Práticas recomendadas e recomendações

Astra Trident

NetApp
December 03, 2024

Índice

Práticas recomendadas e recomendações

Implantação

Use as recomendações listadas aqui quando implantar o Astra Trident.

Implante em um namespace dedicado

"Namespaces" fornecer separação administrativa entre diferentes aplicações e são uma barreira para o compartilhamento de recursos. Por exemplo, um PVC de um namespace não pode ser consumido de outro. O Astra Trident fornece recursos PV para todos os namespaces no cluster do Kubernetes e, consequentemente, utiliza uma conta de serviço que elevou o Privileges.

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

Use cotas e limites de intervalo para controlar o consumo de armazenamento

O Kubernetes tem dois recursos que, quando combinados, fornecem um mecanismo avançado para limitar o consumo de recursos pelas aplicações. O "mecanismo de cota de storage" permite que o administrador implemente limites de consumo globais e específicos de classe de storage, de contagem de objetos e capacidade em uma base por namespace. Além disso, o uso de a "limite de alcance" garante que as solicitações de PVC estejam dentro de um valor mínimo e máximo antes que a solicitação seja encaminhada para o provisionador.

Esses valores são definidos em uma base por namespace, o que significa que cada namespace deve ter valores definidos que se encaixam em seus requisitos de recursos. Consulte aqui para obter informações "como alavancar cotas" sobre .

Configuração de armazenamento

Cada plataforma de storage do portfólio do NetApp tem funcionalidades exclusivas que beneficiam aplicações, em contêineres ou não.

Visão geral da plataforma

O Trident funciona com ONTAP e Element. Não há uma plataforma que seja mais adequada para todos os aplicativos e cenários do que outra, no entanto, as necessidades do aplicativo e da equipe que administra o dispositivo devem ser levadas em conta ao escolher uma plataforma.

Você deve seguir as práticas recomendadas de linha de base para o sistema operacional host com o protocolo que você está utilizando. Opcionalmente, você pode considerar a incorporação de práticas recomendadas de aplicativos, quando disponíveis, com configurações de backend, classe de armazenamento e PVC para otimizar o armazenamento para aplicativos específicos.

Práticas recomendadas de ONTAP e Cloud Volumes ONTAP

Conheça as práticas recomendadas para configurar o ONTAP e o Cloud Volumes ONTAP for Trident.

As recomendações a seguir são diretrizes para configuração do ONTAP para workloads em contêineres, que

consomem volumes provisionados dinamicamente pelo Trident. Cada um deve ser considerado e avaliado quanto à adequação em seu ambiente.

Use SVM(s) dedicados ao Trident

As máquinas virtuais de storage (SVMs) fornecem isolamento e separação administrativa entre locatários em um sistema ONTAP. A dedicação de um SVM a aplicações permite a delegação do Privileges e permite aplicar práticas recomendadas para limitar o consumo de recursos.

Há várias opções disponíveis para o gerenciamento do SVM:

- Fornecer a interface de gerenciamento de cluster na configuração de back-end, juntamente com as credenciais apropriadas, e especificar o nome da SVM.
- Crie uma interface de gerenciamento dedicada ao SVM com o Gerenciador de sistemas do ONTAP ou a CLI.
- Compartilhe a função de gerenciamento com uma interface de dados NFS.

Em cada caso, a interface deve estar em DNS, e o nome DNS deve ser usado ao configurar o Trident. Isso ajuda a facilitar alguns cenários de DR, por exemplo, SVM-DR sem o uso de retenção de identidade de rede.

No entanto, não há preferência entre ter um LIF de gerenciamento dedicado ou compartilhado para o SVM, 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 deve "SVM-DR" ser usado em conjunto com o Trident.

Limite a contagem máxima de volume

Os sistemas de storage ONTAP têm uma contagem de volume máxima, que varia de acordo com a versão do software e a plataforma de hardware. "NetApp Hardware Universe"Consulte para obter a sua plataforma específica e a versão do ONTAP para determinar os limites exatos. Quando a contagem de volume está esgotada, as operações de provisionamento falham não apenas para o Trident, mas para todas as solicitações de storage.

Os Trident `ontap-nas` e `ontap-san` os drivers provisionam um Flexvolume para cada volume persistente (PV) do Kubernetes criado. O `ontap-nas-economy` driver cria aproximadamente um Flexvolume para cada 200 PVS (configurável entre 50 e 300). O `ontap-san-economy` 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 storage, defina um limite para o SVM. Você pode fazer isso a partir da linha de comando:

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

O valor para `max-volumes` varia com base em vários critérios específicos para o seu ambiente:

- O número de volumes existentes no cluster do ONTAP
- O número de volumes que você espera provisionar fora do Trident para outras aplicações
- O número de volumes persistentes esperado para ser consumido pelas aplicações Kubernetes

O `max-volumes` valor é 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 do ONTAP pode ter muito mais ou menos volumes provisionados pelo Trident do que outro nó.

Por exemplo, um cluster ONTAP de dois nós tem a capacidade de hospedar um máximo de 2000 volumes flexíveis. Ter a contagem de volume máxima definida para 1250 parece muito razoável. No entanto, se apenas "agregados" de um nó forem atribuídos à SVM, ou se os agregados atribuídos de um nó não puderem ser provisionados (por exemplo, devido à capacidade), o outro nó se tornará o destino de todos os volumes provisionados pelo Trident. Isso significa que o limite de volume pode ser alcançado para esse nó antes que o `max-volumes` valor seja atingido, resultando em impacto no Trident e em outras operações de volume que usam esse nó. **Você pode evitar essa situação garantindo que os agregados de cada nó no cluster sejam atribuídos ao SVM usado pelo Trident em números iguais.**

Limite o tamanho máximo de volumes criados pelo Trident

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

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

Configure o Trident para usar o CHAP bidirecional

Você pode especificar o iniciador CHAP e os nomes de usuário e senhas de destino em sua definição de back-end e ter o Trident Enable CHAP no SVM. Usando o `useCHAP` parâmetro em sua configuração de back-end, o Trident autentica conexões iSCSI para backends ONTAP com CHAP. O suporte CHAP bidirecional está disponível com o Trident 20,04 e superior.

Criar e usar uma política de QoS SVM

A utilização de uma política de QoS ONTAP aplicada à SVM limita o número de consumíveis de IOPS pelos volumes provisionados pelo Trident. Isso ajuda "evite um bully" a evitar que o volume fora de controle afete workloads fora do SVM do Trident.

Você pode criar uma política de QoS para o SVM em algumas etapas. 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 disponível para o 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 for compatível com ela, considere o uso de um mínimo de QoS para garantir uma taxa de transferência para workloads em contêineres. A QoS adaptável não é compatível com uma política de nível SVM.

O número de IOPS dedicado aos workloads em contêineres depende de muitos aspectos. Entre outras coisas, estas incluem:

- Outros workloads que usam o storage array. Se houver outras cargas de trabalho, não relacionadas à implantação do Kubernetes, utilizando os recursos de storage, deve-se tomar cuidado para garantir que essas cargas de trabalho não sejam acidentalmente afetadas.

- Workloads esperados em execução em contêineres. Se os workloads com requisitos de IOPS altos forem executados em contêineres, uma política de QoS baixa resulta em uma experiência ruim.

É importante lembrar que uma política de QoS atribuída no nível SVM resulta em todos os volumes provisionados ao SVM que compartilham o mesmo pool de IOPS. Se uma, ou um número pequeno, das aplicações em contêiner tiverem um requisito de IOPS alto, isso pode se tornar um bully para os outros workloads em contêiner. Se esse for o caso, você pode considerar o uso de automação externa para atribuir políticas de QoS por volume.

> Você deve atribuir o grupo de políticas de QoS ao SVM **somente** se a versão do ONTAP for anterior a 9,8.

