos 5i** - (autenticación y encriptación con protección de identidad)
- **Kerberos 5p** - (autenticación y encriptación 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 montarán los volúmenes NFS con una combinación de Kerberos 5i y cifrado Kerberos 5p, utilice los siguientes ajustes de acceso:

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

Consulte la siguiente documentación para saber cómo crear políticas de exportación de ONTAP y reglas de políticas de exportación:

- "Cree una política de exportación"
- "Añada una regla a una política de exportación"

Cree un back-end de almacenamiento

Puede crear una configuración de back-end de almacenamiento de Trident que incluya la funcionalidad de cifrado de Kerberos.

Acerca de esta tarea

Al crear un archivo de configuración de backend de almacenamiento que configure el cifrado Kerberos, puede especificar una de las tres versiones diferentes del 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 encriptación con protección de identidad y privacidad)

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

Pasos

1. En el clúster gestionado, cree un archivo de configuración de back-end de almacenamiento utilizando el ejemplo siguiente. Sustituya los valores entre paréntesis <> por 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 la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver 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 ejecutar de nuevo el comando create.

Cree una clase de almacenamiento

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

Acerca de esta tarea

Al crear un objeto de clase de almacenamiento, puede especificar una de las tres versiones diferentes del cifrado de 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 encriptación con protección de identidad y privacidad)

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

Pasos

1. Cree un objeto de Kubernetes StorageClass, mediante 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. Cree la clase de almacenamiento:

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

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

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

   Debería ver una salida similar a la siguiente:

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

Aprovisione los volúmenes

Después de crear un back-end de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar un volumen. Para obtener instrucciones, consulte "Aprovisione un volumen" .

Configure el cifrado de Kerberos en tránsito con volúmenes Azure NetApp Files

Puede habilitar el cifrado de Kerberos en el tráfico de almacenamiento entre su clúster gestionado y un solo back-end de almacenamiento de Azure NetApp Files o un pool virtual de back-ends de almacenamiento de Azure NetApp Files.

Antes de empezar

- Asegúrese de haber habilitado Trident en el clúster gestionado de Red Hat OpenShift.
- Asegúrese de tener acceso a la `tridentctl` utilidad.
- Asegúrese de haber preparado el back-end de almacenamiento de Azure NetApp Files para el cifrado Kerberos siguiendo los requisitos y siguiendo las instrucciones de "Documentación de Azure NetApp Files".
- Asegúrese de que los volúmenes de NFSv4 GB que utilice con el cifrado de Kerberos se hayan configurado correctamente. Consulte la sección Configuración del dominio de NetApp NFSv4 (página 13) de "Guía de mejoras y prácticas recomendadas de NetApp NFSv4".

Cree un back-end de almacenamiento

Puede crear una configuración de back-end de almacenamiento de Azure NetApp Files que incluya la funcionalidad de cifrado de 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 los dos niveles posibles:

- El **storage backend level** usando el `spec.kerberos` campo
- El **nivel de pool virtual** usando el `spec.storage.kerberos` campo

Cuando se define la configuración en el nivel del pool virtual, el pool se selecciona con la etiqueta de la clase de almacenamiento.

En cualquier nivel, puede especificar una de las tres versiones diferentes del cifrado Kerberos:

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

Pasos

1. En el clúster gestionado, cree un archivo de configuración de back-end de almacenamiento mediante uno de los siguientes ejemplos, en función del lugar donde necesite definir el back-end de almacenamiento (nivel de back-end de almacenamiento o nivel de pool virtual). Sustituya los valores entre paréntesis <> por información de su entorno:

Ejemplo de nivel de back-end 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 pool 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 la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver 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 ejecutar de nuevo el comando create.

Cree una clase de almacenamiento

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

Pasos

1. Cree un objeto de Kubernetes StorageClass, mediante 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. Cree la clase de almacenamiento:

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

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

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

Debería ver una salida similar a la siguiente:

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

Aprovisione los volúmenes

Después de crear un back-end de almacenamiento y una clase de almacenamiento, ahora puede aprovisionar un volumen. Para obtener instrucciones, consulte "Aprovisione un volumen" .