Melhores práticas e recomendações

Trident

NetApp
March 05, 2026

Índice

Melhores práticas e recomendações

Implantação

Utilize as recomendações listadas aqui ao implantar o Trident.

Implantar em um namespace dedicado

"Espaços de nomes"Proporcionam separação administrativa entre diferentes aplicações e constituem uma barreira ao compartilhamento de recursos. Por exemplo, um PVC de um namespace não pode ser consumido por outro. O Trident fornece recursos PV para todos os namespaces no cluster Kubernetes e, consequentemente, utiliza uma conta de serviço com privilégios elevados.

Além disso, o acesso ao módulo Trident pode permitir que um usuário acesse credenciais do sistema de armazenamento e outras informações confidenciais. É importante garantir que os usuários do aplicativo e os aplicativos de gerenciamento não tenham a capacidade de acessar as definições de objeto do Trident ou os próprios pods.

Utilize quotas e limites de intervalo para controlar o consumo de armazenamento.

O Kubernetes possui duas funcionalidades que, quando combinadas, fornecem um mecanismo poderoso para limitar o consumo de recursos pelas aplicações. O "mecanismo de cota de armazenamento" Permite ao administrador implementar limites globais e específicos da classe de armazenamento para o consumo de capacidade e contagem de objetos por namespace. Além disso, usando um "limite de alcance" Garante que as solicitações de PVC estejam dentro de um valor mínimo e máximo antes de serem encaminhadas ao provisionador.

Esses valores são definidos para cada namespace individualmente, o que significa que cada namespace deve ter valores definidos que estejam de acordo com seus requisitos de recursos. Veja aqui para obter informações sobre "como aproveitar as quotas" .

Configuração de armazenamento

Cada plataforma de armazenamento no portfólio da NetApp possui recursos exclusivos que beneficiam os aplicativos, sejam eles conteinerizados ou não.

Visão geral da plataforma

O Trident funciona com ONTAP e Element. Não existe uma plataforma que seja mais adequada para todas as aplicações e cenários do que outra; no entanto, as necessidades da aplicação e da equipe que administra o dispositivo devem ser levadas em consideração ao escolher uma plataforma.

Você deve seguir as melhores práticas básicas para o sistema operacional do host com o protocolo que você está utilizando. Opcionalmente, você pode considerar incorporar as melhores práticas de aplicação, quando disponíveis, nas configurações de backend, classe de armazenamento e PVC para otimizar o armazenamento para aplicações específicas.

ONTAP e Cloud Volumes ONTAP: Melhores práticas

Aprenda as melhores práticas para configurar o ONTAP e o Cloud Volumes ONTAP para Trident.

As recomendações a seguir são diretrizes para configurar o ONTAP para cargas de trabalho conteinerizadas, que consomem volumes provisionados dinamicamente pelo Trident. Cada um deve ser considerado e avaliado quanto à sua adequação ao seu ambiente.

Use SVM(s) dedicada(s) ao Trident.

Máquinas virtuais de armazenamento (SVMs) fornecem isolamento e separação administrativa entre locatários em um sistema ONTAP . Dedicar uma SVM a aplicações permite a delegação de privilégios e a aplicação das melhores práticas para limitar o consumo de recursos.

Existem diversas opções disponíveis para o gerenciamento da SVM:

- Forneça a interface de gerenciamento do cluster na configuração do backend, juntamente com as credenciais apropriadas, e especifique o nome da SVM.
- Crie uma interface de gerenciamento dedicada para a SVM usando o ONTAP System Manager ou a CLI.
- Compartilhe a função de gerenciamento com uma interface de dados NFS.

Em todos os casos, a interface deve estar no DNS e o nome DNS deve ser usado ao configurar o Trident. Isso ajuda a facilitar alguns cenários de recuperação de desastres (DR), por exemplo, SVM-DR sem a necessidade de retenção de identidade de rede.

Não há preferência entre ter uma LIF de gerenciamento dedicada ou compartilhada para a SVM; no entanto, você deve garantir que suas políticas de segurança de rede estejam alinhadas com a abordagem escolhida. Independentemente disso, o LIF de gerenciamento deve ser acessível via DNS para facilitar a máxima flexibilidade. "SVM-DR" Pode ser usado em conjunto com o Trident.

Limitar a contagem máxima de volume

Os sistemas de armazenamento ONTAP possuem um número máximo de volumes, que varia de acordo com a versão do software e a plataforma de hardware. Consulte "Hardware Universe da NetApp" Para determinar os limites exatos, consulte a plataforma específica e a versão do ONTAP . Quando o número de volumes disponíveis se esgota, as operações de provisionamento falham não apenas para o Trident, mas para todas as solicitações de armazenamento.

Tridente `ontap-nas` e `ontap-san` Os drivers provisionam um FlexVolume para cada Volume Persistente (PV) do Kubernetes que é criado. O `ontap-nas-economy` O driver cria aproximadamente um FlexVolume para cada 200 PVs (configurável entre 50 e 300). O `ontap-san-economy` O driver cria aproximadamente um FlexVolume para cada 100 PVs (configurável entre 50 e 200). Para evitar que o Trident consuma todos os volumes disponíveis no sistema de armazenamento, você deve definir um limite no SVM. Você pode fazer isso na linha de comando:

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

O valor para `max-volumes` varia de acordo com diversos critérios específicos do seu ambiente:

- O número de volumes existentes no cluster ONTAP
- O número de volumes que você espera provisionar fora do Trident para outros aplicativos.
- O número de volumes persistentes que se espera que sejam consumidos por aplicações Kubernetes.

O `max-volumes` O valor representa o total de volumes provisionados em todos os nós do cluster ONTAP , e não em um nó ONTAP individual. Como resultado, você pode encontrar algumas condições em que um nó de

cluster ONTAP pode ter muito mais ou menos volumes provisionados Trident do que outro nó.

Por exemplo, um cluster ONTAP de dois nós tem a capacidade de hospedar um máximo de 2000 volumes FlexVol . Definir o número máximo de volumes em 1250 parece bastante razoável. No entanto, se apenas "agregados" Se os volumes atribuídos a partir de um nó forem alocados ao SVM, ou se os agregados atribuídos a partir de um nó não puderem ser provisionados (por exemplo, devido à capacidade), o outro nó se torna o destino de todos os volumes provisionados Trident . Isso significa que o limite de volume pode ser atingido para esse nó antes do `max-volumes` O valor é atingido, impactando tanto o Trident quanto outras operações de volume que utilizam esse nó. **Você pode evitar essa situação garantindo que os agregados de cada nó do cluster sejam atribuídos ao SVM usado pelo Trident em números iguais.**

Clonar um volume

O NetApp Trident suporta a clonagem de volumes ao usar o `ontap-nas` , `ontap-san` , `solidfire-san` , e `gcp-cvs` drivers de armazenamento. Ao usar o `ontap-nas-flexgroup` ou `ontap-nas-economy` Drivers, clonagem não é suportada. Criar um novo volume a partir de um volume existente resultará na criação de um novo snapshot.

> Evite clonar um PVC associado a uma StorageClass diferente. Execute operações de clonagem dentro da mesma StorageClass para garantir a compatibilidade e evitar comportamentos inesperados.

Limitar o tamanho máximo dos volumes criados pelo Trident

Para configurar o tamanho máximo dos volumes que podem ser criados pelo Trident, use o `limitVolumeSize` parâmetro em seu `backend.json` definição.

Além de controlar o tamanho do volume no array de armazenamento, você também deve aproveitar os recursos do Kubernetes.

Limitar o tamanho máximo dos FlexVols criados pelo Trident.

Para configurar o tamanho máximo dos FlexVols usados como pools para os drivers ontap-san-economy e ontap-nas-economy, utilize o `limitVolumePoolSize` parâmetro em seu `backend.json` definição.

Configure o Trident para usar CHAP bidirecional.

Você pode especificar os nomes de usuário e senhas do iniciador e do destino CHAP na definição do seu backend e configurar o Trident para habilitar o CHAP na SVM. Usando o `useCHAP` Ao configurar o parâmetro na sua configuração de backend, o Trident autentica as conexões iSCSI para backends ONTAP com CHAP.

Criar e usar uma política de QoS para SVM

Utilizando uma política de QoS do ONTAP , aplicada ao SVM, limita-se o número de IOPS que podem ser consumidos pelos volumes provisionados Trident . Isso ajuda a "prevenir um valentão" ou um contêiner fora de controle que afete cargas de trabalho fora do Trident SVM.