Criar grupos de política de QoS para Trident

A qualidade do serviço (QoS) garante que a performance de workloads essenciais não é degradada pelos workloads da concorrência. Os grupos de política de QoS do ONTAP fornecem opções de QoS para volumes e permitem que os usuários definam o limite máximo de taxa de transferência para um ou mais workloads. Para obter mais informações sobre QoS, "Garantir taxa de transferência com QoS" consulte . É possível especificar grupos de políticas de QoS no back-end ou em um pool de storage, e eles são aplicados a cada volume criado nesse pool ou back-end.

O ONTAP tem dois tipos de grupos de política de QoS: Tradicional e adaptável. Os grupos de políticas tradicionais fornecem uma taxa de transferência máxima fixa (ou mínima, em versões posteriores) em IOPS. O serviço adaptável dimensiona automaticamente a taxa de transferência para o tamanho do workload, mantendo a taxa de IOPS para TBs|GBs conforme o tamanho do workload muda. Isso proporciona uma vantagem significativa ao gerenciar centenas ou milhares de workloads em uma implantação grande.

Considere o seguinte ao criar grupos de política de QoS:

- Você deve definir a `qosPolicy` chave no `defaults` bloco da configuração de back-end. Veja o seguinte exemplo de configuração de 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"
      }
    }
  ]
}
```

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

Para obter mais informações sobre grupos de políticas de QoS, "Comandos de QoS ONTAP 9.8" consulte .

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

Limitar o acesso aos volumes NFS e iSCSI LUNs criados pelo Trident é um componente essencial da postura de segurança para a implantação do Kubernetes. Isso impede que os hosts que não fazem parte do cluster do Kubernetes acessem os volumes e potencialmente modifiquem os dados inesperadamente.

É importante entender que os namespaces são o limite lógico dos recursos no Kubernetes. A suposição é que os recursos no mesmo namespace são capazes de ser compartilhados, no entanto, é importante, não há capacidade entre namespace. Isso significa que, embora os PVS sejam objetos globais, quando vinculados a um PVC, eles só são acessíveis por pods que estão no mesmo namespace. **É fundamental garantir que os namespaces sejam usados para fornecer separação quando apropriado.**

A principal preocupação da maioria das organizações com relação à segurança de dados em um contexto do Kubernetes é que um processo em um contêiner pode acessar o storage montado no host, mas que não se destina ao contêiner. "Namespaces" foram concebidos para evitar este tipo de compromisso. No entanto, há

uma exceção: Contentores privilegiados.

Um contentor privilegiado é aquele que é executado com permissões substancialmente mais no nível do host do que o normal. Estes não são negados por padrão, portanto, certifique-se de desativar a capacidade "diretivas de segurança do pod" usando o .

Para volumes em que o acesso é desejado tanto do Kubernetes quanto de hosts externos, o storage deve ser gerenciado de maneira tradicional, com o PV introduzido pelo administrador e não gerenciado pelo Trident. Isso garante que o volume de storage seja destruído somente quando o Kubernetes e os hosts externos forem desconetados e não estiverem mais usando o volume. Além disso, é possível aplicar uma política de exportação personalizada, que permite o acesso dos nós de cluster do Kubernetes e dos servidores direcionados fora do cluster do Kubernetes.

Para implantações que têm nós de infraestrutura dedicados (por exemplo, OpenShift) ou outros nós que não são agendáveis para 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 de métricas e Registro OpenShift) e aplicativos padrão que são implantados em nós que não são de infraestrutura.

Use uma política de exportação dedicada

Você deve garantir que existe uma política de exportação para cada back-end que permita somente o acesso aos nós presentes no cluster do Kubernetes. O Trident pode criar e gerenciar automaticamente políticas de exportação a partir da versão 20,04. Dessa forma, o Trident limita o acesso aos volumes provisionados por TI aos nós no cluster do Kubernetes e simplifica a adição/exclusão de nós.

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

- Use o `vserver export-policy create` comando ONTAP CLI 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.

`showmount`Desativar o SVM da aplicação

O `showmount` recurso permite que um cliente NFS consulte o SVM para obter uma lista de exportações de NFS disponíveis. Um pod implantado no cluster do Kubernetes pode emitir o `showmount -e` comando contra o LIF de dados e receber uma lista de montagens disponíveis, incluindo aquelas às quais ele não tem acesso. Embora isso, por si só, não seja um compromisso de segurança, ele fornece informações desnecessárias potencialmente ajudando um usuário não autorizado a se conetar a uma exportação NFS.

Você deve desativar `showmount` usando o comando ONTAP CLI no nível da SVM:

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

Práticas recomendadas da SolidFire

Conheça as práticas recomendadas para configurar o armazenamento SolidFire para Trident.

Crie uma conta SolidFire

Cada conta do SolidFire representa um proprietário de volume exclusivo e recebe seu próprio conjunto de credenciais do Protocolo de Autenticação de desafio-aperto (CHAP). Você pode acessar volumes atribuídos a uma conta usando o nome da conta e as credenciais CHAP relativas ou por meio de um grupo de acesso de volume. Uma conta pode ter até dois mil volumes atribuídos a ela, mas um volume pode pertencer a apenas uma conta.

Crie uma política de QoS

Use as políticas de qualidade do serviço (QoS) do SolidFire se quiser criar e salvar uma configuração padronizada de qualidade do serviço que pode ser aplicada a muitos volumes.

Você pode definir parâmetros de QoS em uma base por volume. O desempenho de cada volume pode ser garantido definindo três parâmetros configuráveis que definem a QoS: Min IOPS, Max IOPS e Burst IOPS.

Aqui estão os possíveis valores de IOPS mínimo, máximo e de pico sazonal para o tamanho de bloco 4Kb.

Parâmetro IOPS	Definição	Valor mín	Valor padrão	Valor máximo (4Kb)
IOPS mín	O nível garantido de desempenho para um volume.	50	50	15000
IOPS máx	O desempenho não excederá este limite.	50	15000	200.000
IOPS de explosão	Máximo de IOPS permitido em um cenário de pico curto.	50	15000	200.000

Embora o IOPS máximo e o IOPS Burst possam ser definidos até 200.000 K, o desempenho máximo real de um volume é limitado pelo uso do cluster e pelo desempenho por nó.

O tamanho do bloco e a largura de banda têm uma influência direta no número de IOPS. À medida que os tamanhos de blocos aumentam, o sistema aumenta a largura de banda para um nível necessário para processar os tamanhos de blocos maiores. À medida que a largura de banda aumenta, o número de IOPS que o sistema consegue atingir diminui. Consulte "SolidFire qualidade do serviço" para obter mais informações sobre QoS e desempenho.

Autenticação SolidFire

O Element suporta dois métodos de autenticação: CHAP e volume Access Groups (VAG). O CHAP usa o protocolo CHAP para autenticar o host no back-end. Os grupos de acesso de volume controlam o acesso aos volumes que ele provisiona. O NetApp recomenda usar o CHAP para autenticação, pois é mais simples e não tem limites de escala.

O Trident com o provisionador de CSI aprimorado suporta o uso da autenticação CHAP. Os VAG só devem ser utilizados no modo de funcionamento tradicional não CSI.

A autenticação CHAP (verificação de que o iniciador é o usuário de 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 do SolidFire e o segredo do iniciador. A opção CHAP bidirecional fornece a maneira mais segura de autenticar o volume porque o volume autentica o host através do nome da conta e do segredo do iniciador e, em seguida, o host autentica o volume através do nome da conta e do segredo de destino.

No entanto, se o CHAP não puder ser ativado e os VAG forem necessários, crie o grupo de acesso e adicione os iniciadores e volumes do host ao grupo de acesso. Cada IQN que você adicionar a um grupo de acesso pode acessar cada volume no grupo com ou sem autenticação CHAP. Se o iniciador iSCSI estiver configurado para usar autenticação CHAP, o controle de acesso baseado em conta será usado. Se o iniciador iSCSI não estiver configurado para usar a autenticação CHAP, o controle de acesso ao grupo de acesso de volume será usado.

Onde encontrar mais informações?

Alguns dos documentos de melhores práticas estão listados abaixo. PESQUISE na "Biblioteca NetApp" para as versões mais atuais.

ONTAP

- "Guia de práticas recomendadas e implementação de NFS"
- [Guia de administração DE SAN] (para iSCSI)
- "Configuração iSCSI Express para RHEL"

Software Element

- "Configurando o SolidFire para Linux"

NetApp HCI

- "Pré-requisitos de implantação do NetApp HCI"
- "Acesse o mecanismo de implantação do NetApp"

Informações sobre as melhores práticas de aplicação

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

Nem todos os aplicativos têm diretrizes específicas, é importante trabalhar com sua equipe do NetApp e usar o "Biblioteca NetApp" para encontrar a documentação mais atualizada.

Integre o Astra Trident

Para integrar o Astra Trident, os seguintes elementos de design e arquitetura exigem integração: Seleção e implantação de drivers, design de classe de storage, design de pool de storage virtual, impacto na reivindicação de volume persistente (PVC) no

provisionamento de storage, operações de volume e implantação de serviços OpenShift usando o Astra Trident.

Seleção e implantação do driver

Selecione e implante um driver de back-end para seu sistema de storage.

Drivers de back-end do ONTAP

Os drivers de back-end do ONTAP são diferenciados pelo protocolo usado e pelo modo como os volumes são provisionados no sistema de storage. Portanto, tenha cuidado ao decidir qual driver implantar.

Em um nível mais alto, se seu aplicativo tiver componentes que precisam 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, há pouca diferença entre eles para a maioria dos aplicativos, portanto, muitas vezes a decisão é baseada na necessidade ou não de armazenamento compartilhado (onde mais de um pod precisará de acesso simultâneo).

Os drivers de back-end 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 usados.
- `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 ramificações para os recursos, que são disponibilizados para o aplicativo.

Observe que, nas tabelas abaixo, nem todos os recursos são expostos pelo Astra Trident. Alguns devem ser aplicados pelo administrador de armazenamento após o provisionamento, se essa funcionalidade for desejada. As notas de rodapé sobrescritas distinguem a funcionalidade por recurso e driver.

Drivers nas ONTAP	Instantâneos	Clones	Políticas de exportação dinâmicas	Ligação múltipla	QoS	Redimensionar	Replicação
`ontap-nas`	Sim	Sim	Nota de rodapé:5[]	Sim	Nota de rodapé:1[]	Sim	Nota de rodapé:1[]
`ontap-nas-economy`	Nota de rodapé:3[]	Nota de rodapé:3[]	Nota de rodapé:5[]	Sim	Nota de rodapé:3[]	Sim	Nota de rodapé:3[]
`ontap-nas-flexgroup`	Nota de rodapé:1[]	Não	Nota de rodapé:5[]	Sim	Nota de rodapé:1[]	Sim	Nota de rodapé:1[]

O Astra Trident oferece 2 drivers SAN para ONTAP, cujas funcionalidades são mostradas abaixo.

Controladores SAN ONTAP	Instantâneos	Clones	Ligação múltipla	CHAP bidirecional	QoS	Redimensionar	Replicação
`ontap-san`	Sim	Sim	Nota de rodapé:4[]	Sim	Nota de rodapé:1[]	Sim	Nota de rodapé:1[]
`ontap-san-economy`	Sim	Sim	Nota de rodapé:4[]	Sim	Nota de rodapé:3[]	Sim	Nota de rodapé:3[]

> Nota de rodapé para as tabelas acima: Yesnote:1[]: Não gerenciado por Astra Trident Yesnote:2[]: Gerenciado por Astra Trident, mas não PV granular Yesnote:3[]: Não gerenciado por Astra Trident e não PV granular Yesnote:4[]: Suportado para volumes em bloco bruto Yesnote:5[]: Suportado por CSI Trident

Os recursos que não são granulares PV são aplicados a todo o Flexvolume e todos os PVS (ou seja, qtrees ou LUNs em FlexVols compartilhados) compartilharão um cronograma comum.

Como podemos ver nas tabelas acima, grande parte da funcionalidade entre `ontap-nas` o e `ontap-nas-economy` é a mesma. No entanto, como o `ontap-nas-economy` motorista limita a capacidade de controlar o cronograma em granularidade por PV, isso pode afetar sua recuperação de desastres e Planejamento de backup em particular. Para as equipes de desenvolvimento que desejam utilizar a funcionalidade de clone de PVC no storage ONTAP, isso só é possível ao usar os `ontap-nas` drivers , `ontap-san` ou `ontap-san-economy` .

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

Drivers de back-end do Cloud Volumes ONTAP

O Cloud Volumes ONTAP fornece controle de dados junto a recursos de storage de classe empresarial para vários casos de uso, incluindo compartilhamentos de arquivos e storage em nível de bloco, atendendo aos protocolos nas e SAN (NFS, SMB/CIFS e iSCSI). Os drivers compatíveis para o Cloud volume ONTAP são `ontap-nas`, `ontap-nas-economy` `ontap-san` e `ontap-san-economy`. Eles são aplicáveis ao Cloud volume ONTAP para Azure, Cloud volume ONTAP para GCP.

Drivers de back-end do Amazon FSX para ONTAP

O Amazon FSX for ONTAP permite que os clientes aproveitem os recursos, o desempenho e os recursos administrativos do NetApp com os quais já conhecem, enquanto aproveitam a simplicidade, a agilidade, a segurança e a escalabilidade do armazenamento de dados na AWS. O FSX para ONTAP suporta muitos dos recursos do sistema de arquivos e APIs de administração do ONTAP. Os drivers compatíveis para o Cloud volume ONTAP são `ontap-nas`, `ontap-nas-economy`, `ontap-nas-flexgroup` `ontap-san` e `ontap-san-economy`.

Drivers de back-end NetApp HCI/SolidFire

O `solidfire-san` driver usado com as plataformas NetApp HCI/SolidFire ajuda o administrador a configurar um back-end Element para Trident com base nos limites de QoS. Se você quiser projetar seu back-end para definir os limites de QoS específicos nos volumes provisionados pelo Trident, use o `type` parâmetro no arquivo de back-end. O administrador também pode restringir o tamanho do volume que pode ser criado no

armazenamento usando o `limitVolumeSize` parâmetro. Atualmente, recursos de armazenamento de elementos, como redimensionamento de volume e replicação de volume, não são suportados pelo `solidfire-san` driver. Essas operações devem ser feitas manualmente por meio da IU da Web do Element Software.

Controlador SolidFire	Instantâneos	Clones	Ligação múltipla	CHAP	QoS	Redimensionar	Replicação
`solidfire-san`	Sim	Sim	Nota de rodapé:2[]	Sim	Sim	Sim	Nota de rodapé:1[]

> Nota de rodapé: Yes [1]: Não gerenciado por Astra Trident Yes [2]: Suportado para volumes de blocos brutos

Drivers de back-end do Azure NetApp Files

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

Mais informações sobre esse driver e como configurá-lo podem ser encontradas no "Configuração de back-end do Astra Trident para Azure NetApp Files".

Controlador Azure NetApp Files	Instantâneos	Clones	Ligação múltipla	QoS	Expandir	Replicação
`azure-netapp-files`	Sim	Sim	Sim	Sim	Sim	Nota de rodapé:1[]

> Nota de rodapé: Yes [1]: Não gerenciado pelo Astra Trident

Cloud Volumes Service com drivers de back-end do GCP

O Astra Trident usa `gcp-cvs` o driver para vincular ao Cloud Volumes Service no back-end do GCP. Para configurar o back-end do GCP no Trident, é necessário especificar `projectNumber`, `apiRegion` e `apiKey` no arquivo de back-end. O número do projeto pode ser encontrado no portal da Web do GCP, enquanto a chave da API deve ser retirada do arquivo de chave privada da conta de serviço que você criou ao configurar o acesso à API para o Cloud volumes no GCP. O Astra Trident pode criar volumes CVS em um de dois "tipos de serviço":

1. **CVS**: O tipo de serviço CVS básico, que fornece alta disponibilidade por zonas com níveis de desempenho limitados/moderados.
2. **CVS-Performance**: Tipo de serviço otimizado para desempenho mais adequado para cargas de trabalho de produção que valorizam o desempenho. Escolha entre três níveis de serviço exclusivos [`standard`, , `premium` e `extreme`].

O tamanho mínimo de volume CVS e CVS-Performance é de 100 GiB.

Driver CVS para GCP	Instantâneos	Clones	Ligação múltipla	QoS	Expandir	Replicação
`gcp-cvs`	Sim	Sim	Sim	Sim	Sim	Nota de rodapé:1[]

> Nota de rodapé: Yes [1]: Não gerenciado pelo Astra Trident

O `gcp-cvs` driver usa pools de armazenamento virtual. Os pools de storage virtuais abstraem o back-end, permitindo que o Astra Trident decida o posicionamento do volume. O administrador define os pools de armazenamento virtual no(s) arquivo(s) backend.json. As classes de armazenamento identificam os pools de armazenamento virtual com o uso de rótulos.

Design da classe de armazenamento

As classes de armazenamento individuais precisam ser configuradas e aplicadas para criar um objeto Classe de armazenamento Kubernetes. Esta seção discute como projetar uma classe de armazenamento para seu aplicativo.

Utilização específica no back-end

A filtragem pode ser usada dentro de um objeto de classe de armazenamento específico para determinar qual pool de armazenamento ou conjunto de pools devem ser usados com essa classe de armazenamento específica. Três conjuntos de filtros podem ser definidos na Classe de armazenamento: `storagePools`, `additionalStoragePools` E/ou `excludeStoragePools`.

O `storagePools` parâmetro ajuda a restringir o armazenamento ao conjunto de pools que correspondem a quaisquer atributos especificados. O `additionalStoragePools` parâmetro é usado para estender o conjunto de pools que o Astra Trident usará para provisionar junto com o conjunto de pools selecionados pelos atributos e `storagePools` parâmetros. Você pode usar um parâmetro sozinho ou ambos juntos para garantir que o conjunto apropriado de pools de armazenamento esteja selecionado.

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

Emular políticas de QoS