Você pode criar uma política de QoS para a SVM em poucos passos. Consulte a documentação da sua versão do ONTAP para obter as informações mais precisas. O exemplo abaixo cria uma política de QoS que limita o total de IOPS disponíveis para a 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>
```

Além disso, se a sua versão do ONTAP suportar, você pode considerar usar um mínimo de QoS para garantir uma quantidade de throughput para cargas de trabalho em contêineres. A QoS adaptativa não é compatível com uma política de nível SVM.

O número de IOPS dedicados às cargas de trabalho em contêineres depende de muitos fatores. Entre outras coisas, isso inclui:

- Outras cargas de trabalho que utilizam o array de armazenamento. Caso existam outras cargas de trabalho, não relacionadas à implementação do Kubernetes, utilizando os recursos de armazenamento, deve-se tomar cuidado para garantir que essas cargas de trabalho não sejam afetadas negativamente por acidente.
- Cargas de trabalho esperadas em execução em contêineres. Se cargas de trabalho com altos requisitos de IOPS forem executadas em contêineres, uma política de QoS baixa resultará em uma experiência ruim.

É importante lembrar que uma política de QoS atribuída no nível da SVM resulta em todos os volumes provisionados para a SVM compartilhando o mesmo pool de IOPS. Se uma, ou um pequeno número, das aplicações conteinerizadas tiverem uma alta exigência de IOPS, isso poderá sobrecarregar as outras cargas de trabalho conteinerizadas. Nesse caso, você pode considerar usar automação externa para atribuir políticas de QoS por volume.

> Você deve atribuir o grupo de políticas de QoS à SVM **somente** se a sua versão do ONTAP for anterior à 9.8.

Crie grupos de políticas de QoS para o Trident.

A Qualidade de Serviço (QoS) garante que o desempenho de cargas de trabalho críticas não seja prejudicado por cargas de trabalho concorrentes. Os grupos de políticas de QoS do ONTAP fornecem opções de QoS para volumes e permitem que os usuários definam o limite de taxa de transferência para uma ou mais cargas de trabalho. Para obter mais informações sobre QoS, consulte: "Garantindo a taxa de transferência com QoS" . Você pode especificar grupos de políticas de QoS no backend ou em um pool de armazenamento, e eles serão aplicados a cada volume criado nesse pool ou backend.

O ONTAP possui dois tipos de grupos de políticas de QoS: tradicionais e adaptativos. Os grupos de políticas tradicionais fornecem uma taxa de transferência máxima (ou mínima, em versões posteriores) fixa em IOPS. O QoS adaptativo dimensiona automaticamente a taxa de transferência de acordo com o tamanho da carga de trabalho, mantendo a proporção de IOPS para TBs|GBs à medida que o tamanho da carga de trabalho muda. Isso proporciona uma vantagem significativa ao gerenciar centenas ou milhares de cargas de trabalho em uma implantação de grande porte.

Ao criar grupos de políticas de QoS, considere o seguinte:

- Você deve definir o `qosPolicy` chave no `defaults` bloco da configuração do backend. Veja o exemplo de configuração de backend a seguir:

```
---
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
```

- Você deve aplicar os grupos de políticas por volume, para que cada volume receba toda a taxa de transferência especificada pelo grupo de políticas. Grupos de políticas compartilhadas não são suportados.

Para obter mais informações sobre grupos de políticas de QoS, consulte: "Referência de comandos ONTAP" .

Limitar o acesso a recursos de armazenamento aos membros do cluster Kubernetes

Limitar o acesso aos volumes NFS, LUNs iSCSI e LUNs FC criados pelo Trident é um componente crítico da postura de segurança da sua implementação do Kubernetes. Isso evita que hosts que não fazem parte do cluster do Kubernetes acessem os volumes e potencialmente modifiquem dados inesperadamente.

É importante entender que os namespaces são o limite lógico para recursos no Kubernetes. A premissa é que os recursos no mesmo espaço de nomes podem ser compartilhados; no entanto, é importante ressaltar que não há capacidade de compartilhamento entre espaços de nomes diferentes. Isso significa que, embora os PVs sejam objetos globais, quando vinculados a um PVC, eles só são acessíveis por pods que estejam no mesmo namespace. **É fundamental garantir que os namespaces sejam usados para fornecer separação quando apropriado.**

A principal preocupação da maioria das organizações em relação à segurança de dados em um contexto Kubernetes é que um processo em um contêiner possa acessar o armazenamento montado no host, mas que não se destina ao contêiner. "Espaços de nomes" são projetadas para evitar esse tipo de comprometimento. No entanto, existe uma exceção: os contêineres privilegiados.

Um contêiner privilegiado é aquele que é executado com permissões de nível de host substancialmente maiores do que o normal. Essas opções não são negadas por padrão, portanto, certifique-se de desativar a funcionalidade usando "políticas de segurança de pod" .

Para volumes onde o acesso é desejado tanto do Kubernetes quanto de hosts externos, o armazenamento deve ser gerenciado de maneira tradicional, com o PV (Volume de Processo) introduzido pelo administrador e

não gerenciado pelo Trident. Isso garante que o volume de armazenamento seja destruído somente quando o Kubernetes e os hosts externos estiverem desconectados e não estiverem mais usando o volume. Além disso, é possível aplicar uma política de exportação personalizada, que permite o acesso a partir dos nós do cluster Kubernetes e de servidores de destino fora do cluster Kubernetes.

Para implantações que possuem nós de infraestrutura dedicados (por exemplo, OpenShift) ou outros nós que não conseguem agendar aplicativos de usuário, políticas de exportação separadas devem ser usadas para limitar ainda mais o acesso aos recursos de armazenamento. Isso inclui a criação de uma política de exportação para serviços que são implantados nesses nós de infraestrutura (por exemplo, os serviços OpenShift Metrics e Logging) e aplicativos padrão que são implantados em nós que não são de infraestrutura.

Utilize uma política de exportação específica.

Você deve garantir que exista uma política de exportação para cada backend que permita acesso apenas aos nós presentes no cluster Kubernetes. O Trident pode criar e gerenciar automaticamente políticas de exportação. Dessa forma, o Trident limita o acesso aos volumes que provisiona aos nós no cluster Kubernetes e simplifica a adição/exclusão de nós.

Alternativamente, você também pode criar uma política de exportação manualmente e preenchê-la com uma ou mais regras de exportação que processem cada solicitação de acesso ao nó:

- Use o `vserver export-policy create` Comando da CLI do ONTAP para criar a política de exportação.
- Adicione regras à política de exportação usando o `vserver export-policy rule create` Comando ONTAP CLI.

Executar esses comandos permite restringir quais nós do Kubernetes têm acesso aos dados.

Desativar `showmount` para a aplicação SVM

O `showmount` Esse recurso permite que um cliente NFS consulte a SVM para obter uma lista de exportações NFS disponíveis. Um pod implantado no cluster Kubernetes pode emitir o `showmount -e` Comande o inimigo e receba uma lista de montarias disponíveis, incluindo aquelas às quais ele não tem acesso. Embora isso, por si só, não represente uma falha de segurança, fornece informações desnecessárias que podem auxiliar um usuário não autorizado a se conectar a uma exportação NFS.

Você deve desativar `showmount` utilizando o comando ONTAP CLI em nível de SVM:

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

Melhores práticas do SolidFire

Aprenda as melhores práticas para configurar o armazenamento SolidFire para Trident.

Criar conta Solidfire

Cada conta SolidFire representa um proprietário de volume único e recebe seu próprio conjunto de credenciais do Protocolo de Autenticação por Desafio e Aperto de Mão (CHAP). Você pode acessar os volumes atribuídos a uma conta usando o nome da conta e as credenciais CHAP correspondentes ou por meio de um grupo de acesso a volumes. Uma conta pode ter até dois mil volumes atribuídos a ela, mas um volume só pode pertencer a uma conta.

Criar uma política de QoS

Utilize as políticas de Qualidade de Serviço (QoS) do SolidFire se desejar criar e salvar uma configuração padronizada de qualidade de serviço que possa ser aplicada a vários volumes.

Você pode definir parâmetros de QoS para cada volume individualmente. O desempenho de cada volume pode ser garantido definindo três parâmetros configuráveis que definem a QoS: IOPS mínimo, IOPS máximo e IOPS de rajada.

Aqui estão os possíveis valores mínimos, máximos e de burst de IOPS para um tamanho de bloco de 4Kb.

Parâmetro IOPS	Definição	Valor mínimo	Valor padrão	Valor máximo (4 KB)
IOPS mínimo	Nível de desempenho garantido para um determinado volume.	50	50	15000
IOPS máximo	O desempenho não ultrapassará esse limite.	50	15000	200.000
IOPS de rajada	Máximo de IOPS permitido em um cenário de pico curto.	50	15000	200.000

Embora os valores de Max IOPS e Burst IOPS possam ser configurados para até 200.000, o desempenho máximo real de um volume é limitado pelo uso do cluster e pelo desempenho de cada nó.

O tamanho do bloco e a largura de banda influenciam diretamente o número de IOPS. À medida que o tamanho dos blocos aumenta, o sistema aumenta a largura de banda para um nível necessário para processar os blocos maiores. À medida que a largura de banda aumenta, o número de IOPS que o sistema consegue atingir diminui. Consulte "Qualidade de serviço SolidFire" Para obter mais informações sobre QoS e desempenho.

Autenticação SolidFire

O Element suporta dois métodos de autenticação: CHAP e Grupos de Acesso por Volume (VAG). O CHAP utiliza o protocolo CHAP para autenticar o host no servidor de backend. Os Grupos de Acesso a Volumes controlam o acesso aos volumes que provisionam. A NetApp recomenda o uso do CHAP para autenticação, pois é mais simples e não possui limites de escalabilidade.

O Trident com o provisionador CSI aprimorado suporta o uso da autenticação CHAP. Os VAGs devem ser usados apenas no modo de operação tradicional, não CSI.

A autenticação CHAP (verificação de que o iniciador é o usuário do volume pretendido) é suportada apenas com controle de acesso baseado em conta. Se você estiver usando CHAP para autenticação, duas opções estão disponíveis: CHAP unidirecional e CHAP bidirecional. O CHAP unidirecional autentica o acesso ao

volume usando o nome da conta SolidFire e o segredo do iniciador. A opção CHAP bidirecional oferece a maneira mais segura de autenticar o volume, pois o volume autentica o host por meio do nome da conta e do segredo do iniciador, e então o host autentica o volume por meio do nome da conta e do segredo do destino.

No entanto, se o CHAP não puder ser ativado e os VAGs forem necessários, crie o grupo de acesso e adicione os iniciadores de host e os volumes ao grupo de acesso. Cada IQN adicionado a um grupo de acesso pode acessar todos os volumes do grupo, com ou sem autenticação CHAP. Se o iniciador iSCSI estiver configurado para usar autenticação CHAP, o controle de acesso baseado em conta será utilizado. Se o iniciador iSCSI não estiver configurado para usar autenticação CHAP, o controle de acesso do Grupo de Acesso ao Volume será utilizado.

Onde posso encontrar mais informações?

Abaixo, encontra-se listada parte da documentação sobre as melhores práticas. Pesquise o "Biblioteca NetApp" para as versões mais recentes.

- ONTAP*
- "Guia de Melhores Práticas e Implementação do NFS"
- "Administração SAN"(para iSCSI)
- "Configuração iSCSI Express para RHEL"

Software Elemento

- "Configurando o SolidFire para Linux"
- NetApp HCI*
- "Pré-requisitos para implantação do NetApp HCI"
- "Acesse o mecanismo de implantação da NetApp"

Informações sobre as melhores práticas de aplicação

- "Melhores práticas para MySQL no ONTAP"
- "Melhores práticas para MySQL no SolidFire"
- "NetApp SolidFire e Cassandra"
- "Melhores práticas da Oracle no SolidFire"
- "Melhores práticas do PostgreSQL no SolidFire"

Nem todas as aplicações possuem diretrizes específicas; é importante trabalhar com sua equipe da NetApp e utilizar o… "Biblioteca NetApp" Para encontrar a documentação mais atualizada.

Integrar Trident

Para integrar o Trident, os seguintes elementos de design e arquitetura precisam ser integrados: seleção e implantação de drivers, design de classes de armazenamento, design de pools virtuais, impactos do Persistent Volume Claim (PVC) no provisionamento de armazenamento, operações de volume e implantação de serviços OpenShift usando o Trident.

Seleção e alocação de motoristas

Selecione e implemente um driver de backend para o seu sistema de armazenamento.

Drivers de backend ONTAP

Os drivers de backend do ONTAP são diferenciados pelo protocolo utilizado e pela forma como os volumes são provisionados no sistema de armazenamento. Portanto, considere cuidadosamente ao decidir qual driver implantar.

Em um nível mais elevado, se sua aplicação possui componentes que necessitam de armazenamento compartilhado (vários pods acessando o mesmo PVC), os drivers baseados em NAS seriam a escolha padrão, enquanto os drivers iSCSI baseados em bloco atendem às necessidades de armazenamento não compartilhado. Escolha o protocolo com base nos requisitos da aplicação e no nível de conforto das equipes de armazenamento e infraestrutura. De um modo geral, existe pouca diferença entre eles para a maioria das aplicações, pelo que a decisão costuma basear-se na necessidade ou não de armazenamento partilhado (em que mais do que um pod necessitará de acesso simultâneo).

Os drivers de backend ONTAP disponíveis são:

- `ontap-nas`Cada PV provisionado é um FlexVolume ONTAP completo.
- `ontap-nas-economy`Cada PV provisionado é uma qtree, com um número configurável de qtrees por FlexVolume (o padrão é 200).
- `ontap-nas-flexgroup`Cada PV provisionado como um ONTAP FlexGroup completo e todos os agregados atribuídos a um SVM são utilizados.
- `ontap-san`Cada PV provisionado é um LUN dentro de seu próprio FlexVolume.
- `ontap-san-economy`Cada PV provisionado é um LUN, com um número configurável de LUNs por FlexVolume (o padrão é 100).

A escolha entre os três drivers NAS tem algumas implicações nos recursos disponibilizados para o aplicativo.

Observe que, nas tabelas abaixo, nem todas as funcionalidades estão expostas através do Trident. Algumas configurações devem ser aplicadas pelo administrador de armazenamento após o provisionamento, caso essa funcionalidade seja desejada. As notas de rodapé em sobrescrito distinguem a funcionalidade de cada recurso e driver.

Drivers ONTAP NAS	Instantâneos	Clones	Políticas de exportação dinâmicas	Conexão múltipla	Qualidade de Serviço	Redimensionar	Replicação
`ontap-nas`	Sim	Sim	Sim, nota de rodapé:5[]	Sim	Sim, nota de rodapé:1[]	Sim	Sim, nota de rodapé:1[]
`ontap-nas-economy`	NO [3]	NO [3]	Sim, nota de rodapé:5[]	Sim	NO [3]	Sim	NO [3]
`ontap-nas-flexgroup`	Sim, nota de rodapé:1[]	NÃO	Sim, nota de rodapé:5[]	Sim	Sim, nota de rodapé:1[]	Sim	Sim, nota de rodapé:1[]

A Trident oferece 2 drivers SAN para ONTAP, cujas funcionalidades são apresentadas abaixo.

Motoristas ONTAP SAN	Instantâneos	Clones	Conexão múltipla	CHAP bidirecional	Qualidade de Serviço	Redimensionar	Replicação
`ontap-san`	Sim	Sim	Sim, nota de rodapé:4[]	Sim	Sim, nota de rodapé:1[]	Sim	Sim, nota de rodapé:1[]