Se você quiser criar 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 no `media` atributo mencionado na classe de storage, o Trident selecionará o back-end apropriado que serve `hdd` ou `ssd` agrega para corresponder ao atributo de Mídia e direcionará o provisionamento dos volumes para o agregado específico. Portanto, podemos criar uma classe de armazenamento PREMIUM que teria um conjunto de atributos, `ssd` que `media` poderia ser classificado como a política de QoS PREMIUM. Podemos criar outro PADRÃO de classe de armazenamento que teria o atributo de Mídia definido como "hdd", que poderia ser classificado como a política de QoS PADRÃO. 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 back-end com base em recursos específicos

As classes de storage podem ser projetadas para direcionar o provisionamento de volume em um back-end específico, no qual recursos como provisionamento fino e espesso, snapshots, clones e criptografia são ativados. Para especificar qual armazenamento usar, crie classes de armazenamento que especifiquem o back-end apropriado com o recurso necessário habilitado.

Pools de storage virtuais

Os pools de storage virtual estão disponíveis para todos os back-ends Astra Trident. Você pode definir pools de storage virtuais para qualquer back-end, usando qualquer driver fornecido pelo Astra Trident.

Os pools de armazenamento virtual permitem que um administrador crie um nível de abstração sobre backends que pode ser referenciado por meio de classes de armazenamento, para maior flexibilidade e colocação eficiente de volumes em backends. Diferentes backends podem ser definidos com a mesma classe de serviço. Além disso, vários pools de armazenamento podem ser criados no mesmo back-end, mas com caraterísticas diferentes. Quando uma Classe de armazenamento é configurada com um seletor com as etiquetas específicas, o Astra Trident escolhe um back-end que corresponde a todas as etiquetas do seletor para colocar o volume. Se as etiquetas do seletor de classe de storage corresponderem a vários pools de storage, o Astra Trident escolherá um deles para provisionar o volume.

Design do Virtual Storage Pool

Ao criar um backend, você geralmente pode especificar um conjunto de parâmetros. Era impossível para o administrador criar outro back-end com as mesmas credenciais de armazenamento e com um conjunto diferente de parâmetros. Com a introdução de Virtual Storage Pools, esse problema foi aliviado. O Virtual Storage Pools é uma abstração de nível introduzida entre o back-end 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 de back-end. É possível definir pools de storage virtuais para todos os back-ends NetApp compatíveis com o Astra Trident. Essa lista inclui o SolidFire/NetApp HCI, o ONTAP, o Cloud Volumes Service no GCP e o Azure NetApp Files.

> Ao definir pools de armazenamento virtual, recomenda-se não tentar reorganizar a ordem dos pools virtuais existentes em uma definição de back-end. Também é aconselhável não editar/modificar atributos para um pool virtual existente e definir um novo pool virtual.

Emulando diferentes níveis de serviço/QoS

É possível projetar pools de armazenamento virtual para emular classes de serviço. Usando a implementação do pool virtual para o Cloud volume Service for Azure NetApp Files, vamos examinar como podemos configurar diferentes classes de serviço. Configurar o back-end do ANF com várias etiquetas, o que representa diferentes níveis de performance. Defina `servicelevel` Aspect para o nível de desempenho apropriado e adicione outros aspetos necessários em cada rótulo. Agora crie diferentes classes de armazenamento do Kubernetes que mapeariam para diferentes pools de armazenamento virtual. Usando o `parameters.selector` campo, cada StorageClass chama qual(s) pool(s) virtual(s) pode(m) ser usado(s) para hospedar um volume.

Atribuir um conjunto específico de aspetos

Vários pools de storage virtuais com um conjunto específico de aspectos podem ser projetados a partir de um único back-end de storage. Para fazer isso, configure o back-end com vários rótulos e defina os aspetos necessários em cada rótulo. Agora crie diferentes classes de armazenamento do Kubernetes usando o `parameters.selector` campo que mapearia para diferentes pools de armazenamento virtual. Os volumes que são provisionados no back-end terão os aspetos definidos no pool de armazenamento virtual escolhido.

Caraterísticas de PVC que afetam o provisionamento de armazenamento

Alguns parâmetros além da classe de storage solicitada podem afetar o processo de decisão de provisionamento do Astra Trident ao criar uma PVC.

Modo de acesso

Ao solicitar armazenamento através de um PVC, um dos campos obrigatórios é o modo de acesso. O modo desejado pode afetar o back-end selecionado para hospedar a solicitação de armazenamento.

O Astra Trident tentará corresponder ao protocolo de storage usado com o método de acesso especificado de acordo com a matriz a seguir. Isso é independente da plataforma de storage subjacente.

	ReadWriteOnce	ReadOnlyMany	ReadWriteMany
ISCSI	Sim	Sim	Sim (bloco bruto)
NFS	Sim	Sim	Sim

Uma solicitação de um PVC ReadWriteMany enviado para uma implantação do Trident sem um back-end NFS configurado resultará em nenhum volume sendo provisionado. Por esse motivo, o solicitante deve usar o modo de acesso apropriado para sua aplicação.

Operações de volume

Modificar volumes persistentes

Volumes persistentes são, com duas exceções, objetos imutáveis no Kubernetes. Uma vez criados, 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, para garantir que a capacidade não seja consumida acidentalmente ou simplesmente mover o volume para um controlador de armazenamento diferente por qualquer motivo.

> Atualmente, os provisionadores in-tree do Kubernetes não são compatíveis com operações de redimensionamento de volume para PVS NFS ou iSCSI. O Astra Trident é compatível com a expansão de volumes NFS e iSCSI.

Os detalhes de ligação do PV não podem ser modificados após a criação.

Criar snapshots de volume sob demanda

O Astra Trident é compatível com a criação de snapshot de volume sob demanda e a criação de PVCs a partir de snapshots usando a estrutura CSI. Os snapshots fornecem um método conveniente de manter cópias pontuais dos dados e têm um ciclo de vida independente do PV de origem no Kubernetes. Esses snapshots podem ser usados para clonar PVCs.

Criar volumes a partir de instantâneos

O Astra Trident também suporta a criação de PersistentVolumes a partir de instantâneos de volume. Para conseguir isso, basta criar um PersistentVolumeClaim e mencionar o `datasource` como o instantâneo necessário a partir do qual o volume precisa ser criado. O Astra Trident manipulará 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 um volume de produção danificado ou corrompido em sua totalidade, ou recuperar arquivos e diretórios específicos e transferi-los para outro volume anexado.

Mover volumes no cluster

Os administradores de storage podem mover volumes entre agregados e controladores no cluster ONTAP sem interrupções para o consumidor de storage. Essa operação não afeta o Astra Trident nem o cluster Kubernetes, contanto que o agregado de destino seja aquele ao qual o SVM que o Astra Trident está usando tenha acesso. É importante ressaltar que se o agregado tiver sido adicionado recentemente ao SVM, o back-end precisará ser atualizado readicionando-o ao Astra Trident. Isso fará com que o Astra Trident faça o inventário novamente da SVM para que o novo agregado seja reconhecido.

No entanto, a movimentação de volumes entre back-ends não é compatível automaticamente com o Astra Trident. Isso inclui entre SVMs no mesmo cluster, entre clusters ou em uma plataforma de storage diferente (mesmo que esse sistema de storage seja conetado ao Astra Trident).

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

Expanda volumes

O Astra Trident é compatível com o redimensionamento de PVS NFS e iSCSI. Isso permite que os usuários redimensionem seus volumes diretamente pela camada Kubernetes. A expansão de volume é possível para todas as principais plataformas de storage da NetApp, incluindo backends ONTAP, SolidFire/NetApp HCI e Cloud Volumes Service. Para permitir uma possível expansão posterior, defina `allowVolumeExpansion` como `true` no StorageClass associado ao volume. Sempre que for necessário redimensionar o volume persistente, edite a `spec.resources.requests.storage` anotação na reclamação volume persistente para o tamanho de volume pretendido. O Trident cuidará automaticamente do redimensionamento do volume no cluster de armazenamento.

Importar um volume existente para o Kubernetes

A importação de volume permite importar um volume de storage existente para um ambiente Kubernetes. Atualmente, isso é suportado pelos `ontap-nas` drivers , `ontap-nas-flexgroup`, `solidfire-san`, `azure-netapp-files` e `gcp-cvs` . Esse recurso é útil ao portar um aplicativo existente para o Kubernetes ou durante cenários de recuperação de desastres.

Ao usar o ONTAP e `solidfire-san` os drivers, use o comando `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` para importar um volume existente para o Kubernetes para ser gerenciado pelo Astra Trident. O arquivo de PVC YAML ou JSON usado no comando de volume de importação aponta para uma classe de storage que identifica o Astra Trident como o provisionador. Ao usar um back-end NetApp HCI/SolidFire, certifique-se de que os nomes de volume sejam exclusivos. Se os nomes de volume forem duplicados, clone o volume para um nome exclusivo para que o recurso de importação de volume possa distinguir entre eles.