`ontap-san-economy`	Sim	Sim	Sim, nota de rodapé:4[]	Sim	NO [3]	Sim	NO [3]

> Nota de rodapé para as tabelas acima: SimNota1[]: Não gerenciado pelo Trident SimNota2[]: Gerenciado pelo Trident, mas não granularmente em PV NãoNota3[]: Não gerenciado pelo Trident e não granularmente em PV SimNota4[]: Suportado para volumes de bloco bruto SimNota5[]: Suportado pelo Trident

Os recursos que não são granulares em relação ao PV são aplicados a todo o FlexVolume e todos os PVs (ou seja, qtrees ou LUNs em FlexVols compartilhados) compartilharão um agendamento comum.

Como podemos ver nas tabelas acima, grande parte da funcionalidade entre os `ontap-nas` e `ontap-nas-economy` é o mesmo. No entanto, porque o `ontap-nas-economy` O driver limita a capacidade de controlar o agendamento em nível de granularidade por PV, o que pode afetar, em particular, o planejamento de recuperação de desastres e backup. Para equipes de desenvolvimento que desejam aproveitar a funcionalidade de clonagem de PVC no armazenamento ONTAP , isso só é possível ao usar o `ontap-nas` , `ontap-san` ou `ontap-san-economy` motoristas.

> O `solidfire-san` O driver também é capaz de clonar PVCs.

Drivers de backend do Cloud Volumes ONTAP

O Cloud Volumes ONTAP oferece controle de dados juntamente com recursos de armazenamento de nível empresarial para diversos casos de uso, incluindo compartilhamento de arquivos e armazenamento em nível de bloco, atendendo a protocolos NAS e SAN (NFS, SMB/CIFS e iSCSI). Os drivers compatíveis com o Cloud Volume ONTAP são: `ontap-nas` , `ontap-nas-economy` , `ontap-san` e `ontap-san-economy` . Estas opções são aplicáveis ao Cloud Volume ONTAP para Azure e ao Cloud Volume ONTAP para GCP.

Drivers de backend do Amazon FSx para ONTAP

O Amazon FSx for NetApp ONTAP permite que você aproveite os recursos, o desempenho e as capacidades administrativas da NetApp com os quais você já está familiarizado, ao mesmo tempo que desfruta da simplicidade, agilidade, segurança e escalabilidade do armazenamento de dados na AWS. O FSx para ONTAP oferece suporte a muitos recursos do sistema de arquivos ONTAP e APIs de administração. Os drivers compatíveis com o Cloud Volume ONTAP são: `ontap-nas` , `ontap-nas-economy` , `ontap-nas-flexgroup` , `ontap-san` e `ontap-san-economy` .

Drivers de backend NetApp HCI/ SolidFire

O `solidfire-san` O driver usado com as plataformas NetApp HCI/ SolidFire ajuda o administrador a configurar um backend Element para o Trident com base nos limites de QoS. Se você deseja projetar seu

backend para definir limites de QoS específicos nos volumes provisionados pelo Trident, use o `type` parâmetro no arquivo de backend. O administrador também pode restringir o tamanho do volume que pode ser criado no armazenamento usando o `limitVolumeSize` parâmetro. Atualmente, recursos de armazenamento do Element, como redimensionamento e replicação de volumes, não são suportados pelo sistema. `solidfire-san` motorista. Essas operações devem ser realizadas manualmente através da interface web do Element Software.

Driver SolidFire	Instantâneos	Clones	Conexão múltipla	RACHAR	Qualidade de Serviço	Redimensionar	Replicação
`solidfire-san`	Sim	Sim	Sim, nota de rodapé:2[]	Sim	Sim	Sim	Sim, nota de rodapé:1[]

> Nota de rodapé: SimNota de rodapé:1[]: Não gerenciado pelo Trident SimNota de rodapé:2[]: Compatível com volumes de bloco bruto

Drivers de back-end do Azure NetApp Files

Trident usa o `azure-netapp-files` motorista para gerenciar o"Azure NetApp Files" serviço.

Mais informações sobre este driver e como configurá-lo podem ser encontradas em"Configuração do backend Trident para Azure NetApp Files" .

Driver de Azure NetApp Files	Instantâneos	Clones	Conexão múltipla	Qualidade de Serviço	Expandir	Replicação
`azure-netapp-files`	Sim	Sim	Sim	Sim	Sim	Sim, nota de rodapé:1[]

> Nota de rodapé: Sim [1]: Não gerenciado pela Trident

Cloud Volumes Service no driver de backend do Google Cloud

Trident usa o `gcp-cvs` Driver para conectar com o Cloud Volumes Service no Google Cloud.

O `gcp-cvs` O driver utiliza pools virtuais para abstrair o backend e permitir que o Trident determine o posicionamento dos volumes. O administrador define os pools virtuais no `backend.json` arquivos. As classes de armazenamento usam seletores para identificar pools virtuais por rótulo.

- Se os pools virtuais forem definidos no backend, o Trident tentará criar um volume nos pools de armazenamento do Google Cloud aos quais esses pools virtuais estão limitados.
- Caso os pools virtuais não estejam definidos no backend, o Trident selecionará um pool de armazenamento do Google Cloud dentre os pools de armazenamento disponíveis na região.

Para configurar o backend do Google Cloud no Trident, você deve especificar `projectNumber` , `apiRegion` , e `apiKey` no arquivo de backend. Você pode encontrar o número do projeto no console do Google Cloud. A chave da API é obtida do arquivo de chave privada da conta de serviço que você criou ao configurar o acesso à API do Cloud Volumes Service no Google Cloud.

Para obter detalhes sobre os tipos e níveis de serviço do Cloud Volumes Service no Google Cloud,

consulte:"Saiba mais sobre o suporte do Trident para CVS em GCP" .

Driver do Cloud Volumes Service para Google Cloud	Instantâneos	Clones	Conexão múltipla	Qualidade de Serviço	Expandir	Replicação
`gcp-cvs`	Sim	Sim	Sim	Sim	Sim	Disponível apenas no tipo de serviço CVS-Performance.

Notas de replicação

- A replicação não é gerenciada pelo Trident.
- O clone será criado no mesmo pool de armazenamento que o volume de origem.

projeto de classe de armazenamento

É necessário configurar e aplicar classes de armazenamento individuais para criar um objeto de classe de armazenamento do Kubernetes. Esta seção discute como projetar uma classe de armazenamento para sua aplicação.

Utilização específica do backend

A filtragem pode ser usada dentro de um objeto de classe de armazenamento específico para determinar qual pool de armazenamento ou conjunto de pools deve ser usado com essa classe de armazenamento específica. É possível definir três conjuntos de filtros na classe de armazenamento: `storagePools` , `additionalStoragePools` , e/ou `excludeStoragePools` .

O `storagePools` O parâmetro ajuda a restringir o armazenamento ao conjunto de pools que correspondem a quaisquer atributos especificados. O `additionalStoragePools` O parâmetro é usado para estender o conjunto de pools que o Trident usa para provisionamento, juntamente com o conjunto de pools selecionados pelos atributos e `storagePools` parâmetros. Você pode usar qualquer um dos parâmetros individualmente ou ambos em conjunto para garantir que o conjunto apropriado de pools de armazenamento seja selecionado.

O `excludeStoragePools` O parâmetro é usado para excluir especificamente o conjunto listado de pools que correspondem aos atributos.

Emular políticas de QoS

Se você deseja projetar classes de armazenamento para emular políticas de Qualidade de Serviço, crie uma classe de armazenamento com o `media` atributo como `hdd` ou `ssd` . Com base em `media` Com base no atributo mencionado na classe de armazenamento, o Trident selecionará o backend apropriado que atende ao serviço. `hdd` ou `ssd` os agregados correspondem ao atributo de mídia e, em seguida, direcionam o provisionamento dos volumes para o agregado específico. Portanto, podemos criar uma classe de armazenamento PREMIUM que teria `media` atributo definido como `ssd` que poderia ser classificada como a política de QoS PREMIUM. Podemos criar outra classe de armazenamento STANDARD que teria o atributo de mídia definido como `hdd`, o que poderia ser classificado como a política de QoS STANDARD. Também podemos usar o atributo "IOPS" na classe de armazenamento para redirecionar o provisionamento para um dispositivo Element que pode ser definido como uma Política de QoS.

Utilize o backend com base em funcionalidades específicas.

As classes de armazenamento podem ser projetadas para direcionar o provisionamento de volumes em um backend específico, onde recursos como provisionamento fino e espesso, snapshots, clones e criptografia estão habilitados. Para especificar qual armazenamento usar, crie classes de armazenamento que especifiquem o backend apropriado com o recurso necessário habilitado.

Piscinas virtuais

Pools virtuais estão disponíveis para todos os backends do Trident . Você pode definir pools virtuais para qualquer backend, usando qualquer driver fornecido Trident .

Os pools virtuais permitem que um administrador crie um nível de abstração sobre os backends, que podem ser referenciados por meio de classes de armazenamento, para maior flexibilidade e alocação eficiente de volumes nos backends. Diferentes backends podem ser definidos com a mesma classe de serviço. Além disso, é possível criar vários pools de armazenamento no mesmo backend, mas com características diferentes. Quando uma classe de armazenamento é configurada com um seletor contendo rótulos específicos, o Trident escolhe um backend que corresponda a todos os rótulos do seletor para alocar o volume. Se os rótulos do seletor de Classe de Armazenamento corresponderem a vários pools de armazenamento, o Trident escolherá um deles para provisionar o volume.

Projeto de piscina virtual

Ao criar um backend, geralmente é possível especificar um conjunto de parâmetros. Era impossível para o administrador criar outro backend com as mesmas credenciais de armazenamento e um conjunto diferente de parâmetros. Com a introdução de pools virtuais, esse problema foi amenizado. Um pool virtual é uma abstração de nível introduzida entre o backend e a Classe de Armazenamento do Kubernetes para que o administrador possa definir parâmetros junto com rótulos que podem ser referenciados por meio das Classes de Armazenamento do Kubernetes como um seletor, de forma independente do backend. Pools virtuais podem ser definidos para todos os backends NetApp suportados com o Trident. Essa lista inclui SolidFire/ NetApp HCI, ONTAP, Cloud Volumes Service no GCP, bem como Azure NetApp Files.

> Ao definir pools virtuais, recomenda-se não tentar reorganizar a ordem dos pools virtuais existentes em uma definição de backend. Também é recomendável não editar/modificar os atributos de um pool virtual existente e, em vez disso, definir um novo pool virtual.

Emulação de diferentes níveis de serviço/QoS

É possível projetar pools virtuais para emular classes de serviço. Usando a implementação de pool virtual para o Cloud Volume Service para Azure NetApp Files, vamos examinar como podemos configurar diferentes classes de serviço. Configure o backend do Azure NetApp Files com vários rótulos, representando diferentes níveis de desempenho. Definir `servicelevel` Atribua o aspecto ao nível de desempenho apropriado e adicione outros aspectos necessários a cada rótulo. Agora, crie diferentes classes de armazenamento do Kubernetes que serão mapeadas para diferentes pools virtuais. Usando o `parameters.selector` No campo `StorageClass`, cada `StorageClass` especifica quais pools virtuais podem ser usados para hospedar um volume.

Atribuir um conjunto específico de aspectos

É possível projetar vários pools virtuais com um conjunto específico de características a partir de um único backend de armazenamento. Para isso, configure o backend com vários rótulos e defina os aspectos necessários em cada rótulo. Agora, crie diferentes classes de armazenamento do Kubernetes usando o `parameters.selector` campo que mapearia diferentes pools virtuais. Os volumes provisionados no backend terão os aspectos definidos no pool virtual escolhido.

Características do PVC que afetam o fornecimento de armazenamento

Alguns parâmetros além da classe de armazenamento solicitada podem afetar o processo de decisão de provisionamento do Trident ao criar um PVC.

Modo de acesso

Ao solicitar armazenamento por meio de um PVC, um dos campos obrigatórios é o modo de acesso. O modo desejado pode afetar o servidor selecionado para hospedar a solicitação de armazenamento.

O Trident tentará encontrar uma correspondência entre o protocolo de armazenamento utilizado e o método de acesso especificado, de acordo com a seguinte matriz. Isso é independente da plataforma de armazenamento subjacente.

	LerEscreverUmaVez	Somente leitura	LerEscreverMuitos
iSCSI	Sim	Sim	Sim (bloco bruto)