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

Quando o comando acima é executado, o Astra Trident encontrará o volume no back-end e lê seu tamanho. Ele irá adicionar automaticamente (e substituir, se necessário) o tamanho de volume do PVC configurado. Em seguida, o Astra Trident cria o novo PV e o Kubernetes liga o PVC ao PV.

Se um recipiente fosse implantado de modo que fosse necessário o PVC importado específico, ele permaneceria em um estado pendente até que o par PVC/PV seja vinculado através do processo de importação de volume. Depois que o par de PVC / PV são ligados, o recipiente deve surgir, desde que não haja outros problemas.

Implantar serviços OpenShift

Os serviços de cluster de valor agregado do OpenShift fornecem funcionalidade importante aos administradores de cluster e aos aplicativos que estão sendo hospedados. O storage que esses serviços usam pode ser provisionado usando os recursos do nó local. No entanto, isso geralmente limita a capacidade, o desempenho, a capacidade de recuperação e a sustentabilidade do serviço. Ao aproveitar um storage array empresarial para fornecer capacidade a esses serviços, é possível melhorar significativamente o serviço. No entanto, como em todas as aplicações, o OpenShift e os administradores de storage devem trabalhar em

conjunto para determinar as melhores opções para cada um. A documentação da Red Hat deve ser muito utilizada para determinar os requisitos e garantir que as necessidades de dimensionamento e desempenho sejam atendidas.

Serviço de registo

A implantação e o gerenciamento do armazenamento para o Registro foram documentados "NetApp.io" "blog"no .

Serviço de registo

Assim como outros serviços OpenShift, o serviço de log é implantado usando o Ansible com parâmetros de configuração fornecidos pelo arquivo de inventário, também conhecido como hosts, fornecidos ao manual de estratégia. Há dois métodos de instalação que serão abordados: Implantação de logs durante a instalação inicial do OpenShift e implantação de logs após a instalação do OpenShift.

A partir do Red Hat OpenShift versão 3,9, a documentação oficial recomenda contra o NFS para o serviço de log devido a preocupações com a corrupção de dados. Isso é baseado no teste da Red Hat de seus produtos. O servidor NFS da ONTAP não tem esses problemas e pode facilmente fazer backup de uma implantação de log. Em última análise, a escolha do protocolo para o serviço de Registro é sua, apenas saiba que ambos funcionarão muito bem ao usar plataformas NetApp e não há motivo para evitar o NFS se essa for sua preferência.

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

Comece agora

O serviço de log pode, opcionalmente, ser implantado tanto para aplicativos quanto para as operações principais do próprio cluster OpenShift. Se você optar por implantar o Registro de operações, especificando a variável `openshift_logging_use_ops` como `true`, duas instâncias do serviço serão criadas. As variáveis que controlam a instância de log para operações contêm "OPS" nelas, enquanto a instância para aplicativos não.

A configuração das variáveis do Ansible de acordo com o método de implantação é importante para garantir que o storage correto seja utilizado pelos serviços subjacentes. Vamos ver as opções para cada um dos métodos de implantação.

As tabelas abaixo contêm apenas as variáveis que são relevantes para a configuração de armazenamento, uma vez que se refere ao serviço de registo. Você pode encontrar outras opções nas "Documentação de Registro do RedHat OpenShift" quais devem ser revisadas, configuradas e usadas de acordo com sua implantação.

As variáveis na tabela abaixo resultarão no manual do Ansible criando um PV e PVC para o serviço de Registro usando os detalhes fornecidos. Esse método é significativamente menos flexível do que usar o manual de instalação de componentes após a instalação do OpenShift, no entanto, se você tiver volumes existentes disponíveis, é uma opção.

Variável	Detalhes
`openshift_logging_storage_kind`	Defina como `nfs` para que o instalador crie um NFS PV para o serviço de log.

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

Se o cluster do OpenShift já estiver em execução e, portanto, o Trident tiver sido implantado e configurado, o instalador poderá usar o provisionamento dinâmico para criar os volumes. As variáveis a seguir 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 usado 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.
`openshift_logging_es_ops_pvc_dynamic`	Defina como `true` para usar volumes provisionados dinamicamente para a instância de log de operações.
`openshift_logging_es_ops_pvc_storage_class_name`	O nome da classe de armazenamento para a instância de log 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 de instância de OPS.

Implantar a pilha de logs

Se você estiver implantando o log como parte do processo inicial de instalação do OpenShift, então você só precisará seguir o processo de implantação padrão. O Ansible configurará e implantará os serviços necessários e os objetos OpenShift para que o serviço fique disponível assim que o Ansible for concluído.

No entanto, se você estiver implantando após a instalação inicial, o manual de estratégia de componentes precisará ser usado pelo Ansible. Este processo pode mudar ligeiramente com versões diferentes do OpenShift, portanto, certifique-se de ler e seguir "Documentação do RedHat 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 escala automática de

pods e muitas organizações usam dados do serviço de métricas para seus aplicativos de cobrança e/ou exibição.

Assim como no serviço de log e no OpenShift como um todo, o Ansible é usado para implantar o serviço de métricas. Além disso, tal como o serviço de registo, o serviço de métricas pode ser implementado durante uma configuração inicial do cluster ou depois de estar operacional utilizando o método de instalação do componente. As tabelas a seguir contêm as variáveis que são importantes ao configurar o armazenamento persistente para o serviço de métricas.

> As tabelas abaixo contêm apenas as variáveis que são relevantes para a configuração de armazenamento, já que se refere ao serviço de métricas. Há muitas outras opções encontradas na documentação que devem ser revisadas, configuradas e usadas de acordo com sua implantação.

Variável	Detalhes
`openshift_metrics_storage_kind`	Defina como `nfs` para que o instalador crie um NFS PV para o serviço de log.
`openshift_metrics_storage_host`	O nome do host ou endereço IP do host NFS. Isso deve ser definido como o LIF de dados para o SVM.
`openshift_metrics_storage_nfs_directory`	O caminho de montagem para a exportação NFS. Por exemplo, se o volume for juntado como `/openshift_metrics`, você usaria esse caminho para essa variável.
`openshift_metrics_storage_volume_name`	O nome, por exemplo `pv_ose_metrics`, do PV a criar.
`openshift_metrics_storage_volume_size`	O tamanho da exportação NFS, por `100Gi` exemplo .

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

Variável	Detalhes
`openshift_metrics_cassandra_pvc_prefix`	Um prefixo a ser usado para as PVCs de métricas.
`openshift_metrics_cassandra_pvc_size`	O tamanho dos volumes a solicitar.
`openshift_metrics_cassandra_storage_type`	O tipo de storage a ser usado para métricas, isso precisa ser definido como dinâmico para que o Ansible crie PVCs com a classe de storage apropriada.
`openshift_metrics_cassanda_pvc_storage_class_name`	O nome da classe de armazenamento a utilizar.

Implantar o serviço de métricas

Com as variáveis apropriadas do Ansible definidas no arquivo de hosts/inventário, implante o serviço com o Ansible. Se você estiver implantando no horário de instalação do OpenShift, o PV será criado e usado automaticamente. Se você estiver implantando usando os playbooks de componentes, após a instalação do OpenShift, o Ansible criará todos os PVCs necessários e, depois que o Astra Trident provisionou o storage

para eles, implantará o serviço.

As variáveis acima, e o processo de implantação, podem mudar com cada versão do OpenShift. Certifique-se de rever e seguir "Guia de implantação do OpenShift da RedHat" a sua versão para que ela seja configurada para o seu ambiente.

Proteção de dados

Saiba mais sobre as opções de proteção de dados e capacidade de recuperação que as plataformas de storage da NetApp oferecem. O Astra Trident provisiona volumes que podem aproveitar alguns desses recursos. Você deve ter uma estratégia de proteção e recuperação de dados para cada aplicação com um requisito de persistência.

Faça backup dos `etcd` dados do cluster

O Astra Trident armazena seus metadados no banco de dados do cluster do Kubernetes `etcd`. É importante fazer backup periódico `etcd` dos dados do cluster para recuperar clusters do Kubernetes em cenários de desastre.

Passos

1. O `etcdctl snapshot save` comando permite obter um instantâneo pontual do `etcd` cluster:

```
sudo docker run --rm -v /backup:/backup \
  --network host \
  -v /etc/kubernetes/pki/etcd:/etc/kubernetes/pki/etcd \
  --env ETCDCTL_API=3 \
  registry.k8s.io/etcd-amd64:3.2.18 \
  etcdctl --endpoints=https://127.0.0.1:2379 \
  --cacert=/etc/kubernetes/pki/etcd/ca.crt \
  --cert=/etc/kubernetes/pki/etcd/healthcheck-client.crt \
  --key=/etc/kubernetes/pki/etcd/healthcheck-client.key \
  snapshot save /backup/etcd-snapshot.db
```

   Este comando cria um snapshot etcd girando um contentor etcd e salva-o `/backup` no diretório.

2. No caso de um desastre, você pode aumentar um cluster do Kubernetes usando os snapshots do etcd. Use o `etcdctl snapshot restore` comando para restaurar um instantâneo específico levado para a `/var/lib/etcd` pasta. Depois de restaurar, confirme se a `/var/lib/etcd` pasta foi preenchida com a `member` pasta. O seguinte é um exemplo `etcdctl snapshot restore` de comando:

```
etcdctl snapshot restore '/backup/etcd-snapshot-latest.db' ; mv
/default.etcd/member/ /var/lib/etcd/
```

3. Antes de inicializar o cluster do Kubernetes, copie todos os certificados necessários.
4. Crie o cluster com o `--ignore-preflight-errors=DirAvailable—var-lib-etcd` sinalizador.

5. Depois que o cluster aparecer, certifique-se de que os pods do sistema kube foram iniciados.
6. Use o `kubectl get crd` comando para verificar se os recursos personalizados criados pelo Trident estão presentes e recuperar objetos Trident para garantir que todos os dados estejam disponíveis.

Recuperar data usando snapshots ONTAP

Os snapshots desempenham um papel importante fornecendo opções de recuperação pontuais para dados de aplicativos. No entanto, os snapshots não são backups sozinhos, eles não protegem contra falhas no sistema de storage ou outras catástrofes. Mas eles são uma maneira conveniente, rápida e fácil de recuperar dados na maioria dos cenários. Saiba mais sobre como usar a tecnologia de snapshot do ONTAP para fazer backups do volume e como restaurá-los.

- Se a política de snapshot não tiver sido definida no back-end, ela será o padrão de uso da `none` política. Isso faz com que o ONTAP não tire snapshots automáticos. No entanto, o administrador de armazenamento pode tirar instantâneos manuais ou alterar a política de instantâneos através da interface de gerenciamento do ONTAP. Isto não afeta o funcionamento do Trident.
- O diretório instantâneo está oculto por padrão. Isso ajuda a facilitar a compatibilidade máxima dos volumes provisionados usando os `ontap-nas` drivers e `ontap-nas-economy`. Ative o `.snapshot` diretório ao usar os `ontap-nas` drivers e `ontap-nas-economy` para permitir que os aplicativos recuperem dados de snapshots diretamente.
- Restaure um volume para um estado gravado em um instantâneo anterior usando o `volume snapshot restore` comando ONTAP CLI. Quando você restaura uma cópia snapshot, a operação de restauração substitui a configuração de volume existente. Todas as alterações feitas aos dados no volume após a criação da cópia Snapshot são perdidas.