NFS	Sim	Sim	Sim

Uma solicitação de um PVC ReadWriteMany enviada a uma implementação do Trident sem um backend NFS configurado resultará na ausência de provisionamento de volume. Por essa razão, o solicitante deve usar o modo de acesso apropriado para sua aplicação.

Operações de volume

Modificar volumes persistentes

Os volumes persistentes são, com duas exceções, objetos imutáveis no Kubernetes. Uma vez criada, a política de recuperação e o tamanho podem ser modificados. No entanto, isso não impede que alguns aspectos do volume sejam modificados fora do Kubernetes. Isso pode ser desejável para personalizar o volume para aplicações específicas, garantir que a capacidade não seja consumida acidentalmente ou simplesmente mover o volume para um controlador de armazenamento diferente por qualquer motivo.

> Os provisionadores integrados do Kubernetes não suportam operações de redimensionamento de volumes para PVs NFS, iSCSI ou FC neste momento. O Trident suporta a expansão de volumes NFS, iSCSI e FC.

Os detalhes de conexão do sistema fotovoltaico não podem ser modificados após a sua criação.

Criar snapshots de volume sob demanda

O Trident suporta a criação de snapshots de volume sob demanda e a criação de PVCs a partir de snapshots usando a estrutura CSI. Os snapshots fornecem um método conveniente para manter cópias pontuais dos dados e têm um ciclo de vida independente do PV de origem no Kubernetes. Essas imagens podem ser usadas para clonar PVCs.

Criar volumes a partir de snapshots

O Trident também suporta a criação de PersistentVolumes a partir de snapshots de volume. Para fazer isso, basta criar um PersistentVolumeClaim e mencionar o `datasource` como o instantâneo necessário a partir do qual o volume precisa ser criado. O Trident lidará com esse PVC criando um volume com os dados presentes no snapshot. Com esse recurso, é possível duplicar dados entre regiões, criar ambientes de teste, substituir integralmente um volume de produção danificado ou corrompido, ou recuperar arquivos e diretórios

específicos e transferi-los para outro volume conectado.

Mover volumes no cluster

Os administradores de armazenamento têm a capacidade de mover volumes entre agregados e controladores no cluster ONTAP sem interromper o funcionamento do consumidor de armazenamento. Essa operação não afeta o Trident nem o cluster Kubernetes, desde que o agregado de destino seja um ao qual a SVM que o Trident está usando tenha acesso. É importante ressaltar que, se o agregado foi adicionado recentemente ao SVM, o backend precisará ser atualizado, adicionando-o novamente ao Trident. Isso fará com que o Trident reinvente o SVM para que o novo agregado seja reconhecido.

No entanto, a transferência de volumes entre sistemas de backend não é suportada automaticamente pelo Trident. Isso inclui transferências entre SVMs no mesmo cluster, entre clusters diferentes ou para uma plataforma de armazenamento diferente (mesmo que esse sistema de armazenamento esteja conectado ao Trident).

Se um volume for copiado para outro local, o recurso de importação de volume poderá ser usado para importar os volumes atuais para o Trident.

Expandir volumes

O Trident suporta o redimensionamento de PVs NFS, iSCSI e FC. Isso permite que os usuários redimensionem seus volumes diretamente através da camada Kubernetes. A expansão de volume é possível para todas as principais plataformas de armazenamento da NetApp , incluindo ONTAP, SolidFire/ NetApp HCI e backends do Cloud Volumes Service . Para permitir uma possível expansão posterior, defina `allowVolumeExpansion` para `true` na sua StorageClass associada ao volume. Sempre que o Volume Persistente precisar ser redimensionado, edite o `spec.resources.requests.storage` anotação na Solicitação de Volume Persistente referente ao tamanho de volume necessário. O Trident se encarregará automaticamente de redimensionar o volume no cluster de armazenamento.

Importar um volume existente para o Kubernetes

A importação de volumes permite importar um volume de armazenamento existente para um ambiente Kubernetes. Isso é atualmente suportado pelo `ontap-nas` , `ontap-nas-flexgroup` , `solidfire-san` , `azure-netapp-files` , e `gcp-cvs` motoristas. Essa funcionalidade é útil ao migrar um aplicativo existente para o Kubernetes ou em cenários de recuperação de desastres.

Ao usar o ONTAP e `solidfire-san` motoristas, usem o comando `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` Importar um volume existente para o Kubernetes para ser gerenciado pelo Trident. O arquivo PVC YAML ou JSON usado no comando de importação de volume aponta para uma classe de armazenamento que identifica o Trident como o provisionador. Ao usar um backend NetApp HCI/ SolidFire , certifique-se de que os nomes dos volumes sejam exclusivos. Se os nomes dos volumes estiverem duplicados, clone o volume para um nome exclusivo para que o recurso de importação de volumes possa distingui-los.

Se o `azure-netapp-files` ou `gcp-cvs` O driver está sendo usado, use o comando `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` Importar o volume para o Kubernetes para ser gerenciado pelo Trident. Isso garante uma referência de volume única.

Ao executar o comando acima, o Trident localizará o volume no servidor e lerá seu tamanho. Isso adicionará automaticamente (e sobrescreverá, se necessário) o tamanho do volume do PVC configurado. Em seguida, o Trident cria o novo PV e o Kubernetes vincula o PVC ao PV.

Caso um contêiner tenha sido implantado de forma a exigir o PVC importado específico, ele permanecerá em estado pendente até que o par PVC/PV seja vinculado por meio do processo de importação em volume. Após

a união do par PVC/PV, o contêiner deverá subir, desde que não haja outros problemas.

Serviço de registro

A implementação e o gerenciamento do armazenamento para o registro foram documentados em"netapp.io" no"blog" .

Serviço de registro

Assim como outros serviços do OpenShift, o serviço de registro de logs é implantado usando o Ansible com parâmetros de configuração fornecidos pelo arquivo de inventário, também conhecido como hosts, fornecido ao playbook. Serão abordados dois métodos de instalação: a implementação do registro de logs durante a instalação inicial do OpenShift e a implementação do registro de logs após a instalação do OpenShift.

> A partir da versão 3.9 do Red Hat OpenShift, a documentação oficial recomenda não utilizar NFS para o serviço de registro de logs devido a preocupações com a corrupção de dados. Isso se baseia nos testes que a Red Hat fez com seus produtos. O servidor ONTAP NFS não apresenta esses problemas e pode facilmente suportar uma implementação de registro de logs. Em última análise, a escolha do protocolo para o serviço de registro de logs é sua, mas saiba que ambos funcionarão perfeitamente com as plataformas NetApp e não há motivo para evitar o NFS se essa for sua preferência.

Se você optar por usar NFS com o serviço de registro de logs, precisará configurar a variável Ansible. `openshift_enable_unsupported_configurations` para `true` para evitar que o instalador falhe.

Começar

O serviço de registro de logs pode, opcionalmente, ser implementado tanto para aplicativos quanto para as operações principais do próprio cluster OpenShift. Se optar por implementar o registro de operações, especifique a variável. `openshift_logging_use_ops` como `true` Serão criadas duas instâncias do serviço. As variáveis que controlam a instância de registro de operações contêm "ops", enquanto a instância para aplicativos não contém.

Configurar as variáveis do Ansible de acordo com o método de implantação é importante para garantir que o armazenamento correto seja utilizado pelos serviços subjacentes. Vamos analisar as opções para cada um dos métodos de implantação.

> As tabelas abaixo contêm apenas as variáveis relevantes para a configuração de armazenamento relacionada ao serviço de registro de logs. Você pode encontrar outras opções em"Documentação de registro do Red Hat OpenShift" que devem ser revisados, configurados e utilizados de acordo com a sua implementação.

As variáveis na tabela abaixo farão com que o playbook do Ansible crie um PV (Perfil de Variável) e um PVC (Perfil de Variável Contínua) para o serviço de registro de logs, utilizando os detalhes fornecidos. Este método é significativamente menos flexível do que usar o playbook de instalação de componentes após a instalação do OpenShift; no entanto, se você já tiver volumes disponíveis, é uma opção viável.

Variável	Detalhes
`openshift_logging_storage_kind`	Definir para `nfs` Para que o instalador crie um PV NFS para o serviço de registro de logs.

Variável	Detalhes
`openshift_logging_storage_host`	O nome do host ou o endereço IP do host NFS. Este valor deve ser definido como o dataLIF da sua máquina virtual.
`openshift_logging_storage_nfs_directory`	O caminho de montagem para a exportação NFS. Por exemplo, se o volume for dividido como `/openshift_logging` , você usaria esse caminho para essa variável.
`openshift_logging_storage_volume_name`	O nome, por exemplo `pv_ose_logs` , do PV para criar.
`openshift_logging_storage_volume_size`	O tamanho da exportação NFS, por exemplo `100Gi` .

Se o seu cluster OpenShift já estiver em execução e, portanto, o Trident já tiver sido implantado e configurado, o instalador poderá usar o provisionamento dinâmico para criar os volumes. As seguintes variáveis precisarão ser configuradas.

Variável	Detalhes
`openshift_logging_es_pvc_dynamic`	Defina como verdadeiro para usar volumes provisionados dinamicamente.
`openshift_logging_es_pvc_storage_class_name`	O nome da classe de armazenamento que será utilizada no PVC.
`openshift_logging_es_pvc_size`	O tamanho do volume solicitado no PVC.
`openshift_logging_es_pvc_prefix`	Um prefixo para os PVCs usados pelo serviço de registro de dados.
`openshift_logging_es_ops_pvc_dynamic`	Definir para `true` Utilizar volumes provisionados dinamicamente para a instância de registro de operações.
`openshift_logging_es_ops_pvc_storage_class_name`	O nome da classe de armazenamento para a instância de registro de operações.
`openshift_logging_es_ops_pvc_size`	O tamanho da solicitação de volume para a instância de operações.
`openshift_logging_es_ops_pvc_prefix`	Um prefixo para os PVCs da instância de operações.

Implante a pilha de registro de logs.

Se você estiver implementando o registro de logs como parte do processo inicial de instalação do OpenShift, basta seguir o processo de implementação padrão. O Ansible irá configurar e implantar os serviços e objetos do OpenShift necessários para que o serviço esteja disponível assim que o Ansible for concluído.

No entanto, se você estiver realizando a implantação após a instalação inicial, o playbook do componente precisará ser usado pelo Ansible. Este processo pode variar ligeiramente dependendo da versão do OpenShift, portanto, certifique-se de ler e seguir as instruções."Documentação do Red Hat OpenShift Container Platform 3.11" para a sua versão.

Serviço de métricas

O serviço de métricas fornece informações valiosas ao administrador sobre o status, a utilização de recursos e a disponibilidade do cluster OpenShift. Também é necessário para a funcionalidade de dimensionamento automático de pods e muitas organizações usam dados do serviço de métricas para seus aplicativos de cobrança e/ou demonstração de resultados.

Assim como no serviço de registro de logs e no OpenShift como um todo, o Ansible é usado para implantar o serviço de métricas. Assim como o serviço de registro de logs, o serviço de métricas pode ser implantado durante a configuração inicial do cluster ou após sua entrada em operação, utilizando o método de instalação de componentes. As tabelas a seguir contêm as variáveis importantes na configuração do armazenamento persistente para o serviço de métricas.

As tabelas abaixo contêm apenas as variáveis relevantes para a configuração de armazenamento relacionada ao serviço de métricas. Existem muitas outras opções na documentação que devem ser analisadas, configuradas e utilizadas de acordo com a sua implementação.

Variável	Detalhes
`openshift_metrics_storage_kind`	Definir para `nfs` Para que o instalador crie um PV NFS para o serviço de registro de logs.
`openshift_metrics_storage_host`	O nome do host ou o endereço IP do host NFS. Este valor deve ser definido como o dataLIF da sua SVM.
`openshift_metrics_storage_nfs_directory`	O caminho de montagem para a exportação NFS. Por exemplo, se o volume for dividido como `/openshift_metrics` , você usaria esse caminho para essa variável.
`openshift_metrics_storage_volume_name`	O nome, por exemplo `pv_ose_metrics` , do PV para criar.
`openshift_metrics_storage_volume_size`	O tamanho da exportação NFS, por exemplo `100Gi` .

Se o seu cluster OpenShift já estiver em execução e, portanto, o Trident já tiver sido implantado e configurado, o instalador poderá usar o provisionamento dinâmico para criar os volumes. As seguintes variáveis precisarão ser configuradas.

Variável	Detalhes
`openshift_metrics_cassandra_pvc_prefix`	Um prefixo a ser usado para as métricas PVCs.
`openshift_metrics_cassandra_pvc_size`	O tamanho dos volumes a serem solicitados.
`openshift_metrics_cassandra_storage_type`	O tipo de armazenamento a ser usado para métricas; isso deve ser definido como dinâmico para que o Ansible crie PVCs com a classe de armazenamento apropriada.
`openshift_metrics_cassanda_pvc_storage_class_name`	O nome da classe de armazenamento a ser usada.

Implante o serviço de métricas

Com as variáveis Ansible apropriadas definidas no seu arquivo hosts/inventory, implante o serviço usando o Ansible. Se você estiver realizando a implantação durante a instalação do OpenShift, o PV será criado e utilizado automaticamente. Se você estiver realizando a implantação usando os playbooks de componentes, após a instalação do OpenShift, o Ansible cria todos os PVCs necessários e, depois que o Trident provisiona o armazenamento para eles, implanta o serviço.

As variáveis acima, bem como o processo de implantação, podem mudar a cada versão do OpenShift. Certifique-se de revisar e seguir as instruções."Guia de implantação do OpenShift da Red Hat" para a sua versão, de forma que esteja configurada para o seu ambiente.

Proteção de dados e recuperação de desastres

Saiba mais sobre as opções de proteção e recuperação para o Trident e para os volumes criados com o Trident. Você deve ter uma estratégia de proteção e recuperação de dados para cada aplicação que exija persistência.

Replicação e recuperação do Trident

Você pode criar um backup para restaurar o Trident em caso de desastre.

Replicação do Trident

O Trident usa CRDs do Kubernetes para armazenar e gerenciar seu próprio estado e o cluster Kubernetes etcd para armazenar seus metadados.

Passos

1. Faça backup do cluster Kubernetes etcd usando"Kubernetes: Fazendo backup de um cluster etcd" .
2. Coloque os artefatos de backup em um FlexVol volume.

> ⓘ A NetApp recomenda que você proteja a SVM onde o FlexVol reside com uma relação SnapMirror com outra SVM.

Recuperação Trident

Utilizando CRDs do Kubernetes e o snapshot do etcd do cluster Kubernetes, você pode recuperar o Trident.

Passos

1. A partir da SVM de destino, monte o volume que contém os arquivos de dados e certificados do Kubernetes etcd no host que será configurado como nó mestre.
2. Copie todos os certificados necessários referentes ao cluster Kubernetes em `/etc/kubernetes/pki` e os arquivos de membro do etcd em `/var/lib/etcd` .
3. Restaure o cluster Kubernetes a partir do backup do etcd usando"Kubernetes: Restaurando um cluster etcd" .
4. Correr `kubectl get crd` Para verificar se todos os recursos personalizados do Trident foram ativados e recuperar os objetos do Trident para confirmar se todos os dados estão disponíveis.

Replicação e recuperação de SVM

O Trident não consegue configurar relações de replicação; no entanto, o administrador de armazenamento pode usar "ONTAP SnapMirror" para replicar uma SVM.

Em caso de desastre, você pode ativar o SVM de destino do SnapMirror para começar a fornecer dados. Você poderá retornar ao servidor primário quando os sistemas forem restaurados.

Sobre esta tarefa

Ao usar o recurso de replicação SVM do SnapMirror, considere o seguinte:

- Você deve criar um backend distinto para cada SVM com SVM-DR habilitado.
- Configure as classes de armazenamento para selecionar os backends replicados somente quando necessário, evitando assim o provisionamento de volumes que não precisam de replicação nos backends que suportam SVM-DR.
- Os administradores de aplicativos devem compreender o custo e a complexidade adicionais associados à replicação e considerar cuidadosamente seu plano de recuperação antes de iniciar esse processo.

Replicação SVM

Você pode usar"ONTAP: Replicação SnapMirror SVM" para criar a relação de replicação SVM.

O SnapMirror permite que você defina opções para controlar o que será replicado. Você precisará saber quais opções selecionou ao realizar a operação.Recuperação de SVM usando Trident .

- "-preservar identidade verdadeiro"replica toda a configuração da SVM.
- "-descartar-configurações rede"Exclui LIFs e configurações de rede relacionadas.
- "-preservar identidade falso"replica apenas os volumes e a configuração de segurança.

Recuperação de SVM usando Trident

O Trident não detecta automaticamente falhas no SVM. Em caso de desastre, o administrador pode iniciar manualmente o failover do Trident para a nova SVM.

Passos

1. Cancele as transferências SnapMirror agendadas e em andamento, interrompa a relação de replicação, pare o SVM de origem e, em seguida, ative o SVM de destino do SnapMirror .
2. Se você especificou `-identity-preserve false` ou `-discard-config network` Ao configurar a replicação do seu SVM, atualize o `managementLIF` e `dataLIF` no arquivo de definição do backend Trident .
3. Confirmar `storagePrefix` está presente no arquivo de definição do backend Trident . Este parâmetro não pode ser alterado. omitindo `storagePrefix` fará com que a atualização do backend falhe.
4. Atualize todos os backends necessários para refletir o novo nome da SVM de destino usando:

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

5. Se você especificou `-identity-preserve false` ou `discard-config network` Você deve reiniciar todos os pods da aplicação.

Se você especificou `-identity-preserve true` Todos os volumes provisionados pelo Trident começam a fornecer dados quando o SVM de destino é ativado.

Replicação e recuperação de volume

O Trident não consegue configurar relações de replicação SnapMirror ; no entanto, o administrador de armazenamento pode usar"Replicação e recuperação do SnapMirror do ONTAP" para replicar volumes criados pelo Trident.

Em seguida, você pode importar os volumes recuperados para o Trident usando"importação de volume tridentctl" .

A importação não é suportada em `ontap-nas-economy` , `ontap-san-economy` , ou `ontap-flexgroup-economy` motoristas.

Proteção de dados instantâneos

Você pode proteger e restaurar dados usando:

- Um controlador de snapshots externo e CRDs para criar snapshots de volumes persistentes (PVs) do Kubernetes.

  "Instantâneos de volume"

- Os snapshots do ONTAP permitem restaurar todo o conteúdo de um volume ou recuperar arquivos ou LUNs individuais.

  "Capturas instantâneas do ONTAP"

Segurança

Segurança

Utilize as recomendações listadas aqui para garantir a segurança da sua instalação do Trident .

Execute o Trident em seu próprio espaço de nomes.

É importante impedir que aplicativos, administradores de aplicativos, usuários e aplicativos de gerenciamento acessem as definições de objetos do Trident ou os pods para garantir um armazenamento confiável e bloquear possíveis atividades maliciosas.

Para separar os outros aplicativos e usuários do Trident, sempre instale o Trident em seu próprio namespace do Kubernetes.(`trident`). Ao colocar o Trident em seu próprio namespace, garante-se que apenas a equipe administrativa do Kubernetes tenha acesso ao pod do Trident e aos artefatos (como segredos de backend e CHAP, se aplicável) armazenados nos objetos CRD do namespace. Você deve garantir que apenas administradores tenham acesso ao namespace Trident e, portanto, acesso ao… `tridentctl` aplicativo.

Utilize a autenticação CHAP com backends SAN do ONTAP.

O Trident oferece suporte à autenticação baseada em CHAP para cargas de trabalho ONTAP SAN (usando o `ontap-san` e `ontap-san-economy` motoristas). A NetApp recomenda o uso de CHAP bidirecional com Trident para autenticação entre um host e o backend de armazenamento.

Para backends ONTAP que utilizam drivers de armazenamento SAN, o Trident pode configurar CHAP bidirecional e gerenciar nomes de usuário e segredos CHAP através de `tridentctl` . Consulte"Prepare-se para configurar o backend com os drivers ONTAP SAN." Para entender como o Trident configura o CHAP em backends ONTAP .

Utilize a autenticação CHAP com os backends NetApp HCI e SolidFire.

A NetApp recomenda a implementação do CHAP bidirecional para garantir a autenticação entre um host e os backends do NetApp HCI e SolidFire . O Trident utiliza um objeto secreto que inclui duas senhas CHAP por locatário. Quando o Trident é instalado, ele gerencia os segredos CHAP e os armazena em um `tridentvolume` Objeto CR para o respectivo PV. Ao criar um PV, o Trident usa os segredos CHAP para iniciar uma sessão iSCSI e se comunicar com o sistema NetApp HCI e SolidFire via CHAP.

Os volumes criados pelo Trident não estão associados a nenhum Grupo de Acesso a Volumes.

Use Trident com NVE e NAE

O NetApp ONTAP oferece criptografia de dados em repouso para proteger dados confidenciais caso um disco seja roubado, devolvido ou reutilizado. Para mais detalhes, consulte"Visão geral da configuração da criptografia de volume do NetApp" .

- Se o NAE estiver habilitado no backend, qualquer volume provisionado no Trident terá o NAE habilitado.
  - Você pode definir o sinalizador de criptografia NVE para `""` Para criar volumes habilitados para NAE.
- Se o NAE não estiver habilitado no backend, qualquer volume provisionado no Trident terá o NVE habilitado, a menos que o sinalizador de criptografia NVE esteja definido como `false` (o valor padrão) na configuração do backend.

Os volumes criados no Trident em um backend habilitado para NAE devem ser criptografados com NVE ou NAE.

- Você pode definir o sinalizador de criptografia NVE para `true` Na configuração do backend do Trident , é possível substituir a criptografia NAE e usar uma chave de criptografia específica para cada volume.
- Definir o sinalizador de criptografia NVE para `false` Em um backend habilitado para NAE, cria-se um volume habilitado para NAE. Não é possível desativar a criptografia NAE definindo o sinalizador de criptografia NVE como `false` .

- Você pode criar manualmente um volume NVE no Trident definindo explicitamente o sinalizador de criptografia NVE para `true` .

Para obter mais informações sobre as opções de configuração do backend, consulte:

- "Opções de configuração do ONTAP SAN"
- "Opções de configuração do ONTAP NAS"

Configuração Unificada de Chaves do Linux (LUKS)

Você pode habilitar o Linux Unified Key Setup (LUKS) para criptografar volumes ONTAP SAN e ONTAP SAN ECONOMY no Trident. O Trident suporta rotação de senha e expansão de volume para volumes criptografados com LUKS.

No Trident, os volumes criptografados com LUKS usam a cifra e o modo aes-xts-plain64, conforme recomendado por"NIST" .

> A criptografia LUKS não é compatível com sistemas ASA r2. Para obter informações sobre sistemas ASA r2, consulte"Saiba mais sobre os sistemas de armazenamento ASA r2" .

Antes de começar

- Os nós de trabalho devem ter o cryptsetup 2.1 ou superior (mas inferior a 3.0) instalado. Para mais informações, visite"Gitlab: cryptsetup" .
- Por motivos de desempenho, a NetApp recomenda que os nós de trabalho suportem o padrão de criptografia avançada New Instructions (AES-NI). Para verificar a compatibilidade com AES-NI, execute o seguinte comando:

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

  Se nada for retornado, seu processador não suporta AES-NI. Para obter mais informações sobre AES-NI, visite:"Intel: Instruções do Padrão de Criptografia Avançada (AES-NI)" .

Ativar criptografia LUKS

Você pode habilitar a criptografia por volume no lado do host usando o Linux Unified Key Setup (LUKS) para volumes ONTAP SAN e ONTAP SAN ECONOMY.

Passos

1. Defina os atributos de criptografia LUKS na configuração do backend. Para obter mais informações sobre as opções de configuração de backend para ONTAP SAN, consulte"Opções de configuração do ONTAP SAN" .