```
cluster1::*> volume snapshot restore -vserver vs0 -volume vol3 -snapshot
vol3_snap_archive
```

Replique dados usando o ONTAP

A replicação de dados pode desempenhar um papel importante na proteção contra perda de dados devido a falha do storage array.

Para saber mais sobre as tecnologias de replicação do ONTAP, consulte o "Documentação do ONTAP".

Replicação de máquinas virtuais de storage (SVM) da SnapMirror

Use "SnapMirror" o para replicar um SVM completo, que inclui suas configurações e volumes. Em caso de desastre, você pode ativar o SVM de destino do SnapMirror para começar a fornecer dados. Você pode voltar para o primário quando os sistemas forem restaurados.

O Astra Trident não pode configurar as relações de replicação por si só. Portanto, o administrador de storage pode usar o recurso replicação do SnapMirror SVM da ONTAP para replicar volumes automaticamente para um destino de recuperação de desastres (DR).

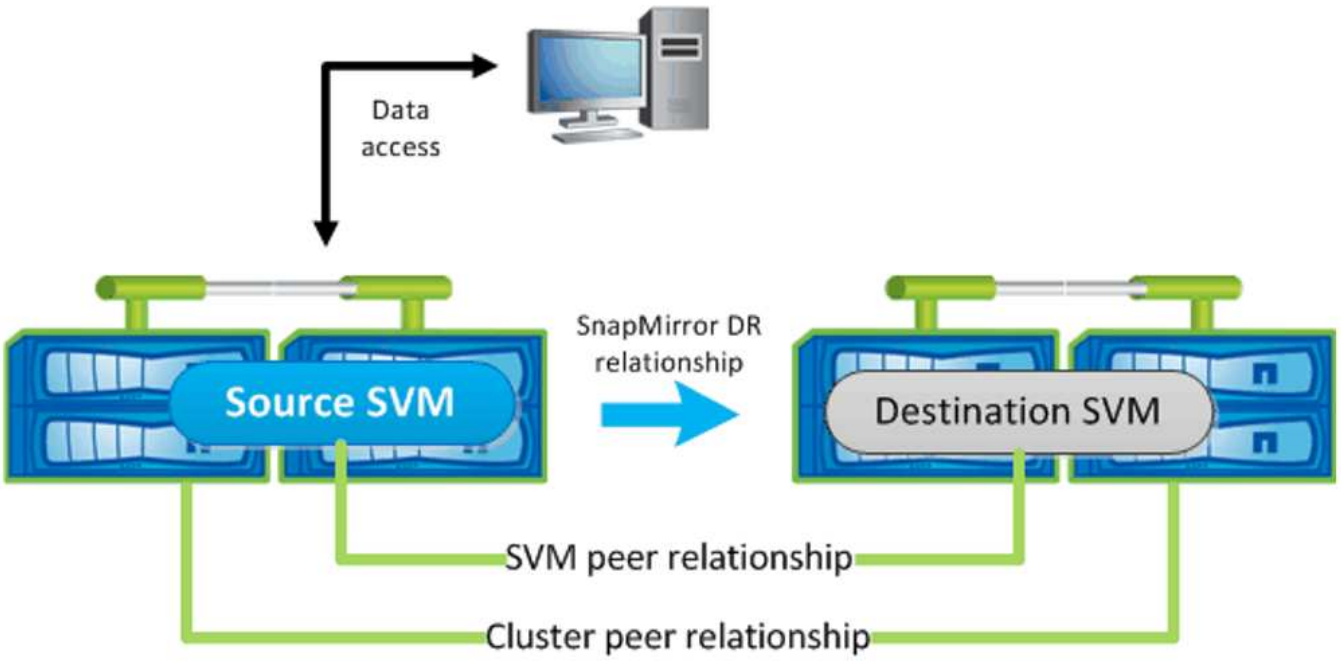
Considere o seguinte caso você esteja planejando usar o recurso replicação do SnapMirror SVM ou esteja usando o recurso atualmente:

- Você deve criar um back-end distinto para cada SVM, que tenha SVM-DR ativado.

- Você deve configurar as classes de armazenamento de modo a não selecionar os backends replicados, exceto quando desejado. Isso é importante para evitar ter volumes que não precisam que a proteção de uma relação de replicação seja provisionada no(s) back(s) que é compatível com a SVM-DR.
- Os administradores de aplicações devem entender o custo e a complexidade adicionais associados à replicação dos dados e um plano de recuperação deve ser determinado antes de utilizar a replicação de dados.
- Antes de ativar o SVM de destino do SnapMirror, interrompa todas as transferências de SnapMirror agendadas, cancele todas as transferências de SnapMirror contínuas, interrompa a relação de replicação, pare a SVM de origem e inicie o SVM de destino do SnapMirror.
- O Astra Trident não detecta automaticamente falhas na SVM. Portanto, após uma falha, o administrador deve executar o `tridentctl backend update` comando para acionar o failover do Trident para o novo back-end.

Aqui está uma visão geral das etapas de configuração da SVM:

- Configure o peering entre o cluster de origem e destino e o SVM.
- Crie o SVM de destino usando a `-subtype dp-destination` opção.
- Crie um agendamento de trabalho de replicação para garantir que a replicação ocorra nos intervalos necessários.
- Crie uma replicação do SnapMirror do SVM de destino para o SVM de origem, usando a `-identity -preserve true` opção para garantir que as configurações de SVM de origem e as interfaces de SVM de origem sejam copiadas para o destino. No SVM de destino, inicialize a relação de replicação do SnapMirror SVM.



Fluxo de trabalho de recuperação de desastres para Trident

O Astra Trident 19,07 e versões posteriores usam CRDs do Kubernetes para armazenar e gerenciar seu próprio estado. Ele usa os clusters do Kubernetes `etcd` para armazenar seus metadados. Aqui assumimos que os arquivos de dados do Kubernetes `etcd` e os certificados são armazenados no NetApp Flexvolume. Esse Flexvolume reside em uma SVM, que tem uma relação SnapMirror SVM-DR com um SVM de destino no

local secundário.

As etapas a seguir descrevem como recuperar um único cluster mestre do Kubernetes com o Astra Trident em caso de desastre:

1. Se o SVM de origem falhar, ative o SVM de destino do SnapMirror. Para fazer isso, você deve interromper as transferências agendadas do SnapMirror, cancelar as transferências contínuas do SnapMirror, interromper a relação de replicação, parar o SVM de origem e iniciar o SVM de destino.
2. No SVM de destino, monte o volume que contém os arquivos de dados e certificados do Kubernetes `etcd` no host, que será configurado como um nó mestre.
3. Copie todos os certificados necessários referentes ao cluster do Kubernetes em `/etc/kubernetes/pki` e os arquivos etcd `member` em `/var/lib/etcd`.
4. Crie um cluster do Kubernetes usando o `kubeadm init` comando com o `--ignore-preflight-errors=DirAvailable—var-lib-etcd` sinalizador. Os nomes de host usados para os nós do Kubernetes devem ser os mesmos que o cluster de origem do Kubernetes.
5. Execute o `kubectl get crd` comando para verificar se todos os recursos personalizados do Trident foram criados e recuperar os objetos Trident para verificar se todos os dados estão disponíveis.
6. Atualize todos os backends necessários para refletir o novo nome SVM de destino executando o `./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>` comando.

> Para volumes persistentes de aplicações, quando o SVM de destino é ativado, todos os volumes provisionados pelo Trident começam a fornecer dados. Depois que o cluster do Kubernetes for configurado no lado do destino usando as etapas descritas acima, todas as implantações e pods são iniciados e as aplicações em contêiner devem ser executadas sem problemas.

Replicação de volume SnapMirror

A replicação de volume ONTAP SnapMirror é um recurso de recuperação de desastres que permite o failover para o storage de destino do storage primário em um nível de volume. O SnapMirror cria uma réplica de volume ou espelhamento do storage primário no storage secundário sincronizando snapshots.

Aqui está uma visão geral das etapas de configuração da replicação de volume do ONTAP SnapMirror:

- Configure o peering entre os clusters nos quais os volumes residem e os SVMs que atendem dados dos volumes.
- Crie uma política SnapMirror, que controla o comportamento da relação e especifica os atributos de configuração para essa relação.
- Crie uma relação SnapMirror entre o volume de destino e o volume de origem usando o[`snapmirror create` comando…] e atribua a política SnapMirror apropriada.
- Depois que a relação SnapMirror for criada, inicialize a relação de modo que uma transferência de linha de base do volume de origem para o volume de destino seja concluída.

Fluxo de trabalho de recuperação de desastres do volume SnapMirror para Trident

As etapas a seguir descrevem como recuperar um único cluster mestre do Kubernetes com o Astra Trident.

1. Em caso de desastre, pare todas as transferências SnapMirror programadas e aborte todas as transferências SnapMirror em curso. Quebre a relação de replicação entre o destino e os volumes de origem para que o volume de destino seja leitura/gravação.
2. No SVM de destino, monte o volume que contém os arquivos de dados e certificados do Kubernetes `etcd` no host, que será configurado como nó principal.
3. Copie todos os certificados necessários referentes ao cluster do Kubernetes em `/etc/kubernetes/pki` e os arquivos etcd `member` em `/var/lib/etcd`.
4. Crie um cluster do Kubernetes executando o `kubeadm init` comando com o `--ignore-preflight-errors=DirAvailable—var-lib-etcd` sinalizador. Os nomes de host devem ser os mesmos que o cluster de origem do Kubernetes.
5. Execute o `kubectl get crd` comando para verificar se todos os recursos personalizados do Trident foram criados e recuperam objetos do Trident para se certificar de que todos os dados estão disponíveis.
6. Limpe os backends anteriores e crie novos backends no Trident. Especifique o novo LIF de dados e gerenciamento, o novo nome da SVM e a senha do SVM de destino.

Fluxo de trabalho de recuperação de desastres para volumes persistentes da aplicação

As etapas a seguir descrevem como os volumes de destino do SnapMirror podem ser disponibilizados para workloads em contêineres em caso de desastre:

1. Pare todas as transferências SnapMirror programadas e aborte todas as transferências SnapMirror em curso. Quebre a relação de replicação entre o destino e o volume de origem para que o volume de destino se torne leitura/gravação. Limpe as implantações que estavam consumindo PVC vinculado a volumes na SVM de origem.
2. Depois que o cluster do Kubernetes for configurado no lado do destino usando as etapas descritas acima, limpe as implantações, PVCs e PV, do cluster do Kubernetes.
3. Crie novos backends no Trident especificando o novo gerenciamento e LIF de dados, o novo nome do SVM e a senha do SVM de destino.

4. Importe os volumes necessários como um PV vinculado a um novo PVC usando o recurso de importação Trident.
5. Reimplante as implantações de aplicativos com os PVCs recém-criados.

Recuperar dados usando snapshots do Element

Faça backup dos dados em um volume de elemento definindo uma programação de instantâneos para o volume e garantindo que os instantâneos sejam obtidos nos intervalos necessários. Você deve definir a programação de snapshot usando a IU ou APIs do Element. Atualmente, não é possível definir um agendamento instantâneo para um volume através `solidfire-san` do controlador.

No caso de corrupção de dados, você pode escolher um snapshot específico e reverter o volume para o snapshot manualmente usando a IU ou APIs do elemento. Isso reverte todas as alterações feitas no volume desde que o snapshot foi criado.

Segurança

Use as recomendações listadas aqui para garantir a segurança da instalação do seu Astra Trident.

Execute o Astra Trident em seu próprio namespace

É importante impedir que aplicações, administradores de aplicações, usuários e aplicações de gerenciamento acessem as definições de objetos do Astra Trident ou os pods para garantir um storage confiável e bloquear atividades maliciosas em potencial.

Para separar as outras aplicações e usuários do Astra Trident, instale sempre o Astra Trident em seu próprio namespace Kubernetes (`trident`). A colocação do Astra Trident em seu próprio namespace garante que apenas o pessoal administrativo do Kubernetes tenha acesso ao pod Astra Trident e aos artefatos (como segredos de back-end e CHAP, se aplicável) armazenados nos objetos CRD com namespaces. Você deve garantir que somente os administradores acessem o namespace Astra Trident e, assim, o acesso `tridentctl` à aplicação.

Use a autenticação CHAP com backends ONTAP SAN

O Astra Trident é compatível com autenticação baseada em CHAP para workloads SAN ONTAP (usando os `ontap-san` drivers e `ontap-san-economy`). A NetApp recomenda o uso de CHAP bidirecional com Astra Trident para autenticação entre um host e o back-end de storage.

Para backends ONTAP que usam os drivers de armazenamento SAN, o Astra Trident pode configurar CHAP bidirecional e gerenciar nomes de usuário e segredos do CHAP por meio `tridentctl`do . Veja "aqui" para entender como o Astra Trident configura o CHAP nos backends do ONTAP.

O suporte CHAP para backends ONTAP está disponível com o Trident 20,04 e posterior.

Use a autenticação CHAP com backends NetApp HCI e SolidFire

O NetApp recomenda a implantação de CHAP bidirecional para garantir a autenticação entre um host e os backends NetApp HCI e SolidFire. O Astra Trident usa um objeto secreto que inclui duas senhas CHAP por locatário. Quando o Trident é instalado como um provisionador CSI, ele gerencia os segredos CHAP e os armazena em um `tridentvolume` objeto CR para o respetivo PV. Quando você cria um PV, o CSI Astra

Trident usa os segredos CHAP para iniciar uma sessão iSCSI e se comunicar com o sistema NetApp HCI e SolidFire através do CHAP.

> Os volumes criados pelo CSI Trident não estão associados a nenhum Grupo de Acesso por volume.

No frontend não-CSI, a vinculação de volumes como dispositivos nos nós de trabalho é tratada pelo Kubernetes. Após a criação de volume, o Astra Trident faz uma chamada de API para o sistema NetApp HCI/SolidFire para recuperar os segredos se o segredo para esse locatário ainda não existir. Em seguida, o Astra Trident passa os segredos para o Kubernetes. O kubelet localizado em cada nó acessa os segredos por meio da API do Kubernetes e os usa para executar/habilitar o CHAP entre cada nó acessando o volume e o sistema NetApp HCI/SolidFire onde os volumes estão localizados.

Use o Astra Trident com NVE e NAE

O NetApp ONTAP fornece criptografia de dados em repouso para proteger dados confidenciais caso um disco seja roubado, retornado ou reutilizado. Para obter detalhes, "Configurar a visão geral da encriptação de volume do NetApp"consulte .

- Se o NAE estiver ativado no back-end, qualquer volume provisionado no Astra Trident será habilitado para NAE.
- Se o NAE não estiver habilitado no back-end, qualquer volume provisionado no Astra Trident será habilitado para NVE, a menos que você defina o sinalizador de criptografia NVE como `false` na configuração de back-end.

> Os volumes criados no Astra Trident em um back-end habilitado para NAE devem ser criptografados com NVE ou NAE.
>
> - Você pode definir o sinalizador de criptografia NVE como `true` na configuração de back-end do Trident para substituir a criptografia NAE e usar uma chave de criptografia específica por volume.
> - Definir o sinalizador de criptografia NVE como `false` em um back-end habilitado para NAE criará 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 Astra Trident definindo explicitamente o sinalizador de criptografia NVE como `true`.

Para obter mais informações sobre opções de configuração de back-end, consulte:

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

Habilite a criptografia por volume no lado do host usando o Linux Unified Key Setup (LUKS)

Você pode ativar o LUKS (configuração de chave unificada do Linux) para criptografar volumes DE ECONOMIA SAN ONTAP e SAN ONTAP no Astra Trident. No Astra Trident, os volumes criptografados por LUKS usam a cifra e o modo aes-xts-plain64, conforme recomendado "NIST"pelo .

Para obter mais informações sobre opções de configuração de back-end para SAN ONTAP, consulte "Opções de configuração de SAN ONTAP"

Antes de começar

- Os nós de trabalho devem ter o cryptsetup 2,1 ou superior instalado. Para obter mais informações, visite "Gitlab: Cryptsetup".
- Por motivos de desempenho, recomendamos que os nós de trabalho suportem Advanced Encryption Standard New Instructions (AES-NI). Para verificar o suporte ao AES-NI, execute o seguinte comando:

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

Se nada for devolvido, o processador não suporta AES-NI. Para obter mais informações sobre o AES-NI, visite: "Intel: Advanced Encryption Standard Instructions (AES-NI)".

Passos

1. Defina atributos de criptografia LUKS na configuração de back-end.

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

2. Use `parameters.selector` para definir os pools de armazenamento usando a criptografia LUKS. Por exemplo:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
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 frase-passe LUKS. Por exemplo:

```
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
```

Limitações

- Os volumes criptografados LUKS não poderão aproveitar a deduplicação e a compactação do ONTAP.
- Neste momento, a rotação da frase-passe LUKS não é suportada. Para alterar senhas, copie manualmente os dados de um PVC para outro.

Informações sobre direitos autorais

Informações sobre marcas comerciais