```
{
  "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 os pools de armazenamento usando criptografia LUKS. Por exemplo:

```
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. Crie um segredo que contenha a senha LUKS. Por exemplo:

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

Limitações

Volumes criptografados com LUKS não podem aproveitar a deduplicação e a compressão do ONTAP .

Configuração de backend para importação de volumes LUKS

Para importar um volume LUKS, você deve configurar `luksEncryption` para(`true` nos bastidores. O `luksEncryption` Essa opção informa ao Trident se o volume é compatível com LUKS.(`true`) ou não compatível com LUKS(`false`) conforme mostrado no exemplo a seguir.

```
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'
```

Configuração de PVC para importação de volumes LUKS

Para importar volumes LUKS dinamicamente, defina a anotação. `trident.netapp.io/luksEncryption` para `true` e inclua uma classe de armazenamento habilitada para LUKS no PVC, conforme mostrado neste exemplo.

```
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
```

Rotacionar uma senha LUKS

Você pode alternar a senha LUKS e confirmar a alternância.

> Não se esqueça de uma senha até verificar se ela não está mais sendo referenciada por nenhum volume, snapshot ou segredo. Caso a senha referenciada seja perdida, você poderá não conseguir montar o volume e os dados permanecerão criptografados e inacessíveis.

Sobre esta tarefa

A rotação da senha LUKS ocorre quando um pod que monta o volume é criado após a especificação de uma nova senha LUKS. Quando um novo pod é criado, o Trident compara a senha LUKS no volume com a senha ativa no segredo.

- Se a senha no volume não corresponder à senha ativa no segredo, ocorrerá a rotação.
- Se a senha no volume corresponder à senha ativa no segredo, o `previous-luks-passphrase` O parâmetro é ignorado.

Passos

1. Adicione o `node-publish-secret-name` e `node-publish-secret-namespace` Parâmetros da classe de armazenamento. Por exemplo:

```
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 as senhas existentes no volume ou no snapshot.

Volume

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

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

Instantâneo

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

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

3. Atualize o segredo LUKS do volume para especificar as senhas novas e anteriores. Garantir `previous-luke-passphrase-name` e `previous-luks-passphrase` A senha corresponde à senha 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. Crie um novo pod para montar o volume. Isso é necessário para iniciar a rotação.
5. Verifique se a senha foi rotacionada.

Volume

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

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

Instantâneo

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

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

Resultados

A senha foi rotacionada quando apenas a nova senha foi retornada no volume e no snapshot.

> Se duas senhas forem retornadas, por exemplo `luksPassphraseNames: ["B", "A"]`, a rotação está incompleta. Você pode acionar um novo módulo para tentar completar a rotação.

Ativar expansão de volume

Você pode habilitar a expansão de volume em um volume criptografado com LUKS.

Passos

1. Ative o `CSINodeExpandSecret` recurso gate (beta 1.25+). Consulte "Kubernetes 1.25: Use segredos para expansão de volumes CSI orientada a nós" para mais detalhes.
2. Adicione o `node-expand-secret-name` e `node-expand-secret-namespace` Parâmetros da classe de armazenamento. Por exemplo:

```
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

Ao iniciar a expansão do armazenamento online, o kubelet passa as credenciais apropriadas para o driver.

Criptografia Kerberos em voo

Ao usar a criptografia Kerberos em trânsito, você pode melhorar a segurança do acesso aos dados, habilitando a criptografia para o tráfego entre seu cluster gerenciado e o backend de armazenamento.

O Trident oferece suporte à criptografia Kerberos para ONTAP como backend de armazenamento:

- * ONTAP local* - O Trident oferece suporte à criptografia Kerberos em conexões NFSv3 e NFSv4 de clusters Red Hat OpenShift e Kubernetes upstream para volumes ONTAP locais.

Você pode criar, excluir, redimensionar, criar snapshots, clonar, clonar em modo somente leitura e importar volumes que utilizam criptografia NFS.

Configure a criptografia Kerberos em trânsito com volumes ONTAP locais.

Você pode habilitar a criptografia Kerberos no tráfego de armazenamento entre seu cluster gerenciado e um backend de armazenamento ONTAP local.

> A criptografia Kerberos para tráfego NFS com backends de armazenamento ONTAP locais só é compatível com o uso do `ontap-nas` driver de armazenamento.

Antes de começar

- Certifique-se de ter acesso ao `tridentctl` utilidade.
- Certifique-se de ter acesso de administrador ao backend de armazenamento do ONTAP .
- Certifique-se de saber o nome do(s) volume(s) que você compartilhará do backend de armazenamento ONTAP .
- Certifique-se de ter preparado a máquina virtual de armazenamento ONTAP para suportar a criptografia Kerberos para volumes NFS. Consulte "Habilitar Kerberos em um dataLIF" para obter instruções.
- Certifique-se de que todos os volumes NFSv4 que você usa com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de Domínio NFSv4 da NetApp (página 13) do manual. "Guia de Aprimoramentos e Melhores Práticas do NetApp NFSv4" .

Adicionar ou modificar políticas de exportação do ONTAP

Você precisa adicionar regras às políticas de exportação ONTAP existentes ou criar novas políticas de exportação que suportem criptografia Kerberos para o volume raiz da VM de armazenamento ONTAP , bem como para quaisquer volumes ONTAP compartilhados com o cluster Kubernetes upstream. As regras de política de exportação que você adicionar, ou as novas políticas de exportação que você criar, precisam ser compatíveis com os seguintes protocolos de acesso e permissões de acesso:

Protocolos de acesso

Configure a política de exportação com os protocolos de acesso NFS, NFSv3 e NFSv4.

Detalhes de acesso

Você pode configurar uma das três versões diferentes de criptografia Kerberos, dependendo das suas necessidades para o volume:

- **Kerberos 5** - (autenticação e criptografia)
- **Kerberos 5i** - (autenticação e criptografia com proteção de identidade)

- **Kerberos 5p** - (autenticação e criptografia com proteção de identidade e privacidade)

Configure a regra de política de exportação do ONTAP com as permissões de acesso apropriadas. Por exemplo, se os clusters forem montar os volumes NFS com uma combinação de criptografia Kerberos 5i e Kerberos 5p, use as seguintes configurações de acesso:

Tipo	Acesso somente leitura	Acesso de leitura/gravação	Acesso de superusuário
UNIX	Habilitado	Habilitado	Habilitado
Kerberos 5i	Habilitado	Habilitado	Habilitado
Kerberos 5p	Habilitado	Habilitado	Habilitado

Consulte a seguinte documentação para obter informações sobre como criar políticas de exportação e regras de política de exportação do ONTAP :

- "Crie uma política de exportação"
- "Adicionar uma regra a uma política de exportação"

Crie um backend de armazenamento

Você pode criar uma configuração de backend de armazenamento Trident que inclua a capacidade de criptografia Kerberos.

Sobre esta tarefa

Ao criar um arquivo de configuração de backend de armazenamento que configura a criptografia Kerberos, você pode especificar uma das três versões diferentes de criptografia Kerberos usando o `spec.nfsMountOptions` parâmetro:

- `spec.nfsMountOptions: sec=krb5`(autenticação e criptografia)
- `spec.nfsMountOptions: sec=krb5i`(autenticação e criptografia com proteção de identidade)
- `spec.nfsMountOptions: sec=krb5p`(autenticação e criptografia com proteção de identidade e privacidade)

Especifique apenas um nível Kerberos. Se você especificar mais de um nível de criptografia Kerberos na lista de parâmetros, somente a primeira opção será utilizada.

Passos

1. No cluster gerenciado, crie um arquivo de configuração de backend de armazenamento usando o seguinte exemplo. Substitua os valores entre colchetes <> por informações do seu ambiente:

```
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. Utilize o arquivo de configuração que você criou na etapa anterior para criar o backend:

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

Se a criação do backend falhar, há algo errado com a configuração do backend. Você pode visualizar os registros para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

Após identificar e corrigir o problema com o arquivo de configuração, você poderá executar o comando de criação novamente.

Criar uma classe de armazenamento

Você pode criar uma classe de armazenamento para provisionar volumes com criptografia Kerberos.

Sobre esta tarefa

Ao criar um objeto de classe de armazenamento, você pode especificar uma das três versões diferentes de criptografia Kerberos usando o `mountOptions` parâmetro:

- `mountOptions: sec=krb5`(autenticação e criptografia)
- `mountOptions: sec=krb5i`(autenticação e criptografia com proteção de identidade)
- `mountOptions: sec=krb5p`(autenticação e criptografia com proteção de identidade e privacidade)

Especifique apenas um nível Kerberos. Se você especificar mais de um nível de criptografia Kerberos na lista de parâmetros, somente a primeira opção será utilizada. Se o nível de criptografia especificado na configuração do backend de armazenamento for diferente do nível especificado no objeto da classe de armazenamento, o objeto da classe de armazenamento terá precedência.

Passos

1. Crie um objeto Kubernetes do tipo StorageClass, utilizando o seguinte exemplo:

```
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. Crie a classe de armazenamento:

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

3. Certifique-se de que a classe de armazenamento foi criada:

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

   Você deverá ver uma saída semelhante à seguinte:

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

volumes de provisão

Após criar um backend de armazenamento e uma classe de armazenamento, você poderá provisionar um volume. Para obter instruções, consulte "Forneça um volume" .

Configure a criptografia Kerberos em trânsito com volumes do Azure NetApp Files.

Você pode habilitar a criptografia Kerberos no tráfego de armazenamento entre seu cluster gerenciado e um único backend de armazenamento do Azure NetApp Files ou um pool virtual de backends de armazenamento do Azure NetApp Files .

Antes de começar

- Certifique-se de ter habilitado o Trident no cluster Red Hat OpenShift gerenciado.
- Certifique-se de ter acesso ao `tridentctl` utilidade.
- Certifique-se de ter preparado o backend de armazenamento do Azure NetApp Files para criptografia Kerberos, observando os requisitos e seguindo as instruções em "Documentação do Azure NetApp Files" .
- Certifique-se de que todos os volumes NFSv4 que você usa com criptografia Kerberos estejam configurados corretamente. Consulte a seção Configuração de Domínio NFSv4 da NetApp (página 13) do manual. "Guia de Aprimoramentos e Melhores Práticas do NetApp NFSv4" .

Crie um backend de armazenamento

Você pode criar uma configuração de back-end de armazenamento do Azure NetApp Files que inclua a capacidade de criptografia Kerberos.

Sobre esta tarefa

Ao criar um arquivo de configuração de backend de armazenamento que configura a criptografia Kerberos, você pode defini-lo para ser aplicado em um dos dois níveis possíveis:

- O **nível de backend de armazenamento** usando o `spec.kerberos` campo
- O **nível da piscina virtual** usando o `spec.storage.kerberos` campo

Ao definir a configuração no nível do pool virtual, o pool é selecionado usando o rótulo na classe de armazenamento.

Em qualquer um dos níveis, você pode especificar uma das três versões diferentes de criptografia Kerberos:

- `kerberos: sec=krb5`(autenticação e criptografia)
- `kerberos: sec=krb5i`(autenticação e criptografia com proteção de identidade)
- `kerberos: sec=krb5p`(autenticação e criptografia com proteção de identidade e privacidade)

Passos

1. No cluster gerenciado, crie um arquivo de configuração de backend de armazenamento usando um dos exemplos a seguir, dependendo de onde você precisa definir o backend de armazenamento (nível de backend de armazenamento ou nível de pool virtual). Substitua os valores entre colchetes <> por informações do seu ambiente:

Exemplo de nível de backend de armazenamento

```
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
```

Exemplo de nível 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. Utilize o arquivo de configuração que você criou na etapa anterior para criar o backend:

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

Se a criação do backend falhar, há algo errado com a configuração do backend. Você pode visualizar os registros para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

Após identificar e corrigir o problema com o arquivo de configuração, você poderá executar o comando de criação novamente.

Criar uma classe de armazenamento

Você pode criar uma classe de armazenamento para provisionar volumes com criptografia Kerberos.

Passos

1. Crie um objeto Kubernetes do tipo StorageClass, utilizando o seguinte exemplo:

```
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. Crie a classe de armazenamento:

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

3. Certifique-se de que a classe de armazenamento foi criada:

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

Você deverá ver uma saída semelhante à seguinte:

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

volumes de provisão

Após criar um backend de armazenamento e uma classe de armazenamento, você poderá provisionar um volume. Para obter instruções, consulte "Forneça um volume" .

Informações sobre direitos autorais

Informações sobre marcas comerciais